Cisco Firepower App and IBM QRadar SIEM

Stop Threats at the Edge

Benefits

In today's fast-evolving threat landscape, organizations must quickly identify and thwart suspicious activity in their networks. Through the Cisco Firepower app and IBM QRadar, organizations can:

- Enhance visibility across the entire network
- Accelerate threat detection and incident response
- Avoid alert fatigue with the potential of missing alerts in the noise of event data
- Detect long and slow attacks
- Identify and prioritize threats in real time and escalate to identify the most critical incidents

Overview

The Cisco Firepower® app and IBM QRadar Security Information and Event Management (SIEM) integration delivers more streamlined and effective security for organizations. Downloadable via the IBM Security App Exchange, this powerful integration shares valuable threat data while providing a consolidated view of security events across the network, applications, and users without the need to pivot on disparate tools and interfaces. Security analysts can more quickly identify top priorities for threat investigation, understand the full scope and veracity of attacks, and automate incident investigation and response.

The Cisco Firepower and IBM QRadar integration provides extended visibility and context across Cisco® alerts and log data derived from Cisco Firepower's firewalls, intrusion prevention, and advanced malware protection capabilities and flows it directly into the QRadar security event dashboard. This consolidated view of easy-to-understand metrics and graphs enables security analysts to drill down into the detailed event data for faster, more accurate threat detection and response.

QRadar collects highly contextualized security information from Cisco Firepower and parses it into the QRadar database for analysis. Joint customers of both solutions can search, correlate, and analyze Cisco Firepower event types. Event components include intrusion events prioritized and organized by impact flag, malware events, connection and firewall events, discovery events, file events, and user events. This results in a more cohesive security architecture for improved efficiency and optimization by quickly identifying the top priorities for threat investigation.

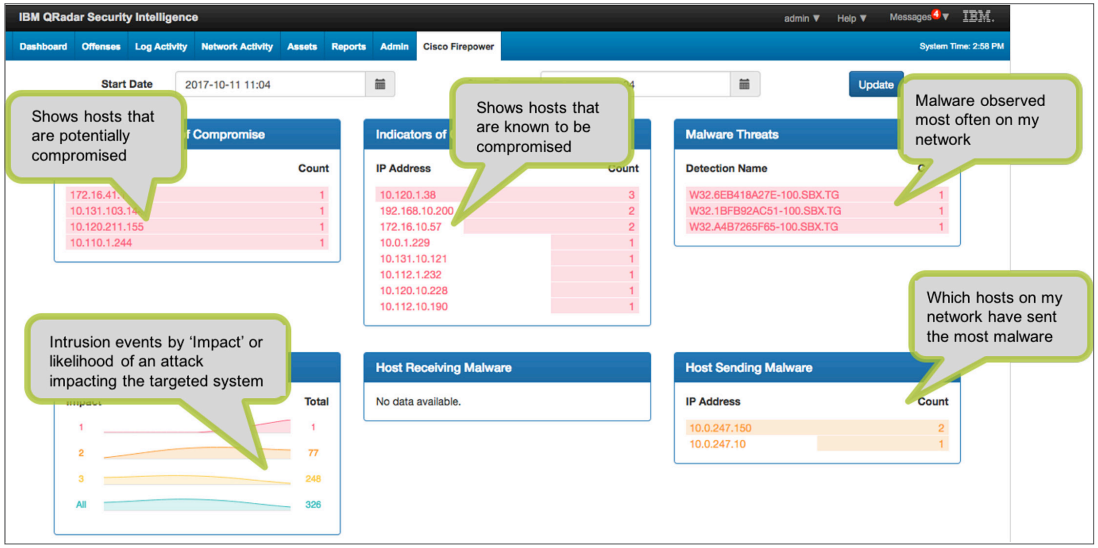
Customer Challenges

Cyber threats are more complex as cyber criminals are developing more creative methods to compromise and exploit sensitive business data. As a result, customers are challenged to keep pace and protect their business interests. They are faced with:

- Complex multivendor environments
- A lack of visibility into threats to users, devices, processes, and applications
- The inability to effectively share security event data to detect one and protect everywhere in the network
- Alert fatigue, lacking the ability to discern serious threats from innocuous events
- The inability to correlate, prioritize, and analyze incidents to determine potential threats

Customers require tools that facilitate easier security operations to simplify protection and mitigate risks.

QRadar and Firepower Integrated Dashboard



How It Works

The Cisco Firepower app and IBM QRadar integration provides two key capabilities:

1. It presents metrics and trends about the data collected by QRadar and then displays this on the QRadar accurate threat detection and response.
2. QRadar collects and parses security data into its database for analysis, allowing security teams to search, correlate, and analyze Cisco Firepower events. These events are prioritized and organized by impact flag, malware, connection, firewall, discovery, file and user events.

The QRadar SIEM consumes and analyzes tremendous amounts of Cisco threat data (logs and network flows) and uses analytics and context to transform it into useful, actionable information, enabling the analyst to quickly see the who, what, and where behind the offense and quickly determine if it's a legitimate threat or a false positive.

QRadar is effective at event correlation, threat detection, and analysis as it leverages a broad range of data and applies context for greater classification. This input is ultimately integrated into a single prioritized list of offenses for further action.

The Cisco Security and IBM Security Advantage

The ongoing collaboration between IBM Security and Cisco is helping organizations strengthen their posture against increasingly sophisticated cyberattacks. Rather than working in silos, as is the industry norm, these two leading security providers are collaborating to build solutions and share threat information that will empower clients to see a threat once, act at extreme speed and scale, and protect everywhere.

Next Steps

The Cisco Firepower and IBM QRadar integration provides customers with more efficient tools to rapidly detect and respond to advanced, stealthy threats. These capabilities enable customers to transform their security perimeter into an advanced threat defense perimeter, to streamline and create more effective security operations.

For additional information, visit: https://cs.co/ibmsec.

For additional questions or for opportunities and connections, email us:
cisco-ibm-security@cisco.com
cisco-ibm-security@us.ibm.com

Download the app for free at https://www.ibm.com/security/community/app-exchange.

C22-740807-01 10/18