Evolving Security Operations for Financial Services

3 Steps + 3 Keys to Transform and Automate Security Operations to Combat Advanced Attacks and Improve SOC Efficiency

Table of Contents

Introduction: Threat Actors Follow the Funds

The financial services industry (FSI) is constantly in the crosshairs for everything ranging from errant insider threats to well-funded cybercrime networks and nation-states seeking data, money, and influence, with no signs of threats diminishing in quantity or severity.

According to Verizon's 2022 Data Breach and Investigations Report, "The Financial sector continues to be victimized by financially motivated organized crime, often via the actions of Social (Phishing), Hacking (Use of stolen credentials) and Malware (Ransomware). Finally, Miscellaneous Errors, often in the form of Misdelivery, is still very common as it has been for the past three years in a row."[1]

Between 2021 and 2022, financial regulators shortened the notification window for cybersecurity incidents, impacting the operations of a financial institution or harming the confidentiality, integrity, or availability of systems or information. In the U.S., banks and credit unions must notify their primary financial regulator within 36 hours of a reportable cybersecurity incident. In Canada, this notification window is even shorter and must occur within 24 hours.

In addition to a steady stream of cyberattacks, financial institutions face challenges, including:

- Managing a mix of modern and legacy applications, including internally developed software (cloud-native and on-premises), commercial applications that may be highly customized, and those inherited from past mergers and acquisitions. Aging applications and associated infrastructure have been referred to as "technical debt."
- Maintaining a multivendor philosophy across the technology infrastructure to address resilience, vendor management, and cloud concentration risk.
- Supporting IT infrastructure for multiple lines of business across diverse geographies with disparate requirements and varying perspectives. For example, low-latency trading applications have needs distinct from those of consumer banking applications.
- Sharing data with multiple third parties, such as service providers, business partners, and even competitors (e.g., APIs for open banking), in support of new business models and customer experience expectations for enhanced engagements.
- Adhering to local, regional, national, and industry regulations, increasing the time and effort required for compliance. Some of these explicitly call for a "defense-in-depth" approach for the evolving consumer data privacy regulations.
- Operating in cost-optimization mode due to growth and inflationary pressures and other macroeconomic conditions.
- Battle for primary ownership of customer relationships between traditional financial institutions, fintech, and Big Tech, which may be both competitors and partners.

Compared to other industry sectors, healthcare and financial services organizations store, transmit, and process high volumes of monetizable sensitive information that disproportionately attracts threat actors.[2]

The extended network of a financial institution (FI) runs wide and deep, spanning personal, financial, and corporate data found in private data centers or the cloud from a variety of locations, including retail bank branches, campus sites, mobile devices, standalone ATMs, and a growing business partner ecosystem.

As we've learned, supply chain attacks, such as those on SolarWinds, can infect whole ecosystems through a single third-party vendor. And the four zero-day vulnerabilities in Microsoft Exchange Server traced back to the state-sponsored APT group Hafnium from 2021 all further underscore the need for SOC and security teams to rethink their strategies moving forward, including having real-world incident response plans and current risk assessments in place.

Companies and organizations across the globe were tasked with undertaking a phenomenal exercise because of the COVID-19 pandemic: bring workers online, remotely, quickly, and securely. At the start of the pandemic, seemingly overnight, operations were migrated—some of them business-critical—to home networks on multiple devices with little to no planning for this widespread event, executed in a short timeframe.

1. *2022 Data Breach Investigations Report*, Verizon, last visited on August 4, 2022, https://www.verizon.com/business/resources/reports/dbir/2022/master-guide/.
2. *2020 Incident Response and Data Breach Report*, Unit 42, December 23, 2020, https://www.paloaltonetworks.com/resources/research/2020-unit42-incident-response-and-data-breach-report.

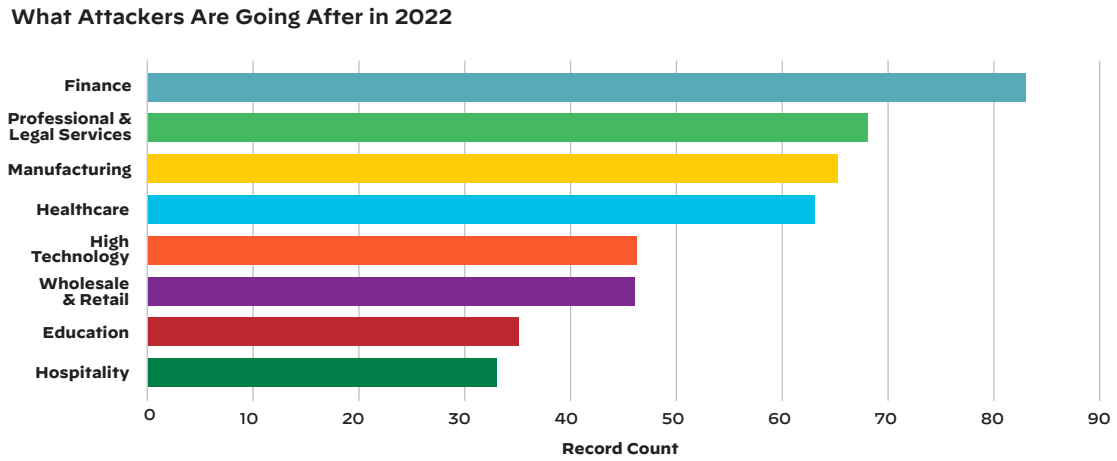


Figure 1: Top affected industries in 2022, according to the 2022 Unit 42 Incident Response Report

Not only did this place a huge burden on corporate cybersecurity teams, protocols, and systems, it exposed technology gaps between corporate locations and remote home offices. The necessity to support a fully remote user workforce and ecosystem, including updating incident response plans, became job number one for countless IT and security teams.

> Across the globe, those in the financial industry act as the gatekeepers to huge amounts of sensitive financial data. The integrity and safety of that information is critical for these firms' business operations and their reputations. A ransomware attack against a financial firm not only puts large amounts of financial information at risk, but also cripples the firm's ability to conduct financial transactions, potentially putting millions of customer dollars and contracts in jeopardy.[3]

The resulting security challenges for FIs and their supply chains have certainly been impacted by the abrupt shift in operations, but it has also exposed a host of other issues that are a direct result of a collective response to the global pandemic. As workers pivot between home and corporate networks, this hyper-distributed workforce will continue to be vulnerable, with threat actors continuing to take advantage of the situation, potentially for years.

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

Security Challenges for Financial Services

Business Email Compromise (BEC)

BEC is a cyberattack method involving hacking a business email account or spoofing (falsely imitating the domain of) a valid business email address. The victim of a BEC attack receives an email that appears to come from a trusted business, looking and feeling genuine. However, it typically contains a phishing link, a malicious attachment, or a request to transfer money to the attacker.

> The FBI Internet Crime Complaint Center (IC3) estimates that in the aggregate, BEC attacks cost organizations three times more than any other cybercrime.[4]

3. *2020 Incident Response and Data Breach Report*, Unit 42, December 23, 2020, https://www.paloaltonetworks.com/resources/research/2020-unit42-incident-response-and-data-breach-report.
4. *2020 Internet Crime Report*, Federal Bureau of Investigation, last visited on August 4, 2022, https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.

Because of the large volume of financial transactions FIs handle every day, ransomware and BEC accounted for approximately 70% of Unit 42 incident response cases in 2021. From banks to local real estate firms, threat actors target these organizations because of the access their employees have to large sums of money. For organizations like title companies, the risk goes beyond the firm and can affect customers who are preparing to wire large payments to purchase houses, for example.

1. Employ regular and robust security awareness training to combat phishing attempts.
2. Implement MFA as a security policy for all employees.
3. Require that wire transfer verification takes place outside of email to ensure a multistep verification process.

Figure 2: Top three pro tips to prevent BEC attacks

Insider Threats

Internal threat actors account for 27% of the data breaches in the FSI,[5] although not all of this is malicious activity. Misdelivery—when personally identifiable information (PII) or other sensitive information is sent to the wrong recipient due to negligence—accounts for a portion of the data lost as well. Anomalous traffic patterns serve as an indication that lateral movement is underway and provide cause for further investigation by the security operations center. The Zero Trust Model would help limit the ability of a malicious actor to move laterally and certainly reduce the "blast radius" of an intrusion as well.

> "The error variety of 'Misdelivery' (16%) is the second most common action variety in the financial sector. Misdelivery is exactly what it sounds like, delivering PII or other sensitive information to the wrong recipient … our data indicates that Misdelivery is approximately three times higher in Financial than in the other industries."[6]

Insider-caused security incidents—whether due to malice or negligence—are a pervasive problem for many firms and can be hard to prevent without disrupting the ability of employees to do their jobs. Here are some steps to take in order to minimize the chances of an insider threat:

1. **Identify and manage critical or sensitive assets**. The development of workplace technologies has allowed for rapid collaboration and access to information, but it also allows for those assets to be more easily exfiltrated. Security teams should have a complete account of an organization's assets along with access management tools and policies to defend against an insider threat.
2. **Document and enforce security policies**. At times, employees may become unintentional insider threats due to unclear or inconsistent security policies regarding an organization's assets. Organizations must clearly outline the acceptable use of assets, use of privileged accounts, ownership of intellectual property, and other similar topics. Along with the policies, organizations should be able to provide clear justification and reasoning behind each policy.
3. **Create a response strategy for insider threats**. While we may not be able to completely eliminate insider threats, an organization can construct strategies to rapidly respond to insider threat incidents, thus helping to minimize damage to the organization should one occur. These strategies may involve creating a working group across departments and functions or having dedicated personnel to handle insider threat incidents.

> The cost of breaches caused by insiders has risen by more than one-third over previous years to $15.38 million. The time to rectify an insider breach also increased, from 77 days to 85 days, leading organizations to spend the most on containment.[7]

Public Cloud and Other Internet-Based Assets

On average, FIs report that 28% of their workloads are already in the public cloud. Another 33% of the workloads are slated for the cloud.[8] The FSI has finally embraced the use of the public cloud as a business

5. *2022 Data Breach Investigation Report*, Verizon.
6. *Ibid.*
7. *2022 Cost of Insider Threats Global Report*, Ponemon Institute, last visited on August 4, 2022 .
8. *Building a More Advanced Cloud Security Framework for Financial Institutions*, Palo Alto Networks, last viewed on August 4, 2022, https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/white-papers/fs-cloud-whitepaper-emea.pdf.

enabler and a competitive differentiator. Of course, many FIs opt to use multiple public cloud providers and also private clouds for their computing needs. All of these environments need to be protected with an ever-growing set of traditional, cloud provider-specific, and third-party cloud security tools.

Another aspect of this expansive public cloud and internet-visible footprint is the need for an accurate inventory of both internal- and external-facing assets. Cloud resources are easily created with or without the involvement of the IT or info security teams. The same is true for local internet connections. Creating and maintaining an asset inventory of all cloud and internet-visible resources is fundamental to the cybersecurity program.

Third-Party/Supply Chain Risk

FIs are faced with a growing ecosystem of third-party partners to remain competitive. Partnerships have been formed with fintech, Big Tech companies, and even traditional competitors—all of which require some degree of data sharing. The open banking movement bears some responsibility for this, as banks must make financial data available to third parties. Additionally, financial institutions are collecting information about their clients from multiple sources for data analytics to gain insights into customer preferences. However, with increased data sharing, there is a greater risk of potential data loss and misuse.

Regulatory Notifications and Operational Resilience

The financial services industry is considered a component of critical infrastructure as its operation is vital to the well-being of the economy. Technology and cybersecurity incidents can severely inhibit a FI from fulfilling its role in the financial marketplace. In the US, critical infrastructure companies (including financial institutions) must report cybersecurity incidents within 72 hours to the Cybersecurity and Infrastructure Security Agency (CISA).

As mentioned previously, US banks and other depository institutions have 36 hours to report computer or cybersecurity incidents that may disrupt or degrade banking operations, customer access to deposits, or impact the stability of the financial sector. In the EU, the Digital Operation Resilience Act (DORA) is expected to be finalized later in 2022. Its objective is to ensure FIs are able to maintain resilient operations through severe operational disruptions (including cyberattacks). FIs need to detect, identify, and assess cyber incidents quickly to meet these regulatory notification requirements while simultaneously working on remediation to minimize operational impact.

Ransomware

Malicious actors continue to target the FSI, and ransomware remains one of their favorite tools. FIs have obtained cyber insurance policies in the past, but premiums are now more expensive and offer less coverage. This combination has reduced the value of cyber insurance as a means to manage risk. Consequently, FIs continue to pursue technology-related solutions to detect, prevent, and respond to ransomware. Beyond the cost of the ransom itself, ransomware may impact the normal business operations of both the firm and its third-party partners. Without timely incident response and remediation, a ransomware attack can easily become a reportable event to one or more regulatory agencies.

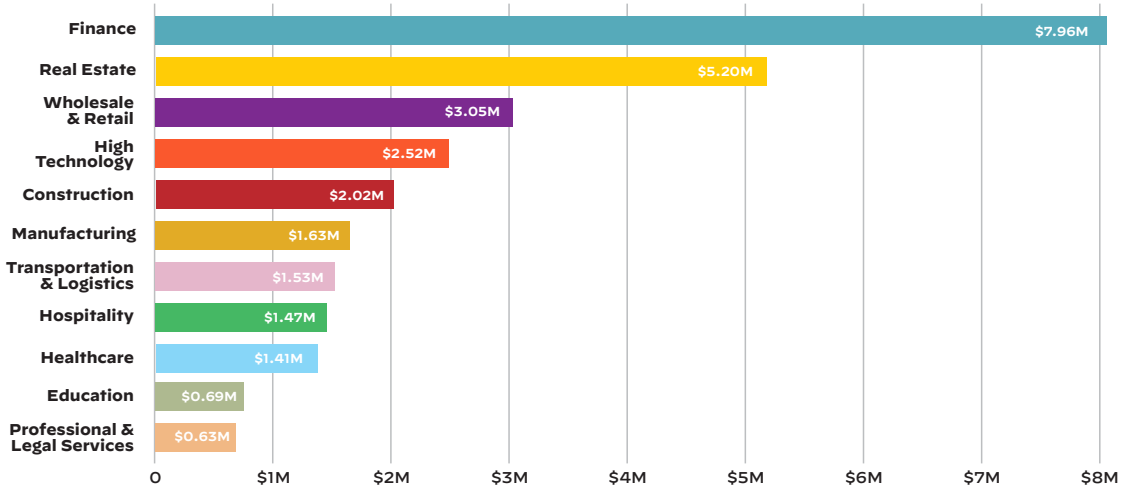


Figure 3: Average ransom demand by industry, according to the 2022 Unit 42 Incident Response Report

Recommendations to Mitigate the Impact of a Ransomware Attack

Develop and execute a plan for an end-user awareness program.

- It can be difficult to get approval to send regular company-wide security reminders, but smarter end users who are more aware of cybersecurity risks will surely experience fewer ransomware incidents.

Review/Validate server backup processes.

- Backups that are configured improperly or in a location that can allow for further compromise can result in further losses, both monetary and otherwise.
- Review critical file servers that host network shares for critical departments and plan for regular review of the recovery process for these servers.

Conduct end-user privilege reviews.

- Assign a trusted delegate to develop and organize a process to evaluate permissions that users have on mapped network drives. Whenever possible, implement the principle of least privilege to minimize the impact that any single user can have.
- Start the review process by looking at end-user privileges for critical resources and departments.
- Require strong, unique, and complex passwords for all accounts.
- Review network drive permissions to minimize the impact a single user can have.

Define administrator user privilege reviews.

- Audit privileged roles used by the server, backup, and network teams to validate appropriate access.
- Ensure administrators are assigned normal, restricted accounts, separate from their highly privileged accounts.
- Require administrators to use their highly privileged accounts only when they need them.
- Remove automatic network drive mappings from administrative accounts, where possible.
- Restrict administrative accounts from receiving email.
- Require multifactor authentication for all users, including administrative accounts, and monitor for abnormal use.
- Require strong, unique, and complex passwords for all accounts.

Document your incident response plan for ransomware.

- Ensure ransomware response processes are included in your incident response plan. Ransomware requires a unique process to recover and should stand out on its own.
- Cases, where all the files on an entire department drive are encrypted, can become quite complex as multiple teams need to be engaged—backup team, file-server team, endpoint, directory team, and others. The more you plan now, the quicker your response time will be.

A Permanent, Partially Remote Workforce

In the new hybrid work model, "work is no longer a place you go; it's something you do." Some well-known FIs have been very vocal about bringing employees back to the office on a full-time basis as the pandemic becomes endemic. However, there are others that have been more open to the hybrid work concept, allowing employees to work from home or other locations. For example, an employee may work in the office two or three days a week and work remotely the rest of the week. This permanent arrangement is very different from pre-pandemic days when even partial work-from-home instances were uncommon. This effectively creates a set of remote offices that need an appropriate level of security, monitoring, and service for each such employee.

Before COVID

29%

of FS companies had at least 60% of their workforce working from home at least once a week.

After COVID

69%

of FS companies expect to have 60% of their workforce working from home at least once a week going forward.

Source: PwC's US Remote Work Survey June 25, 2020: FS employer base of 50

Figure 4: The changing work-from-home landscape post-COVID

SOCs Are Tested 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.

Combine challenges such as noisy false positives, event storage (volume and cost), poor investigation workflows with the adoption of hybrid and multicloud architectures, and the proliferation of devices and endpoints and you get overwhelmed 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

Three Steps Toward Creating a Future-Forward SOC

Step 1: Asset Management—Reduce Complexity and 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 to maintain complete visibility of their internet-connected assets and would benefit from a dedicated attack surface management (ASM) solution.

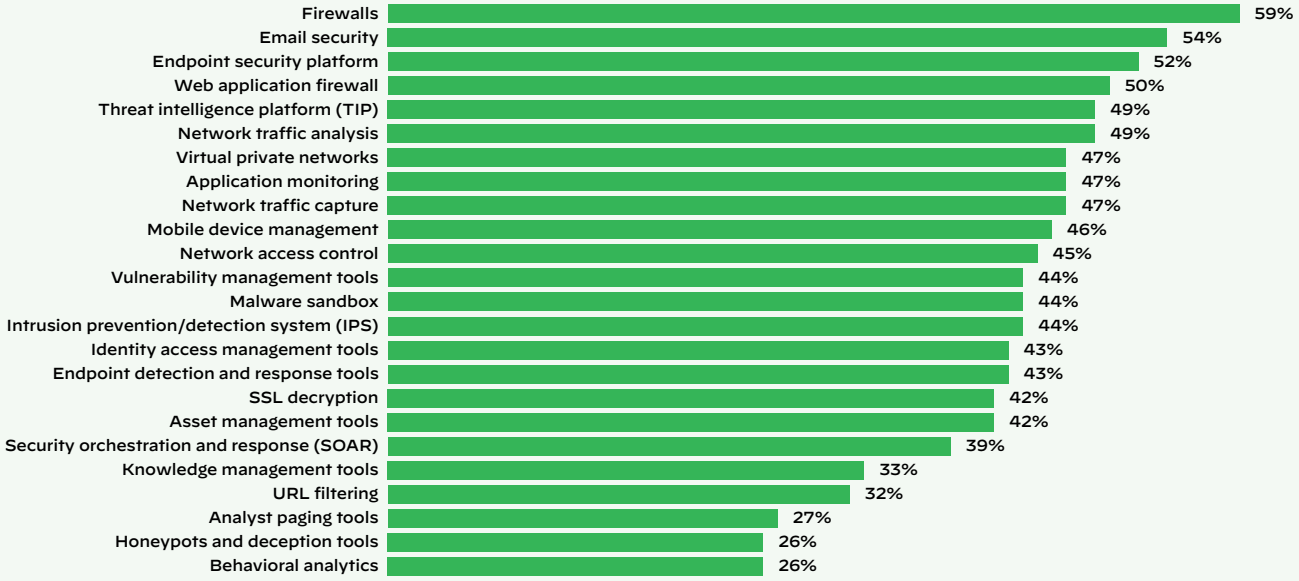
For some teams, tool sprawl can begin by deploying a point solution to fix a specific issue. Unfortunately, this piecemeal approach, combined with managing numerous agents, can (ironically) leave networks even more vulnerable, exposing gaps due to issues from a lack of interoperability and improper configurations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

The complexity of these challenges is exacerbated by many FSIs having acquired multiple security products and services that do not function cohesively, making them less effective. Some of this security infrastructure sprawl is intentional in "defense in depth"—the notion that if one system misses an attack or instance of malware, another will catch it. As attack sophistication outpaces the capabilities of standalone point products, institutions buy the next "best" security technology to further defend themselves.

As institutions adopt public cloud computing, they are also drawn to proprietary security offerings from cloud service providers (CSPs) that are specific to that one environment. Security tools proliferate over time with each new threat vector or expanding attack surface. Some large financial institutions have accumulated over 100 often narrowly focused security tools. All of these must be monitored, managed, and administered by both IT and security operations teams, consuming valuable time and resources.

One of the first steps an organization can take to reduce the security impact of tool sprawl is to audit protected systems and entities to better manage IT and security assets. 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 the protection of high-value and high-risk data.

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
Source: A commissioned study conducted by Forrester Consulting on behalf of Palo Alto Networks, February 2020

Figure 5: Tools security operations pros use, self-reported to ESG

Step 2: Automation—Automate Workflows for Operational Efficiency

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.

One-to-Five 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.

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.

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."[9] The same report noted that respondents revealed only 24% of investigated alerts were considered legitimate, down from 34% in 2018.[10] 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.[11]

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 doesn't always enable consolidation of event data. Even the use of 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: People—Augment People with ML-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, and automate system-level action, workflows, and decision-making.

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 31% between 2019 and 2029.[12] Additionally, the National Center 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.[13]

In concert with filling critical roles, organizations must adopt cybersecurity awareness training to ensure employees, contractors, and in some cases, partners, are well-versed in helping to prevent

9. *Anticipating the Unknowns: Chief Information Security Officer (CISO) Benchmark Study*, Cisco, March 2019, https://ebooks.cisco.com/story/anticipating-unknowns/page/6/6.
10. Ibid.
11. Ibid.
12. "Occupational Outlook Handbook," U.S. Bureau of Labor Statistics, last viewed on August 4, 2022, https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm.
13. "Cyber Security Job Outlook in 2021," NEIT, November 19, 2020, https://www.neit.edu/blog/cyber-security-job-outlook.

breaches. Stolen credentials, phishing attacks, and social engineering require people to execute campaigns, so building a cyber-savvy 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."

We Walk the Talk—Protecting Our Own SOC

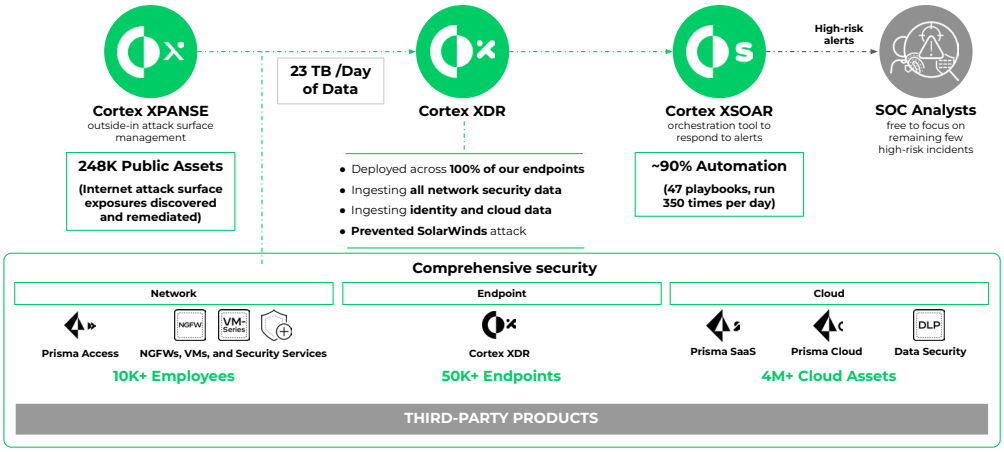


Figure 6: In action: The Palo Alto Networks SOC

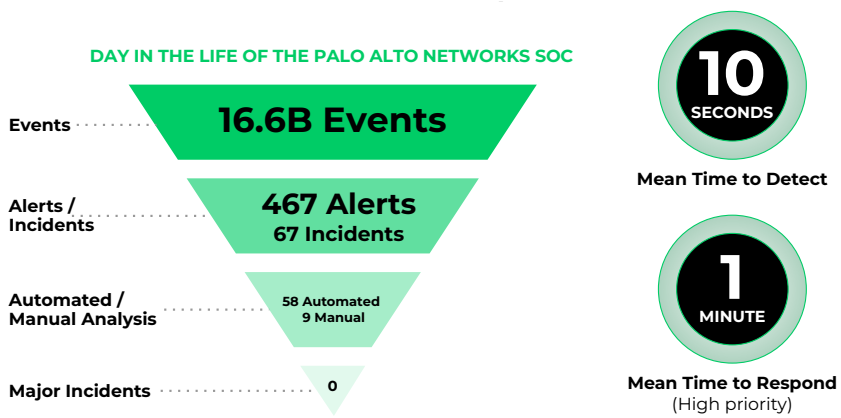


Figure 7: In action: We have achieved a 1 min. response time

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 PANW SOC team follows this general philosophy:

- Staff 80% of the SOC with people who have previous SOC experience.
- Cross-train the SOC team in all domains, including alert triage, incident response, threat hunting, etc.
- 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.

Three Keys—ASM, SOAR, and XDR: The Bedrock for SOC Transformation

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

Key 1: Power Up Your Risk Management Function by Understanding Your Attack Surface

One foundational component of a SOC transformation is to have a strong risk management function. Identifying the things you are trying to protect should be an opportunity to create a resilient risk management process. 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 as part of a larger risk management plan.

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.

Most data (77%) within a financial institution needs to be secured, while 52% is considered confidential/secret, requiring robust security.[14]

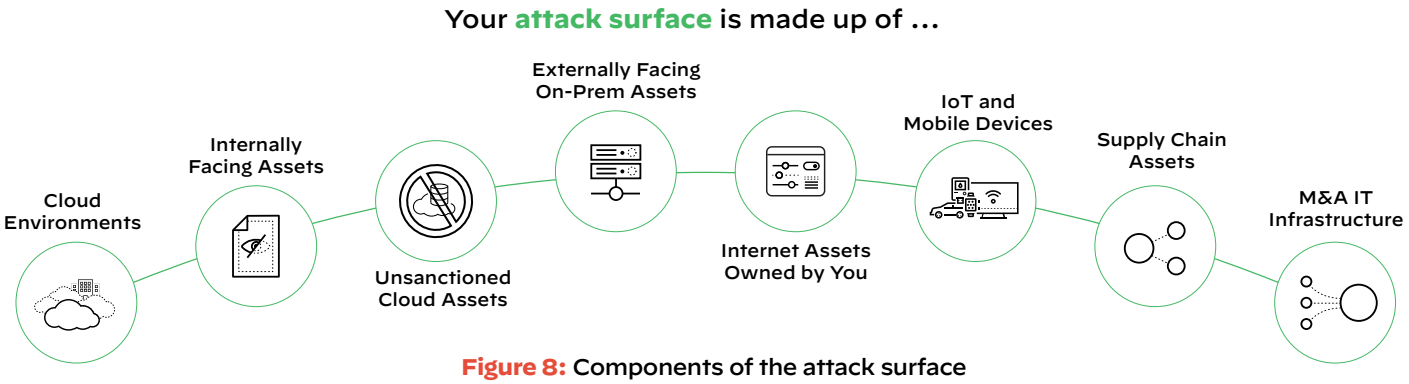


Figure 8: Components of the attack surface

Defined by SANS Institute:[15]

> *Attack surface management (ASM) "is an emerging category of solutions that aims to help organizations address this challenge by providing an external perspective of an organization's attack surface. An organization's attack surface is made up of all internet-accessible hardware, software, SaaS and cloud assets that are discoverable by an attacker. In short, your attack surface is any external asset that an adversary could discover, attack, and use to gain a foothold into your environment."*

SANS lists some common use cases for adoption of an ASM solution, including:

- Identification of external gaps in visibility
- Discovery of unknown assets and shadow IT
- Attack surface risk management
- Risk-based vulnerability prioritization
- Assessment of M&A and subsidiary risk

In our report, *2022 Cortex Xpanse Attack Surface Threat Report*, we outlined some key findings from our research of the public-facing internet attack surfaces of some of the world's largest businesses:[16]

- **What is new becomes old on attack surfaces**. Modern attack surfaces are inherently dynamic, constantly shifting, moving, and growing. Xpanse tracked attack surface growth and found

14. "Data Protection and Privacy Survey," IDC, December 2020.
15. Pierre Lidome, "The SANS Guide to Evaluating Attack Surface Management," SANS Institute, October 26, 2020, https://www.sans.org/white-papers/39905/.
16. *2022 Cortex Xpanse Attack Surface Threat Report*, Palo Alto Networks, July 19, 2022, https://www.paloaltonetworks.com/resources/research/cortex_xpanse-attack-surface-threat-report.

security teams can't keep pace. Attack surfaces continue to grow, and the unremediated issues become persistent threats.

- **Low-hanging fruit continues to hang**. Nearly one out of every four issues we found on the attack surface was related to exposed RDP servers, a key vector for ransomware attacks. Even looking at the next most common issues, the end result was often an exposed administration login portal.
- **RDP and cloud exposures are persistent**. RDP exposures are not only common but persistent too. We tracked the average number of days per month that various industries had exposed RDP issues, and found that FSI had more than seven days per month (7.78) with exposed RDP.

See figure 9 for a breakdown of the attack surface i.e., internet-exposed assets seen across the FSI.

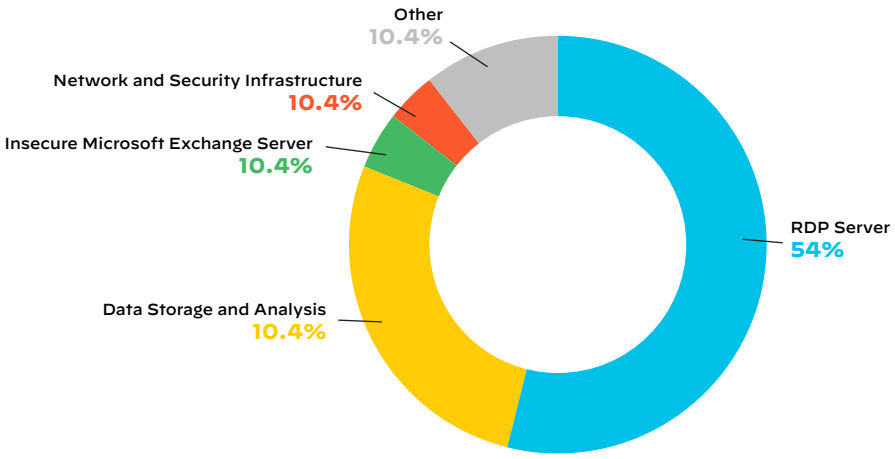


Figure 9: Distribution of risks across the financial services industry attack surface

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. Security teams should be doing the same by deploying an attack surface management solution that can provide a continuous assessment of an organization's external attack surface.

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."[17] 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

17. Claudio Neiva, et al., *Market Guide for Security Orchestration, Automation and Response Solutions*, Gartner, 21 September 2020, https://www.gartner.com/en/documents/3990720.

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 platform 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
- 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 platforms continue to build toward becoming the control plane for the modern SOC environment. To achieve this end, SOAR platforms are starting to integrate threat intelligence, vulnerability management, etc., directly into the platform 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 "time savers" for the month of February 2021.

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

Total hours saved in February 2021

XSOAR automates the workload of 13.72 FTEs

Figure 10: 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.

Key 3: XDR—the Next Logical Evolution of EDR

The term "XDR," short for "extended detection and response," was coined in 2018 by Nir Zuk, CTO and co-founder of Palo Alto Networks. The basic reason for creating XDR was to stop attacks more efficiently, detect attacker techniques and tactics that cannot be prevented, and help SOC teams better respond to threats that require investigation. The vision was to provide a seamless approach to 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 by consolidating siloed tools, streamlining processes, and providing greater visibility for threat detection and investigations. Teams can eliminate blind spots, reduce investigation times, and ultimately improve security outcomes using XDR. 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."

Forrester defines XDR as:

> *The evolution of endpoint detection and response (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 (IAM), 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.*[18]

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, more robust automation, advanced analytics, and machine learning. XDR's value is gaining momentum by 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.19

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

XDR Fills the Detection and Response Void

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 verifying 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 from an XDR approach to security architecture.

According to Forrester Analyst Allie Mellen, who covers SecOps, "XDR and SIEM are not converging but colliding."[20] 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 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."*[21]
>
> *"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."*[22]

Takeaway: XDR is a viable alternative approach to SIEM solutions by providing threat detection, investigation, response, and hunting rooted in endpoint threat detection and response with the ability to scale to cloud environments which is where enterprise data is moving.

18. Allie Mellen, "XDR Defined: Giving Meaning to Extended Detection and Response," April 2021, https://go.forrester.com/blogs/xdr-defined-giving-meaning-to-extended-detection-and-response/.
19. Ibid.
20. Ibid.
21. Ibid.
22. Ibid.

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

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.

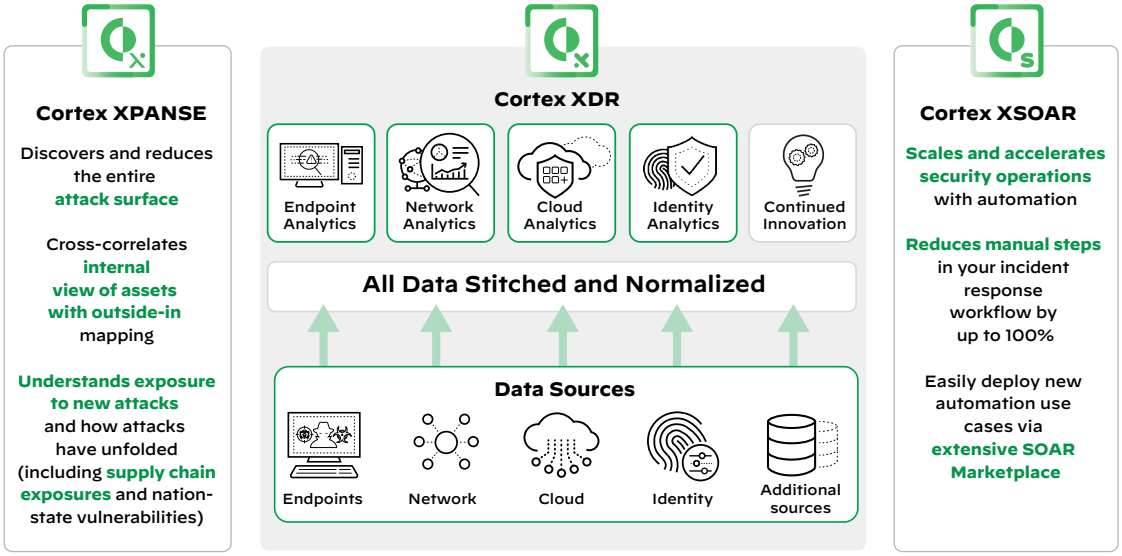


Figure 11: End-to-end workflow automation for security operations

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. Immediate high-level advantages include:

Cortex XDR: The ability to stop attacks at the endpoint and host with world-class EDR for Windows and Linux hosts, providing 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.

Cortex XSOAR: A single platform for end-to-end incident and security operational process lifecycle management. Security teams of all sizes can leverage the extensive 800+ prebuilt integration content packs, and robust security-focused case management with real-time collaboration to orchestrate, automate, and speed incident response and any security workflow or security process across their environment. In addition, with integrated threat intel management, security teams get a central threat library, the ability to automatically map threat information to incidents, and operationalize threat intelligence with automation.

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

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.

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 of breaches with a comprehensive product suite for security operations, empowering enterprises with best-in-class detection, investigation, automation, and response capabilities, bar none.

With end-to-end native integration and interoperability, SOC 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 detection, response, and investigation capabilities:

- Cortex XDR and Cortex Xpanse provide ultimate visibility and detections across the internet attack surface, endpoints, cloud, and network, including remote workers.

- 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

The financial services industry continues to be an attractive target for threat actors. Despite financial services routinely outspending other verticals in cybersecurity staff, tools, and associated investments, aggressive cyberattacks persist, enticed by the trove of rich customer, financial, and personal data. As critical workloads shift to cloud environments, protecting financial institutions and their data has become even more complicated.

Compounding the FSI's security challenges, many institutions are also laden with technical debt from legacy and proprietary systems accumulated over decades. The FSI's dependency on the internet and third-party partners has further expanded the attack surface and stretched the limits of what a traditional SOC can manage effectively.

The path forward requires financial institutions to detect, identify, and respond to threats across their entire estate with both simplicity and automation as force multipliers for SOC analysts. The ultimate goal is to improve cybersecurity outcomes in spite of the challenging environment in which financial institutions operate.

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 and integrated 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

Interested in scheduling a demo? Get started today.

Enlist Unit 42's Expert Security Services

Visit Unit 42's page dedicated to financial services for more resources and information.

Execute an IR plan or call an IR team such as Palo Alto Networks Unit 42. Unit 42 brings together an elite group of cyber researchers and incident responders with a deeply rooted reputation for delivering industry-leading threat intelligence.

If you think you may have been breached or have an urgent matter, get in touch with the Unit 42 Incident Response team by emailing unit42-investigations@paloaltonetworks.com or calling:

- North America Toll-Free: +1.866.486.4842 (+1.866.4.UNIT42)
- EMEA: +31.20.299.3130
- APAC: +65.6983.8730
- Japan: +81.50.1790.0200

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

cortex_wp_evolving-security-operations-for-financial-services_082522