WHITE PAPER

Seven Steps to Ease the Pain of Managing a SOC

Seven Steps to Ease the Pain of Managing a SOC

If the complex, stressful, and time-consuming nature of running a security operations center (SOC) is getting you down, it's time to re-evaluate your strategy.

Running a security operations center (SOC) requires staying ahead of threats, whether you head a vast army of security professionals or operate as a one-person band. Reassessing your strategy and operations in a few critical areas can be all it takes to stay on track. As threats mount, expand, and increase in complexity, velocity, and frequency, this checklist can be utilized to turn chaos into order and confusion into confidence.

Seven Steps SOC Managers Should Take Now

1. **Have a plan: Create a comprehensive strategy for correlating and prioritizing alerts.** McAfee® research indicates the average time to detect and contain advanced threats is 39 hours.[1] As SOC managers juggle the realities of increased threats, shorter attack timeframes, and tight security resources, developing a methodology for dealing with alerts is essential. There are a number of publicly available methodologies for alert correlation and prioritization, such as Mitre Corp.'s Adversarial Tactics, Techniques, and Common Knowledge framework for understanding and defending against threats.[2] SOC managers need to look at attack indicators that go beyond common malware, such as persistence, privilege escalation, or lateral movement threats. Threat management featured in a security information and event management (SIEM) solution can help you set up baselines, rules, watchlists, and alarms to focus on the most important and riskiest threats.
2. **Get the right context: Develop a decision matrix for convicting threats.** This should be done as a collaborative effort among IT, security, and business stakeholders in order to properly evaluate and categorize risk. Which threats warrant simple monitoring, and which ones need to be elevated to detection, deletion, or disruption? One of the key variables is asset value. What would happen to the business if a specific server, application, or host were taken down and/or destroyed? What sort of information might that asset contain, and what type of attack would be used to penetrate that asset's countermeasures? Knowing importance and

Connect With Us

relevance to attack forms can help prioritize actions and inform decisions. Some enterprises put together a formal "attack chain" that provides a methodology and process for deciding what course of action to take—from detection to outright denial of a threat. But the attack chain also needs to be aligned with a security tool set, so organizations are ensured that they have the right tool in the right place at the right time for the right response. For instance, a standard antivirus tool will often be suitable for commodity malware and exploitation management. But once you identify the presence of a more advanced threat, you need processes and tools in place to quickly analyze scope, provide containment, and eradicate a threat with defined decision processes for threat mitigation.

3. **Set the right kind of alerts: Know how to scope and contain threats before they become a breach.** Once you understand how an adversary is likely to attack you, it becomes easier to create policies, rules, and responses that sift through all those false positive alerts in order to pinpoint true threats. By anticipating attacks, you create an understanding of possible motivations. For instance, advanced persistent threat (APT) actors often don't want to destroy your network; they want to continue to have access to it. Hacktivists, on the other hand, want the notoriety of the attack—they will claim responsibility, brag about it, and possibly disrupt and/or destroy your systems. Your alert systems should reflect these and other motivations so you can triage threats before they take hold.

4. **Listen to your malware: Learn from the indicators you encounter.** Modern tools can detect the zero-day and targeted malware used in an APT by detonating and analyzing the malware to reveal the attack from indicators within. This data can be used to update and inoculate systems to prevent the attack from maintaining a foothold. Taking these indicators and hunting them in your environment will also help you track down systems that may be associated with an ongoing attack.

5. **Turn insight into action: Correct problems quickly across the full scope of the enterprise.** Think of this as a continuum or a lifecycle: the ongoing challenge to protect, detect, and correct. Part of what you learn from an attack should help you focus on identifying and fixing the root causes of systemic problems, such as the appearance of familiar vulnerabilities with known exploits. It's important to work with your business users as well. For example, certain users may be using Word documents with macros, and their systems may be constantly getting exploited. Yet, the users may not allow you to quarantine those files. In that case, the best thing to do is to go back to the business unit and explain why security is essential for the security of their systems. Have the numbers that explain the impact to show the relevance to protection. If you can't protect them, then make sure you can detect and mitigate exploits as fast as possible.

6. **Simplify now and for the future: Automate against future attacks.** As security threats expand and threat vectors spread, it's understandable that SOC managers are clamoring for more help in the form of larger staffs. But that isn't happening. Computer Economics notes that spending on security staffing within overall IT budgets has remained flat at 2.6% since 2011.[3] That means that SOC managers need to adopt higher levels of automation in order to keep up with growing threats, respond to events more confidently and quickly, and allow existing IT security staff to play a more strategic role in the creation and delivery of new services. Two starting points are automation of low-risk actions and workflow tasks (such as submitting a file for analysis or clearing a browser cache), followed by automation of several tasks into an approved process that can be initiated by a responder or administrator. Security consultant David Bianco created and popularized the "Pyramid of Pain" concept, which prioritizes indicators that can be addressed most easily through automated responses, starting with hash values, IP addresses, and domain names.[4] These "less painful" indicators of an adversary's activities are the easiest to respond to, thus denying their use to intruders looking to break into systems. Indicators that change frequently are key targets for automated response within the SOC framework. Once you automate removal of, say, hashes, you can continue to move up the pyramid and apply additional automation steps and spend more time developing better, higher-fidelity indicators.

7. **Do the important things consistently well over time.** It's essential to find leverage points where you can repeatedly address key issues without having to reinvent the wheel every week. For instance, be sure to document recurring use cases and their methodologies. This will help bring new staff members up to speed faster and let them begin solving problems right away. You're always going to have staff rotation, and you don't want to lose institutional memory every time someone leaves. This often requires an investment in knowledge management processes so security risk identification and resolution steps are catalogued and indexed. Process and workflow automation contribute to efficiencies here as well, reducing the uncertainty about which actions to take in which order.

Putting in Place the Right Processes and Tools for SOC Managers

Without the right processes and tools, SOC managers are fighting a losing battle as they struggle to investigate and fully comprehend the nature, scope, and details of a potential attack. Look for tools that create measurable outcomes, like the reduction of dwell time or reduction of malware events. These automation tools are essential to any SOC manager's ability to stay ahead of the curve, prevent and detect threats, and correct incursions as quickly as possible.

SOC managers too often have to sort through a maze of disparate tools and technologies from a wide array of security solutions vendors, forcing them to reconcile integration issues such as compatibility, visibility, and, in particular, management. That's a big reason why many SOC managers choose to work with security technology vendors that offer a comprehensive, integrated set of solutions optimized for real-world SOC challenges.

SOC managers should evaluate solutions and technology partners on the basis of three key principles in order to become less reactive and more proactive:

1. An integrated process incorporating protection, detection, and correction that produces measurable outcomes
2. A centralized, real-time visibility and management layer
3. A solid, reliable, and scalable framework that can be expanded seamlessly and cost efficiently as conditions require

McAfee Solutions for the SOC

McAfee's open and connected security system provides a proactive set of security defenses that work across the data center, endpoints, physical and virtual network infrastructures, and cloud computing architecture. One of the key benefits in working with McAfee is its ability to craft tightly integrated, optimized solutions to address multiple challenges in a centrally managed, cost-efficient manner. SOC managers can overcome challenges using McAfee solutions that include:

- **McAfee Enterprise Security Manager** (SIEM) unifies collection and analysis of security information and event data, providing real-time visibility into infrastructure and application activity, monitoring of prioritized alerts and watchlists, as well as a command center for expediting containment and response.
- **McAfee Threat Intelligence Exchange** provides a second line of defense behind endpoints to identify and manage evolving file and application reputations, working with McAfee and partner products to rapidly detect and spark remediation of advanced attacks.
- **McAfee Advanced Threat Defense** provides deep analysis of malware using reputation, emulation, sandboxing, and static analysis and then shares indicators of compromise and convictions with other controls and management systems to reduce exposure to advanced persistent threats.
- **McAfee Active Response** acts as an intelligent endpoint detection and response (EDR) mechanism to provide deep endpoint system and state visibility to help the SOC and endpoint teams identify, scope, remediate, and set alerts to monitor for the return of malicious and suspicious events and conditions.
- **McAfee ePolicy Orchestrator® software** provides a central, single-pane-of-glass security management framework to help endpoint operations automatically monitor and manage a wide range of security events, alerts, and threat responses from McAfee and partner products.
- **McAfee Web Protection** filters and scans web traffic to reduce exposure to risky web content, malware, and other threats before they can infiltrate networks, endpoints or applications through user browsing and cloud-based sites.

Our experts are your experts. For SOCs of all sizes, whether fully operational or just getting started, McAfee's professional services team offers the expertise to ensure that your solution is designed and deployed efficiently and that your organization is up to date on policies, procedures, and compliance requirements. For SOC managers struggling with resource constraints, our consultants can also provide short-term or long-term staff augmentation.

Conclusion

Even as security threats escalate, broaden, and become more complex, SOC managers need to take a deep breath and consider a new set of tactics to deal with their challenges. Increasingly, this means identifying and implementing new, real-world solutions that simplify management, improve protection and detection, increase confidence in deciding whether to convict potential threats, and speed correction and/ or mitigation. By embracing the seven steps identified in this paper, SOC managers will improve their ability to spot and eradicate threats at several points in the IT ecosystem, from the data center to the endpoint, both on premises and in the cloud.

McAfee offers a broad and deep portfolio for SOC managers, acting as a platform to unify and simplify security solutions. McAfee's long experience in security architecture engineering, SOC consulting, incident response, and threat intelligence are just some of the proven capabilities it can leverage on behalf of SOC managers.

Learn More

For more information about how SOC managers can address the rising tide of threats, alerts ,and security-related noise, please visit:

http://www.mcafee.com/us/resources/reports/rp-soc-collaboration-advanced-threats.pdf

http://www.mcafee.com/us/resources/misc/infographic-soc-collaboration.pdf

1. "2016 State of Monitoring Survey," BigPanda, March 2016.
2. "Adversarial Tactics, Techniques and Common Knowledge," Mitre Corp., 2015.
3. "Stronger IT Security Not Same as Higher Staffing Levels," Computer Economics, June 2015.
4. "The Pyramid of Pain," David Bianco, 2013

About McAfee

McAfee is one of the world's leading independent cybersecurity companies. Inspired by the power of working together, McAfee creates business and consumer solutions that make the world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

Visit us at **www.mcafee.com**.

McAfee™
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com