IBM Security QRadar SIEM

Boost threat protection and compliance with an integrated investigative reporting system

Highlights

- Integrate log management and network threat protection technologies within a common database and shared dashboard user interface
- Reduce thousands of security events into a manageable list of suspected offenses
- Detect and track malicious activity over extended time periods, helping to uncover advanced threats often missed by other security solutions
- Detect insider fraud with advanced capabilities
- Help exceed regulation mandates and support compliance

Today's networks are larger and more complex than ever before, and protecting them against malicious activity is a never-ending task. Organizations seeking to safeguard their intellectual property, protect their customer identities and avoid business disruptions need to do more than monitor logs and network flow data; they need to leverage advanced tools to detect these activities in a consumable manner. IBM® Security QRadar® SIEM can serve as the anchor solution within a small or large organization's security operations center to collect, normalize and correlate available network data using years' worth of contextual insights. The result is something called *security intelligence*.

At the heart of this product sits a highly scalable database designed to capture real-time log event and network flow data, revealing the footprints of would-be attackers. QRadar SIEM is an enterprise solution that consolidates log source event data from thousands of devices distributed across a network, storing every activity in its raw form, and then performing immediate correlation activities to distinguish the real threats from false positives. It also captures real-time Layer 4 network flow data and, more uniquely, Layer 7 application payloads, using deep packet inspection technology.

An intuitive user interface shared across all QRadar family components helps IT personnel quickly identify and remediate network attacks by rank, ordering hundreds of alerts and patterns of anomalous activity into a drastically reduced number of *offenses* warranting further investigation.

Providing real-time visibility for threat detection and prioritization

QRadar SIEM provides contextual and actionable surveillance across the entire IT infrastructure, helping organizations detect and remediate threats often missed by other security solutions. These threats can include inappropriate use of applications; insider fraud; and advanced, "low and slow" threats easily lost in the "noise" of millions of events.

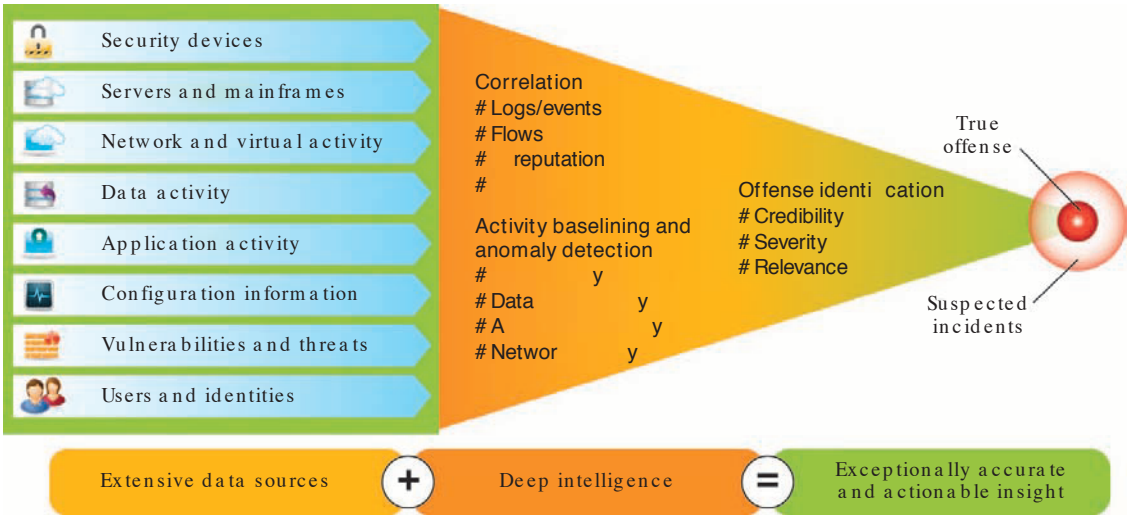
QRadar SIEM collects information that includes:

- **Security events:** Events from firewalls, virtual private networks, intrusion detection systems, intrusion prevention systems and more
- **Network events:** Events from switches, routers, servers, hosts and more
- **Network activity context:** Layer 7 application context from network and application traffic
- **User or asset context:** Contextual data from identity and access-management products and vulnerability scanners
- **Operating system information:** Vendor name and version number specifics for network assets
- **Application logs:** Enterprise resource planning (ERP), workflow, application databases, management platforms and more

Reducing and prioritizing alerts to focus investigations into actionable offenses

Many organizations create millions—or even billions—of events per day, and distilling that data down to a short list of priority offenses can be daunting. QRadar SIEM automatically discovers most network log source devices and inspects network flow data to find and classify valid hosts and servers (assets) on the network—tracking the applications, protocols, services and ports they use. It collects, stores and analyzes this data and performs real-time event correlation for use in threat detection and compliance reporting and auditing. Billions of events and flows can therefore be reduced and prioritized into a handful of actionable offenses, according to their business impact.

As a result, security professionals normally begin to see value from a QRadar SIEM installation in days rather than weeks, and deployments occur without a small army of expensive consultants. Automatic discovery features and out-of-the-box templates and filters mean you don't spend months teaching the system about your environment as with more generalized IT operational tools. The architecture employs multiple models of event processor appliances, event collector appliances, flow processor appliances and a central console, all available as hardware-based, software-only or as virtual software appliances. Smaller installations can start with a single all-in-one solution and easily be upgraded to console deployments, adding event and flow processor appliances as needed.



QRadar SIEM captures data across a broad range of feeds, reducing it to a manageable list of offenses using pre-existing and customer-defined rules.

Answering key questions for more effective threat management

Security teams need to answer key questions to fully understand the nature of their potential threats: Who is attacking? What is being attacked? What is the business impact? Where do I investigate? QRadar SIEM tracks significant incidents and threats, building a history of supporting data and relevant information. Details such as attack targets, point in time, asset value, vulnerability state, offending users' identities, attacker profiles, active threats and records of previous offenses all help provide security teams with the intelligence they need to act.

Real-time, location-based and historical searching of event and flow data for analysis and forensics can greatly improve an organization's ability to assess activities and resolve incidents. With easy-to-use dashboards, time-series views, drill-down searching, packet-level content visibility and hundreds of predefined searches, users can quickly aggregate data to summarize and identify anomalies and top activity contributors. They can also perform federated searches across large, geographically distributed environments.

Gaining application visibility and anomaly detection

QRadar SIEM supports a variety of anomaly detection capabilities to identify changes in behavior affecting applications, hosts, servers and areas of the network. For example, QRadar SIEM can detect off-hours or excessive usage of an application or cloud-based service, or network activity patterns that are inconsistent with historical, moving-average profiles and seasonal usage patterns. QRadar SIEM learns to recognize these daily and weekly usage profiles, helping IT personnel to quickly identify meaningful deviations.

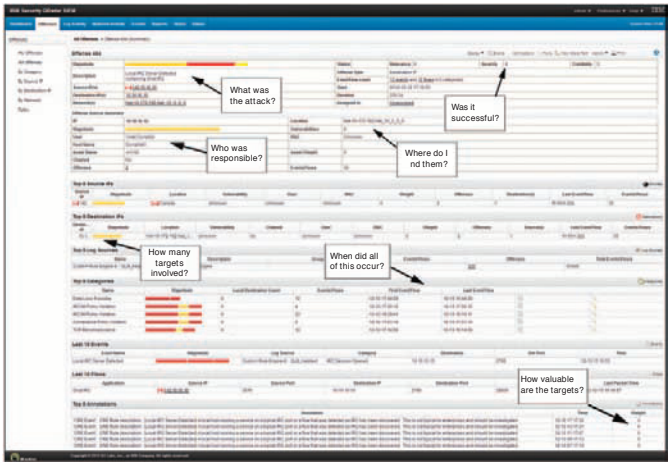
The QRadar SIEM centralized database stores log source events and network flow traffic together, helping to correlate discrete events with bidirectional network flow activity emanating from the same IP source. It also can group network flow traffic and record operations occurring within a narrow time period as a single database entry to help reduce storage consumption and conserve license requirements.

Its ability to detect application traffic at Layer 7 enables QRadar SIEM to provide accurate analysis and insight into an organization's network for policy, threat and general network activity monitoring. With the addition of an IBM Security QRadar QFlow or VFlow Collector appliance, QRadar SIEM can monitor the use of applications such as ERP, databases, Skype, voice over IP (VoIP) and social media from within the network. This includes insight into who is using what, analysis and alerts for content transmission, and correlation with other network and log activity to reveal inappropriate data transfers and excessive usage patterns. While QRadar SIEM ships with numerous anomaly and behavioral detection rules, security teams can also create their own through a filtering capability that enables them to apply anomaly detection against time-series data.

Commanding a highly intuitive, one-console security solution

QRadar SIEM provides a solid foundation for an organization's security operations center by providing a centralized user interface that offers role-based access by function and a global view to access real-time analysis, incident management and reporting. Five default dashboards are available—including security, network activity, application activity, system monitoring and compliance—plus users can create and customize their own workspaces.

These dashboards make it easy to spot spikes in alert activity that may signal the beginnings of an attack. Clicking on a graph launches a drill-down capability that enables security teams to quickly investigate the highlighted events or network flows related to a suspected offense. Furthermore, hundreds of templates relevant to specific roles, devices, compliance regulations and vertical industries are available to speed report generation.



QRadar SIEM offers a wealth of forensic detail behind every suspected offense and an ability to tune existing rules or add new ones to reduce false positives.

Extending threat protection to virtual environments

Since virtual servers are just as susceptible to security vulnerabilities as physical servers, comprehensive security intelligence solutions must also include appropriate measures to protect the applications and data residing within the virtual data center. Using QRadar VFlow Collector appliances, IT professionals gain increased visibility into the vast amount of business

application activity within their virtual networks and can better identify these applications for security monitoring, application layer behavior analysis and anomaly detection. Operators can also capture application content for deeper security and policy forensics.

Producing detailed data access and user activity reports to manage compliance

QRadar SIEM provides the transparency, accountability and measurability critical to an organization's success in meeting regulatory mandates and reporting on compliance. The solution's ability to correlate and integrate surveillance feeds yields more complete metrics reporting on IT risks for auditors, as well as hundreds of reports and rules templates to address industry compliance requirements.

Organizations can efficiently respond to compliance-driven IT security requirements with the extensibility of QRadar SIEM to include new definitions, regulations and best practices through automatic updates. In addition, profiles of all network assets can be grouped by business function—for example, servers that are subject to Health Insurance Portability and Accountability Act (HIPAA) compliance audits.

The solution's pre-built dashboards, reports and rules templates are designed for the following regulations and control frameworks: CobiT, SOX, GLBA, NERC/FERC, FISMA, PCI DSS, HIPAA, UK GSi/GCSx, GPG and more.

Adding high-availability and disaster-recovery capabilities

To achieve high-availability and disaster-recovery capabilities, identical secondary systems can be paired with all members of the QRadar appliance family. From event processor appliances, to flow processor appliances, to all-in-one and console SIEM appliances, users can add robustness and protection where and when it is needed—helping to ensure continuous operations.

For organizations seeking business resiliency, QRadar high-availability solutions deliver integrated automatic failover and full-disk synchronization between systems. These solutions are easily deployed through architecturally elegant plug-and-play appliances, and there is no need for additional third-party fault management products.

For organizations seeking data protection and recovery, QRadar disaster-recovery solutions forward live data (e.g., flows and events) from a primary QRadar system to a secondary parallel system located at a separate facility.

Profiling for vulnerabilities

IBM Security QRadar Risk Manager complements QRadar SIEM by identifying a network's most vulnerable assets. It can immediately generate alerts when these systems engage in activity that potentially exposes them. For example, organizations can scan their networks for unpatched applications, devices and systems, determine which ones connect to the Internet and prioritize remediation based on the risk profile of each application. For more information please see the QRadar Risk Manager data sheet.

Receiving comprehensive device support to capture network events and flows

With support for more than 450 products from virtually every leading vendor deployed in enterprise networks, QRadar SIEM provides collection, analysis and correlation across a broad spectrum of systems, including networked solutions, security solutions, servers, hosts, operating systems and applications. In addition, QRadar SIEM is easily extended to support proprietary applications and new systems from IBM and many other vendors.

Why IBM?

IBM operates the world's broadest security research, development and delivery organization. IBM solutions empower organizations to reduce their security vulnerabilities and focus more on the success of their strategic initiatives.

For more information

To learn more about how IBM Security QRadar SIEM can solve your organization's threat management and compliance challenges, contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/security.

About IBM Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 13 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

Additionally, IBM Global Financing can help you acquire the software capabilities that your business needs in the most cost-effective and strategic way possible. We'll partner with credit-qualified clients to customize a financing solution to suit your business and development goals, enable effective cash management, and improve your total cost of ownership. Fund your critical IT investment and propel your business forward with IBM Global Financing. For more information, visit: **ibm.com**/financing

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
January 2013

WGD03021-USEN-00