Enterprise Strategy Group
by TechTarget

SOC Modernization and the Role of XDR

The extended detection and response (XDR) megatrend has influenced virtually every security solution provider to participate in some way in the XDR movement, as security strategies require more comprehensive visibility and speed to shut down threats before they cause damage. Beyond better detection and response, XDR is helping IT and security leaders consolidate tools; improve team skills, efficiency, and effectiveness; and support business growth and IT transformation initiatives.

Facing Unprecedented IT Change Velocity, SOC Modernization Is Needed

As IT investments continue to expand and diversify the attack surface, adversaries are quick to find new paths in. Security teams must rethink both proactive and reactive strategies to level up. Advance threats are leveraging both managed and unmanaged entry points to find novel entry points, moving laterally to higher-value targets. Correlating movement through email, endpoint, and cloud requires deep network insights and integrated analytics capable of detecting attacks designed to evade local controls. Most SecOps teams see more data, more automation, and better analytics as the path forward.

» Security Operations Environment Opinions

89%
agree that their organization would benefit from collecting, processing, and analyzing more data.

80%
are still dependent upon numerous disconnected analytics engines and point tools.

78%
are still dependent upon numerous manual processes.

67%
think it is difficult for their organization to keep up with and/or remediate the wide variety of security alerts generated by their security analytics tools.

Advanced Threats Are Challenging Even the Most Sophisticated Security Teams

Despite continued investment in new and improved security mechanisms, advance threats are finding a path around them. Misconfigured cloud resources, stolen credentials, privilege escalation, and unpatched vulnerabilities are among the many avenues involved. "Human-assisted" paths involving phishing and other impersonation techniques used across email and other collaboration tools further help evade security controls. Security teams need a more integrated, automated approach to keep up.

Multi-vector, socially engineered attacks are becoming commonplace, with

more than half
of organizations reporting weekly (36%) or even daily (16%) attack frequency.

XDR: More than Just Another SecOps Tool

XDR unifies control points, security telemetry, analytics, and operations into one enterprise system capable of improving all aspects of security operations, including preparation, investigation, containment, eradication, and post-incident analysis. While many organizations are leveraging XDR solutions to consolidate two or more earlier implementations, for many, XDR will supplement current security operations tools.

52%
of organizations believe **XDR will supplement** current security operations technologies.

44%
XDR will help to consolidate current security operations technologies into a common platform.

XDR Is Being Applied to Many Use Cases

Respondents to a research survey by TechTarget's Enterprise Strategy Group most commonly reported that their organizations were prioritizing an XDR solution that could:

Help prioritize alerts **based on risk.**

Improve the detection of **advanced threats.**

Offer more efficient **threat or forensics investigations.**

Act as a layered addition to existing threat detection tools in order to identify advance or more complex threats.

Reinforce security controls and **prevent future similar attacks.**

Consolidate disparate tools into a common, simplified threat detection and response architecture, streamlining incident response workflows.

"**More than just a detection and response operational tool,** XDR solutions are helping organizations gain new levels of visibility into risk and threats, detect and mitigate advance threats, and improve operational efficiency and analyst retention. Collectively, XDR is helping SOC teams operate more efficiently, while improving overall security posture, program scalability, and team satisfaction."

- Dave Gruber, *Principal Analyst, Enterprise Strategy Group*

Conclusion

XDR investments are contributing to many critical business outcomes and strengthening overall security posture while increasing team throughput. Enterprise Strategy Group recommends that security leaders take the time to explore how and why XDR solutions from security platform providers such as Cisco Systems can strengthen security outcomes, improve the overall scalability of security investments, and help consolidate security tools reducing cost and complexity.

LEARN MORE

cisco

Source: Enterprise Strategy Group Research Report, *2022 SOC Modernization and the Role of XDR*, October 2022.
Source: Enterprise Strategy Group Research Report, *Challenges in Securing an Overabundance of Communication and Collaboration Tools*, July 2023.