Overview

Introduction to the Cisco Firepower App for IBM QRadar

The Cisco Firepower App for IBM QRadar helps you analyze and contain threats to your network by providing insight from multiple security products in QRadar.

The QRadar Security Information and Event Management (SIEM) tool provides anomaly detection, incident forensics, and vulnerability management.

After you set up the app, you can view event data from your Firepower system in graphical form in the QRadar console.

DSM Custom Field Properties

The following fields are part of the DSM:

- Custom Extraction Properties (32)
  - Bytes IN
  - Priority
  - User ID
  - Protocol Name
  - PolicyName
  - Security Intelligence List
  - Sensor
  - Impact
  - Malware Detector ID
  - Bytes Out
  - RecordType
  - securityIntelligenceName
  - Client Application Name
  - IP Protocol
  - Application Protocol
  - Blocked
  - MAC Address
  - Client Application ID
  - Malware File Size
  - Malware Threat Score
  - SHA256
  - Web Application Name
  - Zone
  - IOC Value
  - Web Application ID
  - Classification
  - Time
  - Firewall Rule ID
  - Malware URI
  - Agent ID
  - Malware
  - Message