Demisto Special Edition

Security Orchestration

for dummies

A Wiley Brand

Identify security orchestration drivers

Study popular security orchestration use cases

Adhere to best practices

Compliments of

DEMISTO

Abhishek Iyer

About Demisto

Demisto is the only Security Orchestration, Automation, and Response (SOAR) platform that combines security orchestration, incident management, and interactive investigation to serve security teams across the incident life cycle. Its orchestration engine coordinates and automates tasks across hundreds of products, resulting in an increased return on existing security investments. Demisto enables security teams to reduce Mean Time to Response (MTTR), create consistent incident management processes, and increase team productivity.

For more information, visit **https://www.demisto.com,** email **info@demisto.com**, or follow **@demistoinc** on Twitter.

Security Orchestration

Demisto Special Edition

by Abhishek Iyer

for
dummies®
A Wiley Brand

Security Orchestration For Dummies®, Demisto Special Edition

Publisher's Acknowledgments

Table of Contents

Introduction

Three security analysts walk into a bar. Actually, they don't because no security analyst has the time for that.

The above joke (if you can call it that) accurately describes the state of cybersecurity teams today. Alert volumes continue to rise, security product stacks continue to grow, and the threat landscape continues to expand. Security analysts are tough to hire and retain, leading to understaffed teams manually combing through data as the candles burn out. It's a tough gig.

Security teams need something — a technology, a process, a lucky rabbit's foot — that simplifies data visibility by unifying intelligence from multiple security tools. They also need to reduce the time they spend on carrying out important but repetitive actions.

Enter stage right, security orchestration. I can simply describe it as making a bunch of products work together in a coordinated manner under your control to safeguard your organization's security, but there's a literal book to be written with all the necessary details. So let's get to it!

About This Book

This book explains security orchestration in six short chapters:

- » Chapter 1 shows you how the modern threat landscape evolved to set the stage for security orchestration.
- » Chapter 2 lays out the basic building blocks of security orchestration and how they all come together.
- » Chapter 3 takes a look at vendor selection and implementing security orchestration at your organization.
- » Chapter 4 explains why security orchestration is beneficial to your organization, including specific use cases.
- » Chapter 5 delves into what trends and overlaps lie in store for security orchestration in the future.
- » Chapter 6 clarifies some common myths about security orchestration to reach an improved understanding.

Foolish Assumptions

Those who don't know, assume. And while I'd love to get to know you better, these assumptions about you must suffice in the meantime:

>> You're a security analyst, security operations center (SOC) manager, or incident responder. You haven't heard of security orchestration and want to know how it can improve your daily operations.

>> You're a chief information security officer (CISO) and want to evaluate security orchestration as part of the overall vision of enterprise security at your organization.

>> You work in the security or IT team at your organization (but not in the SOC). You're interested in learning about the cross-departmental benefits of security orchestration.

>> You're a student familiar with basic cybersecurity concepts, technologies, and attacker techniques. You want to learn about security orchestration to expand your skill-sets.

If any of these assumptions describes you, this book is a great place to start your security orchestration deep-dive. If you don't fit my assumptions, I'd love it if you exercised your free will to challenge my assumptions and read the book regardless.

Icons Used in This Book

From hieroglyphs to emoticons, pictures have always held a special place in human hearts. I use some icons in this book to highlight specific information.

TIP

My parents always taught me to tip well! The Tip icon identifies useful nuggets of information related to security orchestration and its uses.

WARNING

The Warning icon identifies common mistakes and pitfalls that you should avoid during your orchestration journey.

Specially crafted for busy professionals and multitaskers, the information with the Remember icon identifies the most useful parts of the book that you should (probably) commit to memory.

This book won't give you the meaning of life, but it will still go deep at times. This icon identifies the jargon beneath the jargon that you can skip or gravitate toward.

Beyond the Book

Although this book is a good way to start your security orchestration journey, you can take many paths beyond the book as well. If you want more security orchestration information, visit the following resources:

- ▶ To explore security orchestration in action, you can download the Demisto Community Edition for free by visiting this link: `http://demis.to/free-edition`.

- ▶ For a deeper look at security orchestration, its moving parts, and how they all connect together, you can read this conceptual whitepaper: `http://demis.to/orchestrationmusic`.

- ▶ For insight into how security orchestration positively impacts your organization's return on investment, you can read this ROI-focused whitepaper: `http://demis.to/orchestrationROI`.

- ▶ For a demonstration of security orchestration, you can view Demisto's product deep-dive by visiting this link: `http://demis.to/productdemo`.

Chapter **1**

Meeting Enterprise Security Challenges

Technology makes it easier for you to conduct business, connect with people, and live your life. However, these advancements lead to security challenges at work, home, and beyond. Technological innovation has always been at a tug-of-war with security improvements, and security teams are inevitably pulled in both directions.

In this chapter, you learn about the major security challenges that enterprises face today, how modern developments sometimes exacerbate these challenges, and the resulting gaps in the landscape that security orchestration is poised to fill (but I'll let you be the judge of that).

How We Got Here

As the Internet has matured over the years, more and more businesses have become technology companies by adding digital capabilities, selling goods online, collecting tons of user information,

and creating smart devices. These advancements have come at a cost, however. The industry faces some pretty complex security challenges today. These challenges often feed into and worsen each other.

Growing alerts

The most critical and lasting challenge affecting enterprise security today is the growing volume of security alerts. Demisto's 2018 State of SOAR Report polled security professionals and found that teams face an average of 10 to 12 thousand alerts per week. This results in *alert fatigue,* which means that the alerts eventually mean nothing because there are simply too many of them.

This high alert volume is due to several factors.

Too many security products

According to a NASDAQ Global Information Services report, the average security operations center (SOC) uses more than 15 security products. Staying on top of alert data from each product becomes a taxing exercise mired in duplication and manual parsing.

Varying product sensitivity settings

It's always a challenge to decide the level of sensitivity a security product should have for its alert detection. If the setting isn't sensitive enough, dangerous alerts might slip through the cracks and result in real organizational harm. If the setting is too sensitive, analysts end up receiving false positives that take up huge chunks of their time and decrease work satisfaction.

The modern organization is evolving

As businesses continue to expand across product lines and geographies, they open themselves up to new forms of security attacks. For example, modern retail companies can be exposed to point-of-sale compromise, credit card frauds, data theft, and Dedicated Denial of Service (DDoS) attacks.

Not enough people

Security professionals are difficult to hire, train, and retain because security jobs are usually strenuous, have highly technical

educational prerequisites, and include the expectation of always learning on the job, among other reasons.

TECHNICAL STUFF

A *security alert* is any potentially dangerous situation that affects the confidentiality, availability, or integrity of organizational data. These alerts are brought to the security teams' attention through detection products, such as Security Information and Event Management (SIEM) tools and network security tools.

TIP

Most of the security industry still uses the terms *alerts, events, incidents,* and *cases* interchangeably. Usually, alerts are relatively narrower incursions into target systems. Incidents, events, or cases are either an aggregation of alerts or alerts that have been deemed to be critically malicious. While I use the terms *alert* and *incident* interchangeably in this book for simplicity's sake, it's always better to ask what people mean when they say *alert.*

Product proliferation

By all accounts, organizations today use more security products than their teams can handle. Each new security product — even while delivering unique value — brings with it a learning curve, different data classification models, context, and measurement requirements. This product proliferation ultimately leads to a lot of screen switching, fragmented information, and disjointed record keeping once alerts have been resolved.

TECHNICAL STUFF

Demisto's 2018 State of SOAR Report found more than 50 percent of respondents citing that they needed to learn and use at least five distinct security tools to manage their daily operations.

Security skills gap

Demand far outstrips supply in the security job market today. A study commissioned by CyberSeek found that US employers in the private and public sectors posted an estimated 313,735 job openings for cybersecurity workers between September 2017 and August 2018. A U.S. Bureau of Labor Statistics report projected employment of information security analysts to grow by 28 percent from 2016 to 2026, much faster than the average for all occupations.

This skills gap is due to several factors.

Long training cycles

Security professionals — even experienced ones — usually need to be trained on an organization's specific security tools, processes, team hierarchies, and response scenarios. In Demisto's 2018 State of SOAR Report, almost 50 percent of respondents took more than eight months to properly train a new team member.

Low retention

Cybersecurity jobs are strenuous and — perhaps partly because of this — have high monetary remuneration. These two factors have resulted in consistently low retention rates for security jobs, as employees usually switch for better pay, more learning opportunities, and improved work-life balance. Many employees are likely to switch jobs within two years.

Siloed workforce

Security professionals may start out having a broad array of knowledge, but they tend to gravitate toward narrower, more specific skill-sets with time. These skills may align with particular incident types, security tools, or response methodologies. As a result, security teams often suffer from tunnel vision while dealing with alerts, leading to inconsistent processes and rework.

Our most experienced analyst left, so what now?

Security teams are fighting daily fires, usually leading to fragmented recordkeeping and incomplete knowledge management. In such a scenario, an experienced security analyst switching jobs holds dire consequences for the organization. Because departing employees take a ton of the knowledge with them, the remaining security team needs to start from scratch (at least in the departing employee's area of expertise).

While jobs in security continue to be lucrative and hiring rates continue to rise, Figure 1-1 shows this increase is more than counteracted by the growing volume of security alerts and product proliferation.
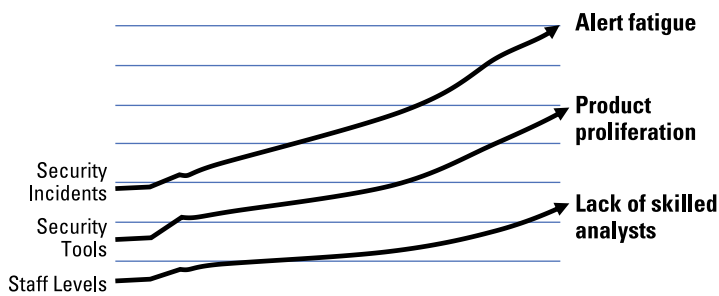
FIGURE 1-1: Growth isn't always good.

Where's the process?

The human capital crunch and high alert volumes prevalent in security today result in teams following inconsistent processes while responding to alerts. To examine this challenge more closely, take a look at this example: Suppose an SOC has to deal with around 50 phishing emails per day. They have a rough pro-cess in place:

1. **The email address, IP address, and URL of the phishing email are checked against threat intelligence tools.**

2. **If the email has an attachment, the file is scanned through a malware analysis tool.**

3. **The security analysts manually check URL misrepresen-tation, host-domain distance, and other minor telltale signs that the mail is malicious.**

4. **If the email is malicious, a ticket is opened, and the security team sends an email to the affected employee directing them to not access the phishing email again.**

5. **All endpoints in the system are scanned for occurrences of the malicious email.**

6. **The malicious indicators are added to blacklists so that web and email gateways automatically block them going forward.**

The first challenge security teams run into while executing this process is the sheer number of phishing alerts they receive

per day. Following such a laborious process for 50 emails per day takes time, but teams must still follow through because even a single successful phishing attack can have serious organizational and financial consequences.

The second challenge is coordinating among multiple security tools for each phishing investigation. Security teams need to have access to threat intelligence tools, email platforms, malware analysis tools, endpoint security tools, and email and web gateways. Manual correlation and context-switching across these platforms can lead to increased rates of error, fatigue, and precious lost time.

Taking a wider perspective, these phishing alerts are only a single type of alert that security teams must handle every day. So while following a process for each phishing investigation is time-consuming in itself, coordinating these investigations with the other activities in a security team's portfolio only worsens the situation. There's only so much time in the day.

In a best-case scenario, security teams handle this process and get faster with time at executing each step. But a junior security analyst will always have more trouble handling the process than a senior analyst will. This factor will inevitably lead to a variance in quality while handling phishing alerts, a dangerous scenario if SLA requirements are strict.

Taking all these challenges into account, it's not surprising that security organizations struggle to enforce incident response processes. In Demisto's 2018 State of SOAR Report, over 50 percent of respondents stated that they either didn't have set processes in place or that the processes were rarely updated after initial implementation. These responses are captured in Figure 1-2.

To explore security challenges and the drivers leading to the rise of security orchestration in greater detail, read Demisto's 2018 State of SOAR Report by visiting `https://go.demisto.com/the-state-of-soar-report-2018`.
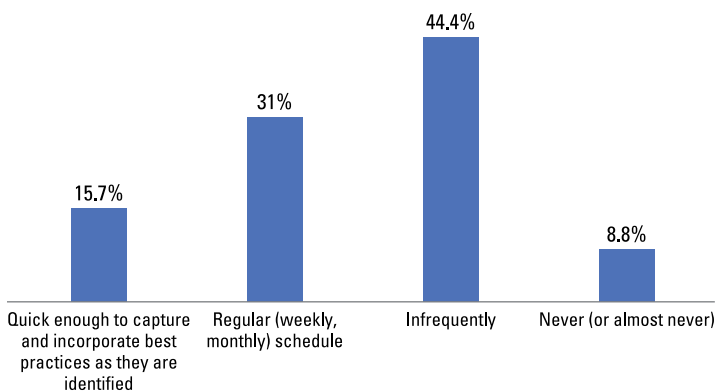
FIGURE 1-2: Incident response process update frequency.

Limited visibility

Technological and business advancements such as cloud, big data, the Internet of Things (IoT), and global supply chains have resulted in better products, greater customer choice, and improved quality of work. However, lurking under the surface of this progress is a lack of visibility that eventually leads to security compromise.

In this section, you look at a few trends that have heralded new security challenges.

Increased cloud adoption

The cloud has improved organizational agility, reduced products' time-to-market, and leveled the playing field with respect to computational power. However, no two clouds are alike, resulting in disparate environments that security teams struggle to monitor on a regular basis. This problem is especially true if the security teams are isolated from other teams that deal with DevOps, cloud infrastructure setup, and product development.

Increased user data collection

Because of advancements in data analytics and recommendation engines, organizations are incentivized to collect troves of user data in order to deliver greater business value. This data collection

leads to privacy concerns and — due to the collection and processing being done by third-party firms — also results in lax security and eventual data theft.

Distributed workforce and portable devices

Most organizations now offer flexible working hours and a work-from-home component that have improved the quality of employee life. However, this development coupled with Bring-Your-Own-Device (BYOD) policies has led to a lack of perimeter security enforcement. Even with virtual private network (VPN) execution, organizations don't always know what applications employees are using on their devices, increasing the chances of a security breach.

The Internet of (dangerous) Things

Cisco projects that there will be 50 billion connected devices by 2020, including everything from cars and refrigerators to toys and wearables. But whenever a product company makes an IoT-enabled device, it struggles to reconcile its expertise in its original industry with its unfamiliarity in Internet connectivity and security. This results in manufacturers using outdated OS and patching features on their products (if they can be updated at all), providing lax password protection and changes, and lacking regular software update mechanisms to communicate to their customers.

Smart but insecure supply chains

Product manufacturing straddles nations and industries, each with their own regulations, economics, and political climates. Therefore, organizations struggle to be cognizant of processes, vendor relationships, and regulatory requirements for each step of the product lifecycle. This results in breaches where malicious actors in one country can compromise the device manufacture process itself to gather sensitive data from users living in another country.

TIP

To learn more about security challenges stemming from IoT, head to `blog.demisto.com/iot-security-challenges-solutions`.

All about that risk

All security challenges, no matter how sprawling or minute, can be distilled down to the financial and business risk caused. The financial risk stemming from successful breaches may have low probability, but the extent of loss when a breach does happen can be devastating. A Ponemon study identified the average cost of a breach to be $3.62 million — a figure large enough to sink a small or medium business. Couple these figures with stringent new fines attached to regulations such as the General Data Protection Regulation (GDPR) in the European Union, and organizations literally can't afford to be hacked.

Other tangential factors contribute to financial risk as well:

» Infrastructure and server downtime

» Lost customer trust and customer switching

» Legal and media fees while dealing with breach crises

» Ransom payments to attackers

Even when a security breach doesn't result in huge financial outlays, the news cycles spawned in the breach's wake can cause considerable loss of reputation, especially for large enterprises. Attackers can steal huge swathes of data from a company — including sensitive information such as employee financials and product code — before dealing reputational blows by posting everything online.

Even if organizations don't relent to attackers' financial demands, overall breach response can still leave a sour taste in your mouth. Take this example: A media and entertainment giant gets hacked, and the attacker releases several unaired programs and scripts from popular TV shows online. Although the hacked organization doesn't yield to the attacker's ransom demands, it's still affected by the PR storm, working with authorities, and the lost revenue from shows that were leaked.

The bottom line is that organizations struggle to keep alerts at bay due to a confluence of factors, and they have to pay heavily (either literally or otherwise) whenever an attack is successful.

Setting the Stage for Security Orchestration

If you read all the security challenges mentioned in this chapter so far, it makes for a somber read, but don't close the book just yet. The security industry has done plenty of things right. Some gaps still exist between these areas of expertise, though, and identifying these gaps is the first step on the way to filling them.

A lot of data but little follow-up

Security tools today are sophisticated in their methods of data collection and drawing insights from that data. However, the question of "what next?" often pops up when security teams view all this data. After a breach is detected, security teams are often left with scores of manual actions to complete in order to resolve the alert.

Tools that don't talk to each other

Security tools might provide useful information about a security alert, but they each have a narrow area of expertise. Security teams must open all tool consoles in parallel and try to coordinate actions across their product stack while responding to alerts. Because most security tools don't integrate with each other in an open, extensible fashion, security teams must manually correlate data across tools and make sense of the alerts they receive. Imagine trying to solve several puzzles at the same time.

People that don't talk to each other

Security teams are busy, drowning in a flood of alerts and being asked to execute repetitive manual actions across tools to handle these alerts. In such a scenario, security professionals tend to focus on their areas of expertise, leading to siloed work, duplication of efforts, and not learning from their peers whenever possible.

These areas of focus need to work in concert for organizations to solidify and improve their security posture. The stage is set for a security technology to do just that. If only something steps up to the plate. . .

Spoiler alert, it has. Check out Chapter 2 for more information.

Chapter **2**

Looking at the Basics of Security Orchestration

Organizations need to make sense of the vast amounts of data (check out Chapter 1 for more information) at their disposal and ensure that both their tools and their people talk with each other for effective response to security alerts. In this chapter, I discuss security orchestration and break down its various components to show you how they all work in concert — like an orchestra, if that's not too obvious.

Security orchestration is a method of connecting disparate security technologies through standardized and automatable workflows that enables security teams to effectively carry out incident response and security operations. If you study this definition carefully, a few terms jump out:

» Security technologies
» Workflows
» Security teams

This list nicely sets up a discussion on the three pillars of security orchestration, starting with technology.

TIP You can get a lightning-quick overview of security orchestration by viewing this concept explanation video on Demisto's YouTube channel: www.youtube.com/watch?v=BzB10GGQ8ms.

The Technology

A fundamental truth in security today is that there's a product for everything. And while most, if not all, of these security products are useful in their own way, their numbers quickly balloon.

And, as with any system that has a huge number of moving parts, coordinating actions across products becomes a challenge for security teams.

This section gives you the major types of security technologies utilized by organizations today. You can broadly divide these tools into detection tools, enrichment tools, and response tools. However, some tools can cover multiple responsibilities.

>> **Security information and event management (SIEM):** SIEM tools monitor various sources for machine data, correlate and aggregate them for context, and provide real-time detection and monitoring of alerts generated by applications and network hardware. These tools are useful for alert detection and initial enrichment.

>> **Threat intelligence:** Threat intelligence tools collect and correlate data from external and internal sources to provide information regarding the malice of an incident or indicator. These tools are useful for alert enrichment.

>> **Endpoint security:** Endpoint security tools are responsible for the protection of devices such as laptops, mobile phones, and desktops that are connected to organizational networks. These tools help with detection, enrichment, and response actions.

>> **Network security:** Network security tools involve both hardware and software that protect the underlying network infrastructure from misuse or compromise. These tools are a critical part of alert detection.

>> **Email and web gateways:** Email and web gateway tools are designed to prevent the transmission of emails or access of websites that break company policy or result in information transfer with malicious intent. These tools are important for response and enforcement.

>> **Ticketing systems:** Within security, ticketing systems are usually responsible for assigning tasks, capturing the flow of an incident, and helping deal with incidents in a more effective manner.

» **Vulnerability management:** Vulnerability management tools are responsible for uncovering any potential weaknesses in existing organizational systems that can be exploited by malicious actors.

» **Cloud Access Security Broker (CASB):** For organizations with cloud-based resources, CASBs act as a middle layer between customers and providers to ensure enterprise security policy enforcement.

» **User and Entity Behavior Analytics (UEBA):** UEBA tools monitor and analyze the behavior of users and entities to detect anomalous and potentially malicious intrusions into organizational systems.

REMEMBER

This list of technologies is merely illustrative and isn't a recommended or best-practice list of security technologies by any means. Each organization needs a tailored stack of security technologies depending on their industry, existing processes, and security maturity.

Even walking through this illustrative list of technologies is enough to showcase the coordination struggle that security teams constantly face while trying to execute incident response.

Joining Forces

Security orchestration tools integrate with all the other security tools (and many non-security tools) that an organization uses to provide teams with a central console to coordinate and activate all these tools. These integrations enable inter-product conversations, data transfer, and remote execution of commands.

REMEMBER

Product integrations or apps are mechanisms through which security orchestration platforms communicate with other products to enable data transfer and remote execution of commands.

These product integrations are possible through a range of mechanisms, such as REST APIs, SOAP APIs, SSH, SQL, and HTTPS. The connective mechanism depends on the types of

products being integrated, which in turn influences the depth and fidelity of data transfer that's allowed between the two integrated products.

So, if a security orchestration tool integrates with another tool, what possible actions can be executed through the integration? Well, this partly depends on the capabilities of the security tool itself, but you discover the main types of actions possible in this section.

Ingestion of security data

If the security orchestration tool integrates with a product that's responsible for alert detection (like a SIEM), the security orchestration platform can ingest this alert data in an automated or manual fashion. Once ingested, this alert data can automatically be driven to response through playbooks.

Enrichment of security data

If the security orchestration tool integrates with a product that's responsible for providing additional context to an alert (like a threat intelligence tool), security teams can use the integration to access this additional context within the security orchestration tool in an automated or manual fashion and find out more about an alert.

Response actions

If the security orchestration tool integrates with a product that's responsible for enforcement and response actions (like an endpoint security tool), security teams can use the integration to execute these response actions from within the security orchestration tool in an automated or manual fashion.

Operational and engagement actions

If the security orchestration tool integrates with a product that's responsible for maintaining operational efficiency or end user engagement (like ticketing systems and email tools respectively),

security teams can use the integration to automate actions, such as creating a ticket or sending an email to a hacked employee.

Choose your own direction

Product integrations within security orchestration tools can be either unidirectional or bidirectional. A *unidirectional integration* only allows for transfer of data from the integrated security product to the security orchestration tool. A *bidirectional integration* allows for two-way transfer of data between both integrated tools.

For example, a security orchestration tool that has a bidirectional integration with an endpoint tool can perform these actions:

» The security orchestration tool can ping the endpoint tool for device details, asset data, infected endpoints, and similar information.

» The security orchestration tool can also perform create, read, update, and delete (CRUD) actions on the endpoint tool, such as quarantining an endpoint or updating an indicator blacklist.

The Process

After the security orchestration tool has integrated with most, or all, of an organization's other security products, data from multiple sources is flowing into one platform for triage and resolution. This triage and resolution should take place in a standardized, coordinated, and repeatable manner. Within security orchestration, this is made possible through playbooks.

REMEMBER

Security orchestration 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.

Standardized processes

Playbooks enable the codification of best practices to follow during any process. With rising alert volumes, overworked security teams, and the general chaos associated with detecting a cyber-attack, it's more convenient (but not more effective) to follow a "everyone do what you can" approach. This method leads to variance in response quality and vital information slipping through the cracks. Security orchestration playbooks minimize, and hopefully prevent, these practices by enforcing a consistent set of steps that every team member can adhere to.

After processes are standardized, security orchestration playbooks can go one step further and automate high-quantity actions to accelerate overall incident response times. Check out this detailed, but not comprehensive, list of security actions:

» Finding indicator reputation from threat intelligence tools

» Opening, editing, and closing support tickets

» Sending emails to affected end users

» Detonating files in malware analysis tools

» Quarantining infected endpoints

» Setting the severity levels of incoming alerts

» Correlating data between a SIEM and a threat intelligence tool

» Updating indicator watchlists and blacklists

These actions are important but, due to their repetitive and high-volume nature, take up far more of a security professional's time than they should. This mismatch between a task's importance and the time devoted to it further feeds into the vicious cycle of overworked security teams and dormant, unaddressed security alerts.

Security orchestration playbooks address this shortcoming by enabling the automation of a wide variety of security actions across products. While specific actions that can be automated

will depend upon the depth and openness of APIs, all the actions mentioned in the list above are prime candidates and are usually the first to be automated during security orchestration deployment.

The language of security orchestration playbooks, while still evolving, is similar to the language of workflows in general. Take a look at the building blocks of security orchestration playbooks.

Playbook trigger

If a playbook must automatically execute within a security orchestration tool, it needs a trigger point. This trigger point can be any condition that, when met, results in the start of the playbook. For example, whenever a phishing email is ingested from a mailbox into the security orchestration tool, a phishing response playbook can trigger and begin its execution.

Automated playbook task

Automated playbook tasks are visual abstractions for a piece of code, called an *automation,* running in the background. Users can either select from pre-existing automation codes (most security orchestration tools will come with an out-of-the-box list) or code their own automations for these tasks.

Manual playbook task

Manual playbook tasks are visual abstractions where users can enter any task comments and instructions that are meant to be performed manually.

Conditional task

Security orchestration playbooks use conditional tasks to check the value of any incident-related artifact and execute different branches depending on the result. For example, a conditional task can check the severity of an alert and execute different sets of tasks if the severity is high, medium, and low respectively.

Check out Figure 2-1 for an example of standardized processes in a security orchestration playbook.
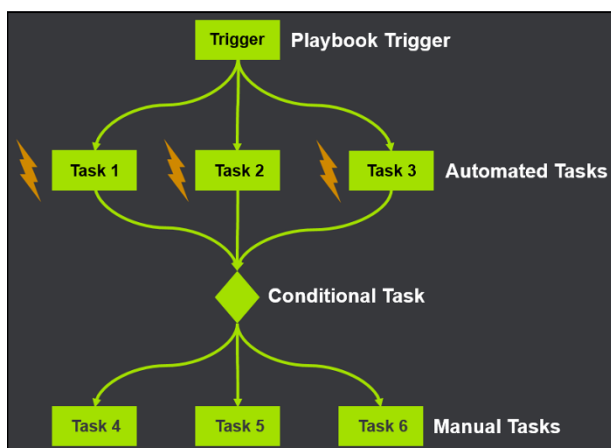
FIGURE 2-1: The standardized processes in a security orchestration playbook.

Unstandardized processes

Unstandardized processes may seem like an oxymoron, but they're part and parcel of a security professional's responsibilities. Cyberattacks are always evolving, and a step-by-step playbook may not always be enough to handle a sophisticated incident. These unstructured investigations usually require additional real-time tasks, such as

» Pivoting from one suspicious indicator to another to gather critical evidence

» Drawing relations between incidents

» Grabbing and archiving evidence

» Finalizing resolution

Running these commands traps security analysts in a screen-switching cycle during investigation and a documentation-chasing cycle after investigations end.

For such unstandardized investigations, security orchestration tools sometimes include a real-time collaboration platform that enables security teams to converse with their peers, run security commands, and document their actions at one source.

WARNING

Although collaboration is fast becoming a point-of-parity for security orchestration vendors, not all solutions have the same levels of maturity for this feature. When choosing a security orchestration solution, conduct a thorough due diligence to verify whether collaboration is a core part of the offering.

This collaboration platform won't have the same level of structure as a playbook, but the aim is to provide just enough structural and documentation support when investigations enter unforeseen territories. Some security orchestration tools meet this aim through a concept called *Security ChatOps.*

REMEMBER

Security ChatOps is a platform for conversation-driven investigation. When security analysts, security tools, chatbots, and incident response workflows exist in the same chat window and reinforce each other, that's ChatOps in action.

In a nutshell, ChatOps is a single console where security professionals can perform these tasks:

>> Chat and collaborate with each other as well as with relevant external teams.

>> Run security commands in real-time (usually by leveraging chatbots).

>> Automatically document all commands, chats, and actions.

A collaboration platform powered by ChatOps results in some pretty impressive benefits.

Increased transparency

When a team of analysts collaborates on a single window, every chat, action, and command is tracked and visible to all parties. This information provides full transparency to both analysts and any external stakeholders with access who want to view progress. You can also track accountability and link ownership of tasks with specific analysts, aiding measurement and making successful tasks repeatable.

Knowledge management

Working in ChatOps provides robust one-stop archival of all actions, comments, and investigation commands. Because everything is indexed, the security database becomes a vault where all

analyst knowledge is stored for posterity. Personnel changes no longer engulf incident response (IR) in darkness, and greenhorn analysts can fall back on a wealth of historical precedent when dealing with unfamiliar incidents.

Faster response times

ChatOps uses a single window for collaboration, investigation, and documentation, eliminating the need to jump between screens. The chat-based interface encourages analysts to share knowledge and work together, and these joint investigations directly lead to a reduction in response times.

Look at Figure 2-2 for a visual definition of ChatOps.
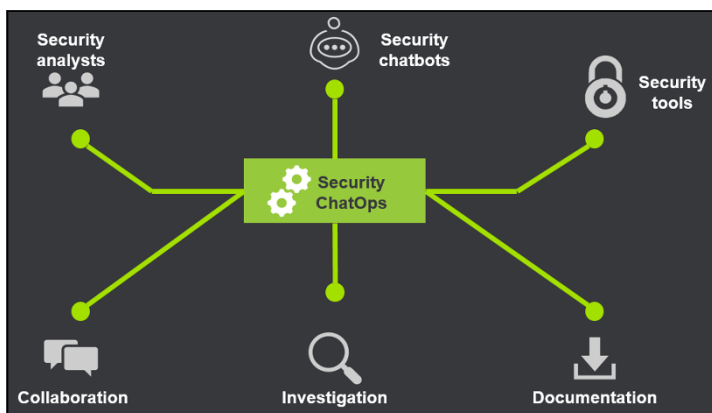
FIGURE 2-2: Chatting looks so much more professional in this diagram.

The People

The last piece of the security orchestration puzzle is perhaps the most important — security teams. Even when a security orchestration tool integrates with many products and has scores of playbooks, these efforts count for naught without humans to exercise oversight and discretion over when and how to use them. The machines haven't replaced us yet.

The major roles and responsibilities within a security operations center (SOC) are shown in Table 2-1.

TABLE 2-1 The Roles and Responsibilities within a SOC

Role	Responsibilities
SOC Analyst — Tier 1	Review alerts and triage them to determine severity. Open tickets for relevant alerts and forward to tier 2/tier 3 analysts. Run vulnerability scans and manage security monitoring tools.
SOC Analyst — Tier 2	Review tickets forwarded by tier 1 analyst. Collect data across tools, such as asset data, logs, and threat intel, to execute response efforts.
SOC Analyst — Tier 3	In addition to tier 2 responsibilities, this role is more proactive and focused on hunting threats. Review asset, vulnerability, and complex threat intel data to identify shortcomings and capture stealthy threats before they affect the organization.
SOC Manager	Supervise activities of the SOC team. Hire and train workforce, measure relevant metrics and generate reports for external stakeholders, create and execute strategic plans for the SOC.

REMEMBER

Table 2-1 is an illustrative description of SOC roles and responsibilities. Each organization might have a different division of labor between tiers of SOC analysts.

In this section, you look at a few ways in which security orchestration playbooks can work in concert with human teams for unified security operations and incident response.

Manual tasks

When an action is too unique, nuanced, or infrequent to be automated, security orchestration playbooks can have manual tasks that act as directives for the SOC analyst handling the respective incident. You can combine these manual tasks with automated tasks within a playbook, so you only bother analysts when their expertise is required.

Task approval

Even if some actions are prime candidates for automation, they might be too sensitive to carry out without having a human verify their need and relevance. Nobody wants to be the person that quarantines a CEO's laptop or shuts down a cloud instance

without a darn good reason. In such cases, automated actions can use built-in task approvals. These actions wait for the relevant SOC analyst's approval before beginning execution.

End-user engagement

If a security orchestration tool has rich integrations with email tools, these integrations can engage SOC analysts and end users within the organization to improve overall process flow. For example, if users log in from an unusual location, such as another country, the security orchestration tool can send a warning email as part of a playbook. This email can ask users to verify whether they're in another country, and different branches of the playbook can execute depending on the reply.

Bringing It All Together

Enterprise security has gotten many things right, but some critical gaps still exist between these areas of expertise. Security suffers from a lot of data but little follow-up, a lack of product interconnectivity, and a largely siloed workforce. See Chapter 1 for more information.

Security orchestration is well-placed to fill these gaps by leveraging multi-source data ingestion and correlation, an extensible product integration network, and playbooks and collaboration features that democratize a security team's knowledge. Table 2-2 explains how security orchestration fills in the gaps.

TABLE 2-2 **Filling in the Gaps with Security Orchestration**

Gap	How Security Orchestration Fills Gap
A lot of data but little follow-up	The security orchestration tool ingests data and performs actions based on automated playbooks.
Tools that don't talk to each other	Data from multiple products flows into the security orchestration tool for centralized collection and correlation of alerts.
People that don't talk to each other	Playbooks provide codified best practices for analysts to follow, removing variation in response quality. Collaboration features provide structure and documentation support during real-time investigations.

Figure 2-3 summarizes the components of security orchestration and how they come together to form a unified whole.

SIEM   EDR   NetSec   Email

Security Orchestration

Threat Intelligence

DevOps

Ticketing   UEBA   DLP   Malware Analysis

REST API
SOAP
SSH
HTTPS

Product **Integrations**

Playbook
Runbook
Workflow

Structured **Process**

Task Approval

End User Engagement

Human **Control**

Manual Tasks
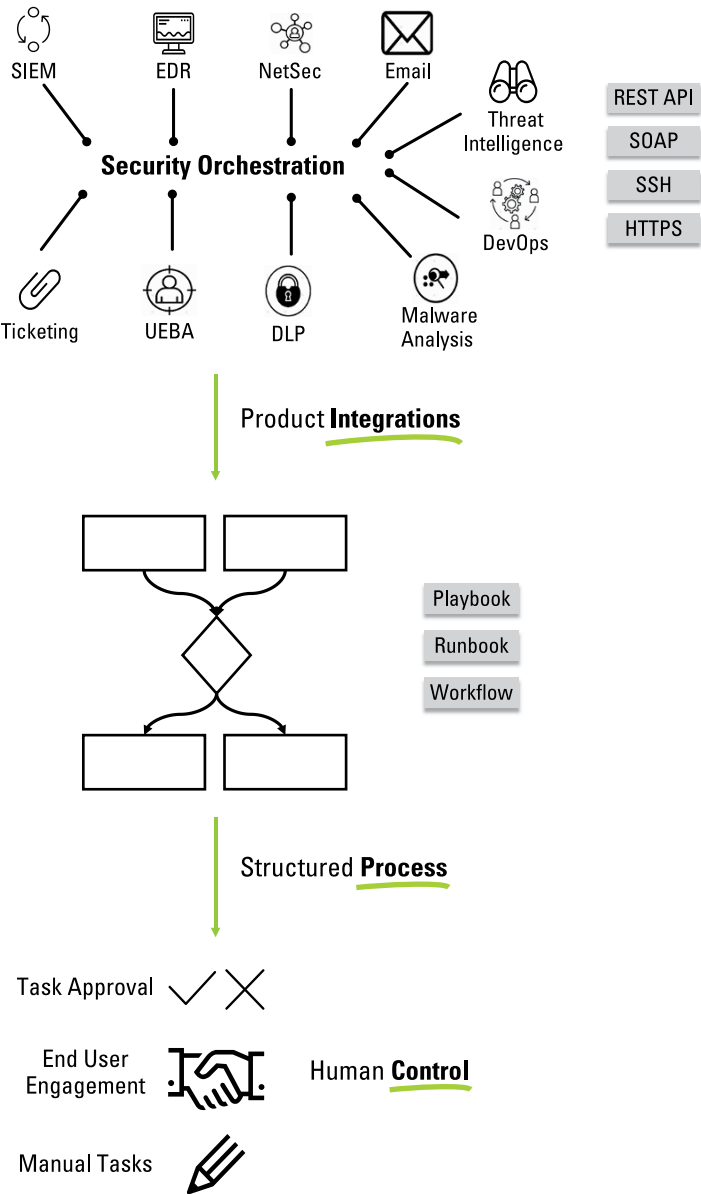
FIGURE 2-3: Presenting a unified security front.

IN THIS CHAPTER

» **Choosing relevant technologies**

» **Assigning roles and privileges**

» **Conceptualizing and implementing processes**

» **Considering different deployment and pricing options**

» **Measuring and improving security orchestration performance**

Chapter **3**

Conducting Your Security Orchestra: Implementation Best Practices

mplementing security orchestration within an organization is usually not a simple "I don't have it" to "Okay, now I have it" journey. Organizations need to evaluate their maturity, tool stack, existing processes, and choose their method of deployment accordingly. In this chapter, you take a look at all the moving parts within security orchestration, and I guide you in making (hopefully) wise choices.

Choosing Your Technology Stack

Security orchestration tools help an organization's existing prod-ucts work in unison and enable users to maximize the return on existing investments. Thus, a security orchestration tool will only

be as powerful as its inter-product connectivity and extensible integration network.

Broadly, security operations centers (SOCs) regularly use four types of products:

» **Security monitoring and detection tools:** These tools collect raw security-relevant data from a variety of sources for aggregation, correlation, and eventual alert detection. Examples include SIEMs, log management tools, and data analytics tools.

» **Data enrichment and intelligence tools:** These tools are used to analyze alerts and confirm or deny malicious activity via threat scores and unique analysis. Examples include threat intelligence tools and malware analysis tools.

» **Enforcement and response tools:** These tools are responsible for monitoring organizational systems and networks to ensure compliance as well as take enforcement actions when necessary. Examples include endpoint security tools, firewalls, and email gateways.

» **Allied and supporting tools:** These tools, while not directly related to security, are used in the SOC to improve efficiency or due to the lack of better alternatives. Examples include ticketing systems, email, and chat and messaging tools.

TIP

This categorization isn't strict, and some tools can simultaneously perform detection, enrichment, and response. These abilities depend on the tool's capabilities and how an organization chooses to use the tool.

REMEMBER

To fully leverage a security orchestration tool, it should act as a connective fiber between detection, enrichment, response, and allied tools. Organizations should work toward an end-state scenario where the security orchestration tool ingests alerts from detection tools and executes automated playbooks that coordinate actions across enrichment, response, and allied tools.

Feature Checklist for Technology Integrations

While evaluating a security orchestration tool with respect to integration capabilities, consider these concepts:

» Breadth and depth of integrations

» Option to deploy in-house or custom integrations

» Richness of APIs and number of commands/actions

» Simple classification and mapping of labels between products

» Bidirectional integrations that ensure push and pull of data

» A good mix among integrations with detection, enrichment, enforcement, and allied tools

You can also use this more robust checklist to evaluate your options:

» Extensible integration network

- How many integrations (breadth of categories and depth in each category) does the platform have?

- Are new integrations added to the platform with time? At what frequency? Are these updates free or add-on services?

» Custom integration capabilities

- Does the platform have a mechanism (for example, an internal SDK) to build custom integrations?

- Does the platform onboarding period include custom integration support from the services team? Are these services added on or part of the product purchase price?

» Integration depth

- For your chosen product stack, how many commands or actions can be executed from within the platform?

- For your chosen product stack, how many bidirectional integrations does the platform support?

>> Integration classification and mapping

- Does the platform have guidelines and in-product capabilities for easy classification and mapping of labels between products?

- Does the platform support the creation of custom incident types and fields and indicator types and fields?

>> Integrations with detection and monitoring tools

- For your chosen detection and monitoring tools, does the platform allow for both automatic alert ingestion and rule-based alert ingestion?

- Does the platform have bidirectional integrations with your chosen detection and monitoring tools, ensuring push and pull of data?

>> Integrations with data enrichment and intelligence tools

- For your chosen data enrichment and intelligence tools, how many commands and actions can be executed from within the platform?

- Does the platform have bidirectional integrations with your chosen data enrichment and intelligence tools, ensuring push and pull of data?

>> Integrations with enforcement and response tools

- For your chosen enforcement/response tools, how many commands and actions can be executed from within the platform?

- Does the platform have bidirectional integrations with your chosen enforcement and response tools, ensuring push and pull of data?

Looking at Roles and Privileges

While security orchestration tools are currently focused on the SOC, their playbooks have the potential for general purpose pro-cesses. Additionally, incident response might typically involve security teams, but external stakeholders also need to be kept abreast of major breach investigation statuses.

With these caveats in mind, organizations need to spend time on role definition and access while implementing security orchestration tools in their environments. See Chapter 2 for a brief overview of SOC roles.

While evaluating a security orchestration tool with respect to roles and privileges, here are some things to consider:

>> **Deciding levels of ownership:** Within the SOC workforce, organizations need to decide the level of ownership afforded to tier 1 to 3 analysts and SOC managers respectively.

>> **Choosing supporting users:** Apart from security teams, organizations should examine whether other teams need access to the security orchestration tool (for example, legal teams, IT teams, and DevOps teams) and, if they do, what level of access should be afforded to them.

>> **Pivots for access restriction:** Security orchestration tools have many potential elements with varying levels of sensitivity. For example, a product integration, a playbook, or an incident type might each need to have separate levels of restricted access. Consider the breadth of elements that can be granted varied access levels within the security orchestration platform.

>> **Centralizing authentication:** Using multiple security tools and maintaining separate login credentials for each one is a time-consuming exercise that security orchestration tools can potentially worsen. To avoid this misstep, organizations should verify the presence and robustness of user and device identity management (either native or through integrations) within security orchestration tools.

>> **Assigning roles to products:** Because security orchestration involves products talking to other products and automating actions, these conversations might involve the transfer and storage of username and password credentials. To avoid this exposure of sensitive assets, organizations should inspect whether the security orchestration tool can assign roles to products and avoid the repeated transfer of credentials.

The following checklist expands on features and capabilities to look for within a security orchestration tool when focusing on roles and privileges:

» **Granular role-based access control:** Does the platform allow for the creation of custom organizational roles? Does the platform allow for flexible permissions and authorizations per role? Does the platform have different pivots for role-based access control, such as restricted access to incidents, playbooks, dashboards, automation commands, and integrations?

» **Playbook approval flow:** Do the platform's playbooks have a task approval option for automated and manual tasks?

» **Keyless automations:** Does the platform have mechanisms to implement inter-product connectivity without the need for credential storage and transfer?

» **Authentication support:** Does the platform offer identity access management or integrate with products that offer identity access management?

Set Up Processes

The codification of processes is the bread and butter of a security orchestration tool. However, both right and wrong processes can be woven into security orchestration. A common mistake that organizations might make is implementing security orchestration when they don't have set processes, or the processes aren't a good fit for implementing security orchestration.

By jumping into process implementation too fast, organizations will not only fail to leverage the benefits of security orchestration but also potentially close the door on future security orchestration implementation when the need is more explicit.

Organizations should employ discretion while choosing which processes are prime candidates for security orchestration. Taking phishing enrichment and response as an example, Table 3-1 gives you a framework to evaluate process relevance.

TABLE 3-1 **Evaluating Process Relevance**

Criteria	Answers
Does phishing response involve a combination of automated and manual tasks?	**Yes.** Mail parsing, enrichment, and initial triage are automated. Deeper investigative actions are manual and performed by analysts.
Do you have trouble mapping incidents and tasks to specific analysts to track accountability?	**Yes.** It's tough to know which actions were performed, their order, their effectiveness, and who performed them.
Do you have trouble coordinating between security tools at your disposal?	**Yes**. During phishing response, different tools are used for mail lookup, indicator enrichment, ticket management, and endpoint protection.
Do you need to collate information from multiple sources for auditing and documentation?	**Yes** and **No.** Ticket management provides a good, broad audit trail, but you don't have task-specific visibility and lack a single documentation source for sophisticated investigations.
Are incident response times too long when analysts work separately (in silos) to resolve them?	**Yes.** There is often a back-and-forth where analysts perform an action, wait for feedback while analysts "down the queue" perform their actions, and have to usually change their work after receiving feedback.
Is your team experiencing alert fatigue?	**Yes.** Phishing attacks are frequent and easy to execute. You're witnessing rising alert numbers and varied attack vectors.
Are you facing challenges in training new analysts?	**Yes.** Senior analysts are too busy with day-to-day work to train junior analysts and there is no dynamic information source that junior analysts can access and experiment with to accelerate their training.
CONCLUSION	Pilot security orchestration for your phishing incident response.

Apart from selecting which processes to implement, organizations should also evaluate security orchestration vendors with respect to their overall case management and workflow capabilities.

The following checklist expands on desired features.

» Incident and case management

- Does the platform have native case management or integrate with relevant case management tools?
- Does the platform enable reconstruction of incident timelines?
- Does the platform support post-incident documentation and review?
- Does the platform create audit trails to highlight data flow and maintain accountability?

» Workflow and playbook capabilities

- Does the platform have workflow capabilities (visual task-based processes)?
- Does the platform show a live run of playbooks for each incident?
- Does the platform support nesting of playbooks?
- Does the platform support creation of custom playbook tasks (both automated and manual)?
- Does the platform support transfer of custom tasks across playbooks?

Considering Deployment and Pricing Options

After you have set up your technology stack, roles, and pro-cesses to align with a security orchestration tool, consider the deployment and pricing options available before finalizing implementation. Deployment and pricing are factors usually found "down the funnel" but can still result in a unique setup (or lack thereof).

Deployment flexibility

Technologies that organizations use to conduct their business and secure their data are constantly in a state of evolution and flux.

For example, the agility and scalability of the cloud may need to be matched with the regulatory need to keep data on premise. With all these moving pieces, choosing a security orchestration tool depends heavily on the flexibility of deployment options available and how those options align with other tools and requirements within the organization.

This checklist expands on desired features and capabilities to look for within a security orchestration tool when focusing on deployment options:

» Deployment flexibility

- Does the platform support both on-premise and cloud-hosted deployment options?

- Does the platform enable quick proof-of-concept tests with standardized data ingestion and use cases?

» Multitenancy and security

- Is the platform designed for multitenancy with full separation between master and child tenants?

- Does the platform support common playbook designs across tenants?

- Does the platform have full database and execution isolation for tenants?

- Does the platform support network segmentation for communication across organizational networks?

- Does the platform have a mechanism (for example, a dissolvable agent) to conduct remote operations without violating firewall rules?

» Scalability and availability

- Does the platform have horizontal scalability across multiple tenants?

- Does the platform support load balanced automations to improve computing efficiency?

- Does the platform have any level of guaranteed high availability, such as live backups, active backups, and failover and failback procedures?

Multitenancy is a mode of operation where multiple instances of an application (or multiple applications) exist in a shared environment. These instances are physically integrated (to some degree) but logically separate. For example, a Managed Security Services Provider (MSSP) might use multitenancy to logically isolate its customer instances.

Pricing

Because security orchestration is currently an emergent market, the pricing outlook is still fragmented for two reasons:

» If security orchestration is a product-line extension developed by a vendor, pricing outlooks usually carry over from other existing product lines, even if they may not make sense.

» Many buyers are still not able to accurately quantify the impact of security orchestration and are thus unable to decide what pricing level is acceptable to them. This situation sometimes leads to vendor discounts.

Consider what pricing method fits well with your overall budgeting processes before selecting a security orchestration tool. The prevalent pricing methods in the market today are as follows:

» Pricing per action or automation

» Pricing per node or endpoint

» Annual subscription with add-on prices for additional admin users

Improving Utilization with Iteration and Measurements

While the initial implementation of security orchestration might be a linear process, getting the most out of a security orchestration tool is a closed loop where iteration and measurement improve its utilization with time.

Tweaking a security orchestration platform after deployment is necessary for multiple reasons:

» **Cyberattacks are always evolving.** Every few months heralds a new attack vector, entry point, or technique of compromise. The incidents of tomorrow will be different from the incidents of today, and a security orchestration platform needs to adapt accordingly.

» **Every organization is different.** Segmentation by industry, size, or geographical location is useful up to a point, but eventually each organization and its security team have unique processes, incident classifications, SLAs, and terms used to define security concepts. A security orchestration platform must adapt to organizational needs rather than enforce vendor lock-in.

To support users with iteration, a security orchestration vendor should provide enough guidance during onboarding and should also include relevant customization options within the product. One of the driving forces behind iteration (as well as a good way to verify successful iteration) is through the measurement of relevant metrics. A security orchestration tool is the ideal place for measuring metrics because

» Data from multiple security tools flows into one console.

» Information about analyst processes and actions are captured in the platform.

» Security orchestration reduces alert volumes and response times (thus handing back more time to security teams for effective measurement).

REMEMBER

To support users with measurement, a security orchestration tool should support the creation of customizable dashboards and reports. While a standardized out-of-the-box collection of dashboards is a good start, organizational security is varied enough to require that users be able to create their own dashboards from scratch.

Another forward-thinking application of recording metrics is the learning that ensues and makes security teams perform better.

While not a core feature of security orchestration, supporting learning and knowledge management mechanisms within the product can have multiplicative effects on response efficiency and analyst productivity.

This checklist expands on the desired features and capabilities to look for within a security orchestration tool when focusing on post–deployment iteration and measurement:

>> Post-deployment customization

- Does the platform contain response templates or afford the capability to create response templates for industry standards, such as NIST and CERT?

- Does the platform enable the creation of custom incident types and labels?

- Does the platform enable the creation of custom indicator types and labels?

- Does the platform support both standardized and custom incident summary layouts?

>> SLA measurement and tracking

- Does the platform enable the measurement of incident, indicator, and analyst level metrics?

- Does the platform allow for custom dashboard creation with user-driven widgets and templates?

- Does the platform support custom reports that can both be generated in real-time and scheduled at pre-determined intervals?

>> Knowledge management and learning

- Does the platform automatically document all commands, analyst comments, and actions for posterity?

- Does the platform contain learning mechanisms that give insights into analyst productivity, response efficiency, and the most effective security actions?

>> Customer support

- Does the platform include in-product walkthroughs, tutorials, and help menus?

- Does the platform include an external documentation portal with best practices, instructions, and illustrative examples?

- Does the platform onboarding include use case formulation, integration and playbook support, and product training?

- Does the platform provide ongoing support through multiple channels, such as a 24/7 phone line, online support, or on-site support?

IN THIS CHAPTER

» **Enhancing and enriching your response to phishing alerts**

» **Securing and protecting endpoints**

» **Managing your vulnerabilities**

» **Hunting down potential threats**

» **Evaluating the severity of threats**

Chapter **4**

Security Orchestration in Action

I n previous chapters, I present you with the enterprise security challenges that drive the need for security orchestration, discuss a working definition of security orchestration with its interconnected parts, and lay out best practices to implement security orchestration in your organization. Now, you look at that theory in practice.

In this chapter, you see the major benefits of security orchestration and go through specific use cases to highlight how security orchestration playbooks can help improve response times.

Bringing the Benefits of Security Orchestration into Reality

Proper implementation of security orchestration results in improvements across security teams, security processes, and security technologies. For security teams, automating and unifying actions across environments can increase their productivity and free up their time for important decision-making and strategic activities that they were too busy to perform before.

For security processes, standardized incident response steps can remove quality variance and scale these processes to meet grow-ing alert volumes. For security technologies, unifying actions across a security operations center's (SOC) entire product stack can enable security teams to maximize the returns on existing security and IT investments.

TIP

The benefits of security orchestration are as follows:

>> **Accelerates incident response:** By replacing low-level manual tasks with corresponding automations, security orchestration can shave off large chunks from incident response times while also improving accuracy and employee satisfaction.

>> **Standardizes and scales processes:** Through step-wise, replicable workflows, security orchestration can help standardize incident enrichment and response processes that increases the baseline quality of response and is primed for scale.

>> **Unifies security infrastructures:** A security orchestration platform can act as a connective fabric that runs through hitherto disparate security products, providing analysts with a central console through which to action incident response.

>> **Increases analyst productivity:** Because low-level tasks are automated and processes are standardized, analysts can spend their time making decisions and charting future security improvements instead of getting mired in grunt-work.

>> **Leverages existing investments:** By automating repeatable actions and minimizing console-switching, security orches-tration enables teams to coordinate among multiple products easily and extract more value out of existing security investments.

>> **Improves overall security posture:** The sum of all benefits is an overall improvement of the organization's security posture and a corresponding reduction in security and business risk.

Let's Skip the Phishing Trip

Just like lowly ants can send mighty elephants scurrying away in terror, simple phishing emails can bring multinational enterprises to their knees. Therefore, phishing enrichment and response is the perfect place to begin the use case discussions for security orchestration.

REMEMBER

Phishing is the practice of sending fraudulent emails that pretend to be from reputable sources and are meant to either extract ("fish out") personal information from the target or infect the target's system with malware.

Phishing emails are one of the most frequent, easily executable, and harmful security attacks that organizations — regardless of size — face today. According to research by the SANS Institute, 95 percent of all attacks on enterprise networks are the result of successful *spear phishing* (which is just another name for a targeted and personalized phishing attempt).

Current drawbacks

Security teams face numerous challenges while responding to phishing attacks. Because phishing attacks are so quick and easy to execute, security teams usually face high attack numbers. It's a challenge to not only respond to all these alerts without burning out but also to sift through each alert to ascertain whether it's genuinely malicious or a false positive.

Response to phishing attacks involves coordinating among multiple security products. Security teams usually conduct this coordination manually due to a lack of inter-product connectivity, leading to an increased error rate while completing mundane tasks and a lack of standardization in response processes and reporting procedures.

How orchestration helps

Security orchestration platforms include 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 with more time to deal with genuine phishing attacks and prevents these attacks from slipping through the cracks, as shown in Figure 4-1.
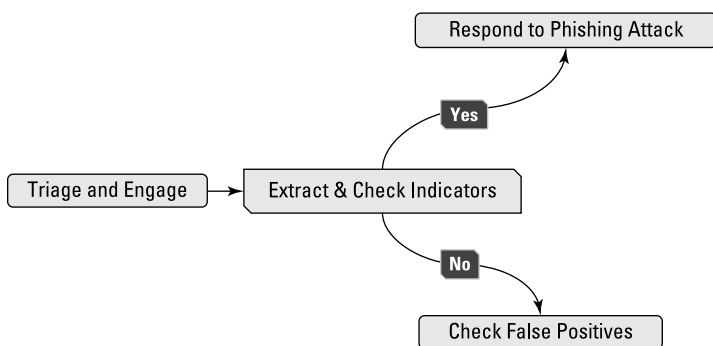
FIGURE 4-1: Orchestrating your phishing response.

Take a walk through one example of a phishing playbook:

1. **Ingestion.**

   A security orchestration platform can ingest suspected phishing emails as alerts from a variety of detection sources such as SIEMs and logging services. If the SOC aggregates all suspected phishing emails in a common mailbox, then a mail listener integration can be configured on the orchestration platform for ingestion. After the email is ingested, a playbook is triggered and goes through steps to automate enrichment and response.

2. **Enrichment.**

   To keep the end-users updated, the playbook sends an automated email to affected users and lets them know that the suspected phishing email is being investigated. The playbook can perform two key steps for enrichment:

   a. Triage

   b. Indicator of Compromise (IOC) extraction

   An IOC is any artifact (such as a URL, an IP address, or an MD5 hash) that, after observation, indicates with a high confidence that an intrusion or attack has occurred.

   By looking at the ingredients of the email, such as title, email address, and attachments, the playbook assigns alert severity by cross-referencing these details against external threat databases. The playbook extracts IOCs from the email and checks for any reputational red flags from existing threat intelligence tools that the SOC uses. After this enrichment is done, the playbook checks if any malicious indicators were found. Based on this check, different branches of response can ensue.

3. **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 deletes all instances to avoid further damage. Finally, the playbook adds the malicious IOCs to blacklists/watchlists on the SOC's other tools.

TECHNICAL STUFF

If malicious indicators weren't detected, precautions are still taken before confirming that the email is harmless. The playbook checks if any attachments exist within the email and detonates 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. After 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.

Protecting Endpoints

With the surfeit of devices present over organizational networks today, their connections with each other and to the network at large creates new attack paths for security threats. Employee devices, such as laptops, desktops, and mobile phones, must be properly equipped with protection measures to both prevent attacks and respond to any threats that get through defenses.

Current drawbacks

Endpoint protection is a critical part of enterprise security, but it's unfortunately overcome with implementation challenges. Security teams often have to coordinate between endpoint tools and other security tools, using multiple consoles 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 4-2 shows an example of this workflow.
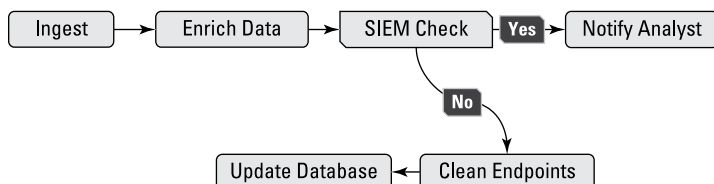
FIGURE 4-2: Orchestrating endpoint protection.

Here's a rough walkthrough of one possible endpoint protection playbook:

1. **Ingestion.**

   The playbook ingests threat feed data from an endpoint tool.

2. **Enrichment.**

   The playbook queries the endpoint tool for machine and endpoint names with malicious indicators such as SHA1, MD5, and SHA256.

3. **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. The playbook notifies the analyst if SIEM-led actions have already resolved any malicious indicators.

4. **Clean endpoints.**

   For any indicators not picked up by the SIEM, the playbook communicates with either the same endpoint tool or a different one, depending on how many the SOC uses, to run queries across endpoints. These queries can kill malicious processes, remove infected files, and more, depending upon the endpoint tool's capabilities.

5. **Update database.**

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

I Feel so Vulnerable . . .

Although incident response is traditionally thought of as a reactive practice, it's equally important for security teams to continuously monitor their organizational environments for vulnerabilities and remediate any vulnerabilities that are discovered.

REMEMBER

In security terms, a vulnerability is any system weakness that can be exploited by malicious actors, such as attackers, to execute unauthorized actions on the target system.

Current drawbacks

Vulnerability management is a strategically important process that covers both proactive and reactive aspects of security operations. Because 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 process 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 4-3 shows one such example.
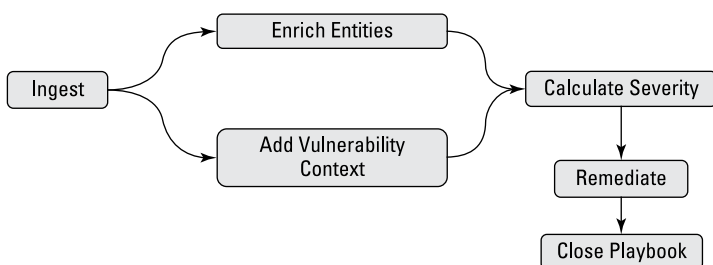
FIGURE 4-3: Managing vulnerabilities with security orchestration.

Check out a rough walkthrough of one possible vulnerability management playbook:

1. **Ingestion.**

    The playbook ingests asset and vulnerability information from a vulnerability management tool.

2. **Enrich entities.**

    The playbook enriches endpoint and Common Vulnerabilities and Exposures (CVE) data through integrations with relevant tools. It also adds custom fields to the alert if the newly gathered data requires additional context.

3. **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 alert data.

4. **Calculate severity.**

   Based on the gathered context, the playbook calculates the severity of the alert. For more information about how this severity setting process works, see the later section "Setting Alert Severity."

5. **Remediate.**

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

Be Very Quiet; I'm Hunting Threats!

Just like vulnerability management, threat hunting is another proactive practice that security teams should align with traditional reactive processes. This practice maintains a balance between catching undetected threats and dealing with threats that have already been detected.

REMEMBER

Threat hunting is a proactive process of searching through security tools and environments to identify and respond to threats that have evaded existing security solutions.

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 tools help with threat hunting in two ways. Firstly, automated playbooks for incident response free up analyst

time to focus on proactive tasks such as threat hunting. Secondly, 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.

These playbooks can be run in real-time or scheduled at predetermined intervals, ensuring both proactive and reactive approaches to threat hunting (as shown in Figure 4-4).
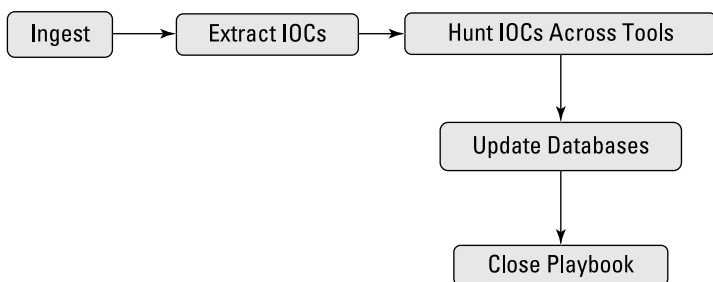
FIGURE 4-4: Hunting down threats with security orchestration.

Look at this rough walkthrough of one possible threat hunting playbook:

1. **Ingestion.**

   The playbook ingests a list of IOCs as attached CSV or TXT files.

2. **Extract IOCs.**

   The playbook extracts the IOCs, including IP addresses, domains, and hashes, from the CSV and TXT files using regular expressions.

3. **Hunt IOCs across tools.**

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

4. **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.

TECHNICAL STUFF

A *regular expression* (or regex) is a sequence or pattern used to find or find and replace string sequences. They're used in search engines, word processors, and the threat hunting playbook as illustrated in Figure 4-4.

Setting Alert Severity

A big reason why high alert volume continues to be a challenge for security teams is the inability to quickly, accurately, and repeatedly assign a severity level to alerts.

Current drawbacks

As SOCs start expanding their security product stack, each product sends out its own alerts. This process results 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 attacks might slip through the cracks and result in real organizational harm. If the detection is 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 alert is ingested into a security orchestration platform, a severity scoring playbook can reconcile alert severity across data-sets and assign the correct priority to the alert, ensuring that analysts can give their attention to the most critical alerts first (as shown in Figure 4-5).
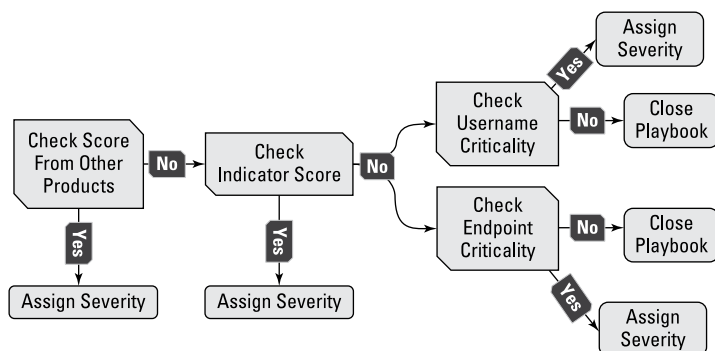
FIGURE 4-5: Choosing which alerts to deal with first.

Take a look at this possible alert severity assignment playbook:

1. **Check external product scores.**

    The playbook first validates whether any external vulnerability management products have recorded a severity level for the alert at hand. If there is a severity score recorded within any of these products, the playbook assigns the same severity to the alert. This process ensures that security teams use the strengths of their security products without having multiple tabs open and manually performing low-level actions.

2. **Check indicator scores.**

    If there's no third-party severity input, the playbook checks the indicators, such as IP addresses, domains, and hashes, found with the alert and validates whether there's a threat score attached to any indicator. If there is a score attached to any indicator, the playbook assigns a high, medium, or low severity to the alert accordingly.

3. **Check critical entities.**

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

REMEMBER

If SOCs integrate with multiple threat intelligence products, the indicator score is an ideal way to utilize the insights from each product through a combined reputation rating. Some security orchestration platforms automatically record all indicators that are ingested as part of alerts, assigning each indicator a reputation score based on an amalgamation of scores from other threat intelligence platforms that the SOC integrates with.

TIP

To explore more processes where security orchestration can help, read Demisto's whitepaper on popular security orchestration use cases: https://go.demisto.com/top-security-orchestration-use-cases.

Chapter **5**

Where You Go From Here

Enterprise security, and security orchestration in particular, is a rapidly evolving space. New features are developed and deployed in months rather than years, so you'll need to deal with new users, new use cases, and different use cases for existing users. It's almost too much to deal with on your own. Fortunately, security orchestration is poised to help.

In this chapter, you look at how security orchestration's evolution results in use cases outside the existing realms of security and incident response.

Moving Beyond Security

Security operations centers (SOCs) are usually isolated from other teams in the organization that are also responsible for security. Even within SOCs, response to incidents understandably takes precedence over more operational, day-to-day activities that, if performed regularly, would lead to fewer incidents in the first place.

These scenarios and use cases show where security orchestration tools can leverage their unique capabilities to make a difference.

Compliance and breach notification

While responding to breaches on a security front can involve isolated teams, broader response usually requires coordinated participation from PR and media teams, legal departments, and IT teams to implement correctly. You need to respond with a single voice and unified effort. With the enforcement of GDPR and United States state breach notification laws, you can't afford the organizational consequences of handling a data breach in a suboptimal manner.

Security orchestration tools, when combined with process knowledge within the organization, can be used to execute compliance and breach notification playbooks that will run in parallel to standard incident response playbooks. You can populate these playbooks with notification templates, contact details of law enforcement officials, and best practices to follow in the event of a breach.

Just like incident response playbooks, these compliance playbooks ensure that organizations follow the same process every time and eliminate any variance in response quality.

Examples of compliance playbooks include the following:

» PCI compliance

» HIPAA compliance (for healthcare organizations)

» GLBA compliance (for financial organizations)

» Breach notification process

» Mapping to NIST information security standards

IT operations

Security and IT teams are too busy fulfilling their intended responsibilities to coordinate on activities that need their joint attention. Rather than leading to outright breaches, this lack of coordination results in exposed assets and vulnerabilities that act as prime targets for attackers.

Security orchestration tools can bridge the divide between IT and security through playbooks that span across products, teams, and processes on both sides of the aisle.

For instance, a playbook can run at regular intervals and check all organizational endpoints for vulnerable or outdated SSL certificates. For every vulnerable SSL certificate found, the playbook can inform the affected user and relevant members from both IT and security teams to take further action.

These playbooks will provide an initial framework for IT and security teams to work together in a standardized manner with full transparency and documented task accountability for each team.

Examples of IT operations playbooks include

>> SSL certificate compliance check
>> Provisioning and deprovisioning users
>> Employee and device onboarding
>> VPN checks
>> Failed login follow-ups

The alphabet soup of DevSecOps

While the SOC is responsible for protecting an organization's employees, systems, and data from cyberattacks, another fast-rising outlook towards security called DevSecOps aims to weave security into the entire product development and deployment life cycle.

DevSecOps is a collection of tools, processes, and mindsets that have the aim of instilling security across the product development and deployment lifecycle. DevSecOps visualizes security as everyone's responsibility instead of just the security team's responsibility.

TECHNICAL STUFF

For more information on DevSecOps, you can visit this link: `www.devsecops.org/blog/2015/2/15/what-is-devsecops`.

Organizations with a DevSecOps mindset are defined by agile product development, rapid cross-team collaboration, and quick iteration on a security front. In these scenarios, security

orchestration tools can act as a vital connective tissue across a vast number of tools. Use cases involving security orchestration within DevSecOps are still being discovered, but here are a few examples from integrations with relevant security and operational products:

» Monitoring potentially open ports and vulnerabilities in the product code

» Provisioning and deprovisioning cloud infrastructure instances

» Recording incident timelines and evidence for posterity

» Providing a collaboration platform between security, operations, and development teams

Head in the Clouds

Increased cloud adoption has improved organizational agility, reduced products' time-to-market, and leveled the playing field with respect to computational power. However, this implementation has also resulted in disparate environments that security teams struggle to monitor regularly. This challenge is especially relevant if the security teams are isolated from other teams that deal with DevOps, cloud infrastructure setup, and product development.

TECHNICAL STUFF

The cloud is a shared pool of storage, computing, and networking resources that can be provisioned on-demand, scaled, and customized to end user requirements.

In this section, you look at a few cloud-specific security challenges that go unaccounted for today.

Different deployment models demand security agility

Cloud deployment is flexible by nature and depends on organizational requirements, with a mixture of public, private, and hybrid deployments visible in the market. Even within an organization, production and development environments might be provisioned on different clouds, leading to fragmented compliance processes

and improper device encryption techniques. The bottom line is, cloud provisioning and usage is very agile, which demands a corresponding agility and flexibility in securing these environments.

Limited visibility demands central security oversight

Cloud adoption has expanded the computing surface but also the threat surface for organizations, creating disparate ecosystems that hamper visibility. The geographical expanse over which resources are spread leads to a "Shadow IT" problem and a lack of perimeter enforcement. A disconnect between cloud and on-premise environments also hampers security efforts, both during day-to-day operations and incident response.

Exposed assets demand secure identity access management

Exposed account credentials on the cloud are being accessed by attackers with worrying frequency and being used as entry points for account hijacks and lateral movement. You need to only look back to a 2017 car service hack, where attackers found account credentials on a third-party cloud-based service and were able to access sensitive user data. An important part of cloud security should be enabling current levels of performance and inter-product connectivity without sacrificing security through weak credential management.

These needs and challenges align well with some critical features that security orchestration tools provide:

>> First, the extensible technology integrations and automatable actions that security orchestration tools provide can prime organizations for agile cloud incident response. Responding to alerts due to errant behavior on the cloud might require quick deprovisioning of cloud instances, revocation of user privileges, compliance checks, and more. Executing as many of these actions as possible at machine speed will result in improved accuracy and lower response times.

REMEMBER

In a cloud-first world, where each second of downtime can cost millions, these automations can make a critical difference.

>> Next, the standardized task-based workflows that security orchestration tools provide can help bridge the divide between cloud and on-premise environments. These playbooks can integrate with multiple security and IT tools to provide centralized, correlated data to security teams and enable them to visualize wider attack patterns rather than be stuck in ecosystem-based silos.

>> Finally, security orchestration tools can provide scalable cloud security automation without the need for managing user credentials and passwords. This keyless automation driven by security orchestration tools can pave the way for coordinated and automated response but with products "talking" with each other without exchanging sensitive login credentials that might be compromised.

Keyless automation can be driven by security orchestration tools if they integrate with an identity access management solution and use that integration to execute role–based rather than credential–based calls to other products. Figure 5-1 shows just such an example.
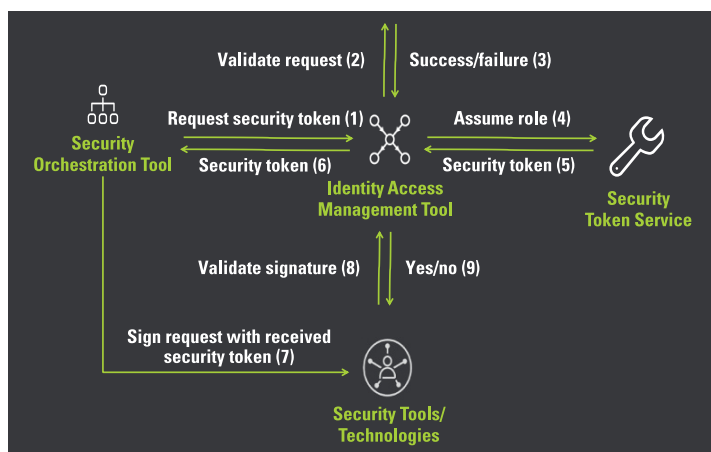
FIGURE 5-1: An example of keyless automation.

Always Be Learning

While security orchestration platforms help reduce response times through standardized playbooks and automated actions, just those features applied across use cases will result in a plateauing

of benefits with time. One way to deliver organizational value that compounds with time is through insights driven by machine learning.

Machine learning provokes reactions of both endless potential and considerable skepticism. But security orchestration tools occupy a unique position in the security landscape because

» These tools collect and correlate data from multiple security products.

» Teams can use these tools to execute actions across their product stack.

» These tools provide a platform to document analyst actions, comments, and incident evidence.

» These tools ingest a wide variety of incident data and indicator information.

Machine learning can help you make the best use of this data and extract greater value from existing security tools. Keeping these differentiators in mind, these use cases show where security orchestration tools can use machine learning to improve the efficiency of user operations.

Incident owner recommendations

As SOCs scale, they end up following a "whoever's available" approach for assigning incident owners. This approach not only leads to uneven load times for analysts who are already overworked but also results in analyst expertise getting ignored while deciding assignment. Improperly assigned incidents eventually lead to improperly handled incidents.

Whenever incident owners are assigned within security orchestration tools, machine learning algorithms can study details of all past incidents in the system including incident types and category fields. This data can then be cross-referenced with existing analyst loads to give the top two or three analysts to own the incident.

These suggestions ensure that load time is not the only criterion considered during incident assignment. By studying incident types and fields, a security orchestration tool can suggest analysts that are best suited to own incidents with respect to both time and expertise.

Security expert suggestions

End-to-end handling of incident response is rarely an isolated process. Unfortunately, SOC analysts often operate in silos while performing investigations, oblivious to their colleagues' specific skill sets that might come in handy for complex incidents. Junior analysts especially operate in the dark here, left to contend with investigations alone as senior analysts are occupied with other day-to-day operations.

A security orchestration platform can enable collaborative response where analysts can invite their teammates to conduct joint investigations. Here, machine learning algorithms study the history of all closed incidents, specifically looking at manual actions performed by analysts in the past. After parsing through this data, the security orchestration platform can suggest the top two or three analysts that can provide relevant assistance for a particular incident.

By both enabling joint investigations and facilitating intelligent team composition, a security orchestration platform can herald a consistent decrease in resolution times and increase in resolution quality. This feature can also act as a guiding hand for junior analysts by highlighting which experts can help them through specific investigations, thus reducing error rate and analyst anxiety.

Commonly used security commands

While conducting real-time investigations after incident triage, analysts literally have hundreds of possible security actions to choose from. As SOCs keep expanding their product stack, there is an observed divergence in the type, order, and fidelity of security actions taken from analyst to analyst. This leads to varying resolution times and quality for similar incidents, which can negatively impact SLAs and metric tracking.

A security orchestration platform can study manual commands that were used for all incidents in the past. This data can enable recommendations on which security commands to run first for a particular incident. Even if analysts have already run some

commands and are stuck in the middle of an investigation, machine learning suggestions can set them on the right path with commands they might have missed.

Security command suggestions move analysts toward standardized response and guarantee that no commonly used actions are missed out for an isolated incident. Ultimately, this can help maintain and improve SOC service-level agreements (SLAs) by preventing rogue investigation processes that miss out on critical actions.

Simplifying playbook creation

After playbooks make the initial journey from paper (or the analysts' minds) onto security orchestration platforms, they facilitate automated response but may not undergo any further measurement and review. Unless analysts capture better knowledge from elsewhere and feed it into the platform, the benefits of these playbooks plateau after a period of time.

To prevent this, security orchestration platforms can use machine learning to accelerate the creation of relevant playbook tasks. While creating playbook tasks and selecting inputs, analysts can see suggestions for arguments and parameters that fit best with those inputs. Machine learning algorithms can go through all existing playbook tasks (both out-of-box and within customer environments) and study frequency of task parameters to identify commonly used arguments.

Rather than stopping at alert fatigue reduction and quicker triage, security orchestration playbooks can use machine learning to always traverse the path of improvement through more efficient tasks. This process helps tackle the eventual stagnation in efficacy of static playbooks and ensures that even playbooks go to digital gyms to get leaner.

TIP

To explore how Demisto's machine learning helps security and IT teams improve their response processes with time, you can read a whitepaper on machine learning use cases by visiting `https://go.demisto.com/demistos-top-machine-learning-use-cases`.

Internet of (Vulnerable) Things

Progressions in device computing and processing have resulted in the creation of a wide variety of Internet-connected devices, spanning everything from cars and refrigerators to watches and industrial machinery. But while these devices have made your business and lives easier, the security advancements tied to the devices haven't kept pace with the technological advancements.

In June 2018, major retailers stopped selling toys from an IoT toy manufacturer after more than 2 million recorded messages were leaked in a major security breach. Some additional security compromises have involved medical devices being turned off by remote hackers, researchers exposing flaws in Michigan's traffic lights, and millions of automobiles being recalled after a remote hack. Ultimately, each connected device that joins the big bad World Wide Web brings additional security mysteries to the fore.

The key IoT challenges identified in this section can impact your organization's security.

Square pegs in round holes

Organizations may struggle to achieve competence in multiple fields. Whenever a product company makes an IoT-enabled device,

it struggles to reconcile its expertise in its original industry with its unfamiliarity in Internet connectivity and security. This inattention results in manufacturers having outdated or non-existent operating systems and patching features on their products, being lax with password protection and changes, and lacking regular software update mechanisms to communicate to their customers.

Insecure supply chains

Many physical products have complex supply chains with outsourced production, cost-saving exercises, and clearly defined team structures. It's an expensive and — from the companies' point of view — unnecessary undertaking to weave device security into the process when there's no requirement for it.

Attack by proxy

The range of dangers posed by IoT attacks is so great because of their interconnected and dual nature. Because the devices serve an offline purpose (like a TV or fridge) but are also connected to the internet, they can be compromised without affecting their original purpose, making the compromise harder to spot. And because they're interconnected, one loose stone can quickly lead to an avalanche.

Lack of regulation

Recent years have brought welcome strides in IoT security regulation. While the IoT Cybersecurity Improvement Act of 2017 is a good start, the industry still lacks a unifying, robust piece of legislation that puts the onus on vendors to comply with requirements or face consequences. Because IoT sits at the intersection of technology and a bevy of other industries, governments face a challenge to enact legislation that intersects across these industries, doesn't impose unfair restrictions, but also doesn't leave requirements too lax to make any difference.

The features inherent in security orchestration tools can fill in these IoT security gaps to a great extent. Specifically, security orchestration tools can bridge the gap between IT and operational technology (OT) environments. OT alerts can be ingested into security orchestration tools along with relevant data such as asset details, part alerts, and connectivity information. These alerts enable security teams to perform enforcement actions either

automatically or upon approval as part of playbooks that include both IT and OT information. Enforcement actions might include adding firewall rules, issuing malware scans, and so on.

REMEMBER

OT is a combination of hardware and software that's responsible for monitoring and altering the states of physical (usually industrial) devices such as valves and pumps.

Security teams can also utilize a security orchestration tool's integration with industrial network protection products to build a detailed OT exposure map whenever suspicious activity or infections occur on IT networks. These integrations can enable collection of asset data, connectivity data, anomalies, and past OT events into the security orchestration tool, helping security teams identify exposed and vulnerable assets in the OT network. This functionality enables security teams to either proactively identify OT vulnerabilities and threats or — if the OT networks are already infected — to respond to attacks in an efficient, standardized, and cross-platform manner.

Chapter **6**

Ten Myths about Security Orchestration

Because security orchestration is still an evolving space with competing definitions and maturing feature sets, you might encounter some misconceptions that exist about its scope of use, consequences, and effort required in deployment. Remember, we still can't agree on how to pronounce GIF, so a little uncertainty on more nebulous concepts is natural.

This chapter gives you ten myths about security orchestration that I've tried to clarify throughout this book (I hope!). These myths don't quite reach the heroic scales of Hercules and the Nemean Lion, but they are interesting and insightful nonetheless.

Security Orchestration Will Replace Your Security Teams

Automation always has a negative connotation with respect to job replacement and a removal of the human element. But in security orchestration's case, nothing could be further from the truth. Security orchestration aims to achieve a balance between

machine-powered automation and human-powered decision-making to improve security operations.

In an ideal security orchestration process, only the tasks that are repetitive, time-consuming, and not intellectually stimulating are automated. Any action that requires further human investigation or approval, whether through email response, task approval, or collaboration, will be open for security teams to weigh in.

Security Orchestration is a Fancy Term for SIEMs

Almost every organization that's serious about security has a Security Information and Event Management (SIEM) tool deployed in its environment. SIEM tools and security orchestration tools have some feature similarities on the surface such as automation of actions, product integrations, and correlation of data. However, it's incorrect to assume that either tool could do the job of the other.

TECHNICAL STUFF

SIEM tools monitor various sources for machine data, correlate and aggregate them for context, and provide real-time detection and monitoring of alerts generated by applications and network hardware.

While SIEMs deal with collection of machine data, correlation, and aggregation, current SIEM tools don't have the capabilities to coordinate further enrichment of alerts and automate response to alerts. Likewise, security orchestration tools can coordinate and automate cross-product response to alerts, but they can't currently detect these alerts to begin with. In this scenario, SIEMs collect disparate pieces of data and aggregate them into alerts, and security orchestration tools take alerts and drive them to response.

In the future, if SIEMs incorporate cross-product playbooks and response automations, they will still not be equivalent to security orchestration tools because of SIEMs' relatively narrow focus of detection. Security orchestration tools are poised to be general-purpose process and response solutions for security and IT teams that will ingest alerts (maybe from SIEMs), vulnerabilities, emails, cloud data, and correlate all these disparate data sets before driving automated resolution, as shown in Figure 6-1.
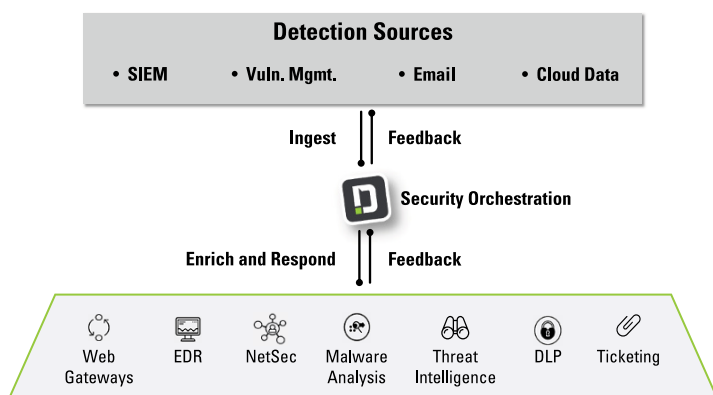
FIGURE 6-1: Take in alerts, push out automated resolution.

REMEMBER

SIEMs collect disparate pieces of data and aggregate them into alerts, while security orchestration tools ingest alerts and drive them to response.

Any Technology with Playbooks is Security Orchestration

As with any new industry term that gains adoption and market buzz, security orchestration's rise has led to a parade of ven-dors attaching the security orchestration name to their products, whether genuine or not.

TIP

To separate true security orchestration from the rest of the band-wagon, follow these tips:

» **Determine the scope of use:** If a security orchestration tool is narrow in its scope of focus (for example, just dealing with phishing response), then it's not a true security orchestration tool. Security orchestration is defined by its general-purpose nature and execution across a wide range of use cases.

» **Examine the range of integrations:** A security orchestra-tion tool is only as strong as its partner integration network. If a vendor builds a security orchestration product-line extension just to strengthen its initial products and limit other integrations, such a product doesn't align with security orchestration's true tenets.

>> **Verify the customizability of the technology:** Out-of-the-box, vendor-provided content such as playbooks, automation tasks, and product integrations should just be the foundation instead of the whole building. Users should be free to build their own combination of automated and manual tasks, custom playbooks, in-house integrations, and more.

Security Orchestration and Security Automation are the Same Thing

While educating users on new technologies, people in the industry sometimes enthusiastically, and incorrectly, interchange the terms *security orchestration* and *security automation.* Security automation makes machines do task-oriented human work. Security orchestration executes tasks using the interconnectivity of different products (both security and non-security) and automates tasks across products through workflows. Security orchestration also allows for end-user oversight and interaction.

Security automation is a subset of security orchestration. Security orchestration involves the combination of people, processes, and technology to improve an organization's security posture. Security automation is more focused on the technology aspect of the aforementioned trio.

Security Orchestration Playbooks are "One Size Fits All"

Unfortunately, no security orchestration playbook is a one-shot panacea for an organization's process woes. Vendor-provided playbooks are meant to be both teaching material and guidelines for users to follow and build their own (undoubtedly better) playbooks.

Out-of-the-box playbooks can be useful because they combine best practices across customer deployments that a vendor has been privy to. Ultimately though, security is an organization-based

practice. A company's security processes are perfectly tailored to its industry, hierarchies, and level of agility. Playbooks should reflect the same degree of personalization. A good security orchestration tool provides users with this flexibility.

Security Orchestration is Only Meant for Large Enterprises

Because security orchestration involves the coordination of actions across multiple security products, people often assume that only large enterprises with well-defined security operations centers (SOCs) and a wide range of products will extract value out of security orchestration. But with a 2018 Verizon report claiming that 58 percent of data breach victims are small businesses, the need for repeatable and automated alert response is apparent for companies of any size.

Even SOCs with a small team of three to five security analysts and a handful of tools can benefit from security orchestration through well-defined processes, increased team productivity, and setting the SOC up for eventual scale. Smaller firms can also use Managed Security Service Providers (MSSPs) to oversee their security posture. These providers can use security orchestration tools to provide a valuable console for collaboration and data centralization.

Every Security Process can (and should) be Automated

"Automate or die" is a pithy, marketing-friendly way to convey the urgency and need for automation, but it incorrectly paints the situation in black and white. Not every security process and action can (or even should) be automated.

Some tasks continue to be too sensitive for unsupervised automation and require manual approval processes. Some tasks continue to be too sophisticated and nuanced for machine execution and require security teams. For those high-quantity, repeatable tasks, however, bring on that automation!

Creating Playbooks Will Require Coding Expertise

Although coding expertise is never a bad thing to have, security orchestration tools provide layers of abstraction to help level the playing field and increase the productivity of employees who are experienced in security practices, but may be out-of-touch with coding.

To aid in your efforts, security orchestration tools should ideally provide these features:

» Visual task-based flowchart views for playbook creation and editing

» Drag-and-drop menus for choosing security automations and product integrations

» Classification wizards for mapping data values between various products and standardizing data collection formats within the security orchestration tool

While knowledge of Python, JSON file handling, and JavaScript will always help, security orchestration tools should aim toward the ideal of codeless automation and keep on refining feature sets until they get there.

Just Deploying a Security Orchestration Tool Will Solve My Security Problems

Security orchestration is not an end-state, but a journey of constant flux and churn. After the initial deployment of security orchestration tools, organizations need to iterate and keep tweaking elements of their security outlook, such as the following:

» Verify the effectiveness of playbooks and make them more concise or descriptive, according to requirements.

» Add new security tools to and remove existing security tools from the product stack.

>> Conduct regular process audits and search for currently manual processes that can be automated with time.

>> Create and review dashboards for specific security analysts, alert types, and product integrations to measure what's good and what can be made better.

Security Orchestration is Only for Reactive Processes

Because security orchestration is usually touted as a solution to deal with rising alert volumes, it's easy to perceive orchestration's value being limited to reactive processes. But some benefits of security orchestration also transfer over to proactive and scheduled processes that security teams otherwise don't have the time to perform.

Security orchestration playbooks can usually be scheduled to run at pre-determined time intervals. For example, playbooks can conduct health checks on organizational endpoints or verify the presence of systemic vulnerabilities. Playbooks can also run in real-time to execute threat hunting operations across user environments after some malicious indicators were detected in a separate alert.

Security orchestration's value is contingent on organizational need and the process itself more than the method of deployment (reactive or proactive).

Cloud Security

Vulnerability Management

Email

UEBA

Malware Analysis

SIEM

Endpoint Security

Threat Intelligence

DEMISTO

For Security to Bear Fruits, Strengthen Your Roots

Respond to incidents with speed and scale. Standardize processes across products, teams, and use cases. Improve investigation quality by working together.

Download Free Community Edition at http://demis.to/free-edition

Coordinate actions across products at scale

Understaffed security teams struggle to execute standard processes across products in the face of rising alert volumes. Security orchestration has rapidly emerged to fill in these industry gaps by providing general-purpose workflow automation and oversight across security products. In this book, you discover the basics of security orchestration, its underlying need, implementation best practices, popular use cases, and major trends that are driving future growth.

Inside…

- Study enterprise security challenges
- Define security orchestration
- Understand its working components
- Get implementation guidelines
- Review popular and specific use cases
- Examine trends driving future growth
- Clarify security orchestration myths

DEMISTO

Abhishek Iyer is Technical Marketing Manager at Demisto and is catching his breath chasing after the fast-moving world of security. Abhishek has been a writer forever and has a water-resistant typewriter in his shower. Seriously, he enjoys writing so much that he'll probably overshoot this word lim-

Go to Dummies.com®
for videos, step-by-step photos, how-to articles, or to shop!

for dummies
A Wiley Brand

Also available
as an e-book

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley's ebook EULA.