Hewlett Packard Enterprise

Business white paper

# State of Security Operations

2016 report of capabilities and maturity of cyber defense organizations



# Table of contents


3 Introduction

4 Abstract

4 Executive summary

6 Summary of findings

7 Relevance of our data—qualification to present this report

8 Security operations maturity model and methodology

9 Regional trends

10 Category medians

11 Industry summary

12 Customer case studies

14 Findings

22 Conclusion

23 About HPE Security

## Introduction

This is the third annual State of Security Operations report and I am excited to join this team at such a pivotal moment in the evolution of security monitoring. Over the last three years, the industry has seen the transformation of IT to hybrid models including cloud, mobile, social, and Big Data, as well as a continued focus on cost management within the security operations center (SOC). These forces are putting pressure on cyber defense centers to keep pace with the New Style of IT while consuming fewer resources. This, coupled with the continued collaboration and professionalization of the attacker community, explains the **year-over-year decline in overall security operation maturity** that we are reporting for 2015.

This decline in maturity and effectiveness leads us to believe there is a transition needed in the modern SOC. Hewlett Packard Enterprise sees this as a pivotal moment for SOC leaders to **adapt and re-invent** their operations in order to show definitive value to the business. We did observe a few adaptive trends in the more modern SOCs in the form of hunt teams, deception grids, and data analytics-driven security. As a consulting practice in our own network of SOCs, Hewlett Packard Enterprise has dedicated time and resources to these types of innovative techniques that leverage the power of data and analytics to stay ahead of the adversary.

As businesses continue to adopt new cloud and mobile functionality rapidly, we find the edges of the network even more blurred, and our definitions of data ownership and breach responsibility continue to evolve. Staffing and training continue to be the foremost challenge of the modern SOC. This is paving the way to hybrid staffing models and hybrid infrastructures that require less in-house expertise. As a result, highly skilled security team members can then be utilized for a more specialized hunt and analytics-focused work.

There is no question this year has been both an exciting and challenging time to be in the field of cyber security. On one hand, it is disheartening to see the continued decline in the maturity and effectiveness of security operations, while, on the other, I know that we are in the middle of an exciting and transformative change in our field. You can feel it. We must go where the data leads us, and we believe that is to widen our definition of security operations to leverage analytics, data science, Big Data, and shared intelligence to become more effective in protecting today's digital enterprise.

**Chris Triolo**
**HPE Vice President, Security Product Global Services**

## Abstract

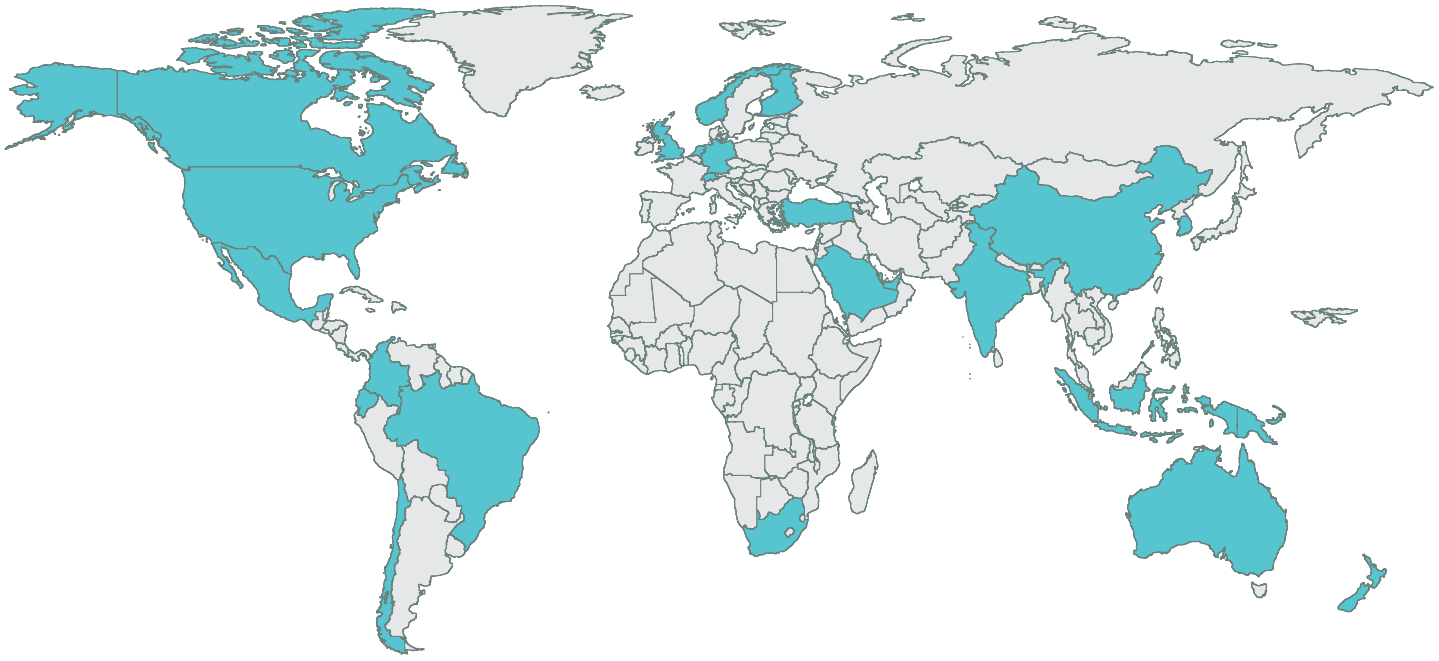
Organizations around the globe are investing heavily in information technology (IT) cyber defense capabilities to protect their critical assets. Whether protecting a brand, intellectual capital, and customer information or providing controls for critical infrastructure, the means for incident detection 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 the State of Security Operations Maturity report, Hewlett Packard Enterprise provides updates to the capabilities, lessons learned, and performance levels of security operations based upon maturity assessments performed on worldwide organizations.**

Hewlett Packard Enterprise has over a decade of experience in supplying information security technology to world's most advanced cyber defense and enterprise SOCs. We have worked with more of the world's top cyber defense teams than any other IT security organization, so we are uniquely qualified to publish this report.

## Executive summary

HPE Security Intelligence and Operations Consulting (SIOC) has assessed the capability and maturity of 114 discreet SOCs in **154 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 **26 countries** on **six continents**. This is the largest available dataset to draw conclusions about the state of cyber defense and enterprise security operations around the globe.



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

The **HPE 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 information security trends and threat capabilities. The focus of the assessments is inclusive of the business alignment, people, process, and technology aspects of the subject's security 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.

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. Hewlett Packard Enterprise 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 an overall low level of effectiveness.

Cyber defense teams (or providers offering managed SOC services) who 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. Given an agile and adaptive threat actor, optimizing for repeatability and consistency is only marginally effective.

Managed security service providers (MSSPs) should target a maturity level of between 3 and 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 evolve capabilities continually, to keep pace with a rapidly evolving threat landscape.

To learn more about 5G/SOC, visit **hpe.com/software/5gsoc**

While the fifth-generation (5G/SOC) of security operations is still evolving, they are best equipped to recognize the change in the threat landscape and are approaching the challenge holistically. They are training analysts in security counter-intelligence, surveillance, criminal psychology, and analytical thinking to augment the technology investment. Most organizations have not implemented a 5G/SOC but those who have, seem to have benefited greatly from the intelligence-driven methodologies, information sharing, and the human adversary approach.

The industry is still struggling with measuring the cost of cyber security breaches upon commercial organizations. The adage had been that the impact following an adverse security event was measurable through declining stock prices. Yet, a few months and years after highly visible breaches of entertainment, financial services, banking, and investment, as well as retail organizations it is clear that beyond the immediate uncertainty, investors and consumers are not penalizing those organizations.

Market data shows that recovery, as far as stock price is concerned, takes a few weeks. Business disruption and data loss do represent the greatest cost components of significant security events.[1] Following a breach, recovering organizations do face long-term effects on profitability such as higher costs from new security programs, litigation, and organizational turnover.

This report summarizes data gathered during maturity assessments performed by Hewlett Packard Enterprise and shares enterprise security 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 centers**.

[1] Cost of Cyber Crime Study, Ponemon, October 2015

**Hewlett Packard Enterprise has found that over the last five years, 25 percent of cyber defense organizations that were assessed failed to score a security operations maturity model (SOMM) level 1. This is aligned with the current year finding that 24 percent score below a 1. We find that a quarter of security organizations operate in an ad-hoc manner with undocumented processes.**

**In 2015, only 15 percent of assessed organizations are meeting business goals and are working toward or have achieved recommended maturity levels. This leaves 85 percent of organizations that are not achieving the recommended maturity levels, which is slightly lower than last year's findings.**

The assessments have shown some interesting trends:

- The mind-shift to the "we've already been breached" way of thinking has fueled the industry's adoption of hunt teams and analytics solutions. When implemented properly, these teams and tools help organizations identify attackers that have gotten past the traditional security measures in place. Most organizations are striving for analytics capabilities while only a few are mature enough to benefit significantly from these tools and programs.
- Access to skilled security resources continues to be the main concern of enterprises. To deal with this, organizations are moving toward hybrid staffing and hybrid security infrastructure models. These new models require less in-house expertise while retaining control over critical pieces of the security organization's detection capability.
- Another result of the staffing squeeze is an increased adoption and investment in security orchestration and automation. Organizations are looking to streamline incident investigation and remediation so that the more highly skilled (expensive) resources can be utilized for breach investigations and hunt team.

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 dramatically**.

## Summary of findings

The Hewlett Packard Enterprise 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 previous State of Security Operations[2] report are still valid. Additionally, the following observations and findings were made:

- **Migration to hybrid infrastructure—**there is a significant increase in the need for security operations for hybrid IT infrastructures; within the cloud, from the cloud, and across the cloud, as IT organizations take advantage of modern computing methods. There is an industry misperception that adoption of cloud equals transferred risk. This is not the case. Risk persists and unless the hosted solution includes infrastructure components to retain situational awareness, SOCs are losing the ability to monitor critical applications and data.
- **Hybrid staffing—**as a reaction to industry personnel shortages, organizations are implementing an MSS overlay of managed security information and event management (SIEM) or off-hours monitoring. This allows the organization to retain the technology and security information but lean on external resources for level 1 monitoring. They typically keep level 2 and incident response capabilities in-house.
- **Advancements in incident and investigation orchestration—**tools such as incident response case management and operational orchestration are being adopted from the IT operations world to automate manual post detection activities.

[2] **State of security operations** (2015 report of capabilities and maturity of cyber defense organizations) **hpe.com/software/StateofSecOps2015**

- **Disaster recovery is still a priority—**the fear of getting "bricked" by an attack requires organizations to maintain solid business continuity and disaster recovery programs.
- **Is Hunting replacing monitoring?—**some organizations that are not able to make an OPEX investment in people, subscriptions, and processes are turning to fast search capabilities instead of monitoring solutions. These organizations are not reaching minimum security capabilities and are operating without any real-time monitoring abilities.
- **Using SOC as a competitive advantage—**security operations capabilities are being used as a selling point for organizations. It showcases their commitment to security and ability to monitor for threats.
- **Regional impact from unions—**employee protection in some markets does not allow information security (InfoSec) managers to develop talent from within, manage up, or manage out. This limits the capabilities and advancement of a security organization.
- **Global cyber security agreements—**an increase in global agreements between countries to limit or stop cyber-attacks on each other has occurred over the last year. The effects of these agreements have not yet been noticed in cyber defense centers around the globe.
- **Variation in role definition—**there remains a lot of variation, especially in mid-market enterprises, around role definition of the CISO and the security organization. The CISO role can vary greatly from enterprise to enterprise based on diversity of industries, organizational reporting structures, enterprise size, and IT security budget.
- **Overwhelming number of vendors—**vendor management remains a top time requirement for CISOs. Reliance on partners and service integrators is necessary for larger enterprises.
- **Information sharing is increasing—**the sharing of threat information continues to increase. Reliance on government provided threat information is decreasing due to the perceived lack of timeliness. This increase can have a negative effect as analysts lose time by chasing alarms for indicators that are more nuisance than directed threat.

## Relevance of our data—qualification to present this report

HPE Security Products portfolio includes the industry-leading HPE ArcSight suite of logging and SIEM products as well as services. The HPE ArcSight Enterprise Security Management (ESM) products 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 security operations 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, as well as generate metrics and reports. The SIEM is the technical nerve center of the cyber defense program and SOC.

Hewlett Packard Enterprise 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.

Hewlett Packard Enterprise created the SOMM in 2008 to help clients by assessing their current SOC state against industry best practices and individual goals. We also built plans based on experience to close the gap in an 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 the assessment within the SOMM are based on the HPE SIOC methodology, as derived from over a decade of experience in dozens of enterprise SOC environments.

Our industry-leading products, proven methodologies, and a decade of experience with the largest dataset of its kind make Hewlett Packard Enterprise uniquely qualified to produce this report.

## Security operations maturity model and methodology

The CMMI is a process improvement approach that provides organizations with the essential elements of effective information security processes. It can be used to guide process improvement across a project, division, or an organization.

The CMMI helps integrate traditionally separate organizational functions, set process improvement goals and priorities, provide guidance for quality improvement, and offer a point of reference for appraising current processes. Hewlett Packard Enterprise has modified the CMMI approach to measure the maturity of an organization's security operations capability effectively. The HPE model, SOMM, focuses on multiple aspects of a successful and mature security intelligence and monitoring capability including people, process, technology, and the 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 1 and 2.

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

| SOMM LEVEL | RATING | DESCRIPTION |
|---|---|---|
| **Level 0** | Incomplete | Operational elements do not exist. |
| **Level 1** | Initial | Minimum requirements to provide security monitoring are met.<br>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.<br>Compliance requirements are met. Processes are defined or modified reactively. |
| **Level 3** | Defined | Operations are well defined, subjectively evaluated, and flexible.<br>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. |

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 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. They are 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 a change is needed in operational procedures, they can make an on-the-spot correction and all subsequent analysts will benefit immediately from the improvements.

The HPE SOMM assessment focuses on four major categories, each of which has 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.

| 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 |

These four main categories and all subordinate areas are scored independently. They use a weighted average technique and combine 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, therefore, major gains are achieved initially, and 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 1.5.

## Regional trends

There are only minor discrepancies in regional maturity and capabilities across the globe. While SOCs across Europe (BeNeLux, DACH, Nordics, and the UK) and North America have typically experienced slightly higher SOMM scores, HPE SIOC's access to organizations in South America has resulted in noticeable improvements in the past year. This is due to an increase in investment in the areas of security monitoring, operations, managed services, and automation. The MENA region (Middle East, and North Africa) experiences lower SOMM scores speculatively based on smaller investments as well as due to its focus on the people and process aspects of their security programs.

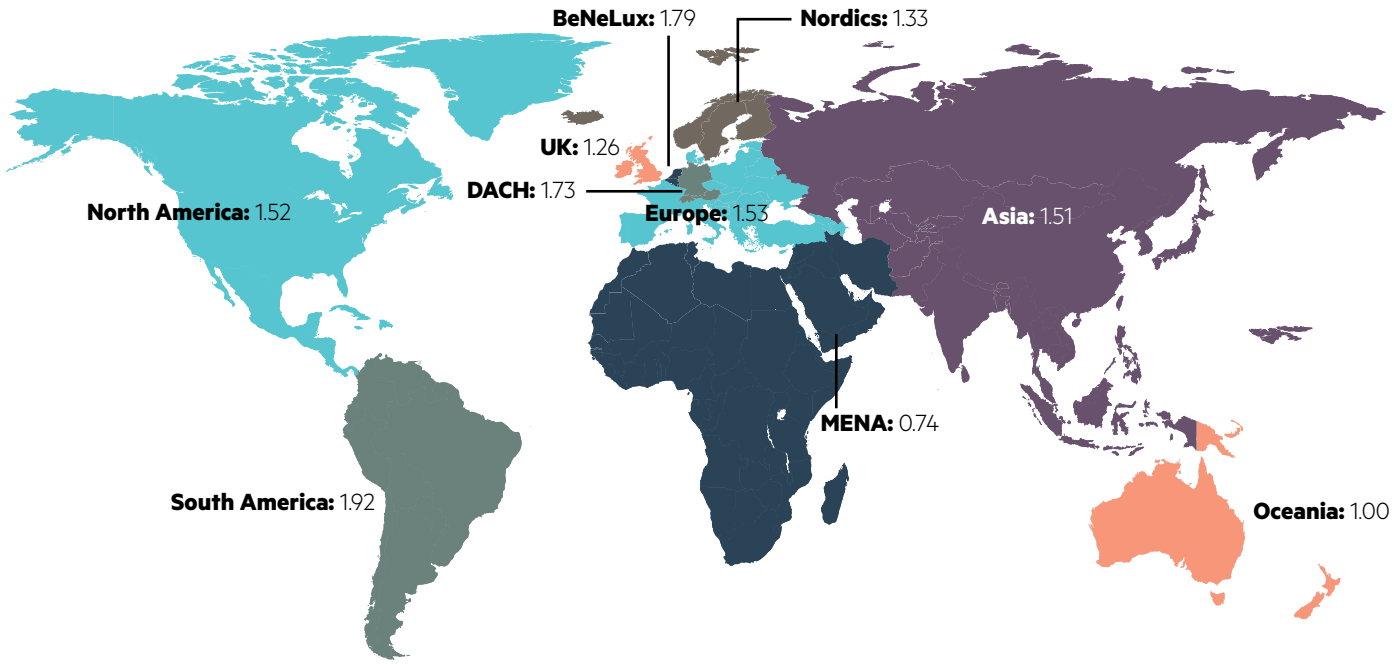



**Figure 1:** Median SOMM per region

## Category medians

Over the course of seven years, Hewlett Packard Enterprise has performed 154 SOC maturity assessments around the globe. This data sample set allows Hewlett Packard Enterprise to draw conclusions about the 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. For the first year ever, we see that the business SOMM area has overcome technology with the strongest median score of 1.50. This is consistent with the rapid maturity growth in the business areas that we have seen for the past few years and mirrors the impact of security to an entire business and not just an IT organization.

Technology remains strong with the second-highest SOMM scores with a median of 1.46. 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 1.4 and 1.2 respectively. 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 and tools without matching that effort with the people and process aspects of a cyber defense program.

**Overall median SOMM score by dimension in last five years**

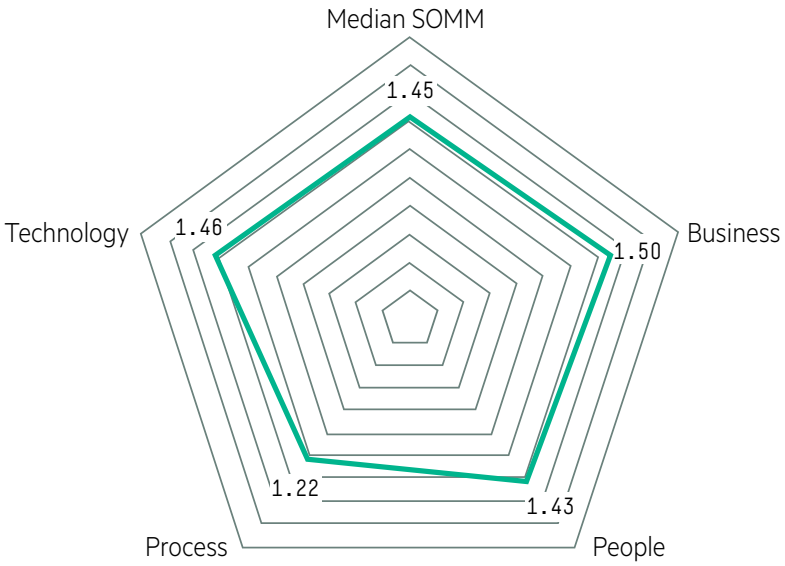



**Figure 2:** Median SOMM score–last five years

## Industry summary

Looking at median scores by industry vertical, we see that technology organizations have had the highest SOMM scores over the last five years. As an industry, technology is higher because of advanced investments and balance across all dimensions of the SOMM. The importance of equal focus and investment to all four areas of the SOMM has resulted in the most-effective organizations. Over the last five years, Hewlett Packard Enterprise also noticed a significant dip in the telecom industry. As the team investigated the change, it noted that many new telecom organizations are joining the cyber defense market in developing economies. We expect them to grow and improve as they formalize the investment in these young offerings and programs.

**Median SOMM score by industry in last five years**

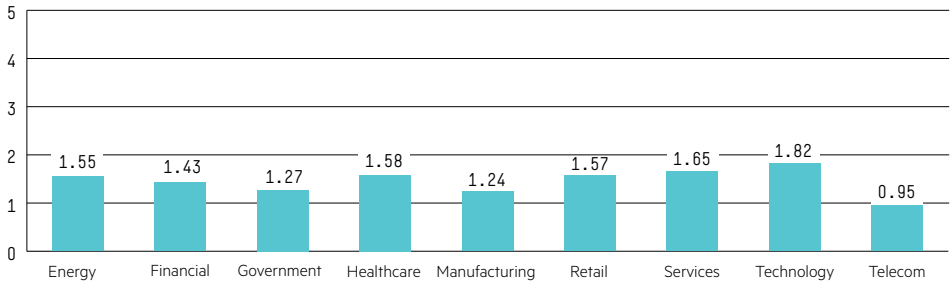



**Figure 3:** Median SOMM score by industry–last five years

**Industry findings**

- Security monitoring in the Internet of Things (IoT) has seen an emergence of industry-specific use cases such as smart meter monitoring in the energy industry and medical device monitoring in healthcare. This capability has raised the capabilities scores for organizations with implementations in both of these industries.
- International government agreements have not yet had an effect on security monitoring or operations.
- The most mature organizations in each industry are layering on capabilities to hunt for unknown attacks and using advanced analytics as an aid to detection. Maturity and effectiveness are still attributed to individual enterprises and no industry trends can be seen yet.
- Education (public sector under the Government industry) lags behind in capabilities. The biggest risk is intellectual property (IP) theft and the vast numbers of people accessing the network from different countries make baselining for advanced analytics difficult.

The majority of industries are weakest when it comes to process. Even with the increased regulation for the financial and retail industries, the median score is below the "Managed" level (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 where most companies should strive to do better.

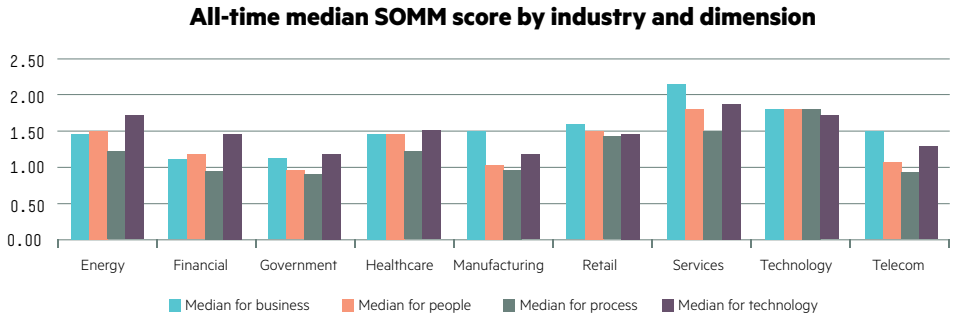



**Figure 4:** Median SOMM score by industry and dimension—last five years

## Customer case studies

Following are case studies of two companies, each of which had multiple maturity assessments over time. Hewlett Packard Enterprise has worked with numerous companies to assess capability growth over time and some companies will have an annual or more frequent assessment performed based on business need.

**Customer A**

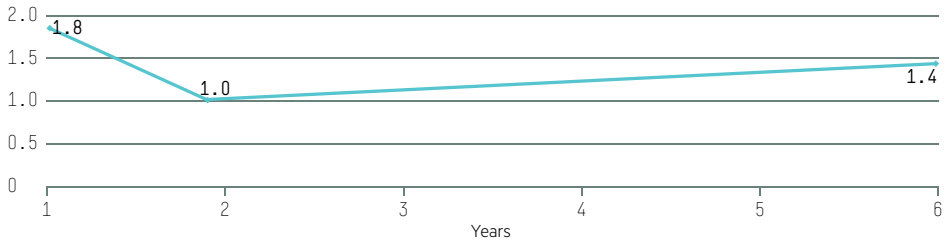



**Figure 5:** SOMM score by SOC age—Customer "A"

**Organization A** is in the public sector and runs a 24x7 SOC to detect cyber threats against the organization's multiple environments. Maturity has been a seesaw over the past six years mostly based on business challenges that adversely impact people, process, and technology investments.

Critical components present:

- Analysis of key performance indicators (KPIs) for Level 1 or 2 analysts are tracked and readily available
- Structured development program for analysts with continuous investment in key skills
- Repeatable operations components well documented with consistent execution across team

Critical gaps:

- Multitenant SOC missing overarching sponsorship and mission to overcome inconsistent agendas at mid-level manager roles
- Content development and data integration KPIs missing for SIEM engineers
- Infrastructure stability is an issue; rigid system management policies and guidelines have resulted in out-of-date systems

### Customer B

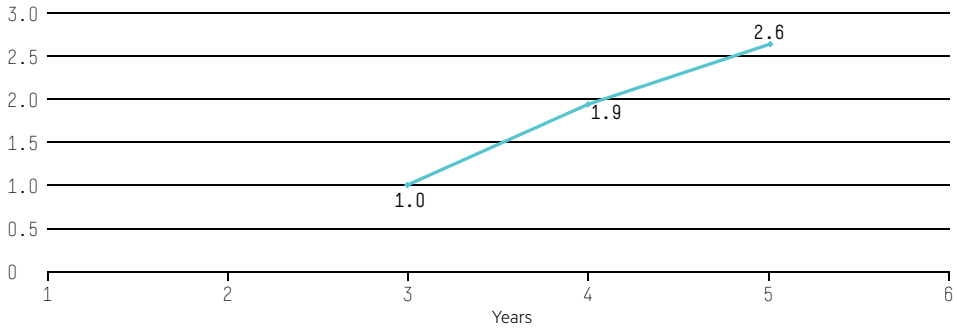



**Figure 6:** SOMM score by SOC age–Customer "B"

**Organization B** is in the energy sector and went through a rebuild under new leadership at the 3-year mark to develop a 24x7 SOC. There has been a steady maturity progression over a 3-year window and prescriptive investment across all SOMM areas.

Critical components present:

- Strong sponsorship from executive visibility of security ROI from SOC program and tools
- Collaborative culture with strong relationships inside and outside of security organization
- Investment in security solutions to meet strategic security needs

Critical gaps:

- Needs talent pipeline and repeatable program to support growth objectives
- Development to monitor custom, home-grown applications, and systems
- Expanded hunting and visual analysis for context and threats

## Findings

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

### People

**SOMM score for people**

**Median:** 1.58; 5-year median: 1.43

**Min:** 0.1

**Max:** 3.8

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 following major elements of the people working in, around, and leading the SOC:

| ASSESSMENT CATEGORY | ELEMENTS OF ASSESSMENT |
|---|---|
| General | Roles definition<br>Organizational structure<br>Staffing levels<br>Staff retention |
| Training | Funding<br>Relevance<br>Effectiveness |
| Certifications | Funding<br>Relevance<br>Effectiveness |
| Experience | Industry<br>Organizational<br>Environment<br>Role |
| Skill assessments | Frequency<br>Relevance |
| Career path | Candidate pools<br>Succession planning<br>Opportunity |
| Leadership | Vision<br>Organizational alignment<br>HR support<br>Style and feedback<br>Experience<br>Span of control |

**New**

- Utilizing hybrid staffing models such as outsourcing first-line analysis or various security operations functions can reduce the negative effect of attrition or skills acquisition. It must be paired with tight, well-defined processes to be effective and not miss anything when incidents are being handed from one group to another. Roles and responsibilities must be documented and agreed upon.

**New**

- The move to Big Data security analytics often requires hiring one or multiple data scientists. These resources are often very expensive due to their expertise level. Implement advanced analytics that do not require a data scientist on staff to run in order to reduce this cost.

**New**

- Non-security staff are still at the greatest risk of falling prey to phishing techniques and social engineering. Organizations that promote the existence of their security organization, instead of letting them exist in a dark corner, should have more effective programs on employee security education.

- 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 have 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.
- 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.
- 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.
- Teams comprising various skills and specialties (network architecture, dba, support, automation, and more) 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.
- Creating a stable team and minimizing attrition is important, but the most mature enterprise security organizations realize after 1–3 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), Information Systems Audit and Control Association (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 the afternoon, night, and weekend shifts leave the 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 for process**

**Median:** 1.44; 5-year median: 1.22

**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 support compliance efforts easily 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, Hewlett Packard Enterprise evaluates the following elements:

| ASSESSMENT CATEGORY | ELEMENTS OF ASSESSMENT |
|---|---|
| General | Knowledge management tools<br>Document control<br>Currency of documentation |
| Operational processes | Roles and responsibilities<br>Incident management<br>Scheduling<br>Shift turnover<br>Case management<br>Crisis response<br>Problem and change<br>Employee onboarding<br>Training<br>Skills assessment<br>Operational status management |
| Analytical processes | Threat intelligence<br>Investigations<br>Data exploration<br>Focused monitoring<br>Forensics<br>Advanced content<br>Information fusion |

| ASSESSMENT CATEGORY | ELEMENTS OF ASSESSMENT |
|---|---|
| Technical processes | System and solution architecture<br>Data flow and data quality<br>Data onboarding<br>User provisioning<br>Access controls<br>Configuration management<br>Use case lifecycle<br>Maintenance<br>Health and availability<br>Backup and restoration |
| Business processes | Mission<br>Sponsorship<br>Service commitment<br>Metrics and key performance indicators (KPIs)<br>Compliance<br>Project management<br>Continual improvement<br>Knowledge management<br>Business continuity (BC)/Disaster recovery (DR) |

**New**

- Orchestration of duties before, during, and after a breach can reduce the cost of the breach to an organization. Automation and integration of compliance, analysis, audit, and incident response tools should be implemented before an incident to be effective.

**New**

- Hybrid organizations must pay special attention to escalation and shift turnover processes between insourced and outsourced functions. Strictly defined and followed processes ensure that all relevant information is passed between groups and allows for the best capabilities at identifying and isolating breaches.

**New**

- Smaller organizations with combined IT and InfoSec organizations must ensure that incident response process do not have conflict between IT responsibilities of keeping the business running and InfoSec responsibilities of ensuring confidentiality, integrity of data, and availability of systems.
- 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.
- Successful cyber defense teams utilize threat intelligence and build processes around its use. The consumption of this intelligence—by tools and people—must be defined so it can be quickly acted upon when needed.
- 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 frontline 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 ROI by keeping workload off CERT organizations.

  This shift is possible because of new technology investments, which allow immediate forensic analysis of systems suspected of compromise. However, it is still common 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 multinational 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 for technology**

**Median:** 1.59; 5-year median: 1.46

**Min:** 0.13

**Max:** 4.06

## 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 as follows:

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

New

- Organizations that deploy tools, which push incident identification and remediation closer to the first-line analysts, will save money. An example is a right-click integration with a firewall from a SIEM console that allows an analyst to put a temporary block on a suspicious or malicious IP. This allows less-expensive resources to remediate incidents, which also fixes them faster than what would be possible through an escalation path.

New

- Flood of incident management and automation solutions are carving a market for cyber-specific incident tracking. This function previously existed inside of IT security management or governance, risk and compliance (GRC) ticket-based solutions. Many of these solutions integrate industry- and region-specific disclosure regulations, as well as vendor supplied investigation and remediation information. The more mature solutions take it a step further to enable the automation of investigation or remediation actions between technology products.

New

- Well-integrated organizations deploy application security monitoring use cases into their cyber defense centers. This allows them to identify issues with applications running in production, which can indicate possible serious breaches.
- 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.
- 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) are being adapted to address the opportunity for broad detection and analytics from large datasets. 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 after-incident forensics activity. Value from security data analytics solutions are most apparent where findings are operationally integrated with security operations capabilities.
- Successful SOCs assess all aspects of their operations (people, process, technology, and business) before making drastic changes. Some organizations blame the technology for failed ROI or threat mitigation, which leads to a rip-and-replace of systems. These major projects lead 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 earlier—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 adoptable for global or multinational 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 actively. 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 monitored actively need to be defined thoughtfully 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 for business**

**Median:** 1.50; 3-year median: 1.50

**Min:** 0.59

**Max:** 3.34

## Business

The measurement of business functions and capability have grown steadily over the last few years. Basic trends, general findings, and areas of assessment are as follows:

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

**New**

- Solid business-wide disaster recovery and continuity programs are required to tie into security operations. The threat of getting "bricked" by destructive malware can be mitigated with tight collaboration between IT backup and recovery organizations as well as the cyber defense group.

**New**

- CISOs are more increasingly coming from a business background. Earlier, this position was dominated by military and technical experience. No conclusions can be drawn at this point on if either background is more effective, however, it does indicate a shift toward acknowledging security as a core function of business and not just an IT function.

**New**

- Organizations are still struggling with risk management and aligned investments. Gaps can be masked through managed services and cloud without investment in monitoring observable secondary controls and measuring the development of risk-based use cases as a KPI. Organizations that understand risk, deploy observable secondary controls, and drive their teams to develop measurable use cases around those controls are more effective.

- Board-level and C-level visibility into security threats have led to an increased need for businesses-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.
- Effective SOCs are often aligned with the 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 security organization must acknowledge and address the business goals constantly.
- Interest in converged security implementations has 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 are necessary.
- SOCs frequently fail to define a succinct mission and scope. This dilutes the organization's perception of value due to misaligned expectations. It also results 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 and does 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. These tasks not only 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 as well as 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 are key to creating a sustainable capability. Those organizations that fail to gain proper executive sponsorship find themselves working under increasingly tight 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 communicate its successes frequently 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 the 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. Many companies are still building and operating a 24x7 capability in-house. Others are taking the viewpoint that a highly skilled, business hours-centric, internal team with effective tools can independently or with the augmentation of a managed service, can 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 cause 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, as well as 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 datastores 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 an accurate detection of attacks in progress.

## Conclusion

The industry continues to evolve toward a business mindset for security. This is seen through investment patterns, report-to chains, and stakeholder involvement. However, this has not made a great impact on overall maturity scores due to the continued focus on technology. People and process aspects of security operations still lag behind in capabilities and efficacy. This has a direct impact on the length of time it takes to identify and remediate breaches.

Hewlett Packard Enterprise continues to find that the majority of cyber defense organization's maturity remains below target levels. A continual focus on mastering the basics and creating a solid foundation of risk identification, incident detection, and breach escalation as well as response remains key to effectiveness. Benefits from advanced analytics capabilities and threat intelligence will only be realized if a strong foundation of security operations exists.

No "single" product or service can provide the protection and operational awareness that organizations need. A continuous investment into all facets of a cyber-defense organization is necessary to achieve and maintain optimal maturity. Regular maturity assessments ensure that your SOC is increasing in maturity and capability to reduce risk effectively and diligently in your organization over time.



## About HPE Security

Hewlett Packard Enterprise 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 HPE Security ArcSight, HPE Security Fortify, HPE Data Security (Voltage/Atalla), and HPE Security Research, the HPE Security Intelligence Platform uniquely delivers the advanced correlation, incident response orchestration, application protection, and information defenses to protect today's hybrid IT infrastructure from sophisticated cyber threats.

Learn more at
**hpe.com/software/SIOC**



**Sign up for updates**

★ Rate this document

Hewlett Packard Enterprise

© Copyright 2016 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

4AA6-3593ENW, January 2016