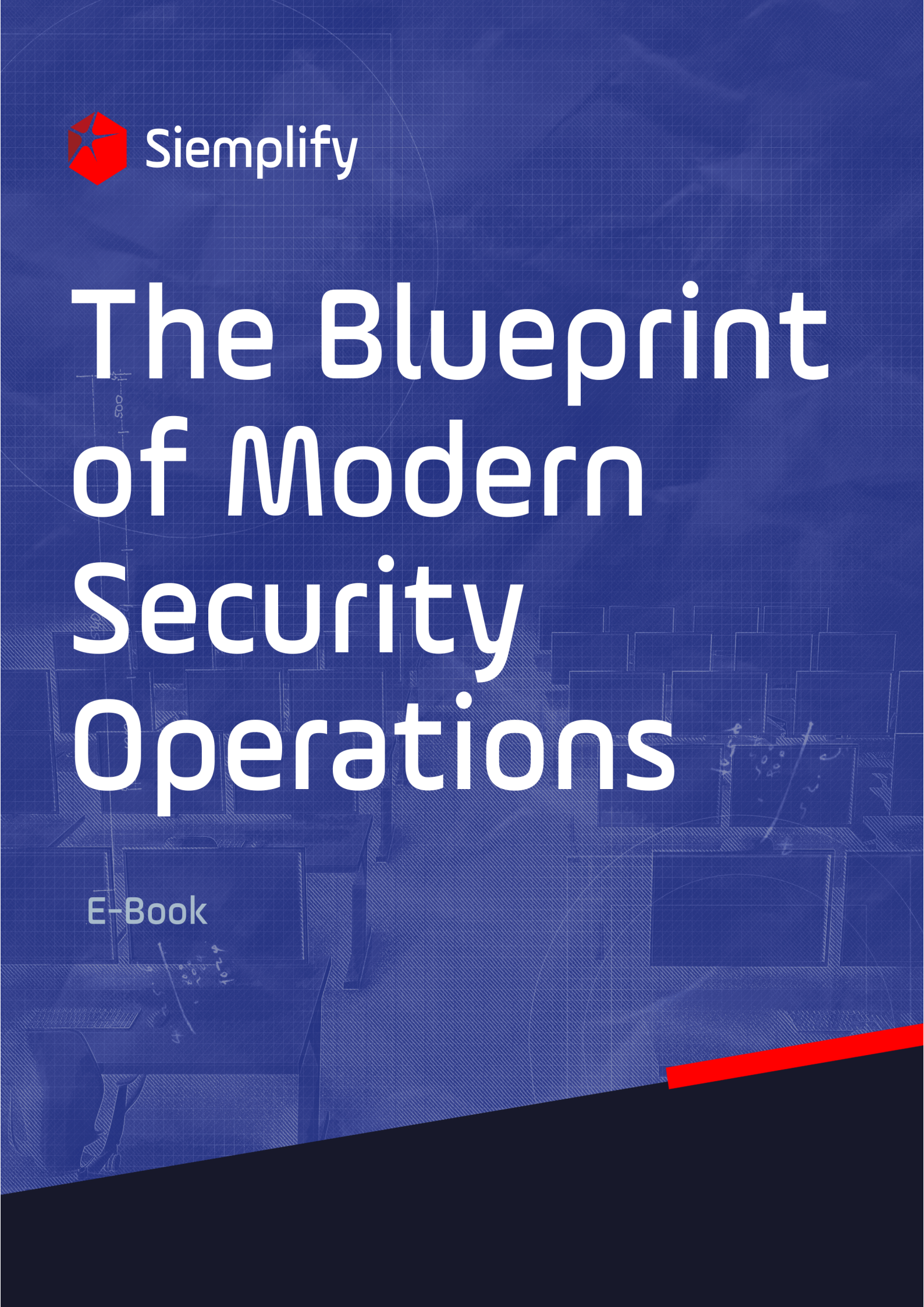

Siemplify
The Blueprint of Modern Security Operations
E-Book

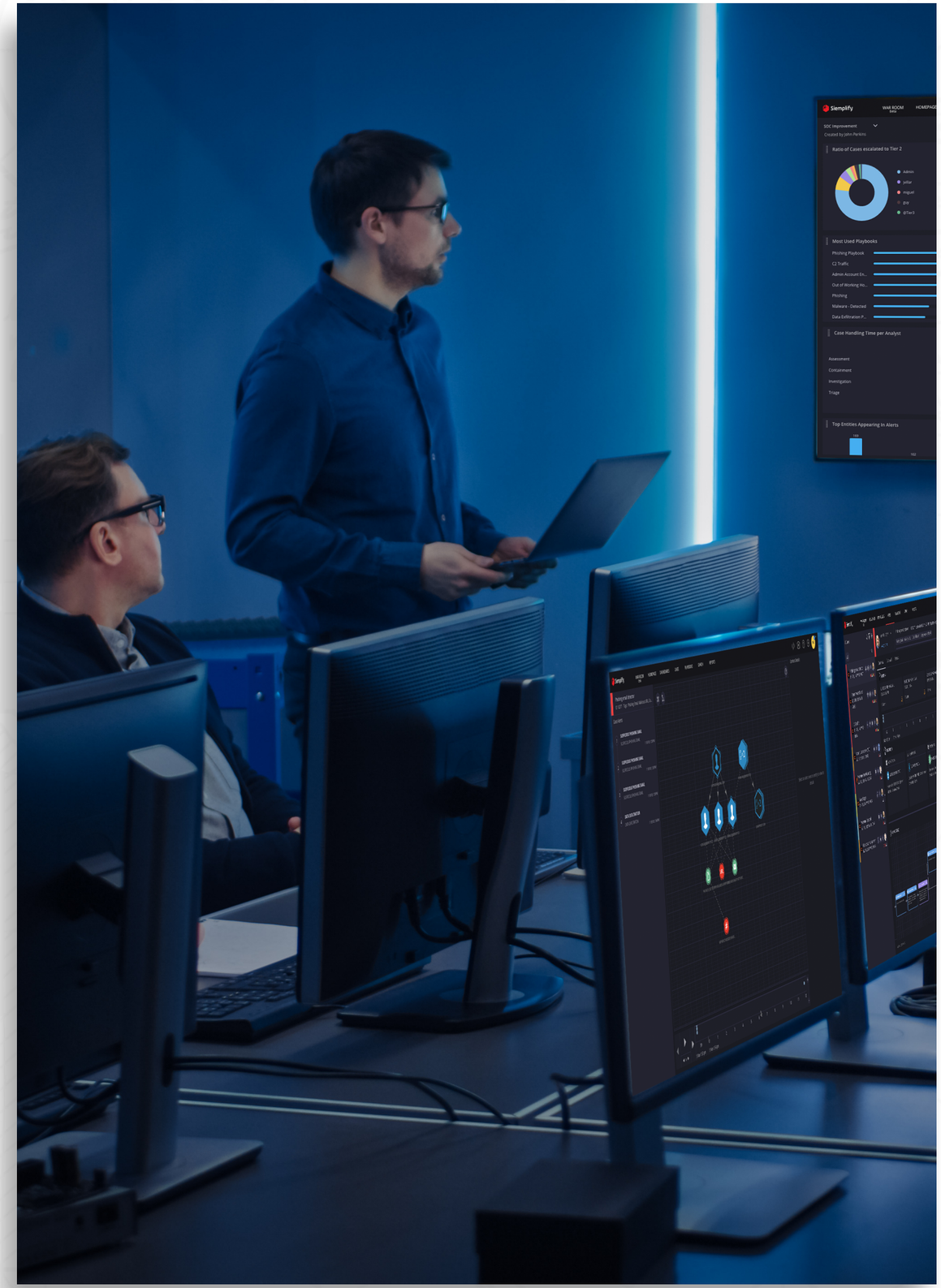


Table Of Contents

Introduction: The Mission of the Modern SOC

When the first generation of security operations centers, or SOCs, sprung up some 50 years ago (it's really been that long, look it up!) – and extending for many years following their earliest iterations – these command hubs largely were concerned with threat prevention. Attacks were plentiful, but not overwhelming, and the perimeter was adequately contained within most businesses, allowing security teams to rely on traditional technologies like anti-virus, firewalls and intrusion prevention systems to deflect the brunt of threats, which were reasonable, if not rudimentary, in terms of sophistication.

In the mid-2000s, SIEM arrived on the scene, taking large collections of log data and turning them into actionable information for analysts. Its appearance coincided with the emergence of data breach disclosure laws, triggering a never-ending stream of publicly acknowledged security gaffes and incidents that continues to this day.

These two independent events heralded the dawning of a new era in cybersecurity, in which corporate strategies began to shift to emphasize holistic visibility, the first hint that malicious behavior and successful intrusions and compromises would one day be accepted as inevitable.

Nowadays, you don't need to be reminded, from Stuxnet to SolarWinds, the threat landscape is organized, advanced and well funded, purposely designed to trip up security solutions and essentially deteriorate the efficacy of prevention-focused security.

At the same time, thanks to stringent compliance requirements, evolving corporate attitudes around risk and a perpetually ballooning attack surface, organizations now desire greater control over the monitoring, detection and response to threats.

This has midwifed a situation where the average enterprise is locked and loaded with an assortment of security tools, meaning alerts are incessantly firing off and threats invariably need triaging and prioritizing (some of which may grow into full-fledged incidents). This has only grown more pronounced in the post-COVID world, where remote workforces prompted furious cloud and IoT adoption, itself opening a litany of new exposure points – and as one cyber expert described them "entirely new security black holes."

Complicating matters, in addition to the ongoing security skills shortage, is that all this noise results in a lot of unorganized, out-of-context and unactionable data for you and the team to ingest. Another side effect is "alert fatigue," the result of manually performing too many redundant and perfunctory tasks. This has – and continues to – take an emotional toll, from missing important alerts to burning out. In total, the situation is currently one big powder keg, demanding an innovative and deliberate refresh, complete, perhaps ironically, with the familiar prose of people, processes and technology. Except lots of the old rules are crumbling. A modern security operations master plan is required. Consider yourself an architect, and here is your blueprint to getting started.

Part 1: The Economics of the Modern SOC

Like virtually all business functions, the success of security operations can be measured by return on investment, profitability and sound financial position. Cybersecurity was long considered a cost center, but over time, business leaders have more readily embraced cyber risk management because of the significant monetary impact that cyberattacks can cause, leading some forward-thinking companies to now view security as a business enabler instead of a revenue drain.

The pandemic may have been the clincher. While the COVID-19 crisis initially sparked confusion and disorder as teams fled office buildings to the safe confines of their homes, it was industrious cybersecurity teams that stepped in to pacify the situation and keep the newly remote workforce secure as it turned to new (often in the cloud) technologies to remain productive.

Although the health emergency may have been a "win" for security teams in terms of awareness – 74% of IT leaders shifted funds to cybersecurity – it also recast an unremitting light on the challenges and deficiencies facing the function, particularly security operations. The number of alerts, already a problem, went up. So did the disparate nature of security tools, more of which were needed to counter the remote threat. Longer hours due to existing skills being unable to keep up with the new demands meant more fatigue, retention shortfalls and burnout.

It is therefore no wonder that the Ponemon Institute in January determined more businesses than ever view security operations as "essential," listing their most important SOC activities as reducing false positives, creating agile DevSecOps functions and automating processes. According to the findings, 80 percent of respondents say their SOCs are "essential" or "very important" to having a strong security posture, an increase from 73 percent of respondents last year.

But indispensability doesn't always equate to a good investment. Fifty-one percent of respondents said the return on investment (ROI) of their SOC was getting worse, not better, an increase from 44 percent of respondents in 2019.

Here are three factors affecting ROI in the SOC:

1. The Attack Surface is Swelling, and Adversaries Are Growing Stronger

In the business world, COVID-19 accelerated digital transformation, including hybrid and multi-cloud cloud, IoT and other emerging tech. But it also grew the potential attack surface and exposed weaknesses in organizations now forced to accommodate a distributed workforce using unmanaged technologies. A recent report by Zscaler assessed the attack surface of 1,500 companies, uncovering more than 202,000 vulnerabilities, nearly half of which were classified as "critical" or "high" in severity. Over the course of just a few days during production of this e-book, Microsoft shipped an emergency patch for a critical WIndows flaw. The nickname? "PrintNightmare." In addition, a crushing global "supply chain" ransomware attack originating at Kaseya, an IT solutions developer for MSPs and enterprise clients, impacted potentially thousands of small and midsize businesses.

> "I think the only reason we didn't see breaches of this scale and magnitude in prior years is simply because there weren't enough adversaries. InfoSec didn't change all that much on the defense side, offense did.
>
> Jeremiah Grossman
> **@jeremiahg**

2. There's Not Enough Skilled Help and Ones Who Are Skilled Are Leaving

This one is obvious. The lack of proficient cybersecurity professionals is neither native nor exclusive to SOC. It's everywhere in infosec, so much so that multiple studies have reported the skills gap has greatly tipped the scales in favor of your adversaries. Combine the talent dearth with the overwhelming number of alerts that require processing and documentation – a preponderance of which are false positives – and an already meager and overstretched staff runs the risk of burning out, with members either getting plucked by other firms or simply quitting with the hope of finding greener (and more serene) pastures. There's a reason the SOC is sometimes dubiously monikered "sitting on chair." If an analyst's only duty is receiving an alert, submitting a hash to VirusTotal, and copying and pasting the results to a ticketing system, whatever passion they had for the job will quickly erode. There is only so long an intellectually inspired individual can perform mundane and repetitive tasks.

3. Security Tools Are Aplenty, But They Don't Play Well Together

Companies are spending more money than ever on cybersecurity, and a healthy portion of that investment is being earmarked for security tools, with large companies averaging well over 100. Not surprisingly, many of these solutions don't co-mingle. This creates added management complexity, higher costs and the potential to miss something important.

Flipping the Script on ROI

Of course, cybersecurity will never be a revenue generator (at least not in a traditional enterprise), but it still can generate ROI if an organization considers how much exposure it has and how much that exposure is being reduced by security controls.

Automation in the SOC will not eliminate threats or remove the work from analysts and engineers, but it is an obvious option for streamlining your detection and response efforts, as well make your team happier and involved in more inspiring work. This e-book will discuss more on the technology component of the modern SOC in Part 3. But first, let's explore the fabric of the modern SOC: the people – and the role they must play.

Part 2: The Culture of the Modern SOC

If you think about it, the concept of modern security operations was preordained, a product of years of digital transformation and rapidly changing business dynamics, each more aggressive than the last. So for as much as the modern SOC is an achievement in technology, engineering and composition, it also must be a feat in approachability, support and collaboration with the greater organization – because everything touches security and security touches everything.

Security operations will yield the greatest benefit for a business if it is seen as a trusted partner, especially in a time when cyber-risks are stretching beyond traditional SOC use cases. In the words of Drizly CSO Joe McManus, speaking at SOCstock 2021, security operations must "become a group of yes." Gone are the days when SecOps can be seen as a roadblock. If such an inhospitable attitude is to persist – for example feature requests are regularly negged over perceived security issues – business groups will work around the SOC, which will give birth to shadow IT. A plethora of ways already exist to invite malicious content or data-leakage risks into an organization, and the proliferation of web- and cloud-based software outside of the SOC's auspices will swing that door open even wider. The magnitude of the threat is already enormous. Why be responsible for creating even more exposure points?

To avoid this fate requires the modern security operations practitioner to be empathetic, accessible and helpful. The SOC staffer is not here to make employees look bad or dismiss their needs. That means helping to troubleshoot problems that you may not think are yours such as outages (where synergy with system admins and network engineering is mandatory). Ultimately, the goal is to join forces to mitigate risk together. Consider some key areas necessitating harmony:

Software Development

Arguably the most important internal relationship for the SOC to sew is with the development team (hence why 'DevSecOps' has become a hot buzzword due to its mantra of advocating for security automation and monitoring throughout the software development lifecycle). In organizations where these disciplines have not been formally reconciled, the burden falls on the SOC team to engage developers as peers. Not only will this allow you to participate in two-way conversation regarding architecture and code review, helping identify errors before an application goes live, but also aid you in understanding more about how to properly monitor for alerts of the very real-time security alerts and notifications being integrated into these newly developed applications.

Incident Response

Whether you are investigating an ordinary alert, trying to determine whether something is a false positive or embroiled in a full-blown incident, chances are you will need the help of others , especially the IR squad. To obtain all the log data and other details you require, goodwill will encourage others to give you what you need to resolve the case and determine a course of action to avoid a similar issue in the future. Afterward, be sure to thank the sources from which you drew information and share with them the outcome of your investigation, as they may be curious of the result.

Vulnerability Management

In the case of addressing security flaws and misconfigurations, SecOps pros will be working with more IT-inclined staff than in a typical security awareness training exchange, but empathy is still needed. When you interact with IT and operational teams, you need to be kind so that you can understand their challenges and tolerance for patching, which is known to occasionally break business applications and cause downtime. And if patching isn't an option, you also need to understand their comfortability with compensating controls.

SIDEBAR

How Diversity and Inclusion Can Disrupt the SOC

Diversity, equity and inclusion (DEI) is another area that the modern SOC must embrace. Women continue to be significantly underrepresented, and while minority representation in infosec is slightly higher than the U.S. average, inclusive cultures remain elusive. Yet studies have consistently shown that organizations with greater gender and Black, indigenous, people of color (BIPOC) equity outperform companies with more homogenous workforces.

For security teams, that means being better equipped to more creatively and innovatively detect and respond to threats, and practitioners feeling more comfortable, connected and confident in their ability to keep security postures strong. Consider how Christine Izuakor, founder and CEO of Cyber Pop-up, a start-up that connects high-demand businesses to on-demand cybersecurity services, described the benefits of a heterogeneous SOC team:

"The people who are carrying out these attacks don't look one kind of way or come from one different background. They come from so many different backgrounds across so many different parts of the world. You can't defend against that, by having one train of thought. You need those different perspectives, you need the people who are defending against these attacks to look just like the people who are attacking and that looks like a variety of different people."

DEI also extends beyond race, gender and ethnicity to also include brain function and behavioral characteristics. A push is underway within the cybersecurity industry — for example, the Asia-Pacific CSO of banking giant HSBC is leading an ambassador program — to ensure neurodiversity is more accepted by digital teams. Neurodiversity is defined as the concept that neurological differences, typically manifested in disorders like dyslexia, ADHD and autism, are nothing more than normal genome variations within the human mind.

Here are is a tip-list to help you on your journey for diversity and beyond:

Phase 1: Prepare	Phase 2: Write the Plan	Phase 3: Implement and Track
☑ Assess where you are	☑ Get collaborative	☑ Determine your tracking cadence
☑ Define the business case	☑ Identify how to reach your goals	☑ Find your tracking tool
☑ Engage the right stakeholders	☑ Outline your action items	☑ Review and improve on purpose
☑ Identify your "why" and goals	☑ Put it all together	
☑ Garner broader feedback	☑ Communicate your plan	

Source: ISC(2)

Maximizing Capabilities by Skills, Not Tiers

Consider the extent of all that SecOps must account for: from system diagnostics, application output and user actions to network traffic, account creation and detection tools. This requires a litany of skills that should prompt teams to challenge the traditional tiered model.

In the tiered SOC model, junior analysts triage inbound events and escalate those they can't close out quickly to more experienced staff. It's a time-honored staple of security operations. But this model is changing, especially as more perfunctory tasks are largely solved by automation. A recent Cyentia Institute research report commissioned by Siemplify showed that barely over half of survey respondents still work in traditional tiered SOCs made up of different analyst levels. The rest form teams of mixed roles and experience. A SOC categorized by skills instead of tiers is more flexible, ensuring everyone is delivering what they excel at — and, hopefully, enjoy doing.

So how can you get started with this model? Build out your team in a new way: Staff it with well-rounded personnel, who according to McManus from Drizly, should carry skills in these areas:

- Network engineering
- Software development
- System administration
- DevOps
- Cloud
- Compliance
- Forensics/Incident Response
- Analysis

You might be wondering: How can I afford to hire all of these people? When making the case, draw on the simple fact that the cost of a breach will be significantly higher than the salaries required to construct a more versatile team. Going the skills-based (versus tier-based route) will allow you to better secure systems, limit downtime, model threats and execute tabletop exercises.

Of course, while your team should not be expected to be the end-all-be-all in the above bulleted disciplines, members should know enough to be able to both help the SOC team and interact with the specific function within the organization. For example, your software development-focused SOC person does not have to be a coding whiz, but they should have cursory knowledge in common programming languages.

Part 3: Design Trends of the Modern SOC

While there is widespread agreement that many SecOps programs are not where they need to be in terms of performance and maturity, there is less consensus on exactly where they should be and how best to get there. This state of perplexity was only compounded by pandemic-introduced risks, as well as a series of high-profile attacks that continue to pervade mainstream news cycles. Major shifts are forcing organizations' hands, however, and are metamorphosing the way in which security operations is being conducted:

Cloud & Infrastructure Transformation

Cloud deployments are surging, with Gartner estimating that by 2024, more than 45% of IT spending on system infrastructure, infrastructure software, application software and business process outsourcing will shift from traditional solutions to cloud. "This evolution makes cloud computing one of the most continually disruptive forces in IT markets since the early days of the digital age," according to Gartner.

Adversaries are naturally drawn to this new paradigm, and a moment of reckoning is upon us. The cloud era, of course, delivers a golden opportunity for businesses to revolutionize their offerings and provide workers with more productive ways of doing business.

But it also presents security teams with the ability to reimagine efforts to remain resilient and protect end-users and customers. This can be accomplished through the adoption of cloud-native tools and platforms (such as SIEM, EDR and SOAR) which allows organizations to adapt their use cases to cloud workloads and be more nimble (with less operational overhead required) in the complex effort that is threat detection and response.

Remote Workforces and Team Organization

Speaking of uprooting tradition, the days of in-person SOCs may be waning. Dedicated, in-house facilities are designed for maximum productivity and comfort for analysts and engineers (and, depending on how many bells and whistles these command hubs contain, present a "wow factor" for touring prospects and customers). But now COVID-19 has compelled security operations teams to do their threat detection and response in completely fractionalized and federated settings. But as the months have gone on and early gaps and vulnerabilities have been filled, pros – with the help of smart leadership and collaboration tools – are learning that virtually everything they do can be accomplished remotely, in many cases just as well as in a physical space.

Accelerated Managed Security Services Utilization

The aforementioned pressure points facing security operations teams (overload of alerts, expanding attack surface, skill shortages, etc.) happen to also be some of the primary reasons why the modern SOC is continuing to call on third-party service providers to help offset their internal limitations and amplify their detection and response capabilities. The relationships and needs that end-users require from their MSSP and MDR vendors will be unique, but in general, the most optimal partnerships are a mix between what you do well and what the provider does well. Much more on this in the "Operations" section below and the MSSP section in the final page of this report.

Low-Code/No-Code Automation

Automation in the modern SOC aims to reduce human intervention in time-consuming and often humdrum tasks, from enrichment through response, work that can contribute to burnout. Automation, however, will always have its limitations, even as it matures to take on more cognitive processes. This assures that humans will always have a key role to play in the modern SOC.
All of these factors have coalesced to assemble a budding default model for security teams: "anywhere security operations." Not only is the notion of practicing SecOps agnostic of a single location an obvious byproduct of a workplace dynamic ineluctably reshaped by a health crisis, it is also is a signal of nimbleness and maturity — those organizations whose security operations are most primed to succeed in this era will prioritize anywhere success.

"The philosophy of anywhere security operations will be underpinned not just by decentralized locations, but also by secure remote access technologies and policies (helpful tips here), cloud infrastructure, outsourced partnerships, greater collaboration and automated workflows."

1) Location: Remote and Distributed

In a January 2021 survey conducted of 133 executives and 1,200 office workers in the United States, PwC declared remote work has been an "overwhelming success" with 83% of employers now reporting that the transition to remote work has been "successful" for their organization.

The "dark room with the screens," as a SOC is traditionally characterized, is not exactly an anachronism, but it may be past its prime. Going forward perhaps, the SOC, as Duran Duran described his ninth studio album, "will be the name of a place, but not a physical space."

With the pandemic firmly implanting a new work-from-home norm, security operations is being performed in as distributed a way as ever. What the SOC gains from this flexibility to hire outside of a certain geographical area and keep workers happier – in fact, 39% of respondents to the Siemplify State of Remote Security Operations survey report said their morale has "greatly" or "somewhat" improved while working from home – new challenges have cropped up.

No longer able to tap on the shoulder of a peer, SOC teams must ensure they are adequately collaborating – for example, to make sure they can communicate effectively in a crisis or are not duplicating work – and that there are step-by-step instructions and knowledge transfer in place to ensure the fluid onboarding of new analysts and engineers.

Make sure you have:

- ☐ Central collaboration and information sharing.
- ☐ Consistent and documented organizational know-how and operating procedures.
- ☐ Visibility and live measurement of the security operations function.

2) Operations: External Collaboration

It's becoming extremely rare for any SOC to be self-contained. SecOps teams are increasingly leveraging MSSPs and MDR providers for agility, scale and cost savings during these rough-and-tumble times. These arrangements also free up organizations to eventually gain the internal knowledge that they were originally lacking, which led to calling on a provider to help fill competency gaps in the first place.

Yet these relationships remain rife with shortcomings. Still common are service providers delivering obscure and confusing emails to clients about malicious discoveries and what they need to do to remediate the issue, often with zero accountability about whether the end customer understood the issue or took the required action to rectify it.

End-users are demanding more than ever nowadays, no matter how prominent of a role they play in the customer-MSSP partnership. In particular, they are yearning for greater visibility into their expanding network, more transparency around what is happening within it, and, most of all, the ability for an outsider provider to do more than simply notify and decree marching orders for self-remediating threats. In the modern and mature outsourced arrangement, each relationship looks different, not just in composition (e.g. fully managed, where the MSSP owns SOC processes; co-managed, where the MSSP leads SOC know-how with input from the end-user; or a collaboration model, where the end-user leads with input from the MSSP) but also in terms of divergent levels of needs, processes, decision making and overall maturity.

An MSSP whose limits are the alerting of suspected malicious activity is no longer adequate because of the speed, precision and concealment by which attackers strike. Customers care more than ever about positive outcomes from their providers, which means finding, disrupting and eradicating adversaries and helping get their affected business back on its feet as quickly as possible.

Understanding that each customer profile is distinct and empowering each through collaboration, accountability and visibility is no longer a nice-to-have within your portfolio. But if you succeed here, good fortune awaits as you will curate a more satisfied and "sticky" customer while limiting a liability you need to take on behalf of the client.

If you're the client that is looking for the optimal services provider to support your security operations, you should:

- ☐ Prepare adequately before engaging MSS providers by having well-defined, risk-based security requirements and use cases.
- ☐ Focus on outcomes and deliverables and, where possible, avoid being prescriptive around the delivery model or technologies used to deliver against requirements.
- ☐ Assess if existing managed service providers (MSPs) and IT outsourcing partners meet security technology management requirements before approaching dedicated security service providers.
- ☐ Prepare the internal processes that will be used to consume and respond to the outcomes and deliverables that an MSS provider will deliver.
- ☐ Ensure that constraints on technology choices or deployment restrictions (such as compliance, regulatory or legal needs) are well-communicated to potential providers early in the stages of engagement.

Source: Gartner Market Guide for Managed Security Services

3) Environment: Infrastructure

The move to the cloud, proliferation of IoT devices, and the push for digital transformation are all contributing to a rapidly expanding digital footprint and growing complexity of an organization's environment. The ability to harden and reinforce infrastructure is more important than ever.

The COVID-19 pandemic has forced security teams to leave the traditional on-site SOC model behind and embrace a dispersed security team. In a post-pandemic world, retaining flexible work policies will be the key to success – making it possible to secure hard-to-find talent wherever they might be, improve morale and increase retention.

Assure you:

- ☐ **Obtain clear visibility into your IT infrastructure.**
  Visibility of all endpoints connecting to your network is important, as they serve as a common starting point for malicious hackers. But it's even more critical when those endpoints are IoT devices that may not be approved for connection, unpatched or improperly configured.

- ☐ **Understand your biggest threat use cases**
  A recent study, which examined the challenges of the modern SOC, found that 27% and 24% of respondents, respectively, said that alert fatigue and false positives served as their largest sources of pain. One of the ways this can be resolved is by reviewing case histories and studying issues that arise most frequently. Allocate resources to addressing them quickly and look for ways to automate management, such as grouping by threat instead of working individual alerts.

- ☐ **Embrace automation**
  You already know that the security industry is operating with a massive talent gap – limiting, among other things, the ability to not only manage your fleet of connected devices but for security operations centers to operate with enough analysts who are trained at detecting the types of anomalous traffic that a digital transformation may bring. But even if your SOC was filled to the rafters with qualified analysts, the sheer number of invading most companies alone calls for the need for automation.

4) Processes: Integrated, Automated and Agile

Security tools – and the networks and assets that security teams need to secure – are increasingly in the cloud. Organizations are demanding use cases that predominantly or exclusively leverage cloud-native security tools (think AWS GuardDuty, Azure Security Center or Google Cloud). A cloud-native SOAR is an optimal solution to bridge cloud and on-premises detection, investigation and response – integrating seamlessly to all cloud-based and on-prem security tools in an organization's arsenal. SOCs that embrace this cloud-native and cloud-heavy approach will be more scalable and flexible and able to innovate faster.

In this type of environment, efficient, repeatable, adaptable processes will rule the day, and that is where cloud nativity comes in. According to the Cloud Native Computing Foundation, "cloud-native technologies empower organizations to build and run scalable applications in modern, dynamic environments such as public, private, and hybrid clouds … Combined with robust automation, they allow engineers to make high-impact changes frequently and predictably with minimal toil."

Other Things to Utilize in the Modern SOC Architecture

1) Use XDR to Expand Your Visibility

Extended detection and response (XDR) is one of the hottest catch phrases in security operations these days. When implemented successfully, XDR can deliver better detection through the consolidation and correlation of multiple detection technologies. However, XDR does not eliminate the need for repeatable investigation and response processes (aka playbooks) that leverage automation wherever possible.

When referring to XDR strategies and offerings, it is important to distinguish between closed and open approaches to XDR.

- Open (or "Hybrid") XDR is a vendor-agnostic approach that relies on integrations, and typically an additional analytics layer, to bring together multiple detection and response technologies. Through deep integration with best-of-breed technologies (such as SIEM, EDR, NTA, cloud and many others), open XDR offerings deliver the contextual visibility, analytics and processes required to streamline security operations and detect and respond effectively at scale.
- Closed (or "Native") XDR consolidates telemetry from multiple detection tools offered by a single vendor. These detection tools typically include endpoint detection (network detection, cloud security, user-behavior analytics and more.) Ideally a closed XDR product should offer all required sensors, as well as other components required for effective detection and response (such as threat intelligence) in one tightly integrated and cost-effective offering.

2) Use the MITRE ATT&CK Framework to Classify Attacks & Assess Risks

The MITRE ATT&CK Framework is a globally accessible matrix that documents real-world adversarial tactics, techniques and procedures. It can deliver extensive operational value to modern SOC teams, especially in three areas:

- **Education:** Not all security analysts possess the knowledge or experience to have seen every type of attack. The framework helps guide them through investigations, and equips SOC managers with threat trends as they emerge.
- **Information:** The framework informs decision-making in the SOC, particularly around threat investigation, mitigation and response flows, and proper tuning of your security stack.
- **Speed:** This is arguably the most valuable component of the framework. Time is of the essence during active attacks. Integrating the MITRE ATT&CK model into your playbooks can give you the output you need to save critical time during a response.

3) Use Zero Trust to Address Security Requirements in the New Remote Normal

The Zero Trust security model was first proposed by the analyst firm Forester. It is based on the premise of "always verify, never trust." In the updated version, released in 2018, the Zero Trust eXtended Ecosystem places data as a central point from which security decisions are made. There is much work involved in using the model, but the expansion of the enterprise network and complications of moving data across IoT and the cloud means that this is a useful way to approach security. Authentication is a key principle of Zero Trust. OWASP provides a Top 10 list of IoT weaknesses, and authentication tops the list. Using a zero-trust detect-and-response approach is increasingly being used within the SOC to plug the gaps new digital technologies create.

Source: https://blogs.cisco.com/government/zero-trust-cybersecurity-for-government-part-one

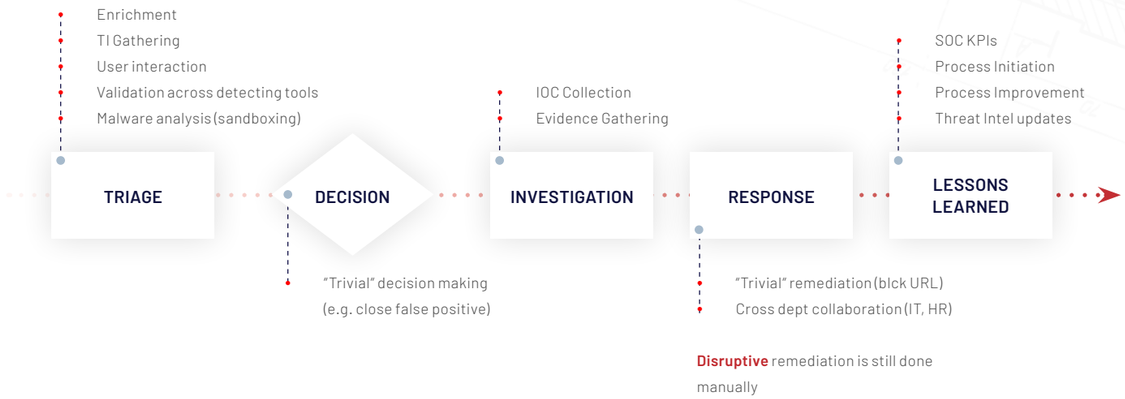
Conclusion: Automation of the Modern SOC

Earlier, we talked about the importance of automation in the modern SOC as organizations are forced to be more agile and nimble in the face of everything that has been documented in this e-book.

Eventually automation will reach what Deloitte and Google Cloud describe in this paper as "the next frontier for automation," involving the automation of decision-making, and this would allow humans in the SOC to be even further freed up to concentrate on the "hardest tasks."

Until then, many organizations, from enterprises to MSSPs, are finding comfort in the value that security orchestration, automation and response (SOAR) brings. These platforms not only deliver extreme process value to one's security operations but also liberate your most precious capital – your people – to creatively problem solve and actually make businesses more secure.

The adoption of SOAR platforms has grown significantly in recent years. Countless end-user and service provider security operations teams are leveraging SOAR to address the most common security operations challenges – too many disparate technologies, alert overload, limited staff and manual processes.



WHAT CAN YOU AUTOMATE?

Naturally, SOAR platforms have matured and evolved over time. With over a dozen SOAR solutions to choose from, and given that by now most offerings cover "the basics" such as drag-and-drop playbook creation and common integrations such as SIEM and threat intelligence, zeroing in on the right questions to ask when choosing a SOAR solution is more important than ever.

SIDEBAR

QUESTION: Is your organization mature enough for SOAR?

ANSWER: Likely, yes. Although running a SIEM and having a security operations center in place are typically key indicators for SOAR readiness, the technology isn't just for large corporations and MSSPs. The reason why? All organizations bear the ire of cyberattacks, and all organizations need to scale, especially small and midsize businesses operating with limited security staff and other resource constraints, and the automation element of SOAR allows you to do exactly that: Scale your security.

How Managed Security Services Providers (MSSPs) Use Automation

Security service providers have become big winners during these rough-and-tumble times because of their ability to provide agility, scale and cost savings to organizations. The Siemplify-commissioned State of Remote Security Operations survey report supported this foreceast and found that 52% of respondents have increased their use of an MSSP since the pandemic began.

Security orchestration, automation & response (SOAR) platforms streamline and enhance incident response, allowing traditional MSSPs to go beyond basic management and monitoring to rapidly transform into MDR providers.

SOAR platforms ingest aggregated alerts and indicators of compromise (IOCs) from detection sources and then execute automatable, process-driven playbooks to enrich and respond to these incidents. These playbooks coordinate across technologies, security teams and external users for centralized data visibility and action – for both analysts and customers.

How to Evaluate a SOAR Solution

An MSSP seeking to deploy a SOAR should be vetting for a host of requirements during the selection process, including core capabilities (features and functionality), platform characteristics, and unique business considerations.

Core Capabilities and Functionality

SOAR should provide a centralized security operations platform as the nucleus of its security management. A single console provides an MSSP with ability to service multiple customers without switching to other tools. Within the scope of the SOAR, core features and functionality are standard "table stakes" requirements that drive an effective product.

Triage
Filtering out noise, grouping related alerts, and integrating multiple data sources to enrich and provide insight across grouped alerts.

Case Management & Collaboration
Support every stage of the case workflow, from creation to closure, ideally from a single workbench designed for the analysts.

Playbooks
Out-of-the-box playbook knowledge base that can accelerate time to value by driving the full range of playbook requirements and providing a balance between automation and analyst interaction.

Case Visualization
Visual representation of each case provides intuitive understanding of complex cases and threats in a fraction of the usual time required.

The Dawning of a New Day

There you have it, the elements of a modern SOC. Your marching orders have been set for a quest toward cutting-edge security operations. In the face of everything we've discussed, this strategy is not optional, but mandatory. If you're looking for help in achieving a modern SOC, visit siemplify.co.

Siemplify

About Siemplify

Siemplify is a security orchestration, automation and response (SOAR) provider that is redefining security operations for enterprises and MSSPs worldwide. Its holistic security operations platform is a simple, centralized workbench that enables security teams to better investigate, analyze, and remediate threats. And, using automated, repeatable processes and enhanced measurement of KPIs, Siemplify empowers SOC teams to create a culture of continuous improvement. Siemplify's patented context-driven approach reduces caseload and complexity for security analysts, resulting in greater efficiency and faster response times. Founded by Israeli Defense Forces security operations experts with extensive experience running and training numerous SOCs worldwide, Siemplify is headquartered in New York with offices in Tel Aviv.

siemplify.co