

WHITE PAPER

Improving Security Operations Center (SOC) Efficiency

An examination of core SOC responsibilities and design considerations with actionable guidance to enhance efficiencies

Contents

What Is a SOC? 4

The SOC Operating Model 4

The Four Primary Tasks of SOC Teams 5

Challenges Facing SOCs Today 6

Four Tips to Improve SOC Efficiency 7

Map & Rationalize Security Processes 7

Simplify & Streamline Communication 8

Deploy Smart Integrations to Address Tool Sprawl 8

Emphasize Control Validation & Attack Simulation 10

SOC Efficiency Is a Never-Ending Process 11

Introduction

Cybersecurity teams are in a constant race against time. **The Ponemon Institute's 2021 Cost of Data Breaches study** found that security organizations take 287 days on average to detect a breach and more than a month to contain it. The number of common vulnerability and exposures (CVEs) continues to grow, with **2021 setting another record** for published vulnerabilities—malicious hackers race to create viable exploits for these vulnerabilities as soon as they are released.

For example, on May 4, 2022, the security and networking company **F5** issued a security advisory warning about a vulnerability that could allow unauthenticated attackers with network access to execute arbitrary system commands, perform file actions, and disable services on the company's BIG-IP load balancers. Less than a week later, attackers **used the vulnerability in a live exploit**. A similar **VMWare vulnerability was exploited** by attackers less than a week after release. This is not an anomaly. In addition, CISOs are struggling to hire enough engineers. According to **research by (ISC)²**, the cybersecurity workforce will need to increase by roughly 65% to provide sufficient coverage for enterprises and governments.

To surmount these challenges and keep up with the rapidly evolving threat landscape, an organization must constantly strive to improve the efficiency of its security operations. This means carefully designing a security operations center (SOC) model and consistently identifying ways to improve detection and response time, prioritization, and security posture. In this paper, we'll provide a high-level overview of a SOC and its responsibilities, outline different SOC design considerations, and identify areas where most organizations can improve efficiency.

80%

of exploits appear
in public faster than
their accompanying
CVEs.



What Is a SOC?

The SOC is designed to protect a company from security breaches by quickly and efficiently identifying, analyzing, and responding to security threats. Until the past decade, a SOC was a physical room or command center where the different members of a security team worked. This may have included both physical and cybersecurity teams, composed of security analysts, security engineers, and individuals responsible for security operations, blue-team activities, and DevSecOps. While also part of the security team, red-team members usually work elsewhere due to their adversarial role.

Due to high operating costs and the challenges of building the instrumentation and management planes for security operations, only large enterprises had SOC until the past decade. Today, many mid-sized organizations now invest in small SOC due to the wide acceptance of the SOC operating model and the rise of open source and other tooling to automate and streamline many SOC operations. A growing number of organizations opt for virtual or hybrid SOC to enable better global coverage and to accommodate high-skill workers who prefer to work from home some or all of the time. Some enterprises also outsource SOC operations to managed security services providers who leverage institutional knowledge and economies of scale to protect multiple enterprises using the same set of tools and security teams.

Virtual, physical, or outsourced, the SOC serves as the unifying element that combines all the information and resources necessary to improve performance and enhance data sharing within an organization. Because the work of a SOC now takes place primarily in the digital realm, opportunities for greater efficiency require the careful and conscious design of workflows, data sharing, and collaboration.

The SOC Operating Model

The SOC is the tip of the spear for an organization's security strategy, but it also contains a number of subsystems that must be thoughtfully designed and coordinated. In addition, the SOC must work closely with other teams including IT, HR, legal, compliance, and finance. In some instances, SOC are co-located with network operations centers due to the overlapping responsibilities and the integral role that network security plays in security posture.

To improve efficiency and enhance collaboration between the SOC and other units within an organization, it's important to first understand the SOC's key responsibilities.

The Four Primary Tasks of SOC Teams



Testing and validating security controls and security posture fidelity

This is the responsibility of the blue team, the vulnerability management team, and sometimes security engineers.



Investigating indicators of compromise (IOCs) or suspicious activities

The incident response team (often the blue team) investigates suspicious and malicious activity within networks and systems.



Maintaining security tools and controls

This is typically handled by security engineers, who work to constantly tune controls to reduce security drift and block new attacks. They also help facilitate patch management efforts.



Analyzing potential threats to inform strategy and tactical approaches.

This is the task of the threat modeling and security intelligence team.

These four buckets of security team tasks can be broken down further.

Threat modeling and intelligence. This proactive task bucket enables security teams to assess threat trends and apply more specific testing against scenarios likely to be invoked by specific threat types and threat actors against their organization or specific vertical. These tasks overlap with other disciplines, especially breach and attack simulation (BAS).

Vulnerability and risk management. This is the process of identifying vulnerabilities on devices, endpoints, and systems and rating the business or technological risk of each to prioritize remediation. While the responsibilities within this bucket may not include scanning for vulnerabilities, it does require results of scans and other detection activities applied to devices, software, systems, networks, and infrastructure.

Control validation and posture verification. This is both a proactive and reactive responsibility, shared by multiple teams. Red teams test security controls as part of their adversarial exercises. Blue teams, security engineers, and vulnerability management stakeholders all participate in this activity, as well. Many cross-functional security teams now rely on BAS solutions to continuously and programmatically test security controls against known attacks.

IOC Data acquisition and triage. SOC teams collect and correlate log file data from various systems (e.g., security information and event management [SIEMs], individual security controls) and parse those files for IOCs or other security events. They also provide tools that allow analysts to review that information and detect relevant security events.

IOC prioritization. Security analysts correlate alerts across multiple tools, prioritize them, and decide which events represent false positives versus real security incidents.

Remediation. If an incident is discovered, one of the teams in the SOC spearheads efforts to clean and patch affected systems and reconfigure controls to block similar incidents in the future.

Revalidation. Once a patch has been deployed or a security configuration updated, security engineers or blue-team members often retest the updated security control to ensure it can adequately detect/prevent the threat. This also provides the SOC an opportunity to determine if the configuration fix has caused any changes to other deployed security controls. Security teams heavily leverage BAS tools to revalidate configuration changes and ensure a hardened security posture.

Postmortem and reporting. To be effective, a SOC must be a learning organization and document incidents to add them to databases for future study. An incident postmortem and forensic analysis is useful to ensure that lessons learned are internalized and properly acted upon in the future.

Response orchestration and automation. More modern SOC's increasingly incorporate automated incident response capabilities, often handled by security orchestration and automated response (SOAR) solutions. This can include multi-stage and concurrent actions triggered by detection of IOCs or other activation actions. Automation and orchestration capabilities allow security teams and SOC's to move quickly and better protect the increasingly convoluted and sprawling attack surface across on-premise, hybrid, and virtual infrastructure and systems.

Challenges Facing SOC's Today

SOC's today face a variety of critical challenges that can impact their efficiency, including:

- Increasing “noise” from higher volumes of security alerts (and false positives)
- Difficulties identifying and prioritizing remediations that matter most
- More complex and diverse attack surfaces
- Faster exploitation of released vulnerabilities
- Increased sophistication of cyber attackers
- Security tool sprawl and an inability to orchestrate tools effectively
- Poor communication and collaboration across team functions
- Siloed information sources and tools within security teams and among related departments (e.g., IT, network operations, compliance)
- Difficulties in hiring and maintaining experienced security staff
- Employee burnout from an ever-increasing list of responsibilities amid chronic understaffing

Four Tips to Improve SOC Efficiency

To keep up with attackers, organizations operating SOCs need to address these sources of inefficiencies from a “design thinking” standpoint that takes into account the jobs to be done and leverages modern cybersecurity solutions to reduce, rather than increase, complexity. This exercise should help identify ways to reduce repetitive manual tasks across all SOC roles.

In particular, SOC leadership should look for ways to automate or eliminate manual, point-in-time testing of controls and configurations, allowing security team members to refocus on higher-value work that requires creativity and reasoning. In the sections below, we provide several guiding principles and recommendations to help SOC leaders design processes and team activities for intentional enhancement of efficiency.

Map & Rationalize Security Processes

Security processes are the guidebook to more effectively working as a team, and technology can help streamline these processes. Understanding the processes and potential bottlenecks can also highlight areas for automation and workflow modification.

To begin, SOC managers and CISOs should:

- 1. Identify all key security processes.** Begin by understanding the types of processes you have beginning with the most critical, such as intrusion detection, data loss prevention, incident response, and security control validation.
- 2. Create visual process maps.** Identify and map the proper sequence of all major processes and related sub-tasks. Security process maps need to be clear, visual, and easy to understand. This will also simplify onboarding of new employees and bringing new members of the security unit up to speed.
- 3. Identify tools and stakeholders.** For the processes and sub-tasks identified above, document the tools required to carry out those processes and the stakeholders responsible for managing each task and tool.
- 4. Determine areas for automation.** Identify which sub-tasks can be automated/semi-automated (e.g., ticket creation, IP lookups) and where information-sharing across tools would improve performance.
- 5. Establish key metrics.** Discuss and decide on metrics that can be used to measure the success of each process. This will help establish benchmarks, track ongoing progress, and identify processes in need of further refinement.

Once established, these security maps can serve as the source of truth about how members of the SOC team should work together to accomplish repeated tasks. They can also serve as a roadmap to provide guidance about the most impactful ways to integrate, collaborate, and continuously improve SOC processes and operations.

Simplify & Streamline Communication

Good communication is the currency of all team activities—teams that communicate well usually perform well. In security, time is of the essence and there is little room for confusion. However, communications can be complicated when they are spread across different work environments or tools (e.g., email, chat, comments on alerts in a SIEM) that require team members to sift through communications across a variety of channels to identify the information they need. These types of communication miscues can lead to errors, duplication of tasks, and diminished performance when critical information is not shared in a timely fashion. This problem has become increasingly more acute with the proliferation of remote teams and work-from-home arrangements.

To simplify the SOC team's communications, SOC managers and CISOs should:

- 1. Select a primary communication tool.** A single tool should be chosen that the entire SOC team can use for real-time and chat-based communication. Different parts of the SOC team can have unique or private sub-channels, but they must easily be able to share information with others in the same tool.
- 2. Identify the key communication types.** Document the different types of communications needed and the stakeholder responsible for those communications. For example, determine different communication formats, templates, or requirements for configuration changes, low-priority issues, high-priority issues, and metrics reporting to the larger organization and C-suite.
- 3. Decide what communications belong where.** Identify which types of communication should be conducted in the unified environment selected above. Next, decide if there are unique types of communication that may require a different channel. For example, communications around incident response and acknowledgement of a breach may require a formal notification to compliance teams via email, while monthly metrics for company leadership might be best communicated as a shareable business analytics dashboard (such as Tableau) or a report in Google Sheets.
- 4. Create a visual communications map.** Just as you mapped out processes, map out the types of communications needed, the responsible stakeholders, and the designated channels for each form of communication. Again, these maps need to be clear, visual, and easy to understand to aid in employee onboarding and ensure consistent use.

Deploy Smart Integrations to Address Tool Sprawl

A modern cybersecurity organization has dozens of security controls and likely a handful of security management and orchestration platforms. Some of these controls, such as network load balancers, may nominally live outside of the security operations team. Others, such as IT asset management, may be primarily tasked with IT jobs, but are still essential for vulnerability management, compliance, and incident response because it contains information about who controls what assets, where assets are located, and what the security status of assets is. To alleviate this sprawl, many SOC teams have adopted either SIEM and/or SOAR tools. Many popular enterprise SIEM and SOAR solutions have marketplaces and pre-existing integrations with hundreds of security controls.

That said, integrations need to be properly tuned to avoid information overload. Successful integrations require the following:



Accurate data signals

If a security scanner consistently reports false positives or false negatives, or a logging tool is misconfigured to report incomplete information, integrations can create more work and amplify existing pain points



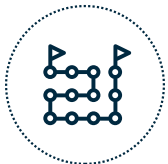
Simple, clear query capability

A critical part of integrations, as well, is to ensure that the team can more easily query information and test hypotheses.



The ability to correlate tests with affected endpoints, systems, or IPs

In IT environments where tens or hundreds of thousands of assets are managed and secured, SOC teams can struggle to map every IOC instantly to the relevant endpoints and systems. Having instant real-time correlation accelerates root-cause analysis and triaging, improving efficiencies. Smart integrations with logging tools and log analyzers are critical for enabling this correlation and distributing that information in real-time into the SIEM or SOAR.



Establish an integration roadmap

It is recommended that at least one SOC member be tasked with planning, managing, and monitoring integrations. A simple checklist for integrations might include:

- ❑ Collaborating with the entire SOC team to create an integration strategy prioritizing integrations and roadmapping integration execution.
- ❑ Creating and maintaining a list of all potential and actual integrations, along with links to accompanying documentation and APIs.
- ❑ Running regular tests of integrations to ensure they are working as intended—especially if any of the solutions or software have been versioned or patched.
- ❑ Updating a team “integration bible” on a quarterly basis to ensure that all integrations and processes around integrations are clearly documented in case of staff turnover or other unforeseen circumstances.

Emphasize Control Validation & Attack Simulation

SOCs have traditionally organized around the activities of incident response, intrusion detection, and remediation. For control validation, they have leveraged tools like penetration testing and red-team exercises, which are manual exercises conducted sporadically, and vulnerability scanning, which is primarily focused on identifying unpatched security vulnerabilities, rather than mimicking real TTPs and playbooks.

New BAS tools are changing that by making it possible to continuously run simulations of thousands of attack types customized to mirror relevant threat actors. The most modern BAS systems can actually run against production environments in the cloud and on-premise around the clock without requiring manual guidance and without compromising their performance or posing any threat to them. Because these systems can validate controls at scale, they provide a proactive strategy that is far more powerful and effective than reactive approaches. Only BAS can test multi-stage playbooks and sophisticated attacks as code, at scale.

SMART BAS SOLUTIONS CAN IMPROVE SOC EFFICIENCY IN A VARIETY OF WAYS BY:

- Easily integrating with SIEM/SOAR, vulnerability management, and other SOC staple tools to enable teams to continuously identify configuration gaps and prioritize unpatched vulnerabilities
- Increasing the value of all the other security tools by keeping them honest and by unifying and correlating testing results into a single BAS solution
- Improving team communication and coordination by simplifying reporting and research
- Automating the creation and collection of reports on control efficacy and status, providing an easy way to build SOC metrics to track security drift, security gap exposure, and remediation rates
- Automating and continuously running attacks to allow security team members to focus on higher-value work that requires creativity and reasoning
- Visually analyzing results of attacks to identify security gaps
- Receiving and prioritizing remediation for those gaps before attackers find them, and testing remediation effectiveness autonomously

SOC Efficiency Is a Never-Ending Process

Modern SOC's are complex environments with dozens of tools, overlapping teams, and greater diversity of devices, endpoints and infrastructure to protect. As more computing moves to the cloud, infrastructure continues to atomize into more and smaller siloed applications and systems for networking and IT, and as security talent becomes more difficult to acquire, the complexities facing SOC teams will continue to grow.

Taking a systematic approach to improving SOC efficiency is crucial to keep teams engaged, inspired, and focused on the work that matters most. For CISOs, this means ensuring that underlying processes and workflows are optimized to reduce manual tasks, share information wisely and comprehensively, and emphasize proactive approaches that address risk sooner rather than later.

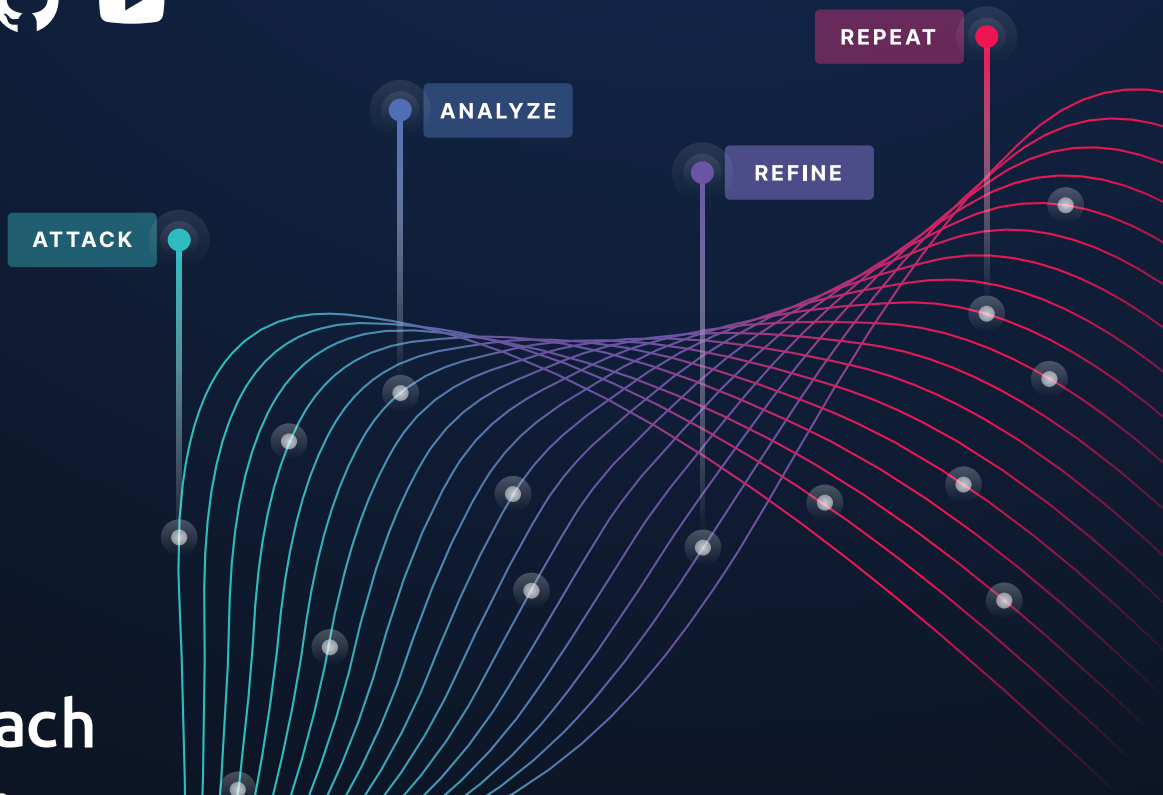
It also means leveraging the best and latest tools, like BAS solutions, to proactively validate security controls at scale. Check out [SafeBreach.com](https://www.safebreach.com) to learn more about our pioneering BAS platform and [schedule a personalized demo](#) to discover how SafeBreach can enhance the efficacy of your SOC team.

About SafeBreach

Combining the mindset of a CISO and the toolset of a Hacker, SafeBreach is the pioneer in breach and attack simulation (BAS) and is the most widely used continuous security control validation platform.

SafeBreach continuously executes attacks, correlates results to help visualize security gaps, and leverages contextual insights to highlight remediation efforts. With its Hacker's Playbook™, the industry's most extensive collection of attack data enabled by state-of-the-art threat intelligence research, SafeBreach empowers organizations to get proactive about security with a simple approach that replaces hope with data.

Learn more at [SafeBreach.com](https://www.safebreach.com).



All content ©SafeBreach 2022.
All rights reserved.