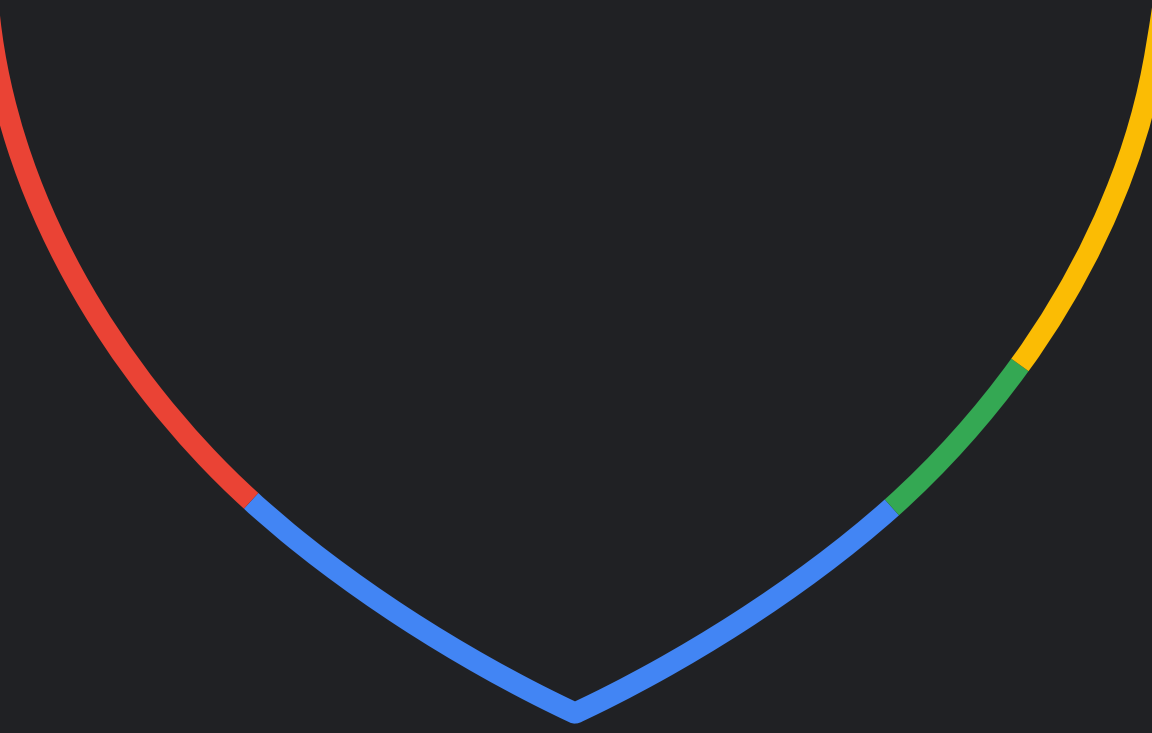
The Defender's Advantage

A guide to activating cyber defense



Mandiant

Google Cloud Security

The Defender's Advantage

A guide to activating cyber defense

Mandiant

Google Cloud Security

Table of Contents

Foreword

The importance of cybersecurity cannot be overstated

No organization today is immune to cyber threats. Attackers target large and small organizations across all industry verticals for any number of reasons—most notably espionage and cybercrime. Even the most security mature organizations are at risk. Attackers are increasingly leveraging zero-day vulnerabilities and other tactics to evade even the best detections, and traditional threats such as phishing continue to evolve and adapt in order to remain effective.

For organizations, a security breach can be devastating and costly. The impact can be everything from data and intellectual property theft to financial losses to reputational harm—and often a mix of several. Further, attacks on critical infrastructure, financial institutions, and government organizations, as well as cyber-physical warfare seen in global conflicts, can threaten our way of life.

Defenders equipped with cybersecurity tools and technologies, threat intelligence, and robust processes serve as guardians, protecting the confidentiality, integrity, and availability of information and systems. Throughout my career with Mandiant and now Google Cloud, I have observed that organizations that are well prepared with robust cyber defenses are significantly more effective at reducing the impact of security breaches and may even be able prevent some attacks from being successful.

In my view, the best way to defend against adversaries is to leverage intelligence to better understand their tradecraft, and infuse it into all aspects of a cyber defense program, including hunting, detection, response, remediation, and validation. When aligned to the organization's overall security mission, these functions create a framework—a well-organized set of core capabilities—required to be ready for modern threats.

On top of all this, organizations must feel confident in their cyber defenses and readiness if they want to effectively protect data, employees, and even our way of life. Part of this confidence comes when organizations fully understand their own environments, where they will be meeting adversaries. We have control over these environments, and this is what gives us the Defender's Advantage. Organizations have it, and now is the time to capitalize on it.

Jurgen Kutscher
VP, Mandiant Consulting at Google Cloud

Introduction

Cyber adversaries continue to relentlessly target organizations with increasingly sophisticated and impactful attacks. These highly motivated, well financed, and coordinated attackers have a single focus: exploiting insecurities in digital systems for their own gains. Cyber attackers are often larger in numbers and have greater access to resources than many of the individual organizations they target. Ransomware attacks continue to be on the rise, exploiting organizations for their sensitive information resulting in significant operational, financial, and reputational damage. Newly discovered, unreported vulnerabilities (zero-days), continue to be a valuable method for cyber attackers to leverage, as these allow compromise of organizations with no advanced notice. Cyber attacks are often conducted by multiple adversary groups with different specialties working together to execute attacks. In many cases, defending enterprise systems can feel like an insurmountable task.

The Defender's Advantage is the concept that organizations are defending attacks against their own environment. This provides a fundamental advantage arising from the fact that they have control over the landscape where they will meet their adversaries. **Organizations often struggle to capitalize on this advantage.**

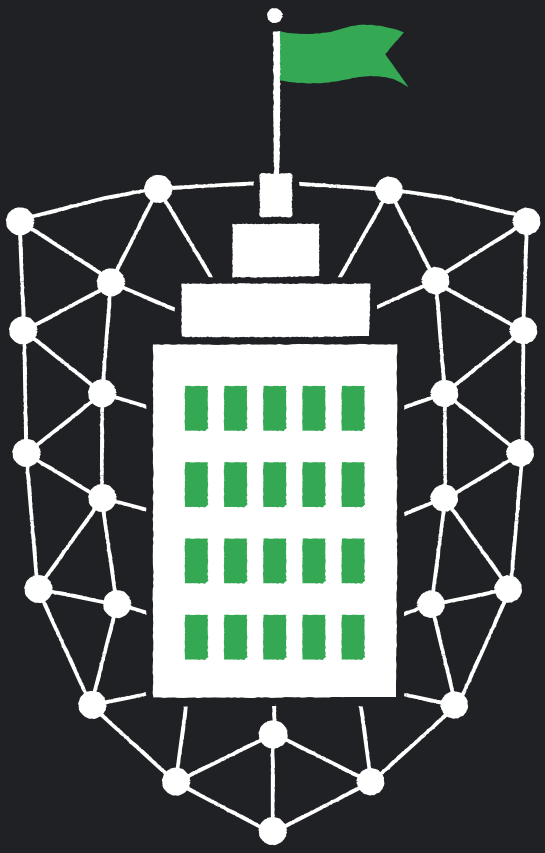
Properly coordinated cyber defense programs can deter the most advanced cyber attackers and the principles of The Defender's Advantage will explain how.

The threats will change all the time. Don't ever forget the advantage that you do have. You should know more about your business, your systems, your topology, your infrastructure than any attacker does. This is an incredible advantage.

Kevin Mandia
Founder, Mandiant

Advanced cyber defense programs leverage strengths developed within and across different teams in an organization's cybersecurity and operations units, establishing a fortified position for an organization. Through the application of cyber intelligence, they prioritize their efforts on the highest value and most likely targets, working to anticipate adversaries actions. Proactive application of intelligence allows organizations to focus their cyber defense programs to detect malicious activity, respond to compromise, and validate the effectiveness of controls and operations against active threats. Once established, security organizations must activate their cyber defenses, advancing capabilities from a prepared state to active duty.

Organizations can utilize expert in-house and outside resources to design and operate a robust cyber defense program. They can work to operationalize intelligence, develop, deploy, and maintain detection capabilities while working to apply proper automation, and establish mature response procedures. To maximize and maintain their upper hand, organizations can also leverage managed services to provide cyber defense coverage specific to their needs. These capabilities maximize the Defender's Advantage.



What is Cyber Defense?

Cyber Defense is the act of actively resisting attacks and minimizing the impact of a compromise. It is one of the four domains of Information Security with the other domains being Security Governance, Security Architecture, and Security Risk Management. A robust Cyber Defense program integrates with the other information security domains to create a hardened and resilient security posture for an organization.

Figure 1. Four domains of Information Security

The Cyber Defense domain is made up of six critical functions to achieve the mission of identifying and responding to threats to an organization. **The mission of a Cyber Defense organization is to allow an organization to continue to operate in the face of threats.** The functions of the Cyber Defense domain are Intelligence, Detect, Respond, Validate, Hunt, and Mission Control. These functions work together to provide a common front against attackers.

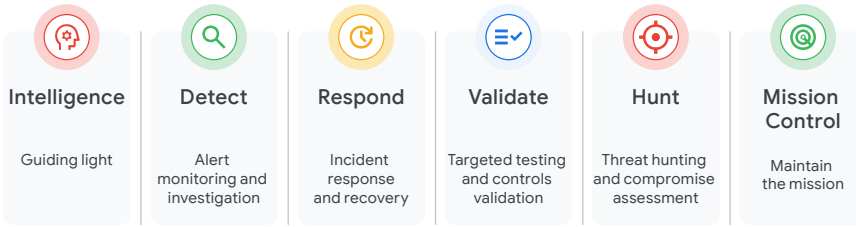


Figure 2. Six critical functions of Cyber Defense

> *Resources (time, people, and money) are always constrained. Using intel to focus your efforts to the most critical areas helps make the best of those precious resources.*
>
> **Alex Wood**
> CISO, Uplight

Each of these functions focuses on a unique piece of the Cyber Defense mission, and feeds into each other, allowing each function to benefit from the capabilities of the other functions. Each of the functions are associated with different activities, actions, or responsibilities, but they all represent core strengths used collectively to improve cyber defenses.

Figure 3. Functions of Cyber Defense in action

Intelligence is a cornerstone of a strong Cyber Defense program. It provides the forward knowledge of threat actors, their tactics, techniques, and procedures (TTPs). Through collecting, analyzing and disseminating threat actors' indicators of compromise (IOCs), the other Cyber Defense functions operate from a position of knowledge. This allows prioritization of actions across the entire Cyber Defense program.

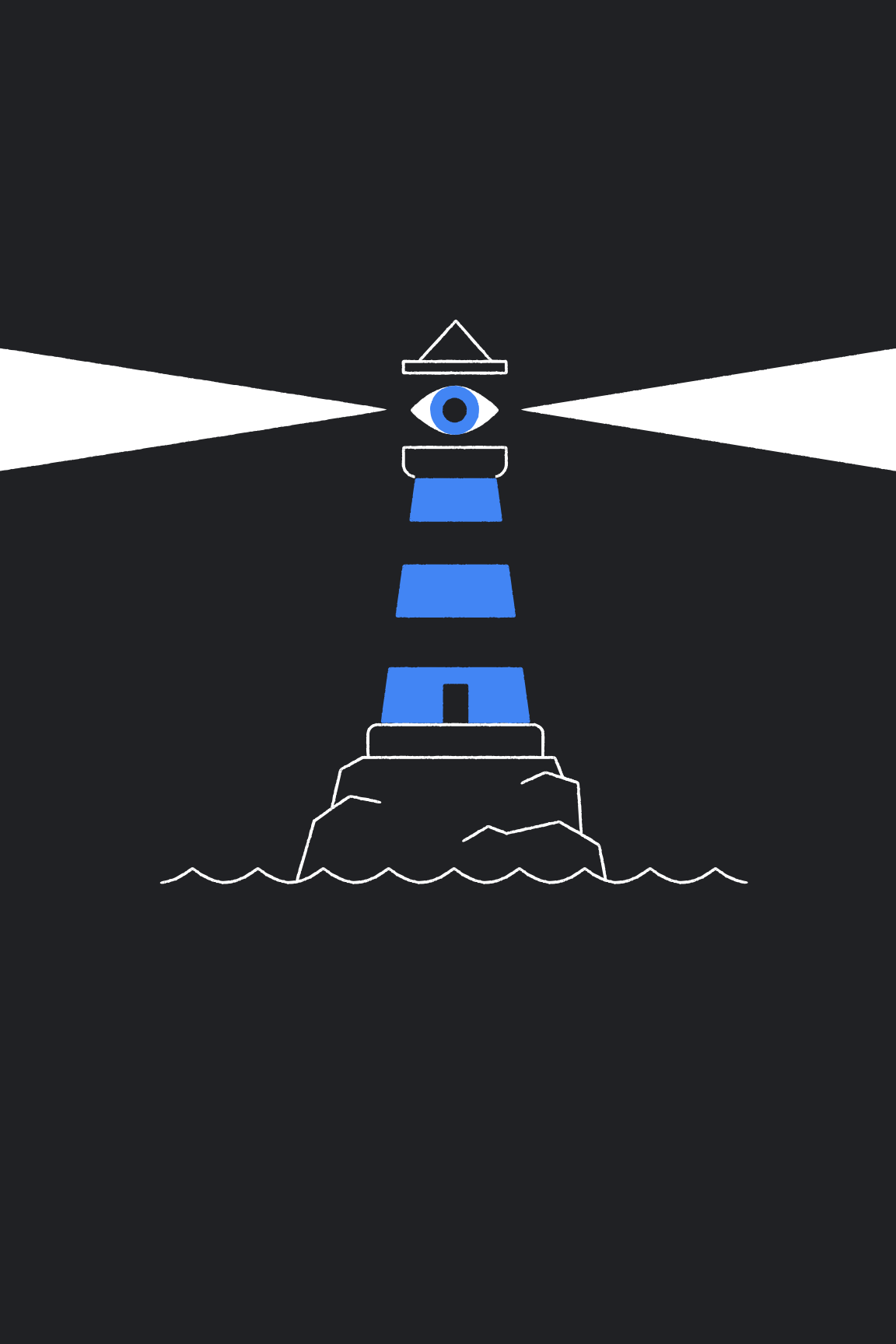
Many of the traditional elements seen in security operations, or security operations centers (SOCs), are performed in the **Detect** function. This function also includes enhancing contextualization, providing detection analytics, increasing visibility to give an organization a clearer picture of threats to the environment, and providing a more comprehensive view of the environment itself.

The **Respond** function focuses on capabilities such as investigation and containment, and includes automation and orchestration, which drive faster remediation of incidents to minimize impact. This function is dedicated to minimizing the impact of any compromise, ensuring rapid recovery to normal operations, and relaying information to the other functions to increase resiliency across the program.

The continuous management of threat exposures within an organization is the purpose of the **Validate** function. In addition to providing assurance that the security control ecosystem is operating as designed throughout changes to the environment, the Validate function also manages the program's readiness to respond, vulnerabilities in the environment, and the capabilities of its resources.

The **Hunt** function expands the detection capabilities of the Cyber Defense program by becoming proactive as it examines the environment for active compromises. It helps to ensure defense controls are operating as designed and provides defenders with the opportunity to identify weaknesses in their controls or undesired activity. Hunt activities provide a very practical complement to the Validate function.

The **Mission Control** function provides the connective tissue that holds the other Cyber Defense functions together and drives coordination and unified management across the program. It also ensures that the functions are connected to the organization's business goals and values. This function is focused on Cyber Defense program management and establishes formal processes for resources management, communications, metrics, and crisis management. Additionally, Mission Control ensures coordination with non-cybersecurity teams across an organization. This program management ensures that the Cyber Defense capabilities remain resilient and aligned to changes within an organization and threat landscape.



Intelligence provides a guiding light

The Intelligence function is designed to help cyber defense organizations understand the threats they face, proactively implement detection strategies and processes, prioritize response actions and resources, and support strategic risk-management decisions. Mandiant advocates for an intelligence-led approach to cyber defense, where intelligence is the differentiator that guides actions and decisions across the entire cyber defense organization.

Threat Intelligence is evaluated information that is relevant, timely, and actionable for a decision-maker.

Intelligence is the lifeblood of cyber defense, as it directly feeds into every other function. From providing IOCs that can be used to develop use cases within the Detect function, providing guidance to build Hunt activities, or developing adversary emulation to test security controls within the Validation function, intelligence is critical to every element of the cyber defense eco-system. Being intelligence-led means aligning organizational defenses to meet the threats that are most likely to impact an organization. It assists with resource allocation and prioritization for the cyber defense organization aligned to the most likely avenues of compromise.

Activating the Threat Intelligence Lifecycle

An impactful Intelligence function produces and disseminates actionable intelligence into the hands of the appropriate audience, in a format and language they can understand and use to make decisions. A best practice within the intelligence community is to use an intelligence lifecycle to guide development, production, and consumption of intelligence throughout an organization. The intelligence lifecycle standardizes operating practices to encourage consistent, measurable responses aligned to the threats an organization faces. This allows resources to prioritize actions to identify and handle the most impactful threats to an organization.

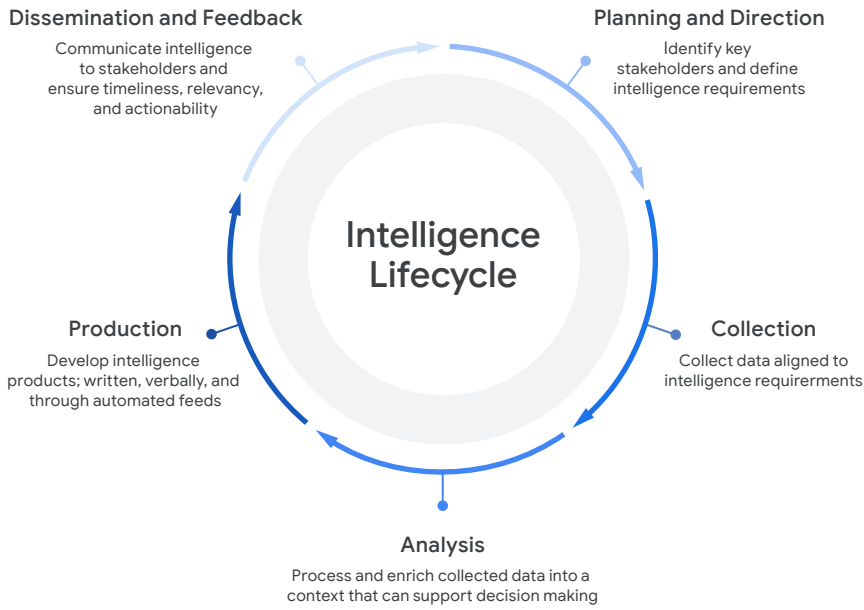


Figure 4: Intelligence Lifecycle

Planning and direction

The Intelligence function must consider who their audience is, as each end user of intelligence has different needs. Conducting stakeholder identification and defining intelligence requirements is a foundational component of a strong Intelligence function.

This is critical for impactful Intelligence, as it will guide the remaining steps of the intelligence lifecycle, determining what intelligence matters to an organization, how it's collected, produced, and disseminated. The Intelligence function should build relationships with key individuals in each cyber defense function to ensure consistent, effective, and efficient communication. Example stakeholders include: SOC analysts, red teams, incident response teams, forensic investigators, hunt teams, senior decision makers, upper management, and executives.

Once the Intelligence function identifies the stakeholders, it needs to understand, define, and document the intelligence requirements (i.e. what each stakeholder cares about.) A list of intelligence requirements should clearly define what each stakeholder needs from the Intelligence function to optimize operations and defend an organization. Each intelligence requirement should be aligned to the appropriate stakeholder(s) and prioritized. Intelligence requirements can also be tied to specific actions and outcomes across the cyber defense organization.

For example, the Detect and Validate functions require information on new and emerging IOCs and TTPs aligned to key threats to an organization. To fulfill this need, the Intelligence function may document intelligence requirements that include identifying and maintaining a list of threats to an organization aligned to threat actors, malware families, campaigns, vulnerabilities, etc., and a requirement to collect both tactical and operational intelligence aligned to those threats.

In addition to maintaining a list of standing and prioritized intelligence requirements that would proactively drive the Intelligence function, there should also be a formalized process for stakeholders to submit ad hoc requests for information (RFIs) to the Intelligence function as questions arise. This may include sending an email, a formalized intake form, or directing questions to a function point of contact. This process must be clearly documented and communicated to each stakeholder.

Collection

Intelligence requires data collection and information gathering for analysis to be conducted. The collection of key data sources needs to be documented and aligned to established intelligence requirements. Aligning collection with intelligence requirements allows organizations to ensure they have the data and information available to fulfill intelligence requirements and to document and potentially fill any gaps in data sources. Organizations should also make a determination on the reliability and credibility of each collection source, which includes visibility, fidelity, relevance, and timeliness. It is critical for organizations to focus on the quality of data versus the quantity. Many security organizations subscribe to multiple intelligence feeds, but struggle to operationalize the intelligence in a way that protects an organization.

For example, the Validate function may define an intelligence requirement around vulnerabilities and exploitation status aligned to stakeholders supporting threat and vulnerability management. The Intelligence function should identify collection sources that include information not only on the vulnerability itself, but if the vulnerability is actively being exploited in the wild, and if so, the TTPs leveraged by the threat actor and/or malware family exploiting that vulnerability.

Analysis

Data that has been collected does not become intelligence until it has been analyzed, distilled, and made relevant to an organization. Analysis involves enriching and combining collected data points into a context that can support tactical, operational, and strategic decisions. For example, an IP address is a data point that will not provide any actionable value when presented on its own. It is not until an analyst has enriched and contextualized an IP address with relevant data that threat intel begins to form. Contextualizing and analyzing data around an IP may include identifying that a threat actor leveraged the IP address in a credential harvesting campaign, at a certain time period, and leveraged specific tools. This analysis provides actionability for the Detect

function to operationalize the intelligence by leveraging it as an IOC, within a specific time frame, and associated with credential harvesting activity. The concept of contextualization, or adding analysis and enrichment to data, is the root of all intelligence analysis, and is pivotal in an organization's ability to operationalize intelligence and become intelligence-led.

> *Just remember that research isn't a straight line. It's a series of rabbit holes. Some of them will take you in the right direction and some of them won't. Be flexible enough to accommodate new and important information so you don't end up missing out on what matters.*
>
> **Shanyn Ronis**
> Head of Cyber Threat Coordination Center, Google Cloud

Methods of analysis can vary from analyst to analyst, team to team, and organization to organization depending on the tools and expertise available. Intelligence functions should seek to incorporate best practices and structured analytic techniques as much as possible to ensure the highest fidelity and reliability of assessments. Popular frameworks, such as MITRE ATT&CK®, can streamline analysis processes and provide common terms for communicating intelligence across an organization.

MITRE ATT&CK is a framework and standardized knowledge base of threat actor TTPs that provide a shared lexicon for cyber defense organizations to categorize cyber threat activity.

While Intelligence analysis can be done manually, ideally analysis incorporates some degree of automation. This is dependent on the Intelligence function first establishing structured, repeatable, and standardized analytic methodologies that are documented, stored, and shared across the function. Automation allows for a more consistent, repeatable, and efficient cadence for the Intelligence function to review data and make key assessments. Automation should also power the operationalization of intelligence by helping to automatically create rules and alerts for new threats. This can reduce manual intervention and allow analysts to respond quicker to threats in their quest to stay ahead of the attack.

Production

Communication plays a big role in the Intelligence function. It is important for threat intelligence teams to meet stakeholders where they are in their intelligence journey, while making efforts to uplift an organization's overall understanding of how to use cyber threat intelligence to enable business decisions. To accomplish this, Intelligence functions should establish a service catalog, which defines, correlates, and documents stakeholders, intelligence requirements, and production needs to analytic methodologies. The function should also develop intelligence report templates and outputs aligned to the service catalog.

By establishing a service catalog, the Intelligence function effectively aligns different types of intelligence to the various users and uses. Understanding which audience needs which type of intelligence and delivering it in a timely and digestible manner can make the difference between simply having an Intelligence function and being an intelligence-led security organization.

There are three types of intelligence that define production and are determined by audience:

1. **Strategic intelligence** provides a high-level look at what is happening in the cyber threat landscape and is intended to inform senior decision makers of potential threats to an organization in order to make decisions that will protect and/or enable the business. This type of intelligence focuses on trends observed over time, emerging threats, and predictive analysis to help answer the questions of "who" and "why".

2. **Operational intelligence** provides an understanding of how a threat operates to assist incident responders, forensic investigators, and threat hunters to identify, contain, and remediate intrusions. This type of intelligence focuses on identifying threat actors' motivations, associated TTPs, and changes to infrastructure to help answer the questions of "how" and "where".

3. **Tactical intelligence** provides atomic and contextualized indicators associated with known malicious or suspicious activity along with associated threat context to help organizations develop detections, assist SOC analysts with alert triage, and identify threats within an environment. This type of intelligence focuses IOC management associated with threats and helps to answer the questions of "what".

It is important to also understand how these types of intelligence build on each other. Tactical intelligence is considered the foundation of cyber threat intelligence. This level of intelligence is where malware analysis, attack telemetry, network analysis, pivoting, and identification of attacker infrastructure is conducted. As an intelligence function matures, it builds on the tactical level to identify campaigns, TTPs, and motivations. Strategic intelligence is layered on top of this looking at industry threats, regional trends, threat sponsors, and changes over time. Both operational and strategic intelligence are based on tactical intelligence so producing reliable and credible tactical and technical analysis is critical for the Intelligence function.

A key piece of intelligence production is asking: "So what?" The "So what?" should address why the report is relevant to the audience, and why the reader should care. It should be the key takeaway for the reader, clearly communicating how the identified activity can or does affect an organization, and what is likely to happen next. It should also make follow-on actions apparent for the target audience and clearly outline the implications of the activity. The "So what?" does not, however, identify actions taken or to be taken by the target audience. An intelligence report may provide recommendations to help improve an organization's cyber defenses against a specific threat, but it is up to the stakeholder(s) to determine if, how, and when the actions should be taken and execute those actions—also known as operationalizing intelligence.

Dissemination

Due to the different needs of various stakeholders, the Intelligence function must tailor dissemination to each audience and stakeholder. Language, format, and delivery methods, such as frequency, intent, and expected actions, may vary between the different audiences and stakeholders. For example, if the Intelligence function is asked to provide a briefing to an executive team on potential cyber threats to an organization, this would typically not include IOCs, malware analysis, or other technical information. The briefing would include narratives that indicate trends, key activity of interest, and how that activity could adversely impact an organization, as well as controls and mitigations

that could be put in place to defend against this type of activity. Conversely, if the Intelligence function were asked to provide a briefing to an organization's incident response team on a new method leveraged by a threat actor, the briefing would focus more on the technical aspects, initial infection vectors, attack lifecycle, and persistence mechanisms to assist in investigations.

Feedback

Feedback is a critical phase of the intelligence lifecycle and often overlooked. In worst case scenarios, a lack of feedback results in an Intelligence function operating in a silo and not communicating effectively with stakeholders. Without clear, regular, and effective feedback that is actioned by the Intelligence function, intelligence products can miss the mark and their intended consumers "tune out" the intelligence. The delicate trust relationship between the Intelligence function and its stakeholders would be lost, resulting in minimally effective intelligence, limiting the overall effectiveness of the cyber defense organization.

A mature Intelligence function consistently seeks feedback from their stakeholders to ensure the maximum value of intelligence production. A formalized Intelligence function will have established feedback loops between intelligence producers and consumers through multiple modalities. At minimum this will take the form of regularly scheduled intelligence requirements reviews between the Intelligence function and its stakeholders, as well as one-on-one meetings with stakeholders or management, cross-team project work, at all-hands and off-site meetings, and via periodic surveys.

The Intelligence function should consistently seek to understand the intended use of their services to ensure production is meeting the needs of the consumers.

Key intelligence services

Table A: Value of Intelligence in Cyber Defense

	Tactical Level	Operational Level	Strategic Level
Security Roles	Security Operations Center Network Operations Center Vulnerability and Patch Management Team	Incident Response Team Forensics Team Red Team/Pen Testing	Chief Information Security Officer Risk Management Security Management
Tasks	Indicators to security tools Patch systems Monitor, triage, and escalate alerts	Determine attack vectors Remediate Hunt for breaches Emulate adversaries	Allocate resources Communicate with executives
Problems	False positives Difficult to prioritize patches Alert overload	Event reconstruction is tedious Difficult to identify damage	No clear investment priorities Executives are not technical
Value of CTI	Validate and prioritize indicators Prioritize patches Prioritize alerts	Add context to reconstruction Focus in on potential targets	Demystify threats Prioritize based on business risk

While the Intelligence Lifecycle guides development, production, and consumption of intelligence throughout an organization, an Intelligence function should also identify the key services it provides. Defining and scoping services, based on available resourcing and business needs identified in the planning and direction phase of the Intelligence Lifecycle, is the key to success for the Intelligence function. Each intelligence service is an output of the Intelligence Lifecycle, as the service is defined by the requirements set by stakeholders, data collected with an established plan, analysis conducted with standardized methodologies, production occurring in a repeatable fashion, dissemination aligned to stakeholders, and the feedback loop established to ensure operationalization.

Understanding the threat landscape

Intelligence functions have a responsibility to constantly maintain an active understanding of the ever-evolving threat landscape. This mandate extends beyond simply reading the latest cybersecurity-related news headlines. Successful Intelligence functions leverage internal data sources like incident response reports, threat hunt reports, and crown jewel lists compared against external data sources such as threat feeds and other intelligence to constantly assess the risk that new and existing threats pose to an organization. Intelligence functions also typically answer RFIs from the other cyber defense functions on pertinent or emerging threats.

Vulnerability prioritization

The Intelligence function provides valuable context around vulnerabilities relevant to an organization. Intelligence on existing proof of concepts or successful exploitation of a vulnerability can enhance risk assessments for vulnerability management teams, allowing teams to better prioritize vulnerabilities for mitigation and patching. Additionally, intelligence can strengthen business justifications for mitigation and patching by incorporating threat intelligence into risk assessments.

I use CTI risk ratings to create vulnerability situation reports. The report provides CISOs information about critical vulnerabilities, so they have immediate and actionable intelligence, often before I am asked for it. The automated report correlates data between our vulnerability vendor and our CTI vendor to show overall company exposure, the vulnerability severity rating, the CTI risk rating, the exposure broken out for each line of business or subsidiary and a write up on how the vulnerability works and key links for more information.

Gibby McCaleb,
Director of Security Operations

Security operations integration

Intelligence functions should strive to integrate threat intelligence into existing security operations workflows, particularly through automation. While intelligence analysis can never be fully automated, some stakeholders may not need finished intelligence products, such as formal reports, to enhance existing detection and response workflows. Providing reliable, relevant, and timely threat intelligence from vendor-maintained threat feeds, APIs, and third-party information sharing groups directly into existing stakeholder workflows can improve a team's ability to assess risks. For example, vetted and reviewed indicator feeds from trusted intelligence sources can be engineered to automatically detect and block high-confidence IOCs within an organization's environment.

Brand Intelligence

Social media and dark web monitoring falls under the purview of the Intelligence function. Intelligence functions monitor these sources for information on the latest cyber threats and any mention of an organization or its vendors. This can aid in threat mitigation efforts along with assessing possible physical threats to an organization. While social media and dark web chatter is not always the most reliable source of information, this service can help organizations unlock new brand intelligence data sources.

The Cyber Threat Profile

Cyber defense organizations must understand how the cyber threat landscape applies to their organization. The cyber threat profile is intended to identify the cyber threats that are most likely to impact an organization based on industry, geography, high-value assets, and partnerships. It must also take into consideration an organization's attack surface, vulnerabilities, critical technologies, crown jewels, and the potential risk and impact to business operations. When communicated in a timely manner, the cyber threat profile provides decision makers comprehensive situational awareness, and aids the overall cyber defense organization in prioritizing, coordinating, and taking appropriate actions based on the same threat picture.

An actionable and impactful cyber threat profile is a key element of a cyber defense program. It is a blend of strategic, operational, and tactical cyber threat intelligence. It leverages insights from past incident data, intelligence information, and observations in peer organizations or regionally focused activity. The cyber threat profile helps an organization not only understand the threats that matter, but informs security detection content, highlights gaps, trends and patterns, and guides security policy. Mapping threat activity and vulnerabilities across common frameworks offers a powerful depiction of an organization's security stack, where threat activity is detected, and measures the effectiveness of security controls. Additionally, understanding the vulnerability landscape and mapping to threat actor capabilities will illuminate potentially exposed assets and help with cyber defense prioritization efforts.

The cyber threat profile serves as a crucial tool to drive risk-based decisions and protect business priorities from malicious actors.

The Cyber Threat Profile is arguably the most important document for a cyber intelligence program. And most organizations either don't have one or aren't using it to drive their operations.

Andrew Close
Manager Intelligence Consulting and Training Solutions,
Google Threat Intelligence

Developing a cyber threat profile

A cyber threat profile should be composed of essentially two pieces from the Intel function, a cyber threat landscape and an operational threat picture, combined with a third piece from a risk perspective on the potential impact of a breach. The cyber threat landscape is an outward look of the threat environment designed to provide a proactive view of cyber threats to help develop detections and capabilities, allocate resources, and build and implement risk-management strategies. The operational threat picture is intended to identify the cyber threats that are currently impacting an organization. This is an inward look at the threats both currently and historically identified within an environment to help an organization review its current cyber defense posture and make improvements where necessary.

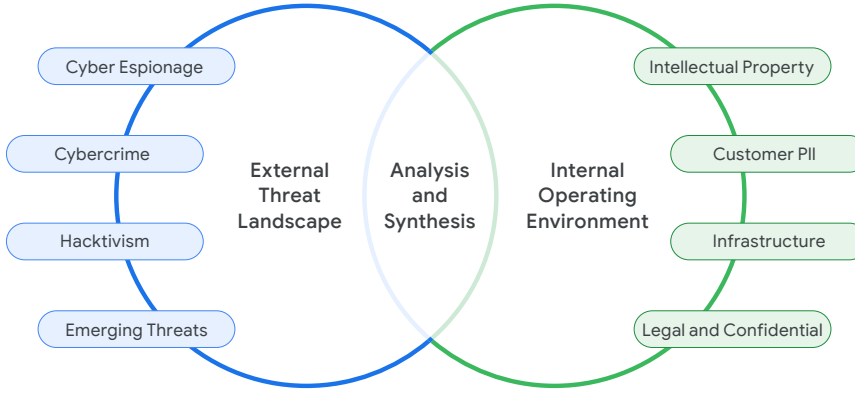


Figure 5: Intelligence inputs for an effective cyber threat profile

The cyber threat landscape should be based on an organization's industry, geographies, high-value assets, and partnerships. It should include at a minimum:

- Identified and potential emerging threats to an organization that could impact business operations such as supply chain compromises, ransomware, third party compromises, or potential geopolitical activity or conflict
- Known threat actors that could impact similar organizations
- Associated TTPs aligned to the threat actors, mapped to the MITRE ATT&CK Framework where possible
- Threats correlated to an organization's high-value assets, crown jewels, and business operations
- Potential vulnerabilities within an organization that could be exploited
- IOCs connected to the assessed threats

In general, the following information should be included in an operational threat picture:

- Identified phishing campaigns, malware families, TTPs, exploited vulnerabilities, and known threat actors within existing log data
- Alignment of the threats to an organization's high-value assets, crown jewels, and business operations
- Associated IOCs and forensic artifacts related to the identified threats
- Event volume, patterns, and trends information useful for establishing baseline levels of activity

> *Humans aren't great at evaluating risk. We tend to catastrophize, focusing on the worst-case scenario, and then start to view this worst case as the most likely case—even if there is no evidence or reason for us to do so. Once we're aware of threats, we come to see them as more likely to happen. And this is where cyber threat intelligence can play a big role in keeping our evaluations of cyber risk honest.*
>
> **Mark Owens**
> Head of Intelligence Training, Google Threat Intelligence

The third portion of a cyber threat profile should be developed in partnership between the Intelligence function, Mission Control function, and the Security Risk Management domain to determine the potential risks and impacts the identified threats pose to the organization. This includes conducting a risk assessment and impact analysis around potential business outages, disruptions to operations, reputational damage, data theft, or a financial loss. Leveraging

the intelligence identified in the first two sections of the threat profile and connecting it to the organization's specific risk and impact analysis will allow organizations to also identify proactive mitigation strategies to better defend themselves against cyber threats.

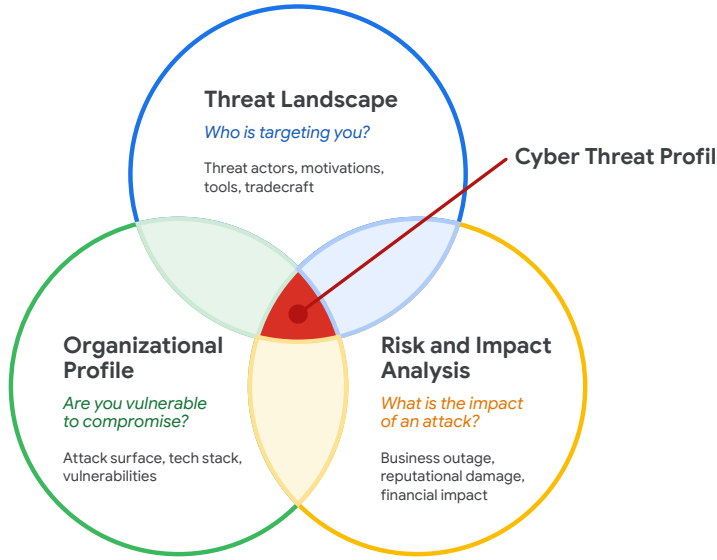


Figure 6: Components of a cyber threat profile

Organizations should maintain an understanding of their cyber threat profile, and update it on a bi-annual or annual basis. The operational threat picture should be updated on a monthly basis and data should be trended over time to identify changes based on newly implemented defense capabilities and shifts in the cyber threat landscape.

Operationalizing intelligence across the Cyber Defense functions

Intelligence is a key differentiator for each cyber defense function as it helps guide and prioritize actions across an organization. In a world where cyber threats, large scale data breaches, corporate compromises, and evolving technology are a daily occurrence, organizations need to be agile, proactive, and responsive to the constantly changing threat landscape. By implementing an intelligence-led cyber defense approach, organizations will be prepared to identify malicious activity in their environment, detect and respond to compromises and changes in the overall threat landscape, and validate the effectiveness of their controls and operations against active threats. By understanding the threats that matter, organizations can proactively implement decision strategies and processes, prioritize response actions and resources, and support strategic risk-management decisions. In order to accomplish this, organizations need to effectively operationalize intelligence across the other cyber defense functions.

In my experience, most organizations fall short in operationalizing intelligence across the different functions within a cyber defense organization. This often materializes in two key areas: First, communication breakdowns and silos existing across teams and functions. Second, a lack of understanding in leveraging intelligence to guide operations within those functions. For example, many organizations are focused on collecting IOCs, which are static, as opposed to also focusing on a more behavioral approach and leveraging identified threat actors' TTPs to build detections.

Emily Cranston
Manager of Global Cyber Defense, Mandiant Consulting at Google Cloud

Detect: Operationalize intelligence to drive the development of both detection use cases and rules aligned to the identified threats, to ensure appropriate defenses are in place based on known threats.

Respond: Operationalize intelligence to aid in locating, isolating, and remediating intrusions. Intelligence should enable the Respond function to more quickly and effectively detect, respond to, and remediate incidents by providing insight in threat actor operations.

Validate: Operationalize intelligence to evaluate the effectiveness of security controls against the threat actors that are most likely to impact an organization. Using threat actors and their respective TTPs as input, security validation should seek to methodically evaluate the ability of the existing security controls to detect, alert on, or prevent adversarial actions in the environment. This intelligence should also serve as input for attack surface management and vulnerability prioritization. The results of this testing will be critical to informing security policy changes, developing detection rules, informing potential hunt missions, and closing critical security gaps.

Hunt: Operationalize intelligence to guide hunt missions within an environment to identify malicious activity. By leveraging intelligence, the Hunt function will be able to search for malicious activity within an environment that is the most relevant and highest risk to an organization.

Mission Control: Operationalize intelligence to ensure that relevant risks, impacts, and action items are identified, assigned to resources, executed on, and closed out in a timely manner to align an organization's cyber defenses to the threats facing an organization. It should also be leveraged to communicate priority threats and risks to business leaders.

Detecting and investigating malicious activity

The Detect function identifies malicious behavior based on activity seen in an environment. This function coordinates and supports the other functions by operationalizing intelligence, observations, and other requirements into actionable triggers that activate a coordinated defense. It also is responsible for producing proactive deliverables that enable long-term defense.

Successful detection requires research, testing, and coordination to identify the most relevant threat techniques, alert the security operators, and initiate response actions. It relies heavily on contextualized intelligence that describes adversary capabilities and objectives. A great detection not only indicates the presence of an adversary, but also conveys what stages of the attack the adversary has completed. The detect function relies on a methodical approach to digest intelligence and produce reliable alerts, dashboards, reports, and automation triggers.

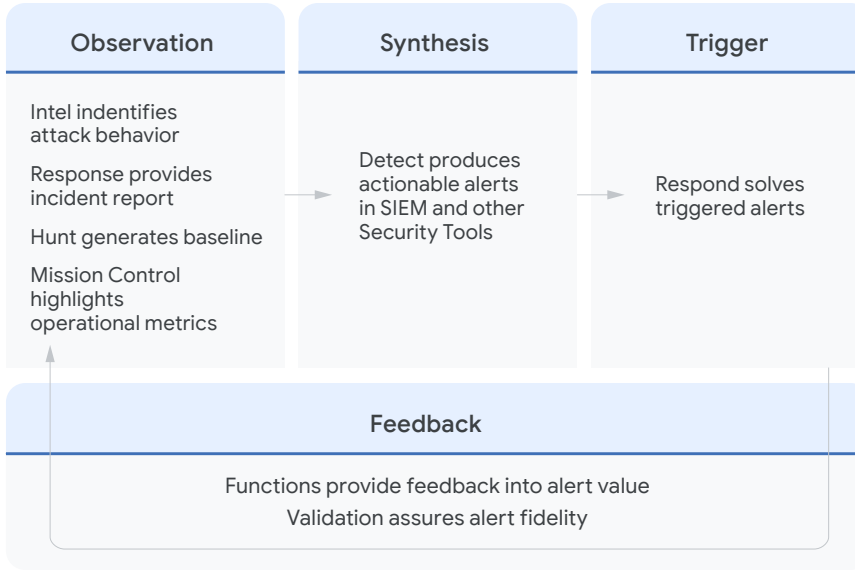


Figure 7: Methodical approach to the Detect function

This methodical approach includes intelligence and observation inputs from other functions, which enable effective security monitoring in the Detect function. The monitoring can then trigger response activities and provide feedback to bolster the other functions. Monitoring is more than just logging sent to a security information and event management (SIEM), it requires awareness as to what threat behaviors are likely to affect the environment, what visibility is required to identify them, and what is needed to affirm malicious intent. The Detect function collects inputs from the various teams, including intelligence, compliance, response, and risk management to identify alert requirements. The function works with technology engineering teams to secure the appropriate visibility and logging. Then, the function produces content that processes the visibility, threat lists, inventories, and other elements into tooling that triggers a security response.

> *Like it or not, it's the threat actors that decide which techniques are the highest priority. Without threat intelligence, you have no idea if your detections are relevant.*
>
> **Daniel Nutting**
> Manager for Cyber Defense Operations Consulting,
> Mandiant at Google Cloud

Detection engineering

Detection engineering is a systematic discipline built upon analysis and adaptation. At its core lies a continuous loop: understanding threats, generating detections, tuning responses, and refining the cycle. Intelligence on adversary behaviors inform and shape detections that keep organizations secure. This iterative process mirrors the way adversaries constantly evolve, ensuring defenders are always adapting and never caught off guard.

Adversaries aren't bound by rigid rules. They study their targets, identifying weaknesses within an organization's environment, people, and processes. From this reconnaissance, they strategically choose TTPs to best exploit those vulnerabilities and achieve their objectives. Each step an attacker takes where they leave a trace, subtle or overt, is an opportunity for detection engineers to uncover and create detections to alert on. No matter how novel, impressive, or complex a detection is written, if it does not address the relevant TTPs, it is useless.

Having an in-depth understanding of TTPs based on reliable threat intelligence is critical for SOC analysts. Understanding past breaches aids analysts in predicting future attacker activity to a single system and an enterprise-wide incident.

David Lindquist
Senior Manager, Managed Defense Security Operations Center, Mandiant at Google Cloud

Aligning detections to attacker tactics, techniques, and procedures

While defenders certainly have a role in shaping the threat landscape, it is ultimately the attackers who dictate the specific TTPs. Attackers are driven by their objectives, which could range from financial gain to espionage or simply causing disruption. These objectives, combined with their technical capabilities and the resources at their disposal, heavily influence their choice of TTPs. This is why Intel is a critical partner to the detect function. Intel informs Detect which TTPs to prioritize. Detection engineers analyze patterns indicative of malicious activity and translate into detections—rules, queries, and behavioral models—that flag any potential match within an organization's environment.

Attackers carefully assess their targets, identifying vulnerabilities within an organization's network, systems, and even personnel. They leverage this reconnaissance to tailor their TTPs to exploit the weakest points, maximizing their chances of success. For example, an attacker might identify a vulnerability in a specific software application used by an organization and craft a custom exploit to gain access.

Attackers constantly adapt their TTPs to evade detection and overcome new security measures implemented by defenders. They analyze the effectiveness of their past attacks, learning from both their successes and failures. This continuous learning process allows them to refine their TTPs, making them more sophisticated and harder to detect. As a result, defenders are often in a reactive position, playing catch-up with the latest attacker techniques.

Logging driven by TTPs

Robust logging is the bedrock of effective detection. Every system interaction, network flow, and user action must be diligently captured to give detection engineers the data they need. But logging alone is insufficient—intelligence applied to the logs through analytics, detections, reports and dashboards enable the defense center to operate.

The selection of logs forwarded to a SIEM system should be directly informed by the TTPs used by the adversaries identified by the Intel function. Only by understanding the common TTPs utilized by attackers can defenders identify and prioritize the collection of logs that are most likely to contain evidence of malicious activity. This targeted approach ensures that the SIEM is not overwhelmed with irrelevant data and that analysts can focus on the most critical security events.

For instance, if a prevalent TTP involves deploying web shells for persistent access, defenders should prioritize collecting web server logs, including access logs, error logs, and application-specific logs. These logs can reveal suspicious file uploads, unexpected script executions, and abnormal traffic patterns that might indicate the presence of a web shell. Similarly, if a common TTP involves using web shells to execute commands and manipulate files on compromised servers, defenders should concentrate on gathering file integrity monitoring (FIM) logs, process execution logs, and system event logs. These logs can help identify unauthorized file modifications, suspicious processes, and unexpected system events that could point to malicious activity originating from a web shell.

By aligning log collection with the observed TTPs, defenders can create a more effective and efficient security monitoring strategy. This approach allows them to proactively identify and investigate potential threats, reducing the risk of successful attacks and minimizing the impact of any breaches that do occur. It also helps to ensure that the SIEM is a valuable tool for security analysts, providing them with the relevant information they need to detect and respond to threats in a timely manner.

Pursuit of fidelity

The process of detection creation isn't haphazard. A mature methodology follows a defined lifecycle—from initial research and development, to testing and validation, to production deployment and ongoing maintenance. By adhering to this structure, detection engineers ensure that their work is of the highest quality, reducing noise for analysts and offering true defensive value.

A detection is only as good as its validation. Not every alert is a true attack. False positives plague analysts so detection engineers must subject their creations to rigorous testing. This process involves simulating adversary behaviors and verifying that the alert fires as intended. Once in production, alerts undergo thorough triage, separating benign activity from real threats. This stage is often a collaborative effort involving security analysts and incident responders.

Visibility into detection performance is paramount. Metrics like the number of alerts fired, true positives versus false positives, and time-to-detection illuminate the effectiveness of the detection engineering program. These metrics aid in prioritization, highlight areas for improvement, and ultimately demonstrate the value detection engineers bring to an organization's overall security stance.

Detection optimization

Detection engineering rarely occurs in a vacuum. Detections often rely upon dependencies like system configurations, tools, and intelligence feeds. A robust dependency management process becomes non-negotiable. Changes in underlying systems can quietly break detections, and outdated threat data leads to coverage gaps. Engineers must track these dependencies meticulously, ensuring any modifications upstream are reflected in their downstream detection logic.

To maintain the effectiveness of SIEM detections, organizations must adopt a proactive and continuous approach to dependency management. For instance, a common dependency in various SIEMs are lookup lists. These lists are used for things like enrichment, filtering, and data normalization. Often one lookup list supports multiple alerts. Who is keeping that list up to date? Who is tracking which alerts are affected by changes to that list? Ultimately, mature engineering relies on processes and communication to provide assurance that changes, even seemingly small ones, do not create unintended consequences.

Commonly, organizations write alerts for specific, high risk servers or applications, with the asset name explicitly written into the alert logic. Years later, the server owner changes the name of the server, because the OS was upgraded or it was moved to a different datacenter, an innocuous reason. However, they neglect to inform the security team of the change. Since so often no news is good news in security, a lack of alerts may not be obvious. Regular testing is necessary to ensure that the entire log to alert pipeline is still functioning.

Similar issues arise when log formats or schemas change. An alert may be written when a firewall logs a "block" action. If a vendor upgrade shifts the logging schema, and now the firewalls log "drop" actions instead, the alert is now blind. As such, data normalization is a detection engineer's best friend.

Different systems produce logs in vastly different formats, creating confusion when attempting to correlate events. Adopting a common data model ensures that regardless of the source, log events share a uniform structure and semantic meaning. This makes creating cross-system, holistic detections far more efficient while simultaneously increasing their fidelity.

Detection optimization should execute with automation in mind. If Security Orchestration, Automation, and Response (SOAR) platforms are to revolutionize how teams respond to threats, engineers must consider potential downstream actions—what enrichment data is needed for rapid triage, what containment steps could be automated, and how does the detection integrate with the wider incident response playbook. Detections built with these considerations empower SOAR to aggressively contextualize, enable analyst decision making, and expedite containment and eradication, limiting the adversary's ability to maneuver and minimizing potential damage of an attack.

Automation strategy

Automation allows them to scale beyond the constraints of manual processes, reduce alert fatigue, and accelerate response times. It can also mitigate the risk of procedural and human error in the investigation and evidence gathering process.

Automated defense technologies augment the role and responsibilities of security analysts. By providing security analysts with scoped and prioritized investigative cases from which to quickly choose the appropriate incident response path, the security analysts can focus more on identifying adversarial intent versus vetting false positives.

By providing analysts with prioritized and enriched data, automated defense technologies remove many of the initial triage steps when investigating suspicious activity. This allows the analysts to spend their time analyzing and responding to activity rather than validating alerts. Automated defense technologies will never replace a human analyst's ability to understand the context of the data; however, it is a highly useful tool in an analysts' toolkit. It should be the goal of all SOC teams to present analysts with high fidelity alerts that contain actionable data so that skilled analysts can reduce the dwell time of attackers and prevent catastrophic impact of an attack.

Automated defense technologies scope all related systems and activity for the duration of an attack. The incident may span a few seconds or many days; sometimes even years. The technology prioritizes the incident investigation, factoring in the scope, asset criticality, attack stage, and confidence in the escalation. The prioritized incident is then presented to the analyst with supporting evidence including:

- The identified malicious behaviors and signatures
- An event timeline (a series of events from various security tools over time)
- The internal systems and assets impacted
- Attributed threat intelligence data
- Attack stage progression mapped to the MITRE ATT&CK Framework

An effective automation strategy must address several facets:

- **Detection as code:** Embracing this methodology allows detections to be treated as version-controlled, testable artifacts. This empowers collaborative development, continuous improvement cycles, and eases deployment across multiple environments.
- **Enabling SOAR:** Detection is just the first step, followed by the whirlwind of triage, enrichment, and containment action. Integrating detection logic with SOAR platforms unlocks the true potential of automation. Detections that are built alongside SOAR playbooks streamline the analyst workflow and enable decisive, automated responses to emerging threats.
- **Field normalization:** Ensuring normalized data structures, regardless of the source, paves the way for reliable automation. When detection logic and SOAR playbooks expect consistent field names and event structures, the ability to orchestrate responses between systems becomes seamless.

- **Automating context:** Context can turn a simple alert into actionable intelligence. Automated enrichment can pull relevant information from vulnerability databases, asset inventories, or external threat intelligence platforms. This additional context gives analysts more information at their fingertips for rapid decision-making.

Not all automation is created equal. Prioritization is key for maximum impact. Detection engineers must be in constant dialogue with analysts and incident responders—where are the pain points? Where is time wasted on mundane, repetitive tasks? High-fidelity detections that trigger excessive false positives are ripe for automated triage. These insights, coupled with an understanding of the adversary's most likely TTPs and an organization's crown jewels, inform the automation roadmap.

Detection tooling strategy

A well-crafted detection program requires a carefully selected suite of tools and the tooling landscape is full of an array of vendors, overlapping capabilities. Detection engineers must work strategically with security architects, evaluating solutions not just on their standalone merits, but on how they integrate into the larger defensive ecosystem. They must prioritize functionality based on defined requirements, avoid solutions that merely replicate existing capabilities, and champion tools that reduce complexity rather than add to it.

Mergers and acquisitions can add complications to tooling plans. Organizations may inherit disparate systems, security stacks, and logging standards from the acquired company. A swift assessment of the new technology must be made. Can it be integrated and if so, at what cost? Are there redundant capabilities affording potential consolidation? Mergers and acquisitions can be times of upheaval, but they also offer an opportunity to reassess and potentially redefine an organization's tooling strategy.

Managing multiple SIEMs is a reality for many organizations. Legacy systems linger, regional teams may favor different solutions, and niche use-cases arise that the primary SIEM doesn't adequately cover. This situation calls for a centralized strategy. Detection engineers must analyze data sources, critical assets, and core defensive needs to determine where SIEMs can be consolidated. When that's not feasible, robust data normalization and cross-SIEM correlation become essential to avoid security blind spots.

The lure of the latest and greatest security tool is strong, but unmanaged adoption can lead to a sprawling ecosystem of underutilized systems. This sprawl increases cost, introduces complexity, and hinders detection engineering efficiency. A governance process must be in place to vet new tools, ensuring they align with clear objectives, address existing gaps, and create a plan for long-term management and support.

Logging agents often collect overlapping data. It's essential to be aware of this redundancy. Duplicated logs increase storage costs and can introduce noise when detections fire against both sources. Understanding exactly which tool provides the most accurate, timely, and enriched data for a given use case allows detection engineers to streamline and optimize their detection logic. Identifying high-priority sources—authentication logs, system events, sensitive data access—is key for focusing engineering efforts. A risk-based approach, in collaboration with business units, drives this prioritization.

Identity technologies are important to continuously answer: Do I know you? Do I trust you? How much access will I give you? In order to do this well, it is important to gather context. This is a first line of defense, and in-line defense to stop inhuman and fraudulent access attempts.

Mary Writz
SVP Products

The sheer volume of logs and alerts can overwhelm analysts and detections. Noise reduction becomes paramount. This includes filtering out routine events, aggregating logs where possible, and tuning out unnecessary data fields. Log retention practices must also be established, striking a balance between investigative needs and storage costs. All these steps, informed by threat intelligence, refine the data gathered to make finding actual threats far more feasible.

Personnel strategy

The recruitment or engagement of individuals for cyber defense detection frequently necessitates unconventional thinking, given the abundance of entry-level candidates and security providers relative to seasoned and highly skilled professionals. Establishing roles and responsibilities for cyber defense detection requires an examination of existing resources and the desired outcomes to be achieved through contractual arrangements. In most instances, it is feasible to hire, contract, and employ a Managed Security Service Provider (MSSP) to fill roles and responsibilities requiring specific expertise.

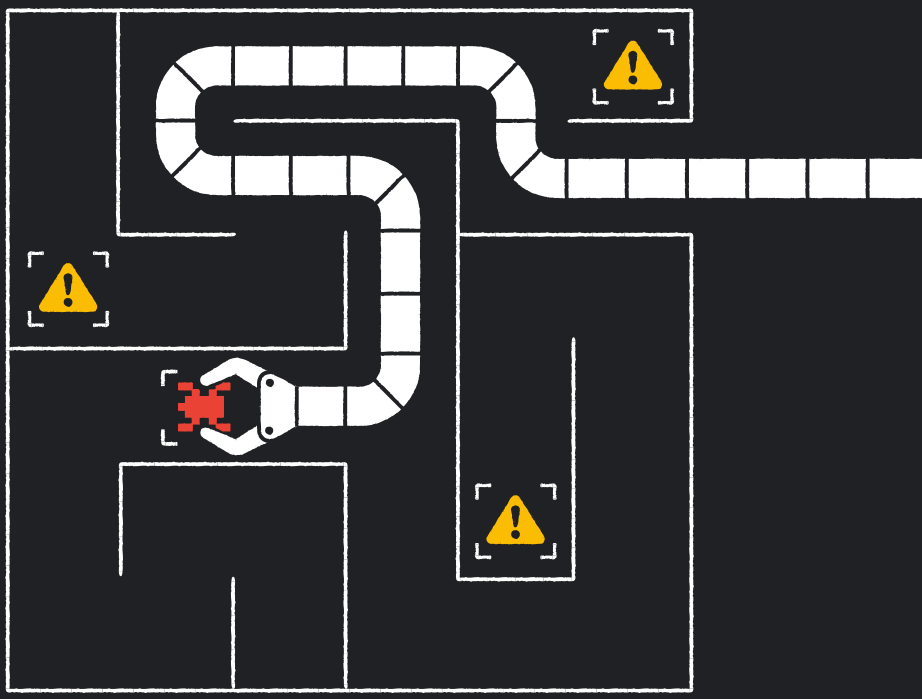
Critical detection roles constitute the initial point of contact for an incident. Ensuring adequate training and experience for individuals in these roles is essential. A notable challenge within the industry pertains to analyst errors leading to the closure of genuine incidents due to misinterpretations of associated events under review. Consequently, ongoing training efforts are necessary for the role and the solutions employed to maintain a robust state of vigilance for incident investigation. A comprehensive training plan should be developed, encompassing the expertise of diverse cybersecurity industry training, and incorporating the solutions utilized by the team.

It is important to challenge existing detection analysis teams and services through red teaming and purple teaming. These exercises provide opportunities to validate event analysis skills within a controlled learning environment. Detection analysts should possess the ability to review events and make factual determinations regarding the nature of incidents. Zero-fault root cause analysis enables the identification of missed activities, facilitating the targeted development of personnel and rules to drive continuous improvement in cyber defense.

Two critical roles that should be involved in testing and root cause analysis are event analysis and detection engineering. In many instances, these roles may be performed by the same team members or service. Striking a balance between the performance of both roles is essential to align team priorities when responsibilities are shared. Additionally, as capabilities evolve, it may be beneficial to introduce dedicated content development experts over time.

Providing flexibility within detection roles often enhances continuity and retention by offering team members greater variety and responsibility. This approach also fosters diversity in detection use case objectives and development, leveraging broader perspectives to contribute to detection improvement. Moreover, mentoring should be encouraged, not only from senior to junior members but also from skilled staff to the broader team.

Key performance indicators (KPIs) should be established to drive continuous improvement and assess the performance of team members and contracts in terms of process efficiency, tooling, and automation. It is important to avoid placing undue time constraints on detection analysis, as this may lead to premature conclusions without thorough vetting. KPIs should serve as performance metrics to confirm the efficacy of the detection process, ensuring that personnel are well-trained and equipped with the necessary tools to effectively carry out their roles.



Responding to compromise

The Respond function is responsible for timely and effective management of suspicious activities flagged by the Intelligence, Detect, and Hunt functions. The speed and agility with which an organization can respond to a threat can mean the difference between a minor inconvenience and a full-blown crisis. The Respond function is multifaceted and extends from confirming if the activity is malicious and returning computing services to normal operation to ejecting the threats and contributing to an organization's threat readiness and strategic development. The Respond function is also charged with preventing repeat incidents by identifying lessons learned, directing tactical and strategic enhancements through the Mission Control function, and feeding observations back to the Intelligence function.

Initial triage

Response begins when evidence of potential unauthorized activity is escalated for further investigation. This initiates the triage phase which guides future phases of the investigation based on the following.

- **Confirm the accuracy of information provided by the alert:** Determining if an alert is of real concern or just digital noise is pivotal to ensuring that the focus remains on genuine threats.

- **Determine if the alert is actionable:** Assess if the threat signifies an immediate danger. Some threats may exist but may not pose a pressing risk to the organization.
- **Determine acute remediation steps:** Some alerts require urgent action. Identifying these alerts is crucial for timely remediation, preventing potential escalation into bigger problems.
- **Prioritize the incident queue based on other active incidents:** Focus on rapid action on the most severe incidents with the largest potential impact to the organization.

The triage phase goes beyond surface-level evaluation. Analysts must dig deeper, understand the context of an alert, and gather additional evidence. This can be assisted or amplified by the collection of data or artifacts through automated activities or by the correlation and analysis of previous observed behavior. If a breach is revealed then the incident transitions from suspicion to confirmed incident that warrants a full-scale investigation.

Central to triage is the evaluation of alerts as true positives or false positives. A distinction that hinges on whether the alert faithfully represents a real threat in line with its detection logic. This nuanced analysis involves understanding the intent behind the alert setup, and distinguishing between malicious activities and legitimate operations that may trigger similar alerts.

Consider the example of a security team setting up alerts for the use of the "whoami" command within your environment. This command is a favorite among attackers and legitimate users alike, complicating its interpretation. If the intent of an alert is to flag any usage of "whoami" for review, then even legitimate use is a true positive, and the alert should fire in all cases. However, if the aim is solely to spot malicious use, legitimate use flagged as an alert is a false positive.

Data collection and analysis

Data collection and analysis are essential tasks for responders. This process demands the careful accumulation of both technical and non-technical details to form a complete understanding of the incident. The extent of this collection is customized based on the unique aspects and severity of the potential incident. As previously mentioned, the use of automation may help inform or support data collection with SOAR playbooks capable of providing collected inputs and artifacts to an analyst at the outset of triage and investigation efforts.

When it comes to technical data, the preservation of the target system's integrity is paramount. This is particularly vital in scenarios where the incident might lead to legal actions. In such cases, meticulously documenting each interaction with the system and ensuring a robust chain of custody for the collected data becomes non-negotiable practices. Collecting and reviewing the quality of collected data post-incident also provides an opportunity to improve manual and automated processes, helping to identify opportunities for improvement in the types, comprehensiveness, and timeliness of data collection or the process used to analyze and assess the collected data.

Non-technical information often surfaces through direct reports from users experiencing or observing suspicious activities. Such accounts may not always offer immediate access to raw data, prompting a direct dialogue with the reporters. This conversation aims to unearth insights into the system's use before or during the detection of the suspicious event, helping to distinguish between a simple misuse of resources and a significant security threat. This information may not always be provided in real time, but may provide important information about a current or future event. In conjunction with direct dialogue, enabling historical searches of previously captured non-technical information may provide additional context or insights that responders may not have had otherwise.

Engaging with the user to extract as much detail as possible provides invaluable context, whether related to activity timelines or additional investigation "self-help" steps. This dialogue not only aids in identifying the presence of malicious tools or malware, but also in gauging the user's awareness of such anomalies.

Further depth is added to the analysis through inputs from system administrators or from monitoring tools. These sources enrich the understanding of the incident by offering details such as hostnames, IP addresses, operating systems, programs, and user roles.

A critical reminder for analysts is the ephemeral nature of digital evidence; delayed collection can result in the loss of crucial information. Hence, there is an imperative to swiftly prioritize evidence gathering, balancing the need for comprehensive data collection against potential impacts on system performance. Before embarking on activities that might strain the system, engaging with IT and infrastructure teams is advisable to mitigate unintended disruptions. Based on review with IT and infrastructure teams, along with an assessment of the potential risk, disruption, and importance to the investigation, the use of automated playbooks to support common information gathering activities after specific triggers can also help expedite collection and enable timely data collection activities.

Decision points and next steps

As the triage phase unfolds, the analyst is tasked with evaluating the identified activity to decide on the most appropriate course of action. This decision making process hinges on the level of context available about the incident. In some cases, the analyst may have sufficient information to proceed with containment measures and resolve the incident swiftly. This decision is significantly supported by well developed incident playbooks, which guide analysts through the process based on predefined scenarios and responses. In certain cases, automated playbooks may have been actioned through a SOAR solution—resulting in the quick implementation of specific containment activities and artifact collection. In addition to providing contextual details for

the ongoing investigation, a quick analysis of the collected information may help identify follow-on questions or gaps that need to be answered.

If the analyst concludes that immediate resolution isn't feasible, the collected evidence and findings are then transitioned to the investigation lifecycle phase. Here, a deeper dive into the incident continues, aimed at uncovering more details and determining a comprehensive response strategy.

At this critical junction, the analyst coordinates with the Mission Control function to engage additional stakeholders necessary for the decision making process. For widespread incidents or those that involve sensitive or time-critical operational processes, incident response efforts are likely to require an organizational-level response that involves areas outside of the response process.

This includes determining the need for activating cyber insurance or consulting legal counsel. Such decisions are pivotal, particularly for organizations under stringent regulatory requirements regarding data breaches. Regulations often dictate specific protocols for reporting incidents like data theft or ransomware infections, with a clear timeline for notifications once an incident is identified. Engaging legal counsel early ensures that an organization understands its notification obligations and prioritized actions to comply with legal and regulatory standards.

Other considerations, such as engaging stakeholders to draft, manage, and disseminate internal or external communications, as detailed in the Mission Control function, may be important to protect a company's reputation and manage the ongoing narrative. Bringing in teams involved with communications early on provides stakeholders with more time to prepare and craft messaging before they are forced to react due to external pressures.

Playbook review

The responsibility of keeping incident response playbooks current falls to the analyst spearheading the triage process. Given the dynamic nature of cybersecurity threats, any automated or manual playbook requires regular review and updates. Using an outdated playbook can severely hamper incident response efforts, as it may refer to processes, people, and or infrastructure that are no longer applicable or relevant.

An actively used and periodically updated playbook signifies its value and utility to the Cyber Defense team. Conversely, a playbook that becomes obsolete is no longer a dependable asset for analysts to use. To avoid this, analysts need a process and the authority to promptly amend playbooks whenever they spot any inaccuracies or changes in the operational environment or even in the threat landscape (e.g., variations in attacker TTPs).

Beyond keeping content current, the SOC must also evaluate the effectiveness and accessibility of the playbooks. This involves developing metrics to gauge:

- **Frequency of use:** How often each playbook is utilized indicates their relevance and effectiveness.
- **Utilization patterns:** Identifying playbooks that are rarely or never used can signal the need for updates or consolidation.
- **Search efficiency:** Reviewing search terms and the number of searches required to locate a specific playbook helps in understanding if an analyst can easily find the resources they need.
- **Alignment with the threat landscape:** Playbooks should be reviewed to ensure they cover appropriate response actions to mitigate a commonly seen or novel threat scenario or specific attacker tactics that are of concern to an organization. If a playbook is missing a substantial amount of topical content, it should be updated for relevance.

- **Maintenance history:** Regularly reviewing when a playbook was last reviewed, updated, and executed can ensure that it remains relevant.

Addressing these aspects helps in fostering a robust, dynamic knowledge base. It's not just about updating playbooks for the sake of keeping them fresh, but rather making sure they evolve in tandem with the threat landscape and internal processes. This adaptability enhances the SOC's ability to respond to incidents at a consistently high speed, and in an effective manner.

To further improve playbook relevance and effectiveness, incorporating a mechanism for continuous feedback from users is crucial. This could include:

- **Post-incident review:** Analyzing the effectiveness of a playbook in real incident scenarios, and identifying areas for improvement.
- **Technology and threat landscape changes:** Updating playbook to reflect new technologies, security tools, and emerging threats.
- **Training and drills:** Utilizing playbooks in training scenarios, such as walkthroughs, tabletop exercises, or cyber ranges to identify gaps and areas where additional guidance is needed. Walking through an existing playbook end-to-end against a specific or subset of threat scenarios can help identify where updates are required in a simulated environment. More considerations for testing have been provided in the testing and validation section.

By prioritizing the maintenance and continuous improvement of incident response playbooks, analysts and the SOC can ensure that their incident response efforts are not only effective, but also efficient and tailored to the current threat landscape. The SOC should ensure that this responsibility is clearly defined and shared on a rotational basis, while maintaining clear accountability and reporting to validate that this important task has been completed.

Investigation lifecycle

The investigation lifecycle is pivotal for unraveling the complexities of a cybersecurity incident. Its primary aim is to uncover crucial insights about the attack, thereby empowering stakeholders to navigate legal, regulatory, and communication landscapes effectively. The intelligence gathered during this phase is instrumental in shaping the strategies for incident containment, and the ultimate eradication of the threat.

Core activities of the investigation phase

The investigative journey encompasses several key activities designed to peel back the layers of the incident:

- **Scope and status assessment:** Evaluating the breadth of the intrusion and determining if the threat attacker is still active in the environment
- **Chronology and origin:** Pinpointing the earliest evidence of compromise and identifying the initial attack vector
- **Data exposure analysis:** Assessing the nature and volume of data that was compromised
- **Adversary identification:** Unveiling the identity, TTPs, and motivations of the threat actors
- **Strategic contextualization:** Leveraging the findings to inform and guide containment and eradication efforts

The cyclical nature of the investigation

The dynamic investigation lifecycle begins with leads from the triage phase, such as forensic evidence of unauthorized activity. A classic example might be log entries that indicate unauthorized access, possibly stemming from a successful phishing attack.

Investigators embark on a meticulous process to preserve evidence, and dive deeper into the forensic artifacts. This exploration can include a variety of analyses:

- **System triage:** Performing live response analyses on affected systems
- **Forensic imaging:** Analyzing complete snapshots of compromised systems
- **Malware dissection:** Understanding the malicious software involved
- **Log scrutiny:** Delving into system, application, and security logs
- **Network traffic examination:** Reviewing network flows for signs of compromise
- **Intelligence queries:** Leveraging external and internal threat intelligence for clues

Dual pathways from analysis

The insights derived from these analyses pave the way for two critical paths:

1. **Unearthing additional leads:** By constructing a timeline of the attacker's movements, investigators can pinpoint further areas of interest, propelling the analysis forward.
2. **Gilding environment sweeps:** Knowledge about the attack can be distilled into IOCs, which then guide targeted searches across an organization's digital footprint. These sweeps aim to uncover similar attack vectors or artifacts, melding automated tooling with hands-on examination to ensure nothing is overlooked. These IOCs—and known related IOCs and TTPs—can later be integrated into the Hunt function.

A critical question that must be asked regularly is, "Does this make sense?"

Crafting a comprehensive attacker timeline

As the investigation iterates through these cycles, a detailed timeline of the attacker's activities emerge. This timeline is critical in answering the questions posed at the investigation's outset and fully delineating the incident's scope.

Incorporating modern enhancements

To further enrich the investigation lifecycle, integrating advanced technologies and methodologies can offer deeper insights and streamline processes:

- **Machine learning and AI:** Employing artificial intelligence to sift through massive datasets can highlight anomalies faster than traditional methods.
- **Automated sweeps and analysis:** Automated tools can help perform initial sweeps based on IOCs. Automated analysis should then be followed by manual, detailed analysis for nuanced understanding.
- **Threat intelligence integration:** Real-time threat intelligence should be continuously incorporated to refine IOCs and adapt to evolving threat actor tactics.

By embracing these enhancements, the investigation lifecycle becomes a more robust, efficient, and effective mechanism for navigating the aftermath of a cybersecurity incident, ensuring that each step is informed by the latest in technology and strategic insight.

Incident remediation

The remediation phase is crucial for eliminating threats from the environment and restoring normal operations. It also serves as a preparatory stage for the lessons learned phase by providing insights that can enhance an organization's security posture. The extent and complexity of remediation depends on the findings from earlier phases like triage and investigation lifecycle, as well as the scale of the impacted environment and any operational considerations that require minimal downtime for critical operations (e.g., systems supporting human safety).

For many incidents, remediation involves straightforward actions to cut off the attacker's access. These measures may include disconnecting or isolating the compromised systems, disabling affected user accounts, changing passwords, or blocking known malicious connections. Some of these actions may even be able to be taken automatically, following the triggering of specific playbooks within a SOAR. However, situations where an attacker has extensive system access or involving multiple entry points, long-term presence, or complex threat landscapes require a more detailed and planned approach.

Organizations facing significant threats should adopt a two-part, four-stage remediation strategy that aligns with ongoing investigative efforts.

1. Acute Incident Response

   A. **Containment:** Implement measures to disrupt ongoing attacker activities, monitor for further actions, and secure sensitive parts of the network.

   B. **Restoration:** Actions to revert any damage caused by the attack, such as decrypting data and restoring services to operational status.

   C. **Eradication:** Systematically removing the attacker's presence from the environment and making security enhancements to prevent reentry.

      Note: In significant ransomware incidents, it may be necessary to focus on restoration of critical services before eradication is achieved.

2. Long-term Security Enhancement

   A. **Security enhancement:** Use insights from the Remediation and earlier phases to inform the lessons learned phase, focusing on improving overall security measures, such as revising.

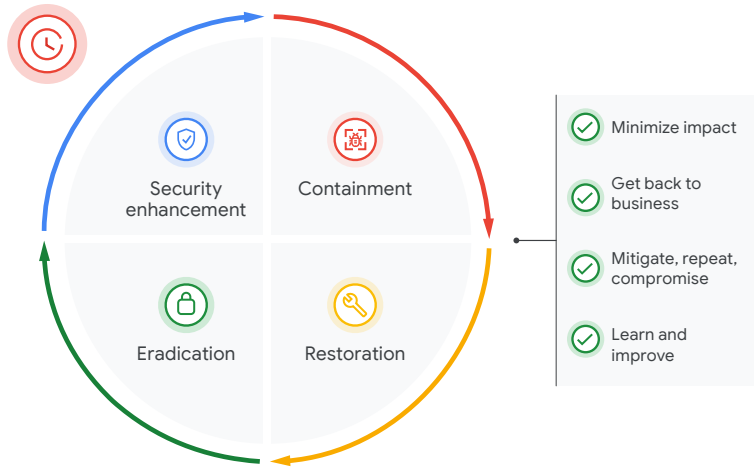


Figure 8: Incident remediation flow

Successful execution of these stages often requires robust communication and coordination with a wide range of stakeholders, including executive leadership, legal teams, compliance, IT, and HR. This collaborative effort is essential to ensure that the remediation actions align with the broader business objectives and legal obligations, minimizing operational disruptions and potential reputational damage.

Remediation plans should be adaptable to the specific circumstances of each incident, reflecting the unique operational complexities and needs of an organization. It's crucial that the Cyber Defense team, including the SOC analysts and incident responders, is empowered to make informed decisions based on a comprehensive understanding of the threat. This requires robust playbooks, ongoing training, and regular participation in simulation exercises to build and maintain effective response capabilities. Certain decision authorities for containment and eradication can be defined and documented in advance, following appropriate playbook definition, training, and review, to reduce ambiguity during a live incident.

The timing of containment and eradication efforts is a critical consideration. While rapid action can be momentous, especially in the early stages of an attack or in anticipation of a destructive action like ransomware deployment, it is essential to balance these actions with the need for thorough understanding. Premature or ill-informed decisions can exacerbate the situation, prolonging the incident and increasing the potential negative effects. Creation of a checklist of pre-defined considerations to help guide analysts to make decisions can help empower and reassure decision makers that their decisions are being made with a set of appropriate considerations.

Analysts must be equipped to make swift decisions, even with incomplete information, particularly when the risk of inaction exceeds the potential disruption of aggressive containment measures. An organization's ability to effectively manage these decisions comes from not only technical skills and tools but also from a culture that actively supports dynamic and informed decision making within the Cyber Defense team.

Structuring the remediation phase to address both immediate threats and long-term security enhancements, while also empowering analysts with the tools and authority to act decisively, can help organizations to effectively mitigate threats and strengthen their resilience against future attacks.

Containment

The primary objective of the containment stage within incident response is to curtail the attacker's access to an organization's environment and mitigate further damage. This stage is crucial as it supports ongoing investigative efforts and lays the groundwork for a comprehensive eradication strategy.

During containment, the remediation team implements a series of immediate and tactical actions designed to limit the attacker's reach and disrupt ongoing malicious activities. These measures also aim to enhance an organization's defensive posture, ensuring the environment is more resilient to future compromises.

Key actions include:

- **Enhanced visibility:** Boosting logging and monitoring capabilities to gain better visibility and track the attacker's movements and methods
- **Vulnerability management:** Promptly patching vulnerabilities that were exploited and applying necessary mitigations to prevent further exploitation
- **Communication hardening:** Restricting system-to-system communications where possible and tightening endpoint controls to avoid lateral movement
- **Credential protection:** Limiting the exposure of sensitive credentials on endpoints and reducing the footprint of privileged accounts. Organizations can also consider triggering automatic credential rotation for service accounts, or manually rotating them if required, if there is an indication of a broader or concentrated compromise across the environment
- **Account security:** Enhancing the security of local administrative accounts by reviewing and tightening permissions. This may include revoking or limiting privileges for certain groups of users during an active incident, or by requiring a check-in or just-in-time provisioning of permissions
- **Access control:** Overhauling remote access protocols, including hardening access to cloud systems, to prevent unauthorized entities

- **Operational safeguards:** Temporarily revoking access to critical systems or taking them offline to prevent data loss or corruption

In preparation for eradication, the containment stage also involves meticulous planning and documentation of an organizational and technological landscape. This preparation is vital to ensuring the eradication phase can be executed in a smooth and effective manner

Areas of focus in preparation for eradication include:

- **Authentication audit:** Cataloging all backend authentication mechanisms to understand all potential entry points that need securing
- **Directory services:** Reviewing an organizational unit (OU) structure within Active Directory to ensure account segregation and security
- **Privilege review:** Conducting a thorough audit of privileged accounts across all enterprise and cloud platforms to restrict attacker movement
- **Traffic control:** Identifying all egress paths and implementing robust control to restrict unauthorized data exfiltration
- **Stakeholder mapping:** Documenting application and business unit ownership to streamline communication and decision-making during eradication
- **Remote access overhaul:** Assessing and securing remote access technologies and SaaS platforms that are remotely accessible

Identifying and evaluating key actions against known attacker behavior during this phase is critical to limiting the scope and impact of the incident, while also reducing the extent of eradication activities that will be required later on. Playbooks, documentation, and checklists can help guide responders and expedite conscientious decision-making activities. All containment actions must be coordinated carefully with various stakeholders to ensure that the impact on business operations is minimized and that all actions are compliant with legal and regulatory requirements. This collaborative approach ensures

that the containment strategies are robust, comprehensive, and tailored to the specific needs and vulnerabilities of an organization and the ongoing incident.

Eradication

The eradication stage is a critical component of incident response, focusing on completely removing unauthorized access and restoring full control over the affected systems. Depending on the specific circumstances of the intrusion, the actions in this stage can be carried out concurrently with containment efforts, especially in urgent situations involving active threats like data exfiltration.

To effectively eradicate a threat, a coordinated approach is essential. This approach involves a sequence of deliberate and tactical actions executed in a timely manner to ensure that the threat actor is completely removed from the environment.

These actions typically include:

- **Network security enhancements:** Setting up network blocks and creating DNS sinkholes to prevent communication with attacker-controlled servers.
- **Account management:** Disabling compromised user accounts to cut off access for attackers.
- **System remediation:** Removing infected systems from the network to halt any ongoing malicious activity.
- **Privileged account security:** Implementing a comprehensive security plan for privileged accounts to reduce the risk of credential misuse.
- **Password controls:** Conducting an enterprise-wide password reset and rotating local administrator passwords to secure access points.
- **Hardware updates:** Replacing compromised hardware to eliminate any backdoors or persistence mechanisms installed by the attackers.

The execution of these eradication actions requires careful coordination across multiple teams within an organization, including IT, security, network operations, and HR. This coordination ensures that all aspects of the eradication are handled comprehensively and that there are no gaps in the security posture. In certain cases, these eradication efforts may be automated; however, implementing automation should be reviewed with business, IT, and security resources to ensure that this is acceptable given the possible impact to operations (whether during an incident or a false positive) and the possible impact of tipping off an attacker.

The timing of eradication efforts is crucial. In scenarios where the threat involves active exfiltration of data, immediate disruptive actions are necessary to mitigate damage while a more thorough eradication plan is developed. This might involve initial quick fixes that are later followed by sustainable security measures.

While the primary focus of the eradication stage is related to immediate threat removal, it is also the foundation for longer-term security enhancements. Once the threat is neutralized, the focus shifts to reinforcing systems against future attacks, which might include upgraded security software or specific configuration changes, enhancing monitoring capabilities, and revising response strategies based on the lessons learned during the incident.

Eradication efforts are closely linked with the broader incident response process, particularly the containment and lessons learned stages. Insights gained during eradication inform future prevention strategies, helping to refine an organization's overall cybersecurity posture and resilience against new threats.

Organizations can regain control over their systems by enacting a thorough and coordinated eradication stage. The timing, sequence, and coordination of activities can be critical to reduce the impact on an organization, reduce alerting the attacker in advance, and to improve the short-term and long-term security posture of an organization. It is imperative to review the efficacy of eradication actions during the lessons learned stage in order to inform process improvements or personnel knowledge prior to the next incident.

Security enhancement

The security enhancement and lessons learned stage serves as the final phase in the remediation process, focusing on reinforcing an organization's defenses to minimize the likelihood of future security breaches and to improve an organization's response capabilities if an incident does re-occur. This stage is crucial because attackers often re-target organizations they have successfully compromised before. Therefore, taking aggressive measures to strengthen the environment and response team capabilities post-remediation is essential.

One of the primary objectives of this stage is to conduct a thorough root cause analysis of the incident. Understanding the underlying causes of the attack is fundamental to preventing similar incidents in the future. This analysis not only helps in identifying the specific weaknesses that were exploited but also informs an organization's ability to fortify those areas against future attacks. This may include rule changes, configuration updates, or security awareness training for personnel.

In addition to preventive measures, this stage aims to enhance an organization's monitoring mechanisms. Improving these systems ensures earlier detection of IOCs and other signs of unauthorized activity, allowing for quicker responses and minimizing potential damage. This may occur through alert creation or enrichment, playbook updates for both manual and automated actions, integration of different tooling, or training for responders.

Throughout the remediation process, particularly during containment, eradication, and initial recovery stages, the remediation team often discovers various vulnerabilities and operational weaknesses.

The security enhancement stage includes:

- **Documenting findings:** Capturing detailed insights and observations made during the incident response about the nature of the vulnerabilities and the effectiveness of the deployed countermeasures

- **Developing and implementing recommendations:** Based on these findings, the team creates targeted recommendations aimed at closing security gaps and enhancing overall resilience. As mentioned above, these recommendations might include updates to processes and policies, changes to infrastructure, enhancements to security protocols, or new training programs for staff

The insights and recommendations generated during this phase helps to ensure that all valuable information acquired during the incident is preserved and utilized to improve an organization's security posture systematically.

Overall, actions derived from the lessons learned phase include:

- **Policy revisions:** Updating security policies to reflect new understandings and organizationally-required conditions to improve general security practices
- **Process revisions:** Updating playbooks to reflect improvements to response activities based on lessons learned from the past incident
- **Documentation uplift:** Revising or updating documentation to improve information available during an incident, such as clearly identifying business or asset owners for organizational crown jewels
- **Decision authority clarification:** Revising or reviewing key decision makers and approvers for actions that may impact key business functions or have a significant public-facing impact
- **Security training:** Enhancing employee training programs to improve general security awareness, latest security best practices, and, where applicable for a more technical audience, awareness of the specific TTPs used in the recent incident
- **Infrastructure upgrades:** Implementing technological upgrades or changes in the IT infrastructure to fortify the environment against identified threats
- **Continuous monitoring:** Establishing, upgrading, and tuning continuous monitoring tools to detect unusual activities faster and more accurately

- **Security technology upgrades**: Enhancing or implementing additional tooling to improve the security team's visibility or capabilities to take rapid containment or broader eradication actions

Ultimately, the goal of the security enhancement stage is not just to recover from a specific incident but to move an organization towards a more proactive security posture. This involves continuous improvement of security practices, regular reviews of the security landscape, and swift adaptation to new threats.

By effectively implementing this stage, organizations not only recover from the immediate impacts of an attack but also build stronger defenses that reduce the risk of future incidents and enhance their resilience in an ever-evolving cybersecurity landscape.

Testing response plans

Prior to or after an actual incident, it is important to socialize and test existing incident response and remediation plans to improve the timely and effective delivery of response activities and identify any areas requiring improvement. Tabletop exercises help identify gaps in response and remediation plans or playbooks and provide an opportunity to update plans based on the latest threats, while also providing a controlled environment to support training and upskilling for response and recovery teams. How an organization can establish an effective security validation and testing program are discussed in greater detail in the Targeted testing and validation of controls and operations section of this book.

Investigation accelerators

The technical demands of investigation, such as malware analysis, often exceed the in-house capabilities of many organizations. Developing these specified skills internally can be both costly and challenging, particularly when it comes to retaining talent. An effective solution is to forge partnerships with specialized consulting firms that offer targeted incident response and crisis

communications microservices. This approach extends an organization's investigative capabilities similar to if they had dedicated teams for these tasks, without the overhead of developing and maintaining such expertise in-house.

> *It is very common for organizations performing their own incident response to panic and attempt a premature remediation. They often jump to remediation efforts and introduce changes that complicate the investigation. This whack-a-mole approach will lengthen the investigation, cause incomplete remediation efforts and can lead to repeat attacks.*
>
> **Eric Scales**
> Vice President, Mandiant at Google Cloud

Consider outsourcing for defined, specialized skill sets that may not be present in-house:

- **Intelligence gathering**, given the depth and breath of available information and databases curated by specialized firms.
- **Malware analysis**, given the nature, complexity, and associated risk.
- **Forensics**, given the nature and complexity of evidence protection and analysis.
- **Digital threat monitoring**, providing an organization with additional visibility into any dark web chatter that they may not have the means to view themselves.
- **Legal/compliance advisory**, including enabling the enactment of privilege where required.
- **Managed detection and response**, for around-the-clock monitoring of the environment throughout the investigation.

- **Training and simulations**, to diversify the training provided to the team, and ensure comprehensive coverage of topical subjects.

Leveraging attacker intelligence

Understanding the threat actor is a game-changer in cybersecurity investigations. Integrating cyber threat intelligence (CTI) into the process allows teams to rapidly attribute malicious activities to known attackers or groups. This insight not only sheds light on the attacker's potential motives, but also their historical tactics and behaviors. Utilizing this information, investigators can efficiently prioritize their efforts in data gathering, analysis, and subsequent containment and eradication steps. This strategic approach enhances the team's efficiency, conserves resources, and, most importantly, accelerates the pace of the investigation to outpace the adversary, reducing the chance of their mission's completion or success.

IOC hunting automation

Automation of IOCs hunting represents a significant gain in efficiency. Given the consistency and repeatability in searching for simple IOCs such as IP addresses, domain names, and file hashes, organizations can deploy automation and orchestration tools to conduct these searches systematically. This strategy reallocates human expertise to more nuanced aspects of the investigation or other critical tasks, optimizing the use of valuable investigative resources. The output of these hunts can be used to enrich alerts, whether to adjust prioritization or provide additional context for analysis, or identify the need for additional alerts. In certain cases, it may identify indicators of an unknown potential incident that may require immediate review by an organization's responders.

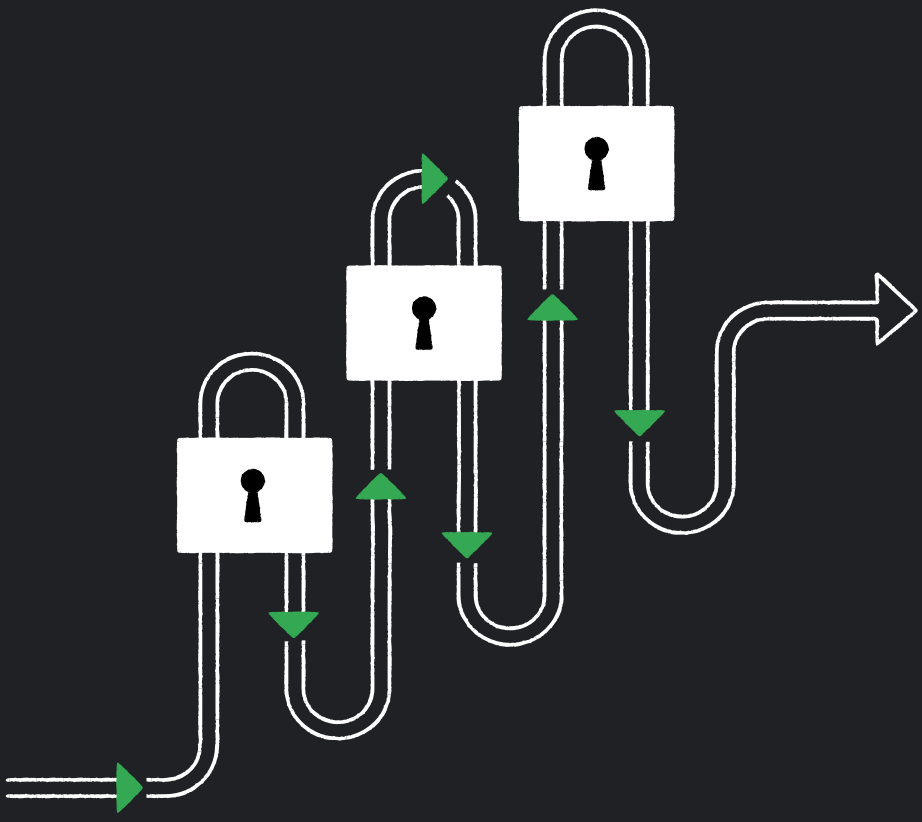
Incident Response Retainers

Most organizations face large-scale intrusions infrequently, and may lack the necessary experience for a comprehensive response. Securing incident response retainers (IRRs) with experienced providers ensures readiness and rapid deployment of expert resources when needed. Establishing service-level agreements with these providers guarantees prompt action, minimizing the impact of an intrusion. For added security, considering retainers with multiple vendors can mitigate the risk of any single provider not having available resources, ensuring that expertise is always at hand.

By adopting investigation accelerators such as CTI, hunt, microservices, and retainers, organizations can significantly enhance the speed and effectiveness of their response efforts. These strategies not only improve operational efficiency, but also bolster the overall cybersecurity posture, enabling a proactive and agile response to threats.

Enabling, empowering, and encouraging continuous learning for the Respond function is imperative to improving an organization's security posture and enhancing the ability for responders to conduct effective actions and make informed decisions. Triaging and collecting information is important to inform remediation actions, and evaluating these remediation actions post-incident is critical to building a positive feedback loop and enabling continuous improvement.

Across the entire incident lifecycle—from initial triage to the completion of incident remediation activities—defined processes help direct the timely sequence of activities. Within these processes, organizations should consider applying tools and automation to reduce the demand on resources, expedite the collection and analysis of information, and to trigger automated containment activities where possible to reduce the potential scope and impact of an incident. Executing on these activities collectively can be difficult, especially in a team with differing experiences and knowledge; therefore, walking through, testing, and reviewing each of these capabilities prior to or immediately following an incident is important in improving an organization's Respond function and overall Cyber Defense capabilities.



Targeted testing and validation of controls and operations

Targeted testing and continuous controls validation are an important function of Cyber Defense to understand strengths and weaknesses across the entire attack surface, to measure expectations versus reality. It is also the only process through which an organization can effectively assess the effectiveness of their cybersecurity strategy short of being breached by a threat actor. There are three key ideas that the cybersecurity management should keep in mind when trying to answer the question: *Why should we perform security validation?*

- It is elemental to acknowledge the holistic nature of our cybersecurity program commonly integrated by people, processes, technology. This will help to understand that technology is just one component of the attack surface and that threat actors will not hesitate to go after any of the other components in order to reach its objectives.
- Security validation must be aimed at enhancing the protection of what matters the most for the business, nevertheless, secondary assets might provide a way for threat actors to reach the crown jewels. This is why adequate scoping work becomes one of the most important aspects of security validation, considering the limited resources that the company may be able to allocate to this task.

- Security validation must be seen from a risk management perspective. Security validation can be highly technical in nature, however organizations must identify risks to the business in the vulnerabilities, attack paths, and exploits that may be revealed.

Without any Security Validation an organization is left operating with assumptions. Assumptions that the security controls are working effectively, that the technology is operating as expected, that security staff is critically evaluating all alerts, and that business staff are adjusting behaviors based on security awareness. Operating without security validation is akin to installing security cameras without assuring that they are working, monitoring anything meaningful, or assessing if there are blind spots that an intruder could take advantage of.

Security Validation is the means by which an organization can empirically evaluate their defenses in a controlled manner to drive decision making. Validation testing ensures that an organization understands their attack surface, knows where vulnerabilities exist, measures the effectiveness of controls and processes, and that they understand the organizational risk profile.

The mere-exposure effect creates a cognitive bias that can cause leaders to prioritize controls they are most familiar with over the ones that are most needed. It is vital to use validation techniques that don't reinforce your assumptions, but allow you to make objective, data-driven decisions.

Andrew Roths
Distinguished Security Engineer, Uber

An effective Security Validation program has the capabilities to reach across all cyber defense functions to drive change in the security posture of an organization. One common challenge is to recognize which components of Security Validation best suit an organization's needs. For example, is traditional penetration testing or a red team assessment going to be most beneficial? Acknowledging the details of each exercise and the value it can provide can help an organization make this determination.

Managing the attack surface

Identifying and comprehending the attack surface is a prerequisite for designing and implementing robust security testing strategies. An organization's attack surface encompasses all potential entry points that malicious actors could exploit to infiltrate systems or networks. Understanding the scope and components of this surface is paramount for pinpointing areas needing focused security testing and assessing the crown jewels and other critical assets that may be at risk. An organization's attack surface encompasses its cloud, hybrid, or on-prem infrastructure, software, applications, third-party suppliers, and employees. Traditionally, an organization's understanding of an attack surface would be to gather a list of external-facing assets, or to run simple vulnerability management scans to inventory IP ranges/netblocks, web applications, VPN servers, and external remote management services. Asset inventories can be manually compiled and stored in spreadsheets or gathered using Attack Surface Management (ASM) solutions. ASM solutions automate asset discovery across internal and external ecosystems, fingerprint technologies, and assess assets for exploitable vulnerabilities and misconfigurations. While spreadsheets offer convenience, sensitive information about business-critical assets should be stored securely in databases or within ASM solutions to minimize risk.

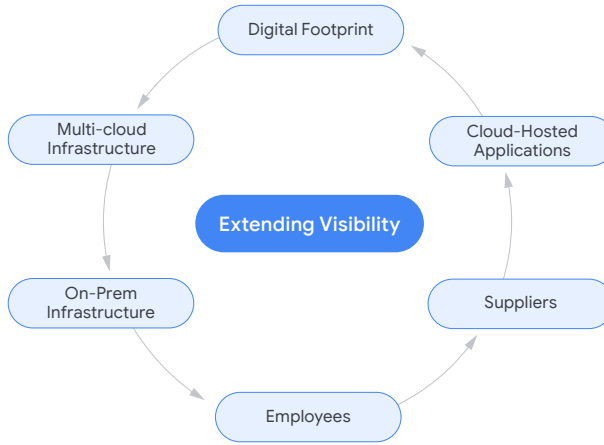


Figure 9: Scoping the attack surface

Critical assets that are typically overlooked or left off the list of assets within the attack surface include:

- External-facing database and remote access services
- Developer accounts on sites such as Github or Gitlab
- Staging and QA environments
- External-facing buckets or blob storage within a cloud environment
- Service accounts used for externally facing systems
- More esoteric application software and/or network services exposed to the Internet
- Secondary email systems that can be used to deliver payloads without content filtering
- Cloud-hosted applications with read and write access
- AI solutions' components (model, data, infrastructure, and applications)

Asset discovery can be performed manually or with the help of specialized tools. ASM solutions and third-party asset management tools offer automated solutions. It's important to note that ASM complements, rather than replaces, vulnerability management, penetration testing, and security validation. In addition to the asset inventory, the cyber defense organization needs several asset details, including the owner, location, criticality level, vulnerability assessment results, and security configuration. It provides valuable scope and context to focus these efforts.

Understanding the components of security validation

When discussing security validation, it is important to define the various components that comprise the function. Below are terms and respective definitions that an organization should be familiar with when building a program.

- **Penetration testing** is the systematic testing of defenses and critical assets to pinpoint and reduce vulnerabilities and misconfigurations. Penetration testers use real-world threat actor TTPs against systems, applications, embedded devices, industrial control systems, and even against people using social engineering. The purpose of penetration testing is to determine if critical assets are at risk and to identify complex security vulnerabilities.
- **Red Teams** test security effectiveness to gain an understanding of where an organization's weaknesses exist. Red teams provide an objective based approach to testing by leveraging current threat actor TTPs to accomplish a specific mission. These activities use highly skilled practitioners attempting to complete the object while avoiding detection. This provides an organization with an excellent perspective on what a threat actor might be able to achieve. The usefulness of Red Teams relies on the skillfulness of their methods and the currency of the intelligence on active TTPs, especially those of threat actors likely to target an organization. By utilizing highly skilled Red Teams to perform unannounced exercises, an organization can identify gaps in team member skill sets, cyber defense processes, and toolsets.

Our adversary simulation tests consistently identify vulnerabilities and gaps in security configurations and network architecture. Finding these risks is not a bad thing, doing nothing about it is. Using the latest intelligence in these tests is crucial to outpace attackers and ensure an effective security program against evolving threats.

Evan Peña
Senior Regional Leader of Global Proactive Services,
Mandiant at Google Cloud

- **Blue Teams** attempt to detect and prevent the actions of a Red Team and when they are unsuccessful in doing so, take the data provided by Red Teams and remediate where needed to optimize security effectiveness. The Blue Team relies on the Red Team's findings to tune controls and address gaps and vulnerabilities. Red and Blue Teams typically perform their functions in an asymmetric mode of operation.
- **Purple Teams** bring Red and Blue Teams together to work in a more collaborative fashion. These teams often leverage automated security validation tests integrated with threat intelligence. This lets Red Teamers test controls with multiple step-by-step scenarios to demonstrate how the security technologies and the Blue Team perform against the threats most likely targeting an organization. For Blue Teams, automated validation testing delivers prescriptive analytics that allows metrics showing improvement in the effectiveness of their controls and operations over time while still having meaningful red team curated tests executed.

- **Tabletop Exercises** evaluate and improve the capabilities of security personnel to respond to a simulated incident. Tabletop exercises typically entail a discussion based session designed to simulate relevant threats to an organization. These exercises are a critical component of validation, providing a means to assess the people and processes that make up an organization's security apparatus. Ultimately, a well conducted tabletop exercise will provide actionable insights into the capabilities, opportunities, and gaps of an organization's cyber defense capabilities.

Table B: Security validation terms and examples

Security Validation Term	Examples
Visibility. Event data and telemetry that may or may not be related to a security event	• Firewall flow or session log with basic connection information (SourceIP, DestinationIP, Port) • A windows event log
Detection. Aggregated telemetry that can indicate malicious activity has occurred. Detection data falls into two categories: • State. Events related to session state and identification. These do not identify security-related behavior, rather any type of communication. These may be relevant for post-compromise investigation; however, they do not provide context related to malicious activity • Security. Events related to the detection or prevention of malicious behaviors	• A log from a NGFW indicating malware has traversed the network • A log from an EDR indicating malicious activity is present on an endpoint
Prevention. Proactive or reactive action taken to stop an attack from being successful. This action is based on the detection and identification of malicious behavior *Note: While SOAR actions like isolating a host or disabling a user account may be compensating controls for responding to malicious activity, it is not considered prevention*	• Ransomware identified and blocked by a NGFW • EDR blocking the execution of a malicious file based on reputation or signature information
Alerting. SIEM-generated alerts stem from predefined rules within security controls, pin-pointing noteworthy events within the environment. They serve to notify SOC analysts of potentially concerning behavior, prompting either manual investigation or automated response. This aspect of security validation ensures that suspicious activities detected across all security measures are promptly brought to the attention of analysts for scrutiny	• An incident related to malicious activity is opened and ready to triage in a ticketing system

Intelligence-led validation

Intelligence-led validation refers to a structured approach of evaluating an organization's defenses based on the TTPs threat actors are most likely to leverage against an organization. The process involves identifying the top threats of concern, testing the environment against those threats, categorizing the results of those tests, and remediating identified gaps. An intelligence led approach most often involves the use of security validation testing platforms, but can also be conducted periodically through the use of red teams or purple teams.

Prioritizing how and what to test requires active adversary intelligence about what threats are most relevant to the company. Cyber defense organizations should not limit threat intelligence to historical analysis, but data that informs what attackers will likely do next, who they will target, and what methods they will use. As a first step in the validation process, the Intelligence can identify the threats that matter and drive a validation strategy. This insight enables security teams to execute relevant validation content and attacker TTPs to challenge security controls.

For instance, Intelligence-led validation helps keep defenders informed of how an attacker might perform should they be successful in gaining initial access in the environment.

Figure 10: Example of security validation process execution

Validating the effectiveness of controls

Having a basis of expectation for how an organization's security controls will respond to an attack is integral to a successful Security Validation program. A Security Validation program will evaluate how security controls respond to real world TTPs threat actors are leveraging. Through testing, organizations will derive the reality of security control performance. Comparing expectations to that newly found reality can then be the foundation of security posture improvements. A mature Security Validation program will regularly assess all of an organization's key cybersecurity controls, preventative or detective, manual or automated.

Expectations should be realistic. "I will block 100% of attacks" is an unrealistic expectation. Typically, the more granular and precise an expectation is, the more accurate and valuable the results of the comparison will be.

Example scenario

Expectation The organization logs all powershell activity through our endpoint security software.

Reality Through security validation testing it is determined that powershell activity is only logged in relation to malware detection.

Evaluate Are all "raw" powershell logs for compliance, incident response, or detection engineering purposes?

Finding Implement powershell logging through recommended means and re-test to determine if reality meets our expectations.

Validating the effectiveness of operations and staff

As part of the technical security validation program, evaluation of the effectiveness of the cyber defense organization's ability to respond to security events is needed. A security validation program provides actionable data on the performance of technologies and respective processes, but is not suited to assess the effectiveness of staff and procedures. To address this, organizations should perform frequent tabletop exercises and other simulated exercises. Tabletop exercises provide organizations with a means for evaluating their technical and executive response to an incident. These can also be performed in conjunction with managed service providers to validate the responsibilities and communications of each party during response.

Tabletop exercises can test preparedness across differing scenarios and can be designed for both Executive and Technical-level participants. Both approaches are key to validating an organization's incident response plans. Executive level exercises simulate strategic-level scenarios with significant business impact. These scenarios are aimed at providing insight into communications flows, processes, and procedures involving executive level staff spanning business units not typically associated with security. Executive exercises might involve legal counsel, communications, and human resources in order to evaluate preparedness to respond to an organization-wide ransomware incident.

Conversely, technical exercises are focused toward security operations staff, are more focused in scope, and evaluate tactical plans and processes. Technical exercises provide organizations with an understanding of the technical skills and abilities of their operational teams, while also indicating ways to enhance communication and coordination within and between Security Operations and IT teams. These exercises involve detailed technical scenarios involving critical or common threats to an organization. For example, zero-day exploits, data exfiltration, and ransomware attacks all present relevant technical scenarios worth evaluating. These exercises provide actionable insights on gaps in knowledge and tools, but should also improve existing workflows and processes with lessons learned.

Executive tabletop exercises should be performed twice a year and technical tabletop exercises should be performed quarterly at a minimum.

Table C: High-level comparison between executive and technical level exercises

	Executive Level Exercises	Technical Level Exercises
Scope	Strategic, Operational	Operational, Tactical
Scenarios	Organization-wide ransomware event, data breaches, Malicious insider	Zero-day exploits, Ransomware, Data exfiltration, Malicious insider, Supply chain compromise
Participants	CISO, Legal, Communications, Security Operations, Executives	Security Operations, Incident Response, Threat Intelligence, IT Staff
Outcomes	Assess: • Strategic-level decisions made in high impact events • Knowledge of crisis management plans and decision authorities • Crisis communications	Assess: • Technical knowledge, skills and abilities • Knowledge of Incident Response Plan and Playbooks • Knowledge and ability to execute on widescale containment and remediation strategies

Focused on organizational reputation, obligations, and oversight of incident management, Executive tabletop exercises should consider the following five major elements:

Elements	Sample topics
Incident management: Oversee investigative, containment, and recovery efforts	**Incident involvement:** When and how is the Executive team involved in incident response and remediation? Which Mission Control responsibilities transition to or require Executive approval after a certain threshold? **Decision authorities:** Who will have the ultimate decision-making authority for an organization during an incident including business impacting decisions like—disconnecting from the Internet, conducting enterprise-wide password resets, payment or non-payment of ransom and public disclosure timing? **Incident confidentiality and privilege:** Is a process in place to maintain privilege? Who is responsible for managing this?
Crisis management: Manage the declaration and handling of an organization-wide crisis	**Crisis declaration:** Who is responsible to declare an organizational crisis and what does this entail? **Crisis management:** Who is involved in managing a crisis? How does this differ from an incident? What responsibilities will transition to the Mission Control function?
Third-party management: Identify how and when third-parties may be engaged	**Legal and insurance coverage:** When will Legal Counsel and the insurance provider be notified or involved? **Third-party providers:** Which third-party providers will be brought in for support and when? Are service level agreements (SLA) in place? **Third-party partners or customers:** Who will be notified during an incident and by who? Are there any contractual obligations to do so within a defined time period?

Elements	Sample topics
Crisis communications: Manage reputation and sharing of information internally and externally	**Communication development:** When are Executives involved in overseeing or reviewing the development of internal or external communications? Are holding statements or templates available? **Communication approval:** Who is responsible to approve internal and external communications prior to publishing and dissemination? Does this vary based on the audience? **Communication dissemination and feedback loop:** Who needs to receive these communications? How will they be delivered and prioritized? How will recipient feedback be collected and provided back to the Communication development team?
Regulatory and privacy: Examine how regulatory and privacy obligations are assessed and handled	**Regulatory obligations:** What regulatory obligations must be met by an organization? What are the associated timeframes and who is responsible to ensure that these are met? **Privacy assessment:** How will an organization assess if a privacy breach has occurred? What are the key response activities required to manage a privacy breach?

Technical tabletops are designed to review an organization's technical capabilities and processes within the detection, response, and recovery phases. Technical tabletop exercises should consider the following six major elements:

Elements	Sample topics
Incident management: Direct investigative, containment, and recovery activities	**Incident declaration and activation:** Who is responsible to declare an incident and activate the incident response team? When is the Mission Control function notified or engaged? **Incident lifecycle and oversight:** Which role(s) have the authority to provide oversight to ongoing response activities and, where needed, assume Mission Control roles? Given the nature of the threat, attack, and business context, who is responsible to ensure the incident response activities are proceeding in an efficient, timely, and thorough manner? **Decision authorities:** Who has technical decision-making authority during an incident—including the decision to quarantine an endpoint, re-image a device, or reset passwords?
Triage: Qualifies events highlighted by the Detect and Hunt functions	**Timely intake:** Is there a defined and understood process in place to review and triage events identified by the Detect and Hunt functions? **Analysis and evidence gathering:** Do responders have a methodology and knowledge base to determine whether the event necessitates an investigation?
Investigation: Collect information to answer key questions about the attack	**Intrusion details:** Do responders have a defined methodology to determine the timeline and scope of the intrusion? How does the team confirm which assets and business functions are impacted? **Attacker motivation:** How do responders identify and analyze any available indicators that hint at the threat actor and their motives? Are raw intelligence artifacts and briefs provided by the Intelligence function and utilized by the Respond function? **Engagement of third-parties:** When should third-parties be engaged to provide incident response and technical assistance?

Elements	Sample topics
Containment: Take actions to disrupt attacker activities and regain control of the affected environment	**Playbook comprehension and familiarity:** Are playbooks available to guide containment activities? Depending on the type of incident and nature of the attacker, are incident responders familiar with the prioritization, identification, and execution of various containment activities? **Available tools:** Are responders familiar with existing tools that can be leveraged to conduct containment activities? **Decision authorities:** Which containment activities can be executed by the responder immediately? Which containment activities require additional approval or assistance?
Incident tracking and communications: Managing and maintaining a source of truth and timeline of events	**Remediation scope:** Is there a defined methodology that is followed by responders to properly identify and inform remediation activities—i.e.: fully remove the attacker from the environment and prevent re-compromise? **Restoration execution:** Are plans and playbooks in place to guide remediation and recovery activities, including large-scale remediation activities (e.g., password resets, mass rebuild)? Given the fact that additional teams will be involved in addition to the Incident Response team, are all teams and team members familiar with the division of roles and responsibilities? **Decision authorities:** Which remediation activities require additional approval or assistance? When does the Mission Control function need to be informed or involved?
Remediation: Remove the attacker from the environment and restore environments impacted by destructive attacks	**Incident tracking:** Who is responsible to maintain a record of incident developments and decisions? Where will these be recorded and who has access to this information? **Internal communications:** Who will draft any internal messaging required to be disseminated during an incident? When does this require additional levels of review and approval?

Following an incident or the completion of an exercise, it is imperative that the Mission Control function reviews the execution of response activities and outcomes of decisions that were made with the Response team and associated functions (e.g., Intelligence, Detect, Hunt). Identifying areas for improvement and taking proactive decisions to improve processes, tooling, or available training will help an organization to be better prepared when another incident occurs.

In addition to tabletop exercises, virtual environments and cyber ranges help validate a security team's technical capabilities, processes, and procedures by providing simulated scenarios allowing staff to practice responding to real-world threats without real-world consequences. Cyber Defense teams use virtualized environments that simulate typical IT infrastructure such as cloud environments, network segments, workstations, servers, and applications. These exercises are useful in the following ways:

- **Identify areas for team improvement**: Investigate real-world incidents to identify gaps in training, processes, procedures, and communication plans.
- **Investigate critical security incidents:** Test your response and intelligence teams with the latest attack scenarios and attacker TTPs.
- **Research and analyze identified threats**: Learn to research attacker TTPs and identify IOCs from host-, cloud-, and network-based artifacts.

These exercises should cover various attack scenarios including:

- Ransomware
- Insider threat
- Data exfiltration
- Active directory attacks
- Lateral movement

Validate and enhance the detection engineering lifecycle

At the core of the detection engineering lifecycle lies the foundation of visibility and telemetry data. This data serves as the bedrock for crafting effective detections that can identify and respond to potential threats within an organization's network. Security Validation can be employed in the Detection Engineering Lifecycle in two main use cases:

- Identify detection gaps and create new detections based on missed malicious activity
- Test and tune existing detections to ensure high fidelity

For example, the Intelligence function is tracking a new or novel attack technique that threat actors are using in the wild with the end goal of deploying ransomware. An organization can leverage security validation testing, either through a red team simulating adversary activity or a security validation tool to quickly test their existing detection capabilities against the new attack method. Validation testing can either reveal that existing detection rules cover the new attack method or an organization will have identified a detection gap. Detection engineering resources can either create new rules or tune existing rules to detect the activity and the attack method is re-validated to ensure coverage. The detections created and refined from this process can then be further tuned and continuously validated for consistency. At this point in the process, a business decision is to be made to assess whether this detection can be enabled for prevention or alerting.

Manage organizational vulnerabilities

Define processes, procedures, and plan to address an organization's threat exposure management

The sheer volume of vulnerability data that needs to be processed, analyzed, and prioritized can be overwhelming and very resource-intensive for organizations. Traditionally, organizations take a reactive approach to threat and vulnerability management by identifying vulnerabilities, assessing their severity based on Common Vulnerability Scoring System (CVSS) assessment measures, and patch or update configurations on a monthly cycle. Based on how quickly vulnerabilities can be exploited, organizations must be more proactive in managing threat exposure.

To accomplish these goals, organizations must establish a threat exposure management plan that defines the processes and procedures for exposure management and remediation, methodology for asset discovery, asset owner identification, and roles and responsibilities for critical stakeholders which often include resources outside of the cyber defense organization. Additionally, this plan should focus on identifying commonly known vulnerabilities and misconfigurations in the environment and be capable of scoping out specific risks based on business impact priorities and actual risk of exposure based on credible vulnerability threat intelligence (VTI), the organization's cyber threat profile, and the context of the asset (network exposure, data criticality, business criticality, compliance implications).

VTI gives considerable weight to active or potentially active exploitation as well as the impact of successful exploitation. Vulnerabilities actively exploited by threat actors targeting an organization identified through ad-hoc intelligence or an organization's threat profile should significantly influence prioritization. In addition to credible VTI, the Exploitation prediction Scoring System (EPSS) provides an additional attribute to predict exploitation and help drive prioritization in instances where there is no credible commercial VTI available to the organization. With a defined methodology that uses a combination of credible VTI, EPSS, asset/environment context, organizations are enabled to distill the mass of vulnerability information into actionable data.

Focus prioritization on criticality to an organization

By using factors including exploitability based on real-world attacks that are actively occurring, consequences an attacker could have on a targeted organization, and ease of exploitation significantly reduces the number of vulnerabilities that CVSS deems as critical or high and allows cyber defense teams to focus their attention on the most dangerous vulnerabilities. Critical vulnerability ratings should be used sparingly and when remediation is the top priority for an organization due the ease of exploitation and potential impact to an organization.

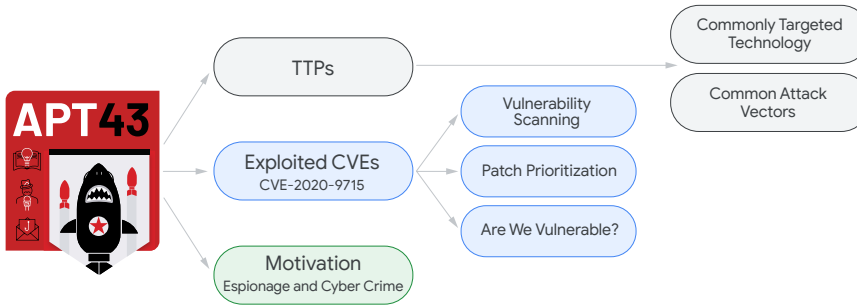


Figure 11: Example of intelligence feeding the threat exposure management process

This graphic demonstrates a sample methodology of how cyber threat intelligence feeds into the threat exposure management process to enhance and contextualize the patch prioritization process. In this example, threat exposure management curates vulnerabilities and assesses their severity based on factors critical to an organization. The threat exposure management process will determine whether an organization is vulnerable. Threat intelligence provides the latest information on whether the vulnerability is being actively exploited in the wild and if threat actor's motivations are specifically relevant to an organization. Based on inputs from threat intelligence, threat exposure management makes the final prioritization decision. In this case, an otherwise medium priority vulnerability is escalated to high priority based on use by specific threat actors known to target an organization.

Evaluating the likelihood of attack success and estimating the highest potential impact by analyzing all potential attack paths to the most critical assets is also a part of a threat exposure management program. To assess the likelihood of a successful attack or confirm that attackers can exploit the most critical exposures, the cyber threat intelligence (CTI) and/or vulnerability management team should perform additional security testing using security validation to prove which discovered vulnerability exposure could impact the organization. The output of security validation testing can be used to prioritize exposure remediation and hardening cyber defense gaps.

Automate threat exposure management workflows and reporting
As organizations prioritize vulnerability based on business impact and VTI, organizations should investigate the benefits of automating workflows throughout the threat exposure management Lifecycle. Automating threat exposure management capabilities should be gradual as the CTI or vulnerability management teams provide more visibility to all stakeholders and mitigation timelines are agreed upon and enforced. Organizations should consider the benefits of a unified vulnerability management or exposure management platform. Many unified vulnerability management solutions can provide the capability of ingesting scan data from most vulnerability scanning tools and provide ticket tracking throughout the vulnerability management lifecycle including the tracking vulnerability risk exceptions. Unified vulnerability management solutions can provide the platform for prioritizing vulnerabilities based on credible VTI and business risk factors, integrate with other cyber defense workflows, and serve as the primary platform for vulnerability metrics and reporting to IT stakeholders and senior leadership.

Informing organizational risk

A key output of any mature Security Validation program is clear and concise reporting that answers key questions regarding an organization's current security posture. This reporting should help an organization understand their risk profile based on the performance of their security controls against threats likely to impact it. This can involve comparing security controls against the

MITRE ATT&CK techniques used by threat actors likely to target an organization. As a key point, security validation reporting highlights security gaps in the existing controls' configuration. Previously unknown security risks can become known and actionable items for teams to address.

Security validation reporting should reflect the operating realities of an organization. When threat intelligence identifies a new threat actor targeting it, security validation testing data can help highlight how that threat actor might perform in the environment and if they were to succeed in bypassing first line defenses. This helps ensure testing is relevant, proactive, and drives immediate change in an organization's security posture.

Key output of a successful security validation program is to provide quantifiable data which drives business decision making such as policy changes, technology acquisition, and other security investments.

This data allows cyber defense teams to:

- **Rationalize security investments with continuous security validation:** Security teams can capture data required to prove effectiveness of security to support rationalization of security investments. Additionally, the use of security validation can provide insight into the impact of a change or removal of a control within the security infrastructure and in the context of a company's risk tolerance. Once controls are optimized, security leaders can use validation data to continuously measure and demonstrate an improvement to the security program and investments. Equally important, companies can pinpoint where overlaps exist and find ways to cut costs without impacting risk.
- **Tune and create detection rules within the environment:** Using data from security validation testing, detection and engineering teams are enabled to tune and enhance existing security rules to detect malicious behavior in the environment against real world attack scenarios. New rules are developed to close visibility gaps in the environment.

- **Schedule Hunt Missions:** In some cases, detection may not be feasible for all potential actions that a threat actor may use in the environment. These cases include living off the land techniques which may be too noisy for a SOC to respond to on a regular basis. For techniques in which there are known visibility gaps, threat actors of concern are known to leverage, and it is not practical to prevent the activity, these techniques become ideal places for threat hunting to be used to mitigate risk. In areas in which detection is not viable, hunt missions should be scheduled to search for malicious activity in areas in which an organization has known detection gaps.
- **Inform security policy:** It is almost certain that security validation testing will shed light on gaps in security controls that cannot be adequately mitigated through technology acquisition, detection rules, or hunt missions. Security validation will indicate areas in which a security policy change is needed to mitigate discovered gaps in the environment.

Identify gaps in cyber defenses

ASM offers a crucial foundation for effective security validation. Traditional approaches often miss hidden assets and vulnerabilities, leaving organizations with incomplete risk assessments. ASM provides a comprehensive, up-to-date map of your entire attack surface, including cloud resources, external-facing systems, and overlooked or unknown entry points.

By understanding the full scope of potential attack vectors, security validation efforts can be focused on the most critical areas. ASM pinpoints where your most valuable assets are exposed, allowing security teams to prioritize testing and simulate realistic attack scenarios. This integration of ASM and security validation ensures that your defenses are robust against the threats that truly matter.

Consider the following decision tree. Upon identifying a detection gap, an organization will attempt to either remediate that gap and create a security capability, accept the risk that gap poses, or mitigate the risk through regularly scheduled hunt missions. Remediation may involve crafting new detection rules, tuning existing rules, updating security policies to prevent the activity in question or, in some cases, acquiring new technology with greater capabilities.

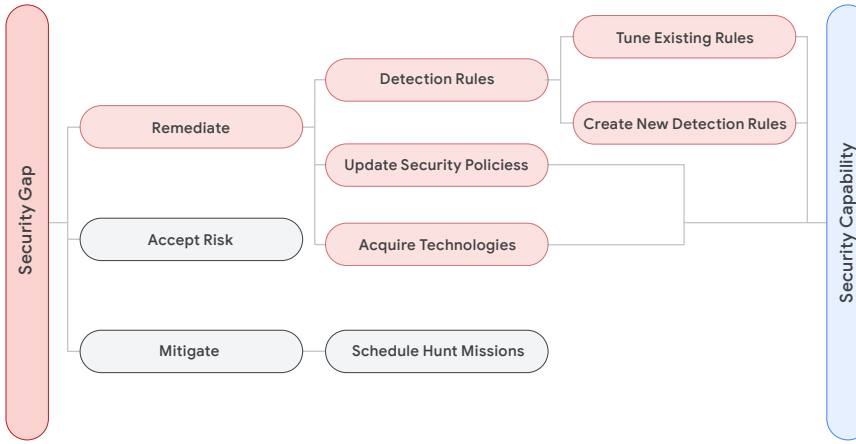


Figure 12: Validation decision tree

Without security validation, an organization is effectively blind to the effectiveness of their controls. They are given no other option than to trust that every detection rule has been accurately crafted, that every security tool works precisely as advertised, and security configurations never drift from their intended state. Unfortunately, the reality is that without security validation, organizations are forced to operate with unknown security gaps.

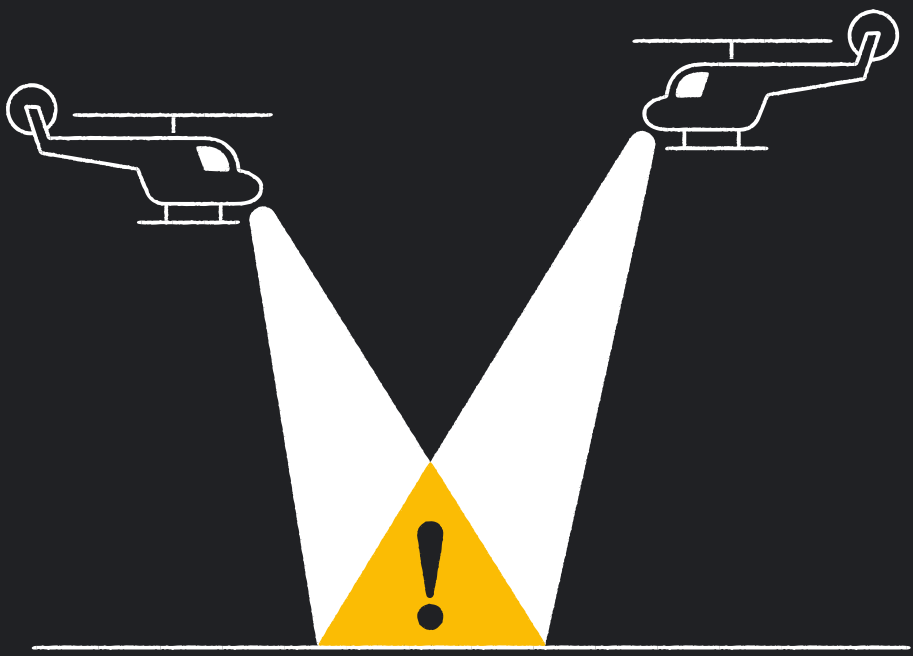
Alternatively, with systematic and continuous adversary simulation testing, security gaps that exist in the environment are revealed. Previously unknown security gaps become known and either documented as acceptable risks or closed. Security validation provides a methodology for identifying detection

capabilities, opportunities for improvement, and security gaps in the environment. Security teams are enabled to highlight gaps with quantifiable data. Once gaps are identified, those gaps can be addressed directly or mitigation strategies can be implemented. For instance, in scenarios where alerting is not viable for particular malicious activities, scheduled hunts may be implemented to mitigate a security gap.

Identify environmental and configuration drift

Consider an organization that must dynamically meet the rapidly changing business needs. For instance, a CEO might ask that a video sharing application be temporarily allowed to meet with an important partner. A remote desktop session is permitted for an emergency use case and a local user requests administrator access to install a business critical application. This type of scenario is part of typical business operations but any of these steps can introduce configuration drift. As a result, configurations are modified then forgotten and endpoints and servers end up in a state far from their intended secure configuration.

This scenario helps highlight the importance of continuous monitoring for environmental and configuration drift. Changes naturally occur in the IT environment which may affect security effectiveness. To ensure cyber defenses are not weakened, it's critical to continually monitor, detect, and alert on drift to accurately measure effectiveness.



Hunting for active threats

Goals of threat hunting

The Hunt function proactively applies intelligence about an adversary and its operations to identify active or previous compromise. It also works to strengthen an organization's overall security posture by revealing weaknesses in security controls and/or gaps in visibility across digital assets. A successful threat hunt program can reveal an ongoing attack, help address vulnerabilities, improve detection and visibility, and increase the difficulty for attackers to compromise systems.

A threat hunt has four goals aligning to the discovery of adversary activity outside of existing detection methods and reducing dwell time.

- **Systematically reduce threat exposure:** Identify detection strategies for new attacker TTPs through creative use of available logs and data sets.
- **Provide decision advantage:** Threat hunting bridges the gap between automated, computer-driven detection, and human analysis to increase the fidelity of findings driving security tool and operations choices.
- **Align resources to threats:** Discovery and awareness of gaps in security controls inform security and architecture decisions.
- **Higher fidelity cyber threat intelligence:** Understanding of the operating environment informs the Intelligence function to facilitate delivery of IOCs tailored to the organization.

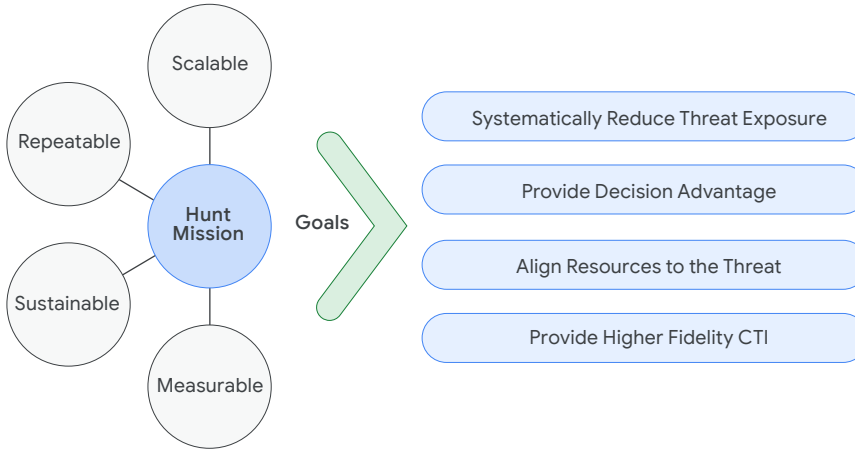


Figure #13: Goals of Threat Hunting

Developing a threat hunt program

Developing structure, governance, and validating technical capability are paramount for long term success. Consideration must be given to the scope and frequency of hunt missions and aligned to the maturity level of current detection technology, logging and asset visibility, potential attack paths, and staff qualification levels.

Programmatic considerations

Threat evaluation: Threat hunting should be predicated on specific threats to inform an understanding of who is targeting an organization, their intent and objectives, their level of sophistication, and the possible impact to your organization if they were successful. Additional considerations when evaluating a threat include:

- TTPs threat actors employ during operations and evidence they leave behind
- Anomalous user behaviors
- Critical controls and systems likely to be targeted, exploited, or leveraged
- Time the threat actor typically takes to complete their objectives from initial contact to compromise
- Detection mechanisms associated with the threat actor's TTPs

Security posture: Threat hunting should enable identification and analysis of gaps in technology configurations and detection coverage. Additional factors to consider include:

- Visibility in the environments to conduct the hunt mission
- Areas of the environment not being monitored or where additional logs could be collected for analysis
- The current logging and data retention strategy

Intra-team communication: Collaboration with other cyber defense functions should focus on reducing the time to detect compromise, increase situational awareness, and facilitate an intelligence-led detection process. Threat Hunt and offensive security teams should share information bidirectionally, validating threat hunt findings are viable exploitation paths, and checking for IOCs based upon penetration testing findings. Additional considerations include:

- Communication of hunting results to other teams
- Application of lessons learned to inform future hunts

Threat hunting skills: As threat hunt complexity and sophistication increase, the capabilities of team members also must increase. Core analyst competencies in incident response, log analysis, and threat intelligence can be enhanced by data science skills to facilitate finding patterns and drawing meaningful conclusions from large datasets. Additional considerations include:

- The availability and capability of in-house security team
- Integration points for 3rd party or outside hunt resources
- Formal threat hunt training and/or mentorship opportunities

Capability considerations

An effective threat hunt function should have some level of capability across the following components to enable success:

- **Enterprise visibility:** Effective threat hunts start with well-formed hypotheses based on knowledge of an organization's assets, their exposure, and their criticality.
- **CTI:** High-quality CTI provides insights into current threats, attacker TTPs, and emerging trends, enabling hunters to focus on the most likely and impactful scenarios.
- **Logging:** Logging should capture relevant events across an organization's environment, including endpoints, network devices, applicable cloud providers and applications.
- **Technology:** Access to detection and analytics platforms (e.g., EDR, SIEM, Network IDS/IPS and Cloud Security and/or Logging Tools) to provide data on activities related to digital assets.
- **Capacity:** Teams need to have dedicated time for hunt activities and have access to the right internal subject matter experts or external resources.

Threat hunt pipeline

After considering the programmatic and governance factors related to the Hunt function and deciding to continue toward a hunt mission, preparation is key. Teams follow a structured process called the threat hunt pipeline to plan for a Hunt:

Figure 14: Threat hunt pipeline

By following this structured approach, threat hunts can increase the chances of detecting compromise.

Threat intelligence considerations

Threat hunting must be driven by intelligence which identifies the types of adversaries that could target an organization. In the CTI portion of the pipeline an organization's threat landscape is analyzed, based on risks and threats to its industry and region it operates in as well as its cyber threat profile, the specific vulnerabilities and its attractiveness to attackers. Armed with this knowledge, potential adversaries can be categorized based on the following factors:

- **Motivations:** Reasons why an attacker would target an organization
- **Capabilities:** Sophistication and resourcefulness of adversary

Figure 15: Adversary capabilities and motivations

Once potential adversaries are identified, focus shifts to the identified threat actor's TTPs. These are the specific methods attackers use to infiltrate, move within, and achieve their goals in a target network.

CTI and the associated TTPs can be derived from a variety of source to include:

- Threat intelligence reports
- Previous incidents within an organization or industry
- Open-source research

Threat modeling is a process by which potential threats are identified and enumerated, and detection opportunities and countermeasures are developed.

Threat modeling and visibility mapping

Once CTI insights on adversary TTPs are collected, they are combined with an understanding of the 'crown jewels' data and systems to construct realistic attack scenarios and identify likely places an adversary will conduct operations. The threat models created in this step will then be the basis for hypothesis development in the next step of the threat hunt pipeline. Threat models are developed by creating a visual representation of scenarios targeting a system, application, or network called an attack tree.

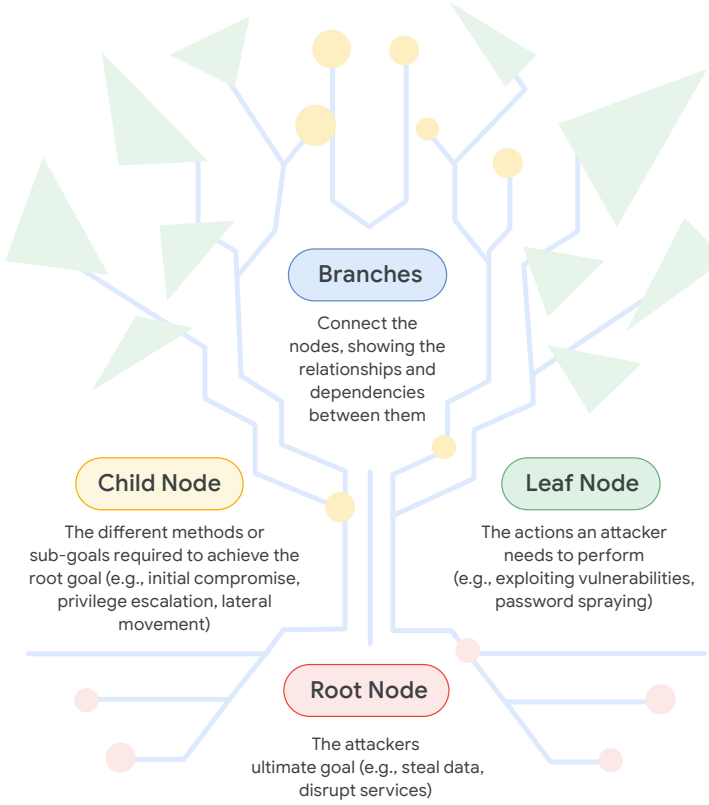


Figure 16: Components of an attack tree

To build an attack tree, follow these steps:

1. **Determine the goal:** Identify the high-level objective an attacker might have.
2. **Break it down:** Break the goal down into smaller steps, asking "How could an attacker achieve this?" at each step.
3. **Identify vulnerabilities:** For each action an adversary needs to perform to achieve their goal, pinpoint specific weaknesses that could be exploited or gaps that could be taken advantage of.
4. **Analyze paths:** Trace the different paths through the tree, gauging their likelihood and potential impact. Attack trees can be valuable when preparing for a threat hunt as they help teams focus and prioritize their efforts on the most likely and impactful scenarios. The leaf nodes of an attack tree correspond to specific actions and events which can be analyzed to discover IOCs.

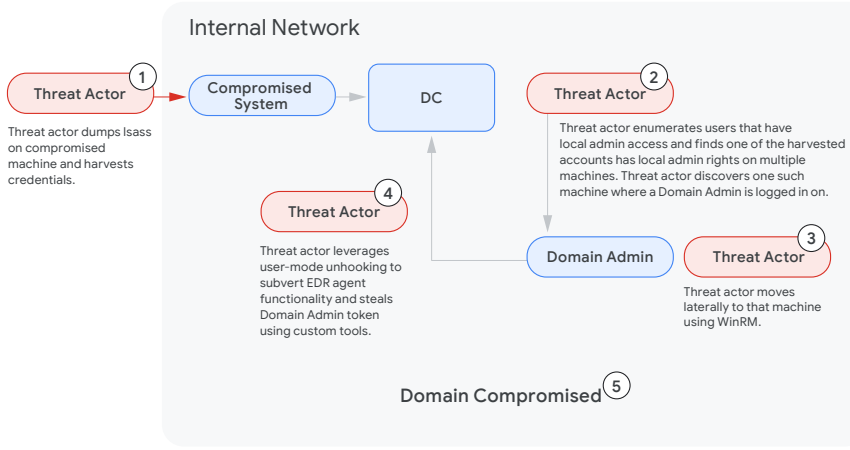


Figure 17: Example of an attack path

Attack trees can be valuable when preparing for a threat hunt as they help teams focus and prioritize their efforts on the most likely and impactful scenarios. The leaf nodes of an attack tree correspond to specific actions and events which can be analyzed to discover IOCs.

Hypothesis development

The hunt pipeline culminates in hypothesis development. Importantly, each hypothesis assumes a compromise has already occurred. During a threat hunt, teams will try to prove or disprove this assumption by seeking evidence of the hypothesized scenario.

When developing a hypothesis, there are several ways to guide development to achieve higher relevance. The use of past incident data or red team assessments can provide indications of previous weaknesses or previous critical controls that, had they been bypassed, would have allowed more significant exposure. This form of data has a high fidelity as it has already been demonstrated and observed in the environment. Further hypothesis

development can be guided using internal and external CTI, especially when combined with local knowledge of an organization's environment and critical assets. Hypothesis creation can be aligned to and further refined with threat trending and attacker TTPs. Ideally these would be mapped to a common framework such as the Mandiant Targeted Attack Lifecycle, Lockheed Martin Cyber Kill Chain®, or MITRE ATT&CK framework.

> *Security tools are vital, but they're not a substitute for human expertise. Threat hunting brings that expertise to the forefront, proactively seeking out threats which may have bypassed automated defenses*
>
> **Muhammad Muneer**
> Principal Consultant, Incident Response, Mandiant at Google Cloud

Performing threat hunts

With a Hunt program established and the planning of the threat hunt pipeline complete, a threat hunt can commence. The four pieces of a threat hunt are assess, acquire, analyze, and action. A hunt mission is created during the assess phase, and executed during the acquire phase with the goal of proving or disproving a hypothesis. The four step process also includes a security sub-process to activate upon discovery of a certain triggering action for example a confirmed threat actor command and control beacon. The security sub-process could include activating an incident response plan, developing new threat detections, performing a security architecture review, or incorporating lessons learned into other Cyber Defense functions.

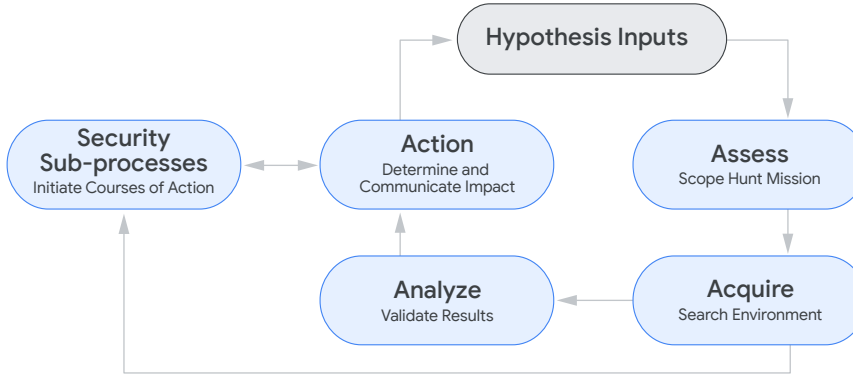


Figure 18: Hunt mission process

Assess (Scope the hunt mission)

Already completed pipeline steps of threat modeling and visibility mapping have identified the targeted attacker TTPs and IOCs. In this phase these are leveraged to identify the specific sources and acquisition methods for data in the future aquire phase.

- Identify targeted data, hunt mission timeframe and potential cost limits
- Determine visibility, data collection and search capabilities
- Assess the value of gathering new data for a hunt mission versus using existing data sources

Acquire (Search the environment and gather data)
This is the data-gathering phase. Based on the outputs of the Assess phase and defined collection methods, conduct a hunt mission to search for activity in the environment.

To conduct the hunt mission:

- Identify access requirements and tools
- Initiate data collection and search
- Validate the completion of searches
- Perform initial analysis, inclusive of stacking and frequency analysis
- Escalate high-impact threats by activating the security sub-process

Analyze (Validate results)
Outputs need to be validated before continuing, to make sure results match what was expected. The outputs are logical conclusions, judgements and facts based on analysis. Assessment of the outcome will serve as a guide to next steps, for example, written recommendations, threat summary, additional searches, data sources or requests for new CTI products.

To validate results:

- Evaluate target matches
- Correlate, sort, and link data, then prioritize
- Pivot to related/new data
- Perform inferential analysis
- Determine attack vectors and TTPs
- Determine control effectiveness
- Identify hunt limitations and constraints

Action (Communicate impact)
Information and recommendations need to be disseminated. This includes a strategic view and recommendations. This can be a combination of very tactical (e.g., patch management), and strategic, such as a business decision around budgeting.

To communicate impact:

- Determine overall impact
- Develop threat summary
- Form strategic outlook
- Identify gaps in process
- Identify data to block or alert on
- Deliver report and obtain feedback

Security sub-process (Initiate courses of action)
The security sub-process is initiated based on the results of the hunt. To initiate courses of action:

- Activate incident response plan
- Develop new threat detection content
- Perform a security architecture review
- Resource allocation assignments
- Incorporate lessons learned into Cyber Defense functions

Pivoting

Pivoting is a tactic and mindset used by threat hunters to move between data sources and improve hunt mission findings. Pivoting provides a chance to be creative in finding unique correlations, patterns and insights. Pivoting sources can include:

Previous hunts

- Previously observed similar activity
- Documented previous analysis/actions which can save time and effort

Intelligence (internal and external)

- CTI enrichment on specific indicators
- CTI context on associated threat actors, TTPs, and other adjacent IOCs

Automated tools (sandboxes, web page scanners)

- Output shows context on potential maliciousness and other IOCs to review

Community sources (blogs, etc.)

- IOCs discussed in community forums or blog posts may link other TTPs, IOCs, or Threat Actors to observations

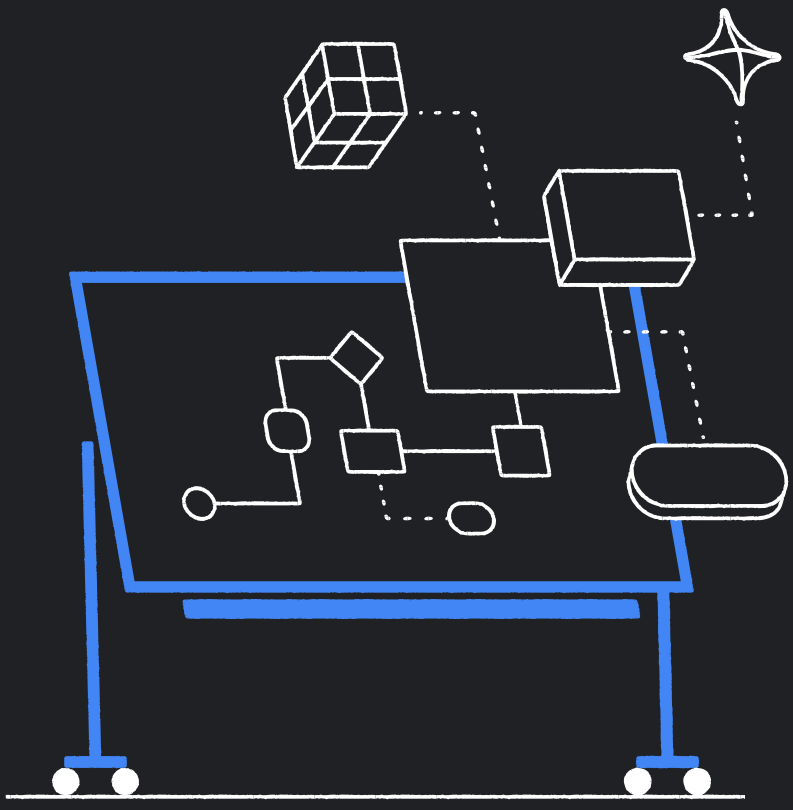
Indicator investigation (whois, pDNS)

- Indicators may be tied to high-risk infrastructure (IPs in unexpected countries' domain registrars) or other suspicious elements which provide new information to investigate

Developing detection use cases through hunting

A threat hunt can be an excellent driver of creating new detection use cases to be used on a more frequent basis. Hunt missions and associated analysis can be evaluated for translation into actionable detection rules and alerts. This can help security systems and identify similar threats more effectively in the future and can be incorporated into security automation tools. Additionally, it can help improve the fidelity of future threat hunts by focusing on TTPs outside the scope of current automated detections.

The Hunt function helps shore up defenses by identifying previously unknown compromises or gaps in security controls. Intelligence-driven hypotheses are predicated on an understanding of the cyber threat landscape, common attacker behavior, an organization's security posture, business processes, and the attack surface to guide hunt efforts. Threat hunters must stay nimble and maintain awareness of shifts in organizational decisions or commentary from senior leadership—such as announcements of potential mergers or acquisitions, expansion into different geographic locales, or other public announcements—and threat actors' motivations and targeting.



Coordinating Cyber Defense through Mission Control

Mission Control acts as a centralized hub for coordinating and managing cyber defense operations. It should operate as a wellspring of strategy, communication, and decisive action. It is necessary to define the fundamental purpose for the function's existence within the larger Defender's Advantage concept. When working through understanding how Mission Control fits into organization's larger strategy, consider the below statements as starting points:

"To protect an organization's information assets and mission-critical operations against the evolving cyber threat landscape."

"To provide consistent, continuous, and real-time situational awareness of an organization's cybersecurity posture."

"To promote and aid coordinated incident response activities."

As an organization looks to define the scope of Mission Control, it's imperative that the other critical functions of cyber defense are taken into consideration. Examples of how Mission Control connects to each of these areas, is given on the following page.

Figure 19. The role of Mission Control in the Defender's Advantage

Coordinate and guide intelligence gathering
- Partner with intelligence resources to establish key questions for collection
- Advise intelligence resources on what data is most impactful or of interest
- Hold intelligence resources accountable to ensure collected intel is timely, actionable, and relevant

Support detection and alert monitoring activities
- Own responsibility for enacting retainer, response plans
- Ensure consistent and clear communications throughout an incident
- Determine participant roles and responsibilities, while providing resources and authorization necessary

Support detection and alert monitoring activities
- Act as the central hub for technical teams and leadership on notable detected alerts
- Provide situational awareness

Conduct post-incident analysis, update defender strategies, and measure effectiveness
- Assess incident activities to determine strengths and opportunities for improvement
- Leverage opportunities and validation to help teams improve detection capabilities and refine incident response processes
- Track metrics to gauge overall effectiveness and identify further areas of improvement

Empower and support threat hunting activities
- Monitor and track progress of hunt team
- Monitor overall security posture of the organization
- Report and summarize finding to senior leadership and stakeholders

It's imperative that an organization outline their primary goals and corresponding objectives as it pertains to Mission Control. As previously mentioned, Mission Control is the central hub for providing direction, coordination, structure, and communications for effective cyber defense operations.

Table D: Mission Control goals and objectives

Goals	Objectives
1. Centralize mission control through accountability and empowerment	• Establish chain of command, accountability, decision-making • Define roles and responsibilities
2. Provide situational awareness	• Facilitate communication and collaboration • Centralize incident data, metrics, and reporting
3. Foster proactive defense and cohesive incident management	• Establish comprehensible plans, processes, and procedures • Outline escalation paths and response actions
4. Ensure resilient operations	• Conduct regular exercises and provide training opportunities • Prioritize investments, resources, and activities based on an organization's risk profile and critical assets

Overcoming challenges

An organization's cybersecurity program will likely face a variety of technical, organizational, and resource challenges. While these challenges may appear daunting, or at times insurmountable, they can be mitigated through a human-centered approach:

Figure 20: Human-centered approach to Mission Control

Prioritize: Threats to an organization are likely top of mind so critical risks and vulnerabilities be addressed first.

People: A comprehensive resourcing strategy should be developed to ensure that an organization has the right amount of talent at the right time. This includes:

- Skills development. Continuous investment in developing and honing the skills of current employees through training, mentorship, and professional development opportunities.
- Talent acquisition. Proactive planning for future talent needs by identifying critical roles and the skill sets required for each.
- Staffing pipeline. Building a robust pipeline of talent through internal development and external recruitment initiatives and partnerships.
- Outsourcing strategy. Assessing opportunities where staff augmentation is possible or necessary, either due to growth or requiring specialized skill sets, by partnering with external staffing firms.

Partner: In addition to partnering with external parties, care should be taken to ensure that collaboration is occurring internally between IT, Cyber Risk, and other teams. One way to overcome this hurdle is by ensuring Mission Control is facilitating communication between the teams and clarifying roles and responsibilities.

Practice: Successful execution across an organization's cyber defense program will only be as strong as the people, processes, and technology that are in place. By conducting cybersecurity tabletop exercises on a regular cadence, and ensuring that results and controls are validated, an organization can identify areas that should be addressed immediately or that require improvement.

By placing people at the center, prioritizing effectively, fostering collaboration, and committing to continuous learning, an organization will be able to navigate challenges (either during or prior to a cybersecurity incident) with resilience, adaptability, and a sense of shared purpose.

Fostering alignment and resiliency

Promoting empowerment and accountability

The ability to successfully execute Mission Control, within an organization, relies not only on the technologies and processes but also on an organizational culture. As part of this organizational culture, two main pillars are responsible for supporting an effective implementation of the Defender's Advantage: empowerment and accountability. It is imperative that an organizational culture support the promotion of both to fully realize success.

Facilitate agility and expertise

Mission Control is chartered with, and responsible for, creating and fostering an environment where cybersecurity teams are empowered to make decisions in a timely manner. The ability to operate in a flexible and agile fashion is a critical success factor in the Defender's Advantage. Care should be taken to avoid a centralized decision-making structure as it can create unnecessary bottlenecks for cybersecurity and supporting teams. Such bottlenecks may include:

- Limited resources
- Inadequate planning
- Mismatched/unbalanced workloads
- Unclear priorities
- Technology and process issues/inefficiencies
- Resistance to change

Empowerment should promote trust in an organization's frontline personnel. These frontline personnel are the individuals and teams responsible for, and supporting, cyber events and incidents. This frontline experience gives them a unique perspective and insight that is invaluable throughout an incident. This is why leaders must trust their judgment and expertise.

Additionally, empowerment applies to the continuous learning mindset discussed previously. The cyber threat landscape is ever-changing and personnel should be encouraged to pursue continuous learning through training programs, industry conferences, and professional-development opportunities. Empowering a team to make decisions and act may make little difference if the frontline personnel aren't adequately equipped with the knowledge to do so.

Drive responsibility and transparency

Expectations for frontline personnel cannot reasonably be set without defining accountability. Accountability can be more easily adhered to when personnel are told directly what is on the line for the team and then utilizing that to motivate personnel to achieve their mission goals. This is an effective approach to reducing faults and inaccuracies and improving performance and productivity when it is most needed. There are three effective methods in tracking accountability:

Clearly defined roles and responsibilities: When a cyber event happens, every single individual should have a clearly defined role, assigned responsibilities, and clear expectations. This will assist in alleviating overlap in work being performed and ensures that each individual understands their role as part of the larger team.

Utilize constructive feedback mechanisms: Constructive feedback is a method to help teams learn from successes and to also identify areas of improvement. A simple way to provide constructive feedback is by celebrating the successes (wins) and having debriefs (or post-mortems) on areas where improvements can be made without assigning blame. This helps promote continuous improvement and a strong learning culture.

Transparency in metrics and reporting: Lastly, it is necessary to establish a method for tracking how actions taken during a cyber event directly impact the success and overall cybersecurity posture of an organization. Having well-defined performance metrics (such as KPIs) and transparent reporting of these metrics promotes accountability and provides a means for course-correction, where necessary, early on.

Resource management and staffing

Organizations that have a comprehensive, widely deployed security stack, operate at increased risk if they don't have sufficient personnel with adequate training and authority to leverage it. Managing resources and staff is just as critical to an organization's healthy security posture as acquiring and deploying the security tooling itself.

Establishing Expertise Requirements: When staffing a security team, a key step in analyzing expertise requirements is to document a security staffing plan that identifies both current personnel status and desired future growth across each of the Cyber Defense roles. This can take the form of, or be augmented with, a matrix that aligns with an organization's strategic plan and is monitored and continuously updated to account for changes in technology and personnel.

Following creation of the staffing plan, organizations should populate a skills matrix that incorporates soft and hard skills as well as relevant certifications associated with roles such as the following:

- Incident Detection and Response
- Vulnerability Management
- Security Architecture
- Security Risk Management
- Detection Engineering
- Threat Intelligence
- Validation Activities (i.e., Red Team, penetration testing, etc.)
- Threat Hunting
- Coordinator (i.e., Project Management, Lead, etc.)

A gap analysis of the resulting skills matrix enables leadership in the Mission Control function to identify training opportunities for current staff and serves as an input to future hiring requirements. Before filling staffing gaps, formulate job descriptions that identify the required education, training, and experience necessary to perform each needed role.

Investing in people: When possible, organizations should consider allocating funds to a dedicated cyber defense budget for hiring staff and training existing and future personnel. Formal training requirements should be documented and tailored to each role by function, security technology, and desired skill sets. These requirements should map to the skills matrix which in turn maps to the staffing plan. In addition to formal training, organizations should also look to implement informal training options that can be utilized throughout the year, such as cyber ranges, capture-the-flag challenges, or weekly "teach back" training sessions among cybersecurity team members. When developing training, consider a variety of training formats, such as in-person, web-based, conferences, and vendor-supplied training. Update the skills matrix to track completion of required or optional training and certifications.

Career progression opportunities are an integral part of retaining highly skilled staff. Leadership should disseminate clearly defined career paths and promotion criteria to personnel within Cyber Defense. Routine check-ins can be leveraged to ascertain each resource's current status, desired future position, knowledge and skill gaps critical for success, and a tailored training and development plan to fill those gaps.

Ensuring knowledge transfer: Turnover is a challenging reality of any organization's Cyber Defense team. Preparation is critical to reducing the impact of lost institutional knowledge due to staffing changes or unforeseen circumstances. A key concept within Mission Control is to enable both initial competency and redundancy amongst all roles by establishing the following processes:

- **Onboarding.** Implement a repeatable, streamlined on-boarding process for new staff to gain the accounts, privileges, and accesses required to accomplish duties outlined within their respective roles
- **Mentoring program.** Develop, implement, and administer a mentoring program to train new or junior resources on established processes applicable to each role and function

- **Cross-training.** Cross-training programs not only reduce single points of failure within roles, but also encourage interdepartmental knowledge sharing across the Cyber Defense functions

Strengthening organizational security posture

Developing and maintaining processes and procedures

Planning is the key to success. Whether it's sports, business, or cyber defense, preparation is fundamental to reach the desired goals. Mission Control guides cyber defense efforts through proper planning in the form of properly defined processes and procedures.

Processes and procedures can vary in format, length, and level of detail while maintaining effectiveness for a given organization. No matter what documented processes and procedures look like, in order to be effective they all share some key characteristics that make them:

- **Comprehensive:** Processes should cover the full spectrum of potential incidents while providing an ability to identify critical assets, vulnerabilities, threat actors, and attack vectors.
- **Risk-based:** Actions and responses should be prioritized based on the potential impact of different incident types and focused on the protection of the most critical assets and addressing only the most likely threats.
- **Tailored and integrated:** Documentation structure, format, language, and level of detail change depending on the Cyber Defense organization's risk appetite, daily practices, and culture. Once documentation has been tailored for an organizational audience, it should be able to be integrated with other security processes and procedures, such as vulnerability management, threat intelligence, and business continuity planning.

- **Tested and rehearsed:** Processes and procedures should be regularly reviewed and tested to ensure documented plans are validated and individuals are familiar and comfortable with their roles. Examples may include tabletop exercises, red/blue/purple team exercises, and crisis management exercises.
- **Clear and actionable:** Processes and procedures should be easy to interpret and follow under pressure. Additionally, they should outline clear roles and responsibilities for each individual in the process.
- **Adaptable:** Effective processes and procedures recognize the threat landscape is constantly evolving and include the appropriate mechanisms for maintenance based on new threats, vulnerabilities, and technologies. Maintenance of documentation should follow an agile approach to foster bottom-up contribution from all involved stakeholders.

From a hierarchical perspective, processes and procedures can be grouped into three categories:

- Incident Response Plan
- Incident Response Playbooks
- Standard Operating Procedures

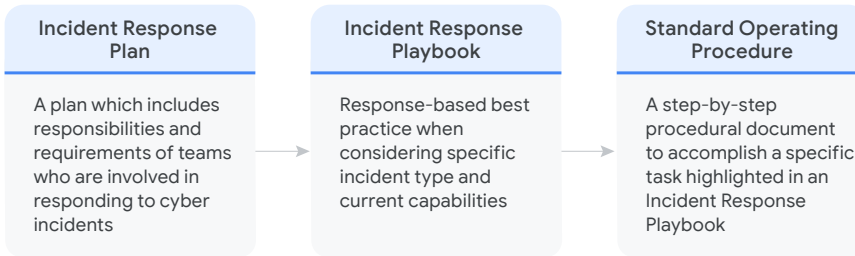


Figure 21: Hierarchical model of Mission Control supporting processes and procedures

The **Incident Response Plan** (IRP) represents the foundational document guiding Cyber Defense operations. This document formalizes an organization's incident response process, assigns roles and responsibilities, establishes an incident response communications plan, and details how incidents should be escalated and notified to relevant stakeholders. Through the IRP an organization creates a standardized, tested, and repeatable process to respond to cybersecurity incidents in a more effective and efficient manner.

At a high level, the IRP should include the following four sections:

- **Mission statement** defines the scope of the IRP.
- **Terms of reference** establish a common language for all involved stakeholders. Examples include Terms and Definitions, as well as the description of Alert Priorities, Incident Categories, Incident Severity levels, and referenced threat taxonomy (e.g., MITRE ATT&CK).
- **Incident response lifecycle** details the phases of the incident response process. Commonly accepted security incident response reference frameworks exist (e.g., NIST SP800-61r2[1], ISO/IEC 27035-1:20230[2]). However, an organization should adopt a model that is properly tailored and customized to their needs, as mentioned earlier in this section.
- **Roles and responsibilities** describes the individual roles and associated responsibilities required within the IRP.
- **Escalation matrix** documents who shall be notified and when they will be notified of an incident, based on incident category and severity.
- **Metrics and service level objectives** detail incident response metrics and service level objectives that the Cyber Defense organization has set. Basic incident response metrics include "time to detect" and "time to respond" to an incident.

1. *https://www.iso.org/standard/27001*
2. *https://www.nist.gov/privacy-framework/nist-sp-800-61*

- **Communications** outlines guidance for effective incident response communications, differentiating between primary and emergency channels. Primary channels encompass standard methods used in daily Cyber Defense operations. Emergency channels, utilizing out-of-band processes and tools, are activated only when primary channels are unavailable or potentially compromised. This approach ensures efficient communication while minimizing unnecessary escalation or disruptions to stakeholders like the CISO.

Incident Response Playbooks are documents that outline the planned actions a Cyber Defense organization takes to effectively respond to specific security incidents or threats. Playbooks ensure that the team follows a standardized response process aligned to their specific mission and capabilities.

Playbooks can take various formats and may include detailed instructions, checklists, process workflows, and references to external tools or documents. They are designed to support manual and automated task execution. In the latter case, Cyber Defense organizations can integrate playbook instructions into their security orchestration workflows, streamlining processes such as:

- **Case Management Data Collation:** Improves incident triage by gathering relevant information
- **Data Enrichment:** Enhances analysis through collection from multiple sources
- **Response Action Automation:** Executes response steps for faster and more efficient mitigation

Standard operating procedures (SOPs) are detailed blueprints that provide step-by-step instructions for completing specific tasks or operations. In contrast to Playbooks, which offer high-level guidance and decision-making pathways, SOPs focus on precise and repeatable instructions ensuring consistent execution.

SOPs are inherently more rigid than Playbooks, prescribing a specific sequence of actions designed to be followed with minimal variation. They offer detailed guidance, leaving little room for deviation or individual judgment. This makes SOPs suitable to guide incident responders when using specialized tools or services where strict adherence to protocols is essential.

The Cyber Defense organization must regularly schedule and conduct IRP drills to guarantee the plan's effectiveness and keep incident responders' skills honed. Testing drills can take diverse forms as described in the Validate function. Regularly testing the IRP helps an organization in:

- Breaking silos among different parts of the team involved in incident response
- Improving communications and reducing time-to-response for high-impact incidents
- Identifying inconsistencies and reducing confusion created by non-standardized processes
- Reducing duplicate or conflicting efforts during a breach and during ongoing operations

Incorporating metrics and trending

Metrics offer essential insights into the current state of people, processes, and technology in the cyber defense organization. They employ consistent, trackable, and automatable methods to provide these objective measures over time.

Metrics are critical at various organizational levels:

- **Operational Level (e.g., Cyber Defense Center, SOC, CERT):** Metrics focus on measuring threat detection and response capabilities
- **Program Level (e.g., CISO function):** Metrics offer a broader view, encompassing all aspects of the security organization

This section concentrates on operational-level metrics.

A well-functioning metrics program provides different benefits to the Cyber Defense organization. Some of these benefits are listed below:

- **Clear Communication:** Establish a system to report the status of people, processes, and technology to Cyber Defense leadership and key stakeholders.
- **Vulnerability identification:** Pinpoint weaknesses in security posture, facilitating alignment with an organization's risk tolerance.
- **Impact quantification:** Measure the effectiveness of implemented initiatives or controls over time (backward-looking).
- **Optimized Resource Allocation:** Provide data-driven insights for future resource decisions (forward-looking).

A robust metrics framework for Cyber Defense operations can be built upon these four pillars:

- **Implementation metrics:** These widely-tracked metrics measure the deployment of security controls against an established baseline (e.g., installed EDR agents vs. total number of endpoints). They leverage data sourced from centralized security control solutions like Identity and Access Management, vulnerability scanners, anti-malware systems, and firewalls. Implementation metrics demonstrate progress towards:
  - Alignment with security frameworks (e.g., ISO27K, NIST CSF)
  - Completion of security initiative, controls deployment, and policy implementation

- **Impact metrics:** These metrics gauge the ongoing business impact of cyber threats despite security controls. Primarily based on incident response data, they provide a historical view of threats impacting an organization. Frameworks like VERIS[3] and MITRE ATT&CK enhance data collection and analysis for impact metrics.
- **Effectiveness metrics:** These metrics determine how well existing security controls protect against or detect specific threats. When combined with the coverage data from Implementation metrics, they offer a comprehensive picture of how effectively controls minimize organizational risk.
- **Efficiency Metrics:** These metrics focus on the operational health of the cyber defense team by tracking recurring actions and tasks. They highlight effects of changes that might affect Cyber Defense, such as:
  - Team headcount changes
  - New detection rules implementation
  - Changes in infrastructure (e.g., installing a new security control or modifying architecture or configurations)

Commanding the crisis: Leadership in major incident management

Incident and crisis communications

Modern threat actors know they are more likely to accomplish their objective if they can use the public domain to increase risk to their victim organizations. This is why so many attacks include highly publicized actions like dark web data leak and direct media engagement by threat actors.

When an organization is targeted by a threat actor, in addition to the critical technical issues, there are acute communications challenges that the traditional approach to crisis communications approaches fail to address.

3. *https://verisframework.org/*

Attackers, at least initially, are a step ahead of the victim organization. It is a reactive environment that requires deft incident response which is enhanced by an agile, tailored communications approach.

Victim organizations who do not strive to 'own the issue', or communicate clearly and decisively (by design), risk impacting their long term brand reputation by turning the focus from an organization being the victim of an attack to failing to adequately respond during and after the event. It adds additional complicating facets, often requiring valuable time and effort from senior executives. Information ownership and control, once lost, is nearly impossible to regain damaging organizational brand—impacting (and adding further complexity) business recovery and wellbeing.

> *Now more than ever, breach notification obligations often force decisions to be made in hours or even minutes. Because these decisions are often made on incomplete intelligence and even less certain law, having counsel familiar with the business, available on speed dial is critical to effective response.*
>
> **Gerry Stegmaier**
> Law Partner, Reed Smith LLP

The pace, risk and duration of a cyber attack varies, from the immediacy of the attack to longer term remediation and recovery stages, all impacting organizational capability including communications.

An organization's crisis communication capability should be robust and regularly exercised to test and build strategic readiness. Exercising and the development of communication playbooks incorporating contingency and risk planning directly helps to equip communications teams to activate quickly in the early stages of a cyber incident, and position them to contribute across all subsequent phases of a cyber incident investigation, resolution and post incident analysis.

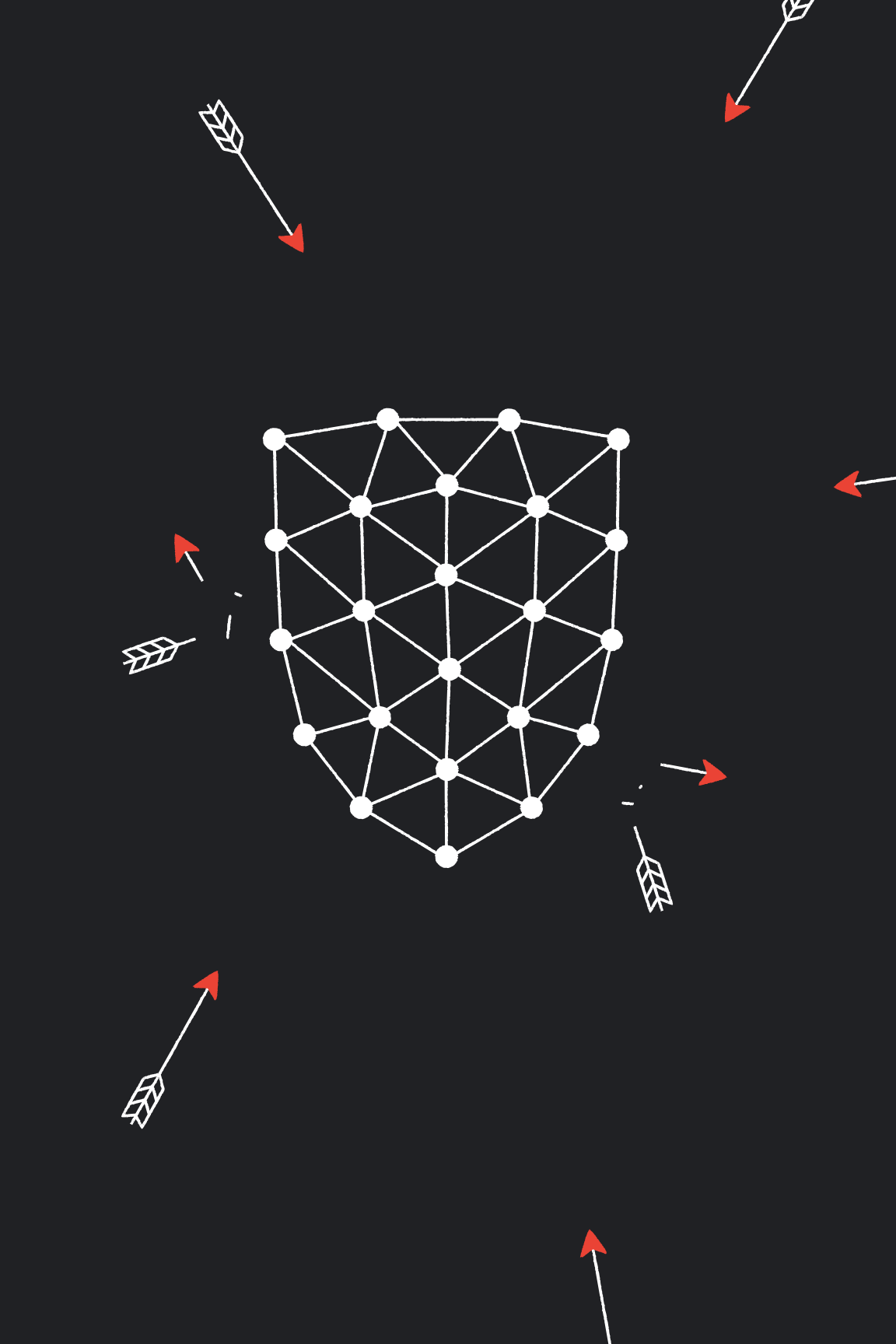
Communications teams are pivotal in coordinating between the business and technical response. This coordination enables communicators to activate crisis planning and initiate work including: identifying and prioritizing key audiences (for example; internal, clients, shareholders, government authorities, and the media), defining communication objectives, identifying key audiences (and stakeholders) and relevant communication channels, developing key messaging and commu-nication channels, and, keeping pace with the investigation.

Every cyber incident presents unique challenges, but key principles guide effective communication management during an incident:

- **Own the story:** Demonstrate authentic leadership, integrate messaging, and ensure consistency across communication channels.
- **Be the single point of truth:** Centralize organizational multimedia, information channels, and media engagement.
- **Integrate communications planning:** Adapt and adjust communications tactics and actions as the cyberattack evolves.
- **Commit to clear and transparent communication:** Timely, tailored to audiences, and sustained throughout.
  - Factual: Grounded in accurate information
  - Action based: Providing guidance and next steps
- **Know an organization's stakeholders:** Respect and meet their expectations, keeping them informed.
- **Good governance:** Maintain records of actions and key decisions as a foundation for continuous learning, refinement, and potential external review.

Clarity of purpose and scope is crucial for Mission Control to coordinate effectively with the other five Defender's Advantage functions. Coordination among all Cyber Defense functions is essential for effective security incident response. Mission Control's role is crucial in providing guidance and support to the other Cyber Defense functions throughout the entire incident response lifecycle.

Before incident response is activated, Mission Control can identify staffing and resource needs for proactive threat identification (Hunt), and align detection engineering requirements with business and risk priorities (Detect). During active response to security incidents, Mission Control can provide decision support and effort prioritization guidance (Respond). After an incident is resolved, Mission Control can support post-mortem analysis and drive improvement initiatives (Validate). Finally, and throughout the whole incident response lifecycle, Mission Control can support identification of intelligence requirements and ensure alignment between Intelligence and other Cyber Defense functions (Intel).



Activating Cyber Defense

Many organizations struggle to maintain the necessary depth of expertise across all functional areas required to leverage their Defender's Advantage. Instead, they rely on a balance of in-house resources, SaaS products, microservices, and expertise from strategic partners. This allows an organization to blend services from the most capable, cost effective, trusted sources to deliver the robust cyber defense services necessary to maximize their Defender's Advantage.

Stakeholder buy-in

A successful Cyber Defense program is one that partners with other business leaders to establish a metered risk mitigation strategy against other risks facing an organization. Cyber attacks, while serious and often with significant business impacts, are only one of the risks facing today's organizations. In order to prioritize an organization's limited resources, it is critical that leaders of the Cyber Defense program can articulate the business risks and impact of cyber attacks against an organization. This translation from highly technical cyber threats into business terms that can be consumed by executive leaders and the Board of Directors is absolutely critical for building stakeholder buy-in.

> *Cyber Defense organizations must communicate not only cyber risk but the risks from a revenue and strategy perspective. In an era of digital transformation, the CISO's role is focused on protecting the strategy.*
>
> **Dawn Marie-Hutchinson**
> Chief Information Security Officer

Staffing considerations

According to the 2023 ISC2 Workforce Study, the cybersecurity staffing gap grew 12.6% in 2023 to nearly four million positions. Automation of defenses, including advances through the implementation of AI solutions, can be put in place to relieve some of the workload and reduce burnout that comes from sifting through mountains of data for many hours, day after day. By 2025, lack of talent or human failure will be responsible for over half of significant cybersecurity incidents.[4]

Security training for staff is one of the best investments an organization can make. Training increases employee satisfaction and retention rates, and matures their skill sets so they can provide a higher level of expertise back to the company. Training programs with development paths or certification programs offer better return on investment over piecemeal courses.

Organizations can also invest in AI and automation to help repurpose traditionally lower tier staff roles by refocusing those resources away from lower value tasks. By implementing technology that can automate lower value tasks and aggregate massive volumes of data quickly, analysts can stay focused on more critical work while also producing results at a faster pace. As the Cyber Defense program and its use of automation matures, there are also opportunities to leverage automation for higher fidelity alerts, leaving the more difficult analysis to the most skilled at separating the signal from the noise.

4. *Gartner Predicts 2023*

Leveraging accelerators

Business priorities continue to change, and as they do, so too does the focus provided by an organization's cybersecurity team to critical Cyber Defense tasks. This can distract from the essential mission of Cyber Defense teams and detract from the Defender's Advantage that the team should focus on maximizing.

One approach to address this is applying "accelerators" or microservices to help bypass many of the traditional hurdles by relying on external resources to address Cyber Defense components that an organization does not have the cycles to address, or gets too distracted to address, on their own. By utilizing partner resources to analyze and provide objective solutions for identified issues, organizations get an unbiased, expert perspective on improvement needs and access to specialized deeply-knowledged skills to fix the issues without having to hire new resources or maintain less-frequently called upon and expensive skill sets. In-house personnel can learn from, and develop their skill sets through their interaction with these seasoned cybersecurity experts.

> *Intelligence allows us to show management that the money spent protecting our business, our image, our reputation, and the personal information of our customers is absolutely worth it. It has clearly shown us that we are a target, that we are being attacked daily, that we could never manage all of our cyber defenses in-house.*
>
> **Gary Winder**
> IT Network Engineer, Baptcare

Engaging Managed Services

Another approach for accelerating Cyber Defense capabilities with a limited budget is to engage with a managed service provider. Managed services allow an organization to outsource a portion of Cyber Defense functions such as detection and response, hunting, or validation. The services provide confidence in 24x7 protection while benefiting from the provider's intelligence and deep expertise gleaned from other customers and attacker visibility. This approach allows an organization to derive a portion of their Defender's Advantage from the expertise and capabilities provided by their trusted provider.

Managed services offer the additional benefit of intelligence gained from broad exposure to attacks. This exposure allows analysts within the managed service to gain experience responding to a wide range of incidents and activities. A managed service can observe campaigns as they unfold across their client-base and adjust response actions accordingly. This frontline experience is highly beneficial as it allows the managed service provider's analysts to leverage the knowledge they have developed defending other organizations to protect others before they ever experiences a similar attack.

As the leader of a small team, it is impossible to keep up with the current volume of alerts. Partnering with a service provider to monitor threats is the only way to have confidence in our ability to detect compromise.

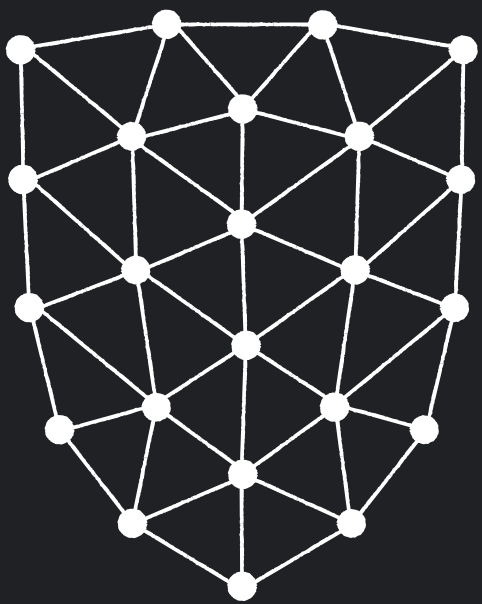
Andi Hill
Product Owner-Cybersecurity, Movement Mortgage

Example

The Mandiant Managed Defense organization received information about a zero-day vulnerability in a widely used product that was being exploited to deploy ransomware. Managed Defense initiated a threat hunting campaign to identify evidence of attacker activity across the entire customer base. Additional intelligence, fed by Mandiant's frontline incident responders, led the MDR services team to begin scoping customer environments for hosts running the vulnerable software. Affected customers were quickly identified and advised to contain certain on-premises systems. Protections were put in place before the ransomware could be deployed. In this case, all customers of the Managed Defense and Mandiant intelligence services benefited from the adversary IOCs provided from intelligence gathered across the customer base.

Flexible consumption models

Organizations can augment existing teams, outsource services with managed services, or utilize microservices to maximize their Defender's Advantage. These services are typically purchased as six-, 12-month, or multi-year subscriptions. Many services providers also provide flexible spending options that allow organizations to make a single purchase of credits to be used over the subscription period. This flexible option is a good choice when organizations know they will have to respond to changing threat actor activities but are unsure about the specific responses that will be required. This is also a common option leveraged for expanding knowledge held by internal teams and for on-demand access to deeply knowledgeable cybersecurity experts.



Conclusion

The threat actors attacking organizations in the cyber theater today are relentless and will stop at nothing to get access to an organization's most critical assets. They are greater in numbers, have more resources, and are not bound by the same governmental and regulatory restrictions that limit an organization's Cyber Defense program. By all accounts, they should have the advantage. Afterall, a threat actor only needs to be successful once; a Cyber Defense program needs to be successful 100% of the time.

This is an incorrect and dangerous supposition. Organizations that actively maximize their Defender's Advantage have the edge.

These organizations leverage cyber threat **Intelligence**, gained through internal and partner resources, to focus their Cyber Defense program on the most critical threat actor activities and their most likely targets. They feed this essential intelligence data throughout their Cyber Defence program to keep their Defenders one step ahead of the threat actors as they attack them.

They **Hunt** for any evidence of adversary activity in their environment and feed the results, both from identified threat actor activity and from any of their actions that emulated threat actor activity, back to the other functions of the Cyber Defense program.

They maintain a robust **Detection** program to identify threat actor activities early in the attack cycle.

They define their **Response** procedures and regularly exercise them to ensure operational excellence in cyber response capabilities.

They continuously manage their threat exposure through the **Validation** of their technical and procedural controls, measuring and up-leveling the capabilities of their personnel, and managing vulnerabilities in their environment.

Finally, they maintain the constant **Mission Control** overwatch, management, preparedness, and connectivity throughout the Cyber Defense and other adjacent business functions that allows them to deeply understand their current Cyber Defense posture and readiness to respond throughout the ongoing battle that every organization faces against the threat actors that attack them.

In today's threat landscape, trying to gain an advantage in cybersecurity is not an easy task. An organization's Cyber Defenders face constant attack from sophisticated threat actors and must perform at advanced levels to be successful. Nevertheless, Defenders have the Advantage. They have control over their terrain, they know their landscape, they can manipulate it, and they have the ability to determine where they will meet their adversary. With the proper preparation and vigilance, leveraging the in-house, SaaS, microservice, and partner capabilities available to them, they can achieve their Defender's Advantage.

Contributors

Alex Flores
Alexa Rzasa
Alishia Hui
Angelo Perniola
Brandon Gilbert
Caleb Hoch
Camile Felx Leduc
Chris Ingram
Christopher Satanek
Colby Gilbert
Dan Nutting
Dan Wire
Doug Foss
Emily Cranston
Glen Chason
Jason Brown
John DeLozier
Kerry Matre
Lisa Dobson
Matt Acunto
Muhammad Muneer
Nate Toll
Neal Gay
Nick Bartosch
Omar Toor
Pablo Nova
Paul Kolars
Paul Shaver
Ryan Taylor
Tim Tuller
Todd Keith
Travis Fry
Trisha Alexander
Ya'aqov "Jim" Meyer

The Defender's Advantage: A guide to activating cyber defense

Second Edition. © September 2024

We are facing off against adversaries in our own environments. This provides an advantage arising from the fact that we have control of the landscape that is under attack. Organizations struggle to capitalize on this advantage. As security organizations, we must activate our cyber defenses, advancing capabilities from a prepared state to active duty. This activation is guided by Intelligence and orchestrated through the other critical functions of Cyber Defense: Detect, Respond, Validate, Hunt, and Mission Control. It is through this activation that we can take control and galvanize our defender's advantage.

The Defender's Advantage: A guide to activating cyber defense

Second Edition.

About Mandiant. Mandiant is a recognized leader in dynamic cyber defense, threat intelligence, and incident response services. By scaling decades of frontline experience, Mandiant helps organizations to be confident in their readiness to defend against and respond to cyber threats. Mandiant is part of Google Cloud.

cloud.google.com/security/mandiant