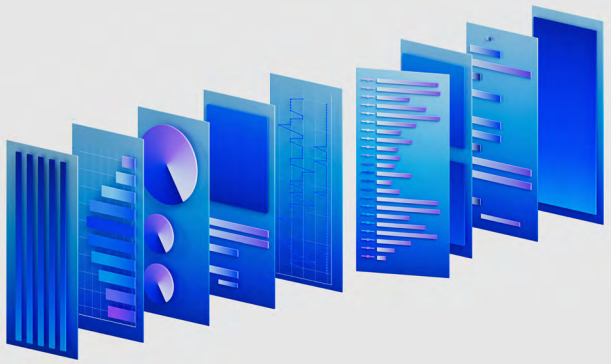
IBM Security QRadar Suite

Designed around the analyst experience



More infrastructure, more tools and more alerts are challenging analysts. Organizations' digital footprint expanding across hybrid cloud environments creates complexity and makes it difficult for security teams to find and respond to immediate threats. SOC professionals state that they're unable to review 51% of the alerts during a typical workday and that the number one factor slowing them down is manual investigation processes.[1] Security analysts need more efficiency to keep pace with today's attacks. This requires a more streamlined user experience that automatically brings together insights, prioritizes risk, and helps them respond with greater precision and speed before attacks cause major damage and losses.

IBM Security® QRadar® Suite is an open, modular, threat detection and response suite designed to unify the security analyst experience and accelerate efficiency across the full incident lifecycle and associated tools. Enterprise-grade AI and automation dramatically increase analysts' productivity, helping resource-strained security teams work more effectively across core technologies. The portfolio offers integrated products for endpoint security (EDR, XDR and MDR), log management, SIEM and SOAR–all with a common user interface, shared insights and connected workflows. It's built on a platform with a wide ecosystem of partners and integrations and delivered as a service on AWS.

Key benefits

- **Unified analyst experience:** The suite features a common, integrated user interface that empowers analysts to work more quickly and efficiently throughout investigation and response processes, with shared insights and automated actions across multiple tools and data sources. This streamlined process has been shown to reduce incident response times by 85%.[2]
- **Cloud delivery, speed and scale:** Delivered as a service on AWS, QRadar Suite products allow for simplified deployment across cloud environments and integration with public cloud and SaaS log data. The suite also includes a new, cloud-native security observability and log management capability optimized for large scale data ingestion, sub-second search and rapid analytics.
- **Open platform and built-in integrations:** QRadar Suite brings together core tools needed for an effective SOC. Built on a broad partner ecosystem with more than 900 pre-built integrations for flexibility and choice across IBM and third-party products, it includes native, pre-integrated capabilities for threat intelligence, log management, EDR, SIEM and SOAR.

Open Platform. Open Integration. Open Threat Intelligence.

Key components and use cases

- **Unified analyst experience:** Get automated investigation and response recommendations. Federated search and threat hunting included with Log Insights, SIEM and SOAR.
- **QRadar EDR and XDR:** Remediate known and unknown endpoint threats in near real-time with intelligent automation and AI, attack visualization storyboards and automated alert management. Take threat detection and response beyond the endpoint to include cloud, email, network, user and data into a single correlated view to see and stop threats faster.
- **QRadar Log Insights:** Gain complete visibility with cloud-scale log ingestion, rapid search, powerful visualization and federated threat hunting and collaboration.
- **QRadar SIEM:** Run your business in the cloud and on-prem with visibility and security analytics built to stay ahead of advanced threats and save more than 90% of analysts' time investigating an incident.[3]
- **QRadar SOAR:** Streamline your SOC with an automated and intelligent response using the industry's most open and interoperable SOAR platform.

"I equate the UAX to five additional FTEs. It was easier to get better data out of my tools with AI than investing in more people. It made my people faster and better at their job."[4]

Why IBM QRadar Suite

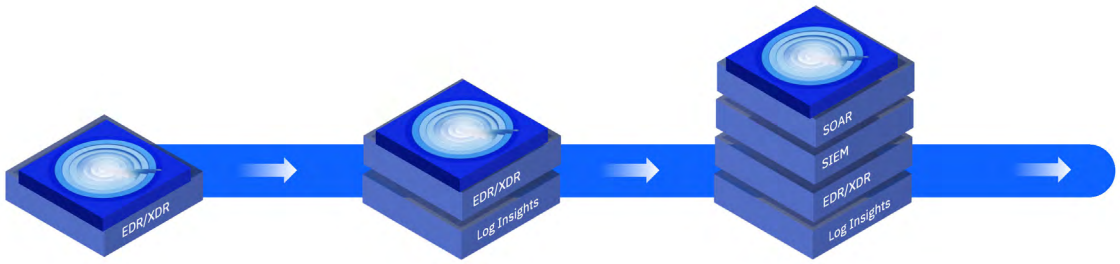
This unique, purpose-built, security analyst-centric approach can drastically reduce the number of steps and screens required to investigate and respond to threats. Examples include:

- **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 toolset. Analysis has shown that this solution can automate more than 70% of alert closures and reduce alert triage timelines by 55%[5] on average within the first year of implementation.
- **Automated threat investigation:** Identifies high-priority incidents that may warrant investigation and automatically initiates investigation by fetching associated artifacts and gathering evidence through 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.

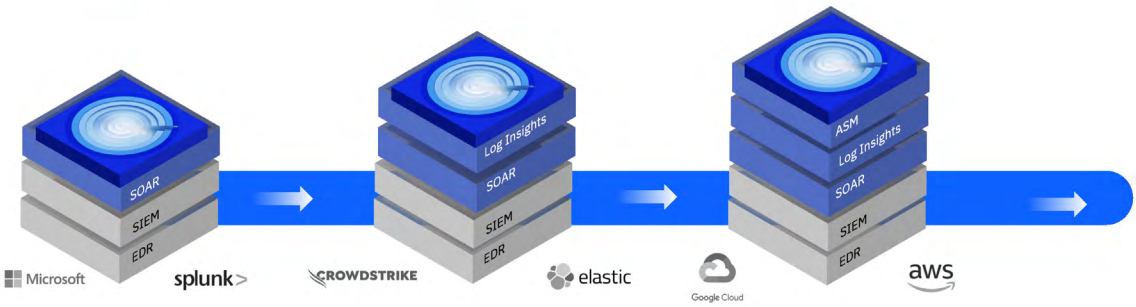
Start where you need–easily expand for additional capabilities

Examples

Start where you need, and easily expand for additional capabilities



Start with what you have, and add what you need



Sources
1. 2023 IBM Global Security Operations Center Study
2. New cyberthreats demand new approaches, ibm.com
3. 2023 Forrester TEI of QRadar SIEM
4. North American State Government Agency
5. Analysis of managed service over 400 clients / IBM Institute for Business Value report, "AI and automation for cybersecurity," 2022.

IBM Corporation New Orchard Road, Armonk, NY 10504
Produced in the United States of America, April 2023