Top 10 Ways to Automate Your SOC

Automate the Repetitive Things You Do Every Day to Ease Daily Life in SecOps

Are you spending too much time and effort on all of those "little tasks" in a SOC that can take hours out of your day?

Automating these repetitive, low-skill activities can free up valuable time so you can focus on the critical threats, and proactively refine your defenses against the next attack.

More importantly, automation can help in processing incidents and speeding response where time to react is of the essence.

Here are 10 ways you can automate repetitive tasks and streamline your security incident response processes for maximum efficiency. These are tried and tested automation use cases that have been leveraged by our own Palo Alto Networks SOC, ITOps, and our customers to gain operational efficiencies and scale.

1. 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 switching between multiple screens to coordinate response and respond to end users, and these tasks can easily take 30–45 minutes of your time per incident.

Automation "phishing playbooks" can help you execute repeatable tasks at machine speed, identify false positives, and prime your operations for standardized phishing responses at scale. More importantly, the quick identification and resolution of false positives gives you more time to deal with genuine phishing attacks and prevents them from slipping through the cracks. An advanced phishing response solution like Cortex XSOAR has machine learning intelligence built in, allowing you to "train" the phishing engine to recognize future phishing attacks.

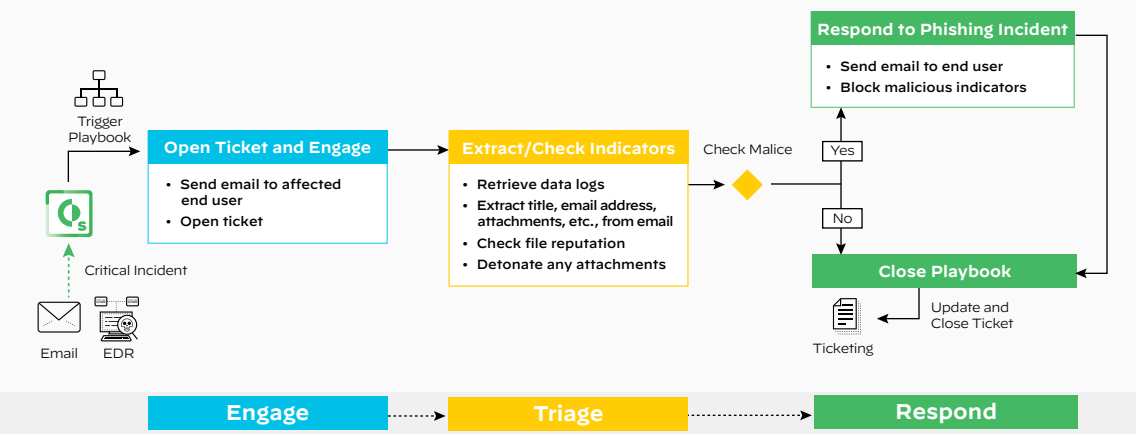

Figure 1: Workflow automating phishing response

Engage

A SOAR platform like Cortex XSOAR can ingest suspected phishing emails as incidents from a variety of detection sources such as SIEMs, EDRs, email security, or phishing services. If you aggregate all suspected phishing emails in a common mailbox, these emails can be ingested as incidents via a mail listener integration.

Once the email is ingested, a playbook is triggered, going through the steps to automate enrichment and response. To keep end users updated, the playbook sends an automated email to the affected user and lets them know that the suspected phishing email is being investigated.

Triage

In the triage process, the playbook can perform extraction and enrichment of indicators of compromise (IoC) extraction.

By looking at the "ingredients" of the email, such as title, email address, attachments, and so on, the playbook assigns incident severity by cross-referencing these details against external threat databases. Following this, the playbook extracts IoCs from the email and checks for any reputational red flags from threat intelligence tools that your team uses.

Once this enrichment is done, the playbook checks if any malicious indicators were found. Based on this check, different branches of response can ensue.

Respond

Different branches of the playbook will execute depending on whether malicious indicators were detected in the suspected phishing email.

If malicious indicators were detected, the playbook sends an email to the affected user with further instructions. The playbook also scans all organizational mailboxes/endpoints to identify other instances of that email and delete all instances to avoid further damage. Finally, the playbook adds the malicious IoCs to block lists/watchlists on the SOC's other tools.

If no malicious indicators are detected, there are still precautions to be taken before confirming that the email is harmless. The playbook checks if there are any attachments in the email that can be sent for detonation in a sandbox. Threat intel analyses are then presented in an incident war room for the analyst to do a final check. Once the analyst is satisfied that the email isn't malicious, the playbook sends an email to the affected user apprising them of the false alarm. The incident ticket is marked closed.

The result? You easily eliminate 10 or more steps that your security team has to touch, saving them hours responding to phishing alerts.

"Of the 730 phishing alerts a week, we were able to auto-close 430 of these using XSOAR. We estimate this saves us around four analyst days a week"

– US insurance company

2. Malware Investigation and Response

Determining if alerts for unknown activity from your endpoint security tools are malicious often involves coordinating between multiple security tools. It's a cross-referencing nightmare with multiple consoles open simultaneously and valuable time spent performing repetitive data collection tasks. Decreasing the investigation and response time means less dwell time for malicious activity to wreak havoc in your network.

Automation playbooks can unify processes across SIEMs and endpoint tools in a single workflow, performing repetitive steps before bringing analysts in for important decision-making and investigative activities.

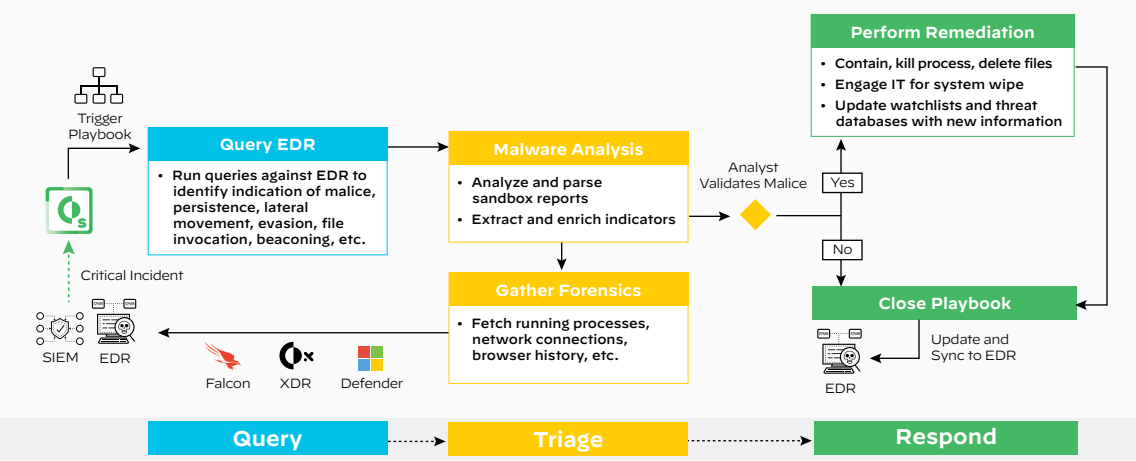

Figure 2: Workflow automating malware investigation and response

Query

An incoming endpoint security alert triggers a series of playbooks that automatically query for evidence of malice, such as:

- Is there evidence of attempted lateral movement?
- Is there evidence of persistence?
  - » Did the process create any scheduled jobs?
  - » Did it write to the registry?
  - » Was autorun updated?
- Is the file digitally signed?
- How did the file get on the machine?
- What is the process execution chain?
- Does the process appear to be beaconing?
- Has the file executed PowerShell?
- Are there any known abuse points in the process chain?
- What triggered the execution of the file?
- Was the network traffic blocked at the firewall?
- Did the file delete itself?

The findings are presented via an incident dashboard for analyst review, eliminating the need to manually collect and piece the evidence together.

Triage

Detonating suspicious files in sandboxes for malware analysis is an ever-present and important investigative step during incident response. However, it's taxing for security analysts to coordinate across consoles while executing this repetitive task because malware analysis tools are isolated from other security products. Transferring results from one console to another for documentation is also time-consuming and increases the chances of error.

In this scenario, playbooks can be run concurrently to automate the entire file detonation process either as an isolated workflow or in concert with other enrichment activities. Playbooks can parse through the results of the sandbox detonation and be configured to run specific queries against the EDR tool. Since playbooks document the result of all actions on a central console, the need for manual post-incident documentation is also eliminated.

Another aspect of malware analysis involves gathering forensics data, such as all the processes running on a machine. This, too, can be automated. During an investigation, it can be critical to understand what is happening on the endpoint at the time the alert is detected. Sometimes it can be minutes or even hours before an analyst looks at a detected alert, at which point the state of the endpoint is likely different, which makes the re-creation of what happened more challenging. These playbooks can communicate continuously with the same endpoint tools to run queries on processes, network connections, browser history, etc. to track incident status.

Respond

If the file is malicious, the playbook updates relevant watchlists/block lists with that information. From here, the playbook can branch into other actions such as quarantining infected endpoints, killing malicious processes, removing infected files, opening tickets, and reconciling data from other third-party threat feeds.

After the queries have been run, the playbook updates the endpoint tool database with new indicator information, so repeat offenses are eliminated.

3. Zero-Day Threat Response

Zero-day threats and ransomware breaches are constantly in the news: SolarWinds SUNBURST, HAFNIUM Microsoft zero-day exploit, Nobelium threat actor, Kaseya supply chain ransomware attack, Log4j vulnerability, and the list goes on.

Every time a critical vulnerability is reported, it's an all-hands-on-deck effort to ensure that your organization is not exposed to the potential exploits of the vulnerability. Your executive team likely has heard it in the news and needs an assessment of exposure for the organization. Speed is of the essence here if potential malicious activity is detected.

Automation can be a helpful partner in helping you quickly process, collect, and hunt for indicators, as well as performing quick response actions upon discovery of said IoCs.

> **"Implementing the automations in this malware pack will easily save me 2–3 days of analyst time per month."**
>
> – Financial services SOC leader

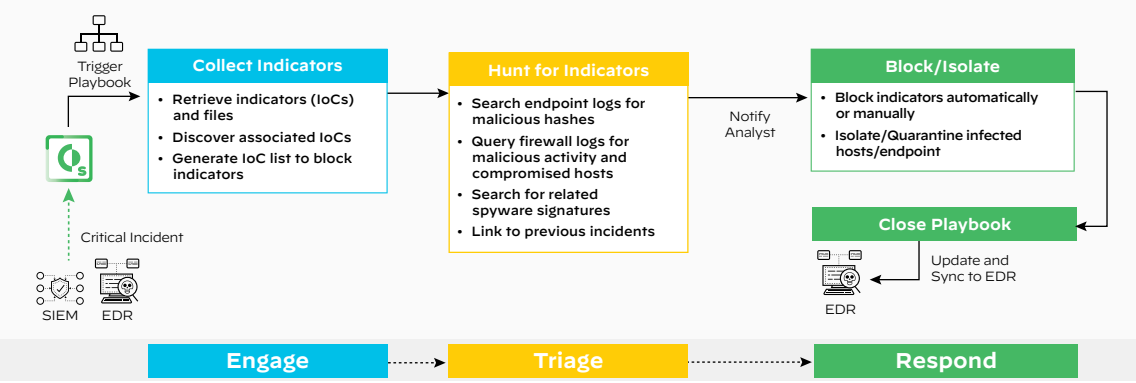

Figure 3: Workflow automating zero-day threat response

Engage & Triage

In the case of a breach alert, the process of retrieving and discovering associated IoCs is as repetitive as it is important. Your analysts risk getting mired in this grunt work while the attack continues to manifest. Secondly, isolated security tools result in a struggle to reconcile threat data across platforms to get an overall understanding of malicious activity and spread.

By running this playbook at the outset of incident response, your team can query endpoints, firewalls, and other incidents in seconds, avoiding wasted time that can be used towards locking down defenses.

Respond

The playbook executes initial response actions based on indicator malice. For instance, the playbook can block indicators, isolate, or quarantine infected hosts, or feed malicious indicators back into threat intelligence databases and tool watchlists to avoid future attacks using the same indicators.

We provide specific rapid breach response playbooks for high-profile breaches to help you speed up your investigation efforts.

4. Remote User Access Provisioning

Remote work has become the norm, and your business is increasingly moving to the cloud. This has increased the threat exposure and attack surface your team has to account for.

Automation can play a role in many areas, including 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.

Failed User Logins

Despite the increased sophistication of security measures you have implemented, it's possible for attackers to brute-force their way into accounts by obtaining the email address and resetting the password. This behavior is tricky to preempt because there are high chances of it being innocuous (a genuine employee resetting their password). Constant communication between you and end users to separate the anomalies from the usual is critical.

At user-defined triggers (such as five failed login attempts), a playbook can execute and verify whether the case is genuine or malicious.

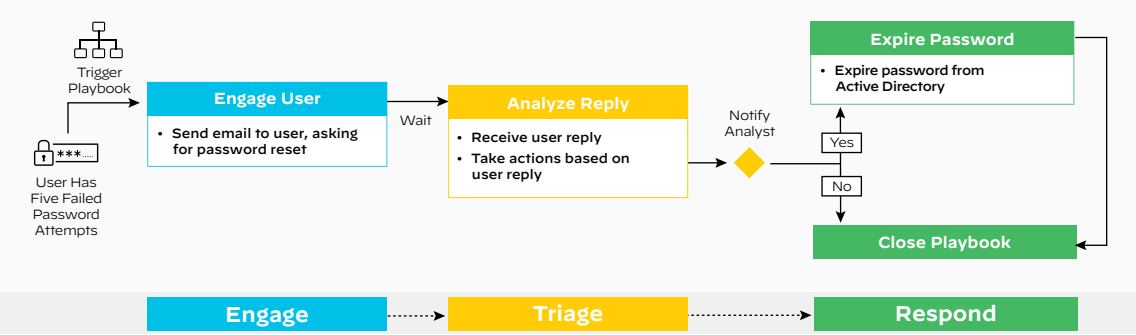

Figure 4: Workflow automating multiple failed logins alert response

Engage

The playbook sends an automated email to the affected user, notifying them of the five failed login attempts and asking them to confirm that the behavior was indeed theirs. The email requests the user to reply with "Yes/No," and spells out the ensuing action for each response.

Analyze

Some orchestration platforms can analyze the replies to automated emails and accordingly execute different playbook branches.

Respond

If the end-user behavior was genuine, the playbook resets the password on Active Directory and sends a new email to the affected user with revised login credentials.

If the end user confirms that they were not the ones making the failed login attempts, the playbook sends a new email notifying them of these account takeover attempts. The playbook can also execute investigative actions, such as extracting the IP/location where the failed attempts were made from, quarantining the affected endpoint, and so on.

Logins from Unusual Locations

With remote work and the ability to work from anywhere, it's tough to spot a malicious access attempt from a genuine case of employee access from multiple geographical locations. Moreover, with increased cloud adoption, there are multiple sources of geographical presence to verify, heaping more work on your security team and presenting a window of opportunity to attackers.

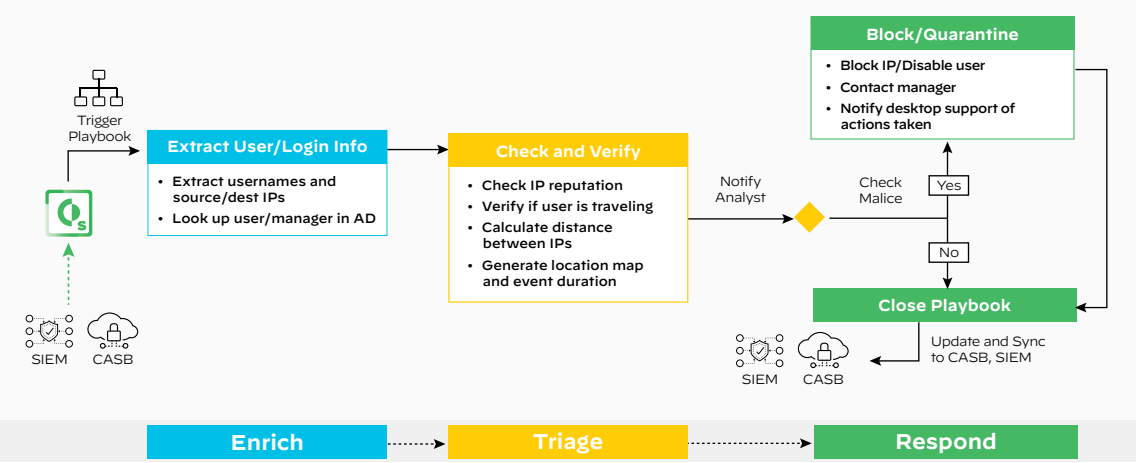

Figure 5: Workflow automating suspicious login activity response

Take, for instance, the case of "impossible travel," where two logins from two different locations at the same time are flagged by the playbook and trigger action. In this case, a modified version of the failed user login playbook would include enriching IP information by checking the reputations of the IP addresses using threat intelligence sources and calculating the distance between IPs, generating a location map and login time duration.

Once the analyst deems that this activity is malicious, the playbook then executes a series of containment steps, such as disabling user accounts, blocking malicious IPs at the firewall, and notifying IT Support of actions taken.

Enforcing Multifactor Authentication

Multifactor authentication (MFA) is often required when end users connect from untrusted or unknown IPs. Trusted network IPs are defined in identity and access management (IAM) systems like Okta, so users connecting from a trusted network such as HQ or branch offices do not need MFA, but if they connect from a coffee shop, they would be required to authenticate with MFA.

However, in SASE solutions such as Prisma Access, due to auto scaling or provisioning of new locations, the list of assigned IPs for an enterprise often changes. So, if these egress IPs are not listed or added to their IAM, any user connecting to these new IPs to access their software-as-a-service (SaaS) applications, even if they are on a trusted network, will be required to use MFA. This can result in an inconsistent end-user experience.

With the integration between Cortex XSOAR and Prisma Access, an automated playbook can "listen" to auto scaling and new provisioning events, immediately pick up the new list of Prisma Access egress IPs, and automatically update the IAM. This provides a seamless login experience for users connecting from a trusted network.

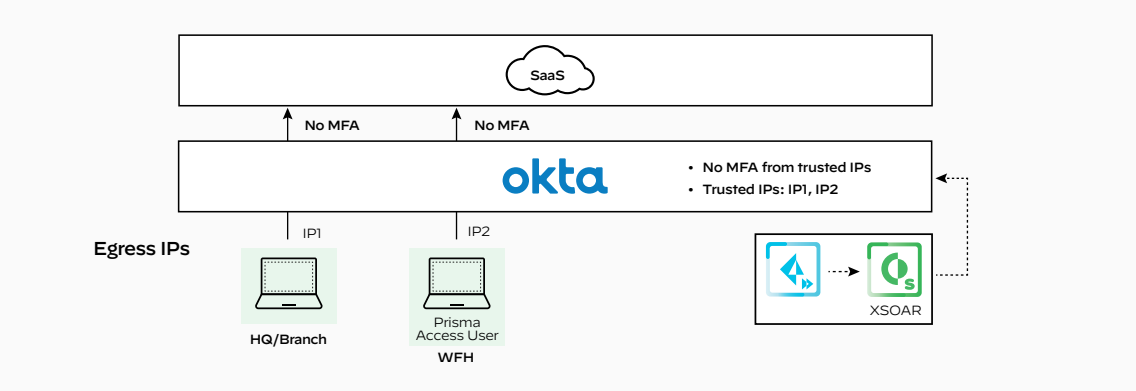

Figure 6: Enforcing multifactor authentication

Monitoring VPN Tunnel Health

In a security team's busy day, there is no time to proactively monitor for potential connectivity downtime as the staff is usually busy firefighting and triaging critical incidents. Among other things, this makes it difficult to keep track of the health status of all VPN tunnels to ensure 100% uptime for end users.

In this case, an automated VPN tunnel monitoring playbook can be scheduled to poll Prisma Access connection statuses on a regular basis and send a Slack alert to the security or ITOps team if a tunnel is down.

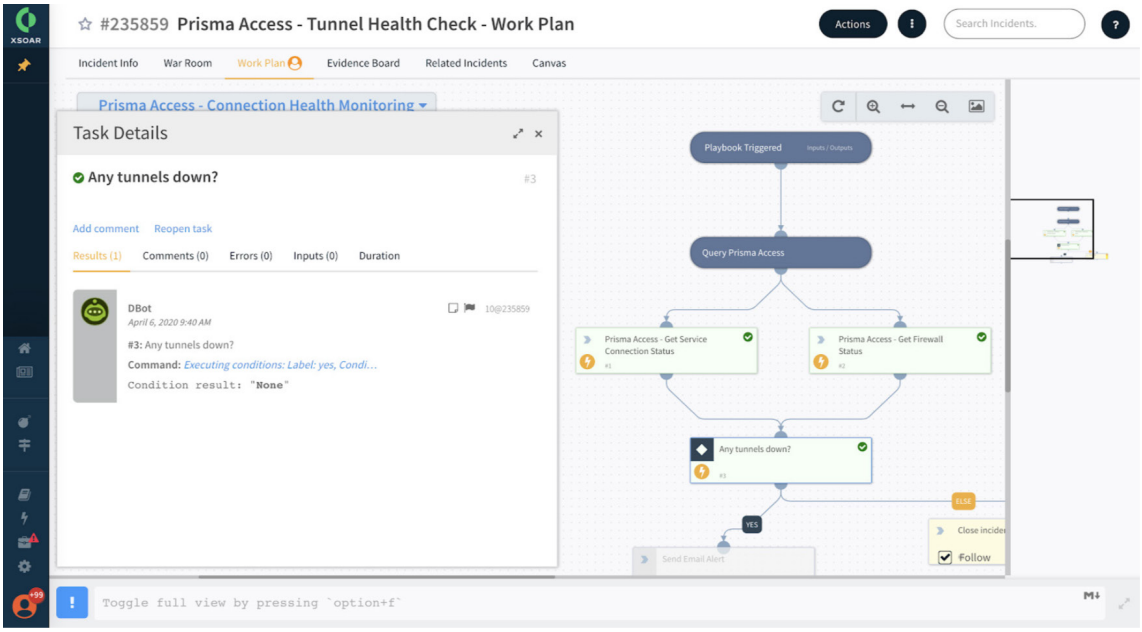

Figure 7: Monitoring VPN tunnel status

With the new normal of remote work, these automation use cases can help streamline operations and help your ITOps and security teams scale to address remote access security incidents and keep track of remote activity.

5. Threat Intelligence Management

If you think about it, integrating threat feeds into a SOAR makes perfect sense. As you ingest alerts, you can automatically enrich them with the latest threat intel from your feeds. This now gives you context for how external and emerging threats are impacting your environment and also helps you quickly home in on critical threats.

Proactive Blocking of Threats

The indicators collected from many different threat feeds need to be aggregated, normalized, scored, and prioritized before they can be pushed to enforcement points. A threat intel platform can automate all of these feed management functions, ensuring that your external dynamic lists (EDLs) are always up to date per the latest threats.

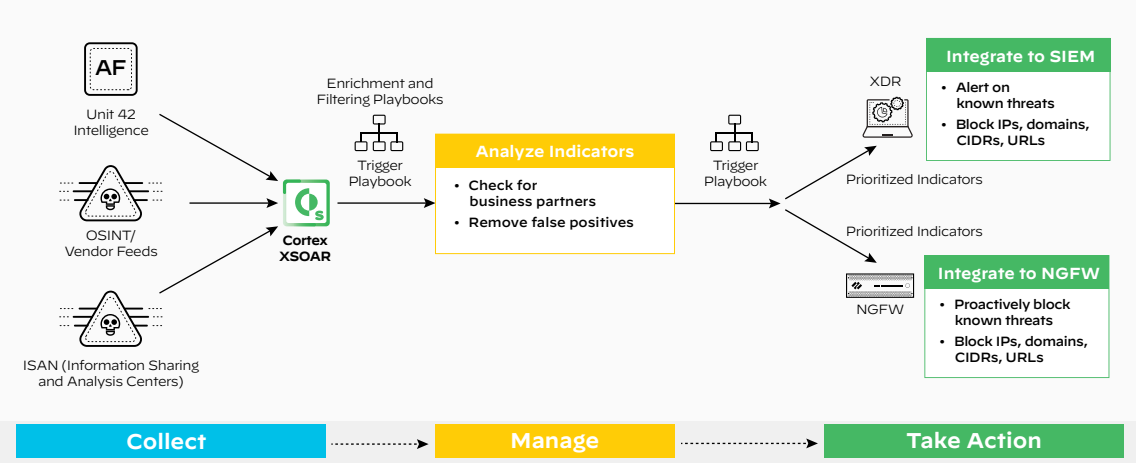

Figure 8: Threat intel management—proactive blocking of threats

Continuous Incident Enrichment

Oftentimes, as you investigate incidents, you need threat intel context on associated indicators. Curated threat intelligence, such as those from the Palo Alto Networks Unit 42 threat research that comes packaged with the XSOAR Threat Intel Management (TIM) module, helps you automate indicator enrichment, giving your analysts early warning and rich context into emerging threats in the wild that might be impacting your network.

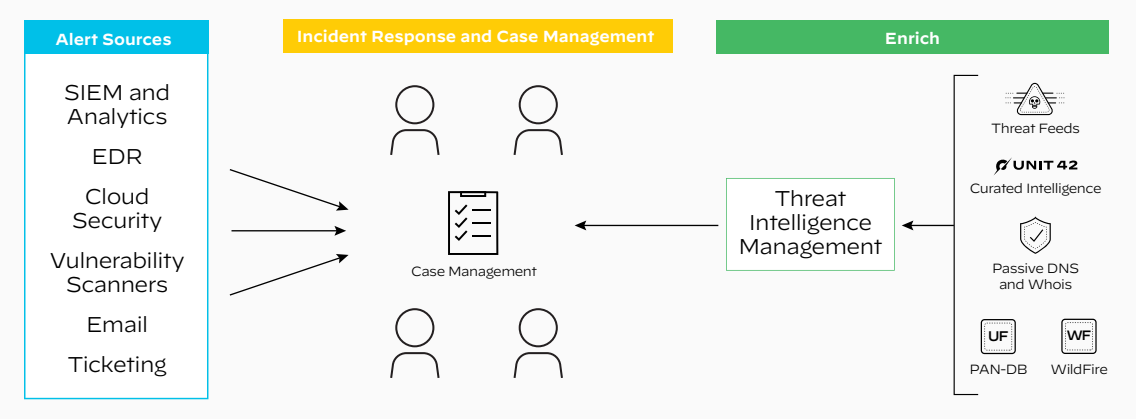

Figure 9: Threat intel management—automated incident enrichment

Generating Weekly OSINT (Open Source Intelligence) and Other Threat Reports

Your threat intel team is charged with producing and disseminating threat intelligence reports to various business units/stakeholders to keep them up to date on the latest threats targeting their industry. Most intelligence is still shared via unstructured formats such as email, blogs, etc., so your threat analysts may go through hours of manual work aggregating and digging for known malware families, curated news, and industry-specific threats, as well as providing analyses on why each threat is relevant to the business. Cortex XSOAR TIM provides automated workflows and a central repository for intelligence analysts to create, collaborate, and share curated intelligence reports with stakeholders.

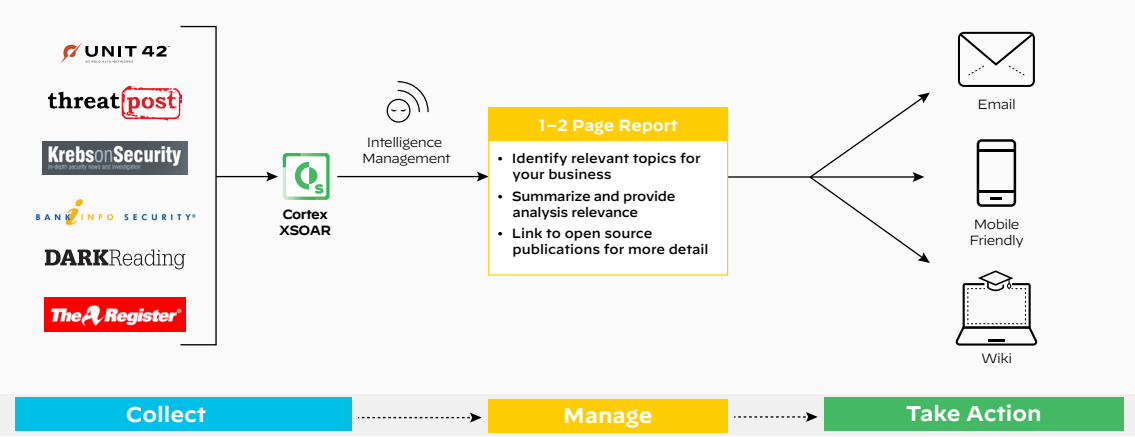

Figure 10: Automated threat feed curation

External Threat Landscape Modeling

Threat intelligence teams need to understand the details of attacks and how their organizations may be vulnerable. The intel team builds profiles of threat actors, identifying if there are related attacks and which techniques and tools the threat actor used. This information is shared with stakeholders, including security operations and leadership.

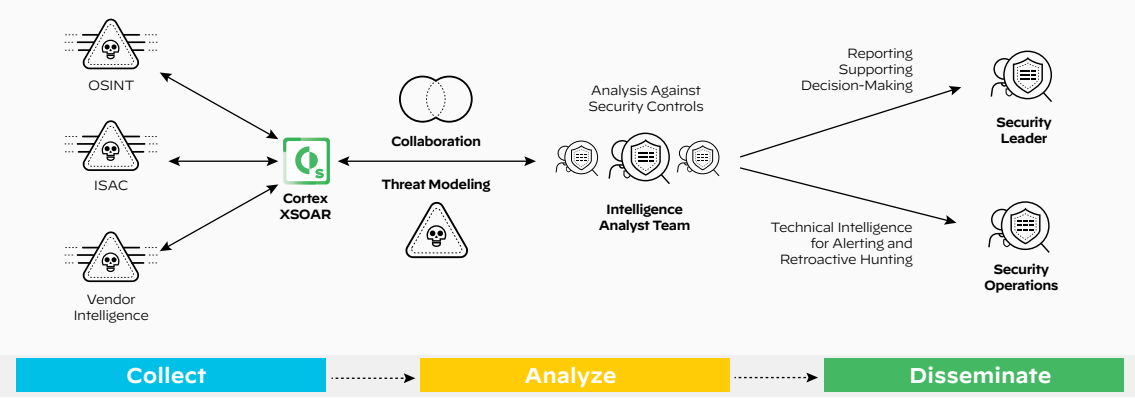

Figure 11: Threat intel management—external threat modeling

For more information on how you can better manage your threat feeds, check out this whitepaper.

6. Cloud Security Incident Response

In the world of cloud security, there are lots of infrastructures and products to deal with. The security of your cloud is often a shared responsibility between you, your cloud service provider, and other teams. From conversations with cloud SecOps teams, we've seen that cloud security incidents are treated on a case-by-case basis, and the remediation process is high-touch and manual. There is often no correlation between cloud platforms or on-premises security.

Cortex XSOAR can unify processes across multicloud and on-premises security infrastructures, providing your security teams with a single console from which to execute incident response. We also integrate with cloud-based identity management tools, enabling role-based and keyless deployment of services without the need for credential management.

Cloud Threat Detection

With the move towards digital currency and acceptance of cryptocurrency for financial transactions, cryptojacking is probably not going to wane anytime soon.

In this example, we will cover how you might automate response to a cryptomining alert. Cortex XSOAR can ingest cloud security alerts from AWS, Google Cloud, Microsoft Azure, or Prisma Cloud to fully or partially automate incident response.

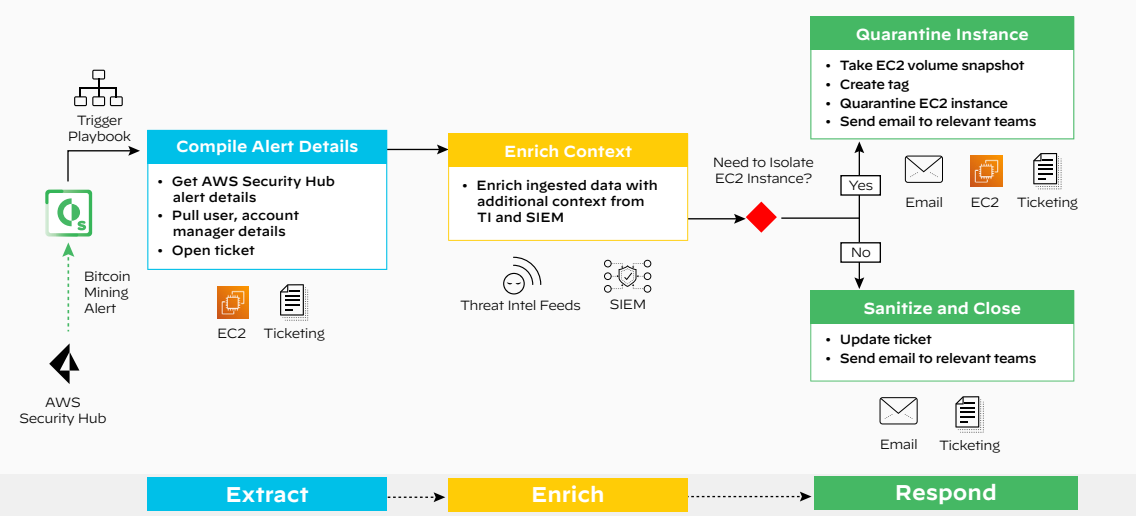

Figure 12: Automating cloud security alert response

Extract

The playbook extracts indicators (IPs, URLs, hashes, and so on) from the incident data. It can also open a ticket for the incident.

Enrich

The playbook enriches indicators with reputation data from threat intelligence tools that the SOC uses. It also enriches the ingested data with additional context from SIEMs and other non-cloud-based event management tools to identify the full extent of the suspected attack. The playbook checks if the indicators are identified as malicious.

Respond

If they are, the playbook gets the instance details, security group details, takes volume snapshots, and creates a tag for the EC2 instance to be isolated. These steps are classic digital incident response and forensics actions but done in the cloud. What we are doing is moving the EC2 instance into a separate virtual PC (VPC) as we would on a virtual LAN (VLAN) in the on-premises world, getting a list of running processes, analyzing the results, and also sending an email to the analyst for review.

If the indicators are not identified as malicious, the playbook brings in a security analyst to review the information and verify that it's not dangerous before closing the incident as a false positive.

Considering that each of these tasks in the playbook would have been a manual action requiring a lot of coordination between teams as well as changes on different security products, automation not only saves analyst hours but also speeds up response.

An additional benefit here with automation is that you can enforce standard operating procedures across different teams for cloud security incident response.

This is just one example of how you can automate cloud security incident response. 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/port sweeps. Check out more automation packs in the Cortex Marketplace.

7. Vulnerability Management

Vulnerability management is a strategically important process that covers both the proactive and reactive aspects of security operations. Since vulnerability management encompasses all computing and internet-facing assets, security teams often grapple unsuccessfully with correlating data across environments, spending too much time unifying context and not enough time remediating the vulnerability.

Security orchestration playbooks can automate enrichment and context addition for vulnerabilities before handing off control to the appropriate teams for patch 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.

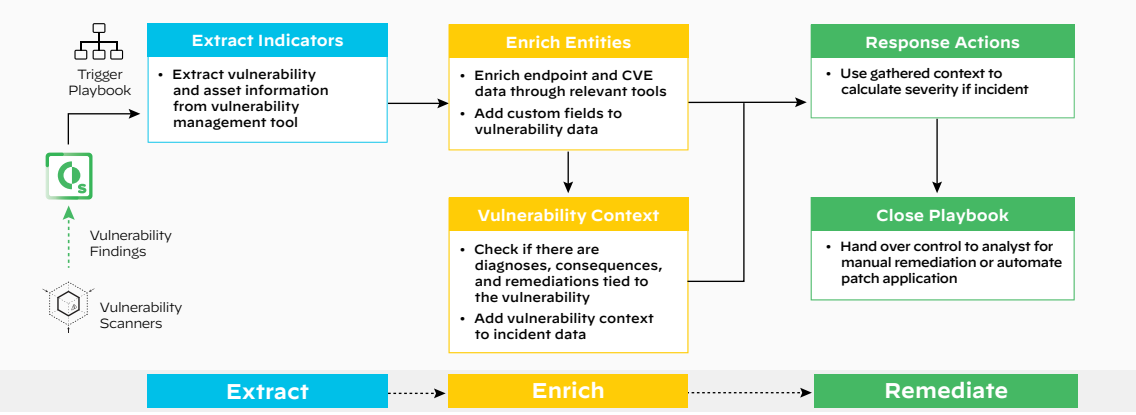

Figure 13: Automated vulnerability remediation workflow

Extract

The playbook ingests 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.

The playbook then enriches endpoint and CVE data through relevant tools. It also adds custom fields to the incident if the newly gathered data requires them.

To provide the analyst with a richer vulnerability context, the playbook queries the vulnerability management tool for any diagnoses, consequences, and remediations tied to the vulnerability. If any vulnerability context is found, it's added to the incident data. Based on the gathered context, the playbook then calculates the severity of the incident.

Remediate

Playbooks can also use vulnerabilities to inform threat priority and initiate the patching process. Response actions can be taken by playbooks, including:

- Checking if assets (IP, domain, or certificate) associated with the issue are excluded in the exclusions list and closing the incident automatically.
- Enriching indicators and calculating the severity of the issue.
- Adding associated assets (IP, domain, or certificate) to the exclusions list.
- Tagging associated assets and updating the status of the issue.

The playbook now hands over control to the security analyst for manual investigation and remediation of the vulnerability.

8. Attack Surface Management

Vulnerability scanners are great for monitoring your known assets, but what about your unknown assets? To uncover these blind spots, your organization needs an automated attack surface management (ASM) solution like Cortex Xpanse that continuously discovers and monitors the entirety of IPv4 space to provide a complete and accurate inventory of your global internet-facing assets and misconfigurations.

Together with XSOAR, Xpanse enables you to automate the identification and remediation of web-facing exposures to reduce your mean time to detect and respond (MTTD and MTTR).

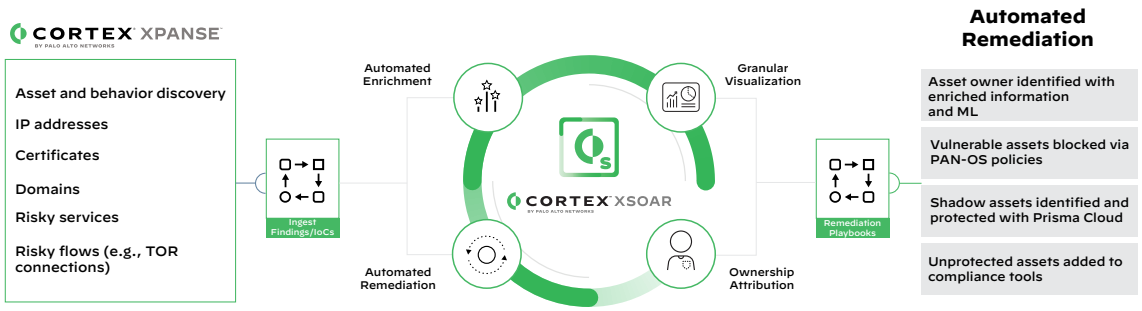

Figure 14: Automate attack surface remediation with Cortex XSOAR and Cortex Xpanse

The integration enables the fetching and mirroring of Xpanse issues into XSOAR incidents as well as the ingestion of indicators (IPs, domains, and certificates), referring to the corporate network perimeter as discovered by Xpanse. Leveraging both technologies, your security team will be able to respond to asset vulnerabilities and incidents with automated orchestration playbooks. You can trigger scans to enrich incidents and automatically generate tickets for on-premises and cloud assets.

Discover

Scan the internet and accurately attribute unknown assets using multiple sources to reduce false positives and map your full attack surface.

Enrich

Use automated playbooks to enrich incidents using Xpanse asset information and threat intelligence indicators, helping you reduce MTTD and MTTR across your cloud native, hybrid, and on-premises environments.

Remediate

Improve your team's efficiency with a host of integrations and prebuilt scripts to automate attack surface management.

For more details, check out our Xpanse automation pack in the Cortex Marketplace.

9. MITRE ATT&CK Mapping

The MITRE ATT&CK framework was created to organize the real-world industry observations of threat actors into a standardized language of tactics, techniques, and procedures (TTPs) to help organizations share information and recommendations which can be used to harden security programs.

Given the breadth and depth of the framework, understanding, consuming, and mapping the tactics and techniques within the MITRE ATT&CK framework into reliable and usable remediation steps can be a complicated and time-consuming task.

Our next set of playbooks in the MITRE ATT&CK Courses of Action content pack helps you automatically map your incident response to MITRE ATT&CK techniques and sub-techniques in an organized and automated manner. This will make sure your organization not only blocks specific reported IoCs but

also takes a more holistic approach to preventing future attacks. With a SOAR solution like Cortex XSOAR, you can leverage prebuilt automation playbooks to cross reference every incident with the tactics and techniques of the MITRE ATT&CK framework.

This pack provides both manual or automated remediation of MITRE ATT&CK techniques and kill chain. The security analyst simply needs to choose the techniques that are relevant to their security program and run the prebuilt playbooks that leverage expert remediation workflows. This can be found in the built-in XSOAR MITRE ATT&CK dashboard (as seen in figure 15).

When used with Unit 42's feed ingesting Actionable Threat Objects and Mitigations (ATOMs), your team gets notified as soon as there is a new threat actor report, with recommendations for immediate remediation action.

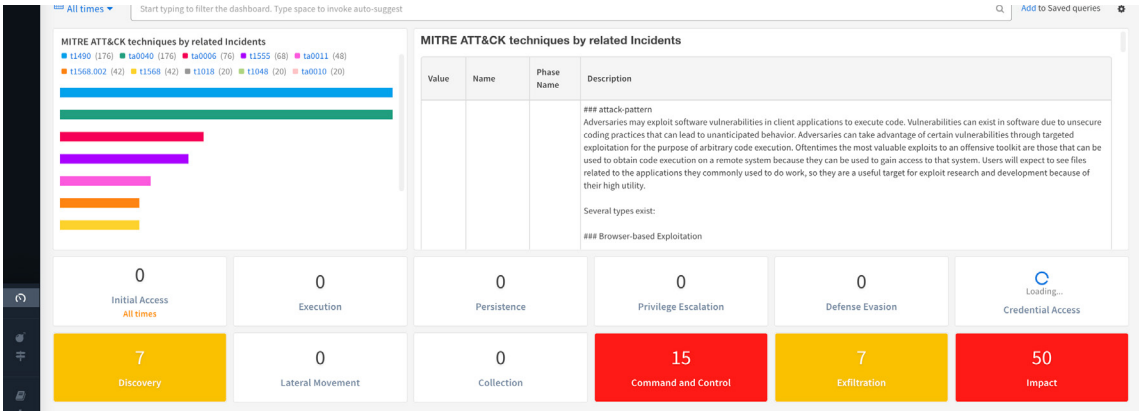

Figure 15: Dashboard for easy visualization of MITRE ATT&CK to incident mappings

This allows your security team to apply industry threat response protocols and best practices to block specific reported IoCs and take a more holistic approach to prevent future attacks.

10. Network Operations Automation

For this final use case, we will pivot from the SOC to the NOC. A flexible and scalable SOAR platform can be applied to any workflow or process, and our own Palo Alto Networks operations teams are using Cortex XSOAR internally for automating their manual processes.

One area where we have seen great benefits is network operations, where manual but necessary tasks are a time burden for the ITOps and NetOps teams.

Manual Firewall Device Onboarding and Upgrades

It's a tedious and manual process to upgrade and validate all firewalls distributed across your network. There is significant time investment needed in the process where your team needs to download the firewall update, install, reboot, and verify that the upgrade was successful. For enterprises with over 100 firewalls distributed across their organization, this process is not scalable and is done infrequently.

> *"We manage about 450 firewalls. It takes us two hours to upgrade each firewall. We can only do a few at a time to ensure everything upgrades correctly." – Insurance industry customer*

With Cortex XSOAR, you can onboard and upgrade all your devices within the environment and automatically verify upgrade status. There is still time required to download and reboot the system, but your NetOps team no longer has to "babysit" the process. Snapshots of the configuration can be captured to enable rollbacks if necessary. Once the upgrade is complete, verification steps can be performed to ensure the firewall is functioning properly.

There are many more automation use cases that can be deployed to streamline network operations, from policy and rule change management to monitoring network health and outages, but your NetOps teams will derive great efficiency benefits just from starting their automation journey with this key use case.

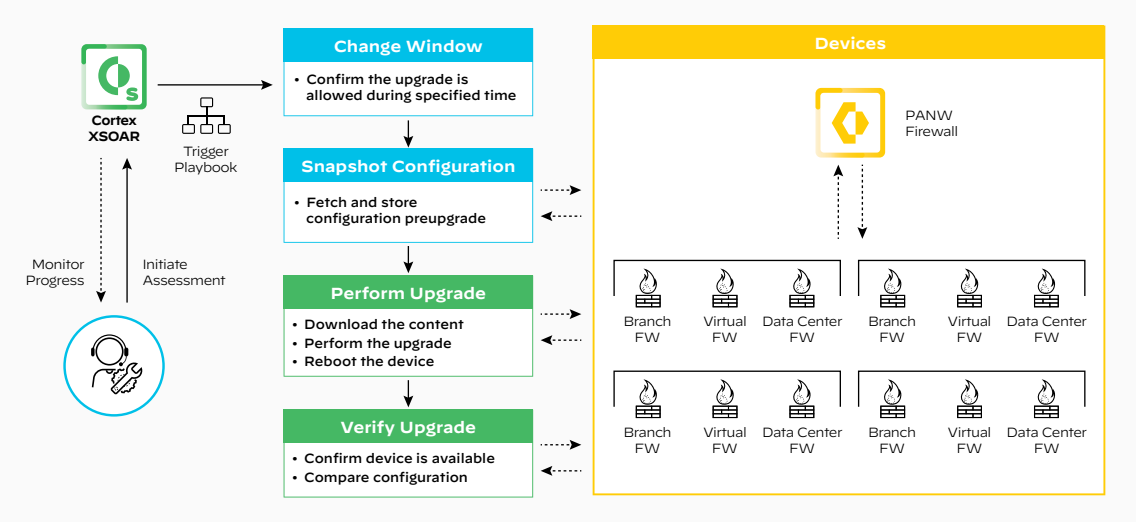

Figure 16: Automated firewall upgrade workflow

How Automation Makes Life Easier in the SOC (and NOC)

- **Accelerate incident response**: By replacing low-level manual tasks with corresponding automations, security automation can shave off large chunks from incident response times while also improving accuracy and analyst satisfaction.
- **Standardize and scale processes**: Through stepwise, replicable workflows, security automation can help standardize incident enrichment and response processes that increase the baseline quality of response and is primed for scale.
- **Unify security infrastructures**: A SOAR platform like Cortex XSOAR can act as a connective fabric that runs through hitherto disparate security products, providing analysts with a central console from which to action incident response.
- **Increase analyst productivity**: Since low-level tasks are automated, and processes are standardized, analysts can spend their time in more important decision-making and charting future security improvements rather than getting mired in grunt work.
- **Leverage existing investments**: By automating repeatable actions and minimizing console switching, security orchestration enables teams to coordinate among multiple products easily and extract more value out of existing security investments.
- **Streamline incident handling**: By applying automation to incident ticket management via integrations with key ITSM vendors such as ServiceNow, Jira, and Remedy, as well as communication tools such as Slack, security teams can speed incident handling and closure. Incidents can also be distributed automatically to the respective stakeholders based on predefined incident types.
- **Improve overall security posture**: The sum of all aforementioned benefits is an overall improvement of the organization's security posture and a corresponding reduction in security and business risk.

Terms to Know

- **Playbooks**: Playbooks (or runbooks) are task-based graphic workflows that help visualize processes across security products. These playbooks can be fully automated, fully manual, or anywhere in between.
- **Integrations**: Product integrations (or apps) are mechanisms through which security orchestration platforms communicate with other products. These integrations can be executed through REST APIs, webhooks, and other techniques. An integration can be unidirectional or bidirectional, with the latter allowing both products to execute cross-console actions.
- **Content packs**: Cortex XSOAR content packs are prebuilt bundles of integrations, playbooks, dashboards, fields, subscription services, and all the dependencies needed to support specific security automation use cases. These content packs are available for download via the Cortex Marketplace.

To learn more about these automation use cases, as well as hundreds more, you can download our Cortex XSOAR free Community Edition.

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