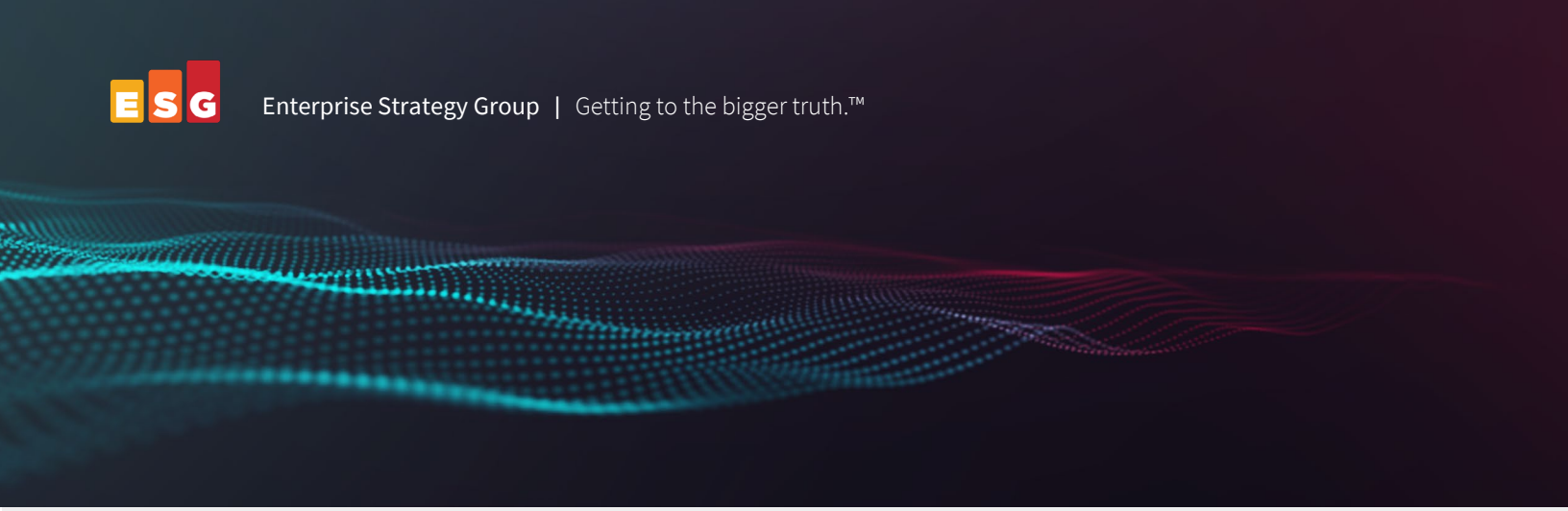


ESG WHITE PAPER

SOAPA: Unifying SIEM and SOAR with IBM Security QRadar and IBM Security Resilient

By Jon Oltsik, Senior Principal Analyst and ESG Fellow

February 2020

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

Contents

Executive Summary

Security analytics and operations can be extremely difficult. Organizations face a range of relentless and sophisticated cyber-adversaries willing to conduct long-term advanced persistent threat (APT) attacks or overwhelm companies with devastating ransomware.

Are enterprise organizations prepared for a perpetual onslaught of cyber-attacks? The answer is an alarming "no" in most cases, but fortunately there's some emerging hope. New technologies that integrate advanced analytics with security operations process management can help organizations improve security lifecycles from data collection to threat detection through incident response. This white paper concludes:

- Security analytics and operations present common challenges. Many organizations address security analytics and operations with a series of point tools, disorganized manual processes, and a cybersecurity team lacking the right size and skills. This leaves defenders scrambling and overwhelmed, shifting the balance of cyber power toward cyber-adversaries.

- Technology integration can improve security analytics and operations. ESG believes that organizations will build or buy a security operations and analytics platform architecture (SOAPA) that integrates technologies across data collection, processing, analytics, and security operations. This tightly coupled architecture adds advanced analytics (i.e., artificial intelligence [AI] and machine learning [ML]) and process automation and orchestration to improve threat prevention, detection, and response. Through technology integration, organizations can also streamline security operations processes, accelerating security activities and freeing staff to focus on high-priority security issues.

- IBM Security provides its own SOAPA solution through the integration of QRadar and Resilient. IBM Security understands the security analytics and operations challenges enterprises face and is one of few vendors that can offer an end-to-end SOAPA solution. IBM Security QRadar, a security information and event management (SIEM) platform, can provide security analytics for insight into the most critical threats. Once threats are detected, QRadar works with IBM Security Resilient, a security orchestration, automation, and response (SOAR) platform, to manage incident response while applying automation to additional security use cases such as threat hunting, vulnerability management, and security alert triaging. In this way, QRadar and Resilient act as force multipliers for one another, helping organizations improve security efficacy while streamlining and augmenting the efficiency of security operations.

The State of Security Operations

According to a recent ESG research survey, 63% of organizations believe that security analytics and operations are more difficult today than they were two years ago.[1] This increasing complexity is driven by many factors. For example (see Figure 1):

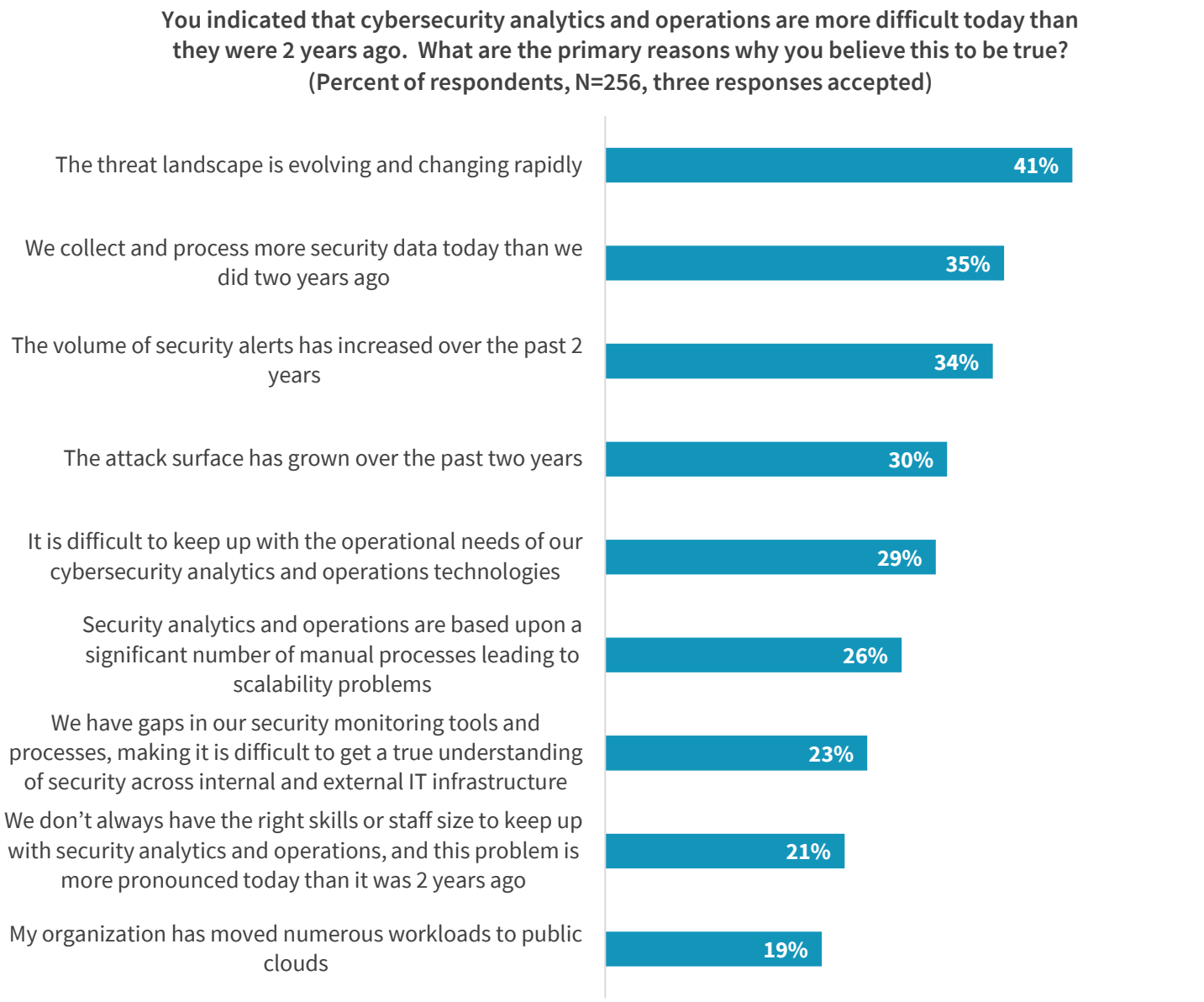
- 41% of survey respondents claim that security analytics and operations have grown more difficult because the threat landscape is evolving and changing rapidly, leading to more targeted and sophisticated attacks. Security operations staff must understand cyber-adversaries, the tactics, techniques, and procedures (TTPs) they use, and indicators of compromise (IoCs) that may indicate a cyber-attack in progress. This tends to require advanced skills most organizations don't have.

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

- 35% of survey respondents claim that security analytics and operations have grown more difficult because their organization collects more security data today than it did 2 years ago. This is related to the security data pipeline of batch and real-time data. Security teams must be able to collect, normalize, index, and process growing volumes of security telemetry for continuous monitoring and data-driven decisions. Since security professionals aren't usually skilled in data engineering and management, security data pipelines can suffer from performance and scalability problems.

- 34% of survey respondents claim that security analytics and operations have grown more difficult because the volume of security alerts has increased over the past 2 years, making it difficult to triage, investigate, and prioritize them. This is especially true for tier-1 junior analysts lacking enough security operations experience. When junior analysts default to escalating alerts, it can cause upstream process bottlenecks, leading to inefficiencies, human error, and increased risk.

Figure 1. Reasons Why Cybersecurity Analytics and Operations Have Become More Difficult



Source: Enterprise Strategy Group

- 30% of survey respondents claim that security analytics and operations have grown more difficult because the attack surface has grown over the past few years. This is due to the preponderance of digital transformation applications, IoT device proliferation, user mobility, and public cloud computing. Security personnel can't alter the growing attack surface—their job is to make sure they can understand, monitor, and protect it.

Why Can't Security Teams Keep Up?

The ESG data indicates that security teams find it difficult to keep up with an environment featuring rapid and constant changes. There are three main reasons why addressing security analytics and operations is so challenging, as many organizations suffer from:

- Too many disconnected tools. ESG research demonstrates that 35% of organizations use 26 or more disparate technologies for security analytics and operations.[2] These tools tend to work independently, with their own user interfaces, reports, and day-to-day operations, making it difficult to piece together a holistic view of enterprise security status, triage security alerts, or investigate multifaceted cyber-attacks. Point tools fatigue also leads to operational complexity, forcing the security staff into a never-ending cycle of managing configurations, fine-tuning rule sets, and working with vendors to address their changing needs.

- A reliance on manual and inconsistent processes. Too often, security analytics and operations rely upon manual and inconsistent processes. This means that human beings must be involved in all security operations tasks like fetching data artifacts, running queries, or updating security rule sets. Aside from introducing an opportunity for human error, security teams using manual and inconsistent processes can't triage, prioritize, or investigate the growing volume of security alerts in a timely and efficient way.

- A cybersecurity skills gap. 44% of organizations claim to have a problematic shortage of cybersecurity skills.[3] This means that cybersecurity teams are understaffed *and* lacking advanced skills often necessary for security analytics and operations. The skills shortage exacerbates the issues described above as there simply aren't enough people or hours in the day to get everything done. Furthermore, security teams are often overwhelmed, creating a work environment fraught with stress, employee burnout, and high turnover.

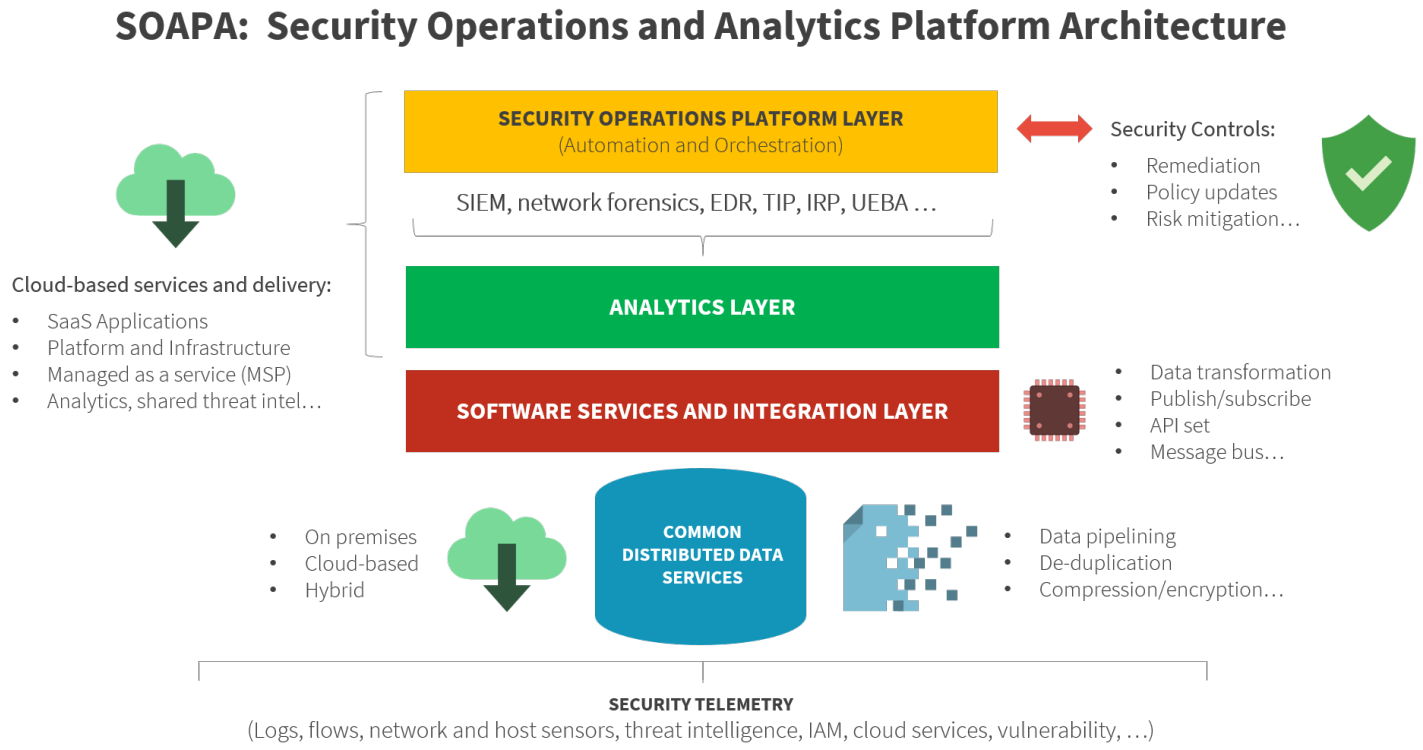
Taken together, security analytics and operations are ineffective and inefficient, leading to increasing cyber-risk, system compromises, and data breaches. CISOs must address *all* these issues if they have any hope of protecting critical business assets.

Strategic Changes Are Underway

Smart CISOs are aware of the problems described above and are aggressively addressing them. For example, many organizations are consolidating security analytics and operations tools to build a tightly integrated security operations and analytics platform architecture (SOAPA) (see Figure 2). ESG research indicates that 36% of enterprise organizations are actively consolidating tools as one of their highest security priorities, while another 48% are somewhat active in this area.

[2] Source: ESG Master Survey Results, *Cloud-scale Security Analytics Survey*, December 2019.
[3] Source: ESG Master Survey Results, *2020 Technology Spending Intentions Survey*, January 2020.

Figure 2. SOAPA Technology Stack



Source: Enterprise Strategy Group

SOAPA is composed of:

- A common distributed data service. SOAPA creates an aggregated data pipeline for batch and streaming data. In this way, SOAPA can accommodate massive amounts of security data for all types of analytics—from real-time threat detection to long-term retrospective investigations spanning months or even years-worth of security data.
- Software services and integration layer. This layer serves as a bridge between security telemetry and analytics engines that consume the data. In simple terms, the software services and integration layer makes all security data available to analytics engines when they want it and in the format they want it.
- Analytics layer. Security data is processed and analyzed by a variety of security tools that monitor endpoint processes, network behavior, threat intelligence patterns, or all these (and many other) areas at once using analytics like event correlation, statistical analysis, heuristics, and machine learning. The SOAPA analytics layer is designed for efficient monitoring and analysis of all security data to help SOC teams accelerate threat detection, pinpoint problems, and prioritize actions.
- Security operations platform layer. When security analytics discover and isolate a problem, it can then hand off remediation tasks to the security operations platform layer for process execution by the security staff. The top layer of the SOAPA stack is programmable and can be instrumented to take automated actions like gathering data for an investigation, blocking a network connection, or opening a ticket in a case management system. Security remediation operations can also be orchestrated to take actions across multiple security controls like firewalls, network proxies,

web or DNS gateways, etc. Finally, the security operations layer acts as a workbench for SOC analysts for complex operations that require a combination of automated and manual intervention. Using a common security operations platform layer, organizations can capture and promote institutional knowledge. This not only formalizes best practices, it can also help transfer knowledge from experienced to junior analysts, improving the efficiency of training programs.

SOAPA Use Case

Through tight technology integration, advanced analytics, and process automation and orchestration, SOAPA is designed to vastly improve security operations across a lifecycle from threat detection through incident response. Here's an example of SOAPA in a threat scenario:

1. The CFO's system begins acting suspiciously and then beacons out to an unknown IP address.
2. Based upon real-time data, a SIEM platform detects malware on the CFO's Windows desktop. Since the CFO is a corporate officer, her PC is considered a business-critical asset. The SIEM is configured to know that this is a high-value system and treats this alert as a priority.
3. The SIEM automatically creates a trouble ticket in a SOAPA case management system and alerts the on-duty security, IT operations, and incident response team immediately.
4. SOAPA associates this type of malware attack with a specific investigations and remediation playbook. The playbook sets off and automatically begins collecting other related data (i.e., EDR data, threat intelligence data, DNS logs, IoCs/artifacts, etc.) necessary to enrich this alert/event. By automatically pulling in associated data for analysis and comparing it to historic and active incidents, analysts can get a head start in their security investigation.
5. Under normal circumstances, a security incident like this would immediately trigger an automated remediation rule to quarantine the system from the network. Since this is the CFO's system, this action is not taken so that the CFO can continue working. Alternatively, SOAPA communicates directly with the firewall with instructions to block all communications to the unknown IP address while all other PC activity is closely monitored.
6. Given the fact that the CFO's system has been compromised, a junior analyst performs only basic incident triage and then escalates the security incident to a tier-3 security analyst in the SOC per playbook instructions. All relevant data is included in the escalation message, including any notes from the junior analyst. The tier-3 analyst can then view the CFO's system activity as a timeline as part of his investigation, assign someone to manage the incident lifecycle, and schedule check-in meetings for progress updates.
7. Based upon analysis, the tier-3 analyst discovers that the CFO fell victim to a phishing email that installed malware on her system. The malware then reached out to a command-and-control server for further instructions. Fortunately, the security operations platform and firewall were able to block this communication before any further damage could be done. The analyst identifies the malicious file installed on the PC and adds this information into the case management system. Based upon the playbook, the details are sent to the IT operations team who can then dispatch a technician to remove the malicious file and any other artifacts from the CFO's system.

8. Examples of the phishing email and all associated indicators of compromise (IoCs) are sent to the threat hunting team. Threat hunters will then scan the network, looking for these IoCs on other systems. They will also research the IoCs to see if they can learn anything about threat actors or similar tactics, techniques, and procedures (TTPs). Based upon this secondary research, they will scan the network again looking for similar patterns. To streamline security tasks, searching and deleting phishing emails from other inboxes can be automated.

9. Once the IT operations team remediates the CFO's system, the incident can be closed in the security operations case management system. A senior SOC team member can review the entire incident lifecycle to assess playbook efficiency. The playbook can be modified to accommodate any lessons learned.

In summary, SOAPA facilitates everything necessary—from collecting, processing, and analyzing the data for incident detection, through investigations, workflow, and remediation for incident response. Tasks can be automated based upon playbooks, including triggering remediation rules for quarantining systems, deleting malicious files, or blocking network traffic, while a case management system organizes and tracks each step throughout the lifecycle. The playbook in this case was customized for the compromise of an executive's system. In this way, SOAPA can improve security efficacy and bolster operational efficiency through the automation and orchestration of data-driven security analysis and decision making. Aside from overall security improvements, SOAPA can help the SOC staff directly by decreasing "alert fatigue." This can help junior security analysts to become more productive while enabling the entire SOC team to focus on important decisions, not mundane tasks.

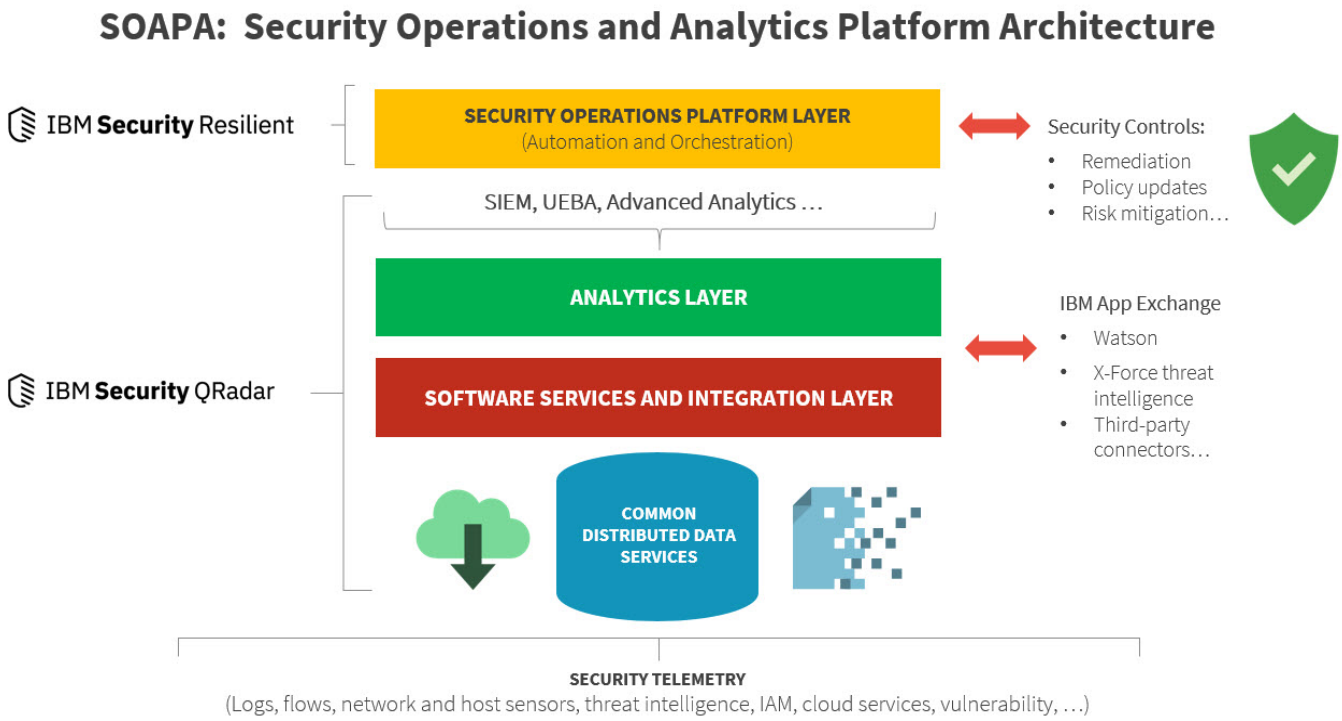
IBM Security's Approach to SOAPA with QRadar and Resilient

Designing and building SOAPA can be a multi-phased project where organizations integrate a variety of security analytics and operations tools into a common architecture. This can take years and require lots of customization to achieve. Given the state of cybersecurity, few organizations have the luxury of multi-year security technology projects.

IBM Security provides an alternative to this burden through its own comprehensive SOAPA offering: IBM Security QRadar for security information and event management (SIEM) and IBM Security Resilient, a platform for security orchestration, automation, and response (SOAR) (see Figure 3). As part of IBM's SOAPA offering:

- IBM Security QRadar collects, processes, and performs advanced analytics on security-relevant data for threat visibility and detection. QRadar employs over 500 commercial solution connectors to collect data from containers, endpoints, users, applications, networks, and clouds, and can then apply business context to the data to align security incidents with business-critical assets. This gives security analysts visibility into a wide variety of security events. Upon processing, security data is analyzed through custom rules, event correlation, user and entity behavior analytics (UEBA), and machine learning algorithms to detect known and unknown threats. QRadar also interoperates with other types of security telemetry including network flows, partner technologies, and analytics engines through the IBM and third-party applications available through the IBM Security App Exchange. Once QRadar detects a threat, it escalates the offense to Resilient.

Figure 3. IBM SOAPA



Source: Enterprise Strategy Group

- IBM Security Resilient can automate and orchestrate incident response processes. QRadar works cooperatively with Resilient for incident investigation and remediation across various security operations use cases. Resilient includes functionality for case management, playbook creation and management, process automation, and response orchestration, covering the entire security incident lifecycle from detection through remediation. The QRadar and Resilient integration can help in a variety of ways including escalating offenses (along with a timeline of evidence and communication to all involved parties), automating data enrichment tasks for investigation, and orchestrating response actions through direct integration with security controls and access to the right stakeholders. Through the integrated solution, organizations can be better prepared to respond to cyber-attacks with improved processes through predesigned workflows that include people, process, and technology and through improved detection accuracy from a continuous feedback loop between Resilient and QRadar. Finally, security teams can also identify security gaps by reviewing metrics within Resilient after security incidents to modify playbook details and workflows to achieve continuous process improvement.

Resilient Integrations with QRadar

Organizations vary in terms of their cybersecurity maturity and requirements. To address these variations, IBM provides 4 different integrations, all available through the IBM Security App Exchange for QRadar and Resilient as part of its SOAPA:

1. Resilient + QRadar Integration. This option includes core integration, a Resilient plug-in, built natively into QRadar, that is regularly updated to support new use cases. This tight integration provides seamless flow of data between QRadar and Resilient. The creation of a Resilient incident can be automated based on severity, type, or other

criteria, or can be manually triggered by an analyst. This is a bidirectional integration that reports back on the fidelity of the information received, improving the detection rules on QRadar.

2. Resilient + QRadar Functions. The QRadar Functions application includes additional features and workflows to extend the capabilities within the Resilient platform. Security teams can trigger automated or manual searches of QRadar data from inside a Resilient incident. The data can be used to populate data tables and enrich incidents to help accelerate security investigations or enable threat hunting actions.

3. Resilient + QRadar Advisor with Watson. QRadar Advisor with Watson is an application that enhances QRadar by leveraging artificial intelligence to enrich security investigations. Organizations using QRadar Advisor with Watson can extend Watson for Cyber Security insights to Resilient to enrich incidents, dive deeper into artifacts, map offenses against MITRE ATT&CK tactics, and establish better context around individual security incidents. This integration can help improve incident response (IR) accuracy and timeliness.

4. QRadar-MITRE content package for Resilient. Built to work with QRadar Advisor with Watson, this application aligns QRadar analytics, Watson for Cyber Security insights, and Resilient process management with the MITRE ATT&CK framework (MAF). By enabling this integration, QRadar offenses that have been investigated by QRadar Advisor with Watson can pass MITRE tactic and technique information to Resilient. Resilient can create new tasks for further security investigations, threat hunting, and controls modifications.

The Bigger Truth

When it comes to security analytics and operations, many organizations face three consistent issues:

1. Too many independent point tools that can't interoperate.

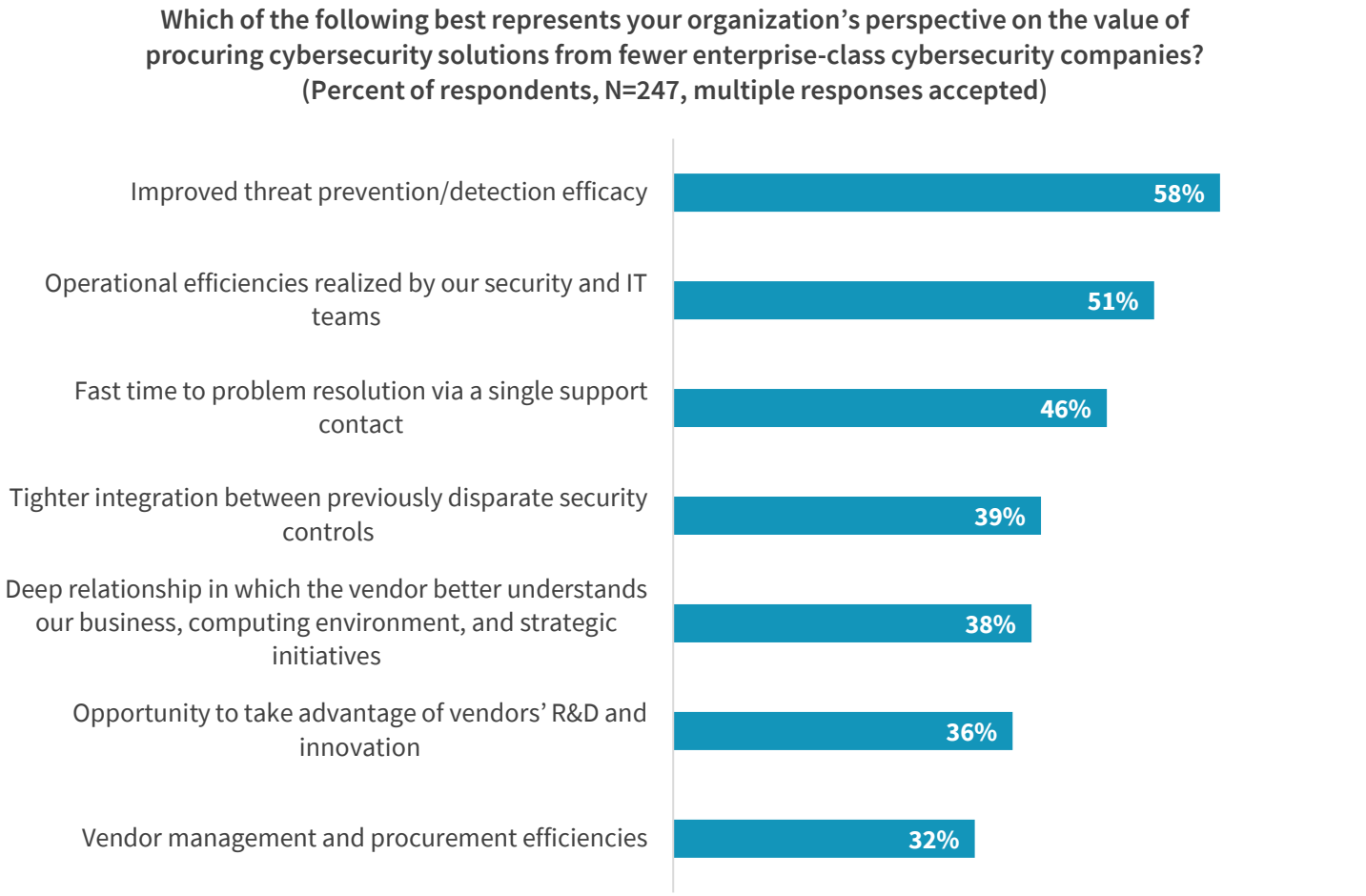
2. Manual, informal, and inconsistent processes that can't scale to keep up with an increasingly sophisticated threat landscape.

3. A cybersecurity staff and skills shortage.

To address these challenges, security teams must work smarter, not harder. This means scaling the security data pipeline, improving the fidelity of security analytics, and then formalizing and automating security operations processes. ESG believes that accomplishing these goals will require a new level of technology integration and vendor consolidation using a tightly coupled security operations and analytics platform architecture (SOAPA). In fact, 39% of organizations are actively consolidating the number of cybersecurity vendors they do business with, while 38% are doing so on a limited basis. CISOs believe that vendor consolidation and SOAPA can lead to benefits like operational efficiencies, tighter technology integration, and a greater level of security technology innovation, among other things (see Figure 4).[4]

[4] Source: ESG Master Survey Results, *Enterprise-class Cybersecurity Vendors and Platforms Landscape*, to be published.

Figure 4. Benefits Associated with Vendor Consolidation



Source: Enterprise Strategy Group

IBM Security recognizes these challenges. Its tight integration between QRadar (SIEM) and Resilient (SOAR) result in a one-stop SOAPA shop that can help organizations enhance threat prevention, detection, and response. IBM is also extending its SOAPA offering through its recently announced Cloud Pak for Security, a cloud-based platform that allows organizations to connect disparate data sources for security operations activities like case management, federated search, and process automation/orchestration. Given its end-to-end one-stop-shop SOAPA offering, CISOs may want to contact IBM to see if the combination of IBM Security QRadar and Resilient (along with Cloud Pak for Security) can help them improve security efficacy, streamline operations, and enable the business.

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