FORTRA™

Is Your Organization Ready for an In-house SOC?

Protecting your IT infrastructure is vital for the health of your business. Deep visibility and round-the-clock monitoring to analyze and identify risks are essential for maintaining a secure environment. However, businesses often struggle with determining the best way to ensure their security.

While large enterprises might find that an internal, "do-it-yourself" security operations center (SOC) suits their needs, this approach may not be feasible for small to midsize organizations due to the significant expense, mean time to deployment, and talent resources required.

This guide empowers you to make a strategic decision: build an in-house SOC or partner with a managed security services provider for envisioned security outcomes.

People, Process, Technology: The Three Pillars of an In-house SOC

While no two internal SOCs are identical, every effective SOC relies on three core elements: people, process, and technology. As you evaluate whether an internal SOC is the right fit for your organization, it's crucial to thoroughly examine each of these components, the associated costs, and the potential challenges they may present.

People

What is the average cost of hiring and retaining top-tier talent for an in-house SOC?

On average, attracting and hiring a Tier 1 or Tier 2 analyst costs approximately $10,000, according to **Fortra's Alert Logic TCO Calculator**. This figure, based on our experience, excludes salary and represents the internal burdened cost of recruitment and onboarding. It's important to note that hiring and retention costs can vary significantly depending on the candidate's location, education, and professional experience. Additionally, this initial $10,000 is only a starting point; the fully burdened cost of an employee will be higher.

How many team members should we have in our SOC?

The most effective SOCs provide 24/7 monitoring. Our experience indicates most midsize organizations require a minimum of 11 security professionals in an internal SOC. Ultimately, the number of SOC personnel will be based on the volume of assets, desired level of service, and number of alerts generated from critical assets in the environment.

What roles are essential for an effective SOC?

To build an effective in-house SOC, it's crucial to have a diverse team covering various specialties. Key roles can include:

Tier 1 Security Analyst: This triage specialist reviews the latest alerts for relevancy and urgency; creates new trouble tickets for alerts that signal an incident and requires a Tier 2 Security Analyst review; runs vulnerability scans and reviews vulnerability assessment reports; and manages and configures security monitoring tools. In-house SOCs should have more than one Tier 1 Security Analyst.

Tier 2 Security Analyst: This incident responder reviews trouble tickets generated by Tier 1 Security Analysts; leverages emerging threat intelligence to identify affected systems and scope of the attack; reviews and collects asset data on these systems for further investigation; and determines and directs remediation and recovery efforts. In-house SOCs should have more than one Tier 2 Security Analyst.

Tier 3 Expert Security Analyst: This threat hunter reviews asset discovery and vulnerability assessment data; explores ways to identify threats that are within the network; and recommends how to optimize security monitoring tools based on threat hunting discoveries. In-house SOCs should have more than one Tier 3 Expert Security Analyst.

Tier 4 SOC Manager/Director: Leading operations and managing the SOC, this leader supervises the SOC team; hires, trains, and assesses staff; manages the escalation process and reviews incident reports; develops and executes crisis communication plan to the CISO; runs compliance reports and supports audit processes; and measures SOC performance metrics and communicates the value of security operations to business leaders. In-house SOCs will have one Tier 4 SOC Manager/Director.

What essential training, skills, and certifications should SOC team members possess?

While there's no definitive checklist, a high-impact SOC team typically includes members with a range of technical and soft skills. Key technical proficiencies include system administration across platforms (Linux, Mac, Windows), programming languages (Python, Ruby, PHP, C, C#, Java, Perl), and advanced security certifications (CISSP, GCIA, GCIH, GCFA, GCFE). Equally important are soft skills, such as an insatiable curiosity for problem-solving and the ability to maintain composure under pressure.

Process

What compliance or governance requirements must a SOC manage, meet, and maintain?

This will vary based on industry, geography, and nature of the services or products your organization provides. Whether required by regulations or used as guiding frameworks, these will empower your organization to implement industry best practices and pave the way for scalable future growth.

Which standards will your SOC be responsible for in your security compliance program?

Common standards and frameworks that will fall within the responsibility of the SOC can include:

- GDPR
- HIPAA
- HITRUST
- ISO/IEC 27001
- NIST
- PCI DSS 4.0
- SOC 2

Technology

The array of tools and products available to monitor your IT enterprise is vast, with significant variations in quality, cost, and interoperability. These tools only provide the best protection if they don't leave gaps and you can maintain visibility and control across all network segments. Common SOC tools include:

SOC Management Tools
Incident tracking and management system
Data Center/On-premises Management, Maintenance, and Mitigation Platform
• Asset discovery and monitoring systems • Compliance monitoring solutions • Data monitoring tools • Endpoint protection systems • Extended detection and response • Firewall and antivirus software • Identity and access management • Intelligent automated application security • Intrustion prevention • Security information and event management • Security posture assessment ratings
Cloud Management, Maintenance, and Mitigation Platform
• Cloud infrastructure entitlement management • Cloud-native application protection platform • Cloud security posture monitoring • Cloud workload protection platforms • Kubernetes security posture management

Comparing Your Options	Internal SOC	Managed Security Services Provider
SOC is tailored to meet organization's needs	Yes, with right budget and personnel	Yes, if right partner is selected
Upfront and ongoing costs	Significant, especially in the first 24 months	The cost of deploying on average is 5%-15% of the cost of building out an in-house SOC
Hiring and retaining personnel	Challenging as there is a documented shortage of cybersecurity experts and a competitive marketplace	Has experienced personnel immediately available
Average deployment for SOC	An in-house SOC takes 12-24 months to deploy	Can take as little as six weeks to roll out a security soulution for an organization
Acquiring and implementing AI security technologies	Several AI-driven security tools will need to be purchased, which can be a significant expense both for the tools and personnel to operate them	MSSP will have the tools necessary for all emerging threat hunting and monitoring

Next Steps

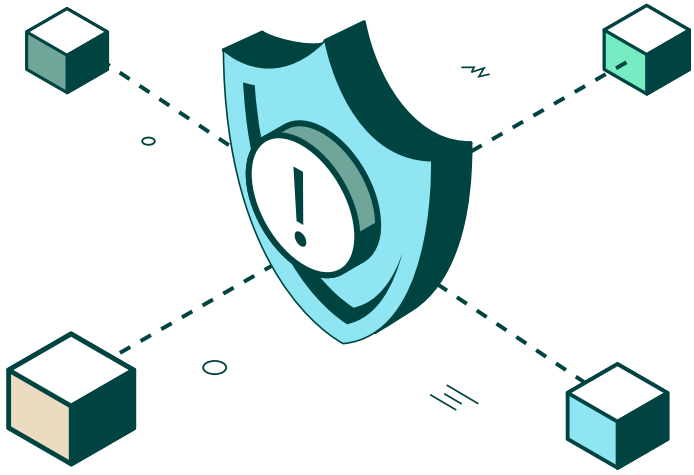
You've pinpointed the people, processes, and technologies needed for building an internal SOC, and you now may be questioning if this is the right solution for your organization. Would partnering with an external resource that provides unrivaled security for any environment, 24/7 coverage, and industry-leading service value be a better fit?

To effectively address their security needs, many organizations are striking a strategic balance by managing key cybersecurity operations internally while partnering with an external managed security services provider.

While an internal security operations center has some benefits, for most organizations, the high costs and expert-level personnel needed to operate the SOC is simply not realistic. Instead, they work with an external MSSP who learns their environment and delivers comprehensive security using technology and expertise honed from working with many different organizations.

Fortra's Alert Logic: Unmatched Managed Security Tailored for Your Organization

With over 20 years of experience, Fortra's Alert Logic offers unmatched security expertise and robust, proven processes. Our comprehensive coverage spans public clouds, on-premises, and hybrid environments. Leveraging continuous threat detection, our global SOC provides 24/7 monitoring and delivers actionable insights derived from innovative threat intelligence and proactive threat hunting. Experience top-tier security and peace of mind, all achieved far more quickly than developing and maintaining an in-house SOC.



Alert Logic offers three managed security service solutions:

Fortra XDR: Enhance your security by extending coverage to every layer of your environment—endpoint, network, identity, and cloud. Our solution goes beyond the typical tools-only approach of many XDR providers. We offer a fully managed service designed for organizations that need expert support to effectively detect, respond to threats, and achieve their security goals. Whether you're lacking resources, expertise, or struggling with your current security stack, we provide the comprehensive solution you need.

Alert Logic MDR: Alert Logic MDR is not just technology; it's a game-changer in security. Our solution combines an industry-leading platform with unmatched coverage, cutting-edge threat intelligence, and a top-tier SOC team. This powerful combination ensures you achieve the security outcomes you need. Tailored to your specific requirements, our MDR service equips you to safeguard your critical systems with confidence.

Fortra Managed WAF: Web apps and APIs are integral to business operations and profitability. The downside of this digital transformation is attackers have another gateway into your organization's critical assets and data. Distinguishing good traffic from bad in real-time is crucial but can be challenging for many organizations. Our managed web application firewall delivers a competitively priced, highly versatile, enterprise-level, cloud-ready WAF that comes with a team of experts to eliminate the complexity of managing your WAF.

Ready to Find Out More About Alert Logic?

You've done the research, looked at the costs, and examined your in-house margins. You've learned that choosing Alert Logic's managed security services will be a small fraction of the cost of building and maintaining an in-house SOC. You don't have to do it alone. Our expertise, service, and technology can be your advantage.

Let's get started on your managed security journey! Our cybersecurity experts are ready to collaborate with you. For more information, visit **alertlogic.com** or **schedule a demo**.

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.