



Enterprise Strategy Group | Getting to the bigger truth.™

**ESG WHITE PAPER**

# The SOC Modernization Journey

By Jon Oltsik, ESG Senior Principal Analyst and Fellow

February 2022

This ESG White Paper was commissioned by Google and is distributed under license from TechTarget, Inc.

---

## Contents

Executive Summary .....	3
Same Old Security Operations Story .....	3
It Sure Seems Like Time for SOC Modernization .....	5
SOC Modernization and the Role of XDR .....	7
The SOC Modernization Journey .....	9
SOC Modernization and the Organization .....	9
SOC Modernization and Processes .....	11
SOC Modernization and Technology .....	11
The Bigger Truth .....	12

## Executive Summary

Famed physicist Albert Einstein is quoted as saying, “The definition of insanity is doing the same thing over and over again and expecting different results” (note: There’s no evidence that he said this, but bear with me). Whether Einstein said this or not, the adage holds true regarding security operations. Sadly, too many security operations center (SOC) managers bang their proverbial heads against the wall as cyber-risk increases and it takes ever longer to detect and respond to cyber-threats.

Why is this the case and can anything be done to rectify this unacceptable situation? This white paper concludes:

- **Chronic security operations challenges make improvement nearly impossible.** SOCs grew organically over the past 15 years as organizations added tools for security monitoring and detection of the latest threat du jour (i.e., malware, web threats, DDoS, command-and-control [C2] traffic, etc.). Unfortunately, this haphazard growth led to the deployment of an army of disconnected point tools, each needing its own care and feeding. If that wasn’t bad enough, many SOCs still depend on time-consuming manual processes that can’t scale to keep up with the growing hybrid IT infrastructure or an increase in pernicious threats. Finally, SOCs require specialized skills that can be difficult to find—especially considering the global cybersecurity skills shortage. There’s a cumulative effect here: Overwhelmed SOC personnel operate in perpetual firefighting mode when their jobs require working through security technology silos using manual processes. What a mess!
- **SOCs need a transformation, not an adjustment.** CISOs have spent the last 10 years trying to fine-tune their way out of their security operations woes, hiring an analyst here or adding some new tool there, largely to no avail. To truly address historic SOC limitations, it’s time for a concerted effort toward SOC modernization. SOC modernization encompasses people, process, and technology, adding scale, intelligence, integration, and automation to existing security technologies. SOC modernization is also intended to break down silos (within and outside of the security department) while aligning security with business goals like risk management and business operations resilience. Want more details? Read on.
- **SOC modernization is a journey, not a destination.** As the old saying goes, “A goal without a plan is a dream.” Accordingly, CISOs need a plan for SOC modernization that starts with an honest assessment of their current performance to establish a baseline of where they are compared to where they need to go. They’ll need to present a situational analysis to executives, along with a list of SOC goals and objectives that align with the business to get buy-in and resources. CISOs should then create a multi-phased SOC modernization plan (comprising people, process, and technology), complete with the right metrics to measure progress for continuous improvement. While SOC modernization is a new initiative, it shouldn’t start with a tabula rasa. Rather, the goal should be consolidating, integrating, and optimizing existing investments to start, with technology transitions built in as SOC modernization progresses.

## Same Old Security Operations Story

According to ESG research, 48% of organizations reported having a security operations center, 19% had a project underway to build and staff a SOC, 16% planned on building/staffing a SOC within the next 24 months, and 7% were interested in building/staffing a SOC sometime in the future.<sup>1</sup> Organizations create SOCs to centralize all activities related to monitoring

<sup>1</sup> Source: ESG Survey Results, [Cloud-scale Security Analytics Survey](#), December 2019.

security; improving security readiness; and preventing, detecting, and responding to threats that could impact business operations.

This sure seems like an important function, so you'd think that SOC's would run like a Swiss clock. After all, organizations have been dealing with cyber-threats since they first connected their networks to the internet—before we even coined the term cybersecurity. Regrettably, this logical assumption is dead wrong. While organizations continue to suffer from a cornucopia of disparate issues, nearly every SOC manager admits to 3 common challenges:

1. **Too many security operations tools.** SOC analysts are often forced to be jacks of all trades (and masters of none), as ESG research indicates that 35% of organizations use 26 to 50 commercial, open source, or custom technologies for security operations.<sup>2</sup> Since many of these tools operate independently, it is difficult, if not impossible, to get a complete picture of the security status, adding unnecessary friction to accomplishing any security operations objective. SOC analysts often complain about “swivel chair” management where analysts are forced to learn multiple technologies as they pivot from tool to tool to get anything done. Alas, security operations technology is often more akin to a Rube Goldberg machine than a fine time piece.
2. **Too many manual processes.** As if security tools' sprawl wasn't bad enough, security operations also tend to be based on manual processes, tribal knowledge, and individual “heroes,” rather than formal, documented runbooks and workflows across security, risk management, and IT operations teams. This adds operational complexity and overhead to security operations and can't scale to meet growing requirements (i.e., attack surface growth, alert growth, increasing threats, etc.). Organizations in this situation can be in real trouble when Tier-2 analysts and experienced threat hunters who've anchored security operations with their personal knowledge and skills pursue lucrative offers and leave the organization for “greener” pastures. Alarmingly, this can lead to a situation where no one really knows what to do.
3. **A lack of security staff and skills.** Research from ESG and ISSA indicates that 57% of organizations claim they are impacted by the global security skills shortage, and 44% believe the skills shortage has gotten worse over the past few years!<sup>3</sup> Just what are the ramifications of the skills shortage? An increasing workload on existing staff, unfilled job requisitions, high “burn out” rates, and many more (see Figure 1). Organizations should be especially concerned that 26% of respondents say that the skills shortage has led to a situation where cybersecurity staff has limited time to work with business units (isn't that what security teams are supposed to do?).<sup>4</sup> It's simply impossible to hire and grow the security staff in synch with threats and asset growth.

It's worth noting that these challenges have a “Murphy's Law” effect in combination. SOC's with too many tools struggle to manage them with manual processes and a staff and skills shortage. As if that weren't bad enough, ALL these issues are exacerbated by increasing threats and a continuously growing attack surface. Yikes!

---

<sup>2</sup> Ibid.

<sup>3</sup> Source: ESG Research Report, [The Life and Times of Cybersecurity Professionals 2021](#), July 2021.

<sup>4</sup> Ibid.

**Figure 1. Top Six Ramifications of the Cybersecurity Skills Shortage**

You indicated that the organization you work for has been impacted by the global cybersecurity skills shortage. What type of impact has the global cybersecurity skills shortage had on your organization? (Percent of respondents, N=282, check all that apply)



Source: ESG, a division of TechTarget, Inc.

## It Sure Seems Like Time for SOC Modernization

CISOs must face facts—there’s a “perfect storm” approaching their security operations centers, and tactical tinkering with point tools and manual processes won’t help them batten down their SOC hatches. This should be especially concerning given the plethora of technology initiatives in play at many organizations like digital transformation projects, remote employee support, third-party IT connections, and so on. All these efforts require risk modeling, security oversight, rapid threat detection, and finely tuned incident response processes.

Note to CISOs: It’s time to address all these challenges directly through a SOC modernization program, including:

- **Massive scale and flexibility.** Modern SOC’s will require terabyte to petabyte scale for the collection, processing, and analysis of a growing assortment of data sources and formats. Since most organizations don’t have unlimited budgets for equipment and staff, SOC scale depends upon moving technologies to the cloud and using cloud-native infrastructure and tooling. Beyond scale and operations alone, a cloud-based SOC can help security teams accommodate new applications and technology initiatives—like digital transformation—demanding security oversight for risk management and threat detection.
- **A fusion center combining security analysis, threat research/hunting, and incident response.** There are way too many silos in today’s SOC’s, leading to communication gaps and inefficient collaboration. By combining these functions in a fusion center, organizations can drive greater cooperation and collaboration, while consolidating workflows between threat prevention, detection, and response. This effort goes beyond security “world peace,”—improved collaboration, coordination, and workflows should act as the foundation for enhancing protection of critical business assets. Heck,

this could also encourage the formation of “purple teams” where security personnel join forces to gain greater understanding of the enemy, hunt for active threats, and reinforce their defenses. Before pursuing a fusion center, CISOs should assess current threat detection and response metrics, identify bottlenecks, build programs for continuous improvement, and measure the results.

- **Greater visibility across all data types and hybrid IT.** You’ve heard it a million times: “You can’t manage what you can’t measure.” As tired as that adage is, it’s a security certainty—SOC teams need visibility across everything—endpoints, IoT devices, networks, cloud workloads, applications, and data. Oh, and visibility alone isn’t enough. To understand when the organization is under attack, SOC teams need to structure and contextualize security monitoring across a cyber kill chain or by using models like the MITRE ATT&CK framework. This will help them view individual security events/alerts in the context of the tactics, techniques, and procedures (TTPs) used by cyber-adversaries. Additionally, it will be extremely helpful if comprehensive visibility includes a common security operations workspace to alleviate the “swivel chair” management described above. Aside from radically improving security operations, greater visibility and a common SOC workspace should also help assuage issues around SOC analyst burnout and staff attrition. CISOs will welcome this with open arms.
- **Increased intelligence for threat detection, risk scoring, and prioritization.** Okay, there’s a few buzz words here and no one is suggesting that machines will save or take over the security world. Rather, advanced intelligence using AI/ML, detections-as-code methodologies, and more intelligent threat-sharing methodologies should be viewed as “analyst-assist” technologies. Think driver-assist systems like automatic braking systems and smart parking rather than fully autonomous cars. In other words, advanced analytics provide a service, helping SOC teams become more effective, efficient, and productive.
- **Way, way more process automation.** Security operations encompasses complex processes across multiple individuals and groups as well as mundane tasks like looking up IP addresses, checking suspicious file hashes with VirusTotal, and blocking suspicious URLs. The goal with SOC modernization is to automate as much of this work as possible. As a historical analogy, think about the introduction of the assembly line at Ford Motor Company in 1913. This operations improvement reduced the time it took to build a single car from more than 12 hours to 1 hour and 33 minutes. Similarly, automating humdrum tasks and multi-phased processes could lead to substantial increases in threat detection efficacy, IR response times, and analyst productivity.
- **Smarter integrated risk management.** When analysts conduct investigations, they want to know everything about an asset exhibiting suspicious behavior—its configuration, owner, location, business value, what it’s connected to, and so on. Unfortunately, gathering this information (if it’s available at all) can be a wild goose chase. Why? Organizations often have little understanding of what assets are on the attack surface, data is inaccurate and spread across lots of tools, systems of record are often owned by IT (not security), etc. SOC modernization seeks to alleviate this visibility gap with a more integrated approach to asset inventory using API connections to collect, process, normalize, and analyze asset data. This more accurate data will then be consolidated and accessible to analysts as part of their sleuthing.
- **Change the SOC workforce model.** Today’s SOCs are regimented, with multiple tiers of analysts with varying skills and competencies. It’s hard to hire, train, and onboard Tier-1 (junior) analysts, while SOC workloads and pace lead to burn out and high attrition rates. Meanwhile, there aren’t enough more senior SOC analyst wizards to go around. Using advanced analytics, automation, and some help from friendly neighborhood managed service providers, SOC modernization seeks to re-engineer the entire personnel structure. In this model, alert triage is mostly automated, freeing junior analysts to get more involved in investigations, threat hunting, or other SOC specialty skills. Analyst

actions will be constantly monitored and evaluated for highly efficient analyst methodologies and dead-end processes that lead back to square one. Senior analysts will then split their time between security operations and automation engineering for continuous improvement.

While improving security efficacy and efficiency is critical, SOC modernization is ultimately intended to provide appropriate security oversight over rapidly changing business processes. For example, many healthcare organizations are undertaking digital transformation projects to extend care with virtual doctor appointments, analytics systems for triage and diagnosis, and continuous patient monitoring. While these initiatives can improve the end-to-end healthcare service-delivery chain from diagnosis to post-care and improve the relationship between patients and caregivers, they also expand the attack surface while collecting, processing, and analyzing private patient data. SOC modernization is intended to provide the right scale, intelligence, processes, and personnel model, enabling organizations to move forward with initiatives like these with the proper levels of visibility, oversight, risk management, and threat detection/response on the backend.

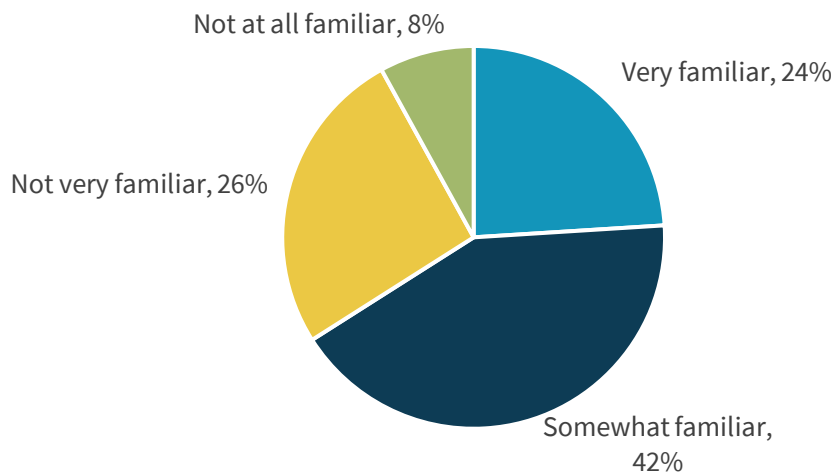
### SOC Modernization and the Role of XDR

SOC modernization won't depend upon your father's security operations technologies but rather innovative cloud-based solutions driven by outcomes and common use cases. Now, there's been a lot of buzz in the industry about eXtended detection and response (XDR) technology over the past few years, so it's worth asking what, if any, role will XDR play in SOC modernization?

Before addressing this, there's a more fundamental question in play: Just what is XDR? Given all the hyperbole around this topic, you'd think the answer would be clear, but ESG research proves otherwise—only 24% of security professionals claim to be very familiar with the XDR concept, and even this group probably can't agree on a common XDR definition (see Figure 2).<sup>5</sup>

**Figure 2. Security Professionals Remain Confused about XDR**

**There is a relatively new security technology concept called extended detection and response (XDR). How familiar are you with this concept? (Percent of respondents, N=138)**



Source: ESG, a division of TechTarget, Inc.

<sup>5</sup> Source: ESG Survey Results, [The Impact of XDR in the Modern SOC](#), February 2021.

The XDR question often leads to passionate industry debate, but as a point of clarity, ESG defines XDR as follows:

*An integrated security architecture spanning hybrid IT architectures, designed to interoperate and coordinate on threat prevention, detection, and response. XDR unifies control points, security telemetry, analytics, and operations into one enterprise system.*

So, what will XDR do for SOC modernization? Since XDR products are relatively immature, the answer to this question is still in flux, but ESG believes that XDR could:

- **Act as an aggregation layer for security controls telemetry.** XDR varies from vendor to vendor. Some include email security telemetry, others don't. Some are based around endpoint detection and response (EDR) solutions, some aren't. Some gain cloud workload visibility through agent deployment while others depend upon telemetry from cloud service provider (CSP) APIs and services. Some are open to third-party data sources while others are designed as black box proprietary solutions. Regardless of their composition, XDR solutions provide a common storage/data service for disparate telemetry feeds. Vendors then normalize this data, use the data to create correlation rules, and write analytics for threat detection. In some cases, vendors provide access to this data for users to build their own custom detection rules.
- **Reduce the volume of noisy alerts.** SOCs today regularly receive thousands of security events/alerts from an assortment of threat detection tools deployed on endpoints, networks, in the cloud, and so on. Typically, tier-1 analysts with "eyes on glass" are asked to triage this cacophony of alerts, figure out which are truly relevant, and then escalate incidents up the chain for investigations. Tier-2 analysts then act as detectives, piecing together all distinct alerts in pursuit of kill chains of real cyber-attacks in progress. XDR promises a better mousetrap, with detection rules that aggregate individual alerts into cohesive threat-centric timelines of what happened when and how the puzzle pieces fit together. XDR solutions use models like the MITRE ATT&CK framework to map alerts into TTPs and adversary campaigns.
- **Provide basic response actions.** XDR solutions tend to be built around security controls themselves (i.e., endpoint security software, IDS/IPS, firewalls, CASB, email security, etc.). Depending upon the vendor portfolio or cross-vendor interoperability, this integration provides the opportunity for closed-loop incident response actions without the need for full security orchestration, automation, and response (SOAR) tools or direct collaboration with IT operations (although IT operations cooperation is ultimately required for strong cybersecurity across an organization). When a PC downloads a malicious file, XDR can deny network access and then repair the system. A high-risk IP address can be blocked on endpoints, network proxies, and perimeter firewalls. Suspicious end-user behavior can lead to decommissioning an account, escalating an investigation, and alerting HR. These IR actions could stop or at least delay an attack in progress more competently than today's manual process slog. While these basic response actions are better than nothing, enterprises will still need a fully functional SOAR platform for a more comprehensive IR strategy.

Of course, the points made above must be presented with an asterisk. XDR solutions are in their genesis phase, so many of these benefits remain hypothetical. It's also worth noting that leading SOCs don't necessarily need XDR to attain these results. They already use things like stream processing, message queuing, active detection rule creation/tuning, and workflow automation to attain similar outcomes, while a trained and organized SOC team can gain better results with a cloud-based SIEM and SOAR platform focused on outcomes and use cases (as opposed to log management and basic detection correlation rules).



All in all, the role of XDR in SOC modernization is murky at best. It will likely provide the benefits described above over time—especially to smaller organizations or those with limited security operations staff and skill sets. The crystal ball isn't as clear for large enterprises, however. These organizations may add XDR as a consolidation layer or simply build consolidation and integration abstraction layers on top of existing tools, adding their own detection rules, analytics, and automation.

## The SOC Modernization Journey

The deafening noise around XDR represents a constant and fundamental cybersecurity issue. The cybersecurity diaspora often looks toward new security technologies as the final piece of the puzzle, tilting the cyber battlefield in its favor. So, while XDR is lauded as the “next big thing” in cybersecurity, it is preceded by a long list of other final solutions like user and entity behavior analytics (UEBA), endpoint detection and response (EDR), and network detection and response (NDR) systems. Indeed, many standard security operations technologies were once touted as cybersecurity nirvana.

Famed cybersecurity author Bruce Schneier is quoted as saying that “security is a process, not a product.” CISOs should take this message to heart when contemplating SOC modernization. Indeed, SOC modernization must be built around people, process, and technology—not technology alone.

## SOC Modernization and the Organization

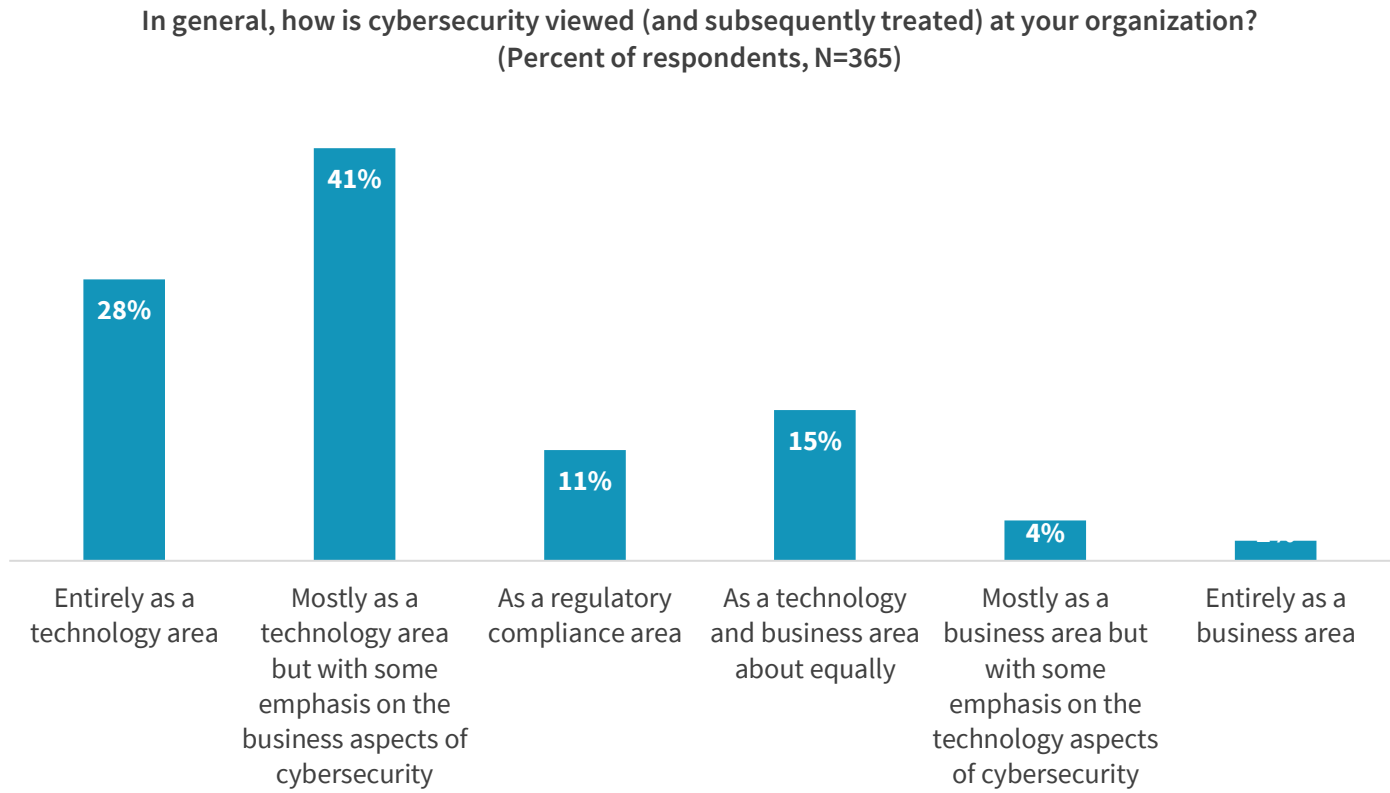
SOC modernization must be viewed by all constituents as a strategic initiative intended to align proper security oversight with 21<sup>st</sup> century business and technology initiatives. Anything less should be unacceptable. Achieving this goal will require a mindset change toward personnel and the business, including:

- **An understanding that cybersecurity is a business priority.** This may seem blatantly obvious, but ESG research reveals a sad truth—28% of business and technology professionals still view cybersecurity entirely as a technology issue, while 41% say it is mostly a technology area but with some emphasis on business aspects (see Figure 3).<sup>6</sup> SOC modernization will fail without changes to these beliefs. To address these historical biases, CISOs must educate executives and corporate boards about SOC modernization. Technical details? Heavens no! Rather, the measurable benefits in terms of cyber-risk management and business enablement. CISOs should come prepared with a list of business metrics possible through SOC modernization (i.e., greater uptime, accelerated MTTD/MTTR, improved ROI on security spending, etc.) and be ready to provide a baseline for current performance and track improvement over time.

---

<sup>6</sup> Source: ESG Research Report, [Cybersecurity in the C-Suite and Boardroom](#), February 2021.

**Figure 3. Cybersecurity Is Still Perceived as a Technology Domain**



Source: ESG, a division of TechTarget, Inc.

- A commitment to training and skills development.** When asked how difficult it is to recruit and hire cybersecurity professionals at their organization, 18% of the information systems security association (ISSA) members said it was extremely difficult, while another 54% reported that it was somewhat difficult.<sup>7</sup> It’s safe to conclude then that CISOs can’t hire their way out of the current skills shortage conundrum. Even those fortunate organizations that can add bodies still can’t do so at a pace that keeps up with business demands and persistent cyber-threats. Given this situation, what’s a CISO to do? First, SOC operations need to “shift left” by instrumenting and automating security into IT processes (i.e., planning, application development, deployment, etc.). The goal? Build security collaboration and transparency throughout IT lifecycles. Second, CISOs must be willing to cast a wider net for SOC personnel recruitment, getting out of their comfort zone of only hiring those with a technology background. This also means a greater commitment to training and mentoring programs, which should be managed for continuous improvement. Finally, SOC managers must be realistic about what they can and cannot do on their own and fill gaps with qualified service providers. To get the most out of these relationships, CISOs must develop and improve third-party management skills as well.

Finally, organizations must be willing to move from today’s stratified SOC personnel tiers to a more collaborative model that aligns skills to use cases. Achieving this model depends upon intelligent and thorough process automation.

<sup>7</sup> Source: ESG Research Report, [The Life and Times of Cybersecurity Professionals 2021](#), July 2021.

## SOC Modernization and Processes

Regardless of the focus on recruitment and training, SOC modernization will fall flat unless there is a focus on all the processes required. Status quo solutions won't do here—CISOs must lead a cultural shift in the SOC toward:

- **Process optimization.** Beyond process automation, organizations should start by fully understanding existing processes. Who is involved? Where are the handoffs? How are processes tracked? Where are the bottlenecks? Is there any analysis and efforts toward continuous improvement? Once processes are understood, CISOs should look toward best practices, see how existing methodologies compare, and then build a plan toward their goals. Start with small improvements, like automating pedestrian tasks, and proceed forward from there. Make sure to develop metrics for improvement.
- **Continuous process engineering.** As part of this transition, organizations must develop expertise in process engineering, and experienced SOC personnel should lead the way. For example, current Tier-2 and -3 analysts could be tasked with creating and managing a site reliability engineering (SRE)-style team that divides its security operations time equally between security operations and process automation development. This model demands knowledge and specialization. For example, detection engineers should be tasked with detection rules development re-engineering at scale and be given the freedom and resources to be creative in their approach. Similarly, incident responders need to have buy-in from IT operations to automate and orchestrate remediation actions that eschew cumbersome change management processes while satisfying the requirement for auditing and regulatory compliance.

As part of this transition, SOC personnel must be on the lookout for any process that can be automated. A few minutes of time on some trivial process may not seem like much, but when SOC repeats this process dozens of times per day, time savings add up quickly and have the potential to bolster productivity significantly.

## SOC Modernization and Technology

Yes, SOC modernization requires technology changes as they relate to overall objectives and desired outcomes—not products, services, or some esoteric bucket defined by an analyst. From a technology perspective, SOC modernization should include:

- **A plan for massive scale.** As previously described, SOC modernization should be built to accommodate massive storage and processing needs. While these obviously point to the public cloud, SOC technologies should be cloud native and designed for the SOC team's unique workflows and data analysis needs. For example, security telemetry needs are always growing, encompassing sources like EDR, cloud logs, authentication systems, and threat intelligence. SOC modernization scale must be able to collect, process, analyze, and act upon this heterogeneous data with aplomb.
- **A focus on architecture and integration.** Organizations have invested oodles of money in security technologies over the past 10 years, so they shouldn't have to throw their babies out with the bathwater for SOC modernization. Rather than "rip and replace," SOC modernization should be built around technology architectures (like ESG's security operations and analytics platform architecture) optimized for scale and integration. The goal? Consolidate and optimize existing security controls with greater interoperability and orchestration. For example, a modern SOC platform should be able to ingest and normalize disparate data types at scale for efficient data analysis and query. The demand for integration will drive the security technology industry toward more open standards, vendor cooperation, and SOC platforms.

- **A commitment to better detection engineering.** While detection improvement is a game of inches, security professionals should monitor a few developments. For example, the creation of standard detection rule creation using technologies like Yara, Yara-L, Sigma, and Kestrel should produce more efficient rules development and sharing. ESG also expects improvements in advanced analytics using AI and ML. The best systems will employ “nested algorithms,” which work together to improve alert accuracy correlated across a kill chain.

## The Bigger Truth

In ancient times when SOC's were first created, they were really built so that security personnel had visibility and a central location to monitor perimeter security devices like firewalls, proxies, and IDS/IPS. Events flowed into log management and SIEMs so security analysts could make some sense of network security chaos. Fast forward to today, and SOC's have a much bigger role. Since technology is used as the foundation for most business processes, SOC's are essential to keep all the business trains running on time. Therefore, when SOC's fail, businesses fail.

It's time for business leaders, CIOs, and CISOs to recognize the business-critical SOC role and invest accordingly. Based on the challenges described above, tactical changes just aren't enough; it's time for a full-fledged effort toward SOC modernization that protects and supports the business. Easy to write but hard to do! This paper provides a few guidelines and suggestions, but it is only a starting point. Moving forward:

- **Business executives must be convinced to get on board with commitments and investments.** CISOs will need to act as educator and cheerleader here. The key will be convincing executives that SOC modernization will help mitigate cyber-risk, while protecting and enabling the business.
- **CISOs must develop a plan.** Starting with an assessment, CISOs must provide a baseline for the people, process, and technology aspects of current SOC's and then build a detailed, multi-phased plan for continuous improvement.
- **Security professionals must get on board.** Everyone loves lone wolf cybersecurity magicians who have the skills and technique to outsmart cyber-adversaries, but these folks don't scale, and there aren't enough of them to go around. SOC modernization is an opportunity to systematize this type of knowledge. Those analysts blessed with these skills must be incented to become teachers, coaches, and process engineers.

All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.'s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.


This publication is copyrighted by TechTarget, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at [cr@esg-global.com](mailto:cr@esg-global.com).



**Enterprise Strategy Group** is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community.

 [www.esg-global.com](http://www.esg-global.com)

 [contact@esg-global.com](mailto:contact@esg-global.com)

 508.482.0188