Cool Vendors in Security Operations

Published 18 June 2021 - ID G00746492 - 16 min read

By Analyst(s): Toby Bussa, Mitchell Schneider, Kelly Kavanagh, John Collins, Craig Lawson, Pete Shoard

Initiatives: Security Operations

Organizations struggle to obtain visibility of where IT operates, awareness of exposures, and the ability to detect and respond to threats. These cool vendors focus on innovative ways to support security operations through the use of automation and counterintuitive approaches.

Overview

Key Findings

- Digital environments have wider scales and higher rates of change, and they are often not controlled by IT, which causes stress for security operations.
- Automating cybersecurity operations activities is still impractical for a majority of organizations, and as a result, most are insufficiently protected and unable to defend against current attacks.
- Security technology and services vendors rarely incentivize customers to do better and improve their cybersecurity operations.

Recommendations

Security and risk management leaders should:

- Use all available data sources to improve incident investigation and response, and threat hunting capabilities. A decentralized approach may be faster to implement, more efficient and more cost-effective compared with using a traditional, centralized log management approach.
- Select security services providers that incentivize customers to improve security and reduce risk, rather than service providers with prices that are indifferent to the customer's investment in maturing their security operations capabilities.

- Use automation to help scale internal testing capabilities and free up time for human testers to focus on areas that are too risky to automate and that require organizational and system-specific expertise.
- Implement automation in as many security operations activities as possible by using no-code solutions — which will be easier to implement for a majority of enterprises and organizations.

Analysis

This research does not constitute an exhaustive list of vendors in any given technology area, but rather is designed to highlight interesting, new and innovative vendors, products and services. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

What You Need to Know

Organization's struggle to protect and defend themselves against an increasing volume of hostile attackers, and across an increasing number of environments. Organizations must have a foundational set of security operations functions. However, those organizations that want to avoid security failure must be willing to change their approach, adapting their people and processes, and experimenting with new technology and service approaches. Security and risk management leaders need:

- Visibility beyond existing risks and threats to an organization, encompassing those that are still emerging. As organizations undertake digital transformation initiatives, become cloud-first, and adapt to external forces that stress organizational resiliency, new risks and threats will pose new challenges.
- Awareness of the exposures in new environments and of how solutions can be abused by attackers.
- A 24/7 ability to detect and respond to threats in real-time, as and when they occur — to shut them down before they can harm the organization.

Technologies and services alone will not help security operations teams better protect and defend themselves, but they are an important part of an organizations' security operations capabilities.

Where technologies and services are required, those leading security operations functions should use two approaches:

1. Implement and embed sustainable automation across security operations functions.

2. Embrace security solutions and services that take counterintuitive approaches to current challenges.

Security operations teams need to be willing to embrace less established vendors and service providers, acknowledging that there are both risks and rewards to this approach.

This requires having a backup plan in the event the vendor goes out of business or is acquired, and putting additional resources into maximizing the relationship with the vendor. Ultimately, this can allow customers and vendors to help drive the direction of the product where it would benefit both parties.

Query.AI

Brookings, South Dakota, U.S. (query.ai)

Analysis by John Collins and Toby Bussa

Why Cool: Query.AI is cool because it disrupts conventional thinking about centralizing security data. Big data lakes and central data stores have been the trend in security for several years, but Query.AI challenges this approach — asking why bring all the data to one location if you can search it where it resides? Query.AI provides a security investigations control plane to deliver a virtual data layer through a browser for data access, investigation, and response. This allows for federated searches, dashboards, reporting and correlation, eliminating the need for data centralization.

This decentralized data solution addresses several challenges faced by security teams, such as those around:

1. Owning and maintaining a central log management solution or a security data lake — and ensuring that the data sources are connected and supplying the central repositories with logs and data.

2. Data privacy and sovereignty issues — by keeping all the data in-country or region. Query.AI can deliver this functionality because they do not require a client to send them data and they never have access to the data. All queries occur via API connections spawned in the user's browser, where it is translated into a target data source search script. For on-premises or legacy platforms with limited API support, a proxy docker container brokers the connection to heavy software development kits (SDKs), Open Database Connectivity (ODBC) and available APIs.

3. Support for using multiple security information and event management (SIEM) solutions (for example, when migrating from one to another) or multiple log repositories across an organization. For example, such support may be required if the security operations team is investigating an incident and needs to query their SIEM solution, the infrastructure and operations (I&O) team's logging tool, and logs that are not centralized (such as those that are stored in cloud infrastructure and platform services [CIPS]).

One of the biggest challenges that security operation teams face, particularly with threat hunting and incident response, is speed and access to data repositories. Query.AI's product features natural language processing (NLP), giving security analysts, threat hunters and incident responders the ability to tell Query.AI what they want to search for, and where, without having to type anything. Out of the box, Query.AI provides more than 550 workflows for investigations and hunting. These workflows are created by Query.AI and their customers in a crowdsourcing mode. The community features give users the option to share or make their workflows private.

Challenges:

- Query.AI does not fit perfectly into any existing solution category for security operations (SecOps). This can present issues when asking for the budget to purchase the solution if an influencer or buyer cannot articulate how it will add value to existing security controls.
- Query.AI is on a continuous journey to support more data sources. This will come with time, but organizations with custom-built or lesser-known data storage solutions will have to investigate whether Query.AI does or can support their environments and data stores.

Who Should Care: Query.AI will appeal to organizations with highly distributed and decentralized data stores, as well as organizations that have to address data residency requirements. Threat hunters and incident responders looking for increased speed and efficiency across cloud and on-premises environments where different data stores exist, will benefit from Query.AI's approach. Organizations looking to reduce storage cost and use a tool for their existing scattered data locations should consider Query.AI too.

Quorum Cyber

Edinburgh, U.K. (quorumcyber.com)

Analysis by Kelly Kavanagh and Craig Lawson

Why Cool: Quorum Cyber's novel approach to the market is to offer discounts based on customer adoption of recommended security controls and practices. As customers reduce their cyber risk through program maturity, they can reduce the costs of security operations center (SOC) services provided by Quorum Cyber.

Quorum Cyber's managed detection and response (MDR) services, Azure Sentinel SOC and MDR, are built on threat detection content and response playbooks deployed in the customer's Azure tenancy. Typically, MDR providers deliver services through a platform that they manage, and the detection and response content that they develop. When an MDR provider and customer end their relationship, the platform and content are no longer available to the customer. Quorum Cyber's offering provides that content in the customer's environment, available for use after the service relationship is ended.

Quorum Cyber's comprehensive services include 24/7 monitoring, detection and threat validation, phishing protection, vulnerability management, red team ATT&CK simulation and threat modeling, incident response and threat hunting. Coverage for monitoring includes the event sources and security technologies integrated with the Microsoft Azure Sentinel product, as well as a variety of other existing integrations into the Quorum Cyber platform. Quorum Cyber also has a dedicated team of developers that can create new connectors as part of their service. Customer insight into these services is provided by Quorum Cyber's Clarity portal.

Engagements are via subscriptions — including monthly options — with pricing based on number of staff and number of signals monitored.

Challenges:

- The MDR market is crowded with service providers ranging from large, well-known security product and services brands, to small, boutique providers. Standing apart from the competitors is challenging, as nearly all claim fast, comprehensive detection and response capabilities.
- Quorum Cyber will have to demonstrate the effectiveness of its services and the advantages of its delivery model over time.
- By allowing more portability through their service delivery model (for example, the customer owns the Azure Sentinel instance), Quorum will have to sustain high customer satisfaction in order to avoid customers changing service providers.
- Quorum Cyber's capabilities are deeply integrated with and dependent upon Microsoft's security products. They are both enabled and constrained by the capabilities and market success of Microsoft's products.

Who Should Care: Security and risk management leaders with significant current or planned investment in Microsoft security products and the Azure platform will be increasingly interested in how Microsoft's security tools and Azure Sentinel might fit into their threat detection and response program. Quorum Cyber should be of interest because:

- The relative newness of the Sentinel platform, and the complexity of developing detection and response content in it (or any SIEM or security orchestration, automation and response [SOAR] solution), can be addressed via managed services for security detection and response.
- Organizations may be able to offset the costs of improving security program maturity with the reduced costs for managed detection and response services.

Randori

Waltham, Massachusetts, U.S. (randori.com)

Analysis by Mitchell Schneider

Why Cool: Randori is cool because it unifies external attack surface management (EASM) and continuous, automated red teaming in a single platform. Randori's product covers all the way from the reconnaissance phase through to launching campaigns to emulate attacks against an organization, without the need for the organization to have expertise in red teaming. Randori's platform consists of two modules — Recon and Attack. Recon provides EASM capabilities that focus on identifying external-facing assets (that is, systems, applications and "things") and any vulnerabilities that could be exploited (see Emerging Technologies: Critical Insights for External Attack Surface Management). The EASM output from Recon can be fed into Attack once it finds a "tempting target," and then can autonomously and continuously test the defenses against specific techniques and approaches used by real attackers.

The benefit of having both modules is to discover and understand a target of temptation, and then immediately and automatically attack it to determine whether someone (for example, the blue team) would notice. This also allows you to figure out how far an attacker could compromise an infrastructure from that one weak asset.

Recon supports an organization's vulnerability management program by providing further visibility into their internet-facing, digital assets. Randori can integrate with other asset management and vulnerability assessment solutions, enriching the data from those solutions to help users better prioritize the assets with the highest risk of being compromised. The more visibility an organization has into their assets and environments, the better they can understand, manage, and ultimately reduce exposure. Randori Attack supports both red team and blue activities. It can help with validating and optimizing defenses, and training staff to detect, disrupt and defend against attacks more efficiently.

Challenges:

- Although Randori's Recon and Attack modules automate many functions, they do not fully replace the human element. Organizations will still require their staff members to do any follow up actions, such as remediation or mitigation.
- Awareness of EASM capabilities is limited among end users. However, end-user awareness of digital risks and vulnerabilities outside of traditional IT infrastructures is increasing.
- Gartner has observed only a small percentage of customers are performing red team activities internally, and many instead choose to outsource red teaming to service providers. Building awareness of a SaaS-based red team platform is another challenge.

- Autonomous red teaming hasn't been implemented outside of very lean-forward organizations, and therefore hasn't been battle tested yet. Only a very small percentage of organizations take advantage of red teaming. Most organizations still perform pen tests on an annual basis.
- Buyers may be confused or struggle to decide whether they should purchase a breach and attack simulation (BAS) solution, an autonomous testing solution, or both. Each tool has its place — however, buyers will need to understand their specific use cases, and the different approaches offered by these technologies.

Who Should Care:

Randori will appeal to enterprises who have a heavy presence of digital assets outside the confines of the enterprise perimeter, or that have invested in vulnerability assessment solutions and are looking for more actionable ways to prioritize vulnerabilities. It will also attract interest from organizations thinking about building or maturing an internal red team function and looking to include more automated tools to support their analysts. Organizations looking to strengthen their resilience and understand how well their security controls and processes are operating should also look into Randori. Some organizations may want to grow into a tool by starting with Recon — to understand their digital footprint and exposures. Then, as they mature their internal offensive and defensive teams and capabilities, these organizations can expand to Attack to validate those exposures.

Tines

Dublin, Ireland (tines.com)

Analysis by Pete Shoard

Why Cool: Tines is cool, because it focuses on simplicity in automation — democratizing security orchestration and automation through the implementation of automation building blocks. It focuses on a no-code development process and not on prebaked playbooks. Tines provides automation and orchestration technology for security operations through a simple but extensible web-based user interface (UI).

The product set is able to achieve a wide range of automation tasks for security professionals with little or no previous programming experience. Tines' approach includes seven core action types — Email, Event Transform, IMAP, HTTP Request, Trigger, Send to Story, and Webhook. These actions perform simple interactions with third-party services, mirror existing processes or provide data capture and manipulation. The product is extensible, and combined with its library of action templates (130 vendors supported as of June 2021), it also crosses from security into other areas such as social media, messaging, and standard Linux library functions. This means that there are few limitations on workflow capabilities.

The platform focuses on SaaS, but can also support on-premises deployments. It offers shared workspaces, role-based user access and granular auditing — providing a basis on which to build metrics to measure the performance of the platform and the team that it assists. Subscription pricing is transparent and volume-driven, and there is a free community version.

Organizations with or without large security teams can utilize the platform for both simple and complex security requirements, enabling them to address the security challenges of digital transformation. These challenges include increasing automation, reducing staff burdens and the potential impact of cyberattacks. Tines is well positioned to assist with security use cases, but also has potential beyond this, going into other areas of an organization that may benefit from process automation.

Challenges:

- Tines is a young company and has the speed and agility to develop in areas that it's team finds interesting and innovative. Prioritizing technology features and functionality against more traditional customer demand may create friction and make it hard to guess which features and capabilities will be in the roadmap and which will get priority. It should be expected that Tines will see pressure to grow quickly from investors and this may mean that priorities move away from client-facing product development and onto more business-focused areas, such as marketing and sales growth.
- While advertised as a "no-code" platform, it may be beneficial to have some experience in programming to get the best out of the platform.

- Current tutorials are comprehensive and well thought out, but they are not supported by any formal subscription or service, so are not guaranteed to continue. Buyers should take advantage of the community version to test and confirm that the solution will meet their needs before purchasing.

Who Should Care: Tines will appeal mainly to small and midsize organizations with lower security maturity — although it is useful for and used by large multinationals. Those organizations that will benefit most will be those that have more-developed security response plans and processes, and those that have set aside time and investment funds to develop content to run on the platform. As with all SOAR solutions, investment goes beyond simply purchasing a technology, requiring a commitment to developing and implementing workflows in the platform.

Where Are They Now?

Respond Software

Mountain View, California, U.S.

Analysis by Toby Bussa

Profiled in Cool Vendors in Security Operations and Vulnerability Management.

Why Cool Then: SIEM technologies, which provide centralized log event collection and analysis, are complex tools that continue to be adopted by enterprises and service providers offering remote managed security monitoring (for example, managed security service providers [MSSPs] and MDR providers). These organizations also face challenges in hiring and retaining skilled analysts, which can impact the value realization from a SIEM solution. Midsize enterprises are adopting SIEM tools with the expectation that these tools are self-driving once deployed, which they realize is not the case once they attempt to run and use them.

Respond Software built a tool that leverages an expert decision support approach to support threat monitoring, detection and response. The vendor's solution codifies the tradecraft and the decisions that an analyst responsible for monitoring and analyzing security alerts would make with it. These can then be used alongside a SIEM solution (or in a stand-alone approach) to assist analysts by automating analysis.

Where They Are Now: FireEye acquired Respond Software on 19 November 2020. At the time of the acquisition, Respond Software's XDR Engine, the Respond Analyst, was being positioned as a component of FireEye's Mandiant Advantage platform — as well as supporting FireEye's Helix SIEM and other FireEye security solutions. [1] On 21 April 2021, FireEye's Mandiant division officially rebranded the Respond Analyst as Mandiant Automated Defense, a module within the Mandiant Advantage SaaS Platform. [2]

Who Should Care: Mandiant Advantage customers and potential buyers stand to benefit from FireEye's acquisition of Respond Software. The need for skilled security experts who know how to monitor, detect and respond to threats has only increased as attacks proliferate and the impacts to organizations grow (see How to Respond to the 2020 Threat Landscape). The application of automated threat detection and analysis through the Mandiant Advantage solution — using Mandiant's threat intelligence, and awareness of an organization's defenses capabilities surfaced through Mandiant Security Validation — is compelling. This approach could create an enhanced automated analyst solution that would appeal to buyers looking to implement more autonomous support and automation for their modern security operations center functions. The solution could also extend and scale SOC analyst capabilities to organizations without a formalized SOC (see Tips for Selecting the Right Tools for Your Security Operations Center).

Acronym Key and Glossary Terms

MDR	managed detection and response
SIEM	security information and event management
SOAR	security orchestration, automation and response
SOC	security operations center
UI	user interface
XDR	extended detection and response

Notes

[1] Respond Software Joins the FireEye Team, FireEye

[2] Mandiant Advantage Expands SaaS Platform With New Mandiant Automated Defense Module, FireEye

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

Leadership Vision for 2021: Security and Risk Management

How to Respond to the 2020 Threat Landscape

Top Strategic Technology Trends for 2021: Hyperautomation

Is Your Organization Mature Enough for SOAR?