Hewlett Packard Enterprise

Business white paper

Intelligent security operations: A how-to guide

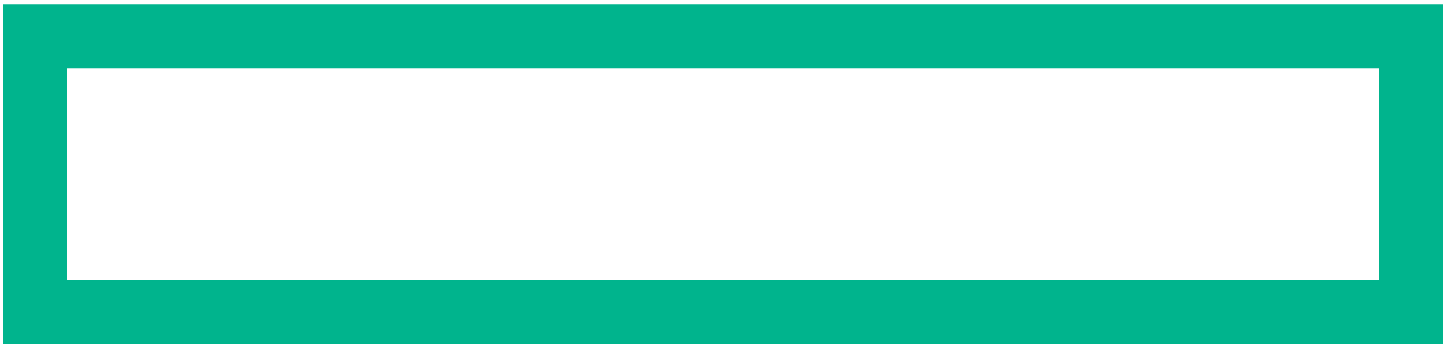

Table of contents

3 **What is the purpose of a SOC?**

4 **Building vs. outsourcing**

5 **Steps for building an intelligent SOC**
5 People
5 Process
5 Technology

7 **Achieving the basics**

8 **Overcoming staffing issues**

9 **Maturing your SOC**

10 **Advanced capabilities of a SOC**

11 **Conclusion—the future of SOC**

Successful businesses need to innovate, grow, and thrive. In order to do this, organizations must be able to mitigate their security risks. They must build security into every piece of their business from their network to their apps, to their data, and even to their users. At the same time, they need visibility into their organizations to detect and respond to existing and new threats. One of the most effective ways to achieve this is with an analytics-driven intelligent security operations center (SOC). An intelligent SOC is not a technology-in-a-box solution but is a progression of maturity and advancing capabilities within an organization.

The following is a roadmap for implementing an intelligent SOC. Whether you are starting from the beginning or looking to take the next step in maturity of your existing security operations, this paper can be used as a guide to confirm steps you have taken to date and plan for what comes next.

What is the purpose of a SOC?

A SOC exists to monitor and protect the critical assets of an organization through standardized and repeatable processes. This means they have the task of having eyes on an entire business to identify and block malicious behavior by insiders or outsiders. They must reduce the risk to the business within an acceptable budget and do this without hampering the operations and moneymaking efforts of the company. As a result of this, the SOC must be tightly aligned to the goals of the business.

The first security operations organizations existed in military and government entities. They focused mostly on blocking incoming attacks and expanded into compliance as regulations were implemented. This has evolved into the monitoring for both internal and external threats, as well as identifying anomalous behavior in users and systems. Some intelligent SOCs have matured into monitoring physical access and utilize intelligence feeds, hunt teams, and analytics to root out advanced attacks already in process.

Most importantly, intelligent SOCs must work in accordance with stakeholders across the organization to align on the security, compliance, and competent risk management objectives. As the situational awareness nerve center for security, the intelligent SOC is able to:

1. **Reconcile organizational risk, policy, governance, security, and financial objectives**
2. **Identify—through analysis by trained experts—the tools, controls, automation, and methods that can best be used to monitor and protect assets**
3. **Work across the organization through repeatable processes to capture the root cause, make improvements in the running policy, configure management of systems, and ultimately remediate the risk to the organization**

Once a threat has been identified, the security operations organization is responsible for escalating the issue to the proper business unit to be remediated. Then, they feed that information back into their own tools to be able to more efficiently alert on and predict future attacks.

Read more about the evolution of security operations capabilities here:
5G/SOC: SOC Generations

Building vs. outsourcing

A common question for organizations is whether they should invest in standing up their own internal SOC or outsource their security operations. Both options have benefits and the best direction will be determined by the needs of an organization. The first step is for the organization to define the business need and expectations of the SOC function. This will guide the decision. Additional questions to raise are "What is the size and geographic footprint of your organization?", "What is your risk tolerance towards breaches?", "How quickly is your organization expanding?", and "What is your budget?"

Figure 1: Considerations of security operations implementation and monitoring

Luckily, there are many effectively proven approaches to modern security operations in the industry. A technology implementation can be on premise, in the cloud, or handled by a managed security service (MSS) in a dedicated or co-mingled model. Technology and content management can be handled in-house or by an MSS. In addition, security event monitoring and analysis can be handled completely in-house, by an MSS, or with a mix of the two. They are customized according to the process stages or business hours. Here are some, but not all, configuration options.

Every SOC has unique demands—achieving the proper mix of owned as well as outsourced security operations tools and functions is necessary to meet the security operations goals of an organization. The IT and physical landscape of each organization is unique—especially its own fingerprint is based on the way it is architected, the company's structure, behavior patterns of its users, business processes, data flows, supplier network, customer interfaces, etc. For example, large organizations might want to handle investigations in-house, but midsized and smaller organizations might need to have those functions managed end to end externally because of a lack of resources.

Read more about what to take into account when creating an SOC, including co-managed and other models here: **Security operations: Build vs. outsource**

Steps for building an intelligent SOC

Whether building a SOC in-house, outsourcing to an MSS, or using a hybrid solution, there are steps that must be taken to assure a viable security operations capability is established. The first and most important step is to define the mission and business case of the SOC. This will make sure that the purpose of the SOC is aligned to the needs of the business and that success can be measured against the mission. A well-defined mission statement also helps with the continuity of expectations when there are turnovers in leadership.

Once the mission is clearly defined then a plan for the people, process, and technology of the security operations organization must be addressed.

People
There is an industry-wide challenge for organizations to hire and retain skilled security resources. A successful SOC must plan for this by identifying the recruiting process, training mechanisms to be utilized, career growth paths laid out to retain good resources. Additional retention steps need to be taken including clear role definition, mutually beneficial scheduling, proper performance metrics reporting, and ongoing training and career development. For perspective on the type of teams (level 1, 2, hunt, engineering, etc.), see **Growing the Security Analyst**.

Process
A good set of processes and procedures enable a SOC to operate in a sustainable and measurable manner, and enable the SOC to support compliance efforts easily when necessary. Without solid processes and procedures, SOCs become reliant on "tribal knowledge" of individuals. Absences or turnover of these individuals can cripple the capability of the SOC. Process considerations include knowledge management, analytical, operational, technical, and business processes. For a SOC to achieve high levels of overall maturity, there needs to be a solid, current, and relevant foundation of processes and procedures that guide consistent execution of critical tasks and define expectations and outcomes. Certain security activities still require a human to separate the wheat from the chaff. However, other key functionality can be automated. It's up to a well-defined process to decide what should be what, as well as how other issues of preparedness and case management will be handled. Processes can be further defined by groups.

Technology
Numerous security technologies are utilized in modern enterprises and are usually supported by different groups. The security operations organization must pull the security event data out of all of these disparate systems and normalize, aggregate, and correlate the security events across technologies. The use of a security information and event management (SIEM) system becomes critical to piece together the details of an attack in real time. Good SIEM tools also allow for quick investigation of breaches and workflow tools to manage incidents. Implementing a single-pane-of-glass SIEM system enables an organization to monitor, analyze, and respond to security events. Utilizing workflow tools in an SIEM system, as well as more advanced capabilities provided by leading SIEM tools, allow for repeatable methods of identifying, measuring, and reducing risk.

While no successful SOC can function without a SIEM, there are other technologies and processes in play. To build a successful SOC, organizations need to utilize a holistic approach to security operations that includes mastering the basics of security monitoring, incident detection, and breach escalation and response. Once baseline capabilities have been established, organizations can grow their SOC to leverage advanced data science, analytics, and shared intelligence to protect the digital enterprise more effectively.

Read more about building a successful SOC here:
Building a successful security operations center

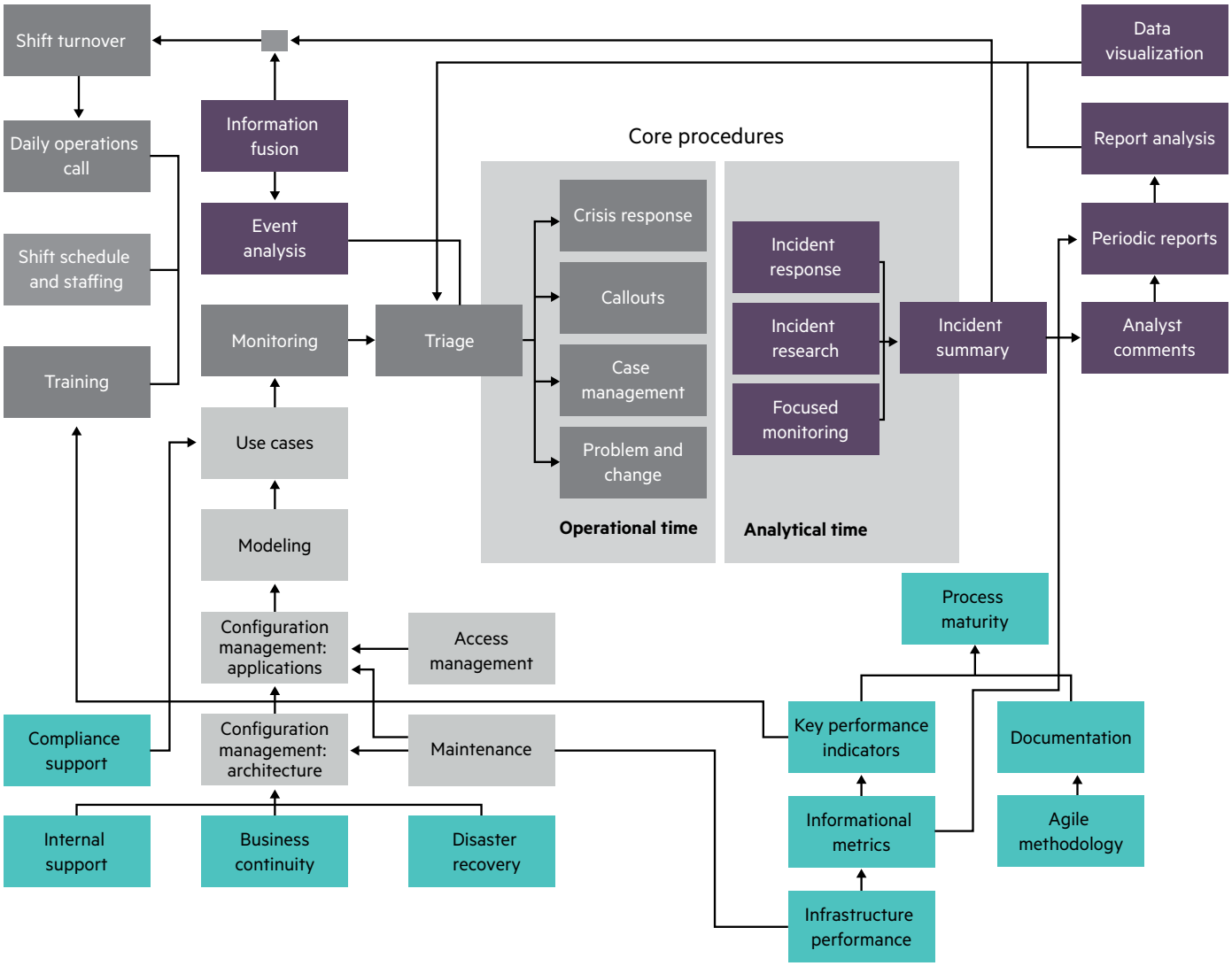

Figure 2: SOC procedure flow

Achieving the basics

A common mistake amongst new SOC implementations is trying to jump to advanced capabilities before solidifying the basics. The basics of a SOC should include (but are not limited to):

- Implementation of mission-critical use cases—three well-implemented use cases are better than 20 poorly implemented ones. For example, a successful login after numerous unsuccessful logins should raise a flag; a high severity intrusion detection system (IDS) alert against a critical system with a known vulnerability should be escalated; a user logged via LAN and simultaneously connected to VPN from a different geolocation should cause alarm; and more.
- For more information on implementing foundational use cases in HPE ArcSight, visit **hpe.com/software/activate**.
- Documented processes and procedures—including compliance requirements and escalation procedures.
- Critical roles filled within the SOC—including diverse skill sets (network, malware, applications, operations, management, etc.).
- Metrics and reporting of operations—including events per analyst hour (not including number of events consumed by a SIEM per hour).

The business needs to have confidence that the SOC is going to identify known attacks (at a minimum) and be able to mitigate them. The aggregation of numerous data sources is not considered a criterion of a successful SOC. Being able to identify threats in a consistent, repeatable fashion using the various data sources is a criterion of a successful SOC. Human analysis plays a huge role in the efficacy of this threat identification. Analysts consume information and alerts generated from SIEM technology and must make judgments whether a particular event constitutes a high-risk breach or is merely a false alarm. How this decision is made is vitally important to an organization's security program as it is the difference between swamping administrators with false alarms, missing critical alerts, and catching the real bad actors. Constantly understanding the context, changing "fingerprint" of the organization, and codifying that within the process are critical to keep false positives low, and make detection and response fast and effective.

Read more about how Hewlett Packard Enterprise uses a security analytics framework to identify and mitigate threats here: **Identify Threats Faster: Security Analytics Framework**

Overcoming staffing issues

The number one security concern enterprises have isn't a data breach, but a lack of skilled resources. The complexity of attacks and time to resolve sophisticated cyber-attacks leaves companies struggling to find the resources to respond. While vendors are continuously creating tools and technologies to strengthen our defenses, technology alone does not solve the problem. Most organizations are aware that they lack the experts to truly utilize the tools that they have invested in. In fact, that number is only poised to get worse as Forbes predicts that a full quarter of global cyber security positions will remain unfilled by 2019 due to a lack of qualified applicants.

Modern SOCs have to be creative when addressing this issue. Some security operations solutions include:

- Growing security expertise within the organization from resources with the right potential (can be faster and cheaper than hiring outside resources)
- Outsourcing operations and/or technology upkeep to managed service providers
- Insourcing resources on-demand as needed during SOC buildout, maturity projects, or to address unforeseen staffing needs such as mass attrition
- Tightening processes and procedures that reduce the skill sets needed to address specified security incidents
- Enhancing automation and orchestration tools to speed investigation and escalation of breaches

Read more on growing security analysts inside your organization here:
Growing the Security Analyst: Hiring, training, retention

Read more about combating the cybersecurity job crunch here:
Combating the cybersecurity job crunch

Maturing your SOC

Maturing your SOC means shifting your focus from specific technology to one that emphasizes on objectives and follows a systematic way to protect those areas that matter most to your organization. Once the foundation has been solidified in your SOC, then you can begin to mature it. The ideal level of maturity is the level 3 step described by the HPE Security Operations Maturity Model (SOMM)—well defined, subjectively evaluated, and flexible. Some areas should be rigid, repeatable, and measured while others should be flexible, agile, adaptable, and nimble. An overly rigid organization will not allow a SOC to adapt to the quickly changing threat landscape.

A maturing organization should assess its current capabilities and potential, and then put together a roadmap towards excellence. When improvements have been made, updated assessment should be performed to measure progress.

Some common opportunities for maturity include:

- Expanding the number of supported use cases in the SOC. Each additional use case should be tied back to a business need and measurable
- Increasing employee retention through education opportunities and career advancement paths
- Closed loop incident investigation and response that feeds back into the SIEM and other SOC processes
- Additional definition of processes especially in the technological, operational, and analytical areas

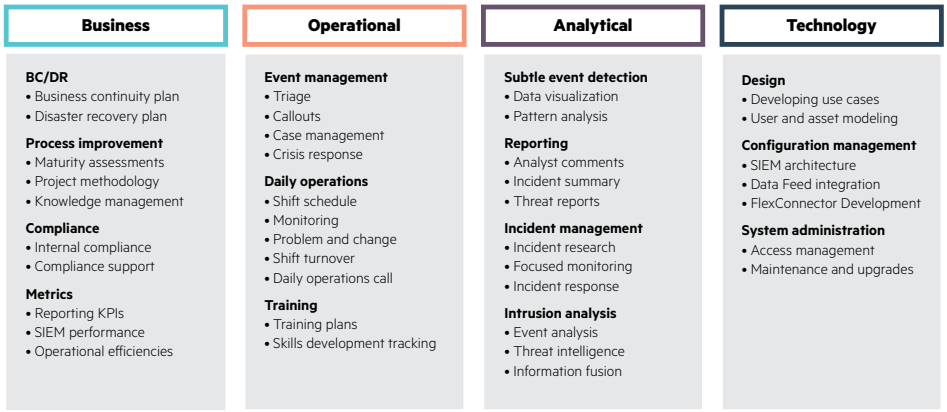

Figure 3: SOC processes and procedures

Every security operations organization differs in maturity and capability. It is hard to evaluate your own effectiveness and create a plan to increase your maturity. HPE Security Operations Maturity Assessment helps you determine your current maturity, as well as how you compare with other organizations in your industry and of comparable size. Based on our extensive experience in building and analyzing security operations, HPE Security Products Global Services consultants provide tactical recommendations and lay out a multiphase roadmap. This facilitates incremental levels of capability toward a long-term objective of establishing a mature and highly capable SOC.

Read more about the HPE SOMM and HPE assessments here:
Security Operations Maturity Assessment

Read more about the world's most mature SOCs here:
2016 State of Security Operations

Advanced capabilities of a SOC

Mature organizations are able to move into the realm of analytics-driven intelligent SOCs. These intelligent SOCs allow enterprises to move beyond detecting and responding to known attacks into the realm of identifying unknown attacks and anomalous behavior. Collecting large amounts of data is not useful by itself. A guiding vision and plan is needed in order to build systems that will grow with the business needs.

Business need should drive any analytics program. Use cases for the analytics program can include insider threat identification, early malware infection detection, inappropriate user access, etc. Collect only the data needed to meet these use cases that will reduce the noise in the environment and allow you to achieve your goals quicker. Utilizing existing analytics technologies can reduce or eliminate the amount of in-house expertise needed and ultimately reduce costs.

Organizations often find that they are able to begin with advanced analytics capabilities using tools that already exist in their environment. To learn more about how to start using analytics, read **Hunting today: Using your existing technology to hunt for cyber threats**

Proper SIEM selection and implementation as well as solid fundamentals allow organizations to smoothly transition into this world of analytics-driven intelligent SOCs. Shortcuts taken when building out a SOC or implementing limited featured SIEM technologies may require retooling to achieve this level of capability.

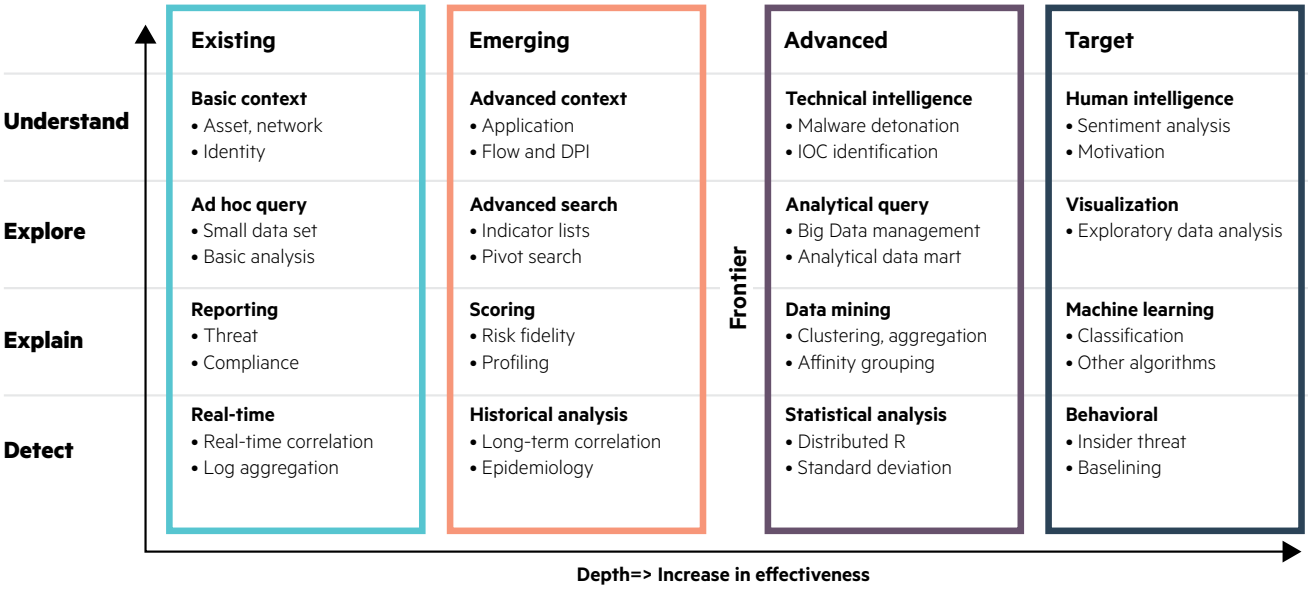

Figure 4: A vision for detection analytics

Read more about the future of cyber security analytics here:
A vision for cyber security detection and analytics

Read more about the HPE Attack Life Cycle use case methodology here:
HPE Attack Life Cycle use case methodology

Conclusion—the future of SOC

Creating and maturing a security operation capability can dramatically improve your organization's ability to rapidly detect and respond to malicious security events. Approaching the challenge across the full scope of people, process, and technologies will ensure the SOC is up to the task of identifying and remediating risks to the business and allowing it to grow confidently. Properly addressing the steps to create a successful security operations center will set you up to embrace advanced technologies and capabilities such as analytics and hunt teams.

Learn more at
hpe.com/software/sioc

Sign up for updates

Hewlett Packard Enterprise

4AA6-6440ENW, July 2016