Business white paper

State of security operations

2014 report of capabilities and maturity of cyber defense organizations

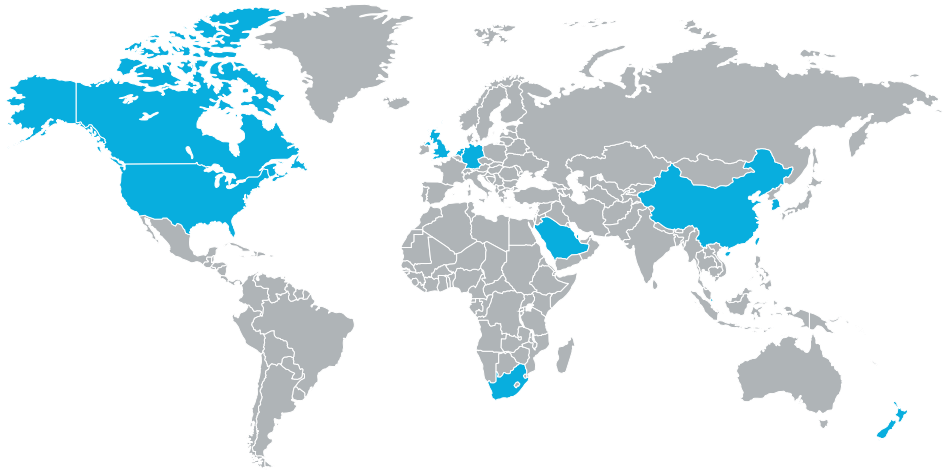
Table of contents

Abstract

Organizations around the globe are investing heavily in information technology (IT) cyber defense capabilities to protect their critical assets. Whether protecting brand, intellectual capital, and customer information, or providing controls for critical infrastructure, the means for incident detection and response to protect organizational interests have common elements: people, processes, and technology. The maturity of these elements varies greatly across individual enterprises and industries. In this first-of-its-kind report, HP summarizes the capabilities, lessons learned, and performance levels of security operations based upon maturity assessments performed on worldwide organizations. With over a decade of experience supplying the technology at the core of the world's most advanced security operations centers (SOCs), HP has worked with more of the world's top SOCs than any other organization and is uniquely qualified to publish this report.

Executive summary

HP Security Intelligence and Operations Consulting (SIOC) has assessed the capability and maturity of 69 discreet SOCs in 93 assessments since 2008. The maturity assessments include organizations in the public and private sectors, enterprises across all industry verticals, and managed security service providers. Geographically, these assessments include SOCs located in 13 countries. This is the largest available dataset from which to draw conclusions about the state of security operations across the globe.



HP's methodology for assessments is based on the Carnegie Mellon Software Engineering Institute Capability Maturity Model for Integration (SEI-CMMI) and has been updated at regular intervals to remain relevant with current trends and threat capabilities. The focus of the assessments is inclusive of the business alignment, people, process, and technology aspects of the subject operations. The reliable detection of malicious activity and threats to the organization, and a systematic approach to manage those threats are the most important success criteria for a mature security operations capability.

The ideal composite maturity score is a level 3—"defined".

The ideal composite maturity score for a modern enterprise security intelligence and operations capability is level 3—where the capability is "defined." This is achieved with a complimentary mixture of agility for certain processes and high maturity for others. HP has observed that overly mature operations result in stagnation and rigidity that results in a low level of effectiveness. SOCs (or providers offering SOC services) that aspire to achieve maturity levels of 5 lack an understanding or appreciation of the nature of such capabilities and the threats they are defending against. Managed security service providers (MSSPs) should target a maturity level of 4 due to the need for consistency in operations and the potential penalties incurred for missed service commitments—yet, there is a compromise in agility and effectiveness that the MSSP and its customers accept with this level of maturity. Once the ideal maturity level is achieved, a SOC's focus should be to continually evolve capabilities to keep pace with a rapidly evolving threat landscape.

The cost of data breaches has increased by 78 percent over the last four years.[1] The time it takes to resolve a cyber attack has increased 130 percent over this same period. There is a clear need for improvement in the effectiveness of security operations to limit the impacts and speed the resolution of such events. This report will summarize data gathered during maturity assessments performed by HP and share the current state of this important security function, including common mistakes, and the lessons that can be learned from them. The intent of this report is to expose and drive the capability and maturity of SOCs as organizations move into the fifth generation of security operations.[2]

24% of assessed security operations organizations do not meet minimum requirements to provide consistent security monitoring.

HP has found that 24% of assessed security operations organizations do not meet minimum requirements to provide consistent security monitoring. Only 30% of assessed organizations are meeting business goals and compliance requirements. Despite these sub-standard findings the data shows there are several areas where improvements are happening:

- Companies are recognizing the strategic nature of IT to their business and are building SOCs to protect their investment.
- Executives are increasingly fluent in IT security. The stewards of IT security within organizations are gaining sophistication in their understanding of the threat and the requirements for capable defense.
- Security vendors are being held accountable for providing transparent and effective solutions that are easy to integrate and manage.
- SOCs are building informal and formal communities and beginning to share information more openly—this is resulting in more widely distributed indicators of compromise (IOCs) and a more complete view into threat actors and methods. Obstacles to the private sharing of specific security data are slowly being overcome.

A key element in the uneven distribution of maturity results across industries can be directly correlated with the experience of negative financial impact from malicious attacks. This means that the organizations that recognize the business criticality of protecting their enterprises, or those who have experienced direct financial loss due to malicious attacks, do a better job of maturing to a higher level. Economic incentive matters.

Summary of findings

While the presence of SOCs is increasing and their capability level is showing improvement, HP assessments of organizations worldwide show the average maturity level of SOCs remains well below ideal levels.

Findings and observations from SOC assessments include:

- The term "operations" results in confusion over a SOC's mission and misaligns expectations for a SOC—Effective SOCs use intelligence disciplines that include collection, analysis, and dissemination, and are analytical in nature. This differentiates a SOC from other operations organizations focused on availability, problem determination, ticket remediation, and recovery disciplines. This is one reason SOCs are being rebranded as cyber defense centers.

[1] Based on internal analysis of the results from the 2010-2013 "Cost of Cyber Crime Study: United States" reports from Ponemon Institute.
[2] hp.com/go/5gsoc

The basics are extremely important and commonly overlooked.

- The basics of IT security are extremely important and commonly overlooked—Asset management, user ID administration, information classification, and vulnerability management are all foundational elements required for a SOC to achieve higher order goals.
- An inability to prioritize efforts in a SOC results in an overall low capability and maturity—It is difficult and costly to protect everything. Successful SOCs utilize a risk-based approach that results in clear priorities and targeted focus.
- Follow-the-sun models[3] and geographically distributed teams are significantly less effective than single-location teams—Geographic shift-change and team boundaries are a significant barrier to establishing positive culture and effective collaboration. Collocated operations are more effective at developing mature capabilities.

Compliance is a side effect of a highly capable threat detection function; effective threat detection does not result from compliance.

- Focus on compliance objectives sets a dangerously low bar for the mission of a SOC—Compliance is a side effect of a highly capable threat detection function; however, effective threat detection rarely results from compliance mandates.
- Performance, capacity, and availability-based frameworks, such as ITIL®, are insufficient for developing mature security operations—Security operations require more process tools than ITIL and must leverage an analytical approach. CMMI, Agile methods, and success-criteria driven metrics for management are more effective in security operations.

Human analytical capability is required to detect and respond to modern threats.

- There is an over-reliance on technology—While many organizations invest heavily in technology, the staffing and skills required to achieve the goals of the solution are often missing. In SOCs, this results in minimal investment in the most expensive CPU in the room: the analyst. Unlike analysts, systems cannot apply non-linear thinking to an incomplete picture in order to develop reasonable hypotheses—human analytical capability is required to detect and respond to modern threats.
- Augmentation of security operations capability through managed security services (MSS) requires mature client-side operations—Very few MSS models can completely offload the risk or responsibility for threat detection and response from the client. Organizations partnering with an MSS provider still require event analysis and incident response capabilities to manage the provider and participate in the service. Companies often fail to integrate with their MSS provider when it comes to effective closed-loop incident remediation. The complete closed-loop process has to be effectively measured and managed to ensure success.

The fastest path to a capable SOC is a public breach.

- The fastest path to a capable SOC is a public breach—Companies that have experienced tangible loss as a result of a breach have a clear business case for investing in a highly capable SOC. Loss can include financial loss, impact to customer confidence, and brand damage. Post-breach SOCs are built up quickly to limit future impact of a breach and demonstrate due diligence in the wake of a loss.
- Advanced use cases are not effectively operationalized—Inadequate content management processes result in development of advanced use cases that lack controls to ensure the full benefit of the use case is achieved. This is commonly driven by breakdowns in communication between engineering teams that create the system content and analysis teams who are expected to use the content. Effective SOCs utilize iterative content development processes that account for the entire lifecycle of the use case.
- Administrative tasks levied on top of analytical tasks in a SOC degrade overall results—Organizations often gauge that there are not enough events detected in the SOC and assign other non-detective tasks to ensure full utilization of SOC analysts. A more mature response is to discover why there is a lack of detection and implement a plan to improve the SOC's detection capability.
- Industry alignment has a direct impact on the maturity and capability of SOCs—Organizations within industries that heavily rely on third parties, that are restricted by strict procurement processes, or that utilize rigid project models experience an adverse impact on the overall capability.

[3] Follow-the-sun is a type of global workflow in which tasks are passed around daily between work sites that are many time zones apart.

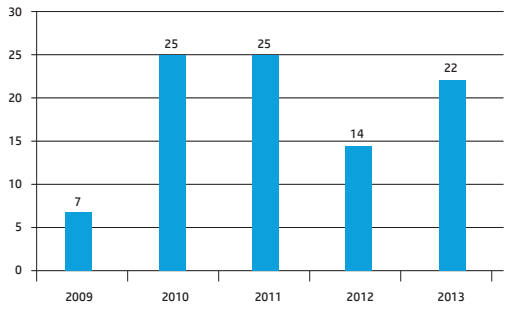
Relevance of our data—qualification to present this report

SIEM is the technical nerve center of a cyber security program and SOC.

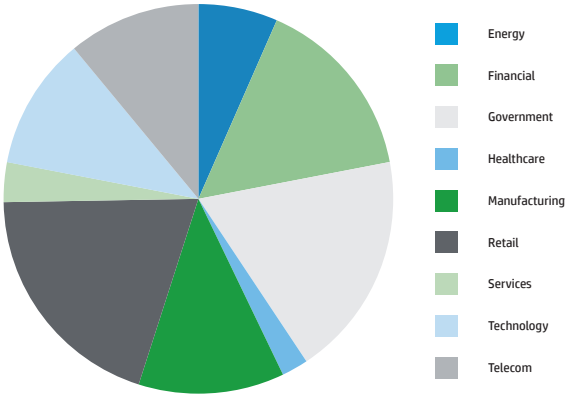
HP Enterprise Security Products portfolio includes the industry-leading HP ArcSight suite of logging and security information and event management (SIEM) products and services. The HP ArcSight ESM product revolutionized the modern SIEM market. SIEM is often referred to as a "force multiplier" for security technologies and is at the core of modern SOCs. SIEMs perform centralization and correlation of discrete data types, enable intelligent correlation of that data, integrate business and asset context, provide an interface for investigation and operational workflow, and generate metrics and reports. The SIEM is the technical nerve center of the cyber security program and SOC. HP formed the SIOC practice in 2007, dedicated to defining SOC best practices and building enterprise-class SOCs. This team combined the experience gained while implementing SIEMs within SOCs since 2001 with experts who have designed, built, and led SOCs for some of the world's largest organizations. Since its inception, the SIOC team has iteratively matured a methodology for SOCs that has been adopted worldwide by dozens of organizations. HP created the security operations maturity model (SOMM) in 2008 to help clients by assessing their current SOC state against industry best-practices and individual goals, and to build plans based on experience to close the gap in the most effective and efficient manner. The SOMM is not a self-assessment that can lead to misleading results, but rather an objective review of an organization's capabilities led by a subject matter expert. The elements of assessment within the SOMM are based on the HP SIOC methodology, as derived from over a decade of experience in dozens of enterprise SOC environments.

HP's industry-leading products, proven methodologies, and a decade of experience with the largest dataset of its kind make HP uniquely qualified to produce this report.

Assessments per year



Total Assessments by Industry



Security operations maturity model and methodology

Capability Maturity Model for Integration (CMMI) is a process improvement approach that provides organizations with the essential elements of effective processes. It can be used to guide process improvement across a project, division, or an organization. CMMI helps integrate traditionally separate organizational functions, set process improvement goals and priorities, provide guidance for quality improvement, and provide a point of reference for appraising current processes. HP has modified the CMMI approach in order to effectively measure the maturity of an organization's security operations capability. The HP model, named the security operations maturity model (SOMM), focuses on multiple aspects of a successful and mature security intelligence and monitoring capability including people, process, technology, and supporting business functions.

The SOMM uses a five-point scale similar to the CMMI model. A score of 0 is given for a complete lack of capability while a 5 is given for a capability that is consistent, repeatable, documented, measured, tracked, and continually improved upon. Organizations that have no formal threat monitoring team will typically score between a level 0 and level 1 because even an organization with no formal full-time equivalent (FTE) or team performs some monitoring functions in an ad-hoc manner. The most advanced security operations centers in the world will typically achieve an overall score between a level 3 and level 4—there are very few of these organizations in existence today. Most organizations with a team focused on threat detection will score between a 2 and 3.

SOMM level	Rating	Description
Level 0	Incomplete	Operational elements do not exist.
Level 1	Initial	Minimum requirements to provide security monitoring are met. Nothing is documented and actions are ad hoc.
Level 2	Managed	Business goals are met and operational tasks are documented, repeatable, and can be performed by any staff member. Compliance requirements are met. Processes are defined or modified reactively.
Level 3	Defined	Operations are well-defined, subjectively evaluated, and flexible. Processes are defined or modified proactively. This is the ideal maturity level for most enterprise SOCs.
Level 4	Measured	Operations are quantitatively evaluated, reviewed consistently, and proactively improved utilizing business and performance metrics to drive the improvements. This is the ideal maturity level for most managed service provider SOCs.
Level 5	Optimizing	Operational improvement program has been implemented to track any deficiencies and ensure all lessons learned to continually drive improvement. Processes are rigid and less flexible and significant overhead is required to manage and maintain this maturity level, outweighing the benefits achieved.

Some areas should be rigid, repeatable, and measured while other areas should be flexible, adaptable, and nimble.

SOCs typically have a large number of processes and procedures. SOMM offers a great architecture to help organize, maintain, and improve this body of work. For most organizations, a consolidated aggregate score of SOMM level 3 is an appropriate goal. Some areas should be rigid, repeatable, and measured while other areas should be flexible, adaptable, and nimble. The mixture of rigid and flexible processes and procedures allows for a mature SOC to provide effective monitoring with an aggregate maturity score of 3. This maturity level ensures that critical processes and procedures are documented and subject to demonstrable, measured improvement over time, while still allowing deviations and ad-hoc processes to emerge to address specific threats or situations. In practical terms, this means that any given analyst on any shift, in every region will execute a given procedure in exactly the same manner. Additionally, when an analyst finds an error or change needed in operational procedures, they can make an on-the-spot correction and all subsequent analysts will benefit immediately from the improvement.

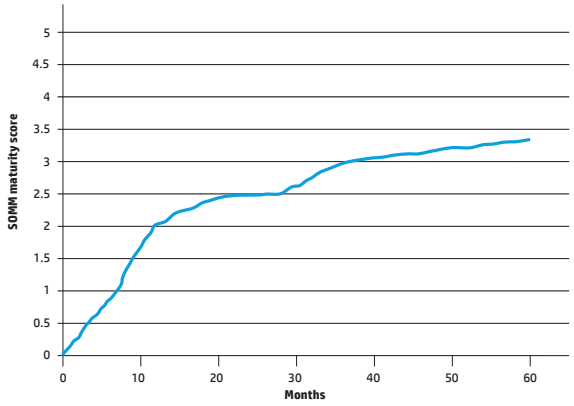
Business	People
Mission	General
Accountability	Training
Sponsorship	Certifications
Relationship	Experience
Deliverables	Skill Assessments
Vendor Engagement	Career Path
Facilities	Leadership

Process	Technology
General	Architecture
Operational Process	Data Collection
Analytical Process	Monitoring
Business Process	Correlation
Technology Process	General

The HP SOMM assessment focuses on four major categories, each of which have several subcategories. Aspects of people, process, technology, as well as business alignment are reviewed using a mixture of observation and interview techniques. Organizations being assessed are asked to demonstrate documented proof of claims made during interviews in order to ensure that scores are not artificially inflated.

These four main categories and all subordinate areas are scored independently using a weighted average technique and then combined to create an overall SOMM maturity score for the organization. This approach allows an organization to track maturity growth in each category or subcategory in order to identify areas of opportunity or strength in addition to focusing on the overall combined score. Regularly scheduled assessments allow SOCs to measure maturity growth over time. However, the growth curve is logarithmic and therefore major gains are achieved initially and then the SOC will see smaller gains in maturity as time progresses. Organizations must continue their maturity focus to avoid slipping backward on the maturity scale. Most SOCs with a funded and dedicated effort that leverages an existing framework and expert consulting will achieve an aggregate maturity score of 2.0 within a year, 2.5 within two years, and 3.0 within three years. Organizations that opt to build such operations independent of an existing framework or experienced program management will struggle to meet and maintain a level of 1.7.

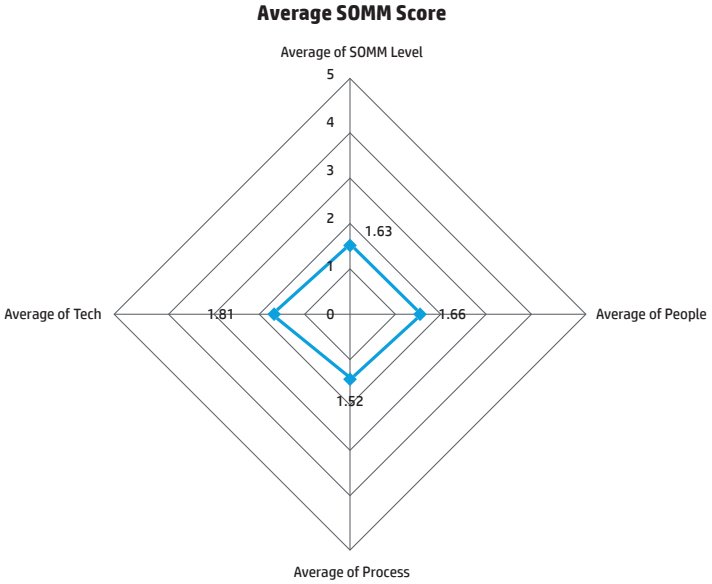
Typical maturity curve over 60 months



Industry averages

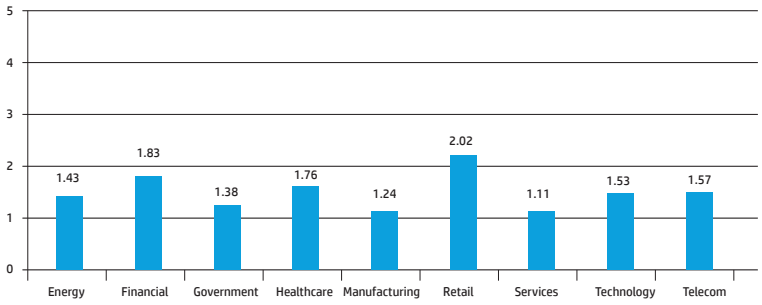
The average SOMM score for an enterprise is 1.63, which indicates that most have a large amount of room for improvement.

Over the course of five years, HP has performed 93 SOC maturity assessments around the globe. This sample set allows HP to draw conclusions about overall maturity of the security monitoring programs in place at the world's largest companies. In each of the areas measured, the industry average score falls between a 1 and 2. We see that of the areas measured, technology is the strongest average at 1.81. This fact makes sense when you consider that engineering and technology deployment tasks are usually the focus in most security organizations. People and process average scores are lower, closer to 1.5. This reinforces what we see when working with companies who have a SOC as well as those that have not yet built this capability. Most organizations focus heavily on technology solutions without putting the proper effort into managing the people and process aspects of a cyber defense program.



Looking at average scores by industry vertical, we see that the retail and financial industries are the most mature on average. This is due to the fact that financial and retail companies were early targets of cyber attacks with financial loss experienced. Additionally, these industries were the most directly affected by the introduction of the Payment Card Industry Data Security Standard (PCI-DSS). While the PCI-DSS standards did not provide a complete roadmap to building a threat detection and response capability, the penalties introduced for level 1 and 2 merchants combined with high visibility losses provided a very clear business case for investing in a capable security program, including the creation of dedicated SOCs.

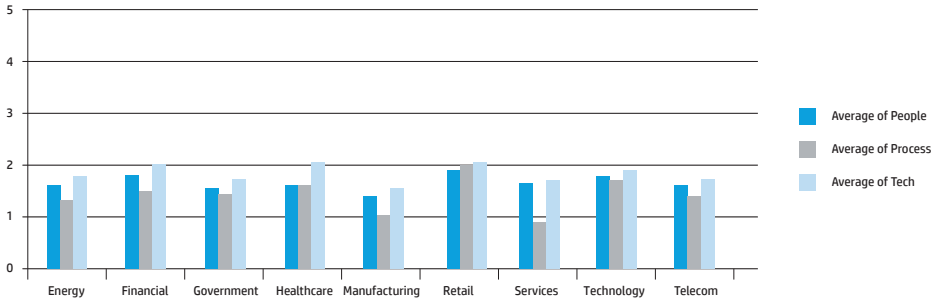
Average SOMM Score by Industry



The majority of industries are weakest when it comes to process.

Even with the increased regulation for the financial and retail industries, the average score is not to the recommended level of 3. Looking deeper, each industry vertical is strongest in technology. The majority of industries are weakest when it comes to process. This is the area where most companies should strive to do better.

Average SOMM Score by industry by assessment area

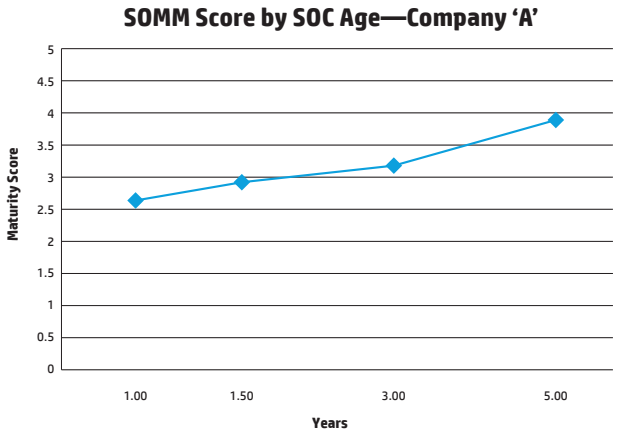


Customer case studies

Below are case studies of three companies, each of which had three or more maturity assessments within a three-year period. HP has worked with numerous companies to assess capability growth over a period of time and some companies will have an annual or more frequent assessment performed based on business need.

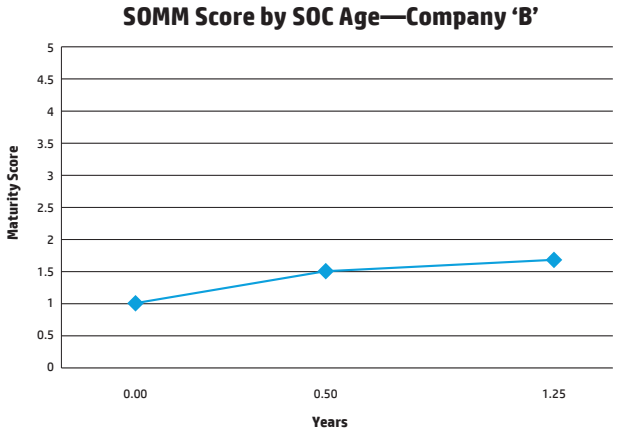
Company 'A'

Company 'A' is a Fortune 100 company, which runs a 24x7 SOC to detect cyber threats against the organization. The SOC was not assessed until it had been in operation for nearly a year. The company was assessed four times between 2009 and 2013. Each assessment saw an increase in the overall SOMM score. It took the company two years to break the 3.0 barrier, which indicates that many of their processes and procedures were well documented, repeatable, and updated regularly, and the team was able to retain key staff over time. The SOC continued to increase scope and capability by adding additional use cases and monitoring procedures each year. This is the typical growth curve we would expect to see with the creation and development of a SOC capability.



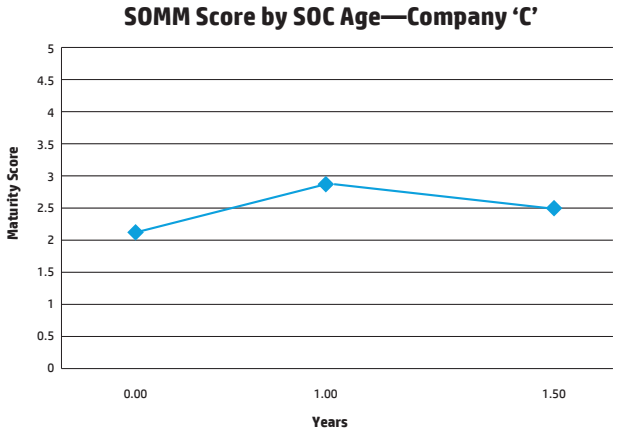
Company 'B'

Company 'B' is a Fortune 100 company, which runs a 12x5 SOC to detect cyber threats against the organization. This company also saw year over year maturity growth, but the total score and rate of growth were not as aggressive as Company 'A'. The main reason for the smaller growth curve is this SOC did not continue to add to its capability aggressively after the first year. The company focused on basic use cases during its initial build out, and once those were complete they did not continue to add scope to their monitoring function, limiting overall capability. The SOC became better, or more mature, at the few use cases that were implemented but they did not add capabilities, which led to a lower overall score as compared to Company 'A'.



Company ‘C’

Company ‘C’ is a Fortune 100 company, which achieves 24x7 coverage with two SOCs, one in the Americas and one in Asia, to detect cyber threats against the organization. This company started strong and had achieved nearly a full point growth within a year after the team’s inception. However, after the first year, the SOC began to decline in overall capability. The team was organizationally fractured as engineering and analysis were owned by two distinct management chains. Agreeing on common priorities between teams was a challenge and little was accomplished over time. The two SOCs on either side of the globe were not effectively sharing information. There had been a change in management within the analysis team and the SOC analysts were not following procedures that were defined during the build phase of the project. As a result, the maturity score declined between assessments. It is important to build the organization properly and maintain continuity, or there is a risk of repeating the mistakes of Company ‘C’.



Findings and lessons for the future

The four elements of security operations capability can be further broken down into assessment categories that are used in HP maturity assessments. Below are the findings and lessons learned for each of the elements: people, process, technology, and business.

SOMM score - people	
Average	**1.66**
Min	**0.12**
Max	**3.80**

People

Having the right people can often have the most profound impact on the overall capability of a SOC. The people capability and maturity score is derived by evaluating the below major elements of the people working in, around, and leading the SOC:

Assessment category	Elements of assessment
General	Roles definition Organizational structure Staffing levels Staff retention
Training	Funding Relevance Effectiveness
Certifications	Funding Relevance Effectiveness
Experience	Industry Organizational Environment Role
Skill assessments	Frequency Relevance
Career path	Candidate pools Succession planning Opportunity
Leadership	Vision Organizational alignment HR support Style and feedback Experience Span of control

- Most SOCs are struggling to find and retain skilled people. The market has a high variance in the definition of the skills and experience profile for SOC professionals, making it difficult to gauge if experience will transfer positively between operations. With a high demand for relevant security skills and sharply rising compensation for experienced individuals, some entities fail to properly appreciate or match the market competitiveness for employees, and attrition becomes a threat to sustainability and capability.
- Creating a stable team and minimizing attrition is important, but the most mature security organizations realize that an analyst has a finite shelf life. After 1–3 years, most analysts will want to move up or out of the organization. This may result in the analyst joining another part of the IT security organization, another IT team, or another company. SOCs must prepare for this inevitability and have hiring pipelines identified before the need to hire appears. Mature SOCs have robust relationships with local universities, ancillary teams in the company, and industry groups such as Information Systems Security Association (ISSA), ISACA, Open Web Application Security Project (OWASP), and others. This allows management to be prepared to reach out and bring in new talent on a regular basis.

- SOCs often produce the most well-rounded individuals in the IT security organization. SOC analysts must interact with almost every team in IT as well as many teams outside of IT. The most mature and capable SOCs will have a clear understanding and appreciation for the value of these individuals and will build a culture where continual investment and clear career progression opportunities exist.
- 24x7 scheduling is still presenting a challenge to most organizations. Common challenges include team culture, consistency, and attrition. Reduced and minimal staffing on afternoon, night, and weekend shifts leave those personnel disconnected from the larger team dynamic and culture. Additionally, heavy reliance on written communication impacts the consistency levels or security operations.
  - Team culture—24x7 SOCs tend to leave the "off-shift" personnel out of the loop except for email. This leads to a feeling of individuality instead of being part of a team.
  - Consistency—In 24x7 SOCs, it is extremely difficult to communicate needs and wants effectively when an operational need is present, which is partly due to non-communication with shifts that aren't in the midst of it all.
  - Attrition—This can be caused by the other two challenges. Both team culture and consistency across all shifts must be paramount.
- The harsh economic climate of the past five years has largely resulted in static or shrinking headcount for IT. Data volume was once a primary driver for staffing metrics, however risk-based correlation, effective analysis, and efficient operations are allowing large organizations to shrink their human footprint while maintaining the same levels of effectiveness. Additionally, some organizations are favoring 8x5 teams rather than 24x7 operations (outsourced or internally staffed). In these models high fidelity correlation rules and automation are leveraged for off-hour conditions, while security analysis and response activities are focused during business hours. This reduces the complexity and challenges of 24x7 operations significantly while still supporting the response requirements for many organizations.
- Organizational structure has a profound impact on the capability and maturity of a SOC. The most mature operations report up through a security-, risk-, or legal-led organization, often to a chief information security officer (CISO) who reports to the CEO or to a chief risk or compliance officer. SOCs that are organized within an IT operations organization may have high process maturity, but typically struggle with effective capability. This is due to a conflict in priorities with a focus on availability and performance as opposed to a focus on integrity and confidentiality in the upper levels of the organization.

SOMM score - process	
Average	**1.52**
Min	**0.12**
Max	**3.81**

Process

For a SOC to achieve high levels of overall maturity, there needs to be a solid, current, and relevant foundation of processes and procedures that guide consistent execution of critical tasks and define expectations and outcomes. A good set of processes and procedures enable a SOC to operate in a sustainable and measurable manner, and enable the SOC to easily support compliance efforts when necessary. Without solid processes and procedures, SOCs become reliant on "tribal knowledge" of individuals. Absences or turnover of these individuals can cripple the capability of the SOC. When assessing the process dimension of SOC, HP evaluates the following elements:

Assessment category	Elements of assessment
General	Knowledge management tools Document control Currency of documentation
Operational processes	Roles and responsibilities Incident management Scheduling Shift turnover Case management Crisis response Problem and change Employee onboarding Training Skills assessment Operational status management
Analytical processes	Threat intelligence Investigations Data exploration Focused monitoring Forensics Advanced content Information fusion
Technical processes	System and solution architecture Data flow and data quality Data onboarding User provisioning Access controls Configuration management Use case lifecycle Maintenance Health and availability Backup and restoration
Business processes	Mission Sponsorship Service commitment Metrics and key performance indicators (KPIs) Compliance Project management Continual improvement Knowledge management Business continuity (BC)/Disaster recovery (DR)

- The most successful SOCs are using an adaptable, portable, and operationally integrated process and procedure collaboration framework such as wiki. With a wiki, organizational documentation remains relevant and fresh, and contributions can be tracked and measured as part of the SOC's KPIs.
- The most capable and mature SOCs are bringing incident handling responsibilities closer to the front line of operations teams. Some organizations are executing containment or response activities at the analyst level, and effectively responding to threats more quickly and efficiently; they are reducing incident response cost and increasing the SOC's return on investment (ROI) by keeping workload off of CERT organizations. This shift is possible because of new technology investments, which allow for immediate forensic analysis of systems suspected of compromise. However, it is still not uncommon to find Fortune 50 companies that do not have any formal incident response capability, or rely solely on a shared responsibility that rotates through the IT organization—this is rarely an effective or sustainable approach.
- While many global or multi-national companies are operating SOCs in multiple geographies, doing so in a "follow-the-sun" model to accomplish 24x7 coverage does not prove as effective as having a 24x7 staff in a single location. Follow-the-sun solutions work best when performed for regional requirements or when staffing senior roles during prime shifts in geography in such a way that they support lower tier resources in a 24x7 location.
- Rotation of duties is critical in a SOC. Organizations that expect level 1 analysts to perform constant monitoring for long periods of time experience the lowest levels of capability and the highest levels of attrition. The most successful SOCs will rotate analysts through on-shift monitoring periods that alternate with other project-based tasks such as communications, research, special projects, and unstructured analysis. However, analysts should not be assigned administration tasks that are not aligned with the SOC mission as this will detract from their effectiveness.
- While core SOC processes are starting to improve at many organizations, incident response and handling is still a challenge for many teams. This has led to a paradigm shift where organizations are moving away from just intrusion prevention toward more threat detection and remediation. This requires that SOCs have well-defined processes in place to respond to potential data breaches and other malicious attacks.

SOMM score - technology	
Average	**1.81**
Min	**0.13**
Max	**4.06**

Technology

The technology in a SOC should support, improve, and even enforce the processes that are being executed. Technology does not provide value independent of people and process, and any implementation of technology in a SOC needs to have the necessary ecosystem in which to produce ROI. The elements of technology that are assessed in this report are below:

Assessment category	Elements of assessment
Architecture	Architectural process Documentation Technology coverage Alignment with business requirements
Data collection	Coverage Data quality Consolidation Data ownership Data access
Monitoring and analysis	Workflow management and measurement Investigation Data visualization tools Coverage Health and availability
Correlation	Aggregation Normalization Cross-technology Asset-relevant correlation Business rules correlation Subtle event detection Automated alerting Multi-stage correlation Pattern detection Dashboards and reporting
General	Infrastructure and endpoint management and administration Relevancy of data collected Currency

- Companies frequently purchase technology point solutions but fail to bring the data together for effective risk remediation and threat detection. A SIEM system is used by mature SOCs to correlate disparate security data and provide a single pane of glass for security analysts to monitor active threats.
- Newly formed SOCs will expose weaknesses in technology deployments that organizations were unable to recognize before. The most successful SOCs act as a force multiplier for security technology investments across the organization by optimizing configurations and integrating technologies through analysis and response activities.
- Organizations that achieve the highest levels of capability are fulfilling advanced use cases for security monitoring and analysis by leveraging SIEM technology. This often includes customizing a SIEM with business context, asset details, identity information, and intelligent correlation that evaluates data for operations and both short-term and long-term analytics. However, there are still entities that are relying on default vendor detection profiles that only address a basic set of use cases for the organization.

- Privacy efforts, including regional laws, are influencing the use cases that SOCs monitor. Technology features that enable advanced security use cases such as insider threat are not universally adoptable for global or multi-national organizations based on regional privacy law. Such use cases are falling under additional scrutiny based on the current privacy regulations and chief privacy officers are becoming more aligned with enterprise SOCs.
- Organizations are maximizing technological investments by implementing a use case methodology to determine which event sources to monitor. Technical resources are finite so each event source monitored by the SOC should have a specific associated use case. SOCs that lead with universal log management simply "boil the ocean" by logging every event source in the environment and are often overwhelmed by false positives reducing the value of the security operations. Operations that place successful broad log collection as a prerequisite to SOC development experience unnecessary delays and rework.

Business

The measurement of business functions and capability is a new addition to HP SOC Maturity Model as of 2013. Previously business items were spread through the people, process, and technology sections and were not a separate section of the assessment. An insufficient data set for this area exists in assessment results to share specific metrics in this year's report, however general findings and areas of assessment are below:

Assessment category	Elements of assessment
Mission	Alignment with business objectives Consistent understanding across business Alignment of operational capability with mission
Accountability	Operating and service level commitments Measurements and KPIs Role in regulatory compliance
Sponsorship	Executive support of SOC Levels of investment Organizational alignment
Relationship	Customer relationships Alignment with peer groups
Deliverables	Threat intelligence Incident notifications Reports and artifacts Operational reports
Vendor engagement	Levels of support Dedicated resources Business understanding Escalations

- SOCs frequently fail to define a succinct mission and scope. This dilutes the organization's perception of value due to misaligned expectations. It also can result in the SOC taking on responsibility for a variety of tasks that can cause resource strain and competing priorities. A SOC that becomes a dumping ground for tasks that do not align with the mission will lower the capability and maturity of the operation. There is a temptation in many organizations to treat a SOC as a security help desk. Those organizations that treat the SOC this way will not achieve a solid return on their investment. Not only do these tasks devalue the investment in the security analysts, but also quickly drive analysts to look for employment elsewhere.
- The most capable and mature SOCs define a mission, retain executive sponsorship, and clearly and frequently communicate the mission throughout the organization. Defining service level objectives for the business as well as effective business-level metrics for effectiveness and efficiencies ensure sustainable business support and focus. Executive sponsorship and communication is key to creating a sustainable capability. Those organizations that fail to gain proper executive sponsorship find themselves working under tighter and tighter budgets. With the exception of managed service providers, SOCs are always a cost center. When budgets are tightened, those SOCs without strong executive sponsorship will be asked to do more with less. It is important for the SOC to frequently communicate its successes to the rest of the organization, including those teams outside of IT.

- A SOC may be created as a business-hours only function (8x5), an extended-hours function (12x5, 18x7, 24x7), or a hybrid of in-sourcing and outsourcing. Many SOCs are now taking the last option, a hybrid services approach. They are leveraging managed and professional security services providers to augment their internal teams. The perceived ROI for such hybrid solutions can vary widely based on a variety of factors, but perception that security can be outsourced completely to a third party has clearly declined in favor of hybrid solutions. This shift has mainly occurred over the past 1–2 years. Many organizations have decided that the effort and cost to staff a 24x7 capability does not produce sufficient ROI. If there is a business requirement to monitor the environment around the clock then leveraging a third party to cover the less desirable hours in the day is a logical choice. The key point here is that the organizations using this model realize that the level of capability will differ between the in-sourced and outsourced teams, and they have made a risk-based decision that the cost to fully staff with their own people is not worth the more in-depth capability. An MSS provider will never know as much about an organization as an internal team, yet there is still value in leveraging an MSS in many situations. This is not to say that the days of the 24x7 enterprise SOC are over. There are still many companies that are building a 24x7 capability in-house, but more are taking the viewpoint that a highly skilled, business-hours, internal team will result in better outcomes than a mediocre 24x7 team.
- The most successful organizations are favoring an agile approach to project management for SOC-related projects. The dynamic threat and regulatory landscape causes traditional waterfall approaches to cyber defense projects to fail. This results in capabilities that are either late or off-the-mark for current needs. Adaptability is key for projects and continues to be key during steady state operations.
- The belief that SOCs and network operations centers (NOCs) can completely merge is proving incorrect. While communication between these two teams is essential, the work being performed and the skills and expectations of the individuals performing them are unique. SOCs that treat their analyst resources as a help desk or up/down monitoring team will miss the attacks that trained and experienced security analysts can find. The perception of a SOC as an operations center that processes security alerts is changing to one that respects the high requirements for original thought, broad skills, high professionalism, and critical thinking. Many organizations no longer treat the SOC analyst role as an entry-level position and are hiring seasoned security professionals to ensure the success of the team. The most mature SOCs are now hiring PhD level data scientists to extract meaning and security context from the vast data stores available to them in addition to “near real-time” monitoring staff.
- Mature SOCs develop and report operational metrics and KPIs to demonstrate the value of security investments. Security metrics should measure the efficiency and effectiveness of security operations. Additionally, SOCs with strong investment support from the business are viewed as key contributors to cost avoidance and risk reduction initiatives within the organization. The single most important success criterion or measurement is accurate detection of attacks in progress.

Conclusion

Cyber Security has been in the headlines and on boardroom agendas with unprecedented visibility. As organizations invest in defenses to mitigate the risks posed by an increasingly aggressive threat landscape, many are creating security operation centers. Whether branded as a SOC, a cyber defense center or any variety of titles being adopted across industries, these functional teams are necessary to detect and respond to attacks and breaches from multiple vectors. To be successful, these operations require maturity and capability in the people, processes, and technology that are the building blocks of the security program.

Based on over 90 assessments performed in 69 different SOCs over the past five years, HP has found that the average maturity of SOCs remains below target levels. To increase maturity and capabilities, SOCs will have to address the people, process, technology, and business aspects of their organization and quickly adopt best practices and market-proven solutions. There is no single product or service in the marketplace that provides the protection and visibility that organizations need, and even the organizations that choose to outsource portions of their security program will still need to invest in capabilities to manage those services and respond to events. Often organizations that have not invested in programs that provide situational awareness and visibility operate in a state of un-detected compromise and false confidence. Regular maturity assessments ensure that your SOC is increasing in maturity and capability to effectively and diligently reduce risk in your organization over time.

To learn more about the HP Security Operations Maturity Assessment go to hp.com/go/SIOC.

About HP Enterprise Security

HP is a leading provider of security and compliance solutions for the modern enterprise that wants to mitigate risk in its hybrid environment and defend against advanced threats. Based on market-leading products from HP ArcSight, HP Fortify, HP Atalla, and HP TippingPoint, the HP Security Intelligence Platform uniquely delivers the advanced correlation, application protection, and network defenses to protect today's hybrid IT infrastructure from sophisticated cyber threats.

Learn more at
hp.com/go/sirm

Sign up for updates
hp.com/go/getupdated

Rate this document

4AA5-0501ENW, January 2014