Business white paper

State of security operations

2015 report of capabilities and maturity of cyber defense organizations

Table of contents

Abstract

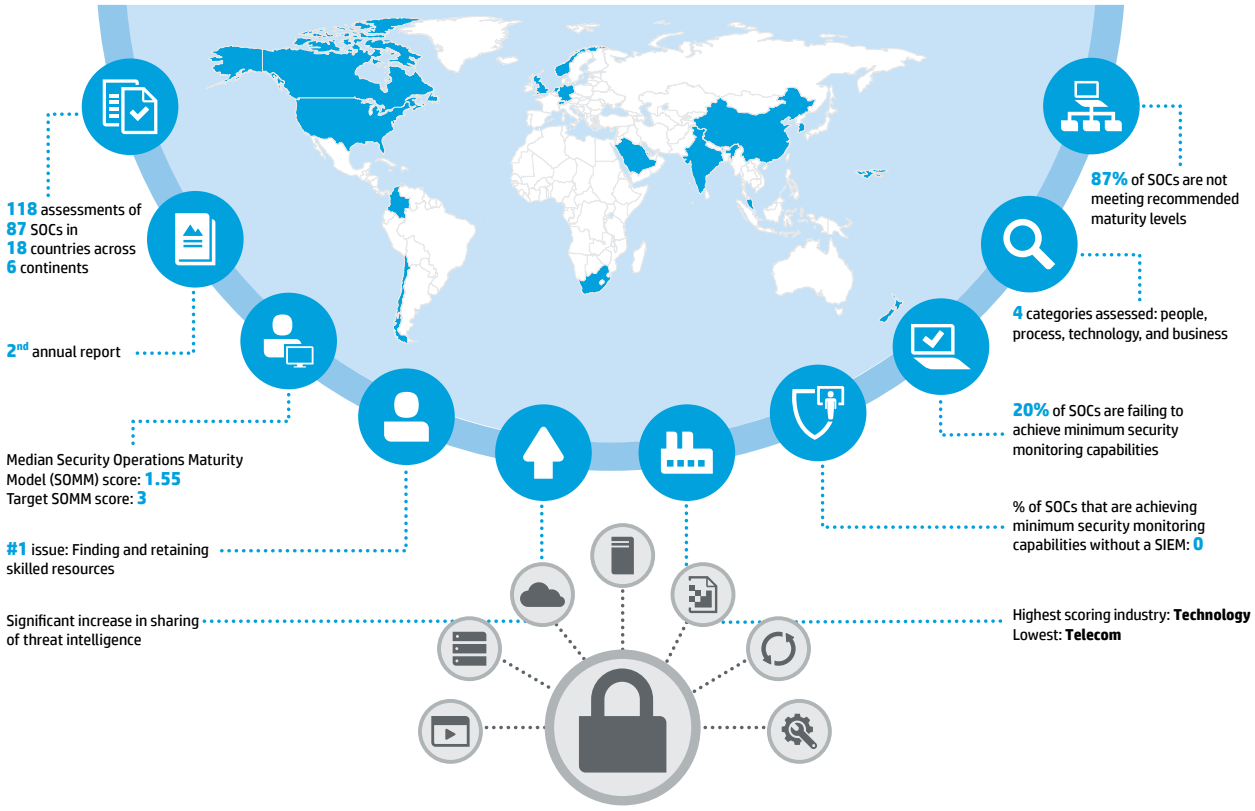
Organizations around the globe are investing heavily in IT cyber defense capabilities to protect their critical assets. Whether protecting brand, intellectual capital, and customer information, or providing controls for critical infrastructure, the means for incident detection and response to protect organizational interests have common elements: people, processes, and technology. The maturity of these elements varies greatly across individual enterprises and industries. In this 2nd annual report, HP provides updates to 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 cyber defense and enterprise security operations centers (SOCs), HP has worked with more of the world's top cyber defense teams 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 87 discreet SOCs in 118 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 18 countries on 6 continents. This is the largest available data set from which to draw conclusions about the state of cyber defense and enterprise security operations around 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 cyber defense capability.

Figure 1. 2015 report of capabilities and maturity of cyber defense organizations



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

The ideal composite maturity score for a modern enterprise cyber defense 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 higher levels of maturity are costly to achieve and that in the quest for higher maturity, operations often suffer from stagnation, rigidity, and a low level of effectiveness. Cyber defense teams (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, effectiveness, and breadth that the MSSP and its customers accept with this level of maturity. Once the ideal maturity level is achieved, a cyber defense team'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 96 percent; the number of successful attacks annually, per company, has increased by 144 percent in the last four years.[1] The time it takes to resolve a cyber attack has increased 221 percent over this same period. With these staggering numbers, there is a clear need for improvement in the effectiveness of enterprise security operations to limit the impact and improve the time to resolution of such events. This report summarizes data gathered during maturity assessments performed by HP and shares trends pertaining to 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 cyber defense teams as organizations move into the fifth generation of security operations.[2]

1 out of 5 SOCs are not minimally prepared to respond to, much less detect, cyber threats affecting their organization.

HP has found that 20 percent of cyber defense organizations assessed failed to score a SOMM level 1. This means that 1/5th of SOCs are not providing minimum security monitoring capabilities to their organizations. By comparison, the 2014 State of Security Operations report[3] found that 24 percent of cyber defense organizations scored below a SOMM level 1. Additionally, 66 percent of SOCs and cyber defense organizations were only achieving minimum ad-hoc threat detection and response capabilities. 87 percent of cyber defense organizations operate at sub-optimal maturity and capability levels. The assessments have shown some interesting trends:

- Organizations are willing to seek capital for "do-it-all" technology that is flexible and can perform advanced tasks.
- Organizations often neglect to seek operational budgets to staff the proper resources or to develop the needed processes resulting in solution deployments that don't provide the expected value. This has caused organizations to accept immature capability that produces basic results or that only addresses simple issues, but does not allow them to achieve strategic business goals, minimize risks, or secure their environments.
- Due to major breaches and industry-wide vulnerabilities such as Heartbleed and Shellshock, there has been a significant increase in organizational willingness to share threat intelligence and temporary solutions to problems. Organizations are still looking to their vendors and technology partners as the primary resource to help them through these urgent, massive scale events.
- Visible breaches have led to C-level and Board-level exposure to the financial and brand impact on organizations; through media coverage and internal evaluations, executives are asking questions about the ingredients necessary for organizational recovery, the importance of a security operations program that provides situational awareness, and the need for security organizations to provide ongoing reporting on business risk and incident activity. Security organizations are being asked to communicate the actual business impact of threats, incidents, and vulnerabilities.

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. This group of organizations recognizing the true financial impact of a breach is growing rapidly.

[1] Based on internal analysis of the results from the 2011–2014 "Cost of Cyber Crime Study" reports from Ponemon Institute.
[2] hp.com/go/5gsoc
[3] hp.com/go/StateofSecOps2014

Summary of findings

HP assessments of organizations worldwide continue to show the median maturity level of cyber defense teams remain well below optimal levels. Many of the findings and observations from the 2014 State of Security Operations report[4] are still valid. Additionally, the following observations and findings have surfaced:

- **Security is a board-level conversation**. Cyber defense teams must provide visibility and high-level business focused reporting to the C-suite and Board. This has driven cyber defense teams to shift their thinking towards the business.
- **The security analyst skills gap is real**. The top issue facing security organizations is availability of skilled resources. This is exacerbated by high levels of attrition in many security organizations and low levels of employer loyalty.
- **Organizations are most concerned about detecting cyber espionage and the compromise of information or systems that can be exploited for financial gain**. Intellectual property theft remains of great concern for organizations. Coordinated large scale attacks in the past year focused on credit card and protected health data that has direct monetary value.
- **Common architectural vulnerabilities have forced InfoSec and IT organizations to work together**. Heartbleed and Shellshock required simultaneous IT-driven patching and security operations situational awareness to look for possible infiltrations based on these vulnerabilities. Vulnerability management and incident response became symbiotic for a short period of time in these instances.
- **The most capable and mature SOCs have a very specific and defined scope**. These SOCs are able to focus their time, tools, and skills on security incident monitoring and response and are not diluted with IT and administrative tasks.
- **SOC alignment under Legal or Governance, Risk & Compliance organizations increases their authority**. When aligned with IT, systems uptime and availability typically trumps addressing security issues.
- **SOCs are overwhelmed with the number of vendors and technologies they need to implement**. A great focus is being put on investing in technologies and frameworks that can provide quick ROI but provide limited capabilities for future expansion. Some organizations are making the mistake of implementing "right now" technologies that seem to meet basic goals but find 12 months out that they have outgrown these technologies.
- **Cloud, SaaS, and IaaS security use cases are entering the SOC**. As many organizations undergo IT transformation projects to alternate modern platforms, security considerations are top of mind. Organizations are requiring Cloud, SaaS, and IaaS vendors to both meet security standards, but also to provide visibility into network, system, application, and user activity for monitoring with enterprise SOCs.
- **Hunt teams are increasing in popularity**. Many cyber defense teams operate in a reactive mode, responding to alerts from systems designed to detect known threats. Most compromises are still present for weeks to years before being detected, and are usually detected by a third party. To close this gap, many organizations are creating roles to "hunt" through existing security and system data to identify conditions of interest and previously undetected incidents.
- **"Advanced Security Analytics" and Big Data for security tools are gaining momentum**. Big Data security analytics solutions are the shiny new technology that cyber defenders are drooling over. While these tools are providing value in some organizations, the space is still being defined and mileage varies greatly based on a variety of factors. Sustained value from these solutions are most apparent where findings are able to be operationally integrated with enterprise security operations capabilities.
- **SOC workflow and metrics programs can drive the wrong behavior**. Ticket-based workflow and metrics around event counts and time-based SLAs encourage SOC to focus on the quantity of events closed rather than quality and risk reduction from effective security investigations. Analyst focus is on quick turnaround and closing alerts rather than addressing organizational security issues.

[4] hp.com/go/StateofSecOps2014

- **Internal MSS organizations are being created within companies to service different business units**. Many large enterprises, especially those that have multiple business units or have grown by acquisition, will have a single business unit make the security investment of building a cyber defense capability, develop it, and offer services to other internal business units to share costs and keep security in-house.
- **Cyber defense capabilities are only as strong as their weakest link**. Organizations that invest in monitoring teams but neglect to define and implement meaningful use cases that model security detection efforts around key business processes are not able to achieve ROI. Similarly, organizations that invest in technology and detective measures but fail to define roles and responsibilities for responding to detected incidents are not able to achieve ROI. Organizations that are able to focus their efforts, end-to-end, around securing and protecting high value business processes are the most successful.
- **Classroom training and certifications are not a substitute for multi-domain experience when it comes to staffing cyber defense roles**. Environment-specific training programs are a necessity to refine the specific skills required of cyber defenders.
- **Management and team leadership has an enormous impact on the overall capability and effectiveness of a cyber defense team**. Leaders must be able to cultivate and maintain a culture where individuals believe in the work that they are performing and feel supported by leadership in their daily activities as well as their professional development. Leaders must be able to work effectively across organizational barriers to accomplish complex tasks. They must also balance subject matter knowledge with an awareness of when external assistance is necessary.

Relevance of our data—qualification to present this report

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 cyber defense and SOC teams. 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 data set of its kind make HP uniquely qualified to produce this report.

Security Operations Maturity Model and methodology

The 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 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 represented by a tightly controlled, rigorously measured system with fully documented detailed procedures, very high consistency and repeatability, and pervasive measurement. 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 SOCs 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 1 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 for 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 improvements.

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 to ensure that scores are not artificially inflated.

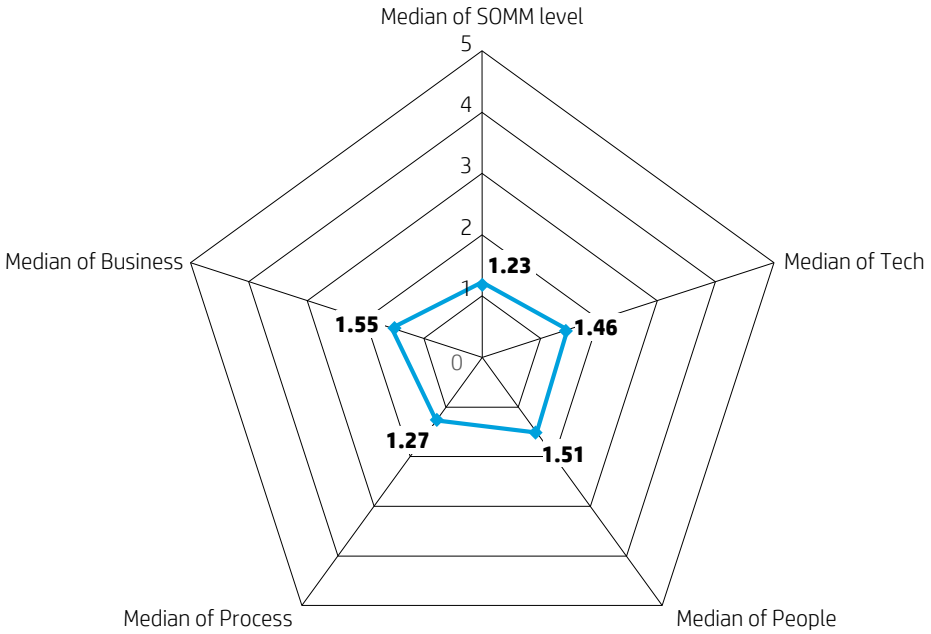
These four main categories and all subordinate areas are scored independently using a weighted average technique and then combined to create an overall SOMM maturity score for the organization. This approach allows an organization to track maturity growth in each category or subcategory to identify areas 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. SOCs with a funded and dedicated effort that leverages an existing framework and expert consulting can 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.

Industry medians

Over the course of six years, HP has performed 118 SOC maturity assessments around the globe. This data sample set allows HP to draw conclusions about overall maturity of the cyber defense programs in place at the world's largest companies. In each of the areas measured, the industry median score continues to fall between a 1 and 2. We see that of the areas measured, technology remains the strongest with a 5-year median of 1.73 and business is where we see the most growth. Technology has traditionally scored the highest because engineering and technology deployment tasks are usually the focus in most enterprise security organizations. Business maturity has increased significantly in the last two years presumably due to the heightened awareness of threats from high-profile breaches. People and process median scores remain lower, closer to 1.6 and 1.4. 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 matching that effort with the people and process aspects of a cyber defense program.

Most organizations focus heavily on technology solutions without matching that effort with people and process.

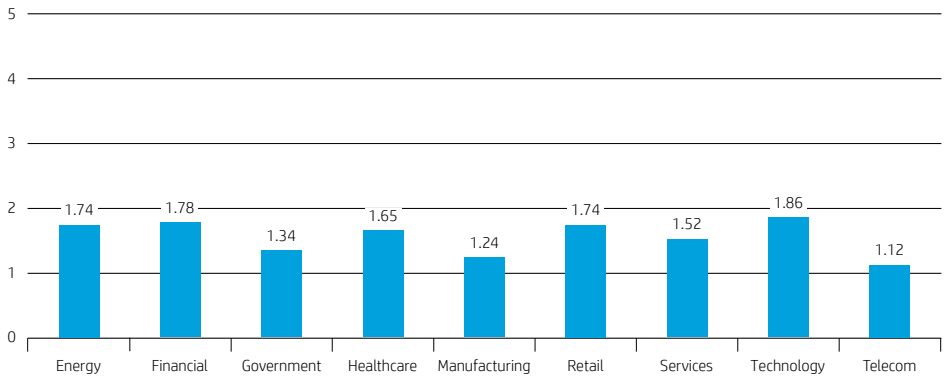
Figure 2. 2014 Median SOMM score



Looking at median scores by industry vertical, we see that the retail industry from this data set is highest. We attribute this to the fact that PCI requirements for level 1 merchants combined with multiple visible breaches in this industry have driven significant investments into cyber defense programs. Even with these investments, the median maturity score is below the recommended levels and breaches continue to occur. The financial industry remains stronger due to their prevalence in cyber attacks and potential for direct financial loss from compromise.

The financial industry remains stronger due to their prevalence in cyber attacks and potential for direct financial loss from compromise.

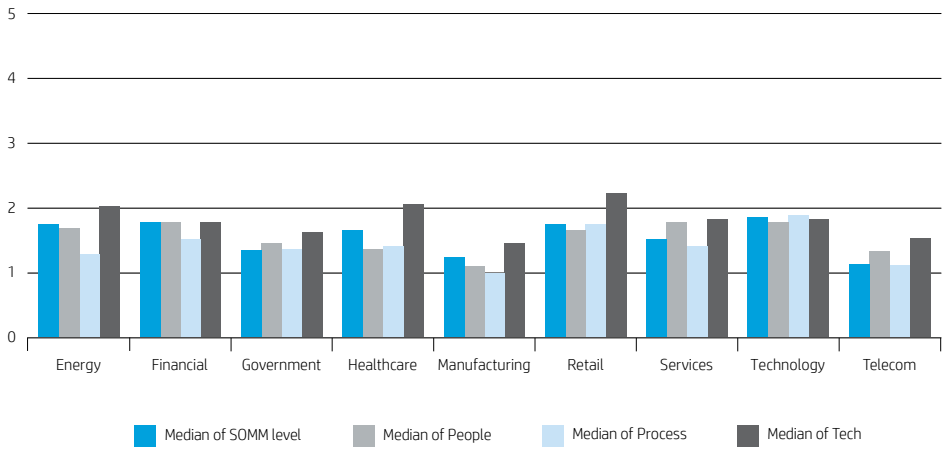
Figure 3. Median SOMM score by industry—5 years



- Healthcare organizations are becoming more aware of the value of health data and are investing more in cyber defense. These operations tend to monitor traditional network data as well as electronic medical records access for security incidents as well as fraud. These investments, especially in medium size organizations are recent and we expect future healthcare SOMM scores to trend higher.
- The energy industry is investing heavily and making slow progress in cyber defense monitoring capabilities. This industry has established a number of working groups and vendors are attempting to solve industry-specific use cases such as Industrial Controls System (ICS) monitoring. Leveraging best practices from other industries for SOC is occurring in pockets, but has not yet gained wide implementation across the industry. Rolling out new security measures in these very high risk but low change environments is a tedious process and faces challenges from logistics through corporate-to-field understanding and adoption of standards.
- Retail organizations have experienced coordinated point of sales (POS) system attacks, where common adversaries and tools were used across multiple companies in a short window of time. This has led to an increased use of threat intelligence and an uptick in collaboration within this vertical. Mature SOCs work this sharing of threat intelligence into their workflows and participate in sharing within their industry.

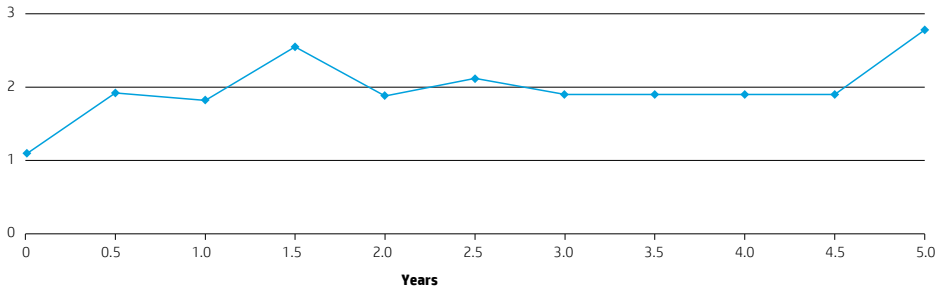
Even with the increased regulation for the financial and retail industries, the median score is below the Managed level of (2) and far below the recommended level of defined (3). Looking deeper, each industry vertical is strongest in technology. The majority of industries are weakest when it comes to process. This is the area where most companies should strive to do better.

Figure 4. Median SOMM score by industry by assessment area graph—5 years



SOC maturity over time

Figure 5. Median SOMM score by age of SOC



The assessments performed show an incline during the development of a cyber defense organization and then a decline starting around 18 months and lasting for three or more years. The contributing factors in this dip include:

Leadership changes and attrition lead to shifting goals and priorities.

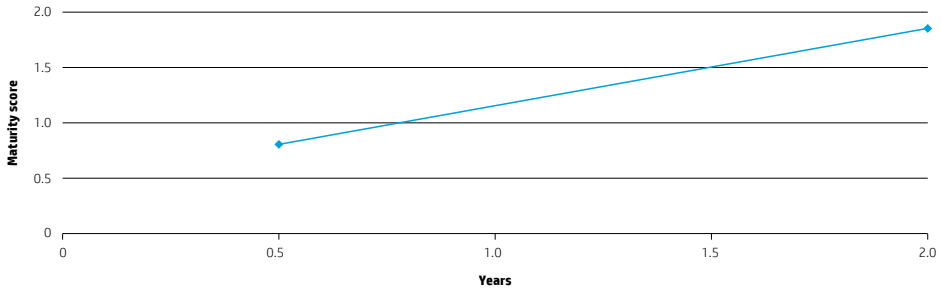
- Leadership change and attrition lead to shifting goals and priorities. The position lifespan of a CISO averages two years. If a mission of the cyber defense organization is not clearly laid out, the priorities of the organization can be derailed as resources enter and leave the organization.
- Poor execution of, or non-existent, fiscal planning can lead to stagnation. A three year fiscal plan (or roadmap) is recommended to ensure budget is attained and the priorities of the cyber defense organization can be worked and developed continually.
- Remaining reactive to external forces rather than transitioning into a predictive or ready state by investing in data analytics, threat intelligence, conducting incident response tabletop exercises and evangelizing their research (outputs) and efforts across the businesses/organizations.
- Failing to establish, maintain, or enhance their rhythm of the business (RoB); daily operations, workflow, influence across organizations and business unit, effective communication and collaboration amongst their immediate organization and across organizations.
- SOC performance goals (or commitments) that are not aligned to the business of security intelligence and incident detection. Many organizations' job descriptions and performance goals are misaligned; successful deployment and maintenance of systems or projects or ticket driven to attempt to illustrate value, hence their employees are not being effectively assessed against the core mission of the cyber defense organization.
- Lack of investment and innovation in appropriate technologies, capabilities, and the personnel.
- Not continuing to leverage the SIOC methodology and practices (processes and procedures) developed and executed during the initial cyber defense build-out stage.

Customer case studies

Below are case studies of three companies, each of which had multiple maturity assessments over time. 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.

Customer A

Figure 6. SOMM score by SOC age—Company "A"

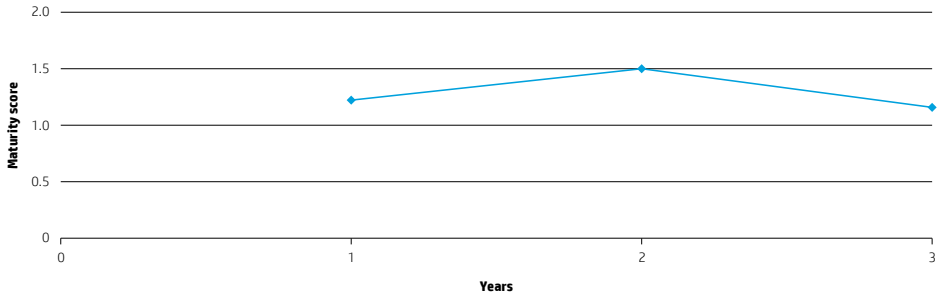


Customer A began the project to build and staff a cyber defense center two years ago. The project was initiated with an incomplete understanding of requirement and a tight budget, leading to what was essentially a complete restart of the project after the first year. The initial effort was constrained by corporate-wide restrictions in hiring, and attempted to staff analyst roles completely through college new hire resources. While this team had some bright individuals, the overall experience of the team did not allow sufficient opportunities for peer mentoring and growth. After the first year, executive management for the corporate information security program changed. The new executive leader saw the cyber defense center as a key project, not only for the protection of the company, but also for the overall value to this company's customers.

By aligning the cyber defense capability with the company's go-to-market efforts, additional funding and support was secured for the program. This allowed the cyber defense center to relocate from a satellite office to the company's headquarters location. While this caused a stutter-step in continuity of efforts with resource changes, the new cyber defense center location also allowed the addition of experienced personnel from the industry, including the formation of formal security engineering and Hunt Team operations staff. Customer A's cyber defense center is following a proven formula for creating base operations and is executing against a roadmap that is aligned with the business, securing support to maintain the upward capability projection.

Customer B

Figure 7. SOMM score by SOC age—Company "B"

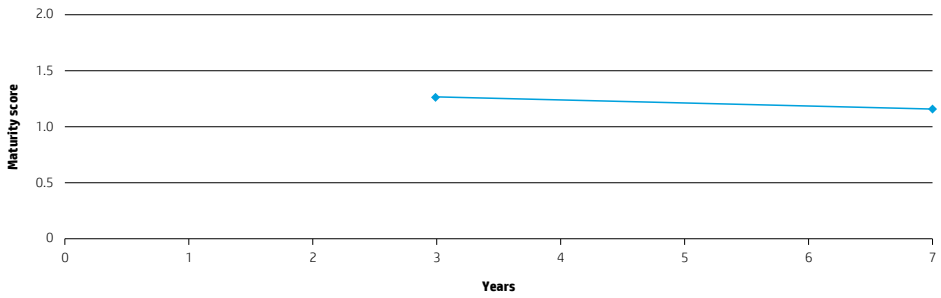


After years of outsourced security monitoring, Customer B realized that their cyber defense needs exceeded what their outsourced provider could provide. While this organization began, their transition to an internal cyber defense and enterprise security operations capability with good intentions and made initial gains in capability, they were not able to keep pace with industry capabilities achieve the ROI that they aspired to over the course of three years. Contributing factors to this decline were many.

An initial investment was made in developing their cyber defense team, however they invested non-linearly with SIEM lagging too far behind the formation of a security monitoring team. The project team experienced high levels of turnover for key roles such as project management, affecting the continuity of the project over time. The cyber defense team experienced high levels of attrition over the course of these three years, where first there was a loss of experienced individuals with key relationships and knowledge of the organization followed by high turnover of new team members due to multiple factors. Vendor negotiations dragged on for key technology components, and rather than a streamlined security and logging infrastructure, multiple technologies and vendors remained in the environment for long periods of time—this caused confusion and complexity. Additionally, the team was slow to identify key business processes, prioritized use cases, and ultimately failed to negotiate the onboarding of critical data feeds across the organization. This customer will need to address core organization problems before they are able to progress significantly against their cyber defense program goals.

Customer C

Figure 8. SOMM score by SOC age—Company "C"



Customer C has operated their SOC for close to a decade. An assessment at the three year mark found that their level one operations team were performing repetitive tasks, had low team morale, and that technology was not being leveraged to the level that would be expected in an organization with such a high level of investment. Level 2 cyber defense resources worked outside of the level 1 team, and with very disconnected processes and tools. While new management at this company during their first assessment had great plans to course correct and improve their overall capability, a return assessment four years later show that the capability had declined rather than improved.

These declines were a result of turnover of key resources in the customer security team, continuous cost pressures from the business on the security team, and a security industry that advanced quicker than the company could keep pace with. Company C today is in a different mode of operation than it was during the first assessment and is in the process of optimizing the operational capability for efficiency and effectiveness, and plans to leverage outside expertise to leapfrog the operational challenges of the past.

Findings

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. New findings from the most recent analysis are noted with **NEW** bullets. Findings from the previous State of Security Operations 2014 report[5] that continue to be relevant are also included.

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:

SOMM score—people	
Median	**1.51, 5 year median: 1.55**
Min	**0.49**
Max	**2.55**

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

NEW Skilled security resources are in very high demand. Most SOCs are struggling to find and retain skilled people. Hiring resources with the proper skills can take months, and is often simply not possible, so many organizations have turned to development programs to cultivate their analysts. Analysts are often developed from individuals who show passion and aptitude for security and come from IT administration, system support, and external roles such as law enforcement. Organizations with these development programs also benefit by ensuring that the skills taught are the exact skills required for their operations.

NEW Regions of the world where IT labor is unionized can struggle with the evolving skills and scope of IT security positions. Organizations can't easily expand the scope of their security staff and the result can be an acceptance of outdated or limited security skills.

NEW Teams comprised of various skills and specialties (network architecture, DBA, support, automation, etc.) are generally most effective. A skills assessment should be performed across the organization yearly and any identified gaps should be filled with training or new team members.

[5] hp.com/go/StateofSecOps2014

- Creating a stable team and minimizing attrition is important, but the most mature enterprise security organizations realize after one to three years, most analysts will be ready 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. Cyber defense teams 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.
- Cyber defense teams often produce the most well-rounded individuals in the IT, Risk, and Compliance organizations. Analysts must interact with almost every team in IT as well as many teams outside of IT. The most mature and capable organizations 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.
- Where around-the-clock security monitoring requirements 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.
- 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	
Median	**1.27, 5 year median: 1.42**
Min	**0.42**
Max	**2.52**

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)

NEW SOCs that are utilizing hunt teams are realizing value when they tie the findings back into the SOC processes. In practice, the "hunt" activity is as much about understanding normal activity that improves other detective measures as it is about directly detecting malicious activity. When attacks or patterns are detected, there must be a process that defines how that information is used and acted upon. Additionally, findings should be fed back into the real-time operations so they can be handled through regular SOC processes in the future.

NEW Successful cyber defense teams utilize threat intelligence and have built processes around its use. The consumption of this intelligence by tools and by people must be defined so it can be quickly acted upon when needed.

NEW Hybrid cyber defense teams use a combination of internal and external (professional or managed services) resources to operate their cyber defense capability. These hybrid environments require advanced maturity of their processes to avoid incidents falling through the cracks.

- 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.

SOMM score—technology	
Median	**1.46, 5 year median: 1.73**
Min	**0.27**
Max	**3.2**

Technology

The technology in a SOC should support, enforce, and measure 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

NEW Organizations who implement a universal log management (ULM) without a SIEM are failing to achieve real-time security threat monitoring and mature operations. The ULM system provides for aggregation and storage of data but not the correlation, automation, and incident workflow possible with a SIEM. In addition, many logging projects do not evaluate collected information for usability in the same way that a security-oriented SIEM project would. This often results in unexpected gaps in log collection or data format issues that are only discovered during an incident response activity, when the logs are most needed and are unusable.

NEW Many organizations are looking to deploy Big Data security analytics solutions. Big Data should be considered a problem statement, not a toolset. Tools such as leading SIEM and Business Intelligence (BI) tools are being adapted to address the opportunity for broad detection and analytics from large data sets. Tools marketed in this space vary widely in capability and ease of use. Some solutions require teams of dedicated data scientists while others operate from proprietary algorithms or threat intelligence sources. Other solutions are little more than log storage solutions that support post-incident forensics activity. Value from security data analytics solutions are most apparent where findings are able to be operationally integrated with security operations capabilities.

NEW Successful SOCs assess all aspects of their operations (people, process, technology, and business) before making drastic changes. Some organizations put the blame on technology for failed ROI or threat mitigation, which leads to a rip-and-replace of systems. These major projects leads to a reduction of maturity in operations while the new solutions are being ramped up and often do not fix the original issues.

- 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 give a level of visibility into infrastructure that organizations were unable to recognize before—often highlighting misconfigurations, deviations from reference architectures, and unknown business processes. 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 adaptable 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 actively monitor. Technical resources are finite so each event source monitored by the SOC should have a specific associated use case. ULM projects can run in parallel to SOC build projects, but the events that will be actively monitored need to be thoughtfully defined as use cases before presentation for analysis. Operations that place successful broad log collection as a prerequisite to SOC development experience unnecessary delays and rework.

SOMM score—business	
Median	**1.55, 2 year median: 1.55**
Min	**0.82**
Max	**3.24**

Business

The measurement of business functions and capability was a new addition to HP SOC Maturity Model in 2013. Basic trends are shown below and 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

NEW Board level and C-level visibility into security threats has led to an increased need for business-level communication on the state of organizational cyber defense and associated projects. Mature security operations organizations should be able to provide explanations of threats and incidents and their impact on specific parts of the business. Executive reports should have a high degree of automation for data crunching and be provided with a regular cadence. The SOC needs to be seen as a business enabler.

NEW Effective SOCs are often aligned with the governance, risk and compliance (GRC) or legal organizations. This alignment can give a security organization more authority to act during incidents. It can also allow for a more stable budget that is not constantly being repurposed for IT. Regardless of where a SOC sits in the organization, the business goals must be constantly acknowledged and addressed by the security organization.

NEW Interest in converged security implementations have increased this year. Successful organizations have been able to pull IT, physical and database system information into their SIEMs to identify performance issues or outages that indicate an attack-in-progress. Difficult political landscapes can restrict SOC access to the necessary system information so executive sponsorship and business alignment is necessary.

- SOCs frequently fail to define a succinct mission and scope. This dilutes the organization's perception of value due to misaligned expectations. It can also 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 (SLOs) 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 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. 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. 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. There are still many companies that are building and operating a 24x7 capability in-house, but more are taking the viewpoint that a highly skilled, business-hours, internal team with effective tools can independently, or with the augmentation of a managed service, meet their objectives.
- 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. Leading cyber defense teams do not view the SOC analyst role as an entry-level position and hire seasoned security professionals to ensure the success of the team. The most mature cyber defense teams are staffing 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

Security operations maturity and capabilities goes beyond a technology investment. The continuation of highly publicized breaches and the effect to the entirety of a business and consumers demands ever more effective and efficient cyber defense organizations. These organizations must continually mature in all operations categories including people, process, technology and business.

Based on over 118 assessments performed in 87 different SOCs over the past six years, HP has found that the majority of cyber defense organization’s maturity remains below target levels. A continual increase in sharing threat intelligence and best practices in people and process will be necessary to attain the higher desired levels of maturity. There is no “silver bullet” product or service in the marketplace that can provide the protection and operational awareness that organizations need. A continuous investment into all facets of a cyber defense organization are necessary to achieve and maintain optimal maturity. Regular maturity assessments ensure that your SOC is increasing in maturity and capability to effectively and diligently reduce risk in your organization over time.

About HP Enterprise Security

HP is a leading provider of security and compliance solutions for the modern enterprise that wants to mitigate risk in hybrid environments and defend against advanced threats. Based on market-leading research and 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/SIOC


Share with colleagues


Rate this document

4AA5-6510ENW, January 2015