Planning the Government Security Operations Center

4 Steps + 3 Keys to Transform Security Operations to Combat Advanced Attacks and Improve SOC Efficiencies

Table of Contents

Introduction

The accelerating pace of evolving threats—including ransomware, supply chain attacks, and newly announced software vulnerabilities—has placed a huge burden on federal government SOCs to secure, operate, and defend their agencies' infrastructure. These challenges also come as many agencies are embarking on an ambitious digital transformation journey, simultaneously migrating to the cloud, expanding telework, and automating many routine security operations tasks. The White House has also renewed the nation's focus on cybersecurity, releasing an ambitious Executive Order on improving the nation's cybersecurity. The Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA) have likewise released a Binding Operational Directive to identify and remediate against Known Exploited Vulnerabilities on federal networks.

At the same time, federal government agencies are also doing more with less. In recent testimony to Congress, Partnership for Public Service President and CEO Max Stier highlighted challenges facing the Federal cybersecurity workforce:

> *"Unpacking the data on the federal cybersecurity workforce reveals different stories across the government. There are areas of growth, including in government-wide totals—the number of full-time federal cyber employees increased by 7.85% between September 2016 and September 2020. Over the same period, the federal workforce overall increased by 3.66%.*[1]
>
> *However, there are concerning trends in other areas of the cyber workforce.* ***For example, some agencies saw declines in full-time employees—the Department of Agriculture's cyber workforce decreased from 3,300 employees in September 2016 to 2,700 in September 2020, while at the Department of Labor it decreased from 750 to 660 employees in the same timeframe."***[2]

As new threats emerge and agencies grapple with staffing shortages, SOCs are challenged like never before. By auditing your environment to identify and reduce tool sprawl, automating workflows to

1. Max Stier, written statement from "The Cyber Talent Pipeline: Educating a Workforce to Match Today's Threats," July 29, 2021, https://homeland.house.gov/imo/media/doc/2021-07-29-CIPI-HRG-Testimony-Stier.pdf.
2. Statistics on federal employees are drawn from Office of Personnel Management FedScope data on the federal workforce unless indicated otherwise.

offload routine/repeatable tasks, augmenting teams with machine learning-driven intelligence, and optimizing security teams, SOCs can transform operations and take a future-forward approach to combat advanced attacks and improve efficiency.

Novel Threats Posed by New Vulnerabilities and Bad Actors Continue to Proliferate

Protecting government networks is of the utmost importance to reduce the risk of data breaches that could compromise taxpayer and government employee PII records or sensitive national security information.

However, recent high-profile CVEs, from SolarWinds to Microsoft Exchange and Apache Log4j, have demonstrated that attackers are always searching for ways to target federal networks, and the frequency at which new CVEs are released is ever-increasing. SOCs are overwhelmed with events, alerts, and incidents to investigate, not to mention remaining on call for emergencies and incident response. Ensuring system availability and reliability is also crucial to the function of government, to provide services, protect the homeland, and further US interests abroad. Federal SOCs must continue to meet this challenge head-on, leveraging new capabilities to remain ahead of bad actors looking to damage networks, steal information, and dent the credibility of the United States.

Renewed Focus on Cyber Hygiene and Implementation of Cybersecurity Technologies

These many challenges require new techniques and technologies for government SOCs to stay ahead of the adversary. The May 2021 Executive Order on Improving the Nation's Cybersecurity highlights many of these, including implementing Zero Trust architectures (ZTAs), requiring endpoint detection and response (EDR) across the entire federal government, requiring secure cloud capabilities (including ZTA in the cloud), and calling for enhanced visibility and monitoring of all public-facing, internet-connected government assets. Continuous verification that services and tools are deployed safely fulfills an important aspect of this executive order, and attack surface management enables that mission.

Recent Binding Operational Directive Requires Enhanced Visibility and Monitoring

Observers will also note the federal government has become increasingly proactive to prevent attacks before an attack can be executed. In November 2021, the Department of Homeland Security/ Cybersecurity and Infrastructure Security Agency (DHS/CISA) published Binding Operational Directive (BOD) 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities, establishing requirements for United States government agencies to remediate a broad range of known critical vulnerabilities.

As of late January 2022, the Known Exploited Vulnerabilities catalog accompanying BOD 22-01 contains 351 individual Common Vulnerabilities and Exposures (CVEs), at least 165 of which involve internet-facing products and services. These numbers continue to increase since BOD 22-01's initial publication, as CISA adds new CVEs to the KEV catalog.

COVID-19 Pandemic Accelerates Shift to Telework

The onset of the COVID-19 pandemic in 2020 dramatically accelerated many agencies' plans to accommodate additional telework opportunities for the federal workforce. Adding to an already complicated, geographically distributed footprint, expanding telework also expands agencies' network boundaries to include their employees' personal or government-furnished devices, connecting via potentially insecure networks. One of the results has been a dramatic increase in the number of remote access exposures (such as Remote Desktop Protocol or telnet) that could be exploited by a bad actor to gain a foothold on a government network. Palo Alto Networks 2021 Cortex Xpanse Attack Surface Threat Report found that Remote Desktop Protocol (RDP) accounted for one-third of all security issues exposed on the public internet. SOC teams will need to ensure that they maintain visibility and management of their network perimeter in order to successfully detect and defend against attacks utilizing this vector.

Agencies Must Transform to Keep Pace

In response to these many threats and challenges, government SOCs can leverage key technologies to inform their security operations strategy, improve government cybersecurity, supply chain, and critical infrastructure to establish centralized visibility and operational control over federal information technology, including:

- **Integrated EDR/XDR, logging, SOAR, and hunt** to prevent anomalous behavior at the endpoint, correlate data across the enterprise, automate response, and support government-wide hunt teams.
- **Internet operations management and national vulnerability and incident remediation** to identify and monitor the government's entire internet-facing attack surface and remediate vulnerable software running in the infrastructure.

SOCs Are Challenged Like Never Before

Modern security threats are evolving at a faster pace than security technologies. While well-funded threat actors are investing in new tools like machine learning, automation, and artificial intelligence, SOCs built around legacy security information and event management (SIEM) fail to provide a flexible and scalable solution that keeps pace with digital transformation, cloud initiatives, and advanced attack campaigns.

Challenges such as noisy false positives, event storage (volume and cost), poor investigation workflows combined with the adoption of hybrid and multicloud architectures and the proliferation of devices and endpoints can overwhelm security analysts struggling to identify, manage, and remediate critical threats.

Furthermore, the cost to maintain SIEMs extends beyond the initial investment, including infrastructure and personnel who have to continually tune and optimize SIEM functionality.

Challenges from legacy SOC environments can include:

- Lack of visibility and context.
- Increased complexity of investigations.
- Alert fatigue and "noise" from a high volume of low-fidelity alerts generated by security controls.
- Lack of interoperability of systems.
- Lack of automation and orchestration.
- Inability to collect, process, and contextualize threat intelligence data.

In this paper, we will review some best practices and technologies to support SOC transformations that align with industry methodologies, as well as insights and predictions from analyst firms such as Gartner, Forrester, and Enterprise Strategy Group (ESG).

4 Steps Toward Creating a Future-Forward SOC

Step 1: Auditing Your Environment Can Help Reduce the Security Risks Associated with Tool Sprawl

Leonardo da Vinci once said, "Simplicity is the ultimate sophistication." Due to acquisitions, mergers, and a lack of standardization for similar security products, many organizations are burdened with a disparate swath of tools across their security stack. To put it simply, having too many tools results in too many issues. And with resources both in cloud environments and on-premises, security IT teams are challenged with complete visibility of their attack surface.

For some teams, tool sprawl can begin by deploying a point solution to fix a specific issue. Unfortunately, this piecemeal approach, combined with managing numerous agents, can (ironically) leave networks even more vulnerable, exposing gaps due to issues from a lack of interoperability and improper configurations across the various solutions.

One of the first steps an organization can do to reduce the security impact of tool sprawl is to audit protected systems and entities. Identify precisely what is being protected and what is being prevented from happening. Is it intellectual property? Customers' personal information? By identifying as much as possible, whether software or physical assets, an organization can better prioritize protecting high-value and high-risk data.

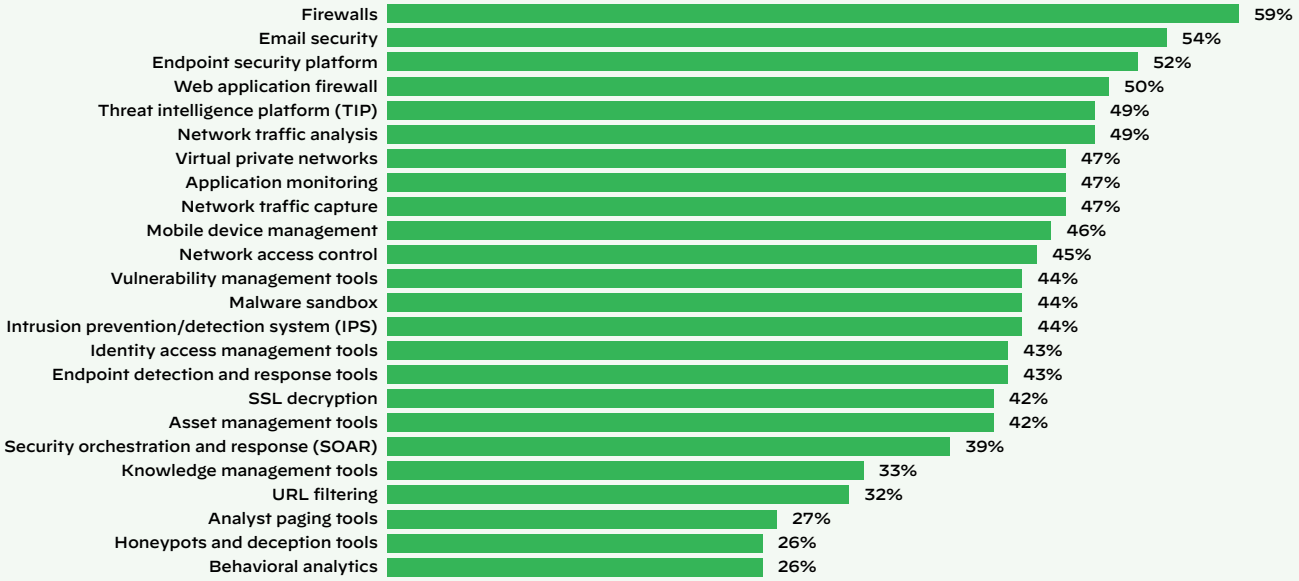
By 2024, 80% of all modern SOCs will leverage tools using machine learning, up from less than 10% today, but it won't significantly reduce industry-wide average attacker dwell time.

– Gartner[3]

3. Toby Bussa and Jeremy D'Hoinne, *Tips for Selecting the Right Tools for Your Security Operations Center*, Gartner, January 23, 2020, https://www.gartner.com/en/documents/3979882/tips-for-selecting-the-right-tools-for-your-security-ope.

Once an organization has a clear understanding of what is being protected, a logical next step is to identify solutions that can solve multiple needs if possible. As reported by ESG (Enterprise Strategy Group), in a 2019 survey of 406 IT and cybersecurity professionals (US and Canada), 42% of respondents used between 10 and 25 security tools, with another 26% using between 26 and 50 security tools.[4] As things stand today, it is unnecessary to have sensors and enforcement happening across various tools, so organizations should consolidate where appropriate.

Security teams have a fragmented view of their environment.
Which of the following tools are in use in your security operations team?



Base: 315 global decision-makers with involvement in security operations or incident response

Figure 1: Tools security operations pros use—a commissioned study conducted by Forrester Consulting on behalf of Palo Alto Networks, February 2020

Step 2: Automate Workflows

Security leaders must consider whether a tool requires a human to configure or run. Must an expert interpret or triage the result? Are people needed to test things? Security leaders can identify repeatable, low-level tasks that can work with human decision-making to help accelerate incident investigations. While advancements in machine learning and artificial intelligence hold great promise, retaining the human element for knowledge transfer in either direction is imperative to achieve optimal outcomes for a smooth SOC transformation.

With too many manual processes involved in security operations and incident response (IR), including numerous threat feeds to monitor, investing in automation capabilities such as those in a SOAR solution can help orchestrate actions across the product stack for faster and more scalable IR.

Manual Alert Investigations Plague Teams

One area that is a continued sticking point for SOC teams is managing the number of alerts. Deploying solutions that can automate a range of tasks, decisions, and workflow associated with alert triage (alert prioritization/ranking, causal event correlation, and enrichment) can help streamline investigations.

1–5 Year Prediction on Automation Takeaways

New SOC operations can start using automation from day one, while more established organizations will have to re-tool and figure out where the move to automation can begin. This is a good three-year goal for an established organization: to move 50% of SOC work into the hands of automation. By year five, most SOC teams can be closer to 75% of activities automated yet continue to rely on human engineers for other activities like threat hunting.

4. Jon Oltsik, *ESG Research Report: The rise of cloud-based security analytics and operations technologies*, ESG, December 23, 2019, https://www.esg-global.com/hubfs/ESG-Research-Report-Cloud-scale-Security-Analytics-Dec-2019.pdf.

Even after deploying a SIEM, or other solutions for better security insights and visibility, SOC teams are often flooded with low-fidelity alerts generated by their security controls. A 2019 survey of CISOs reported that "over 41% see more than 10,000 and that some claim to see more than 500,000 alerts daily."[5] The same report noted that respondents revealed only 24% of investigated alerts were considered legitimate, down from 34% in 2018.[6] The report also observed a substantial drop in the number of legitimate alerts that were in fact remediated—from 51% in 2018 to 43% in 2019.[7]

As one would expect, these types of numbers are not sustainable. The overwhelming number of false positives creating "noise" is often a result of a combination of poorly tuned algorithms, legacy detection tools, and/or configuration errors. These issues, combined with a lack of correlation from disparate tools and operations often done in silos, don't always enable the consolidation of event data. Even using SIEM or log management tools require tuning or customization to accurately correlate alerts. What further muddies the waters is that even though tools may trigger alerts, they are not necessarily malicious. As such, many low-fidelity alerts go ignored.

Step 3: Augment People with Machine Learning with Advanced Analytics-Driven Intelligence

A key component in a modern SOC transformation is to ensure that security teams are leveraging machine learning to its full potential to augment and complement humans in security. Advanced analytics and AI can significantly reduce the amount of time that teams spend processing massive amounts of data in the enterprise to come up with critical security insights. By automatically detecting anomalous patterns across multiple data sources and automatically providing alerts with context, machine learning today can deliver on its promise of speeding investigations and removing blind spots in the enterprise.

This works by training machine learning models, using them to detect patterns among and across the data, and then testing and refining the processes. ML techniques can gather, integrate, and analyze data and interrogate the data to reduce the amount of time and knowledge needed for a human to perform these tasks. This also minimizes the challenge for a SOC team trying to find threat context and evidence across multiple layers of security that are embedded in data.

Supervised machine learning techniques can be used to fingerprint devices, such as desktop computers, mail servers, or file servers, and then learn the behavior of different types of devices and detect anomalous behavior. The promise of machine learning is having the ability to determine causal inferences around what is happening in an environment and letting the software direct next steps instead of relying on human interaction. For instance, flagging "bad" actions based purely on behavior and interactions within the joined datasets, so it can then propagate a decision to the rest of the network with explicit instructions such as instructing an agent to contain it or a firewall not to communicate with it.

At a high level, machine learning techniques can:

- **Integrate:** Enable the data to tell a story about what is happening.
- **Analyze:** Extract insights about the problem space and make predictions.
- **Automate:** Accelerate human decision-making, automate system-level action, workflows, and decision-making.

Step 4: Optimize Security Teams

Beyond investing in security solutions and tools, the most important factor in any successful SOC will remain the human element. While machine learning and automation will undoubtedly improve outcomes like response times, accuracy, and remediation overall—especially for low-level, repetitive tasks—attracting, training, and retaining security personnel, including engineers, analysts, and architects, needs to be baked into any cohesive SOC transformation strategy. By leveraging automation technologies, organizations can be more efficient at protecting the business at hand.

According to the Bureau of Labor Statistics, the number of individuals employed within the cybersecurity sector is slated to grow by 33% between 2019 and 2030.[8] Additionally, the National Center

5. *Anticipating the Unknowns: Chief Information Security Officer (CISO) Benchmark Study*, Cisco, March 2019, https://ebooks.cisco.com/story/anticipating-unknowns/page/6/6.
6. Ibid.
7. Ibid.
8. *Occupational Outlook Handbook*, U.S. Bureau of Labor Statistics, last modified January 12, 2022, https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm.

for Education Statistics (NCES) shows the number of new cybersecurity programs has increased by 33%, while cybersecurity job postings have grown by 94% in the past six years.[9]

In concert with filling critical roles is adopting cybersecurity awareness training to ensure employees, contractors, and in some cases, partners are well-versed in helping to prevent breaches. Stolen credentials, phishing attacks, and social engineering require people to execute campaigns, so building a cybersavvy team holds long-term value. As the noted cryptographer and computer security professional Bruce Schneier says, "People often represent the weakest link in the security chain and are chronically responsible for the failure of security systems."

SOCs Can Come in Many Flavors

At Palo Alto Networks, our SOC story is highly optimized in that we actively chose to break away from the traditional four-tier SOC approach, ranging from Tier 1 analysts who monitor, prioritize, and investigate SIEM alerts to Tier 4 SOC managers responsible for recruitment, security strategy, and reporting to management. Taking more of a hybrid approach, the Palo Alto Networks SOC team follows this general philosophy:

- Staff the SOC with 80% of people who have previous SOC experience.
- Cross-train the SOC team in all domains, including alert triage, incident response, threat hunting, automation, and others.
- Provide a well-funded annual training budget for all analysts.

Our rationale is that we can:

- Maintain a nimble team, able to pivot between responsibilities (and tiers).
- Support business continuity.
- Provide a more engaging atmosphere and reduce staff burnout.
- Promote an environment of continuous learning.
- Provide greater coverage with less staff by relying on the right technology to get the job done.
- Maintain a work/life balance while giving SOC engineers a feeling of positive control of their destinies.

ASM, SOAR, and XDR: Together, the Bedrock for SOC Transformation

Laying a foundation to build a resilient and effective SOC starts with taking the above four steps and considering the following three technology "keys" to help inform your security operations strategy.

Key 1: Power Up Your Risk Management and Service Deployment Functions by Understanding Your Attack Surface

One foundational component of an SOC transformation is to have a strong continuous risk management function. Identifying the "things" you are trying to protect and identifying what is exposed that allows it to be attacked is a logical segue into a risk management process that establishes the context for a risk management plan or strategy, whether basic or more robust. By starting with identification, the ability to prioritize what's at risk makes it easier to analyze what it would take to actually mitigate each risk. By understanding your attack surface, you accelerate and validate that new services are deployed safely to internal and external customers. The accelerated deployment of safe services turns the SOC into a verification function directly supporting agile and secure development methodologies.

A critical step to informing any risk management function is to have a clear understanding of one's attack surface—you can't protect what you can't see.

Yet, whether one chooses to deploy ASM solutions or perform proactive assessments like penetration testing or vulnerability scanning, what is clear is the need to identify both product and operational requirements to determine the best fit. Both product and operational requirements can include functionality, feature/s, capability, and evaluation criteria to help summarize the features and capabilities you might expect in an ASM solution or tool.

9. *Recruiting Watchers for the Virtual Walls: The State of Cybersecurity Hiring*, Burning Glass Technologies, June 2019, https://www.burning-glass.com/wp-content/uploads/recruiting_watchers_cybersecurity_hiring.pdf.

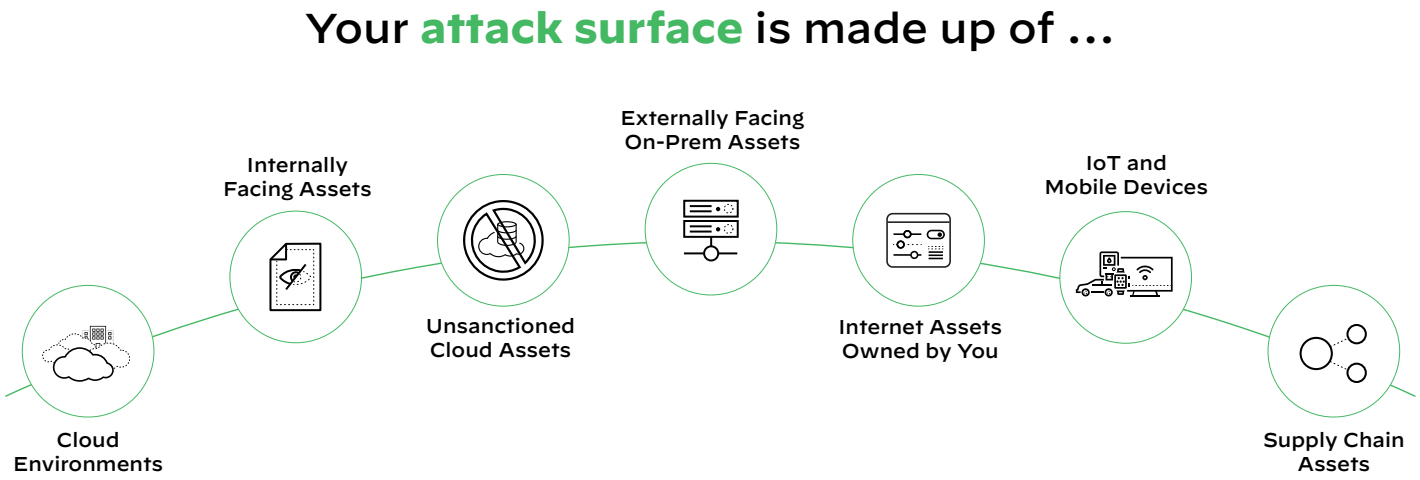


Figure 2: Components of the attack surface

In their recent report, "2021 Cortex Xpanse Attack Surface Threat Report: Lessons in Attack Surface Management from Leading Global Enterprises," Palo Alto Networks outlined some key findings from their research of the public-facing internet attack surfaces of some of the world's largest businesses. From January to March, their team monitored scans of 50 million IP addresses associated with 50 global enterprises to understand how quickly adversaries can identify vulnerable systems for fast exploitation.

One interesting discovery was that nearly one in three exposed assets they uncovered was due to unnecessary use of the Remote Desktop Protocol (RDP), which has surged in use since early 2020 as enterprises expedited moves to the cloud to support remote workers affected by new WFH protocols due to the COVID-19 pandemic. Other findings in this report include:

- **Adversaries scan more frequently than companies**. In a game of never-ending "cat and mouse," threat actors were found to conduct a new scan once every hour, whereas global enterprises can take weeks.
- **Adversaries scan within 15 minutes of new vulnerabilities**. Attackers began scanning within 15 minutes following announcements of new Common Vulnerabilities and Exposures (CVEs) released between January and March and launched scans within five minutes of the Microsoft Exchange Server zero-day security update.
- **Exposed systems every 12 hours**. Cortex Xpanse discovered that, on average, global enterprises present a new serious exposure every 12 hours or twice daily. Issues included insecure remote access (RDP, Telnet, SNMP, VNC, etc.), database servers, and exposures to zero-day vulnerabilities in products such as Microsoft Exchange Server and F5 load balancers.
- **Cloud comprised almost 80% of the global enterprise security concerns**. Cloud footprints were responsible for 79% of the most critical security issues found in global enterprises, reiterating the inherent risk of cloud-hosted/based services, compared to 21% for on-premises.

Takeaway: Advancements in scanning technologies allow attackers to locate attack vectors quickly and easily, revealing abandoned, rogue, or misconfigured assets that can become backdoors for compromise. Deploying an attack surface management solution is the best way to provide a continuous assessment of an organization's external attack surface in a cost-effective, repeatable and scalable manner.

Key 2: SOAR—Orchestrating Across Your Product Stack for Efficient Incident Response

Gartner defines security orchestration, automation, and response (SOAR) as "solutions that combine incident response, orchestration and automation, and threat intelligence (TI) management capabilities in a single platform. SOAR tools allow an organization to define incident analysis and response

procedures in a digital workflow format."[10] Workflows can be orchestrated via integrations with other technologies and automated to achieve desired outcomes, such as:

- Incident alert triage.
- Threat qualification.
- Incident response.
- Threat intel curation and management.
- Compliance monitoring and management.

When it comes to SOAR, solutions running a playbook outlining automated response workflows may come to mind, yet an effective SOAR strategy goes beyond just leveraging automation to streamline and eliminate manual tasks. A comprehensive SOAR solution that addresses all aspects of incident management needs to provide comprehensive out-of-the-box integrations of commonly used tools in the SOC, best practice playbooks to aid in automating workflows, as well as integrated case management and real-time collaboration to enable cross-team incident investigation.

Last but not least, the ability to serve as a central repository for threat intelligence (both internal and external) enables automated correlation between indicators, incidents, and intel, so security analysts and incident responders get enriched strategic intelligence for added insight into threat actors and attack techniques.

SOAR solutions continue to build toward becoming the control plane for the modern SOC environment, with the potential of becoming the control plane for various security operations functions. To achieve this end, SOAR solutions are starting to integrate threat intelligence and expand automation to use cases beyond the SOC. Leading security vendors are also embedding SOAR and incident management capabilities in their products, which are preprogrammed and optimized for the specific technology.

How a Security Company Automates Security

Cortex XSOAR is leveraged within the Palo Alto Network SOC to minimize the repetitive and time-consuming tasks discussed in the above sections. Below is a snapshot of top automation "timesavers" for the month of February 2021. Figure 3 varies significantly from month to month depending on active campaigns; the average is just over nine FTEs.

Automation Type	Times Ran	Hours Saved
Artifact Enrichment	1,195	697.08
Dedupe	12,744	1,062
Email User	822	342.5
Password Reset	4	1.67
GCP Remediation	34	17
Other Jobs*	*	74.73

Repetitive, tedious SOC work that nobody wants to do

*PhishMe metrics, RSS feed job, content update job, hunting assignments and metrics, daily monitoring ticket creation, and JIRA ticket pull

Figure 3: Top automation timesavers

Takeaway: At the heart of any SOAR solution is the ability to set priorities and build streamlined workflows for security events that require minimal human involvement. Improved efficiencies are the result of a SOAR platform that can automate processes, as well as provide a single platform for minimizing complex incident investigations.

10. Claudio Neiva, Craig Lawson, Toby Bussa, and Gorka Sadowski, *Market Guide for Security Orchestration, Automation and Response Solutions*, 21 September 2020, https://www.gartner.com/en/documents/3990720-market-guide-for-security-orchestration-automation-and-r.

Key 3: XDR—the Next Logical Evolution of EDR

The product vision for "XDR," short for "extended detection and response," was created by Nir Zuk, CTO and co-founder of Palo Alto Networks, in 2018. The reason for creating XDR was to stop attacks more efficiently at the endpoint, detect attacker techniques and tactics that cannot be prevented, and help SOC teams better respond to threats that require investigation. The vision is to automate many of the SOC analyst tasks, like writing detection logic, gathering evidence and building an incident from alerts, enriching the incident with identity and threat information, and pulling disparate telemetry together from multiple (and in some cases, complementary) sources, including EDR, network traffic analysis (NTA), user and entity behavior analytics (UEBA), and indicators of compromise (IoCs).

XDR lets security teams stop attacks more efficiently and effectively, eliminating blind spots, reducing investigation times, and ultimately improving security outcomes. And with XDR's ability to stop attack sequences at critical stages such as execution—before persistence techniques result in broader lateral damage—security teams finally have a solution to "head attacks off at the pass."

XDR's value is gaining momentum due to the need in the market for tighter third-party integrations, better analytics, and faster response capabilities—especially when one considers that organizations may use up to 45 security tools on average while responding to an incident requires coordination across approximately 19 tools.[11]

XDR Fills the Detection and Response Void

XDR combines the SIEM-like features of alert integration, normalization, and correlation with SOAR-like automated investigation and remediation.

Forrester defines XDR as:

> *The evolution of EDR, which optimizes threat detection, investigation, response, and hunting in real time. XDR unifies security-relevant endpoint detections with telemetry from security and business tools such as network analysis and visibility (NAV), email security, identity and access management, cloud security, and more. It is a cloud-native platform built on big data infrastructure to provide security teams with flexibility, scalability, and opportunities for automation.*[12]

As an evolution of existing threat detection and response solutions, XDR includes features such as:

- Integrated threat intelligence
- Network analysis
- Machine learning-based detection
- Investigation response orchestration
- Dynamic deployment
- Integrated sandbox (WildFire®) capabilities

Factors driving the adoption of XDR include simplified visualization of complex attacks across the kill chain, presenting information within the MITRE ATT&CK® framework, more robust automation, advanced analytics, and machine learning.

Up until XDR, correlating telemetry from endpoints with other event data was an exercise in sifting through large volumes of data and false positives cluttering analysts' dashboards. Stitching disparate events together is resource-intensive and dependent on seasoned analysts to determine if alert escalations are warranted. As a result, SOC teams could find themselves wasting time to verify the accuracy of low-fidelity alerts while compromising the time needed to investigate legitimate alerts.

Impeded by this nonstop version of security "whack-a-mole" and an increase in attack sophistication and frequency, forward-thinking security organizations are beginning to position themselves to take advantage of all the efficiencies gained by an XDR approach to security architecture.

According to Forrester analyst Allie Mellen, who covers SecOps, "XDR and SIEM are not converging but colliding."[13] In a recent blog post, Mellen explains further:

> *"XDR will compete head to head with security analytics platforms (and SIEMs) for threat detection, investigation, response, and hunting. Security analytics platforms have over a decade of experience in data aggregation they apply to these challenges but have yet to provide incident response capabilities*

11. *2020 Cyber Resilient Organization Report*, IBM Security, June 2020, https://www.ibm.com/account/reg/us-en/signup?formid=urx-45839.
12. Allie Mellen, "XDR Defined: Giving Meaning To Extended Detection and Response," April 28, 2021, https://go.forrester.com/blogs/xdr-defined-giving-meaning-to-extended-detection-and-response/.
13. Ibid.

that are sufficient at enterprise scale, forcing enterprises to prioritize alternate solutions. XDR is rising to fill that void through a distinctly different approach anchored in endpoint and optimization.

"The core difference between XDR and the SIEM is that XDR detections remain anchored in endpoint detections, as opposed to taking the nebulous approach of applying security analytics to a large set of data. As XDR evolves, expect the vendor definition of endpoint to evolve as well based on where the attacker target is, regardless of if it takes the form of a laptop, workstation, mobile device, or the cloud."[14]

Takeaway: XDR can address SIEM use cases by providing threat detection, investigation, response, and hunting rooted in endpoint threat detection and response with the ability to scale to cloud environments.

Better Together, End to End: Cortex XDR, Cortex XSOAR, and Cortex Xpanse

Let's face it. We understand most of our customers and potential customers don't want to be systems integrators. Nor do they want to "run ragged" performing manual, repetitive tasks. An array of siloed tools requires massive time and costs to maintain. Numerous and disparate solutions can limit security outcomes by introducing complexity and fractured visibility for the analytics required by modern SOCs.

And while we can't add hours to the day, we can help our customers optimize, reduce TCO, and integrate with more third-party tools than any other security provider for next-level operations. Beyond these results is the ability to equip the security analyst with the tools they need to keep their data safe so they can focus more on what matters and less on mundane tasks.

Securing the endpoint is not enough. Organizations must unify it with cloud and network data through a single source of truth driven by comprehensive data and deep analytics.

You can begin or accelerate your SOC journey by deploying the Cortex suite of products: Cortex XDR, Cortex XSOAR and Cortex Xpanse, which seamlessly work together as a force multiplier across your security operations.

Cortex XDR® can stop attacks at the endpoint and host with world-class EDR for Windows® and Linux hosts with:

- Machine learning with advanced analytics-based local and behavioral analysis that is updated regularly.
- A suite of endpoint protection features such as device control, host firewall and disk encryption.
- A range of protection modules to protect against pre-execution and post-execution exploits.

Once you prevent everything you can at the endpoint, Cortex provides detection and response that focuses on incidents by automating evidence gathering, groups of alerts associated, putting those alerts into a timeline, and revealing the root cause to speed triage and investigations for analysts of all skill levels.

Palo Alto Networks Security Operations Center Mission Statement: Defend our information and technology resources, intellectual property, and ability to operate by disrupting our adversary's ability to conduct their operations and achieve their desired outcomes.

Cortex® XSOAR provides end-to-end incident and security operational process lifecycle management, helping companies accelerate security operations, reduce the time it takes to investigate and respond to security alerts and incidents and to handle more incidents. Security teams of all sizes can orchestrate, automate, speed incident response and any security workflow or security process across their environment by leveraging the extensive vendor integration and 725+ pre-built integration content packs to maximize enterprise integration coverage.

Cortex Xpanse™ provides a complete and accurate inventory of an organization's global, internet-facing cloud assets and misconfigurations to continuously discover, evaluate, and mitigate an external attack surface and evaluate supplier risk or assess the security of M&A targets.

While each standalone product brings its own unique features and benefits, when combined, the positive results increase exponentially. These three products help lower the risk and impact from breaches with a comprehensive product suite for security operations, empowering enterprises with best-in-class detection, investigation, automation, and response capabilities, bar none.

14. "XDR Defined: Giving Meaning To Extended Detection and Response," April 28, 2021.

With end-to-end native integration and interoperability, security teams can close the loop on threats with continual synergies across the Cortex ecosystem. All three products work in concert to monitor the threat landscape and provide the most robust prevention, detection, response, and investigation capabilities:

- Cortex XDR provides endpoint security and EDR to block sophisticated attacks using AI-driven analysis and a range of protection modules.
- Cortex XDR and Cortex Xpanse provide the ultimate visibility and detections across the internet attack surface, endpoints, cloud, and network.
- Cortex XDR and Cortex Xpanse leverage Cortex XSOAR for full orchestration, automation, and response capabilities.
- Cortex XSOAR leverages Cortex XDR and Cortex Xpanse to provide high-fidelity detections and alerts to drive orchestrated workflows.

Conclusion

Government agencies face unique security challenges, including the need for tools that provide visibility and enhanced operational efficiency over large, federated, geographically distributed networks. Additionally, effective command and control (C2) is difficult to achieve for organizational structures in which multiple entities share responsibility to secure and defend agency infrastructure. Government agencies are also a frequent target of APT groups, nation-states, and other bad actors, given these agencies' vast stores of sensitive national security information and employees' and citizens' data. A breach may impact national security, leak personally identifiable information (PII), or negatively affect the availability of crucial government services.

In addition, the public sector must contend with both talent pipeline and staffing shortfalls while defending legacy systems that are often vulnerable to attack. The migration to the cloud and the expansion of telework compound these challenges, expanding attack surfaces and increasing the overall complexity of networks. Amidst these challenges, government organizations must adopt a robust, forward-leaning cybersecurity strategy that enables an integrated, programmatic approach and leverages innovative, best-in-class technologies and tools.

This way forward will enable federal agencies to detect, identify, and respond to threats to their networks more efficiently and effectively, improving cybersecurity outcomes across government.

Powered and Protected by Cortex

Driven by innovation to protect and defend our customers' most valuable resources, Palo Alto Networks is committed to bringing the newest and most advanced security solutions to market. We invite you to take a look at our solutions, reach out, and talk to us. We're here to help you learn more, do more, and secure more.

Visit our product pages for more information:

Cortex Xpanse

Cortex XSOAR

Cortex XDR

For more on the full range of government solutions offered by Palo Alto Networks, please visit our page.

Interested in scheduling a demo? Get started today.

The full Cortex® product suite is available on the DHS CISA CDM program Approved Products List (APL). Learn how XDR, XSOAR, and Xpanse can improve outcomes and efficiencies for your SOC. Download the DHS Approved Products List here.

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