FORTRA™

SOLUTION BRIEF (Alert Logic)

Is an In-House, DIY SOC Right for Your Organization?

There's no question that protecting your IT estate is critical to the health of your business — having deep visibility and 24/7 monitoring to analyze and identify risks across the threat landscape are the hallmarks of providing a secure environment.

The question businesses often grapple with is how to best provide security for their organization. For some, the answer lands immediately on an in-house, Do-It-Yourself security operations center (SOC) — and for large enterprises, building and maintaining a SOC that is nuanced to their environment may be the right choice. But what about everyone else, such as small to midsize organizations where the significant expense, mean time to deployment, and talent resources needed for an in-house SOC simply is not a viable option?

This resource was created to help you determine whether building an in-house, DIY SOC or outsourcing your SOC needs to a security partner specializing in managed detection and response (MDR) is the best route.

People, Process, Technology – the Three Pillars of an In-House, DIY SOC

While no two in-house SOCs are exactly the same, there are three elements you'll find in each – people, process, and technology. As you determine if an in-house SOC is the right approach for your organization, you need to consider each of these elements, the costs associated with them, and the potential challenges they bring.

People

On average, how much does it cost to hire and retain the talent we need for an in-house SOC?

In **Fortra's Alert Logic TCO Calculator**, $10,000 is set as the average cost to attract and hire an analyst at the Tier 1 and Tier 2 level based on our experience. This cost is not inclusive of salary — it is the internal burdened cost of facilitating the recruitment and subsequent onboarding of a new hire. Hiring and retention costs are variable and influenced by the location of the applicant and their education and professional experience. This is a starting cost and one can expect this expense to go up when considering the fully burdened cost of an employee.

How many team members should we have in our SOC?

The most effective SOCs provide 24/7 monitoring; our experience has shown that for most midsize organizations, you will need a minimum of 11 security professional in your in-house SOC. Ultimately, the number of SOC personnel will be based on the number of assets you have, level of service, and number of alerts at each level created from the critical assets in the environment.

What type of roles are necessary for an effective SOC ?

Within your in-house SOC, positions could and should 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 CISO; runs compliance reports and supports audit process; 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 training, skills, and certifications do team members in a SOC need to have?

While there's no set-in-stone list, common skill sets include sysadmin skills (Linux, Mac, Windows); programming skills (Python, Ruby, PHP, C, C#, Java, Perl, etc.); and security skills (CISSP, GCIA, GCIH, GCFA, GCFE, etc.). Additionally, there's a host of soft skills your SOC teams members should have such as extreme curiosity to get to the root cause of a problem and the ability to remain calm under pressure.

Process

What compliance or governance mandates will your SOC be required to manage, meet, and maintain?

This will vary based on industry, geography, and nature of the service/products your organization offers. Whether mandated or serving as frameworks, these will help your organization deploy industry best practices and enable the best path to scalability for 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 include:

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

Technology

The list of tools and products available to monitor your IT enterprise is immense and varies considerably in quality, price, 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 • Firewalls and antivirus software • Identity and access management • Intelligent automated application security • Intrusion prevention/detection system • 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

Next Steps

As you've identified the people, processes, and technologies necessary for an in-house, DIY SOC, you 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?

Comparing Your Options	In-house, DIY SOC	External MDR Security Partner
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 average cost of deploying an MDR solution with an MDR provider is, on average, 5%-15% of the cost of building out an in-house, DIY 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 four-to-six weeks to roll out a security solution for an organization
Acquiring and implementing AI security technologies	To achieve your security goals, 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	External partner will have the tools necessary for all emerging threat hunting and monitoring

The right approach for many organizations security needs is to find a balance between managing some cybersecurity operations internally and partnering with an external MDR solutions provider.

Forta's Alert Logic – the Most Comprehensive MDR Coverage for Your Organization Providing Industry-Leading Service Value

While an in-house, DIY 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 chose an external partner who provides unrivaled security for any environment, using technology and expertise that offers the industry's most comprehensive MDR coverage. And that partner is Fortra's Alert Logic Managed Detection and Response.

Our MDR solution delivers comprehensive coverage for public clouds, SaaS, on-premises, and hybrid environments. Our continuous threat detection and security expertise gives you the peace of mind that your environment is being monitored 24/7 by a global SOC that delivers actionable insights based on leading emerging threat hunting and intelligence. And this level of security is available in a fraction of the time it would take an organization to develop, launch, and maintain an in-house, DIY SOC on their own.

With Alert Logic MDR, you'll have:

- Scalable MDR platform
- Extensive breadth and depth of coverage across your entire IT architecture
- Unrivaled security expertise with 150+ SOC and threat intelligence experts
- Comprehensive coverage against known and unknown threats
- Incident validation
- Broad and deep coverage across hybrid and multi-cloud environments
- Customer-first mindset and 20+ years' experience delivering measurable service value
- Single point of security expertise who becomes an extension of your team
- Automation at your own pace
- Protection tailored to each asset in your estate
- Unwavering commitment to continuous product innovation
- Adaptable to your security and compliance needs

Ready to Find Out More About Alert Logic MDR?

You've done the research, looked at the costs, examined your in-house margins. You've learned that partnering with Alert Logic for MDR 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 Fortra's Alert Logic MDR journey! Our cybersecurity experts are ready to collaborate with you. For more information, visit **alertlogic.com** or view our **MDR 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.