# IBM Security QRadar SIEM (Cloud-Native SaaS)

## Made to maximize your security team's time and talents

**Highlights**

Risk-based alert prioritization

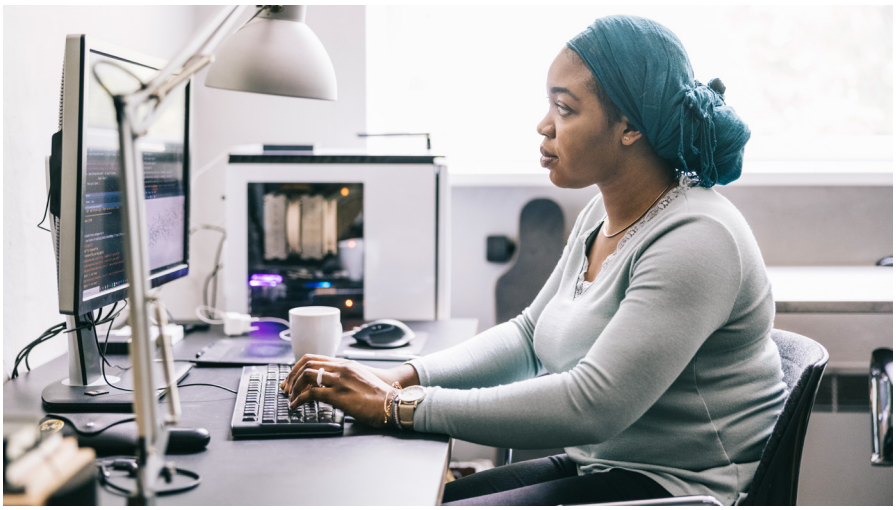
Automated investigations with recommended responses

Quick detection and analysis with open-source technology and standards

Federated search for a holistic view

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 among the noise. Threat hunting is slowed by siloed technologies, manual searches and an overload of alerts that don't have clear context or visualizations. In fact, security operations center (SOC) professionals get to fewer than half (49%) of the alerts they're supposed to review within a typical workday, according to a recent global survey.[1]

Building on over a decade of IBM Security® QRadar® market leadership and analyst recognition, we know having the most powerful technology means nothing if it creates complexity for analysts. That's why we built QRadar SIEM (Cloud-Native SaaS). With a streamlined intuitive interface, the unified analyst experience removes the burden of switching between tools. QRadar SIEM provides visibility and AI-driven capabilities to amplify decisions and automate tasks. Whether it's simplified case management, threat investigation or near real-time alerting, QRadar SIEM is made to help analysts succeed.



### Risk-based alert prioritization

Detecting threats is the main function of a SIEM, but the new cloud-native QRadar SIEM takes it up another level by applying multiple layers of AI to drastically improve the quality of alerts and the efficiency of security analysts. By leveraging mature AI capabilities that have been pre-trained on millions of alerts from the vast network of IBM clients, QRadar SIEM provides context and prioritization to threats. It automatically enriches each alert with data from IBM X-Force® Threat Intelligence and can be configured to utilize several third-party threat intelligence systems. Scoring and identifying high-severity alerts, mapping to linked observables and continuing to correlate findings on a sliding time window after initial detection lets analysts focus on more complex and high-value work.

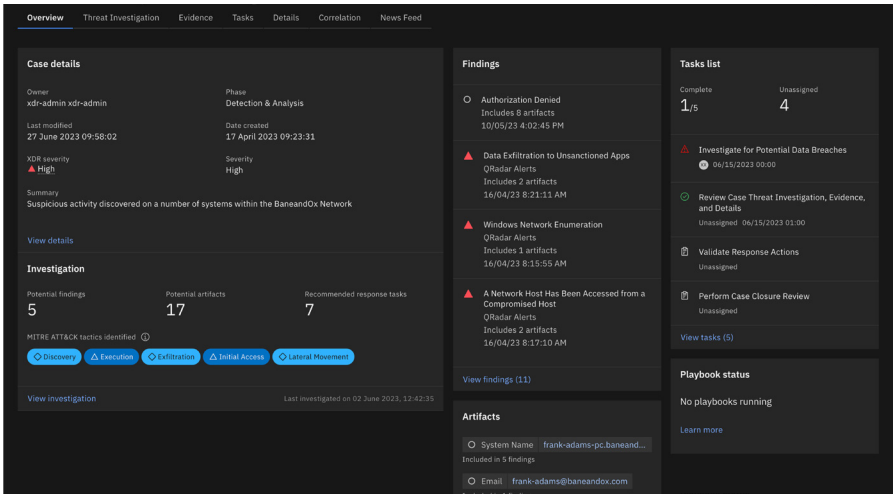



Figure 1. Intelligent algorithms apply multiple layers of risk scoring on each finding and then related findings are grouped together in one case.

### Automated investigations with recommended response

To fast-track suspicious or critical cases, QRadar SIEM applies intelligence enrichment, risk assessment and activity timeline mapping to provide a summary of information and remediation recommendations all in one place—helping to reduce the “swivel chair” approach.

Automated investigations of related alerts are presented in a single pane of glass to reduce noise and save time. Here, an analyst can find a visual breakdown of an attack, mapping affected assets, action timelines and mappings to the MITRE Framework. Key information needed for fast, high-level reporting—like a network connections graph—is generated using intelligent AI models.

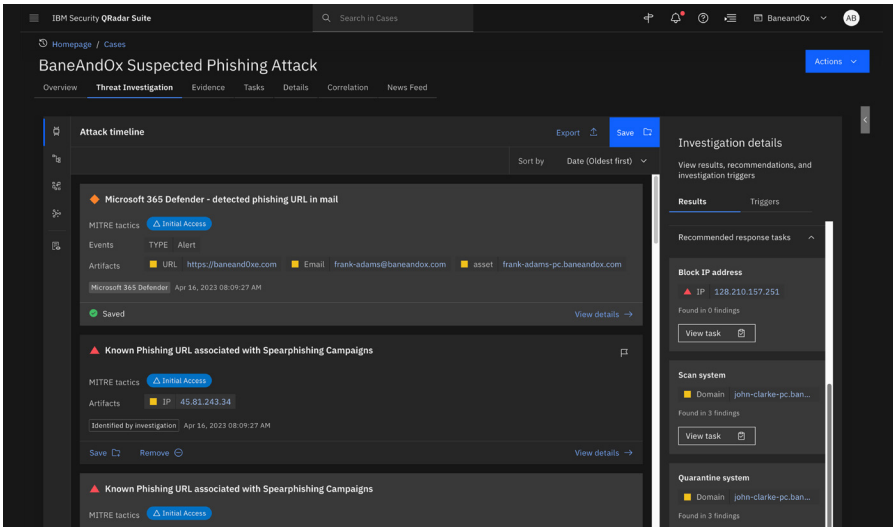



Figure 2. The Threat Investigation dashboard reveals a cross-functional view of the alerts and events in one place where you can view the contributing data, rules and recommended responses.

**Quick detection and analysis with open-source technology and standards**

As a founding member of the Open Cybersecurity Alliance, IBM has adopted open-source technologies, like Sigma rules, to enhance collaboration among security analysts for more effective and efficient identification of incidents in real-time. Security analysts gain valuable advantages as the tool quickly imports new, crowdsourced threat intelligence directly from the security community as threats evolve. Beyond the advantage of accessing timely and actionable intelligence, for organizations strapped on resources and budgets, accessing the free or low-cost threat intel is an affordable solution.

Additionally, IBM intentionally purpose-built the new cloud-native QRadar SIEM to process complex searches in seconds by utilizing Kusto Query Language (KQL), an open-source query language. This puts the core focus on ease of use for your security analyst by offering more intuitive syntax and faster search speeds. Your team can schedule near-real-time monitoring so you automatically have the latest up-to-date information.

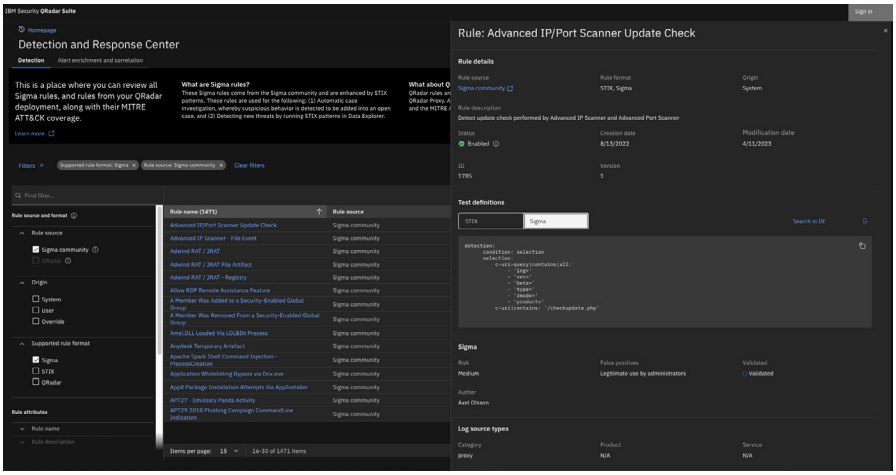



Figure 3. View all of Sigma rules listed from the Sigma community and enhanced by STIX patterns.

## Federated search for a holistic view

Although SIEMs play a critical role in analyzing data, the reality of including the sheer volume of data that the majority of organizations create today in a tool for analysis is challenging—especially when spread across multiple clouds and on-premises locations. Fortunately, new security tools make it so that only specific alerts or data from these tools needs to be ingested. In many cases, initial detection may not require analysis of externally stored data; however, they may still need access to that data for investigation and validation. In these instances, federated search allows users to search for data across their siloed tools, giving you an expanded view across all your datasets and ensuring all data is included in threat analysis—regardless of where it resides.

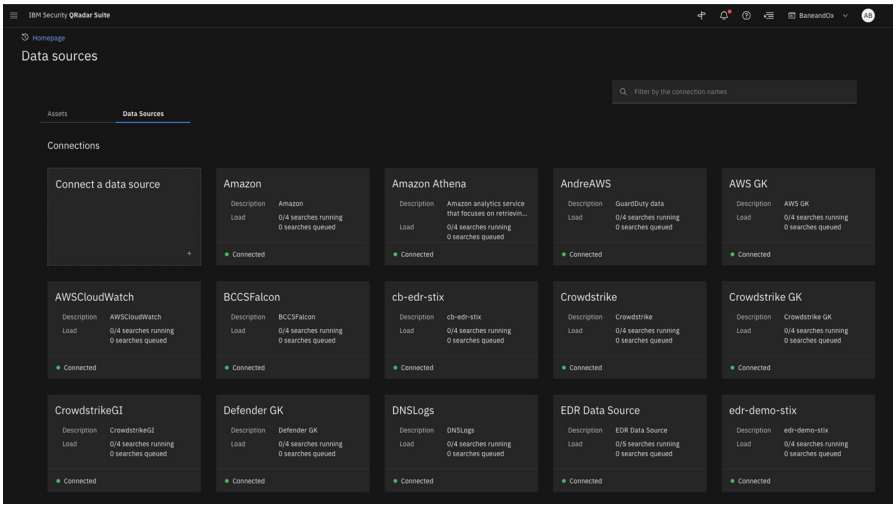



Figure 4. Easily connect and view your data sources in one place.

## Conclusion

The QRadar difference is our dedication to an open approach at a foundational level. Built on Red Hat® OpenShift® and using open source and open standards for core functions including detections and query language, QRadar is natively interoperable across all types of environments and toolsets. When analysts have the right tools and context, they can move with speed and precision to stop sophisticated attacks.

## Why IBM?

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by IBM X-Force research, provides security solutions to help organizations drive security into the fabric of their business so they can thrive in the face of uncertainty.

IBM operates one of the broadest and deepest security research, development and delivery organizations. IBM holds over 3,000 security patents and monitors more than one trillion events per month in more than 130 countries. To learn more, visit ibm.com/security.

## For more information

To learn more about IBM Security QRadar SIEM (Cloud-Native SaaS), please contact your IBM representative or IBM Business Partner or visit ibm.com/products/qradar-cloud-native-siem.

1. Morning Consult, sponsored by IBM, Global Security Operations Center Study, March 2023.



IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
December 2023