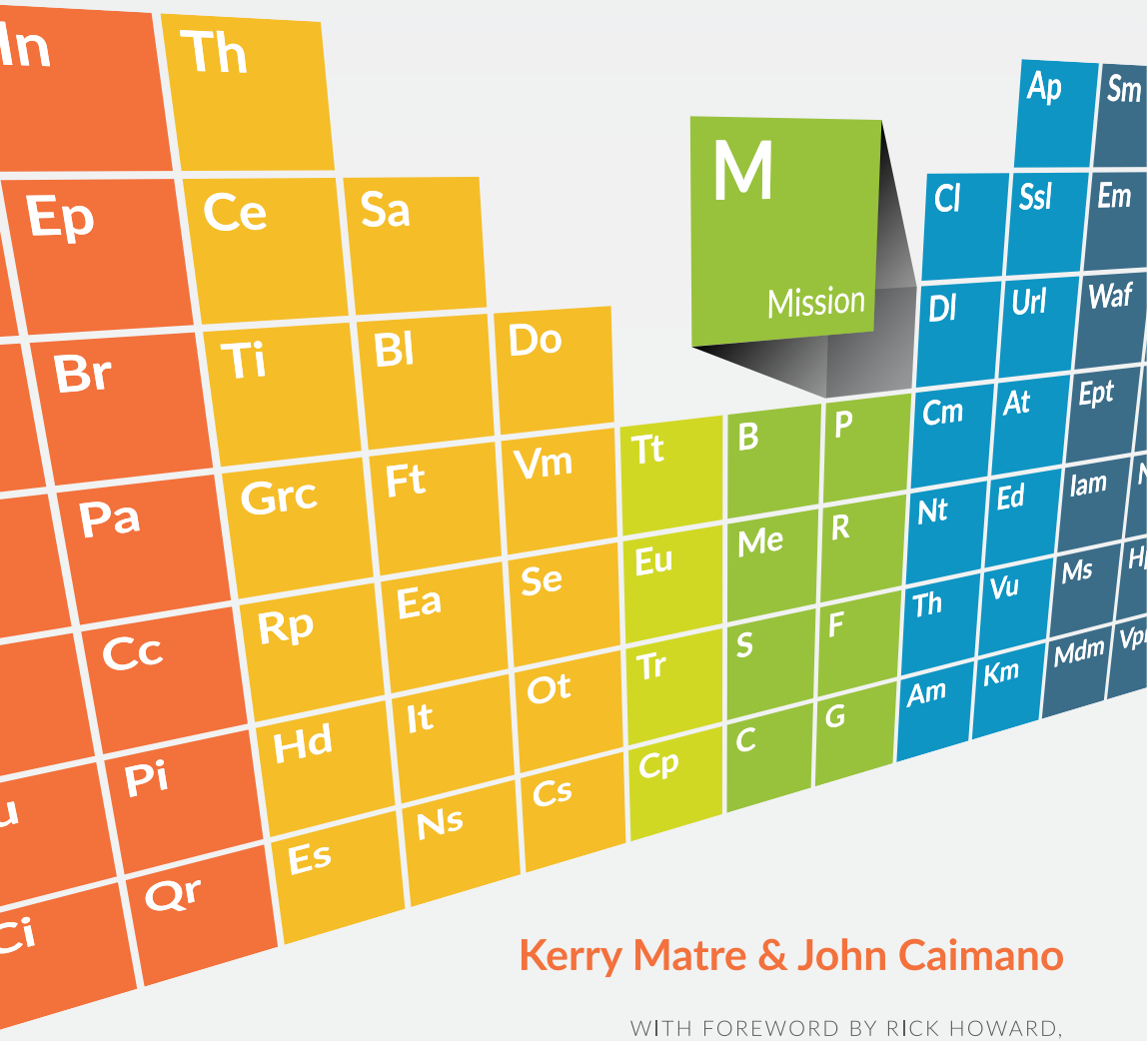
paloalto NETWORKS

ELEMENTS OF

SECURITY OPERATIONS



Kerry Matre & John Caimano

WITH FOREWORD BY RICK HOWARD,
CHIEF SECURITY OFFICER, PALO ALTO NETWORKS

ELEMENTS OF SECURITY OPERATIONS

Kerry Matre & John Caimano

WITH FOREWORD BY RICK HOWARD,
CHIEF SECURITY OFFICER, PALO ALTO NETWORKS

Table of Contents

Foreword

Protect and enable the business. That is what every security leader is charged with. As Chief Security Officer at Palo Alto Networks, I have spoken with hundreds of organizations and each wants to improve their security operations to be able to better serve the business. The question I hear from them most often is, "How do we do better?"

The industry is challenged with a cybersecurity skills gap. We need more people with security expertise than are currently available. Analysts are bombarded with overwhelming amounts of data without the proper automation and processes to effectively use the information. Attackers are highly automated and constantly shifting their attacks, giving them the upper hand. On top of that, businesses are evolving rapidly. Many organizations have embarked on a digital transformation to move to the cloud. They are adopting rapid release cycles for applications. Some are executing large mergers and acquisitions (M&A) strategies and inheriting legacy networks and applications while still needing to move the business forward.

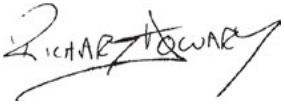
Yes, it can be a lot. So how do we improve security operations to address these challenges? Our approach at Palo Alto Networks is to take a step back. We look at the security operations function as a business enabler beyond responding to alerts. We start by uncovering the purpose of the security operations organization to achieve the goals of each business. From there, our team of security operations experts break out the elements of SecOps to clearly identify what pieces are needed—from people and processes to visibility and interfaces. With the elements laid out, organizations can assess their capabilities and create a plan for addressing gaps to drive greater effectiveness.

This view of security operations reveals opportunities for automation, integration, consolidation, and machine learning. Taking advantage of these opportunities provides numerous desired results for a business:

- **Simplification:** Reduce the number of tools, simplify operations.
- **Up-leveled capabilities:** Automate repetitive tasks, freeing up analysts to work on smart things, aided by machine learning to increase efficacy.
- **Consistency:** Consistent enforcement of security policy across the networks, cloud, and endpoints for better security.
- **Speed:** Rapid response to threats through access to the right information at the right time and flexible playbooks to drive investigations.

Whether you have a full 24x7 manned SOC or a part-time resource that reviews security logs, the elements described in this book apply to you. We need to shift our view from how analysts use the tools in the SOC for detection and response to a larger view of how the security organization serves the business, and how the business serves it.

Yes, we face many challenges in security operations and I, for one, am very excited and optimistic to see the new views of security operations being adopted. To answer the question, "How do we do better?" One element at a time.



Rick Howard
Chief Security Officer, Palo Alto Networks

Introduction

Security operations (SecOps) are a necessary function for protecting our digital way of life, for our businesses and our customers. They require continuous improvement in operations to face fast-evolving threats. They need to arm their security operations professionals with high-fidelity intelligence, contextual data, and automated prevention workflows to quickly identify and respond to these threats. They must leverage automation to reduce strain on their analysts and execute the Security Operation Center's (SOC) mission to identify, investigate and mitigate threats. All of this, though necessary, can be very overwhelming for organizations building out a SecOps function or modernizing an existing SOC.

Executives want the confidence that the SOC can quickly handle attacks when they happen—but are increasingly fearful of losing their job if the company is breached. Security operations managers want automation to stabilize SOC resources and provide consistency in operations—yet are continually frustrated with the headache of staffing-turnover and finding qualified professionals to fill roles given the industry skills gap. Security analysts want a simplified investigation process to determine if a threat is present, so they can allocate time to investigating threats—but they spend their days with the repetitive and menial tasks of weeding through false positives and low-fidelity data.

The problem is your SOC is inundated with low-fidelity data which overwhelms analysts and creates questions around your ability to keep up with the threats. Simplifying operations will help you outpace the attackers and gain confidence in your capabilities. However, it can be difficult to know where to start.

In order to increase confidence in the ability to quickly stop stealthy attacks and adapt your defenses to prevent future attacks, a SecOps function requires the right set of building blocks. These building blocks are defined in this book as the "Elements of Security Operations." They include the people, process, and technology aspects required to support the business, the visibility that is required to defend the business, and the interfaces needed with other organizations outside of the SOC. By utilizing these elements to build a SecOps function, it is possible to strengthen operations by increasing automation and speeding investigations.

Security Operations Definition

Security operations centers can go by many names including Cyber Defense Center or Security Intelligence Center. A security operations center, or SOC, is typically thought of as a physical room or area in an organization's office where cybersecurity analysts work to monitor enterprise systems.

Security operations can be defined more broadly as a function that identifies, investigates, and mitigates threats. If there is a person in an organization responsible for looking at security logs, then that fits the role of security operations. Continuous improvement is also a key activity of a security operations organization. Therefore, the four main functions of security operations are:

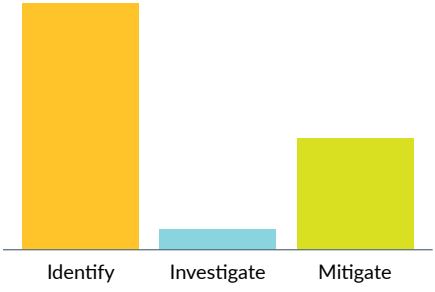
1. **Identify –** Identify an alert as potentially malicious and open an incident.
2. **Investigate –** Investigate the root cause and impact of the incident.
3. **Mitigate –** Stop the attack.
4. **Continuous Improvement –** Adjust and improve operations to keep up with changing and emerging threats.

The majority of a Security Operations Analyst's time is spent in the identify phase due to false positives and low-fidelity alerts that they must weed through. Correctly implemented prevention-based architectures and automated correlation help reduce the time needed for this phase. A lot of time is also spent in the mitigation phase. This is driven by the lack of automated remediation, and complex or lacking interfaces with teams outside of the security operations organization that need to be involved in halting the attack.

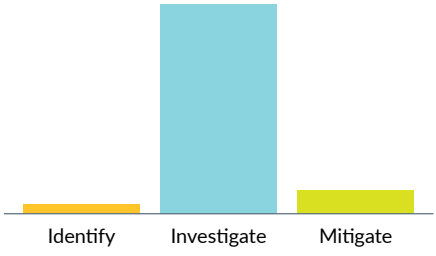
The top 3 wishes of a Security Operations Engineer:

1. **Reduce the number of alerts flowing into the SOC.**
2. **Access tools to quickly investigate threats.**
3. **Lessen the time it takes to contain a breach.**

—Vidya Gopalakrishnan, SOC Engineer, Palo Alto Networks



Traditional analyst time allocation



Ideal analyst time allocation

The purpose of security operations is to identify, investigate, and mitigate threats.

A prevention-based architecture cuts down on the noise in the SOC and is comprised of:

- Consistent protection across the network, cloud, and endpoints
- Centralized management of security controls and devices to provide consistency and reduced administration time
- Automated threat prevention for updates to security controls in minutes, not days
- Prevention based on Data, Assets, Applications, and Services (DAAS) to move controls closer to critical assets and to reduce policy and rule maintenance

The prevention-based architecture exists outside of the SecOps function itself but affects the efficiency and efficacy of achieving the SOC mission. Without a prevention-based architecture, analysts can be overwhelmed with false-positives and low-fidelity data. This can result in detuning sensors and ignoring alerts. Investigations can be rushed and feedback into controls is overlooked, which amplifies the problem.

A prevention-based architecture ensures that machines are used for what they are good at—events, and people can focus on what they are good at—situations.

If you change the inputs and outputs of a SOC, you can fundamentally change what happens within the SOC.

Security Operations Delivery Options

Organizations use various delivery options for the SecOps function. The choice in delivery of security operations is usually driven by key factors, including the needs of the business, global presence, access to resources, and funding.

An **in-house SOC** keeps the knowledge and control of the environment within the business, however, it can require a considerable investment upfront, dependent on the size of the operation. It is also dependent on being able to keep up with in-house staffing, which remains a major challenge for security organizations.

Outsourced security operations, or **SOC-as-a-Service,** provides access to experts, advanced technology, mature processes, and can be spun up quickly. However, it still requires in-house resources to carry out remediation tasks and can reduce the number of custom processes that can be put in place. It requires good service-level agreements (SLAs), and consistent monitoring and testing of the SLAs to ensure quality. This setup may also cause concerns around compliance at different global locations.

Many organizations choose a **hybrid solution** with some functions outsourced, such as level 1 analysts, to identify priority tasks. This solution provides access to additional skills that may not be present in-house and can provide both flexibility and scalability. It requires stringent interface agreements and tight processes around escalations and communication.

An emerging delivery option is to utilize **robotic decision automation** to fill the role of a level 1 analyst and then in-source or out-source the elevated tasks of a SOC. Often branded as artificial intelligence, these systems utilize advanced probabilistic mathematics that can be trained to reason like a SOC analyst and can identify high-fidelity events that warrant further investigation.

Regardless of the security operations delivery option, for the purposes of this book, the security operations function may also be referred to as SecOps function(s) and Security Operations Center may be referred to as SOC.

Elements of Security Operations

Security operations can be complex, however, by breaking them down into discrete elements, it is possible to assess which of the elements are covered in a SOC and to what extent. Then the element map can be used to evolve security operations to provide better prevention and remediation, faster.

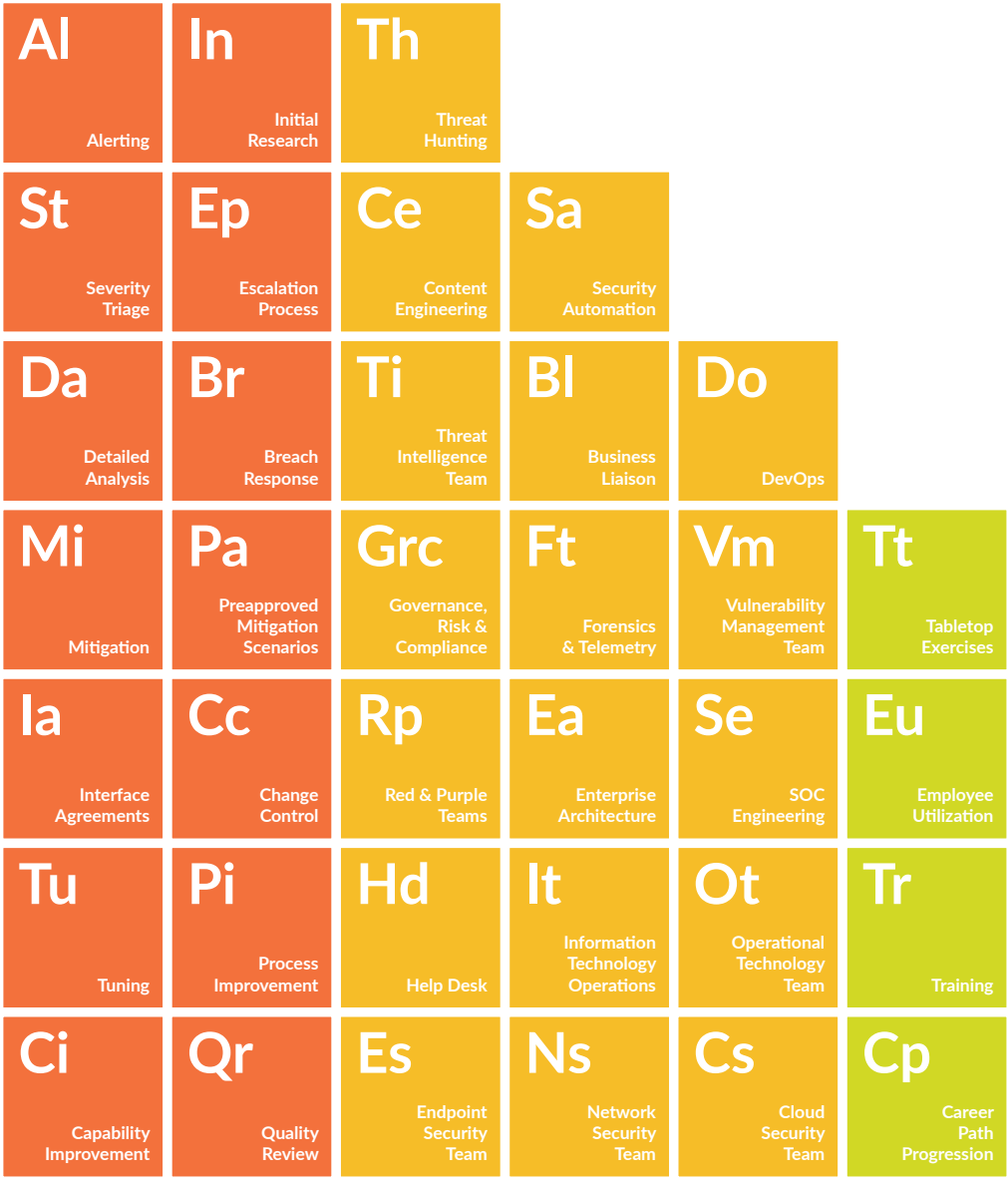
The elements of security operations are broken down into six pillars. These pillars range from capabilities the business requires from the SOC to the operationalization of those capabilities. The six pillars include:

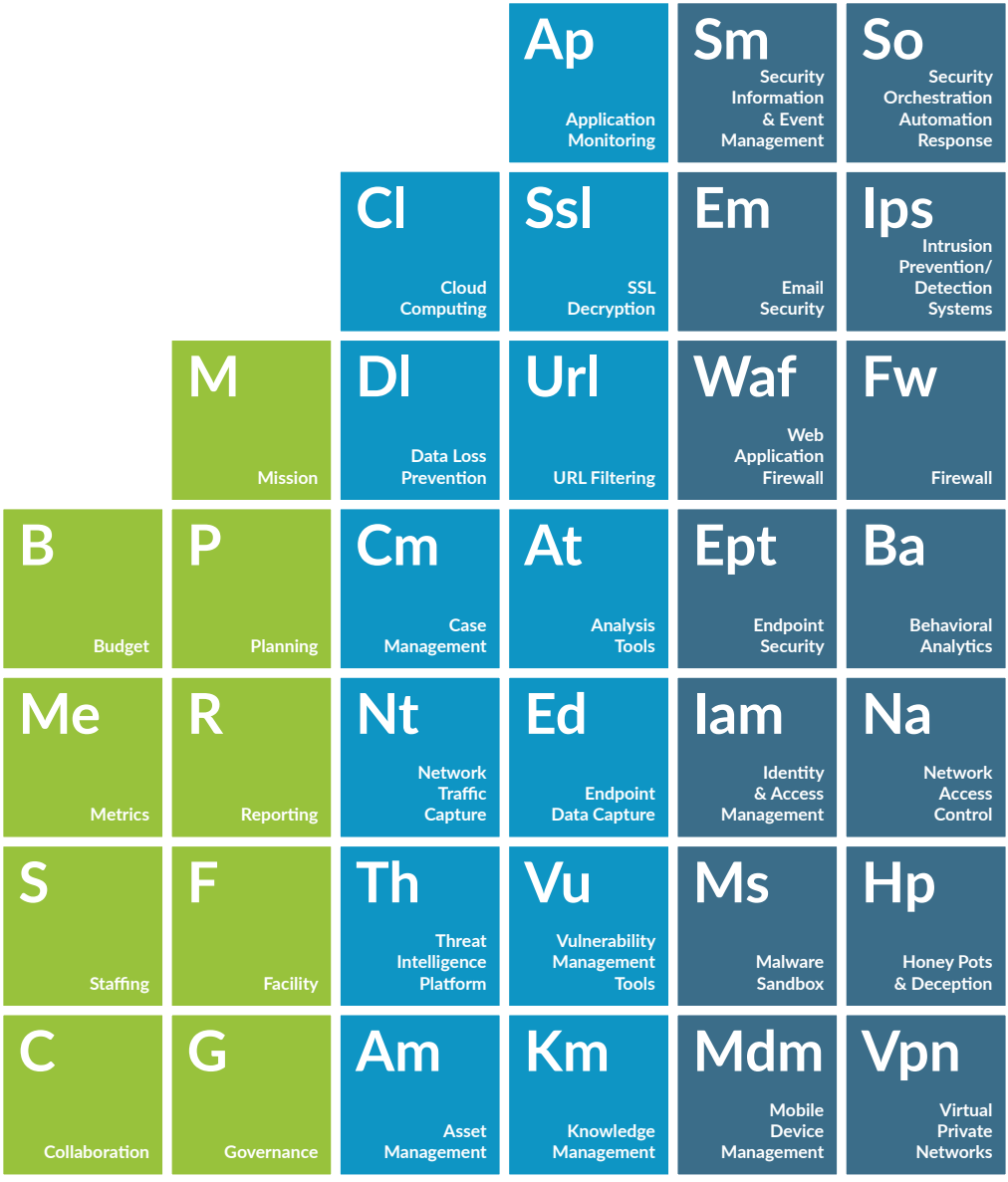
1. Business (goals and outcomes)
2. People (who will perform the work)
3. Interfaces (external functions to help achieve goals)
4. Visibility (information needed to accomplish goals)
5. Technology (capabilities needed to provide visibility and enable people)
6. Processes (tactical steps needed to execute on goals)

All of the elements tie back to the business itself and the goals of the security operations organization.

Elements of Security Operations

OPERATIONALIZATION




Ap
Application Monitoring
Sm
Security Information & Event Management
So
Security Orchestration Automation Response
Cl
Cloud Computing
Ssl
SSL Decryption
Em
Email Security
Ips
Intrusion Prevention/ Detection Systems
M
Mission
Dl
Data Loss Prevention
Url
URL Filtering
Waf
Web Application Firewall
Fw
Firewall
B
Budget
P
Planning
Cm
Case Management
At
Analysis Tools
Ept
Endpoint Security
Ba
Behavioral Analytics
Me
Metrics
R
Reporting
Nt
Network Traffic Capture
Ed
Endpoint Data Capture
Iam
Identity & Access Management
Na
Network Access Control
S
Staffing
F
Facility
Th
Threat Intelligence Platform
Vu
Vulnerability Management Tools
Ms
Malware Sandbox
Hp
Honey Pots & Deception
C
Collaboration
G
Governance
Am
Asset Management
Km
Knowledge Management
Mdm
Mobile Device Management
Vpn
Virtual Private Networks
BUSINESS
VISIBILITY
TECHNOLOGY

Business

The **Business** pillar in the Elements of Security Operations defines the purpose of the security operations team to the business and how it will be managed. Business questions that must be answered:

- Mission: What are we doing?
- Planning: How are we going to do it?
- Governance: How are we going to manage what we are doing?
- Staffing: Who do we need to do this?
- Facility: Where are we going to do this?
- Budget: What will it cost to do this?
- Metrics: How do we know it is working effectively?
- Reporting: How will we track activity and provide updates?
- Collaboration: How will we communicate and track issues with the rest of the business?

People

The **People** pillar in the Elements of Security Operations defines the humans that will be accomplishing the goals of the security operations team and how they will be managed. Questions that must be answered:

- How will we find staff and train them to fulfill their roles?
- What will we do to retain them?
- How will we manage the workloads of the staff?
- How will we validate the actions of the staff for efficacy?

Interfaces

The **Interfaces** pillar defines what functions need to be involved to achieve the stated goals. Security operations is not a silo and needs to work with many other functions of the business. Each of these interactions are what is described as "interfaces" that should be defined so expectations between groups are clearly stated. Each group will have different goals and motivations that, when understood, can help with team interactions. Identifying the scope of responsibility and separation of duties will also reduce friction within an organization. Questions that must be answered:

- What other functions of the business impact security operations?
- What other functions of the business does security operations impact?
- How will the security operations team work alongside these other functions?
- Who has ownership of responsibilities and are there SLAs that need to be documented?
- At what interval will these interfaces be reviewed and updated?

Visibility

The **Visibility** pillar defines what information the SecOps function needs access to. This includes security and systems data, as well as knowledge management content and communications through collaboration tools. Questions that must be answered:

- What primary security data is needed?
- What contextual data is needed?
- How often does this data need to be refreshed?
- What knowledge base information needs to be accessed?
- How will the security operations team see activity in the SOC?
- How will external teams see activity in the SOC?

Technology

The **Technology** pillar defines what is needed to achieve visibility into the information needed in the security operations organization. It is important to note that each element should not be thought of as a different tool but rather a capability that should be achieved with the given technology stack. Technologies and capabilities change rapidly, so these are the most fluid elements of a security operations team.

There is a glut of siloed tools in the industry that lead to a variety of issues, including extensive vendor management, limited feature use, duplicate functionality, and sometimes, end-user degradation. A shift is being seen to move away from best-of-breed siloed tools and towards platforms that provide capabilities needed in the SOC without the need for installation and maintenance of different tools. Questions that must be answered:

- What capabilities are required to achieve the necessary visibility?
- What technology will be used to provide these capabilities?
- Who will be responsible for the licensing, implementation, and maintenance of the technology?
- How will technology and content updates be requested and performed?
- What updates will be carried out automatically and at what interval?

Processes

The **Processes** pillar in the Elements of Security Operations defines the processes and procedures executed by the security operations organization to achieve the determined mission. Questions that must be answered:

- What processes need to be defined?
- Where will the processes and procedures be documented?
- How will this documentation be accessed and socialized?
- Who will have responsibilities for keeping this documentation updated?
- How often will the processes need to be reviewed and updated?

Once the questions for each pillar have been answered, you will have a strong outline ready to assist in the improvement of your SecOps functions. The following sections describe each objective of the elements of security operations in additional detail.

Business Objectives

Mission

Developing, documenting, and socializing the mission statement for your security operations is one of the most important elements of the organization. It will define to you, and to the business, the purpose of the SOC. This should include the objectives of the security operations organization and the goals the organization is expected to achieve for the business.

Socializing the mission statement and getting buy-in from executives provides clear expectations and scope of what the security operations team is responsible for. Some mission statements include defending an organization, protecting assets, or enabling the business. Some are customer-focused, as with service providers. Others provide for openness, as with university systems. Each is unique; however, they do have some common properties. The mission statement should define what actions will be taken, how those actions will be executed, and what the results are to the business.

Palo Alto Networks Security Operations Center Mission Statement:
Defend our information and technology resources, intellectual property and ability to operate by disrupting our adversary's ability to conduct their operations and achieve their desired outcomes.

Governance

Governance is how to measure performance against the defined and socialized mission statement. It defines the rules and processes put in place to ensure proper operation of the organization. It can include principles, mandates, standards, enforcement criteria, and SLAs. Additionally, it will define how the security operations team will be managed and who is responsible for ensuring the team is meeting the mission of the business. This should include actions that will be done to ensure the mission objectives are met.

Governance, at its best, enables teams to make decisions effectively and removes bureaucratic red tape. Conversely, poor governance stifles innovation, erodes trust, and forces too many decisions to be made by senior leadership distracting them from the strategic roadmap.

—Fred Thiele, Chief Information Security Officer, Transport for New South Wales

Planning

Planning includes details on how the security operations organization is going to achieve its goals. Main business drivers will need to be identified and documented. Other inclusions are vision, strategy, service scope, deliverables, responsibilities, accountability, operational hours, stakeholders and a statement of success.

Planning should be done with a 3-year vision, which ensures the continuation of operations—even in times of rotating executives that may have execution variances—to provide the expected value to the business. An investment strategy is also part of planning. This not only includes technology purchases but automation goals and investment in people. It should tightly align to the business. If there is a large M&A strategy or digital transformation to the cloud, for example, the investment plan should align to those initiatives.

Smaller security operations organizations face the same challenges as large SOCs, at a smaller scale with fewer resources. Focus on priorities and planning is key.

—Alex Wood, VP, Information Security/Chief Information Security Officer, Pulte Group, Inc.

Business Execution

Staffing

Roles of a security operations organization can include Tier 1 analysts, Tier 2 analysts, Tier 3 analysts, Threat Intelligence, and Hunting specialists, depending on the size of the organization.

Staffing of a security operations organization includes the recruitment, screening and selection process for analysts and other SOC staff. Staffing of security skills remains one of the biggest challenges of the security industry, with additional challenges existing for organizations located outside of major tech hubs. Organizations with these issues should look to in-sourcing resources (analyst-as-a-service) to alleviate the strain of staffing.

Outsourcing SOC functions are not all-or-nothing. Hybrid or co-sourced arrangements allow flexibility between the skills and resources that an organization has internally and the gaps that can be filled through managed services. The most important thing is to get the right people doing the right things for the business.

—Jesse Emerson, VP, Americas Managed Security Services, Trustwave

Considerations must be made for the staffing model chosen (24x7, 8x5, co-sourcing, etc.). On-call staffing requirements should be defined for critical incidents as well as out-of-hours support that is required. This will drive the number of FTE required to meet the objectives of the team.

When building a security operations team, the most important hire is the security operations manager. They are responsible for creating the "people" procedures, managing the SOC staff, and working with other teams within the organization. For analyst hires, a general rule of thumb is two Tier 1 analysts for every Tier 2 analyst.

Organizations should avoid filling their team with "heroes." These types are valuable to an organization because they can (and do) perform all tasks but in the event of their departure, they are difficult and expensive to backfill. This presents a risk to the business that should be avoided. Instead, you want to staff the appropriate level of knowledge for each role in the SOC. There should be diversification of skills within the security operations organization such as malware analysis, network architecture, and threat intelligence; however, there should be basic knowledge and skill that has overlap amongst team members for vacation backup, illness, and attrition. Attrition will happen, so a healthy hiring pipeline must exist. This pipeline can come from internal hires from other parts of the organization (help desk, IT operations), universities, or from rotating staff throughout the business.

Career Path Progression

Retaining staff is also important and providing a clear career path is necessary to achieve this. A role's definition and skills matrix should be created and a maintenance plan established in order to keep the skills matrix up to date. A semi-annual review of this content is suggested. Additionally, skills gaps/deficiencies should be continually updated by the SOC manager to allow visibility into possible capability holes to drive improvement.

Keep in mind that moving up to management is not the goal of all employees. The career path should allow for a management path, as well as a technical path. These paths should be documented with details of each job role and shared with the team, so they are aware of what is required at each level. Education opportunities should be available to help staff move through their preferred career path.

Sample technical career path

Sample management career path

Employee Utilization

Methods should be developed to maximize the efficiency of a security operations team specific to the existing staff. Security operations staff are prone to burnout due to console burn out and extreme workloads. To avoid this, team members should be assigned different tasks throughout the day. These tasks should be structured and may include:

- Shift turnover stand-up meeting (beginning of shift)
- Event triage
- Incident response
- Project work
- Training
- Reporting
- Shift turnover stand-up meeting (end of shift)

Another tactic to avoid burnout is to schedule shifts to avoid high-traffic commute times. Depending on the area, 8am-5pm may line up with peak (vehicle) traffic patterns. Shifting the schedule by two hours could reduce stress on the staff.

Building great teams may be the most crucial element of a security program. In most SOCs, it's perhaps inevitable that attrition will be a problem, as the job can burn analysts out while the skills they learn enable them to find more engaging work. Great organizations find ways to automate the transactional security activities, to free up their analysts to work on the thing things that excite them and matter more to the organization.

—Brett Wahlen, Chief Information Security Officer, Amazon Prime Video

Training

Proper training of staff will create consistency within an organization. Consistency drives effectiveness and reduced risk. Having a formal training program will also enable the organization to bring on new staff quickly. Some organizations resort to on-the-job or shadow training for new hires, which is not recommended on its own. While shadowing other analysts during initial employment in the SOC is important, it should not be the only means of training.

Formal documentation should exist around capabilities, tools, processes, and communication plans (both internal and external) that new and existing staff can reference. Enablement plans for new tools should also be contained in the formal training program. This continuous education requires time and investment and should be supported by the business.

Types of training content include:

- **Company security and privacy training**
- **Tool-feature use**
- **Process documentation and execution**
- **Communication plans**
- **Continuous education (incident response, threat analysis, etc.)**

One key hallmark of a profession (vice simply a trade) is the promotion of not only training but true scholarship in the area of study. Accompanying that comes research and theory that drives the profession to new heights and to greater applicability in the workplace. This is particularly critical in cybersecurity where practitioners have to be able to make informed decisions at a faster rate than their opponents.

—Dr. Jim Borders, PhD, Lieutenant Colonel, USAF (RET), VP Education, SecureSet Academy

Facility

The facilities needed for your security operations team will depend on how you will be delivering the service—physically or virtually. A physical SOC may need separation from other parts of the business, including the Network Operations Center (NOC). While these two groups need to tightly interface with each other, they may need separate spaces to adhere to need-to-know principles and avoid specific legal issues. Where fusion centers are established, additional training for the network operations staff is required to ensure adherence to privacy principles.

The facility should include basic locking capabilities and preferably, an advanced access schema that includes a 2-factor authentication. Hand geometry readers with a PIN code are an example of advanced access control. Line-of-sight protection should also be accounted for. A closed/windowless room or snap glass is a way to achieve that protection. Snap glass can also lead to better morale since it lets in some outside light and reduces the "dungeon" feel that SOCs are typically known for.

Virtual SOCs (VSOC) are composed of team members that do not hold a physical space. They utilize online, secure portals to monitor traffic. When using a VSOC, extra care must be taken to secure the **VPN** and endpoint devices accessing the security portal, and a private space must be available for phone calls and discussions within the security operations team.

A well-planned space for security operations builds confidence from the business and from customers. Giving tours of your SOC to those you provide services to allows them to gain a greater understanding of your capabilities and creates a forum to answer questions about the SOC's capabilities.

—Wikus Saaiman, Director, Information Security, CITEC

Security Operations Infrastructure

Most customers can tell me every tool they have in their SOC but cannot tell me how they use those tools to achieve better security. In fact, they have barely scratched the surface on what these tools can do and need to make the time to really understand them.

—John Telan, Global Solutions Architect, Palo Alto Networks

Security Information and Event Management

A Security Information and Event Management (SIEM), commercial or homegrown, is used as a central repository to ingest logs from all corporate-owned systems. SIEMs collect and process audit trails, activity logs, security alarms, telemetry, metadata, and other historical or observational data from a variety of different applications, systems, and networks in an enterprise. Most provide correlation capabilities as well.

For a SIEM to operate properly, connectors and interfaces are required to ensure translated flow from the system of interest to the SIEM data lake. The security operations organization should define how ownership of an event will be established, as well as the central point to where an analyst will go to receive alerts. Sometimes it is the SIEM, in other cases, it is a Security Orchestration, Automation and Response (SOAR) platform or ticketing system.

The selected SIEM approach should address any governance, risk, and compliance requirements for the separation of data, privacy, and retention times. This will drive requirements on storage space and controls. Limiting data redundancy between the SIEM and feeder systems can help control costs, as well as offline storage for long-term compliance needs.

Security leaders should have clear risk, security, and operational response objectives in mind when utilizing a SIEM solution. That clarity will not only require the solution to possess features and functions to effectively support incident response but also highlight the processes necessary to keep the SIEM solution relevant and fully integrated to critical organizational functions.

—Roberto Sandoval, Senior Director, Global Threat Detection and Response, Trustwave

Analysis Tools

Analysis tools include advanced techniques, tools, and algorithms that provide the ability to detect evidence of security compromise within large volumes of data. Processes should be defined around how an analyst will determine if an alert is malicious and the chosen tools should assist or automate this process. Additionally, the tools should provide access to gather context about the given event, preferably automated. Ownership, budget, and the support model for the tools needs to be defined.

Analysis tools are often based on **machine learning,** deep learning, and artificial intelligence—that provide either stand-alone, embedded, or add-on functionality to detect evidence of a security compromise. Security analytics can be performed on data that is either stored at rest or collected in motion—even at line speed on a massive network. This is a capability that can be obtained by security operations teams in a variety of different ways with most security products and service including some sort of security analytics function.

> **A security analytics environment requires proper curation. If you constantly toss events into your data lake, you end up with a data canyon. You need to constantly evaluate which bits of your event stream should make it into your analytics environment and how you will navigate the corpus you're building.**
>
> *—Jeremy Kelley, Director of Secure Data Engineering, E*TRADE*

SOC Engineering

The SOC engineering team is responsible for the implementation and ongoing maintenance of the security operation team's tools, including the SIEM and analysis tools. It is important to clearly define the responsibilities of this team. Will they be responsible for licensing, maintenance and updating tools? Will they manage the underlying architecture (CPU, RAM, storage, cloud implementation) or will that be handled by another team? SLAs with the team should be defined to cut down friction between teams, as well as to establish clear communication plans.

> **Most SOCs have too many tools due to an "I need one of everything, best-of-breed" mentality and the tools they do have are poorly implemented. It is important to not only choose the right technologies but to fully utilize all of the features available in them. This cuts down the need for a bunch of tools that don't work together and duplicate functionality.**
>
> *—Robert Dodson, Senior Security Operations Specialist, Palo Alto Networks*

Business Management and Operations

Case Management

A necessary capability for a SOC is a clear protocol for documenting and escalating incidents. Case management is a collaborative process that involves documenting, monitoring, tracking and notifying the entire organization of security incidents and their current status. The minimum set of data points that should be captured in a case, and the tool selected for this function, should be capable of handling this data. Often, organizations will utilize multiple tools (ticketing, SOAR, email, etc.) for case management which is ill-advised, as data continuity is severed and incident handling efficiency takes a hit.

Case management should also include a definition of who will have access to the data and tools, how cases will be documented in a consistent manner, and how teams will collaborate to close out incidents. A case management system should also be encrypted with strict access controls enforced due to the highly sensitive data that it will contain.

Budget

A financial plan for the costs of running the SOC should begin with an agreement on the mission of the SOC. Then, the technology, staff, facility, training, and additional needs to achieve that mission are identified. From there, a budget can be established to meet the minimum requirements of the team. Often, a SOC budget is set from the top-down or assigned a percentage of an IT budget. This approach is not business focused and will result in frustration between capabilities and expectations from the business.

Once the budget is established, it should be followed by a regular review to identify additional needs or surplus. The timeline for regular budget requests and approval should be documented to avoid surprises or a last-minute rush to defend the organization's needs. Define the process needed to change the allocated budget, as well as a process for emergency budget relief.

A business-savvy budgeting resource can help the security operations organization navigate CapEx spending vs. OpEx spending and the expectations of the business. Be aware that government SOCs have additional considerations around the timing of elections and possible party-switching, which could result in dramatic budget shifts.

Metrics

Metrics that matter provide confidence and drive change.

—Tim Treat, Director of Customer Experience Delivery, Palo Alto Networks

If time is spent gathering metrics that cannot drive change, then they are at best, a waste of time; and worse, can drive the wrong behavior. An example of this is Mean Time to Resolution (MTTR). This is a fine metric when used in a NOC (where uptime is key) but it can be detrimental when used in a SOC. Holding analysts accountable for MTTR will result in rushed and incomplete analyses. Analysts will rush to close incidents rather than do full investigations that can feed learning back into the controls to prevent future attacks. This will not produce better outcomes or reduced risk for the business.

Another poor metric is counting the number of firewall rules deployed. 10,000 firewall rules can be in place but if the first is any-any than the rest are useless. This is similar to measuring the number of data feeds into a SIEM. If there are 15 data feeds but only one use-case, then the data feeds aren't being utilized and are a potentially expensive waste.

Caution should be taken when measuring peoples' performance. Ranking top performers by number of incidents handled can have skewed results and may lead to analysts "cherry-picking" incidents that they know are fast to resolve. Additionally, evaluating individual performance in this way violates the law in various countries.

Bad metrics can drive the wrong behavior. Examples include:

- **Mean Time to Resolution (MTTR)**
- **# of incidents handled**
- **# of alerts**
- **# of feeds into the SIEM**
- **# of firewalls/rules deployed**
- **Threat score**

See more about Metrics that Matter in **Appendix A.**

Make sure everyone understands the story you are trying to tell, - Not everyone interprets data the same way you will. Have a clear plan and purpose for the metrics and measurements you and your team are gathering and reporting up to senior management or the board. Knowing the audience can help you craft relatable metrics.

—Kristopher Jamieson, Manager, Cyber Security Operations Centre and Threat Intelligence, Blackberry

Reporting

Reporting is meant to give an account of what has been observed, heard, done or investigated. It is to quantify activity and demonstrate the value the security operations team is providing to the business or client organizations in the case of an MSSP. The outcome of reporting will not necessarily drive changes in behavior but is meant to track current activity. Reports are typically generated daily, weekly and monthly.

Daily reports should include open incidents with details centered on daily activity. Weekly reports should identify security trends to initiate threat-hunting activities, which includes the number of cases opened and closed, and conclusions of the tickets (malicious, benign, false positives). Include such information as how many different security use cases were triggered and their severity, and how were they distributed through hours of the day.

Monthly reports should focus on the overall effectiveness of the SecOps function. These reports should cover topics such as how long events are sitting in queue before being triaged, if the staffing in the SOC is appropriate (do more resources need to be added or reassigned), what is the efficacy of rule fires, and are there rules that never fire or always fire a false-positive.

Using the mean alone as a metric is prone to being skewed by outliers and misrepresenting the bulk of your data. The median (the 50th percentile, or halfway point of the distribution) is better at following the true path of the data. Better yet, give a range from the 5th percentile to the 95th percentile as well to show how much of your data varies, while still being robust to extreme outliers.

—Melissa Santos, Senior Data Analyst, Pingboard

Business Liaisons

A growing trend is for security organizations to hire business liaisons. This role is to tie-in to the different aspects of the business and help identify and explain the impact of security. This includes keeping up-to-date with new product launches and development schedules, onboarding new branch offices, and handling mergers and acquisitions where legacy networks/applications need to be brought into the main security program. This role can also be responsible for partner, vendor, and team interface management.

50 locks on a door makes a really shitty door. If your security keeps the business from doing what it needs to do, you wrecked the door.

—Dawn-Marie Hutchinson, OnePharma Information Security Officer, GSK

Governance, Risk, and Compliance

The governance, risk, and compliance (GRC) function is responsible for creating the guidelines to meet business objectives, manage risk, and meet compliance requirements. Common compliance standards are PCI-DSS, HIPAA, GDPR, etc. These standards require different levels of protection/encryption and data storage. Those requirements are typically handled by other groups; however, the breach disclosure requirements directly involve the security operations team. The SOC team must interface with the GRC team to define escalation intervals, contacts, documentation and forensic requirements.

With GDPR and now CCPA, businesses are having to rethink their SOC strategies. Many data privacy laws include notification requirements or private rights of action. It's no longer enough to recognize you have been breached. Businesses must understand—within the defined notification periods—the 'what' and the 'how' required by the GRC teams in order to work with regulatory bodies, including within any defined notification periods.

—Greg Day, VP and CSO, EMEA, Palo Alto Networks

DevOps

The **DevOps** team is not only responsible for developing and implementing company-created applications, but also, for maintaining them. This role has evolved greatly with the adoption of cloud apps and agile development, where application upgrades are now rolled out within minutes, rather than the long cycles where we would see major releases every 6-12 months only. The DevOps team's main motivation is to push bug-free features out to users as rapidly as possible. Some groups have worked security protocols into their release cycles, but most have not.

Security operations will need to interface with the DevOps team to both work protocol into the release procedures and to get ahead of the new development tools and features that are being tested/used by DevOps. Additionally, the SecOps team will want to familiarize themselves with the DevOps processes and procedures in order to reduce friction between the teams.

Since inheriting legacy applications from acquisitions can add risk, collaboration between DevOps and security teams is essential. When these applications cannot be quickly deprecated, the DevOps teams can implement automation wherever possible to reduce this risk. These teams will continue to collaborate as they move into a DevOps mindset in which security is built into the workflow.

—Clint Ruoho, Lead Acquisition Product Security Engineer, Salesforce

Process: Identification

Alerting

Alerting is how an event is determined to be important enough to become an actionable incident. The function has a high opportunity to utilize automation. When automation is used to bubble-up alerts, then how these automated efforts will be validated for accuracy or missing events must be defined. The alerts themselves are generally created and maintained by the content engineering team. The quality of alerts is extremely important for presenting high-fidelity alerts to analysts and reducing false positives.

> **You can't alert on everything. Generate cases for high-fidelity alerts, then use hunting to work through low-fidelity indicators of compromise.**
>
> *—Matt Mellen, Senior Manager of Information Security, Palo Alto Networks*

Content Engineering

Content engineering is the function that builds alerting profiles which identify the alerts that will be forwarded for investigation. The content engineer and the security operations team need to be tightly interfaced with feedback continuously flowing between the teams.

An interface agreement needs to be put in place identifying how often content updates will be made, how they will be vetted, and the feedback process. It should identify how the security operations team and threat hunting team make requests for new alerts or modifications to existing alerts. Properly configured alerts will allow the security operations team to focus on important alerts that require further investigation.

> **If you find something in a hunt, you should never find it in a hunt again. You should create content to alert or block the threat.**
>
> *—Alex Krepelka, Lead Security Engineer, Palo Alto Networks*

Initial Research

Initial research is a set of high-level processes that are utilized by an organization to begin an investigation into a suspicious alert. The results of the initial research assist by providing context around an incident to help in gathering information to triage, escalate, and determine if further investigation is needed or if the alert is malicious or benign.

When an alert is triggered, the security operations team needs an easy way to gather the information required to determine the severity of an incident and build the foundation for an investigation. Many platforms offer automated severity recommendations and the data required for an analyst to quickly perform the initial review of alerts. Technology should be in place to allow for "right-click" or simple drill-down capabilities to access the context around the alert for the analyst to perform the initial research.

Severity Triage

Severity triage defines the event prioritization based on impact to the business to help guide the analyst's action through the Incident Response lifecycle. When automation is utilized to assign an initial severity, the analyst reviews that severity assignment and then validates it against the uniqueness of the organization. This is done to verify or modify the severity and prioritization of the incident against other priorities.

Each business must determine their own risk tolerance and severity classifications. A 1–5 severity system is recommended: critical, high, medium, low, and informational. Critical indicates a breach of some sort. The exact descriptions and impacts will vary from business to business. Some organizations add a severity 0 to indicate an ongoing breach where the attacker is attempting to exfiltrate, encrypt, or corrupt data.

Recommended severity classifications:

- **1 - Critical**
- **2 - High**
- **3 - Medium**
- **4 - Low**
- **5 - Informational**

There is a fallacy around tribal knowledge in that organizations get comfortable thinking that long-time staffers are more capable of protecting the business. In truth, this presumed 'inside advantage' is often wrong. As is often the case, when security teams are polled asking which IT assets either represent the organizational crown jewels, those that fall under the high category within the CIA triad, or those that have compliance considerations, most are unable to provide a timely and accurate response.

—Joe Bonnell, Founder & CEO, Alchemy Security

Escalation

Escalation is a set of guidelines that enable the security operations team to increase the organization's awareness of a potential issue and receive the necessary support. An interface agreement should be put in place to define what severities require increased awareness from the business. Escalation and communication plans need to be developed with all stakeholders, documented, and socialized. Stakeholders can include but are not limited to, IT Operations, GRC, Legal, Corporate Communications, and Support. This escalation matrix should include specific scenarios and the associated escalation steps. These plans can quickly become obsolete due to revolving staff, so regular reviews are necessary to ensure accuracy and relevancy. Backup contacts and procedures to address unresponsiveness are recommended as well.

Process: Investigation

Detailed Analysis

Detailed analysis is a deeper investigation into an incident to determine if it is truly malicious, identify the scope of the attack, and document the observed impact. It is a manual process to answer the questions: What? Where? When? Why? Who? and How? Additionally, a detailed analysis helps to confidently determine if an incident is a "true" incident. In the event of a false positive, feedback should be provided to the Content Engineer so they can tune alerts, or to the security engineering team so they may update controls.

The procedure developed describes the detailed analysis which is conducted as part of the modular incident response plan. The procedure presumes that initial research has concluded, and all respective pieces of information have been gathered accordingly. This procedure closes any remaining gaps that were left after the initial research. In addition, identification of affected IT assets and business services are conducted. The appropriateness and efficacy of available containment measures are evaluated and provided as input to the mitigation procedures. Detailed analysis ensures that all relevant information is gathered, including:

- The potential impact of the security incident
- The affected assets
- The adversary's objective
- The potential impact of containment measures

Only after these essential pieces of information have been investigated can an informed decision about the containment and mitigation strategy be made.

Analysts need all of the relevant information about the incident and associated context available at their fingertips. Time spent tracking down this information is time not spent responding to the attack.

—Marcel Hoffmann, Former SOC Manager, Hewlett Packard Enterprise

Forensics and Telemetry

Forensics and telemetry provide the data needed to perform the different types of investigation from severity triage to detailed analysis and hunting.

Telemetry is a broad range of activity gathered in real-time from a given source. It is inclusive rather than selective, and rarely collects the contents of an item. Examples of network telemetry would be session and packet headers, rather than packet contents. Endpoint telemetry would include process execution details, file and memory reads and writes, but not their contents. Telemetry is consistently recorded, which makes it more useful than a "log" that collects prescribed information only when triggered by a specific event; it is also more accessible than forensics due to the wider coverage area and speed of collection.

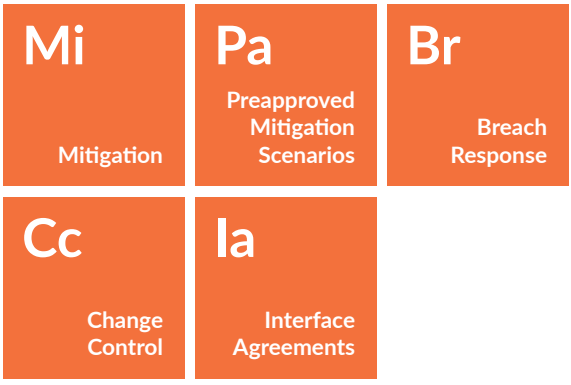
Forensics is a commonly misused term, mostly referred to as "the act of collecting raw data needed to complete the detailed analysis for an investigation." Raw data capture requires specific tools and tends to be slow due to its size and method of collection. In the case of network data, raw data would be capturing whole packets or netflow logs, and for endpoint, it may include a memory dump, whole executable or operating system files, or even whole hard drives. The true use of the term "forensics" is to define the method an expert witness uses to prepare evidence. For electronic (or computer) evidence to be admissible in a court of law, it must be repeatable and defensible, the process taken by an expert must not modify any of the original data in any way, and the results must be factual and not tainted by whichever party is funding the work. The true use of "forensics" defines this method, and raw data capture is an integral component.

The use of both telemetry and forensics is a necessity for every security team. Telemetry from network and endpoint activity, and cloud configurations will provide readily available information necessary to triage and investigate the majority of alerts and incidents. Forensic data capture, while slow, will supplement telemetry and provide the information needed to conclude the small number of high priority or difficult incident investigations that often lead to breach identification. Should a breach be validated, all data and results will be required by government and regulatory bodies; however, the forensic data will be of most use to their investigators because of the way it is collected and the depth of its contents. Types of data include:

- Event: Any action performed by a person or technology
- Alert: Notification of an event
- Log: Details of an event
- Telemetry: Activity consistently gathered electronically and in real-time from a given source
- Forensic (Raw): The complete contents of an item, without change or modification

> **Forensics is the process of preparing evidence in a repeatable and defensible manner acceptable for expert testimony or deposition.**
>
> *—Mitchell Bezzina, Computer Forensic Consultant, Palo Alto Networks*

Process: Mitigation



Mitigation

Once an incident has been validated, a mitigation strategy must be executed. The mitigation strategy is comprised of a set of processes, and interface agreements to contain the security incident. This typically includes documentation of any actions taken by the security team and temporary controls that can be implemented to quickly stop an attack, which should lead to permanent controls to prevent future attacks.

Preapproved Mitigation Scenarios

Some mitigation processes are easily automated for preapproved mitigation scenarios. These are a set of parameters that allow for the immediate containment or prevention of a security incident without further approvals. An example would be to block an infected laptop from the network to prevent the spread of malware. Another example is to create a dynamic process to block against specific IOCs (such as known bad URLs, domains, or IP addresses) without requiring a security commit invoking a change window. The process followed for each scenario by an analyst, when executing the mitigation process, should be documented.

Breach Response

A true breach requires a plan separate from standard mitigation. It defines how to effectively respond during a critical severity incident. The first piece of this plan is to identify the cross-functional stakeholders, including corporate communications, legal teams, and third-parties as appropriate. Then assign a timeline of when each stakeholder should become involved and how they will be initially notified. Details of the information to be collected and shared by the security operations team should be defined, as well as the SOC commander responsible for providing the information to the stakeholders. Also included should be information about the frequency of updates, method of updates, and communication processes (emails, collaboration tools, a war room, etc.). Training and policies should be created to prevent leaks of breach details beyond the breach response team. Breach response plans should be periodically tested, typically a few times per year, and at least once without the security team having prior knowledge of the test.

When a breach impacts customers, Corporate Communications needs to be alerted and brought in immediately. Delays in communication can be a real threat to a company's brand and the trust customers have in it.

—Kristi Rawlinson, Head of Marketing Communications, Strivr

Change Control

In cases of both manual and automated mitigation, a change control process must be in place to monitor, document, and control changes being made. A good change control process ensures alterations to the environment have a minimized impact to business and documentation in case a look-back review needs to be performed. The information required for this documentation should be identified and ideally contained in a formalized template. This process should have timelines for reviewing and rolling back temporary changes. Also included, should be who can request changes, the steps needed to initiate change, and any prerequisites or change windows available for the modification.

All changes should be:

- **Deemed necessary to the business**
- **Consistently documented, even when automated**
- **Created to minimize downtime or disruption**
- **An efficient use of resources**

Many security organizations see change as a threat instead of seeing it as the opportunity to guide progress in a way that accelerates the business while reducing risk. Change is continuous. We can't control everything, so we need to provide the guardrails for changes so the business can move as fast as required to service customers.

—Dan Ward, Solutions Architect, Palo Alto Networks

Interface Agreements

Interface agreements define how the security operations team and surrounding teams will interact with each other. These agreements list the teams involved and detail the scope of work and responsibilities for each team. SLAs should be referred to, as well as change request processes and escalation, in cases where an interface agreement is not being upheld. Communication paths and tools used between the teams should be identified. A regular review of all agreements should occur, and the intervals of reviews set and stated clearly.

See a sample interface agreement in **Appendix D.**

Process: Continuous Improvement

Tuning

Tuning refers to adjustments made to the alerting procedures regarding security incidents based on the outcomes of security investigations. It is an important step in reducing false positives and low-fidelity alerts in the SOC. An analyst may determine, during the course of a security incident, that there is a better way to detect the incident to increase visibility at the SIEM. When this occurs, the analyst will engage the tuning process to improve that visibility for future incidents. General tuning should be based on metrics collected from systems in the SOC. This includes a process to retire alerts when they are stale or ineffective.

The tuning process should define:

- Who or what triggers tuning efforts
- Thresholds for those triggers
- A review process for existing alerts
- The steps to request modifications to existing alerts (to increase visibility of future security incidents based on the outcome of a security investigation)

It is recommended that alerts be reviewed—at minimum—on a quarterly cadence with a monthly review of alert metrics.

> **Configure and tune everything as far up the stack as possible; as close to the source as possible. Just because you can massage garbage in the SIEM doesn't mean you should.**
>
> *—Mary Cordova, Security Orchestration, Automation, and Response Expert, Sony*

Process Improvement

Adjustments must also be made to the incident response lifecycle based on the results of security incidents and new threats. New technologies introduced to the SOC and the business may also require IR process updates. The process should include information about who can update the IR processes (this person must be a qualified resource knowledgeable in IR). Changes need not be made daily, so it should define how often processes should be reviewed, which will vary by process. All improvements should be reviewed and then socialized with affected groups.

Process improvement is like brushing your teeth. You don't just do it once and think you're good. Processes should be continuously evolving to keep up with new technologies, tactics, and threats.

—Bob Hermes, Lead Developer for Operations, AT&T CSO – MSSP

Capability Improvement

Capability improvement is rooted in revisiting prior incidents and asking how these incidents can be better prevented or mitigated in the future. This results in adjustments to the alerting profile, prevention posture, and automation techniques. Sometimes the goal is to prevent an attack, other times it's to stop a breach faster or gather the appropriate information needed for quicker investigation. Ideally, this effort should be on-going and follow every investigation. In most cases that is not possible, so a monthly review of incidents should occur to identify opportunities for capability improvement.

Goals of capability improvement:

- **Prevention of future attacks**
- **Faster identification and stopping a breach**
- **Gathering of necessary data for investigation of specific incidents**
- **Quicker investigations**
- **Automated remediation**

Quality Review

As new tuning measures, processes, and capabilities are implemented, a thorough peer evaluation of the changes should be carried out to ensure effectiveness and value to the business. Additionally, incident workflows and documentation should also be reviewed. This is to confirm consistency within the IR process which will result in a higher level of capability from the security operations organization.

Identifying who is responsible for reviewing changes, as well as closed cases, must be documented along with a cadence for the review process. That resource must be given time to perform these reviews outside of their normal duties. A process should be created to define what severity cases require review, what items in the case will be reviews, how feedback will be provided, and what training opportunities arise from the reviews. Then, that training must be delivered to the security operations organization (and sometimes beyond the SecOps group) to improve the overall efficiency and efficacy of preventing breaches.

Security Operations Automation

So Security Orchestration, Automation & Response

Sa Security Automation

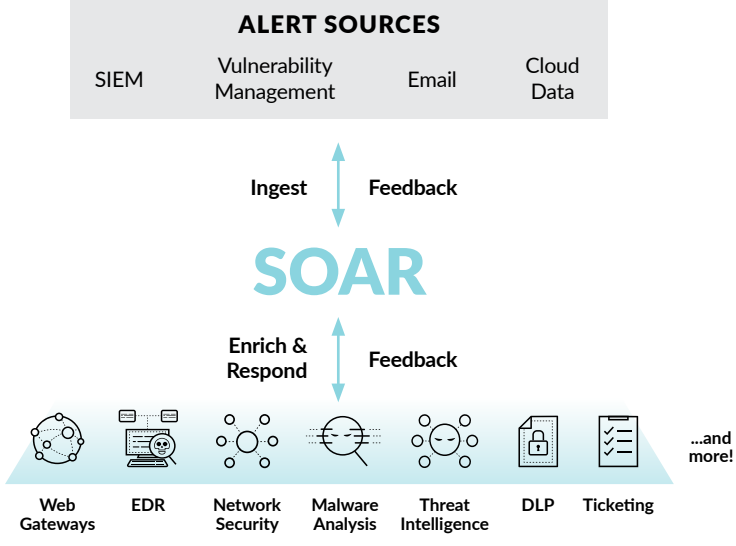
> **We don't have a people problem as much as we have an automation problem.**
> *—Chris Calvert, Co-Founder & VP Product Strategy, Respond Software*

Security Orchestration, Automation, and Response

According to Gartner,

> **SOAR refers to technologies that enable organizations to collect inputs monitored by the security operations team. For example, alerts from the SIEM system and other security technologies — where incident analysis and triage can be performed by leveraging a combination of human and machine power — help define, prioritize and drive standardized incident response activities. SOAR tools allow an organization to define incident analysis and response procedures in a digital workflow format.**
>
> *—Gartner Glossary, Security Orchestration, Automation and Response (SOAR), https://www.gartner.com/it-glossary/security-orchestration-automation-response-soar*

SOAR systems allow for accelerated incident response through the execution of standardized and automated playbooks that work upon inputs from security technology and other data flows.



High-level view of how SOAR tools sit in a SOC

SOAR tools ingest aggregated alerts from detection sources (such as SIEMs, network security tools, and mailboxes) before executing automatable, process-driven playbooks to enrich and respond to these alerts. The playbooks coordinate across technologies, security teams, and external users for centralized data visibility and action. They help accelerate incident response times and increase analyst productivity. By standardizing processes, they provide consistency which improves operational confidence in SOC capabilities.

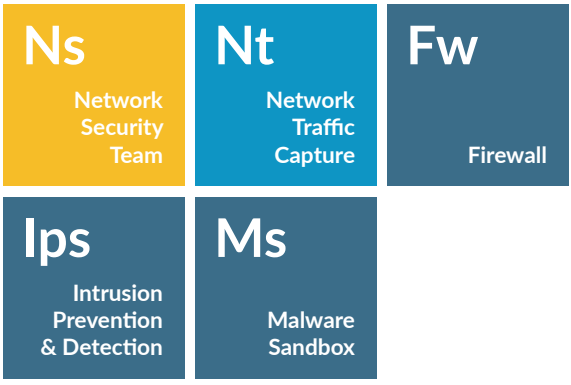
Security Automation

Consistency is a key factor in the effectiveness of a security operations team. Automation helps ensure consistency through machine-driven responses to security issues. A security automation function will own and maintain these automation tools. They must be tightly integrated with the security operations team to continuously maintain the automation playbooks. They are also responsible for implementing new automation technology and playbooks in response to new workflows and processes defined by the security operations team. The requirements, and eventual vetting of the solution, should be the responsibility of the security operations teams. This vetting should consider the time-savings, accuracy, and usefulness of the automation.

There are some cases in which automation increases the need for resources. It is always necessary to consider the return-on-investment before investing in automation. When doing an ROI analysis, take special care to consider the ongoing cost of maintenance and support.

> **If you can document the steps to do an investigation or perform mitigation, chances are good you can automate it. Find those opportunities.**
>
> *—Scott Okupski, Automation Global Practice Lead, Palo Alto Networks*

Network Security



Network Security Team

The network security team is responsible for the development, implementation, and maintenance of the network security policy. The scope of the team's responsibilities may extend into tool selection, implementation, and maintenance including the firewalls, IDS/IPS, URL Filtering, Application Monitoring, and other data flowing across the network.

An interface should be defined between the network security team and the team that will implement the network security policy which could be the same team or different. The change control process should include any specific information that is required for network security updates but should follow the standard change control steps established for other changes within the business.

Network Traffic Capture

Network traffic capture provides the ability to intercept and log traffic traversing network appliances. This can be accomplished with firewalls, IDS/IPS, proxies, routers, switches, and standalone traffic capture technologies. Logging of this traffic provides visibility to the security operations organization for detailed analysis and advanced investigations. Raw traffic logs should be accessible by analysts but not presented to them unless tied to an alert or as queried by the staff.

Firewall

Firewalls are an essential cybersecurity control to separate networks and enforce restrictions for communications between them. They can be physical devices in a datacenter or implemented virtually to protect assets in the cloud. Firewall functionality varies and can include URL Filtering, IPS/IDS, antivirus, SSL decryption, VPNs, among other features to consolidate capabilities into a single tool. They can be set up to monitor boundary traffic as well as lateral traffic and used for network segmentation to further lock down critical assets to a business. They are a key tool for the team to gain visibility into network traffic through logs and alerts received from different points in the environment.

The security operations team should define what information they require from the firewall, including additional context for investigation of alerts. Many firewalls are not configured out-of-the-box to provide this context, so the security operations team may have to drive that requirement with the network security team. Although firewalls provide the visibility that analysts need, they can also be a burden to the analysts if not continuously updated with new policies and/or if they are not tuned properly and provide overwhelming low-fidelity data to the SOC.

> **We have to look at firewalls differently as 5G services come into the picture. Port and protocol controls aren't enough to protect our life-critical and business-critical services. Security operations teams need to quickly correlate the source of the threat, the device which is infected, and the applications being used. Lives are depending on it.**
>
> *—Lakshmi Ananderi Kandadai, Director of Product Marketing, 5G Services, Palo Alto Networks*

Intrusion Prevention and Detection Systems

Other tools used to gain visibility are **Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS),** and DNS sinkholing. These features may be integrated with a firewall or standalone tools. An IDS is considered a reactive control that generates alerts based on rules configured in the system, while an IPS has the added capability to mitigate or block malicious behavior and is considered a proactive control. DNS sinkholing is used to allow, alert on, or sinkhole known malicious traffic.

Agreements must be in place between the group that maintains the IDS/IPS/DNS sinkholing technologies and the SOC, defining how OS upgrades, outages, and patching will be communicated to the SOC and how the SOC will request that additional signatures be added. The SOC should also be aware of basic architecture and configuration settings such as coverage of the functionality and if they are configured to fail open. As with firewalls, additional logging may need to be turned on to generate the context needed by the security operations team to perform investigations.

DNS Security is an important function in the firewall to detect command and control activity as a result of a network compromise. This detection capability and the configurable policy actions, such as block or sinkhole, allow the SOC team to quickly identify and contain threats on the network.

—Martin Walter, Director, Product Management, Palo Alto Networks

Malware Sandbox

A malware sandbox is used as a safe place to simulate an end user's environment to test unknown applications that may contain viruses or other types of malicious code. A security team can "detonate" malicious code to observe the behavior and impact to systems and networks without impacting the whole of the environment. Malware sandbox features can include malicious file analysis, API call tracing, and memory analysis, along with other advanced capabilities.

The sandbox should be set up to analyze the impact to all operating systems used in the environment and should produce ample logs from which to generate security controls. The security operations team is typically not responsible for using the malware sandbox but benefits from the information gathered during simulations.

In malware sandboxing we get to use terms like 'detonate' and 'blast radius'. These are not the terms you want to hear used outside of your sandbox.

—Eric Haller, VP, Security Operations, Palo Alto Networks

Cloud Security

Cloud Security Team

The cloud security team is responsible for the development, implementation, and maintenance of the cloud security policy. The scope of the team's responsibilities may extend into tool selection, implementation, and maintenance, including distributed computing and virtual firewalls, however, that can fall under cloud engineering teams as well. An interface should be defined between the cloud security team and the team that will implement the cloud security policy (which could be the same team or another). The change control process should include any specific information that is required for cloud security updates but should follow the standard change control steps established for other changes within the business.

Cloud Computing

Cloud computing delivers services or applications, on-demand, to achieve increased scalability and transparency, security, monitoring, and management. In cloud computing, services are delivered via private, public, or hybrid cloud. The use of cloud computing requires a cybersecurity policy enforcement point to apply enterprise security policies for cloud-based resources. It can be architected on-premises or cloud-based and provides a consolidation of different types of security policy enforcement. This can include single sign-on, authentication and authorization, device profiling and step-up authentication challenges.

Log collection is what will be most heavily utilized by the SOC. These logs provide both in-depth forensic data and correlated event data to the SOC to ensure security analysts can analyze incidents without becoming overwhelmed with noise. The visibility required from these logs should be defined based on what the SecOps team requires for proper investigation, as well as what access level the analysts will have. If mitigation will be used in the cloud deployment, this should be documented and reviewed as part of the continuous improvement efforts. The SOC also needs to understand what types of alerts will be generated by the cloud security capabilities and worked into the IR plan.

Organizations don't work with just one cloud provider. They work with multiple cloud environments, so it is important to provide consistent security across the continuum of environments. This enables the proper forensic data to be captured in ways that are useful and easily accessible for security analysts.

—John Morello, VP, Products, Palo Alto Networks

Endpoint Security

Endpoint Security Team

The endpoint security team is responsible for the development, implementation, and maintenance of the endpoint security policy. The scope of the team's responsibilities may extend into tool selection, implementation, and maintenance, including **Endpoint Protection Platform (EPP)** and **Endpoint Detection and Response (EDR)** capabilities. An interface should be defined between the endpoint security team, the team implementing the endpoint security policy, and the infrastructure team deploying the technology within change control processes, which could be the same team or different. The change control process should include any specific information that is required for endpoint security updates but should follow the standard change control steps established for other changes within the business.

The endpoint security team must interface with the business to define what endpoint technologies and operating systems will be allowed in the business and to address security concerns around them. An interface directly with the SOC is also fast becoming the norm, as the endpoint telemetry collected from EDR is a beneficial source of information for security alert triage and incident investigation. Regular contact between the team and the business should occur to plan for any new systems that will be incorporated into the business through technology adoption or through M&A activity.

Endpoint Data Capture

Endpoint data capture is the ability to collect information generated on or visible to endpoint devices. The most common form of data collection are logs, telemetry, and forensics (raw data). Within the security team, log data generated when a prescribed event occurs is typically only used in relation to an alert for either creation or correlation, telemetry records real-time activity and is commonly used for triage and incident investigation or threat hunting, while forensics is used for detailed analysis and information retention.

The use of these data types varies widely between security operations, internal investigations, eDiscovery and compliance teams—all with their own specific requirements. Typically, endpoint data capture requires a runtime or persistent agent, in some cases the remote use of operating system tools can also be used. For this reason, endpoints are typically defined as devices that contain a common operating system in which a user can interact (Microsoft Windows, Apple Macintosh, *nix variants, and Chrome OS). The term "endpoints" usually does not include mobile (Apple iOS and Google Android) or Internet of Things (IoT) devices. Mobile devices typically fall under the purview of endpoint security; IoT devices typically fall under network security. The network and endpoint security teams should collectively be aware of each device in the organization and the software running on them.

Endpoint Security

Endpoint security provides control for detecting and protecting servers, PCs, laptops, phones, and tablets, from attacks such as exploits and malware. Endpoint security can include antivirus, EDR, analytics, and device control. The security operations organization should define what data should be captured and forwarded to the SIEM, or a central security log management function. This organization should understand how to identify data or system exposure, as well as mitigation options that are available. An interface agreement should be put in place to determine how mitigation strategies will be executed, how to request changes, and how the changes will be validated.

Behavioral Analytics

Behavior analytics is a security technology that detects malicious activity by identifying anomalous behavior indicative of attacks. It applies to endpoint security, network security, and user activity. Behavioral analytics starts by inspecting endpoint, network, or user data to automatically classify user and device types and develop a baseline of expected behavior. This technology compares current behavior to past behavior and peer behavior to identify anomalous activity. Machine learning models can improve accuracy by tailoring detection thresholds to each organization's environment.

Behavioral analytics can uncover malware, ransomware, exploits, lateral movement, exfiltration, insider threats, and risky user behavior. The security operations team should be aware of what types of events they will encounter and incorporate resulting alerts into the incident response process.

Adversaries are very good at staying under the radar once they have infiltrated an organization. Behavioral analytics helps uncover these hard-to-detect attacks and lateral movement.

—Kasey Cross, Senior Manager, Detection and Response, Palo Alto Networks

Asset and Vulnerability Management

Asset Management

A security operations team needs access to up-to-date asset lists. Asset management provides this information as a database to store information for the organizations' owned hardware, software and the end user responsible for the asset. An interface should exist to define what information access is needed for the SecOps organization, how access to the data will be achieved, and how the data will be updated and kept fresh.

Vulnerability Management Team

The vulnerability management team is responsible for identifying and escalating vulnerabilities in an organization's assets, including hardware and software. They utilize vulnerability scanning technology and other tools to discover vulnerabilities. The SecOps and vulnerability management teams require an interface to define the visibility and access required by the security operations team and to update each other on new observations such as possible malware or newly announced vulnerabilities. When a new vulnerability is announced, the vulnerability management team will work with the security operations team to implement controls to prevent attacks while the patching process is executed. The security operations team needs to stay updated on these new controls, so they can properly address any alerts that reach the SOC.

Vulnerability Management Tools

Vulnerability management involves the processes, tools, and platforms involved in maintaining an accurate inventory and awareness of current and potential security weaknesses in an enterprise. Such weaknesses can include unpatched systems, known (but unfixed) vulnerabilities, and unknown (but suspected) exploitable holes. One tool utilized for this capability is a centralized database that contains the identity, classification, prioritization, remediation or mitigation of vulnerabilities of all corporate-owned and managed systems. This tool is populated by regular scans of the environment for known vulnerabilities. The security operations team requires access to this information when investigating the incident impact on an organization.

Threat Intelligence

Threat Intelligence Team

Threat intelligence is a function in most security organizations but not necessarily a defined team. This function identifies potential risks to the organization that have not yet been observed in the network. It utilizes real-time information feeds from human and automated sources on the background, details, specifics, and consequences of present and future cyber risks, threats, vulnerabilities, and attacks. They are responsible for validating threats and then work with the security operations team to provide IOCs for the analysts and to update controls. Additionally, the deliver threat landscape reports on agreed-upon intervals to security teams who are responsible for updating the security stack based on findings.

A dedicated team handling threat intelligence is not a requirement, but the function is critical to the success of a SOC. Without it, you can only protect against yesterday's threats.

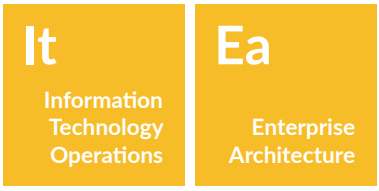
—Darren Lawless, Senior Manager, Threat Monitoring, IBM Security

Threat Intelligence Platform

Intelligence can come from numerous intelligence feeds, industry channels, and is ripe for automation. This is an area where security analysts are drowning in information. Open source feeds include ISACs, the FBI, and other agencies, and are in-line with sharing threat data. Premium feeds deliver more comprehensive information on that data, including risk score and magnitude. It is good to utilize both, then use a threat intelligence platform to automatically ingest threat intelligence feeds and automatically create controls back into the system. Following that course of action, the team is freed up to dive deeper into specific threats and threat actor playbooks.

Threat intelligence often includes recommended actions, but most threat intelligence teams tailor their response to reported threat issues based on local conditions. A threat intelligence platform can be used by the security operations organization to find related attacks, specific IOCs of an attack, and the context around a threat that leads to quicker investigations and higher fidelity results.

Asset and Vulnerability Management



Information Technology Operations

The information technology operations (ITOps) team is responsible for the availability of the IT infrastructure. They are motivated to solve problems quickly. They manage, monitor and respond to alerts from IT systems (which can be seen as similar to the function of security operations but is very different). This function can also consist of server management outside the scope of the help desk and can control cloud technology (**SaaS, PaaS,** and **IaaS**) operations. ITOps is measured in uptime/availability and performance. This will almost always take precedence over vulnerability patching. ITOps and SecOps functions need to work closely to diagnose issues and share information about performance issues that may be attack related. However, they should remain separate functions.

Arguments can be made for physically separating network and security operations as well. Security requires need-to-know handling of information which network operations does not. If the functions are collocated then a basic understanding of security principles (confidentiality, integrity, and availability) should be instilled in the staff. Consideration should also be taken on the reporting structure of SecOps vs. NetOps. NetOps typically reports up through the CIO. When that person also has responsibility for security, a conflict of interest arises. Many organizations have shifted the security function to report to governance, risk, and compliance or directly to the CEO/President.

Enterprise Architecture

The enterprise architecture team is responsible for understanding, developing and maintaining the network (physical and/or virtual) design to meet the business' requirements. They ensure that security is implemented in the design phase and not added as an afterthought. They are also responsible for creating and maintaining architecture flowcharts and diagrams. The end goal is to balance the needs of security with the business needs and ensure that to the degree possible, both are met.

> **The most important question to answer when building out a security architecture is, 'What are we trying to protect?' The 'How?' is secondary.**
>
> *—John Kindervag, Field CTO, Palo Alto Networks*

Collaboration

Collaboration Tools

A set of tools is required to facilitate communication and collaboration within and around the security operations organization. These tools can include features around ticketing, war room collaboration, shift turnover, process documentation, and may contain the entirety of the IR documentation for every event. They can also include communication features such as email distribution lists, shared inboxes, instant messaging, and video conferencing tools.

Collaboration tools are often incorporated into other tools and are at high risk of feature duplication. The security operations team should define what the main tool(s) used will be, which will be the single source of truth, and what information will be captured. Access to these tools typically extends beyond the security operations organization, especially in the case of war rooms, so access control must be addressed by the chosen tools.

Knowledge Management

The knowledge around how a SOC operates and interfaces with other functions is stored in a centralized database known as a knowledge management system. It can be elaborate, or as simple as a Wiki. The knowledge management system should contain the operations, administration, and maintenance of the security operation platforms and the security operations team's processes. Information in knowledge management systems can age quickly, so the SecOps team must define how often the content will be reviewed and updated and time must be set aside for this task. A properly kept knowledge management system can speed new-hire training and is key to providing consistent security to the business. The security operations team will also need to work with IT teams to source the tool and identify who is responsible for the underlying system (CPU, RAM, storage, etc.).

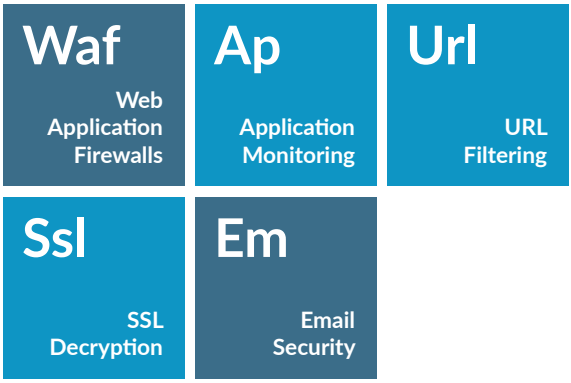
Help Desk

The help desk function can be contained inside an organization or outsourced. They provide end-user support for corporate IT assets. Security operations frequently open tickets with this team to reimage machines, request system patching, or to reject assets joining the network without the proper OS and app version levels. The help desk organization should interface often with the vulnerability management team about patches, outdated operating systems, accepted new operating systems, new supported platforms, etc. Interactions with this team have a great chance for automation, and a closed-loop process between the teams should be in place to ensure follow-through on IT requests to reduce noise in the SOC.

In a small company, IT and security are often the same group. It is important to not let the IT functions of the business overtake securing the business. Time needs to be made for both.

—Ben Price, System Administrator, Dire Wolf Digital

Layer 7 Technologies



Web Application Firewall

A web application firewall (WAF) is a security control that protects HTTP applications from well-known HTTP exploits. It allows a user to craft policy controls to a specific application hosted on a web server. The rules in a WAF are more granular to the specific server than to the grander FW/IDS/IPS controls. They are placed inline of the client/server HTTP(S) conversation and have similar functions as a proxy with security built-in.

Application Monitoring

Application monitoring provides the ability to determine and log the specific application used in a session. By monitoring applications, the SecOps team can gain additional context on specific applications that were used when an event was triggered. It goes beyond port identification and recognizes the application used which can lead credence to proving an IOC was enacted or that the event triggered was a false positive.

URL Filtering

URL filtering gives security organizations the control to track and restrict access to specific URLs and URL categories. It blocks known malicious domains via blacklists and through category blocking. The technology also helps identify suspicious traffic, like traffic to proxy and anonymizers, to assist in threat-hunting cases for controlled assets or internal users attempting to circumvent controls. Organizations can also create white lists to allow specific internal domains from flagging or being subjected to security control that creates false positives. This prevention technology increases protection to an organization and can reduce false positive alerts from reaching the SOC.

SSL Decryption

A significant portion of network traffic is encrypted and, therefore, "invisible" to the SOC. SSL decryption technology provides visibility into HTTPS traffic, which is then logged in a readable format. Without this technology, the SOC can face issues with finding IOCs or high-fidelity indicators if an incident is active. Before implementing SSL Decryption technology, security groups should consult their GRC organizations to ensure it will not violate the rights of the end users.

> **Decrypting traffic without permission and appropriate policy can create real risk in many organizations. Because of the strict international privacy requirements and laws regulating computer use, decrypting traffic carries special risks of legal claims, like unlawful interception and computer invasion of privacy.**
>
> *—Gerry Stegmaier, Attorney, ReedSmith*

Email Security

Email security detects and prevents malicious email content from infecting the recipients, and can also provide protection from phishing scams. Email security functionality supports properties for confidentiality, digital signatures, sender authentication, and integrity control using cryptographic controls. Information from email security systems should be provided to the SOC so they can investigate credential loss issues. Email security is an area with a great opportunity for automation of use cases. A new feature of email security is DMARC (Domain Message Authentication Reporting and Conformance) which is an email authentication, policy, and reporting protocol allowing email senders and receivers to work together in order to better secure emails and users.

War Games

Red and Purple Teams

Red and purple teams provide penetration testing to simulate threats to the organization and provide feedback for improvements to the security operations organization. The red team simulates advanced persistent threats (APTs) and will attempt to hide and slow-play their attacks to avoid detection by SOC analysts. Purple teams work with both red and SecOps teams to help improve operations. They provide information to the red team about gaps in the analyst's focus areas and guide the SecOps team towards approaches to identify red team efforts. Red and purple team exercises should have an allotted time limit and the results should be given as feedback to the SOC to improve capabilities and add processes, procedures and additional controls before an actual APT gains hold of the network.

Larger more mature organizations will benefit the most from Red Team exercises, as they are usually ready to move beyond their reliance on security products and truly test their ability to detect, prevent and respond to an attacker. Smaller, less mature organizations may become overwhelmed with a Red Team exercise, and should first focus on penetration testing to identify and remediate specific weak areas.

—Krissy Safi, IBM X-Force Red

Threat Hunting

Threat hunting is often thought of as a function of the security operations team; however, since it is separate from "identify, investigate, mitigate," it is distinct from analyst activities and is included as an interface. Hunting allows for digging into the data to find situations that the machines and automation may have missed. While machines are excellent at handling events, people are excellent with situations.

Threat hunting can be structured or unstructured. Structured hunts begin with a single piece of intelligence, a hypothesis is formed, and then the hunt to find the threat in the network begins. It's important to note that formalized, structured hunts tend to be more useful to an organization than unstructured efforts.

See more on Successful Threat Hunting in **Appendix C.**

Threat hunting is smart people looking for things missed all other ways.

—Mary Writz, VP Product Management, ForgeRock

Tabletop Exercises

Tabletop exercises are planned events where the stakeholders for the SOC or the entire security organization walk through a security event to test the processes and reactions to the type of incident. They can include simulated network activity or social engineering.

Each stakeholder participating in the exercises receives a different type of tabletop. The security operations team would be given highly technical challenges. The rest of the stakeholders would not be given a number of technical requirements but would have high involvement in areas outside the SOC. These differences in tabletops keep the teams and stakeholders involved and prevent them from losing interest in the exercise.

Tabletops may take time to create and third-parties are often involved to avoid bias in preparation. Execution of the exercises should be limited to half a day. This reduces the likelihood of distractions. Ideally, these exercises should be performed once a quarter, alternating between the types and parties involved. They should also be performed when major changes occur in the security organization to ensure all processes are still valid and effective.

Train like you fight – Security teams need to have a sparring partner to develop new defenses and build muscle memory. SOC teams continuously need to engage with red teams (to run purple team exercises) and conduct adversary simulations to continuously remain ahead of the threats.

—Nick Essner, Incident Response Lead, Accenture Security

Honey Pots and Deception

Honey pots and other deception techniques are put in place to detect, deflect, and counteract malicious activities against an organization. They provide a lure, false leads, and shadow networks to draw an attacker into a controlled environment, so their actions can be studied. Honey pots and deception can be used to assist the SOC in understanding the techniques being used to exploit their defenses leading to new uses cases for alert generation and updated controls. They can also be used to decipher the threat landscape and the types of campaigns that are targeting the organization and vulnerabilities in IT operations.

Access Security

Vpn	Iam	Na	Mdm
Virtual Private Networks	Identity & Access Management	Network Access Control	Mobile Device Management

Virtual Private Networks

VPNs allow remote users to securely participate on the corporate LAN from an external network location. Traffic on VPNs requires special security policies because it is seen as part of the trusted network and connections may not be subject to the same firewall and IDS/IPS controls used for external traffic. The SOC requires visibility into this traffic to monitor for remote users and application anomalies.

Identity and Access Management

Identity and access management (IAM) tools provide control for the provisioning, maintenance, and operation of user identities and the access the identity is allowed. These controls assist the SOC in reducing the amount of stolen credentials when paired with multi-factor authentication (MFA). Users should be educated on when to approve push authentication from MFA systems and to critically look at them to avoid assuming the challenge is related to their current work. GRC should define the least privilege policies to be implemented by the team managing the IAM capabilities.

> **Given that account takeover is one of the top attack vectors, SOCs need to know when credentials have been exposed so they can mitigate risks before an exposed credential becomes a breach. SOCs are the ideal watchdogs to know when high-valued targets (such as executives or admins) are exposed due to third-party credential leaks. As the saying goes, attackers no longer need to break in. Now they just log in.**
>
> *—Ted Ross, CEO and Co-Founder, SpyCloud*

Network Access Control

Network Access Controls (NACs) are designed to restrict access to the network. It can reduce the number of unauthorized devices that connect to the network. This reduces the number of potentially unpatched or compromised systems to connect to the network. It also reduces the number of endpoints for which the SOC has no visibility, or any endpoint security the SOC can use to mitigate threats against these unauthorized devices.

Mobile Device Management

Mobile devices are a focal point of attacks and can be used to gain a foothold into a network. Using mobile device management (MDM) technology increases an organization's prevention posture with the ability to monitor, manage, and secure corporate mobile devices. MDM technology provides the SOC with network activity logs for the device. MDM can also be used to restrict certain types of devices to connect to the network, operating systems, and devices with known vulnerabilities.

Insider Threat Technology

Data Loss Prevention

Data loss prevention (DLP) is a cybersecurity control to detect and prevent the accidental or malicious release of proprietary or sensitive information. The controls for DLP are often defined by GRC and managed by the network, endpoint, and cloud security teams. A DLP system assists in the prevention of data exfiltration and notification of attempts are sent to the SOC. The SOC then uses these notifications to look for a potential incident or APT in the network.

Operational Technologies

Operational Technology Team

Operational technology is a new attack vector for malicious activity. The operational technology team (OTT) is responsible for managing and maintaining the OT, IOT, and IIOT systems (SCADA, PLCs, DCS, CNC, etc.). It is important for the security operations team to be in contact with the operational technology team to share where the OT devices are found on the network, what the vulnerabilities exist on the operating systems, any security controls that can be put in place to protect the OT devices. The SecOps team should also understand the expected traffic flow for the OT network and the OTT should assist the SecOps team in setting up use cases and alerts for abnormal activity to detect malicious events before there is an impact to the business.

IoT and IIoT systems tend to be deficient in key security protections found in more robust systems. This includes patch management, process isolation, access control, and exploit mitigation technologies. It is vital for an SOC to help fill in these gaps by monitoring for abuse and misuse of these systems. This is especially important as IoT and IIoT adoption continues to grow at a record pace with billions of devices anticipated to come online over the next few years.

—Andrew Roths, Internet of Secure Things (ioXt) Board of Directors, Senior Principal Security Engineer, Amazon

Where to Start

With 72 elements that a security operations organization should be covering, it can feel overwhelming. However, few, if any, security operations teams fully address all of the elements. One approach for organizations with an existing SecOps team (even if it is just a person reviewing security logs) is to perform an assessment of coverage of the elements. This allows for the discovery of gaps in capabilities. With this list, a plan can be put together to make incremental changes to address the gaps. These changes should be iterative and do not need to be all done at once.

It is recommended to start with the **Mission** element. This is most critical to the success of the SecOps function. It allows for a clear understanding of the value the organization provides to the business. From there, a modular incident response plan should be created to define how the security operations team and associated stakeholders will identify, investigate and mitigate threats. Plus, it covers how continuous improvement will occur. SecOps is dynamic, and change should be expected and embraced.

If you want a successful SOC, you need to simplify, prioritize, automate, and measure.

Simplify your stack. You don't need one of every tool on the market. What you do need, are capabilities that work together to achieve your goals.

Prioritize capability improvements. If everything is important than nothing is important. Create a prioritized roadmap based on the goals of your business.

Automate processes based on criticality and impact of the threat, as well as confidence in the data. Any processes that are repetitious and can be automated, should be automated.

Finally, measure your progress. Give the business confidence in the continued improvement of services you are providing to them.

—Mario Chiock, Fellow and CISO Emeritus, Schlumberger

Appendix A

Metrics That Matter

When determining good metrics for your business, always keep in mind the mission of the SOC and the value it provides to the business. The business wants confidence that they can prevent attacks and also that if/when a breach does occur then they are able to handle it quickly to limit the impact. Good metrics should provide insight into whether the business should have confidence or not. There are two types of confidence to focus on: configuration confidence and operational confidence.

Configuration confidence is knowing that your technology is properly configured to prevent an attack, that you can automatically remediate it, or the proper intelligence can be gathered for analysis by a human. Example questions to answer are:

- **Are the security controls running?** Oftentimes a "temporary" change is made to controls and is inadvertently left in place. A developer may need a specific port to be opened to perform a test and that port remains open providing an access point for an attack.
- **How many changes are occurring outside of the change control policy?** The change control policy should be followed in every change without any exceptions. Any deviation to the defined process should be noted as it is relevant to the business's confidence in the configuration of security controls.
- **Are the technologies in place configured to best practice?** Once a technology is in place, it is rarely a "set it and forget it" situation. Care must be taken to continually evaluate the configuration against best practices. If the measurement of controls against best practices is low, this can drive a plan to increase adherence. If the metrics drop then a look into why this is happening is warranted.
- **What percent of features and capabilities are being utilized?** The plethora of security technologies is overwhelming security operations. Many of these technologies are poorly utilized, resulting in a false understanding by the business regarding the actual coverage in place. It can also lead to the purchasing of duplicate features, which exacerbates the issue of too many technologies. Measuring the percentage of feature use can provide the business with a simple understanding of actual value being provided by tools vs. perceived value. For example, what percent of traffic flowing is visible to analysts? Estimates state that 70-80% of traffic is encrypted. The business should know how much traffic is being analyzed in a SOC and if SSL decryption technology is being used.

In addition to configuration confidence, businesses should have operational confidence. Operational confidence is knowing that the right people and processes are in place to handle a breach if/when it occurs. Example questions to answer are:

- **How many events are analysts handling per hour?** This is known as events per analyst hour (EPAH). A reasonable EPAH is 8-13. If the EPAH is too high, say 100, then this indicates that analysts are overwhelmed. They will rush investigations, ignore events, and not be set up to properly protect the business. Also, note that it is important to measure per hour and not per day as an analyst's tasks should shift throughout the day and shift lengths can vary causing this number to skew. This metric should also not be gathered to compare employees but rather to show the effectiveness of an entire security operations organization.
- **Are there repeat incidents flowing into the SOC?** If threats are properly investigated, then the outcome should feedback into the controls and the controls should be centralized to eliminate updates to be made in multiple areas that can get out of sync. Repeat incidents flowing into a SOC indicate a failure in this feedback and sync of controls.
- **Is the SOC handling alerts for known threats?** This also indicates a failure in the controls because all known threats should be blocked prior to effecting the business and being passed to the SOC to investigate.
- **How often are there deviations in SOC procedures?** This metric can indicate the need for employee training on the procedures or illuminate out-of-date procedures that need to be updated.

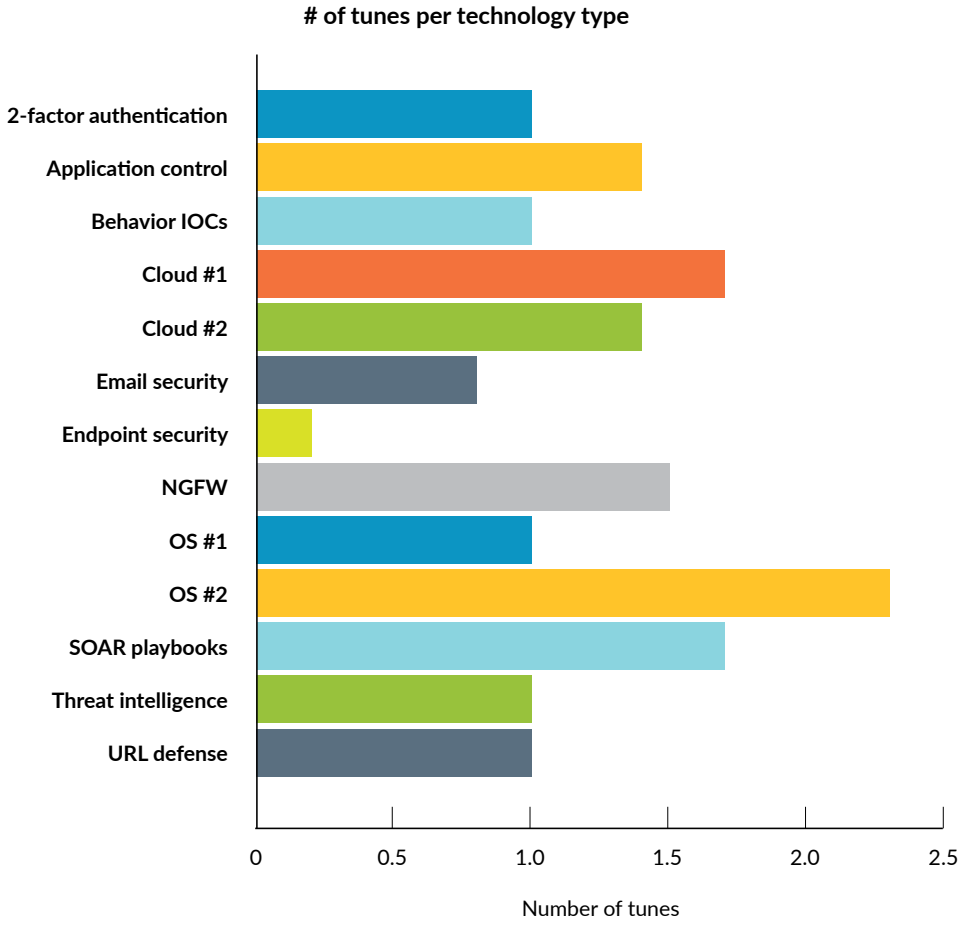
CxO-facing metrics should focus on the confidence that the business is properly set up to prevent a breach and contain a breach, should one occur. (See Metrics section above.) Additionally, CxOs will require occasional briefings on vulnerabilities and threats making headlines. Answer for them: Are we affected? What is the impact to our business? What are the measures in place to mitigate the risk? How long will it take to fully remediate the threat?

Metrics should be used to improve protections and provide confidence to the business that the security operations organization is executing on their mission. However, they are often misused, and this results in a fear of meaningful metrics for some. When metrics are feared it is because they get in the way of the story being told or they make someone look bad. They may be misleading because they are too high-level and require additional, time-consuming backup details to explain. Sometimes, they can be interpreted as failure if they are not 100% or are not gathered to eliminate a possible paper trail that could be used by auditors. Businesses should make sure that the metrics provided are valued, can drive business decisions, and are not derailed by these fears.

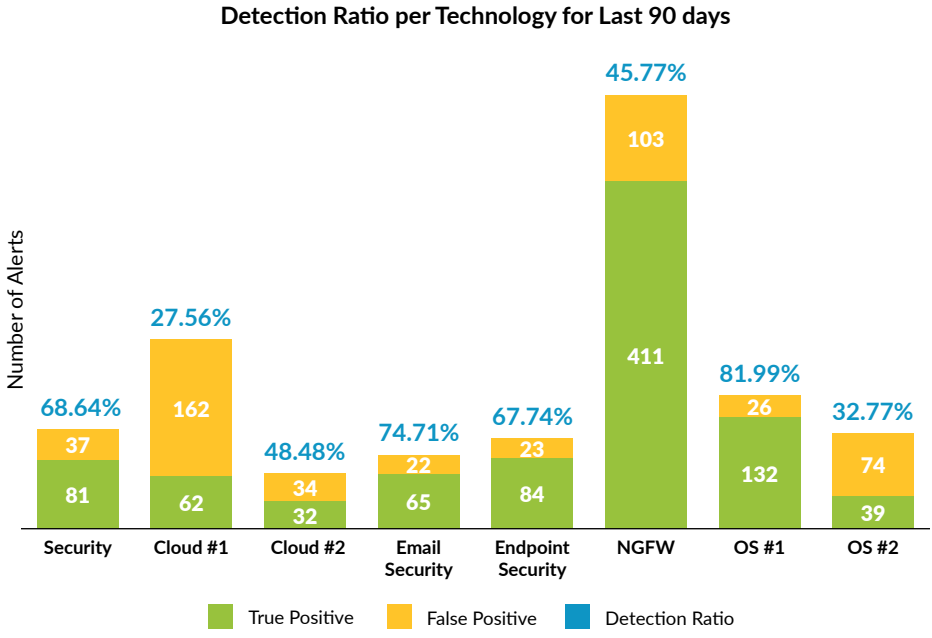
Appendix B

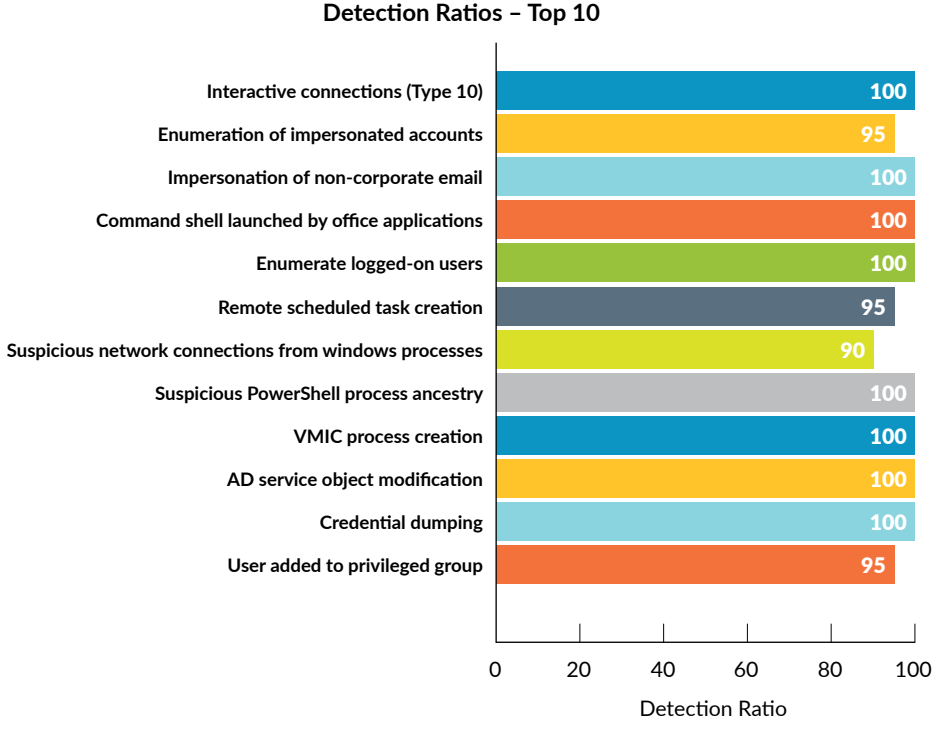
Sample Security Operations Reports

Level of Effort (LOE) for Detection Technologies

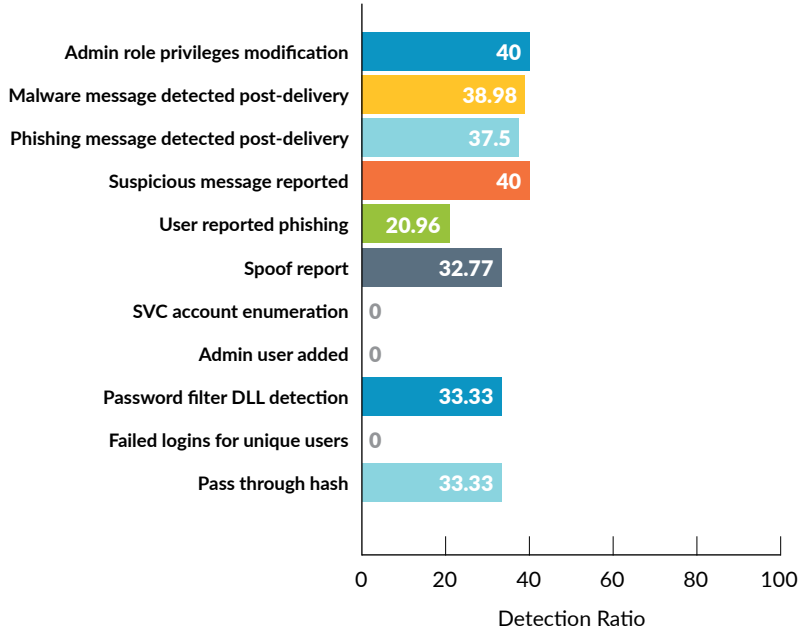


Detection Ratios

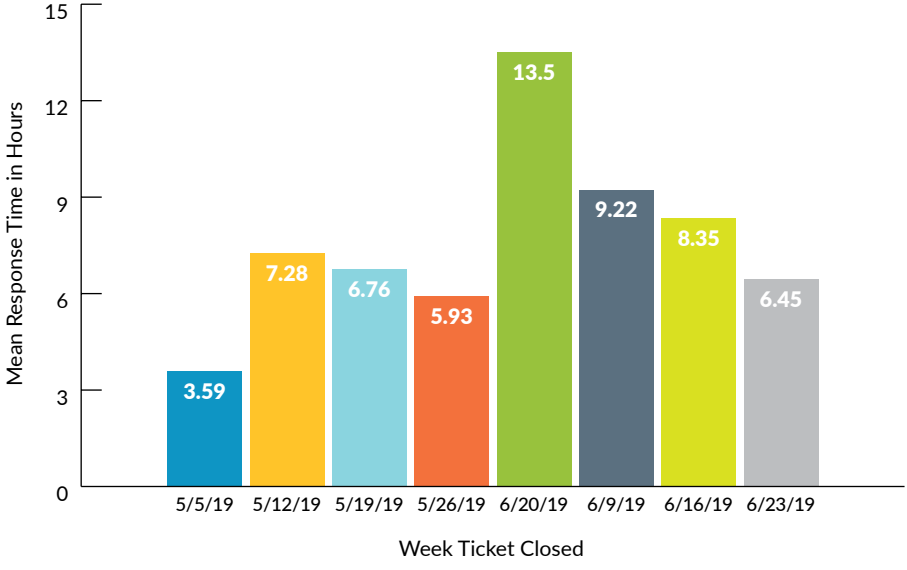


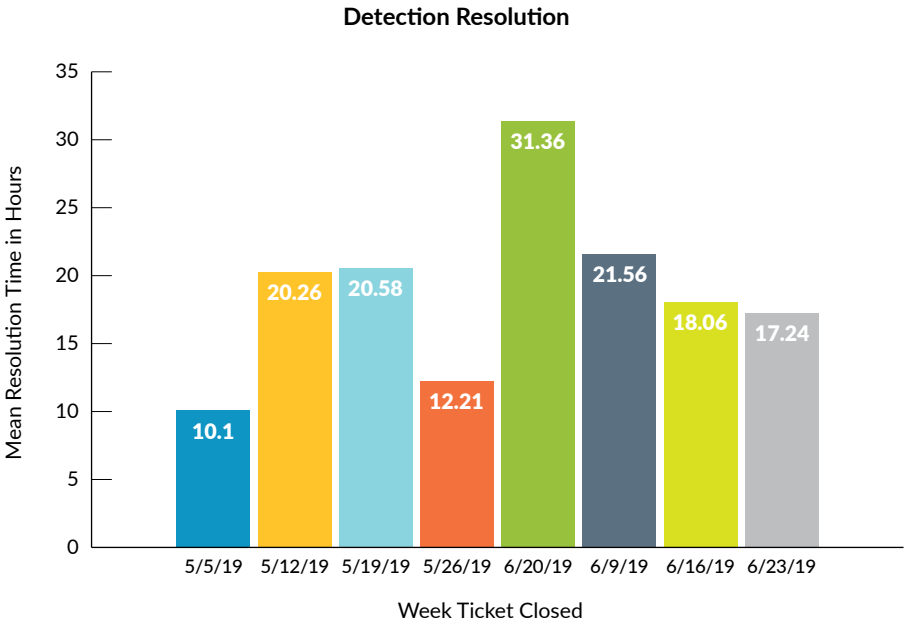


Detection Ratios – Bottom 10



Detection Response




Detection Resolution
Mean Resolution Time in Hours
35
30
25
20
15
10
5
0
10.1
20.26
20.58
12.21
31.36
21.56
18.06
17.24
5/5/19
5/12/19
5/19/19
5/26/19
6/20/19
6/9/19
6/16/19
6/23/19
Week Ticket Closed

Appendix C

Successful Threat Hunting

The success of a threat-hunting team is driven by the following requirements:

- **Time to do it –** Most organizations cannot afford dedicated hunting staff but need to allot committed time for hunting. This can be a few hours per day/week or a dedicated person for a specific time period. Hunts should be goal-oriented sprints that last no longer than two weeks. If the two weeks are exhausted without progress, then you must move on.
- **Process-driven, agile methodology –** Hunting should be process-driven but follow an agile methodology. Threat hunting can lead down many rabbit holes which requires agility, but there should be a formal process in place to guide the hunt and pull back from the rabbit holes as needed.
- **Clean/Structured data –** Most often, threat hunting is performed in a data lake. Efficiency is driven by the consistency and structure of the data. This can be done through auto-tagging via security tools (NGFW) or a SIEM. The data must also be flexible for the many ways you want to use it. Additionally, the hunters need to understand what automated processes, alerts, and behavior analysis has already been performed on the data as not to duplicate efforts. Access to appropriate tools for hunting are also necessary. This may be query access to a data lake, APIs, and visualization tools.
- **Driven by a piece of intelligence –** Each hunt should start with a piece of intelligence and a hypothesis. This could be a new vulnerability or threat that should be investigated to see if it impacts the organization, an unusual behavior, or it could be as simple as following-up on a malware outbreak to make sure it has been fully remediated.
- **The hunt ends with what was learned and feedback into the controls –** The end of the hunt should result in documentation being shared with the SOC, about what was done and learned from the hunt. If a conclusion was reached, then updated prevention should be fed back into the controls to prevent future incidents of this type. The hunt may also end when the two-week hunt period has been exhausted without a conclusion. Note: This still requires documentation about what was done.

One thing to note about hunting: Hunt teams run into configuration issues when they are blindly looking at data. A strong hunt team will specifically look for a particular kind of breach and will not run into configuration issues. If configuration errors are all that are found, then it is worth re-evaluating the structure and cost of the hunt program and see if there are less expensive ways to identify these types of configuration errors.

Appendix D

Interface Motivations

Each function of the business that the security operations organization interfaces with will have goals and motivations distinct from those of the SOC. This can create frustrations between groups that are trying to achieve different things. By understanding the motivations of different functions, the SecOps team can better align requests and communications for better results for the business.

Help Desk	IT Operations	DevOps
Closing tickets quickly	Availability and performance of IT infrastructure	Develop, implement, and maintain applications; Release bug-free features quickly
Business Liaison	**Enterprise Architecture**	**SOC Engineering**
Prepare the security organization to support changing business needs	Meet business' networks requirements	Implement and maintain SecOps tools
Endpoint Security Team	**Network Security Team**	**Cloud Security Team**
Secure the endpoint	Secure the network	Secure the cloud
Threat Hunting	**Content Engineering**	**Security Automation**
Identify high fidelity threats	Create useful alerting profiles	Speed response to security issues
Operational Technology Team	**Forensics and Telemetry**	**Threat Intelligence**
Manage and maintain OT, IOT, IIOT systems	Collect court admissible evidence on breaches	Identify potential risks
Governance, Risk, and Compliance	**Red and Purple Team**	**Vulnerability Management Team**
Create guideline to meet business and compliance requirements	Mimic adversaries to breach the organization	Patch systems quickly

Appendix E

Interface Agreement Template

Document Information
Version History, Author, Reviser, Approvers of current version, Process owners, document official location, revision control, etc.

Introduction
Introduction of the teams involved and their relationship

Purpose
What is this agreement supposed to accomplish, what is the intention of the documents, is it a living document, etc.

Scope
What is the extent of operation for this agreement, etc.

In-Scope Services
Technology/Tools/capabilities and the extent they should be affected, etc.

Out of Scope Services
Specific services to be excluded from this agreement

Tools used for Incident Management
Collaboration tools, ticketing mechanisms, case management, etc.

Incident Management
What will be accomplished by incident management process, how many points of contacts are there, what types of incidents can occur, what is specifically included in process, what is outside of process that may require forgoing some of the outlined process tasks, what are the inputs to create an incident, what are the outputs of the incident management, etc.

Incident Management Roles and Responsibilities
What role(s) owns which function(s) during an incident? End User, Analyst, Incident Manager, Engineer, SOC Manager, etc.

Incident Management Flow Chart
What does the process flow of an incident between the teams?

Incident Minimum Data Set
What is the minimum data required for the team(s) to accomplish incident management? Ticket Number, Date/Time, Location, User(s) affected, IP address, MAC Address, description of problem, etc.

Severity Matrix
What are the severity types, what are the SLAs required by each of the severities, what is the business impact, what is the time to acknowledge, what is the time to respond, what are the escalation requirements, what are the escalation contacts, what is the proper path to engage the escalation contacts, what are the exceptions, what are the consequences, what approvals are needed, etc.

Acronyms and Definitions
Definitions of any and all acronyms found in this document?

Appendix F

Defining Security Orchestration

Security orchestration is a method of connecting disparate security technologies through standardized and automatable workflows that enables security teams to effectively carry out incident response and security operations.

If we study this definition carefully, a few terms jump out: **security technologies, workflows,** and **security teams.**

- **Security technologies**

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

  These product integrations are possible through a range of mechanisms such as Representational State Transfer (REST) APIs, SOAP APIs, SSH, SQL, HTTPS, and so on. The connective mechanism will depend on the types of products being integrated, which will in turn influence the depth and fidelity of data transfer that's allowed between the two integrated products.

- **Workflows/Playbooks**

  Playbooks (runbooks) are task-based graphical workflows that help visualize processes across security products. These playbooks can be fully automated, fully manual, or anywhere in between. Here are some building blocks that compose playbooks:

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

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

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

  – **Conditional task:** Through conditional tasks, security orchestration playbooks can check the value of any incident-related artifact and execute different branches depending on the result. For example, a conditional task can check the severity of an alert and execute different sets of tasks if the severity is High, Medium, and Low respectively.

  – **Security teams**

Here are a few ways in which SOAR playbooks can work in concert with human teams for combined security operations and incident response:

- **Manual tasks:** When an action is too unique, nuanced, or infrequent to be automated, security orchestration playbooks can have manual tasks that act as directives for the SOC analyst handling the respective incident.
- **Task approval:** Even if some actions are prime candidates for automation, they might be too sensitive to carry out without having a human verify their need and relevance. In such cases, automated actions can have built-in task approvals. These actions will wait for the relevant SOC analyst's approval before beginning execution.
- **End-user engagement:** If a SOAR tool has rich integrations with email tools, these integrations can be used to engage SOC analysts as well as end users within the organization and improve overall process flow.

SOAR Common Use Cases

Phishing Enrichment and Response
SOAR phishing playbooks ingest alerts from email inboxes and coordinate actions across threat intelligence tools, sandboxes, EDR solutions, and more for repeatable and accurate response.

Threat Hunting
SOAR threat hunting playbooks can be scheduled to run at pre-determined intervals, rapidly scanning for threats in the environment after ingesting external threat feeds or following up on existing incidents.

IOC Enrichment
SOAR playbooks can automate enrichment of indicators by querying different threat intelligence tools for context and presenting the results to analysts, thus shaving off lost time that can be used towards proactive investigation.

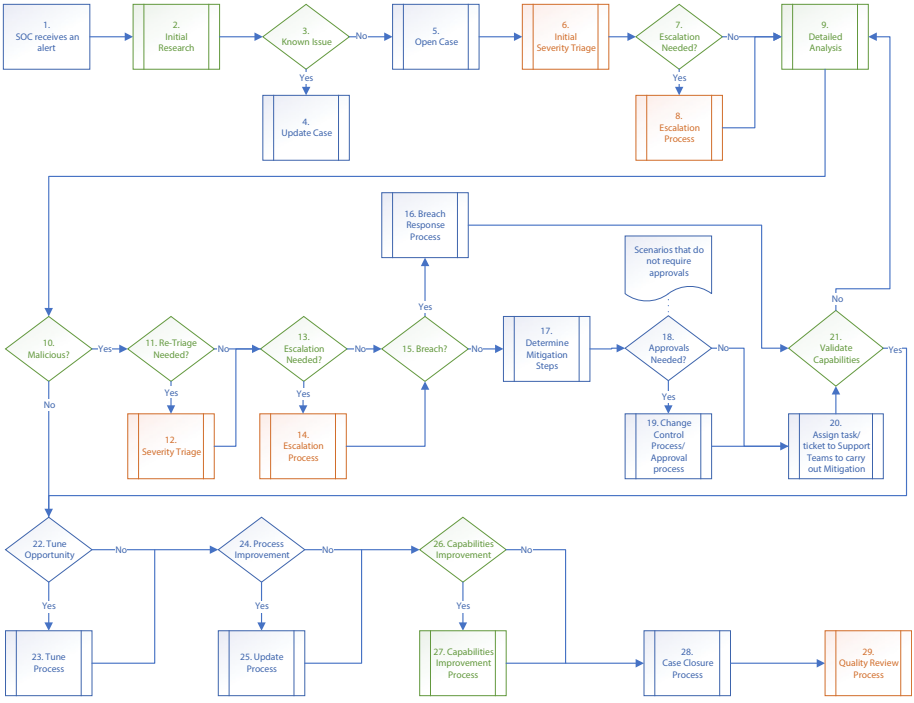
Incident Severity Assignment
SOAR playbooks can automatically assign severity to incidents by checking parameters relevant to the organization. By reconciling threat scores from other products, checking indicator scores, and verifying the criticality of affected endpoints and users, these playbooks ensure that analysts see the incidents that need to be seen.

Cloud Security Orchestration
SOAR playbooks can coordinate response across cloud and on-premise environments. For instance, a playbook can execute after ingesting a cloud security alert and respond by both blocking malicious IOCs on cloud appliances as well as on firewalls that are on-premise.

Sample SOAR Dashboard

Appendix G

Modular Incident Response Plan



About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before.

www.paloaltonetworks.com

About the Authors

Kerry Matre is an expert in security operations and has helped organizations across the globe establish confidence in their ability to protect their most valuable resources. For over 17 years, Kerry has observed what works and what doesn't in over 150 SOCs and believes that understanding the past creates success in the future. She is passionate about shifting from detect and respond approaches in cybersecurity to fully automated prevention-based approaches.

John Caimano is dedicated to making security operations organizations as efficient and effective as possible. As the Professional Services Global Practice Lead for Security Operations at Palo Alto Networks, he works to increase automation within SOCs and up-level SOC efforts to address more sophisticated threats. He joined Palo Alto Networks in August of 2018 with six-plus years of experience with the Palo Alto Networks Security Operating Platform and over seventeen years of experience working at a major telecom MSSP in labs and the CSO organization, supporting MSSP security provisioning, NOC and SOC.

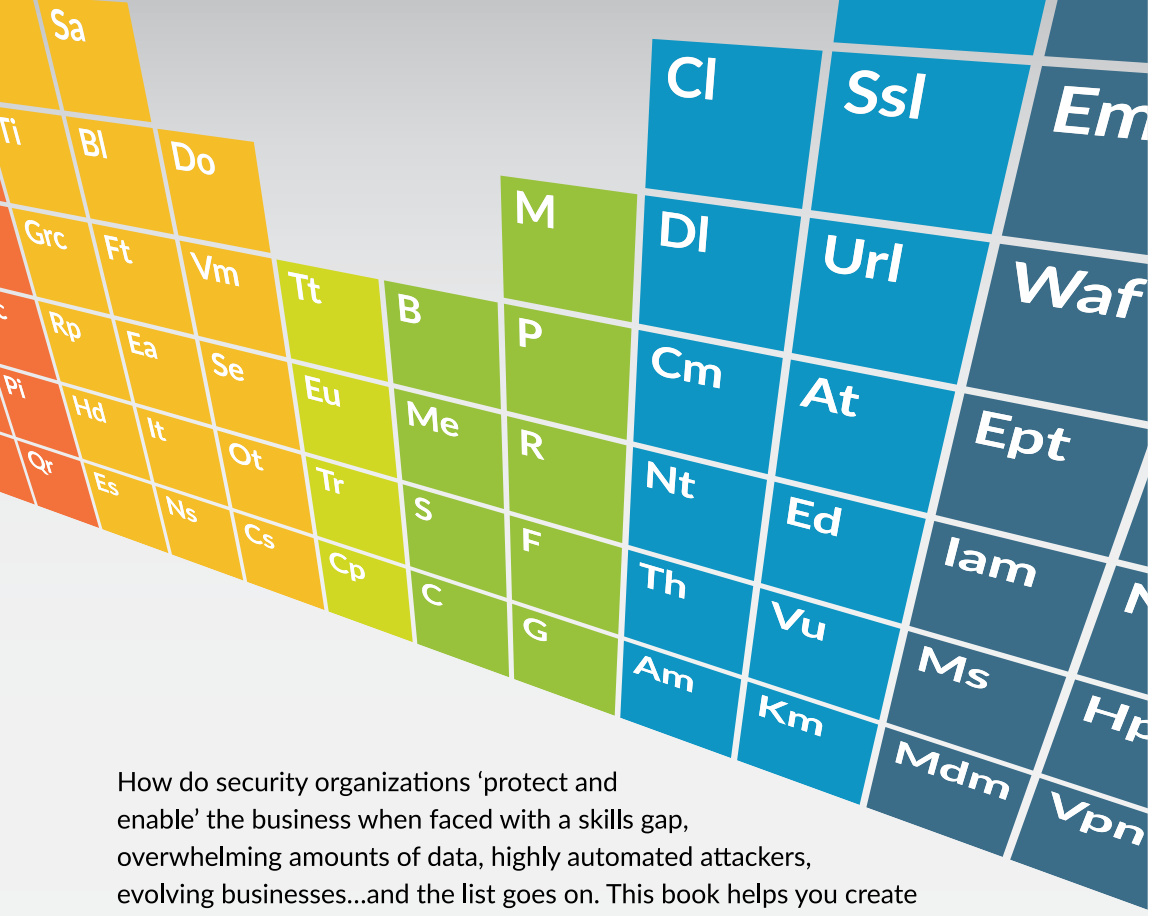
Contributors
Mitchell Bezzina
Mark Brozek
Kacey Cross
Robert Dodson
Marcel Hoffmann
Kamil Imtiaz
Abhishek Iyer
Matt Mellen
Keith Mokris
Austin Robertson
John Telan

Editor
Stephanie Wisdom

Design & Composition
Tim Heraldo

Printer
Almaden Global

Elements of Security Operations



How do security organizations 'protect and enable' the business when faced with a skills gap, overwhelming amounts of data, highly automated attackers, evolving businesses...and the list goes on. This book helps you create a plan by breaking down the elements of security operations—offering clear identification of what building blocks are needed in a security organization to meet the goals of the business.

The elemental pillars include the people, process, and technology aspects required to support the business, the visibility that is required to defend the business, and the interfaces needed with groups outside of the SOC to achieve the mission of the security organization.

By utilizing these elements in security operations, we can improve upon existing functions and develop those that are lacking, creating both opportunity and advantages for the SOC that end in desired results for the business.