SWIMLANE

Get On Track with Executive Order M-21-31

White Paper

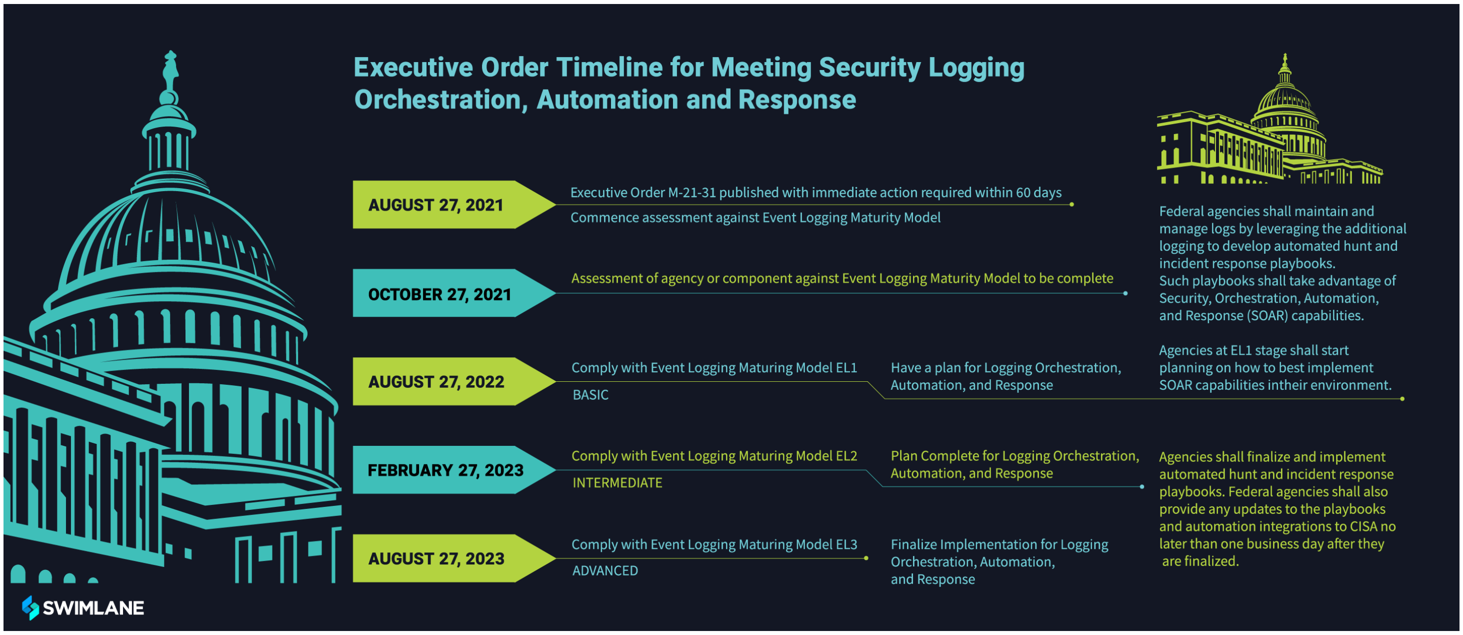
Implementing Low-Code Security Orchestration, Automation and Response (SOAR) to Comply with the Executive Order

Public sector and federal government organizations, and those who work with the government, are under attack every day. These organizations must continue to update the methods, controls, and operational expectations of what it means to keep agencies and component agencies secure. Recent events and active campaigns around the Log4j, Microsoft Exchange, and SolarWinds have all brought to the forefront that the need for visibility and response is greater than ever.

The Department of Homeland Security Cybersecurity & Infrastructure Security Agency (CISA), along with Executive Orders from the President of United States, have mandated several new security directives around Zero Trust, Logging, and Security Orchestration, Automation, and Response (SOAR). Two of the recent Executive Orders include M-22-09 and M-21-31, which are government-wide programs that have immediate impacts to expectations and roadmaps for public sector agency security programs.

EXECUTIVE ORDER M-21-31 goes into detail around the specific timelines and expectations for the mandate for the maturing of Security Logging Orchestration, Automation, and Response, otherwise known as SOAR. The order outlines a three-phase approach that requires for the planning and implementation of standardized logging as well as orchestration, automation and response across all government agencies within 24 months.

Below is the timeline set out in the Executive Order relating to the Logging Orchestration, Automation, and Response:



Executive Order Timeline for Meeting Security Logging Orchestration, Automation and Response

AUGUST 27, 2021
Executive Order M-21-31 published with immediate action required within 60 days
Commence assessment against Event Logging Maturity Model

OCTOBER 27, 2021
Assessment of agency or component against Event Logging Maturity Model to be complete

Federal agencies shall maintain and manage logs by leveraging the additional logging to develop automated hunt and incident response playbooks.
Such playbooks shall take advantage of Security, Orchestration, Automation, and Response (SOAR) capabilities.

AUGUST 27, 2022
Comply with Event Logging Maturing Model EL1
BASIC
Have a plan for Logging Orchestration, Automation, and Response
Agencies at EL1 stage shall start planning on how to best implement SOAR capabilities intheir environment.

FEBRUARY 27, 2023
Comply with Event Logging Maturing Model EL2
INTERMEDIATE
Plan Complete for Logging Orchestration, Automation, and Response
Agencies shall finalize and implement automated hunt and incident response playbooks. Federal agencies shall also provide any updates to the playbooks and automation integrations to CISA no later than one business day after they are finalized.

AUGUST 27, 2023
Comply with Event Logging Maturing Model EL3
ADVANCED
Finalize Implementation for Logging Orchestration, Automation, and Response

SWIMLANE

The schedule outlined by the Executive Order details an extremely aggressive timeline based on enterprise and government agency standards for planning and implementing a robust security logging, automation, incident response, and threat hunting program. While the Executive Order is brief, what it describes are explicit expectations for agencies to be able to observe, monitor, hunt, and respond to security logging in their respective environments.

While many agencies have been implementing logging programs for years, the ability to take automated response to logging activity is still in the planning phases at many agencies, and while there are examples of government components implementing extremely successful programs, most agencies have a lot of planning and work ahead of them.

Understanding the Executive Order Requirements

ORCHESTRATION is the ability to ingest information in real-time, analyze it, make a determination (e.g. risk, severity, etc.) and ultimately use that information to make updates, changes, or take action in multiple disparate systems simultaneously in real-time. The goal of orchestration is to leverage the information and intelligence from one source into multiple other sources without the need for individuals to manually copy and paste data to and from multiple locations.

An example of orchestration could be a SIEM alert triggered from an impossible login, where one user is logging in from two different geographic regions at the same time. With that alert, the workflow might include orchestrating changes to the network and endpoint security tools by taking both source IP addresses from the alert and adding them to the network and endpoint security rules or policies. This is then setup to trigger alerting based on any activity from either source so it can be visualized by network or endpoint security monitoring.

AUTOMATION is the ability to do the work of a person without the need of that person. The goal of automation is to remove the burden on people to process the endless amount of data that is generated every day by security tools.

An example of automation could include an alert triggered from an Endpoint Detection and Response (EDR) implementation that flags a user who is attempting to visit a known malicious website, where the use of automation automatically searches all of the logs for any other users who might be attempting to access the same malicious website. This simple automation workflow could potentially identify a phishing campaign or other attack where multiple hosts or users have been targeted with the same campaign.

RESPONSE is the ability to take mitigative steps to prevent or thwart a security breach. The goal of response, especially the automated type, is to respond as quickly as possible to malicious activity across the environment to reduce the potential impact of malicious actors.

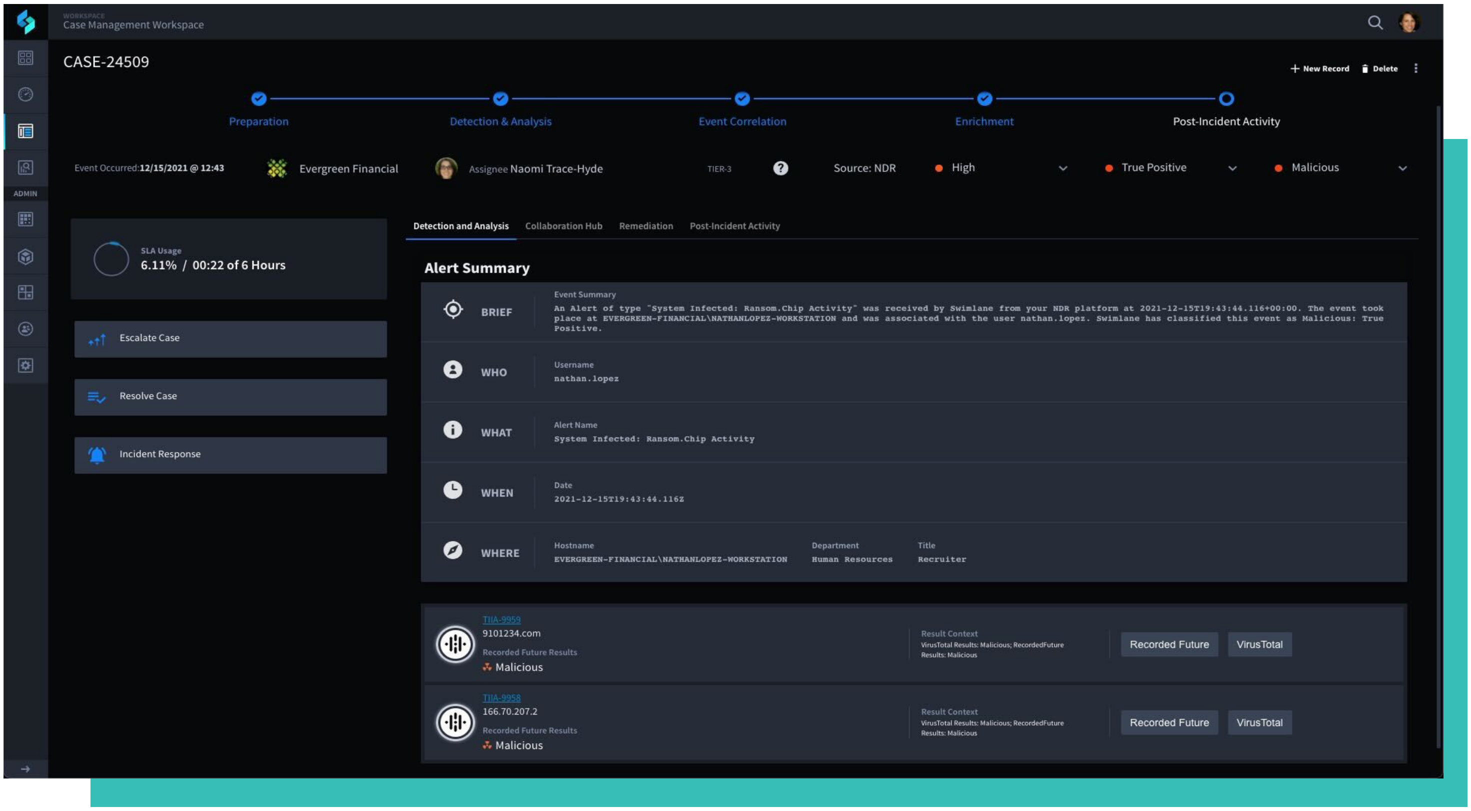
An example of response could include an alert from a User or Entity Behavior Analytics (UEBA) system triggering the SOAR platform to send a request to a Zero Trust infrastructure to force a user to reauthenticate their current session to ensure the identity of the logged-in user.

Compliance with NIST Standards

In order to meet the Executive Order, any Orchestration, Automation and Response capabilities must also comply with The National Institute of Standards and Technology (NIST) requirements for Incident Response outlined under 800-61 Revision 2. This means that methodology used to respond to logging alerts will require the NIST process of:

- Preparation
- Detection & Analysis
- Containment, Eradication, & Recovery
- Post-Incident Activity

The ability to meet the 800-61 guidelines can be extremely difficult with a highly-manual process, but meeting both the 800-61 guidelines and the Executive Order are now impossible to adhere to without the proper tooling. Below is an example of a case management powered by Swimlane that is following both industry best practices, as well as the NIST methodology for incident response.



CASE-24509

Event Occurred: 12/15/2021 @ 12:43 | Evergreen Financial | Assignee Naomi Trace-Hyde | TIER-3 | Source: NDR | High | True Positive | Malicious

SLA Usage
6.11% / 00:22 of 6 Hours

Alert Summary

BRIEF — Event Summary
An Alert of type "System Infected: Ransom.Chip Activity" was received by Swimlane from your NDR platform at 2021-12-15T19:43:44.116+00:00. The event took place at EVERGREEN-FINANCIAL\NATHANLOPEZ-WORKSTATION and was associated with the user nathan.lopez. Swimlane has classified this event as Malicious: True Positive.

WHO — Username
nathan.lopez

WHAT — Alert Name
System Infected: Ransom.Chip Activity

WHEN — Date
2021-12-15T19:43:44.116Z

WHERE — Hostname: EVERGREEN-FINANCIAL\NATHANLOPEZ-WORKSTATION | Department: Human Resources | Title: Recruiter

TIIA-9959
9101234.com
Recorded Future Results
Malicious
Result Context
VirusTotal Results: Malicious; RecordedFuture Results: Malicious

TIIA-9958
166.70.207.2
Recorded Future Results
Malicious
Result Context
VirusTotal Results: Malicious; RecordedFuture Results: Malicious

As you can see, Swimlane is managing all of the important information about the case by checking information against threat intelligence, tracking case severity, status, and who is assigned to the case. More than that, Swimlane is guides the user through the process of Preparation, Detection, Analysis, Containment, Eradication, Recovery, and Post-Incident Activity. This provides the organization a full audit trail of every action and decision, as well as building a centralized set of historical information to serve as a system of record for future analysis, reporting and decision making.

This case management system satisfies the great majority of requirements for a compliant Logging Orchestration, Automation, and Response system. As it relates to NIST, Swimlane satisfies the following NIST requirements:

NIST 800-61 Revision 2 requirements by Section

- 3.2.5 - Incident Documentation
    - The current status of the incident (new, in progress, forwarded for investigation, resolved, etc.)
    - A summary of the incident
    - Indicators related to the incident
    - Other incidents related to this incident
    - Actions taken by all incident handlers on this incident
    - Impact assessments related to the incident
    - Contact information for other involved parties (e.g., system owners, system administrators)
    - A list of evidence gathered during the incident investigation
    - Comments from incident handlers
    - Next steps to be taken (e.g., rebuild the host, upgrade an application).
- 3.2.6 - Incident Prioritization
    - Functional Impact Analysis
    - Information Impact Analysis
- Recoverability Effort Analysis
- 3.2.7 - Incident Notification
- 3.3.2- Evidence Gathering and Handling
- 3.4 - Post Incident Activity Reporting
- 3.4.1 - Lessons Learned Management
- 3.4.2 - Using Collected Incident Data (Metrics and Tracking)
    - Number of Incidents Handled
    - Time Per Incident
    - Objective Assessment of Each Incident
    - Subjective Assessment of Each Incident
- 3.4.3 - Evidence Retention
- 3.5 - Incident Handling Checklist
- 4.1 - Coordination
- 4.1.2 - Information Sharing
    - 4.2.1 – Ad-hoc Information Sharing
    - 4.2.2 - Partially Automated Information Sharing

In addition to the above requirements, NIST outlines in Section 2.3.2 that each of these elements of Incident Handling must "meet its unique requirements, which relates to the organization's mission, size, structure, and functions." To simplify that requirement,

the organization's tooling must be able to be configured to meet the needs of the agency and the agency should not implement generic, vendor defined processes.

In order to meet that specific requirement, agencies should be looking for solutions such as low-code automation offerings that allow agencies to easily configure incident handling procedures into the system.

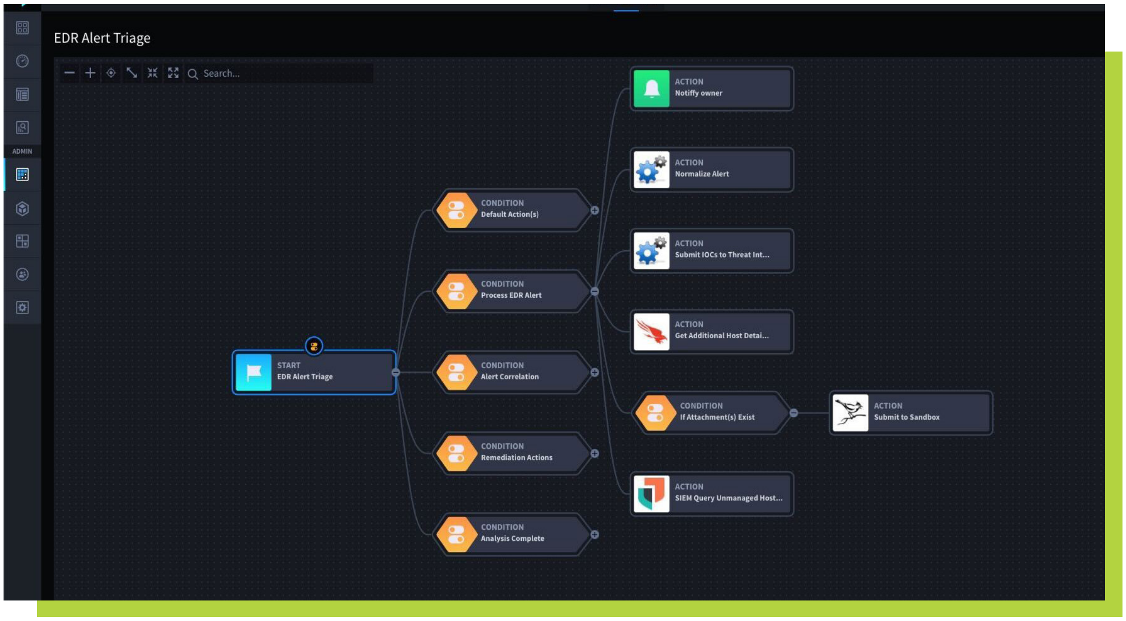
Getting Started on Logging Orchestration, Automation and Response

Per the Executive Order, every federal agency *"shall take advantage of Security, Orchestration, Automation, and Response (SOAR) capabilities. Agencies at EL1 stage shall start planning on how to best implement SOAR capabilities in their environment."*
So what does a plan look like for meeting the M-21-31? below are the key steps:

1. Get clarity on the difference between Logging, SIEM and Automation. Read more about SIEM vs SOAR here.
2. Get your logging in order. Without proper logging, there is nothing to respond to. To setup a strong security logging program, make sure you do the following:
    a. Ensure you have a scalable and robust logging solution.
    b. Ensure you are collecting in accordance with NIST 800-92 and appendices A & C of the Executive Order.
    c. Evaluate your log collection based on the visibility your logs provide for threat hunting playbooks. For more information check out this Threat Hunting for Visbility talk.
    d. Ensure logs are kept in a structured format such as the Elastic Common Schema.
3. Understand the security alerts you get from SIEM and Logging
    a. Adopt a defined methodology. If you do not know where to start, DHS uses their own standard, DHS 4300A Attachment F, that can be easily modified to give your program improved structure. While there are a lot of DHS specifics included, Section 5.0 – Incident Handling Stages for Component SOCs - has a lot of practical guidance for implementing an IR program.
4. Integrate your SOAR with SIEM or logging tools
    a. Build a bi-directional integration with you SIEM, you should be able to:
        i. Ingest alerts. Sometimes called events, incidents, cases, offenses or signals, the SOAR should be able to receive (via an API) alerts from the SIEM or logging platform as the event occurs.
        ii. Ability to execute searches. The SOAR should be able to execute efficiently crafted, ad-hoc searches in the logging platform to enable threat hunting and incident response activities.
        iii. Ability to update rules and searches. The SOAR should be able to add IOCs or other parameters to existing rules or searches to enable the continuous search for malicious activity, and in turn create more high-fidelity security alerts.
    b. For expanded Threat Hunting capabilities, create bi-directional integrations with EDR, NDR and Cloud Security tools.

5. Build automated incident response playbooks
    a. Based on your alert categories, create a series of SOAR playbooks for the primary categories of alerts. Some of these might overlap, such as Reconnaissance and Network Alerts, or Cloud and Data Loss, but the point is to ensure you have playbooks that cover each scenario. A great source for building playbooks is [FIRST's CSIRT Case Classification Example]. Build playbooks for:
        i. Reconnaissance
        ii. Alert Triage
            1. Endpoint Alerts
            2. Network Alerts
            3. Cloud Alerts
            4. Vulnerability Alerts
            5. Logging Alerts
        iii. Unauthorized Asset
            1. User
            2. Device (Rogue Device)
            3. Application / Software
        iv. Malware & Ransomware
        v. Compromised Information and Data Loss
        vi. Denial of Service
        vii. Compromised Asset
            1. User
            2. Devices
            3. Applications
        viii. Policy Violation
        ix. Phishing and Spam
        x. Threat Hunting (see more below)

6. Build automated threat hunting playbooks



a. Determine a methodology for building a threat hunting hypothesis and the tactics, techniques and procedures (TTPs) you are attempting to detect. A good starting place is to leverage the MITRE ATT&CK framework. For more information on automating MITRE ATT&CK and Atomic Operators, see this blog on Atomic Red Team Testing with Swimlane. Also look at MITRE's TTP Based Hunting for best practices.

b. Use SOAR to capture the development of your threat hunting hypothesis, patterns or analytics. This allows you to track and build a knowledge base of what has been tried, what works, and how to improve results. and build-up a threat hunting management system.

c. Test and tune the pattern to determine if it is effective in identifying hypothesized behavior, capturing your test results along the way. Document the results in a threat hunting management system in your SOAR.

d. For each successful threat hunting pattern (based on efficacy and tolerance for false positive rates), build a playbook that continuously searches for that pattern in your logging data.

e. Tune your threat detection system (SIEM, EDR, NDR, etc.) to also search for the TTPs in the threat hunting pattern.

f. Build single or multi-response playbooks for successful hits to threat hunting patterns. These most likely align to the playbooks created for incident response above.

Conclusion

The work required to meet Executive Order M-21-31 is not insignificant, but with proper planning and the right tools, meeting the mandate, and more importantly improving the security of government agencies and components, is possible.

About Swimlane

Swimlane is the leader in cloud-scale, low-code security automation. Supporting use cases beyond SOAR, Swimlane improves the ease with which security teams can overcome process and data fatigue, as well as chronic staffing shortages. Swimlane unlocks the potential of automation beyond the SOC by delivering a low-code platform that serves as the system of record for the entire security organization and enables anyone within the organization to contribute their knowledge and expertise to the protection of the organization. For more information, visit swimlane.com.