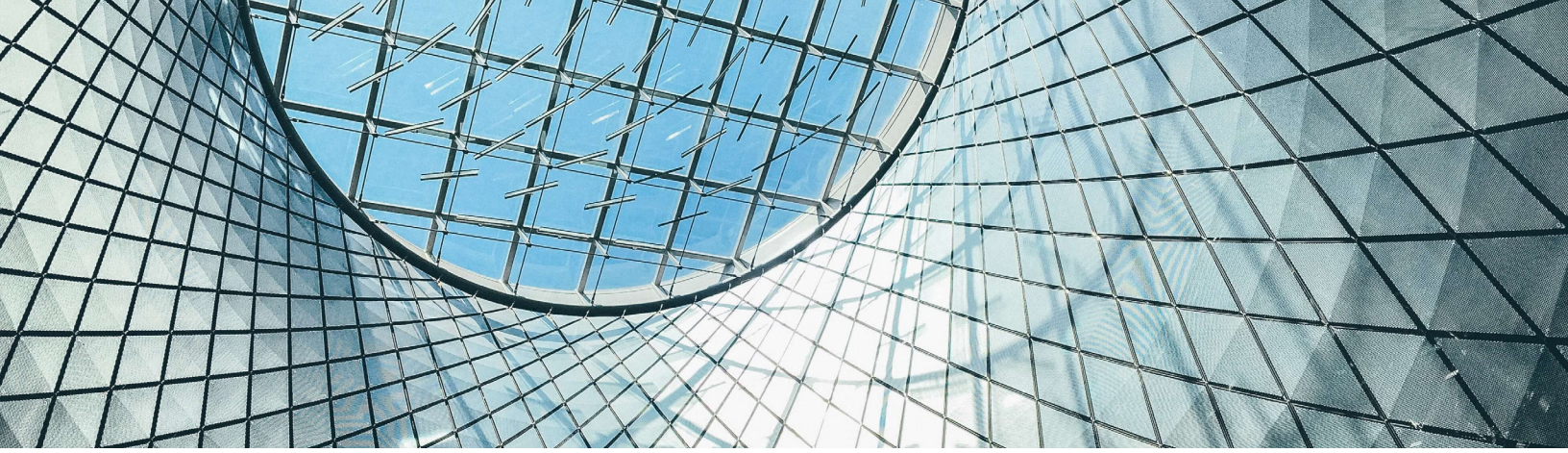

Market Insight Report Reprint

Here to stay: Threat detection and response reaches an inflection point

Highlights from VotE: Information Security

September 8 2022

by Scott Crawford, Megan Goodwin

While SIEM remains an anchor of security operations, threat detection and response is changing the status quo. For the first time in our surveys, it has become the top technology to combine with SIEM/security analytics, while managed threat detection and response services gain ground as well.

451 Research

S&P Global
Market Intelligence

Introduction

Our Voice of the Enterprise: Information Security, Security Operations 2022 survey takes a look at trends in security operations (SecOps) technologies and services. It extends our prior research on the importance given to these offerings, their attributes and the capabilities they give organizations for countering the threat landscape.

THE TAKE

Threat detection and response continues to reshape the status quo in security operations. For the first time, extended detection and response (XDR) is the most cited category of technology to combine with security information and event management/security analytics, edging out threat intelligence, albeit only slightly. While SIEM remains an anchor of SecOps, threat detection and response has become a top choice not only for technologies but through managed services, as well. Some might argue that threat detection and response was always an aspect of SIEM/security analytics. While that may be true, the evidence of adoption points to the impact that these newer entrants have had on the field. Offerings focused on multiple capabilities in this arena are an aspect of the SecOps market that is here to stay.

Summary of Findings

XDR has become the most frequently reported augmentation to SIEM/security analytics. In our prior Voice of the Enterprise: Information Security studies, threat intelligence had often been cited as a top technology to combine with SIEM/security analytics — and often by a wide margin. In our 2021 Information Security, Vendor Evaluations study, threat intelligence was cited by 49%, and incident response workflow came in at a distant second at 36%. In our 2022 survey, the top spot goes to XDR, but narrowly. At 43% of respondents, XDR edges out threat intelligence tools or feeds by a single percentage point, but it is an inflection point regardless, marking a milestone in the increased impact of threat detection and response on security operations.

For centralized security analytics, SIEM remains the anchor, while endpoint detection and response (EDR) leads in detection and response — with a strong showing for managed services. When asked what technologies organizations were using as part of their centralized analytics platform for security operations, SIEM continues to lead with 44% of respondents. EDR, however, comes in a close second at 41%. The next-most-frequent response, however, points to the priority given to the services option, with 33% saying that managed detection and response services are part of their centralized security analytics.

When it comes to the SIEM/security analytics vendors, quality of output remains preeminent, and integration of threat intelligence a high priority. Quality of reports and alerting, the integration and correlation of threat intelligence, and the ease of setup, implementation and tuning remain the top three attributes of an SIEM/security analytics vendor to our respondents in 2022. They remain ranked in that order when rated by respondents as very important when compared with the 2021 study mentioned above. The integration of advanced analysis methods, including machine learning and behavioral analytics, meanwhile, has gained ground in 2022, with 51% of respondents calling it very important compared with 41% in 2021.

The majority cite alerting for cloud assets as very important. Fifty-eight percent of respondents say that SIEM/security analytics vendor support for alerting on architectures beyond on-premises (e.g., cloud, IaaS and SaaS environments) is very important, with another 36% calling this attribute somewhat important. This suggests the opportunity not only for IT observability in security operations, but also for the need for expertise in cloud-native environments on security operations teams.

Despite progress, SecOps teams still struggle with alert overload. The average (mean) percentage of alerts generated by security analytics that respondents say they are unable to investigate on a typical day is 48%. This number has increased from 41% in the 2021 study cited earlier. While detective and analytical technologies are making inroads in optimizing security operations, the growing reach and complexity of technology continues to press secops teams. This, however, also likely drives further interest in managed detection and response services.

CONTACTS

The Americas
+1 877 863 1306
market.intelligence@spglobal.com

Europe, Middle East & Africa
+44 20 7176 1234
market.intelligence@spglobal.com

Asia-Pacific
+852 2533 3565
market.intelligence@spglobal.com

www.spglobal.com/marketintelligence