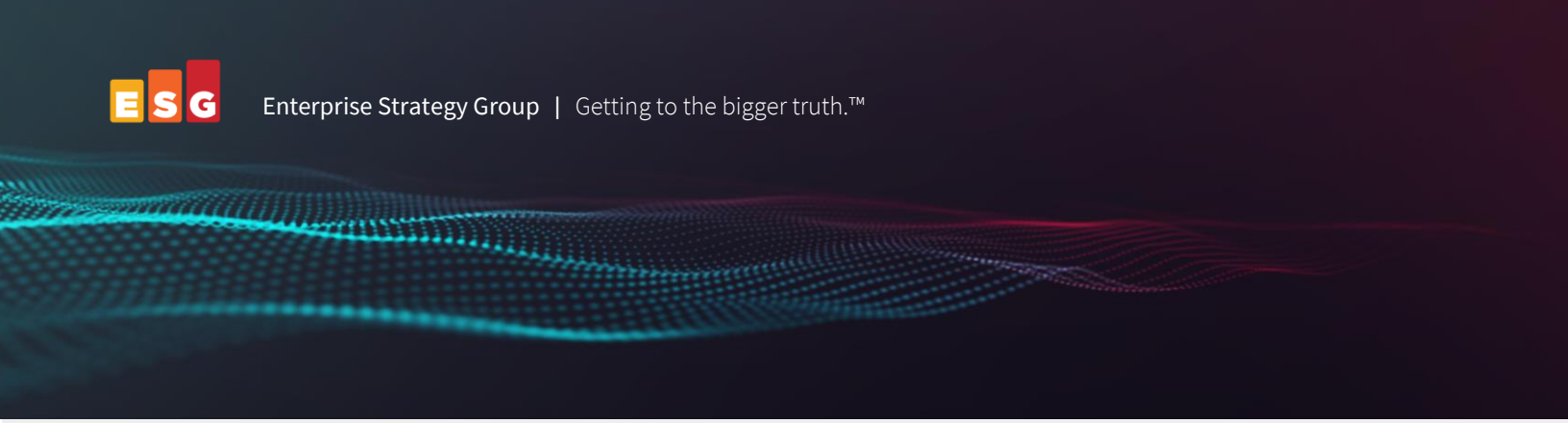


ESG WHITE PAPER

Introducing IBM Security QRadar XDR

A Comprehensive Open Solution in a Crowded and Confusing Space

By Jon Oltsik, ESG Senior Principal Analyst

March 2022

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

Contents

Executive Summary

When asked to identify the business initiatives that will drive IT spending over the next 12 months, nearly half (47%) of respondents to ESG's 2021 Technology Spending Intentions Survey said strengthening cybersecurity.[1] This represents an important realization. In the age of cloud computing, digital transformation, and remote worker support, organizations need strong cybersecurity processes and controls as a foundation for business health and prosperity.

Given the inexorable relationship between business, IT, and security, it would be safe to assume that organizations have modernized their security operations centers (SOCs) to detect and respond to cyber-threats in real time. Alarmingly, this assumption would be incorrect—many SOC teams struggle to keep up with modern threats.

What's going on with threat detection and response today, and are there any promising developments for the future? This white paper concludes:

- Organizations have many threat detection and response goals. SOC teams have threat detection and response objectives, such as improving detection of advanced threats, increasing process automation around remediation tasks, and enhancing incident response (IR) timing. These goals suggest that status quo approaches aren't working.
- Threat detection and response challenges abound. Infosec pros admit to a plethora of threat detection and response challenges, including increasing security operations complexity, resource shortages, a growing/changing attack surface, a reliance on disconnected point solution tools, and difficulties with data analysis and decision making. These issues impact security operations efficacy, efficiency, and SOC analyst productivity.
- XDR may help address threat detection and response challenges. XDR (eXtended detection and response) has emerged as a commercial security operations architecture, much like ESG's security operations and analytics platform architecture (SOAPA) model. While still in its early phases, XDR has the potential to improve threat detection and response while modernizing SOCs.
- Leading XDR solutions should provide enterprise-class functionality. ESG believes that XDR solutions should provide coverage across hybrid IT infrastructures, advanced analytics, and automated playbooks for incident response. To address scaling and integration needs, XDR should also be cloud-based and built using industry standards, open APIs, and common data formats. Leading XDR vendors will also promote integration through partnerships and developer support services.

The State of Threat Detection and Response

Threat detection and response is a top priority at most organizations, as cyber-attacks like ransomware and supply chain breaches can disturb or even halt business operations. As a result, 83% of organizations plan to increase spending on threat detection and response technologies, services, and personnel in the next 12 to 18 months. To counteract cyber-threats, organizations have numerous threat detection and response objectives, including (see Figure 1):[2]

- Improving the detection of advanced threats. Organizations want to develop better detection rules and analytics to accelerate identification of known and unknown threats. Detection improvement methods include enhanced anomaly detection, higher fidelity security alerts, more granular attack "timelines" across the kill chain, and support for complex queries for more advanced threat hunting.

[1] Source: ESG Research Report, *2021 Technology Spending Intentions Survey*, January 2021.
[2] Source: ESG Research Report, *The Impact of XDR in the Modern SOC*, March 2021. All ESG research references and charts in this white paper have been taken from this research report, unless otherwise noted.

- Increasing automation of remediation tasks. Security operations tasks for threat mitigation and incident response are often based on manual processes and the "tribal knowledge" of the SOC team. This behavior may have been appropriate in 2010, but manual processes can't scale to address security alert volume or analytics needs across hybrid IT infrastructure. SOC teams understand the need to automate mundane tasks and orchestrate response actions for alert triage, security investigations, and threat prevention. Automation can streamline processes, bolster analyst productivity, and focus the SOC team on continuous improvement.
- Improving mean time to respond to threats. Once threats are detected, incident response must follow immediately to reduce adversary dwell times and limit damages. This includes blocking cyber-attacks in progress, understanding the blast radius of attacks, and then remediating any remaining vulnerabilities or remnants of the attacks. CISOs know they need to accelerate this process.

Figure 1. Top 6 Threat Detection and Response Program Goals

Source: Enterprise Strategy Group

Threat Detection and Response Challenges

While many organizations have threat detection and response goals, attaining them won't be so easy. Security professionals admit to threat detection and response challenges such as (see Figure 2):

- Chasing high priority alerts. Organizations spend most of their time addressing high priority/emergency threats and not enough time on threat detection and response strategy or continuous improvement. In this scenario, Tier-1 analysts are overwhelmed with alert triage and mundane tasks leading to premature escalation of incidents to Tier-2 analyst investigations, bogging down the whole system. These challenges are exacerbated by staffing issues like inexperienced/new analysts, staff attrition, and employee burnout.

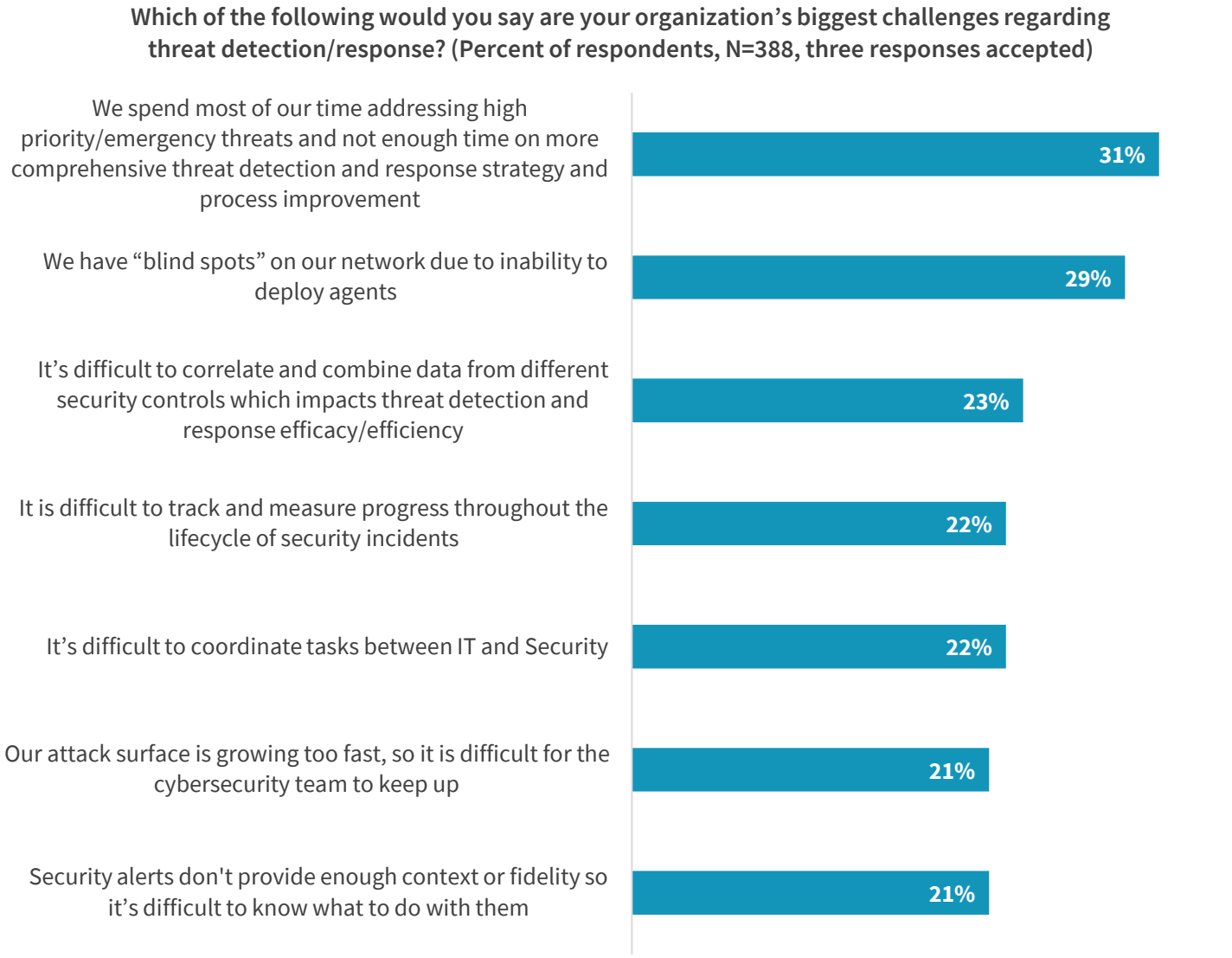
- Blind spots. Twenty-nine percent of organizations claim to have monitoring "blind spots" that limit visibility for threat detection. Blind spots can result from poor integration of siloed technologies, the proliferation of point solutions, or inadequate data sources covering the entire cyber-kill chain. Regardless of the reason, security analysts are forced to piece together threat detection through assorted clues rather than comprehensive data-driven analytics and decision making.

- Difficult data correlation. Threat detection depends upon data correlation from an assortment of tools and data sources. This process requires the right data sources, sound data pipelining, and analysts who know how to combine data elements to recognize adversary behavior. This is understandably complex, requiring security platform engineering and data analytics skills. Sadly, many organizations lack these resources and skills.

It is also worth noting that remediation processes tend to break down, as 22% admit that it is difficult to coordinate tasks between security and IT.

For CISOs this list of threat detection and response challenges should be a real cause for concern. Existing threat detection processes and technologies are cumbersome, manual, and dependent upon too many disconnected point tools. When threats are truly detected, it is difficult to keep up with the attack surface or convince IT and security operations to work together. With cyber-risk growing, CISOs must think creatively about new types of solutions that work with existing infrastructure and find ways to optimize limited—and often under-skilled—staff.

Figure 2. Top Threat Detection and Response Challenges



Source: Enterprise Strategy Group

XDR to the Rescue?

Recognizing the need for tightly integrated security operations technologies, ESG first proposed a concept called "security operations and analytics platform architecture" in 2016. This type of integration has slowly gained traction. In a recent ESG research project, ESG asked security professionals whether their organizations are prioritizing integration of security analytics and operations technologies. Thirty-seven percent of survey respondents said that integrating security analytics and operations technologies was their organization's highest priority, while 56% claimed it is one of their top five priorities.

In the past, security operations technology integration required security engineering and custom coding. More recently, however, security vendors responded with XDR solutions to meet the growing need for technology integration. ESG defines XDR as:

"An integrated security technology architecture spanning hybrid IT (i.e., endpoints, networks, data centers, cloud, etc.), designed to interoperate and coordinate on threat prevention, detection, and response. XDR unifies control points, security telemetry, analytics, and operations into one enterprise system."

While XDR is a relatively new technology, some trends are starting to become clear. Leading XDR solutions include:

- Support and coverage across security controls and data sources. Modern cyber-threats often begin with the compromise of an endpoint device and then proceed through adversary tactics, techniques, and procedures (TTPs) like moving laterally across networks, harvesting user credentials, discovering valuable assets, and then exfiltrating sensitive data. Sometimes, cyber-adversaries use similar TTPs as part of ransomware attacks. To detect advanced cyber-threats effectively, XDR solutions need coverage across the kill chain, with sensors and controls on endpoints, networks, data centers, identity and access management (IAM) systems, cloud-based workloads, and business applications. In this way, XDR goes beyond discrete anomaly detection in one area. Rather, XDR uses a single trigger to piece together an attack timeline designed to connect all evidence (in sequence) of a cyber-attack in progress.

- Analytics that bring together elements of the entire cyber-kill chain. XDR builds on traditional threat detection technologies like signatures, correlation rules, and heuristics with machine learning algorithms, behavior-based analytics, and even cognitive computing for emulating human analysts. The best solutions will use "nested algorithms" that work together to analyze events across the kill chain and improve threat detection accuracy and timing. In this way, XDR is meant to add machine intelligence to Tier-1 analyst alert triage, Tier-2 analyst investigations, and Tier-3 analyst threat hunting activities. Leading systems will map analytics to the MITRE ATT&CK framework, pinpointing the TTPs used in attack campaigns, and giving analysts a map of where adversaries have been and where they are likely headed.

- Automated response capabilities. Upon detecting a cyber-attack in progress, SOC teams want XDR to take immediate defensive actions like quarantining systems, blocking network traffic, halting processes on endpoint, or disabling an administrator account. These automated responses should take place within the security domain (i.e., security controls like endpoint security software, network firewalls/proxies, CASB, etc.), negating the need for IT operations involvement or intricate change management policies. Response actions should also allow for customization to align with IR policies and processes to support different organization and industry requirements.

- A central workspace. Rather than pivot across tools, XDR should provide a central workspace where analysts have the information they need for activities like alert triage, threat intelligence analysis, investigations, incident response, and threat hunting. This requires a UI that provides the right graphics and dashboards, while supporting the ability to query and pivot across different controls and data sources. Of course, XDR should also feature role-based access control (RBAC) and provide specific templates, dashboards, and customization options for different security analyst roles and experience levels.

- An open platform built for integration. XDR should be thought of as a "manager of managers" technology that adds incremental value to existing security investments. As such, XDR platforms will need to interoperate seamlessly with security tools like asset management, case management, vulnerability management, authentication systems, and security controls like EDR, NDR, cloud security controls, email security filters, CASB, firewalls, and web proxies. To accommodate this requirement, XDR solutions should be open, built with published APIs, developer support tools and resources, and a partner ecosystem. Leading vendors will also support open standards as part of their XDR offerings.

Aside from these core requirements, XDR solutions must be built for scale and flexibility. This calls for a cloud-based architecture complete with a backend designed for big data and advanced analytics.

IBM Security QRadar XDR

While the XDR requirements outlined above are clear, the current XDR market is anything but. Vendor marketing rhetoric and industry hyperbole has led to XDR confusion. According to ESG research, only 24% of security professionals claim that they are "very familiar" with XDR.

Amid this XDR conundrum, IBM Security recently entered the fray with QRadar XDR—a portfolio of threat detection and response products that connect tools, workflows, insights, and people. The QRadar XDR suite includes SIEM, NDR, EDR (through the acquisition of ReaQta, which closed on Dec. 1, 2021), SOAR, and XDR Connect.

Unlike many competitors, IBM's XDR story is transparent and comprehensive. IBM is taking a thorough approach to XDR with open standards and automation that unifies endpoint detection and response (EDR), network detection and response (NDR), and security information and event management (SIEM) in a single set of workflows. In other words, QRadar XDR now goes beyond SIEM alone. Instead, it provides a full suite of threat detection and response solutions.

IBM Security QRadar XDR Connect, a cloud-native XDR solution, aligns with the requirements described above, as it:

- Is built with an open design that promotes broad connectivity and SOC unification. Unlike some of its proprietary competitors, IBM is fully committed to open XDR. For example, IBM is an active member of the open cybersecurity alliance (OCA), which describes itself as "building an open ecosystem where cybersecurity products interoperate without the need for custom integrations." QRadar XDR Connect uses OCA standards such as STIX shifter (a method for data normalization across domains), and Kestrel (an abstraction layer to streamline queries and workflows for threat hunting). In addition to its OCA support, QRadar XDR Connect is cloud-native and designed for connecting security tools, whether they come from IBM or third-party providers. For example, XDR Connect enables federated investigations across IBM and third-party data sources.

- Includes advanced analytics and MITRE ATT&CK mapping. QRadar XDR Connect aggregates telemetry from multiple data sources and enriches this data with threat intelligence to correlate and prioritize alerts. Using artificial intelligence (AI), QRadar XDR Connect offers an analytics engine that automatically investigates cases and correlates data across vendors, providing an incident timeline, MITRE ATT&CK mapping, and contextual threat intelligence to help SOC teams prioritize alerts and perform root-cause analysis within security investigations.

- Unifies the SOC experience. QRadar XDR Connect is designed to provide a unified seamless experience to promote better collaboration across siloed security operations teams focused in areas like threat intelligence research, security analysis, and incident response. From a SOC perspective, Tier-1, -2, and -3 analysts can standardize on QRadar XDR Connect as their primary interface for alert triage, investigations, incident response, and threat hunting.

As part of its open design, IBM Security QRadar XDR Connect works with EDR solutions from vendors like Carbon Black/VMware, CrowdStrike, and Cybereason. Additionally, IBM recently announced the acquisition of ReaQta, an AI-powered, automated EDR platform. This acquisition will be integrated into QRadar XDR Connect in the near future.

IBM also has an aggressive roadmap across the entire QRadar XDR family that includes additional advanced analytics (machine learning, behavioral analytics, etc.), transformation to an open standards-based rule engine, and recommended one-click responses. Taken together, IBM's full product portfolio, feature/functionality, open design, and roadmap could

help organizations improve threat detection/response efficacy, streamline security operations processes, and improve analyst productivity. Given this combination, CISOs should be quite interested in hearing more.

The Bigger Truth

British author C.S. Lewis is quoted as saying, "You never know what you can do until you try, and very few try unless they have to." Lewis may as well have been referring to CISOs, SOC managers, and security professionals in this sagacious quote. SOC teams have reached a point where traditional processes and technologies can no longer meet today's threat detection and response requirements. Therefore, they are at the point where they are forced to try something new and benefit from the results of this decision.

XDR may be the new approach that threat detection and response security leaders are looking for. While XDR remains in a genesis phase fraught with hyperbole and confusion, XDR solutions do have the potential to provide a security operations and analytics platform architecture that promotes security technology interoperability. Thus, XDR innovation has the potential to drive new levels of analytics, process automation, security visibility, and collaboration.

While CISOs should approach XDR with a curious and open mind, they must also be prepared for lots of vendor spin and "XDR" offerings that are marginally different than existing security products. To help them through the XDR morass, ESG suggests that true XDR solutions should include coverage across data sources and security controls, advanced analytics, thorough MITRE ATT&CK support, automated response options, and a central workspace for all analyst activities. Furthermore, XDR should be cloud-based, open, and designed for integration with heterogeneous security technologies. In essence, XDR should embrace and extend security tools while driving vast improvements in threat detection efficacy and operational efficiency.

IBM has long played a security operations role with its SIEM, SOAR, NDR, and threat intelligence products and services. To meet modern threat detection and response requirements, IBM has consolidated its security products into a suite including SIEM, NDR, EDR, SOAR, and XDR Connect. Given its pedigree, full suite, and open architecture, CISOs considering XDR should give IBM Security QRadar XDR a look-see.

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