Technical Review

Automate Security Intelligence with IBM Security QRadar SIEM

Date: November 2022 **Author:** Justin Boyer, Validation Analyst; and Tony Palmer, Principal Validation Analyst

Abstract

This Technical Review by TechTarget's Enterprise Strategy Group (ESG) documents IBM Security QRadar SIEM's ability to simplify and improve threat detection, investigation, and response while reducing SIEM overhead through their SaaS offering.

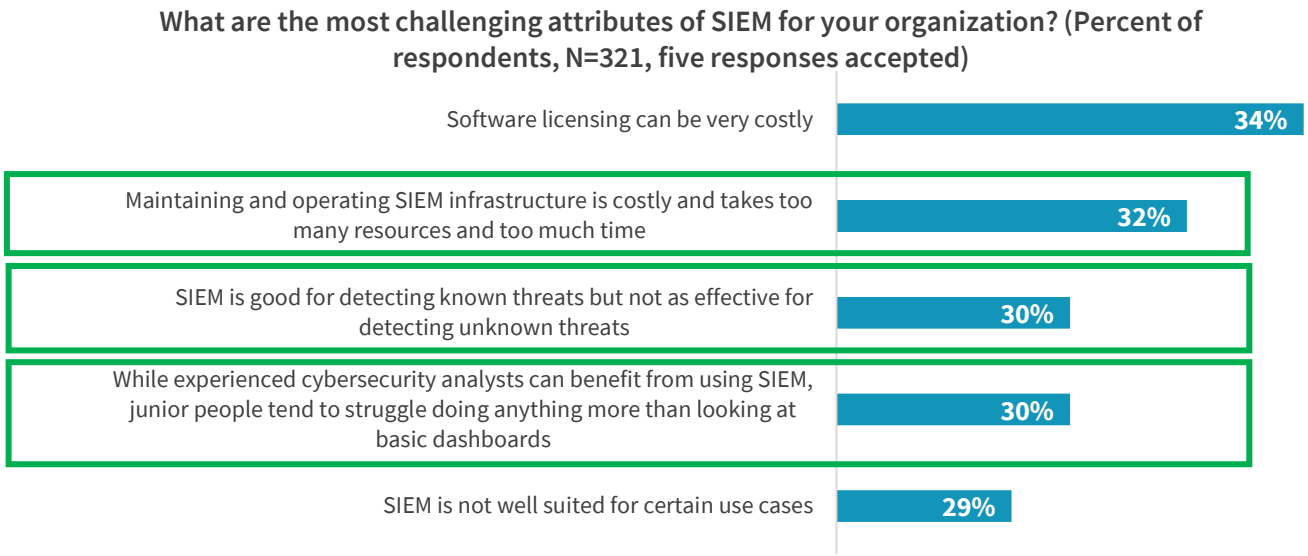
The Challenges

There is a wealth of data available to security analysts, but many have trouble finding what really matters in all the noise. According to Enterprise Strategy Group (ESG) research, organizations believe that making new data pipeline investments in the following areas would add the most significant additional value: keeping up with real-time data sources (40%), performing more comprehensive analytics to recognize complex attacks (39%), and collecting and centralizing data from more security controls and sources (32%).[1]

ESG also discovered that organizations consider security information and event management (SIEM) infrastructure difficult to manage. As shown in Figure 1, 32% of organizations believe maintaining and operating SIEM infrastructure is costly and takes too many resources and too much time. 30% believe that junior analysts tend to struggle to use SIEM effectively, because many SIEMs don't provide real-time correlation and analysis and because the tool is complex and difficult to use.

However, one glaring shortcoming of SIEM products is their inability to detect unknown threats. 30% of organizations surveyed think that SIEM is good for detecting known threats but not as effective for detecting unknown threats. Lacking the ability to detect unknown threats leaves companies always wondering whether an attacker may be lurking within their systems without their knowledge.

Figure 1. Top 5 SIEM Infrastructure Challenges



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

[1] Source: Enterprise Strategy Group Survey Results, *The Impact of XDR in the Modern SOC*, March 2021. All research references and charts in this technical validation have been taken from this survey results set.

Modern security operations centers (SOCs) require data correlation and analysis that can help to find hidden threats within the noise, without using valuable resources to run complex SEIM infrastructure.

The Solution: IBM Security QRadar SIEM

QRadar SIEM collects data from across the enterprise, from both on-premises and cloud sources, and automatically aggregates and analyzes it to help security teams detect, prioritize, and respond to cyber-threats. QRadar SIEM uses over 700 pre-built integrations to collect data, and it allows for custom integrations when needed. These data points are correlated into the QRadar SIEM Offense Dashboard, providing intelligent alerts analysts can use to dig deeper into possible incidents. QRadar SIEM simplifies data collection and analysis for security analysts, helping them become more efficient and effective at stopping cyber-threats.

Figure 2. QRadar SIEM

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Other key features include:

- X-Force Threat Intelligence Application: Pull in any threat intelligence feed using the open standard STIX and TAXII formats, and deploy the data to create custom rules for correlation, searching, and reporting.
- User Behavior Analytics (UBA): Detect insider threats within an organization using existing data in a QRadar SIEM deployment to generate new insights around users and risk. UBA provides risk profiling and unified user identities along with machine learning to establish normal behaviors and learned peer groups so QRadar SIEM can alert on user related anomalies.
- Cloud-based SaaS Deployment Model: IBM Security QRadar on Cloud (QRoC) reduces infrastructure costs and maintenance by deploying to a software-as-a-service (SaaS) environment hosted by IBM. IBM handles maintenance, upgrades, and health monitoring.

Enterprise Strategy Group Tested

Enterprise Strategy Group (ESG) validated QRadar SIEM's ability to correlate and analyze operational data to find and present potential security incidents for analysts to investigate.

Simplify and Improve Threat Detection, Investigation, and Response

We validated QRadar SIEM's ability to provide deep visibility into large amounts of data and give analysts the tools they need to better recognize the highest priority and act.

QRadar SIEM's out-of-the-box integrations, coupled with its ability to correlate insights, eliminate excessive noise and data overload for analysts. QRadar SIEM aggregates information from log sources, network tools, vulnerability data, and threat intelligence to provide meaningful insight into potential threats. It prioritizes events to help analysts see through the noise and act quickly.

Clear, customizable dashboards (Figure 3) allow analysts to drill down into collected data and understand it, launching investigations, assigning offenses, or initiating remediation procedures.

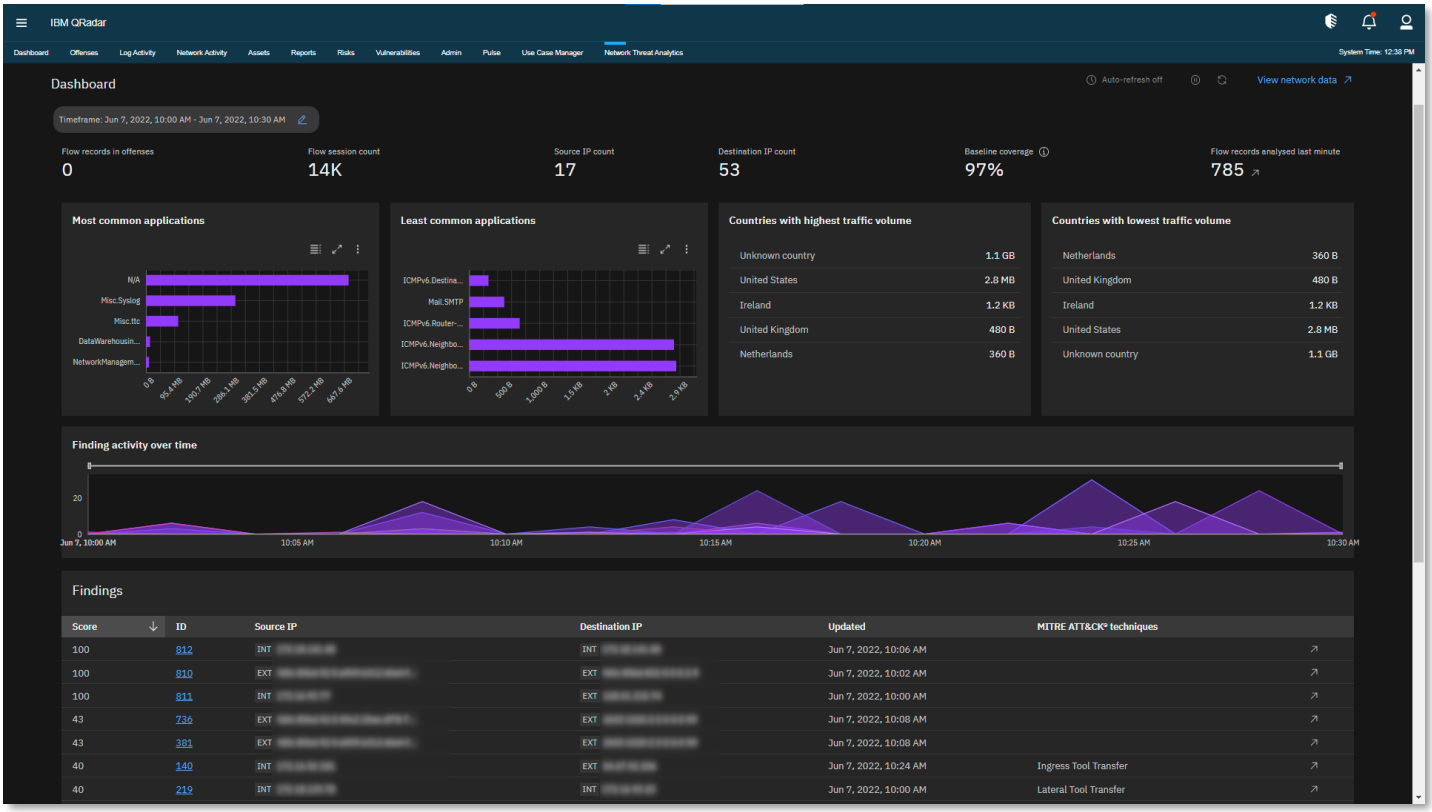
Figure 3. Offenses Overview Dashboard

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

QRadar SIEM provides a dashboard to analysts (Figure 3) to help them prioritize and act on potential security incidents. Through the Network Threat Analytics App (NTA), QRadar SIEM uses machine learning to understand the typical behavior of an organization's network and uses that information to find outliers in real-time traffic. This technique helps analysts find possible intrusions that may have gone unnoticed.

ESG observed the typical workflow used by analysts to uncover suspicious network traffic. Upon selecting the Network Threat Analytics App from the top left menu, the user is presented with a dashboard showing deviations from the norm in network activity for a period of time chosen by the user (Figure 4).

Figure 4. Network Outliers Displayed in the Network Analytics App

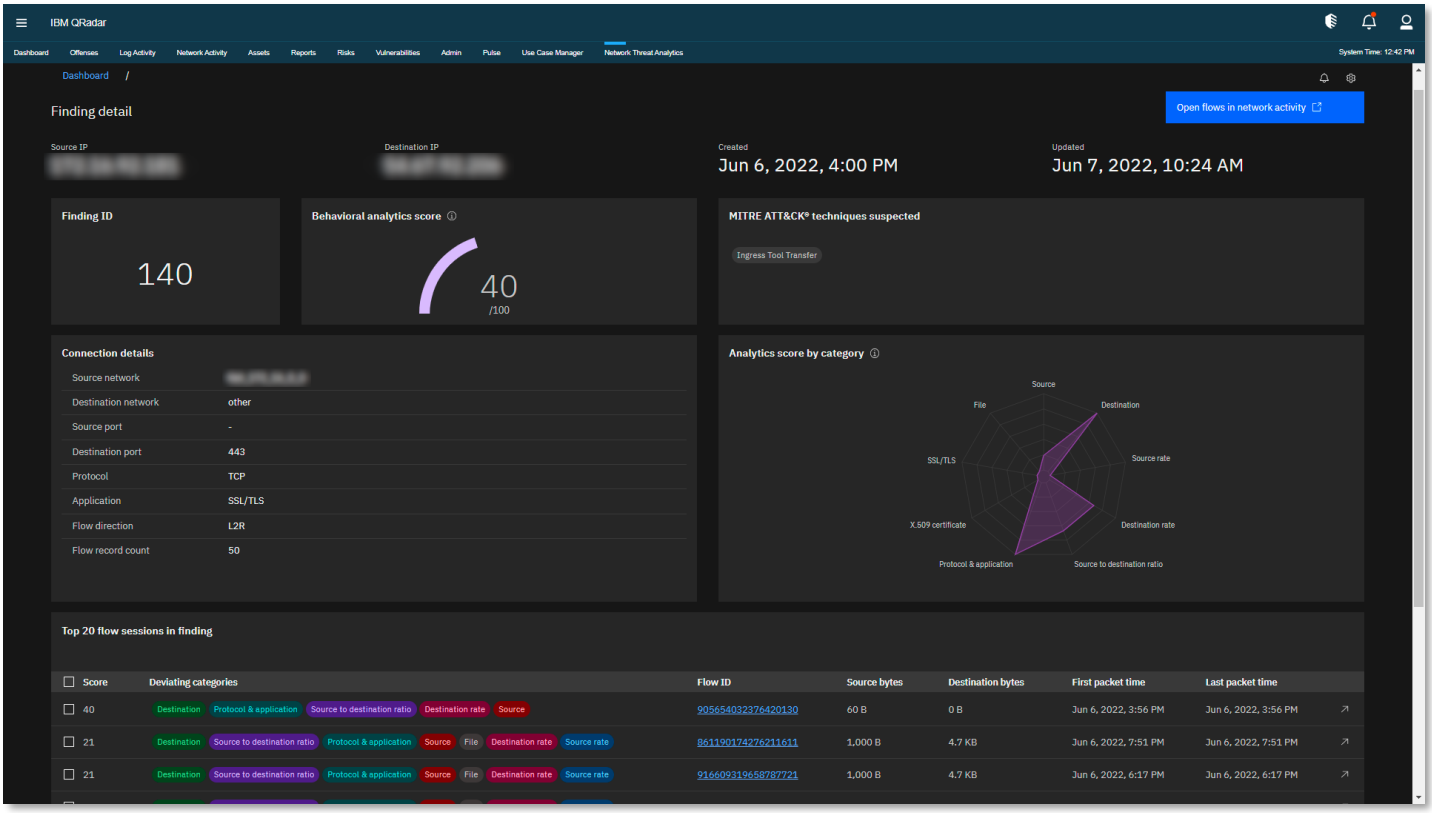


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Below the dashboard is a list of specific requests that have been marked as suspicious. Here, analysts can see basic information such as source and destination IP addresses, the port used, application name, and protocol. QRadar SIEM provides an outlier score for each request, indicating how far it deviates from typical network activity.

The analyst can then select one instance of suspicious activity—for example, a consistent request to an external IP address that may indicate beaconing to a command-and-control server (a common indication of malware infection). QRadar SIEM then displays a detailed page outlining the major contributors to the high outlier score (Figure 5). This page also displays several details about the request and allows the analyst to dive into why this request is so unusual. Perhaps the destination IP is in a country in which the company does no business or is known to be malicious based on threat intelligence data. An investigation can be opened to discover the source of this issue and resolve it.

Figure 5. Finding Details Page



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Why This Matters

According to Enterprise Strategy Group (ESG) research, organizations reported that top challenges related to security data and alerts were filtering out the noise so they can focus on the right signals (38% of respondents) and scaling to collect, process, and analyze the growing volume of security data (37%). It's clear that businesses are struggling to keep up with the avalanche of data produced by application and network logs and activity throughout the business day. It is becoming more difficult to filter out noise to find what matters so security analysts can act to protect the company and its customers.

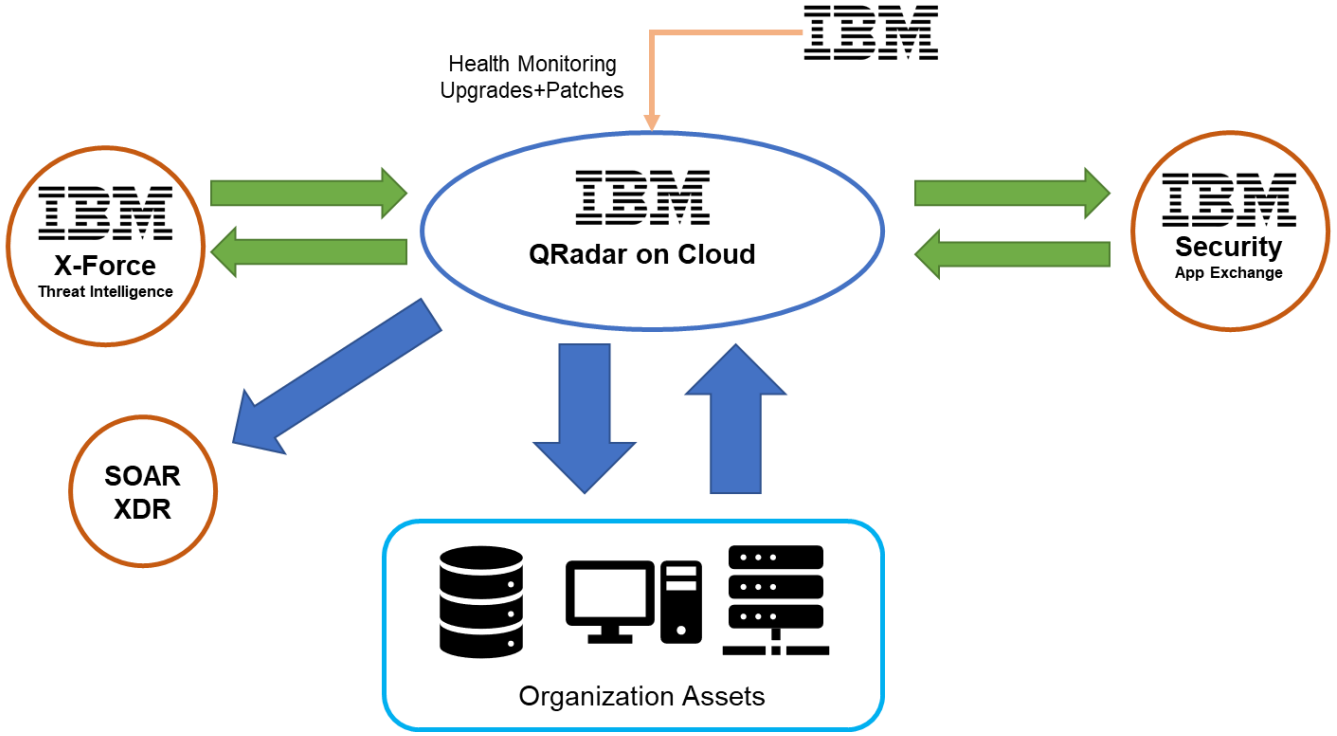
QRadar SIEM gives analysts the tools necessary to dig into critical anomalies and find potential infections or attacks. We outlined one scenario above, but this level of correlation and analysis is present across QRadar SIEM to help organizations sort through mountains of data to find what matters. QRadar SIEM serves the most important information to the analysts front and center to help them make the best decisions that will bring the biggest benefit.

Reduce SIEM Overhead and Focus on What Matters

We investigated the benefits of QRadar on Cloud. QRoC reduces SIEM overhead by offloading application maintenance and upgrades to IBM's experts. QRoC runs 24/7 health checks to ensure the organization's instance is running optimally.

With SIEM infrastructure no longer a concern, organizations can focus on what matters—using QRoC to detect and remediate possible attacks and keeping their data and customers safe.

Figure 6. QRadar on Cloud (QRoC) Architecture



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Figure 6 shows how QRoC, similar to QRadar SIEM, fits within the IBM environment. Data from organizations' assets, such as servers, network devices, and endpoints, is sent to QRadar SIEM. QRoC features built-in integrations with XDR, threat intelligence, and SOAR tools so analysts can act efficiently. Meanwhile, IBM monitors instance health and applies upgrades and patches on behalf of the customer.

Why This Matters

Nearly one in three organizations surveyed by Enterprise Strategy Group (ESG) (32%) view SIEM infrastructure as resource-intensive and expensive to maintain. Companies struggle to keep their systems safe while trying to keep the SIEM up and running.

QRadar on Cloud gives organizations access to powerful correlation and analytical tools while maintaining the health of the SIEM on behalf of the customer. With SIEM infrastructure taken care of, businesses can focus on what matters—detecting and remediating possible attacks and keeping their data and customers safe.

The Bigger Truth

Modern organizations need help from automated systems to detect and remediate threats. However, implementing robust SIEM functionality is difficult due to the massive amount of data and potential false positives analysts must dig through in conjunction with the resource-intensive upkeep of the SIEM application itself.

Enterprise Strategy Group (ESG) observed QRadar SIEM's ability to help analysts find what matters while helping organizations avoid large resource costs to maintain SIEM software through its QRadar on Cloud offering. QRoC provides multiple third-party integrations with tools such as security orchestration, automation, and response (SOAR) and threat intelligence to provide the ability to find possible intrusions and stop them immediately. IBM handles health monitoring and upgrades, so organizations don't have to manage SIEM infrastructure to gain its benefits.

QRadar SIEM's ability to correlate multiple pieces of data allows analysts to spend their time proactively investigating incidents in real time rather than reacting to what has happened in the past. QRadar SIEM sorts out the noise and leaves what matters most. Powerful network and user behavior analysis identifies outliers and divergent behavior so these can be investigated and mitigated. QRadar SIEM's correlation capabilities eliminate data overwhelm for analysts and prioritize events for them. With QRadar SIEM, an organization's SOC can act with confidence and speed.

If your organization is looking to optimize SOC resources without a large investment in SIEM infrastructure, then ESG believes that you should consider QRadar SIEM.

Enterprise Strategy Group by TechTarget

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188