Scale Your SOC with Cortex

How Financial Services Can Automate Attack Surface Management

Online and mobile banking were widely embraced by consumers during the pandemic. The vast majority (85%) of bankers noticed an increase in the use of digital channels in 2021.[1] Beyond that, 82% expect digital channel use to increase in the future.[2] Digital banking has proven convenient and well-aligned with customer expectations for digital experiences.

1. *2022 Banking Priorities Executive Report*, CSI, January 25, 2022.
2. Ibid.

As part of their digital transformation efforts, financial institutions continue to make more assets and resources available on the internet for their customers and partners. This convenience has become expected in today's on-demand mindset. Anything less would be viewed as a shortcoming.

One implication of this journey to the cloud is that remote campus and branch offices now have a strong dependency on the internet for corporate applications (e.g., email, calendaring, CRM) and data. Instead of backhauling this traffic through the corporate data center, financial institutions have adopted direct internet access from these campus and branch offices to optimize the end-user experience. This change makes it difficult for financial institutions to inventory and manage all of these connections centrally, and each untracked internet connection is a potential point of exposure.

Why Financial Institutions Need Attack Surface Management + Automation

With a combination of sensitive private information and financial assets, cybercriminals see financial services as a rich environment to target. Aside from theft of private information, which can be monetized, outright fraud via account takeover attacks is also possible.

Financial institutions are also engaging with more third-party partners (e.g., traditional competitors, fintech, Big Tech) to share data and gain insights into customer behavior and preferences. The ultimate objective is for the financial institution to offer tailored, highly contextual client experiences, but the existence of this additional customer data creates a more valuable target and more potential attack vectors throughout the partner chain.

As financial institutions continue to make additional assets and resources available on the internet for their customers and partners, digital asset sprawl has reached a point where security teams are unable to keep up due to nonexistent or ineffective processes for internet asset discovery, inventory, and management. It is nearly impossible to get the visibility needed to manage everything that can be externally accessed, which leads to a significant amount of risk.

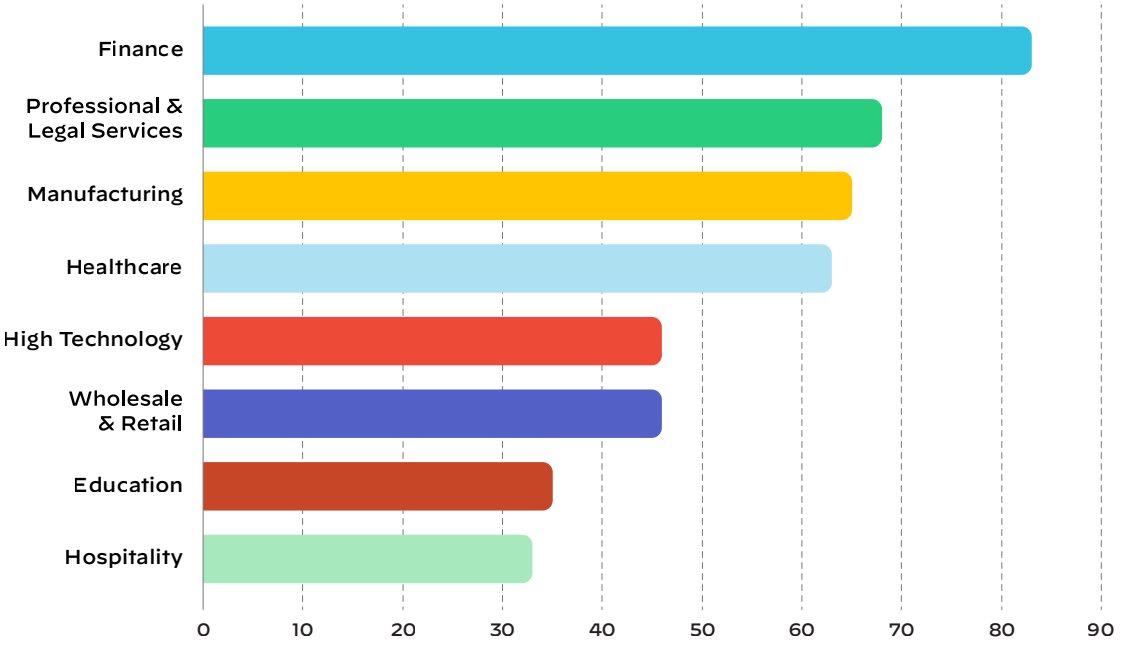

Figure 1: Top affected industries in 2022, according to the *2022 Unit 42 Incident Response Report*[3]

3. *2022 Unit 42 Incident Response Report*, Palo Alto Networks, July 26, 2022.

Amid these growing challenges, financial institutions need to adopt a robust cybersecurity strategy enabling integrated, programmatic approaches to security operations with optimum efficiency and efficacy. This balanced approach will enable them to meet their business objectives and serve as the trustworthy custodian of their customers' financial assets.

Challenges Unique to Financial Institutions

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."[4]

Making matters more urgent, between 2021 and 2022 financial regulators shortened the notification window for cybersecurity incidents that impact the operations of financial institutions or harm 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 must occur within just 24 hours.

That said, IT regulations and compliance directives are perhaps the strongest in the financial services industry. In addition to intense scrutiny from financial regulators, banks must also meet the expectations of customers regarding the security of personally identifiable information (PII), which has been cited as the most important factor in choosing a financial institution.[5] To address these pressures, financial institutions tend to be early adopters of cybersecurity practices and products, but malicious actors still target them due to the critical data they hold and the opportunities this represents.

> More than **80%** of all issues observed in the financial industry's attack surface were either related to exposed RDP servers or worse, were related to accidentally exposed database storage and analytics systems.
>
> **–Unit 42**[6]

Trends in the Financial Services Attack Surface

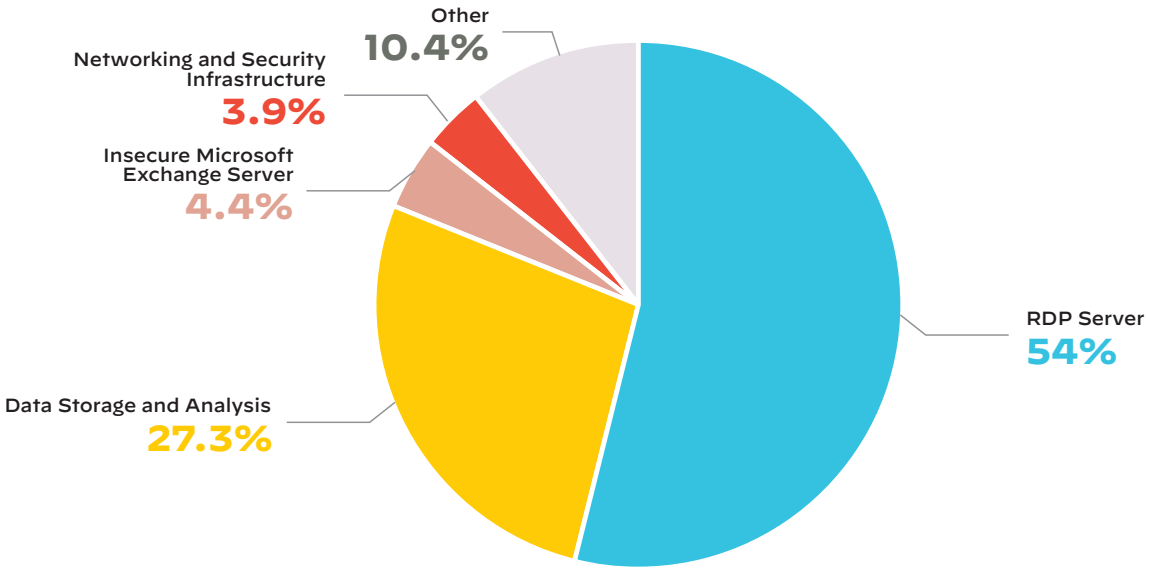

Figure 2: Distribution of risks across the financial services industry attack surface

4. *2022 Data Breach Investigations Report – Master's Guide*, Verizon, May 2022.
5. *Verint Experience Index: Banking Report 2022*, Verint, August 2022.
6. *Cortex Xpanse Attack Surface Theat Report*, Palo Alto Networks, July 12, 2022.

1. **Unmanaged attack surfaces in financial institutions are consistently growing**

   The global attack surface continues to grow and change constantly. This highlights a reality for security practitioners, which is that the work is never done. Worse, the work that doesn't get done becomes a seemingly insurmountable backlog of issues and exposures needing attention. The unfortunate truth of attack surfaces is that there is a constant stream of new issues—new vulnerabilities, changing configurations leading to exposure, expiring certificates, new assets, etc.

   In a study of the global attack surface in 2021 by the Cortex Xpanse team, we looked at an insecure Apache Web Server issue. This issue has been exploited in the wild and was mentioned in several federal advisories.

   In our observation, financial institutions are particularly susceptible to exploits through this vulnerability. On average, in a given month, there were between 50 and 500 active vulnerabilities with new vulnerabilities observed of just this zero day.

2. **Financial institutions' attack surfaces are complex and dynamic**

   This issue only constituted a small sliver of the overall issue types seen on an attack surface. Therefore, as part of our new research based on data collected from December 2021 through June 2022, we widened the scope to look at the rate at which all new issues of high and critical severity were discovered on attack surfaces.

   In this additional research, the Xpanse team found financial institutions saw 4% to 35% of assets connected to their network change every month. Without a continuously updated view of their attack surface, this will undoubtedly lead to large blind spots in their IT infrastructure.

3. **Significant exposures exist in the FSI's attack surface**

   The Cortex Xpanse research team discovered the unmanaged attack surface of the financial industry to be extremely vulnerable. (See figure 2.)

   RDP servers (54% of issues for FSI): Remote Desktop Protocol (RDP) servers provide remote access to a computer over a network connection. Externally accessible RDP servers pose a significant security risk as they are frequent targets for attackers and can be vulnerable to a variety of documented exploits. They are normally used by IT help desk, admins, and users. Ideally, RDP servers should be not publicly exposed to the internet as they are the gateways to ransomware.

   According to the Unit 42 Threat Report, RDP has been the preferred vector for ransomware deployment. Discovered RDPs are sold for anywhere from $3–$10 on the dark web marketplaces for sophisticated ransomware actors to exploit. Hence, it becomes crucial for an organization to identify all their exposed and misconfigured RDP servers and undertake necessary remediation actions to prevent the threat of ransomware.

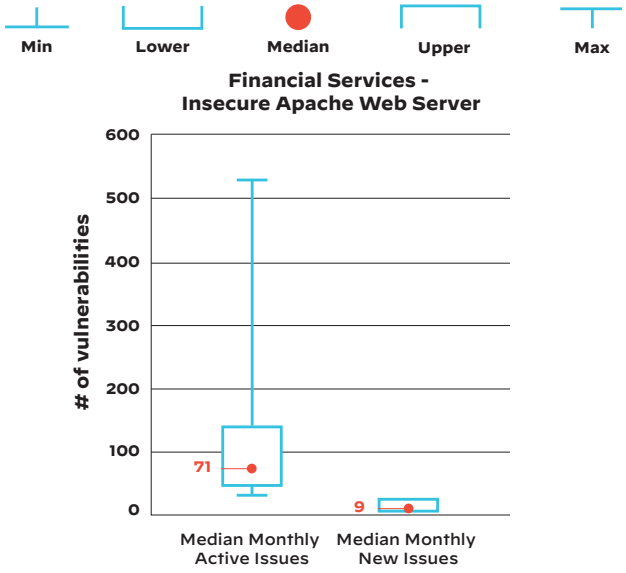

Figure 3: Median active and new insecure Apache Web Server issues per month per company in the Financial Services industry

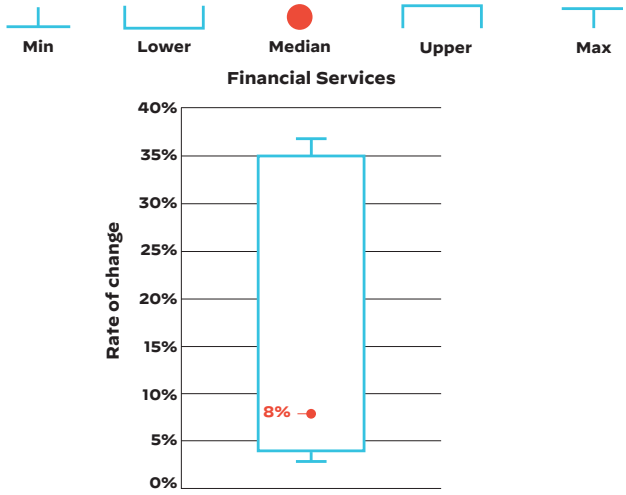

Figure 4: Rate of appearance of new issues and new assets on the internet compared to the previous month

> *"I'll tell you that persistence and focus will get you in, and will achieve that exploitation without zero days. There's so many more vectors that are easier, less risky, and often, more productive"*
>
> **—Rob Joyce, Sr. Advisor to the Director NSA for Cyber Security Strategy**

Data storage and analysis infrastructure (27.3%): Data storage and analysis Infrastructure includes publicly exposed services like MySQL, PostgreSQL servers, MongoDB servers, unclaimed S3 buckets, and several other data and analysis services. None of these services should be publicly accessible over the internet as they regularly contain sensitive enterprise information and are not hardened to the same security standards as systems designed to be publicly accessible, putting them at risk of compromise, data theft, and data leaks.

Data storage exposures in this industry are worrying as they could contain key customer or transaction data. Additionally, with many people now working from home, these exposures become even riskier as employees are accessing critical information through potentially vulnerable, non-consumer-grade access points.

Cortex Xpanse researchers also observed over **150,000 active publicly exposed RDP instances in the financial services industry**. On average, these RDP instances were openly exposed to the public internet for nearly **8 days** over the course of one month, putting those exposed organizations at serious risk.

How Can Financial Services Address Attack Surface Challenges?

Attack surface management (ASM) and security orchestration, automation, and response (SOAR) dramatically reduce your attack surface.

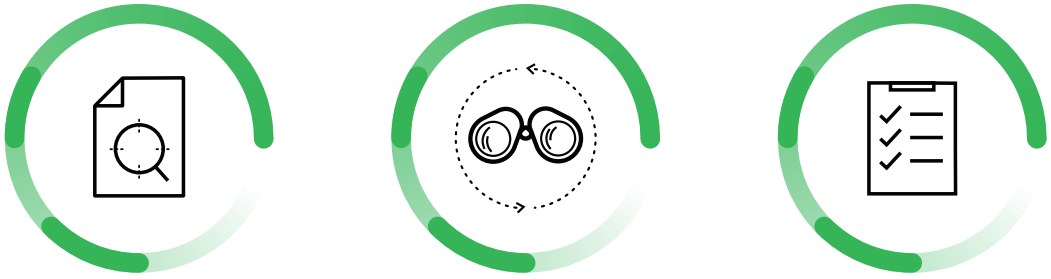

Figure 5: Automated ASM

What Are ASM and SOAR?

An attack surface comprises countless assets and devices, secured and unsecured, managed and unmanaged, those that are known, and those that are not. It encompasses cloud assets and resources, vendor and third-party assets, and even shadow IT. As such, it's a rich source of critical data and intellectual property that can easily be monetized on the dark web or used by threat actors in other malicious endeavors.

Continual port scans, packet sniffing, and reconnaissance happen daily as adversaries search for weak spots and backdoors. For those in InfoSec or SecOps, it's a non-stop game of cat and mouse, a never-ending cycle of managing alerts, triage, and removing or managing risks before attackers make their way past traditional defenses—rinse and repeat ad infinitum.

In the past, manual mapping and inventory analysis, bolstered by firewalls and endpoint security, were adequate. Legacy protocols for protecting digital footprints are downright dangerous today, however, especially as organizations adopt practices like remote and hybrid work fueled by the pandemic, exacerbated by moving applications and data off-premises, driven by cloud migration.

The increasing shift to the cloud is particularly problematic as it can suffer from misconfigurations, create confusion with the shared responsibility model between users and service providers, and overall increase an organization's attack surface. Fortunately, solutions exist to help mitigate these issues.

ASM is the process of continuously identifying, monitoring, and managing all internet-connected assets, both internal and external, for potential attack vectors, exposures, and risks.

SOAR technology helps coordinate, execute, and automate tasks between various people and tools all within a single platform. This allows organizations to quickly respond to cybersecurity attacks as well as observe, understand, and prevent future incidents, thus improving their overall security posture.

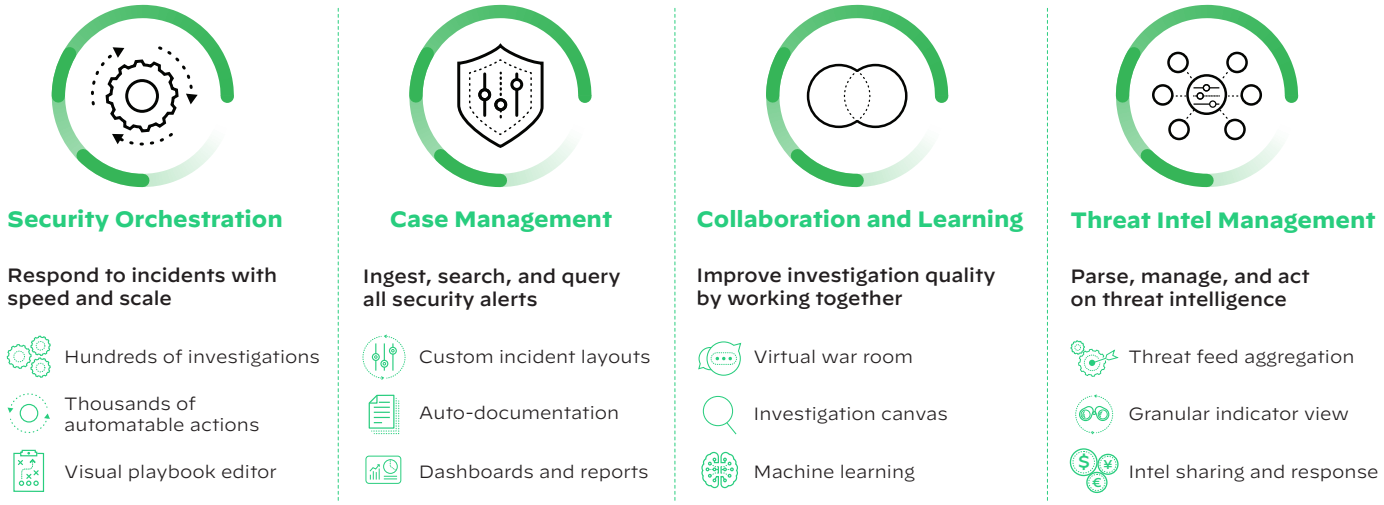

Figure 6: The new pillars of a SOAR platform

How Can Financial Organizations Fix Their Unmanaged Attack Surface?

The ultimate goal should always be attack surface reduction, although that is not currently possible with manual processes and a lack of seasoned security professionals. Attack surfaces are growing, and security teams are left chasing a moving goal post. New issues are not remediated, so they become the old issues that are the low-hanging fruit attackers feast on.

The rate of change of the attack surface highlights the need for more resilient security processes. Organizations need visibility into their attack surfaces and exposures, but they also need to put in place more automated processes to make remediating issues faster and less human-effort-intensive—a powerful solution would be to pair an ASM with a SOAR tool. This way, newly discovered issues can be automatically identified, prioritized, and either remediated or routed to the relevant stakeholder with full context data.

Using automation playbooks specifically designed for attack surface management, such as the Cortex Xpanse content pack, Cortex XSOAR allows you to automate attack surface management to identify internet assets and quickly remediate misconfigurations and exposures.

The integrations included in the pack enable fetching and mirroring of Xpanse issues into Cortex XSOAR incidents, and ingestion of indicators (IP addresses, domains, and certificates) referring to the corporate network perimeter as discovered by Xpanse.

Through a powerful set of playbooks, analysts can correlate the discovered information with data provided from internal security systems (Palo Alto Networks Cortex Data Lake, Prisma Cloud, and Panorama; Active Directory; Splunk SIEM; etc.) to pinpoint asset owners and automate remediation.

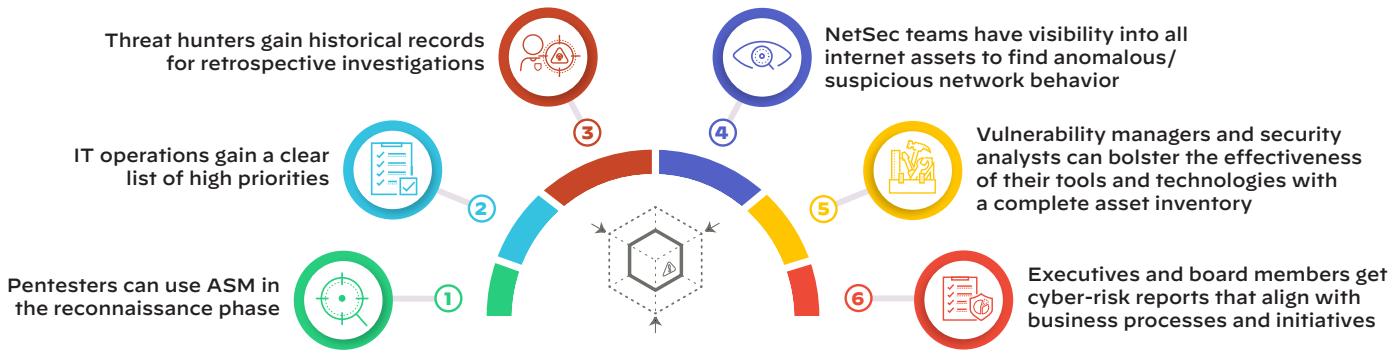

Figure 7: How ASM benefits the broader security team

Common XSOAR Use Cases for Financial Services

In addition to the Cortex Xpanse content pack, XSOAR offers numerous automation playbooks that help SOC teams within the financial services industry maintain a strong security posture. Some of the most common use cases include:

- **Phishing response**: Phishing emails are pernicious, and one of the most frequent, easily executable, and harmful security attacks that organizations—regardless of size—still face today. Responding to a phishing email involves tasks that can easily take 30–45 minutes per incident. Automated phishing playbooks can help execute repeatable tasks at machine speed, identify false positives, and prime operations for standardized phishing responses at scale. More importantly, the quick identification and resolution of false positives gives more time to deal with genuine phishing attacks and prevents them from slipping through the cracks.
- **Zero-day threat response**: Zero-day threats and ransomware breaches are constantly in the news. As mentioned previously, financial organizations are prime targets when a new zero day is discovered.

  Automation can be an invaluable partner in helping you quickly remediate zero-day vulnerabilities before an incident, or it will help to quickly process, collect, and hunt for indicators, as well as perform quick-response actions upon discovery of indicators of compromise (IoCs). XSOAR provides specific rapid breach response playbooks for high-profile breaches to help you speed up your investigation efforts.
- **Cloud security alert response**: With Cortex XSOAR, you can automate the response to digital asset sprawl by ingesting cloud security alerts from Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure, or Prisma Cloud to fully or partially automate incident response using various cloud threat detection playbooks available in the marketplace.

  Other automation use cases include automating incident response for common cloud security incidents like password and security group misconfigurations, access key compromises, unpatched vulnerabilities, and unusual activity like port scans or port sweeps.
- **Remote user access**: With the new normal of remote work and many financial services moving to the cloud, these automation use cases can help streamline operations and help your IT Ops and security teams scale to address remote access security incidents and keep track of remote activity.

  Using automation playbooks, such as the Identity Lifecycle Management content pack or Okta's cloud-based identity management service integration, enables security teams to provision user access as well as play a role in aiding investigations into unsuccessful login attempts and other access violations, monitoring the health of VPNs, and updating dynamic allow/deny IP domain lists to ensure business continuity.
- **RDP**: Adversaries may connect to a remote system over RDP/RDS to expand access if the service is enabled and allows access to accounts with known credentials.

  Adversaries will likely use credential harvesting techniques to acquire credentials to use with RDP. By doing so, the adversaries may use valid accounts to log in to resources using RDP and then perform actions as the logged-on user. Using the intelligence-driven MITRE ATT&CK Courses of Action playbook within XSOAR, security teams are able to immediately handle and remediate the specific technique based on the phase in the attack lifecycle.

- **Vulnerability management**: Cortex XSOAR's orchestration playbooks can automate enrichment and context addition for vulnerabilities before handing off control to the appropriate teams for remediation. This maintains a balance between automated and manual processes by ensuring that analyst time is not spent executing repetitive tasks but on making critical decisions and drawing inferences.

  In addition to the Cortex Xpanse content pack, Cortex XSOAR includes additional playbooks to combat vulnerabilities that ingest asset and vulnerability information from a vulnerability management tool such as Tenable or Qualys. All the related information from the incident is extracted, and related indicators are created and enriched. Playbooks can also use vulnerabilities to inform threat priority and initiate the patching process.

Conclusion

As financial institutions continue to increase their use of and dependency on the internet, their attack surface grows proportionately. This further taxes their SOC analysts who must have an accurate inventory of internet-visible assets and then respond to corresponding alerts as well. Manual response to the high volume of cyber incidents is not scalable. However, with the integrated combination of attack surface management and SOAR, a financial institution's SOC is well-equipped to continuously monitor their entire attack surface and respond quickly with automation to newly discovered exposures.

For more information on the value of attack surface management and how the Cortex suite of products can help defend financial institutions against modern adversaries, please download these resources:

- Report: 2022 Cortex Xpanse Attack Surface Threat Report
- E-Brief: Value Drivers of ASM, Revealed
- Solution brief: Proactive Solutions to Financial Industry Security Operations Challenges
- Demo: See the Cortex Portfolio in action

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