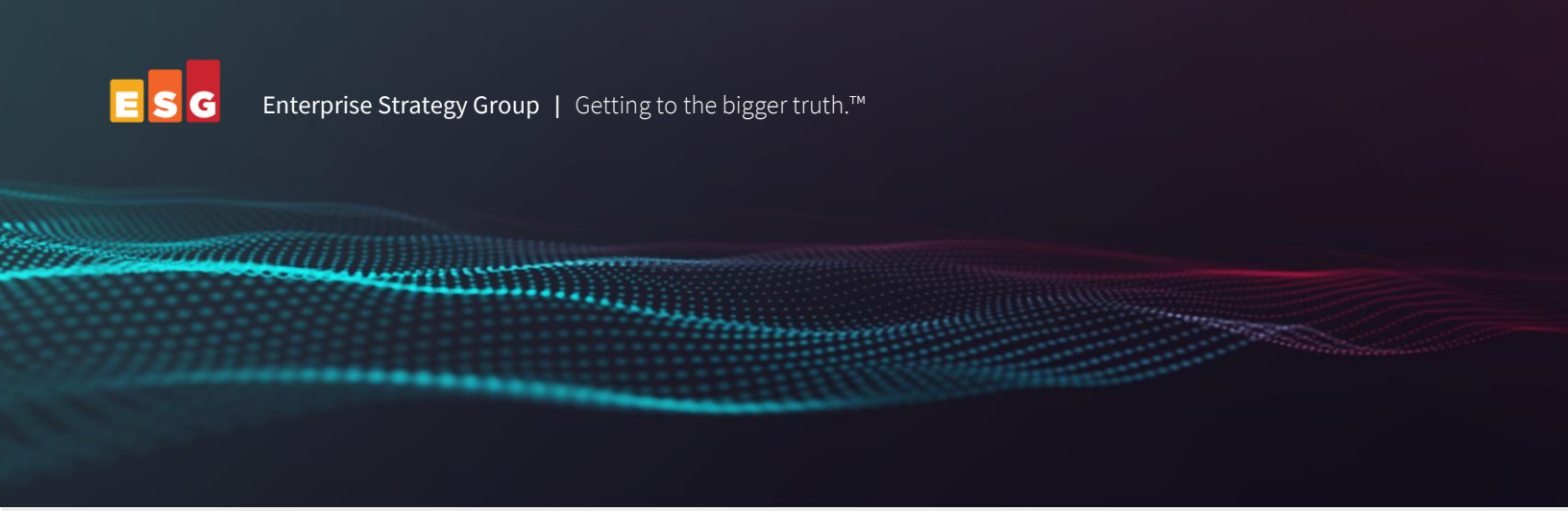


ESG WHITE PAPER

XDR Should Be Viewed as An Open Architecture

By Jon Oltsik, ESG Senior Principal Analyst

December 2021

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

Contents

Executive Summary

The number and sophistication of cyber-threats has precipitously increased in 2021, driven by remote workers, software supply chain attacks, and ransomware. For example, the Identity Theft Research Center (ITRC) reports a 17% increase in data breaches from 2020 to 2021, indicating we could be facing a record-breaking year for data compromises.

These trends should set off alarm bells with business executives and corporate boards. After all, these business leaders are hired to manage risk and protect shareholder value. Just one cyber-attack like those experienced by Solar Winds, Colonial Pipeline, JBS Foods, or the Florida water supply could be extremely costly and result in mass terminations.

Given this, it would be safe to assume that organizations have leading threat detection and response practices anchored by state-of-the-art technologies and staffed by highly experienced staff. Alarmingly, however, this isn't the case. Threat detection and response is stuck in the past at many organizations, leading to increasing cyber-risks.

What are the major threat detection and response issues and what can be done to address them? This white paper concludes:

- Threat detection and response is fraught with many challenges. When it comes to threat detection and response, many organizations are constantly reacting to the latest emergency with limited tools, manual processes, and an overburdened staff. These challenges hold them back while threat detection and response practices continue to increase. This imbalance is a recipe for disaster.
- XDR has great potential but remains confusing. An evolving security technology category called "extended detection and response" (XDR) holds the promise of integrating, consolidating, and simplifying underlying threat detection and response tools. So, what's the problem? Security vendors and industry pundits continue to co-opt the definition of XDR to suit their self-serving needs. This has resulted in industry hyperbole and user confusion, delaying XDR progress and implementation.
- XDR is really a security operations technology architecture. It's time for the security industry to move beyond petty bickering and realize that XDR is an important and evolving architecture that brings together security controls, data sources, and hybrid IT coverage into a common management plane to produce advanced analytics, analyst activities, and automated responses. Security operations center (SOC) teams are looking at XDR to deliver outcomes and aren't too concerned about the technical details of how this happens. Once these SOC teams approach XDR with an open mind, they can leverage and enhance existing security investments while creating a more effective and efficient security architecture.

Threat Detection and Response Situational Analysis

Despite millions of dollars in cybersecurity technology investments, many organizations still find it difficult to detect and respond to threats in a timely manner. In fact, many security professionals admit to a plethora of threat detection and response challenges such as (see Figure 1):[1]

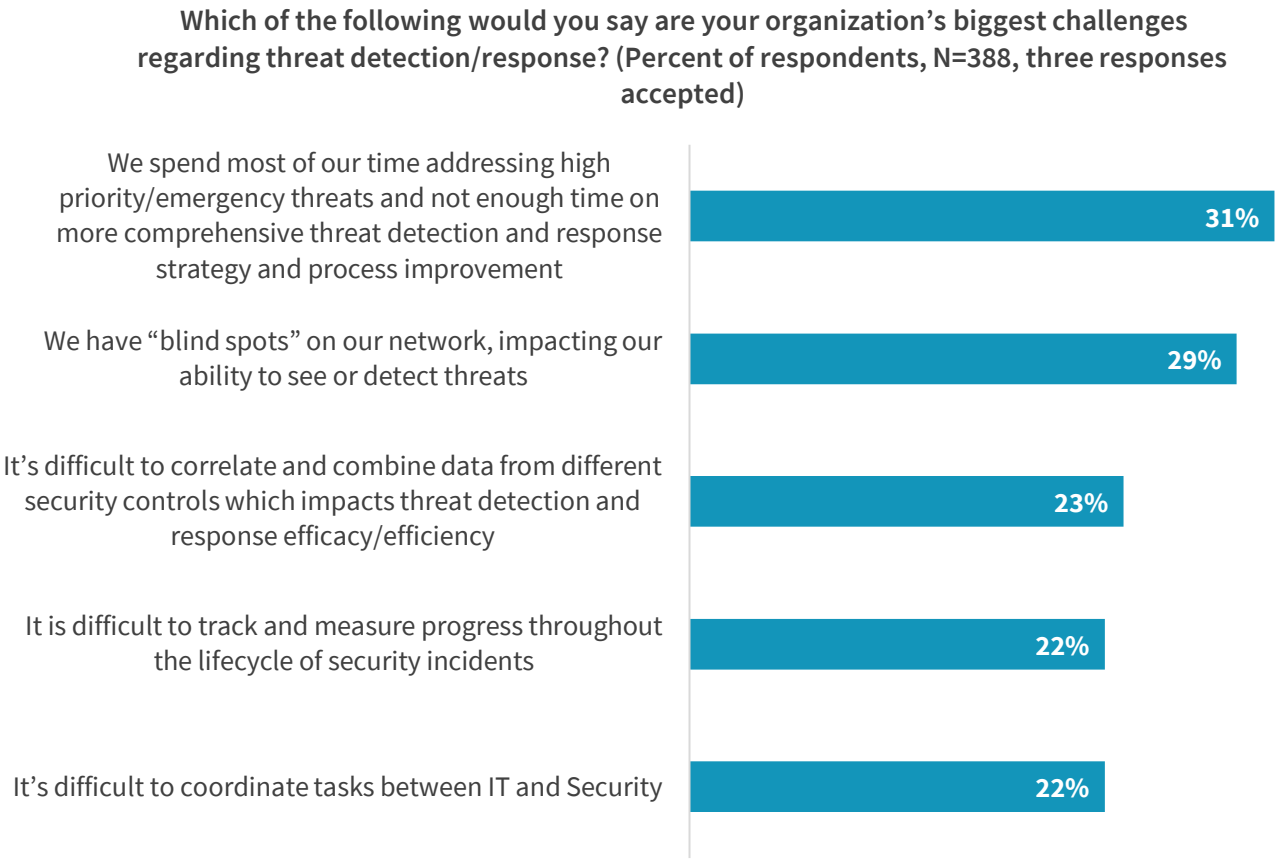
[1] Source: ESG Survey Results, *The Impact of XDR in the Modern SOC*, February 2021. All ESG research references and charts in this white paper have been taken from this survey results set, unless otherwise noted.

- Constant firefighting. SOC teams spend an inordinate amount of time responding to emergency alerts, leading to high stress and burnout while ignoring the need for continuous improvement. This situation is likely related to the fact that two-thirds of security professionals manage threat detection and response using an assortment of disconnected security tools, leading to operations overhead, false positive/negative incidents, human error, and one emergency after another.

- Limited visibility across data and tools. Twenty-nine percent of organizations have security monitoring "blind spots," limiting visibility for threat detection. Additionally, 23% of security pros claim that it is difficult to correlate and combine data from different security controls, which impacts threat detection and response efficacy/efficiency. Alarmingly, this means that SOC teams may not have all the data they need and can't always make sense of the data they have.

- IR processes problems. When real security incidents are discovered, security teams often rely on informal and undocumented manual processes driven by the "tribal knowledge" of a few individuals in the SOC. While SOC personnel should be commended for their efforts and dedication, manual processes can't keep up with the volume and scaling needs of security operations. This is especially troubling since 22% say it is difficult to track and measure progress throughout the lifecycle of security incidents, while another 22% find it difficult to coordinate tasks between security and IT groups. Clearly, SOC teams have people, process, and technology issues.

Figure 1. Top 5 Threat Detection and Response Challenges



Source: Enterprise Strategy Group

Aside from these challenges, research from ESG and the Information Systems Security Association (ISSA) indicates that 57% of security professionals say that their organization has been impacted by the global cybersecurity shortage.[2] What type of impact? Survey respondents point to increasing workloads, open job requisitions, and high burnout of security staff members. Since organizations can't hire their way out of this situation, they will need smarter and more efficient/effective security technologies that help bolster security staff productivity.

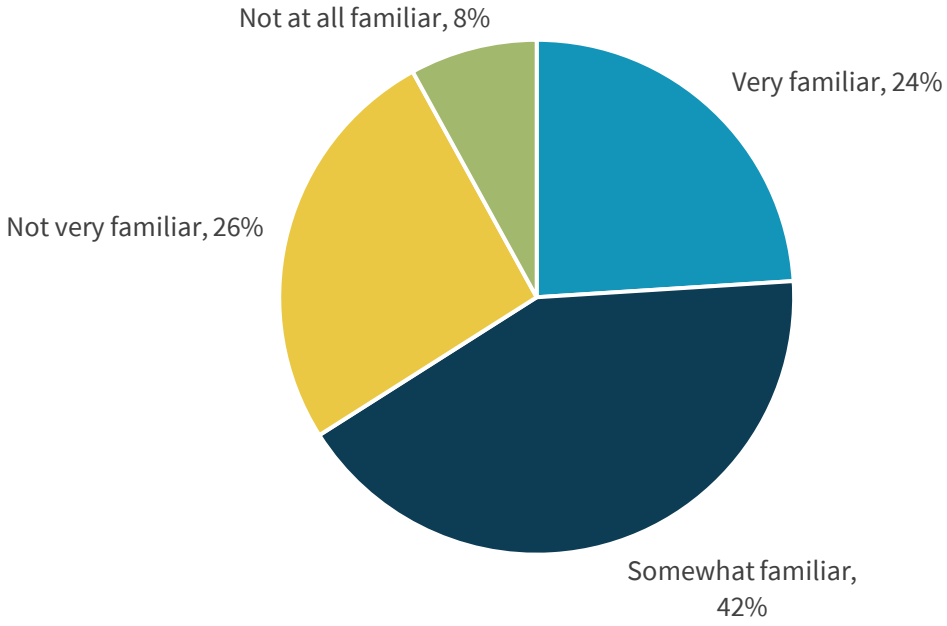
XDR to the Rescue?

To address the challenges described above, many organizations want to move from point tools to a tightly integrated security operations and analytics platform architecture (SOAPA). In fact, 37% of security professionals say that integrating security analytics and operations technology is their organization's highest priority while 56% claim it is one of their top five priorities.

In the past, combining security tools into SOAPA for threat detection and response improvement was a custom project where security engineers integrated technologies using message buses, API calls, and custom code. In recent years however, the security industry responded to these integration requirements with XDR, a commercial alternative to SOAPA. While this innovation is a promising development, the term "XDR" has been derailed by marketing messages and industry hyperbole. This may be one reason why only 24% of security professionals say that they are very familiar with XDR (see Figure 2).

Figure 2. Most Security Professionals are not Very Familiar with 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: Enterprise Strategy Group

[2] Source, ESG Research Report, *The Life and Times of Cybersecurity Professionals 2021 Volume V*, July 2021.

Some of the most common misconceptions about XDR are that:

- XDR is just an evolution of endpoint detection and response (EDR) technology. In this interpretation, endpoint detection and response technology is supplemented with other data sources like network metadata, cloud telemetry, and threat intelligence to create more comprehensive analytics for threat detection. ESG rejects this narrow view of XDR. In this case, outcomes, rather than technology underpinnings, are more important. So, while endpoint data is a rich resource for security telemetry, superior XDR analytics may be anchored by other data sources, with EDR playing a supporting rather than a leading role. It is simply too early in XDR development for EDR to be anointed to this position.

- XDR is an integrated suite from a single vendor. This thesis proposes that XDR is a single-vendor alternative to point-tools like EDR, network detection and response (NDR), cloud workload protection, and threat intelligence platforms (TIPs). Some say that XDR will even replace SOC stalwart technologies like SIEM and SOAR. While it's true that some vendors promote comprehensive XDR offerings, this is also a misguided perspective that assumes organizations will "rip and replace" their existing heterogeneous SOC technology stack with XDR from a single vendor. A single-vendor XDR strategy is simply too risky and too much work for many organizations to consider today.

XDR Reality Check

Given the current state of industry embellishment and confusion, it is important to establish a baseline understanding of exactly what XDR is. ESG defines XDR as follows:

"XDR is 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 an interoperable enterprise system."

Adding to this definition:

1. XDR is an architecture of controls, data sources, and capabilities. It is not a product.

2. XDR brings telemetry together from different sources to monitor and analyze activity and detect attacks across a cyber-kill chain. In other words, XDR stitches together suspicious/malicious activities throughout the lifecycle of cyber-attacks.

3. XDR data sources and control point coverage is expanding. Endpoint, network, and threat intelligence have been the primary data sources for XDR, but security teams also would like support for identity context. In other words, detections must be grounded with an understanding of the locations from which attacks emanate. Identity context can help align detections to specific assets and users. This is especially useful for detecting account takeovers, insider attacks, and IoT-based attacks. For example, when an IoT device, such as a printer (which has no security agent installed), participates in a botnet, XDR should be able to detect this stealthy action based on analysis of suspicious network behavior.

4. Beyond identity, XDR should also be able to detect suspicious/malicious SaaS application activities. This is an emerging requirement as organizations embrace SaaS, especially in response to a growing remote worker population. Attackers often compromise SaaS credentials as part of the kill chain or execute data breaches by stealing sensitive SaaS-based data. To address this risk, leading XDR solutions must have visibility into who is doing what with SaaS applications—especially within critical collaboration applications like Microsoft 365, Google Workspace, etc., and human capital management (HCM) applications such as Workday, SuccessFactors, Oracle HCM Cloud, etc., where a compromise would allow a threat actor to create a legitimate employee account.

5. XDR must offer a variety of native automated response capabilities. Based on detections, XDR solutions must be able to quarantine systems, terminate network connections, block account access, etc. Response actions should be available across the cyber-kill chain. For example, XDR should be able to disable endpoint processes, deactivate a Wi-Fi connection, or deny access to a user or device—on internal networks, cloud-based workloads, or SaaS applications. These options would provide security teams with the ability to fine-tune response policies, regardless of where they detect suspicious/malicious activities.

6. XDR must be open and support ease of integration into the existing security stack. As an architecture, XDR must be flexible, accommodate existing security technologies, and improve security efficacy and efficiency along the way. To allow organizations to build and evolve their XDR over time, each element (EDR, NDR, CDR, etc.) should have standalone value that is amplified by adding it into the XDR architecture (versus requiring that the entire XDR be in place and tuned before delivering value). Leading XDR solutions will integrate with security controls (i.e., endpoint security controls, network security controls, CASB, etc.), consume and analyze data from sensors and threat intelligence sources, and act as inputs into security operations systems like SIEM and SOAR.

Most importantly, XDR technology is a means to an end—providing vastly improved security outcomes. ESG research indicates that some of the most appealing XDR capabilities include (see Figure 3):

- Simplified visualization to bolster analyst productivity. Rather than pivot from one tool to another, security professionals want XDR to simplify visualization of complex attacks in order for analysts to understand how they progress across a cyber-kill chain. In this way, XDR can help tier-1 analysts improve their ability to triage alerts while tier-2 analysts will have the benefit of a timeline of events that can accelerate investigations. Simplified visualization across a cyber-kill chain can also help SOC teams to align XDR with the MITRE ATT&CK framework.

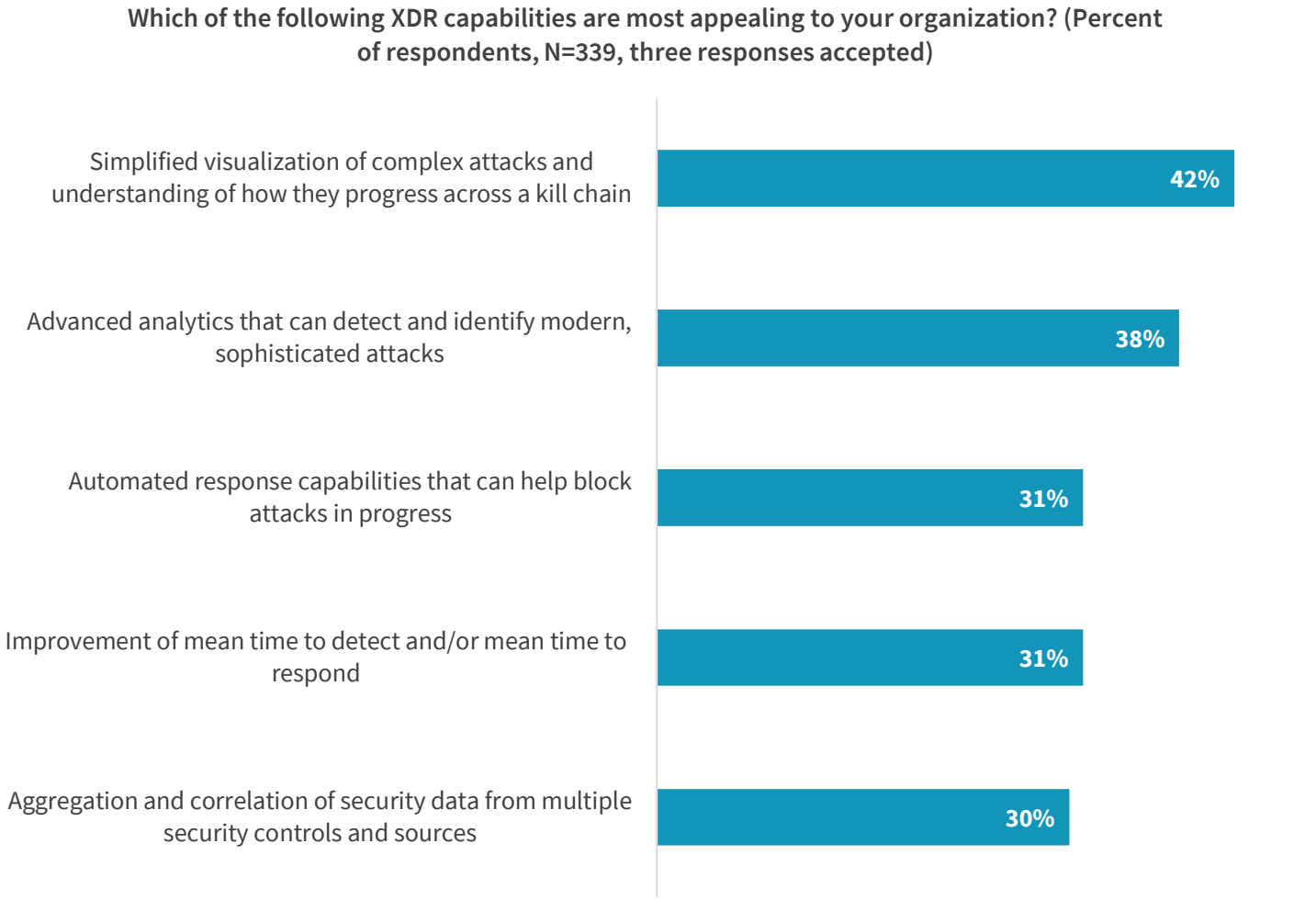
- Advanced analytics to detect unknown attacks. Beyond correlation rules, SOC teams want XDR to provide advanced analytics using artificial intelligence (AI) and machine learning algorithms. This can be particularly important for tier-3 analyst tasks like threat hunting—especially for unknown attacks conducted by nation-state actors or sophisticated cyber-criminals.

- Automated response capabilities to minimize damages. As described above, CISOs want XDR to act as an orchestration hub for addressing attacks in progress. Upon detecting an attack with a high degree of confidence, XDR can immediately communicate with endpoint security controls, identity services, network security devices, cloud workloads, or SaaS applications, and provide specific instructions about which indicators of compromise (IoCs) to block. This information can help minimize damages without involving IT operations teams or processes.

- Accelerated detection/response. These are the most desirable attributes of all—CISOs want XDR to improve threat detection efficacy and incident response efficiency, thus making XDR a security operations staple.

While there are dozens of XDR offerings today, security teams should focus research, testing, and deployment efforts based upon XDR capabilities in two areas: analytics and automation capabilities.

Figure 3. Top Five Most Appealing XDR Capabilities



Source: Enterprise Strategy Group

Vectra AI and XDR

Those who characterize XDR as a superset of EDR would dismiss Vectra, a cloud and network detection and response vendor outright—but ESG believes this would be a mistake. Using the definition and descriptions above, Vectra can assemble an XDR architecture while offering native XDR capabilities. Vectra supports XDR because it:

- Unifies analytics coverage for cloud, SaaS, network, identity, and endpoint. The Vectra Cognito platform ("Cognito") collects and analyzes network metadata, relevant IAM, SaaS and IaaS logs, and cloud events to provide visibility into the actions of all cloud and data center workloads and into user and IoT devices. Once Cognito collects and analyzes data, it then uses more than 100 different AI algorithms to find hidden and unknown attackers in real time, providing a starting point for AI-assisted threat hunting and response.

- Designs its offering for integration. Vectra is designed to detect threats to networks, hosts, cloud workloads, SaaS applications, user identities, and IoT devices. In addition to these out-of-the-box integrations, Vectra is often used in conjunction with other SOC technologies like SIEM, SOAR, and EDR. Unlike EDR-centric XDR, Vectra promotes a "bring your own EDR" philosophy, allowing Cognito users to respond manually or choose an automated response through

integration into native EDR response options including locking down a network host, cloud account, or network account.

- Automates incident response at multiple points across hybrid IT. Vectra enables host-based and/or account-based enforcement for incident response. With host-based enforcement, analysts target the source of an attack and lock down the endpoint being used. Vectra partners with EDR vendors like Microsoft, SentinelOne, CrowdStrike, and Cybereason. In many cases, attackers will gain access to the organization by stealing credentials through phishing or account takeover and logging in as a "legitimate" user. In these instances, account-based enforcement is effective, especially in cloud or hybrid environments where organizations don't own the service or infrastructure. Cognito offers options for automated or manual actions. Automated responses can be used to reduce lateral spread and provide resource-stretched security teams with more time to investigate incidents. Alternatively, manual response actions can help threat hunters monitor attacks in progress to gain additional insight into the tactics, techniques, and procedures (TTPs), and campaigns used to attack their organizations.

- Delivers positive outcomes for SOC teams and the business. Through its AI security modeling, Cognito can help organizations turn typical SOC alert storms into a focused high-priority list of security events for investigations. This reduces SOC analyst workload while improving threat detection efficacy and operational efficiency.

Cognito also aligns with the MITRE ATT&CK framework by mapping detection details to the MITRE taxonomy of adversary TTPs. This orientation can help SOC teams hunt for further evidence of unknown attacks and anticipate future TTPs to monitor along a cyber-attack kill chain.

Vectra embraces the "extended" component of XDR with native capabilities and partnerships to support hybrid IT coverage. In the future, Vectra plans to work with additional partners and extend its analytics algorithms. For example, Vectra uses EDR data for enrichment today but plans on ingesting endpoint telemetry data into its analytics engine in the future. This should help increase the accuracy, timeliness, and comprehensiveness of its threat detection and response capabilities moving forward.

The Bigger Truth

At present, security operations are hamstrung by a series of challenges that include a reliance on too many tools and manual processes. These challenges limit SOC scalability—a critical weakness as security alerts increase, the attack surface grows, and SOC teams are impacted by the global cybersecurity skills shortage.

While XDR is in an early stage of its evolution, it has the potential to address all of these issues by integrating technologies, introducing advanced analytics to threat detection and automated response actions. Therefore, it's important for the security technology industry to move beyond dogmatic and self-serving XDR definitions and start accepting that XDR is an open, heterogeneous security operations and analytics platform architecture (SOAPA) where the technical details aren't nearly as important as the security outcomes and benefits (i.e., accelerated threat detection and response, improved SOC productivity, etc.).

Vectra grew up as a network traffic analysis (NTA) and network detection and response (NDR) vendor. This heritage might eliminate Vectra Cognito from some XDR lists, but this would be a mistake. In fact, Cognito provides the native integrations, advanced analytics, and automated responses that are fundamental attributes of XDR. Furthermore, Vectra extends Cognito for threat detection within public cloud services, SaaS applications, and identity services for more thorough and comprehensive threat detection and response capabilities.

When ESG talks to CISOs about XDR, it advises them to think creatively and cast a wide net when researching or choosing vendor partners. Those that heed this advice would be well served to speak with Vectra to see how Cognito can support their emerging XDR strategies.

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