Q1 Labs®
Total Security Intelligence | An IBM Company

QRadar SIEM

Providing the security intelligence needed to protect IT networks and assets from a growing landscape of sophisticated threats and emerging compliance mandates.

Total Intelligence & Visibility For Today's Security Challenges

As the most intelligent, integrated and automated SIEM solution in the industry, QRadar® SIEM delivers deep visibility into network, user and application activity providing organizations with intelligence into potential and existing threats across their entire network.

SIEM for the Entire Organization

Built on the highly flexible QRadar Security Intelligence Platform, QRadar SIEM provides a next-generation solution that can mature with an organization, scale to support a growing infrastructure and deliver a common user experience to many groups across the organization. With log management, advanced threat detection, and policy-aware compliance management all combined in QRadar SIEM, organizations benefit with a tightly integrated solution that quickly and easily delivers corporate-wide security intelligence.

Real-time Visibility for Threat, Compliance & Log Management

Threat Detection & Prioritization

Internet-based threats and fraud continue to proliferate in today's complex networks. Compounding this problem is a steady rise in insider theft of valuable corporate information. QRadar SIEM consolidates siloed information to more effectively detect and manage complex threats. The information is normalized and correlated to quickly deliver intelligence that allows organizations to detect, notify and respond to threats missed by other security solutions with isolated visibility.

QRadar SIEM provides contextual and actionable surveillance across an entire IT infrastructure allowing an organization to detect and remediate threats such as: inappropriate use of applications, insider fraud, threats that could be lost in the noise of millions of events, and more.

QRadar SIEM collects the following:

- **Security Events** - Events from firewalls, VPNs, IDS/IPS, etc.
- **Network Activity Context** - Layer 7 application context from network and application traffic
- **User/Asset Context** - Contextual data from IAM products and vulnerability scanners
- **Network Events** - Events from switches, routers, servers, hosts, etc.
- **Application Logs** - ERP, workflow, application databases, management platforms, etc.

QRadar® SIEM

QRadar SIEM helps security teams, IT operations, auditing and lines of business:

- DETECT THREATS OTHERS MISS
- EXCEED REGULATION MANDATES
- PREDICT RISKS AGAINST THEIR BUSINESS
- DETECT INSIDER FRAUD
- CONSOLIDATE DATA SILOS

QRadar SIEM

The Key to Data Management: Reduce & Prioritize to Actionable Offenses

With some organizations creating millions or billions of events per day, distilling that data down to priority offenses can be a daunting task. QRadar SIEM collects, stores and analyzes informational data and provides real-time event correlation for use in threat detection and compliance reporting and auditing. Billions of events and flows can be reduced and prioritized down to a handful of actionable offenses according to their business impact.

QRadar SIEM provides long-term collection, archival, search and reporting of events and application data making it easier for auditing and searching for advanced persistent threats or low and slow attacks.

Managing Threats: Who, What, Where, When, How?

Security teams need to understand: Who is attacking? What is being attacked? What is the business impact? Where do I investigate? QRadar SIEM tracks significant incidents and threats and builds a history of supporting and relevant information. Information such as point in time, offending users or targets, attacker profiles, vulnerability state, asset value, active threats and records of previous offenses all help provide security teams with the intelligence they need to act regardless of where they are.

Application Visibility & Anomaly Detection

QRadar SIEM supports a variety of anomaly detection capabilities to identify changes in behavior against applications, hosts, servers and areas of the network. For example, off hours or excessive usage of an application or cloud-based service or network activity patterns which are inconsistent with historical profiles.

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. To further improve visibility into the network, QRadar SIEM now has the ability to monitor the usage of applications like Skype and social media (including Twitter, LinkedIn, etc.) 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.

QRadar SIEM supports a variety of out of the box anomaly and behavioral detection rules. Users can customize their own views through a simple to use filtering capability and apply anomaly detection to any time series data.

Virtual Environments

Since virtual servers are just as susceptible to security vulnerabilities as physical servers, organizations now must define and implement appropriate measures to protect their applications and data that reside within the virtual data center. Now IT professionals can have increased visibility into the vast amount of business application activity appearing across their virtual networks and 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.

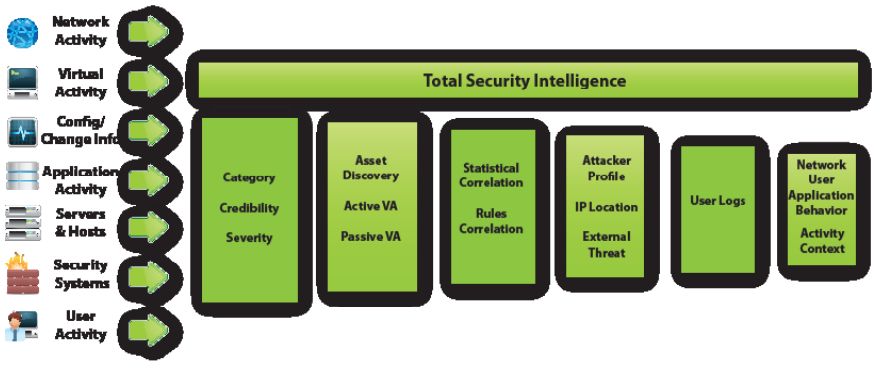
Client-side Vulnerability Profiling

QRadar SIEM identifies a network's most vulnerable assets and detects and alerts immediately when these systems engage in activity that potentially exposes those vulnerabilities. For example, organizations can scan

> One of the greatest benefits we've achieved with QRadar so far was our ability to quickly identify which hosts were affected by the 'Hear You Have' virus that attempted to infiltrate our network," continued Moser. "QRadar alerted us immediately when users tried to access websites that were housing the virus, or when infected hosts attempted to pass through our firewall when calling home.
>
> **–TY MOSER,**
> *Network and Smart Grid Analyst for SRP*

QRadar SIEM

SECURITY INTELLIGENCE: MASSIVE DATA REDUCTION WITH PINPOINT ACCURACY



their network for unpatched applications, devices and systems, determine which ones connect to the internet and prioritize remediation based on the risk profile of each application.

Advanced Forensics

Real-time, location-based and historical searching of flow and event data for analysis and forensics greatly improves the ability to assess activities and incident resolution. With easy to use dashboards, time series views with drill down capabilities, packet level visibility of content and hundreds of predefined searches and views, users can quickly aggregate data to summarize and identify anomalies and top activity contributors. Federated searches can also be performed across large, geographically distributed environments.

Compliance Management

QRadar SIEM brings the transparency, accountability and measurability critical to the success of meeting regulatory mandates and reporting on compliance. QRadar SIEM's unique correlation and integration of all surveillance feeds yields:

- **More complete metrics reporting around IT risks for auditors**
- **Thousands of reports and rules templates to address industry compliance requirements**

Organizations can efficiently respond to compliance-driven IT security requirements with QRadar SIEM's extensibility to include new definitions, regulations and best practices through auto-updates. In addition, profiles of all the assets on the network can be grouped by business function (e.g. servers that are subject to HIPAA compliance audits).

QRadar provides prebuilt dashboards, reports and rules templates for the following regulations and control frameworks: CobiT, SOX, GLBA, NERC/FERC, FISMA, PCI-DSS, HIPAA, & UK GSi/GCSx, GPG, and more.

Highly Intuitive One Console Security

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. Default dashboards are available by function and users can create and customize their own workspaces. This drill down capability makes it easier to identify and select a spike of events or network flows relative to an offense. 3,500 report templates relevant to specific roles, devices, compliance regulations and vertical industry are available out of the box.

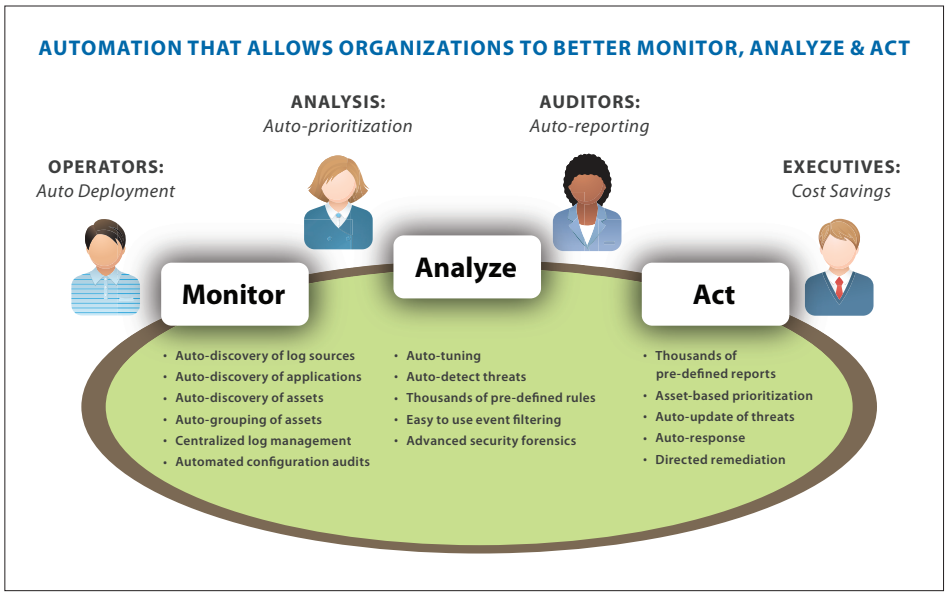
QRadar® SIEM

> Our primary goal for deploying a SIEM was to meet compliance mandates, but we wanted to go above and beyond what the various regulations required of us, and use the additional information captured by QRadar to really make our network, and the services and applications it delivers, secure. We want our customers to have faith that we're keeping their personal information well-protected, and QRadar enables us to do that. Additionally, we chose Q1 Labs because they provided us with the most security intelligence and the best customer support.
>
> **–JEFF DALTON,**
> *Technical Operations Officer for Regulus*

QRadar SIEM

Unlike SIEM solutions that require customization and manual configurations for operation, QRadar SIEM delivers valuable out of the box content that automates processes such as discovery of event sources and assets, as well as the profiling of applications. In addition, QRadar SIEM auto-updates content on a weekly basis including content from third party intelligence sources. With minimal customization required, organizations can realize results almost immediately.

QRadar SIEM allows organizations to better monitor, analyze and act with the most powerful auto-deployment, auto-prioritization, auto-reporting and efficient SIEM available.



Scalability & High Availability

QRadar SIEM was designed from the ground up to work as a complete, integrated solution. QRadar SIEM provides a solution that offers a common platform and user interface for all security intelligence tasks. QRadar SIEM comes as an all-in-one solution for small and medium sized businesses or an enterprise-level solution that is immensely scalable for medium to large deployments.

For organizations looking for business resiliency, QRadar High Availability (HA) delivers highly integrated automatic failover and full disk synchronization between systems. QRadar HA provides high availability of data storage and analysis is easily deployed through architecturally-elegant plug-and-play appliances, and there is no need to add additional third-party fault management products.

Heterogeneous Device Support:

With support for over 200 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. QRadar SIEM supports devices from F5, Cisco, Juniper, Nortel, Checkpoint, Oracle, Sun, Enterasys, Symantec, ISS/IBM, McAfee, Sourcefire, RSA and many more.

Thousands of Customers Depend on Q1 Labs for Security & Compliance Management

The QRadar Security Intelligence Platform is used across the world by healthcare providers, energy firms, retail organizations, utility companies, financial institutions, government agencies, and universities, among others. Contact us today to see a demo or learn how QRadar SIEM can solve your company's threat management and compliance challenges.

Q1 Labs, an IBM company
890 Winter Street , Suite 230
Waltham, MA 02451 USA
1.781.250.5800, info@Q1Labs.com

DSQRSIEM1111