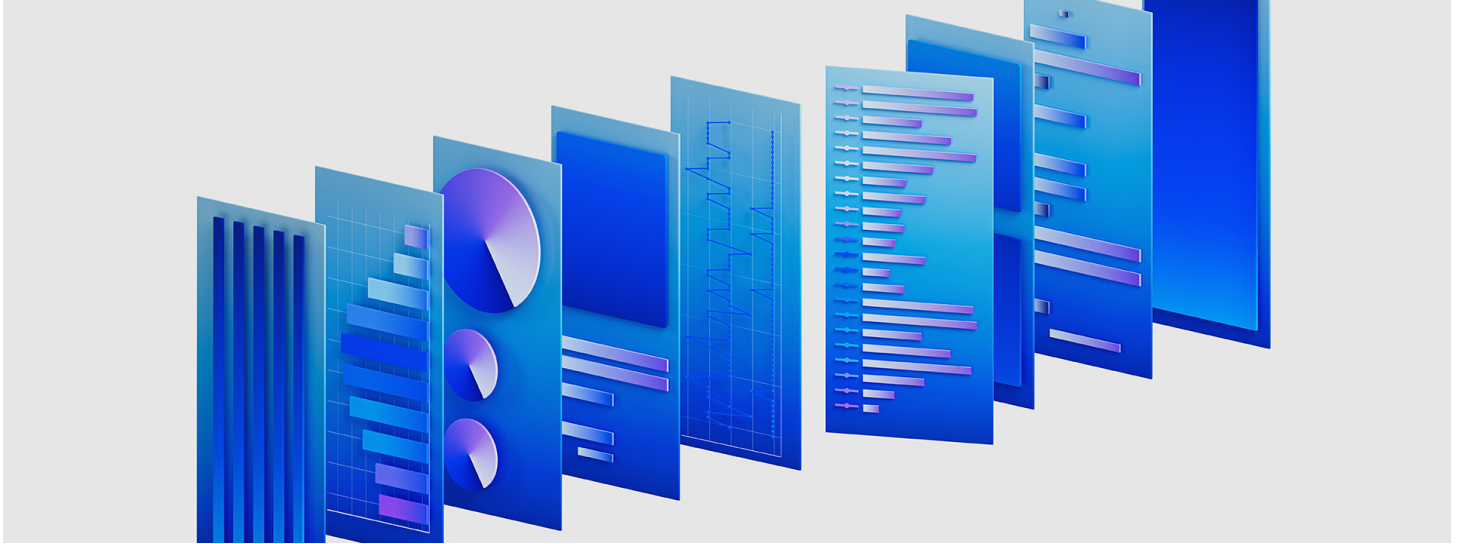


IBM Launches New QRadar Security Suite to Speed Threat Detection and Response

Modernized, unified interface streamlines analyst response across full attack lifecycle

Sophisticated AI and automation capabilities shown to speed alert triage by average of 55%



ARMONK, N.Y., April 24, 2023 -- Today IBM (NYSE: [IBM](#)) unveiled its new security suite designed to unify and accelerate the security analyst experience across the full incident lifecycle. The [IBM Security QRadar Suite](#) represents a major evolution and expansion of the QRadar brand, spanning all core threat detection, investigation and response technologies, with significant investment in innovations across the portfolio.



The new IBM Security QRadar Suite includes EDR/XDR, SIEM, SOAR, –and a new cloud-native log management capability – all built around a common user interface, shared insights and connected workflows

Delivered as a service, the IBM Security QRadar Suite is built on an open foundation and designed specifically for the demands of hybrid cloud. It features a single, modernized user interface across all products – embedded with advanced AI and automation designed to empower analysts to work with greater speed, efficiency and precision across their core toolsets.

Today's Security Operation Center (SOC) teams are protecting a fast-expanding digital footprint that extends across hybrid cloud environments – creating complexity and making it hard to keep pace with accelerating attack speeds. They can be slowed down by labor-intensive alert investigations and response processes,

manually stitching together insights and pivoting between disconnected data, tools and interfaces. SOC professionals say they spend around one-third of their day investigating and validating incidents that turn out to not be real threats, according to a recent survey.²

Built on the company's existing leadership in 12 security technology categories,³ IBM has rearchitected its market leading threat detection and response portfolio to maximize speed and efficiency, and to meet the specific needs of today's security analysts. The new IBM Security QRadar Suite includes EDR/XDR, SIEM, SOAR, - and a new cloud-native log management capability – all built around a common user interface, shared insights and connected workflows, with the following core design elements:

- **Unified Analyst Experience:** Refined in collaboration with hundreds of real-world users, the suite features a common, modernized user interface across all products: designed to dramatically increase analyst speed and efficiency across the entire attack chain. It is embedded with enterprise-grade AI and automation capabilities that have been shown to speed alert investigation and triage by 55% in the first year, on average.¹
- **Cloud Delivery, Speed & Scale:** Delivered as a service on Amazon Web Services (AWS), QRadar Suite products allow for simplified deployment, visibility and integration across cloud environments and data sources. The suite also includes a new, cloud-native log management capability optimized for highly efficient data ingestion, rapid search and analytics at scale.
- **Open Foundation, Pre-Built Integrations:** The suite brings together the core technologies needed across threat detection, investigation and response – built around an open foundation, an extensive partner ecosystem, and more than 900 pre-built integrations that provide strong interoperability between IBM and third-party toolsets.

"In the face of a growing attack surface and shrinking attack timelines, speed and efficiency are fundamental to the success of resource-constrained security teams," said Mary O'Brien, General Manager, IBM Security. "IBM has engineered the new QRadar Suite around a singular, modernized user experience, embedded with sophisticated AI and automation to maximize security analysts' productivity and accelerate their response across each step of the attack chain."

Co-innovation for Real-World Security Demands

The QRadar Suite is the culmination of years of IBM investment, acquisitions and innovations in threat detection and response. It features dozens of mature AI and automation capabilities that have been refined over time with real-world users and data, including IBM Managed Security Service engagements with more than 400 clients. It also includes innovations developed in collaboration with IBM Research and the open source security community.

These AI-powered capabilities have been shown to significantly improve the speed and accuracy of SOC operations: For example, allowing IBM Managed Security Services to automate more than 70% of alert closures^[4] and reduce its alert triage timelines by 55%² on average within the first year of implementation.

Bringing these capabilities together via the unified analyst experience, the QRadar Suite automatically contextualizes and prioritizes alerts, displays data in visual format for rapid consumption, and provides shared insights and automated workflows between products. This approach can drastically reduce the number of steps

and screens required to investigate and respond to threats. Examples include:

- **AI-Powered Alert Triage:** Automatically prioritizes or closes alerts based on AI-driven risk analysis, using AI models trained on prior analyst response patterns, along with external threat intelligence from IBM X-Force and broader contextual insights from across detection toolsets.
- **Automated Threat Investigation:** Identifies high-priority incidents that may warrant investigation, and automatically initiates investigation by fetching associated artifacts and gathering evidence via data mining across environments. The system uses these results to generate a timeline and attack graph of the incident based on MITRE ATT&CK framework and recommends actions to speed response.
- **Accelerated Threat Hunting:** Uses open source threat hunting language and federated search capabilities to help threat hunters discover stealthy attacks and indicators of compromise across their environments, without moving data from its original source.

By helping analysts respond faster and more efficiently, QRadar technologies can also help security teams improve their productivity and free up analysts' time for higher value work.

Open, Connected and Modernized Security Suite

The QRadar Suite leverages open technologies and standards across the portfolio, alongside hundreds of pre-built integrations with IBM Security ecosystem partners. This model enables deeper shared insights and automated actions across third party clouds, point products, and data lakes, which can reduce deployment and integration times from months to days or weeks.

The IBM QRadar Suite includes the following core products, initially delivered as SaaS and updated with the new unified analyst experience:

- **QRadar Log Insights:** A new, cloud-native log management and security observability solution providing simplified data ingestion, sub-second search and rapid analytics. It leverages an elastic security data lake optimized to collect, store and perform analytics on terabytes of data with greater speed and efficiency. It is designed for cost effective security log management alongside federated search and investigation.
- **QRadar EDR and XDR:** Helps companies protect their endpoints against previously unknown, zero-day threats – using automation and hundreds of machine learning and behavioral models to detect behavioral anomalies and respond to attacks in near-real time. It leverages a unique approach that monitors operating systems from the outside, helping avoid manipulation or interference by adversaries. For companies looking to extend their detection and response capabilities beyond the endpoint, IBM also offers XDR with alert correlation, automated investigation, and recommended responses across network, cloud, email, and more, as well as managed detection and response (MDR).
- **QRadar SOAR:** Recent winner of a [Red Dot Design Award](#) for interface & user experience; helps organizations automate and orchestrate incident response workflows and ensure their specific processes are followed in a consistent, optimized and measurable way. It includes 300 pre-built integrations and offers out of the box playbooks for responding to 180+ global data breach and privacy regulations.
- **QRadar SIEM:** IBM's market leading [QRadar SIEM](#) has been enhanced with the new unified analyst interface which provides shared insights and workflows with broader security operations toolsets. It offers real-time detection, leveraging AI, network and user behavior analytics, and real-world threat intelligence

built to provide analysts with more accurate, contextualized and prioritized alerts. IBM also plans to make QRadar SIEM available as a service on AWS by the end of Q2 2023.

The IBM Security QRadar Suite is available today via individual SaaS offerings. For more information, visit: <https://www.ibm.com/qradar>

Statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

About IBM Security

IBM Security helps secure the world's largest enterprises and governments with an integrated portfolio of security products and services, infused with dynamic AI and automation capabilities. The portfolio, supported by world-renowned IBM Security X-Force® research, enables organizations to predict threats, protect data as it moves, and respond with speed and precision without holding back business innovation. IBM is trusted by thousands of organizations as their partner to assess, strategize, implement, and manage security transformations. IBM operates one of the world's broadest security research, development, and delivery organizations, monitors 150 billion+ security events per day in more than 130 countries, and has been granted more than 10,000 security patents worldwide.

Media Contact:

Cassy Lalan
Communications, IBM Security
cllalan@us.ibm.com | 319-230-2232

¹Based on IBM's internal analysis of aggregated performance data observed from Managed Security Service engagements with 400+ clients from 2018-2019, which showed that average alert triage timeline was reduced by 55% during the first year using AI and automation capabilities that are now part of QRadar. Actual results will vary based on client configurations and conditions and, therefore, generally expected results cannot be provided.





²[Global Security Operations Center Study Results](#), administered by Morning Consult and commissioned by IBM, March 2023. Based on responses from 1,000 surveyed security operation center professionals from 10 countries.

³Based on security product evaluations from external analyst firms including Gartner, IDC, Forrester, KuppingerCole and Omdia, which rank IBM as a leader in 12 security product categories: SIEM, SOAR, Fraud Reduction Intelligence Platform, Risk Based Authentication, Identity Governance and Administration, Access Management, Identity and Access Management as a Service, Access Governance & Intelligence and Identity Governance, Authentication, Customer Identity and Access Management, Data Security, Unified Endpoint Management.

⁴IBM Institute for Business Value report, "[AI and automation for cybersecurity](#)," 2022. Results based on IBM analysis of aggregated annual performance data observed from hundreds of global clients using AI and automation capabilities that are now part of QRadar Suite. Actual results will vary based on client configurations

and conditions and, therefore, generally expected results cannot be provided.

SOURCE IBM

Additional assets available online:  [Photos](#) (
 

https://newsroom.ibm.com/2023-04-24-IBM-Launches-New-QRadar-Security-Suite-to-Speed-Threat-Detection-and-Response?utm_medium=Exinfluencer&utm_source=Exinfluencer&utm_content=TNKWW&utm_id=LinkedIn-Zeus-Kerravala-IBMThink2023TakeawaysBlogQRadarSuite-2023-05-18