Q1 Labs®
Total Security Intelligence

QRadar Risk Manager

Assess Information Risk Before the Network is Exploited

Preventing Risk: A Key to Total Security Intelligence

Log Management and Security Information and Event Management (SIEM) have become trusted solutions for network and security operators, enabling them to quickly detect and isolate security incidents and meet specific compliance requirements, as well as a growing number of regulatory mandates.

Although the information provided by SIEM is critical for network and compliance security management efforts, it primarily detects exploits as they occur, rather than prioritize what actions can be taken to prevent exploits from happening in the first place.

Information and security professionals, tasked with keeping their organization secure, are continuously challenged with improving their abilities to manage risk across an ever-growing spectrum of vulnerabilities and compliance mandates, before a breach actually occurs.

QRadar® Risk Manager leverages and extends the value of a SIEM deployment to provide organizations with total security intelligence and greatly improves the ability to automate risk management functions in mission critical areas, including network and security configuration, compliance management, and vulnerability assessment.

's

Risk Manager Connection Viewer

QRadar Risk Manager

Leading Organizations Choose QRadar® Risk Manager to:

- ASSESS COMPLIANCE RISK
- PRIORITIZE VULNERABILITIES
- MEET NETWORK CONFIGURATION BASELINES
- DETERMINE RISK OF NETWORK AND CONFIGURATION CHANGES
- INCREASE OPERATIONAL EFFICIENCY WITH AUTOMATED CONFIGURATION MONITORING AND AUDIT
- GAIN VISIBILITY INTO NETWORK TRAFFIC
- MONITOR HIGH RISK NETWORKS

QRadar Risk Manager - Key Capabilities

Automated Risk Management

Regulations define specific traffic and firewall policies that must be deployed, monitored, audited, and enforced. Yet many attacks on a network come from inconsistent network and security configuration practices highlighting the need for automated network configuration audits and alerts of policy breaches. Unfortunately, due to the silos created by traditional SIEM and log management solutions, organizations often lack the ability to seamlessly assess when a network configuration allows traffic that is "out of policy" by a regulation, corporate mandate, or industry best practice.

QRadar Risk Manager integrates risk management, SIEM, log management and network behavior analysis to automate risk management functions in mission critical areas, including network and security configuration, policy, and compliance management. It greatly improves an organization's ability to assess information security risk and is delivered in a single, integrated console. The solution automates the assessment of security policies while leveraging the broadest range of risk indicators, including network and security configuration data, network activity data, network and security events, and vulnerability scan results. Key capabilities of QRadar Risk Manager include:

A recent data breach investigations report by Verizon [1] revealed that:

> "The majority of breaches still occur because basic controls were not in place or because those that were present were not consistently implemented across the organization"

> "Many organizations set security policies and procedures yet fail to implement them consistently."

[1] 2009 Data Breach Investigations Report, Verizon Business Risk Team

Network Security Configuration

- Detailed configuration audit helps improve consistency of firewall rules
- Security-focused network topology enables automated monitoring of configuration rules
- Configuration change notification quickly alerts risky or out-of-compliance configuration

Network Activity Monitoring

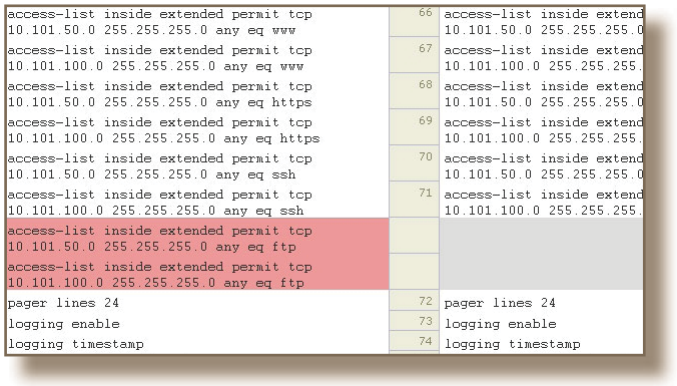
- Advanced monitoring and analysis of network activity features quickly flag out-of-policy traffic
- Fast and efficient search of network activity greatly reduces forensics effort
- Intuitive visualization tool provides interactive analysis of network activity

Network/Security Events

- Analysis of firewall allow/deny events to assess of policy effectiveness
- Automated audit of device configuration, after configuration change events, ensures record of the most up-to-date configuration
- Advanced asset database leverages information from a wide variety of network/security events and improves accuracy of results

Vulnerability Scan Results

- Integrated understanding of network topology helps deliver a prioritized list of vulnerabilities to better assess which systems are most vulnerable to attack
- Centralized policy monitoring delivers improved compliance verification
- Advanced vulnerability modeling, simulation, and visualization provides before, during and after assessment of vulnerability risks



Snapshot of QRadar Risk Manager's Configuration Monitor

QRadar Risk Manager - Key Features and Benefits

Policy Monitoring

QRadar Risk Manager features an automated knowledge engine that simplifies the assessment of a wide spectrum of information security and compliance policies. With an intuitive question-based template, the knowledge engine integrates previously disparate indicators of risk, including configuration data, network activity data, network and security events, and vulnerability scan data.

A comprehensive out-of-the-box library of industry-optimized policy templates help assess risk across multiple regulatory mandates and information security best practices such as PCI, HIPAA, CoCo and ISO 27001, etc. These templates can be easily extended to align with an organization's internal information security policies.

Device Configuration and Topology

QRadar Risk Manager's provides automated collection, monitoring, and audit of configuration of devices across an organization's switches, routers, firewalls, and IDS/IPS's. Through a unique ability to normalize device configuration, QRadar Risk Manager provides a detailed and intuitive assessment of how devices are configured, including defined firewall rules, security policy, and network hierarchy to seamlessly assess when a network configuration allows traffic that is "out of policy" by a regulation, corporate mandate, or industry best practice.

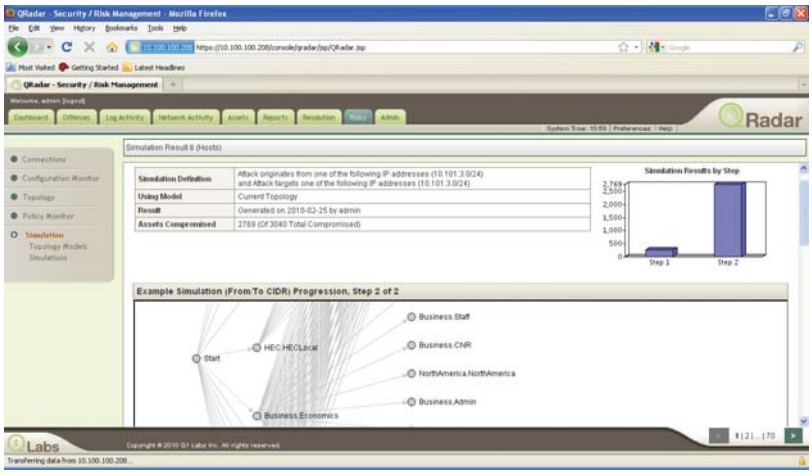
QRadar Risk Manager maintains a history of configuration changes and allows users to audit this history across a multi-vendor network. This powerful capability allows users to compare normalized device configurations, over time, from a single device or from different devices through a single user interface, making it easier to audit configuration. The collection of device configuration data is also instrumental in building an enterprise-wide representation of a network's topology.

This topology mapping helps an organization to understand allowed and denied activity across the entire network, resulting in improved consistency of device configuration that introduce risk to the network and flagged configuration changes.

Modeling and Simulation of Network and Security Events

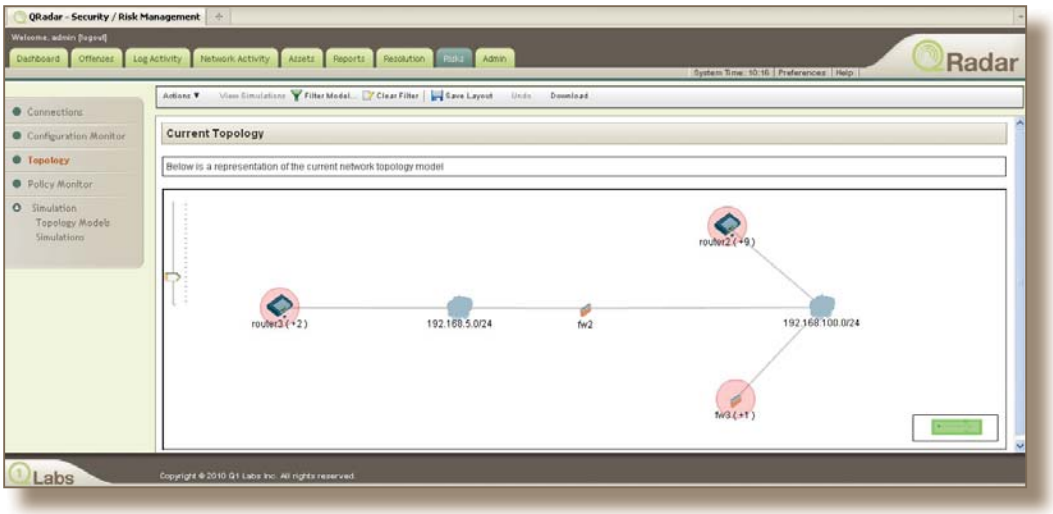
With modeling and simulation, QRadar Risk Manager helps organizations prioritize their most significant areas of risk. With simulation, an organization can quickly understand the risk impact of proposed changes to a network's configuration, before the changes are implemented. For example, QRadar Risk Manager's unique understanding of vulnerabilities, as reported by leading VA scanners, in conjunction with active network topology profiling provided by the device configuration and topology features, provides a unique prioritization of the most vulnerable systems.

This prioritization is delivered via reports and not only summarizes which assets have vulnerabilities, but exposes those assets that are vulnerable due to the configuration of the network, resulting in improved operational efficiency and network security.



QRadar Risk Manager Attack Simulation

QRadar Risk Manager



QRadar Risk Manager
Topology Viewer

Advanced Network Visualization

QRadar Risk Manager offers two network visualization security tools, providing unique, risk-focused, graphical representations of the network. The end result of both these visualizations offers network and security teams a revolutionary investigative capacity by providing before, during and after vulnerability information. The first, called the "Network Topology", delivers detailed views into how network traffic can and does traverse a network. Different than all other network topologies, this insight comes from a unique combination of data sources, including device configuration, network activity data (from flows), and security events (i.e. firewall allows/ denies).

The second, called the "Connection Monitor" is a fast and efficient tool for investigating and analyzing historical network activity. Adding value to these visualizations are network mappings that allow visualizations to assess when traffic can and does occur with specific geographic regions or known high risk networks.

Go On the Offensive with Total Security Intelligence

QRadar Risk Manager provides organizations with a comprehensive network security solution, allowing them to get not only the forensics of the "during" and "after" an attack, but also enabling them to answer the "What if?" ahead of time, minimizing the risk on their networks and their operations.

QRadar Risk Manager's powerful security analytics and simulation and visualization provides a unique opportunity for organizations to move away from day-to-day security fire fighting and adopt a holistic risk-based methodology that greatly strengthens network and security offenses while minimizing risk of exploit.

Log Management and SIEM are necessary for a good defense. By adding QRadar Risk Manager organizations have total security intelligence and can go on the offensive against those that wish to do the network harm.

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

DSQRM0211