White Paper

Security

2018 State of Security Operations:

Report of the Capabilities and Maturity of Cyber Defense Organizations Worldwide

MICRO FOCUS

Table of Contents

page

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

Introduction

Organizations around the globe continue 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 fifth annual State of Security Operations report, Micro Focus® Cyber Security Services provides updates to the current and emerging capabilities, best practices, and performance levels of security operations and cyber defense as learned from the assessment of organizations around the globe.

Every year Micro Focus Security Intelligence & Operations Consulting helps a large number of global organizations assess, design, and build out the capability of their cyber defense programs.

For the 2018 State of Security Operations report, our fifth one to date, we took a look at the security programs we assessed over the past 5 years and provide insights and analysis focused on enumerating the best practices that drive the success of these programs worldwide. For the third consecutive year, we have included insights from our global consulting engagements and include capability trends that allow organizations to compare themselves to other organizations within their specific vertical and region.

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

Executive Summary

Micro Focus Security Intelligence and Operations Consulting (SIOC) has assessed the capability and maturity of 144 discreet SOCs in 200 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 33 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 Micro Focus Security Operations Maturity Model (SOMM) methodology for assessments has been updated annually to remain relevant with current information security trends and capabilities. Micro Focus SIOC consultants perform onsite assessments and review organizational processes and day-to-day operations to objectively score business alignment, people, process, and technology aspects of the subject's cyber defense program against SOMM best practices. The most important success criteria for a mature cyber defense capability is reliable detection of malicious activity and threats to the organization and a systematic approach to manage those threats that fully leverages the people, processes, and technology available to the organization.

Historically organizations have struggled with satisfying the objectives of their cyber defense investments. Most security operations centers continue to be over-invested in technologies that inform them of a problem, yet truly struggle to protect, detect, respond, and recover from the cyber security attacks they fail to discover. Timely response outcomes are possible only through repeatable, mature operations, when organizations establish a culture that keeps up with the dynamics of IT, risk, and regulatory change.

A significant shift occurred as the team analyzed the data for 2017: all SOMM measures went up with the median maturity reaching a 1.42 across all industries. Micro Focus Cyber Security Services found that over the last five years, 25 percent of organizations assessed are meeting business goals and are working toward or have achieved recommended maturity levels. This represents a 7 percent improvement over last year's findings, a 12% improvement over the last 3 years and the most significant shift in the five years Micro Focus SIOC has published the State of Security Operations report.

As the team looked at organizations on the other end of the spectrum, it found that 20 percent of cyber defense organizations that were assessed over the past 5 years failed to score a security operations maturity model (SOMM) level 1. These organizations continue to operate in an ad-hoc manner with undocumented processes and significant gaps in security and risk management. Although the number is still higher than we would like to see, this shift was also an overall improvement over the trend established in previous years.

When it comes to cyber defense capability, Micro Focus Cyber Security Services is seeing a much higher degree of operational sophistication than ever before. Organizations are:

- Quickly shifting to co-managed operations in partnership with vendors and niche providers to overcome the greatest challenge that continues to impact cyber defense programs: a global shortage of cyber security talent
- Rapidly adopting security orchestration, automation, and response (SOAR) solutions to gain efficiencies and repeatability in the handling of high fidelity alerts, and
- Systematically investing in the development of Security Fusion Centers that can span the operational overlap of multiple domains including: data security & compliance, monitoring for insider threats and privileged access through behavior analytics, correlating physical security and cyber security data, and building effective consolidated operations and incident response for Hunt, Threat Intelligence, and IT operations

When it comes to cyber defense capability, Micro Focus Cyber Security Services is seeing a much higher degree of operational sophistication than ever before.

Category	Trend
Overall	△
Business	△
People	△
Process	△
Technology	△

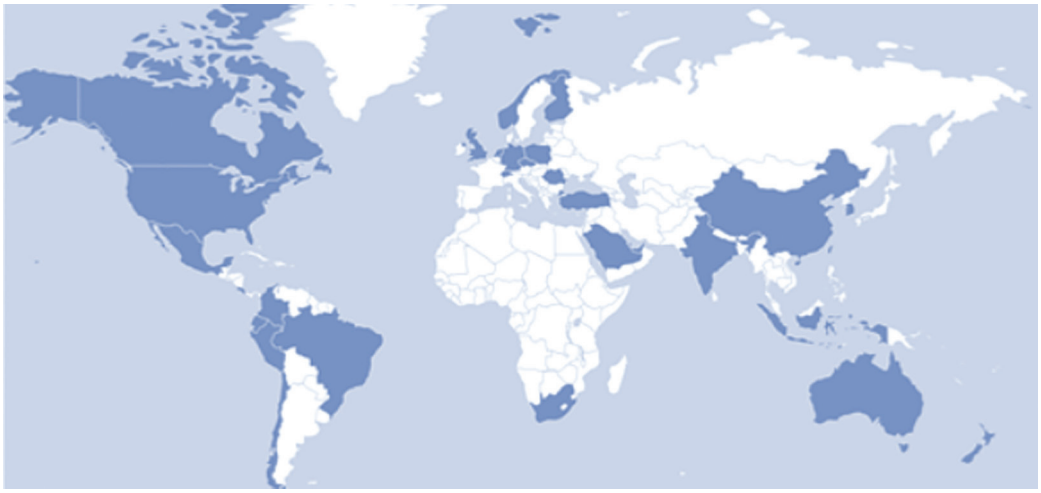

Figure 1. Countries where Micro Focus Cyber Security Services has performed assessments

Median Security Operations Maturity Year over Year

Over the course of nine years, Micro Focus Cyber Security Services has performed 200 SOC maturity assessments around the globe. This data sample set allows Micro Focus Security Intelligence and Operations Consulting to draw conclusions about the overall maturity of the cyber defense programs in place at companies and public sector organizations across the world.

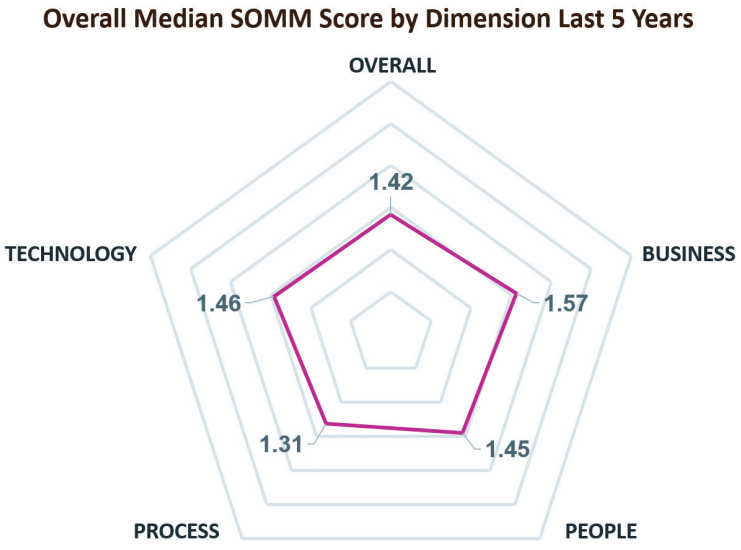

Figure 2. Overall median SOMM score

Overall and within each of the areas measured, the cross industry median capability score continues to fall between a 1 and 2. While SOCs in this range are generally getting the job done, Micro Focus Cyber Security Services continues to observe that a lack of repeatability, metrics, and demonstrated continuous improvement make the effectiveness and sustainability of these cyber defense programs unpredictable across most organizations. The ideal composite maturity score for a modern enterprise cyber defense team remains a level 3—where the capability is "defined." This is achieved with a complimentary mixture of agility for certain processes and high maturity for others. Micro Focus SIOC has observed that levels of aggregate maturity above a 3 are more costly to achieve and should be reserved for organizations looking to protect subsets of applications, data, systems, or users.

Micro Focus SIOC has observed that levels of aggregate maturity above a 3 are more costly to achieve and should be reserved for organizations looking to protect subsets of applications, data, systems, or users.

Category Medians in 2017

The overall SOMM and individual assessment areas have all trended up for the first time since our initial publication in 2014. This is significant as our data contains both new entrants to security operations as well as organizations performing follow-on assessments to continuously improve their cyber defense capability. For the third year in a row, the business SOMM area produced the strongest median score: a 1.57 for the 5-year assessment window. This remains consistent with the rapid growth of security within organizations that we have seen for the past few years driven by the broadening understanding of cyber threat impacts to an entire business (including executives and board members) and not just an IT or compliance organization.

Measurements of the Business aspect of the maturity model have increased significantly in the last three years, largely due to a heightened awareness and impact of breaches driving increased understanding of cyber risk by the business. This has brought increased visibility of and better articulated requirements to the cyber security function. Many organizations are also leveraging more mature products and established vendors in their cyber security solutions, offering a higher degree of business-level relationships and support to solutions.

The People aspect of the maturity model saw the biggest single-year jump to a 1.45 for the 5-year median, almost a 10% increase. Organizations assessed in this window have done a better job aligning the reporting structure of their security teams, consolidating security operations and related hunt, threat intelligence, and incident response functions, developing strategic partnerships with subject matter expert providers, and attracting, training, and retaining security talent under capable leaders.

The Process aspect of the maturity model continues to lag behind at a 1.31 for the 5-year median, yet saw a 6.5% improvement, the second highest, for this year's report. Without a solid foundation of processes and procedures, SOCs become reliant on the "tribal knowledge" of individuals and less predictable in the results they produce. Turnover of individuals cripples the capability of the SOC that lacks good processes and sets organizations back years. The most capable cyber defense programs around the globe stand out in this area with repeatability, continuous improvement, and metrics that track execution of processes.

Region	Median Historical SOMM Level
Asia	1.37
BeNeLux	1.79
DACH	1.57
Europe	1.30
MEMA	1.09
Nordics	1.33
N. America	1.53
Oceania	1.00
S. America	1.89
UK	1.47

Year-to-year measurements of the Technology aspect of the maturity model remain strong with the second-highest SOMM score and a median of 1.46. Technology has traditionally scored the highest due to the fact that engineering and technology deployment tasks are often the focus in most enterprise security organization's investments in cyber security. Most organizations continue to focus heavily on technology solutions and tools in their cyber defense program.

Median Security Operations Maturity around the Globe

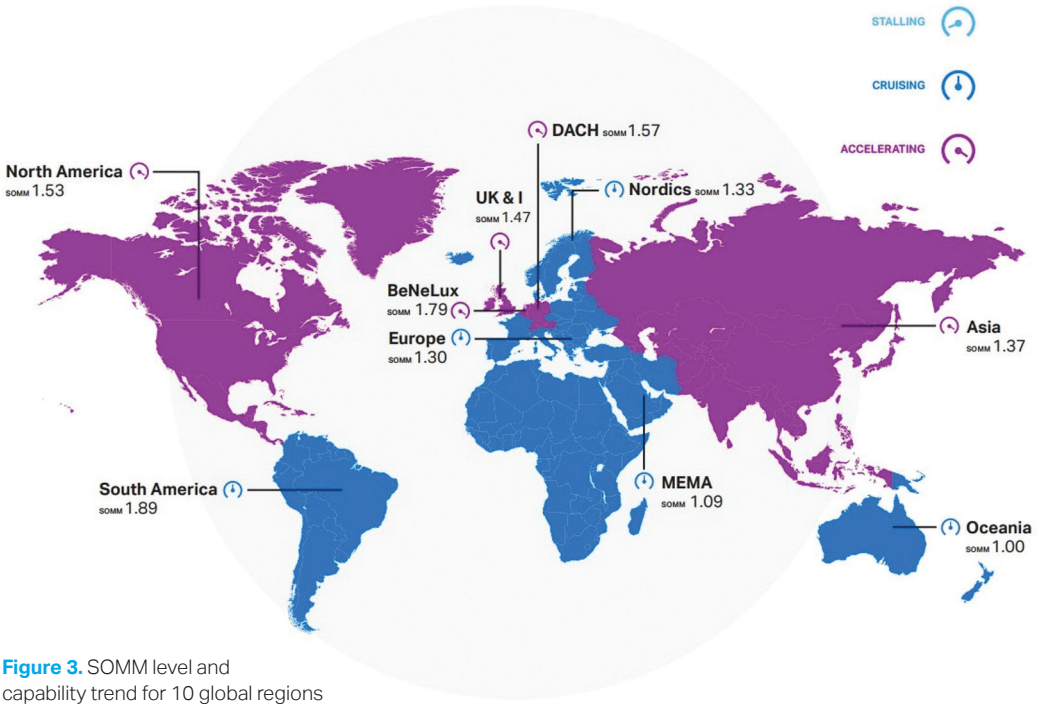

Figure 3. SOMM level and capability trend for 10 global regions

Regional Results in 2017

The UK, DACH, and North America saw shifts in a positive direction. The UK saw a 17% shift upward while DACH had a 9% improvement. Analysis of the swings in those regions revealed multinational organizations making security investments in preparation for the General Data Protection Regulation (GDPR) which is currently scheduled to become enforceable in May of 2018. The consolidation and relocation of SOCs within the EMEA regions to form Security Fusion Centers have also improved the effectiveness of security operations.

North America saw a small 1% improvement in the historical window. However, North American SOCs saw a 34% SOMM improvement in year-to-year comparisons between 2016 and 2017. Security operations teams in North America once again led as the region most willing to undergo external evaluations of their cyber defense capability and experienced accelerated results based on the implementation of targeted roadmaps.

Industry Verticals Assessed	SOMM Trend
Energy	—
Financial	△
Government	△
Healthcare	△
Manfacturing	—
Retail	△
Services	△
Technology	▽
Telecom	△

The historical median maturity levels remained statistically steady across the other seven regions in 2017. However, Micro Focus Cyber Security Services did see significant year-to-year shifts in three additional regions: Asia, BeNeLux (Belgium, the Netherlands and Luxembourg), and South America. In Asia, Micro Focus SIOC observed a significant shift as organizations began to take steps to insource security operations, terminating relationships with managed security service providers in order to meet heightened organizational risk objectives, to satisfy country-specific and industry-specific regulatory guidelines, and to develop internal incident response capability.

In BeNeLux and South America, Micro Focus observed continued trends toward the use of niche service providers with a high degree of maturity and initial investment by new service provider organizations entering the market. Niche provider SOC organizations in those regions are often willing to deliver a highly customized service to their customers and are starting to explore Hunt-as-a-Service offerings as part of their services portfolio.

The Europe region remained steady in our 2017 data. Much of what Micro Focus SIOC has observed in Asia is also impacting the Europe region with country-specific regulations coming into effect at the same time as the EU prepares for GDPR. For example, Turkey saw its new Data Protection Law come into effect in 2016 after a decade-long legislative process. Analysis of our 2017 SOMM data contains initial baseline assessments being made by Turkish organizations to develop roadmaps for their organizations to build cyber defense programs internally or to identify partners that can manage solutions and demonstrate compliance with this regulation on their behalf. Micro Focus Cyber Security Services expects cyber defense service providers and industry-centric SOCs to emerge in Turkey and like markets in the region as government organizations begin to enforce regulatory standards.

MEMA, Nordics, and Oceania saw few entrants into the space in 2017. Established cyber defense programs in the regions dedicated resources to refine the capability and effectiveness of solutions through investments in orchestration and automation (SOAR), improved detection capability of existing tools, and relied on the use of of regional service providers. Service providers in these regions are integral to organizational success and often provide a strong process foundation for their customers.

Security Operations Maturity Industry Medians and Trends

Cyber defense programs across two thirds of all industries experienced median maturity improvement in 2017 with Telecom and Retail showing double digit growth. Services organizations produced the highest SOMM scores once again and saw a 6% plus increase in the most recent 5-year reporting window. Technology organizations displayed the largest drop-off in this year's data, -12%—a dip largely attributable to significantly shifting their cyber defense operations strategy and adopting new tools and hybrid IT solutions that will take time and effort to mature in the environment.

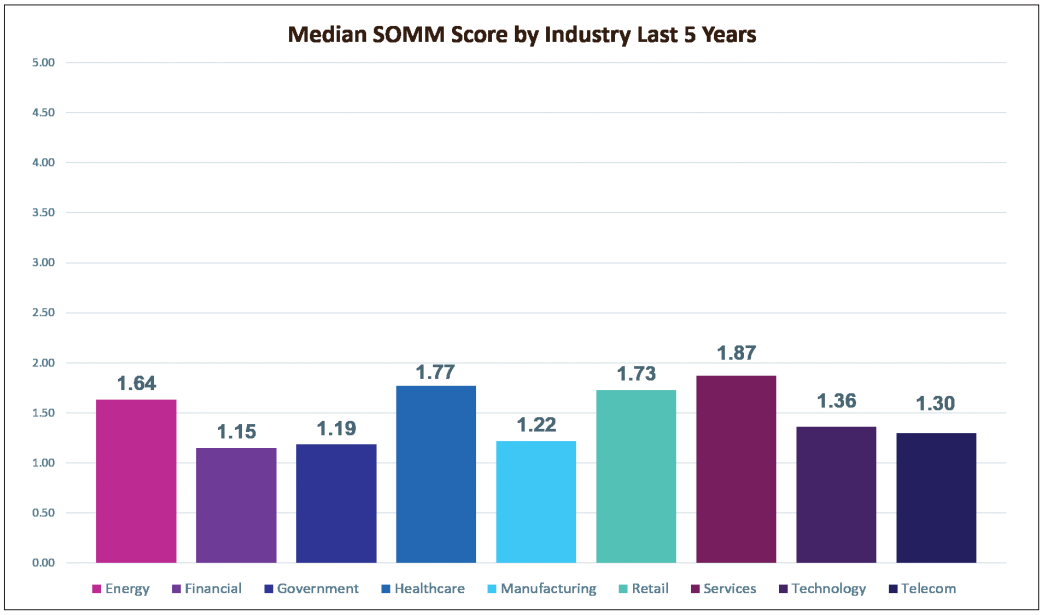

Figure 4. Median SOMM score by industry last 5 years

Energy

Organizations continue to protect critical national infrastructures and monitor the movement and exploration for natural resources through increased monitoring of industrial control systems, physical access, insider threats to competitive data and processes, customized applications, and SCADA. The median maturity for the vertical held steady in 2017.

Financial

Institutions saw a spillover of the previous year's Society for Worldwide Interbank Financial Telecommunication (SWIFT) attacks in early 2017. Many financial organizations in emerging markets adopted a Security Fusion Center approach to deploy use cases that monitor for specific indicators of compromise

(IoCs) for these types of fraudulent attacks at the transactional level, transferring tools and methods traditionally applied to cyber security to additional domains. Both regional and country-specific regulations are driving investment in Europe and Asia.

Government

Agencies saw a 5% upward trend in 2017. State, Local, and Education (SLED) organizations that struggled with long term maturity made initial investments to insource cyber defense operations following visible breaches in North America. Similar organizations are taking note and evaluating long-term solutions for better security operational maturity.

Healthcare

Providers protecting sensitive patient data and critical processes experienced a 7% uptick in SOMM maturity in 2017. Breaches in the North America region in 2017 continued to target the time-sensitive data and records under the protection of healthcare cyber defense teams. Close collaboration between security operations with data protection and disaster recovery teams is critical to reduce the impact of these attacks.

Manufacturing

Companies continue to combat the increased threat of production infrastructure attacks. SOMM capability levels remained steady year-to-year at manufacturing organizations with some companies providing minimal oversight through regional cyber defense teams responsible for functions primarily performed overseas.

Retail

Companies experienced an upward shift over 11% for SOMM level in the 5-year assessment window. Retailers assessed invested in expanded security operations programs that included security orchestration, automation, and response (SOAR) and hunt solutions. Additional budgets are also being applied to data protection, global incident response, and compliance initiatives in order for multi-national retailers to comply with GDPR.

Services

Organizations led all verticals and demonstrated a strong investment in business alignment and people and process dimensions of the SOMM over the last 5 years. Clarity of mission and balanced investment across SOMM areas allow services organizations to surge significantly over the other verticals that are still primarily focusing on their technology deployments. The median services organization has mastered the basics and is applying resources to operationalize hunt and threat intelligence and to build advanced integrations through SOAR solutions.

Technology

Cyber defense organizations displayed a large 12% drop-off in this year's data. The migration to hybrid IT solutions (Public cloud, IaaS, PaaS, SaaS, SDN/NFV, etc.) has simultaneously reduced costs and reduced the visibility into cyber security risks by security operations teams at technology companies. Micro Focus

Cyber Security Services has found that breaches at these organizations are harder to quantify for reach and impact and the long-term effects of this cyber defense operations strategy is something the industry vertical must monitor.

Telecom

Teams have improved globally over the past year. Micro Focus SIOC has seen telecom organizations building new security operations in developing economies and entering the market through new managed services offerings. In 2017, the median telecom organization returned a 1.30 median 5-year SOMM level. The investment in these programs has improved their capability significantly and brought telecom maturity into alignment with all other industries.

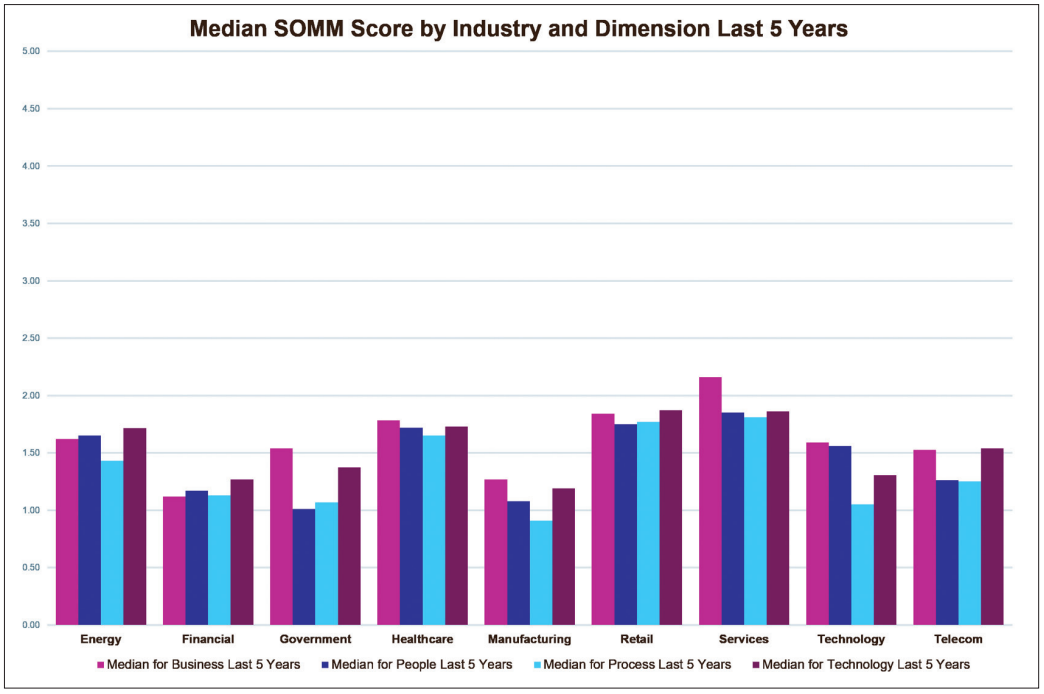

Figure 5. Category medians across industries

2017 Summary of Observations and Findings

Keys to Success

Leaders that performed year-over-year assessments credit the improvement of their cyber security programs to organizational alignment that included a number of factors. Based on their feedback these include in no particular order:

i. board-level support and visibility into the KPIs of security programs,
ii. clarity of mission for the cyber defense program,
iii. insight into the applications, data, systems, and users most likely to impact customers,
iv. immediate security investments following direct financial loss,
v. the continuity and retention of key security personnel,
vi. a narrower focus to protect specific assets for the organization,
vii. strategic partnerships with niche security service providers,
viii. the use of automation for repeatable tasks,
ix. leveraging expert consulting organizations to guide design, development & optimization,
x. a willingness to transform IT culture,
xi. advanced integrations that provide better end-to-end visibility, and
xii. tools that are faster and easier to use

"Do more with less!" Because of either necessity or maturity SOC leaders are turning to workflow and process automation tools that allow them to improve the consistency and effectiveness of operations.

Co-Managed Operations

The team explored this topic in last year's publication under the "Increased Capabilities via Hybrid Solutions" heading. This topic created a great deal of chatter and requests for clarification in 2017. To put it more simply, security operations leaders are quickly shifting to co-managed operations in partnership with the technology vendors themselves or with niche, boutique providers that can manage the technology on their behalf.

This approach has allowed cyber defense programs to overcome the greatest challenge that continues to impact the industry: a global shortage of cyber security talent. By setting up an operational relationship with a partner that includes regular interactions (daily/weekly/monthly), SOC leaders can narrowly focus on identifying the assets they want to protect and work with the partner operationally to perform the technology integration to make it happen. Niche service providers usually provide a strong, transparent process foundation, the area where industry SOCs struggle the most. This allows internal cyber defense teams to focus their time on identifying the key assets that must be protected by the solution and to dedicate time refining the outputs of the solution in coordination with the partner.

Security Orchestration, Automation, and Response (SOAR)

"Do more with less!" Because of either necessity or maturity SOC leaders are turning to workflow and process automation tools that allow them to improve the consistency and effectiveness of operations. SOCs running short on personnel are able to gain repeatability in the handling of high fidelity alerts by adopting security orchestration, automation, and response (SOAR) solutions. SOCs that are more mature gain efficiencies and bandwidth that can be spent on activities that are less mature, like hunt and data enrichment, or other advances in cyber defense operations. In either scenario, a few organizations are investing in automating security incident investigation and management toolsets, and with deliberate implementation goals in mind are experiencing positive results.

Micro Focus SIOC has observed that over the past year fusion centers have evolved into combined disciplines that most organizations would deliberately separate in the past.

The concept is sound yet adoption is still slow. For the majority of organizations, SOAR simply moves workloads from analysts to developers. While the intent is to leverage the capabilities of security tools fully, most SOAR implementations shift the problem to developers that may not understand the operational implications of an automated response action.

Finally, some organizations are just struggling to flip on the switch on automation because of knowledge gaps in operations. What if an application deployed by a vendor uses resources that are not well understood? What if a system administrator used a non-service ID to automate tasks across multiple systems and the actions look like lateral movement? Organizations with organic growth and the complexity of M&A integrations each have operational knowledge gaps that temper the rate of SOAR adoption. For SOCs looking at taking advantage of SOAR sticking the following points are key: start small and automate where already operationally mature.

Security Fusion Centers

The development of security fusion centers is a continuing trend for many enterprise security operations organizations Micro Focus Cyber Security Services assessed in 2017. Private sector organizations are systematically investing in the development of fusion centers that can span the operational overlap of multiple domains. In their initial form, fusion centers took the "One SOC to Rule Them All" approach which resulted in teams designed to see the complete risk and security picture from their existing SOC environments spread across multiple regions and lines of business. This model continues to serve decentralized organizations well and those that have grown quickly through M&A activity.

Micro Focus SIOC has observed that over the past year fusion centers have evolved into combined disciplines that most organizations would deliberately separate in the past. The new form includes fusion centers that are preparing to combine data security monitoring & incident response and compliance reporting for GDPR. Historically, data security teams are accustomed to working with application development teams across the organization in order to protect information as close to the applications where data is generated, processed, or stored. With new regulation that establishes response and reporting timelines coming into effect organizations are now leveraging incident response know-how from existing IT teams and adding data breach monitoring into centers of excellence (CoEs) that can meet the new regulatory requirement. These CoEs are essentially a fusion center for cyber security that allows organizations to centralize operations and improve the maturity of their programs.

Deception Grids

Know thy enemy. Micro Focus has worked with organizations in 2017 investing time into deception grid solutions. Cyber security across most business and public sector organizations is defensive in nature, creating an asynchronous situation where the adversary knows more about the target and can afford to fail in most attacks, as long as a single attack is successful. This asymmetry means that SOCs usually find themselves reacting to events impacting applications, data, systems, or users across an expanding perimeter and sometimes learning much about the attack and attacker at the same time.

A number of organizations that provide threat intelligence entered the market around the time of Micro Focus SIOC's first State of Security Operations publication in 2014. The industry-wide response to these solutions has been primarily to ingest atomic and computed indicators for real-time correlation and historical incident identification and response. Few organizations have gone a step further to analyze behavioral attributes of intelligence or developed internal programs that can repeatedly curate and categorize timely intelligence.

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

The use of deception grid solutions is not a new concept. Historically, intrusion analysts could learn about the tactics and behaviors of an attacker through the deployment of honeypots. As attackers got better at automating the earlier stages of an attack and as the economics and competition for targets became more intense, attackers became more selective about spending resources. It is because of the shift in the economy of an attack that deception grid solutions can be very attractive. By deploying systems that spread misinformation about the target system and leveraging a layer of automated deception, organizations can alter the findings of scripted reconnaissance and cause attackers to deploy resources that are ineffective on the target system and reveal information about themselves. Organizations can also learn much about the attacker and the target of their campaign by analyzing the behavior of the attacker in the deception-oriented environment. The use of deception grids and impact on operations maturity is something Micro Focus will continue to measure during assessments in 2018.

Cloud and Hybrid IT Impact on Security Operations

A large number of cyber defense organizations assessed in 2017 faced the challenge of protecting hybrid IT infrastructure. Organizations experienced reduced costs from IT spanning cloud, traditional data center, hosted space, SaaS, IaaS, and PaaS. Yet security leaders at these organizations expressed concern that the migration of some applications to the cloud expanded the attack surface and introduced new risks to the IT solutions they are responsible to monitor and to secure.

For most SOCs a cloud strategy resulted in the loss of visibility and greater initial risk as they now lack insight and can no longer report on the security of many functions moved to the cloud. Assessments performed last year exposed that most organizations' cloud strategies focused on application functionality and did not account for the security and logging requirements, storage, and bandwidth necessary for security monitoring. Many cloud providers have developed native security features, the capability to deploy security tools in the cloud, and offer some visibility that can be integrated into legacy security operations. Yet, plans to monitor did not follow key assets to the cloud for most security operations centers, leaving these SOCs with visibility only into the functionality that remained within legacy data center space.

Some organizations operating hybrid architectures have deployed solutions that integrate both on-premise and cloud workloads for a subset of critical applications, data, systems, or users. These organizations are protecting critical systems and are more capable by enabling detection through a targeted SIEM deployed within their cloud environment, building detection use cases that focus on the specific security

Enterprise SOCs continued to invest in the development of data lakes and analytics tools yet … such investments continue to be a science experiment with an uncertain future.

requirements of the applications deployed within that environment, and forwarding a small subset of alerts back to centralized systems utilized to drive SOC workflow and incident response. With intentional planning or through quick corrective action, these security operations centers are able to communicate key performance indicators back to executive leaders that are concerned with the bottom line and organizational risk.

Update on Data Lakes & Security Analytics

In 2015 Micro Focus Cyber Security Services (then part of Hewlett Packard) noted through this publication that big data and security analytics were the "shiny new technology that cyber defenders are drooling over. While these tools are providing value in some organizations, the space is still being defined and mileage varies greatly based on a variety of factors. Sustained value from these solutions are most apparent where findings are able to be operationally integrated with enterprise security operations capabilities." Over the past 3 years enterprise SOCs continued to invest in the development of data lakes and analytics tools yet for the majority of organizations assessed such investments continue to be a science experiment with an uncertain future.

Many organizations have spent years of development on open-source tools to recreate the collection, detection, and analytics capabilities SIEM brought to the industry several years ago. These home-grown systems can handle vast amounts of data but are also more complex to maintain and present an ongoing supportability challenge. Many data lake adopters have found that significant gains made in simplified collection of unformatted machine logs are quickly lost in the labor required to maintain these systems and the post-processing of the data collected to meet analytics and reporting objectives.

In some cases, as customers have prepared to meet compliance objectives, data lakes present a new security exposure. Many of these big data solutions contain personally identifiable information and other privileged data collected and stored in the clear. High turnover within the organizations that adopted data lakes masks this issue until new personnel discover gaps in data collection architecture, encryption, and overall security strategy. Micro Focus SIOC observed that as the GDPR deadline loomed in late 2017 many organizations executed Legitimate Interest Assessments to ensure that the acknowledgement and controls are in place so that the security data lakes do not end up being a compliance exposure as the regulation goes into effect.

Assessments performed in 2017 revealed some security operations centers performing effective security analytics on their data lakes. Most of these organizations are mining historical data for TTPs and IoCs and utilizing those findings for real-time detection, contextual investigations, and valuable visualizations. Micro Focus Cyber Security Services found that these teams had selected tools that were easy to use and allowed analysts to quickly search, filter, and visualize. However, the number of SOCs performing analytics processes in a mature manner is very low. Few organizations have made the operational investment to continuously reap value from security analytics performed on their data lake investments.

Conclusion

Over the past 5 years Micro Focus Cyber Security Services has seen cyber defense programs zig and zag in terms of maturity. Between 2014 and 2016 many sought to apply band aids through trendy products while others completely dismantled programs and performed full transformations of the technology deployed only to find similar, dissatisfying results based on internal operational weaknesses and poor business alignment.

In 2017 there has been a turning of the tide. For the first time in the publication of State of Security Operations report Micro Focus SIOC has seen an upward trend across all assessment areas. The detection and response capability of organizations continues to shift and to evolve. Yet, no matter at what capability stage you are at by now it should be evident that there is no quick fix product or service that can provide the protection and operational awareness your organization needs. Successful security operations programs require an assessment of the risk management, security, and compliance objectives of the organization and the active tuning of the solutions deployed.

Analysis of the assessments performed and data collected over the past years highlighted some core areas: operational relationships with vendors you trust to co-manage solutions are key; SOAR can help you but will require you to pick an initially narrow scope, start small; security fusion centers in the private sector come in all shapes and sizes, what is the right fit for you?

Micro Focus Security Intelligence and Operations Consulting has worked with some of the world's most advanced security operations centers. Over the last five years through the State of Security Operations report we have shared our findings from 200 assessments of 144 discreet SOC organizations in 33 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.

Appendix

The Micro Focus Cyber Security Services 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.

Business
Median: 1.57
5-year median: 1.57
Min: 0 .59
Max: 3.46

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. Micro Focus SIOC 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.

Micro Focus Cyber Security Services (then ArcSight Professional Services) 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 hundreds of organizations.

Micro Focus SIOC 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 Micro Focus 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 Micro Focus uniquely qualified to produce this report.

Security Operations Maturity Model and Methodology

The SEI-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 SEI-CMMI helps integrate traditionally separate organizational functions, sets process improvement goals and priorities, provides guidance for quality improvement, and offers a point of reference for appraising current processes. Micro Focus Cyber Security Services has modified the SEI-CMMI approach to measure the maturity of an organization's security operations capability effectively. The Micro Focus Security Operations Maturity 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 SEI-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.

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.

Figure 6. Levels and ratings

People
Median: 1.57
5-year median: 1.45
Min: 0 .10
Max: 3.80

Historical Category Details & Findings

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 and systematic response to those attacks.
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.

Continued on next page

Process
Median: 1.42
5-year median: 1.31
Min: 0 .12
Max: 3.81

Assessment Category	Findings
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.

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	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.

Continued on next page

Assessment Category	Findings
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 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.
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.

Technology
Median: 1.54
5-year median: 1.46
Min: 0 .13
Max: 4.06

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, Micro Focus 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. Manager's track and measure contributions to documentation as one of the SOC's KPIs.

Continued on next page

Assessment Category	Findings
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.
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.

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.

Learn More At
software.microfocus.com/en-us/services/security-operations-center
software.microfocus.com/en-us/services/enterprise-security-consulting-services

Additional contact information and office locations:
www.microfocus.com

www.microfocus.com

362-000077-001 | 9463 | H | DS | 03/18 | © 2018 Micro Focus. All rights reserved. Micro Focus and the Micro Focus logo, among others, are trademarks or registered trademarks of Micro Focus or its subsidiaries or affiliated companies in the United Kingdom, United States and other countries. All other marks are the property of their respective owners.