CISO Insights | How to Get the Most Out of XDR

August 2, 2022
by Resha Chheda & Michael Leland

Extended Detection and Response (XDR) has generated a lot of buzz in recent times with security practitioners, analysts, and the vendor community. According to the Gartner Hype Cycle™ for Security Operations, 2022, XDR is at peak market interest, promising to deliver significant security visibility and response improvements to threat exposures.

XDR promises to reduce complexity and cost while improving incident response and remediation, and increasing productivity. With so much to gain, it's not surprising that these benefits have at times met with some over-zealous marketing, leaving CISOs and other interested buyers with the unenviable task of sorting through the messaging to understand the true benefits.

Analysts and industry pundits say the potential of XDR is that it can make good on unmet security promises, like those made by SIEM (security information and event management) platforms, accelerating how security teams detect, investigate, and remediate threats with greater productivity and lower ownership costs.

And while many companies are interested in adopting XDR, what should organizations consider as they research the growing number of solutions in the market? Here are three key insights from CISOs we interviewed to help you prioritize as you look to adopt XDR.

Start With an XDR Solution With Roots in EDR

> *"I want to replicate what is working with EDR to other areas in my organization."*

As we talked to different CISOs, one common insight we heard for implementing XDR was extending what works currently in their organization to other attack surfaces–XDR that is based on a solid EDR foundation and all the benefits that brings. That means, for example, drawing on EDR's high-fidelity telemetry to provide critical supporting data from endpoints, as well as the real-time detection and remediation capabilities of EDR.

However, XDR extends beyond endpoint protection to providing detection and response coverage across the entire organization. This means that it provides greater visibility and more context into threats. The high fidelity telemetry that makes EDR so valuable and provides vital supporting data from endpoints, is now available from more sources.

Good EDRs offer real-time behavioral detection and remediation, which can be deployed more broadly across the organization with XDR. Alerts that might otherwise have been missed at an early stage can now be identified earlier and remediated before they have a significant impact. And it is easier to get a more complete understanding of what is happening within the whole enterprise security estate.

Choose an XDR That Increases SecOps Efficiency

> *"One of our key objectives this year is to improve security productivity with built-in controls."*

Look for an XDR solution that increases SecOps efficiency with various built-in integrations that extend functionality and lighten the burden on taxed security teams.

Cybersecurity analysts are already overloaded and the situation is likely to get worse as threats increase, tools proliferate and the skills shortage continues to negatively impact the efficacy of security operations practitioners. That's why it's important to have a tool that automatically correlates related activity into unified alerts, which drastically simplifies the task for analysts. Central to the above points is automation. It's crucial to maximizing the value of your existing tools and to unburdening the SOC team. Automation can improve threat detection, triage and response.

For example, with SentinelOne's threat intelligence integration, threats are auto enriched from various sources, enabling customers to accelerate threat investigation and triage capabilities. Customers can also make use of an extensive library of threat hunting queries curated by SentinelOne research which continually evaluates the latest methodologies to uncover new IOCs and Tactics, Techniques, and Procedures (TTPs).

And all of this can be consolidated into fewer alerts, which reduces the strain on security teams. For example, in the 2022 MITRE Engenuity's ATT&CK Evaluation, which tested leading XDR solutions against a range of benchmarks, SentinelOne's Singularity XDR consolidated two days of continuous testing into just nine campaign-level console alerts. This demonstrates the ability to alleviate SOC burdens by using machine speed to correlate and contextualize large numbers of alerts. In the end, fewer alerts, fewer clicks and fewer screens mean increased SOC efficiency.

Invest in an XDR That Maximizes Existing Security Investments

> *"You are ONE of the many solutions that my SOC uses. Do you play nice with others?"*

A strong XDR solution helps maximize the value of your security investments. While a closed XDR requires the vendor to supply all the required sensors for typical use cases, an open XDR concentrates on backend analytics and workflow and integrates with the organization's existing security controls.

That makes sense because many organizations have tools and technologies deployed in their SOC that it would be wasteful to simply decommission. These best-in-breed technologies provide point solution coverage and each comes with a steep learning curve and operational burden for SecOps efficiency. Switching those out for a new tool simply starts you on another learning curve with a new burden. XDR can allow you to make use of these existing tools, connecting them through simple built-in integrations.

SentinelOne's Singularity Marketplace makes it easy to add integrations to third-party systems such as SIEM or SOAR solutions, with just a few clicks. Email, identity management systems, cloud services and other third-party systems can all be brought into the XDR system, which is a huge improvement on having to secure each one individually and use a different dashboard to manage alerts. These integrations can then be enabled and automated without the need to write complex code.

On top of these benefits is a lower total cost of ownership for the organization. XDR expands the powerful capability to the entire connected ecosystem of security tools across the enterprise. Automated response actions now extend to third-party applications. For example, you can force step-up authentication in your identity management tools when the system detects suspicious behavior. Users will then be asked to submit additional forms of authentication. And you can automatically block email or web connectivity for suspicious resources or users based upon pre-defined rules and triggers. Automated one-click responses serve to reduce adversary dwell time and contain threats quickly.

Seeing Beyond the Buzz for Measurable Outcomes

When choosing an XDR, CISOs need to look beyond the buzz and focus on what really matters: the outcomes it can deliver. Identifying KPIs not only helps to determine the effectiveness of tools and processes but also to communicate that effectiveness to the leadership and board. Cybersecurity is not always something the board understands, but the leadership will be aware of the growing risk of attacks and will want to know that their defenses are aligned with the company's risk profile and appetite.

XDR can improve common KPIs because of its faster, deeper and more effective threat detection and response than individual, disparate tools like EDR and SIEM. Drawing on a wider range of sources means that XDR can improve Mean Time to Detect (MTTD). XDR's central source of information and more manageable alert workload helps to reduce Mean Time to Investigate (MTTI) by accelerating triage and reducing time to investigate and scope. XDR's simple, fast and relevant automation reduces Mean Time to Respond (MTTR) by enabling simple, fast, and relevant automations to quickly contain threats.

Of course, the board is not just concerned with the effectiveness of cybersecurity measures. Its members have to worry about budgets, too. It can sometimes seem as if CISOs are constantly asking for the money to add yet more tools, so XDR's ability to reduce total cost of ownership is welcome. AI and automation mean that security analysts carry less of a burden, which means they can work more efficiently and be more productive.

While it can sometimes be difficult to know how much difference a security tool or platform is making, XDR delivers clear, measurable benefits. It helps reduce costs, increases efficiency and improves visibility across the entire cyber security estate.

Parting Thoughts

The world of cybersecurity is constantly changing and it is often wise to be skeptical about new trends. However, XDR is more than a new trend. It is a new way of thinking about security – a platform that can be deployed to make an organization fit for the modern challenges in the ever-evolving cybersecurity landscape. With teams short of staff and those staff overwhelmed by alerts and drowning in data, a new approach is long overdue. XDR goes beyond the latest marketing buzzwords to deliver meaningful impact for organizations of every size. It is an essential part of the future of the modern SOC.

If you'd like to read more about CISO insights to help you with XDR adoption, read the 5 CISO Best Practices Whitepaper.

To learn more about how the SentinelOne Singularity platform can help your organization achieve these goals, contact us for more information or request a free demo.

Read more about Cyber Security

- More Evil Markets ! How It's Never Been Easier To Buy Initial Access To Compromised Networks
- 7 Ways Hackers Steal Your Passwords
- The Future of CIO and CISO Roles in the Era of AI
- PinnacleOne ExecBrief ! Post-Quantum Cryptography and Enterprise Risks
- EDR vs Antivirus: What's the Difference?
- What Are TTPs? Tactics, Techniques & Procedures – Inside the Mind of a Cyber Attacker