IBM QRadar SIEM

Detect threats with IBM QRadar Security Information and Event Management (SIEM)

Today's networks are larger and more complex than ever before, and protecting them against increasingly malicious attackers is a never-ending task. Organisations 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, easy-to-use solutions to quickly detect security offenses and take action.

IBM® QRadar® SIEM can serve as the anchor solution within a small, medium or large organization's security operations center to collect, normalise and correlate network data using years' worth of contextual insights. It also integrates with hundreds of IBM and non-IBM products and provides complete, unified visibility to security events in on-premises, hybrid, and cloud environments.

An advanced Sense Analytics Engine is at the heart of this solution, designed to capture real-time log event and network flow data, and apply advanced analytics to reveal the footprints of would-be attackers. QRadar SIEM is a highly scalable, enterprise solution that consolidates log source event data from thousands of devices distributed across a network, storing every activity in its database, and then performing immediate correlation and application of analytics to distinguish real threats from false positives. It also captures 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 based on priority, ranking hundreds of alerts and patterns of anomalous activity into a drastically reduced number of offenses warranting further investigation.

QRadar SIEM deploys quickly and easily, providing 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 theft; and advanced, "low and slow" threats easily lost in the "noise" of millions of events.

QRadar SIEM collects information that includes:

- 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
- 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
- Threat Intelligence: From sources such as IBM X-Force

Reducing and prioritizing alerts to focus on the most important offenses

Many organizations create millions—or even billions—of events per day, and distilling that data down to a short, prioritised list of offenses can be daunting. QRadar SIEM automatically discovers 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 be reduced and prioritized into a handful of actionable offenses, according to their importance and business impact.

As a result, security professionals normally begin to see value from a QRadar SIEM installation in days rather than weeks or months, 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 processors, event collectors, flow processors, flow collectors, data nodes (for low cost storage and increased performance), QFlow and VFlow offerings, and a central console, all available as hardware, software, or 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.

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 investigate and resolve incidents. With easy-to-use dashboards, time-series views, drill-down searching, packet-level content visibility, and hundreds of out-of-the box, customizable rules and 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.

Anomaly detection and application visibility

QRadar SIEM contains a variety of anomaly detection capabilities to identify changes in behavior that could be indications of an insider threat. 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 significant deviations. The QRadar SIEM centralised 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.

The 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.

Highly intuitive, single-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.

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 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 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 help 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 rule templates to help 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 frame-works: CobiT, SOX, GLBA, NERC/FERC, FISMA, PCI DSS, HIPAA, UK GSi/GCSx, GPG and more.

For further information contact Kat Hill on 07972 623387 or email kat.hill@scc.com

Extend QRadar SIEM with apps from the IBM Security App Exchange

The capabilities of QRadar SIEM can be expanded further by downloading apps from the IBM Security App Exchange. This exchange allows customers, developers, business partners, and clients to collaborate and share applications, dashboards, custom rules, reports, and other enhancements to QRadar SIEM. Solutions can be found here to help address the latest security threats, without having to wait until the next product release.

Adding high-availability and disasterrecovery

To implement high-availability and disaster-recovery, identical secondary systems can be paired with all members of the QRadar appliance family. From event processor appliances, to flow processor appliances, to data nodes, 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 delivers 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. While QRadar SIEM ships with numerous anomaly and behavioural detection rules out-of-the box, security teams can also create their own rules through a filtering capability that enables them to apply anomaly detection against time-series data.

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 we choose IBM

SCC has partnered with IBM for almost 40 years; SCC bridges the gap between business needs and technology to deliver world-class solutions. We know IBM inside out, from its technology to its people and vision, and whatever we do together delivers the strongest, most agile solution.

SCC's CSS service is powered by IBM QRadar which is an enterprise class toolset which is recognised as a leader by multiple independent analyst firms, including being the Gartner Magic Quadrant Leader in SIEM for the last 8 years. SCC complement our multi-tenanted deployment of QRadar with a team of highly experienced security professionals and proven operational processes to deliver the same CSS service we deliver to Government organisations to our commercial clients, adopting the IS027001 and NIST legislations as standard in every aspect of the service we provide. Built on years of experience SCC are able to significantly reduce both the time and cost of deployment by removing the need for complex professional services work to install and tune the tools, providing our clients quicker time to value

For further information contact Kat Hill on 07972 623387 or email kat.hill@scc.com