MICRO FOCUS

2019 STATE OF SECURITY OPERATIONS UPDATE

TRENDS, SUCCESS FACTORS, AND REAL-WORLD EXAMPLES FOR CYBER DEFENSE

Table of Contents

Introduction

With 4.1 billion compromised records exposed in more than 3,800 publicly disclosed breaches in just the first six months, 2019 is on course to be a record-setting year for data breaches. Compared to 2018, the number of reported breaches as well as the number of exposed records both increased by more than 50 percent.[1]

Given these increases, it's obvious that not enough is being done by organizations in general to protect against cyberattacks. What may not be obvious is how much more organizations with security operations centers (SOCs) need to do to outmaneuver cybercriminals and protect their critical assets. How well are SOCs today performing and how well-prepared are they to overcome struggles such as budget and staffing?

The Micro Focus 2019 State of Security Operations Update aims to answer these and other questions. Using insight gleaned from working with hundreds of organizations around the world to assess, design, and build out cyber defense programs, this update brings you the latest trends, success factors, and best practices for security operations (SecOps) teams.

Whether you're just getting started with a SOC or have years of experience in SecOps, this report provides you with insight and advice to improve your organization's maturity and success. Read on to learn about the common characteristics of high-performing SOCs and discover how your team compares.

150+ Security Operations Centers Assessed

With more than a decade of experience supplying the technology at the core of the world's most advanced security programs and enterprise SOCs, Micro Focus Cyber Security Services has worked with more leading cyber defense teams than any other organization.

Since 2008, Micro Focus Security Intelligence and Operations Consulting (SIOC) has assessed the capability and maturity of more than 150 discrete SOCs in more than 200 assessments, across 33 countries on six continents.

1. "Cyber Risk Analytics: 2019 Midyear QuickView Data Breach Report," Cyber Risk Analytics, July 2019

SecOps: Growing in Importance

Hackers are getting bolder, more organized, and more sophisticated. At some point, they will break through an organization's individual layers of security. While adding layers can help, the answer is not to add layers indefinitely, but rather to quickly detect and contain any threat that breaks through an individual defensive layer. A capable and mature SecOps function does that.

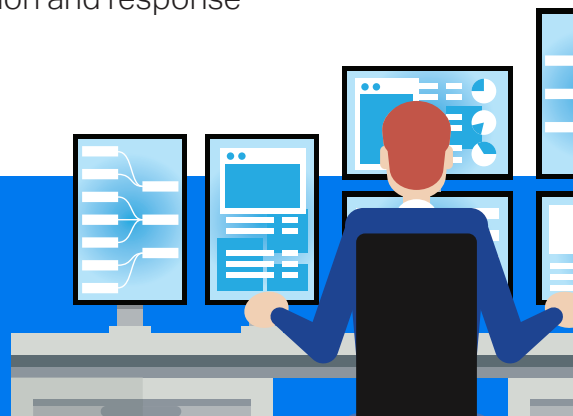
The Four Essential Components of SecOps

BUSINESS ALIGNMENT
Clarity of mission with a focus on protecting specific assets

PROCESSES
Well-documented tasks and workflows for repeatability, consistency, and efficiency

PEOPLE
Continuity, skills, and retention of key people

TECHNOLOGY
Effective use of solutions to improve detection and response



67% of IT and IT security practitioners believe that their SOC is essential or very important to their organization's overall cybersecurity strategy.

Source: "Improving the Effectiveness of the Security Operations Center," Ponemon Institute LLC, June 2019

Key 2019 Findings

Over the past 12 months, Micro Focus spoke with hundreds of companies around the globe about their SecOps capabilities. During these discussions, five topics and challenges emerged as significant trends across companies and countries:

THE WAR FOR TALENT

where hiring and retention issues are a growing challenge

TECHNOLOGY TO THE RESCUE

with optimism around artificial intelligence and machine learning

THE BATTLE FOR BUDGET

as making the business case for SecOps becomes more critical amid increasing cost pressures

MISSION ACCOMPLISHED

Wait, what's our mission again? SOCs lack clarity about what they are protecting

CAN YOU REPEAT THAT?

Security operations centers (SOCs) need to get better at processes and procedures

The War for Talent

A major problem discussed at the Micro Focus customer advisory board in June 2019 was the aptly named "Talent War." Given the industry-wide shortage of skilled security professionals, some companies are reporting that other organizations are luring their trained security professionals away. It's a lamentation we've heard echoed across industries and geographies as the talent shortage continues.

As we've noted in past Micro Focus "State of Security Operations" reports, having the right people in place is a bedrock requirement for success in a security operations center (SOC). In the 2019 SANS SOC survey, 58 percent of respondents said that the top barrier to SOC excellence is the lack of skilled staff.[2]

In our experience, mature and high-performing SOC operations have:

- Adequate staffing levels to handle the volume and velocity of events
- Appropriate training and certifications
- Content tuned for their organization's specific use cases to reduce false positives
- Appropriate documentation
- A clearly defined and communicated career path for staff

2. "Common and Best Practices for Security Operations Centers: Results of the 2019 SOC Survey," Chris Crowley and John Pescatore, July 2019

BEST PRACTICE TIP

Look for people with more diverse backgrounds, such as database administrators or application developers. This gives your SOC staff different viewpoints and a breadth of skills and experience while expanding your access to a broader pool of candidates in a tight job market.

BONUS TIP:

Choose technology to support your SOC that is intuitive and fits well into existing workflows to achieve productivity quickly.

The Battle for Budget

The customers we've been speaking with are expressing greater concern about the difficulty of obtaining funding for SecOps. Many believe that their organizations are not, or are no longer, investing sufficiently in SecOps. A common belief across these organizations is that budget is one of the biggest roadblocks that security operations center (SOC) leadership faces to maturing their SecOps capability.

The struggle around budget has led to increased pressure to cut costs, with outsourcing being one of the outcomes. In a recent study, 60 percent of SOCs reported that they outsourced SecOps functions for the cost savings.[3]

Outsourcing isn't always the only or the best way to "do more with less" in the face of budget shortfalls. Improving analyst efficiency and effectiveness through documented processes and the proper use of technology can help your SOC handle more with the same staff.

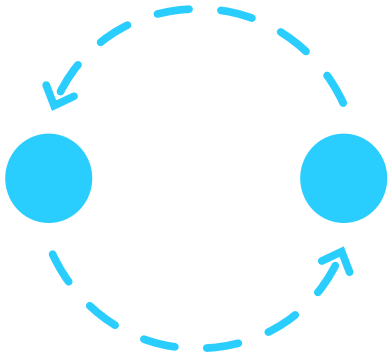
BEST PRACTICE TIP

Improve the SOC's alignment with the business to help you track and demonstrate the value of investing in SecOps to the organization. Be prepared to report on SOC success in protecting valuable company assets that are vital to the mission of the business. For example, a company in the oil and gas industry might show how the SOC is protecting confidential drilling data that could lead a competitor to a new source of oil.

3. "Improving the Effectiveness of the Security Operations Center," Ponemon Institute LLC, June 2019

Can You Repeat That?

Process is the missing piece of the puzzle for many of the SecOps teams we've spoken with in the past year. In assessments, we've seen more security operations centers (SOCs) backslide on developing a solid foundation of processes. Either they are allowing their processes to stagnate, with no continuous improvement effort, or they continue to operate in an ad-hoc way with undocumented processes.



Without the solid foundation that processes and procedures provide, SOCs become reliant on the tribal knowledge of individual "superstars" and are less predictable in the results they produce. The lack of defined processes could also impact the accuracy of operational metrics and increase the risk of not meeting business or contractual obligations around service levels.

Turnover of skilled individuals who have the processes memorized but not documented can cripple the capability of the SOC, often setting it back years in terms of maturity. Lack of processes leads to staff burnout and turnover, further exacerbating the talent problem. Staff struggle with the workload because they must reinvent the wheel every time. Automation can't be used to alleviate the workload stress because processes haven't been defined and therefore can't be automated.

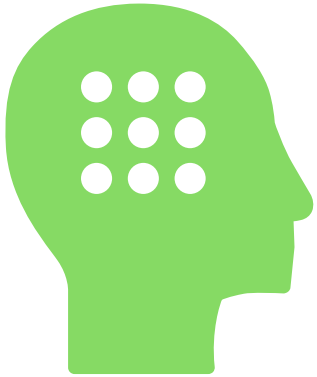
In contrast, the most capable cyber defense programs around the globe stand out in regard to processes with repeatability, continuous improvement programs, and metrics that track execution of their processes.

BEST PRACTICE TIP

The most successful SOCs are using an adaptable, portable, and operationally integrated process and procedure knowledge management system. Portability and ease of maintenance are key requirements for systems that allow images, video captures, scripts, and other operational materials to be published and shared across the team. Managers should track and measure contributions to documentation as one of the SOC's key performance indicators.

Technology to the Rescue

As new technologies such as artificial intelligence (AI), machine learning (ML), user and entity behavior analytics (UEBA), and security orchestration and automation (SOAR) tools appear on the market, SecOps leaders are hoping that these capabilities will alleviate many of the challenges that the security operations center (SOC) faces, from inadequate staffing and skills to handling greater volume of potential threats.



While new technologies can indeed improve SecOps outcomes, they do not automatically solve existing problems. Why not? Because the SOC must first have the proper foundation in people and processes to make the best use of these new technologies.

Both security information and event management (SIEM) and UEBA solutions are critical technologies for today's SOCs. SIEM is foundational for SOCs at all levels of maturity, providing real-time correlation for detecting known threats that follow established attack patterns. Once the foundation is laid, SOCs can add an additional lens of threat detection to find complex, unknown threats, such as insider threats or targeted outside attacks.

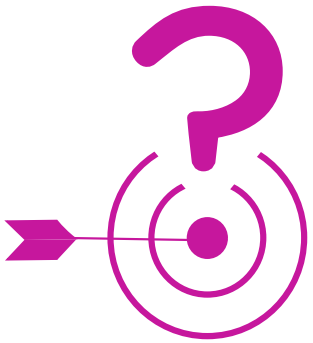
BEST PRACTICE TIP

To maximize the value of the technologies deployed in the SOC, it's important to first identify your security use cases and then select the right tools to meet them. As you document the use cases and create content that supports them, you'll be improving your SOC's ability to effectively identify known threats, which gives your analysts time and resources to look for unknown threats using technology such as UEBA.

MISSION ACCOMPLISHED

Wait, What's Our Mission?

One area of improvement in last year's report was the security operations center's alignment with the business. At the time, this was due in part to new legislation such as the European Union General Data Protection Regulation (GDPR), which forced many different parts of the business—including SecOps—to work together for compliance.



This year, however, a troubling finding is the lack of clarity in the mission of the SOC. Many of the SOCs we spoke with more recently either did not have a defined mission or had not communicated it to staff and other departments. Often this meant that there was a lack of visibility and understanding of which business assets (users, applications, data, intellectual property, and so on) were the most important for the SOC to protect. Consequently, these SOCs couldn't specify which types of threats the SOC should be most focused on to protect the business' valuable assets.

The most capable and mature SOCs define a mission and then clearly and frequently communicate it throughout the organization. With a clear mission and executive sponsorship and support of that mission, the SOC becomes a key contributor to cost avoidance and risk reduction initiatives in the organization.

BEST PRACTICE TIP

Start by understanding exactly what your SOC is protecting. Are you keeping operational technology safe from interruption by state-sponsored bad actors? Are you protecting data about products in your pipeline from competitors interested in beating you to market? Gain absolute clarity on what you are protecting, define your mission clearly, and then align your operational capability with the mission using service-level objectives and key business metrics that drive the right behaviors.

What Top-Performing SOC Teams Have in Common

In addition to uncovering some of the emerging trends in SecOps, we also turned our attention to what separates the high-performing security operations center (SOC) teams from their peers. What are mature, successful SOCs doing differently or better?

Here's what we found. High-performing SOCs share the following characteristics:

#1 **Top-down commitment**
They have top-down leadership in word, deed, and funding from the CEO, down. High-performing SOCs tend to have both operational leadership and an executive sponsor, both with board-level access.

#2 **Discipline**
They continuously look for ways to improve their Security Operations through process development, enhanced training, etc. to deliver better outcomes for the business and greater efficiency for the SOC.

#3 **Investment in talent**
They invest in experienced staff, education, and certifications (such as Certified Ethical Hacker).

#4 **A solid foundation**
They implemented the basics right first, then they continued building on top of their solid foundation. They didn't try to "run" before they could "walk."

#5 **Validation**
They use SecOps assessment services as objective tools to validate and refine their roadmap.

#6 **Alignment with IT**
They understand and have visibility into the entire IT infrastructure, endpoints, and servers.

The Secret of a High-Scoring SOC

A young security operations center (SOC) was one of the highest-scoring SOCs, in terms of maturity, that the Micro Focus SIOC team had ever seen. This SOC did almost everything right in every category of our assessment. What was their secret?

According to one of our consultants, this SOC was exemplary in all areas because it is working from a solid foundation of IT alignment and understanding.

> *"They know their servers. The SIEM has an accurate model of the network. They have an identity and access management tool. They understand user behavior and how the network is being used. They achieved an insanely high measurement because they have a great IT foundation on which they built their SOC."*
>
> **— A Micro Focus SIOC team member**

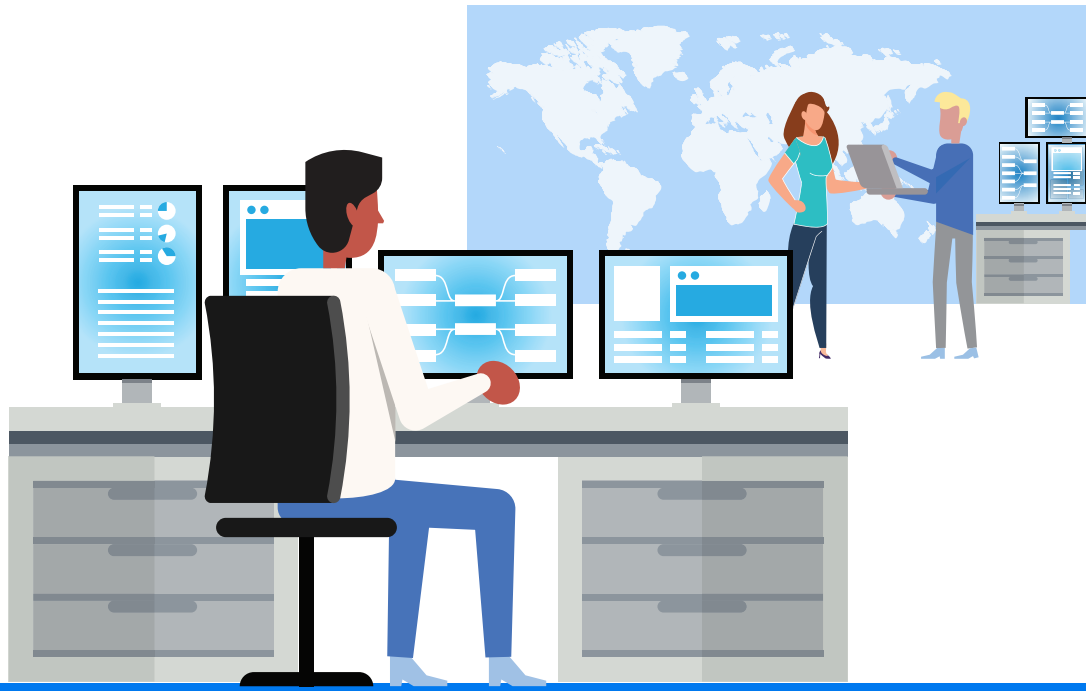
INSIGHTS FROM A REAL-WORLD SOC

KfW

Formed in 1948, KfW is a German, state-owned development bank based in Frankfurt. As of 2018, it was Germany's third-largest bank in terms of its balance sheet. Udo Gross, SOC Manager at KfW, generously shared his thoughts on the trends and challenges his security operations center (SOC) faces.

Like his counterparts in other parts of the world, Gross sees the talent shortage as a top roadblock to success for the company's SOC. "We have second-level analyst positions that we can't fill because of the shortage of available talent and the increasing numbers of SOCs being built that need to be staffed," he says.

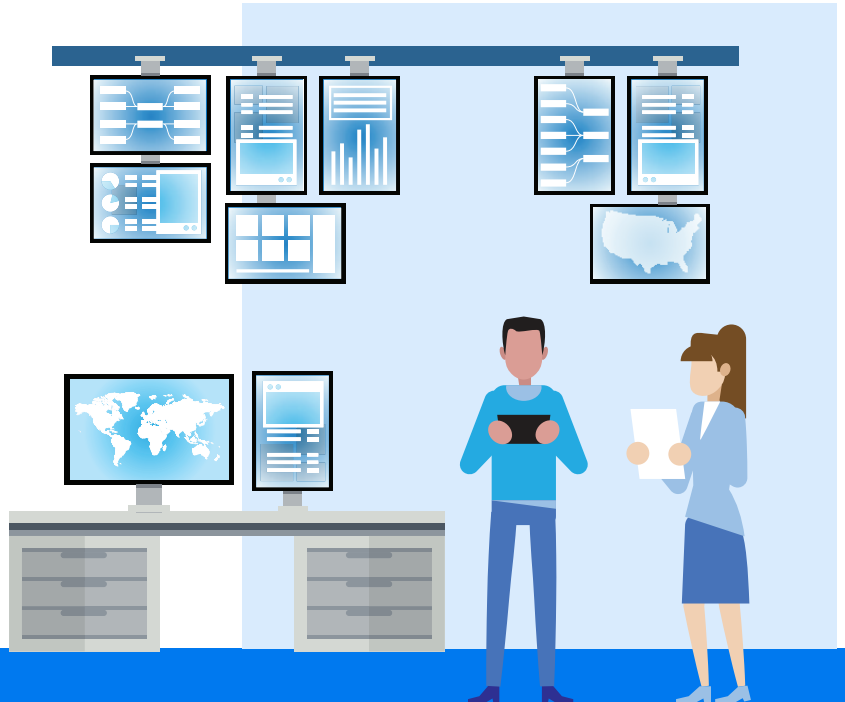
At the same time, he is continuing to grow his SOC's capabilities to support and align with the changing needs of the business and the company assets it must protect. To do so, collaboration and communication across departments becomes more important than ever. "As the number of incidents grows and our SOC scales to handle them, other parts of IT and our business must be prepared to grow as well and to handle increased remediation efforts, for example," says Gross. "It's important to make the value of the SOC absolutely clear to the business. We've found that it's very helpful to be completely open about what the SOC does to enable the security of the business."



INSIGHTS FROM A REAL-WORLD SOC

DNeX

DNeX Technology is a leading service provider in Malaysia's trade facilitation and energy sector. Its core businesses encompass a range of specialized companies, each providing customized services, solutions and infrastructures, engineered and led by industry experts. Its managed security services division offers 24x7 monitoring, as well as Security Information and Event Management, Security Operations Center building, and security log management services.



Rodney Lee is CEO at DNeX Technology and spoke about his SOC's success in overcoming some of the common challenges facing SOCs today.

Faced with a talent shortage, DNeX developed a new strategy. "We're working with universities and training interns from the bottom up to be skilled staff such as threat hunters," he says. At the same time, his SOC is using automation to increase analyst efficiency. "We have a team of people that create use case automation so that we don't have to search for the same threats and incidents, they pop up to us. Today, we have 14,000 use cases across the SOC."

Lee also believes that the right technology plays an important role in SOC success, but only if you commit to learning as much as possible about how to use the technology. "If you spend time in the technology you have chosen, then you get more out of it," he says. "The grass is always greener on the other side, so SOCs may be tempted to switch. But it's not about adding more tools, it's about getting more out of what you have."

INSIGHTS FROM A REAL-WORLD SOC

U.S. Federal Agency

Micro Focus also spoke with a cyber security division director for a U.S. federal government agency and he shared his thoughts on the challenges and successes his security operations center (SOC) is seeing.

"We started off small just a few years ago, but we've made great progress, which enabled us to get more funding," he says. "We then invested in maturing our capabilities, putting the tools we need in place, and creating processes and workflows."

Now that the SOC has been operating for three years, one of the top hurdles for the SOC is staffing. "We need more level 1 and level 2 analysts and threat hunters," says the director. "We need to be fully staffed to do everything we want to do, such as threat hunting."

The other issue is budget, which also hinders the ability to hire the staff needed for the SOC. "When a previous executive sponsor left, we started struggling to get the proper funding," says the director. "There is one executive who understands and supports our mission, so that is starting to help us get the attention and support we need."

Preparing for the Future: The Next-Generation SOC

As more security operations centers (SOCs) continue to mature and improve their capabilities and more organizations invest in creating and sustaining SOCs, cyber threats will increasingly be identified and rendered harmless from disrupting and damaging businesses and organizations. Playing an important role in SOC cyber defense capabilities will be what is currently being called the next-generation SOC.

What does a next-generation SOC look like? Its solutions are scalable, open, integrated, and layered to reduce exposure and empower more intelligent threat detection, investigation, and response. The next-generation SOC includes not only basic capabilities such as log and security event management and correlation, but goes beyond those to integrate threat hunting, artificial intelligence and machine learning, UEBA, SOAR, and other advanced technologies.

That said, the hallmark of the next-gen SOC is interoperability. Core and supporting technologies are integrated to fill defensive gaps or improve efficiency in detection, investigation and response. All the security solutions work together to be more than the sum of the parts.

Getting Your SOC Ready

What should your SOC do now to prepare for the next-generation SOC? The best approach is to start by getting the basics right first (i.e. people, process, technology, and business alignment). This means focusing on monitoring and protecting the right things, having skilled people in place, standardizing repeatable processes, and documenting it all.

Next Steps

While this year's State of Security Operations Update highlights some areas of concern and ongoing challenges for today's security operations centers (SOCs), we're optimistic about the future. We see organizations introducing innovative strategies for overcoming their current roadblocks every day. They are eager to put their technology investments to maximum use in protecting their businesses and maturing the SOC to handle today's and tomorrow's threats.

Regardless of where your organization currently finds itself on the maturity scale, Micro Focus can equip your SOC with solutions and services to improve your security operations and better defend your organization against modern threats—all while increasing the business value of your existing security solutions.

Learn more about Micro Focus Security Operations solutions by visiting
www.microfocus.com/arcsightesm

MICRO FOCUS®