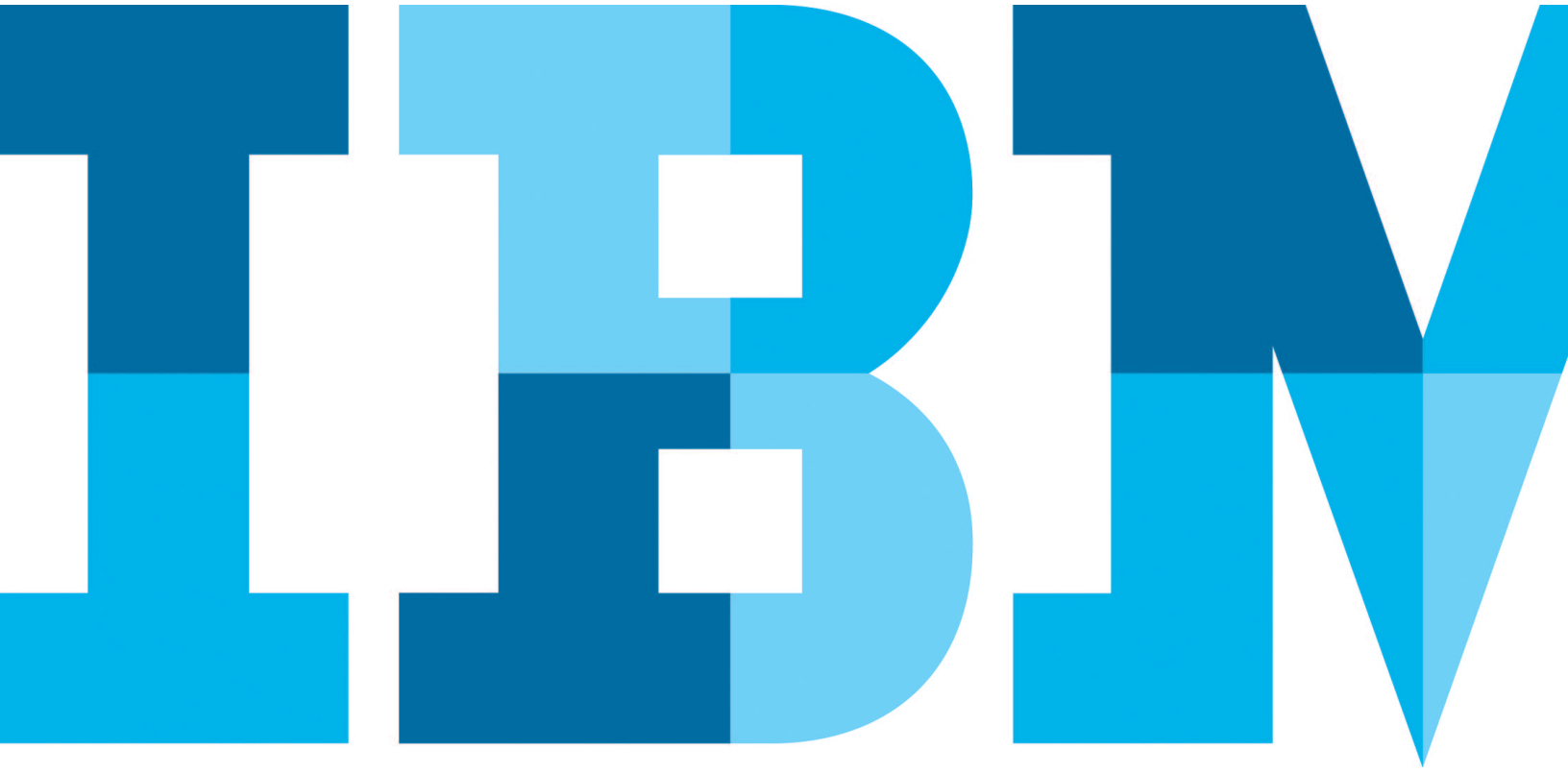
IBM Global Technology Services
Thought Leadership White Paper

Strategy considerations for building a security operations center

Optimize your security intelligence to better safeguard your business from threats



IBM

Contents

Executive summary

The persistent and evolving threat landscape has created a need for smarter security solutions, and organizations are taking notice. Despite the tightening of IT budgets caused by the recent global economic slowdown, Gartner anticipates security spending to reach US$93 billion by 2017.[1] which includes the areas of security testing, managed security service providers and security information and event management.

Building an enterprise security operations center (SOC) can be an effective path to reducing security vulnerabilities. An enterprise SOC encompasses the people, processes and technologies that handle information technology (IT) threat monitoring, forensic investigation, incident management and security reporting. It can include entirely internal operations, processes, technologies and staff, or a hybrid of out-tasked and internal capabilities. An enterprise SOC is particularly appropriate for large, global organizations that deal with significant amounts of data, which may be subject to complex legal and compliance requirements and at risk of targeted and sophisticated threats.

By developing an enterprise SOC, you can facilitate greater control over your threat management activities and help improve protection of your critical data assets. This internal capability can be enhanced by selectively leveraging external service providers to gain additional insight into global threat patterns.

This paper describes the persistent and evolving IT threat landscape, along with the need for and benefits of building an enterprise SOC. It details:

- How to assess the maturity and capabilities of your existing security operations
- Five essential functions that enterprise SOCs should address
- The myriad of considerations necessary to realize each function
- Broad capabilities that consulting partners can bring to the strategy and implementation of your enterprise SOC
- How you can jumpstart your enterprise SOC development efforts

Security challenges abound

The ever-persistent threat landscape poses risks to virtually any organization's operations and bottom line. At the same time, the growing complexity and quantity of structured and unstructured data from networks, mobile platforms and cloud-based environments is making it increasingly more difficult to manage data dispersed across numerous locations and stakeholders. It is no surprise that the most attacked industries include those that handle some of the most sensitive customer data. For example, the health and social services industry is the target of 10.1 million weekly attacks and the finance and insurance industry faces roughly 3.6 million weekly attacks.[2]

Overall, the "IBM Security Services Cyber Security Intelligence Index," which details analyses of security events for 3,700 IBM clients across 130 countries during 2012, uncovered 137.4 million incidents of malicious activity that attempted to collect, disrupt, deny, degrade or destroy information system resources or the information itself. That translates to 2.6 million

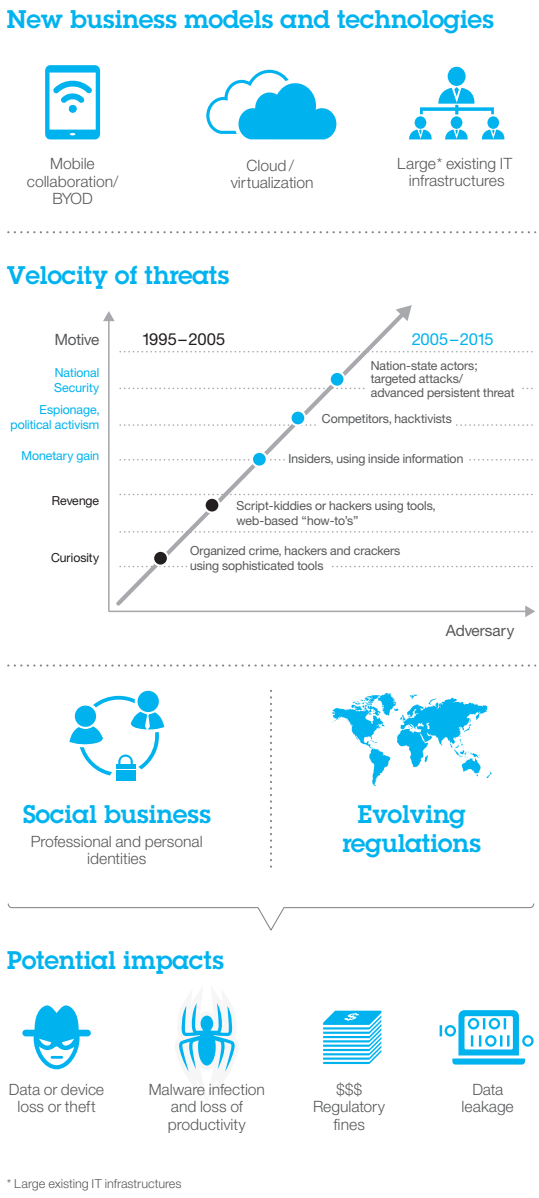


Figure 1. The current environment is putting new demands on security operations.

attack attempts each week and 0.38 million attack attempts each day. Of these threats, 1.07 per 1 million attacks successfully compromised their targets.[2]

What is the cost of these security breaches? The Ponemon Institute estimates the average organizational *cost of a data breach* in the United States is US$188 *per* compromised *record*—amounting to US$5.4 million annually.[3] And the soft costs can be even more significant. The economic value of a company's reputation has been found to decline an average of 21 percent as a result of an IT breach of customer data—or the equivalent of an average of US$332 million.[4] That is why companies need a more comprehensive approach to managing security threats.

Organizations need a way to:

- More cost effectively monitor threats and manage firewalls, AV and intrusion detection system (IDS) devices
- Develop the infrastructure and capabilities to improve security intelligence and respond more effectively to security threats or incidents
- Integrate a security information and event management (SIEM) into the existing infrastructure and optimize the staffing and processes to leverage it

The enterprise SOC: A more effective threat management solution

Technology cannot adapt as quickly as the ever-evolving threat landscape. The question is not a matter of *if* your organization will be attacked, but *when*. And when that attack occurs, the enterprise SOC you have in place can make the difference in reducing the impact of the threat, quickly identifying the nature and seriousness of the threat and providing management with the security intelligence to effectively handle the business risk.

What is an enterprise SOC?

An enterprise SOC functions as a team of skilled people operating under defined processes and supported by integrated security intelligence technologies that are typically housed within one or several on-premise facilities. Operating under the umbrella of your overall security operations environment, the enterprise SOC specifically focuses on cyber threat, monitoring, forensic investigation, incident management and reporting.

Enterprise SOCs are designed to:

- Provide a central point for monitoring, synthesizing and acting on threats (see Figure 2)
- Prepare for and respond to cyber incidents
- Enable business continuity and efficient recovery
- Prevent cyber threats from impacting the business infrastructure
- Provide insightful cyber-risk and compliance reporting
- Ensure that groups managing critical infrastructure components, such as firewalls, IPS, and routers are aware of potential threats to enable quick remediation of risks

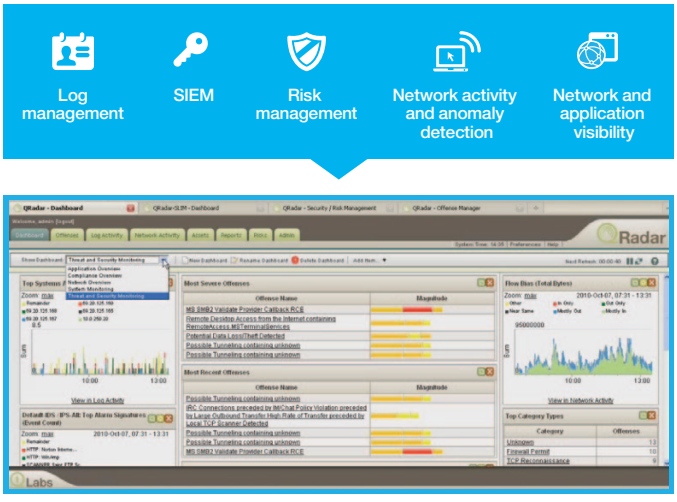


Figure 2. An enterprise SOC can provide a single view of security threats for near real-time decision-making.

More specifically, the enterprise SOC's major responsibilities are to help:

- Monitor, analyze, correlate and escalate intrusion events
- Identify trends in security threats and their potential impact on the business
- Develop appropriate responses for protection, defense and response
- Conduct incident management and forensic investigation
- Maintain security community relationships
- Assist in crisis operations and communications

Identifying the right fit

These are critical IT security functions for organizations in general, but managing them via an enterprise SOC is particularly advantageous for companies that handle significant volumes of sensitive data—particularly data that is subject to stringent legal and compliance requirements and would lead to catastrophic consequences if compromised. Thus, an enterprise SOC is an especially appropriate solution for financial institutions, large pharmaceutical companies and government. And unlike small to mid-size businesses, larger organizations can more easily allot the human resources, technologies and physical space needed to build and manage an enterprise SOC and develop an around-the-clock monitoring capability.

Because each enterprise SOC is as unique as the organization it belongs to, it is critical to understand the factors that influence outcome. An enterprise SOC can include entirely internal operations, processes, technologies and staff, rely heavily on external provider managed services, or include a hybrid of out-tasked and internal capabilities. To determine the right balance for your organization, you will want to consider cost, skills availability, single point versus multiple global locations, the importance of around-the-clock coverage and support.

Whichever model you choose, overall an enterprise SOC can offer the following advantages:

- An around-the-clock operational structure supported by people, processes and technologies charged with more effectively preventing, reducing and remediating security events

- Improved visibility into cyber attacks, infections and misuse that would otherwise require manual discovery and correlation
- A better understanding of how your security program reduces operational risks and therefore business risks
- Improved analytics and reporting to help address growing compliance requirements
- Insight into the current state of your security posture
- A more comprehensive view of threats made possible by threat feeds and analytics from external service providers
- More flexibility to update your security technologies to meet your business's evolving risk management needs
- Improved centralization of threat control to help manage one of your organization's most valuable assets—your information
- Reduced costs and potential damage to the business brand by helping to prevent and mitigate the impact of security threats

A recent study found that companies using security intelligence technologies were more efficient in detecting and containing cyber attacks. As a result, these companies enjoyed an average cost savings of US$1.6 million when compared to companies not deploying security intelligence technologies. Moreover, the study found that companies that invest in adequate resources, appoint a high-level security leader, and employ certified or expert staff have cyber crime costs that are lower than companies that have not implemented these practices. This cost savings for companies deploying good security governance practices is estimated at more than US$1 million, on average.[5]

Assessing your existing security operations

Virtually all organizations have security operations and many even have created dedicated security operations centers. However, they often operate at a sub-optimal level, and do not provide the required level of threat protection. In some cases, security operations are embedded in the network operations center (NOC) to tie threat monitoring to the policy management processes for network devices. The risk is that the group's governance priorities may not be sufficiently weighted toward identifying and analyzing the threats. There may also be gaps in threats outside the realm of the network, as the focus will be on managing the network. A dedicated SOC can place its priorities on how the threats will impact the business, both from an operational standpoint and planning perspective. It also helps enable an organization to bring together a team of skilled analysts that can more readily share knowledge of the evolving nature of the threats and how it is impacting the business.

Current maturity levels

A key consideration when assessing the current operation is the current level of maturity. The maturity of existing operations is a measure of effectiveness in providing the necessary threat management capabilities to protect the organization. Maturity levels should be assessed across multiple dimensions of capabilities or components along a scale of increasing maturity. Capabilities or components to measure can include:

- Technology
- Process and procedures
- Organization
- Metrics
- Governance

Examining each of these areas can determine how the current state compares to industry best practices by rating them across five definitions from initial base capabilities to an optimized environment (see Figure 3). A low ranking in any of the areas would warrant increased management attention and investment. Likewise, a mismatch across the capabilities or components (one low, another high) could suggest an inefficient allocation of investment resources.

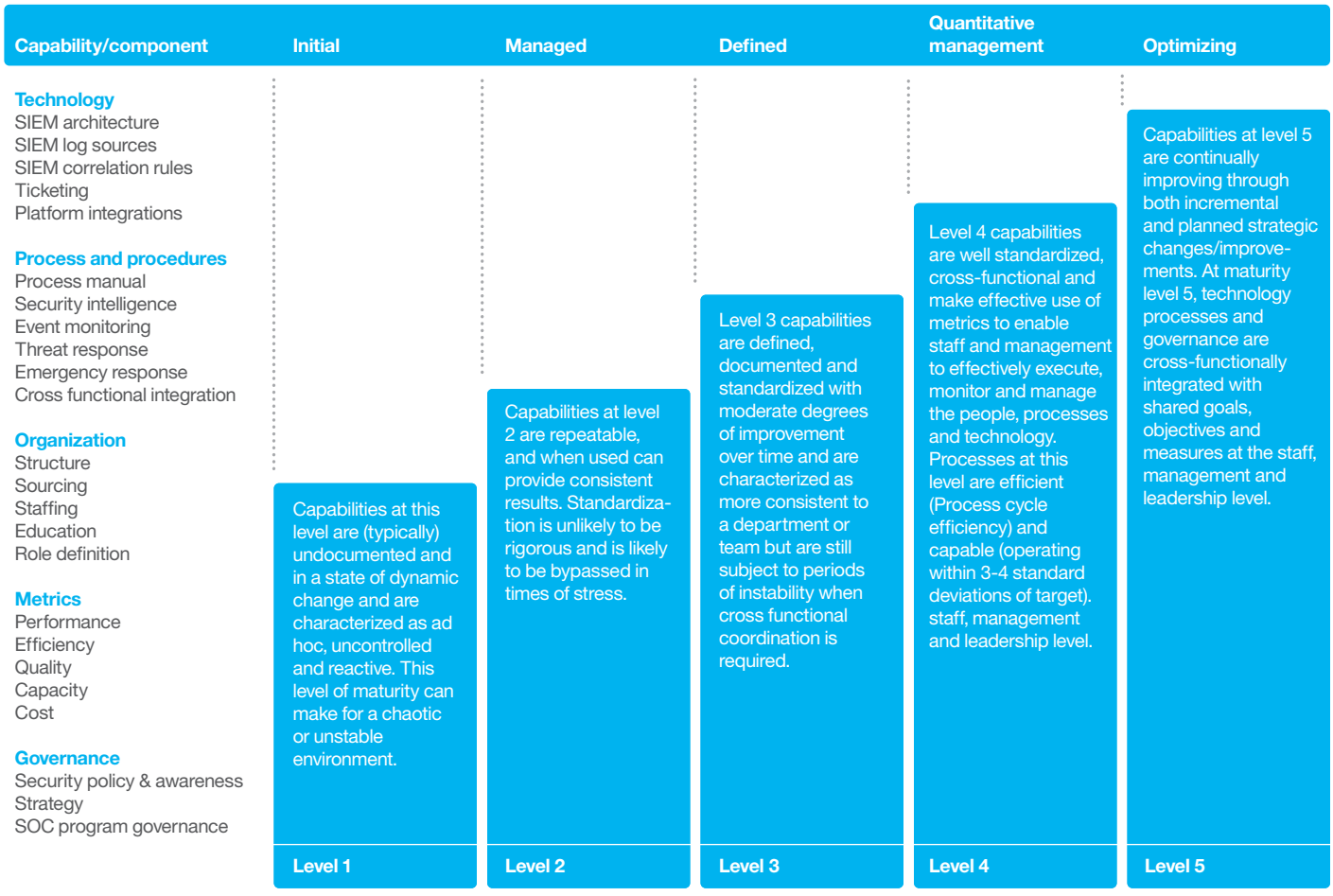


Figure 3. Assessing current maturity levels of existing security operations.

The five essential functions of an enterprise SOC

Realizing the benefits of an enterprise SOC depends on how effectively you define a strategy to address the essential enterprise SOC functions. These five essential functions include:

- Security threat monitoring
- Security incident management
- Personnel recruitment, retainment and management
- Process development, management and optimization
- Emerging threat strategy

Figure 4. The five essential functions of a SOC.

Function one: security threat monitoring

Monitoring threat data and determining where possible security events must be investigated is one of the best ways to preempt security threats. With robust monitoring skills and resources in place, such as SIEM technologies and other tools, you can change your organization's posture from reacting to security events to preventing them from happening in the first place.

SIEM tools provide the technology foundation for the enterprise SOC that enables the identification, correlation and prioritization of threats. Facilitating improved visibility, SIEM technologies collect volumes of log data across multiple devices such as Intrusion Prevention Systems (IPS), firewalls, routers, and turn the data into actionable security intelligence. This helps enable billions of log events to be synthesized into a handful of security offenses that can be prioritized for remediation action.

But the successful prevention of security incidents depends not just on industry-leading technology but also on industry-leading strategy. You will need to consider the following:

Methodology

- What specific data should be monitored, and does it need to be monitored within set hours or around the clock?
- What security events are you going to monitor, and how can you define these incidents via rules for the monitoring technology?
- What compliance and regulation issues warrant specific data monitoring?
- Are the systems you are monitoring critical enough for inclusion in your business continuity and disaster recovery plan?

Logistics

- Do events need to be monitored in near-real time?
- Does the event-monitoring tool need to be multi-tenant?
- Where and how can you get this data flowing into your monitoring tools?
- How do you tune event flow to be more effective?

Resources
- What kinds of monitoring reports will be needed, and who are the consumers of that information?
- What SIEM capabilities will be needed to stay on top of the newest threats?
- What human resources are needed for monitoring, and how many people are needed?
- What are the skill sets that will best serve the business requirements?

Team involvement
- How can you keep your team motivated and educated?
- Does your team have the right amount of information for effective decision making?
- How can you train new employees?

Follow-up
- What will be your escalation process when a security event needs to be investigated? How will the investigation of escalated events take place?
- How do you incorporate continuous process improvement into the monitoring process?
- How do you ensure that the use cases represent the latest threat patterns?
- How do you detect and remediate log and event sources that stop flowing to the monitoring tools?
- How can you update your organization about your monitoring capabilities as technology and threats change?

This list is not meant to be exhaustive, but these are critical items that need to be considered beyond the selection of a SIEM or other monitoring tools. And many of your answers to these questions will help determine not only the monitoring technology you use, but also how effectively you optimize the people and technologies that run your security-monitoring operations.

Function two: security incident management

Identifying security threats is only the first step. Equally important is defining which security incidents demand a response, and how to ensure that the necessary actions are taken to remediate the risk. An integrated ticketing system can provide the mechanism to capture the threat analysis, process it as a security incident, and track that the necessary remediation actions have been taken. This approach includes interfacing with the teams that manage the devices where policy changes are required. As most security devices are typically managed outside the SOC, quick identification of the device at risk and responsible parties will enable organizations to more rapidly update policies and configurations to address the threat.

There are practical aspects of managing security incidents, including:

- The prioritization process for managing the incidents (Severity 1–3)
- Defining the notification process (who and when)
- Managing the workload and aging of tickets
- Defining and enforcing service levels
- Developing meaningful metrics to track performance

There are also device and policy considerations to consider, including:

- How will the policies of the security devices and tools be crafted and tested?
- How will changes be conducted, who will be authorized to make changes and how will authorization be granted? Who will periodically review the overall policies?
- How will you update security definition files?
- Will you implement blocking technologies; and if so, for which items?

- How will you monitor the devices for health and availability?
- Which teams will receive health-monitoring updates?
- How will you update, record and track the health and policy issues?
- How will software and firmware be updated?
- What degree of fault tolerance will be required for gateway and inline devices?
- How will you grant access to the devices, and how will changes be monitored?
- How will access be controlled for third parties?
- What should be the feedback process between the monitoring team and the device and policy team for changes and tuning?

Function three: personnel recruitment, retainment and management

The people you hire who monitor and respond to security events on an ongoing basis will be the heart and soul of your enterprise SOC. And for this reason, you should choose them wisely. Although hiring and training staff with entry-level skills may save you money in the short run, this strategy can backfire in the long run if they are not able to effectively analyze, preempt or resolve security threats.

While the SIEM will filter the threats and identify the most important risks, the human component is still critical. It takes colossal concentration, attention to detail and most importantly, significant analytical skills to stave off IT threats on a daily basis. Network and desktop support and troubleshooting skills tend to translate well in this domain. It is also important to have some subject matter expertise with the particular vendor technology used in the environment.

The teams also need to be proactive in their approach to using security intelligence and identifying how the latest alerts may indicate a new level of threat to the organization, which implies close communication and knowledge sharing among analysts.

In addition, you will need a shift-scheduling program that matches resource allocation to the potential volume and impact of threats. For large organizations with multiple enterprise SOCs spread globally, this could imply a “follow-the-sun” distribution of resources.

And do not forget the critical nature of training. Ongoing training, via a formal program, is a necessity—as both security technologies and the threat environment are ever changing.

Other personnel considerations can include:

- Shift schedules for each staff member based on business needs (for example, 8 a.m. to 5 p.m. Monday through Friday, or around the clock)
- Defined responsibilities and deliverables for each position and for each scheduled shift
- Security monitoring and technology administration skill sets (Note: UNIX and Linux skills often translate well to security)
- Budget considerations for training organizations like SANS and participation at events like Black Hat Briefings and security conferences where innovative security trends are discussed
- Career path for security professionals; a 1-to-3 year tenure is typical for enterprise SOC analysts due to the rigors of the position
- Ongoing recruitment strategies
- Special positions focused on writing new rules for the monitoring tool, which often involves not only deep security expertise, but also script writing

It is also important to understand access and be able to audit that access to those on the security team, including outside security service providers. This is because they will likely have access to privileged information and administrative credentials to critical internal systems. As an example, IBM has extensive controls and audit processes to help make sure authorized changes can only be made by authorized staff.

Function four: process development, management and optimization

Managing an enterprise SOC effectively requires well-defined processes and procedures. Although a process defines who will do a specific task, a procedure defines how that task actually gets done. Both are necessary to operate in an organized, efficient and highly consistent manner on an ongoing basis. They are what help enable teams to know how to perform their duties.

The myriad of enterprise SOC process considerations include:

Analytical processes and procedures for detecting and remediating security issues

- Incident classification methodology
- Incident detection and analytical timeframes for taking action
- Incident escalation process and follow up
- Ticketing to help ensure that incidents lead to analysis and remediation
- Process to evaluate new threats
- Process to write and test new detection rules
- Forensics processes

Business processes and procedures for administrative and management duties

- Log retention
- Unacceptable usage
- Internal communications and public disclosure
- Policy change process and verification, including changes to gateway devices and how those configurations are reviewed
- Content update process and use cases refreshes
- Report preparation and metrics reporting

Operational processes and procedures for day-to-day operations

- Employee recruitment, retention, promotion and turnover
- New employee onboarding
- Company security awareness training
- Employee training

Technology processes for system administration, maintenance and management

- Patch process
- Firmware update process and software updates
- Access to device and management station processes
- New technology implementation process
- Health-check process
- Vulnerability scan and remediation process

Each of these broader categories can be broken down into hundreds of granular procedures. The more thorough you are in planning your processes, the more effective your enterprise SOC will be.

Function five: emerging threat strategy

Without access to the latest security intelligence, organizations may leave their most critical business data exposed to hackers or malware without ever knowing that a threat exists. But despite this reality, many companies do not have access to the latest security intelligence.

This is often due to rapid changes in security intelligence that make it difficult to stay abreast of current and emerging threats. However, there are many resources available, such as subscriptions to threat services like the IBM® X-Force® hosted threat analysis service

It is also possible to subscribe to services that can classify the trustworthiness of the external IP addresses and help alert you if your own address space has been communicating with known botnet control stations.

Additionally, it is helpful to understand if the threats and incidents impacting your organization are representative of comparable companies. This insight can help you evaluate what to expect, how efficient your defenses are and the effectiveness of your security program. Your organization and processes must also have the necessary agility to make use of this security intelligence and redirect resources and priorities as the risk vectors change.

You will need to build security metrics, which will ideally be:

- A set of metrics that help serve as your common threat-based metrics of events per day and per type
- Compliance reports that can satisfy business control needs
- Security reporting that better aligns to your overall company metrics and business objectives

You cannot successfully manage mutating threats unless you are aware of them. Thus, surveying the threat landscape on an ongoing basis can only make your security monitoring efforts more effective.

Capacity management

Capacity management plays a key role in aligning the sizing of the SOC to the type and volume of threats projected and the breadth of the infrastructure to protect. As in the maturity analysis described earlier, it is important that the various elements of the SOC (people, processes and technology) are balanced and sufficient to meet the peak volume needs without over investment. They would typically be sized to attain the performance levels defined in the SLAs and SLOs.

Capacity management can be thought of in four distinct phases (see Figure 5):

Capacity modeling—Analyzing the inputs and outputs of the SOC to understand what the design capacity should be to achieve an effective capacity of output that will produce the right balance of resources to handle the expected workload. A number of modeling tools can be used to allow for different skills required, technology throughput, coverage hours required and so forth. This can range from basic queuing theory, to Erlang modeling, to developing Poisson distributions. This exercise provides a quantitative view of the level of resources required and their allocation.

Capacity planning—The modeling exercise provides the inputs necessary to size and scope the SOC operation and its components. This enables more educated decisions regarding the number and type of skills needed over defined shifts, the number and capacity of servers to support the analytical and incident handling processes, investment to support the requirements and budget preparation. The planning phase typically results in a three-year SOC strategy and plan, which is then updated as the business requirements or threat environment changes. This planning typically includes stakeholders from both business, IT and compliance.

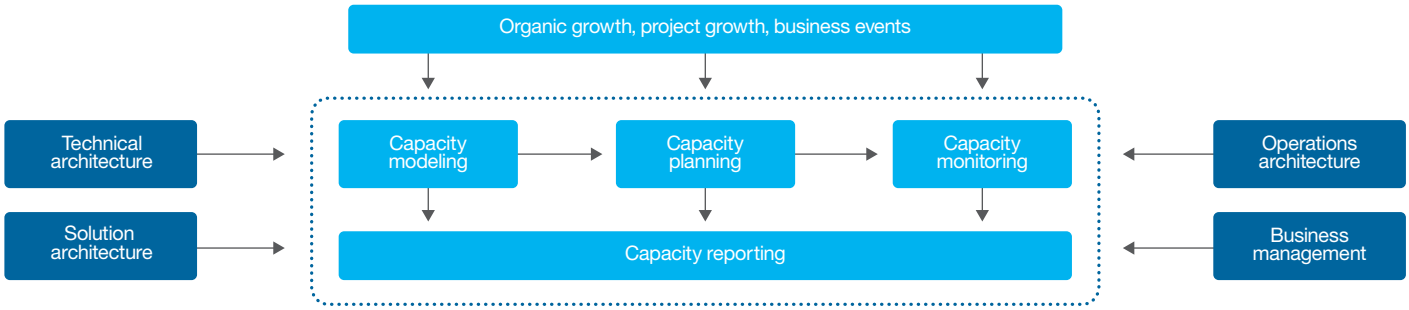


Figure 5. Capacity management typically falls into four distinct phases.

Capacity monitoring—It is important to periodically evaluate the SOC performance to validate the decisions from the modeling exercise. As mentioned earlier, today's threat environment is continually evolving and may demand periodic rebalancing of personnel or a review of available skills. Thus, it is important to institute monitoring capabilities that provide management with the tools and information necessary to assess if the SOC is meeting its defined mission. This not only helps to justify the current operation but provides insights into future requirements, for example, enhanced security intelligence processing technologies or improved reporting capabilities.

Capacity reporting—Supporting the above phases is a need for comprehensive reporting that provides SOC management the information necessary not only to evaluate the performance of the current operation and the meeting of SLAs and SLOs, but also to better understand where process, skills or technology constraints could impede the handling of an increase in volume or change in the business objectives. Effective reporting serves both the SOC managers and CISO's information needs as well as the organization. It can also feed compliance reporting to help demonstrate readiness and support future investment requests as the SOC evolves.

Moving forward to create an enterprise SOC

So how do you get started on an enterprise SOC initiative? A practical place to begin is with understanding the risk management objectives of the organization. What are the business risks or compliance requirements where business management are dedicating time and will steer investment capital? Who are the key business and IT stakeholders that will seek input into the SOC strategy?

These questions and answers will help develop your mission statement. The mission of the enterprise SOC should address the reason you are building it and the problems it seeks to overcome. This mission is something that will be unique to your organization and help determine the people, processes and technologies that will be your enterprise SOC.

Example: A global financial institution seeks strategy guidance and implementation assistance to build an enterprise SOC

Scenario
A global financial institution with many locations distributed around the globe needed insight into industry-leading security practices and assistance to create an in-house, enterprise SOC that helped them improve threat management and better manage compliance.

Solution sought:
- Business and technical workshops to assess the current security operations
- Guidance on developing a best-in-class security operations center leveraging leading SIEM technologies
- Implementation and integration services to build an around-the-clock SOC and staffing support to help quickly ramp up the operation

Benefits:
- A view of the current maturity and capabilities of existing security operations
- Reduced costs and improved return on investment
- Optimized processes for monitoring and managing threats
- Ability to rapidly respond to changing compliance requirements
- Improved visibility into threats and better remediation of risks

When creating the mission, consider your:

- Security pain points based on the defined business and IT risks
- The core enterprise SOC functions that would effectively address your pain points
- Compliance and regulatory requirements, especially for units that might be in other geographies
- Security budget and multi-year commitment
- The volume and types of threats you have faced historically
- Who will consume the information collected and analyzed by the enterprise SOC
- Facilities
- Labor and skills availability
- Technologies in place and required
- Training and threat intelligence educational investments

After you define your goals, compare them to your present security status to determine what is working and what is not working. For example, do you have full visibility into your security devices' log reports? Can you correlate the log information to derive useful security intelligence? Does your security governance help enable rapid response to identified threats? An assessment of your security operations can identify gaps in people, processes or technologies that could leave the door open to a breach. It can also paint a clearer picture of the resources and capabilities you need to move forward. With this insight, you can fine-tune your mission statement and goals—and ultimately, translate them into a roadmap for putting together your enterprise SOC operations.

Finally, you will need to determine how much of the workload and capital investments you want to take on in-house. There are numerous paths to moving forward, including using the skills of a managed security services provider, building the strategy and enterprise SOC entirely in-house, or outsourcing some of the essential functions. For example, you can choose a service provider to manage the SIEM technology or to provide you with skilled analyst resources on a contract basis. Figure 6 illustrates the factors that come into play when determining an optimized model for your enterprise SOC.

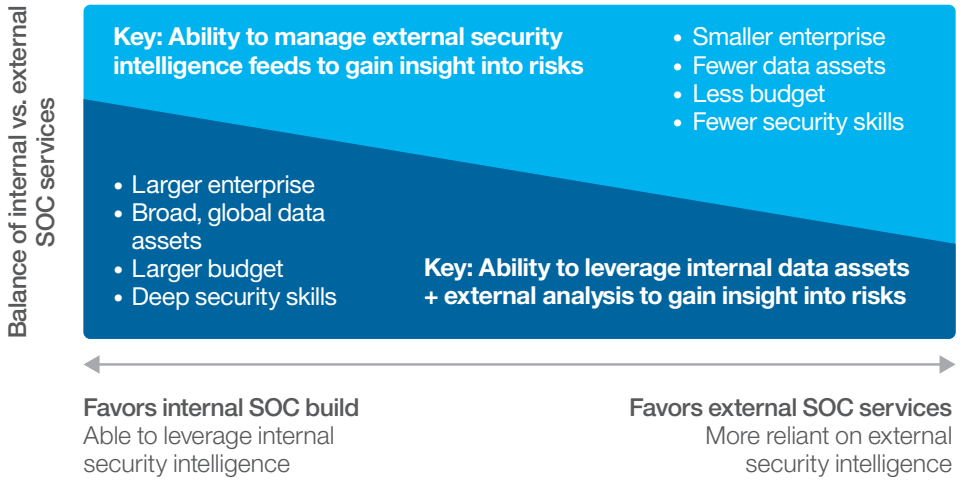


Figure 6. Determining the right fit for your enterprise SOC.

Few, if any, companies can outsource total responsibility for security. However, many organizations have found that partnering with a security services provider can help them more effectively and efficiently address the essential functions raised in this paper. This is because security operations can be overwhelming, involving numerous considerations and a wide range of skills. A provider with vast security resources can streamline the development of your enterprise SOC by providing any one or more of the following services:

- Strategy consulting and enterprise SOC design and implementation expertise
- World-class skills
- Compliance and regulatory management
- Extensive security research to identify evolving threats
- World-class technologies to help monitor, remediate and prevent security threats

IBM enterprise SOC development capabilities

Through workshops, assessments, strategy engagements, and design and build activities tailored to your organization, IBM can help improve your security intelligence capabilities and optimize your security operations. We can offer the critical resources you need to build an enterprise SOC including:

- ***People:*** Skilled resources to analyze threats and monitor a heterogeneous infrastructure around the clock
- ***Processes:*** Efficient operational processes to help you more rapidly respond to threats and remediate risks while facilitating compliance management
- ***Technologies:*** Advanced SIEM and ticket-management technologies that provide the security intelligence to better target the response and manage the security devices

The IBM enterprise SOC offerings include the following:

- **SOC workshop:** a one-day management workshop to establish goals and objectives for developing the SOC, including identifying stakeholders, the types of threats you will monitor and the management model
- **SOC assessment:** consulting assessment for customers that have an existing SOC but are looking for IBM to review their capabilities and maturity and make recommendations for improvements
- **Consulting strategy engagement:** for organizations who want to develop an internal SOC and are seeking a strategy and roadmap for development (see Figure 6)
- **SOC design and build projects:** professional services for customers who already have a SOC strategy and are seeking assistance to design and build one or multiple SOCs (see Figure 7)

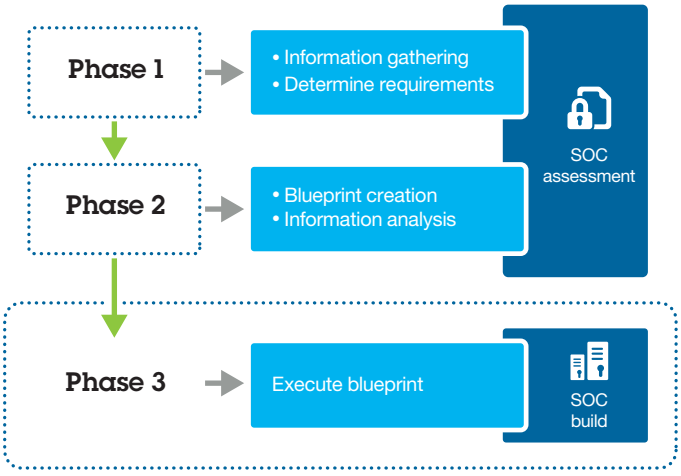


Figure 7. IBM tailors its standard methodology to help organizations evaluate their SOC models, establish a target state and develop a roadmap.

- **SIEM assessments:** for organizations that want to assess their existing SIEM deployments and need guidance to upgrade their capabilities
- IBM QRadar security intelligence platform: security intelligence products that help integrate SIEM, log management, anomaly detection, and configuration and vulnerability management to deliver improved threat detection

Why IBM?

IBM is an analyst-recognized leader in security consulting and managed security services. With over a century of experience supporting clients' business systems—including more than 15 years of experience building and operating SOCs—we can help you reduce and prevent IT risks to your organization. In fact, on any given day, we process and store an average of 20 billion security logs. This diverse experience equips us with unique insight into mutating threats that are impacting numerous industries—enabling us to more effectively recognize and preempt a wide range of security issues.

Moreover, by choosing IBM, you can take advantage of our global security operations and research capabilities, industry-leading methodology and software and world-class skills. Our global footprint includes 10 enterprise SOCs that serve over 2,000 customers in 100 countries, and our clients are supported by the skills of over 6,000 highly skilled security consultants.[6]

We are ready to deliver feature-rich and more flexible solutions to support your enterprise SOC strategy, design and implementation needs.

For more information

To learn more about enterprise security operations centers (SOCs), please contact your IBM representative or IBM Business Partner, or visit the following website: **ibm.com**/services/security

Additionally, IBM Global Financing can help you acquire the IT solutions that your business needs in the most cost-effective and strategic way possible. We'll partner with credit-qualified clients to customize an IT financing solution to suit your business goals, enable effective cash management, and improve your total cost of ownership. IBM Global Financing is your smartest choice to fund critical IT investments and propel your business forward. For more information, visit: **ibm.com**/financing

IBM Corporation
IBM Global Technology Services
Route 100
Somers, NY 10589

Produced in the United States of America
December 2013

[1] Gartner, "Forecast: Information Security, Worldwide, 2011-2017, 3Q13 Update," October 2013. #G00258387

[2] IBM, "IBM Security Services Cyber Security Intelligence Index," March 2013, **ibm.com**/services/multimedia/Cyber_security_Index.pdf

[3] Ponemon Institute, "2013 Cost of Data Breach Study: Global Analysis," May 2013; https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf

[4] Ponemon Institute: "Reputation Impact of a Data Breach: U.S. Study of Executives & Managers," Sponsored by Experian® Data Breach Resolution, November 2011, http://www.experian.com/assets/data-breach/white-papers/reputation-study.pdf

[5] Ponemon Institute: "2012 Cost of Cyber Crime Study: United States," October 2012. http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf

[6] Statistics are current as of 2013

Please Recycle