STATE, LOCAL, TRIBAL, & TERRITORIAL INDICATORS OF COMPROMISE AUTOMATION PILOT

ENABLING RAPID CYBER RESPONSE: SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE WORKFLOWS BEST PRACTICES TO ENABLE SLTT GOVERNMENTS TO RAPIDLY RESPOND TO CYBER INDICATORS OF COMPROMISE

State, local, tribal and territorial (SLTT) governments and organizations depend on information technology systems and computer networks for essential operations. These systems face large and diverse cyber threats that range from unsophisticated criminals to technically competent intruders using state-of-the-art intrusion techniques. Many malicious attacks are designed to steal information and disrupt, deny access to, degrade or destroy critical information systems. The Cybersecurity and Infrastructure Security Agency (CISA) works with SLTT governments to promote the adoption of common policies and best practices that are risk-based and able to effectively respond to the pace of ever-changing threats.

Under Grant Award Number DHS-19-CISA-128-SLT-001 (State, Local, Tribal, and Territorial Indicators of Compromise Automation Pilot) CISA awarded a cooperative agreement to the Johns Hopkins University Applied Physics Laboratory (JHU/APL) to help SLTT governments enhance their cybersecurity defenses and rapidly respond to Indicators of Compromise (IOC) through the development of Security Orchestration, Automation and Response (SOAR) workflows and guides to provide best practices to the SLTT community. These workflows and guides were derived through a successful pilot project utilizing SOAR with the generation and response to IOCs with several SLTT community members. Such workflows are vendor agnostic and provide a starting point for implementing technologies and processes for security automation needs.

Background SLTT Decision Makers

Security Orchestration, Automation and Response (SOAR) is a technology stack of compatible software applications incorporating automated responses to low to mid-level security events. Having such a capability allow organizations to respond rapidly to indicators of compromise.

CISA is providing sample workflows and guides to assist SLTT governments that are using or considering SOAR to automate their cybersecurity operations. Recognizing SOAR is an advanced capability that not all SLTT governments will be able to adopt immediately, the intention is three fold: 1) provide SLTT governments that are ready to implement or procure such services with resources; 2) provide planning considerations for SLTT governments to consider for future action; and 3) initiate a conversation with the broader cybersecurity community on where we should be moving.

PILOT PROJECT OVERVIEW

Under the SLTT IOC Automation pilot project, the states of Arizona, Louisiana, Massachusetts, and Texas, Maricopa County, and the Multi-State Information Sharing and Analysis Center (MS-ISAC) applied SOAR cyber defense capabilities to rapidly respond to cyber IOCs. The pilot utilized multiple SOAR tools to enable the pilot partners to collect security threat data via multiple sources and perform triage response actions significantly faster than manual processes. The pilot initiative enabled SLTT governments to quickly respond and share information in near real-time to prevent or respond to cyber intrusions, reducing the timeframe between the first identification of an IOC to successful blocking the IOC. This dramatically reduced response time from an average of three days to approximately three minutes.

The SLTT IOC Automation Pilot focused on both the curation of the automated feed and the processes used by the 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. In particular, the project:

- Identified key areas for potential reduction of manual tasks
- Promoted actionable information sharing across government levels and agencies
- Identified orchestration services needed to integrate responses – such as sensing, understanding, decision-making and acting – to cyber threats

The pilot project stemmed from recent JHU/APL research with critical infrastructure industries that showed how automated information sharing can shore up cyber defenses by reducing response time. This was made possible by using the Integrated Adaptive Cyber Defense Framework, developed by JHU/APL and sponsored by CISA and the National Security Agency,

SOAR WORKFLOWS

To further assist SLTT governments to rapidly respond to cyber threats, CISA and JHU/APL developed 85 workflows to deploy the capabilities of SOAR. Workflows are the machine understandable codification of playbooks to enable automation of procedures. These workflows are available to all SLTT governments for free via the CISA GitHub within the following repository: https://github.com/cisagov/shareable-soar-workflows.

The SOAR workflows are mapped and organized based on how they align with the National Institute of Standards and Technology (NIST) Cybersecurity Framework. This repository includes 51 SOAR workflows aligned to provide an initial set of processes for processing threat intelligence, processing of alerts, threat detection, response, and mitigation. These workflows provide a starting point for those organizations interested in deploying SOAR capabilities within their organizations and illustrate how workflows can be interconnected to enhance usability.

In addition to the core set of SOAR workflows, CISA provides 34 additional workflows as a Use Case to illustrate how SLTT governments can tailor these workflows to address their own environments. This Use Case is an abstract of the pilot effort.

The SOAR workflows are provided in both visual Portable Network Graphic (i.e., PNG) files and machine-readable Extensible Markup Language (i.e., XML) via the Business Process Model Notation (BPMN) standard. Each workflow has a descriptive guide to assist organizations in understanding the workflow intent and how they can be tailored for specific organizational needs. The interdependencies between workflows are also identified and documentation of those relationships are found in the main README file within the repository.

"LOW REGRET" IOC FEED IMPLEMENTED WITH MS-ISAC

The pilot also resulted in SLTT agencies having access to a new automated IOC feed capability via the MS-ISAC. This feed is operational and available to MS-ISAC members across the nation. This automated SOAR feed utilizes a "low regret" methodology, meaning an SLTT government agency can allow the automatic blocking of IOCs with confidence that it poses a malicious threat and near certainty that the automated block will not disrupt operations. The automated feed serves as a model for other SLTT governments to quickly and easily augment their cyber defense capabilities. More detail on the methodology can be found at https://github.com/JHUAPL/Low-Regret-Methodology. Access to the feed and other MS-ISAC services and products can be found here: https://www.cisecurity.org.

BEST PRACTICES TO RESPOND TO EVER-CHANGING THREATS

To further assist cybersecurity efforts within the SLTT community, CISA, along with JHU/APL, is providing a series of short technical guides and papers on cybersecurity automation and threat intelligence sharing best practices.

These resources assist organizations with the assessment of products, services or feeds and the associated cost to ascertain what solution best aligns with the organization's requirements. The references include the following topics:

- Assessing Cyber Threat Intelligence Feeds
- Operational Value of Indicators of Compromises
- Service Models for Cyber Threat Intelligence
- Cyber Threat Intelligence Sharing Infrastructures
- Enabling Automation in Security Operations - Assessing Automation Potential of Products and Services
- Enabling Automation in Security Operations - Strategy for Efficient Process Automation
- Enabling Automation in Security Operations - Increasing Automation Potential of Processes
- Applying Low Regret Methodology for Cyber Threat Intelligence Triage
- Applying Low Regret Methodology for Response to Indicators
- Cybersecurity Orchestration - Orchestration of Information Technology Automation Framework
- Cybersecurity Orchestration - Information Centric Automation and Orchestration

FREQUENTLY ASKED QUESTIONS

Who is the intended audience for these resources?

The workflow repository is intended for all organizations interested in designing SOAR workflows to automate their cybersecurity operations. The technical guides are intended for all organizations that utilize or are considering utilizing Cyber Threat Intelligence feeds and/or SOAR capabilities.

What can an organization do with the workflows?

While the workflows do not address all possible cybersecurity use cases, they do provide a "starting point" for many activities involving the processing of threat intelligence, alert triage, threat detection, and response. The workflows outline various automated processes that an organization can tailor to aid in their design of SOAR workflows for their organization.

For organizations utilizing a SOAR platform that can ingest BPMN format, the workflows can be imported into those platforms but will require tailoring to map actions to specific technologies and policy. CISA does not wish to endorse any particular technology vendor, and these workflows do not contain any specific references to any particular vendor.

What can an organization do with the technical guides and papers?

The technical guides provide key insights into the use of cyber threat intelligence feeds and automated workflows. They are intended to aid organizations as they evaluate their current capabilities and develop implementation strategies for their cyber threat intelligence feeds and security automation efforts.

FREQUENTLY ASKED QUESTIONS

Is there any cost for these resources?

The workflows and technical guides are provided free of charge to assist the SLTT community and all of critical infrastructure.

Can an organization use these resources without a SOAR platform?

The workflows are intended to be implemented via a SOAR platform but may also provide guidance for general security process steps.

The technical guides referencing cyber threat intelligence feeds do not require a SOAR platform but are designed to assist organizations and their Managed Security Service Providers (MSSP) in achieving maximum benefit from their available resources.

Is CISA providing a SOAR capability for SLTT governments through these resources?

CISA is not a providing a SOAR capability.

Do these resources help against current high priority cyber threats such as ransomware and supply chain risk management?

The SOAR workflows address a large variety of cybersecurity tasks within the NIST Cybersecurity Framework but do not cover all possible tasks. The provided workflows can assist in detection and response to various threats once information is shared or alerts are provided by various vendors. However, they do not address detailed forensics that may lead to new threat discovery.

CONTACT CENTRAL@CISA.DHS.GOV FOR MORE INFORMATION