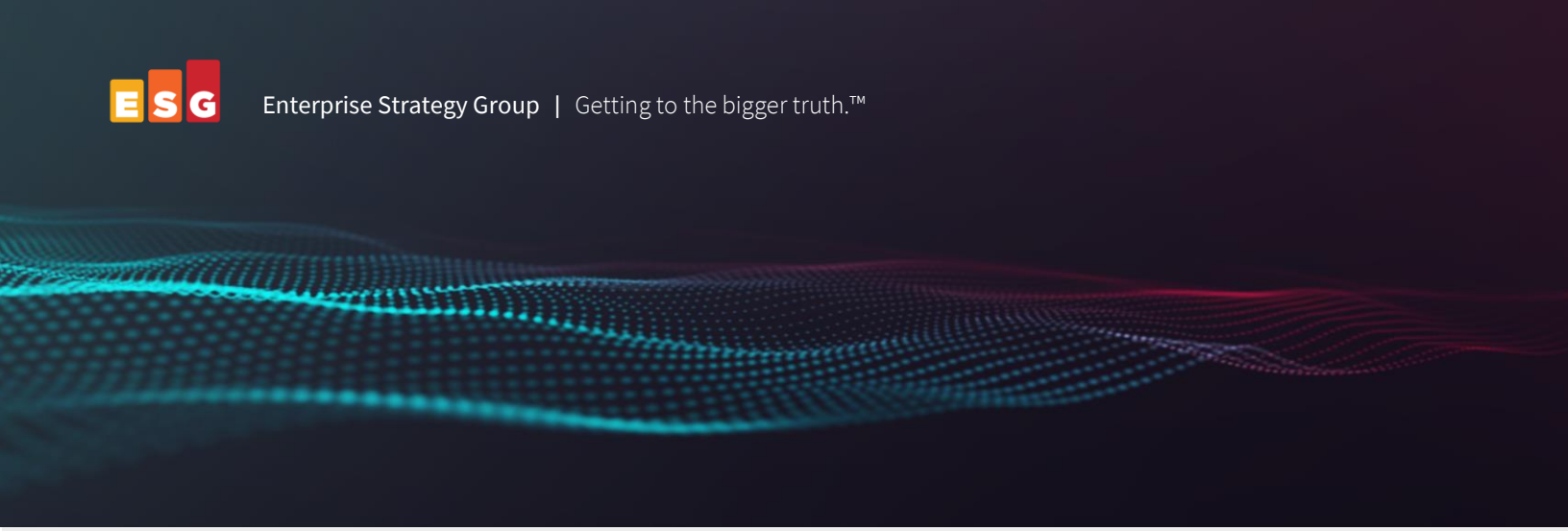


ESG WHITE PAPER

SIEM and NDR: Better Together

Integrating SIEM and Network Detection and Response into a Common SOAPA/XDR Architecture

By Jon Oltsik, ESG Senior Principal Analyst and Fellow

February 2021

This ESG White Paper was commissioned by IBM and is distributed under license from ESG.

Contents

Executive Summary

Security operations grows more difficult on an annual basis as cyber-adversaries collaborate and improve their attacks to circumvent security controls and analytics systems. Meanwhile, the attack surface keeps expanding as CIOs move workloads to public clouds while business managers embrace SaaS applications and new types of devices for digital transformation. Somehow, the security operations center (SOC) team is responsible for monitoring all these systems and network connections to prevent, detect, investigate and respond to security incidents.

Unfortunately, many organizations simply can't keep up with the growing scale and scope of security operations, increasing cyber-risk and the potential for a devastating cyber-attack or data breach. Why have things gotten so difficult and what can be done to address this situation? This report concludes:

- Security operations is fraught with many challenges. Many security operations centers were built using disconnected point tools and manual processes. This design may have worked in the past, but it is no match for today's environment, which requires speed and efficiency. As a result, security teams are buried by security alerts and spend much of their time dealing with one emergency or another.

- Organizations are modernizing their SOCs. The term "SOC modernization" has gained popularity within the cybersecurity professional community. SOC modernization includes things like technology integration, process automation, advanced analytics, and threat intelligence contextualization and enrichment within all other security operations technologies. The goal? Create an interoperable security operations and analytics platform architecture (SOAPA) that can help the SOC team bolster security efficacy and operational efficiency.

- SIEM systems should be integrated with NDR. SIEMs anchor their analytics to event and log data while NDR monitors network flows, packets, and metadata. Many organizations use both systems independently when they really have a common purpose—timely and accurate threat detection and incident response. By combining these two systems, organizations can benefit from higher fidelity, detailed, and actionable alerts. This can lead to improvements in mean-time-to-detect (MTTD) and mean-time-to-respond (MTTR) to threats.

The State of Cybersecurity Operations

According to ESG research, 63% of organizations claim that security analytics and operations is more difficult than 2 years ago. Why? Because SOC teams face numerous security operations challenges such as:[1]

- Monitoring security across a growing attack surface. Driven by digital transformation and work-from-home (WFH) initiatives, organizations have embraced and extended their IT infrastructure, adopting SaaS applications, moving workloads to the public cloud, developing cloud-native applications, and deploying IoT/OT devices. IT expansion creates a security operations challenge, however, as the SOC team is responsible for knowing which devices are connected to the network, the status of each node, normal/anomalous behavior, etc. Unfortunately, many organizations don't have the right monitoring tools or security skills to keep up with securing the growing attack surface.

- Keeping up with the volume of security alerts. According to ESG research, 35% of organizations employ 25 or more different security technologies to support security operations. Each of these tools can generate hundreds of alerts daily, so when combined, security operations tools can easily produce up to thousands per day. Security operations

[1] Source: ESG Research Report, *The rise of cloud-based security analytics and operations technologies*, December 2019. All ESG research references and charts have been taken from this research report, unless otherwise noted.

best practices suggest that each of these alerts should be triaged, prioritized, and investigated, but most organizations lack the bandwidth to accomplish this. As such, it's not unusual for SOC teams to ignore most security alerts regularly because they simply can't keep up.

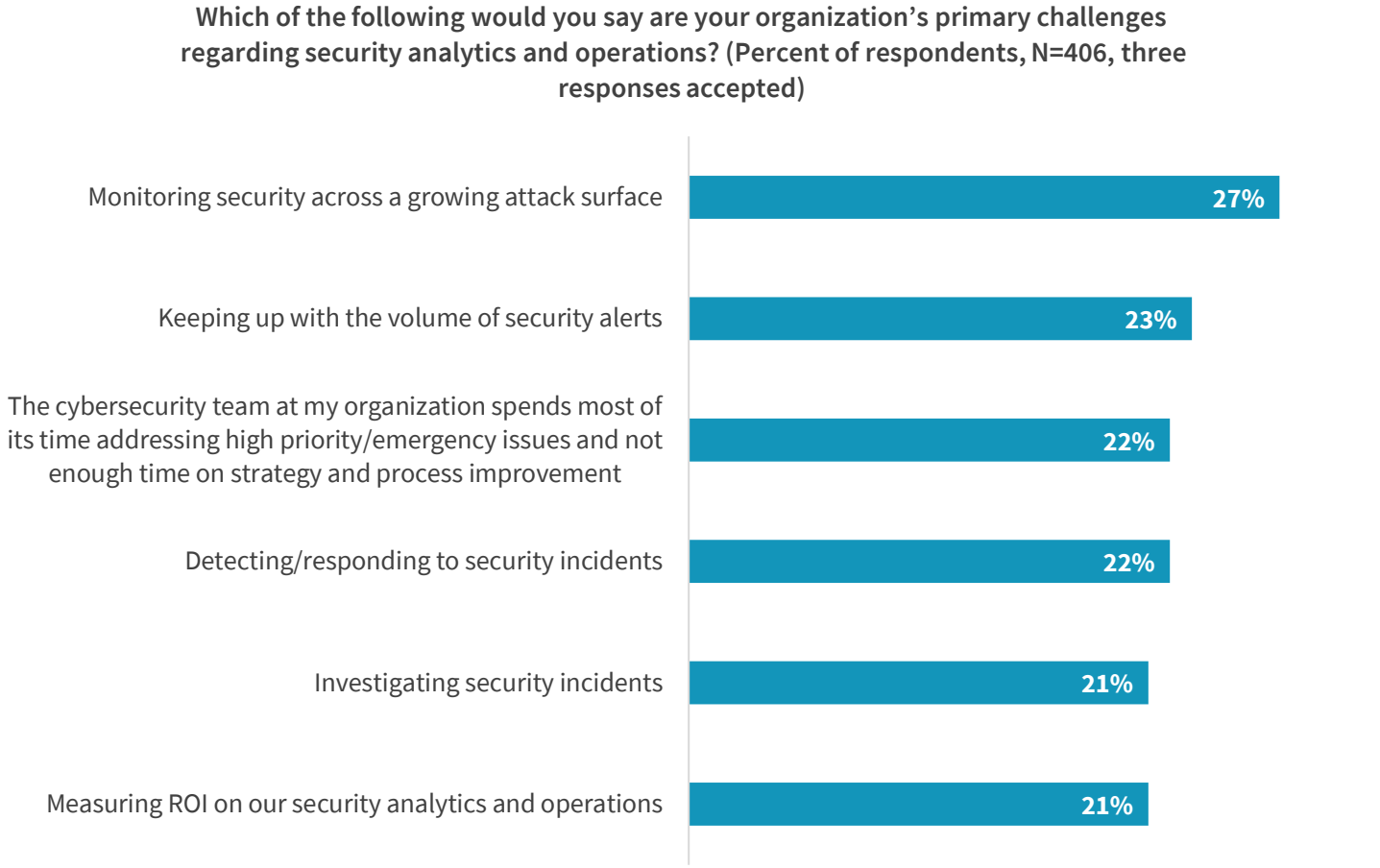
- Dealing with security emergencies. Recent research from ESG and the information systems security association (ISSA) indicates that 70% of organizations say they've been impacted by the global cybersecurity skills shortage.[2] This means that many SOCs remain under-staffed and/or lacking the right skills for security operations. This skills shortage may contribute to the 22% of organizations claiming that their security teams spend most of their time addressing emergency issues and not enough time on security strategy or process improvement. This constant firefighting is not only inefficient, it is also a primary contributing factor to staff burnout and high attrition rates.

Cybersecurity professionals also admit that the threat landscape is evolving rapidly, keeping security operations quite challenging. This is especially true as a result of recent nation state attack on infrastructure software providers. SOC teams must not only understand the threat landscape, but also how their IT infrastructure could expose business-critical assets to compromise and data theft. This requires advanced knowledge around threat intelligence; adversary tactics, techniques, and procedures (TTPs); and the attack surface.

The situation described here is unsustainable. In an environment of advanced cyber-threats and an expanding attack surface, SOCs lack the scale, skills, staff, or right technologies to keep up. CISOs must address these deficiencies as soon as possible or their organizations face increasing cyber-risks to the business along with a future of cyber-attacks, data breaches, and business operations disruptions.

[2] Source: ESG/ISSA Research Report, *The Life and Times of Cybersecurity Professionals 2020*, July 2020.

Figure 1. Top Six Security Operations Challenges



Source: Enterprise Strategy Group

SOC Modernization

Enterprise CISOs recognize that their security operations are falling behind and are addressing this growing gap by implementing a technology foundation for SOC modernization. This effort includes:

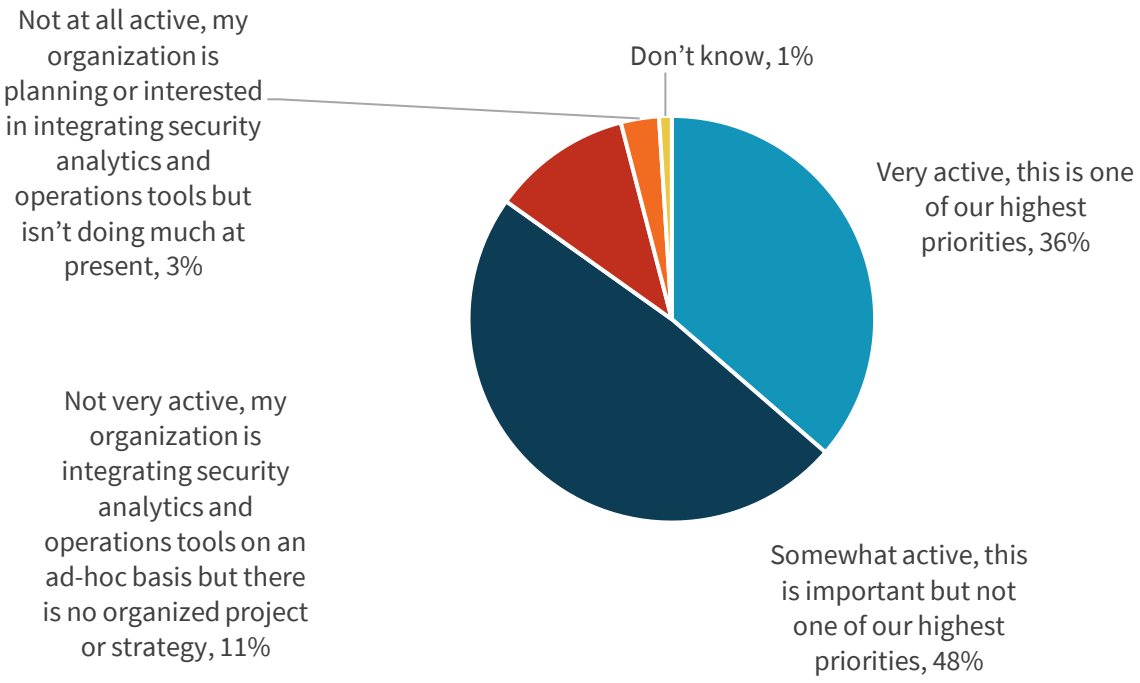
- Creating a security operations and analytics platform architecture (SOAPA). A lot of the overhead associated with security operations is directly related to the SOC team's reliance on dozens of disconnected point tools. Each tool needs to be configured, deployed, and operated, while the SOC team pieces together enterprise security status on a tool-by-tool basis. To address this inefficient model, CISOs are pushing their teams to merge tools into an interoperable SOC technology architecture (SOAPA). According to ESG research, 36% of organizations consider SOAPA development critical and a high priority, while another 48% consider SOAPA development an important initiative (see Figure 2).

- Automating processes. Many SOCs are automating processes in several ways. First, they are automating pedestrian tasks, like matching a user identity with an IP address, that are performed multiple times per day. This alone can help SOC teams bolster productivity and throughput. Beyond this, leading SOCs are automating processes for more advanced use cases like threat hunting investigations or SSL certificate management. This not only helps to scale the SOC staff but also allows analysts to move beyond firefighting and adopt a more proactive security strategy.

- Implementing advanced security analytics. To address the volume of security alerts, SOC managers are employing new types of analytics solutions that can process and analyze massive amounts of data in real time. The goal? Reduce the noise in the system while producing high-fidelity, detailed, and actionable alerts. This can also help SOC teams reduce today's chaos by focusing the right resources on high-priority business-critical security tasks.
- Injecting threat intelligence into everything. When suspicious behavior triggers an alert, security analysts need to know whether it's a random event or tied to known cyber-adversary tactics, techniques, and procedures (TTPs). This means that SOC teams need to process and analyze threat intelligence at scale, enrich security alerts with threat intelligence details, and integrate threat intelligence with security controls to immediately block malicious domains, files, IP addresses, emails, etc. Operationalizing threat intelligence in this way acts as a backbone for a modern SOC.
- Establishing a common workbench for security operations. Rather than pivot from UI to UI, modern SOCs consolidate the input from multiple tools into common dashboards, graphics, and reports that can be customized for different roles, skill sets, and needs. The best workbenches will support SOC team needs for cyber-risk management as well as across threat prevention, detection, and response.

Figure 2. Organizations are Integrating SOC Tools

How active is your organization in terms of integrating disparate security analytics and operations tools together to form a more cohesive security software architecture? (Percent of respondents, N=406)



Source: Enterprise Strategy Group

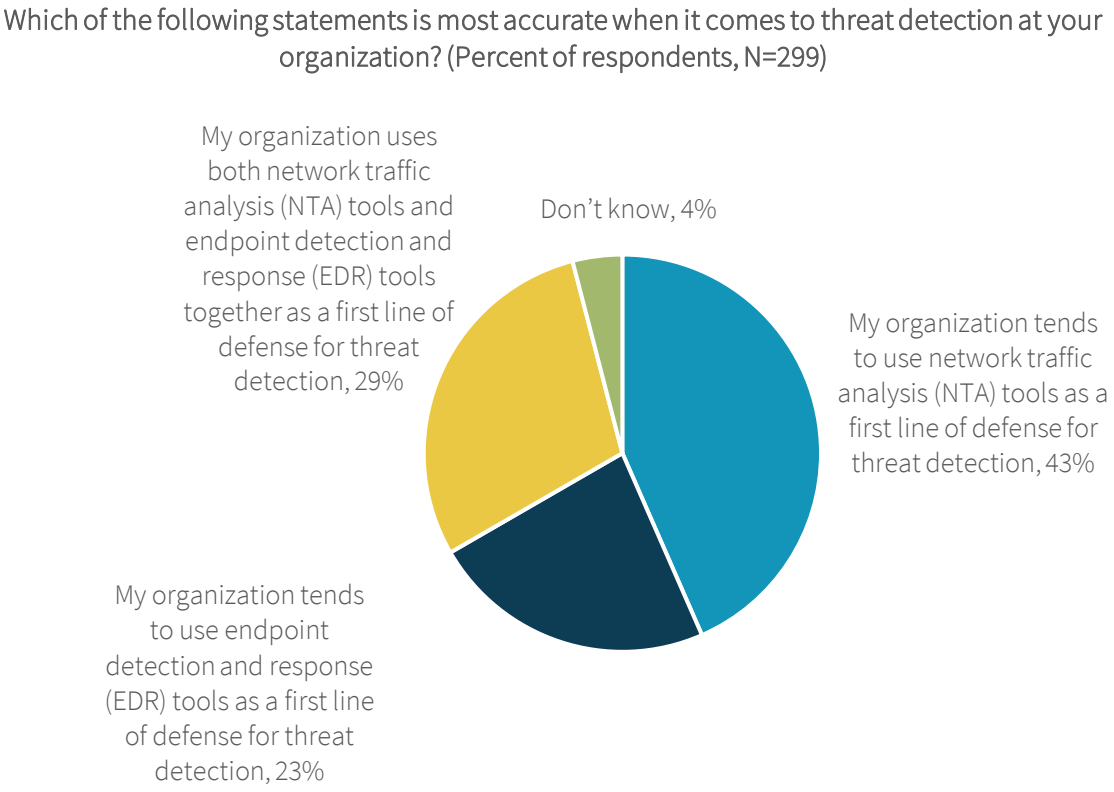
SIEM and Network Detection and Response (NDR): Better Together

Organizations are certainly modernizing their SOCs to enhance the productivity and efficiency of their security teams, but the main objective is usually something else—improve threat detection and response. To achieve these goals, many

organizations believe that SOC modernization must include a plan for integration of SIEM and network detection and response (NDR) tools.

This integration makes a lot of sense. Organizations have long benefited from SIEM for threat detection and response, using features like event correlation, custom detection rules, and behavioral analytics for anomaly detection. These detection methods are perfect for detecting anomalous/suspicious activities like multiple simultaneous logins or privileged escalation that occur on a single system. SOC teams also use NDR tools to identify anomalous/suspicious network behaviors like port scanning, lateral movement, data exfiltration, or connections to malicious IP addresses. Since most cyber-attacks include network communications, many organizations use NDR as a first line of defense for threat detection (see Figure 3).[3]

Figure 3. NTA As a First Line of Defense for Threat Detection



Source: Enterprise Strategy Group

By combining SIEM with NDR, organizations have the analytics foundation for extended detection and response (XDR), an emerging security operations technology architecture. When these two security technologies are tightly integrated, organizations can benefit from:

- Improved threat detection. When SIEM analytics, event correlation, and rule sets trigger an alert, analysts tend to pivot to NDR tools to look at associated connections or dig into the network packets themselves to look for anomalous files. When SIEM and NDR are integrated, this data can be combined into high-fidelity alerts with all log

[3] Source: ESG Master Survey Results, *The Threat Detection and Response Landscape*, April 2019.

and network data presented to analysts simultaneously. Leading systems will also include advanced analytics looking for malicious behavior across a kill chain that includes log and network data.

- Accelerated and streamlined security operations. When a SIEM or NDR system triggers an alert, security analysts begin a time-consuming series of processes, like triaging alerts, querying different systems for supporting data, and then prioritizing remediation tasks with IT operations. By combining all suspicious network- and system-level data, the combination of SIEM and NDR can help organizations streamline and accelerate security operations by presenting suspicious event, network, and log data into compact and comprehensive security alerts.

- Alignment of SIEM and NDR with other data sources and security operations services. Organizations can use the combination of SIEM and NDR integration as a stepping stone toward SOAPA. This may be more straightforward than it seems, since many leading SIEMs have already integrated other security operations services such as:

  - Threat intelligence data enrichment. Threat detection requires a comparison of internal anomalous behavior with TTPs used by cyber-adversaries as part of their attacks. By integrating SIEM and NDR with cyber-threat intelligence, organizations can enrich security alerts with threat intelligence details like malicious IoCs or related attack patterns. Threat intelligence enrichment can also help organizations align individual alerts and events to cyber-adversary intent by mapping to the MITRE ATT&CK framework.

  - Security orchestration, automation, and response (SOAR). To further improve security operations, SIEM and NDR can be integrated with SOAR systems for process automation. This can greatly accelerate MTTD/MTTR while improving security analysts' productivity.

  - Other analytics systems. SIEM and NDR analytics accuracy can be further improved by supplementing them with other systems like vulnerability management, endpoint detection and response (EDR), cognitive computing systems, or user and entity behavior analytics (UEBA).

IBM Security QRadar NDR: A Foundation for SOAPA and XDR

Many organizations have done basic integration between SIEM and NDR, making it easier for analysts to pivot back and forth between tools. This can save a step or two but only provides limited incremental value. IBM has gone well beyond this cursory integration with NDR capabilities delivered natively as part of the platform. With these capabilities, QRadar can:

- Produce high-fidelity alerts that combine event, log, and network data to better detect threats. QRadar ingests event, log, and network data from a range of sources, including Network Flows and full packet analysis from QRadar Network Insights, into common rule sets and analytics for threat detection. For example, anomalous system level activity will be correlated with network data to piece together the root cause, progression, and scope of a cyber-attack. Furthermore, event, log, and network data are enriched with threat intelligence from the IBM X-Force for further alert fidelity improvement. This can help security analysts filter out noise and prioritize critical alerts.

- Consolidate UIs and workflow to maximize analyst productivity. Rather than right-clicking a mouse to move across systems, QRadar provides visibility, dashboards, and alerts through a common UI and integrated workflow. This should help SOC analysts save time while benefiting from specialization and experience gained by using a single tool for multiple use cases.

- Integrate with other QRadar and third-party security technologies for unified visibility and response. The capabilities of QRadar can be expanded into a SOAPA/XDR architecture with the addition of other IBM technologies like QRadar

User Behavior Analytics, IBM Security SOAR , X-Force threat intelligence, vulnerability management, QRadar Advisor with Watson, etc. For example, SOC analysts can leverage IBM Security SOAR to automate repetitive tasks, collaborate across teams with case management, and guide actions with playbooks in order to accelerate incident response. Through the IBM Security AppExchange, security professionals can integrate QRadar with additional threat intelligence, security asset management systems, EDR, CASB, and others.

QRadar with its NDR capabilties can be seen as a single SOAPA/XDR architecture rather than two interoperable technologies. Adding other IBM or third-party technologies only adds to this value. CISOs looking to modernize their SOCs may want to consider IBM Security QRadar as they can provide a strong technology underpinning toward this goal of unified visibility, detection, investigation, and response. Furthermore, accessing these capabilities as part of the IBM Cloud Pak for Security platform provides an attractive option for security teams looking for an open, multi-cloud platform as the foundation of their modern SOC.

The Bigger Truth

CISOs should be extremely concerned—digital transformation applications and cloud-based data represent attractive targets for sophisticated cyber-adversaries. Alarmingly, security operations technologies and processes may not be able to keep up with these trends. This makes SOC modernization a high priority as organizations integrate technologies, adopt new types of analytics solutions, and automate SOC processes.

While there are many ways to approach SOC modernization, integrating SIEM and NDR is a great place to start as part of a broader XDR strategy. SIEM and NDR look for threats in different ways using different data. By combining the two, organizations can gain greater situational awareness, leading to more accurate and timely security alerts.

IBM has taken the integration of SIEM and NDR to another level with analytics that aggregate the data from both technologies and display them through a common interface. Furthermore, IBM supplements SIEM and NDR integration with other capabilities for SOAR, additional analytics, and threat intelligence enrichment. In this way, IBM can help customers modernize their SOCs by providing a tightly integrated scalable SOAPA/XDR architecture for better visibility and enhanced detection, investigation, and response capabilities needed by security teams to keep pace in today's environment.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.


www.esg-global.com


contact@esg-global.com


508.482.0188