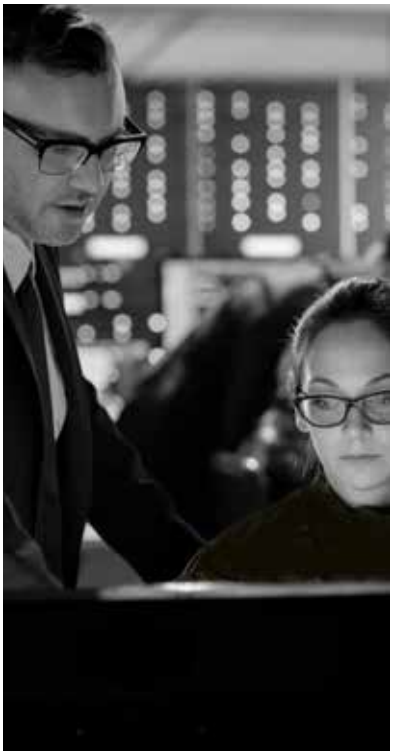
Putting on the right SOC to fit your security operations



Security operations centers (SOCs) bring together the resources needed to direct the defense of digital and even physical assets. As organizations embrace the latest digital technologies, SOCs are critical to enabling key business initiatives (**Figure 1**). With cyberthreats evolving and intensifying in scope and impact, organizations of all sizes are facing major decisions about how to cost-effectively manage security operations.

Organizations typically rely on three models for SOC delivery:

- Create and operate an in-house SOC
- Create an in-house SOC for some capabilities and use an expert vendor's leveraged SOC for specialty functions
- Outsource SOC services to an expert vendor

There's no one-size-fits-all approach. The best model depends on business size, budget, regulatory environment, threat profile, security experience and availability of resources. Deciding which model to choose often depends on whether these services form part of the organization's core business strategy.

Understanding the options and constraints is crucial to making the right decisions for managing security operations. Organizations must identify their needs for detecting and responding to attacks, consider objectives for the level of protection and select the right approach to fit their needs.

SOC responsibilities	Typical SOC functions
Security operations management	Coordination and integration Optimization and continuous improvement
Incident management	Initial triage and analysis Threat hunting and incident response
Security information and event management (SIEM)	Monitoring and event alerts Threat intelligence Automation and orchestration
Vulnerability management	Vulnerability scanning Testing and attack simulation

Figure 1. What do SOCs do?

DXC Labs | Security

DXC Labs delivers thought leadership and technology prototypes to enable enterprises to thrive in the digital age.

DXC Labs | Security brings together our world-class advisors to develop strategic and architectural insights to reduce digital risk. DXC's Cyber Reference Architecture is at the heart of our research, providing clients with detailed guidance on methods to efficiently resolve the most challenging security problems. We help clients minimize risk while taking maximum advantage of the digital commons.

Learn more at **www.dxc.technology/securitylabs**

New rules for SOCs

The approach to information security has changed over the past 20 years from an attempt to build impregnable citadels to one reflected by the widely stated aphorism: It's not a matter of whether you will be hacked, but when — and how you detect and deal with it. A critical part of the continuous monitoring necessary to detect and deal with such situations is a SOC.

SOCs typically define what constitutes suspicious activity, identify vulnerabilities, configure detection technologies, search for active threats and validate them, ultimately notifying affected parties. SOCs must also manage and monitor identities and ensure compliance with internal policies and government regulations.

SOC operatives may also handle deeper investigations and forensic analyses into insider and external breaches, as well as coordinate and implement a response. In large organizations with many operational units, some of which may be outsourced, SOCs may identify security issues, assess risk and make recommendations, but then hand over further response and remediation to separate incident management and operations units.

SIEM: The foundation

Security information and event management (SIEM) technology is the foundation of SOCs, often supplemented with analytical tools for deeper examination of the source data. SOCs may also utilize specialized tools for incident response management and orchestration. SOCs are normally organized into a series of levels of staff.

The first tier takes the notifications of suspicious events, enriches that alert data with additional information, looks for false positives and may take basic actions according to well-defined task lists. Surviving events are escalated to successive tiers in the SOC, so that validated events are referred to better-skilled and experienced investigators, who then ascertain the relevant risk, threat and impact. The SOC management function organizes, monitors and optimizes SOC performance.

Options for implementing SOCs

Historically, organizations had two basic options for implementing SOCs: in-house and outsourced. In-house operations typically provide total control but come with significant costs and challenges related to finding and keeping skilled security specialists. Outsourcing, on the other hand, allows a specialist security organization to apply its core skills and leverage economies of scale, but raises issues of trust and visibility.

An approach gaining wider acceptance is the leveraged or shared SOC. In-house and outsourced are opposite ends of a continuum, while shared SOCs divide responsibilities between the organization and the outside specialist; however, such solutions come with the typical organizational challenges of a shared responsibility (**Figure 2**).

In-house ◀ ▶ **Leveraged/Shared** ◀ ▶ **Outsourced**

In-house and total outsourcing are common options but are really the extreme ends of a spectrum of options that may be considered for delivering security operations.

Figure 2. SOC delivery continuum

Choosing the correct model for SOC delivery and understanding the advantages and disadvantages are critical to obtaining an effective security operation, which in turn may have a major impact on the reputation, function and profitability of your organization. Factors affecting the SOC delivery model include:

- Cost/budget
- Availability of skilled staff
- Retention and continuous training
- Regulation/industry sector
- Specialist organizational knowledge
- Specialist threat knowledge
- Business continuity
- Technology selection
- Content creation and maintenance
- Threat intelligence
- Size of organization
- Global locations
- Threat profile
- Organizational approach to security
- Approach to supply chain
- Times of operation
- Required response times
- Core business priorities
- Regulatory requirements

Developing an effective, fully featured SOC is a significant business decision, so determining the correct strategy is important as it will drive substantial investments.

Developing an effective, fully featured SOC is a significant business decision, so determining the correct strategy is important as it will drive substantial investments.

Some very practical decisions also must be made early in the SOC selection process. For example: Should the SOC operate 24×7? In a globalized world, neither customers nor attackers may operate in the home time zone, yet committing to a 24×7×365 operation requires working in shifts and places a practical minimum size on the SOC team. Most 24×7 operations have at least eight people, although larger ones require more staff. Considering the median annual pay for a security analyst in 2016 was $92,600, an eight-member SOC team would have annual recurring wage costs of $740,800, not counting overhead costs.

When you take into account training, licensing and facilities, total operating costs can easily reach seven figures, making the in-house approach impractical for many small and midsize enterprises.

Model 1: Going it alone with an in-house SOC

If cost is not a factor, an in-house SOC team can undoubtedly better understand the organization than an outside firm is able to. The in-house model also reduces the number of people involved in decision making, avoids the inertia of crossing organizational boundaries, provides insight into the organizational segments that must be involved in a response and adds leverage to make them respond.

However, there's also a trade-off between intimate knowledge of an organization and the need for general visibility and situational awareness. SOCs that deal solely with one organization have a limited view of the relevant threat landscape. Outside vendors, by comparison, typically manage thousands of clients and millions of endpoints and can identify threats around the globe and notify clients about these, in real time.

While in-house SOCs give a comforting sense of ownership over priorities and information and may suit an organization's approach to security, SOCs are a specialty function and may be in conflict with an organization's desire to concentrate available resources on its core business.

As a result, in-house SOCs tend to be the preferred option for large organizations or those with special needs, such as extreme levels of threat or impact, unusually sensitive information or particularly rigorous organizational strategies.

Even where the in-house option has been chosen, there can be significant benefits from bringing in outside expertise to help establish the SOC and then to periodically review its effectiveness from the perspective of an outsider with deep experience in SOC operations.

Model 2: Giving up control to an outsourced SOC

At the other extreme is the outsourced SOC delivered by a specialist security team that can bring to bear the resources necessary to run the SOC effectively and take advantage of economies of scale.

Outsourcing organizations can realize significant savings by using a single group to develop "content" — including reports and dashboards — after correlating events. In addition, an outsourcing vendor that monitors client operations in related industries or geographic locations should be able to provide better threat intelligence and early warnings. What's more, a large outsourcer might be among the first to get access to security patches for emerging threats.

Within the fully outsourced model there are different delivery options: The SOC may be dedicated to a single customer or leveraged across many customers:

- **Dedicated outsourced SOC.** Dedicated SOCs share many of the properties of in-house SOCs, but the service provider can bring additional value by using some shared resources, such as content development, threat intelligence and situational awareness gathered by other teams. Cycling people through accounts also helps share best practices and avoids the blinders that can come with operating in a single, isolated environment. A dedicated operation does, however, limit the possible economies of scale.
- **Leveraged outsourced SOC.** Leveraged operations provide the extreme case for economies of scale. By sharing equipment, experience and people across multiple customers, fragmentation of resources is minimized. This maximizes utilization, while the mixing within a larger pool of resources improves resilience and sharing. Organizations benefit from the experience gained by all of the customers of the service, as mediated through the SOC team, which can learn once and apply knowledge multiple times.

At the same time, leveraged SOCs can develop specialized interests within the larger group in a way not possible with a smaller team, and can address specific technologies, threat groups or industry sectors. For example, specialized technology experience can ensure that appropriate audit settings are turned on in firewall technologies or operating systems. Similarly, organizations in the same industry sector are likely to be targets of the same attack groups; therefore, the leveraged outsourced SOC analysts will have a better understanding of what to hunt for and how to interpret the results. This approach is suitable for organizations with limited or no security expertise and no appetite or budget for achieving it. Organizations must consider whether there is enough scale to effectively operate this way.

Regardless of the outsourced model used, keep in mind that it is not possible to outsource responsibility in either a legal or practical sense. Engaging an outsourced SOC does not allow your organization to ignore security or avoid involvement in security operations. At the very least, organizations should maintain an awareness of the security operation by overseeing the service and supplier.

Model 3: Best of both worlds — Shared SOC delivery

For organizations that can't afford an in-house SOC but worry about completely outsourcing the function, there is the shared SOC option, which can deliver the best of both worlds:

- The intimacy and control of local handling
- The knowledge and economies of scale of an outsourced operation
- The ability to draw on a supplier's larger pool of resources to supplement local capabilities in times of stress, such as during in-house staff shortages or seasonal peaks in business activity and threats.

For organizations that can't afford an in-house SOC but worry about completely outsourcing the function, there is the shared SOC option, which can deliver the best of both worlds.

Organizations have sought to split the load in a variety of ways:

- By platform and analysis: For example, the supplier is responsible for operating the technologies while the in-house organization manages the analysis.
- By time of day: An in-house team perhaps carries out operations during normal office hours.
- By analyst level: A supplier team carries out the lower levels of analysis but hands the higher levels of investigation and response to an in-house team.

In fact, the sheer variety of ways in which responsibilities can be shared represents a problem in its own right. Not all options are likely to be available from any one supplier.

Such SOCs also face questions about authorization, whose tools to use, how to access them and where liabilities lie — plus some inevitable friction between the organizations. Further questions relate to who is responsible for specifying, developing and maintaining the content, and who owns the intellectual property rights to that content.

Undoubtedly, a shared model requires more coordination than either of the other approaches, so both parties must be committed to working closely together to optimize costs and the effectiveness of services.

Bear in mind that a service provider reduces cost through economies of scale, so customizing services can reduce those savings. Depending on the split of responsibilities, a shared operation may be most appropriately delivered by dedicated supplier resources rather than leveraged ones, which could also have an impact on economies of scale. The external costs of a shared operation may not, therefore, be much cheaper than a fully outsourced one, while still retaining some of the in-house cost element.

A shared solution is likely to be of interest to an organization that is not large enough to justify a full in-house operation but wants greater control and involvement than it feels it can get from an outsourced operation. Again, it is worth remembering that is not possible to outsource responsibility, and with any degree of outsourcing comes the need to monitor and manage that operation.

Other considerations for SOCs

The effectiveness of a SOC is to a large degree determined by the ability of its staff analysts. Security professionals are in high demand, with the (ISC)2 2017 Global Information Security Workforce Study projecting a global shortage of 1.8 million information security workers by 2022.[1] Incident and threat management skills are particularly in demand. Consequently, security analysts are difficult and expensive to recruit and retain, particularly at the senior levels.

Because attack techniques and detection strategies are constantly developing, analysts need ongoing training and knowledge development time to retain their effectiveness and situational awareness. The introduction of new incident response tools, orchestration and machine learning will drive the need for constant retraining and, to some extent, change the roles and expectations of analysts. The opportunity to develop skills is an important motivational factor for analysts, which affects retention.

Building, optimizing and retaining analyst teams is a continual challenge for management. That's why organizations need a talent pipeline and career path for analysts, as experience and local knowledge have an impact on the role's effectiveness. Operating such a scheme requires resources and commitment. In the face of rapidly changing threats with higher levels of sophistication, these human factors must be taken into account when selecting the right SOC deployment model for an organization.

[1] 2017 Global Information Security Workforce Study, (ISC)2, 2017. https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf

A matter of scale and structure

In some cases an organization's scale and structure force a degree of structure onto the SOC.

In very large organizations with many operating companies, the SOC may effectively be "outsourced" to a centralized, in-house security function. In such a situation, the advantages and disadvantages are very much akin to the outsourced options discussed.

In other cases, practical considerations of operating hours and languages may make it desirable to have several SOCs that collaborate closely, in which case the considerations under shared SOC delivery apply.

Generally, SOC hierarchy with tiers of analysts can scale significantly, but there may be practical limits to the scalability of the technologies the analysts use. The scale of those platforms may require using multiple instances, but this can complicate the job of maintaining common content. That can also make it challenging to recognize threats if elements of the complete picture fall within different instances or become fragmented across different members of the analyst hierarchy. This is a universal problem across all approaches to delivering SOC services, but it is becoming less of an issue due to the adoption of highly scalable big data techniques.

Approaches for managing multiple SOCs
While not commonly done, an organization might use multiple, largely independent SOCs in a number of scenarios, including the following:

- Different sections of an organization operate under different regulation regimes. For example, a defense contractor may supply multiple governments that require some degree of independence between plants and limits on information sharing.
- A federated organization may have each suborganization responsible for its own security.
- An organization may be in the initial stages of a merger or acquisition.
- An organization relies on closely coupled suppliers, each responsible for the security of their element of the whole. For example, an organization may outsource desktop operations to one supplier, server operations to another and networking to a third.

In such circumstances, there may be a need for one central point of integration to draw together the security information from each segment, sometimes described as a "SOC of SOCs," to gain visibility into the big picture. Organizations take several approaches to this challenge, and there is no consensus on which is the best.

One approach is to draw all the raw event information from each of the segments into one central SOC. This may give a unified picture, but it is unlikely to be able to replace the component SOCs due to issues of contractual obligations and ownership and will therefore result in duplicated effort and cost. In such circumstances, it may be possible to dual-feed raw event information into the different SOCs. One particularly complicated problem with this approach involves complex supply chains with multiple suppliers that "own" their local security information and will therefore be reluctant to share the raw information.

An alternative approach is to share only incident information among SOCs, reducing the information flow to suspicious events. This is likely to be more acceptable in complex organizational environments, and it scales better. But it may result in events "falling between the cracks" of the SOCs and affect the quality and completeness of the content within each SOC.

Recommendations for the best approach

As you can see, SOC design is not a one-size-fits-all approach. To help you determine the best approach for your organization, we suggest the following actions:

1. Identify your need for a SOC

- How effective are your current operations? A maturity review of your current information security operations will assist with this. DXC offers a Security Operations Deep-Dive Maturity Review to help clients understand their current position and provide a clear plan for improvement.

2. Consider your objectives for a SOC

- What should it be protecting?
- Is the SOC core to the business?
- Should it operate 24×7?
- Which other teams will need to interact with it?

3. Select an approach

- In-house, outsourced or hybrid (i.e., leveraged/shared)?
- If hybrid, which functions do you want to manage in-house? Use this paper to review the options and trade-offs.

Whatever option you choose, your outcome will be more effective if you bring in partners that have experience setting up and operating in such environments and can guide you through the process. The DXC Technology Security team has helped hundreds of clients define the best SOC approach for their organizations, and it supports all types of SOC operating models. DXC accelerates our clients' paths to success with our specialized services coupled with our Cyber Defense blueprint, developed through designing, implementing and operating SOCs for hundreds of clients.

Finally, while SOCs play an important part in the detection and response elements of information security, they don't ensure an organization's security. DXC also supports security architecture, security operations, and governance risk and compliance, all of which are important factors in successful security strategies.

About the author

Dr. Rhodri Davies is a lead customer advocate for DXC Security. Rhodri helps organizations to understand the effective security strategies and solutions they need to respond to today's advanced cyberthreats. He was part of the team responsible for developing the strategies and tools for one of the first major European leveraged security operations, putting that SOC through ISO 27001 certification and developing business continuity for it. Recently, he carried out a project to relocate one of DXC's major SOCs.

Learn more at www.dxc.technology/security

MD_8022a-19. February 2019