TechTarget | SearchSecurity

E-guide

PRO+ Content

How-to Guide: Security Operations Centers

Your expert guide to finding the right SOC for your organization

In this e-guide

In this e-guide:

Security operations centers (SOCs) provide an important security support and response function to an organization.

Many SOCs evolved from the enterprise SIEM systems used to monitor environments and the people who monitor the logs. Today, managed security service providers and cloud services companies have been created to provide this monitoring service to enterprises or to supplement an enterprise's internal resources.

How do you know if an SOC is right for your organization?

In this e-guide, you'll uncover:

- **The benefit of SOCs to organizations**
- **How to improve the performance of your SOC**
- **How to find the right provider for your company**
- **And more**

In this e-guide

How security operations centers work to benefit enterprises

Ernie Hayden, Independent consultant & founder, 443 Consulting LLC - SearchSecurity

In his handbook, "Ten Strategies of a World-Class Cybersecurity Operations Center," Carson Zimmerman defines a security operations center as "a team primarily composed of security analysts organized to detect, analyze, respond to, report on and prevent cybersecurity incidents."

Security operations centers (SOCs) have also been called cybersecurity operations centers, computer security incident response centers and computer incident response centers, to name a few. Overall, their purpose is to provide an important security support and response function to the organization.

SOC organizations can range from one or two-person ad hoc operations to large national or international coordination centers that require major capital expenditures for specialized operations center rooms, video walls, and other SOC network and computing resources.

In this e-guide

The roles within security operations centers may include the following:

- Prevention of cybersecurity incidents through:
  - Threat analysis
  - Network and host scanning
  - Countermeasure deployment
  - Security policy and architecture advisory services
- Incident response
- Monitoring, detection and analysis of intrusions
- Situational awareness and reporting
- Threat research and digital forensics
- Compliance support
- E-discovery and legal evidence collection
- Security administration
- Security architecture and engineering

SOC framework: People, processes and technology

A popular model of the SOC framework is described in the SANS Institute whitepaper "Building a World-Class Security Operations Center: A Roadmap" by Alissa Torres. Her model shows the SOC building blocks as a triad of people, processes and technology, with people representing the most important element.

In this e-guide

A security operations center's staff includes the SOC manager, who is supported by an alert analyst -- tier 1 -- an incident responder -- tier 2 -- and a subject matter expert and hunter -- tier 3.

The processes component includes policies, standards, procedures and guidelines to direct the SOC team on such activities as identification of incidents/events, triage of incidents/events, containment, eradication, recovery and capturing lessons learned. Essentially, the processes element deals with the classic elements of cyber incident response discussed in NIST SP 800-61, "Computer Security Incident Handling Guide."

The technology component includes technical capabilities to monitor network traffic, collect and analyze system logs, capture threat intelligence feeds, detect incidents and gather forensics. However, these data feeds by themselves are not adequate to determine the size of a threat, whether it is a false positive or if it is a true attack.

Therefore, some tools -- such as security information and event management (SIEM) systems -- may be useful to analyze and sort the data related to flagged security incidents. However, they are still not complete without the human analyst and their review.

"There is no replacement for the human analyst," Zimmerman said.

In this e-guide

The concept of tier levels

The tier concept basically categorizes the capabilities, experience and basic duties of the various SOC analysts. As a parallel metaphor, when looking at the service desk concept from the Information Technology Infrastructure Library, the tier concept dictates the flow of requests for assistance from elementary -- tier 1 -- to intermediate -- tier 2 -- to expert support -- tier 3.

Tier 1: Alert analyst

Security analysts designated at the tier 1 level continuously monitor all alerts and tickets coming into the SOC. They also monitor security sensors and endpoints for alarms or unusual characteristics, review open tickets, close false positives, and conduct basic investigation and mitigation. The analyst triages security alerts and, if the alert reaches a predefined level or threshold per the SOC escalation policy, a case is created and the alert is escalated to tier 2.

Tier 2: Incident responder

Tier 2 analysts are more experienced security professionals who can perform a more thorough analysis of an incident. This can be done using threat intelligence feeds or by analyzing other similar cases or incidents. The tier 2 analyst then determines if any critical data or systems have been

In this e-guide

affected, and, if so, he or she will recommend and advise on a response/remediation.

Tier 3: Subject matter expert/hunter

A subject matter expert is just that, a highly trained and experienced security professional with expertise in advanced network forensics, intrusion detection and cyber incident response, as well as advanced training in anomaly detection.

SOC workflow

The SOC workflow is generally developed and enhanced over time as users gain experience responding to and resolving security events. Ultimately, the SOC workflow depends on the SOC team's head count and support structure. A typical workflow is described below.

Input

Input into the SOC begin with alerts, alarms and logs from antimalware systems; hosts and servers; intrusion detection systems and intrusion prevention systems; firewalls; VPNs; and data loss prevention systems. SIEM platform output can provide another compendium of information produced by security log analysis.

In this e-guide

Other input sources are calls and email alerts from users to the SOC regarding security concerns, such as unusual events on their workstations, possible phishing attacks or possible ransomware attacks. These calls may come directly from users or via the IT service desk.

Other sources of input include information from device administrators and submissions from the tier 1, tier 2 and tier 3 analysts.

Similarly, input from any threat management subscriptions or open source threat data will be fed into security operations centers for context and perspective. Even alerts from US-CERT, ICS-CERT and local Fusion Centers can and should be fed to the SOC team.

Visibility

The data sources listed above will ideally be consolidated into a situational awareness feed, such as a dashboard or a large status screen in the center. The dashboards can help the SOC manager and other analysts achieve and maintain a satisfactory big picture of the organization's security posture -- i.e., situational awareness.

Additionally, a ticketing system can provide a sense of security to the SOC team. Even simple lists or displays of the number of open security-related tickets by priority can help the team gauge the pace of attacks and security issues.

In this e-guide

Output

The SOC team's output will include ticket closures, feedback to other threat analysts on situations and solutions, and any cases where the SOC requires added resources and expertise.

SOC limitations

The biggest weakness of security operations centers -- as with all security systems and processes -- is that they cannot detect previously unknown threats and zero-day attacks. Therefore, to reduce this weakness, it is imperative that all signatures and security protection devices be kept up to date, patched and refreshed.

Analyst retention and burnout pose further risks to security operations centers. At the 2012 RSA Conference, Ben Rothke provided some excellent perspective on this issue during his session on the care and feeding of security analysts, who are key to the SOC's success. Rothke noted that good SOC analysts are hard to find and hard to keep. Hence, management needs to recognize that you "get what you pay for" and, as such, SOC analysts need to be nurtured with extensive training, bonuses, promotions, job rotation and management opportunities.

In this e-guide

The future for SOCs

The next step for security operations centers appears to be into the cloud.

One perspective being advanced is security operations center as a service (SOCaaS). In this case, the SOCaaS is a hired cloud service provider that collects system and event data and logs from other cloud-based systems. Theoretically, this can help customers outsource their SOC operations; however, it also enables increased scrutiny of the service and data flows. This approach is still in its infancy, and it does not offer the exciting view of the video walls and giant SOC facilities normally seen in advertisements.

Materials referenced in this article

"Ten Strategies of a World-Class Cybersecurity Operations Center" by Carson Zimmerman

The SANS Institute whitepaper "Building a World-Class Security Operations Center: A Roadmap" by Alissa Torres

NIST SP 800-61, "Computer Security Incident Handling Guide"

Next Article

In this e-guide

How SOC metrics improve security operation centers' performance

Nick Lewis, Contributor – SearchSecurity

To some, metrics are the holy grail of information security. Being able to monitor, measure and communicate the information security state of an enterprise can be powerful.

While some enterprises are still struggling with all of the metrics and the changing landscape of tools and processes used as data sources, one rapidly maturing area is security operations centers, where defining metrics has been a challenge.

In this tip, we'll take a closer look at security operation center (SOC) metrics and ways to improve an enterprise's security posture.

SOC metrics

Once enterprises realized that just looking at log data from their IT environment was insufficient, network operations centers evolved and dedicated security operations centers formed. Security operation centers

In this e-guide

can handle many different functions, like monitoring logs, responding to incidents and security administration, all coordinated via people, processes and technology.

Many SOCs evolved from the enterprise SIEM systems used to monitor environments and the people who monitor the logs. Managed security service providers and cloud services companies have been created to provide this service to enterprises or to supplement an enterprise's internal resources.

As SOCs mature, analytics and decision support are being included to drive more value for enterprises and to provide insight into how effectively security resources are being used. As SOCs continue to mature, the need for metrics and their supporting definitions is becoming more important, as is using the metrics to make changes and monitor the environment. Even defining what constitutes an incident is important, as not all security incidents have the same impact or require the same response.

There are several resources enterprises can use to learn more about security metrics, starting with the seminal book *Security Metrics: Replacing Fear, Uncertainty, and Doubt* by Andrew Jaquith. The Center for Internet Security, a nonprofit organization whose mission is to promote cybersecurity, also provides some guidance on security metrics. The SANS Institute offers several papers related to SOC metrics, and the NIST hosts

In this e-guide

the National Vulnerability Database, which provides metrics for tracked vulnerabilities.

As your enterprise determines your SOC metrics, you may also want to review the resources from the SANS Security Operations Summit from July 2018 and the SANS webcasts about their SOC survey.

When developing SOC metrics, identifying the highest value processes or areas that need the most resources can help identify where metrics and management attention may be needed the most. This can be part of continuous improvement and shouldn't be limited to how your SIEM or any particular tool is licensed or can be used.

With an outsourced SOC, it may be critical to set these metrics upfront and include them in a contract to ensure that the SOC can generate the data and support the required metrics.

Ways to improve an enterprise's security posture

The metrics for your enterprise will vary depending on the tools you use, the scope of your environment and your information security program. However, basic security controls can be mapped to the tools and processes to identify the potential metrics to use.

In this e-guide

Monitoring firewall alerts or failed logins alone may be useful if there is a sudden increase, and retaining that data for incident response is absolutely necessary. However, monitoring over time may not yield actionable information without correlation and analysis. For scoping, if you monitor firewall alerts in multiple locations in the network, then it may not be useful to report on a raw number of alerts because a network flow may generate multiple alerts or logs and only get blocked at one point.

Knowing what is included or excluded from monitoring with an SOC is something to be clear about. For example, if you have remote offices that occasionally have local servers, and those servers are not monitored by the SOC, then the metrics may not reflect all the servers in your environment.

Securosis, a cloud security company headquartered in Phoenix, Ariz., recommends focusing on use case categories such as security alerts, forensics, and response and compliance reporting. Each of these categories can be broken down into more detailed metrics, as well as the corresponding data sources or tools used to generate the metrics in the SOC.

Many SOCs monitor endpoint security tool logs and respond when high-risk malware is detected, so a metric could be built around those processes. Data generated in this process can be used to determine the costs required -- in terms of resources, as well as any financial costs -- to respond to an incident and how effective the response can be.

In this e-guide

You can track elapsed time at different steps in the process, starting from when the alert is generated, when an analyst begins investigating and when the analyst determines an incident actually began -- if it's different from the initial alert time -- to when the system is clean. Measuring each step can be useful to evaluate how effective each step in the process is and to potentially evaluate if changes need to be made to a process -- while keeping in mind that gathering this data requires additional resources.

Of course, the process becomes more complicated when multiple systems are included in a single incident or when sensitive data is involved. Having an analyst validate when an incident began should be part of checking the effectiveness of an endpoint security tool.

Measuring the effectiveness of such a tool must take in all the aspects of its performance. For example, consider how long it takes to determine if something malicious happened, if the tool is able to capture the start of an incident and the detection time, or if a different tool detected the incident. These factors could signal a need to study the tool's effectiveness, configuration or usage to ensure the protection of your enterprise.

This metric can also be rolled up into incidents per analyst, incidents per machine or incidents per scope and analyzed over time. Similarly, tracking the time to recover a system from a malware attack can be analyzed to determine whether it is more cost-effective to use an automated reinstall or

In this e-guide

restore from a backup or a known-good state rather than manually cleaning an infected system.

Information security is rapidly changing, and it is continuing to evolve to drive more value for enterprises. As SOCs also continue to evolve, their importance to the enterprise is increasing and helping to drive more improvements to enterprise information security programs and improve the security posture of companies.

However, these improvements will require enterprises to use data gathered from SOCs to create the metrics that will drive this change. While this data will differ based on the tools and the scope, focusing on the highest value systems or processes can provide a starting point that can extend to the rest of the enterprise.

Next Article

In this e-guide

Peer into current and future security operations centers

Kathleen Richards, Editor – *Information Security* magazine

Many organizations are experiencing a rise in security threats. But the talent and tools to investigate the growing number of security incidents -- or worse, previously unknown threats -- continues to be a problem that weighs on senior security staff. A security operations center can help analysts tasked with investigating security incidents monitor the bigger picture by providing services including threat intelligence, scans of systems and devices that address vulnerabilities and timely patch management.

Yet many organizations find that a security operations center is difficult to implement and even harder to staff. Finding trained SOC analysts, especially individuals who have the unique combination of talents required to detect and prevent unknown threats, is another challenge. Elevated security events at many companies are still handled by either an overburdened IT staffer who specializes in security or an ad hoc team that may not have the skills to take advantage of data analysis and visualization tools. Many security operations centers also rely on some manual collection of key performance indicators by analysts who compile SOC metrics.

In this e-guide

The lack of information sharing by internal teams is another area that remains a struggle. According to a 2017 SANS Institute survey, 60% of respondents said their organization had combined the security, remediation and response functions into a single security operations center, but only one-third said their organization's SOC coordinated information with the network operations center.

Integration of tools and automation of prevention, detection and response can help SOCs in the future, but technologies alone cannot replace highly trained security analysts. Some SOC functions can be outsourced, but management and strategic planning to align security operations with business goals should remain in-house.

Next Article

In this e-guide

SOC services: How to find the right provider for your company

Steven Weil, Information Security Director and Cybersecurity Principal Consultant – Point B

As organizations face ever more threats and attacks to their information systems and data, they are increasingly considering setting up security operations centers to centrally manage their detection and management of cybersecurity incidents. Properly implementing a SOC is often a complex undertaking, requiring significant time, money and staff. Plus, organizations can face challenges such as SOC talent shortages and inability to scale. As a result, many businesses are exploring outsourcing some or all of their SOC services to third-party companies, known as SOC service providers.

This article is designed to help you understand which features you should look for as you look to find the appropriate SOC for your organization.

In this e-guide

What a SOC is

A SOC is a set of people, processes and technologies, often centralized, that -- at a minimum -- receives and analyzes user reports and data feeds -- logs, for example -- from information systems and cybersecurity controls. Typically, the primary goal of a SOC is to detect and prioritize cybersecurity incidents that could negatively impact an organization's information systems or data.

SOCs vary from organization to organization and are implemented per structural cybersecurity priorities and risk tolerance. Some SOCs will manage an incident from detection to remediation; others will focus on supporting and coordinating incident responders and handling incident response communication -- e.g., status updates and third-party communication.

Each organization must implement SOC services that are appropriate and reasonable for it.

In this e-guide

How a SOC works

SOC employees and technologies are typically located in a central location that employees with different levels of expertise -- such as analysts, responders and hunters -- staff 24/7 year-round. SOCs tend to be very process-driven: They have standard operating procedures, use cases and play books to define how SOC staff respond to and communicate about various cybersecurity events and incidents.

In addition to real-time analysis of user reports and data feeds, SOCs can also provide the following:

- long-term analysis of data feeds and incident data;
- normalization and storage of security logs;
- creation and dissemination of threat intelligence;
- automation and orchestration;
- threat assessment; and
- vulnerability detection or management (e.g., vulnerability scanning and remediation).

Organizations may consider outsourcing all or some of their SOC services to a SOC service provider for one or more of the following reasons:

- an inability to hire enough SOC staff with necessary skills;

In this e-guide

- the desire to gain better value from existing cybersecurity products by having experienced specialists manage them;
- a requirement to quickly expand SOC services due to changes in an organization's threat landscape or business model (e.g., adding e-commerce);
- a preference or requirement to use cybersecurity budget dollars for operating expenses ("renting" SOC services) rather than capital expenses (buying SOC equipment and hiring employees);
- the ability to apply a third party's threat intelligence gained from monitoring many customers; and
- a strategic decision to have simpler, repetitive tasks like initial log reviews be performed by a third party so that SOC staff can focus on high-level tasks, such as incident response or vulnerability management.

For all of the above reasons, the expectation is that the SOC service provider will be able to provide specific SOC services more effectively or less expensively than the organization itself.

In this e-guide

Features to look for

SOC vendors can provide the following:

- monitored or managed firewalls or unified threat management technology;
- monitored or managed intrusion detection systems (IDSes) and intrusion prevention systems (IPSes);
- managed or monitored web and email security gateways;
- monitoring or management of advanced threat defense technologies;
- triage and short-term analysis of real-time data feeds (e.g., system logs and alerts from applications and information systems) for potential cybersecurity incidents;
- long-term analysis and correlation of data associated with monitored or managed devices and incident response;
- managed vulnerability scanning of information systems and applications;
- monitoring or management of customer-deployed SIEM technologies; and
- current and relevant threat intelligence.

As the above list makes clear, SOC service providers offer many capabilities that could be useful for your organization's SOC. But the variety of services can be overwhelming. One way to start evaluating SOC providers is with two basic steps to identify those services of most value for your company.

In this e-guide

First, identify cybersecurity controls (firewalls, IDS/IPS and so on) that your organization has already implemented but are not being effectively used, either because there are technical challenges or because your team lacks the expertise required. Second, identify services that your organization wants (such as threat intelligence) but cannot effectively implement due to lack of qualified staff or inability to reach necessary scale.

Be sure you're effectively managing and monitoring your existing cybersecurity systems before signing up for advanced services like threat intelligence. For instance, it will be difficult to reap the benefits of threat intelligence if your organization doesn't already have a good understanding of what's happening on its cybersecurity systems.

A key decision you should be prepared to make is whether to have a SOC service provider only monitor (for example, receive logs from some or all of your organization's cybersecurity systems) or also manage certain cybersecurity systems (such as firewalls or SIEMs). Your organization's security policy and risk tolerance will determine this.

Using a SOC service provider can lighten the load on your organization's SOC, but your company will still need to define and assign program-management resources to keep the SOC vendor on task and to evaluate its ongoing effectiveness.

In this e-guide

Regardless of what services you choose from a SOC service provider, look for the following functional features:

- The SOC vendor should provide a customer web portal that has multifactor authentication and role-based access control. The portal should provide analytics and visuals, real-time updating, SOC service provider ticket status and reports that can be customized for different types of users -- executives, SOC personnel and so on.
- The vendor should be able to provide requested services 24/7 year-round, offer multiple communication methods -- such as phone and email -- and have proven experience quickly escalating significant events and incidents to appropriate customer staff.
- The SOC services should integrate into your organization's security incident response plan.
- The SOC should provide requested services from at least two geographically distributed sites to ensure redundancy and ability to recover from a disaster.
- The SOC service provider should have staff certified for the significant cybersecurity technologies they are monitoring or managing at your organization.
- If necessary for compliance, verify that a SOC service provider can guarantee that requested services are only provided from specific (e.g., US-based) locations.

Choosing to use a SOC service provider is an important business decision; you want to have a strong, trusted partner, so look for key business features, such as evidence that the provider is financially stable and has a

In this e-guide

strong customer-retention rate. The SOC provider should offer guaranteed performance-based service-level agreements that include the ability to terminate service in the case of poor performance. Naturally, the provider should have proven experience and expertise in your specific industry. Also, you should be able to reasonably customize provided SOC services; your organization shouldn't have to force itself into a one-size-fits-all service. Using a SOC service provider will likely involve sharing sensitive data or giving the provider access to some of your organization's information systems. In order to prevent cybersecurity incidents and compliance gaps, require the following security features at a minimum:

- The SOC service provider should allow your organization to perform due diligence on their cybersecurity practices. For example, you should be able to add a right to audit cybersecurity practices clause in your contract with the service provider and require them to complete a cybersecurity practices assessment questionnaire.
- The SOC service provider should have a third-party cybersecurity audit plus internal and external penetration tests performed at least annually.
- The SOC service provider should be certified in at least one recognized cybersecurity standard -- e.g., PCI DSS, the Federal Risk and Authorization Management Program and ISO 27001 -- and have an SSAE16 (Statement on Standards for Attestation Engagements 16) assessment performed regularly.
- The SOC service provider should be able to receive and send data to and from your organization via encrypted methods, like TLS 1.1+.

In this e-guide

Bottom line

Properly implemented and managed, outsourced SOC services can be an important part of your business's cybersecurity program; partnering with a service provider can be a smart way to efficiently and effectively improve your organization's security operations center. Be sure to carefully evaluate SOC service providers so that you end up with the right services for your company.

About SearchSecurity

In this e-guide

About SearchSecurity

IT security pros turn to SearchSecurity.com for the information they require to keep their corporate data, systems and assets secure.

We're the only information resource that provides immediate access to breaking industry news, virus alerts, new hacker threats and attacks, security certification training resources, security standard compliance, webcasts, white papers, podcasts, Security Schools, a selection of highly focused security newsletters and more -- all at no cost.

For further reading, visit us at https://searchsecurity.techtarget.com/

Images; Fotalia