Automating Cyber Operations

Federal governments will use automation to build a more effective, efficient, and secure cyber environment. Security operations centers (SOCs) are designed to provide comprehensive cyber protection for on-premises, cloud, or hybrid environments across Information Technology (IT) and Operational Technology (OT) assets. SOCs are an integration point for all cybersecurity activities across a department or agency's enterprise architecture to synchronize the protection of information, systems, functions, and networks.

Spotlight

Industry

Federal Government

Use Case

Optimize cyber operations through automated defense of information technology, operational technology, and intellectual property by disrupting the adversary's ability to conduct their operations and achieve their desired outcomes.

Mission Benefits

- Reduced impact to the mission and lower overall risk through earlier detection of cyber activity
- Enhanced resilience and reliability performance outcomes
- Improved reliability of monitoring security-related information using standardized best practices

Operational Benefits

- Simplified regulatory compliance by automating generation and collection of log data
- Reduced Tier-1/Tier-2 cases and accelerated incident handling to minimize operational downtime
- Increased collaboration between disparate security teams
- Freed up SOC analysts from mundane, repetitive tasks required during routine incident response

Security Benefits

- Standardized how a particular type of incident is handled
- Reduced mean time to detect (MTTD)
- Reduced mean time to respond (MTTR)
- Automated mitigations

Mission Drivers

To gain, maintain, and expand competitive advantage over adversaries in a new digital operating environment, SOCs must be capable of seamlessly employing, integrating, and automating their capabilities across all environments and in any domain.

The key drivers for governments employing automation strategies throughout disparate operating environments are:

- Enhancing command-and-control (C2)
- Gaining digital transformation and operations alignment
- Closing the gap between decisions and data processing
- Addressing the global cybersecurity workforce shortage

Business Problem

As legacy equipment reaches end-of-support, emerging technologies get consumed, replacing analog technology with digital counterparts. In addition, federal agencies will continue to transition and expand their digital footprints, rendering the cyber hygiene of critical IT, OT, or other specialized systems a high priority. The Federal Cloud Smart Strategy has accelerated the government's digital IT transformation initiatives, leaving yet another potential gap amid mission-enabled IT services, modern OT environments, and cybersecurity. Because data and computing reside in so many places, manually monitoring all possible attack vectors is challenging and getting more so every day. Many agencies find it difficult to keep their security posture up to date, and they struggle with their evolving technology environments as they onboard increasing numbers of systems, applications, and devices.

Agencies are often disorganized or lack processes to support synchronized security operations, resulting in:

- Process inefficiencies
- Year-over-year budget increases
- Demand for cybersecurity professionals outpacing supply

Traditional Approach

The security model used by many government programs monitors separate physical, OT, and IT environments—an inefficient practice that can negatively impact incident response times for security events.

The principle drawbacks of this security model are:

- Operational stovepipes
- Duplication of efforts and redundancies
- Reduced situational awareness

A converged security solution tailored to the organization's enterprise cyberspace environment would reduce blind spots, resulting in more comprehensive C2 across the mission's enterprise environment. The pursuit of evolving cyber defenses that can prevent hybrid attack methods involving insider, supply chain, and other technical attack vectors across the mission are key to defending against future sophisticated attacks involving malicious nation-state actors.

Palo Alto Networks Approach

Federal agencies should adopt a unified cyber strategy across architecture, acquisition, and regulatory compliance to reduce risks across the Federal Enterprise Architecture (FEA), cloud ecosystem, and the information and communication infrastructure. By increasing the speed, consistency, quality, and reliability of tasks, automation helps organizations deal with evolving attackers as well as their own evolving technical environments. Agencies can apply automation across many areas of their organizations as well as use it for a variety of deployments and operational use cases.

Using automation to accelerate detection and incident response with respect to malicious cyber activity will help agencies improve operational resilience and make the most of scarce cybersecurity resources while keeping up with the increasing volume, variety, and velocity of cyberattacks. In addition, to achieve mission objectives more quickly, agencies should embrace cloud-delivered security services to help transition and modernize their legacy systems, reduce

costs, and increase scalability. Figure 1 presents an integrated architecture built for enhanced situational awareness and better defense against hybrid attack methods.

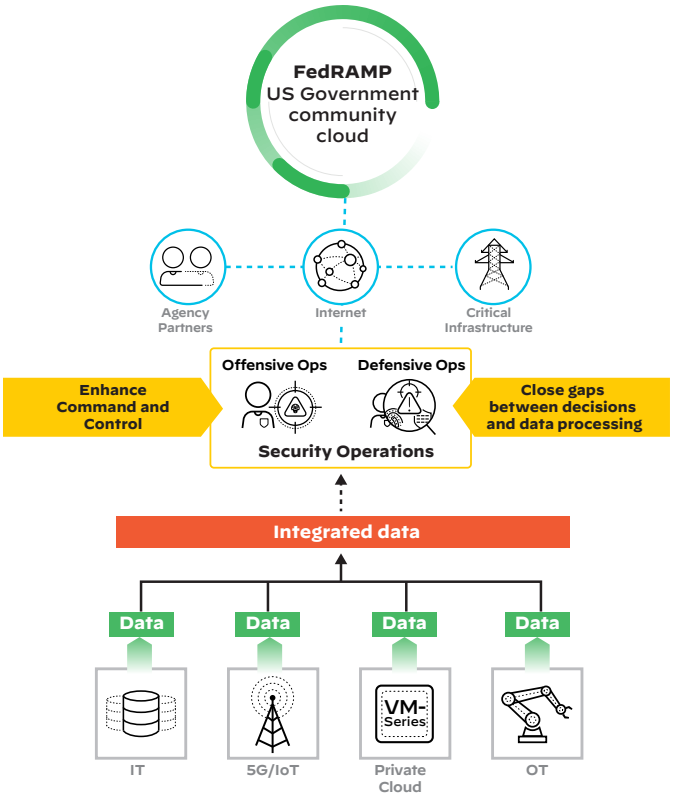

Figure 1: Converged security architecture

Security orchestration is a method of connecting disparate security tools, teams, and infrastructures for seamless and process-based security operations and incident response. It acts as a force multiplier for automation, since well-connected modern systems are more receptive to automation and scale.

Cortex™ XSOAR by Palo Alto Networks can help transition and transform your SOC with a scalable, intelligent platform for extended security orchestration, automation, and response. By offering a single platform for SOC analysts to manage cases and collaborate on investigations, Cortex XSOAR optimizes the efficiency of security operations. It makes use of machine learning to support functions such as incident triage and to list SOC analysts' next steps according to your agency's defined standard operating procedure (SOP). In addition, Cortex XSOAR offers a War Room where analysts can collaborate on incident investigations, with automatic documentation of actions for post-incident reporting. Case management and playbook automation features are available out of the box for more than 370 product integrations.

Palo Alto Networks integrated solutions benefits from a comprehensive, global threat data sharing community to minimize the spread of attacks and raise the costs for attackers. No single organization or industry will ever see all global threats, but as part of a network, they all benefit from collective intelligence. The detection and sharing of a new threat by one organization triggers the automatic creation and dissemination of prevention mechanisms across the entire community. As the community grows, the wider protections propagate, limiting the spread of attacks and, consequently, their effectiveness.

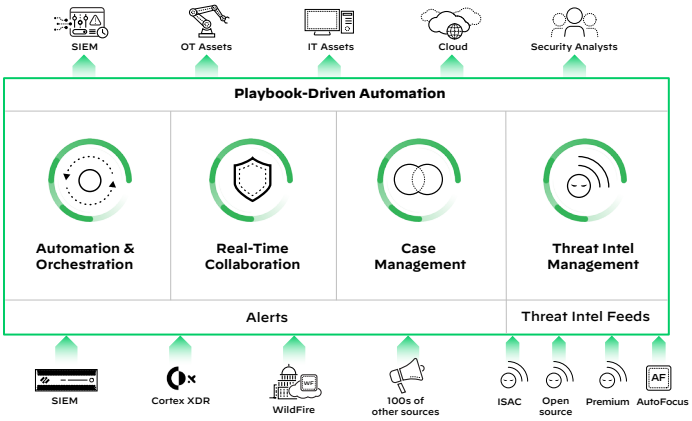

Figure 2: SOC orchestration ecosystems

As a core element of this cloud-delivered protection, our WildFire® malware prevention service leverages a large distributed sensor system that identifies and prevents unknown threats, with tens of thousands of subscribers contributing to the collective community. When sensors, such as a Next-Generation Firewall or Cortex XDR™ endpoint agent, see a suspected new malware or exploit, they send a sample to WildFire for analysis. Should WildFire deem the sample to be malicious, it automatically creates and shares a new prevention control with its network of sensors and enforcement points—all without human intervention.

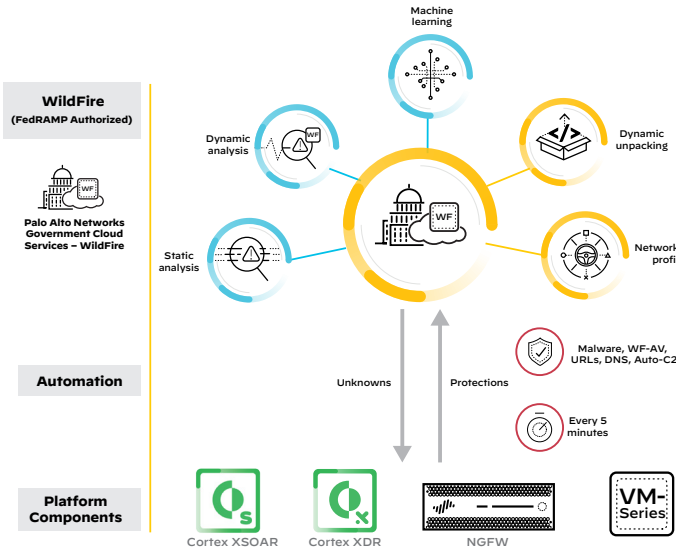

Figure 3: Cyber defense automation with WildFire

WildFire achieved FedRAMP Moderate authorization in 2019, and many agencies are already using it to automatically detect and stop unknown attacks as well as improve operational efficiency in their SOCs. Figure 3 shows a high-level view of automated processes and protections of WildFire.

The Cortex SecOps suite simplifies security operations and improves security outcomes through its open and integrated AI-based continuous security platform. Deployed on a global, scalable government community cloud platform, the Cortex suite automatically speeds up the analysis of the massive amount of security data generated by the components of the Security Operating Platform. Cortex Data Lake, a scalable and secure private data store, normalizes the data, allowing applications such as Cortex XDR to stitch together relevant information received from across the organization to automatically find threats and orchestrate responses. Cortex XDR and Cortex Data Lake are in the process of achieving FedRAMP Moderate authorization.

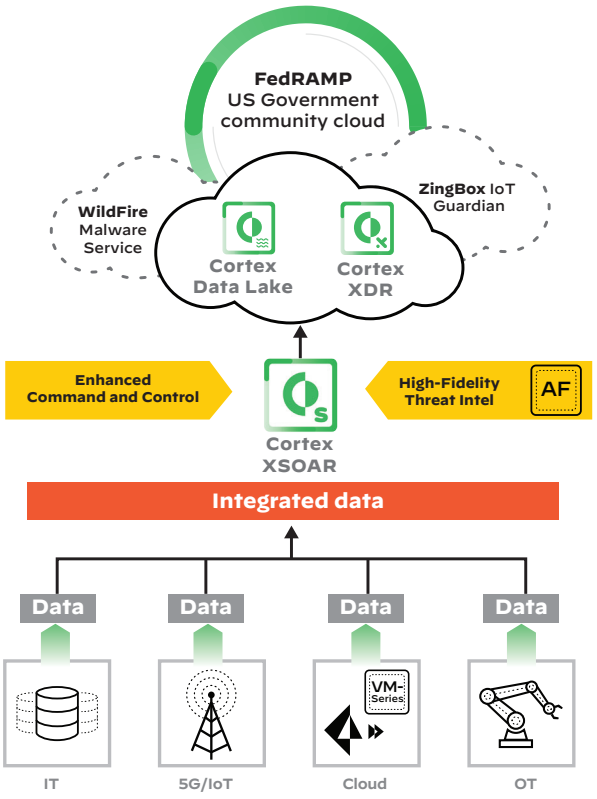

Figure 4: Components of the Cortex suite

For the most up-to-date information pertaining to our product status in the FedRAMP marketplace, please see our Product Certifications webpage.

Customer Implementation

One Palo Alto Networks customer, a large defense agency, serves hundreds of thousands of employees, a large multi-tenant user base, and numerous facilities globally, and operates on a multibillion-dollar cybersecurity budget. The agency owns and operates a private network that connects several branches of government to many data centers that connect to a joint information operating environment.

This customer's challenges included:

- Optimizing cyber operations with automated defense of IT, OT, and sensitive data
- Rotating personnel, which presented challenges around training and "brain drain"
- Inconsistent SOC processes that led to errors, confusion, and delays
- Lack of machine learning to detect advanced threats and shorten time to remediation

Implementation Overview

One of this agency's responsibilities is to track the unauthorized downloading and sharing of Controlled Unclassified Information (CUI). When it finds incidents of unauthorized handling of data, such as peer-to-peer sharing of personally identifiable information (PII), the agency sends a notice to the registered owner of the observed IP address. Traditionally, determining the user associated with the offending IP address was a time-consuming manual process. Administrators had to search through and correlate logs from various systems (e.g., firewalls; DHCP servers; and authentication, authorization, and accounting [AAA] servers). Cortex XSOAR can orchestrate the automation of this workflow, freeing up system administrators to focus on less tedious tasks that fully utilize their skills.

The agency was able to automate its SOP for identifying and notifying users responsible for the sharing of unauthorized CUI. The following steps were incorporated into a Cortex XSOAR playbook, which the agency customized for a search and correlation workflow:

1. Agency user sends an email with a digital watermark containing the CUI data classification to an address monitored by Cortex XSOAR (this event triggers the workflow).
2. Cortex XSOAR extracts the offending public IP address and date from the email, and then creates a ticket with the information.
3. Cortex XSOAR queries Panorama™ network security management and obtains the private IP address that was mapped to the offending public IP on the specified date.
4. Cortex XSOAR queries the agency's security information and event management (SIEM) system to search DHCP and AAA logs to find the username associated with the offending address on the specified date.
5. Cortex XSOAR checks the LDAP server to gather the contact details associated with the username.
6. If successful, Cortex XSOAR sends a response to the security administrator with the user's contact information, logs the details, and closes the ticket. If Cortex XSOAR is unable to obtain the user's contact information, it logs what it can to the ticket and sends it on for an IT administrator to investigate manually.

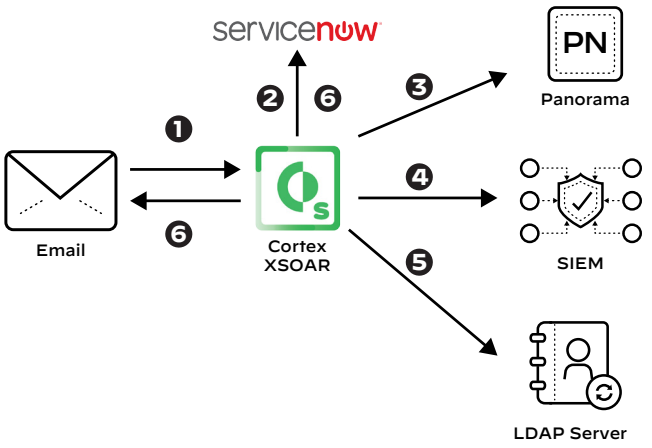

Figure 5: Automated search and correlation workflow

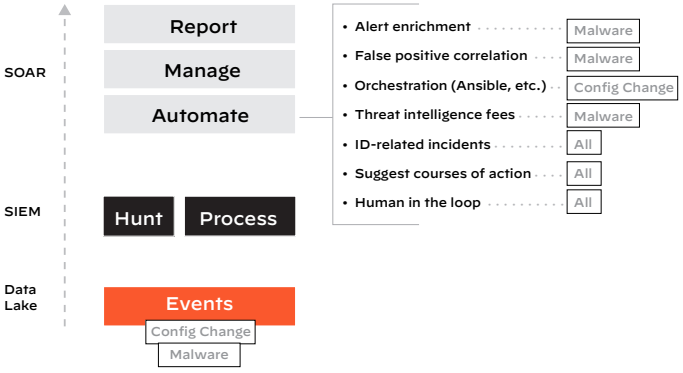

Figure 6: Federal agency SOAR architecture

As a result of the implementation, the agency:

- Ensured cyber operations are compatible department-wide leveraging a unified infrastructure
- Augmented security team processes, reducing time spent on redundant Tier-1/Tier-2 tasks
- Increased the amount of time spent on tasks requiring human cognition

Benefits of Automating Cyber Operations

Automating cyber operations with Palo Alto Networks products, capabilities, and strategies enables simplified operations, empowers the workforce, and deters threats. The defense agency captured in this use case saw multiple mission, operational, and security benefits.

Mission Benefits

- Reduced impact to the mission and lower overall risk through earlier detection of cyber activity
- Enhanced resilience and reliability performance outcomes
- Improved reliability of monitoring security-related information using standardized best practices

Operational Benefits

- Simplified regulatory compliance by automating generation and collection of log data
- Reduced Tier-1/Tier-2 cases and accelerated incident handling to minimize operational downtime
- Increased collaboration between disparate security teams
- Freed up SOC analysts from mundane, repetitive tasks required during routine incident response

Security Benefits

- Standardized how a particular type of incident is handled
- Reduced mean time to detect (MTTD)
- Reduced mean time to respond (MTTR)
- Automated mitigations

Conclusion

Federal agencies can find significant value through automating frequently executed, simple-to-perform, and error-prone tasks. Automation is a broad topic, but by organizing systems into building blocks, you can build modular automation tasks that are scalable and easy to reuse. Even organizations without automation teams can still benefit from using automated tools, features, and processes long before they get to a fully converged SOC environment.

Automation specific to the security layer focuses on four high-level use cases: deployment, configuration, response, and assessment. The elements of the Palo Alto Networks product ecosystem use built-in automation to identify malware and vulnerabilities as well as distribute protections to the platform elements. The platform provides a variety of capabilities and features that allow organizations to build their own automation workflows that may be unique to their specific environments.

The use case discussed in this document shows how automation that leverages these capabilities and features can be used within any organization and across industries. The example is not all-encompassing, but it is a starting point for exploring how automation can be used.

Additional Resources

To learn more about how Palo Alto Networks can help organizations improve cybersecurity risk management, visit our website. You can also visit our Federal Government page to learn how to modernize your agency operations while measuring and managing risks.

Services to Help You

Palo Alto Networks offers a number of services to help you maximize the value of your investment and protect your business. For more information on support services, professional services, and education and training opportunities, visit our Services Overview page.

- **Our global Customer Support** provides timely, expert assistance to keep you up and running safely. Our support has been rated outstanding by third-party assessments. All Customer Support plans include online case management, online support resources, and license keys and upgrades, and Premium and Premium Plus support options offer additional resources.
- **Our Professional Services and Certified Professional Services Partners** deliver the tools, best practices and assistance you need to define an effective strategy, simplify operations and prevent successful cyberattacks.
- **Education and Training Services** help you expand knowledge and skills with world-class training, certification and accreditation, and digital learning options.
- **Cyber Range** is interactive cyber defense training that helps keep your IT network, infrastructure, OT, DevOps and SecOps teams razor-sharp.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com