ESG a division of TechTarget | Enterprise Strategy Group | Getting to the bigger truth.™

SOC Modernization and the Role of XDR

Security operations demand massive scale to collect, process, analyze, and act upon massive amounts of data. Early XDR was anchored to two primary data sources: endpoints and networks. While this was an improvement on disconnected EDR and NDR tools, threat detection and response across enterprise organizations demands a wider aperture. In order to modernize security operations centers and keep up with the volume of security alerts, large organizations need advanced analytics.

Security operations remain challenging.

52% of organizations believe that security operations are more difficult today than they were two years ago.

Top 3 reasons security operations are more difficult today than they were two years ago.

41% The threat landscape is growing and changing rapidly.

40% The attack surface has grown.

39% The attack surface is continuously changing and evolving.

Most common action planned to improve security operations over the next 12–18 months: Purchase security operations tools designed to help automate and orchestrate security operations processes.

SecOps process automation investments are paying dividends.

Most commonly realized benefits from security operations process automation.

51% Improved threat detection using playbooks

49% Improved mean time to respond

44% Improved incident prioritization

44% More quickly isolated assets

43% Faster escalation of critical issues

38% Improved staffing throughput

MITRE ATT&CK framework is proving valuable for most.

Usage of MITRE ATT&CK framework for security operations.

48% Extensive use

41% Used to a limited extent

Importance of MITRE ATT&CK framework to security operations.

XDR momentum continues to build.

Familiarity with XDR technology.

61% Very familiar

37% Somewhat familiar

Most common challenge driving XDR interest: Current tools struggle to detect and investigate advanced threats (51%).

Five highest priority XDR use cases.

MDR is mainstream and expanding.

Use of managed services for security operations.

37% We use managed services for a majority of our security operations.

48% We use managed services for a portion of our security operations as an extension of our internal resources.

11% We use managed services only in a limited capacity as an extension of our internal resources.

Top 3 reasons behind usage of or plans for managed services for security operations.

LEARN MORE For more from this study, read the ESG Research Report, *SOC Modernization and the Role of XDR*.

ESG Research Report, SOC Modernization and the Role of XDR, October 2020