Top Security Orchestration Use Cases

Table of Contents

Security Orchestration Overview 3
Security Alert Handling 4
- Phishing Enrichment and Response 4
- Endpoint Malware Infection 5
- Failed User Logins 6
- Logins from Unusual Locations 7

Security Operations Management 8
- SSL Certificate Management 8
- Endpoint Diagnostics and Kickstart 9
- Vulnerability Management 10

Threat Hunting and Incident Response 11
- Rapid IOC Hunting 11
- Malware Analysis 12
- Cloud-Aware Incident Response 13

Versatile Security Automation 14
- IOC Enrichment 14
- Assigning Incident Severity 15

Security Orchestration Overview

What Is Security Orchestration?

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

The three pillars of security orchestration are people, processes, and technology. By streamlining security processes, connecting different security tools and technologies, and maintaining the right balance of machine-powered security automation and human intervention, security orchestration empowers security professionals to improve the organization's overall security posture.

Why Is It Needed?

A combination of industry trends and market forces have created challenges that security orchestration is perfectly positioned to solve:

- **Rising alert numbers:** With an increased threat surface, a greater number of entry vectors for attackers, and an increase in specialized cybersecurity tools, the number of alerts is constantly on the rise. Analysts need help in identifying false positives, duplicate incidents, and keeping the alert numbers in check without burning out.
- **Product proliferation:** Analysts use numerous tools – both within and outside the purview of security – to coordinate and action their response to incidents. This involves lots of screen switching, fragmented information, and disjointed record keeping.
- **Lack of skilled analysts:** With a shortage of millions of analysts expected over the coming years, many security operations Centers (SOCs) are understaffed, leading to increased workload, stress, and rates of error among staffed analysts.
- **Inconsistent response processes:** As SOCs mature, security teams spend most of their day fighting fires and can't devote enough time to set standard response processes or spot patterns that reduce rework. This results in response quality being dependent on individual analysts, which can lead to variance in quality and effectiveness.

How Does It Help?

Figure 1: Benefits of security orchestration

Terms to Know

Playbooks

Playbooks (or runbooks) are task-based graphical 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.

Let's look at some use cases where security orchestration's capabilities can help simplify, automate, and improve efficiencies of incident response and security operations.

Security Alert Handling

Phishing Enrichment and Response

Current Drawbacks

Phishing emails are among the most frequent, easily executable, and harmful cyberattacks that organizations—regardless of size—face today. With more than 90% of all data breaches starting with a phishing email, the potential for financial damage is real and immediate.

Security analysts face numerous challenges while responding to phishing attacks. Handling attack numbers without burning out, switching between multiple screens to coordinate response, avoiding errors while completing mundane tasks, and standardizing response and reporting procedures are all sources of worry.

How Orchestration Helps

Security orchestration platforms can use "phishing playbooks" that execute repeatable tasks at machine speed, identify false positives, and prime the SOC for standardized phishing response at scale. Importantly, the quick identification and resolution of false positives provides analysts more time to deal with genuine phishing attacks and prevents them from slipping through the cracks.

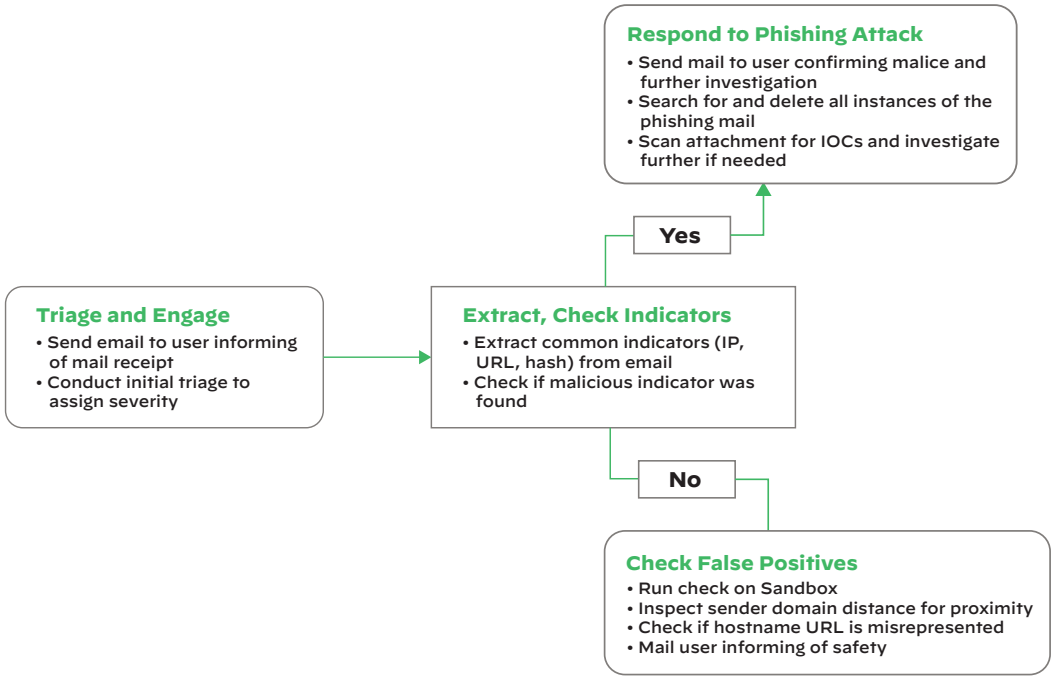

Figure 2: Phishing playbook

Ingestion

An orchestration platform can ingest suspected phishing emails as incidents from a variety of detection sources such as security information and event management (SIEMS) systems and logging services. If the SOC aggregates all suspected phishing mails in a common mailbox, then a mail listener integration can be configured on the orchestration platform for ingestion.

Once the email is ingested, a playbook is triggered and goes through steps to automate enrichment and response.

Enrichment

To keep the end users updated, the playbook sends an automated email to the affected user and let them know that the suspected phishing email is being investigated. The two key steps that the playbook can perform for enrichment are **triage** and **indicator 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 out IOCs from the email and checks for any reputational red flags from existing threat intelligence tools that the SOC 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.

Response

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 blacklists/watchlists on the SOC's other tools.

If malicious indicators were not detected, there are still precautions to be taken before confirming that the email is harmless. The playbook checks if there are any attachments with the email and detonate them in a sandbox for further analysis. If that analysis doesn't throw up any alarms, the playbook can give way to analysts for qualitative and manual investigation. Once the analysts are satisfied that the email isn't malicious, the playbook sends an email to the affected user apprising them of the false alarm.

Endpoint Malware Infection

Current Drawbacks

Endpoint protection is a critical part of incident response but is unfortunately beset by implementation challenges. Security teams often have to coordinate between endpoint tools and other security tools, having multiple consoles open simultaneously and spending valuable time performing repetitive manual tasks. SOCs sometimes use multiple endpoint-focused tools as well, making it difficult to cross-reference data between them.

How Orchestration Helps

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

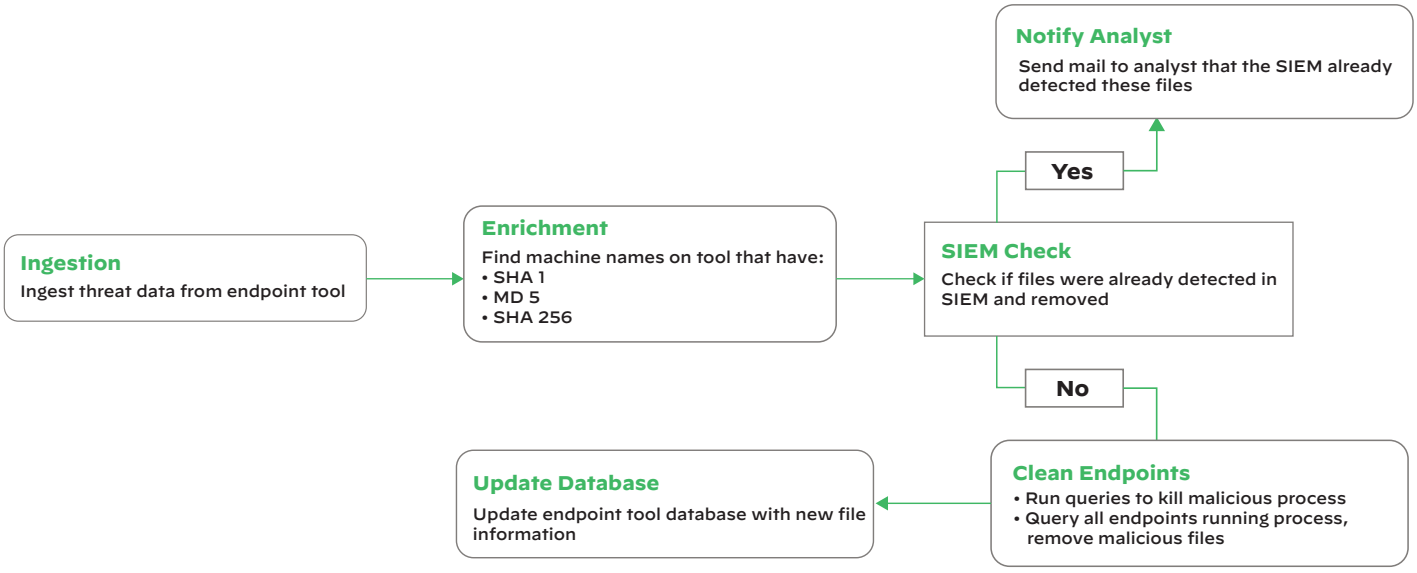

Figure 3: Endpoint malware infection playbook

Ingestion

The playbook ingests threat feed data from an endpoint tool (e.g., CrowdStrike Streaming).

Enrichment

The playbook queries the endpoint tool for machine/endpoint names that have malicious indicators such as SHA1, MD5, SHA256, among others.

Cross-Reference with SIEM Data

The playbook then cross-references these retrieved files/hashes with SIEM data and verifies whether any indicators were picked up and resolved by SIEM-led actions. It notifies the analyst if SIEM-led actions have already resolved any malicious indicators.

Clean Endpoints

For any indicators that have not been picked up by the SIEM, the playbook communicates with either the same endpoint tool or a different one (like Tanium) to run queries across endpoints. These queries can kill all malicious processes, remove infected files, and more, depending upon endpoint tool capabilities.

Update Database

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

Failed User Logins

Current Drawbacks

Despite the increased sophistication of security measures present today, 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 end users and SOCs to separate the anomalies from the usual is critical.

How Orchestration Helps

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

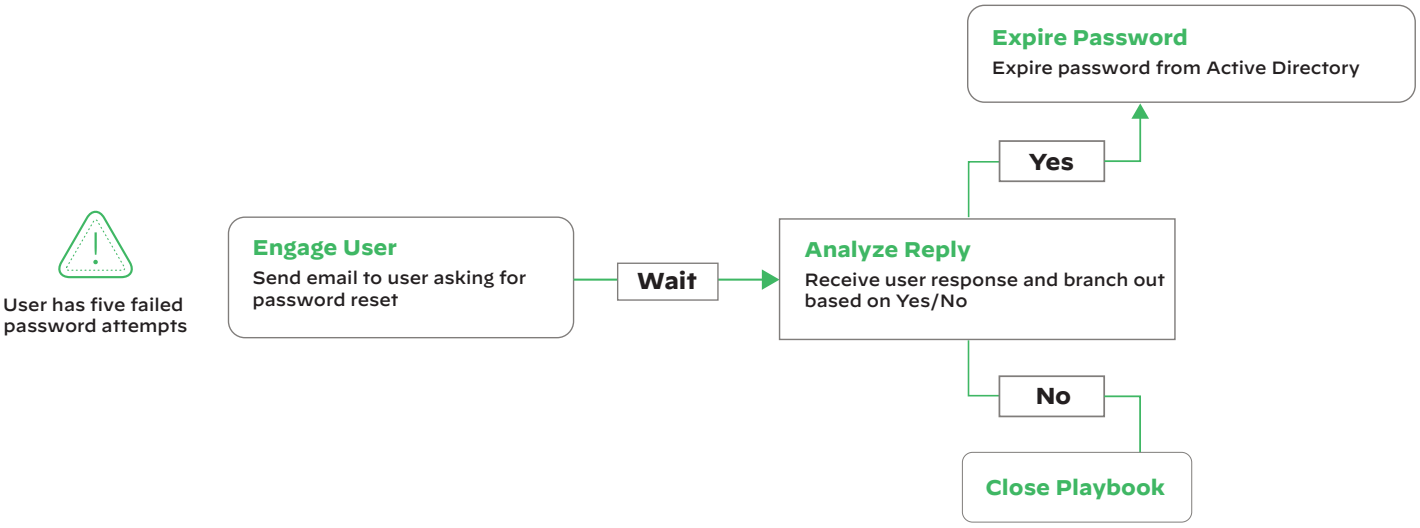

Figure 4: Failed user login playbook

Send Email

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 Reply

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

Genuine Case

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.

Malicious Case

If the end user confirms that they were not the one 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 from which the failed attempts were made, quarantining the affected endpoint, and so on.

Logins from Unusual Locations

Current Drawbacks

In the global age of today's business, it's tough to tell a malicious VPN access attempt apart from a genuine case of employee travel and access from another country. Moreover, with increased cloud adoption, there are multiple sources of geographical presence to verify, heaping more work on security teams and presenting a window of opportunity to attackers.

How Orchestration Helps

Some security orchestration platforms enable playbooks as not just reactive measures, but also as proactive scheduled workflows. In this case, a VPN check playbook can be scheduled to run at timely intervals and identify any VPN anomalies before escalating to security teams for further investigation.

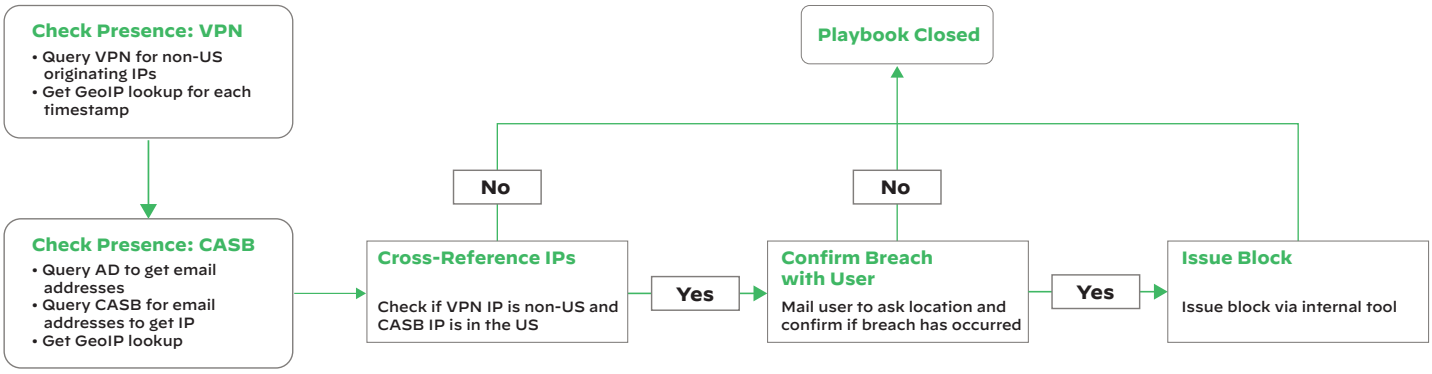

Figure 5: VPN check playbook

Check VPN Presence

The playbook queries the VPN service for non-US originating IPs and gets the GeoIP lookup for each timestamp on those IPs.

Check CASB Presence

To reconcile the VPN data, the playbook queries Active Directory for all email addresses and checks them against a CASB to retrieve IPs. The playbook then gets GeoIP lookups for each timestamp on these IPs.

Cross-Reference IPs

The playbook cross-references IPs gathered from the VPN service with IPs gathered from the CASB. Whenever it spots a non-US VPN IP with a US-based CASB IP, it sends an automated email to the affected user to confirm their location.

Respond to Breach

If the user responds confirming the breach, the playbook blocks the concerned IP using internal tools and brings in the relevant security analyst for further investigation.

Note: The condition given in the playbook in figure 5 is illustrative and can be used with a host of other conditions for VPN checks. For instance, "impossible travel" can be a checked condition wherein two logins from two different locations at the same time is flagged by the playbook and triggers action.

Security Operations Management

SSL Certificate Management

Current Drawbacks

SOCs are usually so preoccupied with responding to incidents that they aren't able to spend much time on the "security operations" part of their responsibilities. Expired SSL certificates, outdated operating systems, and unpatched endpoints are often symptoms of vulnerable targets that lead to eventual attacks.

How Orchestration Helps

A certificate management playbook can be scheduled to run at timely intervals, querying all endpoints for SSL certificates nearing expiry and taking required countermeasures.

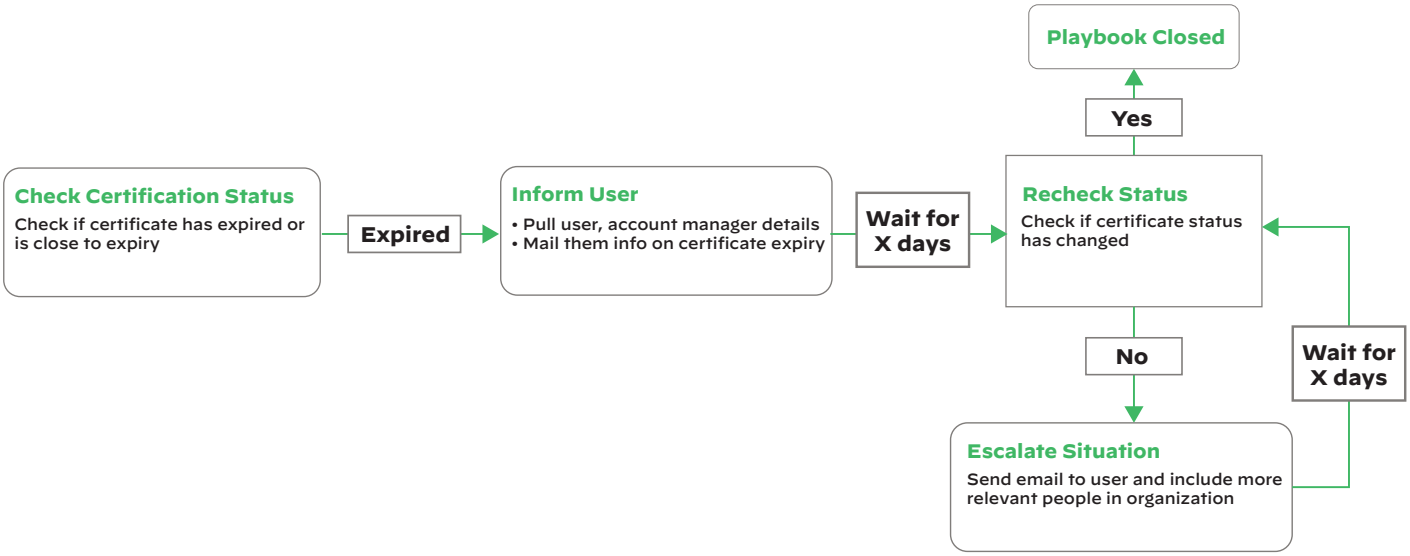

Figure 6: SSL certificate management playbook

Check Certification Status

The playbook queries a certificate management tool (such as Venafi®) to check all endpoints for SSL certificates that have either expired or are nearing expiry.

Inform User

Upon finding problematic certificates, the playbook pulls up user details (from Active Directory, Salesforce® etc.) of the affected user and their manager. The playbook then sends an automated email informing them of the certificate in question and directing them to make updates.

Recheck Status

The playbook rechecks the status of problematic certificates a few days after the initial email was sent out.

Escalate

If the certificate still hasn't been updated, the playbook sends automated emails to the affected user, the user's manager, and other relevant administrators to escalate the situation and bring the situation to their attention.

Endpoint Diagnostics and Kickstart

Current Drawbacks

Endpoint diagnostics and maintenance are as important on the proactive front as endpoint protection is on the reactive front. Machines that are unmanaged, lack agent connectivity, or have outdated policies are usually soft targets for attackers. Security teams often don't have the time to conduct thorough endpoint diagnostics as they're preoccupied with incident response.

How Orchestration Helps

Playbooks can be scheduled to run at timely intervals to conduct diagnostics checks on all endpoints and bring in analysts if required for fixing out-of-date endpoint machines.

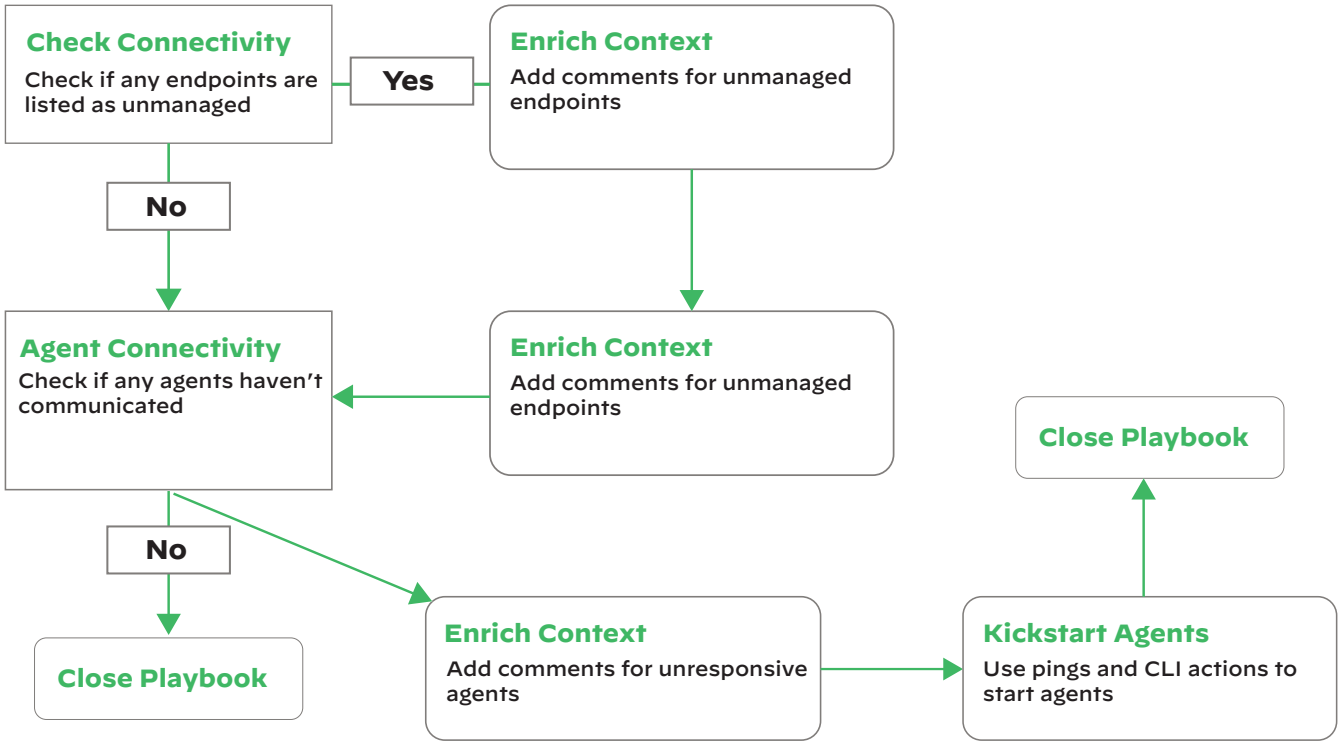

Figure 7: Endpoint diagnostics and kickstart playbook

Check Connectivity

Using tools such as McAfee ePO, the playbook checks if any endpoints are listed as unmanaged. If any endpoints are unmanaged, the playbook adds comments for analyst context and opens a ticket to escalate the issue.

Check Agent Connectivity

The playbook checks if any endpoints are outside the scope of communications of agents. If any such endpoints are found, the playbook adds comments for analyst context, opens a ticket, and attempts to kickstart agents for those endpoints using pings or other methods.

Vulnerability Management

Current Drawbacks

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

How Orchestration Helps

Security orchestration playbooks can automate enrichment and context addition for vulnerabilities before handing off control to the analysts for manual remediation. This maintains a balance between automated and manual processes by ensuring that analyst time is not spent in executing repetitive tasks but in making critical decisions and drawing inferences.

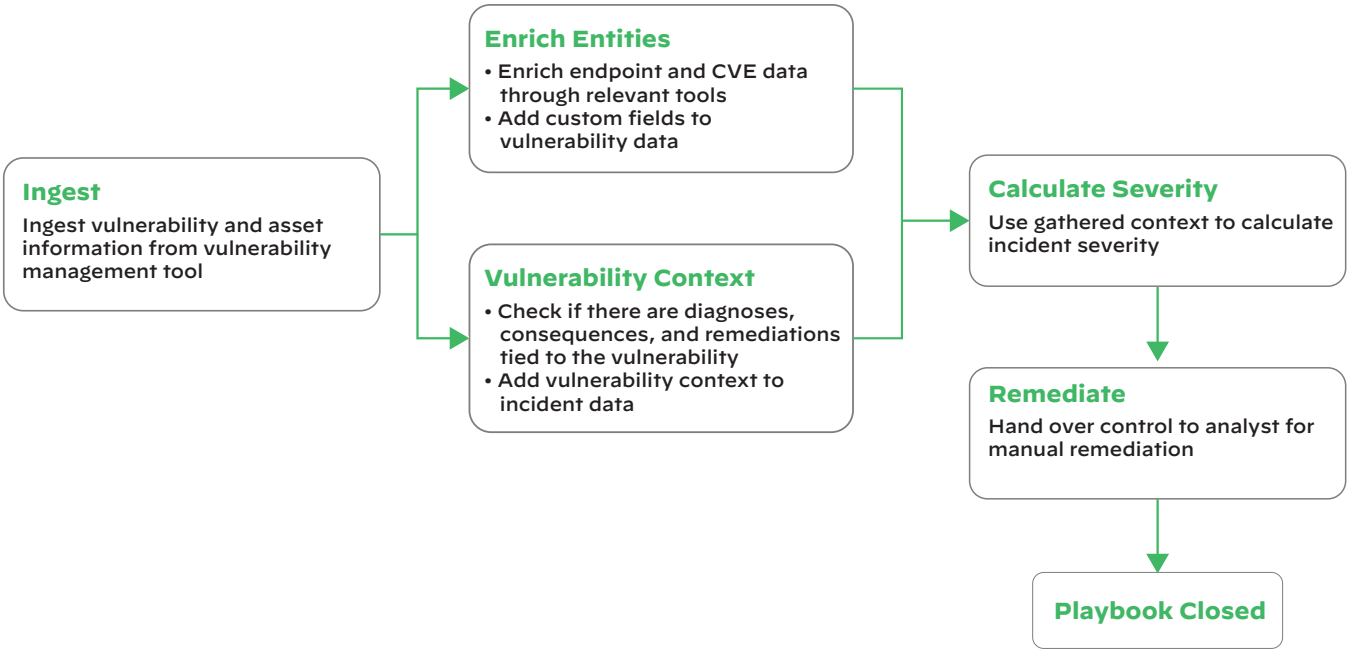

Figure 8: Vulnerability management playbook

Ingestion

The playbook ingests asset and vulnerability information from a vulnerability management tool such as Qualys®.

Enrich Entities

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

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.

Calculate Severity

Based on the gathered context, the playbook calculates the severity of the incident. More information regarding this process can be found in the "Assign Incident Severity" playbook in this whitepaper.

Remediate

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

Threat Hunting and Incident Response

Rapid IOC Hunting

Current Drawbacks

Security teams are often too focused with fighting daily incident response fires to devote time to proactive and scheduled threat hunting operations and catch incipient threats before they manifest on user environments. Even when they have enough time to execute threat hunting exercises, correlating intelligence from multiple threat feeds is a manual, repetitive exercise that doesn't leave enough time for decision-making.

How Orchestration Helps

Security orchestration playbooks for incident response free up analyst time to focus on proactive tasks such as threat hunting. For the hunting exercises themselves, security teams can execute playbooks that ingest malicious IOCs and hunt for more information across a range of threat intelligence tools.

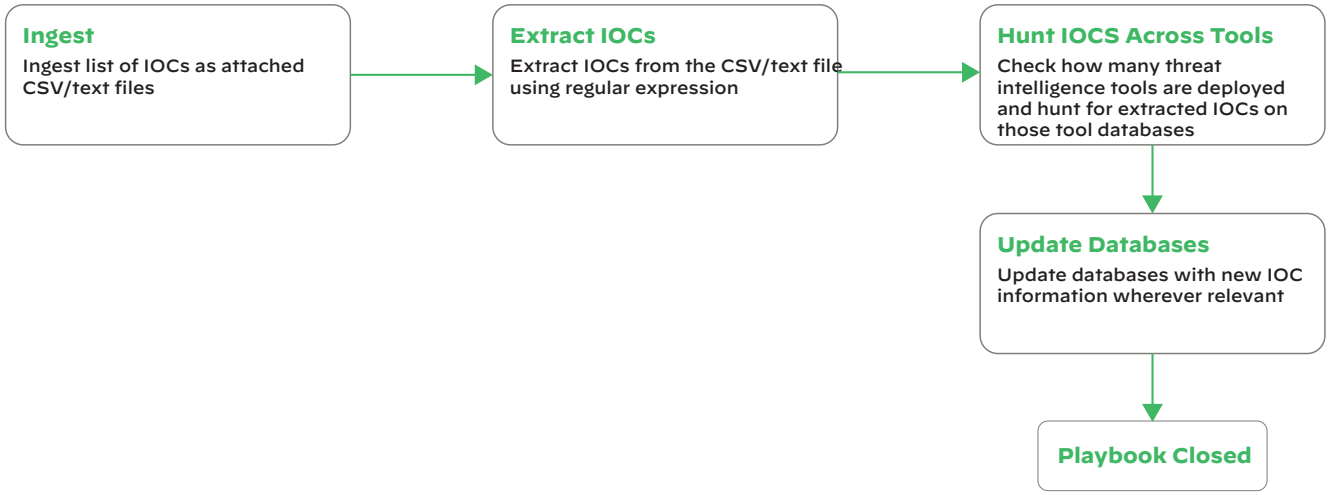

Figure 9: Rapid IOC hunting playbook

Ingestion

The playbook ingests a list of IOCs as attached CSV/text files.

Extract IOCs

The playbook extracts the IOCs (IPs, URLs, hashes, etc.) from the CSV/text file using regular expressions.

Hunt IOCs Across Tools

The playbook verifies how many threat intelligence tools are deployed by the SOC and hunts for the extracted IOCs on those tools. Wherever applicable, the playbook also checks endpoints and identifies if any endpoint has been compromised by the malicious IOCs.

Update Databases

If malicious IOCs were found on any threat intelligence tool, the playbook updates databases of other tools and other watchlists/blacklists with this information.

Malware Analysis

Current Drawbacks

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

How Orchestration Helps

Security orchestration playbooks can automate the entire file detonation process either as an isolated workflow or in concert with other enrichment activities. This ensures that analysts don't waste time performing the activity but are still able to benefit from the results of the analysis. Since playbooks document the result of all actions on a central console, the need for post-fact manual documentation is also eliminated.

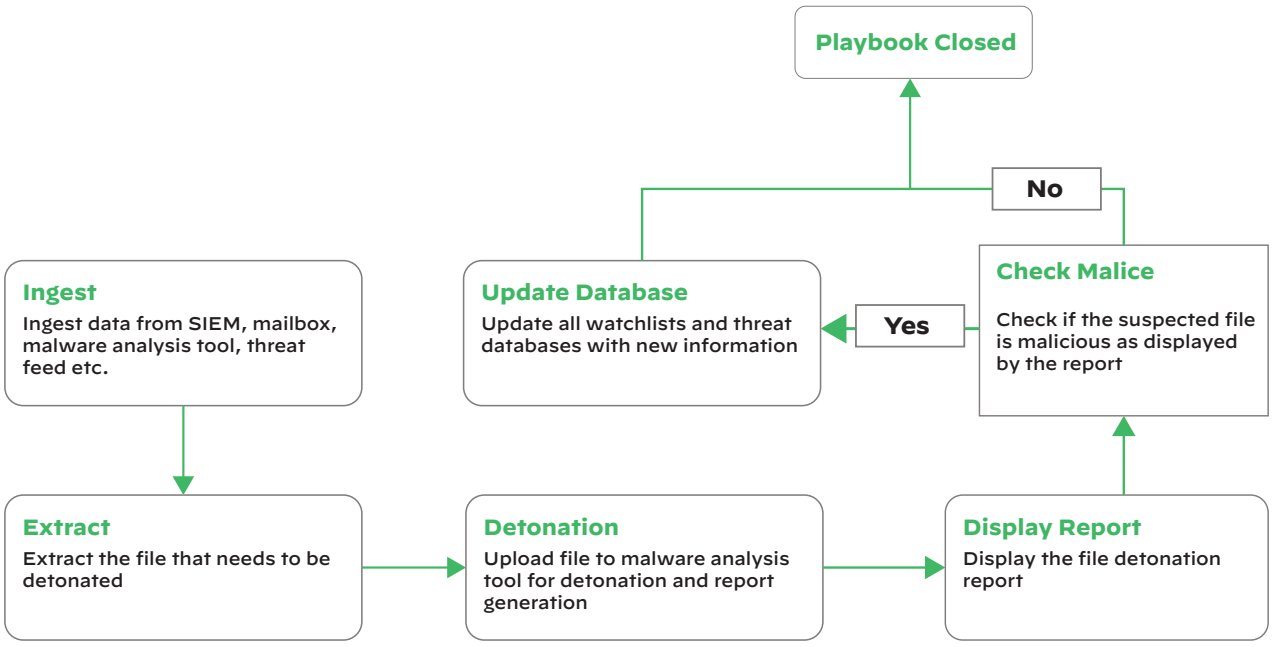

Figure 10: Malware analysis playbook

Ingestion

The playbook can ingest data from a variety of sources such as SIEMs, mailboxes, threat intelligence feeds, and malware analysis tools.

Extraction

The playbook extracts the file that needs to be detonated.

Detonation

The playbook uploads the file to the malware analysis tool where it is detonated and the ensuing malware analysis report is generated.

Display Report

The playbook displays the malware analysis report for analyst study and action.

Update Database

If the file is found to be malicious, the playbook updates relevant watchlists/blacklists with that information. From here, the playbook can branch into other actions such as quarantining infected endpoints, opening tickets, and reconciling data from other third-party threat feeds.

Cloud-Aware Incident Response

Current Drawbacks

From an incident response standpoint, cloud security data and processes are often isolated from traditional security measures, requiring multiple consoles to manage overall security posture. From an operations standpoint, managing service credentials is a tiresome exercise, with each service needing keys or passwords to call different sets of APIs.

How Orchestration Helps

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

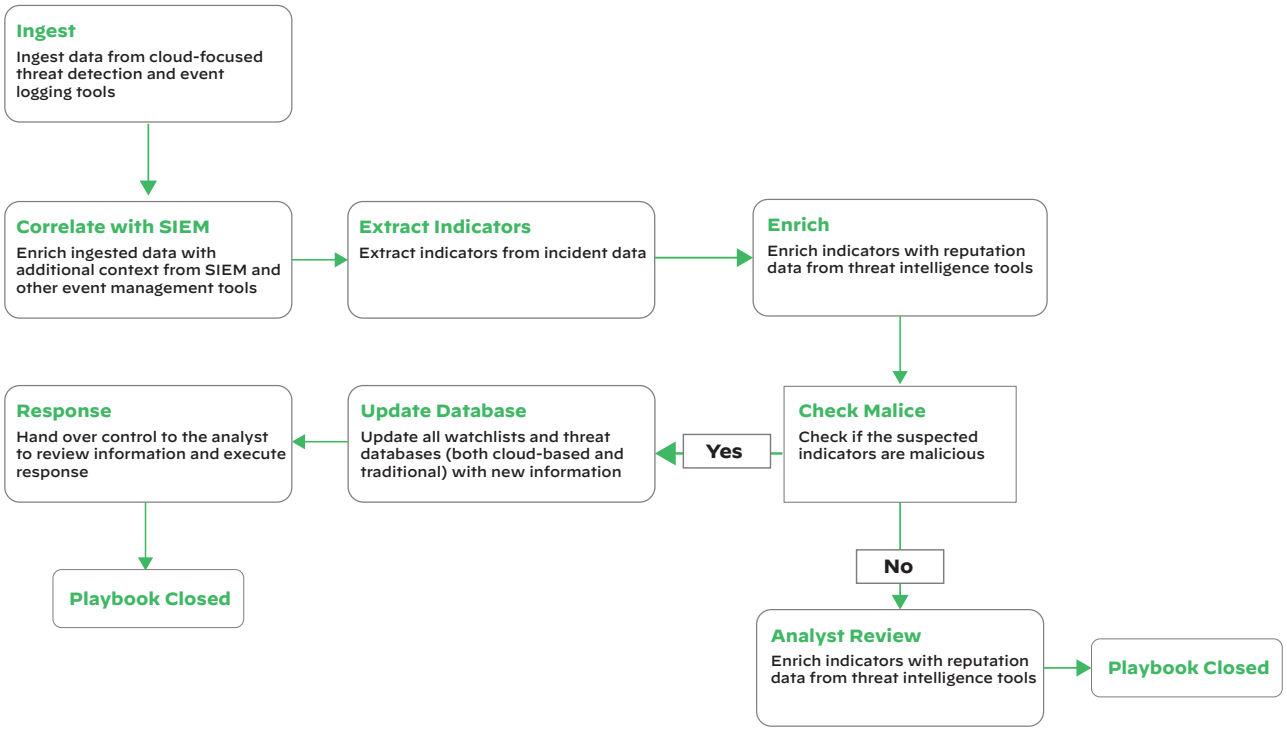

Figure 11: Cloud-aware incident response playbook

Ingestion

The playbook ingests data from cloud-focused threat detection and event logging tools such as Amazon GuardDuty® and Amazon CloudWatch.

Correlate with SIEM

The playbook 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.

Extract Indicators

The playbook extracts indicators (IPs, URLs, hashes, and so on) from the incident data.

Enrich

The playbook enriches indicators with reputation data from threat intelligence tools that the SOC uses.

Malice Check

The playbook checks if the indicators are identified as malicious. If they are, the playbook updates databases and watchlists (both cloud-based and non-cloud-based) with the new information before handing over control to a security analyst for further investigation. 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.

Versatile Security Automation

IOC Enrichment

Current Drawbacks

Enrichment of indicators is one of the first tasks security teams perform during incident response. The challenges here are twofold. Firstly, the process of indicator enrichment is as repetitive as it is important. 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 intelligence data across platforms to get an overall understanding of indicator malice.

How Orchestration Helps

Security orchestration playbooks can automate enrichment of indicators by querying different threat intelligence tools for context. By running this playbook at the outset of incident response, security teams have the enrichment data available for study within seconds, shaving off wasted time that can be used towards proactive investigation.

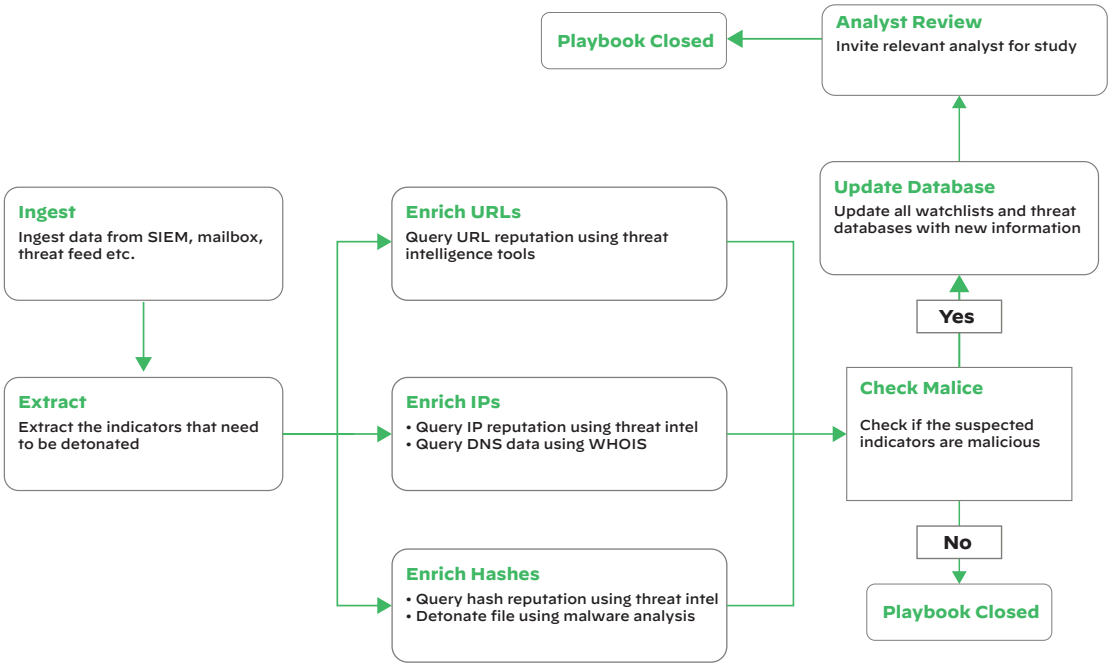

Figure 12: IOC enrichment playbook

Ingestion

The playbook can ingest data from a variety of sources, such as SIEMs, mailboxes, and threat intelligence feeds.

Extraction

The playbook extracts the IOCs (IPs, URLs, hashes, etc.) that need to be enriched.

Enrichment

The playbook enriches the IOCs across however many threat intelligence tools the SOC uses. For instance, URLs are enriched using tools such as Cofense® and CrowdStrike Falcon® Intel, IPs are enriched using threat intelligence tools and DNS services such as WHOIS, and hashes are enriched using threat intelligence tools and malware analysis tools such as Palo Alto Networks WildFire® malware prevention service.

Update Databases

The playbook executes initial response actions based on indicator malice. For instance, malicious indicators are fed back into threat intelligence databases and tool watchlists to avoid future attacks using the same indicators.

Analyst Review

The playbook checks if the indicators are identified as malicious. If they are, the playbook raises the incident severity, opens a ticket, and brings in the relevant analyst for further review and investigation. If the indicators are not identified as malicious, the playbook records the context for future reference and closes the incident, preventing analysts from being bogged down by false positives.

Assigning Incident Severity

Current Drawbacks

As SOCs start expanding their security product stack, each product sends out its own alerts, resulting in repetitive alerts for security analysts to sift through. Moreover, differing sensitivity settings across products pose a problem. If the alert detection is not sensitive enough, dangerous incidents might slip through the cracks and result in real organizational harm. If it's too sensitive, analysts end up receiving false positives that take up huge chunks of their time and decrease work satisfaction.

How Orchestration Helps

Whenever an incident is ingested into the orchestration platform, a "severity scoring playbook" can reconcile incident severity across data sets and assign the correct priority to the incident, ensuring that analysts can give their attention to the most critical incidents first.

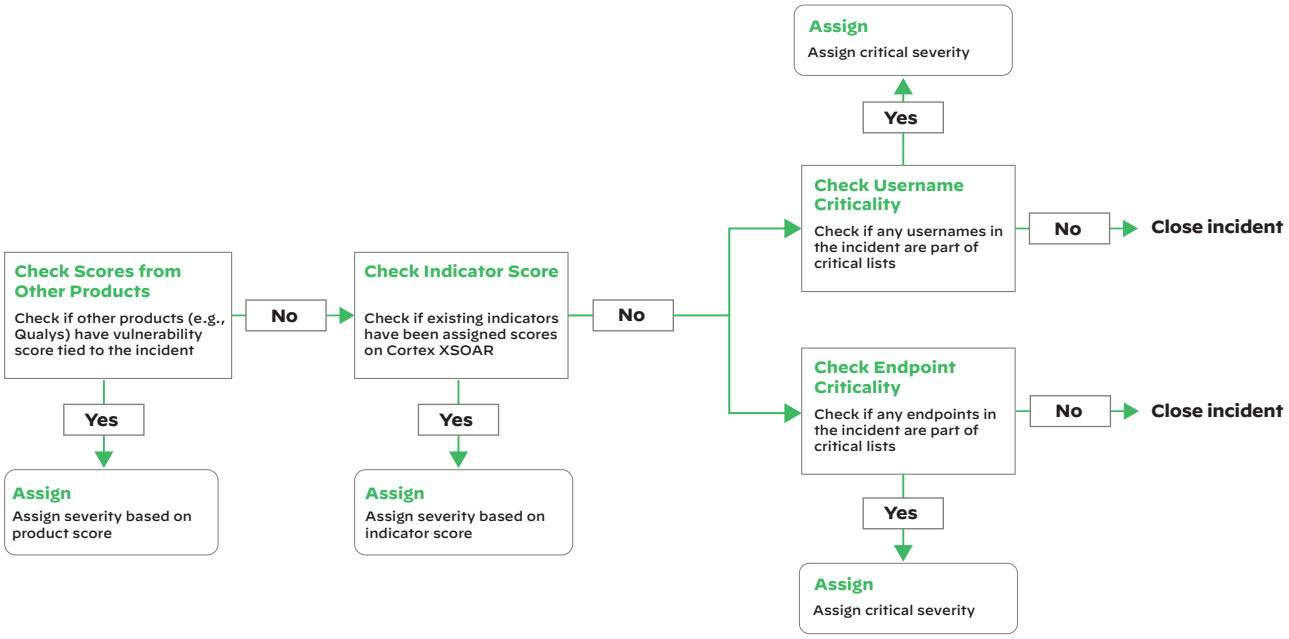

Figure 13: Incident severity playbook

Check External Product Scores

The playbook first validates whether any external vulnerability management products have recorded a severity level for the incident at hand. For example, the playbook can execute a query to Qualys to check if there's a recorded incident severity and assigns the same severity to the incident within the orchestration platform.

These actions ensure that teams utilize the strengths of their security products (like Qualys's strength at severity scoring) without always having multiple tabs open and manually performing low-level actions.

Check Indicator Scores

If there's no third-party severity input, the playbook checks the indicators (IP addresses, URLs, file hashes) of the incident and validates whether there's a "threat score" attached to any indicator.

Note

Some orchestration platforms automatically record all indicators that are ingested as part of incidents, assigning each indicator a "Reputation" based on an amalgamation of scores from other threat intelligence platforms that the SOC integrates with.

If there's a score attached to any indicator, the playbook assigns a High, Medium, or Low severity accordingly. If SOCs integrate with multiple threat intelligence products, the indicator score is an ideal way to action the insights from each product through a combined reputation rating.

Check Critical Entities

In addition to threat intelligence, the playbook should also take user identity and behavior into account while assigning incident severity. The playbook checks if there's a username tied to the incident and whether the username is part of any critical user lists. It performs these same checks with the hostname tied to the incident. If either the username or hostname merit additional agility in response, the playbook assigns a "Critical" severity to the incident.

CORTEX
BY PALO ALTO NETWORKS

Want to Learn More About Orchestration?

Get Cortex XSOAR Free Edition

Try it now

2019 State of SOAR Report

Get the report

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

top-security-orchestration-use-cases-wp-100220