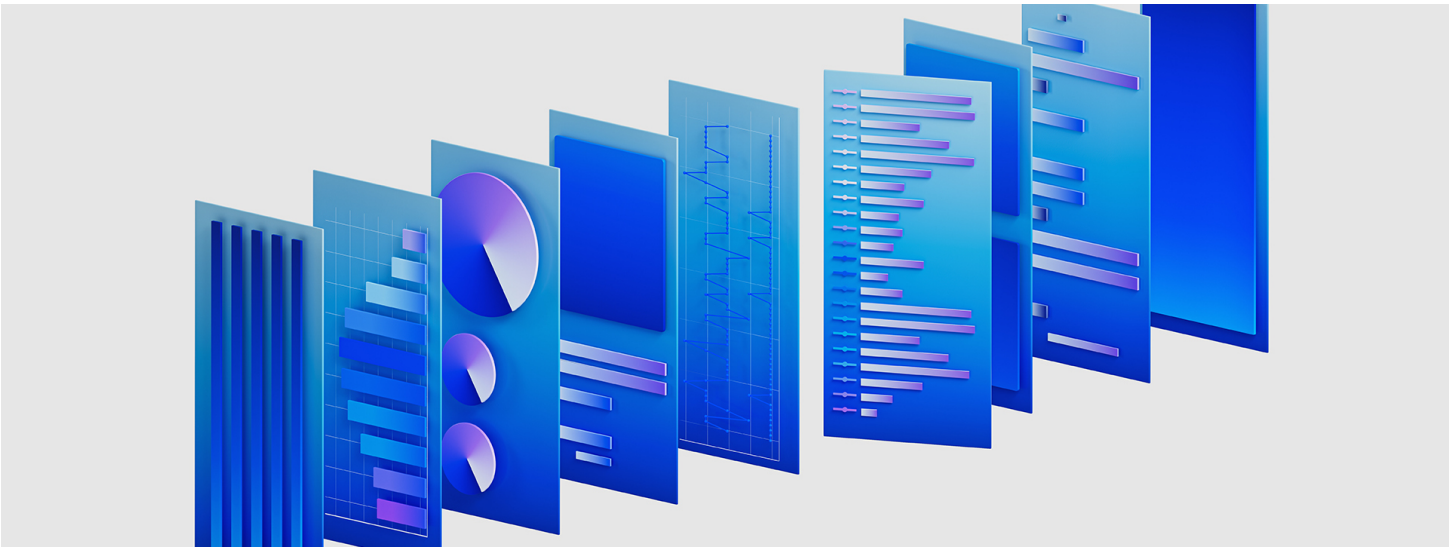
IBM Newsroom

IBM Unveils Cloud-Native SIEM Built to Maximize Security Teams' Time and Talent

Empowers security analysts and AI to work side by side more effectively with modernized foundation and redesigned UX



ARMONK, N.Y., Nov. 7, 2023 /PRNewswire/ -- IBM (NYSE:IBM) today announced a major evolution of its flagshipIBM QRadar SIEM product: redesigned on a new cloud-native architecture, built specifically forhybrid cloud scale, speed and flexibility. IBM also unveiled plans for delivering generative AI capabilities within its threat detection and response portfolio – leveraging watsonx, the company's enterprise-ready data and AI platform.

Today's hybrid cloud environments are evolving and scaling at an exponential rate, creating a larger and more complex attack surface to protect. This growing IT footprint makes it harder to quickly find the true threats amongst the noise – slowed down by siloed technologies, manual searches and an overload of alerts, without clear context or visualizations. In fact, SOC professionals get to less than half (49%) of the alerts that they're supposed to review within a typical workday, according to a recent global survey.[1]

The new cloud-native QRadar SIEM is built to maximize the power of today's security teams. It is designed to augment and up-level security analysts daily work – tapping AI to manage time-consuming and repetitive tasks while empowering security analysts to find and respond to high priority security incidents more effectively.

"Our new cloud native SIEM is a core element of IBM's mission to usher in the next generation of security operations, built for the hybrid cloud and AI era," said Kevin Skapinetz, Vice President, Strategy and Product Management, IBM Security."Instead of forcing analysts to work around the complexity of security technologies, we're designing technology to remove the complexity – weeding out the noise, simplifying the user experience, and empowering analysts to tackle urgent threats with greater speed and confidence."

IBM's cloud-native SIEM builds on QRadar's 13 years market leadership and analyst recognition[2] for deep security analytics – with a redesigned architecture for highly efficient data ingestion, rapid search and analytics at scale. Built on an open foundation, it is the newest addition to QRadar Suite, IBM's integrated portfolio of threat detection and response software.

The new cloud-native QRadar SIEM will be generally available as SaaS in Q4 2023, with plans to offer software for on-premises and multi-cloud deployment in 2024.

Open at its Core

Built on Red Hat OpenShift, QRadar SIEM is designed to be open at a foundational level – allowing for deeper interoperability with multi-vendor tools and clouds. It leverages open source and open standards for core functions including detection rules and search language – allowing it to work across companies' broader security and technology stacks.

- **Harness Security Community Detections:** Leverages common, shared language for detection rules (SIGMA) – allowing clients to quickly import new, crowdsourced detections directly from the security community as threats evolve.
- **Investigate Across Data Sources:** Offers unique federated search and threat hunting capabilities built on open-source technologies, allowing analysts to proactively search for and investigate threats across cloud and on-premise data sources in a single, unified way – without moving data from its original source.
- **Deep Partner Network:** Builds on the QRadar ecosystem, one of the largest partner networks in the industry with more than 700 pre-built integrations.

Full Suite for Connected, Proactive Security Response

As part of QRadar Suite, the new cloud-native SIEM offers customers access to a wide set of integrated capabilities which can allow for more proactive detection, investigation and response across toolsets. With QRadar Suite, organizations can gain visibility into their exposed assets via attack surface management (ASM) capabilities, search for threats across toolsets, protect at the endpoint with EDR, and connect to automated playbooks to speed response (SOAR). QRadar SIEM empowers users with shared insights and automated actions across their core toolsets – accessed directly from their primary user interface, without needing to shift between tools.

Enterprise-Grade AI Speeds Response to Critical Threats

QRadar SIEM applies multiple layers of AI and automation to improve the quality of alerts and the efficiency of security analysts. These mature AI capabilities have been pre-trained on millions of alerts from IBM's vast network of clients and are refined further post-deployment to account for each client's unique environment. For example:

- **Reduce Noise and Improve Alerts:** Alert prioritization capabilities use AI to automatically de-prioritize low priority alerts, while automatically grouping, contextualizing and escalating high priority alerts – factoring in risk context from ongoing threat intelligence and analyst response patterns. This capability allowed IBM Consulting Cybersecurity Services to automate 85% of alert management for clients,[3] and to accelerate their threat triage timelines by 55% in the first year of use.[4]
- **Jump-Start Investigations:** AI capability automatically runs federated searches across connected systems, generating a visual attack timeline, MITRE ATT&CK mappings, and recommended actions – giving analysts a significant head-start on investigation tasks.
- **Automatically Update Detections:** QRadar SIEM's analytics are automatically updated with new detection rules and threat intelligence on an ongoing basis, to keep pace with evolving threats.

IBM's AI security capabilities are embedded natively into the QRadar Suite analyst interface, bringing contextual insights to analysts' fingertips and helping them take advantage of AI more intuitively within their regular workflows.

Generative AI to Advance SOC Productivity

IBM also plans to release generative AI (GAI) security capabilities for QRadar Suite in early 2024 – built on watsonx, the

company's AI and data platform. IBM is designing GAI to help optimize security teams' time and talent by managing certain tedious tasks on behalf of analysts, while also making it easier for them to perform more challenging, higher value work. For example:

- **Automate Reporting:** Create simple summaries of security cases and incidents that can be shared with a variety of stakeholders in a single click.
- **Accelerate Threat Hunting:** Automatically generate searches to detect threats based on natural language descriptions of attack behaviour and patterns – helping to accelerate response to new threat campaigns.
- **Interpret Machine-Generated Data:** Helping analysts to quickly understand security log data by providing simple explanations of events that have taken place on a system – lowering technical barriers and expediting their investigations.
- **Curate Threat Intelligence:** Interpret and summarize highly relevant threat intelligence, honing in on campaigns that are more likely to affect clients based on their unique risk profile.

IBM is also developing predictive generative AI security capabilities which will be trained to create active responses that optimize over time – for instance, helping security team find similar incidents, update affected systems and patch vulnerable code.

Beyond these use-cases, IBM plans to embed generative AI across its broader security software and services portfolio. These capabilities will leverage watsonx infrastructure as well as watsonx AI models, which have been trained on curated, domain-specific datasets – designed to offer greater trust, transparency and accuracy.

For more about QRadar SIEM, visit information visit:https://www.ibm.com/products/qradar-cloud-native-siem

For more information about AI for Security, visit:https://www.ibm.com/security/artificial-intelligence

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

[1] *Global Security Operations Center Study, 2022 conducted by Morning Consult, sponsored by IBM.*

[2] *QRadar has been identified as a market leader for SIEM in multiple third party analyst reports for the past 13 years, including reports from Gartner, Forrester, KuppingerCole, IDC and Omdia.*

[3] *Based on IBM's internal analysis of aggregated performance data observed from engagements with 340+ clients in July 2023. Up to 85% of alerts were handled through automation using AI capabilities that are part of QRadar SIEM. Actual results will vary based on client configurations and conditions and, therefore, generally expected results cannot be provided.*

[4] *Based on IBM's internal analysis of aggregated performance data observed from 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 part of QRadar SIEM. Actual results will vary based on client configurations and conditions and, therefore, generally expected results cannot be provided*

SOURCE IBM
