IBM QRadar SIEM

Highlights

- Gain comprehensive visibility into security data from a single console
- Reduce thousands of events into a manageable list of prioritized offenses
- Analyze network, endpoint, asset and user data to quickly detect threats
- Simplify compliance with automated data ingestion, correlation and reports
- Integrate threat intelligence from IBM® and third-parties using STIX/TAXII
- Achieve a quick time-to-value with over 450 default setting integrations
- Deploy a scalable platform on-premises, in the cloud or as a hybrid model

Today's networks are more complex than ever before, and protecting them from increasingly malicious and sophisticated attackers is a never-ending task. Organizations seeking to protect their customers' identities, safeguard their intellectual property and avoid business disruption need to proactively monitor their environment so that they can rapidly detect threats and accurately respond before attackers are able to cause material damage.

IBM QRadar® Security Information and Event Management (SIEM) is designed to provide security teams with centralized visibility into enterprise-wide security data and actionable insights into the highest priority threats. As a first step, the solution ingests a vast amount of data throughout the enterprise to provide a comprehensive view of activity throughout on-premises and cloud-based environments. As data is ingested, QRadar applies real-time, automated security intelligence to quickly and accurately detect and prioritize threats. Actionable alerts provide greater context into potential incidents, enabling security analysts to swiftly respond to limit the attackers' impact. Unlike other solutions, only QRadar is purpose-built to address security use cases and intentionally designed to easily scale with limited customization effort required.

Gain comprehensive, centralized visibility

Enterprise networks can span across traditional on-premises IT, cloud-based and operational technology (OT) environments, all of which require some level of oversight to effectively protect assets, accurately detect threats and maintain compliance. Before security teams can start analyzing data to detect and manage threats, they must first have centralized visibility into disparate security data. QRadar enables organizations to gain centralized, comprehensive visibility into siloed environments by collecting, parsing and normalizing both log and flow data.

The solution includes more than 450 pre-built Device Support Modules (DSMs), which provide default setting integrations with commercial off-the-shelf technologies. Customers can simply point logs to QRadar, and the solution can automatically detect the log source type and apply the correct DSM to parse and normalize and the log data. As a result, QRadar customers can get up and running much faster than customers of alternative solutions. Additional integrations can easily be added via apps in the IBM Security App Exchange. QRadar also offers a simple DSM Editor with an intuitive graphical user interface GUI that enables security teams to easily define how to parse logs from custom applications.

To help easily establish the asset database, which enables organizations to define critical assets or network segments, QRadar can inspect network flow data to automatically identify and classify valid assets on the network based on the applications, protocols, services and ports they use.

QRadar supports a wide variety of technologies, applications and cloud services to help customers gain comprehensive visibility into enterprise-wide activity. Once this data is centralized, it can be automatically analyzed to identify known threats, anomalies that may indicate unknown threats and critical risks that may leave sensitive data exposed.

Automate security intelligence to rapidly detect threats

QRadar SIEM is designed to automatically analyze and correlate activity across multiple data sources including logs, events, network flows, user activity, vulnerability information and threat intelligence to identify known and unknown threats.

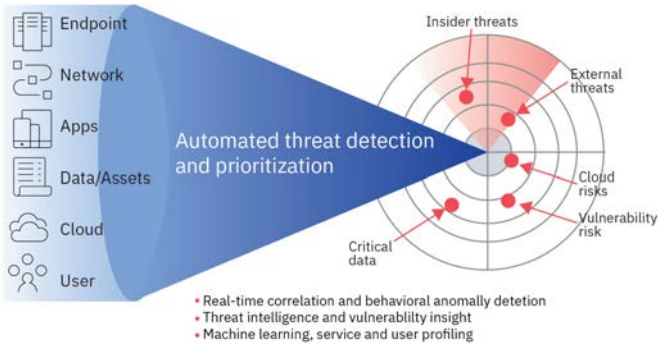

Figure 1: QRadar SIEM collects, analyzes and correlates data from a wide variety of sources to detect and prioritize the most critical threats that require investigation.

QRadar SIEM intelligently correlates and analyzes a variety of information, including the following activities:

- Security events: From firewalls, virtual private networks, intrusion detection systems, intrusion prevention systems, databases and more
- Network events: From switches, routers, servers, hosts and more
- Network activity context: Layer 7 application context from network and application traffic
- Cloud activity: From SaaS and Infrastructure as a Service (IaaS) environments, such as Office365, SalesForce.com, Amazon Web Services (AWS), Azure and Google Cloud
- User and asset context: Contextual data from identity and access management products and vulnerability scanners
- Endpoint events: From the Windows event log, Sysmon, EDR solutions and more
- Application logs: From enterprise resource planning (ERP) solutions, application databases, SaaS applications and more
- Threat intelligence: From sources such as IBM X-Force®

QRadar includes hundreds of pre-built security use cases, anomaly detection algorithms, rules and real-time correlation policies to detect known and unknown threats. As threats are discovered, the solution aggregates related security events into single, prioritized alerts known as “offenses.” Offenses are automatically prioritized based on both the severity of the threat and the criticality of the assets involved.

Within each offense, security analysts can see the full chain of threat activity from one single screen. From here, analysts can easily drill down into specific events or network flows to start an investigation, assign the offense to a specific analyst or close it out. Offenses are automatically updated as new related activity occurs so that analysts can see the most up-to-date information at any given time. This unique approach helps security analysts easily understand the most critical threats in the environment by providing end-to-end insight into each potential incident while simultaneously reducing the total alert volume.

Detect anomalous network, user and application activity

As attackers become more sophisticated in their techniques, known threat detection is no longer sufficient on its own. Instead, organizations must also have the ability to detect slight changes in network, user or system behavior that may indicate unknown threats, such as malicious insiders, compromised credentials or fileless malware.

QRadar contains a variety of anomaly detection capabilities to identify changes in behavior that could be indicators of an unknown threat. And the unique ability of QRadar to monitor and analyze Layer 7 application traffic enables it to more accurately identify anomalies that other solutions may miss.

By optionally using QRadar Network Insights as part of the SIEM deployment, organizations can gain insight into which systems communicated with each other, which applications were involved and what information was exchanged in the packets. By correlating this information with other network, log and user activity, security analysts can uncover abnormal network activity that may be indicative of compromised hosts, compromised users or data exfiltration attempts.

While QRadar ships with numerous anomaly and behavioral detection rules as default settings, security teams can also create their own rules, tailor anomaly detection settings and download over pre-built 160 apps from the IBM Security App Exchange to augment their deployment.

Better manage compliance with pre-built content, rules and reports

QRadar 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 threat intelligence feeds yields more complete metrics for reporting on IT risks for auditors. Hundreds of pre-built reports and rule templates can help organizations more easily address industry compliance requirements.

Profiles of network assets can be grouped by business function—for example, servers that are subject to Health Insurance Portability and Accountability Act (HIPAA) compliance audits—to help teams more easily report on relevant activity as needed.

QRadar has the experience and resources needed to help organizations address risk and regulatory exposure by providing default setting compliance packages for General Data Protection Regulation (GDPR), the Federal Information Security Management Act (FISMA), Sarbanes-Oxley (SOX), HIPAA, ISO 27001, Payment Card Industry Data Security Standard (PCI DSS) and more. These packages are included free of charge with a QRadar SIEM license and are available in the IBM Security App Exchange.

Easily scale with changing needs

The flexible, scalable architecture of QRadar is designed to support both large and small organizations with a variety of needs. Smaller organizations can start with a single all-in-one solution that can be easily upgraded into a distributed deployment as needs evolve. Larger enterprise organizations can deploy dedicated components to support global, distributed networks with high data volumes. The QRadar SIEM solution includes the following components: event collectors, event processors, flow collectors, flow processors, data nodes (for low cost storage and increased performance) and a central console. All components are available as hardware, software or virtual appliances. Software and virtual appliance options can be deployed on-premises, in IaaS environments or distributed across hybrid environments.

Regardless of deployment model, organizations can optionally add in high availability and disaster recovery protection where and when needed to help to ensure continuous operations. For organizations seeking business resiliency, QRadar delivers integrated automatic failover and full-disk synchronization between systems without the need for additional third-party fault management products. For organizations seeking data protection and recovery, QRadar disaster recovery solutions can forward live data, such as flows and events, from a primary QRadar system to a secondary parallel system located at a separate facility.

About IBM QRadar

IBM QRadar SIEM sits at the core of the IBM QRadar Security Intelligence Platform, which applies automated, intelligent analytics to a vast amount of security data to provide security analysts with actionable insight into the most critical threats, enabling them to make better, faster triage and response decisions.

This comprehensive platform brings together log management SIEM, network analysis, vulnerability management, user behavior analytics, threat intelligence and AI-powered investigations into one single platform managed from a single interface.

Components of the solution are fully integrated, enabling customers to start as small or large as they choose and easily scale up or down as their needs change. Learn more at: ibm.com/qradar.

Why IBM Security?

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world renowned 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, monitoring greater than 60 billion security events per day in more than 130 countries, and the corporation holds more than 3,700 security patents.

IBM Corporation
Route 100
Somers, NY 10589

Produced in the United States of America
February 2019

Please Recycle

04023704USEN-00