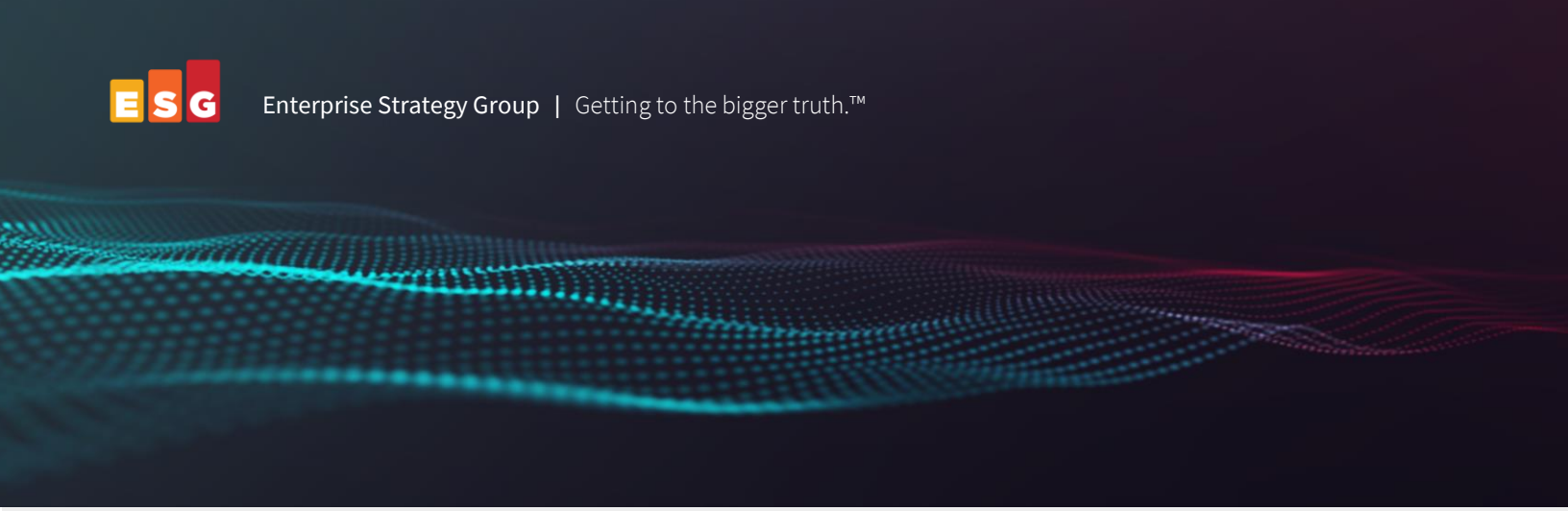


ESG RESEARCH INSIGHTS PAPER

The Promise of XDR for Effective Threat Detection and Response

By Jon Oltsik, ESG Senior Principal Analyst and Fellow

December 2020

This ESG Research Insights Paper was commissioned by Fortinet and is distributed under license from ESG.

Contents

Executive Summary

In October 2020, the Enterprise Strategy Group (ESG), completed a research survey of 388 cybersecurity and IT professionals who are directly involved with their organization's cybersecurity operations and threat detection and response. Twenty-four percent of respondents came from mid-market organizations (i.e., 100 to 999 employees) while the remaining 76% came from enterprise organizations (i.e., more than 1,000 employees). Further description of the research methodology and survey demographics are presented at the end of this report.

Based upon the research collected for this project, ESG reached the following conclusions:

- Threat detection and response efforts are stressed to a breaking point. Organizations suffer from a "perfect storm" of security operations challenges. Many firms are short-staffed or lack advanced cybersecurity skills due to the global cybersecurity skills shortage. SOC teams also tend to anchor threat detection and response with an army of disconnected point tools, generating a large volume of independent security information and feeding a manual process. This haphazard approach can't scale, so SOC teams are struggling to keep up with a combination of security data growth, targeted threats, and a growing attack surface. Alarmingly, security operations may be fast approaching a breaking point at some organizations.

- Organizations want consolidated and integrated security operations solutions. Recognizing these limitations, organizations are aggressively integrating their security analytics and operations technologies. The goal here is to transform disparate point tools into a security operations and analytics platform architecture (SOAPA), consolidating the data pipeline, analytics, visualization, and management. In a tightly integrated SOAPA, the whole architecture is more valuable than the sum of the individual parts (i.e., point tools).

- XDR may help organizations improve security efficacy and operational efficiency. The research survey explored the potential use of a new security technology platform called eXtended detection and response (XDR)—an integrated suite of security products that unifies control points, security telemetry, analytics, and operations into one enterprise system. Based upon the data collected, security professionals appreciate the XDR design point and potential benefits. Anticipating improvements in security efficacy and operational efficiency, many CISOs plan to give it a try in the next 12 months.

The State of Cybersecurity Operations

Threat detection and response is a core responsibility of any cybersecurity team, but many continue to struggle in this area. Beyond the global cybersecurity skills shortage, ESG research points to a range of threat detection and response challenges:

- Manual processes remain a big impediment: 43% of organizations agree that their organization relies on too many manual processes for threat detection and response. This stresses an already overwhelmed staff.

- Security noise is overwhelming security operations as 44% of organizations agree that their team struggles to keep up with the daily volume of security alerts. This means that they are missing important signals while dwelling on white noise and false positive indicators.

- Two-thirds of organizations (67%) manage threat detection and response using an assortment of point tools. This means that the SOC team is forced to monitor enterprise security status by piecing together individual views from each tool, leading to blind spots and inefficiencies.

Threat detection efforts are also dependent on a scalable, high performance data pipeline to collect, process, and analyze real-time security data. This includes endpoint data, network data, cloud data, and threat intelligence. Unfortunately, building and managing a scalable security data pipeline isn't easy. The research reveals that 36% to 38% of respondents reported challenges scaling the data pipeline, integrating threat intelligence with internal security alerts, and filtering through security data to separate signal from noise.

The ESG research paints an alarming picture. For many security teams, threat detection and response isn't working well, and problems are increasing. Organizations need to think differently with a new approach to tools and processes for threat detection and response or face a future of increasing cyber-risk and frequent security incidents.

The Prospects of XDR

Fortunately, CISOs do recognize that improving threat detection and response is critical for protecting mission-critical assets and business processes. Many are already doing things like consolidating vendors and integrating security tools into a security operations and analytics platform architecture (SOAPA). On the supply side, security technology vendors have introduced a new type of SOAPA-like integrated security platform called eXtended detection and response (XDR). ESG defines XDR as:

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

Like SOAPA, XDR integrates individual point tools into a common architecture. XDR also adds advanced analytics and capabilities for process automation. In this way, XDR can address many of the challenges described. Advanced analytics can help bolster the productivity of overworked SOC analysts by filtering noise and aggregating signals into high fidelity alerts. At the same time, process automation addresses the current dependence on manual processes.

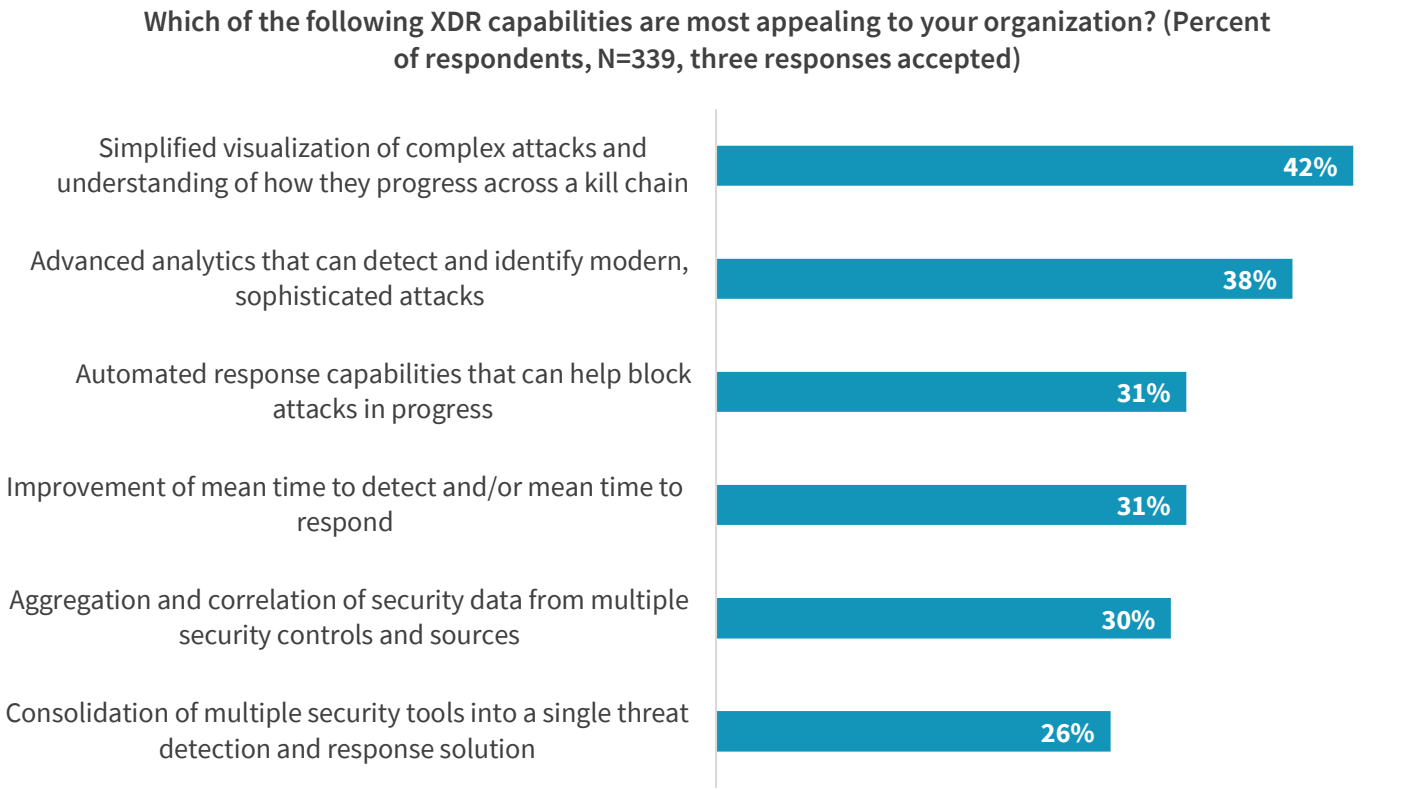
According to ESG research, security professionals see the potential value of XDR. In fact, XDR could be especially appealing for security operations in areas like (see Figure 1):

- Simplifying visualizations of complex attacks across the attack surface. SOC analysts often complain about "swivel chair" management as they are forced to view multiple security dashboards, logs, and reports as part of threat investigations. Survey respondents (42%) believe that XDR would be especially attractive if it could simplify visualization of complex attacks across the attack surface. In other words, they want an XDR interface that lets them monitor and investigate cyber-attack lifecycles as they proceed through the kill chain.

- Advanced analytics for detecting modern, sophisticated attacks. Rather than rely on event correlation and discrete machine learning algorithms and other techniques for every security domain (i.e., endpoint, network, etc.), 38% of cybersecurity professionals want XDR solutions offering advanced analytics that can detect modern, sophisticated attacks. In this way, machines can crunch vast amounts of data across control points, detect real cyber-attacks in progress, and present analysts with detailed timelines of the events involved in the attack lifecycle. Armed with this information, security teams can accelerate investigations and incident response.

- Automated response capabilities. When threats are detected with a high degree of confidence, 31% of security teams want XDR to take automated responses to block attacks in progress. These automated response actions could include updating endpoint security signatures, blocking a DNS domain, or adding a new firewall rule. The goal? Continually fortify the entire cybersecurity infrastructure—not just individual security domains – at machine speed.

Figure 1. Most Appealing XDR Capabilities



Source: Enterprise Strategy Group

Beyond XDR feature/functionality, CISOs want XDR outcomes that address current threat detection and response challenges and produce real business benefits. The ESG research indicates that security professionals rank the top XDR outcomes as (see Figure 2):

- High fidelity alerts for detection and prioritization. 40% of security operations teams want alerts to be timely and accurate, containing a timeline of details that track the progress of cyber-attacks. These specific facts can then help them prioritize responses, pinpoint the root cause and scope of a cyber-attack, and build a remediation plan for reinforcing applicable security controls.

- A central management hub. 38% of security operations analysts want to create and manage security policies, configure security controls, and view security activities through a single interface. By consolidating security controls, XDR can centralize security command and control in this way.

- Coverage for a growing attack surface from endpoints through cloud. 37% of security operations analysts want to extend their threat detection and response capabilities across a growing attack surface. This speaks to XDR's integration and visualization across all control points including endpoints, networks, servers, and cloud workloads. Some XDR offerings will include other controls such as email security, web security, and SaaS security, but the goal remains the same—track malicious/suspicious activities across the entire attack kill chain. This capability can also help align XDR with the MITRE ATT&CK Framework.

Figure 2. XDR Outcomes for Security Efficacy

Source: Enterprise Strategy Group

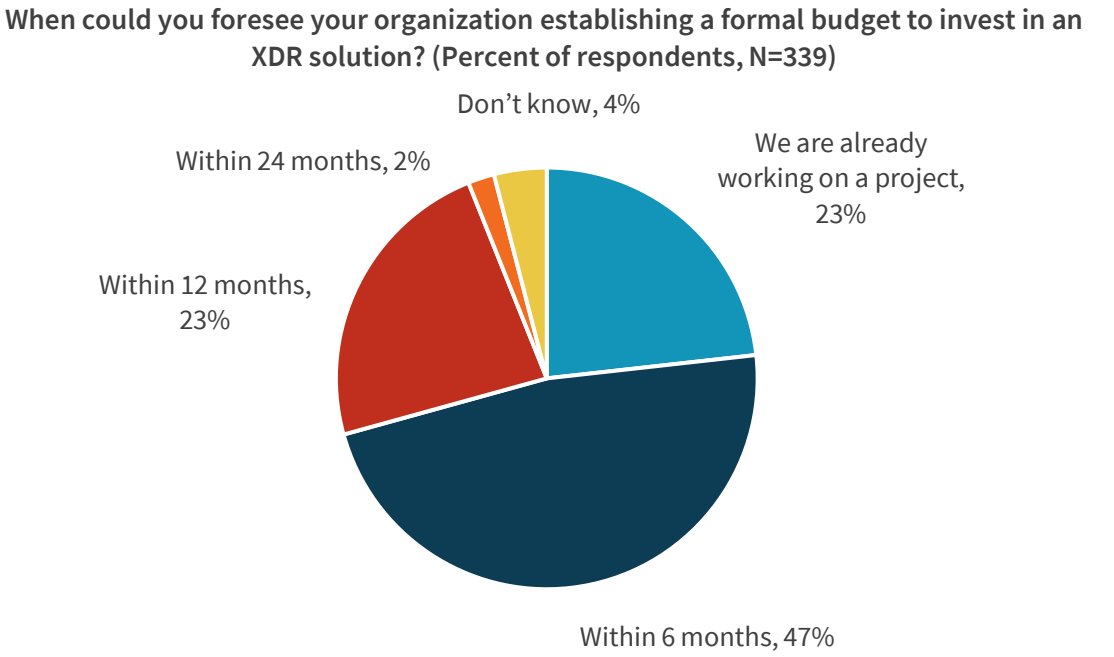
Services remain a big part of threat detection, especially the move to a sophisticated solution set like XDR: 35% of survey respondents indicated that their organization already uses a managed detection and response (MDR) service while another 38% are working on a project to adopt an MDR service. This reliance on services extends to XDR as well—45% of organizations want to utilize deployment services (i.e., project management, test, pilot, implementation, etc.), while 35% want to utilize planning services (i.e., assessment, project design and planning, etc.). CISOs seeking this type of help should work with XDR vendors and/or service providers that offer reference architectures and deployment guides as well as XDR best practice strategies.

XDR in 2021

XDR is a nascent technology today in 2020, but ESG research reports that 2021 will be an active year, highlighted by technology innovation and implementation. Given all the current issues associated with threat detection and response in general, most organizations have plans to see how XDR can help them. For example:

- Organizations are already moving forward towards XDR. The research reveals that nearly one-quarter (23%) of organizations are already working on an XDR project. These are likely custom integration projects between two controls like EDR and network detection and response (NDR). Additionally, 70% believe they could establish an XDR budget within the next 12 months (see Figure 3). This speaks to the pressing need to improve security efficacy and streamline security operations.

Figure 3. XDR Budget Plans



Source: Enterprise Strategy Group

- XDR could replace existing security controls. Nearly half (48%) of organizations would be willing to replace existing controls with XDR while an additional 47% might do so if they were convinced of XDR's effectiveness. Which controls? The most likely areas are endpoint and network security, but the platform nature of XDR could cause organizations to replace others as well. Interestingly, many organizations may start with cloud-based threat detection and response controls and then build out a more comprehensive XDR architecture from there.

- Organizations would be willing to add XDR sensors/agents to their infrastructure. More than three-quarters (76%) of organizations would be willing to add a new sensor or agents if necessary or if XDR could deliver significant benefits. Again, this is indicative of the grave need for security improvement. If organizations need to collect, process, and analyze more data, they are willing to do so to achieve better results.

The Bigger Truth

The ESG research indicates that many organizations don't have the right people, processes, or technology to meet their threat detection and response needs. Their people are overwhelmed and operating sub-optimally, lacking the right sized cybersecurity staff or security analytics skills. Processes are often manual and fraught with repetitive tedious tasks like looking up IP addresses. And threat detection and response processes are often dependent on armies of disconnected point tools with myopic purviews of the enterprise security landscape. CISOs must realize that making incremental people, process, and technology changes can only result in incremental benefits and not the transformational changes they really need.

There appears to be a change on the horizon, however—security technology vendors recognize the acute needs of security professionals and seek to address them with tightly coupled end-to-end security platforms called XDR. XDR may be an emerging market, but ESG believes it will develop quickly in 2021 and beyond. Based on the data presented in this ESG research insights report, it's clear that many organizations will welcome XDR if it can live up to its promises.

As organizations evaluate XDR, ESG recommends that they:

- Start small but plan big. CISOs should focus their short-term XDR efforts on particularly weak or complex areas. For example, for years, organizations have been dissatisfied with traditional endpoint security and more recently many indicated that they need better visibility into malicious/suspicious activities related to cloud workloads, so either or both of these may be an ideal place to start. Beyond a starting point, security teams should view XDR as a phased deployment over time with a goal of complete attack surface coverage in a reasonable timeframe of 18 to 36 months. Each product phase should be measured by consolidation and integration benefits achieved.

- Look for advanced analytics. Leading XDR solutions will distinguish themselves based on content—vendor rule sets, community contributions, machine learning algorithms, etc. Look for vendors with experienced threat research teams committed to analytics innovation and continuous content updates.

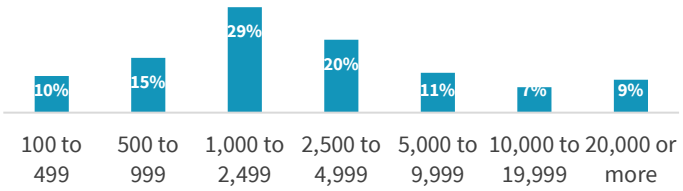
- Consider process automation critical. While XDR won't compete with full-blown SOAR anytime soon, leading XDR platforms should support process automation, especially for incident response and risk mitigation. When malicious IoCs are discovered, XDR should automatically apply blocking rules across the infrastructure from endpoints to public clouds.

Respondent Methodology and Demographics

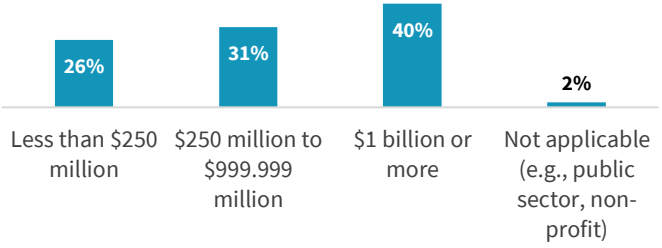
To gather data for this report, ESG conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations in North America (United States and Canada) between October 6, 2020 and October 13, 2020. To qualify for this survey, respondents were required to be IT and cybersecurity professionals personally responsible for evaluating, purchasing, and managing detection and response strategies, processes, and technologies. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 388 IT and cybersecurity professionals.

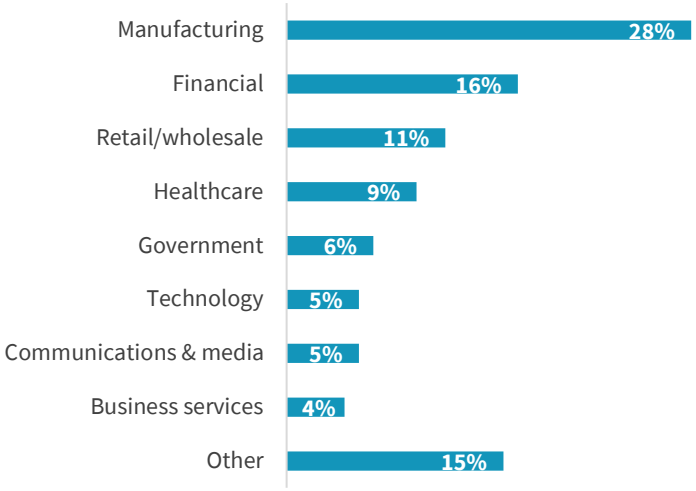
Respondents by number of employees.



Respondents by annual revenue.



Respondents by industry.



Respondents by age of organization.