AVERTIUM

WHITE PAPER

Why You are Missing the Mark if You Think XDR is Only About Technology


While Gartner predicts IT spending will decline by 8% this year...security and risk management (cybersecurity) is predicted to grow 2.4% to reach $123.8 billion in 2020.
- Forbes

Table of Contents

Introduction

Automation technologies promise to expand network monitoring and threat detection capabilities, helping organizations to organize and contextualize risk and threat insights across every layer of the network. The Extended Detection and Response, or XDR, approach uses those technologies to create a more proactive and efficient cybersecurity strategy that's also more comprehensive.

> 54% of organizations are forced to ignore some security alerts and/or events that they believe should really be investigated when security operations can't keep up with the volume of security alerts.
>
> - ESG Research, 2017: Security Operations Challenges, Priorities, and Strategies

Industry-standard definitions of XDR focus squarely on emerging technologies and the extended analytical capabilities they introduce. Technology stacks alone, however, cannot provide the strategic context or level of reasoning and correlation needed to meaningfully evaluate the threat landscape and mitigate exposure. In fact, without additional human expertise, maintenance and analysis, XDR technology stacks run the risk of duplicating (and scaling) the shortcomings of the traditional approaches they are meant to improve upon. In other words, if you think XDR is only about technology – you're missing the boat.

What is XDR?

Today, organizations typically store data in the cloud, share information with third-party vendors and employ a fleet of remote workers, all of which make it increasingly difficult to define the network perimeter. As a result, endpoints have become the new "perimeter," or last line of defense, against cyberattacks. A variety of approaches and technologies, including endpoint detection and response (EDR), security information and event management (SIEM) and managed detection and response (MDR), work together to monitor and secure the entirety of an organization's vulnerability.

EDR, for example, places an agent at each endpoint across an organization's network. The typically large number of endpoints means security teams receive an overwhelming number of individual alerts, which translates to an unmanageable amount of unanalyzed data. Teams are left to sort through these alerts without much context as to which represent an actionable threat, or how to locate and resolve those that are credible. As a result, 54% of professionals ignore alerts worthy of an investigation. Enter XDR. The XDR approach actually involves gathering even more data, sourced from a company's email, servers, networks,

cloud environments, identity management systems, and applications, in addition to endpoint monitoring. The layered approach adds greater context to understand where credible threats are happening. But isn't that even more data to deal with? The approach pairs all that data with analytic tools, including machine learning algorithms, to do the heavy lifting of separating out benign activity, pointing out active threats, and automating protective responses.

XDR is the Best Option, but ...

> "Companies will spend a significant amount of money investing in advanced cybersecurity tools, and then fail to fully configure them. The result is, they don't gain the advantages of what that they bought."
>
> - Paul Caiazzo
> SVP, Avertium

You can reach deeper into the network, and take a more proactive stance against security threats, by adopting an XDR approach within your cybersecurity program. Many XDR technology stacks boast fewer alerts, faster event resolutions and lower costs. With layered monitoring, you can gain greater visibility and control, with the ability to microsegment the network and move more efficiently on actionable alerts. As with any automation tool, perhaps the greatest promise is to your cybersecurity team, who can theoretically regain bandwidth as XDR-powered monitoring and analytics boost operational efficiency.

No matter how much processing and analytic power the platform carries, however, a sizable amount of maintenance and analysis must still take place to make your XDR technology implementation a success. First, if you're considering adopting one of these platforms, it's critical to factor in the significant time and effort required to determine its interoperability with other systems in place, as well as how to configure and integrate it.

Simply failing to properly configure new tools is often a major (preventable) source of network vulnerability, not to mention a waste of budget.

"Companies will spend a significant amount of money investing in advanced cybersecurity tools, and then fail to fully configure them," explained Paul Caiazzo, senior vice president at Avertium. "The result is, they don't gain the advantages of what that they bought,"

Furthermore, without proper integration and configuration, a new platform with an XDR label fails to contribute to the intended multifaceted nature of the approach. For instance, Gartner Research predicts that through 2023 up to 99 percent of all firewall breaches will be caused by misconfigurations, not flaws.

"The mindset behind an XDR approach is creating a fabric of security technologies that work together to produce an outcome. If you don't have that ecosystem viewpoint of how your different security tools work, you're left with a bunch of individual point solutions," Caiazzo said.

Consider the following:

- When was the last time you audited your automated security processes?
- Can you confidently state that none of your security employees is vulnerable?
- Are you confident that your processes are hardened and not vulnerable?
- How comfortable are your security teams with industry-standard automation tooling?

Seasoned security professionals can help you select and configure technologies that best complement your existing systems, while ensuring you attain maximum value. And since they are constantly assessing new tools, they can provide advice on staying current.

But that's just the beginning of the value added by a managed approach to XDR. Not only do these tools require extensive configuration and tuning, they also represent only one piece of the XDR puzzle. Let's explore where human expertise, reasoning, and the analytical process have major roles to play in a comprehensive XDR approach.

Be Realistic – and Holistic

> Hackers attack every 39 seconds, on average 2,244 times a day.
>
> - University of Maryland

The scale and impact of security threats facing companies are no longer manageable by humans. In a RiskBased Security study, 8.4 billion records were exposed in data breaches in Q1 2020, a 273% increase from the same period in 2019. This makes artificial intelligence (AI) the perfect candidate for handling the gathering and analysis of large datasets. AI can gather and process vast amounts of data across thousands of devices and applications, as well as monitor hundreds of potential attack vectors very quickly. This significantly narrows both the manual effort of cybersecurity teams and the number of critical alerts they need to focus on in their daily efforts.

New AI-driven technologies make it possible for people to maintain unprecedented visibility and control over their networks. Relying solely on preset monitoring and automated responses, even if properly configured, however, can have dangerous implications for your organization's security posture. Why? Because the best technical approach is not automatically the socially ideal, recommendable one.

Just as a layered approach to monitoring gives greater context to each potential alert, you need to add strategic context to your tactical "data in context" practices. That way, you can ensure that your efforts align to build a stronger security posture over time.

An initial evaluation can often reveal shadow IT - servers or other network components an organization wasn't aware of that would be left unmonitored by a new platform. A thorough analysis of your organization's threat landscape further helps to establish a baseline for prioritizing alerts and approaches that respond to your specific regulatory requirements, current weaknesses and long-term strategy (including high-level business objectives). Standards like NIST CSF offer a rigorous starting point for evaluating your threat landscape.

Questions to consider:

- Do you understand the full extent of your environment, including the systems, networks, applications and users interacting with data?
- Do you know your organization's baseline? Will your automation tool?
- How can you evaluate the full context of a threat without a baseline against which to measure it?

Let's say, for example, that an initial baseline analysis reveals weaknesses around how your organization handles privilege access management. Perhaps you lack a management tool, or have a lot of users with local administrative privileges. Security analysts can use a framework like MITRE ATT&CK to understand which tactics, techniques and procedures would exploit that weakness, and then select detection strategies to mitigate the immediate risk.

For instance, human experts can assign a higher level of priority to machine alerts indicative of these patterns of behavior. For greater long-term protection, those same experts would guide you toward implementing a privilege access management tool and help your teams understand core security concepts that would minimize privilege in the environment. For all its processing power, the AI platform itself cannot provide that level of context or strategic intervention for your organization.

Interpretation Can be Tricky

Even the most advanced machine learning algorithms cannot offer the level of interpretation necessary for some areas of threat detection. "Even high-quality machine learning is trained to do a very specific thing. Machines can't think laterally – so they cannot take a next step outside their predefined actions," Caiazzo noted.

As threats become more complex and/or human-like, automation software can't detect those subtleties. Advanced social engineering attacks via email, for example, can mirror a regular email correspondence so closely that automated systems struggle to filter them.

Penetration testing is another area in which additional interpretation is needed, as automated services can flag false positives and/or miss other key indicators. The automation can be an efficient first step for filtering, but the results require the review and interpretation of a seasoned security analyst.

A lack of human intervention and analysis can have a major impact given the scalable nature of automation. One mistake becomes a thousand, or a million, and will continue to multiply until someone finally flags it.

Consider this Use Case

A state agency adopted an automated system for managing unemployment claims. The system incorrectly identified 50,000 cases as fraudulent, leading to 30,000 lawsuits. Of the 7,000 cases the agency reviewed by hand, only 8% were actually fraudulent.

Analysts can quickly eliminate false positives, escalate incidents, perform advanced analysis and conduct additional threat hunting to close the gap between automated insights and more complex, lurking threats. The MITRE ATT&CK framework supports those efforts, helping to associate tactics with actions that have been taken in the past by bad actors as well as mechanisms that are effective to detect and mitigate against them.

Armed with this knowledge base, analysts can act on a deeper understanding of the ever-changing threat landscape, combining that understanding with the real-time intelligence of the XDR technology stack.

You Have the Alert. Now What?

It's also important to keep in mind that even with the additional filtering offered by XDR technologies, there will still be a high number of alerts to sort through, particularly when you first implement a stack. Platforms will need additional tuning according to your organization's baseline. From there, alerts continually require additional analysis.

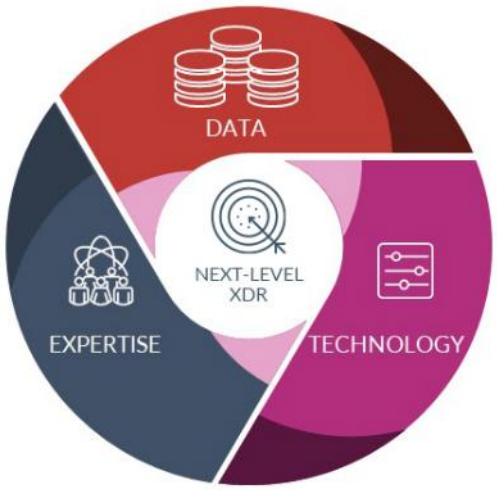
"At the very top of the funnel, you've got billions and billions of events. The machine distills that down to alarms using pattern recognition. And then an analyst takes those alarms and says, does this represent risk or not? And then those alarms become either closed false positives or escalated alerts," said Caiazzo.

With the support of security analysts, you can narrow your team's focus to only those alerts that credibly deserve action. And with the help of tactical and strategic roadmaps based on your

organization's baseline, you have a better sense of which actions are appropriate to mitigate the specific threats involved in those alerts.

Also, remember that some requirements and issues can, and will, outstrip the skillset of your team and call for additional professional consulting. Furthermore, automations can and will fail. The on-call support of managed and professional services adds peace of mind and helps protect against coverage gaps or supplement bandwidth and knowledge in an emergency situation.

Get the Benefits of the Stack – Without the Shortcomings



A technology stack alone cannot fulfill the proactive promise of an XDR approach to cybersecurity. Without the human expertise necessary to think strategically and respond creatively to security insights across your network, you run the risk of replicating the shortcomings of traditional approaches with XDR technology. Namely, you could be left with a number of unactionable alerts, or another "buzz factory" left ignored and poorly maintained. Only this time, the negative consequences of inadequate or inappropriate responses can rapidly multiply, if they're automated.

But what if you could combine best-in-class technologies with human expertise to create a comprehensive approach that captured the benefits of the stack without the shortcomings?

Avertium broadens the definition of XDR by offering a proprietary approach that helps customers address the full spectrum of threats they face. Rather than taking the typical tools-first approach of security providers, we use our broad experience and experience to solve complex cybersecurity problems by leveraging best-in-class toolsets. We start with a health check, centering your organization's baseline and creating an organized effort to heighten your security posture.

By employing certified expertise and broad experience bolstered by carefully selected technology, analysts to sort through alerts, eliminate false positives, analyze and deliver you actionable alerts in context. And with our combined managed and professional service offerings, you can develop the strongest tactical defenses within a long-term cyber strategy.

About Avertium

Avertium, one of the largest cybersecurity services providers to the mid-to-enterprise market, is redefining the landscape with its distinctive show-no-weakness approach. Forged out of three award-winning cybersecurity services companies, each with a unique perspective on the security landscape, Avertium brings enterprise-level security to the many mid-sized and larger organizations that don't have access to comprehensive, specialized protection. More than 2,500 organizations in industries ranging from financial services and manufacturing, to technology and healthcare benefit from Avertium's managed security, consulting and compliance services delivered with more rigor, more relevance, and more responsiveness. The company's dual security operations centers are located in Arizona and Tennessee.

Avertium. Show No Weakness.™

AVERTIUM

© 2020 Avertium, LLC. All rights reserved. MissingMarkXDR_090820

+1 (877)-707-7997
hello@avertium.com
www.avertium.com