



State, Local, Tribal, and Territorial Cyber Information Sharing Program: Pilot Project Overview

Fiscal Years 2018, 2019, and 2020

March 8, 2021

Fiscal Year 2020 Report to Congress



**Homeland
Security**

*Cybersecurity and Infrastructure Security
Agency*

Message from the Director of the Cybersecurity and Infrastructure Security Agency

March 8, 2021

I am pleased to present the following report, “State, Local, Tribal, and Territorial Cyber Information Sharing Program: Pilot Project Overview” for Fiscal Years (FY) 2018, 2019, and 2020, which has been prepared by the Cybersecurity and Infrastructure Security Agency (CISA).



This document has been compiled pursuant to direction in the Joint Explanatory Statement, which accompanies the FY 2018 Department of Homeland Security (DHS) Appropriations Act (P.L. 115-141); Senate Report 115-283, which accompanies the FY 2019 DHS Appropriations Act (P.L. 116-6); and Senate Report 116-125, which accompanies the FY 2020 DHS Appropriations Act (P.L. 116-93). Included is an overview.

Pursuant to congressional requirements, this document is being provided to the following Members of Congress:

The Honorable Lucille Roybal-Allard
Chairwoman, House Appropriations Subcommittee on Homeland Security

The Honorable Chuck Fleischmann
Ranking Member, House Appropriations Subcommittee on Homeland Security

The Honorable Christopher S. Murphy
Chairman, Senate Appropriations Subcommittee on Homeland Security

The Honorable Shelley Moore Capito
Ranking Member, Senate Appropriations Subcommittee on Homeland Security

Inquiries relating to this report may be directed to CISA Legislative Affairs at (202) 819-2612.

Sincerely,

A handwritten signature in black ink, appearing to read "B. Wales".

Brandon Wales
Acting Director
Cybersecurity and Infrastructure Security Agency

Executive Summary

CISA established the State, Local, Tribal, and Territorial (SLTT) Cyber Information Sharing Program to foster a more resilient SLTT cyber ecosystem. Cooperative agreements were awarded in accordance with congressional direction to meet the project objectives set by CISA and to execute the project using a standardized process. Each pilot project includes the development of deliverables (e.g., guidance documents, best practices, etc.) that SLTT governments can adopt to meet their unique needs and constraints.

The Joint Explanatory Statement accompanying the FY 2018 DHS Appropriations Act (P.L. 115-141) directs CISA to provide a report on the results of a pilot program to explore and evaluate the most effective methods for cybersecurity information sharing. In 2018, the Los Angeles Cyber Lab, Inc. (LACL), was awarded \$2,992,863 to execute the first pilot to establish a fully functional Internet Security – Information Sharing and Analysis Organization (IS-ISAO) that can perform information sharing and analysis of cybersecurity threats, as well as can gather and disseminate information among the public and private sectors. For 21 months, LACL sought ways to overcome the obstacles that have been associated with cyber threat intelligence sharing by creating an IS-ISAO, by establishing a threat intelligence sharing platform, by launching a mobile application, and by engaging with more than 800 organizations and 2,000 individuals. LACL made noticeable progress against its key performance metrics by addressing membership growth and sector diversity.

Pursuant to Senate Report 115-283, this report also outlines the results of another pilot titled, “State, Local, Tribal, and Territorial Indicators of Compromise – Automation Pilot” in FY 2019. In 2019, the Johns Hopkins University Applied Physics Laboratory (JHU/APL) was awarded \$1,986,791 to pilot ways to apply automation to enhance the speed and evaluation of cyber threat indicators of compromise (IOC) at the state and local government levels. JHU/APL successfully met every objective of the pilot and demonstrated the ability to act upon the IOCs within minutes of receipt. The findings of this pilot will benefit the entire state, local, tribal, and territorial (SLTT) community.

In addition to the above-mentioned completed pilots, this report summarizes ongoing pilot projects. This includes funding that was awarded in FY 2019 to conduct the “SLTT Reporting and Threat Information Sharing Pilot,” and in FY 2020 to conduct the “SLTT National Information Exchange Model Cyber Pilot” and the “SLTT High Value Asset Pilot.” A summary of the findings from each remaining pilot will be presented in separate reports upon completion of each project.



State, Local, Tribal, and Territorial Information Sharing Program: Pilot Project Overview Fiscal Years 2018, 2019, and 2020

Table of Contents

I.	Congressional Language.....	1
	FY 2018 Congressional Language.....	1
	FY 2019 Congressional Language.....	1
	FY 2020 Congressional Language.....	1
II.	Background.....	3
III.	CISA’s State, Local, Tribal, and Territorial Cyber Information Sharing Program	4
	Internet Security – Information Sharing and Analysis Organization Pilot Program	4
	SLTT Indicators of Compromise – Automation Pilot	5
	SLTT Reporting and Threat Information Sharing Pilot.....	5
	SLTT National Information Exchange Model – Cyber Pilot	5
	SLTT High Value Asset Pilot.....	6
	Conclusion	6
IV.	Analysis of Completed Pilot Projects	7
	Internet Security – Information Sharing and Analysis Organization Pilot Program	7
	Overview.....	7
	Analysis	8
	Considerations	10
	State, Local, Tribal, and Territorial Indicators of Compromise – Automation Pilot.....	11
	Overview.....	11
	Analysis	12
	Considerations	13

V. Conclusion	15
Appendices.....	16
Appendix A: List of Abbreviations	16
Appendix B: Internet Security – Information Sharing and Analysis Organization Pilot Program Report	
Appendix C: State, Local, Tribal, and Territorial Indicators of Compromise – Automation Pilot Report	

I. Congressional Language

FY 2018 Congressional Language

The Joint Explanatory Statement that accompanies the Fiscal Year (FY) 2018 Department of Homeland Security (DHS) Appropriations Act (P.L. 115-141) includes the following requirement¹:

Of the total provided, \$3,000,000 is for the establishment of pilot programs to explore and evaluate the most effective methods for cybersecurity information sharing, focusing on regional information sharing; communications and outreach; training and education; and research and development for the improvement of SLTT government capabilities and capacity. NPPD is directed to provide a report on the results of each pilot not later than 270 days after its completion.

FY 2019 Congressional Language

Senate Report 115-283, which accompanies the FY 2019 DHS Appropriations Act (P.L. 116-6), states:

Cyber Readiness and Response.—Of the total provided, \$3,000,000 is for the continuation of pilot programs to explore and evaluate the most effective methods for cybersecurity information sharing, focusing on regional information sharing; communications and outreach; training and education; and research and development for the improvement of SLTT government capabilities and capacity. NPPD is directed to provide a report on the results of each pilot not later than 270 days after its completion.

FY 2020 Congressional Language

Senate Report 116-125, which accompanies the FY 2020 DHS Appropriations Act (P.L. 116-93), states:

Regional Information Sharing.—Of the total provided, \$3,000,000 is recommended to award grants or cooperative agreements to sustain or conduct new pilot programs to explore and evaluate the most effective methods for cybersecurity information sharing, focusing on regional information sharing; communications and outreach;

¹ Section 2202(a)(2) of the Homeland Security Act, as amended by the Cybersecurity and Infrastructure Security Agency Act of 2018 (P.L. 115-278), states that “Any reference to the National Protection and Programs Directorate of the Department in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Cybersecurity and Infrastructure Security Agency of the Department.” As such, the Joint Explanatory Statements’ reference to the National Protection and Programs Directorate (NPPD) as well as all other statutory references to NPPD contained in this document apply to the Cybersecurity and Infrastructure Security Agency (CISA).

training and education; and research and development for the improvement of SLTT government capabilities and capacity. CISA is directed to provide a report on the results of each pilot not later than 180 days after its completion.

II. Background

CISA is the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build a more secure and resilient infrastructure for the future. The threats that the Nation faces—digital and physical, man-made, technological, and natural—are more complex, and the threat actors are more diverse than at any point in our history. CISA is at the heart of mobilizing a collective defense as it leads the Nation's efforts to understand and manage risk to its critical infrastructure.

CISA's partners in this mission span the public and private sectors, and the programs and services that CISA provides are driven by its comprehensive understanding of the risk environment and the corresponding needs identified by its stakeholders. CISA seeks to help organizations to manage risk better and to increase resilience using all available resources, whether provided by the Federal Government, commercial vendors, or their own capabilities.

CISA builds the national capacity to defend against cyberattacks and works with the Federal Government to provide cybersecurity tools, incident response services, and assessment capabilities to safeguard the “.gov” networks that support the essential operations of partner departments and agencies.

CISA also coordinates security and resilience efforts using trusted partnerships across the private and public sectors and delivers technical assistance and assessments to federal stakeholders as well as to infrastructure owners and operators nationwide. In addition, CISA delivers insights on these assessments related to current capabilities to identify gaps, which—along with an examination of emerging technologies—help to determine the demand for future capabilities (both near- and long-term).

CISA enhances public safety interoperable communications at all levels of government to help partners across the country to develop their emergency communications capabilities. Working with stakeholders across the country, CISA conducts extensive, nationwide outreach to support and promote the ability of emergency response providers and relevant government officials to continue to communicate in the event of a natural disaster, act of terrorism, or other man-made disaster.

III. CISA’s State, Local, Tribal, and Territorial Cyber Information Sharing Program

Established in 2018, the CISA State, Local, Tribal, and Territorial (SLTT) Cyber Information Sharing Program conducts individual pilots to evaluate ways to improve cyber information sharing with and between SLTT agencies. CISA identifies critical issues facing the SLTT community and conducts individual, short-term (12 to 24 months) projects to pilot solutions. Cooperative agreements are awarded to a variety of organizations, each with specialized abilities to meet the unique requirements of each pilot. The findings are used to develop guidance documents, best practices, key considerations, models, processes, and procedures that SLTT agencies can adapt and modify to fit their resource constraints and operational needs. This effort provides tested solutions that SLTT agencies can apply themselves.

This is part of a self-service approach whereby findings are shared nationally so that SLTT agencies can apply them as they see fit. The layered approach complements direct assistance provided by CISA and indirect assistance by CISA sponsors via the Multi-State Information Sharing and Analysis Center (MS-ISAC). The information derived from individual pilot projects also informs products and services provided by CISA and MS-ISAC.

The following summarizes completed and ongoing pilot projects.

Internet Security – Information Sharing and Analysis Organization Pilot Program

In FY 2018, CISA awarded a 1-year² cooperative agreement to the Los Angeles Cyber Lab, Inc. (LACL), to establish the Internet Security – Information Sharing and Analysis Organization (IS-ISAO). The pilot program was established to explore and evaluate the most effective methods for bilateral cybersecurity information sharing, focusing on regional information sharing, communications and outreach, training and education, and research and development for the improvement of SLTT government capabilities and capacity. The IS-ISAO developed the full capability to perform information sharing and analysis of cybersecurity threats and to gather and disseminate government and critical infrastructure information.

The intent of the IS-ISAO Pilot Program was to establish a fully functional ISAO capable of bi-directional information sharing. Also, the pilot promoted and developed a collaboration with SLTT agencies, higher education, industry, and not-for-profit organizations and conducted government outreach. The IS-ISAO will maintain a data center that will allow for the reception storage of cyber threat information and artifacts, analysis programs and platforms, and interconnectivity with information-sharing and analysis centers or other information-sharing organizations.

² The original length of the cooperative agreement was 1 year, and three 3-month extensions were granted for a total period of performance of 21 months.

SLTT Indicators of Compromise – Automation Pilot

All types of organizations need to be able to share information and to respond to cyber risk in as close to real time as possible. In September 2019, CISA awarded a 1-year cooperative agreement to the Johns Hopkins University Applied Physics Laboratory (JHU/APL) to conduct a pilot project with SLTT governments to apply automation to enhance and speed the evaluation of cyber threat indicators of compromise (IOC) at the state and local government levels. JHU/APL conducted the pilot project with four states—Arizona, Louisiana, Massachusetts, and Texas—and partnered with MS-ISAC. The SLTT IOC Automation Pilot identified key areas for potential reduction of manual tasks by humans and actionable information sharing across SLTT enterprises, as well as identified orchestration services needed to integrate the activities of sensing, understanding, decision-making, and acting with respect to cyber threats.

The intent of the pilot effort was to use Security Orchestration, Automation, and Response (SOAR) concepts to develop a network-defender threat intelligence feed at MS-ISAC, to export indicators from the pilot feed in Structured Threat Integration Expression (STIX)/Trusted Automated Exchange of Intelligence Information (TAXII) format, and to use SOAR platforms to respond to those indicators at four state partners with different architectures and operational procedures. The pilot focused on both the curation of the feed as well as the processes used by the SLTT participants to triage, prioritize, and act upon the resultant IOCs. The results and findings of the pilot are contained in this report.

SLTT Reporting and Threat Information Sharing Pilot

In September 2019, CISA entered a 1-year cooperative agreement with the Cybercrime Support Network (CSN) to establish an SLTT Cyber Reporting and Threat Information Sharing Pilot project, related to individuals' and small-to-medium-sized businesses' (SMB) cyber incidents. The Reporting and Threat Information Sharing Pilot project provides SLTT governments with greater visibility of threats affecting their communities and allows law enforcement agencies to respond better to otherwise unreported cyber incidents. The pilot project also identified a standardized list of resources that could be provided to victims of cyber incidents. CISA and CSN also partnered with the Center for Internet Security and the Mississippi State University National Strategic Planning and Analysis Research Center. The project was extended an additional year, and the findings will be presented in a separate report once finalized.

SLTT National Information Exchange Model – Cyber Pilot

In September 2020, CISA entered a 2-year cooperative agreement with CSN to test ways to increase the adoption and utilization of the National Information Exchange Model (NIEM) Cyber Domain across SLTT agencies. NIEM is a common vocabulary that enables efficient information exchange across diverse public and private organizations. NIEM connects communities of people who share a common need to exchange information in order to advance their mission. NIEM has facilitated information exchanges across a variety of mission spaces and subject areas. What began as a solution for the law enforcement and homeland security communities since has evolved into a wide range of subject matters and areas. CISA is building

on these community efforts by facilitating the implementation of the NIEM Cyber Model to enhance data and information exchanges through the NIEM Cyber Domain. The project is ongoing, and the findings will be presented in a separate report once finalized.

SLTT High Value Asset Pilot

In September 2020, CISA entered into a 2-year cooperative agreement with the University of Texas at San Antonio to test ways that SLTT agencies can identify, categorize, and prioritize their high value assets (HVA) in order to protect those assets from compromise better. HVAs are assets that are so critical to an organization that the loss of access to or corruption of these assets would have a serious impact on the organization's ability to perform its mission or to conduct business functions. The pilot will provide guidelines, templates, and tools. The project is ongoing, and the findings will be presented in a separate report once finalized.

Conclusion

Through cooperative agreements, CISA is utilizing pilot projects to build capacity and to provide solutions to defend and protect against cyberattacks at the SLTT government level for a more resilient SLTT cyber ecosystem. The SLTT pilot projects deliver guidance, best practices, model processes, and workflows among other things that SLTT governments can adapt for their own needs and constraints.

IV. Analysis of Completed Pilot Projects

The following section provides an overview, analysis of findings, and considerations for the two pilots completed thus far: the Internet Security – Information Sharing and Analysis Organization Pilot Program (see Appendix B) and the SLTT Indicators of Compromise – Automation Pilot (see Appendix C).

Internet Security – Information Sharing and Analysis Organization Pilot Program

Overview

The purpose of the pilot project was to establish the IS-ISAO to explore and evaluate the most effective methods for bilateral cybersecurity information sharing, focusing on regional information sharing, communications and outreach, training and education, and research and development for the improvement of SLTT government capabilities and capacity. The IS-ISAO developed the full capability to perform information sharing and analysis of cybersecurity threats and to gather and disseminate government and critical infrastructure information, for the purpose of:

- Cyber threat analysis and information sharing,
- Education, training, and workforce development,
- Promotion and development of a collaboration,
- Technical research and development to support effective information sharing, and
- Shared best practices.

Through a competitive process, the cooperative agreement was awarded to LACL, a 501(c)3 California Nonprofit Public Benefit Corporation formed in August 2017 for \$2,992,863. No additional funds were added to this cooperative agreement during the 21-month period of performance (October 1, 2018, through June 30, 2020)³, and all funds were expended following the guidelines provided with the notice of the cooperative agreement award.

The following objectives and key performance metrics were established for the pilot program:

No.	Objectives	Performance Metrics
1	Bilateral Cybersecurity Information Sharing	Explore the most effective methods for bilateral cybersecurity information sharing, focusing on regional information sharing, communications and outreach, training and education, and research and development for the improvement of SLTT government capabilities and capacity.

³ The original length of the cooperative agreement was 1 year, and three 3-month extensions were granted for a total period of performance of 21 months.

No.	Objectives	Performance Metrics
2	Establish Fully Functional IS-ISAO	Establish a fully functional IS-ISAO that can allow real-time or near-real-time sharing of cyber threat information between IS-ISAO and the CISA National Infrastructure Coordinating Center.
3	Identify Barriers to Information Sharing	Identify barriers to cyber information sharing in CISA’s Automated Information Sharing and how to incentivize SLTT agencies to share with both the government and one another to improve the collective defense posture of the Nation and key private-sector entities.
4	Develop Documentation	Develop documentation including design, policies and procedures, concept of operations, and operations manuals.
5	Work with Academic Partners	Work with academic partners who will utilize the IS-ISAO operation center to provide real-world learning environments to improve student skills and to identify research opportunities for students and faculty to explore the full spectrum of cyber technology.
6	Cyber Work Force Development	Develop hands-on cyber workforce development programs in collaboration with academia.

CISA exercised substantial programmatic involvement throughout this cooperative agreement. This included monitoring project progress; providing technical assistance; disapproving and approving subprojects, workplans, or modifications thereto; holding kickoff meetings; conducting biennial reviews; and conducting programmatic reviews.

Analysis

The core initiative of this pilot was to establish a fully functional IS-ISAO to exchange cyber threat intelligence (CTI) across and between private and public sectors. The pilot created collaborative, real-time identification and analysis of regional threats and shared threat data with businesses of all sizes, SLTT governments, and CISA. In addition to identifying barriers to information sharing, LACL performed extensive outreach activities including offering research and development opportunities for academia, workforce development opportunities and career training for entry-level cyber professionals, and innovative conferences and events for all stakeholders.

The pilot project successfully established a fully functional IS-ISAO with bilateral information sharing registered with the International Information Sharing Standards Organization. The effort to create the IS-ISAO was a lengthy process of identifying CTI use cases, partners, and members, and defining requirements and operationalizing the information-sharing process. LACL developed a request for proposal (RFP) and solicited the private sector for technical assistance in creating a means by which LACL could create a CTI sharing community. The process of developing the RFP, selecting a vendor, and executing a contract took 11 months.

Work based on the project began in June 2019 with informal agreements in place between LACL, International Business Machines Corporation, and The Rosslyn Group. The original RFP intended to create a platform capable of completing a full cycle of intelligence and dissemination to members. Through the RFP review and interview process, LACL identified an opportunity to connect with SMBs through a mobile application.

To address the barriers to information sharing and to improve the collective defense, the pilot project developed a mobile application over a 90-day timeline in the summer of 2019. The mobile application is the primary means by which LACL engages SMBs and individuals. The mobile application was built to be a vital connection between SMBs and the greater business community; this pilot may be the first time when enterprise-level CTI has been used as a data source that links SMBs. Managed security services provide some access to SMBs but no direct link or access to higher level CTI. The functionality of the mobile application was designed through a series of small SMB focus groups in conjunction with the LACL team.

The pilot project engaged academic institutions in a variety of ways to explore information-sharing opportunities. The pilot worked with each academic institution to identify unique assets, potential for collaboration, and the audience that these groups served. The pilot explored creating courses in cybersecurity, certificate programs, undergraduate- and graduate-level research projects, and leadership seminars. Ultimately, the pilot abandoned creating courses and certificate programs because of time and resource constraints. Success was achieved with academic partners in two ways: participating in business school cybersecurity seminars and in supporting student learning through hands-on access to CTI via the LACL Threat Intelligence Sharing Platform (TISP).

Outreach activities were constant and consistent throughout the performance period. LACL spoke at local business leader forums and conferences, held an SLTT meeting, hosted several speaker series discussions, and hosted a hands-on analyst training with the National Cyber Forensics Training Agency. These events were successful in bringing many new connections to LACL. The intent was to drive interest toward the Security Summit and to increase information sharing through the daily threat report.

LACL raised its social media profile by hosting training sessions at the Security Summit. The Security Summit increased participants' knowledge and awareness of cyber threats in the region. LACL hosted four 1-hour training sessions throughout the 2-day summit, and two of the training sessions were standing room only. The training sessions were included at the Security Summit at no additional cost. The training topics included: Wireshark, Cyber Analyst Incident/Information Management, Data Breach Incident Tabletop Exercise, and Red Team Hacking.

LACL created a series of products and documents that are available to anyone, at no charge, and are designed to engage the community in a variety of forms. Connecting the community, LACL designed these offerings to reach targeted audiences, to help to educate recipients, and to facilitate partnerships across the region. Below is a list of LACL products and services.

LACL Services:

- Anti-Phishing Analysis and Cybersecurity Threat News via the LACL mobile application,
- Threat Intelligence via the LACL TISP through either an application programming interface (API) or STIX/TAXII feed available to members, and
- Threat intelligence and reports via the LACL TISP for partners and members with access to the platform. Analysts are able to submit or work with data to create cases for IOCs, and analysts can provide feedback to the community about ongoing threats and can request assistance through the platform.

LACL Products:

- Daily Threat Report: a daily emailed list of information and physical security events in the news.
- Daily IOC Report: a daily emailed link to two comma-separated value documents, one including DHS threat data and one including City of Los Angeles threat data.
- Weekly Threat Report: a weekly emailed list of security events in the news covering agriculture, defense, energy, financial information, insurance, healthcare, legal information, litigation, regulatory risk, operational risk, pharmaceutical data, reputational risk, and retail and technology sectors.
- Ad Hoc and Special Report: Ad hoc emails are sent only when a specific information security risk is identified; typically, this communication contains immediate/near real-time threat information and actions that businesses should consider. Special reports are an emailed PDF attachment containing information about either major events or significant information security issues.

Considerations

The intent of the IS-ISAO Pilot Project was to create a regional CTI sharing model to serve as an example for other cities to emulate, on the basis of the cities' own needs and available resources. Specifically, the results of the pilot could export the ISAO model and could leverage the threat TISP to connect regions. Many regions are working toward a coordinated approach, and this will build on those efforts, will promote local innovation, and will ensure national interoperability.

Creating the IS-ISAO was a lengthy process of identifying CTI use cases, partners, and members, and of defining requirements and operationalizing the information-sharing process. Sustaining a regional ISAO poses a real challenge for large metropolitan areas. The pilot taught that without a public-private partnership or without implementing a fee-for-service model such as memberships or crowdsourcing, a regional IS-ISAO can be difficult to sustain long term.

The pilot identified that trust and privacy considerations are critical parts of the information-sharing process and are fundamental to the success of the ISAO, in which information sharing is voluntary and based on trust. Moreover, the improper disclosure of such information could cause harm to individuals, companies, and others and could be in violation of applicable laws

and regulations. As a result, a regional ISAO should consider the privacy implications of information that it is considering sharing, such as personal information about a specific individual; whether or not that information is related directly to a cybersecurity threat; and, if not, whether that information has been removed. The pilot did draw from ISAO Standards Organization guidelines that help to address privacy concerns when sharing information.

The pilot identified that the project was perceived as being affiliated with the City of Los Angeles, leading private sectors to believe that information shared with LACL also would be shared with other parts of the City. Future efforts to establish a regional ISAO should make it clear that an ISAO is a nonprofit organization and not a government entity.

State, Local, Tribal, and Territorial Indicators of Compromise – Automation Pilot

Overview

In FY 2019, CISA awarded a cooperative agreement to execute the SLTT Indicators of Compromise – Automation Pilot. The purpose of the pilot was to apply the usage of automation to enhance and speed the evaluation of threat IOCs at the state and local government levels. In addition, the pilot identified key areas for potential reduction of manual tasks and improved actionable information sharing across enterprises and SLTT agencies. The pilot also identified orchestration services needed to integrate the activities of sensing, understanding, decision-making, and acting.

Through a competitive process, the cooperative agreement was awarded to JHU/APL with the value of \$1,986,791. During the 1-year period of performance (September 30, 2019, through September 30, 2020), all funds were expended following the guidelines provided in the notice of the cooperative agreement award.

The pilot project focused on developing model processes, methods, and accompanying policies and procedures that can be applied by SLTT agencies to accomplish the following:

- Act upon IOCs within minutes of receipt;
- Reduce the time spent on repetitive tasks;
- Provide generation, enrichment, and scoring of IOCs;
- Receive, remediate, and respond to IOCs;
- Demonstrate the use of SOAR operational procedures and capabilities combined with information sharing to make data more actionable and to enable consistent execution across SLTT levels; and
- Develop repeatable processes for orchestration and automation services that bridge existing SLTT policies with SOAR capabilities.

CISA and JHU/APL selected the following four SLTT pilot partners:

- Arizona (Department of Administration and Maricopa County),

- Louisiana (Division of Administration),
- Massachusetts (Executive Office of Technology Services and Security), and
- Texas (Department of Information Resources and Department of Public Safety).

CISA exercised substantial programmatic involvement throughout the cooperative agreement. This included monitoring project progress; providing technical assistance; disapproving and approving subprojects, workplans, or modifications thereto; holding kickoff meetings; conducting biennial reviews; and conducting programmatic reviews.

Analysis

JHU/APL successfully met every objective of the pilot as specified by CISA and collected all data available for the analysis of metrics requested in the notice of funding opportunity. To achieve the SLTT IOC Automation Pilot objectives, CISA and JHU/APL used a four-phase approach:

- Discovery Phase to select pilot partners and to identify the pilot scope;
- Design Phase to collaborate with pilot partners and to create pilot workflows;
- Execution Phase to implement pilot technology on partner production networks and to collect data; and
- Analysis and Reporting Phase to analyze and report the findings of the pilot.

It is important to note that the performance period for this pilot effort was only 1 year. CISA and JHU/APL had to select candidates from the 7,000-member MS-ISAC SLTT community, create a new feed for threat intelligence, identify a transition partner for the feed, develop six enterprise security integration environments, create dozens of workflows, and transition those workflows as well as the feed to operations. To accomplish this successfully, it was determined that a threat feed provider and three SLTT partners were needed. However, after the Discovery Phase was completed, CISA added the Commonwealth of Massachusetts as a single security use case using orchestration as a proof-of-concept given the Massachusetts manual process.

The first objective of the pilot was to demonstrate the ability to act upon IOCs within minutes of receipt. The automation at the MS-ISAC receives IOCs from Intrusion Detection System alerts as well as submissions to the Malicious Code Analysis Platform. Once received, the pilot automation processes these IOCs within an average time of 42 seconds and distributes them to the pilot TAXII server within an additional 30 seconds. Therefore, action not only was initiated but was completed in shortly more than 1 minute. Once an SLTT pilot partner received an IOC from the TAXII feed, the automated actions began, on average, within 2 seconds of receipt and took a total of 98 seconds, on average, to complete. The fact that this automation could provide IOCs rapidly instead of as a weekly publication gave the SLTT organization the opportunity to block potential cyberattacks proactively before an adversary pivots to target that organization after attacking another of the 7,000 SLTT organizations that participate in the MS-ISAC community.

The second objective was to reduce the time spent on repetitive tasks. The pilot performance demonstrated a substantial reduction in the time spent on repetitive tasks. There was a reduction

in the overall process from 4,086 minutes to 3 minutes when comparing the manual and automated processes. This is due to automation that can run in the background and that does not require a human to complete repetitive tasks during the workweek. Even factoring in the substantial amount of time spent on waiting for a human to review an automated prompt, the pilot still demonstrated more than an eightfold speed improvement over the manual process.

The third objective, through the creation of the pilot threat feed, was to generate, enrich, and score the IOCs. The threat feed produced for the SLTT Indicators of Compromise Automation Pilot project is a completely new set of IOCs derived from MS-ISAC data using a low-regret strategy. This unique strategy is based on determining the likelihood of operational impact to an organization if it responds to an IOC. The regret determination and sharing processes are fully automated, and the score provided is used by the receiving sites to determine response actions in an automated fashion.

The fourth objective was to develop workflows for SLTT partner organizations to receive, remediate, and respond to IOCs. The primary method of response to an IOC was to block it. IOCs received by SLTT partners were blocked, but 99 percent of the IOCs had no history on the network and thus were safe to block without disrupting operations. This means that, although the low-regret nature of the feed was preserved, the pilot partners were still able to maintain control of their own policy and chose only to block IOCs that they could confirm as truly malicious.

The fifth and final objective of the pilot was successful deployment of SOAR workflows with four states using various platforms across the SOAR marketplace. Each of the pilot states had a favorable response to the use of SOAR and looks to continue usage of the technology.

Considerations

The pilot proved to be overwhelmingly successful in speeding up the evaluation of IOCs, dramatically increasing the ability of pilot participants to protect their networks from potentially malicious activity. Furthermore, the participants will continue to use SOAR and security automation. Some already have begun to research and develop expanded use cases to leverage the capability identified in the pilot. Additionally, several participants are looking to expand the use of the capability from the pilot either within their states or to provide examples for other states interested in using SOAR. Additionally, the MS-ISAC found distinct value in the automated low-regret feed of IOCs and has transitioned the technology into a production offering. The MS-ISAC is working toward making the threat feed available to its 7,000+ members.

There were technical challenges to users using TAXII clients and servers. None of the pilot partners had much experience using TAXII for the retrieval of IOCs from MS-ISAC. When investigating vendor-based tools, CISA and JHU/APL discovered that critical STIX fields from the IOCs with respect to the regret score were overwritten by the vendor without notification. The use of separate polling scripts and command line-based clients became necessary to ensure that partners received the threat intelligence feed with all the information needed. Although the pilot provided documentation to support the use of these tools, it places a significant burden on

the Security Operations Center (SOC) staff of organizations utilizing TAXII. Alternative distribution methods for IOCs that provide a less complex interface than TAXII may be needed to make information more accessible to the greater SLTT community.

The number of data sources, products, and services deployed in enterprise environments continues to increase as does the number of these capabilities used by SOC personnel to perform different functions (e.g., investigation, remediation). Maintaining accurate insight into the current versions, functionality, licensing restrictions, and organizationwide usage is not a simple matter, especially when different parts of the organization manage different resources and different aspects of the lifecycle for a resource. Every pilot partner had at least one product or service identified for a use case that was either the wrong version, was unable to provide the necessary feature/function in an automated manner, violated vendor usage restrictions, or did not support local policies properly as encoded in the workflow. It is critical that any organization investing in SOAR capabilities has up-to-date information about any resource accessed as part of an automated workflow to include exact versions, licensing restrictions, local policy/usage restrictions, and API functionality. It is also important to consider the ability to automate (e.g., API functionality, integration support) as part of the procurement/acquisition process for external products/services and the requirements/development process for internal products and applications.

The SLTT IOC Automation Pilot represented different levels of interactions with existing processes at different partner locations. In some cases, completely new processes were designed and implemented. In most, steps in existing manual processes were automated, and a ticketing or tracking tool was used to manage the touch points between new tasks and current operations. In every case, a significant amount of time was spent in understanding the current state and in designing the automation to ensure minimal negative impact to ongoing operations and manageable interactions with operators. As organizations implement automation and orchestration in their environments, they need to make sure that there is a plan to implement, monitor, refine, and extend these automation workflows. In particular, they need to ensure that deployment and testing/validation do not have a negative impact on existing operations/operators and that extended automation does not require a redesign of the workflow. Essentially, it is recommended to build with the expectation of full automation and then to add simple touchpoints using existing capabilities whenever possible.

CISA received a considerable number of deliverables and insights from the pilot and is planning to continue making industry guides and best practices available to the entire SLTT community as well as to other members of the critical infrastructure community:

- Differentiating between automation and orchestration,
- Guidance on the best way to enable automation and orchestration in an operational environment,
- Making manual processes supportive of automation,
- CTI triage techniques,
- Sharing courses of action and alternative CTI sharing techniques, and
- Understanding the value of various CTI within the malware lifecycle.

V. Conclusion

The two pilots conducted under the CISA SLTT Cyber Information Sharing Program thus far have tested ways to improve cyber information sharing with and between SLTT agencies. Executed by organizations with specialized abilities to meet the unique requirements of each pilot, the findings have been used to help the broader SLTT community to improve its capabilities. The pilots have produced guidance documents, best practices, key considerations, models, processes, and procedures that SLTT agencies can adapt and modify to fit their resource constraints and operational needs. This effort provides CISA with the flexibility to develop rapidly tested solutions that SLTT agencies can apply themselves.

Appendices

Appendix A: List of Abbreviations

Abbreviation	Definition
API	Application Programming Interface
CISA	Cybersecurity and Infrastructure Security Agency
CSN	Cybercrime Support Network
CTI	Cyber Threat Intelligence
DHS	Department of Homeland Security
FY	Fiscal Year
HVA	High Value Asset
IOC	Indicator of Compromise
IS-ISAO	Internet Security – Information Sharing and Analysis Organization
JHU/APL	Johns Hopkins University Applied Physics Laboratory
LACL	Los Angeles Cyber Lab, Inc.
MS-ISAC	Multi-State Information Sharing and Analysis Center
NIEM	National Information Exchange Model
NPPD	National Protection and Programs Directorate
RFP	Request for Proposal
SLTT	State, Local, Tribal, and Territorial
SMB	Small-to-Medium Business
SOAR	Security Orchestration, Automation, and Response
SOC	Security Operations Center
STIX	Structured Threat Integration Expression
TAXII	Trusted Automated Exchange of Intelligence Information
TISP	Threat Intelligence Sharing Platform

**Appendix B: Internet Security – Information Sharing and Analysis
Organization Pilot Program Report**

FINAL REPORT

Internet Security – Information Sharing and Analysis
Organization (IS-ISAO) Pilot Program 18PDSA000002



Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

Protection Through Partnership

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

Report date	Project Name	Submitted by
March 31, 2020	Internet Security – Information Sharing and Analysis Organizations (IS-ISAO) Pilot - 2018	<p>Joshua Belk <i>Executive Director, LA Cyber Lab</i> jbelk@lacyberlab.org 213-978-3125</p> <p>Christopher Covino <i>Project Lead & Grant Representative</i> christopher.m.covino@lacity.org 213-978-0689</p>

PROGRESS REPORTING PERIOD	FEDERAL AGENCY	RECIPIENT ORGANIZATION
October 1, 2019 – March 31, 2020	U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA)	Los Angeles Cyber Lab, Inc. 200 N Spring Street, STE 303 Los Angeles, CA 90012-3239

GRANT PERIOD	FEDERAL GRANT	DUNS & EIN
September 30, 2018 – March 31, 2020	18PDSAO00002	<p>DUNS - 081371107</p> <p>EIN - 83182160</p>

This report was prepared by the Los Angeles Cyber Lab, Inc. in cooperation with the City of Los Angeles, the Mayor’s Office of Public Safety for Los Angeles Mayor, Eric Garcetti, and with the support of its members OSPEC360, TruSTAR, IBM, and The Rosslyn Group.

Mandatory Statements

This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number, 18PDSAO00002-01-00.

The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied of the U.S. Department of Homeland Security.

Table of Contents

Overview.....	6
Mission	7
Vision	7
Structure	7
Review of Grant Objectives	7
Key Performance Metrics	9
LA Cyber Lab Use Cases	10
LA Cyber Lab Outreach	11
Bi-Lateral Cybersecurity Information Sharing	Error! Bookmark not defined.
Bi-Lateral Cybersecurity Information Sharing	12
The Questions.....	13
Background Research	13
Hypothesis	14
The Pilot Program	14
Pilot Project Timelines	15
The Case For Information Sharing	16
Benefits of Cyber Threat Intelligence	17
Establish Fully Functional IS-ISAO.....	Error! Bookmark not defined.
Establish Fully Functional IS-ISAO.....	20
Threat Intelligence Platforms (TIP).....	22
Threat Intelligence Platform Capabilities	22
Operational Deployments	24
Types of Threat Intelligence	24
Strategic Threat Intelligence	24
Tactical Threat Intelligence	25
Operational Threat Intelligence	25
The Threat Intelligence Lifecycle	25
1. Planning & Direction	26
2. Collection.....	26
3. Processing.....	26
4. Analysis.....	26
5. Dissemination.....	26

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

6. Feedback	26
LACL Threat Intelligence Sharing Platform (TISP).....	27
Sharing Threat Information	29
Sources of Threat Information	29
Choosing What To Share and When To Share It	30
Analysis of Data	32
XFE Threat Intelligence Sources	32
Risk Score Calculation.....	32
IBM Sourced Content Contributing To The Risk Score	33
Understanding The Risk Score.....	33
Traffic Light Protocol	34
Generating and Sharing Analytic Reports	36
Categorizing Indicators & MITRE ATT&CK.....	36
ODNI Cyber Threat Framework	37
MITRE ATT&CK Framework	37
Protecting Privacy.....	38
Redacting Information from TruSTAR Submissions.....	40
How to Share and Export Information with the TruSTAR Platform	40
User Interface	40
Email Submissions	41
Native Integrations.....	42
STIX/TAXII enabled Tools.....	42
API & Python SDK	43
Submit Report [POST /1.3/reports].....	43
Exporting Data	44
Data Format and Transport Standards.....	45
Minimum Technical Requirements	45
Integrating with the TruSTAR Platform	46
IBM QRadar:	46
Splunk	46
TAXII.....	46
LACL Mobile Application.....	51
Understanding The Risk Score.....	54

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

Products and Services.....	55
LA Cyber Lab Services.....	55
LA Cyber Lab Products.....	56
Identify Barriers to Information Sharing	Error! Bookmark not defined.
Identify Barriers to Information Sharing	58
LA Cyber Lab Overview and Progress.....	58
Impacts of the Pilot Project What is the impact of the project? How has it contributed?	68
Develop Documentation	Error! Bookmark not defined.
Develop Documentation	70
Policies, Procedures, Techniques	70
Social Media Outreach	72
Work with Academic Partners.....	74
Work with Academic Partners.....	74
Cyber Work Force Development	78
LACL Sustainability & Future Recommendations	80
LACL Conclusions	85
Appendix XX – Financial Accounting	87
Appendix XX – Outreach Activities	89
Appendix XX – Pilot Project Participants.....	94
Appendix XX – CTI Sharing Partners	99
Appendix XX – TISP Value Proposition	103
Appendix XX – LACL In Publications & Media.....	109
Appendix XX – List of Known ISAOs/ISACs	111

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

(THIS PAGE INTENTIONALLY LEFT BLANK)

“Information sharing is the thoughts and prayers of the cybersecurity community.”

- Ms. Jordan Rae Kelly, Former National Security Council Director of Cyber Incident Response

Overview

The Los Angeles Cyber Lab, Inc. (“LACL” or “Cyber Lab”) is a 501(c)3 California Nonprofit Public Benefit Corporation formed in August 2017 and located in the Los Angeles downtown area. The LA Cyber Lab is a first of its kind public-private partnership and operates with the motto *“Protection Through Partnership.”*

The LA Cyber Lab is dedicated to sharing the latest cybersecurity threat intelligence and alerts gathered by the City of Los Angeles and its public and private partners. A board of advisors, led by Mayor Eric Garcetti and consisting of leadership from over 30 cross-sector businesses and government entities, develops policies and practices to help guide the Cyber Lab’s mission. Membership in the Los Angeles Cyber Lab is open to all business and residents at no cost.

The LA Cyber Lab is recognized by the Department of Homeland Security (DHS) as an Internet Security – Information Sharing and Analysis Organization (IS-ISAO). As such the LA Cyber Lab regularly communicates threat information to its members and builds greater alliances within the public and private sector business community. The LA Cyber Lab currently operates direct, bilateral channels with the Multi-State Information Sharing and Analysis Center (MS-ISAC). These engagements will allow the IS-ISAO to be integrated in a community of industry-leading cyber experts which will benefit the lab’s private sector members, and ultimately with state and local (SLTT) governments.

LA Cyber Lab’s core initiative is the mutual exchange of cyber threat intelligence (CTI) across private and public sectors, creating collaborative, real-time identification and analysis of threats by the City of Los Angeles, businesses of all sizes, and state and federal partners, including the Department of Homeland Security through the National Cybersecurity & Communications Integration Center (NCCIC). In addition to information-sharing, the Cyber Lab performs widespread outreach activities including offering research and development opportunities for academia, job opportunities for entry-level, career training for professionals, and innovative conferences and events for all customers and stakeholders. It is dedicated to protecting personal and proprietary information from malicious cyber threats by facilitating and promoting innovation, education, and information-sharing between Los Angeles’ public and private sectors.

Since founded in 2017, the Cyber Lab has engaged more than 500 small, medium, and large-size businesses in the Los Angeles region, and expanding to establish strategic cross-sector partnerships across the state and nation. The Cyber Lab currently pulls Indicators of Compromise (IOCs) from all departments of the City of Los Angeles and multiple large Los Angeles based private corporations and pushes those IOCs to the NCCIC through DHS’ Automated Information Sharing (AIS) platform. The LACL shares its IOC reports to the public on a daily basis, helping businesses across the region protect themselves from newly discovered cyber threats. LA Cyber Lab’s outreach efforts have effectively

engaged hundreds of cybersecurity professionals, students, academics, and policymakers, and have received positive feedback from the community.

Mission

The mission of the LA Cyber Lab is to provide the greater Los Angeles business community and local government organizations with greater cybersecurity awareness and access to trained and capable workforce.

Vision

LACL is shaping the Cybersecurity ecosystem in Los Angeles through information sharing and workforce development as a center of excellence.

Structure

The LA Cyber Lab is located at 200 N. Main Street, STE 303, Los Angeles, California 90012. The LACL is staffed by contractors and fellows who perform the following roles: Executive Director, Program Director, Policy Director, Outreach Director, Senior Cyber Analyst, Data Scientist, Program Specialist, and Policy Specialist. These roles supported the LACL in its initiatives towards this pilot program. These roles were funded through the pilot program with the exception of the two specialist roles (fellows) which were provided as in-kind support by LACL's members. Technical development and support for the creation of the LACL information sharing tools was completely outsourced for this project.

The award for this grant was \$2,992,863.00, no additional funds were added to this grant during this period and all funds were expended following the guidelines provided for with the notice of the grant award. The pilot program budget was amended and approved twice in accordance with requested extensions. A complete overview and breakdown of the funds expenditures can be found in **(insert appendix)**.

A complete list of individuals and organizations who had significant participation in the pilot program is included in **(insert appendix)** along with a list of organizations which provided in-kind support to the LACL during the pilot project.

The LACL is managed by a board of directors and three officers (president, secretary, treasurer) who are responsible for the oversight and financial responsibilities of the organization. The majority of these tasks were delegated to the LACL staff. Additionally, a board of advisors, exists to provide the LACL support in networking, fund raising, outreach, technical guidance, and business leadership. The Advisory Board consists of public and private sector organizations and is by invitation only, there is no fee to participate in the advisory board and a full list of organizations involved is listed on the LACL website under the "about us" section (<https://www.lacyberlab.org/advisory-board/>).

Review of Grant Objectives

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

The nature of the cybersecurity threat to America is growing, and our nation’s cyber adversaries move with speed and stealth. To keep pace, all types of organizations, including those beyond traditional critical infrastructure sectors, need to be able to share information and respond to cyber risk in as close to real-time as possible. Organizations engaged in information sharing related to cybersecurity risks and incidents play an invaluable role in the collective cybersecurity of the United States.




The purpose of this financial assistance action was to establish a pilot program to create the Internet Security Information Sharing Analysis Organization (IS-ISAO) to explore and evaluate the most effective methods for bi-lateral cybersecurity information sharing, focusing on regional information sharing, communications and outreach, training and education, research and development for the improvement of State Local Tribal and Territorial (SLTT) government capabilities and capacity. The IS-ISAO will develop the full capability to perform information sharing and analysis of cybersecurity threats, gather, and disseminate government and critical infrastructure information, for the purpose of:

- Cyber threat analysis and information sharing
- Education/training/workforce development
- Technical research and development to support effective information sharing
- Share best practices IS-ISAO will promote and develop a collaboration

Pursuant to these goals, the following grant objectives and key performance metrics for the pilot program were established as follows:

IS ISAO Grant Objectives		
No	Grant Objective	Grant Objective Description
1	Bi-Lateral Cybersecurity Information Sharing	Explore the most effective methods for bi-lateral cybersecurity information sharing, focusing on regional information sharing, communications and outreach, training and education, research and development for the improvement of State Local Tribal and Territorial (SLTT) government capabilities and capacity.
2	Establish Fully Functional IS-ISAO	Establish a fully functional IS-ISAO that can allow real time or near-real time sharing of cyber threat information between IS-ISAO and The National Cybersecurity & Communications Integration Center (NCCIC), within the Office of Cybersecurity and Communications, of the Department of Homeland Security (DHS).
3	Identify Barriers to Information Sharing	Identify barriers to cyber information sharing in DHS’ Automated Information Sharing (AIS) and how do we incentivize State Local Tribal and Territorial (SLTT) to share both with the government and one another to

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

		improve the collective defense posture of the nation and key private sector entities?
4	 Develop Documentation	Develop documentation including design, policies and procedures, CONOPS, and operations manual(s).
5	 Work with Academic Partners	Work with academic partners who will utilize the IS-ISAO operation center to provide real world learning environments to improve student skills and identify research opportunities for students and faculty to explore the full spectrum of cyber technology.
6	 Cyber Work Force Development	Develop hands-on cyber work force development programs in collaboration with academia.

Key Performance Metrics

Measurements/Targets	Threshold	Objective	Current	Current - Objective	Objective Status	Outcome
Number of New members	10 - 50	50	277	227	Exceeded	
Number of Private Sector / Business Members	10-50	50	307	257	Exceeded	
Number of Federal Government members	0	0	4	4	Exceeded	
Number of State Government members	5-10	10	5	-5	Under	
Number of Local Government Members	5-10	10	44	34	Exceeded	
Number of Tribal Members	4-6	6	0	-6	Under	
Number of Territorial Members	0-1	1	0	-1	Under	
Number of Fusion Members	4-6	6	6	0	Met	
Number of Academia Members	1-2	2	26	24	Exceeded	
Number of Other Members*	4-6	6	96	90	Exceeded	
Number of Foreign Members	0	0	9	9	Exceeded	
Number of Individuals Representing Total Membership	10 - 50	50	543	493	Exceeded	
Average monthly growth rate	1% - 2%	2%	13.26%	11.26%	Exceeded	
Number of outreach (conference or event) presentations	2 - 4	4	29	25	Exceeded	
Number of cybersecurity tool training events	1 - 2	2	7	5	Exceeded	
Number of Membership Online Teleconference Calls	2-4	4	4	0	Met	
Number of Situational Awareness Room Events	1-2	2	3	1	Exceeded	

* Other Members are defined as private citizens receiving information from the LA Cyber Lab
% of net increase / decrease in membership

LA Cyber Lab Use Cases

A series of use cases were defined by the LACL to help guide its approach to information sharing during the pilot project. Several programs and themes were developed which further defined these use cases. Namely, the idea of information sharing was defined along with threat intelligence sharing, and public-private partnerships all became a theme under the larger strategy of connecting the community. LACL sought to find disarming ways to connect with a skeptical cybersecurity workforce. Often there were generalized and vague discussions about the limitations of what we were attempting, the impacts the pilot program might have on protecting organizations, and worthiness of this effort in its entirety were questioned. Developing good use cases became the key to defining the deliverables of the LACL and its ability to succeed.

Use Case #1: Connecting the Community - bring technology professionals, businesses and municipalities together to discuss cybersecurity related topics. LACL is in its infancy compared to many older, more established organizations. The benefit being that it remains flexible in many ways and able to adapt to a variety of audiences, organizations, and establishments. Organizations rarely connect with the intent to provide protection to each other, but since people seeing the benefit of friendly neighbors and good samaritans are more inclined to collaborate. The basic psychology of group dynamics often lends itself to people's perceptions of what is happening and results in more inclusivity. By placing LACL at the center of groups, organizations, and people it would be in the position to increase its relevance within the community, build its brand, and foster greater interest in information sharing.

Use Case #2: Public-Private Partnerships - establish trust and confidence among technology professionals, business leaders, and government employees. LACL began with the strong support of the Mayor and City of Los Angeles. It had an advisory board and limited business connections within the community. Trust is a critical component in the cybersecurity industry, perhaps more so than in regular business because cybersecurity professionals often know about vulnerabilities which could have devastating impacts. These industry professionals occupy positions of trust within their organizations and are naturally apprehensive about collaborating with foreign (anyone outside their organization) groups. Skepticism is a common professional trait among them. No cybersecurity professional has the ability to master all aspects of the industry which creates the need to collaborate. LACL recognized the limitations among knowledge, skills, and resources which every organization struggles with and identified opportunities to create relationships beneficial to the parties involved.

Use Case #3: Threat Intelligence Sharing - promote the bidirectional exchange of cybersecurity information to protect municipalities, SMBs, and organizations. Every organization has a need for cybersecurity and one component of a mature security program is threat intelligence. Commonly among larger security teams, analysts will collaborate and share tools, tactics, and procedures. It is uncommon for these analysts to work with analysts outside their organization. Threat feeds exist in free to download and paid versions, there are known limitations within threat data and no one threat

feed can be the all-in-one source. LACL identified a robust group of sources to include within its feed which increased the value of LACL data and to differentiate itself from similar threat feeds.

LA Cyber Lab Outreach

A critical component to the success of the pilot program was the LACL's ability to get the word out about CTI sharing and organically grow the LACL's membership. The LACL began attending and participating in local conferences. For the first 11 months LACL promoted the CTI sharing as a concept while the design, construction and launch of the TISP occurred. Thereafter, the LACL promoted genuine information sharing amongst public-private sectors. During the pilot project the LACL staff engaged in 46 events to promote information sharing and collaboration. Through these events the LACL supported its use cases and the grant objectives. The LACL outreach strategy was designed to 1) evolve the LACL brand, 2) increase the credibility and legitimacy of the LACL, 3) be informative, and 4) to drive information sharing.

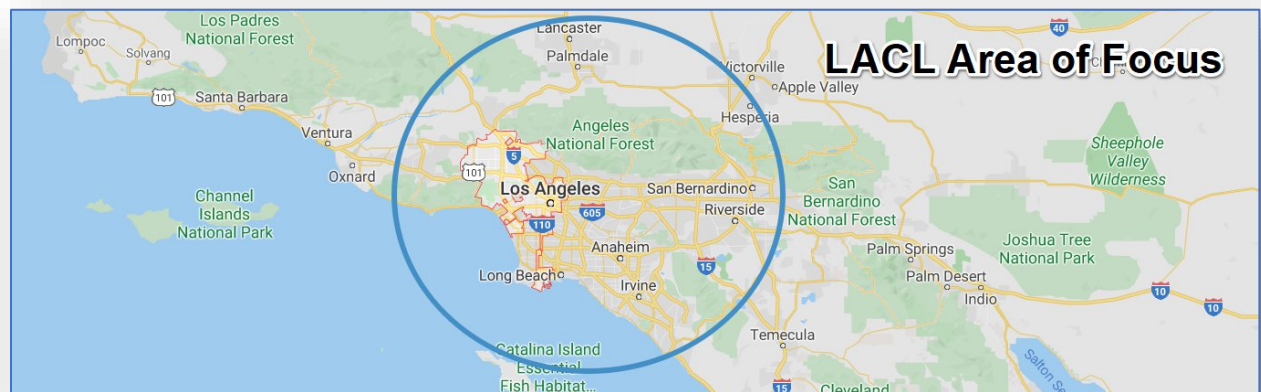
Outreach events included the following: webinars, video teleconferences, face to face meetings, conferences, seminars, public meet-ups, teleconferences, and training. Outreach methods included the use of social media, email, telephone, fliers, ads, short films, and publications. The LA Cyber Lab worked with its Advisory Board to host a series of trainings during the pilot project. These training sessions consisted of hands-on labs for cybersecurity professionals, ranging from novice to advanced skill levels and are further discussed in the "*Cyber Workforce Development*" section. A complete list of outreach activities is documented in appendix [\(insert link\)](#).

LA Cyber Lab Security Summit 2019: LACL launched the TISP and mobile app to increase information sharing and public-private sector partnerships on 9/17 & 9/18; over 350 attendees from SLTT, academia, and business communities participated. There were 527 registered attendees, we have confirmed 40 speakers, 5 moderators and Mayor of Los Angeles, Eric Garcetti provided the welcome address and keynote. Themes for the event include the following categories: aviation security panel, privacy and law discussions, space security panel, cybersecurity risk and best practices along with at least one panel focused on women in tech. DHS Region IX representative Christy Riccardi moderated several panels and the LACL Executive Director provided multiple presentations all focused on information sharing via the TISP or mobile app. The overall event was very successful as it greatly increased the awareness of the LACL in the community and provided a positive experience for all.

Bi-Lateral Cybersecurity Information Sharing

Explore the most effective methods for bi-lateral cybersecurity information sharing, focusing on regional information sharing, communications and outreach, training and education, research and development for the improvement of State Local Tribal and Territorial (SLTT) government capabilities and capacity.

The Los Angeles Cyber Lab (LACL) conducted a pilot program over the course of 18 months, from October 1, 2018 through March 31, 2020. The pilot program focused initially on the greater metropolitan area of Los Angeles encompassing the five counties of Los Angeles, Orange, Ventura, San Bernardino, and Riverside. The Los Angeles Cyber Lab is located at 200 North Main Street, Suite 303, Los Angeles, California 90012 and operates as a 501(c)3 non-profit/public benefit corporation. The Los Angeles Cyber Lab is a virtual lab and shares a close relationship with the City of Los Angeles and the Mayor of Los Angeles. During the program period the LACL made use of a Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) \$2,992,863.00 grant to perform the pilot study.



The purpose of this pilot was to examine information sharing methods for cyber threat intelligence (CTI) amongst public and private sectors and to identify challenges or obstacles related to CTI sharing. The intent and vision of this pilot was to potentially create or design methods (tools, tactics, procedures) to mitigate CTI sharing constraints and establish a model for future CTI sharing endeavors. CTI sharing is widely believed to be the next logical step in the establishment of a national collective cyber defense strategy. Private sector participation is voluntary and public sector resources are limited. Creating connections between these groups by which they might gain greater access to CTI and thereby begin implementing security strategies and processes faster would result in decreases of cyber-crime, data breaches, and economic losses.

Utilizing the scientific method to explore the most effective methods for bi-lateral cybersecurity information sharing, (focusing on regional information sharing, communications and outreach, training and education, research and development for the improvement of State Local Tribal and Territorial (SLTT) government capabilities and capacity to collaborate with the private sector) a series of questions were developed.

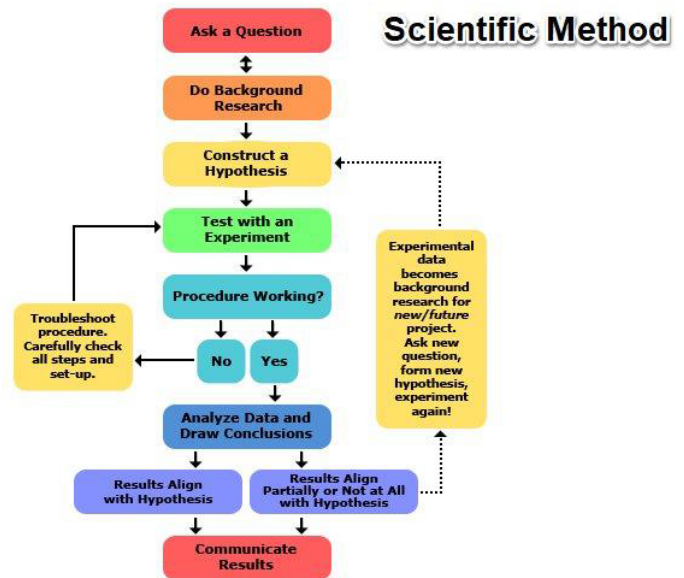
The Questions

- *What existing examples exist of public - private sector threat intelligence sharing?*
- *How do we share information [cyber threat intelligence] between public and private sectors?*
- *How do we do it better [defined as increased ease of sharing and gaining greater participation]?*

Background Research

The nature of the cybersecurity threats in the United States mandates the need for leadership in preventing, mitigating, and recovering from adverse events in cyberspace. As the recent attacks on the cities of Atlanta, Baltimore, New Orleans, and 23 municipalities in Texas, Equifax, Sprint, Yahoo! and Capital One, all indicate a critical need for enhanced bilateral information sharing and collective cyber defense. The Los Angeles metropolitan area is the 13th largest metropolitan area in the world and the second-largest metropolitan area in the United States with nearly 18 million inhabitants.¹ Over 460,000 businesses and 1,000 public organizations (SLTT) in the region contribute to the largest economy in the United States.²

Existing efforts in CTI sharing were reviewed and briefly evaluated as to not recreate an existing model. Several of the most prominent efforts existing in CTI sharing are DHS AIS (Automated Indicator Sharing)³, FBI's Infragard⁴ and Cyberhood Watch, and MS-ISAC⁵ (Multi-State Information Sharing and Analysis Center); additionally, there are numerous existing CTI feeds both open source (OSINT) and commercially available (e.g. IBM X-Force Exchange⁶, CISCO TALOS⁷, Symantec DeepSight⁸). However, each of these has limitations which impact adoption and information sharing. Additionally, is the



¹ United States Census Bureau, 2017.

² <https://www.latimes.com/business/story/2019-12-19/los-angeles-largest-economy>

³ <https://www.us-cert.gov/ais>

⁴ <https://www.infragard.org/>

⁵ <https://www.cisecurity.org/ms-isac/>

⁶ <https://exchange.xforce.ibmcloud.com/>

⁷ <https://talosintelligence.com/>

⁸ <https://www.symantec.com/services/cyber-security-services/deepsight-intelligence>

movement to create Information Sharing and Analysis Organizations (ISAOs)⁹ across the country. These ISAOs are, with few exceptions, limited in their ability to share information or have a meaningful impact on CTI sharing because they lack resources, experience, and direction. A brief review of existing ISAC and ISAOs uncovers a vast web of organizations, not all organizations are even focused on CTI sharing, and of those that are, the majority of these groups were focused on a specific industry. There are no comprehensive efforts to connect existing ISAOs and ISACs to create synergistic efforts in CTI sharing or cyber defense. At best, these organizations communicate ad hoc and irregularly. Our research failed to identify any existing organization with the charter to share CTI across public and private sectors. Existing ISACs/ISAOs either serve only public sector organizations or focus on one niche area of industry. See the full list of existing ISACs and ISAOs [\(insert link\)](#).

Cyber Threat Intelligence is a highly involved and technical discipline which requires a great deal of organizational resources to be effective. It is often reserved for only the largest organizations due to available budgets and the ability to attract and retain skilled professionals. Security architectures are designed based upon the priority of current leadership and often lack a comprehensive and strategic vision. Gaps exist even among the most advanced organizations. Medium organizations do not have mature security programs and generally lack the ability to implement tools or techniques needed to protect their environments. Small organizations are even more limited in their ability to protect themselves and range between outsourcing their security needs or not addressing them at all.

More About CTI can be found under the “*Establishing a fully functional ISAO*” [\(insert link\)](#) section.

Hypothesis

LACL is an Internet Security - Information Sharing and Analysis Organization (IS-ISAO) providing a means of CTI sharing across all sectors and industries, public and private which can be emulated by other cities.

The Pilot Program

In partnership with the City of Los Angeles and Los Angeles Mayor Eric Garcett, the LACL established a network of private sector subject matter experts and leaders with ties to the information technology industry, creating a unique partnership aimed at protecting the business community of Los Angeles. The intent of the LACL was to create a regional CTI sharing model which could serve as an example for other cities to emulate across American and internationally.

The LACL embarked on a journey over the duration of 18 months to discover the elements of success and failure associated with CTI sharing. During this period, LACL emphasized a focus on how to advance the cyber threat intelligence sharing ecosystem by reimagining the tools, tactics, and procedures associated with CTI sharing. Recognizing that existing and previous efforts in CTI sharing have struggled

⁹ <https://www.isao.org/>

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

in adoption, impact on small and medium business, and overall have had limited success; LACL sought to connect the community and find ways to surpass these obstacles.

In order to connect public and private sectors, the LACL created an IS-ISAO, established a threat intelligence sharing platform (TISP), launched a mobile application and conducted outreach to the greater Los Angeles community. The pilot program connected with 800 organizations and over 2,000 individuals. Attempting to problem-solve CTI sharing was not easy and the LACL creatively approached this challenge by recruiting a top industry leader to represent the LA Cyber Lab and provide visionary guidance as the Executive Director. The LACL staff of six contractors and three fellows planned and executed all the business tasks of the Los Angeles Cyber Lab.

From October 2018 through February 2019, the LACL began organizing its plans, recruiting staff and forming the concept of operations which would become the vehicle by which organizations would share via the IS-ISAO. Over a period of six months from March to September 2019 the LACL managed the creation of the LACL mobile application, TISP and hosted Los Angeles’ first major cybersecurity conference, the LACL Security Summit 2019. Managing three major projects under 120 days through an agile process was extremely difficult as the LACL initially intended to meet a project deadline of September 30, 2019. While the LACL successfully completed these projects within the timeline, the true benefits of the TISP were not realized and three-month extension was granted to allow LACL to continue engaging organizations to participate in CTI sharing. During this period, LACL was able to onboard four organizations completely and had begun dialogs with another 21 interested organizations. A final three-month extension approved to give the LACL time to complete these dialogs and fully explore obstacles to CTI sharing.

45 organizations (public and private) were engaged during the pilot program to participate in CTI sharing through the TISP. Of these organizations six successfully completed the process of bidirectional information sharing. Details of the LACL TISP, the LACL mobile application, and LACL services can be found in the “Establishing a Fully Functional ISA0” section of this report. The LACL participated in extensive outreach and grew its total individual membership to 543 with a membership of 307 unique organizations.

Pilot Project Timelines

Project Date	Goal	Actual Date	Notes
April 10, 2019	Closing of RFP	April 10, 2019	
April 19, 2019	Complete internal review of the vendor proposals	April 19, 2019	
May 10, 2019	Interview vendors	May 10, 2019	
May 15, 2019	Award contract	May 20, 2019	Formal notice to non-selected vendors took longer than expected.
May 2019	Execute Contract with Vendor	August 26, 2019	IBM took 89 days to finalize the contract which greatly

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

			impacted the timeline of the partner onboarding.
June 6, 2019	Project Kickoff Meeting	June 6, 2019	
July 3, 2019	Kickoff +30 days – Complete Use Cases, identify data flows and cloud infrastructure, design platform and interface.	July 3, 2019	
August 1, 2019	Kickoff +60 days – Identify analytical tool(s) and reports, test utilization and data flows.	September 1, 2019	Data flows from the mobile application could not occur until the application was built; IBM would not test until a contact was in place.
September 1, 2019	Kickoff +90 days – Complete data flows, incorporate partner integration, create interface, platform and access controls.	March 31, 2020	Onboarding partners became more complex than originally anticipated, as documented in the obstacles to information sharing section of this report.
September 30, 2019	Kickoff +120 days – Complete project	March 31, 2020	Two extensions were provided to complete the project.

Metrics: (include membership growth / sector diversity)

The Case For Information Sharing

We are all part of the cyber ecosystem. Threats are evolving daily and security needs to evolve in a similar manner to protect us. We each have a responsibility to protect our data but we can also be socially responsible by getting involved with the LACL. The LACL information sharing initiative brings together the best of industry and government and you, to protect our communities and our economy from cyber-crime. Through the crowdsourcing of CTI, LACL provides public and private sector partners the opportunity to increase their response to cyber-attack and build a collective cyber defense.

Crowdsourcing CTI isn't a new concept it has existed within the industry since at 2010 and there have been and are many efforts from the government and security companies to collaborate in this manner. The majority of these efforts have fallen short of their intended goal either because of a lack of participation or for a lack of strategy. The LACL believes the best way to protect our communities is through the sharing of information related to cyber attacks and criminals. Crowdsourcing is relatively simple strategy, *collect information into a single location for all to use as needed*. The complexities of crowdsourcing fall into the following five categories:

Contribution v Consumption: Are enough organizations contributing and are the right organizations consuming CTI? If there aren't enough contributors, the data will lack value. If the right organizations aren't consuming the information, the entire point of crowdsourcing is missed and the effort is greatly diminished in its ability to be effective in helping protect against cyber-attacks.

Content v Indicators: Everyone in the industry wants more content around their indicators, we refer to this as *contextualized information*, which is how a cybersecurity analyst will quickly observe TTPs and apply logic to associate them within their organization's environment. Indicators are only one half of the equation, without indicators there is no conversation. However, indicators alone (without contextualized information) slows the process of cybersecurity analysts considerably.

Quality v Quantity: Generally speaking, quality has been the desired of every crowdsourcing effort. Too many false negatives cause analysts to move away from the CTI feed and stop sharing. Too much information is a typical problem among crowdsourced CTI because the value of the data is less attractive, but many industry analysts still prefer too much information verses none at all. The quantity of CTI data available is growing exponentially and with it tools are developing to manage massive amounts of data. Therefore, the issue of quantity will at some point no longer be an outright issue, but a distraction from sharing.

You being able to provide to many v Many being able to provide to you: Perhaps the greatest issue with CTI sharing is the actual process of sharing. Being able to share information requires a series of prerequisites which are not common knowledge. The challenges for all are similar in terms of desire to share or technology limitations. LALC explores these in detail and provides thoughts and ideas about the future of CTI sharing.

Benefits of Cyber Threat Intelligence

Threat intelligence benefits abound, and virtually every big company employs threat intelligence to secure itself from hackers and cyberthieves. Correctly applied, threat intelligence provides you the chance to proactively allay your most unrelenting threats, instead of just responding to attacks or a stream of incoming alerts. This occurs by comprehending your cyber risk and raising effectiveness and confidence in your security processes. Here are some key benefits of threat intelligence.

Comprehending Your Cyber Risk

It's not pragmatic to make a company 100 percent safe, so the only rational method to security is one based on risk. For the average SME, protecting against state-sponsored advanced persistent threat groups (APTs) is simply unthinkable. Given the small probability of such an attack, investing massively in its prevention defies logic.

Similarly, since organizations of all sizes across all industries are convinced to obtain malevolent email (phishing) attacks, investing in a fundamental content filtering solution does make sense. Obviously, prioritizing most threats isn't quite easy. There is the likelihood that those responsible for making

decisions on security investments will only react to marketing, industry catchwords, and newspaper headlines.

The worst consequence is that these organizations then apportion resources based on fear, rather than knowledge. This is where threat intelligence comes in. A powerful threat intelligence competence can help you recognize the particular threats your organization, your industry, or your architecture, is faced with.

Performing Efficient Security Operations

Just adding new processes to your security strategy should not center around threat intelligence. The fact of the matter is that a powerful threat intelligence competence should be the core of your security processes. The blend of external intelligence combined with internal data is possibly a massive input for prevailing security procedures. Vulnerability management and incident response are predominantly good candidates, as they both demand a high degree of background and prioritization to be effective.

On a daily basis, most companies experience scores of security events, most of which are innocuous irregularities. Threat intelligence can provide the answer this question and enable you to perform a solid baseline for your organization to clearly identify the alerting security events and discard other unimportant regular anomalies

Other Important Benefits

- Identify leaked credentials
- Prioritize vulnerability remediation
- Monitor for mentions of your brand online
- Uncover emerging threats
- Track hacktivist activity in your industry
- Study threat actor tactics, techniques, and procedures (TTPs)

Why should I care about Cybersecurity?

As a society we depend more and more on technology, it's important to take steps to protect your personal data and your business. Your data holds information about not just yourself, but your family, friends, and coworkers - so good data security practices benefit everyone. You also want to protect your business, a cyber event can impact your operations, reputation, and create risk for employees and customers.

LA Cyber Lab Supports the Public Sector

With over 300 Ransomware attacks on local and state government since 2013, the City has made it a strategic priority to help other cities regionally and nationally. Through the LA Cyber Lab TISP, the City shares its threat intelligence to a growing network of regional and national partners.

Who can take advantage of LA Cyber Lab services?

LA Cyber Lab services can benefit everyone, anyone can sign up for our daily threat report or download the mobile app. Larger business with advanced cybersecurity tools can be integrated into our threat sharing platform, giving them data on the latest threats and sharing suspicious activity with the community.

What		Who	How
Daily Threat Report	Daily email with articles on the latest threats	Everyone C-Suite & Business Leaders	Sign up here https://www.lacyberlab.org/tools-for-la-businesses/
LACL Mobile Application	beta web application that gives tips and a guide for sharing suspicious emails. Sharing bad emails is like a cyber tip line.	Everyone, especially SMBs	Download from Apple app store or Google play store
Threat Intelligence Sharing Platform (TISP)	Automated threat sharing platform for public and private sectors partners	Business with advanced Security tools or teams	Contact us LACL at TISP@lacyberlab.org
Daily IOC Report	Daily email with IOCs	Everyone, security teams with limited automation	Sign up here https://www.lacyberlab.org/tools-for-la-businesses/
Trainings and workshops	Free Security trainings for all	Everyone, primarily analysts, researchers	Check LACL website or follow on Social Media https://www.lacyberlab.org/cyber-events/

Establish Fully Functional IS-ISAO

Establish a fully functional IS-ISAO that can allow real time or near-real time sharing of cyber threat information between IS-ISAO and The National Cybersecurity & Communications Integration Center (NCCIC), within the Office of Cybersecurity and Communications, of the Department of Homeland Security (DHS).

As part of the pilot project, the LACL established a fully functional IS-ISAO, registered with the International Information Sharing Organization, recognized by the Department of Homeland Security and providing CTI to the National Cybersecurity & Communications Integration Center. The efforts to create the IS-ISAO were a lengthy process of identifying CTI use cases, partners, members, defining requirements and operationalizing the information sharing process. LACL developed a request for proposal (RFP) with the City of Los Angeles and solicited the private sector for technical assistance in creating a means by which the LACL could create a CTI sharing community. The process of developing the RFP, selecting a vendor, and executing a contract took 11 months. Work based on the project began in June 2019 with informal agreements in place between LACL, IBM, and The Rosslyn Group. The original RFP intended to create a platform capable of completing a full cycle of intelligence and dissemination to members. Through the RFP review and interview process the LACL identified an opportunity to connect with SMBs in a unique way which had never been attempted before in the information security industry.

The LACL boldly took a direction to create a mobile application to support SMBs and individuals with business email compromise (BEC), also known as *phishing*, by splitting the RFP and awarding two contracts within the same allotted budget. The uniqueness of the LACL app is that it takes advantage of enterprise cybersecurity information and analysis, and provides access to this information vis-a-vie the app response to the user's inbox. To create this capability two things needed to occur: 1) create a CTI platform, 2) create an app capable of connecting to the CTI platform. LACL simultaneously began efforts to establish what would become the LACL TISP and the LACL mobile app. IBM was selected, along with its partner TruSTAR, to provide the CTI platform and the analytics which would serve both LACL partners & members, and the mobile app. The TISP is the source of all LACL threat intelligence. The Rosslyn Group (TRG) was selected to create the mobile app which would allow users to submit suspicious emails by forwarding them to the LACL inbox (gophish@lacyberlab.net) from which they would receive an answer about their submission inside their mobile app inbox.

SMBs have historically been difficult to assist from an information security discipline. They have limited resources, access to information, and capabilities to allow them to make use of existing resources. Often SMBs fall into one of three categories of cybersecurity related risk: 1) outsourced IT and security offering some protections, 2) internal attempts to secure their business offering little protections, and

3) ignoring security offering no protections. SMBs represent a significant portion of existing businesses within the community. The LACL created the following use cases for assisting SMBs:

SMB Use Case #1) Define the lowest common denominator of cyber-crime/attacks against SBMs

SMB Use Case #2) Create a no cost service

SMB Use Case #3) Offer a simple way to assist SMBs with cybersecurity

SMB Use Case #4) Bring SMBs into the information sharing community

From these use cases the LACL established that offering a means to validate phishing attempts would be an imaginative and creative way to engage SMBs and the community. LACL wanted to find ways to bring the SMBs and individuals into the cybersecurity ecosystem. The result was the creation of the LACL mobile app.

The LACL identified existing CTI platforms on the market, despite these existing products, no commercially available product has a mobile version or the ability to integrate with SMBs. CTI platforms are strictly for advanced users and mature security operations. The challenge created by these platforms is that medium business and many SLTT organizations do not have the ability to utilize CTI even if it is provided at no cost. The LACL identified this challenge immediately and began engaging large corporations and large municipalities to become *partners* in CTI sharing which would in turn be leveraged to provide CTI to *members*. Members were defined as those receiving information from the LACL in any form. The LACL established the following use cases for the TISP:

TISP Use Case #1) Establish a cloud-based platform for the exchange of threat intelligence

TISP Use Case #2) Create a manageable platform capable of providing CTI via API or STIX/TAXII

TISP Use Case #3) Retain data for at least 90 days

TISP Use Case #4) Perform automated analysis of threat data within the platform

TISP Use Case #5) Capable of anonymizing sensitive data

TISP Use Case #6) Leverage the MITRE ATT&CK Framework with threat data

TISP Use Case #7) Utilize the Traffic Light Protocol for community sharing

TISP Use Case #8) Connect via API with the LACL mobile app

TISP Use Case #9) Control access by role (RBAC)

These use cases guided the development of the LACL TISP as it worked with IBM and TruSTAR to create these functions within the TruSTAR Station platform. The TISP is a cloud-based application which

houses all cyber threat data in enclaves which are provisioned to members. Members are able to access LACL community CTI and interact with the data inside the platform. Members can also use the TISP to create their own cases and manage their cyber threats, they can collaborate with other analysts either in their team or in other organizations within the LACL community, and can access CTI reports.

Threat Intelligence Platforms (TIP)

A TIP is a tool which provides a place to collect and analyze threat intelligence. Threat intelligence platforms are used by organizations to gain an advantage over the adversary by detecting the presence of threat actors, blocking and responding to their attacks. Using threat intelligence, businesses and government agencies can identify the threat sources and data that are the most useful and relevant to protecting their own environment, potentially reducing the costs and dependencies associated with commercial paid threat feeds.

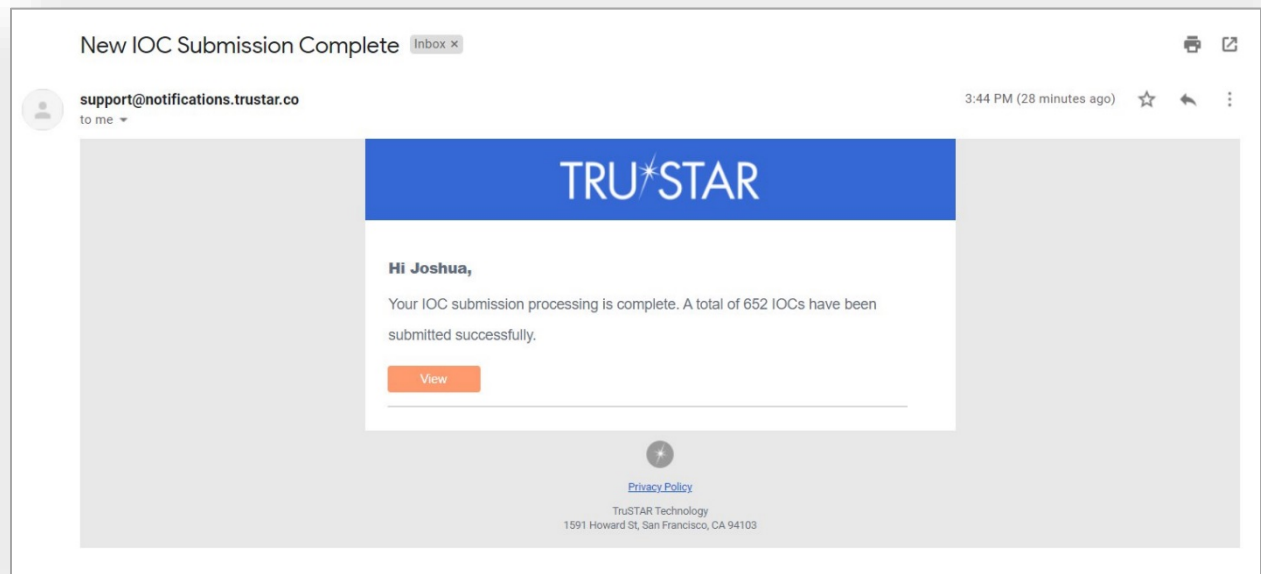
Tactical use cases for threat intelligence include security planning, monitoring and detection, incident response, threat discovery and threat assessment. A TIP also drives smarter practices back into SIEMs, intrusion detection, and other security tools because of the finely curated, relevant, and widely sourced threat intelligence that a TIP produces.

An advantage held by TIPs, is the ability to share threat intelligence with other stakeholders and communities. Adversaries typically coordinate their efforts, across forums and platforms. A TIP provides a common environment for security teams to share threat information among their own trusted circles, interface with security and intelligence experts, and receive guidance on implementing coordinated counter-measures. Full-featured TIPs enable security analysts to simultaneously coordinate these tactical and strategic activities with incident response, security operations, and risk management teams while aggregating data from trusted communities.

Threat Intelligence Platform Capabilities

Threat intelligence platforms are made up of several primary feature areas that allow organizations to implement an intelligence-driven security approach. These stages are supported by automated workflows that streamline the threat detection, management, analysis, and defensive process and track it through to completion:

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization



- **Collect** – A TIP collects and aggregates multiple data formats from multiple sources including CSV, STIX, XML, JSON, IODEK, OpenIOC, email and various other feeds. In this way a TIP differs from a **SIEM** platform. While SIEMs can handle multiple TI feeds, they are less well suited for ad hoc importing or for analyzing unstructured formats that are regularly required for analysis. The effectiveness of the TIP will be heavily influenced by the quality, depth, breadth and timeliness of the sources selected. Most TIPs provide integration to the major commercial and open source intelligence sources.
- **Correlate** – The TIP allows organizations to begin to automatically analyze, correlate, and pivot on data so that actionable intelligence in the who, why and how of a given attack can be gained and blocking measures introduced. Automation of these processing feeds is critical.
- **Enrichment and Contextualization** – To build enriched context around threats, A TIP must be able to automatically augment, or allow threat intelligence analysts to use third party threat analysis applications to augment threat data. This enables the **SOC** and **IR** teams to have as much data as possible regarding a certain threat actor, his capabilities, and his infrastructure to properly act on the threat. A TIP will usually enrich the collected data with information such as IP geolocation, ASN networks and various other information from sources such as IP and domain blocklists.
- **Analyze** – The TIP automatically analyzes the content of threat indicators and the relationships between them to enable the production of usable, relevant, and timely threat intelligence from the data collected. This analysis enables the identification of a threat actor's tactics, techniques and procedures (TTPs). In addition, visualization capabilities help depict complex relationships and allow users to pivot to reveal greater detail and subtle relationships. A

proven method for analysis within the TIP framework builds a clear picture of how adversaries operate and inform an overall response more effectively. This process helps teams refine and place data in context to develop an effective action plan. For example, a threat intelligence analyst may perform relationship modeling on a phishing email to determine who sent it, who received the email, the domains it is registered to, IP addresses that resolve to that domain, etc. From here, the analyst can pivot further to reveal other domains that use the same DNS resolver, the internal hosts that try to connect to it, and what other host/domain name requests have been attempted. This ensures a more effective overall response.

- Integrate – Integrations are a key requirement of a TIP. Data from the platform needs to find a way back into the security tools and products used by an organization. Full-featured TIPs enable the flow of information collected and analyzed from feeds, etc. and disseminate and integrate the cleaned data to other network tools including [SIEMs](#), internal ticketing systems, [firewalls](#), [intrusion detection systems](#), and more. Furthermore, [APIs](#) allow for the automation of actions without direct user involvement.
- Act – A mature threat intelligence platform deployment also handles response processing. Built-in workflows and processes accelerate collaboration within the security team and wider communities like [Information Sharing and Analysis Centers \(ISACs\)](#) and [Information Sharing and Analysis Organizations \(ISAOs\)](#), so that teams can take control of course of action development, mitigation planning, and execution. This level of community participation can't be achieved without a sophisticated threat intelligence platform. Powerful TIPs enable these communities to create tools and applications that can be used to continue to change the game for security professionals. In this model, analysts and developers freely share applications with one another, choose and modify applications, and accelerate solution development through plug-and-play activities. In addition, threat intelligence can also be acted upon strategically to inform necessary network and security architecture changes and optimize security teams.

Operational Deployments

Threat intelligence platforms can be deployed as a software or appliance (physical or virtual) [on-premises](#) or in dedicated or public [clouds](#) for enhanced community collaboration.

Types of Threat Intelligence

Cyber security threat intelligence is often broken down into three subcategories:

- Strategic — Broader trends typically meant for a non-technical audience
- Tactical — Outlines of the tactics, techniques, and procedures of threat actors for a more technical audience
- Operational — Technical details about specific attacks and campaigns

Strategic Threat Intelligence

This strategy provides a comprehensive summary of an organization's threat landscape, and is intended to inform high-level decisions made by a company's managers and executives. Effective

tactical intelligence should provide understanding into domains like the risks related to certain lines of action, extensive designs in threat actor strategies and targets.

Tactical Threat Intelligence

This type of intelligence plans the strategies, methods, and measures of threat actors. It should help protectors comprehend, in precise terms, how their company might be attacked and the best ways to protect against or alleviate those attacks. It typically includes technical setting, and is used by personnel directly involved in the security of a company.

Operational Threat Intelligence

This type of intelligence is knowledge about cyber-attacks, events, or campaigns, giving specific understandings that help incident response teams comprehend the nature, intent, and timing of precise attacks. Since this typically comprises technical information, this kind of intelligence is also referred to as technical threat intelligence.

The Threat Intelligence Lifecycle

The importance of threat intelligence in today's world can hardly be overlooked. The following are the phases of the threat intelligence lifecycle.



1. **Planning & Direction**

This is the phase when goals are set for the threat intelligence program involving comprehension and articulation. Once advanced intelligence needs are found out, a company can frame questions that channel the need for information into separate requirements.

2. **Collection**

It is the method of collecting information to address the most significant intelligence requirements. Information collection can happen naturally through such means as pulling metadata and logs from inner networks and security devices; subscribing to threat data feeds from industry organizations and cybersecurity retailers; holding discussions and targeted interviews with well-informed sources; skimming open source news and blogs; and more.

3. **Processing**

This is the change of gathered information into a setup an organization employs. Nearly all raw data gathered ought to be handled in some way, whether by humans or machines. Various collection systems often need different means of dispensation, while human reports may need to be interrelated and graded, deconflicted, and checked.

“Solutions like SIEMs are a good place to start because they make it relatively easy to structure data with correlation rules that can be set up for a few different use cases, but they can only take in a limited number of data types.”

4. **Analysis**

The next step is to make sense of the processed data. The goal of analysis is to search for potential security issues and notify the relevant teams in a format that fulfills the intelligence requirements outlined in the planning and direction stage. Based on the situations, the decisions might involve whether to probe a possible threat, what actions to take directly to block an attack, how to reinforce security controls, or how much investment in additional security resources is vindicated.

5. **Dissemination**

Dissemination involves having the complete intelligence productivity to the places it ought to go. A majority of cybersecurity organizations have at least six teams that can take advantage of threat intelligence. This type of intelligence entails you to ask what threat intelligence the audiences need, and how external information can support their activities.

6. **Feedback**

It is the final phase of the lifecycle that is making it closely related to the initial planning and direction phase. After receiving the finished intelligence product, whoever makes the initial request reviews it and determines whether their questions were answered. You need steady feedback to ensure you appreciate the requirements of each group, and to make changes as their requirements and priorities vary.

Cyber-threat Intelligence Tools

Commercial Tools

It's a very important threat intelligence platform. The commercial tools generally happen to be very expensive. It is often hard to persuade upper management of the need of some of these types of tools, particularly with their annual upkeep fees. The benefit of these tools is that a lot of them accelerate the penetration test and SOC operations. Another advantage of using commercial tools is that they are highly automated and save a lot of time but this is also considered a drawback because the user cannot learn how to achieve the same procedure independently.

- [FireEye iSIGHT Threat Intelligence](#)
- [IBM X-Force Exchange](#)

Open Source Tools

This refers to a program or tool that carries out a very particular task, in which the source code is openly published for use and/or alteration from its unique design, absolutely free. Open-source intelligence tools generally gather data on Open-Source Intelligence (OSINT), which is one of the most popular feeding processes and techniques.

- [MISP – Malware Information Sharing Platform](#)
- [OSINT Framework](#)

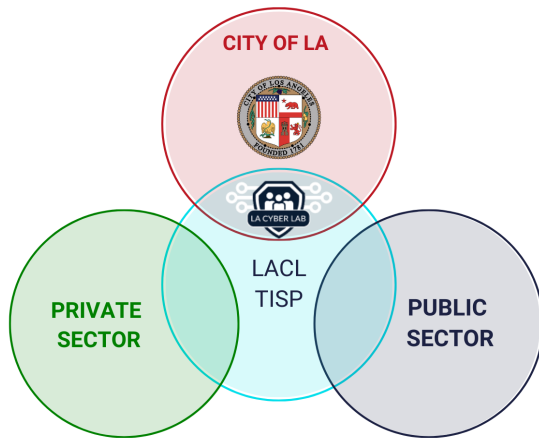
Community Platforms

Community Platforms manage the procedure of producing and upholding a space for prolific debate among community members who can share their opinions, ideas, and worries. There are various types of community platforms that debate, discuss, and describe the latest and emerging threat actors and vectors that could help professionals to use this information as feed and get prepared for the underground ongoing and emerging threats.

LACL Threat Intelligence Sharing Platform (TISP)

Upon its launch, the LACL joined with the City to publish a daily threat report, documenting the “indicators of compromise” identified by the City each day, in hopes that the data would help businesses protect their systems from common attackers. LACL partnered with IBM and TruSTAR to

develop the LACL Threat Intelligence Sharing Platform (TISP). The TISP allows for real-time automated threat indicator sharing between the private and public sector. Features of the TISP include:



Automated Threat Sharing: Using their existing security tools, partners can connect to the TISP to exchange threat data with one another, machine-to-machine, in real time. It enables members to leverage the insights and analysis developed by DHS, the City of LA, and other partners to protect their own systems.

- Connects LACL Partners, a group consisting of nearly 40 organizations, sharing IOCs for greater community good and consumption.
- Accessible to LACL Members at no cost.

Threat Intelligence Platform: The TISP gives analysts and Threat Intelligence interface to pull in additional threat data sources, see trends, and perform research. The Threat Intelligence Platform can be used by organizations lacking the infrastructure for automated sharing.

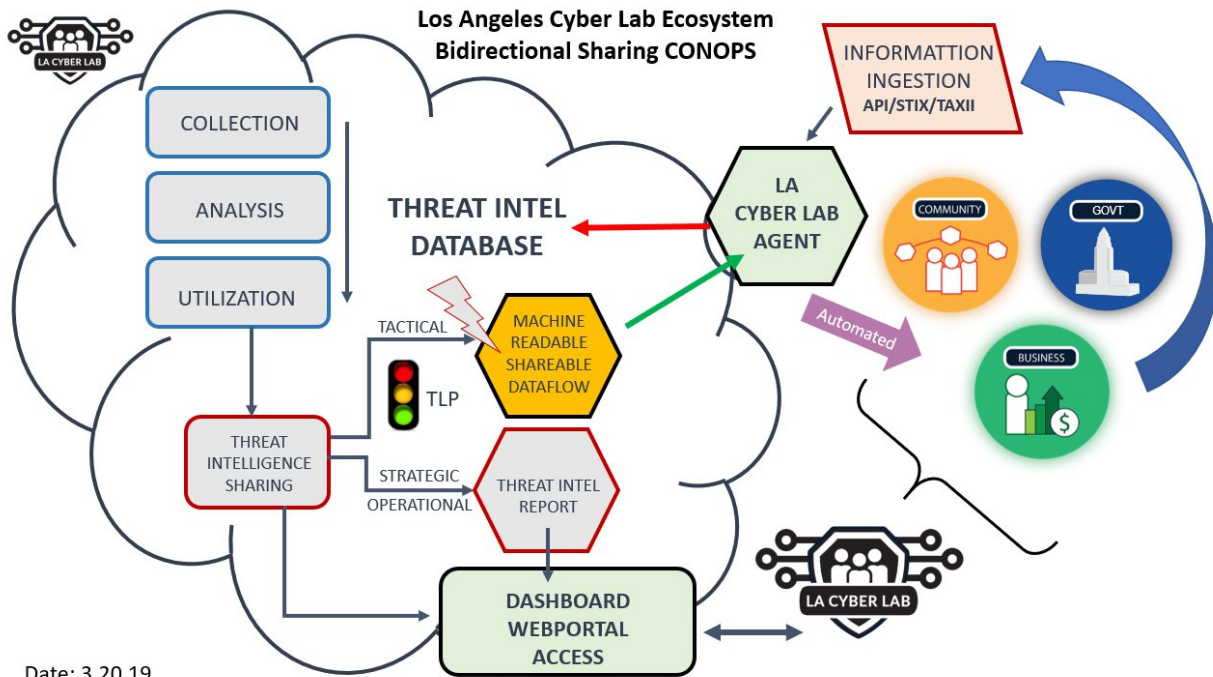
- Threat Reports for Emerging Malware
- Platform for Analysts to Interact with and Research Threats
- Trending data for threats across the LA region

Security Tool Integration: The TISP includes pre-built applications that integrate with existing security tools, such as Security Information and Event Management systems.

LA Cyber Lab Mobile Application: providing phishing analysis which connects SMB and individual citizens to business email compromise information.

- Trending phishing threats across the LA region
- Analysis of suspicious emails for evidence of malware or malicious links
- Individual access to threat intelligence

TISP Concept of Operations: utilizing a cloud-based SAAS TIP to ingest CTI from public, private, and community members, the TISP automatically correlates information with existing CTI via IBM X-Force Exchange IRIS analytics and produces reports which can be exported in a variety of formats.



Date: 3.20.19

Sharing Threat Information

The concept of sharing cyber threat information immediately begs the questions of what kind of information to share and how to share it. This policy guidance provides answers to these and related issues, such as what are the typical sources of threat information that an organization may wish to share; deciding on what information to share and when to share it; how such information might be categorized according to relevant models and frameworks; and how to protect privacy when sharing information. The below information provides guidance on how to address these questions and issues within the LACL ISAO.

Sources of Threat Information

The term “threat information” refers to any information related to a cyber threat that may help an organization identify an attacker’s activities or defend against a cyber threat. Threat information often refers to specific indicators (also called Indicators of Compromise (IOC)) such as IP addresses or phishing emails and may also include a broad range of cyber threat-related information, such as attacker’s behavior or “tactics, techniques, and procedures” (TTPs); security alerts such as advisories or bulletins; vulnerability notifications; or threat intelligence reports.

LACL ISAO Partners/Members are likely to possess a variety of threat information that can be used to support the information sharing community. Such data/information may originate from within an organization’s security tools as well as reside in suspicious emails sent to the Partner organization or its members. Typical security tools that contain threat information include firewalls, intrusion detection/prevention tools (IDS/IPS), anti-virus products, operating system artifacts and logs, browser

history and caches, Security Information and Event Management (SIEM) tools, email systems, case management systems, and other system artifacts.¹⁰

Systems and tools that are already in place and designed to gather threat information to assist decision-making regarding cyber threats—such as SIEMs—are likely to be a good starting point for automatically sharing information such as IOCs to other Partners within the LACL ISAO. Threat information derived from incident response engagements conducted in response to potential cyber threats, such as TTPs and IOCs, is also likely to be useful to other Partners within the LACL ISAO. Finally, inbound emails that suggest an organization is being targeted for attack are likely to contain threat information of value.

There are several types of organizations which represent the community of the LA Cyber Lab. Large corporations and public entities are the ideal candidates for Partners to the LA Cyber Lab. These organizations are self-sustaining, have mature information security teams and capabilities, and resources to contribute to the LACL. Due to their size and maturity, they have the potential to offer the LACL higher quality information (IOCs) and greater volume. Of the public sector entities within the region, roughly 20, are deemed mature enough to be considered Partners. Medium size businesses and public entities vary greatly in their capabilities and resources. They often have gaps within their information security structures (e.g. intermittent funding, manpower shortages, skills shortages, etc.) These organizations represent the best category of members for the LACL because they are somewhat mature but could still benefit greatly from the services offered by the LACL. Small businesses and individuals are typically neither a partner or member of the LACL. Their limited resources and skills make it impractical to provide IOCs or other technical information to because they have no means by which to employ the data. Essentially, they can receive IOCs but cannot put them into use. Instead, this particular group represents a category of people who can engage the LACL via mobile platforms and who can contribute to the LACL by providing random but unique data in the form of business email compromise threat data.

Choosing What To Share and When To Share It

Organizations are typically inundated with potential threat information derived from their internal security operations, many of which are likely to be classified as false positives. When deciding whether to share threat information, organizations should first apply an internal vetting process to determine that the indicator may pose harm to an organization and therefore may also threaten other Partners with the ISAO. Once an organization has decided that there is a reasonable case to be made that the threat information e.g. an IOC may be malicious, the organization should consider sharing that information within the LACL ISAO.¹¹

¹⁰ <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf>

¹¹ https://www.isao.org/storage/2016/10/ISAO-300-1-Introduction-to-Information-Sharing-v1-01_Final.pdf

WHAT TO SHARE

CYBER THREAT SHARING MATRIX				
SOURCE	IDENTIFY	IOC	CORRELATE	SHARE
Networks	Firewall logs	IPs / Domains	External Threat Intel	TISP
	Web Content Filter			
	Irregular Activity			
	hashes/Fingerprints from SSL inspection			
Emails	User reporting phishing	Senders/ URLS		Email/Reports/T ISP
	Email logs			
Endpoint	Antivirus triggers	Hashes/ SHA/ MD5		TISP
	Endpoint detection			
	Window Event Logs			
	Application Whitelist/Blacklist			
Analyst	Analyst investigation/findings	TTPs	Reports/Calls	

After having made a decision that threat information may be of value to other Partners within the ISAO it should be shared as quickly as possible. This is especially important in the case of IOCs such as IP addresses, domain names, or file hashes which may have a very short lifespan. Attacker behavior or TTPs should also be shared quickly as such information could be particularly valuable to Partners' Incident Response teams who might be investigating a similar incident.

The TruSTAR platform currently supports processing of the following IOC Types:

- IPV4
- IPV6
- CIDR BLOCK
- URL (Domains are currently categorized as URL's)
- MD5
- SHA1
- SHA256
- CVE (based on NIST's CVE Standard)
- BITCOIN ADDRESSES
- SOFTWARE (file names are currently treated as Software)
- EMAIL ADDRESS
- REGISTRY KEY

- MALWARE
- THREAT ACTOR
- PHONE NUMBERS

Analysis of Data

XFE threat intelligence analysis and risk scoring methodology for the LACL TISP and mobile application are outlined within this document.

XFE Threat Intelligence Sources

The following are the data sources utilized for the LACL TISP:

- Botnet Traps
- Web Crawling
- Email/Phishing Honeypots
- Open Relay Proxies
- X-Force Vulnerability Database
- WhoIs
- ASN
- Cert Stream
- Regional Internet Registries
- Tor Nodes
- DNS Analytics from PCH/Quad9
- IBM Customer Feedback about URLs, IPs, DGA matches, Squatting matches

Concerning the distribution proprietary threat intel versus external 3rd party feeds we have:

- 89% is XFE proprietary threat intel
- 11% is coming from external feeds

Risk Score Calculation

XFE's analytics engine manages the life-span of an indicator of compromise (IOC) dynamically per source and per category.

Risk Scoring Factors:

- How often have we seen an IOC (e.g. Phishing website observed in initial compromise)
- In how many sources have we seen an IOC (e.g. does a Malware Downloader occur in parallel on our Email Honeypots and on our OpenRelays)
- Is the IOC reoccurring from time to time
- When did we see the IOC the last time
- Is the IOC after a rescanning/recrawling clean now? (e.g. after the owner has fixed the vulnerability / removed an exploit)

XFE normalizes the risk scoring factors. XFE recommends taking steps to defend, block or filter when a risk score is ≥ 5.0 .

XFE uses dynamic risk scoring per IOC Category. For example, the lifespan of a phishing URL differs from a Botnet C2 Server.

XFE maintains an IP Reputation database. For example, a spearphishing email's originating source IP is recorded in the IP Reputation database with a risk score ≥ 5 . If XFE no longer sees spearphishing from this IP, the risk score lessens stepwise. Within a few days it will be below 5 (5 is the recommended threshold for which an action should be taken like a QRadar Offense being created).

For example, in other categories, an IP in our botnet traps or 3rd party list receives a risk score ≥ 5 . XFE lowers the risk score and within in few days it will be below 5 if the IP is not observed.

XFE uses customer feedback to permanently adjust and improve our algorithms to ensure coverage and a low false positive rate.

IBM Sourced Content Contributing To The Risk Score

Data processed per day

- 13M crawled and analyzed web pages and images
- 17M spams received via our spam honeypots

Data processed ever

- 40B analyzed web pages and images
- 3B known web hosts
- 9B unique email bodies
- 4.6M malware samples
- 18k identified Bad Actors
- 800 TB of Threat Intelligence Data in the X-Force Content Intelligence Data Center
- Updates for our consumers (such as XFE, QRadar, XGS, Lotus Protector for Mail Security, update frequency: 3-5 minutes)
- 230k new or updated URL categorizations per day
- 460k new or updated IP categorizations per day
- 1.2M new or updates spam hashes per day

Understanding The Risk Score

XFE aligned the risk score range with the Common Vulnerability Scoring System (CVSS), see <https://www.first.org/cvss/specification-document#5-Qualitative-Severity-Rating-Scale>.

XFE uses colors to express the rating:

Score	Rating	Color
1 - 3	Low	Green
4 - 6	Medium	Yellow
7 - 10	High*	Red

*Unlike CVSS, XFE does not distinguish between High and Critical

Traffic Light Protocol

Los Angeles Cyber Lab Partners/Members are expected to adhere to the Traffic Light Protocol (TLP) when sharing threat intelligence to ensure that sensitive information is distributed only to those who are authorized to receive it.

The TLP provides a mechanism for sharing threat intelligence that is widely accepted among cybersecurity threat researchers, vendors, ISACs and ISAOs. The protocol provides instructions for handling information that are designed to be easy and intuitive to understand. It does not apply to licensing, encryption, or other handling rules.

LACL ISAO Partners should label threat intelligence submitted to the TruSTAR platform or otherwise shared within the LACL ISAO using the instructions and appropriate TLP color codes provided below. Partners/Members shall also respect the TLP designations on information submitted to the ISAO with respect to sharing this information with other entities. If the Partner/Member desires to share the information beyond what is indicated in the TLP designation, they must receive permission from the originator.





TLP use based on sharing mechanism

- TLP-designated email correspondence should indicate the TLP color of the information in the Subject line and in the body of the email, prior to the designated information itself. The TLP color should be in capital letters: TLP:RED, TLP:AMBER, TLP:GREEN, or TLP:WHITE.¹²
- TLP-designated documents should indicate the TLP color of the information in the header and footer of each page. To avoid confusion with existing control marking schemes, it is advisable to right-justify TLP designations. The TLP color should appear in capital letters and in 12-point type or greater.
- Threat information submitted through an automated tool using an acceptable format and standard e.g. the Structured Threat Information Expression (STIX), should apply the appropriate TLP marking within the schema.

It is possible that information submitted to the TruSTAR platform as part of the LACL ISAO will not bear a TLP marking. In these cases, Partners/Members should treat such information as TLP:AMBER and should only share this information with members of their own organization or with clients or customers who need to know the information to protect themselves or prevent further harm.

¹² <https://www.us-cert.gov/tlp>

Definitions

Color	When should it be used?	How may it be shared?
<p>TLP:RED</p>  <p>Not for disclosure, restricted to participants only.</p>	<p>Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.</p>	<p>Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.</p>
<p>TLP:AMBER</p>  <p>Limited disclosure, restricted to participants' organizations.</p>	<p>Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.</p>	<p>Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.</p>
<p>TLP:GREEN</p>  <p>Limited disclosure, restricted to the community.</p>	<p>Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.</p>	<p>Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.</p>
<p>TLP:WHITE</p>  <p>Disclosure is not limited.</p>	<p>Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.</p>	<p>Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.</p>

Source: <https://www.us-cert.gov/tp>

Within TruSTAR, there are several mechanisms through which a Partner/Member can annotate the TLP level of the information being shared.

- TLP markings can be added to the Report Title when uploading a report and within the body of the Report itself.
- Reports and Indicators of Compromise (IOCs) can be tagged with the appropriate TLP level.
- Email submissions can be marked with the TLP level directly in the email subject line or via tags.

For more information on how to submit Reports, IOCs, and Emails to TruSTAR see the section below: *How to Share and Export Information with the TruSTAR Platform.*

Generating and Sharing Analytic Reports

LACL ISAO Partners may also consider sharing threat intelligence reports with the community. Such reports are typically unstructured prose or text as opposed to machine-readable data and go beyond atomic indicators to convey “information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision making.” (NIST SP 800-150). Such threat reports may also employ data visualization techniques to convey the results of analyzing large data sets.

There are several different types of threat intelligence reports that Partners may wish to generate and share. Trend analysis and emerging threats reports aggregate and analyze indicators (e.g. hashes, IP addresses, domain names) to identify trends over time that may point to existing or emerging threats to an organization’s security. Other information derived from open source intelligence (OSINT) or the dark web may also be added to provide historical context or point to planning or intentions. These reports may also include suggestions or methods to neutralize these threats.

Other reports analyze threat information related to a specific threat actor or campaign, such as ransomware or phishing campaigns, together with the actor’s indicators, TTPs, and goals or motivations, including the capabilities of the malware used during attacks. Rich with technical details, these reports will help other Partners to understand the threat actor’s capabilities and how it affects their threat environment and security posture.

These reports may leverage analytic techniques, such as “data storytelling” and “analytic stories,” to enhance their effectiveness. These methods typically involve addressing a new development that is being analyzed (e.g., a series of phishing attacks against a particular industry); a key question that is being answered or “what’s the so what?” of the new development (e.g., why the campaign is important to an industry)¹³; the exploration of data over time through a narrative that adds context and explains events in ways that are easy to follow; and leveraging a series of data visualizations that help to convey this narrative. In addition, a key component of a threat intelligence analytic story is not only the narrative regarding the cyber threat, but also information and analysis that can help operations personnel and decision makers, such as how the threat can be detected, mitigated, or defeated. Finally, an analytic threat intelligence report should be transparent about the level of confidence in any analytic assessments as well as any specific analytic method that is being used.

Categorizing Indicators & MITRE ATT&CK

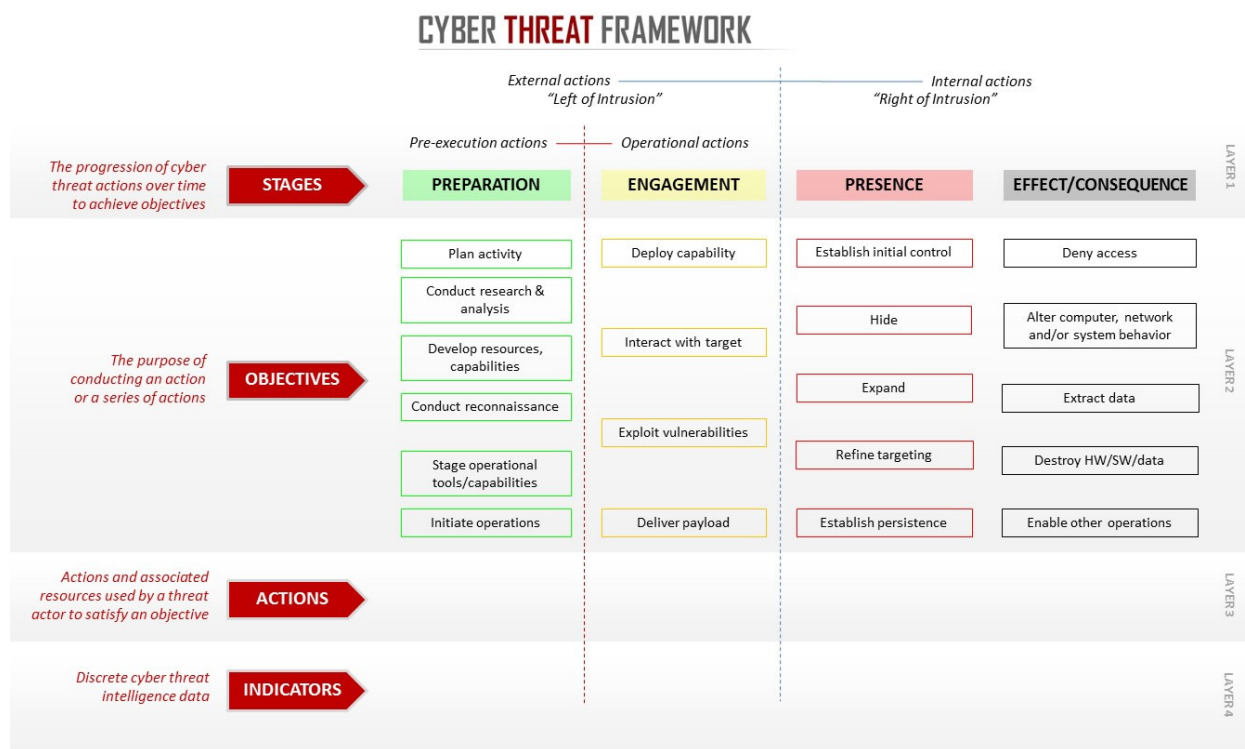
Multiple frameworks have emerged in recent years to assist cybersecurity analysts with categorizing malicious behavior using common lexicon and concepts. These frameworks are also important to information sharing through enabling the use of common terms and concepts. Two noteworthy examples are the Office of the Director of National Intelligence (ODNI) Cyber Threat Framework and

¹³ <https://www.isao.org/storage/2018/06/ISAO-700-1-Introduction-to-Analysis-v1.0.pdf>

the MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) Framework. ISAO Partners/Members are encouraged to use the concepts and terms present in these frameworks where appropriate when describing cyber threat actor behavior to facilitate information sharing. In addition, the TruSTAR platform by October 1st 2019 will enable Partners/Members to tag indicators with the related ATT&CK tactic and technique.

ODNI Cyber Threat Framework

The ODNI Cyber Threat Framework “captures the adversary life cycle from PREPARATION of capabilities and targeting to initial ENGAGEMENT with the targets or temporary nonintrusive disruptions by the adversary, to establishing and expanding the PRESENCE on target networks, to the creation of EFFECTS and CONSEQUENCES from theft, manipulation, or disruption.”



The ODNI offers this high-level model as a tool to describe cyber activity in a consistent and repeatable fashion and as a common reference for other models. More information about the ODNI Cyber Threat Framework can be found here: <https://www.dni.gov/index.php/cyber-threat-framework>

MITRE ATT&CK Framework

The MITRE ATT&CK Framework is a knowledge base of adversarial techniques that can be used against particular platforms e.g. Windows or Linux. The focus of the ATT&CK framework goes beyond

describing an adversary's life cycle and focuses on the tactics, techniques and procedures that adversaries use during their attacks. The emphasis is on how the adversary interacts with the system during their campaign as opposed to the specific tools or malware they deploy. More information on the ATT&CK Framework can be found here: <https://attack.mitre.org/>

The ATT&CK Framework begins with 12 "Tactics" that cover higher-level adversary activities performed during a campaign such as Initial Access, Persistence, Lateral Movement, and Execution. Tactics may also be thought of as goals that an adversary is pursuing e.g. the Tactic Lateral Movement represents the adversaries' goal i.e. to move across the network. These 12 Tactics are enumerated by different "Techniques" to achieve the Tactic. Techniques include the means by which an adversary achieves the Tactic e.g. the Tactic "Persistence" includes Techniques such as Scheduled Tasks, Registry Run Keys / Startup Folder, and New Service.

One noteworthy benefit of the MITRE ATT&CK Framework is the ability to compare different adversary threat groups and their campaigns through their use of different Techniques. An increased understanding of these Techniques and how different threat actors have used them successfully against different organizations can provide valuable information on what types of defenses work best.

To facilitate this kind of analysis, the TruSTAR platform will integrate with the MITRE ATT&CK Framework and Partners and Members may annotate submissions with the corresponding ATT&CK Framework Tactic/Technique and to also search for other indicators based on their ATT&CK Tactic or Technique.

Protecting Privacy

Attention to privacy considerations is a critical part of the information sharing process and is fundamental to the success of the ISAO in which information sharing is voluntary and based on trust. Moreover, the improper disclosure of such information could cause harm to individuals, companies and others and be in violation of applicable laws and regulations. As a result, Partners/Members should consider the privacy implications of information they are considering sharing, such as personal information about a specific individual; whether or not that information is directly related to a cybersecurity threat; and if not, whether that information has been removed. This section is intended to provide guidance to ISAO Partners/Members on how to adequately protect privacy while also fulfilling the goals of the ISAO to enable the sharing of relevant and timely cybersecurity threat information.

The Cybersecurity Information Sharing Act (CISA) of 2015 permits organizations to share personal information as part of a cyber threat indicator only in circumstances where it is directly related to the threat at the time of sharing. This may include information necessary to deter or protect against the threat such as IOCs; threat actor TTPs; and malicious files.

- For a phishing email, information relevant to a threat could include personal information about the sender of the email ("From"/"Sender" address), a malicious URL in the e-mail,

malware files attached to the e-mail, the content of the e-mail, and additional information related to the malicious email or potential cybersecurity threat actor, such as Subject Line, Message ID, and X-Mailer. However, this would typically not include the phishing target email address and names (i.e. the “To” address) because they are considered personal information not directly related to the threat.

The following guidance, drawn from ISAO Standards Organization guidelines¹⁴, is provided to help Partners and Members address privacy concerns when sharing information with the LACL ISAO:

1. Before sharing cybersecurity information, remove or redact information that is known at the time of sharing to be information about a specific individual or that identifies a specific individual, unless it relates directly to the detection, prevention, or mitigation of a cybersecurity threat.
2. Upon receiving information known at the time of sharing to identify a specific individual or is of a specific individual that is not information directly related to a cybersecurity threat, securely dispose of or anonymize such information as soon as practicable.
3. Upon receiving information not related to cybersecurity, promptly notify the submitter or originator.
4. Update cybersecurity information repositories upon receiving a notice of information erroneously identified as cybersecurity information. Securely return, dispose of, or anonymize any such information.
5. Where appropriate, use tools such as the Traffic Light Protocol or similar approaches to designate the sensitivity of cybersecurity information and govern its sharing within and among organizations.
6. Protect cybersecurity information from unauthorized access or acquisition.
7. Regularly review cybersecurity information to ensure it remains useful for cybersecurity purposes.
8. Regularly review the receipt, retention, dissemination, and use of cybersecurity information for consistency with these practices and associated organizational policies.
9. Consistent with organizational privacy policies, provide appropriate transparency about cybersecurity information sharing practices and potential partners, including notice that information that identifies a specific individual may be shared outside the organization for

¹⁴ https://www.isao.org/storage/2016/10/ISAO-300-1-Introduction-to-Information-Sharing-v1-01_Final.pdf

“cybersecurity purposes,” including with the government, which may result in the government’s use of the information for purposes authorized under CISA.¹⁵

Redacting Information from TruSTAR Submissions

TruSTAR provides the ability to redact sensitive information such as employee names, identification numbers, birth dates, etc. from Reports at the time they are manually uploaded into the system. This feature is an automatic part of the process when uploading Reports to TruSTAR.

Partners/Members can also upload a pre-selected list of terms that they wish to be redacted automatically from all submissions. This feature can be found in the Settings on the TruSTAR user interface, and then selecting Redaction.¹⁶

For more information on redacting information from TruSTAR submissions, please see:

<https://support.trustar.co/article/f45yzob9b9-report-submission>

How to Share and Export Information with the TruSTAR Platform

There are a number of options for sharing information such as Reports and IOCs with the TruSTAR platform, including using the User Interface, by Email, and by API.

HOW TO SHARE

THREAT SHARING FRAMEWORK		
1. IDENTIFY	2. CORRELATE	3. SHARE
Identify log sources and potential IOC's from the logs	Correlate potential IOCs with external threat intel	Share IOC with partners

User Interface

Partners/Members can submit reports through the User Interface (UI), by email, and by the TruSTAR API. Once submitted, the indicators within the report are automatically correlated and visible in the TruSTAR UI:

¹⁵ <https://www.isao.org/storage/2017/07/ISAO-SP-4000-Protecting-Consumer-Privacy-in-Cybersecurity-Information-Sharing-v1-0.pdf>

¹⁶ https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf

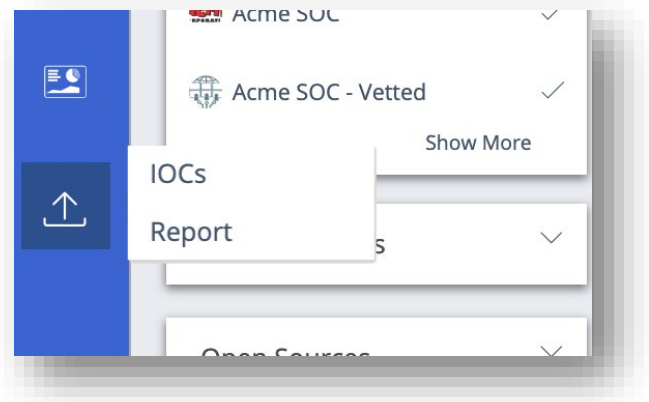
User Interface (Reports):

Through the UI, click the “Import” icon seen in the left side of the bar and select “Report” from the drop-down. (See the box to the right.)

From here, the Partner/Member can upload or drag/drop a file into the Upload File field. File types that can be uploaded include: JSON, DOC, DOCX, XML, XLS, XLSX, EML, MSG, CSV, PDF, STIX, TAXII and TXT files.

For additional and updated information on submitting reports through the UI, please see:

<https://support.trustar.co/article/f45yzob9b9-report-submission>



User Interface (IOCs):

After clicking on the Import icon, select “IOCs” from the dropdown menu. Partners/Members can either paste in a list of indicators or upload a file (DOC, PDF, CSV, XLS, TXT, JSON, XML). Partners/Members will be guided through a series of steps in the UI to submit their IOCs.

For additional and updated information on submitting IOCs through the UI, please see:

<https://support.trustar.co/article/redq0g4hq3-ioc-management>

Email Submissions

TruSTAR allows Partners/Members to submit incident and alert information directly to their enclaves by email. For example, a Partner who belongs to an email listserv for exchanging IOCs, but there is no straightforward way to extract valuable context may choose to share with the LACL ISAO via email submission. Another example, a Partner may setup automated SIEM alerts or case management system and automatically submit the details of an alert or case as a TruStar report.

- Submit phishing emails as an attachment to phishing@lacyberlab.org
- Summit IOC's, analyst investigation/findings, and other information at analyst@lacyberlab.org

Configuration

- Destination Enclave: LACL TISP
- Send to Email Address: lacl_tisp_lro3bflhmcbco@enclave.trustar.co
- LACL TISP Enclave processes emails every minute.
- As with all other submissions, TruSTAR automatically extracts and correlates IOCs.

Email Submission Guidance

- Partners need to send emails from the email account provided during configuration.
- Partners need to use the subject line prefix(s) provided during configuration.

- Partners should verify the subject line prefix is in square brackets [].
- If multiple subject line prefixes exist, then each one has to be in its own square [] bracket.
- Submitted Emails become TruSTAR reports. TruSTAR uses the Subject line Prefix as the Report's Title.
- Partners may include descriptive information about the email submission using tags.
 - Use the subject line. Insert tags as a comma separated list within { } brackets.
 - In the first line of the email body. Insert tags as a comma separated list within { } brackets.
- TruStar uses the email body as report content and automatically extracts IOCs found in the email body.

Email Attachments

TruSTAR automatically connects the email's attachment (PDF, Word, Text file, CSV, Excel or JSON) to the report body. If the attachments have any IOCs, then TruSTAR automatically extracts the indicators. During the email ingestion process, the original format of the attachment may not remain.

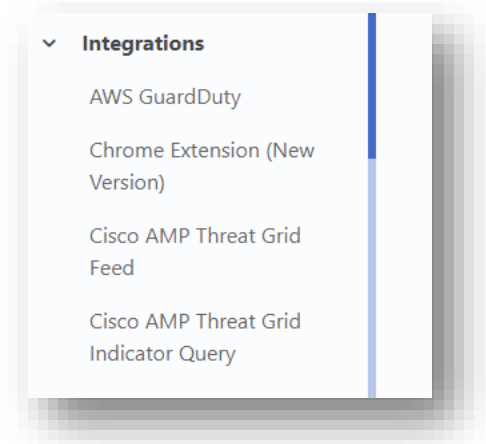
For additional and updated information on email submissions, please see:

<https://support.trustar.co/article/xr5632rgzp-email-ingest>

Native Integrations

TruSTAR integrates with a number of security tools including SIEMS, Case Management systems, and Orchestration tools that enable LACL ISAO Partners/Members to upload information into TruSTAR. For a full list of available integrations, please see: <https://www.trustar.co/integrations>

More information on how to set up these integrations can be found here <https://www.trustar.co/integrations> and on the TruSTAR support page: <https://support.trustar.co/> (select "Integrations" on the menu on the left).



STIX/TAXII enabled Tools

Partners may choose to use existing tools enabled with TAXII. A TAXII Server is software that offers automated exchange services by listening for connections from TAXII Clients looking to ingest data from the available services. Integration information for Partner Tools enabled with TAXII can be found [here](#).

Partners may use the TAXII Message Module Structure to send threat information to TruSTAR. In the TAXII message modules (`libtaxii.messages_10` and `libtaxii.messages_11`), there is a class corresponding to each type of TAXII message.

For example, there is a `DiscoveryRequest` class for the Discovery Request message:

```
import libtaxii.messages_11 as tm11
discovery_request = tm11.DiscoveryRequest( ... )
```

For types used across multiple messages (e.g., a Content Block can exist in both Poll Response and Inbox Message), the corresponding class (`ContentBlock`) is defined at the module level.

```
content_block = tm11.ContentBlock( ... )
```

Other types used exclusively within a TAXII message type defined as nested classes on the corresponding message class and now defined at the top level of the module. For example, a Service Instance is used in a Discovery Response message, so the class standing for a Service Instance, now just `ServiceInstance`, was previously `DiscoveryResponse.ServiceInstance`. The latter name works for backward compatibility but deprecated and may be removed in the future.

```
service_instance = tm11.ServiceInstance( ... )
service_instance = tm11.DiscoveryRequest.ServiceInstance( ... )
```

See the TAXII [API Documentation](#) for proper constructor arguments for each type above.

API & Python SDK

The TruSTAR REST API allows organizations to easily synchronize the incident report information available in the TruSTAR platform to the monitoring tools and analysis workflows within the organization's infrastructure. TruSTAR suggests using the Python SDK to develop specific integrations for workflow automation. All API access is over HTTPS, and all data is transmitted securely in JSON format.

Submit Report [POST /1.3/reports]

1. Submit a new incident report and receive the ID assigned in TruSTAR's system.
2. The ID can be used to find the report through Station, or issue subsequent calls on the API.
3. Note that that a report cannot be tagged during submission. Tags can only be applied afterwards, through a separate call.
4. If a report contains more than 500 indicators, it will be rejected with a `413` (payload too large) error code.

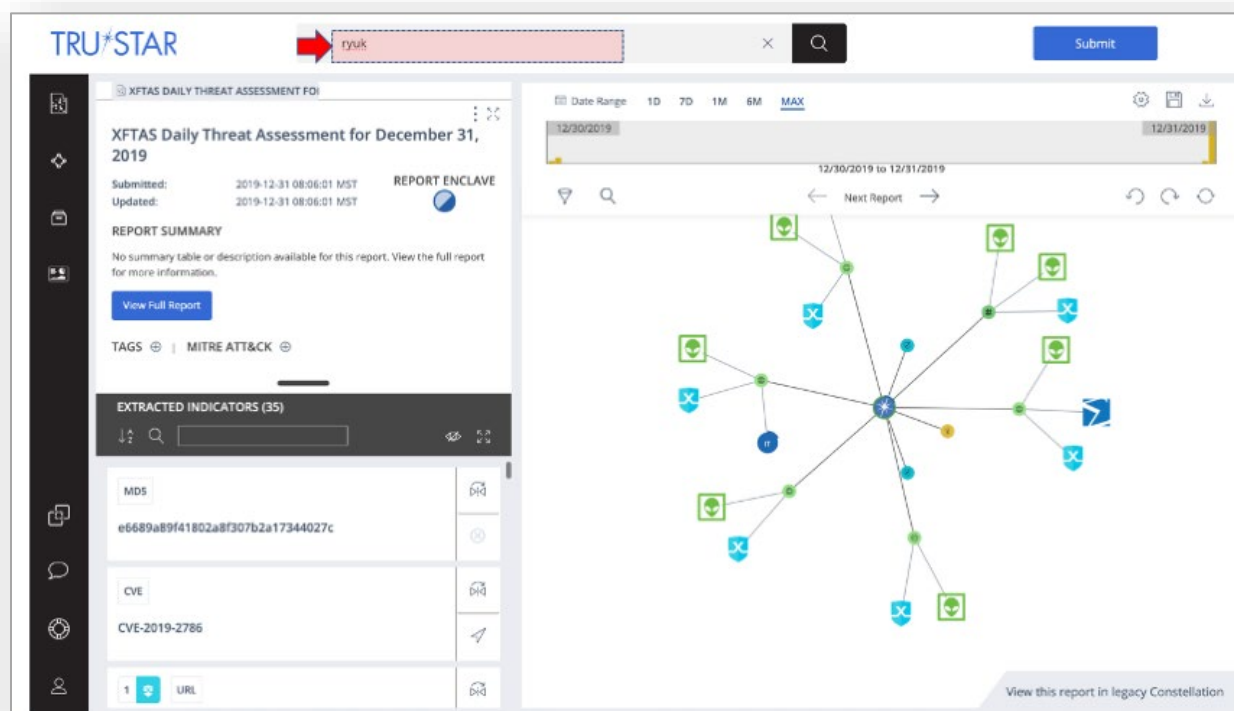
More information about the TruSTAR API and Python SDK can be found here <https://support.trustar.co/article/9u4paxdtdj-api> and here <https://docs.trustar.co/api/index.html>.

Exporting Data

Partners/Members can export data from the TruSTAR platform from the UI or the API. From the UI, there are two options to export or download information. More information on these options can be found here: <https://support.trustar.co/article/d5dct2lxf8-extract-data>

The first option allows the user to export indicators exposed in the graph view in CSV format by selecting the download button on the upper right of the graph.

The example below reflects a query for Ryuk malware information. The report in the example lists 35 IOCs which the user can download to a CSV file by clicking the download icon at the top right of the screen.



The screenshot displays the TruSTAR user interface. At the top, a search bar contains the text "Ryuk" and a "Submit" button is visible. The main content area is divided into two panels. The left panel, titled "XFTAS DAILY THREAT ASSESSMENT FOR", shows a report for "XFTAS Daily Threat Assessment for December 31, 2019". It includes submission and update timestamps, a "REPORT ENCLAVE" icon, and a "REPORT SUMMARY" section with a "View Full Report" button. Below this, there are "TAGS" for "MITRE ATT&CK" and a section for "EXTRACTED INDICATORS (35)". The right panel displays a network graph with nodes and connecting lines, representing relationships between indicators. A date range filter at the top of the graph shows "12/30/2019" to "12/31/2019". A "Next Report" button is located below the date range. The graph contains several nodes, some with green download icons and others with blue 'X' icons. A "View this report in legacy Constellation" link is visible at the bottom right of the graph area.

The second option allows the user to export a file containing report indicators and all data sources from the graph including intel reports, correlated reports, and community reports.



Data Format and Transport Standards

TruSTAR supports a wide variety of data format and transport standards for uploading and retrieving information to and from the platform.

Report Submission: The following file types can be uploaded via the User Interface (Station): JSON, DOC, DOCX, XML, XLS, XLSX, EML, MSG, CSV, PDF, STIX, TAXII and TEXT files.

IOC Submission: The following file types are supported when submitting a file containing a list of IOCs: DOC, PDF, CSV, XLS, TXT, JSON, XML.

Email Submission: The following file types can be processed when submitted as an attachment to an email: PDF, DOC, TXT, CSV, XLS or JSON.

API: All API access is over HTTPS, and all data is transmitted securely in JSON format.

Export: TruSTAR's export options support the following formats: CSV, STIX, JSON, and FireEye TAP.

Minimum Technical Requirements

The minimum technical requirements for Partners/Members to share and receive threat intelligence data are a modern browser and an Internet connection. These are the only requirements needed to access the TruSTAR platform and manually upload and retrieve threat information.

Partners/Members with existing security tools such as SIEMs, Case Management systems, Orchestration tools, or a TAXII client would be able to automatically share and integrate threat information with their existing workflows.

Partners/Members able to implement the TruSTAR API and Python SDK (a Python package that can be used to easily interact with the TruSTAR Rest API from within any Python program) would be able to further integrate TruSTAR threat information with the monitoring tools and analysis workflows used in their infrastructure.

Integrating with the TruSTAR Platform

The TruSTAR platform is able to integrate with a variety of security tools and platforms, including SIEMs, Case Management systems, and Orchestration tools. More information about these integrations can be found here: <https://www.trustar.co/integrations>

The TruSTAR support page <https://support.trustar.co/> provides step by step instructions on how to integrate these tools with the TruSTAR platform. Below we provide an overview of the most popular integrations with TruSTAR, including QRadar, Splunk, and TAXII:

IBM QRadar:

The TruSTAR - QRadar App allows Partners/Members to integrate context from TruSTAR's IOCs and incidents within their QRadar workflow. This integration requires QRadar V7.2.8 and above. Several features of this integration include:

- Submit QRadar offenses and events to your TruSTAR enclave as reports. This can be performed as a manual or automated action.
- Search TruSTAR for all indicators correlated to indicators of interest in QRadar.
- Populate QRadar reference lists with indicators from TruSTAR.
- Age TruSTAR indicators in the QRadar reference list to keep it relevant and actionable.

For more information on setting up the QRadar-TruSTAR integration and a current step by step guide to install, setup and troubleshoot that app, please see: <https://www.trustar.co/integrations/ibm-gradar-siem-integration-partner> and <https://support.trustar.co/article/oUXRwHSmim-gradar>

Splunk

The TruSTAR Splunk app allows Partners/Members to integrate TruSTAR's IOCs and incidents within their Splunk analysis workflow. Several features of this integration include:

- Dashboard displaying IOCs and reports from TruSTAR that match log and event data stored in Splunk indexes.
- View TruSTAR reports in the Splunk app and launch IOC search and investigations against Splunk data.
- SplunkES capability to generate notable events from matched data.

For more information on setting up the Splunk-TruSTAR integration and a current step by step guide to install, setup and troubleshoot that app., please see: <https://www.trustar.co/integrations/splunk-siem-integration-partner> and <https://support.trustar.co/article/zsgux8lk9e-splunk-v-2>

TAXII

LACL ISAO Partners with a TAXII client are able to ingest indicators in STIX format from the TruSTAR TAXII Server for use within their environment. A TAXII Server is software that offers one or more TAXII

Services by listening for connections from TAXII Clients looking to ingest data from the available services. In order to take advantage of this service, Partners must meet the following prerequisites:

- TAXII client running TAXII version 1.1
- TAXII client with ability to connect to a TAXII server running TAXII software version 1.1
- TAXII client with access to connect to TruSTAR TAXII server supported services (Discovery, Collection-Management and Collection Polling)
- TAXII client should be able to accept STIX 1.2 formatted packages

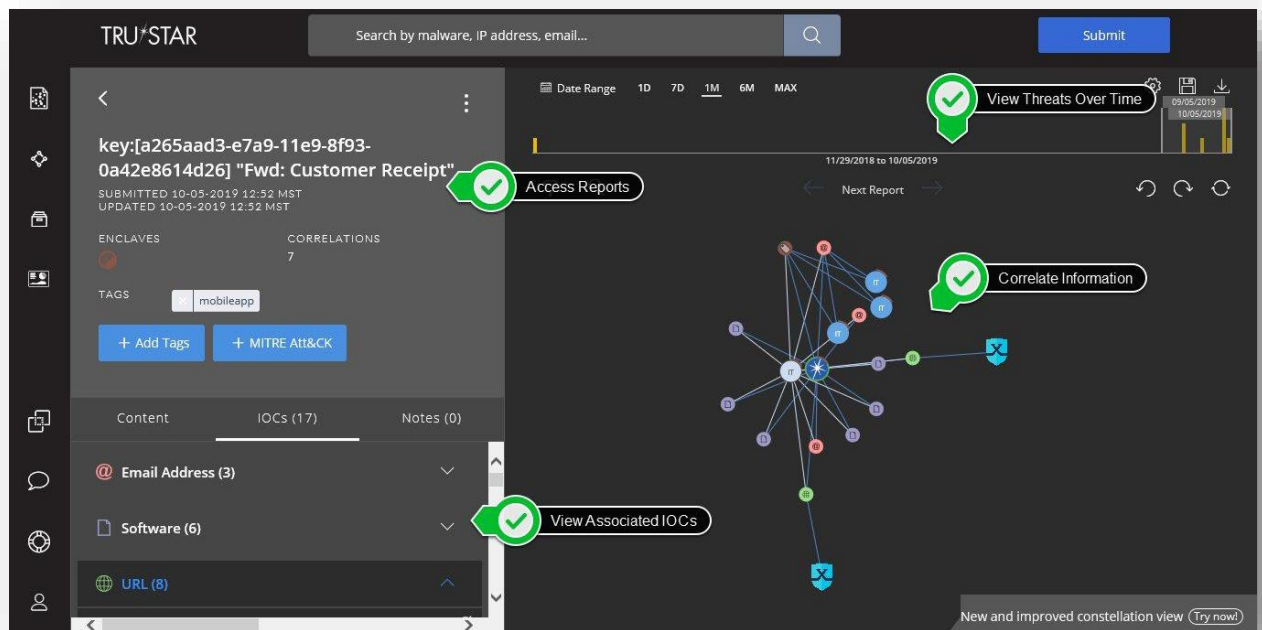
Features of this integration include:

- Allows users to ingest indicators from TruSTAR enclaves of their choice in STIX format into supported tools.
- Users can run discovery service to identify all available services with the TruSTAR TAXII Server.

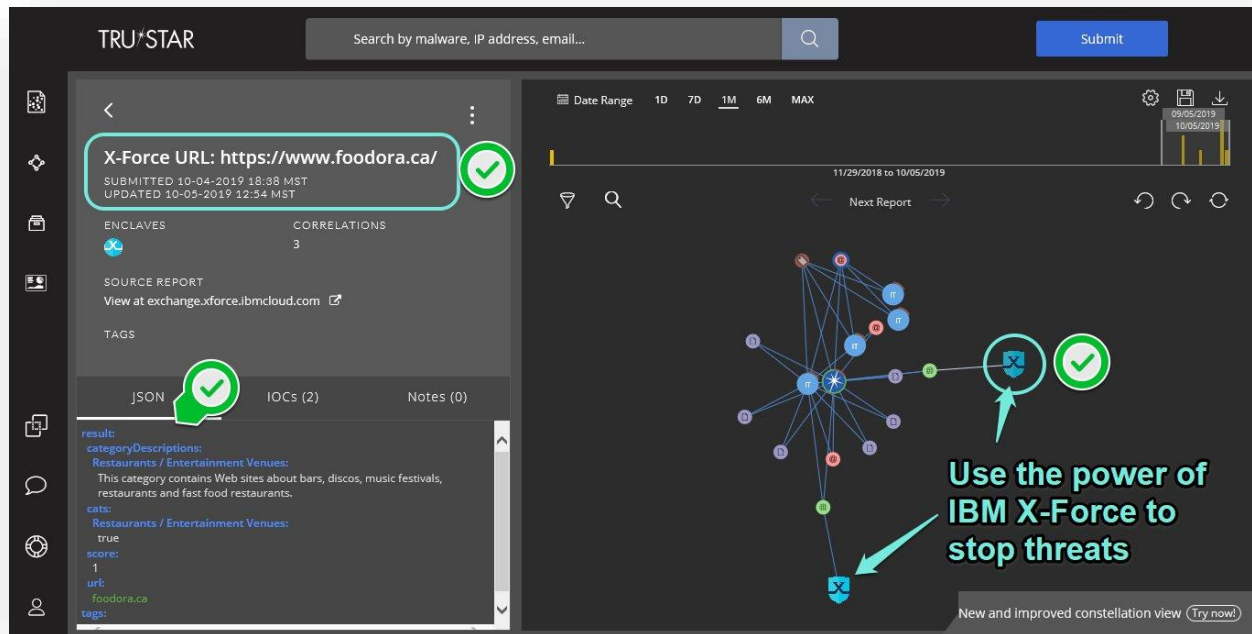
For more information on setting up the Splunk-TruSTAR integration and a current step by step guide to install, setup and troubleshoot that integration, please see:

<https://support.trustar.co/article/r1irw5srpv-server>. More information on STIX/TAXII can be found here: <https://oasis-open.github.io/cti-documentation/>

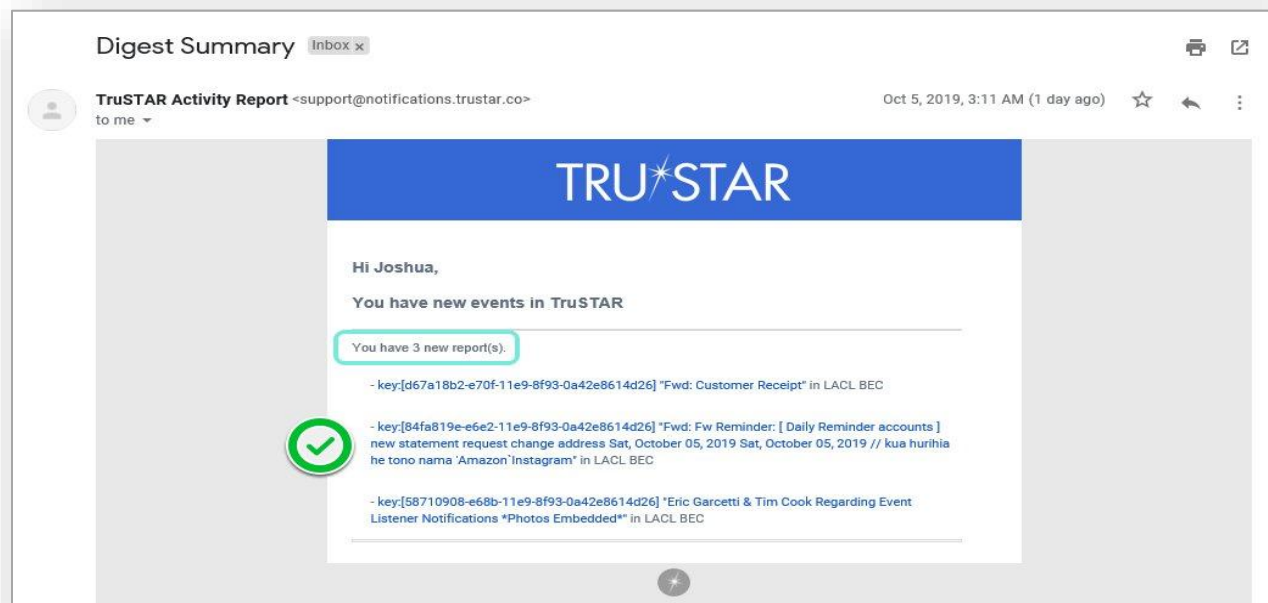
Threat Intelligence Sharing Platform (TISP) Screen Shots



Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization



The TISP is operational and is constructed with multiple data enclaves. The enclaves are 1) IOCs from partners, 2) business email compromise (aka phishing) and 3) Partner specific (e.g. Public Sector). The phishing IOC enclave is connected to the mobile application. On September 13th, the LACL launched the Los Angeles Cyber Lab mobile app in the Apple store and the following day in the Google play store. The app is free to download and offers users a daily tip, news feeds, trending data from the

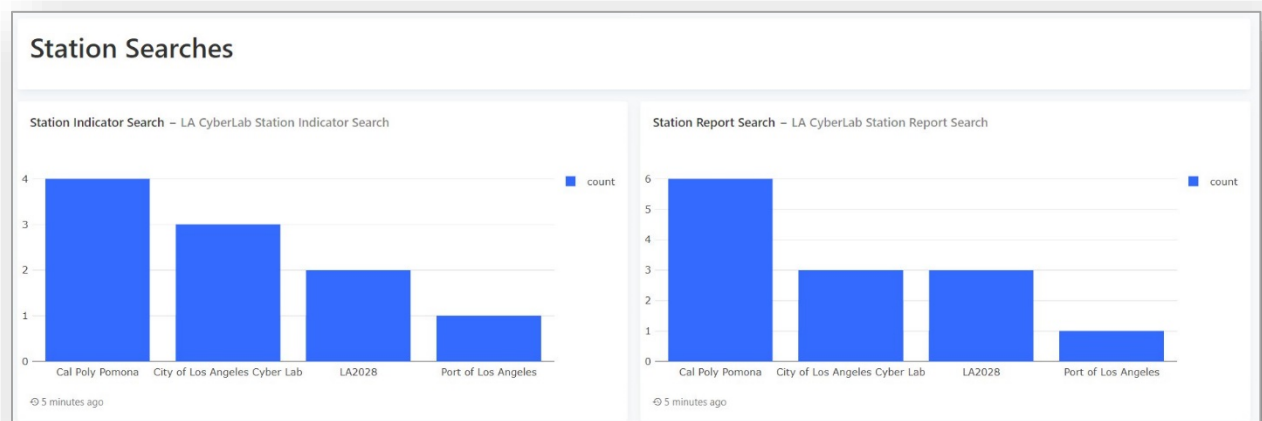


greater Los Angeles region, and has an inbox which provides them notifications about emails they have forwarded to the LACL. Notification responses currently average several hours. When an email is forwarded to the LACL it is ingested with certain selectors being extracted and matched against existing known phishing IOCs. The analysis is being conducted by IBM's X-Force Exchange.

Dashboards

Easy to understand, customized, and shared, dashboards are an assortment of widgets that give you a summary of the reports and metrics you should care about most. Threat intelligence dashboard provides information on threat activities. There are two types of dashboards organization-oriented (internal) and generic (external).

LACL TISP Dashboard



Generic Dashboards

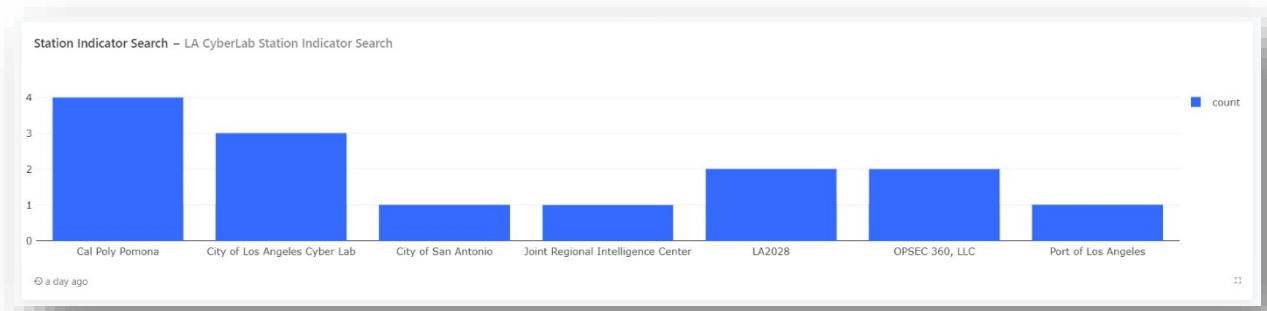
Generic dashboards provide the information about global threat alerts and activities or about the community involvement. LACL uses the generic dashboards to track users with access to the TISP, login frequency, and use.

Organization Oriented Dashboard

These dashboards provide information about specific threats and alerts that organizations care about. LACL uses these dashboards to track high search values, import/export of data, and API usage. Knowing who is using the TISP to search for CTI is valuable as the LACL can collaborate with members to create detailed reports for the community.

LA Cyber Lab's information sharing community dashboard example.

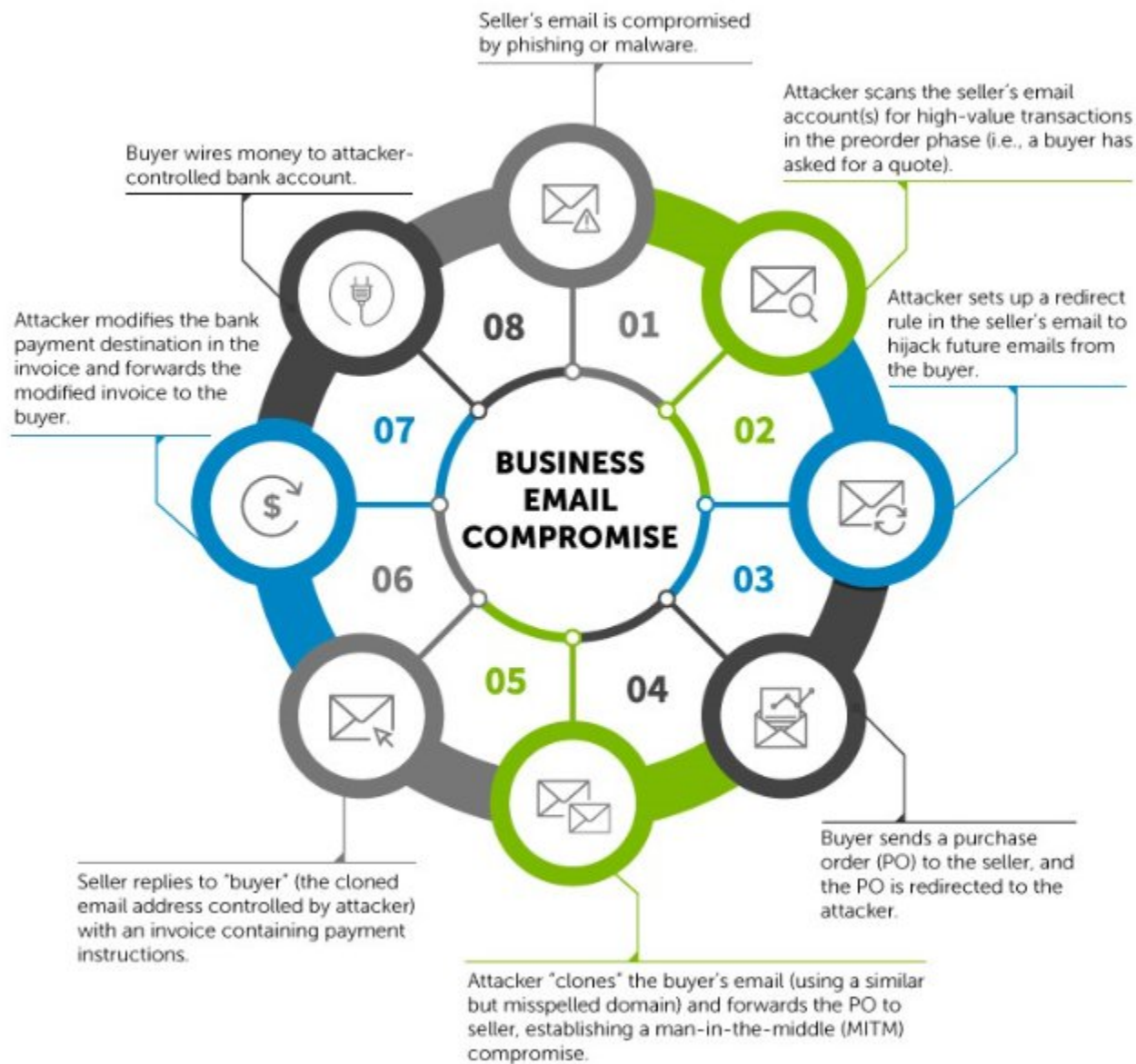
Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization



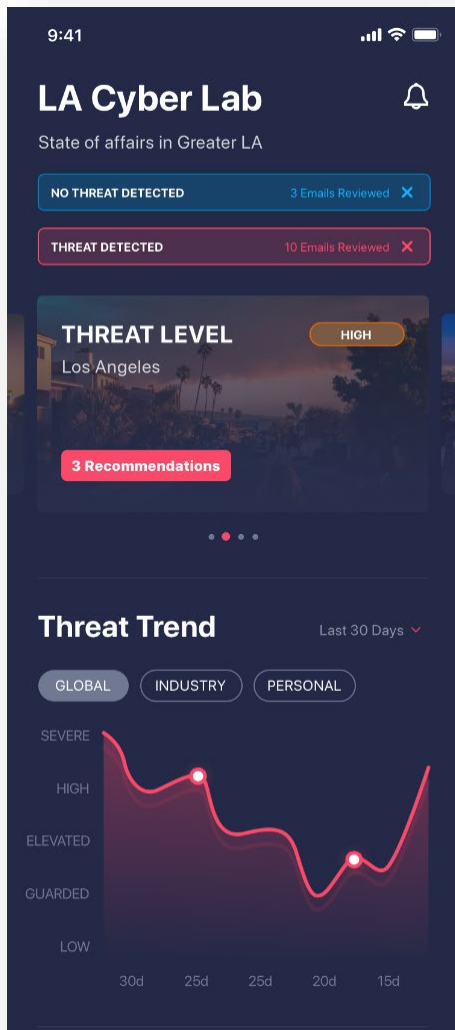
LACL Mobile Application

The LACL Mobile Application was developed in an agile capacity over a 90-day timeline in the summer of 2019. The mobile app was designed, tested, released and beta tested to validate and prove design logic. The application is a light middleware interfacing between the user and the LACL's TISP data lake.

The mobile app is the primary means by which the LACL engages SMBs and individuals. Functionality of the mobile app was designed through a series of small SMB focus groups in conjunction with the LACL team. The app was launched on September 13, 2019 and is available in both Apple App and Google Play stores. The app is free to download and does not have any purchase features.



The concept for the mobile app was created by the LACL to address the gap in SMBs and individuals having access to enterprise CTI. The lowest common denominator among all businesses is *email* and the most common cybersecurity issue associated with email is *business email compromise* (BEC). The LACL defined the scope of the mobile app as follows:



Mobile App Use Case #1) Design and launch a mobile application which connects SMBs and individuals with the LACL TISP.

Mobile App Use Case #2) Leverage the LACL TISP API for a mobile application which can render a score to users about a suspicious email.

Mobile App Use Case #3) Ingest emails, analyze, score, and disseminate the opinion via a mobile application.

Mobile App Use Case #4) Include RSS feeds of relevant cybersecurity news and information for display within the mobile application.

Mobile App Use Case #5) Design and launch a mobile application in both Apple and Google stores simultaneously.

Mobile App Use Case #6) View of a heat map which correlates the geographic location of emails submitted to the LACL.

Mobile App Use Case #7) Provide basic cybersecurity awareness information to users regarding their email submission.

With respect to Mobile Responsiveness Design and Testing, LACL utilized TRG's UX/UI design team, who

focused their approach on implementing an application that renders correctly across different devices, operating systems and screen sizes. TRG implemented the React framework to develop a modular, adaptable and fluid front-end design and user experience. Along with implementing React, The TRG UX/UI design team followed three development principles to ensure a responsive mobile application:

#1) The use of fluid Grids – This approach is based on the percentage of mobile real estate and not the historic pixel-based approach.

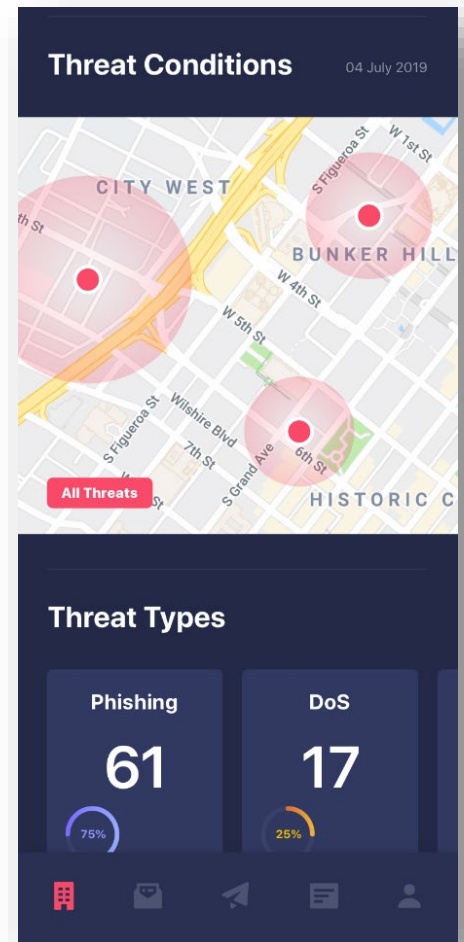
#2) Media Queries – This is used to apply different styles based on the device screen size.

#3) Flexible images and media – This helps to show the images and media differently in different sizes by using scaling or CSS.

Along with the development approach, it is equally important to test the application to ensure it is showing up as expected on all devices. A responsive application needs to give the same experience to the users across mobile operating systems and devices. It needs to be tested for device versions, different screen sizes, modes – landscape or portrait, etc. The content, videos, images, links, etc. all need to be tested for their appearance before releasing the application. For example, plotting on a map may look a little different on Android when compared to iOS. TRG executed the following test cases to ensure responsiveness of the mobile application across a variety of IOS and Android devices:

- 1) Verify whether the content fits on the screen and is not cut out or distorted.
- 2) Verify whether the feeds are loading and do not have broken links in them.
- 3) Verify whether the text color, the font etc, remain the same across devices.
- 4) Verify whether zooming in/out doesn't distort the map.
- 5) Verify whether fast scrolling doesn't distort the content.
- 6) Verify whether the links are working well and if they take the user to the appropriate page.
- 7) Verify whether the application back end calls are not timing out or taking too long to load.
- 8) Verify whether locking of portrait mode so content remains in the most optimum layout.
- 9) Verify whether the images of different types are shown as expected.
- 10) Verify whether navigating between cards in the mobile application doesn't distort the content etc.
- 11) Verify speed and responsiveness to query changes.

With regards to test case 11, TRG UX/UI design team calculated the impact of code and design choices on user experience. For example, typically, people get very frustrated if they have to wait more than one to two seconds for any UI feedback and therefore our mobile design aimed to load data dynamically to reduce the time to content access. For each iteration of the application, TRG measured



timing differentials in already-deployed features so to ensure that future iterations didn't impact performance expectations.

Understanding The Risk Score

The LACL Mobile Application utilizes the IBM's XFE which is aligns the risk score range with the Common Vulnerability Scoring System (CVSS), see <https://www.first.org/cvss/specification-document#5-Qualitative-Severity-Rating-Scale>.

LACL Mobile Application Risk Rating Matrix

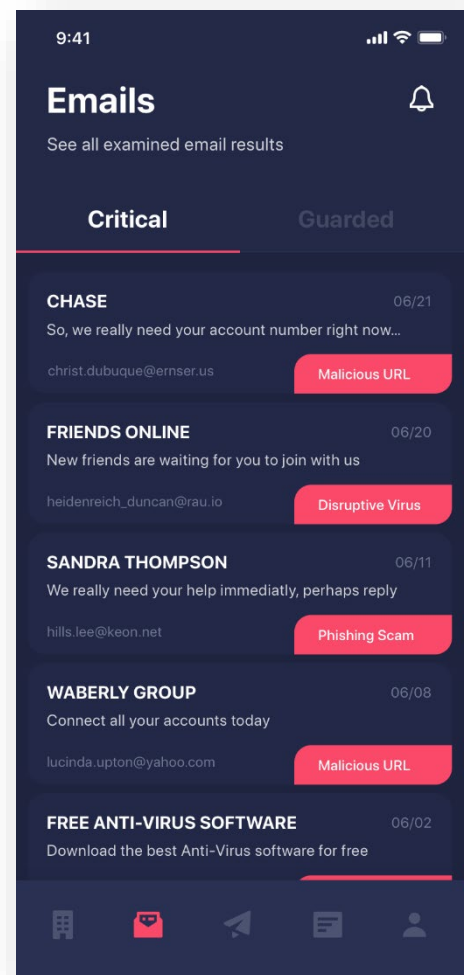
Score	Rating	Risk
0	Unknown (Not previously seen)	Guarded
1 - 3	Low - Medium	Guarded
4 – 10	Medium - High*	Critical

*Unlike CVSS, the Mobile App does not distinguish between High and Critical

Potential Issues and Limitations

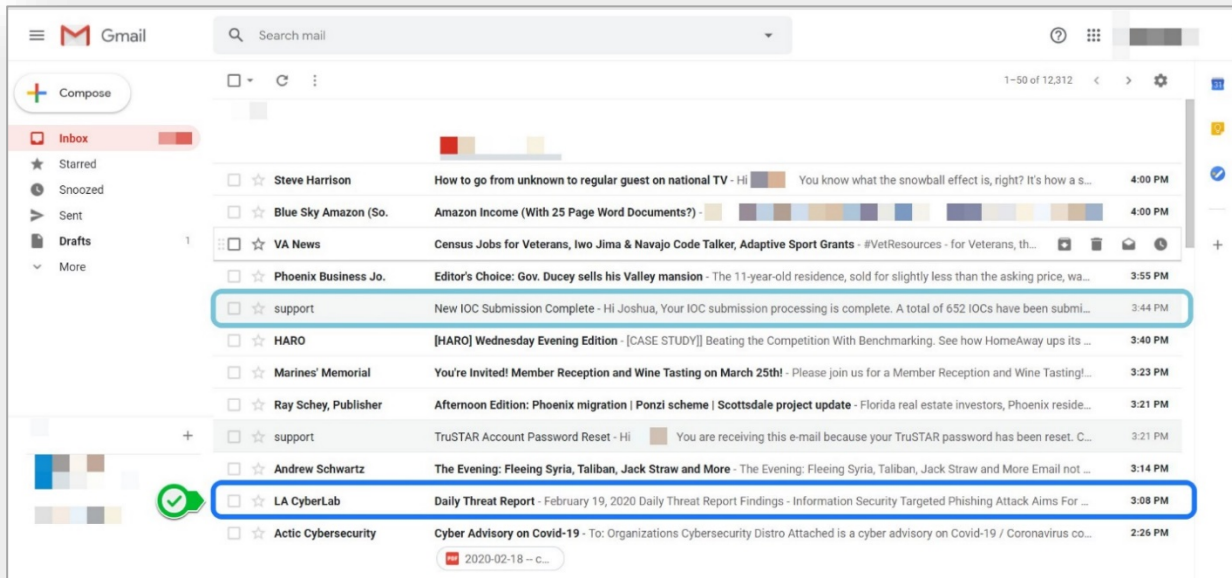
The LACL Mobile App proved to be successful for email providers such as *Hotmail, AOL, Yahoo, and Office 365*. The mobile application provided little value for those organizations utilizing Gmail since this service does a superb job eliminating phishing emails before they reach the user. The mobile application was downloaded over 230 times since its launch. Limitations of the mobile application include:

- False Negative #1: The email submissions are logically analyzed for known malicious IOCs; if a zero day or an IOC which is not within the LACL TISP data lake exists, it will not be positively identified.
- False Negative #2: The email submissions are not reviewed by a human or AI technology which reads the email, therefore, the message may in fact be a phishing attempt but the LACL Mobile App will not recognize it as such because only known indicators are triggering a positive result.
- The mobile app has limitations on the number of submissions which can be used to *call* the API in a 60 second window. While this limitation is not an immediate issue, if the adoption of the mobile app was significant to the point that thousands of submissions were simultaneously sent the result would be delayed responses.



Products and Services

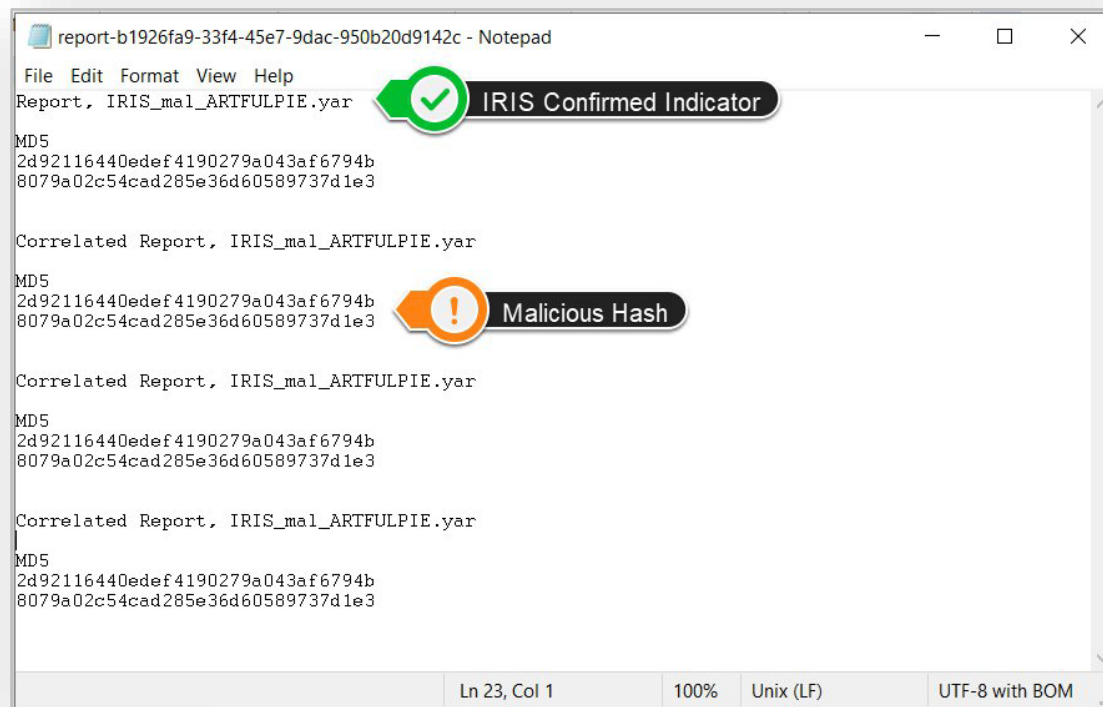
The LACL has created a series of products which are available to anyone, at no charge, and are designed to engage the community in a variety of forms. Connecting the Community, the LACL



designed these offerings to reach targeted audiences and to help educate recipients, grow the LACL brand, and to facilitate partnerships across the region. Below is a list of LACL products and services.

LA Cyber Lab Services

- Anti-Phishing Analysis and Cybersecurity Threat News via the *LA Cyber Lab* mobile app.
- Threat Intelligence via the LACL TISP through either an API or STIX/TAXII feed available to members.
- Threat Intelligence & Reports via the LACL TISP for partners & members with access to the platform; analysts are able to submit or work with data to create cases for IOCs; analysts can provide feedback to the community about ongoing threats and request assistance through the platform.



LA Cyber Lab Products

- **Daily Threat Report:** a daily emailed list of information and physical security events in the news. The communication is sent Monday-Friday excluding holidays.
- **Daily Indications of Compromise (IOC) Report:** a daily emailed link to two CSV documents, one including DHS threat data and one including City of Los Angeles threat data. Examples of IOC consist of malicious hashes, URLs, IP addresses and websites. The communication is sent Monday-Friday excluding holidays.
- **Weekly Threat Report:** a weekly emailed list of security events in the news covering agriculture, defense, energy, financial, insurance, healthcare, legal, litigation, regulatory risk, operational risk, pharmaceutical, reputational risk, retail and technology sectors.
- **Ad-Hoc & Special Report:** ad-hoc emails are sent only when a specific information security risk is identified, typically this communication contains immediate/near real-time threat information and actions which businesses should consider; special reports are an emailed PDF attachment containing information about either major events or significant information security issues.

Example from the Daily Threat Report

New and Updated Information on North Korean Malicious Cyber Activity

Created: Friday, February 14, 2020 - 09:58

Categories: Cyber Security

The U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), the FBI, and the Department of Defense have provided new and updated information on malicious cyber activity by the North Korean government. In six new Malware Analysis Reports (MARs), these agencies discuss and provide technical information for Trojan malware variants used by the North Korean government. The new Trojan malware variants include BISTROMATH, SLICKSHOES, HOTCROISSANT, ARTFULPIE, BUFFETLINE, and CROWDEDFLOUNDER. There is also an updated MAR for HOPLIGHT, which was initially reported on last year. In addition to malware descriptions related to HIDDEN COBRA, the MARs contain suggested response actions and recommended mitigation techniques. The MARs encourage users or administrators to flag and report activity they describe to CISA ([online reporting form](#), CISAservicedesk@cisa.dhs.gov, or 1-888-282-0870) or the FBI CyWatch (cywatch@fbi.gov or 1-855-292-3937), and give the activity the highest priority for enhanced mitigation. *[Read the MARs at CISA.](#)*

Identify Barriers to Information Sharing

Identify barriers to cyber information sharing in DHS' Automated Information Sharing (AIS) and how do we incentivize State Local Tribal and Territorial (SLTT) to share both with the government and one another to improve the collective defense posture of the nation and key private sector entities?

LA Cyber Lab Overview and Progress

The LA Cyber Lab (LACL) has made significant progress towards the information sharing initiative grant objectives. During the past 18 months the LACL has grown 48 percent, reaching hundreds of businesses and SLTT organizations in the region. The efforts of the LACL have focused on establishing a threat intelligence sharing platform (TISP), a mobile application, and significant outreach. The LACL has worked steadily to establish a credible brand whereby organizations within the region can trust the LACL and will want to do business with us. As of March 31, 2020, there were seven TISP partners sharing data. The reason for the slow pace of onboarding are numerous and complex. This request details the systemic, technical, and organizational obstacles encountered.

LACL has identified four systemic issues that exacerbate eight specific technical and organizational obstacles. An extension will allow LACL to continue to identify, document, and solve or mitigate these barriers. The matrix below provides an overview of the systemic issues and specific technical and organizational obstacles LACL has identified.

Barriers to Information Sharing Matrix

Systemic Issues	← Unique Organizations →	
	← Competing Priorities & Lack of Resources →	
	← Time →	
	← Trust →	
Obstacles	I. Technical	II. Organizational
Specific Obstacles	A. Version Control	A. Segmented Organizations
	B. Decentralized IT/Security	B. Risk Aversion
	C. Data Ingestion	C. Awareness
	D. Security Maturity/Technical Infrastructure	
	E. Marketplace	

II. SYSTEMIC ISSUES

LACL has four identified three systemic issues that impact several specific technical and organizational information sharing obstacles. The LACL has had interactions with over 1,000 public and private sector organizations. The interactions with these organizations has allowed the LACL to identify these issues & obstacles.

The systemic issues identified are:

- A. **Unique Organizations:** The LACL sharing partners are diverse, complex, and dynamic organizations with varying security maturities. These organizations have different structures, authorities, and individuals in control of policies and technical security tools. For example, a CISO does not always have the same authority in every organization (*Case- County of Los Angeles 3*). Some organizations are risk averse to the concept of “sharing data” (*Case -City of Santa Monica*). This problem extends to the technical domain, each organization uses different technical tools, configurations, and versions which requires LACL to work closely with each partner, learning about their specific obstacles. **Exploring technical configurations is a case by case approach which is time and resource intensive.**

Mitigation: LACL continues to learn, adjust, and document solutions for the range of onboarding organizations. **Future attempts in CTI sharing require a deep understanding of the partner in order to effectively engage organizations, understand unique challenges, and further develop the onboarding process.** Specifically, the extension will allow for two things:

- 1) Feedback received will inform how LACL refines the TISP and develops streamlined and adaptable onboarding processes and procedures.
- 2) LACL is building a solution catalog, documenting solutions to specific problems.

The combination of a streamlined and adaptable onboarding process, with a solutions catalog will allow LACL to quickly onboard a diverse group of organizations.

- B. **Competing Priorities/Lack of Resources:** The TISP and onboarding support is provided to partners at no financial cost. However, the onboarding process requires partner staff participation with LACL. Competing priorities and lack of resources are a significant onboarding issue. The national cybersecurity workforce shortage further exacerbates this issue within the Los Angeles region; security teams are already understaffed and unable to fill technical positions. Even the LACL experienced difficulty hiring a competent cybersecurity analyst. The LACL onboarding team often waits for partners to provide information or make technical

“People do not understand the term ‘information sharing’ – they think, ‘Oh! I’m sending my personal information to the LA Cyber Lab.’”

– Chris Covino, City of Los Angeles

adjustments. For example, it took one partner three weeks to create a technical security rule to allow information sharing (*Case-Creating a Security Rule*).

Mitigation: LACL has identified a key migration strategy: clearly provide partners with the value of joining the TISP. Currently, LACL is working on a value proposition document that shows the cost benefits of the TISP platform. When potential sharing partners better understand the value of the TISP, they will be more likely to prioritize its implementation. It is important to provide partners information in understandable contexts for executive level decision makers and technical implementers. LACL continues to refine the TISP and develop the onboarding procedures and a streamlined process.

- C. **Time: *The greatest obstacle to CTI sharing is time because it is a requirement of all parties involved.*** The investment of time is something which cannot be quantified owing to the many unknowns both technical and non-technical within each relationship. The average time for an ISAO to begin receiving CTI from a partner is 14 months. The LACL was able to dramatically shorten this timeline for several instances but has discovered that CTI sharing takes months to align people, technology, and coordination, all of which are required to complete the CTI sharing circle.

Mitigation: LACL created the “LACL+1” concept which is the method highlighting the importance of one-on-one relationships with members and partners. Building relationships with the private sector differs greatly from those with the public sector. Each has different objectives, needs, and reasons for participating.

- 1) Public Sector: Is best engaged by leading local municipalities; LACL utilized representatives from the City of Los Angeles to successfully engage other cities & counties leveraging clearly demonstrated common goals.
 - a. Common Goal 1) **Necessity:** Cities need to work together to protect themselves; beyond CTI sharing, public organizations have many other reasons to work together, but few have found a viable way to collaborate on cyber threats – until now.
 - b. Common Goal 2) **Trust:** Public organizations can easily sell their partnership with the City of Los Angeles with limited or no obstacles to share information; contrastingly, when requesting to share with private organizations, public sector officials often had many more questions and were reluctant to move forward without assurances related to privacy and access.
 - c. Common Goal 3) **Public Service:** the City of Los Angeles offered assistance in the form of the LACL to other public organizations as a public service to their fledgling security programs.
- 2) Private Sector: LACL found that in some cases private organizations wanted a relationship with the City of Los Angeles for publicity, positive marketing, and for future sales leads. However, the primary motivation for private organizations was their interest in obtaining access to information previously unavailable to them.

- a. **Social Responsibility:** The LACL has developed a narrative for larger organizations to begin CTI sharing as a part of their social responsibility.
- D. **Trust:** Creating a community in which disparate organizations are willing to provide their CTI is a challenging task. There are several stages in which the LACL gained participation in the TISP: 1) establishing contact – identifying the right person to speak with; 2) building rapport and relationships; 3) establishing value; 4) learning motivations; 5) make natural connections about the CTI sharing framework; 6) invite the organization to share; 7) coach individuals as needed about the ways and means of sharing; 8) provide honest feedback about what works and what doesn't; 9) re-enforce the altruistic and practical necessity of CTI sharing; 10) reward participation.
- a. LACL anticipated that many organizations would require a formal sharing agreement because of data sharing concerns. However, of 45 organizations, only one requested a memorandum of agreement (MOA).
 - b. Some SLTT desired to have a dedicated enclave within the TISP for city/county members only based in some type of fear that their data would be shared with the private sector.
- E. **Mitigation:** Inherent to the TISP are a series of configurations which allow organizations to control (manage) the CTI they want to contribute to the LACL community. The TISP allows for redaction and provides the ability to tag data as desired prior to sharing. These features were sufficient for each organization to have a basic level of confidence and trust in the LACL's TISP. Sharing starts with people and ends with people, relationships are the basis of all trust and the technology is the secondary means. With technology meeting industry requirements, the LACL focused on building relationships. Regarding the segregation of SLTT data, the LACL created a dedicated enclave to encourage CTI sharing but maintains that too many enclaves will further dilute the intentions of CTI sharing. Therefore, the LACL limits the creation of additional enclaves to specific use cases and pushes partners to share to a single enclave. The results have been positive in the majority of cases.

III. TECHNICAL OBSTACLES

- A. **Version Control:** The current version of the LACL TISP (TruSTAR platform) is not compatible with all software. This has slowed the onboarding process and required both LACL and partners to commit more resources towards technical troubleshooting in order to identify the unique organizational issue.

Specific Cases include:

- o *Case- Q-Radar Integration:* One partner attempted to connect with their Q-Radar tool. Organizations utilizing Q-Radar must have a version 7.3.2 or newer to connect with the LACL. Older versions will not integrate.
- o *Case- Splunk Integration:* The LACL TISP has a native integration with Splunk, a well-known and highly utilized security information management tool. However, the TISP

integration is not designed for every version of Splunk. Splunk cloud-based versions require additional configuration and setup in order to connect. Specifically, in both cases the Partner had to whitelist TruSTAR, an IP address, and set their tool to allow for the connection. Each case is different and has required time and multiple dialogs to resolve.

Solutions Moving Forward: The LACL continues to document these lessons learned and catalog them for future onboarding. Specific actions LACL will take include documenting basic configuration requirements. The basic configuration requirements depending upon the tools being used will dictate the onboarding process and reduce time, energy and confusion.

- B. Decentralized IT/Security:** Partner's struggle with internal stakeholder support & approval because there multi-layered approvals which operate on a slow timeline.
- *Case -County of Los Angeles (1):* County of Los Angeles departments provide their own IT services or contract out to the County's Internal Services Division (ISD). County ISD provides some or all IT services depending on the department request. This decentralized approach extends to security, and there is no centralized security operations center that collects data and arrogates IOC's from all County departments. The County can only arrogate IOC's from departments that choose to use ISD's services and the County can not provide an IOC feed from the entire County. To further complicate this issue, the County CISO is within the Chief Executive Office and does not have direct control over ISD.

Solutions Moving Forward: Rather than working with a central IT security agency, LACL must work with both ISD and individual departments. While LACL is pursuing this approach, individual department bureaucracy and security maturity then become issues. LACL will continue to work with the County CISO's to prioritize and strategize. Involving ISD is the first priority. **The LACL spent several months engaging the County of LA before these issues was identified.**

- *Case- Local Cities:* Initially, LACL expected smaller cities to have a more unified IT and cybersecurity. In reaching out to other cities, this assumption proved to be untrue and typically cybersecurity and IT functions have been placed under the individual department in both funding and responsibility. In one case, we observed the police department's cyber-crimes team and the city's IT to be separate and distinct organizations with completely different capabilities.

Solutions Moving Forward: LACL had to rethink its approach to SLTT as a result and has begun engaging. The LACL may need to engage individual departments rather than a centralized IT agency. However, this must happen with the help of City CIO/CISOs.

C. Data Ingestion: LACL was under the impression that organizations were already prepared to share automated threat data. Therefore, we were not anticipating many issues in the onboarding process.

- *Case -City of Los Angeles:* There has been a variety of issues while attempting to ingest City of LA data into the TISP. LACL attempted to ingest City data directly via CSV file and discovered that the City had not properly configured the data to be exported. LACL helped the City make adjustments to the naming of their exported IOCs. The idea was to ensure the information was parsed correctly once ingested. The API could only handle 500 items in a single line or 10k IOCs in a single push of data, this was discovered through trial and error. These particular API limits cannot be adjusted for ingestion purposes. Several other methods were attempted including the use of Splunk to ingest information. The City uses Splunk cloud-based version which was not directly compatible with the TISP's marketplace Splunk native integration. Adjustments to the Splunk cloud configuration and its information is flowing from the LACL to the City of LA. Currently, the City provides data via an email-based push. However, in order to automate the data flow through STIX/TAXII, a script needs to be created by the City and a stash needs to be established by the LACL to parse their data as it ingests through the API even though it will be sent in a STIX compliant format. The City doesn't have the internal capability to write the script.

Solutions Moving Forward: LACL is working with IBM to create the script to parse the data for the City of Los Angeles. However, other organizations plan to utilize Splunk and a STIX compliant format to connect with the LACL.

- **Executive Dashboards:** Partners have expressed a desire to have executive level dashboards. However, executive level dashboards are not available yet because the TruStar platform requires a minimum flow of data over approximately 90 days. LACL and TruStar also need to assess the functionality and fine tune the dashboards for partners.

Solution Moving Forward: Data began to flow into the TISP on October 2019, therefore by January 2020 the minimum data/time threshold will be met. The LACL established dashboards in February 2020 which provide details into which organizations are sharing information, how the information is being shared, and what information is being contributed and consumed.

- **Automation:** Although many of the marketing materials we have refer to a "system" that "automates" the secure sharing of Cyber Threat Intelligence, there are still a number of processes that, from my perspective, are either manual – or the Partner must complete key steps before sending the data to the TISP. For example:
 - i. Identifying data for sharing

- ii. Anonymizing data
- iii. Assigning TLPs

D. Security Infrastructure & Maturity: Many Organizations do not have the tools, processes, and staff in place to share information.

- *Case -County of Los Angeles(2):* The County CISO's have informed LACL that the County IT provider, the Internal Services Division (ISD), may lack the required security infrastructure to adequately arrogate, analyze and share the IOC's to the TISP.
- *Case -Cities of LA County:* This summer, over 85 municipalities (local cities) were invited to join the TISP. Of the five that responded, **none were technically capable of providing threat data to the LACL.**

Solutions Moving Forward: The concern is that LACL will work with Partners through Phase 0 (exploratory) and Phase I (discussion), but in Phase II (Technical onboarding) realize the partner is technically unable or limited. While LACL is actively pursuing additional partners, **time is needed to develop a clearer vetting process.** LACL is still figuring out what questions need to be asked in Phase 0 and I. The extension will allow LACL to engage with more partners and fine tune the vetting component of the onboarding Processes.

E. Marketplace: TruSTAR offers a marketplace of apps which are a list of existing integrations. The marketplace apps include a variety of IOC feeds which are available through the use of an API. The feeds are either no-cost or paid. The particular issue with these integrations is that certain apps such as Splunk, require staff time set up these to connect.

- *Case-Creating a Security Rule:* A partner's internal security measures blocked marketplace integration, this required the partner to create a new security rule. **It took three weeks for the partner to resolve the issues, causing a significant delay in the onboarding.** Although LACL is unsure of the reason for the delay, this was probably due to internal priorities, an example of the systemic issues previously mentioned impeding the onboarding process.

Solutions Moving Forward: As mentioned in the mitigation of *Systemic Issues#2 Competing Priorities/Resources-* LACL must continue to show partners the sharing value, so they are more inclined to prioritize TISP onboarding. Second, it is important to catalog solutions to quickly and clearly provide partners with solutions.

IV. ORGANIZATIONAL OBSTACLES

A. Segmented Organizations & Security Authority: LACL has encountered issues with larger organizations that lack centralized authority over cybersecurity. This issue has been seen in larger public sector (SLTT) and the impact to sharing equals a longer timeline.

- *Case- County of Los Angeles (3):* The County of Los Angeles CISO is within the County Chief Executive Office, this position provides strategic and policy guidance but does not have direct control over day to day security operations. The County's Internal Services Division (ISD) is a separate operational County division that acts as an internal managed services provider. The County's CISO and Deputy CISO have been in ongoing discussions with LACL and want the County to become a LACL sharing partner but they must work internally to bring ISD onboard, then ISD must work directly with LACL to work on the technical onboarding. This has significantly slowed onboarding.

Solutions Moving Forward: LACL continues to work closely with the County CISO to develop an internal value proposition to pitch to ISD. LACL is learning from this process and is prioritizing the creation of documentation that potential partners can use to build support internally. This case highlights *Systemic Issues#1-Unique organizations*, and the need to understand organizations to streamline the onboarding process. LACL considers a best practice to onboarding is to work closely with organizations to understand their issues. **LACL is working to streamline the approach by working closely with partners and expanding brand recognition.**

B. Organizational Risk Aversion: Some potential partners have expressed discomfort with the idea of sharing any data. During Phase I and II meetings, there is often a natural knee jerk reaction to the idea of sharing data. While third party risk is a significant issue, but information shared to the TISP is not and should not be sensitive information.

- *Case -City of Santa Monica:* The CISO for the City of Santa Monica has expressed concern about sharing data with unknown partners (i.e. LACL/TruStar). Understandably, the CISO is concerned about unvetted third parties. The CISO said they were more comfortable working directly with the City of Los Angeles.

Solutions Moving Forward: LACL has identified two strategies to mitigate these issues:

- 1) Clearly inform potential partners of the type of data that is shared into the TISP. LACL only requests IOC's, nothing that would include sensitive data. LACL needs to make it clear to partners that they decide what to share based on their risk tolerance. *Understanding the technical skill level of the partner is difficult to determine initially and at times has required extensive discussion (e.g. teaching).*

2) Leverage existing Partners to help. Work closely with the City of Los Angeles to assuage fears and provide alternative sharing solutions. For example, the City's Cybersecurity Policy Director is now working directly with Santa Monica to address sharing concerns. If a partner is still not comfortable sharing with LACL, alternative sharing options with the City are available. Information shared with the City will then become part of a larger City threat feed into the TISP.

- C. Awareness:** Even in the absence of other obstacles, the LACL discovered that information sharing was vastly more successful when organizations became aware of the LACL's mission organically. In several instances, attendees to the LACL Security Summit returned to their offices and discussed the TISP resulting in their immediate membership. Organizations which self-identify typically contact the LACL through one of their security engineers or architects.
- LACL was not contacted by a cybersecurity analyst or researcher for TISP membership during the pilot project. LACL assesses that the media and marketing campaigns did not connect with professionals in a position to either recognize the benefits of the TISP or were not in a decision-making role to request inclusion.
 - Many people were unclear about what *information sharing* meant. Further, once explained it became obvious that in many conversations the LACL was not reaching the proper individuals to engage which lengthened the process of gaining success in information sharing efforts.

V. OTHER INITIATIVES

Technical Methods / limitations

Mobile application scoring of phishing data: the construction of the light middleware application which feeds to the TISP functions as designed; a better investment in funds and future efforts could be to increase either the enclaves within the TISP or to increase the phishing specific data feeds to the BEC enclave within TruStar.

Dashboards were provided within the TISP. However, they were insufficient for the desired use cases of C-Suite and security leaders. The existing dashboards are designed for analysts which is the core function of the TISP. Executive dashboards are required to help present the information to non-technical audiences and to create business dialogs about threat intelligence and the values of the TISP.

We need to push "protection through partnership" and "how do we work together?" - We work together by sharing information. Not any information but specific information.

TISP Management Best Practices

Sharing Concerns

RH-ISAC for example, two analysts on staff to review submitted data for vetted intelligence which they pull insights out. Intelligence is then shared to another enclave which is subscribed to.

Ingestion:

A community of trust in which members share information of which the value is undetermined. LACL requests all members to provide quality data which they believe to be high confidence intelligence.

Policy and Management: provide best practices of tagging and labeling data prior to sending in IOCs. LACL can mature the program by enforcing submission best practices.

Subscriptions:

Establish a new enclave which can be shared at a later date. As membership grows, LACL can provide a new feed which it rolls out later with vetted intelligence.

Create enclaves for members who were owned by malware and offer it to other members.

LACL has not established a direct feed for members but instead uses the ingestion tool as the exportation location.

SOC best practices: a SOC manager may assign a higher confidence to a vetted source despite subscribing the LACL general feed.

Recommendation #1: DHS NCCIC is requested to confer with LA Cyber Lab about previous/past successes and failures utilizing API & STIX/TAXII protocols for bidirectional machine to machine data sharing. Specifically, any preexisting use cases which could be relevant to the LA Cyber Lab's efforts would be appreciated as it begins the RFP cycle.

Conclusion #1: Feedback from Dollar Shave Club security team was: provide automation on shared IOCs in the form of ingestions rules. When a STIX pull is initiated by the ISAO member IOCs with rules will automatically *"block at firewall & flag for review"* – The LA Cyber Lab is incorporating this request into the scope of work for the project.

Conclusion #3: Members are looking for changes in the current daily threat report which provides infosec news. The LA Cyber Lab is creating a Special Alert Report which will provide members the ability to receive timely notice of LA specific threat intelligence. The special report will focus on one

subject with a brief description of the issue & actions available via embedded links. Additional functionality to the existing reports will give the members the ability to select the frequency of how often they receive reports (e.g. daily, weekly, special, etc.)

Conclusion #4: Private sector companies want more data enrichment on IOCs being shared from the LA Cyber Lab. The most likely way to do this is in the analysis phase of the CONOPS. Additional information is needed to define what type of data enrichment the LA Cyber Lab might be able to provide. *This information is consistent with conclusion #1.*

Conclusion #5: One obstacle to information sharing is the perception that sharing information which is not actionable is viewed by some as “providing more noise.” Specifically, POLA has defined a narrow space within which they want to share threat information but the use of the LACL as their portal is likely not the best strategy because they view the LACL portal as *too much information* for their niche group of partners.

Conclusion #6: The National Homeland Security conference event could have more cyber sharing-centric focused tracks for ISAO/ISACs; the MS-ISAC conference was a good event for networking and for promotion of the LA Cyber Lab.

Conclusion #7: Members sharing information to the LACL via the threat intelligence sharing portal might be limited by the software version of their existing tools. The LACL is identifying which tools and versions are compatible.

Conclusion #8: Partners will share information on their own timeline. There is virtually no incentive to motivate partners to share before they are ready. LACL has attempted to motivate partners with vary limited success despite employing the standard methods of engagement.

Conclusion #9: Most SLTT members were not in a position to take advantage of the Cyber Lab’s free threat intelligence. We found that the majority of attendees were outsourcing their IT and cybersecurity. We also discovered that the key to making connections with the tribal organizations was to attend their meetings in person versus electronic or telephonic communications.

Conclusion #10: SMB has traditionally been a difficult group to engage through information sharing. The mobile app is creating a new means of interacting with these businesses. Adoption of the app and usage will be the keys to future success.

Impacts of the Pilot Project

What is the impact of the project? How has it contributed?

The pilot project is providing a nexus for SLTT and business to communicate. Further outreach is required to broaden the impact of this grant funded opportunity.

SMB has traditionally been a difficult group to engage through information sharing. The mobile app is creating a new means of interacting with these businesses. Adoption of the app and usage will be the keys to future success. Currently there are 219 authenticated downloads of the mobile app.

The mobile app has become a great conversation starter with people at all levels of business and often leads to a deeper conversation of the TISP.

What is the impact on the development of the principal discipline(s) of the project?

No other convergence of technology currently exists. This is the first time an enterprise tool is being used to facilitate sharing to a community level. Existing solutions and tools provide threat intelligence to mature security organizations and teams.

The mobile phishing app wraps around the TruSTAR API and pulls IBM IRIS results for emails being ingested through the app. This effort is pioneering the future of threat information sharing and aggregation.

What is the impact on other disciplines?

Data from the pilot project may become useful for researchers looking to discover trends and analysis of indications of compromise in the region.

What is the impact on the development of human resources?

None, this project does not substantially change the process or fundamentals utilized by cybersecurity analysts. The impact to cyber threat analysts' being informed and able to work with and collaborate with other analysts is improved through this pilot project.

What is the impact on physical, institutional, and information resources that form infrastructure?

None, the pilot project is a cloud-based architecture and does not create additional infrastructure physically or institutionally.

What is the impact on technology transfer?

None, this pilot project had no impact on technology transfer.

What is the impact on society beyond science and technology?

The LACL's mobile app could prove to be a vital connection between SMB and the greater Los Angeles business community; this is the first time where enterprise level CTI has been used as a data source linking SMBs. Managed security services provide some access to SMBs but no direct link or access to higher level CTI.

What dollar amount of the award's budget is being spent in foreign country(ies)?

None of the grant funds were spent with foreign countries or outside of the United States of America.

Develop Documentation

Develop documentation including design, policies and procedures, CONOPS, and operations manual(s).

Policies, Procedures, Techniques

The LACL created the following documentation during the pilot project to guide

Policies

- LACL Acceptable Use Policy
- LACL Access Control Policy
- LACL AWS Database Credentials Policy
- LACL Frequently Asked Questions (FAQs)
- LACL IBM Policy Guidance
- LACL Intellectual Property
- LACL ISAO Framework
- LACL Mobile App Security Policy
- LACL Mobile App User Manual
- LACL Mobile Application Responsiveness Policy
- LACL Payment Process
- LACL Privacy Policy
- LACL Systems and Infrastructure
- LACL Threat Sharing Capability
- LACL TISP Support & Maintenance Procedures
- LACL Travel Policy
- Threat Intelligence Sharing RFP Diagram (CONOPS)
- TruSTAR Support & User Manual

Procedures

- LACL Change Request Form
- LACL Configuration Management Policy
- LACL Information Protection Security Change Management Policy
- LACL Information Protection Security Password Policy
- LACL Partner Sharing Policy
- LACL Data Retention Policy
- LACL TISP Partner Onboarding Policy

Techniques

- Analysis Methodology
- Feed Overlap Analysis Matrix

- IOC Use Cases (MISP)
- LACL IBM X-Force Exchange Risk Scoring
- LACL Middleware Email Scoring
- LACL Mobile App Final Wording for Threat Levels
- LACL Threat Data Sources
- LACL TISP Dashboards
- LACL TISP Middleware Cloud Architecture
- LACL TISP Reports
- LACL TISP Admin Instructions
- LA Cyber Lab Mobile Application Test Scrips Execution
- LA Cyber Lab Unit Tests Execution Consolidated Feedback and Issues

LACL TISP Maturity Model

Threat Intelligence Sharing Platform (TISP) Maturity Model			
	Basic <-----> Advanced		
Level	Access	Integration	Sharing
What	Access to threat intelligence data through the TISP (TruSTAR platform web application).	TISP access and threat intelligence data integrating with security tools	Full security tool integration, including aggregating and sharing IOC to the TISP
	Indicators of Compromise (IOC)	IOCs & Research Enrichment	IOC Reports & Case Enrichment
Benefit	Provides additional security insight. Users can see shared threat data, perform research, see trends etc.	Integrated threat data to make analysts and tools more accurate and efficient.	IOC's from the TISP are integrated into security tools, organizations share IOC into the TISP.
	Benefit to Member	Benefit to Community	Benefit to All
Sharing	Can manually upload reports (e.g. CSV)	Can manually upload reports. Limited Automated Sharing with existing integrations.	Automated Sharing between tools and TISP via API or STIX/TAXII
Who	Smaller organizations that lack the infrastructure for integration of sharing.	Medium organization with some security tools and limited staff.	Organizations with dedicated security staff and mature security infrastructure.

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

Role	Researcher, Analysts, Engineers, Investigators		
		Security Engineers	
Requirements	TISP account and web browser	TISP account & Tools capable of ingesting threat intelligence	Organizational capability to identify suspicious and malicious traffic and the ability to share data

Social Media Outreach

The Facebook groups LACL engaged included communities of information security professionals, IT professionals, programmers, computer scientists/engineers as well as women groups wanting to explore the cyber field. The primary mission of these groups is to advance women in cybersecurity by providing programs and partnerships that promote networking, education, mentoring, resource-sharing and opportunities. Most LACL followers are interested in LACL TISP, training programs, networking and job searches.

- Women in Cybersecurity (WiCyS)**most interested in LACL*
- Women’s Cyber Jjutsu
- Los Angeles Business Group
- Cybersecurity Professionals
- Cybersecurity Jobs
- Cybersecurity Lounge

LACL maintains the following social media accounts used to interact with the community:

Facebook	Los Angeles Cyber Lab	Created July 2, 2019 with no presence or followers; currently has 147 followers
Twitter	@LACyberLab1	Created in 2017 – Posting tweets regularly
Instagram	CyberLabLA	Created in 2018 – Limited Use
LinkedIn	Los Angeles Cyber Lab	Created September 2019 – abandoning the LA Cyber Lab account
YouTube	Los Angeles Cyber Lab	Created August 2017 - 7 videos

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization



Conclusions

More interest and followers could be gained with providing academic cybersecurity training programs, job placement/opportunities and networking events.

Work with Academic Partners

Work with Academic Partners

Work with academic partners who will utilize the IS-ISAO operation center to provide real world learning environments to improve student skills and identify research opportunities for students and faculty to explore the full spectrum of cyber technology.

The LACL engaged the academic institutions in a variety of ways to explore information sharing opportunities. Academic institutions each have their own niche within the cybersecurity education continuum. As the LACL worked with each organization it identified the unique assets, potential for collaboration and audience these groups served. Larger academic institutions have multiple departments and organizations within the overarching structure and are largely siloed both in terms of budget and information. Effectively engaging these organizations requires a deep understanding of their capabilities and interests. The LACL explored creating courses in cybersecurity, certificate programs, undergraduate and graduate level research projects, and leadership seminars. Ultimately, the LACL was abandoned creating courses and certificate programs because of time and resource constraints. The LACL lacked substantial data to propose a meaningful research program and decided to re-engage in those conversations at a later date. Success was achieved with academic partners in two ways: participating in business school cybersecurity seminars and in supporting student learning through hands on access to CTI via the LACL TISP.

University of Southern California (USC) Information Sciences Institute (ISI), a leading graduate research university within Los Angeles, California, has been a member of the LACL Advisory Board since its inception. USC-ISI provided some initial thoughts and posed questions to the LACL during its creation of the TISP concept of operations. USC-ISI expressed desire to further discuss potential research opportunities with its engineering students but was unable to provide the LACL with any ideas, research proposals or concepts. The LACL database of IOCs was too small for USC-ISI to work with during the pilot period. As LACL IOC data grows through contributions of its members, USC-ISI and LACL will revisit the topic and determine what contributions can be made to the community through academic research.

USC Policy Program Initiative:

The University of Southern California, in partnership with the Office of Los Angeles Mayor Eric Garcetti is planning an interdisciplinary Cyber Policy Initiative. This joint initiative will include USC's schools of Public Policy, engineering, law, business administration, communication, the Mayor's Office of Public Safety, and the Los Angeles Cyber Lab. Strategic Direction would come from an interdisciplinary advisory board. The objective of the initiative is to produce interdisciplinary policy, people, and

programs to address the growing cyber challenges. To achieve this, the initiative will 1) *Develop a Cyber Policy Master and certificate programs* 2) *Produce cyber policy-relevant research focused on interdisciplinary understanding and solutions* 3) *Create real word opportunities for students and practitioners* 4) *Host events to promote the USC's Cyber policy initiatives and other national cyber policy initiatives.*

I. Developing a Cyber Policy Master's and certificate programs

- Create integrated cyber policy degree and certification program options for students in the Policy, Engineering, Law, Business, and communications schools.
- Explore other interdisciplinary cyber degree programs

II. Produce cyber policy-relevant research focused on interdisciplinary understanding and solutions to cyber issues - possible areas of research:

- Providing cybersecurity as a public service
- Economic, social, and physical cyber resilience
- Public - Private information sharing challenges
- Public - Private Partnerships
- Cyber risk perception and translating risk to decision makers and the public
- Entertainment and media cyber/tech perception

III. Create real word opportunities for students and practitioners

- City of Los Angeles Mayor's Office, Cyber Policy Fellowship (govt focused)
- Los Angeles Cyber Lab, Cyber Policy Fellowships (public-private focused)
- Capstone and practicum cyber projects
- Workshops for the community
- Local government workshops and table tops
- Partnerships with LA's entertainment and media industry

IV. Host events to promote the USC's Cyber policy initiatives and other national cyber policy initiatives.

- Co- host an annual summit with the City of Los Angeles focused on Cyber policy and collaboration
- Host National workshops/events for highlighting specific policy issues (ex. elections, risk perception, information sharing, translating etc.)

University of California at Los Angeles (UCLA) Extension is a non-degree conferring organization offering courses for those seeking to learn without gaining credit hours or participating in a formal degree earning program. UCLA Extension is a popular way for professionals to gain knowledge without

the rigors and commitment of advanced academic programs. The courses are open to all levels of learners. LACL engaged UCLA Extension to discuss the creation of cybersecurity programs and courses. UCLA Extension was open to discussing the creation of courses if the LACL had content and course curriculums to propose. UCLA Extension is interested in helping fill the skills gap among the cybersecurity workforce. The timeline for UCLA Extension to move through the course creation and certification is about 18 months. LACL did not have content or the capacity to develop courses within the pilot period. LACL abandoned this effort since many other cybersecurity higher education programs exist both within the greater Los Angeles area and online. Our efforts and resources were better spent on developing the TISP.

On July 24th, the Outreach Director spoke about the LACL and the Security Summit at the UCLA Bruins Alumni Professional Organization.

LACL cohosted a community event in partnership with the University of California Los Angeles (UCLA) Burkle Center for International Relations; *“How Hackers, Laws, Cybersecurity and Regulators Connect in a Connected World”*.

The LACL sought to engage academic partners in a variety of ways. In particular, DHS CISA Director Bob Kolasky participated in a community event with the Executive Director and a partner providing a thoughtful and engaging discussion on the collective cyber defense of our community and nation. The event had over 100 attendees and was held in conjunction with the University of California Irvine Cybersecurity Policy & Research Institute.

Pepperdine University - Graziadio Business School (GBS) is an emerging leader among business schools in California. GBS hosted the LACL as part of the 2019 Cybersecure SoCal event in October 2019. During this event the LACL discovered that business graduate school students and alumni represent a unique subgroup of the business community, with their own networks and events catered to meeting their business needs. LACL presented to the group and posted information from the event via linked-in which saw the greatest number of interactions for any LACL related post during the pilot period. LACL concluded that previous efforts to connect with academic partners in engineering, information, and computer science departments while important, left out a major portion of business professionals from the business schools and other programs such as public policy and criminal justice. From this event, the LACL gained support from the Pepperdine University CISO and added the university to its Advisory Board.

LACL presented at the Pepperdine University, Graziadio Business School event in association with SecureTheVillage; the event connected with CISOs and tech professionals during Cybersecurity Awareness Month. *Pepperdine was added to the LA Cyber Lab’s Advisory Board expanding its partnership with the ISAO.*

California State Polytechnic University, Pomona (Cal Poly) is an undergraduate university focused on hands-on learning. The unique focus of Cal Poly led to the LACL’s discovery of their student led security operations center (SOC). The Student SOC is part of the university’s College of Sciences and is in its

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

infancy and was initially funded by Northrop Gruman. LACL attended the school's technology fair and offered the TISP to the Student SOC at no cost, in order to fill a gap in their security tool set. Cal Poly gained access to the TISP four months later. Currently, the LACL is partnering with their faculty to identify opportunities to promote their Student SOC program. LACL intends to help Cal Poly establish a cadre of cyber analyst students who will interact with TISP data and provide reports back to the LACL TISP community based upon the members shared information. Cal Poly is one of the newest members of the LACL Advisory Board.

Cyber Work Force Development

Cyber Work Force Development

Develop hands-on cyber work force development programs in collaboration with academia.

Trainings – Types

The LA Cyber Lab Program Director led the fellowship program; they reviewed over 60 resumes and offered eight interviews of which four were accepted. Two interviewees were selected to replace the existing fellows and will begin in August and September; the fellowships are sponsored by City National Bank.

Outreach for the LACL was significant during the month of August 2019. The LACL spoke at local business leader forums and conferences, held an SLTT meeting, hosted several speaker series discussions, and hosted a hands-on analyst training with the National Cyber Forensics Training Agency (NCFTA). These events were successful in bringing many new connections to the LACL. The intent was to drive interest towards the Security Summit in September and increase information sharing through our daily threat report.

The darkweb training event received positive feedback and interest. LACL raised its social media profile through this event because the training was free to the public. The training increased participant's knowledge and awareness of threats. The LACL was able to connect with Sony threat researchers and build a dialog for future potential collaboration. The training had 33 registrants and 20 attendees for the 2.5-day sessions. These training sessions are a positive way of engaging the community because it allows peers to meet, learn, and interact with the LACL.

LACL held 4 one-hour training sessions throughout the two-day event and received the greatest interest, at least two sessions were standing room only. The training sessions were included in the event at no additional cost; training topics included 1) Wireshark, 2) Cyber Analyst Incident/Information management, 3) Data breach incident tabletop exercise, 4) Red Team Hacking

and one other additional analyst focused topic. ISSA offered CPEs for attending the summit.

Connecting The Community

September 17-18, 2019 - Training Agenda

Time	Training Topic	Presenter
9/17 - 2:00 Santa Monica D	Deep Packet Analysis with Wireshark and Tshark Part #1	Candan Bolukbas, NormShield In this meetup we used Wireshark to decrypt HTTPS streams, reconstruct audio streams and analyze sophisticated attacks. We also used tshark to analyze pcap file and extract field to process with command line tools. Please make sure that you have Wireshark and Tshark installed.
9/17 - 3:00 Santa Monica D	IT Risk in Motion Tabletop Exercise	Robert Kang, Loyola University & Special Guests Crisis response in a major cyber breach takes planning and training; get the full effect of what are the best practices and also the things not to do during this role-playing session.
9/18 - 10:00 Santa Monica D	Red Team Hacking	Dioly Alexandre, BlackShield The most successful teams have to know how they are being attacked. Thinking like a hacker is only half of the equation; learn the general methodology and explore concepts in tools which make your job easier.
9/18 - 2:00 Santa Monica D	Operationalizing Intelligence from Sharing Communities	Patrick Coughlin, TruStar Sharing communities like the LA Cyber Lab provide critical connective tissue for exchanging intelligence across enterprises. But they come in many different forms and the data is often unstructured and orthogonal to existing security workflows. In this session, we'll present the common challenges associated with operationalizing intelligence from different types of sharing communities and we'll share some technical tools and tips for how to make the most of your sharing community intelligence.

The Cyber Lab hosted a day long training with CISCO Security for students, analysts, researchers, and cybersecurity professionals. There were 28 attendees who learned about network security and participated in a capture the flag event. Both SLTT and private sectors were among the attendees.

Partners – STV, CISCO, NormShield, BlackShield, etc.

Speakers Series, Summit, Hands-on

LACL Sustainability & Future Recommendations

REGIONAL CYBER ISAO PILOT PROGRAM

The Cybersecurity and Infrastructure Agency (CISA) has identified threat sharing as essential to protecting critical infrastructure and furthering national cybersecurity. Federal agencies and national sector-based information sharing centers have led threat sharing efforts through a top down approach for years. However, the Ransomware epidemic highlights the need for a new level of threat sharing between federal, state, and local governments, as well as the private sector. The LA Cyber Lab and City of Los Angeles are now advocating for state and local governments to lead local efforts to complement existing federal and national threat sharing by establishing regional interconnected Information Sharing Analysis Organizations.

This pilot program lays the foundation for a nationwide and locally implemented threat sharing network by establishing 3-4 regional Information Sharing Analysis Organizations (ISAO). Specifically, the pilot will export the LA Cyber Lab ISAO model and leverage the LA Cyber Lab's Threat Intelligence Sharing Platform (TISP) to connect regions. Many regions are working towards a coordinated approach, and this will build on those efforts, promote local innovation, and ensure national interoperability. To implement this, LA Cyber Lab will provide pilots sites with a regional coordinator, a sharing platform, and ongoing support.

Connecting the Community

Through the *Connecting the Community* initiative LACL has become a foundational member of the Los Angeles cybersecurity ecosystem. The LACL advisory board includes over 30 private sector partners and the County of Los Angeles. In January 2020, the City of Los Angeles, LA Cyber Lab, and the other local municipalities partner to establish the Regional Cyber Coordination Group (RCCG). The RCCG provides local governments with cybersecurity resources, knowledge, and works towards future collaboration.

Joint Cyber Intelligence Integration Task Force

In February 2020, LA Cyber Lab, the City, and the Joint Regional Intelligence Center partnered to form the Joint Cyber Intelligence Integration Task Force (JCIITF). The JCIITF's innovative approach brings together the Greater Los Angeles Region's intelligence partners to integrate and improve cyber threat analysis and information sharing. The JCIITF works closely with the Regional Cyber Coordination Group

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

(RCCG), California Cybersecurity Integration Center (CAL-CSIC), the Cybersecurity and Infrastructure Security Agency (CISA), and the Federal Bureau of Investigation (FBI).



CONTINUING THE PARTNERSHIP AND EXPANDING THE MODEL

The LACL now seeks to continue its partnerships with the Cybersecurity and Infrastructure Security Agency (CISA) to build on these successes and further develop the LA Cyber Lab as model Internet Security - Information Sharing Analysis Organization (IS-
ISAO). Specifically, funding will allow LACL to stay a key player in the region's security by continuing to expand private sector TISP participation, workforce development, and be active in the RCCG and JCIITF. Further, funding will allow LA Cyber Lab to support the City of Los Angeles as it establishes threat sharing partnerships with other major metropolitan cities.

In addition to regional initiatives, LACL is also looking to export the ISAO model and lay foundation for a national threat sharing network by establishing 3-4 regional Information Sharing Analysis Organizations (ISAO). The pilot program will promote local relationships, regional innovation, and ensure national interoperability. Specifically, LACL will provide pilot sites with a regional coordinator, 15-30 sharing platform accounts, and ongoing support. Cities of San Antonio, San Francisco, and the Cyber Resilient Massachusetts Working Group have all expressed interest in becoming pilots sites.

LACL suggests sustainment funding for one year: \$1.1M; two years: \$2.1M.

Funding to the LACL will support existing and expanding capabilities. A high-level overview of LA Cyber Lab Initiatives

Threat Intelligence Sharing Platform (TISP)

- Expand participation and continue to provide the service free for the private and public sectors.
- Threat Analyst team to analyze and refine TISP partner data to produce improve TISP data and produce in depth intelligence products and timely advisories.
- Additional licenses for new TISP members

Regional ISAO Pilots - Extending the Cyber Lab Network

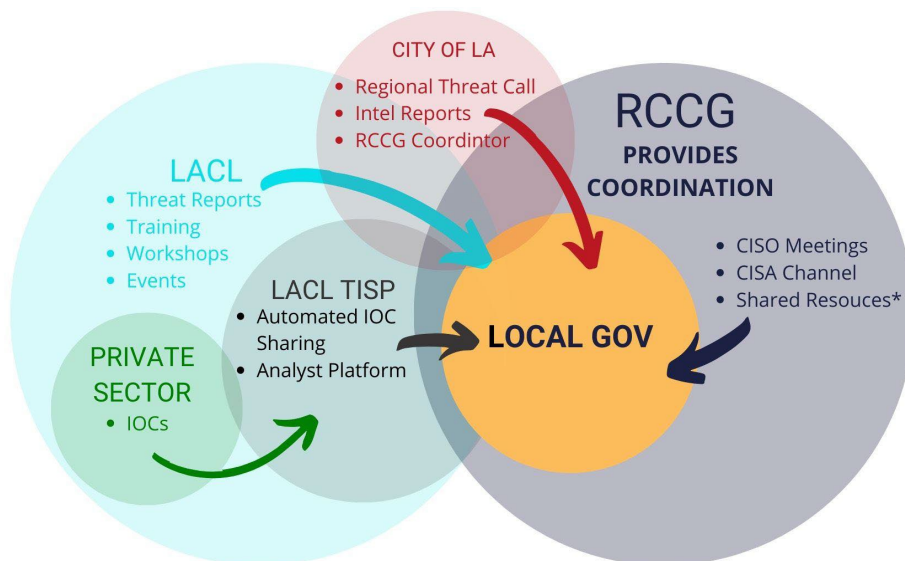
- Establish pilot program to build a nationwide threat sharing network by establishing 3-4 regional Information Sharing Analysis Organizations (ISAO).
- Provide pilots sites with a regional coordinator, sharing platform accounts, and ongoing support.

Workforce Development, Education, and Events

- LA Cyber Lab Academy - provide advanced training opportunities to tech professionals
- Expand training opportunities - connect tech community and underserved workforce populations in the region
- Workshops for small and medium business - town hall style meet-ups which provide practical application of security

Regional and National Cybersecurity

- Continue to be a key member in the RCCG and JCITF, supporting the regions SLTT community with threat sharing, training, and other support.
- Build joint threat sharing partnerships with the City of Los Angeles and major US cities



Center of Cyber Excellence for Information Sharing

- Establish a Center of Cyber Excellence with Academic partners
- Study and analyze information sharing to understand barriers, benefits, and best practices.
- Make policy recommendations to local, state, and federal lawmakers to improve private and public sector information sharing

Regional ISAO Pilot Overview

LA Cyber Lab and the City of Los Angeles are now looking to export this model and connect regions through a single sharing platform. LA Cyber Lab will provide¹⁷ 3-4 sites with:

- The Threat Intelligence Sharing Platform

¹⁷ Depends on federal funding

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

- Regional Coordinator/Analyst
- Regional advising, support, and assistance

Regional ISAO Objectives

Establishment

- Establish a regional ISAO by integrating the function into an existing organization or establishing a new organization
- Integrate the ISAO into existing threat sharing and regional cybersecurity efforts

Threat Sharing

- Provide public and private sector partners with timely and relevant cyber threat information through the TISP, briefings, advisories, and reports
- Build local relationships and capacity to facilitate threat sharing with the public and private partners
- Identify threat sharing barriers and best practices
- Share threat information with LA Cyber Lab, other pilot ISAOs, and federal partners through the TISP, briefings, and reports.

Regional Cyber Support

- Assist State Local Tribal and Territorial (SLTT) governments
- Other innovative initiatives as decided by pilot sites

Pilot Principles

- **Local Implementation:** Locally implemented ISAOs are in the best position to build trust and relationships that are necessary for threat sharing. Furthermore, local authorities will know the best way to integrate ISAOs into the existing cybersecurity ecosystems. For example, the ISAO function could be integrated into an existing SLTT organization, such as a major city, fusion center, state agency, or a non profit. Alternatively, pilot partners could follow the LA Cyber Lab approach and create a public-private partnership.



Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

- **Regional Innovation:** Pilot sites would be regional experiments in ISAO integration, relationship building, partnership collaboration, threat sharing and new initiatives. Success and failure can be documented and best practices can be developed. Cyber threat sharing is still in its infancy, and experimentation and innovation will drive progress.
- **National Network:** Pilot sites would be directly connected to Los Angeles Cyber Lab through the Threat Intelligence Sharing Platform. The goal is a national network of ISAOs, allowing for rapid threat sharing. This regional ISAO will also provide federal partners with an established network.
- **Long Term Interoperability:** IASOs will facilitate technical connections and formal relationships between major metropolitan areas. Building these connections and relationships now will ensure long term threat sharing interoperability. As regions improve their ability and infrastructure to identify and share indicators of compromise, it's important regions use common methods and tools for communicating

LACL Conclusions

The LA Cyber Lab has made great progress in the fulfillment of its Mission and Vision. However, much work remains, and it is critical to the continued success of the LA Cyber Lab to have a fully engaged team of staff, volunteers, Advisory Board Members and the business community that are willing to creatively engage the private sector and dedicate the needed time and resources. The threat of Cyber attacks is all too real and becomes more lethal every day making the Mission of the LACL truly important to a free society and the maintenance of our way of life.

Future sustainability of the LA Cyber Lab

The project is tied too close to the City of Los Angeles in that when people hear about the LA Cyber Lab, they think this is a city managed initiative. The City of Los Angeles is a municipality and doesn't treat the LA Cyber Lab as a non-profit business which has had a negative impact on relationships with the private sector. The perception by businesses is that the LA Cyber Lab is part of the City which implies they are being requested to share information with a local government.

Businesses do not prioritize the LA Cyber Lab and therefore while they have expressed interest in sharing they move slowly, often requiring months of engagement before moving forward with real threat intelligence sharing.

Participating in the LA Cyber Lab is not properly incentivized. Businesses and local governments do not perceive a real value from their participation. Despite LA Cyber Lab efforts to explain and express the benefits of sharing information the businesses struggle to define the benefit they might derive from participation. Participating to benefit the community is altruistic and does not necessarily resonate as a motivation for businesses to allocate resources to provide information to the LA Cyber Lab when resources are already limited.

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

The image shows a screenshot of the Los Angeles Cyber Lab LinkedIn profile page. At the top, the LinkedIn navigation bar includes a search bar, Home, My Network, Jobs, Messaging, Notifications, Me, Work, and Learning. The profile header features the LA Cyber Lab logo (a shield with three people icons) and a cityscape background. The page title is "Los Angeles Cyber Lab" with the description "Information Technology & Services - Los Angeles, CA" and "19 followers". A "Following" button is visible. Below the header, there is a "Connecting The Community" section with a "Learn more" link and a note that "Rick works here" with a link to "See all 2 employees on LinkedIn". The main content area shows a post from the Los Angeles Cyber Lab (19 followers) thanking Joshua Belk, CEH, and partners for their support, using hashtags #informationsharing, #cyberdefense, #losangeles, and #communities. Below this is a post by Joshua Belk, CEH, a Cyber Expert and Security Evangelist, praising a community social impact. A "Highlight" section on the right shows a trending post in #cybersecurity about "500 Chrome Extensions Caught" from thehackernews.com.

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

Appendix A – Financial Accounting

A detailed listing of the financial activities of the pilot project are recorded via FFR submissions to GrantSolutions.Gov. LACL maintains accounting records for the pilot project which have been provided to DHS CISA and are available upon request. Below is a high-level spending breakdown of the pilot project.

Annual Budget Internet - Security Information Sharing and Analysis Organization (IS-ISAO) Pilot <i>Project Period: 10/1/2018-3/31/2020</i>				
APPR CODE	Cost Category <i>Select from Dropdown</i>	IS ISAO Grant Objective(s) <i>Select from Dropdown</i>	Item	Total Budgeted Cost
ISAO-C-0001	Travel	Bi-Lateral Cybersecurity Information Sharing	MS-ISAC Annual Meeting - 28 April - 1 May Denver, CO	\$ 3,420.82
ISAO-C-0002	Travel	Bi-Lateral Cybersecurity Information Sharing	ISAO Standards Organization International Information Sharing Conference (IISC) - 20-23 August, 2019, San Antonio, TX	\$ 2,464.08
ISAO-C-0003	Travel	Bi-Lateral Cybersecurity Information Sharing	National Homeland Security Conference - June 17-20, 2019, Phoenix, AZ	\$ 2,636.31
ISAO-C-0004	Travel	Bi-Lateral Cybersecurity Information Sharing	ISSA CISO Forum & Women in Cyber Confernece	\$ 1,956.54
ISAO-C-0005	Travel	Bi-Lateral Cybersecurity Information Sharing	FEMA Region IX Cyber Workshop Series - July 9, 2019, Mountain View, CA	\$ 306.84
ISAO-C-0006	Travel	Identify Barriers to Information Sharing	LA Cyber Lab Security Summit 2019; Sept 17-18, 2019, Los Angeles, CA	\$ 2,565.41
ISAO-C-0007	Travel	Bi-Lateral Cybersecurity Information Sharing	RSACON 2020, Feb 24-28, 2020, San Francisco, CA	\$ 8,000.00
Total				\$ 21,350.00
ISAO-D-0001	Equipment	Establish Fully Functional IS-ISAO	Smart Board Screens or Situational Awareness Monitors (x2)	\$ 23,000.00
ISAO-D-0002	Equipment	Establish Fully Functional IS-ISAO	Other Situational Awareness Equipment	\$ -
ISAO-D-0003	Equipment	Develop Documentation	Laptop or Desktop Computer Suite (x4)	\$ 12,000.00
ISAO-D-0004	Equipment	Establish Fully Functional IS-ISAO	Office Furniture	\$ 12,242.66
Total				\$ 47,242.66
ISAO-E-0001	Supplies	Establish Fully Functional IS-ISAO	Office Supplies	\$ 2,000.00
Total				\$ 2,000.00
ISAO-F-0001	Contractual	Bi-Lateral Cybersecurity Information Sharing	Threat Intelligence, Analysis, and Sharing Platform (TIASP) - Hardware, Software, Labor, Etc.	\$ 1,200,000.00

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

ISAO-F-0002	Contractual	Bi-Lateral Cybersecurity Information Sharing	Threat Intelligence, Analysis, and Sharing Platform (TIASP) - Support & Maintenance	\$ 634,290.00
ISAO-F-0003	Contractual	Establish Fully Functional IS- ISAO	Executive Director (ED) / Chief Development Officer (CDO)	\$ 173,838.28
ISAO-F-0004	Contractual	Identify Barriers to Information Sharing	Policy Director	\$ 36,000.00
ISAO-F-0005	Contractual	Identify Barriers to Information Sharing	Program Director	\$ 91,400.00
ISAO-F-0006	Contractual	Cyber Work Force Development	Outreach Director	\$ 26,710.00
ISAO-F-0007	Contractual	Establish Fully Functional IS- ISAO	Cyber Threat Analyst	\$ 247,987.06
ISAO-F-0008	Contractual	Establish Fully Functional IS- ISAO	Data Scientist / Visualization Analyst	\$ 39,045.00
ISAO-F-0009	Contractual	Establish Fully Functional IS- ISAO	Grant Management & Administration	\$ 150,000.00
Total				\$ 2,599,270.34
ISAO-H-0001	Other Direct Costs	Establish Fully Functional IS- ISAO	LA Cyber Lab Website	\$ 18,944.67
ISAO-H-0002	Other Direct Costs	Bi-Lateral Cybersecurity Information Sharing	Situational Awareness Room Events	\$ 19,000.00
ISAO-H-0003	Other Direct Costs	Bi-Lateral Cybersecurity Information Sharing	LA Cyber Lab Summit	\$ 147,230.33
ISAO-H-0004	Other Direct Costs	Work with Academic Partners	Conference/Outreach Events	\$ 30,000.00
ISAO-H-0005	Other Direct Costs	Establish Fully Functional IS- ISAO	Media Production (Photo/Video)	\$ 56,825.00
ISAO-H-0006	Other Direct Costs	Establish Fully Functional IS- ISAO	Marketing - LA Cyber Lab Continual	\$ 21,000.00
ISAO-H-0007	Other Direct Costs	Cyber Work Force Development	Marketing - Events, Outreach, and Conferences	\$ 30,000.00
Total				\$ 323,000.00
Grand Total				\$ 2,992,863.00

Appendix B – Outreach Activities

The following is a list of the outreach activities conducted during the pilot project.

Training

Oct 2018

Nov 2018

Dec 2018

Jan

Feb

Mar

Apr – MS-ISAC

May

On **May 30th**, the Outreach Director participated in the SecureTheVillage Leadership Council, attended by 41 local professionals, where he discussed the LA Cyber Lab key initiatives, the current status of the threat sharing portal and upcoming events.

On **June 4th**, the Executive Director and Mr. Jacob Finn attended the Southern California CISO Summit. The two engaged attendees and participated in various presentations obtaining several new commitments from SLTT and private sector organizations to become members of the LA Cyber Lab with the potential for partnership inclusion in the current bidirectional information sharing initiative.

On **June 6th**, **June 9th**, **June 11th**, and **June 14th**, the Outreach Director participated in networking events and attended two webinars to evaluate current trends in the security industry and to identify potential subjects for future LA Cyber Lab events.

On **June 13th**, the LA Cyber Lab staff completed a web application bootcamp with The Rosslyn Group. The teams explored the user experience of the mobile application and developed the framework for the user interface. The mobile app will be the primary means of interaction with SMB and the community.

On **June 17th**-, the LACL attended the National Homeland Security Conference, Phoenix, AZ to facilitate further adoption and increased participation amongst SLTT.

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

On **July 24th**, the Outreach Director spoke about the LACL and the Security Summit at the UCLA Bruins Alumni Professional Organization.

On **July 31st**, the LALC is hosted a Situational Awareness briefing for members to update them on the pending launch of the mobile phishing application and the threat intelligence sharing platform. There were 27 attendees and from the group breakout sessions the following feedback was provided by the members: 1) LACL TISP data should be non-attributable; 2) Security Summit outreach should include connections with the LA Chamber of Commerce and upcoming SLTT events.

On **August 7th**, the LACL hosted an SLTT event at the City of LA EOC to discuss participation as part of the LA Cyber Lab threat sharing initiative. The cities of Burbank, Lynwood, and Monrovia were represented. Each of these cities expressed interest in membership but none were in a position to become sharing partners.

On **August 7th**, the LACL co-hosted a speaker's series panel discussion *Cyber Risk: The Cyber Security and Cyber Privacy Threat Landscape*. Over 28 professionals attended the event.

On **August 9th**, the LACL Executive Director spoke at the SecureTheVillage monthly leaders in security business breakfast.

On **August 21st & 22nd**, the LACL Executive Director presented *Anatomy of an IOC and Information Sharing Changes* at the annual Information Sharing Conference for ISAOs.

On **August 22nd**, the LACL co-hosted a cyber resiliency speaker's discussion with Homeland Security Advisors Council (HSAC), an Advisory Board member of the LACL, which was attended by 95 public sector and non-profit professional.

On **August 27-28th**, the LALC is hosted a hands-on analyst training workshop *Accessing The Darkweb* with NCFTA.

On **August 28th**, the LACL is cohosted a speaker's series panel discussion *Securing The Human: Growing the Community*.

On **August 28th**, the LACL sought to engage academic partners in a variety of ways. In particular, DHS CISA Director Bob Kolasky participated in a community event with the Executive Director and a partner providing a thoughtful and engaging discussion on the collective cyber defense of our community and nation. The event had over 100 attendees and was held in conjunction with the University of California Irvine Cybersecurity Policy & Research Institute.

On **September 16th**, LACL hosted DHS CISA for a site visit.

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

On **September 17th & 18th**, LA Cyber Lab Security Summit 2019: LACL launched the TISP and mobile app to increase information sharing and public-private sector partnerships on 9/17 & 9/18; over 350 attendees from SLTT, academia, and business communities participated. There were 527 registered attendees, we have confirmed 40 speakers, 5 moderators and Mayor of Los Angeles, Eric Garcetti provided the welcome address and keynote. Themes for the event include the following categories: aviation security panel, privacy and law discussions, space security panel, cybersecurity risk and best practices along with at least one panel focused on women in tech. DHS Region IX representative Christy Riccardi moderated several panels and the LACL Executive Director provided multiple presentations all focused on information sharing via the TISP or mobile app. The overall event was very successful as it greatly increased the awareness of the LACL in the community and provided a positive experience for all. The event began late on the first day due to street closures and traffic associated with a POTUS visit at a nearby venue.



On **October 17th**, the LACL presented at the Pepperdine Cybersecure SoCal 2019 conference.

On **October 23rd**, the LACL presented to local SLTT leaders at the 2019 Maritime Cybersecurity Symposium.

On **October 30th**, the LACL attended a local Small Business conference to engage companies in information sharing.

On **November 21st**, the LACL cohosted a community event "How Hackers, Laws, Cybersecurity and Regulators Connect in a Connected World".

On **December 4th**, the LACL participated in the Media-Entertainment ISAC Summit.

On **December 6th**, the LACL participated in the Southern California ISACA/CSA Holiday Mixer.

On **December 11th**, the LACL participated in the Southern California CISO Executive Summit.

On **January 15th**, the LACL

Webinars:

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

- Hosted Technical Information Sharing & Challenges Webinar
- Participated in 2019 LA City Club Tech Conference
- Participated in the Cyber Risk Management Forum
- Attended The California Consumer Privacy Act Webinar (CCPA)
- Attended The Power of AI to Disrupt Security Ops
- Attended the CISA Infrastructure Security and Resilience Forum in Irwindale, CA
- Attended Cyber Risk Management

Events:

- LACL Security Summit 2019 – Connecting the Community – GO LOUD event for the launch of the mobile app and information sharing community related event
- Hosted hands-on analyst training workshop *Accessing The Darkweb*
- Hosted Cybersecurity and Cyber Privacy Legal Threat Landscape
- Hosted *Cyber Risk: The Cyber Security and Cyber Privacy Threat Landscape*
- Cohosting a speaker's series panel discussion *Securing The Human: Growing the Community*
- Cohosting a Cybersecurity Leaders Forum with HSA Council
- Presented *Anatomy of an IOC* at the annual Information Sharing Conference for ISAOs
- Presented *LACL Mobile Phishing App* at the annual Information Sharing Conference for ISAOs
- Presented at the UCLA Alumni - Silicon Beach Chapter
- Presented at the Business Leaders in Security
- Presented at the Tripartite Security Forum in Auckland, New Zealand
- Presented at the SecureTheVillage Leadership Council
- Presented at the Content Privacy Summit
- Participated at Cybersecure LA 2018
- Participated in DataConLA 2019
- Attended MS-ISAC Conference
- Attended National Homeland Security Conference
- Attended ISSA CISO Conference & Cyber Security Woman of the Year 2019 Awards
- Attended InfraGuard Pacific Region Information Sharing Initiative (ISI)
- Attended the Managed Security Services Forum

Ongoing Outreach Efforts

- American Business Bank
- Bogaard International Group
- British-American Business Council
- California State University, Dominguez Hills
- California State University, Polytech Pomona
- Citadel Group
- Crucyble

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

- Cybertegic
- DataConLA
- FBI Science and Technology
- First Republic Bank
- Forcepoint
- GM, Ecosystem Strategy & Business Development,
- Herbalife
- Intel
- ISSA
- JASK
- LA Chamber of Commerce
- LBW Insurance & Financial Services, Inc
- Obsidian Security
- Pacific City Bank
- Polsinelli Law Firm, Century City
- Resecurity
- Response Software
- San Bernardino County
- SkylinkTV
- TruStar
- UC Berkeley
- UCLA Extension
- USC Information Science Institute

Appendix XX – Pilot Project Participants

This section documents support from both organizations and individuals who contributed to the LACL. The following is a list of the key participants who worked on the pilot project.

Name	Project Role	Contributions to Project
Joshua Belk	Executive Director, Los Angeles Cyber Lab, Inc. (OPSEC360, LLC)	Led LA Cyber Lab daily efforts and pilot platform project. He provided overall management and direction to the information sharing initiative.
Christopher Covino	Project Lead & Grant Representative; Mayor's Office of Public Safety, City of Los Angeles	Managed the grant, was a public advocate for the LA Cyber Lab pilot platform and information sharing.
Magdalena Kenon	Program Director, Los Angeles Cyber Lab, Inc. (OPSEC360, LLC)	Led business operations and finance for the grant.
Daniel Lee	Senior Cyber Analyst, Los Angeles Cyber Lab, Inc.	Collaborated with the City of Los Angeles analysts in threat intelligence information sharing.
Kian Rahimnejad	Fellow, Los Angeles Cyber Lab, Inc.	Researched information used in promotional materials and created content to support the pilot project.
Jasmine Vu	Fellow, Los Angeles Cyber Lab, Inc.	Facilitated membership meetings and coordinated events in support of the pilot project.
Ariana Kim	Fellow, Los Angeles Cyber Lab, Inc.	Researched information used in promotional materials and created content to support the pilot project.
Jens Bechmann	Outreach Director, Los Angeles Cyber Lab, Inc. (Independent Contractor)	Led outreach to community and business partners for grant initiatives.
Robert Velsaco	Policy Director, Los Angeles Cyber Lab, Inc. (OPSEC360, LLC)	Led technical teams and managed vendors to provide information sharing products supporting the grant.
Haroon Azar	The Rosslyn Group	Led mobile phishing app coordination and strategic engagement for the LA Cyber Lab's business email compromise initiatives.
Imran Chaudhari	The Rosslyn Group	Technical lead for development of the mobile phishing application (aka LACL app).
Ahmed Salem	The Rosslyn Group	Technical engineer of the mobile phishing app and API integration.
Kevin Albano	IBM	IRIS and analytics point of contact for threat analysis for IBM.
Patrick Coughlin	TruSTAR	Cofounder of TruSTAR, led project development and integration with LA Cyber Lab.
Chris Godfrey	TruSTAR	Primary client engagement for the threat intelligence platform to the LA Cyber Lab. Facilitates all requirements for the TruSTAR API and platform.
Eve LaDue	Mayor's Office of Public Safety, City of Los Angeles	Procurement and contract specialist for LA Cyber Lab's cyber threat information sharing RFP.
Carlos Carrillo	IBM	IBM point of contact, coordinates and manages IBM and TruSTAR teams. Is the primary point of contact for threat sharing for the LA Cyber Lab.
Stan Stahl	SecureTheVillage; Los Angeles Cyber Lab, Inc. Advisory Board Member	Participated in outreach efforts, marketing, and facilitated community involvement.

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

Ara Aslanian	InverseLogic; Los Angeles Cyber Lab, Inc. Advisory Board Member	Participated in outreach efforts, marketing, and facilitated community involvement.
Jayson Gibson	Phoenix Online Media (POM)	Owner of POM. Primary for the LA Cyber Lab's website and establishment of social media.
Michael Estrella	Avelane Road	Owner of Avelane Road, primary consultant for video and multimedia production of LACL video series.
Jayson Garcia	TruSTAR	Primary client engagement for the threat intelligence platform to the LA Cyber Lab. Facilitates all requirements for the TruSTAR API and platform.
Lena Hwang	Mayor's Office of Public Safety, City of Los Angeles	Accounting and finance approver.
Miho Yoshimura	Mayor's Office of Public Safety, City of Los Angeles	Accounting and finance reviewer.
Neeraj Bhatnagar	Mayor's Office of Public Safety, City of Los Angeles	Los Angeles Cyber Lab Board of Directors
Reuben Wilson	Mayor's Office of Public Safety, City of Los Angeles	Los Angeles Cyber Lab Board of Directors
Jeffrey Gorell	Deputy Mayor for Homeland Security and Public Safety – Mayor's Office of Public Safety, City of Los Angeles	Los Angeles Cyber Lab Board of Directors
Timothy Lee	Chief Information Security Officer, City of Los Angeles	Los Angeles Cyber Lab Board of Directors
Ahmad Ishaq	ByteCubed	Los Angeles Cyber Lab Board of Directors
Rick Orloff	CSO Advisors	Los Angeles Cyber Lab Board of Directors
Bently Au	Chief Information Security Officer, AEG	Los Angeles Cyber Lab Board of Directors
Glenn Haddox	President, Los Angeles Cyber Lab, Inc.; Chief Information Security Officer, Southern California Edison	Provided thought leadership to the Executive Director.
Karl Mattson	President, Los Angeles Cyber Lab, Inc.; Chief Information Security Officer, City National Bank	Provided thought leadership to the Executive Director.
Jacob Finn	Project Lead & Grant Representative; Mayor's Office of Public Safety, City of Los Angeles	Managed the grant, was a public advocate for the LA Cyber Lab pilot platform and information sharing.

The following is a list of organizations who provided support to the LACL during the pilot project.

Organization Name:	City of Los Angeles, local municipal government, is a member of the cyber lab advisory board.
Location of Organization:	https://www.lacity.org/
Partner's contribution to the project (identify one or more)	
Financial support	
X In-kind support	Provided office space and logistics for LA Cyber Lab staff to conduct business.
X Facilities	Provided office space and conference rooms for meetings.

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

X	Collaborative research	Conducted joint analyst research of indications of compromise and threat intelligence.
X	Personnel exchanges	Provided two part-time resources to facilitate LA Cyber Lab daily threat report activities, web support, and platform discussion.
Organization Name:		City National Bank, a Los Angeles based regional financial institution, is a member of the cyber lab advisory board.
Location of Organization:		https://cnbbank.bank
Partner's contribution to the project (identify one or more)		
X	Financial support	Provided \$10,00.00 in sponsorship for the Security Summit 2019.
X	In-kind support	Funded two part-time fellowship positions beginning February 2019 for one year.
X	Facilities	Provided conference rooms for board meetings and fellowship interviews.
	Collaborative research	
	Personnel exchanges	
Organization Name:		CISCO Systems, a Fortune 500 technology corporation, is a member of the cyber lab advisory board.
Location of Organization:		https://www.cisco.com/
Partner's contribution to the project (identify one or more)		
	Financial support	
X	In-kind support	Co-sponsored and provided two cyber defense hands-on training March 1 st , 2019 & January 28, 2020.
	Facilities	
	Collaborative research	
	Personnel exchanges	
Organization Name:		Resecurity, Inc., a cybersecurity solutions company providing darkweb monitoring.
Location of Organization:		
Partner's contribution to the project (identify one or more)		
X	Financial support	Provided \$6,000.00 in sponsorship at the Security Summit 2019.
	In-kind support	
	Facilities	
	Collaborative research	

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

Personnel exchanges	
Organization Name:	NormShield, Inc., a third party vendor security company providing security risk scorecards.
Location of Organization:	
Partner's contribution to the project (identify one or more)	
Financial support	
X In-kind support	Provided cybersecurity training at the Security Summit 2019.
Facilities	
Collaborative research	
Personnel exchanges	
Organization Name:	Silent Sector, a security consulting firm.
Location of Organization:	
Partner's contribution to the project (identify one or more)	
X Financial support	Provided \$500.00 in sponsorship at the Security Summit 2019.
In-kind support	
Facilities	
Collaborative research	
Personnel exchanges	
Organization Name:	Silent Storm Security, a security consulting firm.
Location of Organization:	
Partner's contribution to the project (identify one or more)	
X Financial support	Provided \$500.00 in sponsorship at the Security Summit 2019.
In-kind support	
Facilities	
Collaborative research	
Personnel exchanges	
Organization Name:	Working Scholars, a workforce development organization.
Location of Organization:	www.study.com
Partner's contribution to the project (identify one or more)	
X Financial support	Provided \$4,000.00 in sponsorship at the Security Summit 2019.
In-kind support	

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

Facilities	
Collaborative research	
Personnel exchanges	
Organization Name:	Fioressence, a beauty and wellness company.
Location of Organization:	www.fioressence.com
Partner's contribution to the project (identify one or more)	
Financial support	
X In-kind support	Provided free products for attendees as a sponsor at the Security Summit 2019.
Facilities	
Collaborative research	
Personnel exchanges	
Organization Name:	OPSEC360, LLC, a security consulting firm, is a member of the cyber lab advisory board.
Location of Organization:	www.opsec360.com
Partner's contribution to the project (identify one or more)	
Financial support	
X In-kind support	Provided artwork and graphic design as a sponsor at the Security Summit 2019.
Facilities	
Collaborative research	
Personnel exchanges	

Appendix XX – CTI Sharing Partners

The following tables are the status of the public and private sector engagement for TISP CTI sharing.

Contact	DISCUSSION	ACCESS	SHARING
PHASE 0	PHASE I	PHASE II	PHASE III
<i>CAL OES (Cal-CSIC)</i>	<i>Cedar-Sinai Hospitals</i>	<i>AEG</i>	<i>Avery Dennison</i>
<i>Fox</i>	<i>City of San Diego</i>	<i>City National Bank</i>	<i>City of Los Angeles</i>
<i>City of Beverly Hills</i>	<i>County of Los Angeles</i>	<i>City of Atlanta</i>	<i>IBM</i>
<i>City of Phoenix</i>	<i>Dollar Shave Club</i>	<i>City of Boston</i>	<i>ME-ISAC</i>
<i>City of San Diego</i>	<i>Port of Long Beach</i>	<i>City of Burbank - DWP</i>	<i>InverseLogic</i>
<i>County of San Bernardino</i>	<i>Shepard-Mullin</i>	<i>City of Glendale</i>	
<i>JRIC Phoenix</i>	<i>Southern California Edison</i>	<i>City of Long Beach</i>	
<i>KPMG</i>		<i>City of Pasadena</i>	
<i>NASA JPL</i>		<i>City of Pasadena - DWP</i>	
<i>American Airlines</i>		<i>City of Riverside</i>	
<i>Riot Games</i>		<i>City of San Antonio</i>	
		<i>City of San Fernando</i>	
		<i>City of San Francisco</i>	
		<i>City of Santa Monica</i>	
		<i>City of Torrance</i>	
		<i>County of Los Angeles</i>	
		<i>FBI Cyberhood Watch LA</i>	
		<i>Hulu</i>	
		<i>iHerb LLC</i>	
		<i>OPSEC360</i>	
		<i>JRIC Los Angeles</i>	
		<i>Cal Poly Pomona</i>	

Phase	Organization	Notes	Industry	Initial Contact
PHASE 0 -	<i>CAL OES (Cal-CSIC)</i>	<i>Unknown</i>	<i>State</i>	<i>February</i>

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

Contact				2019
PHASE 0 - Contact	Cal Poly Pomona	On Hold – February	Academia	April 2019
PHASE 0 - Contact	City of Beverly Hills	No Response Yet	Gov -Local	December 2019
PHASE 0 - Contact	City of Phoenix	Reconnect Jan 2020	Gov -Local	November 2019
PHASE 0 - Contact	City of San Diego	Pending Call 2nd call	Gov -Local	November 2019
PHASE 0 - Contact	County of San Bernardino	No Response	Gov - Local	August 2019
PHASE 0 - Contact	JRIC Phoenix	On Hold – February	Fusion	November 2019
PHASE 0 - Contact	KPMG	Pending Follow Up	Consulting	September 2019
PHASE 0 - Contact	NASA JPL	No Response Yet		December 2019
PHASE 0 - Contact	Riot Games	No Response Yet	Tech	June 2019
PHASE 0 - Contact	American Airlines	Initial Contact	Aerospace	February 2020
PHASE I - Discussion	Cedar-Sinai Hospitals	Pending Follow Up Call	Healthcare	March 2019
PHASE I - Discussion	City of San Diego	Follow up Required		December 2019
PHASE I - Discussion	County of Los Angeles	Pending Follow Up	Gov - Local	August 2019
PHASE I - Discussion	Dollar Shave Club	Pending Follow Up Call	Beauty	February 2019
PHASE I - Discussion	Port of Long Beach	Pending Follow Up	Transportation	June 2019
PHASE I - Discussion	Shepard-Mullin	Pending Technical Call	Law	July 2019
PHASE I - Discussion	Southern California Edison	On Hold Until 2020	Energy	March 2019
PHASE II Access	AEG	Pending Follow Up	Entertainment	February 2019
PHASE II Access	City National Bank	Pending Partner Update	Finance	February 2019
PHASE II	City of Atlanta	Phase III pending Tech	Gov - Local	December

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

Access				2019
PHASE II Access	City of Boston	Phase III pending Tech	Gov - Local	January 2020
PHASE II Access	City of Burbank - DWP	Access Only - Tech Limitations	Energy	December 2019
PHASE II Access	City of Glendale	Access Only - Tech Limitations	Gov - Local	December 2019
PHASE II Access	City of Long Beach	Access Only - Tech Limitations	Gov - Local	January 2020
PHASE II Access	City of Pasadena	Access Only - Tech Limitations	Gov - Local	December 2019
PHASE II Access	City of Pasadena - DWP	Access Only - Tech Limitations	Energy	December 2019
PHASE II Access	City of Riverside	Access Only - Tech Limitations	Gov - Local	December 2019
PHASE II Access	City of San Antonio	Phase III pending Tech	Gov - Local	January 2020
PHASE II Access	City of San Fernando	Phase III pending Tech	Gov - Local	January 2020
PHASE II Access	City of San Francisco	Phase III pending Tech	Gov - Local	January 2020
PHASE II Access	City of Santa Monica	On Hold Until 2020	Gov - Local	June 2019
PHASE II Access	City of Torrance	Access Only - Tech Limitations	Gov - Local	December 2019
PHASE II Access	County of Los Angeles	Phase III pending Tech	Gov - Local	December 2019
PHASE II Access	FBI Cyberhood Watch LA	For Intel	Gov - Federal	December 2019
PHASE II Access	Hulu	Pending Technical Call	Tech/Entertainment	July 2019
PHASE II Access	iHerb LLC	Call Scheduled	Food	November 2019
PHASE II Access	JRIC Los Angeles	For Intel only	Fusion	October 2019
PHASE II Access	LA 2028 -Olympic Organizer	Phase III pending Tech	non profit	January 2020
PHASE II Access	LA Community College District	Phase III pending Tech	Education	January 2020
PHASE II Access	LA Metro	Phase III pending	Transportatio	December

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

Access			<i>n</i>	<i>2019</i>
PHASE II Access	<i>LA Unified School District</i>	<i>Pending Technical Call</i>	<i>Gov - Local</i>	<i>November 2019</i>
PHASE II Access	<i>Quibi</i>	<i>Verify Technology</i>	<i>Tech</i>	<i>December 2019</i>
PHASE II Access	<i>TCW</i>	<i>Tech Follow Up</i>	<i>Tech</i>	<i>October 2019</i>
PHASE II Access	<i>OPSEC360</i>	<i>Tech Follow Up</i>	<i>Tech</i>	<i>January 2020</i>
PHASE II Access	<i>USCG Sector Los Angeles/Long Beach</i>	<i>For Intel only</i>		
PHASE III Sharing	<i>InverseLogic</i>	<i>Verify Technology</i>	<i>Tech</i>	<i>December 2019</i>
PHASE III Sharing	<i>Avery Dennison</i>	<i>Complete</i>	<i>Manufacturing</i>	<i>November 2019</i>
PHASE III Sharing	<i>City of Los Angeles</i>	<i>Complete - Includes LAWA, PoLA, LADWP</i>	<i>Gov -Local</i>	<i>February 2019</i>
PHASE III Sharing	<i>IBM</i>	<i>Complete</i>	<i>Tech</i>	<i>June 2019</i>
PHASE III Sharing	<i>ME-ISAC</i>	<i>Complete</i>	<i>ISAC</i>	<i>February 2019</i>
PHASE X	<i>CISCO</i>	<i>Not Interested</i>	<i>Tech</i>	<i>March 2019</i>

Appendix XX – TISP Value Proposition

Threat Intelligence Sharing Platform (TISP) Value Proposition

DHS made a \$3M investment in the LACL pilot project to increase information sharing among the public and private sectors. Through the grant the LACL established a mechanism to enable organizations to easily share threat intelligence through crowdsourcing indicators of compromise (IOC) in a TISP. The TISP is intended to augment and not replace any existing TIP. The LACL utilizes the TruSTAR platform for its TISP; TruSTAR provides the aggregation of IOCs and related threat intelligence information which is shared within the community. Furthermore, the TISP provides users an easy to use interface (API access also) for enriching and analyzing threat information. The LACL threat sharing model comprises of the following components:

- A threat intelligence sharing platform (TruSTAR)
- Existing LACL IOC data
- OSINT data feeds
- Analytics
- Reports
- Partner IOC data
- Business Email Compromise data

The value of these individual components are outlined in the table below as well as the advantages to becoming a partner and sharing information to with the LACL community.

Partners: Are those entities (academic, public or private sectors) which share threat intelligence to the LACL TISP.

Members: Are those entities or individuals who receive (consume) threat intelligence from the LACL.

Threat Intelligence: Partners have access to 57 threat feeds; Members may receive 32 threat feeds.

LACL TISP saves organizations on average \$570K by providing access to an enterprise level tool and analyst vetted CTI.

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

Product	Value	Cost	Partner	Member
TISP (TruStar)	TISP	\$200K	✓	
Existing LACL IOC Data	Over 24 months of vetted IOC data with contextualized information	\$250K	✓	
OSINT Data Feeds	<p>Consisting of 16 feeds which are analyzed, arranged, and ingested into the existing LACL IOC data feed; analysts work through these feeds to provide high fidelity IOCs with further enriching existing data (<i>partial list</i>):</p> <ul style="list-style-type: none"> • Abuse Ransomware • Abuse SSL IP Blacklist • Bambenek • Broadanalysis • DHS-AIS • EU-Cert • H-ISAC • Hail A TAXII • Hybrid Analysis Public • Infosecislands • Internet Storm Center • Malware bytes • NIST NVD • Packetstorm • Unit 42 • US-Cert 	\$320K	✓	✓
Analytics	IBM Incident Response Information System (IRIS) analysis of IOC data	\$100K	✓	
Reports	<p>IRIS Monthly Reports:</p> <p>Threat Activity (10)</p> <p>Malware Analysis (5)</p> <p>Threat Group (1)</p>	\$100K	✓	✓
Partner Data (IOC Enclave)	High fidelity IOCs contributed by partners into a single enclave.	\$250K	✓	✓

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

Phishing Data (BEC Enclave)	Community provided data about potential phishing IOCs	\$75K		
Total Value of the LACL Information Sharing Model		\$1.295M	\$1.22M	\$570K

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

Partner Received Threat Intelligence Feeds Included:

Feed Name	Enclave_id
a_de_pasquale	649b15c1-dfb8-408d-b359-0cd1411d14ef
Abuse Ransomware	170c3077-f502-4b1a-b8f7-7538f83a66c1
Abuse SSL IP Blacklist	00cbe17f-8d3c-4dd8-84ac-3c0c4e6a7c02
anand_himanshu	751511a8-3499-42b5-a6e5-acfece24bd33
asset_island_	34908b5d-2d3d-4582-8a42-aa6d4b2f003d
atindermann08	bef7dc37-8e50-498b-baea-1043585c74d1
Avman1995	0199dd32-575d-4361-8c14-d1c468816381
Bambenek	ed9d7459-dd90-414f-96ee-5e37f232cd18
Bauldini	9bfa800b-4a74-4be7-a09b-5724fb71ec5f
Broadanalysis	0e4443fc-2b50-4756-b5e0-4ea30030bcb3
Community	28177710-9cb8-aa2f-29e8-135c14365e80
DecayPotato	f83278e1-4f41-4602-8d3b-1e35d18f07b6
DHS-AIS	cabbfa67-afd7-4a0c-a20f-e51e25923629
Diemiurgo	63a16f2e-e163-456b-99dc-4b12ac1cd755
Dodge This Security	87753c77-44e8-4786-bc46-01608dc23a77
EU-CERT	e7f4907a-2909-48e8-9c2d-74ffc4b22e8c
FewAtoms	4a9891a5-0e65-41df-a0d1-9c77f17cd6ff
H-ISAC TLP Green & White Alerts	5392b0a7-32fb-4825-aac7-1e6c6d437de3
h3x2b	9b116216-a46b-472a-af44-c5b16ac4c9a8
Hail A TAXII	7819c8d1-2b7b-48ac-b127-c71d8e7de612
HazMalware	e6e48dcb-51cb-4911-9343-11f02ffe2bad
Hybrid Analysis Public Feed	2ecccdd-c740-4ad9-aa5c-82744cd1f6aa
IBM X-Force	c13392e3-8d5c-49bb-8a5b-bb55b41eb3b7
Infosecisland	eec779f5-7abc-48ea-ad19-4c5a5f8f5822
Internet Storm Center	eecdff2d-22ae-4e4a-b924-42da4e7ccd4b
issuemakerslab	d13bf951-6071-4ca3-811a-89378decff3f
James_inthe_box	5fetc6f4-57f4-47a6-8f23-b97ce83d2c32
JanOfficial	4355d90d-bd77-4612-9073-012b11a56e98
JROdriguezB	9adb22a9-417a-472f-9650-ba8f1f3a2849
JRoosen	645717ce-6c43-49b4-aaaa-b1cc642f764b
justmlwhunting	279f247e-39f7-4911-a2d3-a545095d1d7d
LACL BEC	08d99eac-d197-4193-86d9-b637a70df1cb
LACL TISP	a28684aa-d047-4770-bac7-1c5a67f7dacb
MaelSecurity	9dcbb428-52d5-400c-bc62-cfba02376018
Mak Wana	c10226c8-21dd-463c-b4cd-b8e14983d248
malhunters	09a1512e-581c-4e02-abce-97ecf5469f13
Malware Traffic Analysis	e13e0b52-0977-4cf6-be37-3445865c9e8a
Malwarebytes	5d5d1eee-f65f-4fd9-a14b-43c597d9af9e
My Online Security	752d5f90-3281-455d-8162-d629db21f37e
NeonPrimetime	3a8c95e0-6689-4142-b3ab-2900e59429d7
NIST NVD	d2eec321-34bc-4db6-aa20-2ad0a52135fc
Packetstorm	d2cf82f0-5aba-4cf4-ba3b-fc990829b663

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

pancak3lullz	89eb5207-0965-4400-bb83-f5c3d6e2f881
PolarToffee	7504840b-79c9-4fa3-812c-026bc7068393
pollo290987 _(@_@)_/	74f32d63-33c6-4edb-8cb9-c3c2a86b80d1
ps66uk	f6205545-3c00-490e-bf77-cbae6afc997c
Racco42	ad45e7fe-db06-4628-809f-dded2e65344b
RealRalf9000	0978b56c-fdc7-4aaa-8d3a-2367196a144f
Ring0x0	1474353b-cbf8-450c-8c6b-e5973e073ab2
SaurabhSha15	588ca83f-91d4-462d-b781-f7a4505a619e
scsinusy	b5fe326e-1b9c-4cc1-9726-070b83c6acba
Sohn von Erde	9feb9831-2867-4d36-a7ad-466108affa65
Techhelplist	42eed79a-5a4e-48da-a412-190bf4a3acbc
Unit 42	11125bbd-ca70-4f16-bce2-7e361693ceb2
US-CERT	919879d7-88b3-4605-9464-b2a8fca5473a
VK_Intel	9d21c878-b914-41d3-9ad2-47a7c430fd9a
Zerophage	e83a4fa6-af05-417d-b13a-b18a5fc9b426

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

Member Received Threat Intelligence Feeds Included:

Feed Name	Enclave_id
a_de_pasquale	649b15c1-dfb8-408d-b359-0cd1411d14ef
Abuse Ransomware	170c3077-f502-4b1a-b8f7-7538f83a66c1
Abuse SSL IP Blacklist	00cbe17f-8d3c-4dd8-84ac-3c0c4e6a7c02
Avman1995	0199dd32-575d-4361-8c14-d1c468816381
Bambenek	ed9d7459-dd90-414f-96ee-5e37f232cd18
Broadanalysis	0e4443fc-2b50-4756-b5e0-4ea30030bcb3
Community	28177710-9cb8-aa2f-29e8-135c14365e80
DHS-AIS	cabbfa67-afd7-4a0c-a20f-e51e25923629
EU-CERT	e7f4907a-2909-48e8-9c2d-74ffc4b22e8c
H-ISAC TLP Green & White Alerts	5392b0a7-32fb-4825-aac7-1e6c6d437de3
HazMalware	e6e48dcb-51cb-4911-9343-11f02ffe2bad
IBM X-Force	c13392e3-8d5c-49bb-8a5b-bb55b41eb3b7
Infosecisland	eec779f5-7abc-48ea-ad19-4c5a5f8f5822
Internet Storm Center	eecdff2d-22ae-4e4a-b924-42da4e7ccd4b
James_inthe_box	5fefc6f4-57f4-47a6-8f23-b97ce83d2c32
JanOfficial	4355d90d-bd77-4612-9073-012b11a56e98
JRoosen	645717ce-6c43-49b4-aaaa-b1cc642f764b
LACL BEC	08d99eac-d197-4193-86d9-b637a70df1cb
LACL TISP	a28684aa-d047-4770-bac7-1c5a67f7dacb
Mak Wana	c10226c8-21dd-463c-b4cd-b8e14983d248
Malware Traffic Analysis	e13e0b52-0977-4cf6-be37-3445865c9e8a
Malwarebytes	5d5d1eee-f65f-4fd9-a14b-43c597d9af9e
NeonPrimetime	3a8c95e0-6689-4142-b3ab-2900e59429d7
pancak3lullz	89eb5207-0965-4400-bb83-f5c3d6e2f881
pollo290987 _(O_O)_/	74f32d63-33c6-4edb-8cb9-c3c2a86b80d1
ps66uk	f6205545-3c00-490e-bf77-cbae6afc997c
Ring0x0	1474353b-cbf8-450c-8c6b-e5973e073ab2
SaurabhSha15	588ca83f-91d4-462d-b781-f7a4505a619e
Techhelplist	42eed79a-5a4e-48da-a412-190bf4a3acbc
Unit 42	11125bbd-ca70-4f16-bce2-7e361693ceb2
US-CERT	919879d7-88b3-4605-9464-b2a8fca5473a
Zerophage	e83a4fa6-af05-417d-b13a-b18a5fc9b426

Appendix XX – LACL In Publications & Media

Published Articles

- Ars Technica, [Los Angeles partnership launches platform to help people catch phishes](#) [Sean Gallagher] September 18, 2019
- Government Technology, [L.A., IBM Launch Threat Intelligence Platform for Businesses](#) [Lucas Ropek] September 18, 2019
- Inside Cybersecurity, [LA Cyber Lab set to unveil threat app aimed at bolstering small business cybersecurity](#) [Charlie Mitchell] September 17, 2019
- StateScoop, [LA Cyber Lab launches threat platform, mobile app for local businesses](#) [Ryan Johnston] September 17, 2019
- Politico, [Morning Cybersecurity 9/17/19](#) [Tim Starks] September 17, 2019

Self-Published Videos

Cyber Lab: Don't Get Phished, <https://www.youtube.com/watch?v=lr--tDWs2pc>, February 22, 2020; Protect yourself and your business from phishing attacks, download the LACL app today for the latest in protection from the those trying to steal your data and money. Don't become a victim, after downloading the app you will be able to forward suspicious emails to the LACL for review. You'll shortly receive a response indicating if your email was truly malicious or not. Some phishing emails don't contain malware but ask you to provide personal information in response...don't be fooled. Read carefully and follow your instincts.

LACL TISP Threat Sharing, <https://www.youtube.com/watch?v=Aplm5-04qZl>, January 15, 2020; The LA Cyber Lab Threat Intelligence Sharing Platform (TISP) allows members to collaborate by sharing threat intelligence to defend our community "Protection Through Partnership" The TISP is a free service available to public and private sector organizations who want to gain greater insight into their network environments.

Connecting The Community, <https://www.youtube.com/watch?v=5Krd6LkPuP4>, December 4, 2019; LA Cyber Lab Security Summit 2019 - Connecting The Community - helped usher in a new age in information sharing and partnerships between public and private sectors. LACL launched a mobile app and a Threat Intelligence Sharing Platform which connects businesses creating a collective cyber defense for the community. We become part of the change in the cyber ecosystem! Information is available at www.lacyberlab.org/toolsforlabusinesses.

LA Cyber Lab: About US, <https://www.youtube.com/watch?v=9cU4QdF4OZc>, October 28, 2019; Welcome to LA Cyber Lab! Learn about the latest in threat intelligence as we evolve the cyber ecosystem in the LA business community. Protection through Partnership.

Cyber Lab Mobile App: Protect Against Phishing, <https://www.youtube.com/watch?v=SfNKgsV0xY0>, October 3, 2019; Follow a local business owner as she protects herself and her business against phishing attacks. Download the LACL app today!

LA Cyber Lab Security Summit 2019, <https://www.youtube.com/watch?v=Q1CM24FFFjY>, July 17, 2019; REGISTRATION IS OPEN FOR THE LA CYBER LAB SECURITY SUMMIT 2019!!! Join business leaders and security professionals in the Los Angeles greater area and beyond...See the latest trends in tech, engage with industry leaders, and be a part of the cyber ecosystem changes in phishing and information sharing from the LA Cyber Lab.

Appendix XX – List of Known ISAOs/ISACs

ISAO/ISAC	Web Address
Advanced Cyber Security Center	www.acscenter.org
Arizona Cyber Threat Response Alliance	azinfragard.org/actra
Automotive ISAC	automotiveisac.com
Aviation ISAC	a-isac.com
California Cybersecurity Information Sharing Organization	https://www.californiatechnology.org/calciso
Center for Model Based Regulation	www.cmbreg.org
Columbus Collaboratory	ColumbusCollaboratory.com
Communications ISAC	https://www.cisa.gov/national-coordinating-center-communications
Cyber Houston	cyberhouston.org
Cyber Information Sharing and Collaboration Program	dhs.gov/ciscp
Cyber Resilience Institute	www.cyberresilienceinstitute.org
Cyber Threat Alliance	www.cyberthreatalliance.org
Cyber Warfare Range	azcwr.org
CyberHawaii	CyberHawaii.org
Cybersecurity Collaborative	cyberleadersunite.com
CyberUSA	cyberusa.us
CyberWyoming	www.madesafeinwyoming.org
Defense Industrial Base ISAC	www.dibisac.net
Defense Security Information Exchange	www.dsie.org
Downstream Natural Gas ISAC	dngisac.com
Electricity ISAC	eisac.com
Emergency Management and Response ISAC	www.usfa.fema.gov/operations/ops_cip_emr-isac.html
Energy Analytic Security Exchange	grfederation.org/ease
EnergySec	www.energysec.org
Faith-Based ISAO	faithbased-isao.org
Financial Services ISAC	fsisac.com
Fortify 24x7	www.fortify24x7.com
Geographically-Based Community ISAOs	gbcisaos.org
GICSR Global Situational Awareness Center	www.gicsr.org
Global Directors & Officers ISAO	global-do.org
Global Resilience Federation	www.GRFederation.org
Global Trafficking ISAO	TraffickingISAO.org
Health ISAC	h-isac.org
Healthcare Ready	www.healthcareready.org
HITRUST	hitrustalliance.net
Hospitality Technology Next Generation	www.htng.org

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

Houston Banking ISAO	HouBankISAO.org
Indiana ISAC	www.in.gov/isac
Information Technoogy ISAC	www.it-isac.org
InfraGard	www.infragardnational.org
InsuraShield	InsuraShield.net
International Association of Certified ISAOs	www.certifiedisao.org
IoT ISAO	iot-isao.org
Legal Services ISAO	https://grfederation.org/lis-isao
Los Angeles Cyber Lab	LACyberLab.org
Louisiana Business Emergency Operations Center	LABEOC.org
Maritime and Port Security ISAO	portsecure.org/about/
Maritime ISAC	www.maritimesecurity.org
Maryland ISAO	www.mdisao.org
Medical Device ISAO	www.medisao.com
Mid-Atlantic Cyber center	macc-isao.mitre.org
Multi-State ISAC	www.cisecurity.org/ms-isac/
National Council of ISACs	www.nationalisacs.org
National Credit Union ISAO	ncuisao.org
National Cybersecurity Society	http://www.nationalcybersecuritysociety.org/
National Defense ISAC	ndisac.org
Northeast Ohio CyberConsortium	www.neocc.us
NRF Cyber Risk Exchange	NRF.com/nrf-cyber-risk-exchange
Oil and Natural Gas ISAC	www.ongisac.org
Political Campaign ISAO	USCyberdome.com
Real Estate ISAC	www.reisac.org
Regional Information Sharing Systems	www.riss.net/
Research and Education Network ISAC	www.ren-isac.net
Retail and Hospitality ISAC	https://rhisac.org
Sensato ISAO	sensato.co
Small and Mid-Sized Business ISAO	smbisao.com
Small Business Suply Chain ISAO	https://stc-ntc-lsu.org
Southern California ISAO	www.socalisao.com
Sports ISAO	sports-isao.org/site
Surface Transportation, Public Transportation, and Over-The-Road Bus ISACs	www.surfacetransportationisac.org
Texas CISO Council	www.texascisocouncil.org
Trustworthy Accountability Group	www.tagtoday.net
Water ISAC	WaterISAC.org

Appendix C: State, Local, Tribal, and Territorial Indicators of
Compromise – Automation Pilot Report

DHS-19-CISA-128-SLT-001 State, Local, Tribal and Territorial Indicators of Compromise Automation Pilot

Grant Effort Final Report

30 September 2020

Charles Frick
Cynthia Widick
Kevin Cropper
Dave Halla
Jason Mok
Karl Siil
Kim Watson
Mike Yoo

Table of Contents

- 1. Executive Summary 3**
 - 1.1 Pilot overview and objectives 3
 - 1.2 Pilot participants 4
 - 1.3 High level pilot results 4
 - 1.4 Next steps for pilot participants..... 8
 - 1.5 Pilot effort summary 8
- 2. Introduction 8**
 - 2.1 High level pilot design..... 11
 - 2.2 Pilot partners..... 12
 - 2.3 Pilot use cases 13
- 3. Discovery Phase summary 14**
- 4. Design Phase summary 14**
- 5. Execution Phase summary 15**
- 6. Analysis and findings..... 15**
 - 6.1 Objective 1: Acting upon IOCs within minutes of receipt..... 15
 - 6.2 Objective 2: Reducing time spent on repetitive tasks..... 17
 - 6.3 Objective 3: Providing the generation, enrichment, and scoring of IOCs 18
 - 6.4 Objective 4: Receiving, remediating, and responding to IOCs..... 20
 - 6.5 Objective 5: Demonstrating the use of SOAR 21
 - 6.6 Objective 6: Making data more actionable for consistent execution across SLTT levels 21
 - 6.7 Review of metrics as specified in the Notice of Funding Opportunity (NOFO) 22
- 7. Additional insights and lessons learned 29**
 - 7.1 Insights from pilot partner discussions 29
 - 7.2 Analysis of survey responses 30
- 8. Next steps for pilot participants 32**
- 9. Conclusion..... 32**

1. Executive Summary

1.1 Pilot overview and objectives

Using a Department of Homeland Security (DHS) Cybersecurity & Infrastructure Security Agency (CISA) grant, the Johns Hopkins University Applied Physics Laboratory (JHU/APL) conducted a joint pilot with four State, Local, Tribal and Territorial (SLTT) organizations and the Multi-State Information Sharing & Analysis Center (MS-ISAC) to apply automation to enhance and speed the evaluation of cyber threat Indicators of Compromise (IOC) at the state and local government levels.

The intent of the pilot effort was to use Security Orchestration, Automation and Response (SOAR) concepts to develop a network-defender threat intelligence feed at the MS-ISAC, export indicators from the pilot feed in Structured Threat Integration Expression (STIX) / Trusted Automated Exchange of Intelligence Information (TAXII) format, and use SOAR platforms to respond to those indicators at four state partners with different architectures and operational procedures (Figure 1). The pilot focused on both the curation of the feed as well as the processes used by the SLTT participants to triage, prioritize, and act upon the resultant IOCs. Automation and orchestration were to be used to gain efficiencies in tasks, processes, and resultant actions for both the producer and consumers of the IOCs. The outcomes include:

- Acting upon IOCs within minutes of receipt
- Reducing time spent on repetitive tasks
- Providing the generation, enrichment, and scoring of IOCs
- Receiving, remediating, and responding to IOCs
- Demonstrating the use of Security Orchestration, Automation, and Response (SOAR) concepts
- Defining operational procedures and capabilities combined with information sharing to make data more actionable and enable consistent execution at and across SLTT levels
- Developing repeatable processes for orchestration and automation services that bridge existing SLTT policies with SOAR capabilities

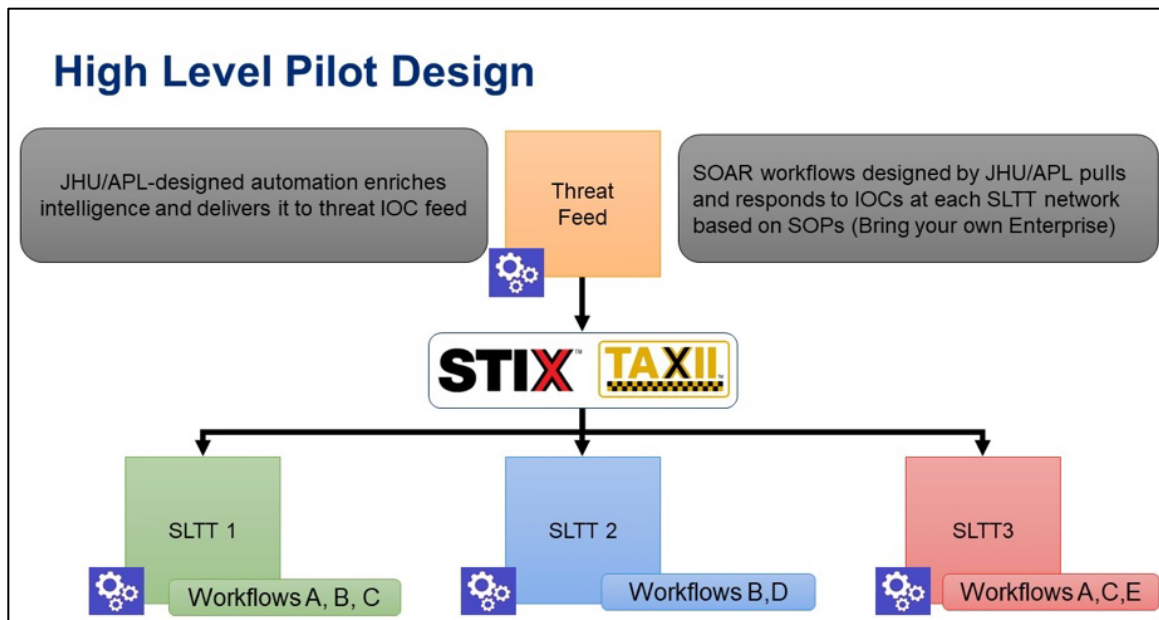


Figure 1 SLTT IOC Automation Pilot Design

1.2 Pilot participants

To successfully accomplish the objectives of the pilot, JHU/APL and CISA determined that a threat feed provider and three SLTT partners were needed. However, after the Discovery Phase was completed, JHU/APL and CISA added Massachusetts as a single security use case using an orchestration proof of concept given its current manual process. MS-ISAC was the chosen threat feed provider and the four pilot partners were:

- Arizona State (Department of Administration and Maricopa County)
- Louisiana (Division of Administration)
- Massachusetts (Executive Office of Technology Services and Security)
- Texas (Department of Information Resources and Department of Public Safety)

1.3 High level pilot results

JHU/APL successfully met every objective of the pilot as specified by CISA. The pilot effort demonstrated the ability to act upon IOCs within minutes of receipt in two distinct ways. Figure 2 provides a summary of the pilot response times for both the automation and the baseline manual processes.

The automation at the MS-ISAC receives IOCs from Intrusion Detection System (IDS) alerts as well as submissions to the Malicious Code Analysis Platform (MCAP). Once received, the pilot automation processes these IOCs within an average time of 42 seconds and distributes them to the pilot TAXII server within an additional 30 seconds. Therefore, action has not only initiated but completed in shortly over 1 minute.

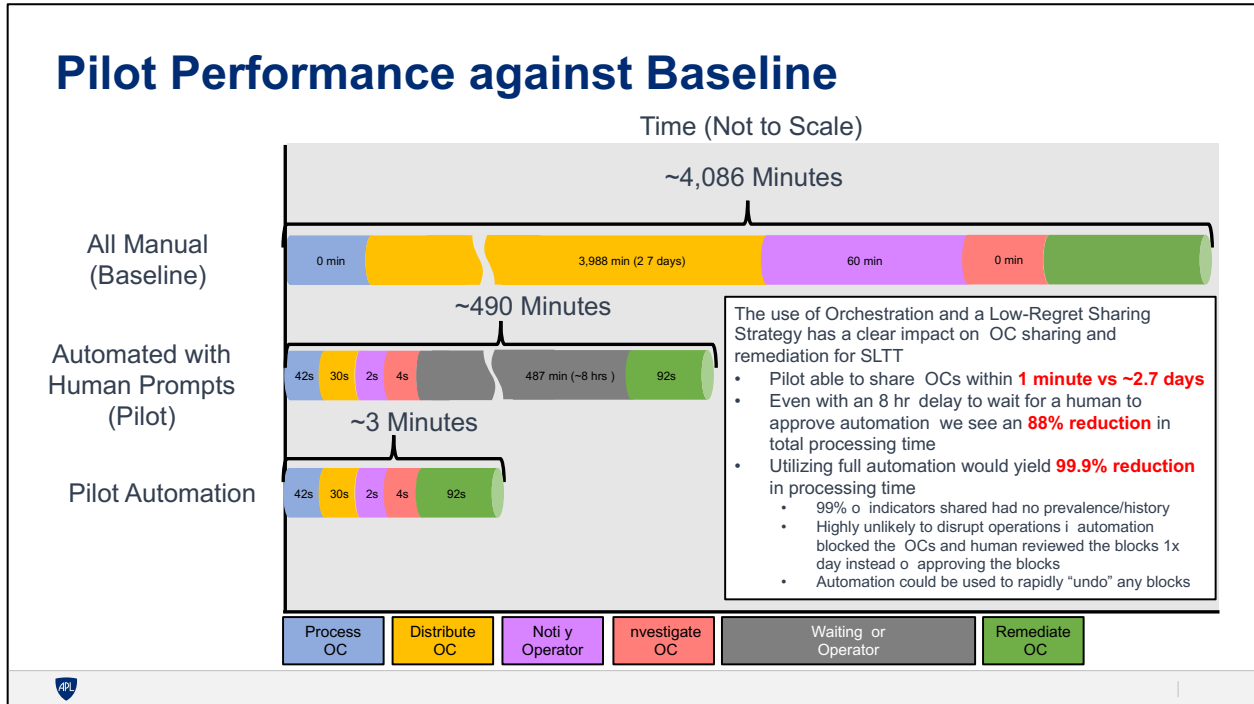


Figure 2 Pilot Performance

Once an SLTT pilot partner has received an IOC from the TAXII feed, the automated actions begin on average within 2 seconds of receipt and take a total of 98 seconds on average to complete. However, this does not represent the full picture of pilot response actions as captured in the pilot data. The SLTT partners requested certain “human-in-the-loop” controls for the pilot because the automation would be on their production environments. This is both an appropriate and understandable risk reduction strategy for the SLTT partners, but it yields a significant delay in the actual execution of the pilot workflows. Analysis of the automation and case open/close timestamps shows that an average of 490 minutes was spent waiting for an operator to review the automated steps and approve them. This is due to certain organizations only reviewing automated actions for the pilot once per shift or per day. Based on reviews with multiple operators, this design would not continue into full operations once further trust in the automation was achieved.

One particular SLTT pilot organization provided additional data on their use of the pilot threat feed that demonstrated significant benefits of an automated feed that can send IOCs rapidly upon observation at MS-ISAC. As any “low-regret” IOC is observed from any Albert Intrusion Detection System or any submission to the MS-ISAC’s detonation service (MCAP), it is packaged into a STIX object and placed on the TAXII server within a minute of arriving to the automation. Figure 3 helps illustrate these benefits. This SLTT partner witnessed attempted attacks from 35 of the received IOCs, while only 27

of the received IOCs had malicious reputation scores. While it is not known whether all the IOCs with reputations attempted attacks, the fact that there are more IOCs attempting attacks than those with malicious reputations illustrates that the pilot feed is sharing malicious IOCs that have yet to develop an online reputation. This is further demonstrated by the several hundred thousand “hits” or attempted attacks by those blocked IOCs. 273,137 of those hits were attempted on the same day of IOC receipt. The fact that this automation can provide IOCs rapidly instead of as a weekly publication gave the SLTT organization the opportunity to proactively block potential cyber attacks before an adversary pivoted to target them after attacking another one of the 7,000 SLTT organizations that participate in the MS-ISAC community.

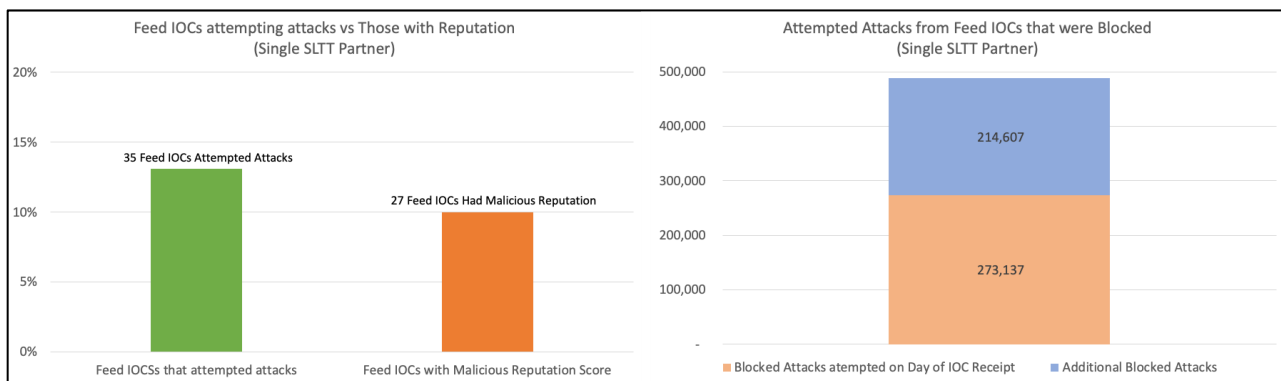


Figure 3 Receipt and Response to Feed IOCs (Single SLTT Partner)

The speed improvements were also witnessed in the additional SOAR proof of concept pilot activity conducted with the Commonwealth of Massachusetts. This task focused on the single use case of threat intelligence enrichment, which was identified as a very repetitive manual task by their security personnel. As seen in Figure 4, the pilot automation reduced the time spent on the task from an average of 41 minutes per case to 9 minutes, 41 seconds.

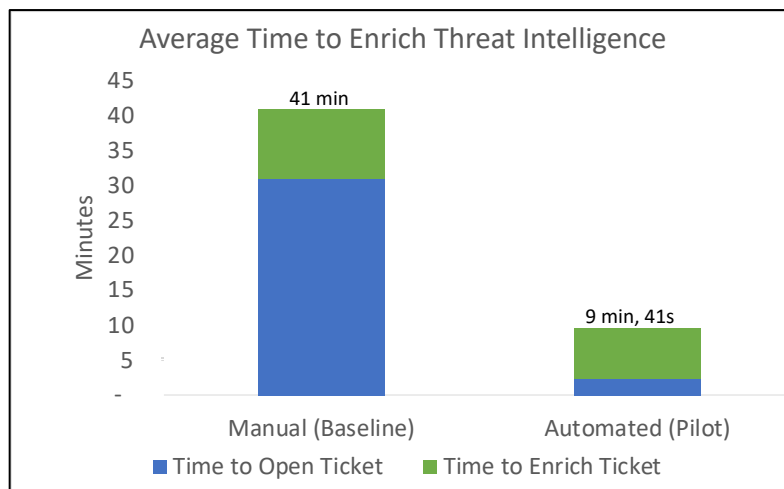


Figure 4 Threat Intelligence Enrichment Timelines

The pilot threat feed provided different types of IOCs than the existing manual feed provided weekly by the MS-ISAC. Figure 5 demonstrates that the automated feed generated significantly more IOCs than the manual feed and that very few of the IOCs were common between the feeds. This was due to the automated feed identifying IOCs that may be bad but should not disrupt operations if blocked (low-regret), whereas the manual feed was identifying IOCs that are good to block but cannot quickly be identified as low-regret.

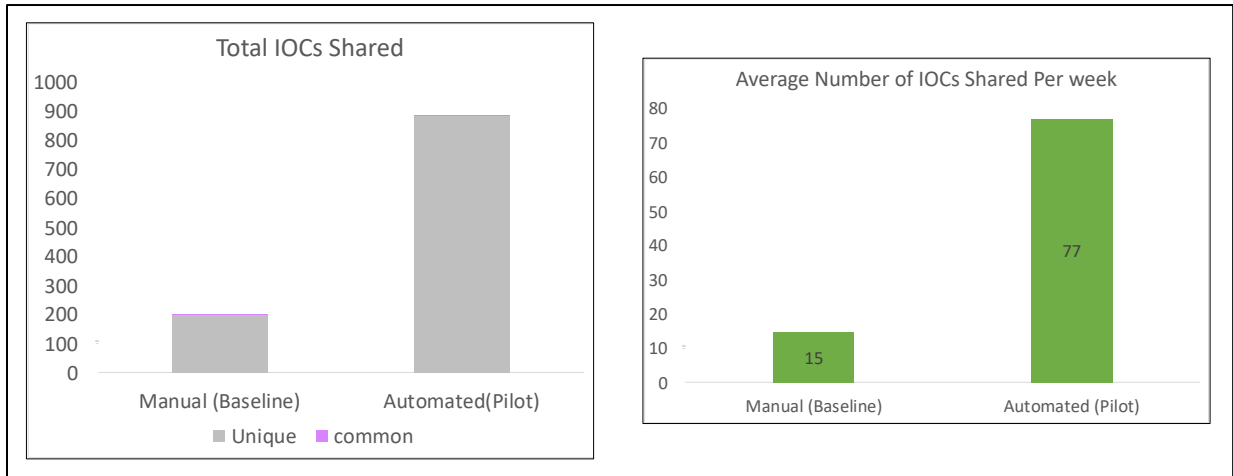


Figure 5 IOC counts from pilot and manual feeds

A summary of the numbers, types and sharing speed for IOCs in the pilot feed are provided in Figure 6. These charts provide data on the total number of IOCs received internally by MS-ISAC as well as the total number of IOCs meeting the “low-regret” threshold. It is important note that only the IOCs meeting a “low-regret” threshold are sent to the feed.

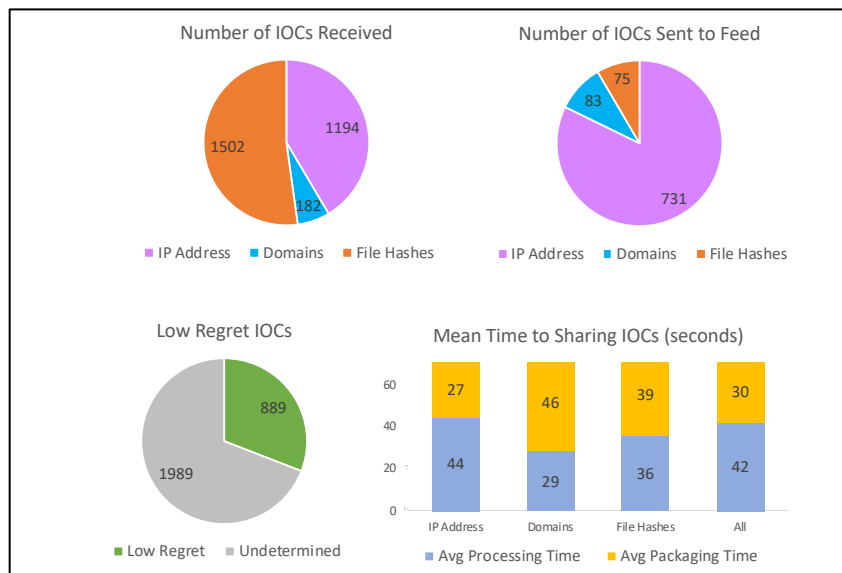


Figure 6 Pilot threat feed summary statistics

1.4 Next steps for pilot participants

The efforts of this pilot will continue to be applied by the participants and will help the overall SLTT community. The MS-ISAC found distinct value in the automated low-regret feed of IOCs and has transitioned the technology into a production offering. After the pilot's conclusion, MS-ISAC will work to make the feed available to their 7,000+ members. The majority of SLTT organizational participants are planning to continue their use of SOAR and security automation based on their experiences with this pilot. Many have already begun to research and develop expanded use cases to leverage the capability identified in the pilot. JHU/APL collected a large amount of data and insights from the pilot and will provide industry guides and best practices to the entire SLTT community as well as other members of the critical infrastructure community.

1.5 Pilot effort summary

The core effort of the *DHS-19-CISA-128-SLT-001 State, Local, Tribal and Territorial Indicators of Compromise Automation Pilot* has been a resounding success. Through the support and efforts of CISA Stakeholder Engagement, the MS-ISAC, Arizona, Louisiana, Massachusetts, and Texas, JHU/APL collaborated on the creation of a new threat feed that provides more actionable cyber threat intelligence at a faster rate, as well as deploying orchestrated security actions that allow for overall process improvements several orders of magnitude faster than current manual processes. Through sharing of the findings, shareable workflows, and the planned development of additional guidance, the entire SLTT community will be able to leverage the findings of this work to improve their survivability against an ever growing cyber threat.

2. Introduction

The nature of the cybersecurity threat to America is growing, and our nation's cyber adversaries move with speed and stealth, often utilizing automation to increase the scale of their attacks. To keep pace, all types of organizations need to be able to share information and respond to cyber risks in as close to real-time as possible. Using a Department of Homeland Security (DHS) Cybersecurity & Infrastructure Security Agency (CISA) grant, the Johns Hopkins University Applied Physics Laboratory (JHU/APL) conducted a joint pilot with four State, Local, Tribal and Territorial (SLTT) organizations and the Multi-State Information Sharing & Analysis Center (MS-ISAC) to apply automation to enhance and speed the evaluation of cyber threat Indicators of Compromise (IOC) at the state and local government levels. The SLTT IOC Automation Pilot identified key areas for potential reduction of manual tasks by humans and actionable information sharing across SLTT enterprises as well as identified orchestration services needed to integrate the activities of sensing, understanding, decision-making, and acting with respect to cyber threats.

To achieve the SLTT IOC Automation Pilot objectives, JHU/APL used a 4-phase approach:

- **Discovery Phase** – to select pilot partners and identify pilot scope, which has been completed and summarized in the JHU/APL AOS-L-20-0180 report entitled *DHS-19-CISA-128-SLT-001 State, Local Tribal and Territorial Indicators of Compromise Automation Pilot Phase 1*.
- **Design Phase** – to collaborate with pilot partners and create pilot workflows, which has been completed and summarized in the JHU/APL AOS-20-0630 report entitled *DHS-19-CISA-128-SLT-001 State, Local, Tribal and Territorial Indicators of Compromise Automation Pilot Phase 2 – Design Report Summary for the Cybersecurity & Infrastructure Security Agency*
- **Execution Phase** – to implement pilot technology on partner production networks and collect data, which has been completed and summarized in the JHU/APL AOS-20-1036 report entitled *DHS-19-CISA-128-SLT-001 State, Local, Tribal and Territorial Indicators of Compromise Automation Pilot Phase 3 – Execution Phase Summary Report*
- **Analysis and Reporting Phase** – to analyze and report the findings of the pilot (this report)

A description of each phase and the pilot timelines is provided in Table 1.

Table 1 SLTT IOC Automation Pilot Phased Approach

Pilot Phase	High-Level Description	Notional Schedule
Discovery Phase	<ul style="list-style-type: none"> Identify and select key partners for pilot Design and refine key pilot Use Cases Conduct kickoff / initial data collect on pilot environment Document pilot scope, use cases and schedule 	October 2019 – January 2020
Design Phase	<ul style="list-style-type: none"> Collaborate with pilot partners to design pilot playbooks, workflows, and reference implementations Integrate reference implementation in JHU/APL lab to verify effectiveness Routinely refine playbooks, workflows, and reference implementations to incorporate pilot partner feedback/requirements Document design, implementation guides, data collection needs, and metrics 	February 2020 – May 2020
Execution Phase	<ul style="list-style-type: none"> Provide consultation and guidance with pilot partners to integrate pilot technology in partner environments Execute pilot plan Collect data to support metrics 	June 2020 – August 2020
Analysis and Reporting Phase	<ul style="list-style-type: none"> Analyze data provided by pilot Evaluate metrics Design follow-on activities and adoption plans Document results and pilot outcomes 	September 2020

It is important to note the aggressive timeline for this pilot effort. In order to succeed in the pilot objectives, JHU/APL was required to identify candidates within the 7,000 member SLTT community, create a new feed for threat intelligence, identify a transition partner for the feed, develop six enterprise security integration environments, create dozens of workflows, and transition those workflows as well as the feed to operations within a 12 month period. Only due to the level of support and commitment from all the SLTT participants, MS-ISAC, and CISA was this achievable.

2.1 High level pilot design

The intent of the pilot effort was to use Security Orchestration, Automation and Response (SOAR) concepts to develop a network-defender threat intelligence feed at the MS-ISAC, export indicators from the pilot feed in Structured Threat Integration Expression (STIX)/Trusted Automated Exchange of Intelligence Information (TAXII) format, and use SOAR platforms to respond to those indicators at four state partners with different architectures and operational procedures (Figure 7). The pilot focused on both the curation of the feed as well as the processes used by the SLTT participants to triage, prioritize, and act upon the resultant IOCs. Automation and orchestration were used to gain efficiencies in tasks, processes, and resultant actions for both the producer and consumers of the IOCs. The outcomes include:

- Acting upon IOCs within minutes of receipt
- Reducing time spent on repetitive tasks
- Providing the generation, enrichment, and scoring of IOCs
- Receiving, remediating, and responding to IOCs
- Demonstrating the use of Security Orchestration, Automation, and Response (SOAR)
- Defining operational procedures and capabilities combined with information sharing to make data more actionable and enable consistent execution at and across SLTT levels
- Developing repeatable processes for orchestration and automation services that bridge existing SLTT policies with SOAR capabilities

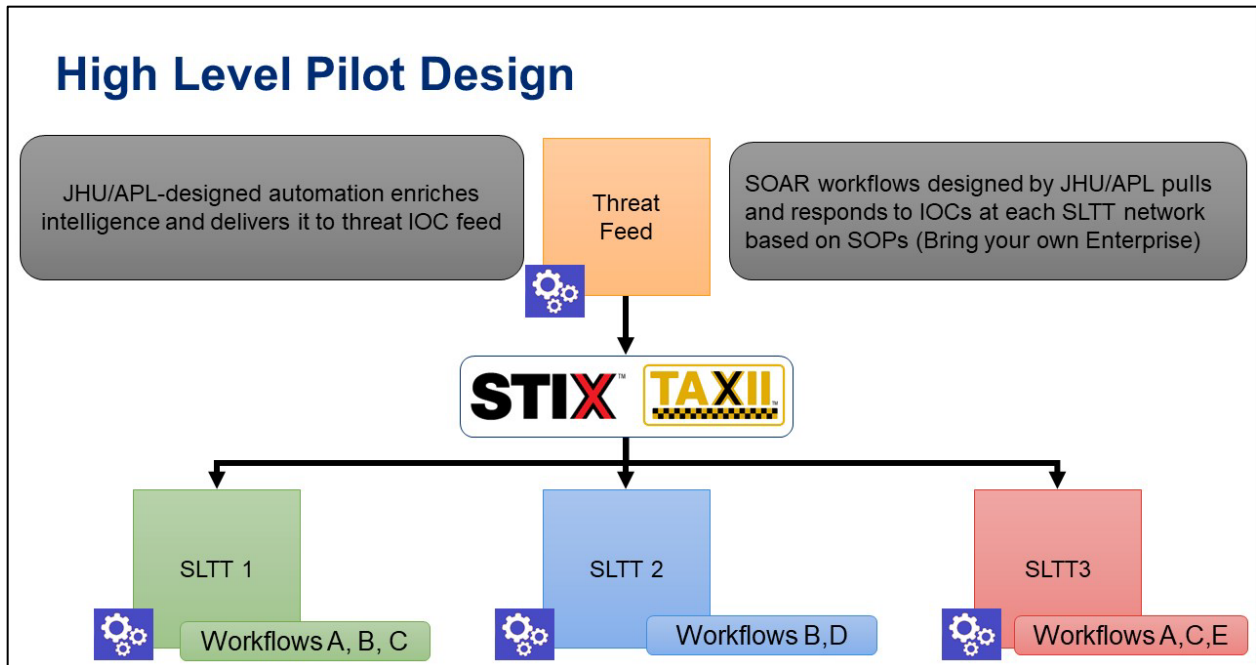


Figure 7 SLTT IOC Automation Pilot Design

2.2 Pilot partners

To successfully accomplish the objectives of the pilot, JHU/APL and CISA determined that a threat feed provider and three SLTT partners were needed. However, after the Discovery Phase was completed, JHU/APL and CISA added Massachusetts as a single security use case using orchestration as a proof of concept given its current manual process. MS-ISAC was the chosen threat feed provider and the four pilot partners were:

- Arizona (Department of Administration and Maricopa County)
- Louisiana (Division of Administration)
- Massachusetts (Executive Office of Technology Services and Security)
- Texas (Department of Information Resources and Department of Public Safety)

2.3 Pilot use cases

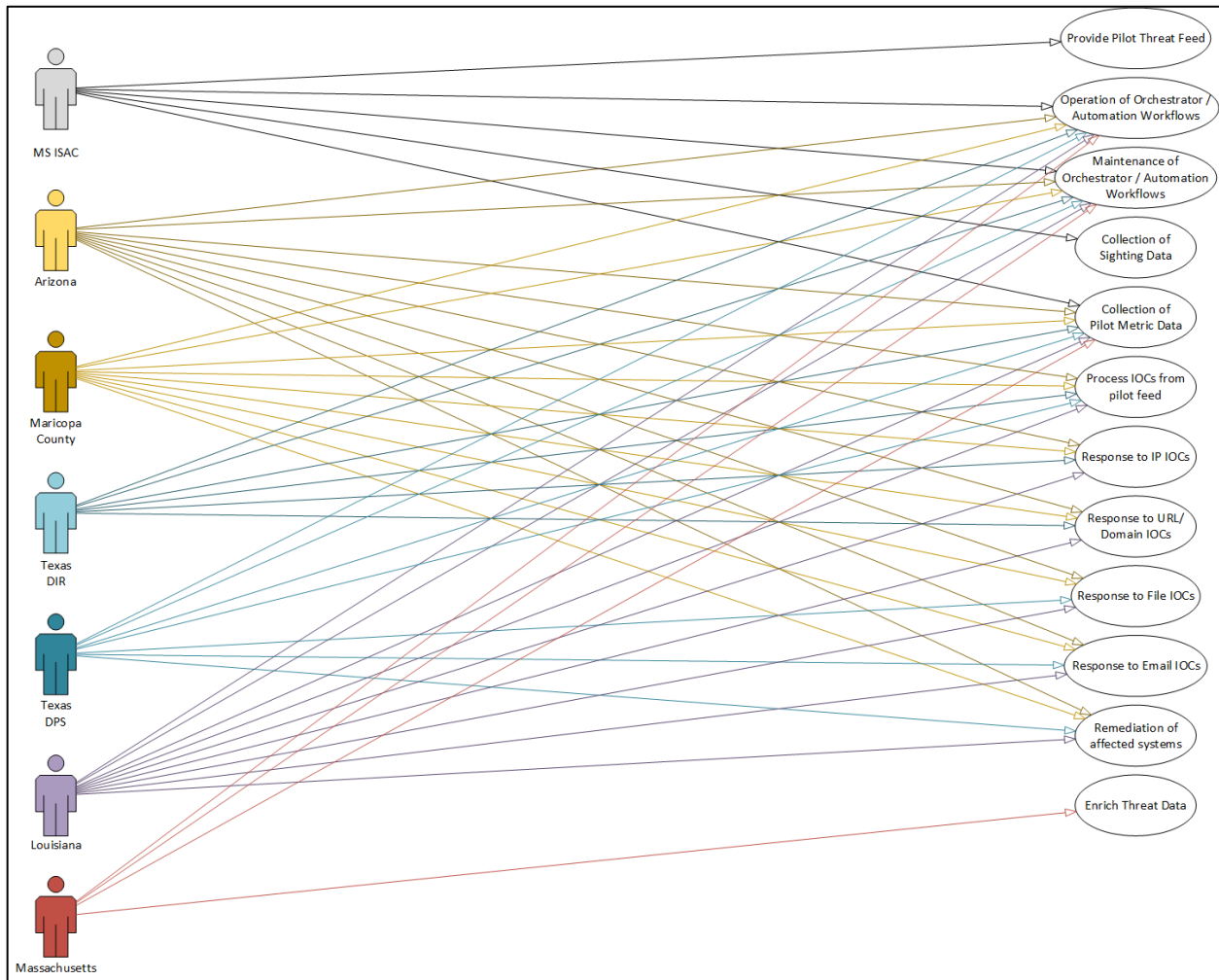


Figure 8 Summary of All Pilot Use Cases

Figure 8 provides an overview of all the use cases for this pilot effort and designations of which pilot partner participated in each use case. In general, the breakdown of use cases follows the following construct:

- MS-ISAC – participated in use cases required to generate the automated feed of IOCs for the pilot
- SLTT organizations – participated in use cases required to receive the feed and take orchestrated action on the IOCs

The one unique caveat to this construct is the Commonwealth of Massachusetts. As stated earlier, Massachusetts’ participation in the pilot was smaller in scope and conducted primarily as a proof of concept for security orchestration. Therefore, the primary focus was orchestration for the use case of threat data enrichment, which was identified by Massachusetts as the desired case for the proof of concept.

There were two areas where JHU/APL observed the planned use cases for the pilot not executing as originally expected. These insights are provided in this report in order to help highlight key considerations if/when other SLTT organizations wish to implement SOAR for processing IOCs.

The response use cases include a use case for processing email sender IOCs. In the Design phase, it was intended that these IOCs would be part of the low-regret feed and would be extracted from file detonation services at the MS-ISAC. Initial integration showed that the IOCs accessed via this service for the pilot did not include email sender information. Due to this limitation, the email IOC use case did not execute during the pilot. As MS-ISAC makes the feed a full production offering, access to email IOCs will be incorporated in a future update.

The original set of use cases identified in the Discovery phase report provided to CISA in February 2020 (JHU/APL document ID AOS-20-0180) included a use case for the submission of sighting data. This use case was identified as somewhat extraneous for this pilot due to the partnership with MS-ISAC. Since IOC extraction is sourced from either member submissions to a detonation chamber or from Albert Intrusion Detection System alerts for an MS-ISAC member, the need for that same member to submit sighting data to MS-ISAC for those IOCs becomes moot. It is expected that the incorporation of other threat feeds by SLTT organizations may later benefit from the generation of sightings and the use of SOAR to assist with the delivery of those sightings, but this task was removed from the pilot since it would provide minimal insight toward achieving the goals of the pilot.

3. Discovery Phase summary

During the Discovery Phase, and with DHS-CISA concurrence, JHU/APL evaluated and selected Arizona, Louisiana, and Texas as the SLTT IOC Automation Pilot partners. Massachusetts was selected for a mini-pilot focused on a single SOAR use case. All state partners consented to participate, as well as MS-ISAC as the threat feed provider. Preliminary discussions and site visits were held in order to ascertain pilot environments and determine the scope for each pilot partner.

4. Design Phase summary

During the Design Phase, JHU/APL worked closely with the pilot SLTT partner agencies and the MS-ISAC, to understand their current procedures and develop an automated MS-ISAC threat feed as well as automated responses to IOCs from the MS-ISAC threat feed.

Additionally, a shareable set of all pilot workflows was developed in a vendor-agnostic format and made available to the general public. These workflows may be found in the

JHU/APL report AOS-20-0915 entitled *Shareable Automation and Orchestration Workflows for scoring, sharing, and responding to Cyber Indicators of Compromise* which may be found on the webpage, <https://www.iacdautomate.org/slitt-pilot-shareable-workflows>.

5. Execution Phase summary

During the Execution phase, JHU/APL worked closely with the SLTT partners and the MS-ISAC to provide consultation and guidance to integrate pilot technology in the partner environments and assist each partner with execution of the pilot plan. This led to successful integration of pilot capabilities and allowed for the collection of data necessary to evaluate the core metrics of this effort.

6. Analysis and findings

JHU/APL successfully met every objective of the pilot as specified by CISA and collected all data available for the analysis of metrics requested in the Notice of Funding Opportunity (NOFO). In this section, relevant analytical findings are provided to support the completion of each objective.

With respect to the additional metrics specified in the NOFO, JHU/APL repeatedly identified metrics that were not possible to calculate given the data that was available. This report addresses every metric and provides an explanation for every metric that could not be calculated.

6.1 Objective 1: Acting upon IOCs within minutes of receipt

The first objective of the pilot as specified by CISA was to demonstrate the ability to act upon Indicators of Compromise within minutes of receipt. The pilot effort represented this objective in two distinct ways. Figure 9 provides a summary of the pilot response times for both the automation and the baseline manual processes.

The automation at the MS-ISAC receives IOCs from Intrusion Detection System (IDS) alerts as well as submissions to the Malicious Code Analysis Platform (MCAP). Once received, the pilot automation processes these IOCs within an average time of 42 seconds and distributes them to the pilot TAXII server within an additional 30 seconds. Therefore, action was not only initiated but completed in shortly over 1 minute.

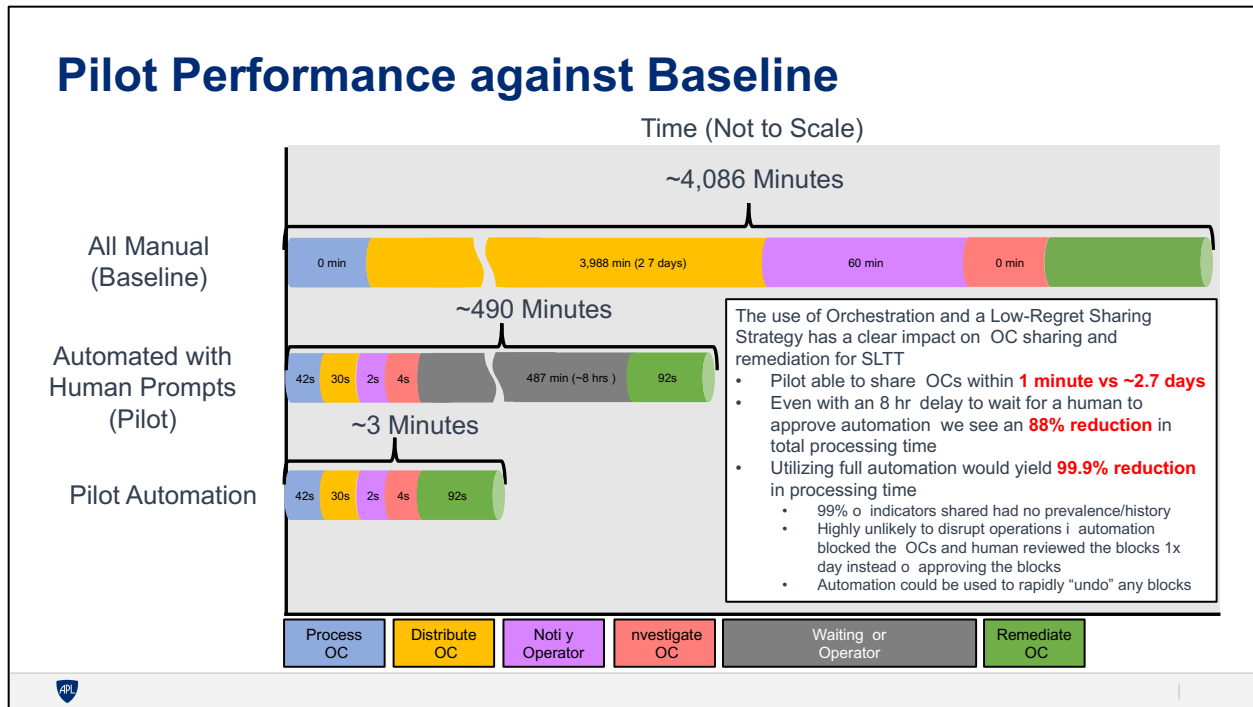


Figure 9 Pilot Performance

Once an SLTT pilot partner received an IOC from the TAXII feed, the automated actions began on average within 2 seconds of receipt and took a total of 98 seconds on average to complete. However, this does not represent the full picture of pilot response actions as captured in the pilot data. The SLTT partners requested certain “human-in-the-loop” controls for the pilot since the automation would be on their production environments. This is both an appropriate and understandable risk reduction strategy for the SLTT partners, but it yields a significant delay in the actual execution of the pilot workflows. Analysis of the automation and case open/close timestamps shows that an average of 490 minutes was spent waiting for an operator to review the automated steps and approve them. This is due to certain organizations only reviewing automated actions for the pilot once per shift or per day. Based on reviews with multiple operators, this design would not continue into full operations once further trust in the automation was achieved.

One particular SLTT pilot organization provided additional data on their use of the pilot threat feed that demonstrated significant benefits of an automated feed that can send IOCs rapidly upon observation at MS-ISAC. As any “low-regret” IOC is observed from any Albert Intrusion Detection System or any submission to the MS-ISAC’s detonation service (MCAP), it is packaged into a STIX object and placed on the TAXII server within a minute of arriving to the automation. Figure 10 helps illustrate these benefits. This SLTT partner witnessed attempted attacks from 35 of the received IOCs, while only 27 of the received IOCs had malicious reputation scores. While it is not known whether all the IOCs with reputations attempted attacks, the fact that there are more IOCs attempting attacks than those with malicious reputations illustrates that the pilot feed is

identifying malicious IOCs that have yet to develop an online reputation. This is further demonstrated by the several hundred thousand “hits” or attempted attacks by those blocked IOCs. 273,137 of those hits were attempted on the same day of IOC receipt. The fact that this automation can provide IOCs rapidly instead of as a weekly publication gave the SLTT organization the opportunity to proactively block potential cyber attacks before an adversary pivoted to target them after attacking another one of the 7,000 SLTT organizations that participate in the MS-ISAC community.

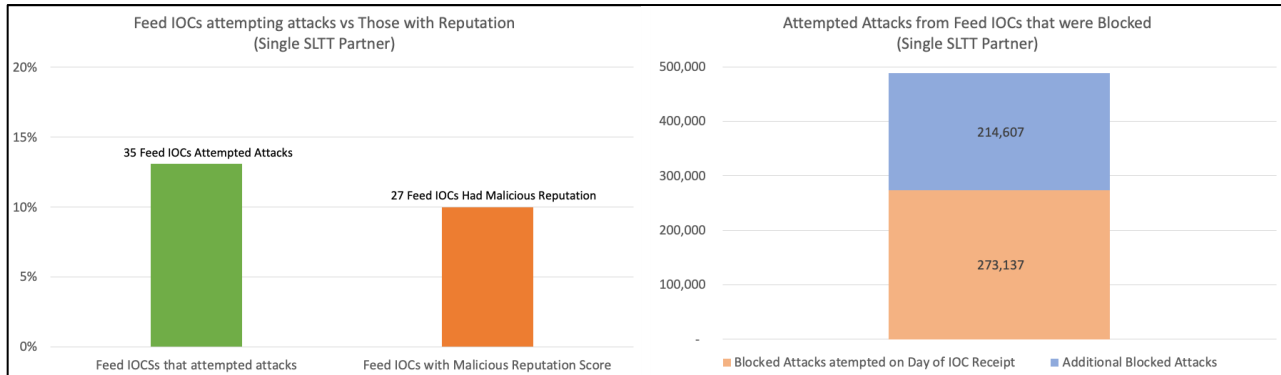


Figure 10 Receipt and Response to Feed IOCs (Single SLTT Partner)

6.2 Objective 2: Reducing time spent on repetitive tasks

The overall timelines for the core pilot performance demonstrate a substantial reduction in time spent on repetitive tasks. By reviewing the overall timelines in Figure 9, one can see a reduction in the overall process from 4,086 minutes to 3 minutes when comparing the manual and automated processes. This is due to the fact that the automation can run in the background and does not require a human to complete repetitive tasks during their work week. Even factoring in the substantial amount of time spent on waiting for a human to review an automated prompt, the pilot still demonstrates more than an eight-fold speed improvement over the manual process.

These speed improvements were also witnessed in the additional SOAR proof of concept pilot activity conducted with the Commonwealth of Massachusetts. This task focused on the single use case of threat intelligence enrichment, which was identified as a very repetitive manual task by their security personnel. As seen in Figure 11, the pilot automation reduced the time spent on the task from an average of 41 minutes per case to 9 minutes, 41 seconds.

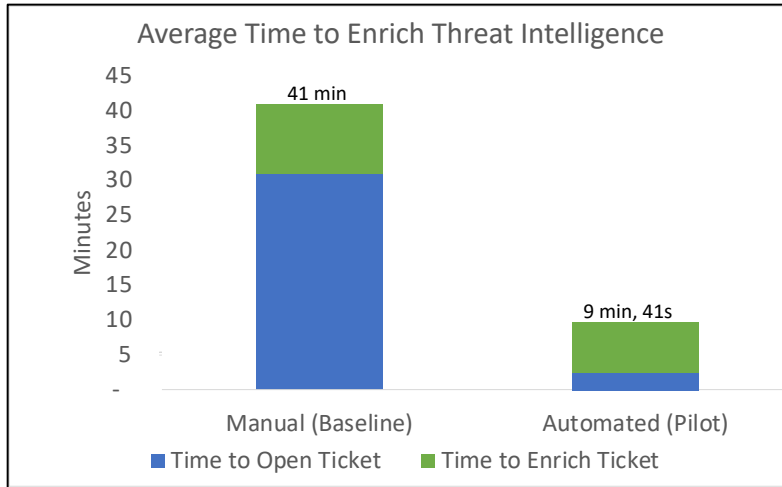


Figure 11 Threat Intelligence Enrichment Timelines

6.3 Objective 3: Providing the generation, enrichment, and scoring of IOCs

The generation, enrichment and scoring of IOCs was achieved by the creation of the pilot threat feed. The threat feed being produced for the SLTT IOC automation grant is a completely new set of IOCs derived from MS-ISAC data using a low-regret strategy. This unique strategy is based on determining the likelihood of operational impact to an organization if they respond to an IOC more than determining the “malicious-ness” or accuracy of the IOC. The regret determination and sharing processes are fully automated, and the score provided is used by the receiving sites to determine response actions in an automated fashion. Figure 12 and Figure 13 provide an overview to the scoring logic as well as the specific criteria used for enrichment and scoring.

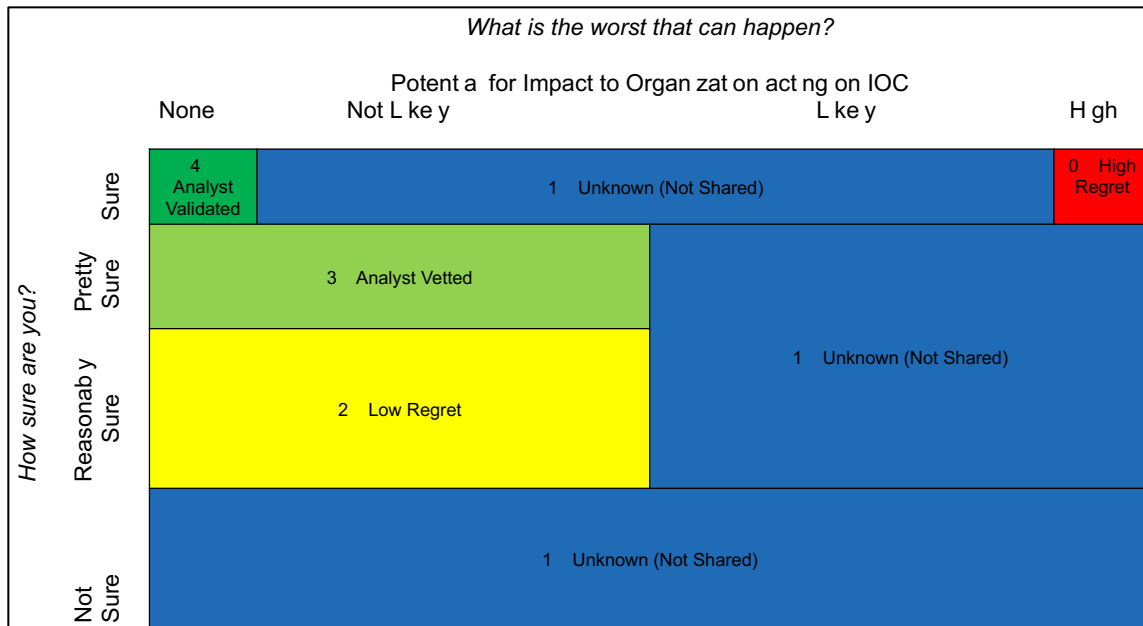


Figure 12 Threat feed scoring logic

IOC Type	Regret Score				
	0 (not shared)	1 (not shared)	2 (shared)	3 (shared)	4 (shared)
IP Address	On MS- SAC Allow list	Does NOT meet source signature Low Regret check OR P maps to more than 3 domains	Meets source signature Low Regret check And P on block list And P maps to 3 or fewer domains	(Albert) Analyst escalates associated event to an incident (MCAP) Signature meets Analyst Vetted criteria And P maps to 3 or fewer domains	On Weekly op O ends list
Domain/URL	On SL list OR On op 500 list	Does NOT meet source signature Low Regret check OR Domain is more than 365 days old	Domain is less than 30 days old OR Meets source signature Low Regret check And Domain is less than 365 days old	(Albert) Analyst escalates associated event to an incident (MCAP) Signature meets Analyst Vetted criteria And Domain is less than 365 days old	On Weekly op O ends list
File Hash	On MS- SAC Allow list	Does NOT meet source signature Low Regret check	Meets source signature Low Regret check	Signature meets Analyst Vetted criteria	On Weekly op O ends list

Figure 13 Pilot threat feed scoring criteria

The pilot threat feed provided different types of IOCs than the existing manual feed provided weekly by the MS-ISAC. Figure 14 demonstrates that the automated feed generated significantly more IOCs than the manual feed and that very few of the IOCs were common among the feeds during the time period that both feeds were running (12 weeks). This was due to the automated feed identifying IOCs that may be bad but should not disrupt operations if blocked (low-regret), whereas the manual feed was identifying IOCs that are good to block but cannot quickly be identified as low-regret.

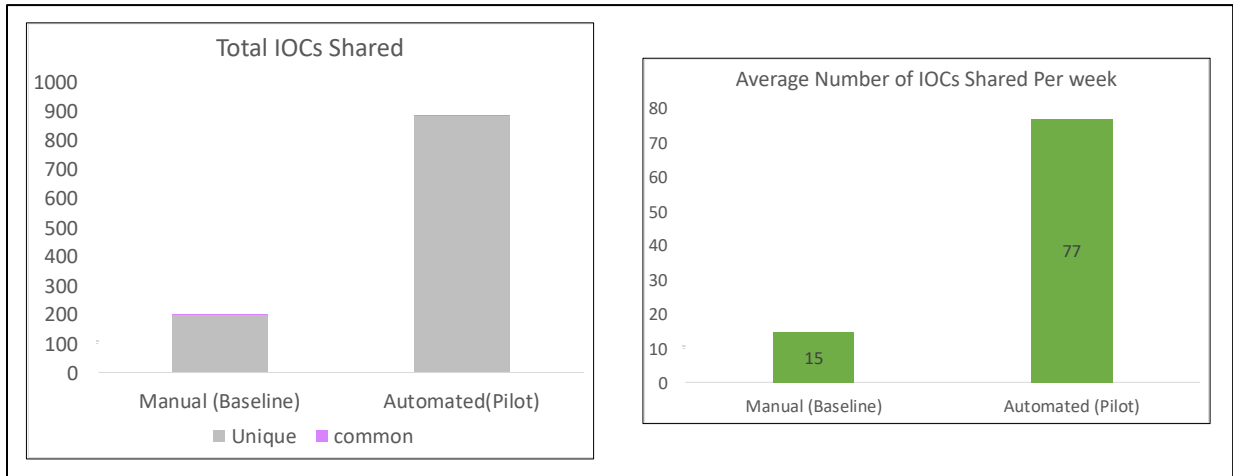


Figure 14 IOC counts from pilot and manual feeds

A summary of the numbers, types and sharing speed for IOCs in the pilot feed are provided in Figure 15. These charts provide data on the total number of IOCs received internally by MS-ISAC as well as the total number of IOCs meeting the “low-regret” threshold. It is important note that only the IOCs meeting a “low-regret” threshold are sent to the feed. The percent of IOCs meeting the “low-regret” threshold varied by

indicator type with 61% of IP addresses, 45% of domains, and 5% of file hashes meeting the “low-regret” criteria for sharing on the automated feed.

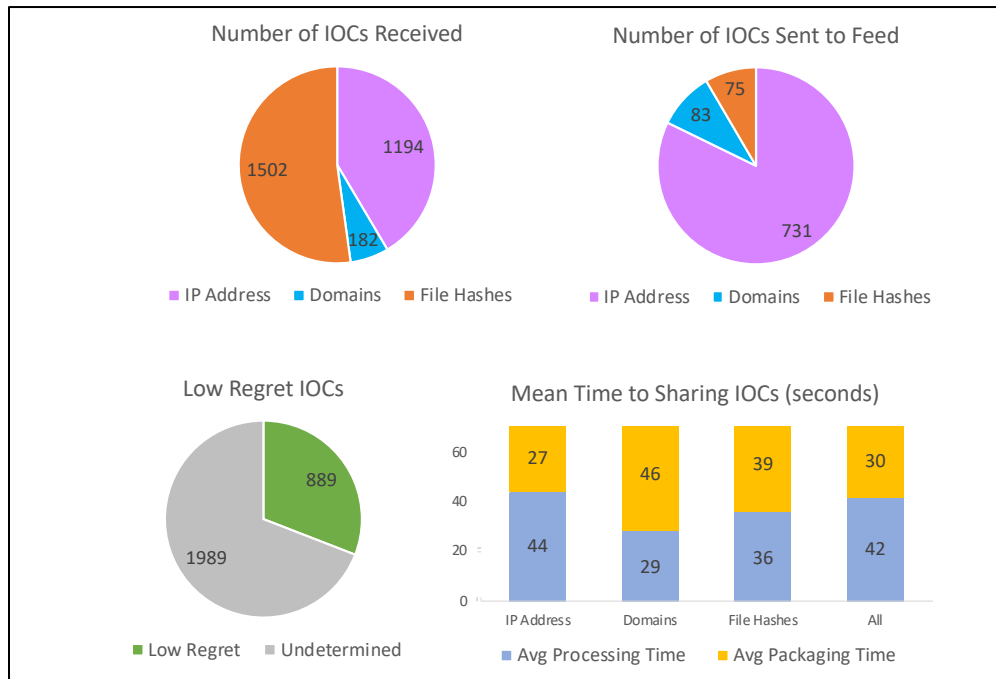


Figure 15 Pilot threat feed summary statistics

6.4 Objective 4: Receiving, remediating, and responding to IOCs

As referenced in the Design Phase Summary document (AOS-20-0915), the workflows developed for the SLTT partner organizations were developed to receive, remediate and respond to IOCs. The primary method of response to an IOC was to block it.

As seen in Figure 16, 60% of the IOCs received by SLTT partners were blocked, but 99% of the IOCs had no history on the network and were thus safe to block without disrupting operations. This means that, while the low-regret nature of the feed was preserved, the pilot partners were still able to maintain control of their own policy and chose to only block IOCs that they could confirm as truly malicious.

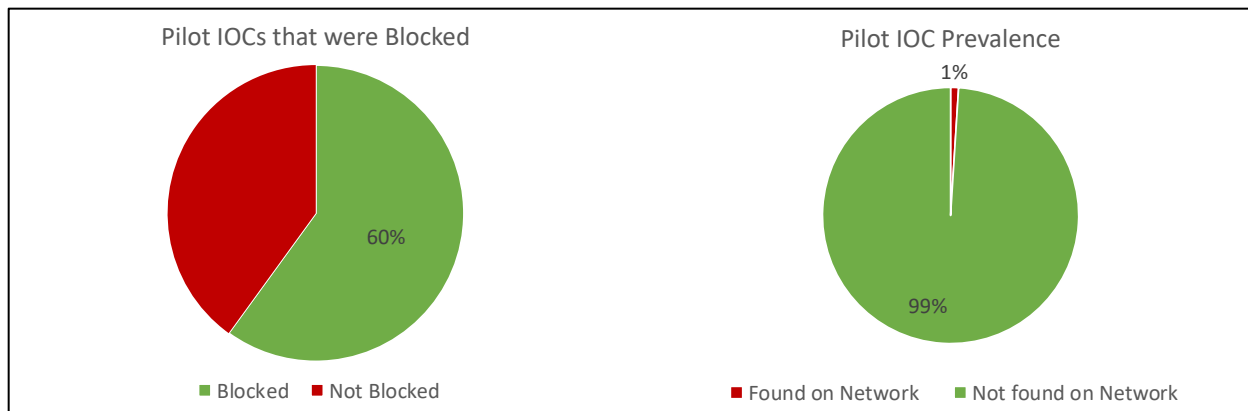


Figure 16 IOC response actions and prevalence

With longer term tracking of the IOC prevalence, an organization may be able to increase its trust in automation and allow for more automated blocking or for a greater number of IOCs to be blocked in accordance with local policy. It is plausible that the IOCs being shared by the pilot feed were arriving so early in the malware lifecycle that traditional reputation lookups would not yield a confirmation of maliciousness because the automation was seeing the IOC for the first time in its existence. By trusting the low-regret nature of the feed, organizations could significantly improve their defensive capability.

6.5 Objective 5: Demonstrating the use of SOAR

JHU/APL successfully deployed SOAR workflows with four states using various platforms across the SOAR marketplace. Each of the pilot states had a favorable response to the use of SOAR and look to continue usage of the technology.

6.6 Objective 6: Making data more actionable for consistent execution across SLTT levels

The combination of SOAR platform usage at the SLTT pilot partner and the automated, low-regret feed at MS-ISAC accomplished multiple steps toward making data more actionable and execution more consistent across SLTT levels.

There is a lifecycle to malware, and only certain types of IOCs can be detected at different operational stages by different types of technologies. In order to share IOCs that limit or prevent the compromise of SLTT members from malware infections identified by other members, an actionable feed of IOCs needs to be provided with earlier stages of the malware lifecycle. The MS-ISAC pilot feed has the ability to identify certain IOCs early in the lifecycle because the sources are behavior-based IDS alerts and forensic information. This results in the MS-ISAC feed being uniquely suited to sharing IOCs in a manner that maximizes the window of “value” for the IOC that is shared.

The core purpose of SOAR platforms guarantees consistently repeatable execution of workflows within a specific SLTT organization. To help foster reliable execution across the SLTT community, JHU/APL published vendor and organization-agnostic versions of the SOAR workflows in a standardized format (Business Process Modeling Notation, or BPMN).

6.7 Review of metrics as specified in the Notice of Funding Opportunity (NOFO)

In the NOFO for this effort, 30 metrics were identified and requested to be calculated for the completion of the grant. JHU/APL, and the IACD team in particular, is very familiar with this list as it appears derived from previous IACD community guidance on SOAR metrics.

As the authors of the source material for these metrics, JHU/APL attempted to complete all metrics possible for this effort. Several of these metrics were developed for an organization to only use internally as they are of a very sensitive nature for that organization. In the event of metrics that would require data that would not be appropriate to request, JHU/APL documented the rationale for not calculating that metric in this report.

6.7.1 Mean time to notification

Mean time to notification is defined as the time between a potential malicious activity detected and an alert is provided to the person or system responsible for investigating. For the pilot effort, this was calculated to be 2 seconds on average.

6.7.2 Mean time to investigation

Mean time to investigation is defined as the amount of time that passes between an alert being sent and the start of an investigation. For this pilot effort, this was calculated to be 4 seconds on average.

6.7.3 Mean time to remediation

Mean time to remediation is defined as the total elapsed time from alert investigation to remediation. The calculation of this metric does require some clarification. With no additional context, the average time to remediation was 488 minutes and 32 seconds. The SLTT pilot partners chose to implement a manual prompt to close-out any automated action during the pilot so that they could retain control of any automated effects. This led to operators waiting until once a day or shift to review and approve the actions. This waiting time was approximately 487 minutes on average. With that taken into account, the automation required approximately 1 minute, 32 seconds on average to remediate.

6.7.4 Remediation summary statistics

The remediation summary statistics are defined as statistics tracking manual, semi-automated and automated remediation. With the exception of time spent waiting for an operator to look at the SOAR prompts and approve the actions, each case for the pilot showed substantial improvement over the manual processes. Figure 17 provides a summary of these statistics.

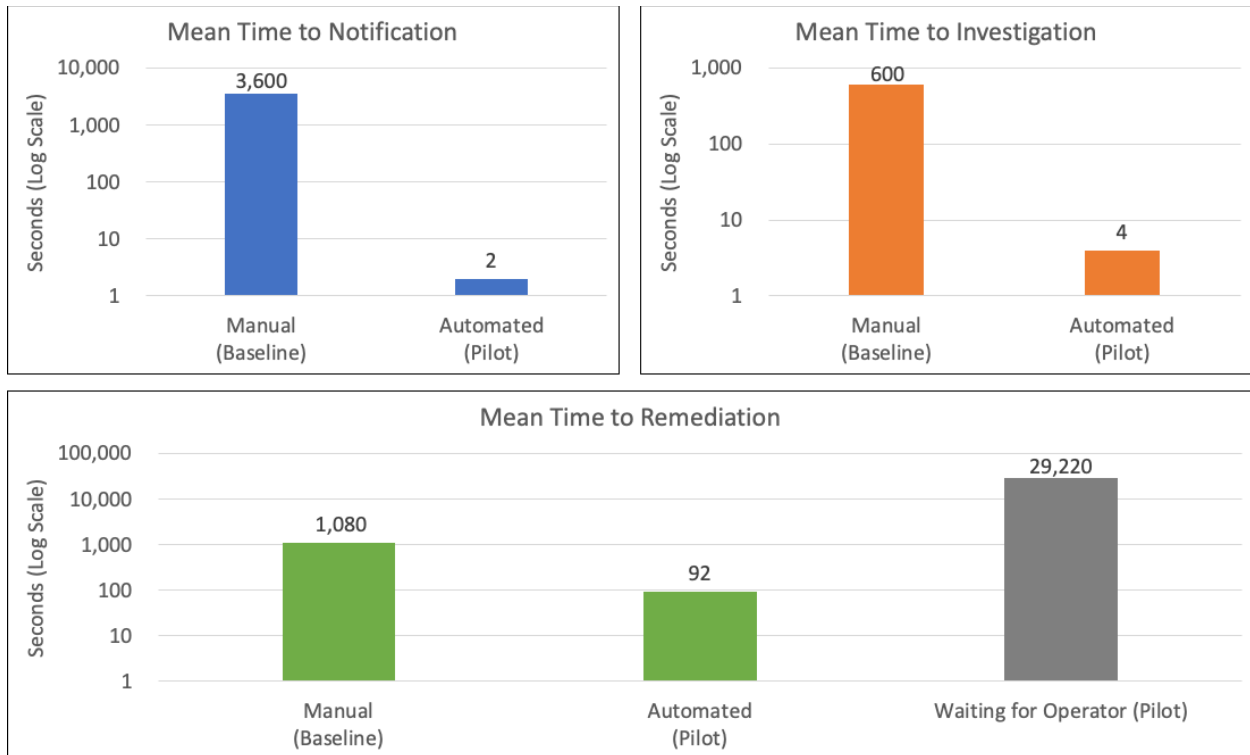


Figure 17 Remediation summary statistics

6.7.5 Percent Investigated vs. Alert Volume

The percent investigated vs alert volume metric is defined as the ratio of investigations to the total number of alerts generated.

The SLTT pilot partners did not have a method to identify alerts strictly specific to the pilot as opposed to their total alert volume. Due to this, they did not provide the total alert volume to JHU/APL and this metric could not be calculated.

6.7.6 Performance Improvements

The performance improvements metrics are defined as the information collected to show how automation is improving processes and resource utilization. Based on the data provided in Figure 9 and Figure 17, the pilot demonstrated an 88% improvement in

total response time, and if the average of 487 minutes wait time is removed, the pilot demonstrates a 99.9% reduction in total response time.

6.7.7 Workflow utility

Workflow utility is defined as the total number of incidents occurring and the number of incidents that were aided by workflows. Since the existence of a security incident for the SLTT organization is a sensitive matter, it was not appropriate to request this data as part of the pilot or to share that information with third parties. Therefore, JHU/APL did not collect this information and did not calculate this metric.

6.7.8 Sensor utilization

Sensor utilization is the tracking of playbook/workflow dependencies on sensors, threat feeds and data sources. For this pilot, the workflows at the SLTT organizations utilized the following sensors:

- The MS-ISAC automated feed
- Threat Intelligence platforms
- Firewalls
- Internet Proxies
- Endpoint Defense and Response
- Security Incident Event Manager

6.7.9 Sensor value

Sensor value is defined as the tracking of which sensors, threat feeds and data (sources) aided an investigation or remediation. For this pilot, the following aided in investigation and remediation:

- The MS-ISAC automated feed
- Threat Intelligence platforms
- Firewalls
- Internet Proxies
- Endpoint Defense and Response
- Security Incident Event Manager

6.7.10 Threat Indicator or IOC value

The threat indicator or IOC value is defined as tracking which threat indicator(s) aided an investigation or remediation. For this pilot, there were 95 IOCs that were blocked. This number accounts for about 60% of the IOCs received by SLTT partners which was a total of 158. It is important to note that more IOCs were generated by the feed but this metric only accounts for IOCs received by SLTT partners during their time of reporting metrics. It is also important to note that only 2 of the SLTT partners provided data for this metric. As a main theme of the pilot was to generate a low-regret feed, 99% of the

IOCs met the low-regret threshold of being potentially malicious but very unlikely to impact operations (having no history on the SLTT network). However, SLTT partners maintain their own policies to only block IOCs that they can assure are definitely malicious regardless of prevalence.

6.7.11 Queued workflows or actions

The queued workflows or actions is defined as the number of playbooks, workflows, investigations queued. For this pilot there was no report of any queue so the number is 0.

6.7.12 Concurrency/ Parallel workflows

Concurrency/parallel workflows is defined as the number of playbooks, workflows or investigations executed per time period. For this pilot, that was reported to JHU/APL as eight per day.

6.7.13 Workflow interface dependencies

Workflow interface dependencies is defined as tracking which product integration interfaces were used in or are required for workflow execution. The following product integrations were required for workflow execution:

- The MS-ISAC automated feed
- Threat Intelligence platforms
- Firewalls
- Internet Proxies
- Endpoint Defense and Response
- Security Incident Event Manager

Specific technology integrations would be useful for each individual SLTT partner but is not an appropriate statistic to share with third parties as it could greatly shape purchasing decisions and reveal overall defensive strategy.

6.7.14 Performance Degradation

Performance degradation is defined as information collected to show how automated processes are negatively impacting system or process performance. There were no reports of negative impact. Even in the event of waiting for the operators to interact with the automation, this was not seen as a negative impact as it still removed repetitive tasking from the operator.

6.7.15 Custom Measures & Metrics

The custom measures & metrics are defined as those created by admins and users for the pilot. This did not occur during the pilot and thus there is nothing to report for this category.

6.7.16 External process dependencies

External process dependencies is defined as tracking workflows that have a dependency on an external process or system. The details for this metric can be found in the design report, but as most workflows require either the MS-ISAC feed or a cloud-based infrastructure it does account for the majority of workflows. Based on the information from the design report, 28 of 34 (82%) of the workflows had an external process dependency.

6.7.17 Workflows requiring human intervention (as designed)

This metric is defined as the count of workflows designed requiring human intervention. This was originally 11, but several members requested to remove the human intervention after using the automation and developing more trust in the process.

6.7.18 Workflow effectiveness

Workflow effectiveness is defined as tracking which workflows were effective for their intended goal vs. required additional investigation or analysis. This was 100% of the workflows developed in this pilot. This is summarized in Figure 18.

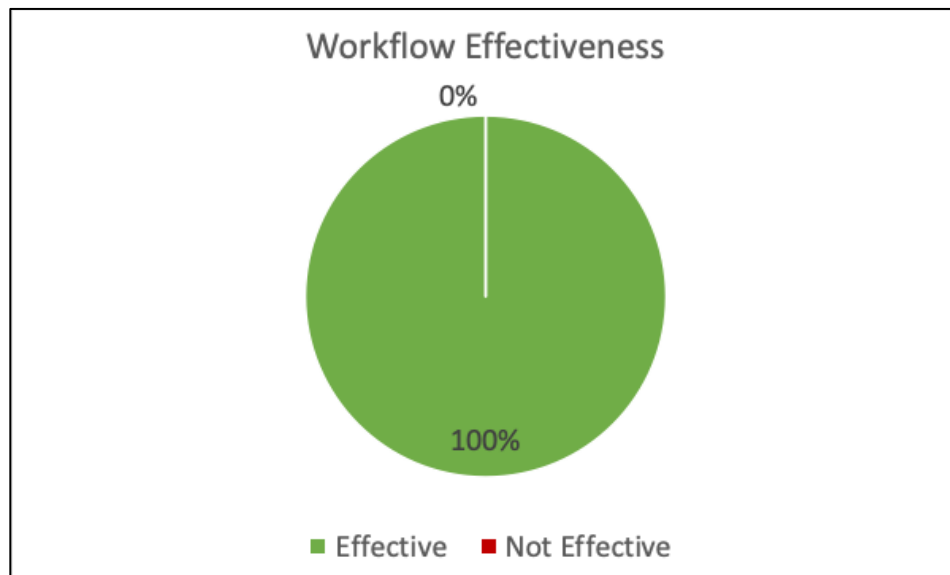


Figure 18 Workflow Effectiveness

6.7.19 Analyst / Practitioner / Organization interactions

This metric is defined as tracking which organizations and staff were required to interact with a workflow to facilitate an end goal. In general, this was the SOC staff for each organization. However, more specific results would be divulging the detailed defensive plans for each SLTT organization and would not be appropriate to share with third parties. Therefore further information was not collected for this metric.

6.7.20 Frequency of workflow revisions

This metric is defined as statistics tracking the frequency of workflow / playbook revisions. It is intended for an organization to use internally over a long period of time to help with workflow configuration management. It was not reported to JHU/APL during this pilot but is assumed to be fairly low.

6.7.21 Frequency of workflow execution

This metric is defined as statistics tracking the frequency of workflow / playbook execution and is intended to be used by an organization internally to understand which workflows are used the most. As a small set of core workflows were deployed for this pilot, the data does not provide a useful insight into pilot performance and was not recorded.

6.7.22 Frequency of remediation actions taken

This metric is defined as statistics tracking the frequency of actions taken to remediate threats / risks. It is intended to be used internally by an organization to better understand the actions that are being handled by automation versus those taken by manual actions. As the pilot scope primarily only allows for blocking of IOCs, there is not useful information to collect for this metric during this pilot.

6.7.23 Workflow utilization

Workflow utilization is defined as tracking how many times a workflow is selected manually vs. how many times it is selected in an automated action. As manual launching of workflows was only done for integration testing, this metric is not applicable to the data from this pilot.

6.7.24 Workflow value

Workflow value is defined as the savings estimate by multiplying the cost of performing repetitive tasks manually by the estimated number of times the system performs those tasks automatically during a specific date / time range. As this requires very sensitive salary information for different organizations and contract details for events managed by

third parties for the SLTT organizations, it was deemed inappropriate to request this level of costing information for the pilot.

6.7.25 Workflow confidence level

Workflow confidence level is defined as statistics tracking the frequency automated recommendations are confirmed for execution. This information was not reported or captured by the SOAR platforms and was thus not analyzed.

6.7.26 Workflow idle time

Workflow idle time is defined as statistics tracking times workflows were paused waiting for data, a decision, action or approval. On average, this was 487 minutes due to operators only visiting orchestrator prompts once per shift or day. It is important to note that this occurred in parallel and not in series for all workflows within a given day.

6.7.27 Workflow reliability

This metric is defined as tracking successful versus unsuccessful workflow executions. For this pilot, that was 99% of the workflow executions. This is summarized in Figure 19. For the 1% that have failed, SLTT partners reported infrastructure upgrades to be the most likely reason.

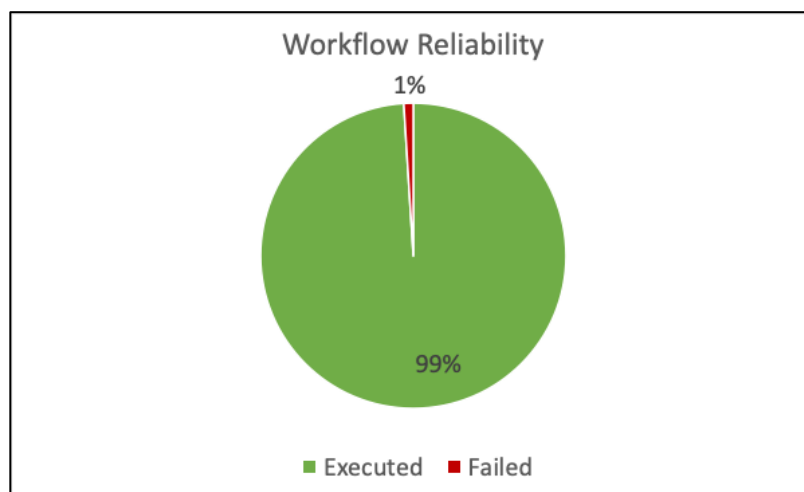


Figure 19 Workflow Reliability

6.7.28 Workflow decision processing

This metric is defined as the capture of triggering condition, key values/decision points, and end state for workflows. This is not a metric as much as it is an element of the workflow design. Please consult the design summary report for a full description of this for each workflow developed in this pilot.

6.7.29 Workflow dwell time

This metric is defined as statistics tracking workflow execution times. Please see Figure 9 for a summary of these timelines.

6.7.30 Workflow deployment readiness

This metric is defined as evidence verifying and validating workflows were created by compliant practices and execute as intended. Based on acceptance criteria and discussions with all pilot participants, 100% of the workflows met these criteria.

7. Additional insights and lessons learned

Outside of the core metrics for the grant effort, JHU/APL has also captured several qualitative insights based on both discussions with the pilot partners and survey responses. While these are subjective inputs, they do provide additional insight into the progress made by pilot partners and the existing challenges for the deployment of security automation.

7.1 Insights from pilot partner discussions

The core lessons learned from these discussions are documented in the JHU/APL AOS-20-1036 report entitled *DHS-19-CISA-128-SLT-001 State, Local, Tribal and Territorial Indicators of Compromise Automation Pilot Phase 3 – Execution Phase Summary Report*. However, the high level lessons learned are provided here for consistency in the reporting:

- Impacts of COVID-19
 - All organizations rose to the challenges presented by the pandemic
- Technical challenges of using TAXII
 - Use of TAXII clients and servers presents challenges to users
- Stakeholder identification
 - Proper identification of all internal stakeholders plays a critical role
 - Vendor interaction varied from one organization to another; when vendors were committed, efforts moved at far greater speed
- Familiarity with programming and scripting in SOCs
 - Some SOC operators cannot incorporate scripts easily
 - Design of “turn-key” workflows, use of containers, etc. are needed for widespread adoption
- API access for cloud versions of tools
 - Certain tools migrated to the cloud have reduced their API access for cloud versions which has reduced access to increased security features
 - Use of API gateways and other feature requests are needed for cloud based tools to leverage automation fully

7.2 Analysis of survey responses

Overall, the SLTT partners found the pilot to be a worthwhile experience and have begun transitioning pilot technologies to secure their networks. This can be seen in Figure 20. While two of the SLTT organizations replied that the technology did not help secure their networks, the comments provided with those responses stated that one partner had not finished deploying the technology and the other used the insights from the pilot to design their enterprise security strategy.

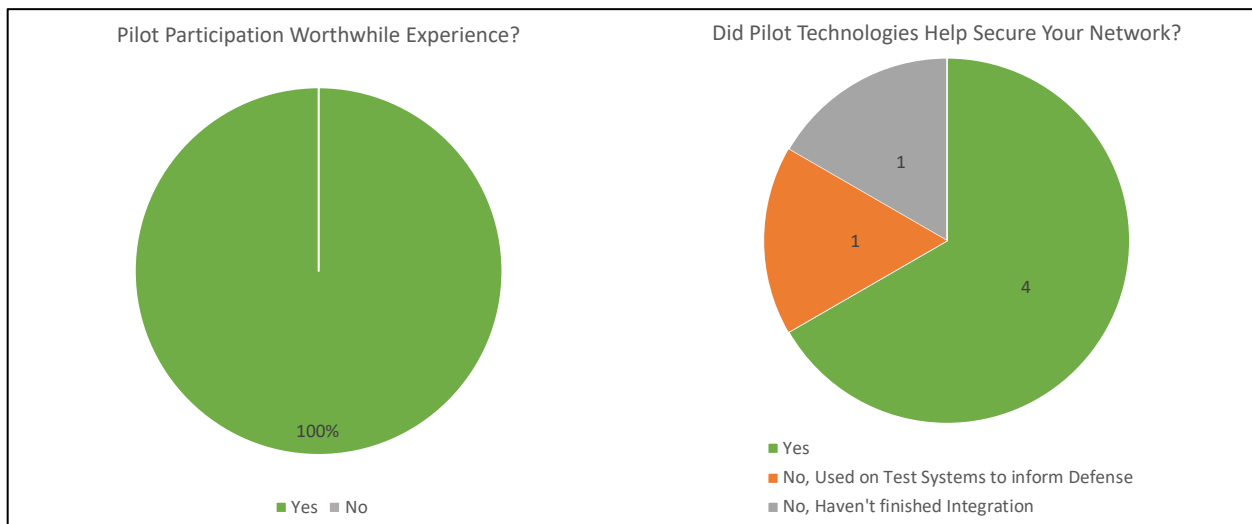


Figure 20 Survey results on pilot effectiveness

Figure 21 provides a summary of which pilot capabilities were in use before the pilot and which are now planned for future use after completing the pilot. The use of automation both for ingest of IOCs and SOAR workflows for response has been very well received by the pilot partners. There is also an interesting observation that while only a minority of the pilot partners were using MS-ISAC IOCs prior to the pilot, the majority have found value in the pilot feed and plan to continue using it. This demonstrates the value of a low-regret feed of IOCs and the automation capabilities evaluated during this pilot.

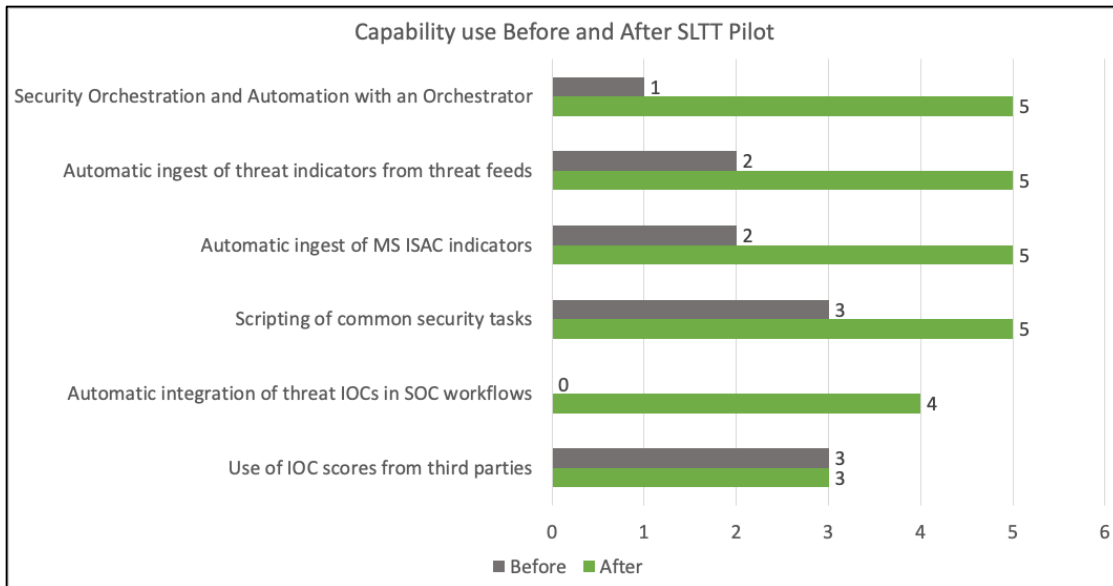


Figure 21 Pilot partner plans for future use

Figure 22 provides a summary of the pilot partner responses with respect to the value of various pilot resources. As can be seen in the responses, the technical exchanges, SOAR workflows, playbooks, and support from JHU/APL were viewed the most favorably.

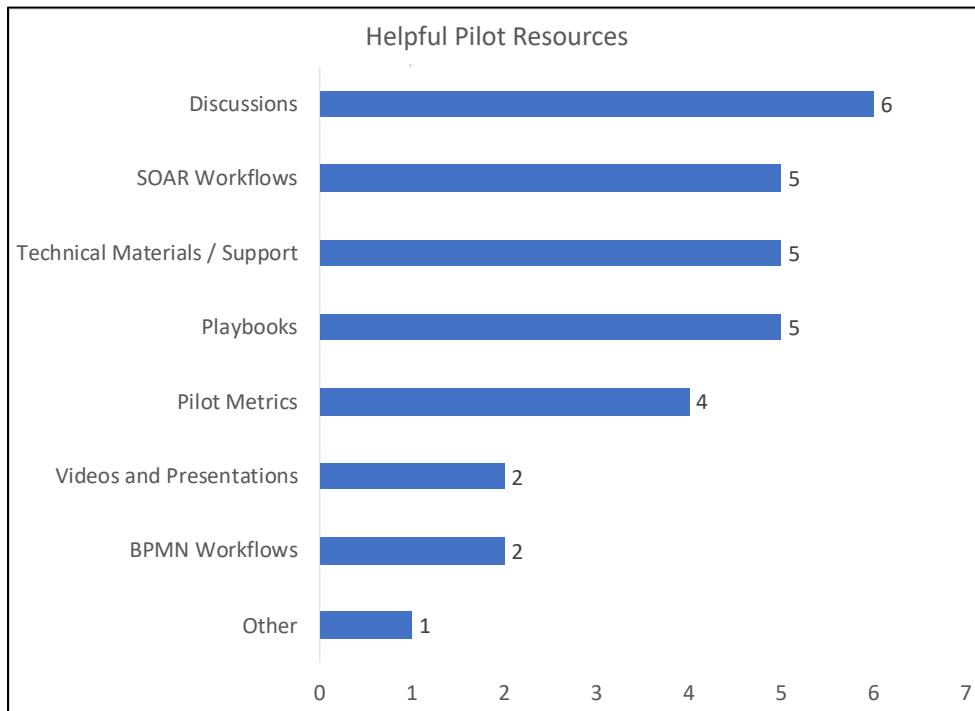


Figure 22 Pilot partner opinions on pilot resources

8. Next steps for pilot participants

The efforts of this pilot will continue to be applied by the participants and will help the overall SLTT community. The following summary is provided to give an overview for each of the pilot partners.

The MS-ISAC found distinct value in the automated low-regret feed of IOCs and has transitioned the technology into a production offering. On September 28, 2020, a production version of the feed will be made available to all pilot participants and integrated with those interested. After the pilot's conclusion, MS-ISAC will work to make the feed available to their 7,000+ members.

The majority of SLTT organizational participants are planning to continue their use of SOAR and security automation based on their experiences with this pilot. Many have already begun to research and develop expanded use cases to leverage the capability identified in the pilot. Additionally, several members are looking to expand similar capability from the pilot either within their states (reaching out to the "LTT" organizations) or to provide examples for other states interested in using SOAR.

JHU/APL collected a large amount of data and insights from the pilot and is planning to continue making industry guides and best practices available to the entire SLTT community as well as other members of the critical infrastructure community. This will include the creation of various whitepapers, job aids, and reports on a variety of topics not limited to:

- Differentiating between automation and orchestration
- Guidance to best enable automation and orchestration in an operational environment
- Making manual processes supportive of automation
- Cyber threat intelligence (CTI) triage techniques
- Sharing courses of action and alternative CTI sharing techniques
- Understanding the value of various CTI within the malware lifecycle

9. Conclusion

The core effort of the *DHS-19-CISA-128-SLT-001 State, Local, Tribal and Territorial Indicators of Compromise Automation Pilot* has been a resounding success. Through the support and efforts of CISA Stakeholder Engagement, the MS-ISAC, Arizona, Louisiana, Massachusetts, and Texas, JHU/APL collaborated on the creation of both a new threat feed that provides more actionable cyber threat intelligence at a faster rate as well as deployed orchestrated security actions that allow for overall process improvements several orders of magnitude faster than current manual processes. Through the sharing of the findings, shareable workflows, and the planned development of additional guidance, the entire SLTT community will be able to leverage the findings of this work to improve their survivability against an ever growing cyber threat.



The fact that this work was completed within a 12-month period is in itself impressive, but of definite note is the fact that this pilot occurred during the globally historic COVID-19 pandemic. The continued dedication of all the participants during this trying time is worthy of commendation. JHU/APL sincerely thanks all participants for their steadfast support and participation in this effort.

For any questions on the findings of this effort, please do not hesitate to contact the Principal Investigator from JHU/APL, Charlie Frick:

Charlie Frick
11100 Johns Hopkins Road
Laurel, MD 20723
(240) 228-3894
Charles.Frick@jhuapl.edu