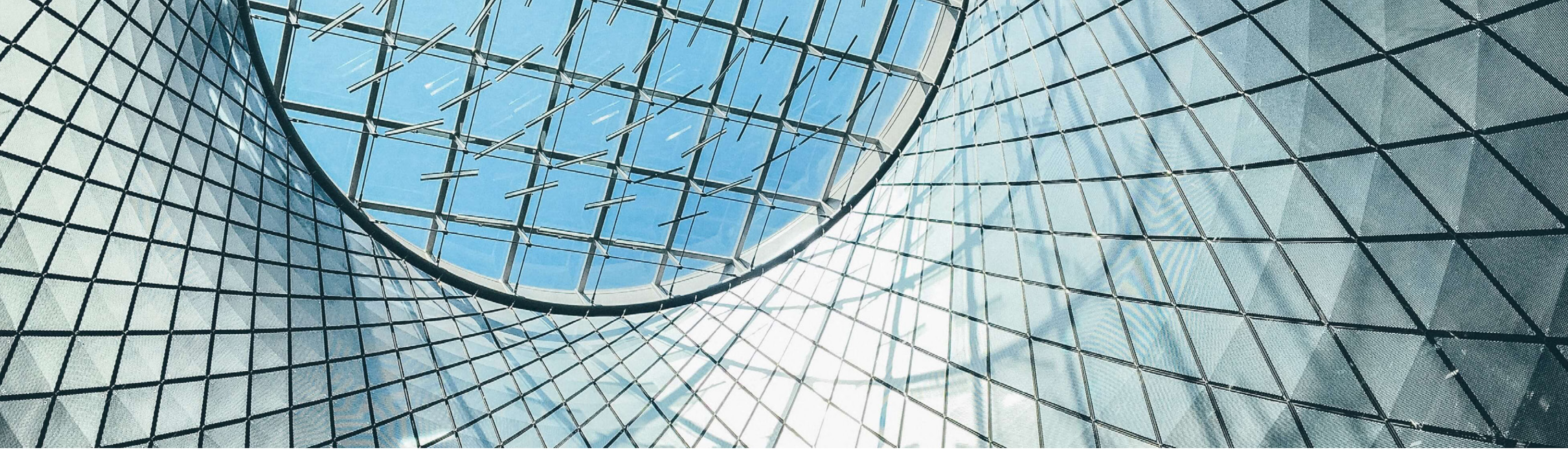

451 Research Market Insight Report Reprint

Tectonic shifts in the SIEM landscape create disruption in the market

May 23, 2024

by Scott Crawford, Brenon Daly

A series of transformations in security information and event management recently culminated in two high-profile deals that drew the market's challenges into stark relief. Meanwhile, for the first time since we have asked organizations what percentage of security alerts they are unable to investigate in a typical day, more than half said over 50%. We examine the factors behind these developments.

S&P Global
Market Intelligence

Introduction

A number of disruptions and realignments in the security information and event management market — long an anchor of security operations — culminated recently in a pair of deals that marked a generational turning point in this segment. In a single day, Thoma Bravo-backed LogRhythm announced its acquisition of Exabeam, consolidating the two competitors in a deal charitably described as “unusual,” while IBM Corp. announced its intent to divest its QRadar SaaS business to Palo Alto Networks Inc., where the intended destination for QRadar SaaS customers will be Palo Alto’s Cortex XSIAM.

THE TAKE

What is behind the disruption? Our data indicates that the challenge of responding to potential threats has become overwhelming. Over the years, our VotE surveys have been asking organizations to estimate the percentage of security alerts they cannot investigate in a typical day. In 2023 — for the first time since we have asked the question — more than half of respondents told us that the number exceeded 50%. Factors that contribute to the scale and complexity of this problem include the technology landscape and (for some) the nature of investment. However, people remain the overarching challenge. Human interaction with technology has itself become a target; meanwhile, the sourcing, training and retention of security expertise remains daunting. Simply put, cybersecurity has grown beyond being a human-scale problem. Although the current (or even next) generation of technology may not provide a solution, threat detection and response will have to rise to the occasion, and in ways that organizations can actually afford. Today’s market could bear little resemblance to what is to come.

Context

Signs of disruption were appearing well before the landmark Cisco Systems Inc.-Splunk deal in August 2023. In June 2022, Devo Technology fielded a down round of funding and swapped out its CEO. A year ago, Francisco Partners took Sumo Logic private for $1.7 billion, after Sumo lost two-thirds of its market value from its post-IPO peak.

On May 15, things took a turn for the dramatic: First, LogRhythm, a 21-year-old vendor controlled by buyout firm Thoma Bravo, announced its purchase of heavily venture-funded Exabeam. The former competitors have differing origin stories that map out key aspects of the evolution of security information and event management (SIEM). As its brand implies, LogRhythm arose to offer an alternative to approaches that had long been predicated on log data, while Exabeam started out in user and entity behavior analytics (UEBA) for greater visibility into identity-linked activity that could pose a threat. Although terms of the deal were not disclosed, we understand Exabeam is being consolidated at a discount from its last private market valuation of $2.4 billion.

Second, Palo Alto Networks and IBM announced a partnership that includes Palo Alto’s acquisition of IBM’s QRadar SaaS business and all related assets (security orchestration, automation and response, endpoint detection and response, attack surface management, and X-Force threat intelligence SaaS offerings). The partners will facilitate the migration of existing QRadar SaaS customers to Palo Alto Cortex XSIAM, while offering an earnout to IBM for customers that move on-premises QRadar deployments (a substantial share of QRadar customers) to XSIAM.

Palo Alto also intends to incorporate IBM’s watsonx generative AI capabilities into XSIAM, part of its response to major competitors investing in GenAI for SecOps. The move signals IBM’s departure from a market where it once challenged leaders, beginning with its acquisition of QRadar parent (at the time, also an SIEM disruptor) Q1Labs in 2011. For Palo Alto, the deal creates an opportunity to win QRadar customers to XSIAM without having to organically generate leads against a competitor. It also takes the prospect’s objection of abandoning its investment in the incumbent off the table, since the incumbent is retiring from the field.

Together, these strengthen Palo Alto's hand against Microsoft Corp. and Cisco (with its Splunk acquisition), and further add to Palo Alto's challenge to competitors across a range of threat detection and response technology. IBM, meanwhile, can raise cash from the sale of an asset that is no longer strategic to its goals — particularly in light of its HashiCorp Inc. acquisition that focuses squarely on a substantial player in tools and practices for building and running cloud-native environments. Accordingly, IBM plans to expand its relationship with Palo Alto's Prisma portfolio in cloud-native application protection platforms.

For customers, some of these moves are a major disruption. The alignment of Cisco with Splunk users and their distinctive community culture was an open question when that deal was announced. For IBM's QRadar SaaS customers, the shift is even more dramatic. It is also not without considerable risk — QRadar customers have been put on notice that they will be moving off that product. What is to keep them from considering other choices, particularly at this inflection point, when numerous options have turned SecOps into a virtual smorgasbord? Palo Alto's bet is that, despite that risk, there's more to be gained here than not, especially if IBM has already decided to turn away from the field.

The tech factor

At its core, cloud-native IT can spin up and scale with high elasticity in response to changing demand, throwing off data in unprecedented volumes. However, in the distributed environment, the ability to detect and respond to threats means "four wheeling" across a varied landscape, which further complicates the problem. Organizations need to find a way to handle security monitoring/response for both. Compounding the issue, many approaches to threat detection still do not incorporate native telemetry gathered directly from points of observation. User interfaces and experiences must be adapted to specific use cases, which often means that multiple techniques must be incorporated into an enterprise security operations center (SOC).

Many approaches to gathering and analyzing data on potential threats, then turning data into insight that supports action, reflect the challenge that existed before these factors became reality. Seconds count now, yet in too many cases, dwell or response times are measured in days, if not weeks or months. Meanwhile, as noted earlier, people are a concern on two fronts. Attackers recognize human interaction as more exploitable than technology; while developing and retaining skills in the SOC presents difficulties of its own.

These factors have forced organizations to rethink their investment across the SecOps landscape. Much attention has focused on innovations in AI, but SecOps technicians have been leveraging machine learning and behavioral analytics for many iterations. As a practical matter, the high cost of dedicated SIEM storage (for example) has created an opening for more affordable options, such as data transformation and pipeline plays that would "decouple" telemetry from storage and user interfaces, enabling organizations to store what they want, where they want, integrated with user tools best fitted to use case. Platform providers can offer integrations of what they regard as the most attractive combinations.

We have already covered these trends in SecOps architecture. While change often comes at a cost, those affected by the tectonic shifts in the SIEM landscape may be forced to rethink their entire investment.

The money factor

If technology challenges are fueling the SIEM shakeup, funding over the last few years has taken the trajectory toward too much cheap money, secured by overvaluation that cannot be met by actual business performance. For some of the pure plays, this means their valuations have evaporated, along with the money they supposedly justified. When additional funding is needed, the outlook for future rounds looks discouraging, leading to more bargain-hunting M&A. SIEM, of course, is not the only market affected by this development. The failure of the rumored Wiz-Lacework deal is a stark example, with Lacework having raised roughly $2 billion from venture investors.

LogRhythm-Exabeam, however, brings added complications for the financial acquirer. The integration will push out any return that Thoma Bravo could make on its six-year-old investment. Given the vintage of its original purchase, the company has booked a paper gain on LogRhythm (our understanding is that the buyout shop paid $525 million, or just 4x trailing sales, in the LogRhythm recap).

Today, LogRhythm and Exabeam have complementary technologies representative of SIEM's longstanding combination of UEBA (where Exabeam began) with log-based analytics. But exiting the combined investment would seem to require challenging product rationalization and operational realignments — another example of how incumbents must adapt to a changing landscape.

What comes next?

Where the technology goes from here is a vital question. The SIEM market may be transforming, but it is far from a death knell for security operations. What we see instead is generational change, with one major difference — the scale and complexity of the security challenge is significantly different now, meaning approaches to tackling it will reflect the transformations reshaping the technology industry itself.

SIEM up to now has been less a stand-alone market than an aspect of SecOps, but it is perhaps better characterized as a combination of data collection and analytics for many types of security-relevant data. Customers seek outcomes, and SIEM aims to address this expectation in areas ranging from compliance obligations to having near-real-time insight into threats that actually merit a prioritized response. That is the "why." The "how" has largely focused on centralizing data and supplying tools for analysis and action.

Vendors will need to more effectively explain the "how" with respect to five hurdles (at least):

- The massive volumes of data generated by modern technology, particularly by cloud-native assets, and an expanding attack surface must be coped with; at the same time, vast amounts of data generated by on-premises and legacy technologies need to be accommodated.
- The time and performance of effective detection and response must be accelerated, no small feat given the scale and complexity of assets at risk and potential threats.
- Vendors have to embrace modern digital architectures and techniques, not just lift-and-shift legacy approaches.
- Knowing what "larger than human scale" really entails means relying on more than generative eye candy. GenAI captures attention, and has its place in SecOps, but it is not the only aspect of ML evolution that could introduce opportunity for companies that show they understand the problem.
- Organizations will need to be enabled to strike the right balance between human and machine involvement. The explosion in scale aside, cybersecurity fundamentally remains a human problem, with adversaries looking to exploit weaknesses to achieve human objectives, and defenders required to make the most effective use of valuable expertise. Service providers have a significant role to play here.

In upcoming reports, we will be exploring these themes and looking at examples of the vendors that are taking on the challenges.

CONTACTS

Americas: +1 800 447 2273
Japan: +81 3 6262 1887
Asia-Pacific: +60 4 291 3600
Europe, Middle East, Africa: +44 (0) 134 432 8300

www.spglobal.com/marketintelligence
www.spglobal.com/en/enterprise/about/contact-us.html

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 keeps certain activities of its divisions separate from each other 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 nonpublic 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 (free of charge) and 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.