Hewlett Packard Enterprise

Business white paper

State of Security Operations

2017 report of capabilities and maturity of cyber defense organizations

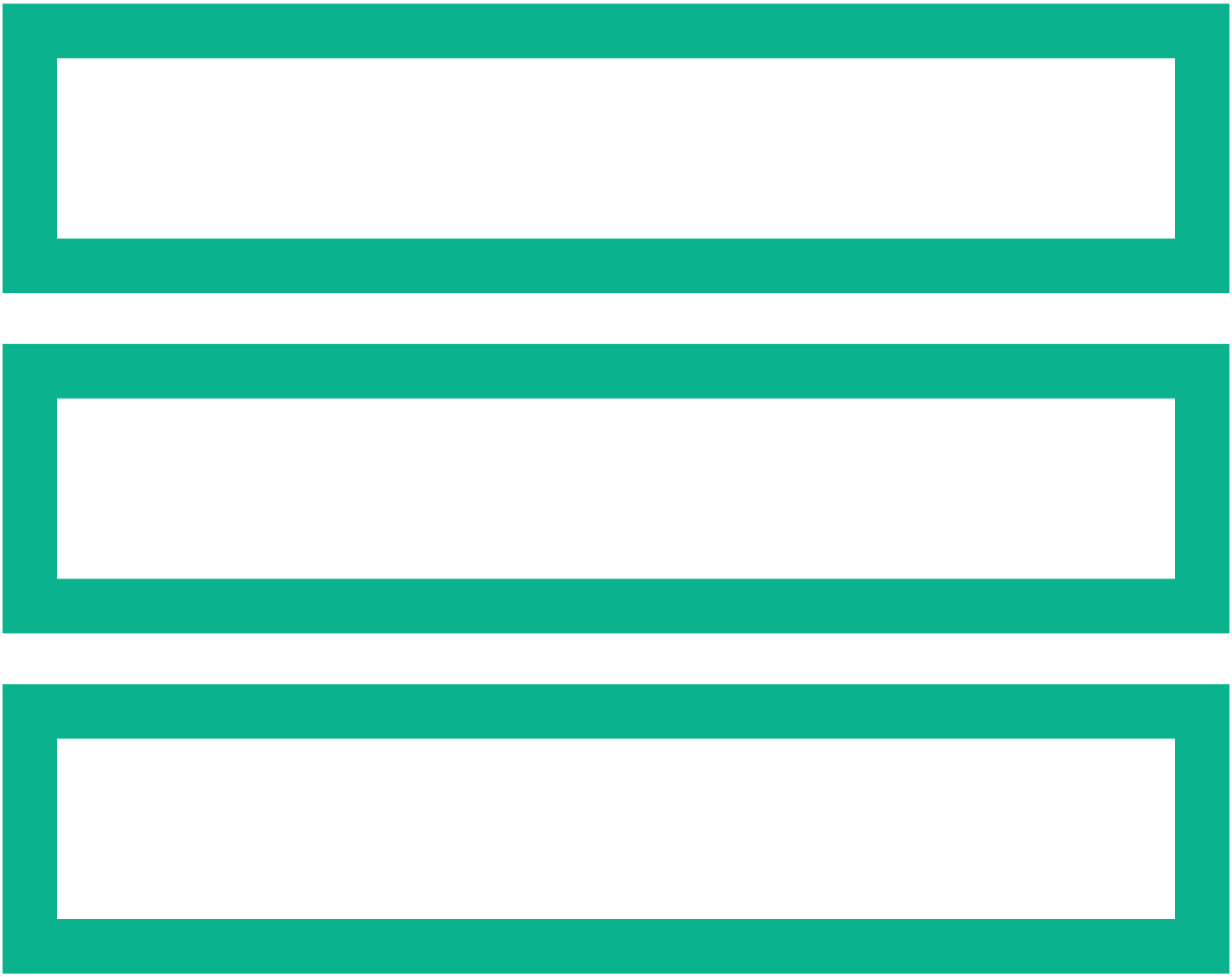


Table of contents

4 **Executive summary**

5 **Summary of Findings**

11 **Regional trends**

12 **Enterprise size vs. Maturity**

12 **Industry medians**

14 **Category Findings**
15 People
16 Process
18 Technology
19 Business

20 **Conclusion**

20 **About HPE Security Products**

21 **Appendix**

I am pleased to share our findings in this fourth annual State of Security Operations report. Having witnessed cyber defense organizations grow and mature over the last 20 years, I can say that these are interesting times. There has never been a stronger connection between security initiatives and business goals. The speed of organizations adoption of new innovations such as cloud, IoT and big data platforms is matched head-on by advancement of the attackers. The sophistication, agility, and scale of attacks has made speed an imperative for any successful security operations center, and has led to a renewed focus on automation, real-time detection and response at scale.

Along with this focus, we are continuing to see a struggle to find and maintain skilled resources necessary to run security operations. Automation and outsourcing have been utilized to ease this burden with varying degrees of success, as you will see in the report. Throughout our assessments, performed on 6 continents, we have seen a multitude of SOC people, process, and technology configurations. Our data provides us with a view of the most effective configurations, along with insights into the opportunities and limitations of automation and outsourcing.

This year has also seen a sharp decline in maturity for organizations that are opting out of real-time security monitoring in favor of post-event search technologies. While this is a disturbing trend, organizations that have adopted hunt team capabilities as an add-on to their existing real-time monitoring programs have seen success in rapid detection of configuration issues, previously undetected malware infections, and SWIFT attack identification. This data will help the industry to really understand what works and what doesn't with security data analytics and hunt capabilities.

As we look forward to the upcoming year we see there will be great challenges: further adoption of the new style of IT, adhering to new regulations such as GDPR, an increase in politically motivated attacks, and more. I remain steadfast in the belief that organizations' best defense will be to remain steady with their security operations foundations. ***Focus on the people****. The people will drive the process, and the process will ensure the most effective use of the technologies. Excel at the basics and enhance capabilities with analytics to uncover advanced attacks with greater visibility across the organization providing confidence for your business to innovate securely.*

Matthew Shriner
VP Professional Services, HPE Security

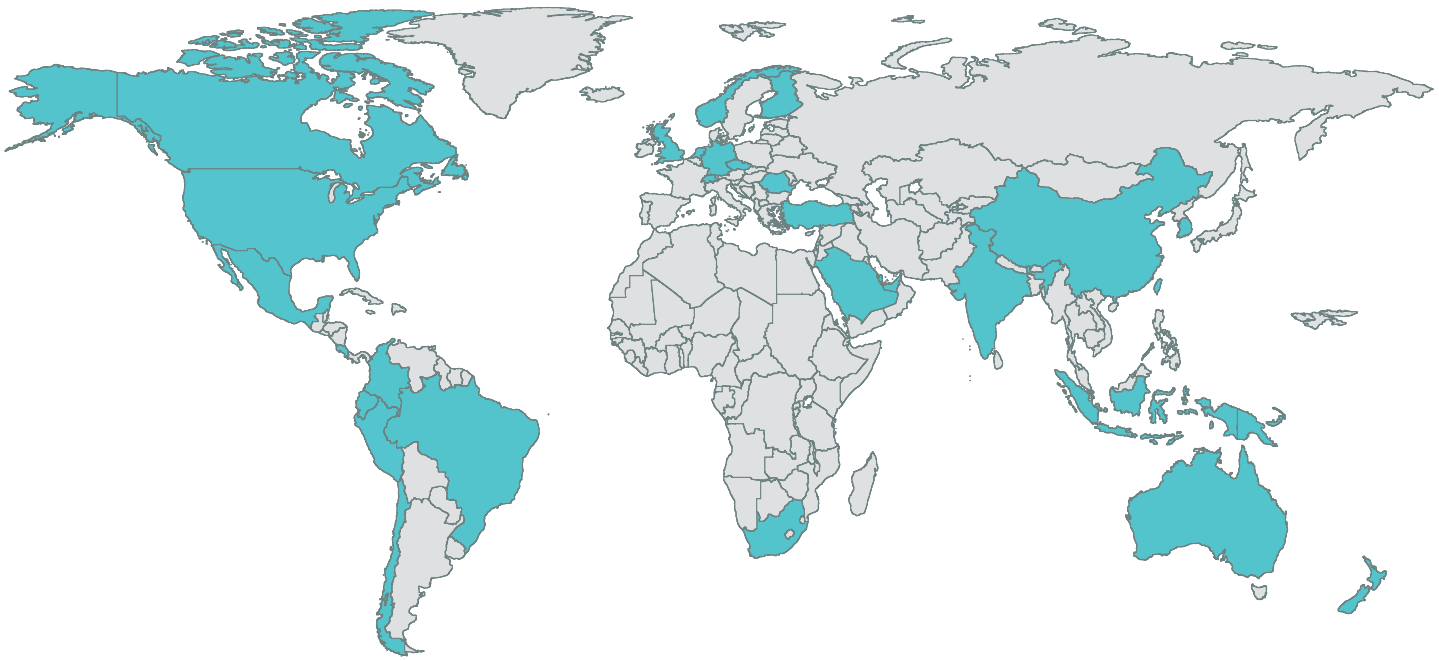
Executive summary

Organizations around the globe are investing heavily in 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 organizations and industries. In this fourth annual State of Security Operations report, Hewlett Packard Enterprise provides updates to the current and emerging capabilities, best practices, and performance levels of security operations as learned from the assessment of organizations around the globe.

With over a decade of experience supplying the information security technology and services at the core of the world's most advanced cyber defense programs and enterprise SOCs, HPE has worked with more of the world's top cyber defense teams than any other organization and is uniquely qualified to publish this report.

HPE Security Intelligence and Operations Consulting (SIOC) has assessed the capability and maturity of 137 discreet SOCs via 183 in-depth 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 31 countries on six continents across 9 regions. This is the largest available dataset to draw conclusions about the state of cyber defense and enterprise security operations around the globe.



Over the last five years Hewlett Packard Enterprise has found that 26.61 percent of cyber defense organizations that were assessed failed to score a security operations maturity model (SOMM) level 1, a 1% decrease over last year and a drop for the second year in a row. These organizations operate in an ad-hoc manner with undocumented processes and significant gaps in security and risk management.

Yet, after the assessments conducted this year, we found that over the last 5 years 18 percent of assessed organizations are meeting business goals and are working toward or have achieved recommended maturity levels which is 3 percent better than last year's findings and a 5 percent improvement in 2 years.

The assessments have shown some interesting trends:

- Consistency of mission, technology, management, and staff has a strong effect on the maturity of cyber defense organizations. Teams with low turnover, strong business alignment, and who follow multi-year plans tend to have greater capabilities as well as overall maturity.
- Organizations are continuing to try a variety of models to create right-size operations, including partnering with service providers or off-shoring specific roles or functions (such as level 1 monitoring). This has mixed results and often solving one challenge creates several new ones.
- Hunt teams that perform analysis on historical logs (as opposed to real-time analysis) are being adopted rapidly. HPE found that significant time and effort is being spent on data hygiene, contextualization, and preparation before these hunt teams are able to distinguish true threats from a myriad of misconfigured systems and process deficiencies in the management of IT assets.
- Increasing levels of workflow and process automation allow organizations to improve consistency, bandwidth, and speed of operations. Many organizations are investing in security incident investigation and management toolsets. Deliberate and diligent implementation of these capabilities as well as proper management has led to positive results.

The uneven distribution of maturity results across industries can be directly correlated with the experience of negative financial impact from malicious attacks. Organizations who have experienced direct financial loss due to malicious attacks do a better job of immediately maturing to a higher level. **This group of organizations continues to grow significantly in number.**

Summary of Findings

Decreased maturity with hunt-only programs
The proliferation of threat hunt programs is a continuing trend for security operations organizations in 2016.

The widespread adoption in data lake deployments using open source software and commodity hardware has provided the data retention and retrieval solutions required to support hunt operations. Organizations have raced to deploy security analytics tools to leverage these data stores, expecting useful information to bubble to the surface. While many interesting patterns and indicators are often uncovered by these tools, these are often lacking meaningful context and require extensive investigation. In today's hunt programs, the majority of investigations point to reveal data collection issues or misconfigured applications and systems.

In a few instances organizations have gone as far as opting for open hunt as the sole means for detection and response while eliminating SIEM-based real-time monitoring efforts. Many of these organizations were frustrated by security operations that were difficult to staff and not producing the expected value, and thus, decided to try something new. The result? Much of the same. Searches that return data from misconfigured applications and systems but not much in terms of useful results about threats to the organization. The maturity of these organizations actually regressed and risks increased as response to known-bad threats slowed and decreased in consistency. In most cases the operational context of the previous solution was lost in the transition to a new approach.

While most organizations in the early adoption phase of this emerging area of security operations are experiencing mixed results, there are some that have successfully added threat hunt capability to their security programs in complimentary ways to existing real-time operations. HPE is working with organizations who have leveraged the mature methodologies that made their security operations center (SOC) programs successful and expanded those lessons learned into threat hunt.

Development of Fusion Centers

The development of security fusion centers (internal information sharing centers) is an emerging trend for many large enterprise and public sector security operations organizations in 2016.

The common challenge described by these organizations is an inability to see the complete risk and security picture from their existing SOC environments spread across multiple regions and lines of business. There are simply too many applications, data, systems, and users within functional groups that organizations struggle to consolidate the information necessary to make effective risk decisions. Large organizations have attempted to handle the challenge through either more people or more technology solutions.

Yet, most organizations end up either deploying tools that require support and generate more volume, or end up without the human expertise to support the environment. In many of these organizations siloed security operations spring up that represent business units, an operating company, a department, or other logical divisions within the organization, each with varying degrees of maturity, and each providing visibility into a portion of the business but not the parent organization as whole.

Organizations that have best overcome these challenges have adopted an organizational model that designates or creates a SOC as a fusion center for the entire organization. These fusion centers provide process governance, information sharing, and security expertise that allow either each of the subscriber SOCs to collaborate better or to fold down and become functional customers to one of the SOCs at a more mature service stage. Large organizations using this approach usually see an overall benefit from economies of scale and improved coordination from a reduced set of common processes, the use of common technology solutions, and the use of common metrics from a fusion center.

Providing Effective Business Metrics

Security operations centers continue to struggle with development of metrics that communicate an effective business contribution.

Most security operations centers develop metrics packages that report technology attributes like system health, policy level, and functional performance. How do these metrics demonstrate a reduction of risk, an increase in security, or satisfaction of compliance objectives? The metrics listed are critical to those responsible for technology management, but add little value to stakeholders that seek to satisfy a business outcome.

Leading SOCs go beyond reporting basic functional performance data and deploy metrics programs that focus on measuring operational activities linked directly to business priorities and communicated in business terms. These metrics communicate security at lower total direct, indirect, and opportunity costs over time. Everyday activities like policy tuning, performance optimization, contextual customization, and response automation are reported along with their immediate and trended impact to the organization.

Attempts to Transfer Risk with Managed Services

Without proper management of service providers, organizations looking to transfer risk by moving to a managed service model experience a decline in the effectiveness of security operations over time.

Through outsourcing, organizations may receive reduced cost and an immediate boost in the maturity of operational and technology processes, especially where this capability does not already exist. However, by completely handing off the solution to a provider that is not aware of the day-to-day operations and change within the organization, there is a gradual erosion in the business value from outsourced security solutions that results in gaps managing risk, security, and compliance objectives.

After an extended period of outsourcing, organizations usually end up with security solutions being managed to agreed-upon provider service level agreements but little in terms of useful organizational context. Providers assume day-to-day responsibility to proactively apply up-to-date vendor policies, update firmware, track general uptime and availability, and report technology performance metrics, yet, these activities do not result in increased levels of maturity without the recurring customer interactions and frequent reviews required to maintain solution value.

Furthermore, outsourcing solution management to a provider is often mistaken as being equivalent to transferring business risk to the service provider. This is not the case. Service providers ensure that individual organizations remain responsible for managing their own overarching business risk by defining services with strict parameters and taking on limited liability based on service scope. Organizations that need to augment security capability but are unable to add staff should consider adopting a hybrid staffing or operational solution strategy for security operations.

Increased Capabilities via Hybrid Solutions

Organizations employing a hybrid approach to managed services solutions are more likely to maintain and improve maturity over time.

Hybrid solutions combine the operational capability of a service provider with an internal security operations capability focused on driving value from the total security controls deployed to protect the business. This can include technology management, eyes-on-screen monitoring, shared-insourced operations, and a number of other models that keep organizations and service providers working closely together.

Outsourcing success requires that organizations maintain some internally sourced operational capability to assure themselves of a few things. First, internal operational capability is able to perform the due diligence necessary to appropriately manage risks. Second, organizations maintain an internal stakeholder that gets the most out of what the service provider has to offer, and who is quickly able to coordinate activities related to incident response based on his or her familiarity with the environment. Lastly, and perhaps the most critical of all, organizations maintain an internal function that is vested in organizational success and develops a pipeline of talent that the organization can rely upon for years to come.

Successful services relationships go beyond superficial vendor management to standard industry SLAs. They require service transparency and interactions that allow security leaders to assess service performance quickly through established key performance indicators which ensure the financial and risk considerations that led to outsourcing in the first place are still being satisfied. Service providers can be integral to organizational success when there is a strong process foundation that ensures key organizational attributes are constantly integrated into the managed service and measured and optimized to meet the organization's objectives. All of these factors, working together, result in effective hybrid operations and can be measured for maturity over time.

Public Sector SOC Struggles

Public sector SOC organizations really struggle to grow beyond a Managed maturity level.

Being at a Managed maturity stage onto itself is not a bad thing. Generally it means that public sector SOCs have planned and executed implementation of a SOC in accordance with policy, decree, act, or charter based on the mission of the parent organization; these SOCs employ skilled people who have adequate resources to produce predictable outputs. There is a high degree of repeatability and relevant stakeholders are involved in operations. These are all positive attributes.

However, challenges quickly creep up because of deficiencies in three areas: misaligned expectations, lack of continuity of personnel, and rigid organizational roles and responsibilities. Similar to many organizations utilizing managed services, public sector leaders heavily rely on external vendors and mistakenly assume the use of a vendor is equivalent to transferring risk. In most instances this is not the case. Public sector leaders remain responsible for ensuring the security operations deployed satisfy the overall objective of the organization. The vendor may be a trusted advisor, but a robust metrics program needs to demonstrate successful security operations and not simply basic staffing and repeatability.

Somm level	Rating	Description
Level 0	Incomplete	operational elements do not exist
Level 1	Initial	Ad-hoc
Level 2	Managed	Repeatable
Level 3	**Defined**	**subjectively evaluated***
Level 4	**Measured**	**quantitatively evaluated****
Level 5	Optimizing	rigid, overkill

See the Appendix for a full description of each level

* Objective for commercial and public sector

** Objective for service providers

Public sector SOCs are highly leveraged and thus the vendor personnel deployed in key roles are prone to constant turnover. Organizations invest in training and development activities, however, there are usually limitations in upward career mobility for team members based on the scope established by the outsourcing contract agreement. Without and ability to move up in the organization, capable contracted security professionals will seek opportunities for continued growth and influence outside of the organization. Those that remain are usually in a state of deficient operational coverage until the staffing gap is mitigated causing public sector SOCs to stall on any new initiatives and increased maturity.

HPE has also observed an adverse effect from rigid organizational roles and responsibilities within public sector SOCs. The acknowledgement of individual team scope, rank of the individuals involved, or communications protocols to get things done significantly impact the interactions and timeliness of response to events that involve risk, security, and compliance priorities. This results in diminished maturity and reduced value from security solutions to the organization. Leaders in these SOCs often view process as a cumbersome burden instead of it being an effective agent of change that enables security professionals to protect the organization from emerging threats.

Effective public sector SOCs benefit a great deal from internally sourced operational leadership that provides oversight and measures success in terms of reduced risk, improved security, or satisfactory compliance. These internal stakeholders help contracted service providers navigate complex organizational structures and enable change to occur in a timely manner thus optimizing the security solutions the organization has deployed. Continuity in leadership is able to overcome some of the staffing turnover that can be expected in a vendor relationship. HPE has observed that when internal leaders are effective in breaking down walls, this often leads to higher rates of personnel retention and the ability to focus on projects and initiatives that make the organization more mature over time.

Commercial vs Open Source Tools in Security Operations

Some security operations centers have increased their reliance on open source tools in 2016. This strategy may add capability or reduce spend on software license during that budget cycle, but rarely are those solutions deployed with the level of support, documentation, and metrics that ensures organizational risk, security, or compliance objectives are sustainable.

Many of the open source tools and community resources available for security operations require a degree of customization and ongoing maintenance that organizations must carefully evaluate. Through our assessments over the last eight years HPE has observed security leadership turning over on average every 18 months, and some key staff turning over even quicker. Staff transitions at this rate can have a tremendous negative impact on the supportability and sustainability of highly customized and proprietary solutions and ultimately on SOC effectiveness and maturity. HPE has observed this migration to open-source consistently hinder organizations, with most programs deteriorating and collapsing after the departure of key personnel that were intimately familiar with the custom solutions.

Most organizations do not discover this gap until after an adverse event which costs the organization a significant amount of resources. There is certainly a place for custom tools in SecOps where commercial applications fall short. Leaders must simply evaluate their security strategy and determine whether the operational cost to maintain these systems results in significant value and advantages over vendor supported solutions.

Automation and Elimination of Entry Level Analysts

A number of organizations are considering the elimination of front line detection and response analysts and opting instead for automation to address emerging threats to the organization. Given the shortage of security talent, this approach resonates with a number of security leaders. The reality of how this plays out is not as clear cut or beneficial as it sounds.

The level of automation most organizations envision by eliminating front line analysts is seldom realized. True automated detection and response, not merely augmented data collection, requires a high degree of confidence and accuracy in configuration management data. This happens to be an area where most organizations truly suffer in terms of maturity with information about the applications, users, systems, and data residing in disparate repositories or not available at all. Automation might be possible in small, static, or highly controlled segments of a network, but in most organizations the risk of breaking something that is not well documented and matters a great deal to the organization is enough of a deterrent to keep effective automation from ever being deployed.

Crestfallen that their ultimate automation objective could not be accomplished, most security leaders turn to another ineffective triage practice: automated ticket generation. This approach is not always bad. When the indicators of attack are atomic or computed, this level of automation makes sense. The outcomes from these indicators are either actionable or not and those with a high degree of fidelity that are actionable should move along to the next step in the incident response process. However, when dealing with the behavior of an advanced threat actor and coordinated campaigns that span time, this approach usually turns the analyst into a myopic responder.

HPE has consistently assessed organizations where the correlation timeframe that resulted in an automated ticket was not long enough to capture the true intent and actions of the threat actor. The creation of a ticket has an impact on the analytical mindset of the analyst responding and their behavior is altered to seek the quickest conclusion. This level of automation has two adverse outcomes observed for most organizations employing it: increased triage and response costs and greater risk based on the interruption of the analytical process. Organizations contemplating elimination of front line analysts because of an inability to attract or retain talent are encouraged to review the **Growing the Security Analyst** and the follow-on **Intelligent Security Operations: A staffing guide** publications.

Additional findings

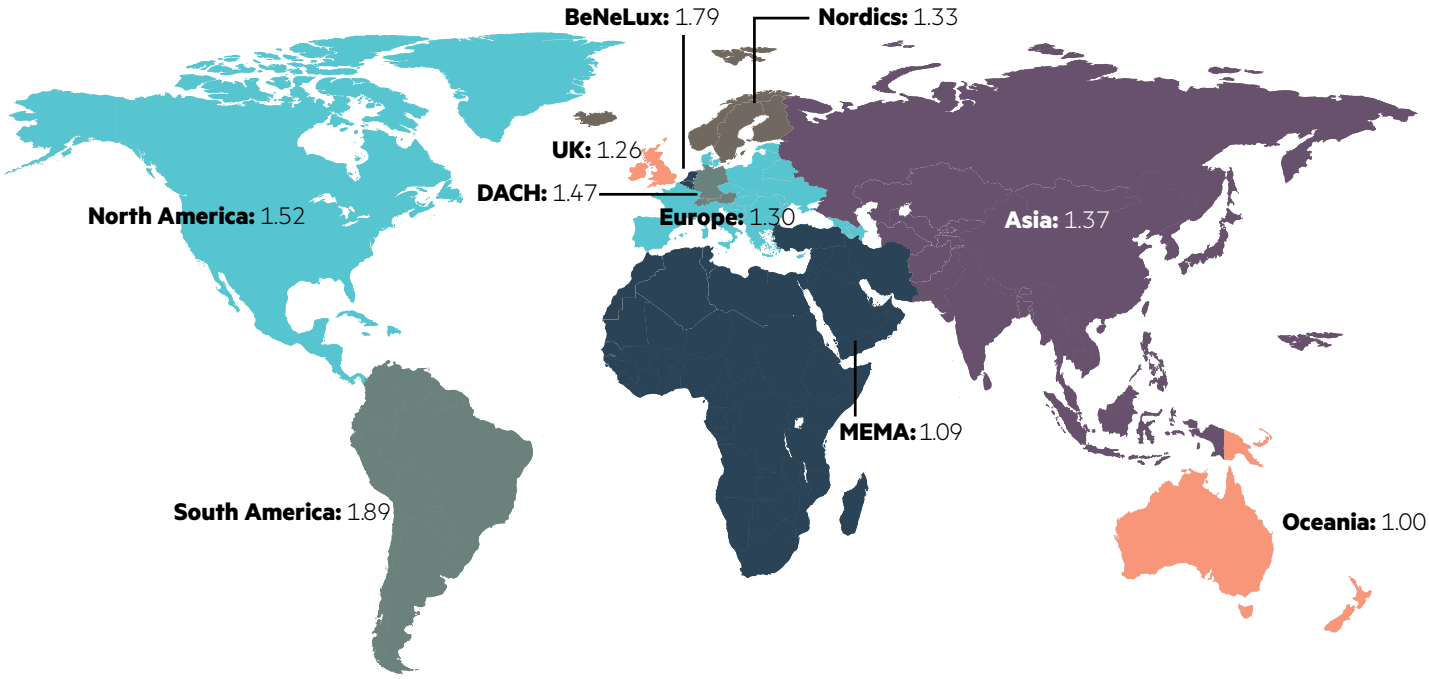
The Hewlett Packard Enterprise assessments of organizations worldwide continue to show the median maturity level of cyber defense teams remains well below optimal levels. Many of the findings and observations from the previous State of Security Operations report (**hpe.com/software/StateOfSecOps2016**) are still valid. Additionally, the following observations and findings were made throughout this last assessment year:

- SOCs are spending a large portion of their time identifying misconfiguration issues. Ideally these issues would be handled by an IT team freeing up the security operations organization to focus on identifying and investigating attacks.
- Most SOCs are heterogeneous, supporting multiple vendor technologies as well as a proliferation of automation and tools. The visibility and breadth of these SOCs is an advantage because it can bring together the best features of each technology solution deployed yet it can also be cumbersome when these SOCs must perform integration work themselves.
- The European Union's General Data Protection Regulation (GDPR) is on organizations' radar with the compliance deadline being May 2018 however organizations have not yet implemented necessary changes. In addition to several other requirements, the requirement to detect and inform EU citizens of personal data compromises within 72 hours will drive new SOC detection and response use cases and investment for compliance around the globe.

- Destructive malware and ransomware has demanded closer ties between the SOC and disaster recovery and business continuity teams.
- Turnover and staffing challenges still plague the industry. Through the interviews conducted during our maturity assessments we find that the number one issue facing security operations organizations continues to be identifying and retaining the human resources needed to run the business. Often, optimal staffing is not achievable and required skill sets are not accessible.
- There are continued efforts to converge and streamline functions, tools, and resources between Security Operations and IT Operations. Best practices still prescribe separate functional groups, however, tight collaboration and a level of convergence is possible and even necessary.

Regional trends

There are only minor discrepancies in regional maturity and capabilities across the globe. While SOCs across North America have typically experienced slightly higher SOMM scores, HPE SIOC's access to new service provider organizations in South America has resulted in continued maturity within that region in the past year. This is due to an increase in investment in the areas of security monitoring, operations, managed services, and automation. The MEMA region (Middle East, Mediterranean, and Africa) saw a significant increase in SOMM scores compared to last year with investments across commercial and public sector organizations on the people and process aspects of their security programs. Asia and DACH saw a slight drop with new entrants into the space in 2016. The remainder of Europe (BeNeLux, Nordics, and UK) remained steady in 2016 with few entrants into the space.



Enterprise size vs. Maturity

HPE did not observe a direct relationship between the size of the organization and operational maturity across commercial and public sector organizations. While there are larger organizations at or near the top, an exploration of the lowest performing organizations reveals some large multinationals that have simply not prioritized security operations. The allocation of IT budget and security budget to protect revenue, privacy, critical infrastructure, market share, safety, and intellectual capital is sizable when there is much to lose. Despite access to significant resources those organizations are not more mature. Security as a competitive differentiator, market leadership, and industry alignment are better predictors of maturity according to our data.

Industry medians

Looking at median scores by industry vertical, we see that services organizations have had the highest SOMM scores over the last five years. This is a change over the previous 2 years when SOCs in the technology vertical led all organizations. As an industry, services organizations demonstrate a strong investment in business alignment and people dimensions of the SOMM over the last 5 years causing them to surge over other verticals that are still primarily focusing on their technology deployments. During the last five years, Hewlett Packard Enterprise (then HP) has continued to see low performance from telecom industry organizations. As the team investigated the multi-year trend in telecom, it noted new telecom organizations joining the cyber defense market in developing economies through new managed services offerings that should improve as they formalize the investment in these programs.

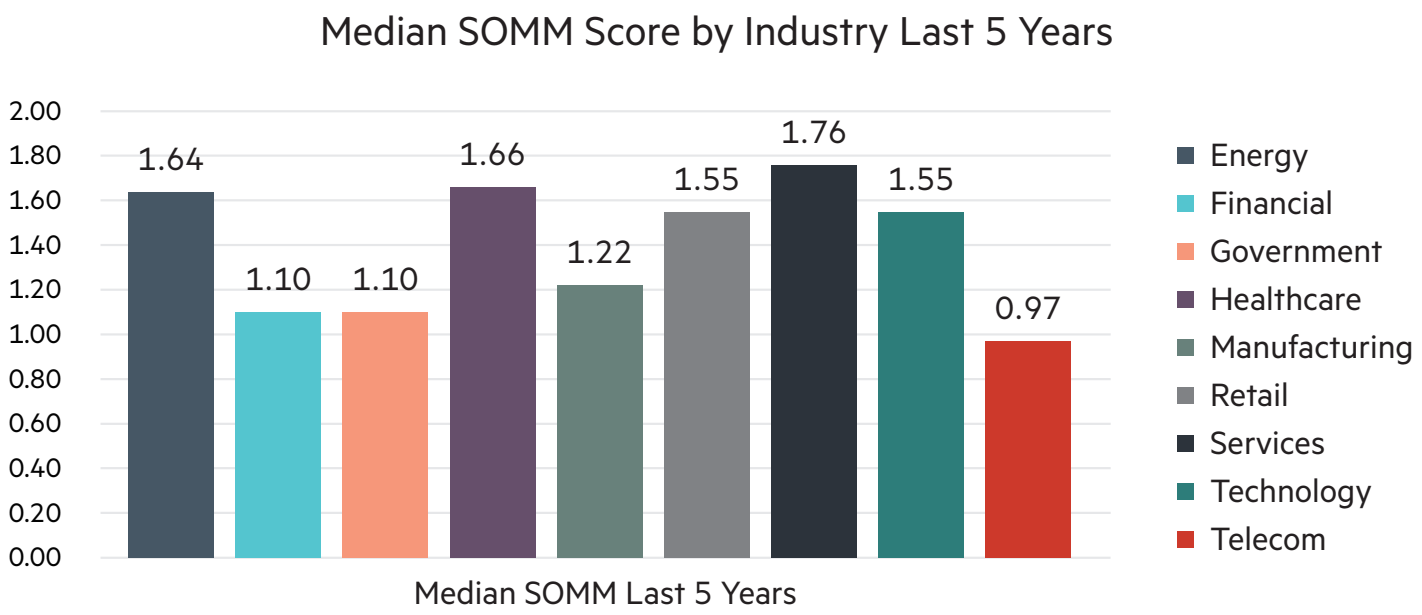


Figure 1. Median SOMM score by industry—last five years

- **Healthcare** companies have become a preferred target of ransomware due to the time-sensitive data that runs their business. Close collaboration with disaster recovery and backup teams is imperative to shrink the window of leverage for these attacks.
- **Government** organizations struggle with long term maturity. Fixed length contracts for outsourced resources drive metrics based on staffing rather than maturity and effectiveness.
- **Financial** institutions have been plagued by large Society for Worldwide Interbank Financial Telecommunication (SWIFT) attacks. Organizations that monitor for specific indicators of compromise (IoCs) for these types of attacks have been the most effective at lowering their risk.
- **Energy** companies have increased monitoring of physical, SCADA and industrial control systems to combat the increased threat of infrastructure attacks. Real-time monitoring has proven most effective at identifying these attacks for quick remediation.
- **Telecommunications** companies are generally concerned with service availability. Organizations that have expanded into managed services and security as a competitive differentiator have demonstrated greater maturity.

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, most industry verticals are now strongest in the Business category. This is a change from previous years where organizations were generally overinvested in Technology. The majority of industries are weakest when it comes to the Process category. Process is where most SOCs should strive to do better as those organizations that do usually see better value from their People and Technology solutions.

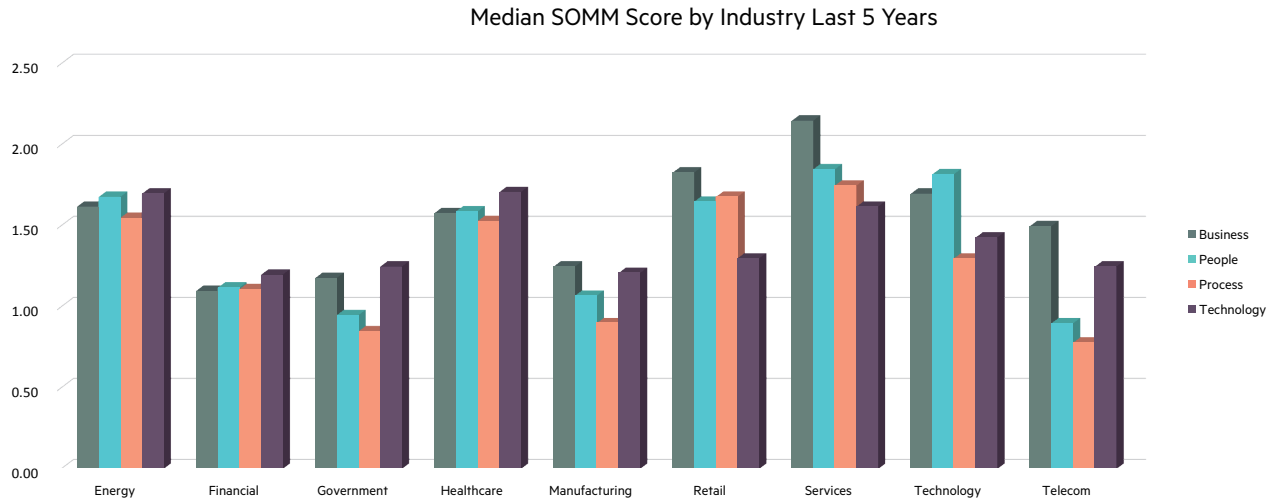


Figure 2: Median SOMM Score by Industry Last 5 Years

* See the Appendix for a full description of each level

Category Findings

The four elements of security operations capability can be further broken down into assessment categories that are used in the HPE maturity assessments.

Category medians
Over the course of eight years, Hewlett Packard Enterprise has performed 183 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 second year in a row, the business SOMM area produced the strongest median score of 1.52. This remains consistent with the rapid growth of security within organizations 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 1.40. 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 three years due to the heightened awareness of threats from high-profile breaches.

People and process median scores remain lower, closer to 1.3 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.

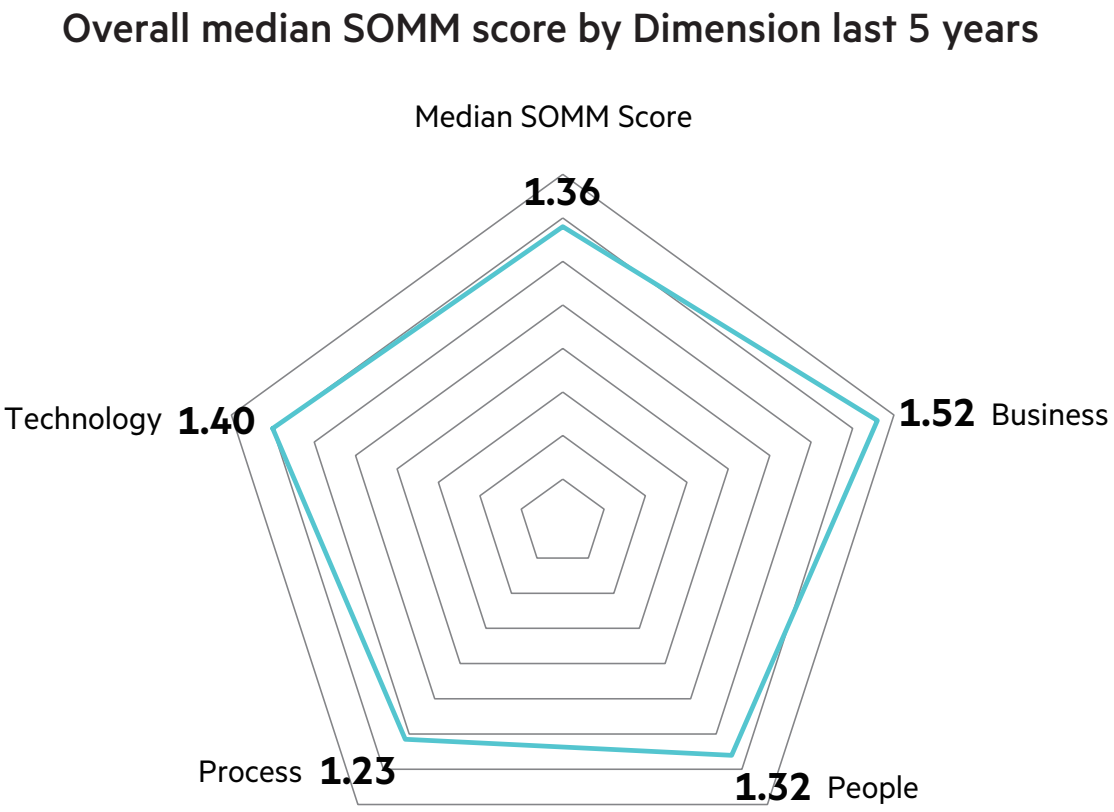


Figure 3: Median SOMM score—last five years

SOMM score for people

Median: 1.56; 5-year median: 1.32

Min: 0.1

Max: 3.8

Learn more about staffing your SOC:
hpe.com/software/StaffingSOC

Following are the findings and lessons learned from each of the elements: people, process, technology, and business.

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

Assessment category and elements	Findings
General – Roles definition – Organizational structure – Staffing levels – Staff retention	The number one issue facing security operations organizations is finding the resources needed to run the business. Often, optimal staffing is not achievable. Staffing the right people is arguably the most critical element. Hiring experienced analysts from the marketplace presents a number of challenges, especially for a new organization that has not yet established a critical mass of positive culture and established processes. Another common problem is attrition. Where around-the-clock security monitoring requirements exist, 24x7 scheduling is still presenting a challenge to most organizations.
Training – Funding – Relevance – Effectiveness	Skilled security resources are in very high demand and finding the right skills can be a daunting task. 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 train and cultivate their analysts.
Certifications – Funding – Relevance – Effectiveness	Classroom training and certifications are not a substitute for multi-domain experience when it comes to staffing cyber defense roles. Environment-specific and vendor-specific training programs are a necessity to refine the specific skills required of cyber defenders.
Experience – Industry – Organizational – Environment – Role	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.
Skill assessments – Frequency – Relevance	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.
Career path – Candidate pools – Succession planning – Opportunity	There is a broad disparity in the quality of existing SOCs in the marketplace. While analysts coming from existing SOCs arrive with valuable experiences, they also come with baggage. If you build a full team of these individuals, the There is a broad disparity in the quality of existing SOCs in the marketplace. While analysts coming from existing SOCs arrive with valuable experiences, they also come with baggage. If you build a full team of these individuals, the result is often conflict and inconsistency. While being a security operations analyst can be an exciting and flexible role, there is a need for operational consistency and predictability, otherwise, it can wreak havoc on the performance of the SOC. Also, experienced analysts in the market are seeking career progression and are not interested in another level 1 analyst role. Since we know organizations are working very hard to keep their top-performing analysts, there is a chance that those with SOC experience who are actively seeking level 1 security analyst roles are not the top performers on their team. 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.

SOMM score for process

Median: 1.35; 5-year median: 1.23

Min: 0.12

Max: 3.81

Assessment category and elements	Findings
Leadership – Vision – Organizational alignment – HR support – Style and feedback – Experience – Span of control	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. 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.

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	Findings
General – Knowledge management tools – Document control – Currency of documentation	The most successful SOCs are using an adaptable, portable, and operationally integrated process and procedure knowledge management system. Commercially available and open source tools such as a wiki are used to maintain organizational documentation that remains relevant and fresh. Portability and ease of maintenance are key in systems that allow images, video captures, scripts and other operational materials to be published and shared across the team. Managers track and measure contributions to documentation as one of the SOC's KPIs.
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	Hybrid environments require advanced maturity of their processes to be effective and to avoid mishandling of incidents. Utilizing hybrid staffing models, such as outsourcing first-line analysis, can not only reduce the negative effect of attrition or skills acquisition but also make the total cost of recovery more expensive. 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.

Assessment category	Findings
Analytical processes – Threat intelligence – Investigations – Data exploration – Focused monitoring – Forensics – Advanced content – Information fusion	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. 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.
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	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. A hunt starts with some form of cyber threat intelligence or internal awareness as a basis for the formation of a hypothesis. This hypothesis is an educated guess based on prior knowledge and observation that the hunt tests or validates by collecting and analyzing the necessary data. 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.
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)	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. 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: 1.54; 5-year median: 1.40

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	Findings
Architecture – Architectural process – Documentation – Technology coverage – Alignment with business requirements	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.
Data collection – Coverage – Data quality – Consolidation – Data ownership – Data access	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.
Monitoring and analysis – Workflow management and measurement – Investigation – Data visualization tools – Coverage – Health and availability	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. 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.
Correlation – Aggregation – Normalization – Cross-technology – Asset-relevant correlation – Business rules correlation – Subtle event detection – Automated alerting – Multi-stage correlation – Pattern detection – Dashboards and reporting	Companies frequently purchase technology point solutions but fail to bring the data together for effective risk remediation and threat detection. 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.
General – Infrastructure and endpoint management and administration – Relevancy of data collected – Currency	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.

SOMM score for business

Median: 1.52; 4-year median: 1.52

Min: 0.59

Max: 3.46

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

Conclusion

The detection and response capability of organizations continues to shift and evolve. Industry collaboration, sharing, and open source tools now provide a more palpable entry point for organizations struggling under minimal security budgets to deploy security operations. Some regions of the globe are seeing a boom and shift toward outsourcing via Managed Security Services to help organizations overcome the shortage of qualified cyber security professionals. In some regions and industries there is a gradual shift towards insourcing through hybrid security staffing models that allow organizations to recapture the overall security strategy and manage a vendor relationship where providers execute what they do best. For others, breaches or an adverse event within their industry are driving an accelerated timeline and motivated stakeholders looking for a security solution.

No matter what stage organizations are at, it should be evident that there is no quick fix product or service that can provide the protection and operational awareness an organization needs. Successful security operations programs require an assessment of the risk management, security, and compliance objectives of the organization and the constant tuning of the people, process and technology components of the solutions deployed. Targeted investment into all facets of a security operations program is necessary to achieve and to maintain maturity.

HPE Security Intelligence and Operations Consulting has worked with some of the world's most advanced security operations centers. During the last four years through the State of Security Operations report we have shared our findings from 183 assessments of 137 discreet SOC organizations in 31 countries. By sharing insight into what makes some of the most advanced cyber defense centers around the globe successful we trust that you too can realize the benefits from the advanced analytics, threat intelligence, and repeatable processes deployed within your organization.

About HPE Security Products

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

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

Appendix

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 a low level overall 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.

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 following an adverse security event the impact was measurable through declining stock prices. Yet, 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] There is a longer-term effect on profitability as recovering organizations face higher costs from new security programs, litigation, and organizational turnover that occurs following a breach.

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

Relevance of our data—qualification to present this report

HPE Enterprise 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 (then 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.

Hewlett Packard Enterprise (then HP) 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. Nothing is documented and actions are ad hoc.
Level 2	Managed	Business goals are met and operational tasks are documented, repeatable, and can be performed by any staff member. Compliance requirements are met. Processes are defined or modified reactively.
Level 3	Defined	Operations are well defined, subjectively evaluated, and flexible. Processes are defined or modified proactively. This is the ideal maturity level for most enterprise SOCs.
Level 4	Measured	Operations are quantitatively evaluated, reviewed consistently, and proactively improved utilizing business and performance metrics to drive the improvements. This is the ideal maturity level for most managed service provider SOCs.
Level 5	Optimizing	Operational improvement program has been implemented to track any deficiencies and ensure all lessons learned to continually drive improvement. Processes are rigid and less flexible, and significant overhead is required to manage and maintain this maturity level, outweighing the benefits achieved.

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.

Sign up for updates

Hewlett Packard Enterprise

4AA6-9062ENW, January 2017