Critical Insight

Detection & Response

4 Options for Security Operations

Introduction

The use of rapid detection and response is now recognized as a method to meaningfully reduce security risk. Organizations are moving beyond simply lowering the probability of a breach to limiting the impact if a breach occurs.

Rapid detection and response are a clear focus, and organizations are spending time and money to manage growing security responsibilities, including operating a monitoring infrastructure, investigating alerts, and responding to incidents. Without this investment, organizations risk missing requirements necessary for regulatory compliance and missing the warning signs of incidents while they are in progress.

Critical Insight has identified four options to manage detection and response:

- Do nothing and accept the risk of breach
- Assign security event review, investigation, and response tasks to existing IT staff
- Build and staff an in-house security operations center (SOC) to manage the day-to-day elements of detection and response
- Hire a trusted third party to provide the detection and response capabilities of a mature SOC

In this paper, we compare these four options and consider benefits and costs. We cover the necessary elements of a functional SOC, including human resource and capital investments and the operational expenses that go with it. We use data from our direct experience building a SOC, along with expectations for a representative organization. The pros and cons of building a SOC or contracting for SOC capabilities from a trusted 3rd party provider.

In conclusion, we illustrate how outsourcing SOC operations to a trusted third-party provider can save an organization 80% relative to building an in-house SOC.

> **“Outsourcing SOC operations to a trusted third-party provider can save an organization 80%”**

Options to Detect and Respond

Do Nothing

Accepting the risk posed by threats is the baseline security decision, and many organizations do choose to leave their security outcomes up to chance. We include it here because it is indeed one way to address your security risks. However, such a decision is impossible to defend, especially after an attacker breaches your organization's defenses. It would not look good to regulators, customers, or investors when a CEO must address a reportable event that was ultimately foreseeable if the organization did not adequately resource prevention and detection capabilities. Furthermore, the magnitude of this risk in dollar terms will likely hit an average of $150M per event.

Multi-Task Security and IT Teams

Another common strategy, which is especially common at less mature and smaller organizations, is to leverage existing IT staff to address information security requirements. This is the default option when an organization is first building out infrastructure and protective controls. Unfortunately, when security tasks are assigned to IT staff, the security requirements are at odds with key IT projects designed to advance the organization's mission.

This strategy creates a clear opportunity cost. By assigning tasks that don't advance business objectives to IT staff, the key strategic priorities are delayed or completed sub-optimally. Digital transformation impacts all industries, and organizations risk being less able to compete when IT projects slip. Hospital teams should be optimizing their e-health strategy. Local governments and small businesses should be working on transformative "smart-city" initiatives.

Secondly, the critical investigation tasks will not receive the attention they deserve from a security perspective when an organization assigns responsibilities to multi-tasking IT staff. Actual breaches may slip through unnoticed among the alerts.

Put simply, if an IT team is also the security team, the chances of them doing a good job in either capacity is significantly diminished. If an organization repurposes existing resources to security, they are implicitly paying for security staff. If 50% of a network engineer's time is spent reviewing logs and investigating potential security events, then half that engineer's salary is being applied to security. The analogy commonly used from the manufacturing industry is unplanned work: an hour of planned work is equivalent to two hours of unplanned work. Combining that cost with the certain opportunity cost of delayed IT projects means that they are significantly overpaying for security and underachieving in terms of results.

Less obviously, when IT staff are given security tasks, they receive extremely valuable security training while simultaneously experiencing multi-tasking that reduces job satisfaction. Considering that these employees will be overworked and probably underpaid, they will likely seek greener pastures and higher pay. The job market for security professionals is hot. Tasking IT staff with security tasks can lead to employee turnover.

Build an SOC Operation

For established organizations, investing in internal SOCs is a good way to improve the effectiveness of detection, triage, investigation, confirmation, response, and recovery and the associated compliance activities such as record-keeping.

Building a sufficiently capable SOC is a considerable undertaking requiring significant funding and buy-in from senior leadership.

Although a SOC can take several forms, all SOCs require some combination of large data set management, hardware, office space, and employees. The industry-accepted SOC models, as defined by Gartner research, are bucketed based on the level of complexity and the characteristics of typical adopters:

SOC MODEL	ATTRIBUTES	TYPICAL ADOPTER
Virtual SOC	• No dedicated facility • Part-time team members • Reactive, activated when a critical alert or incident occurs • Primary model when fully delegated to MSSP	Upper mid-market organizations
Dedicated SOC	• Dedicated facility • Dedicated team • Fully in-house • 24/7 operations	Large enterprises, service providers, high-risk organizations
Distributed/ Co-Managed SOC	• Dedicated and semi-dedicated team members • Typically, 5×8 operations • When used with an MSSP, it is co-managed	Small and midsize enterprises
Command SOC	• Coordinates other SOCs • Provides threat intelligence, situational awareness and additional expertise • Rarely directly involved in day-to-day operations	Very large enterprises and service providers; governments, military, intelligence
Multifunction SOC/NOC[3]	• Dedicated facility with a dedicated team performing not just security, but other critical 24/7 IT operations from the same facility to reduce costs	Small, midsize and low-risk large enterprises where network and security functions are already performed by the same or an over-lapping group of people and teams
Fusion SOC	• Traditional SOC functions and new ones, such as threat intelligence, CIRT[4] and OT[5] functions, are integrated into one SOC facility	Large enterprises with a broad security operations mandate that covers disparate types of risk considerations and use cases

[3] NOC = Network Operations Center

[4] CIRT = Computer Incident Response Team

[5] OT = Operational Technology

The right investment level for a SOC depends on the organization's size, business model, and risk tolerance. A thorough risk assessment can help security leaders and C-Suite managers determine how vulnerable they are to attack and help justify the considerable investment they will have to make to build a capable SOC. Security assessments can also help security managers determine how they will address each of the critical resources they will need to run the SOC including, but not limited to people, hardware, and software.

People

To operate a SOC, you need to hire trained, experienced InfoSec professionals or create a program to "build" SOC engineers by hiring people with aptitude and then training them to the point of becoming credentialed.

Common InfoSec credentials and qualifications include:

- Certified Information Systems Security Professional (CISSP)
- ECSA - EC-Council Certified Security Analyst
- Applicable network, server, and workstation administration certifications (i.e., Windows Server, MCSA, CompTIA Network+)
- 3-5 years of related on-the-job experience (IT, and preferably InfoSec)

For a SOC that maintains 7/24/365 coverage, an organization needs to hire twelve professional analysts to cover shift work and PTO, with at least three that have 3-5 years related experience.

Facility

SOC operations must be conducted in a secured facility to maintain compliance with data protection requirements. Physical access controls, cameras, routine access reviews, management of authentication tokens, and other technologies designed to restrict physical access to those authorized for entry are required.

Hardware

The SOC hardware must handle large volumes of incoming data and include resources to process and analyze data near-real-time. Adequate storage systems will be required to underpin the data aggregation and retention requirements. Organizations should budget for annual operational costs, depreciation in hardware, and most importantly, maintain optimal performance by staying up to date with technology.

The SOC hardware will typically include enterprise-class, high-availability servers to support the data ingestion, processing, indexing, search clustering, and a separate facility and hardware set for disaster recovery.

Finally, each analyst will need a high-powered workstation with multiple monitors.

Tools

The SOC will include tools to apply correlation and advanced analytics to the data to facilitate the prioritization of suspicious events. SOC operations teams frequently use a Security Information and Event Management (SIEM) system.

Note that SIEM technologies, in general, do not apply robust analytics; they are dependent on the messaging created by other technologies, which are aggregated at the SIEM. Analysts must then 'tune' the system to alert on correlated events. This tuning process is time-consuming and prone to error. It is critical to ensure that the signal-to-noise ratio is appropriate for the environment and that reducing false-positive alerts does not create false negatives. Modern SOC operations are increasingly leaning toward unstructured databases for event aggregation, to which analytics are applied to tease out statistical aberrations, strongly periodic signals, and other anomalous events..

Process

SOC processes must be well-defined and repeatable. SOC analysts must consistently execute and document processes for each element from initial detection to asset recovery. Success metrics and service levels should be documented to ensure the SOC is effectively reducing the potential dwell time, the cost per incident, the time to incident close, etc.

Data Security and Audibility

To assure internal customers and business partners, the facility and associated infrastructure should be assessed against a recognized standard such as SSAE-18. This is especially important if the SOC operation will have access to regulated information with special handling requirements such as PHI or PII. The security program administrator is responsible for audit readiness, including documented standards for data protection, articulated protective controls, and processes that create artifacts that can be provided to examiners.

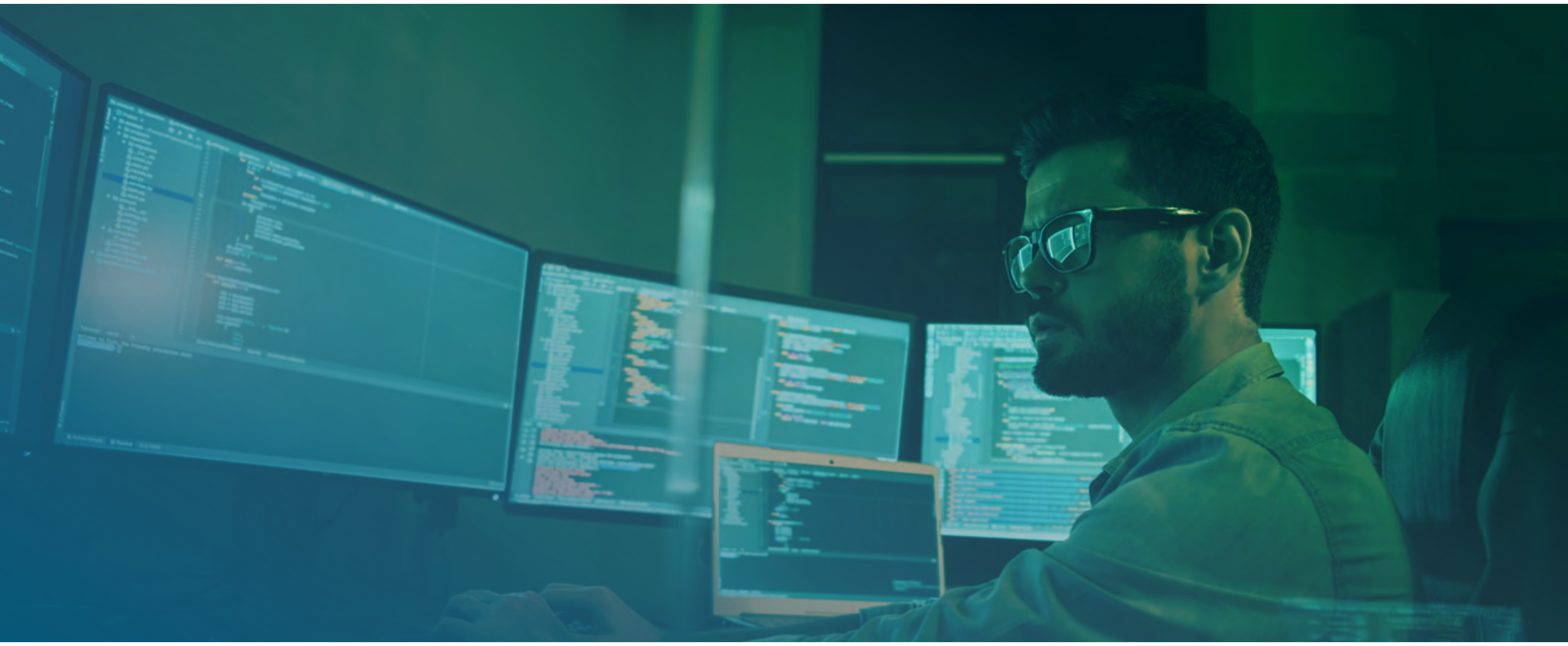
Overall SOC Cost Estimates

The following table estimates the top-level investments required and costs associated when building a Security Operation Center. These figures are based on a medium-sized business with 1000 users.

[6]

Hardware	$32,199
Software	$3,600
Total Employee Compensation	$490,000
Initial Recruiting Costs	$90,000
Analyst Replacement Recruiting	$15,000
Space Hardening	$60,000
Process Ramp Up	$90,000
TOTAL ANNUAL COST	**$765,799**
TOTAL 3-YEAR COST	**$1,782,999**

[6] Cost Comparison Methodology: To illustrate the potential cost differences between common network security solutions, we compared 2017 data associated with the implementation of Critical Insight's MDR product to the true costs of building an internal SOC using equipment and software from certified manufacturers. The costs of building a SOC were itemized to its most elementary components. Assumptions for employee headcount, salary, and time have been incorporated. Additionally, office space, technology (hardware/software) costs, and setup costs were included.



Outsource Managed Detection and Response

With the appearance of Managed Detection and Response (MDR) solutions in the market, outsourcing is now a possibility. Gartner Research has identified Managed Detection and Response (MDR) as a category of service that directly addresses the need to manage detection, investigation, response, and recovery while acknowledging the shortage and expense of qualified practitioners. Gartner releases an annual Market Guide for Managed Detection and Response[7], highlighting the MDR providers in North America, including Critical Insight (formerly CI Security).

Some organizations use Managed Security Service Providers (MSSPs) for security needs. To understand the difference between MSSPs, MDR, SEIM, and other acronyms used in this field, see our related article.

Outsourcing SOC capabilities to an MDR service offers the following benefits:

- Ensures regulatory compliance with easily producible artifacts for auditors and business partner
- Leverages existing technology investments
- Empowers lowest-cost resources (i.e. help desk) to facilitate incident response activity
- Provides SLAs for performance targets
- Avoids HR costs in managing SOC analyst "churn"
- Allows internal IT Staff to focus on strategic projects to advance the business
- Ensures new analytics are continuously applied to keep up with the threat environment

Most importantly, an MDR service will help an organization avoid the significant capital costs, operational costs, and management attention required to build an internal SOC.

[7] “2020 Market Guide for Managed Detection and Response,” Gartner Research, August 2020, https://www.gartner.com/en/documents/3989507/market-guide-for-managed-detection-and-response-services

Critical Insight offers MDR on an annual subscription basis, with no up-front capital costs. In comparison to the "In-House SOC" example above, Critical Insight could provide the same capabilities for a 1000 user organization for 19% of the first-year cost and 24% of the 3-year cost:

	IN-HOUSE SOC	CRITICAL INSIGHT MDR	% COST DIFFERENCE
1 Year Cost	$765,799	$141,400	19%
3 Year Cost	$1,782,999	$424,200	24%

Conclusion

Every organization has specific needs that will inform the decision whether to build an internal SOC or outsource SOC capabilities to a trusted MDR provider. The operational costs associated with an in-house SOC are significant but may be justified for large organizations.

The following tables outlining of Pros and Cons for these two options can assist in decision making.

Build the SOC In-house for MDR

CATEGORY	PROS	CONS
People	• Manage staff personnel and operations under one roof • Full accountability within organization	• Expensive to attract and retain • Owning all liability and compliance requirements internally is risky • New employee training due to staff turnover
Space	• Keep all data on premise • Internally-controlled operations	• Expensive square footage • Maintain specific HVAC controls • Must address redundancy • Create disaster recovery plan and make necessary investments
Hardware	• Leverage existing infrastructure	• On-going Maintenance and Infrastructure Costs
Software	• Use existing technology stack to build upon	• Expensive for both initial investments and annual renewal costs • Not all software is of the same quality • Tech debt due to employee turnover

Outsource the SOC for MDR

CATEGORY	PROS	CONS
People	• No HR Costs • No Operations Required to Manage SOC Activities • Cheaper than hiring FTEs • IT Staff enabled to quickly contain threats and manage Incident Response • SLAs for detection and response (liability transfer)	• Not a capital cost; budget requirements are perpetual • Budget may need to be increased YOY to manage / increase capabilities if needed
Space	• No On-Going Costs Associated • Space can be freed up for other operations	• New budget line item to allocate the cost of MDR
Hardware	• Existing infrastructure can be leveraged to work in tandem with external SOC • No need to invest in new hardware for SOC activities managed off-site	• No administrative access to vendor supplied appliance
Software	• Current software can be leveraged to integrate with outside firm's services and tech stack • Reduce technology spend on-going by eliminating duplicative licenses • Assistance with eliminating false positives • Reduce residency time of infected property, thereby reducing spread of damage company-wide • Holistic internal software integration to seamlessly connect to external service provider	• No access to vendor intellectual property

The potential costs of doing nothing are vastly more than what an organization would spend in either SOC strategy. The dynamic pace of threat actors is indisputable, and preventive controls are not enough to limit the far-reaching impacts of an undetected breach. Repurposing IT Staff results in sub-optimal detection capabilities and significant opportunity costs in reduced strategic velocity. In-house SOC solutions can result in robust detection capabilities but at a substantial expense.

In conclusion, we recognize that contracting with the right MDR provider can provide material risk reduction while significantly reducing the DIY approach's costs.

At Critical Insight, our data demonstrate 80% or more in savings for companies who select our MDR service. When combined with our professional services for strategy, regulatory compliance, forensic investigation, etc., organizations can manage risk, meet compliance requirements, and keep IT projects on track. While at the same time delivering a comprehensive security program previously unattainable to mid-market enterprises.