Mighty Guides | ANOMALI

7 Experts on Extended Detection and Response

KEY ADVICE FROM THE EXPERTS

1 **XDR solutions should integrate with your existing security stack to correlate local telemetry with global threat intelligence while integrating automation and artificial intelligence engine to help produce high fidelity actionable alerts.**

Automation and big data management are needed to collect data across all installed security telemetry, along with advanced intelligence to understand and correlate threats.

MARK ALBA
Chief Product Officer, Anomali

2 **Threat intelligence, aided by visualization in threat frameworks such as MITRE ATT&CK, contextualizes alerts to better inform decision-making.**

When threat intelligence is incorporated into the XDR framework, this reduces the need for extra labor in an area that has traditionally suffered from a shortage of highly skilled staff.

DAVE RUEDGER
CISO, Invitae

3 **Overloaded security teams must keep pace with the modern threat landscape against a backdrop of digital transformation, talent shortages, and cost constraints.**

The pandemic brought a massive expansion in which locations, devices, and people make up the new enterprise perimeter. Now malicious actors are utilizing new attack vectors to get inside. XDR solutions integrate automation which helps improve organizational efficiency to keep track of the ever growing threat landscape.

DMITRIY SOKOLOVSKIY
VP and CSO/CISO,

4 **XDR should help break down silos between SOC, IR, and CTI teams. By mapping threat intelligence throughout the platform and across your organization, a good XDR solution will help your business more thoroughly understand where security controls are the most crucial.**

XDR offers a synergistic platform for CTI, SOC, and IR teams to function as a single entity with shared goals, processes, and continuous improvement from lessons learned. Expanding to Red Team, Fraud, Physical Security, DevOps, SRE, and related teams is a further force multiplier in successful XDR implementations.

LANCE AUMAN
Lead Security Engineer, iHerb

5 **A vendor-agnostic XDR solution capable of integrating with and augmenting your existing (and prospective) security investments is essential.**

I've already made significant investments in security tools, and need something to make them better. XDR collects threat pointers and telemetry from multiple technologies, regardless of vendor, and builds a threat intelligence ecosystem. Then it provides actionable steps to alert on or block the identified risks.

GENADY VISHNEVETSKY
CISO, Stewart Title

6 **Extended Detection and Response (XDR) is an evolution beyond signature based anti-malware, driven by a core of automation and threat intelligence.**

Analysts have a tremendous amount of data coming in from many sources, which is time- and resource intensive to analyze. XDR automatically correlates data from many disparate sources, which helps analysts prioritize their actions, improving detection and response time.

KONRAD FELLMANN
VP and CISO, Cubic Corporation

7 **XDR is a key and revolutionary advance needed to continue to transform cybersecurity to keep up with today's sophisticated attackers to drive reduced risk and heightened defense.**

XDR is a must-have tool for every security team with a clear ROI to the business. It saves money while reducing risk, one of the few "win-win" solutions out there when it comes to investing in security solutions.

MICHAEL MARSCHEAN
CIO, Subcom

Anomali's cloud-native extended detection and response (XDR) solution automatically correlates ALL security telemetry against active threat intelligence to enable organizations to understand what's happening inside and outside their network to quickly identify threats and effectively respond.

To hear more from the experts, download our ebook here.

To learn more about how Anomali can help you visit us at anomali.com.

Mighty Guides

Sponsored by ANOMALI