



## 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

This report, licensed to Swimlane, developed and as provided by S&P Global Market Intelligence (S&P), was published as part of S&P's syndicated market insight subscription service. It shall be owned in its entirety by S&P. This report is solely intended for use by the recipient and may not be reproduced or re-posted, in whole or in part, by the recipient without express permission from S&P.

## 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](mailto:market.intelligence@spglobal.com)

### Europe, Middle East & Africa

+44 20 7176 1234

[market.intelligence@spglobal.com](mailto:market.intelligence@spglobal.com)

### Asia-Pacific

+852 2533 3565

[market.intelligence@spglobal.com](mailto:market.intelligence@spglobal.com)

[www.spglobal.com/marketintelligence](http://www.spglobal.com/marketintelligence)

Copyright © 2022 by S&P Global Market Intelligence, a division of S&P Global Inc. All rights reserved.

These materials have been prepared solely for information purposes based upon information generally available to the public and from sources believed to be reliable. No content (including index data, ratings, credit-related analyses and data, research, model, software or other application or output therefrom) or any part thereof (Content) may be modified, reverse engineered, reproduced or distributed in any form by any means, or stored in a database or retrieval system, without the prior written permission of S&P Global Market Intelligence or its affiliates (collectively, S&P Global). The Content shall not be used for any unlawful or unauthorized purposes. S&P Global and any third-party providers, (collectively S&P Global Parties) do not guarantee the accuracy, completeness, timeliness or availability of the Content. S&P Global Parties are not responsible for any errors or omissions, regardless of the cause, for the results obtained from the use of the Content. THE CONTENT IS PROVIDED ON "AS IS" BASIS. S&P GLOBAL PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, FREEDOM FROM BUGS, SOFTWARE ERRORS OR DEFECTS, THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED OR THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION. In no event shall S&P Global Parties be liable to any party for any direct, indirect, incidental, exemplary, compensatory, punitive, special or consequential damages, costs, expenses, legal fees, or losses (including, without limitation, lost income or lost profits and opportunity costs or losses caused by negligence) in connection with any use of the Content even if advised of the possibility of such damages.

S&P Global Market Intelligence's opinions, quotes and credit-related and other analyses are statements of opinion as of the date they are expressed and not statements of fact or recommendations to purchase, hold, or sell any securities or to make any investment decisions, and do not address the suitability of any security. S&P Global Market Intelligence may provide index data. Direct investment in an index is not possible. Exposure to an asset class represented by an index is available through investable instruments based on that index. S&P Global Market Intelligence assumes no obligation to update the Content following publication in any form or format. The Content should not be relied on and is not a substitute for the skill, judgment and experience of the user, its management, employees, advisors and/or clients when making investment and other business decisions. S&P Global Market Intelligence does not endorse companies, technologies, products, services, or solutions.

S&P Global keeps certain activities of its divisions separate from each other in order to preserve the independence and objectivity of their respective activities. As a result, certain divisions of S&P Global may have information that is not available to other S&P Global divisions. S&P Global has established policies and procedures to maintain the confidentiality of certain non-public information received in connection with each analytical process.

S&P Global may receive compensation for its ratings and certain analyses, normally from issuers or underwriters of securities or from obligors. S&P Global reserves the right to disseminate its opinions and analyses. S&P Global's public ratings and analyses are made available on its websites, [www.standardandpoors.com](http://www.standardandpoors.com) (free of charge) and [www.ratingsdirect.com](http://www.ratingsdirect.com) (subscription), and may be distributed through other means, including via S&P Global publications and third-party redistributors. Additional information about our ratings fees is available at [www.standardandpoors.com/usratingsfees](http://www.standardandpoors.com/usratingsfees).