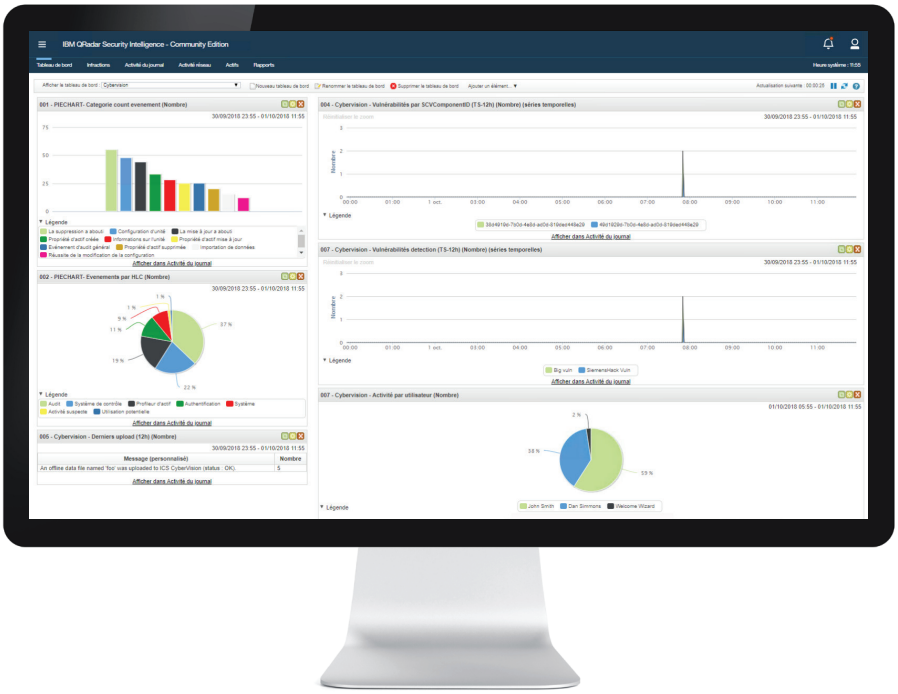
IBM QRadar and Cisco Cyber Vision

Integrated IT/OT Security Events Management in QRadar

Highlights

- Automatically discover and monitor OT infrastructure, vulnerabilities and traffic
- Gain real-time visibility into your OT network in IBM QRadar to identify and analyze IT/OT security risks
- Focus on real threats using machine Learning-classified information and pre-defined analytics rules
- Correlate OT and IT events to quickly remediate threats
- Get the free app from the IBM X-Force App Exchange



The Industrial Internet is relying on the convergence of operational technologies (OT) and information technologies (IT). The cyber threats that make headlines every day are now targeting OT networks and are impacting the real world in the form of production outages, environmental disasters, and threats to human safety. The Cisco® Cyber Vision and QRadar integration gives cybersecurity teams real-time visibility into their OT networks for a coordinated IT/OT threat management strategy.

Integrated IT/OT security operations center

Cisco Cyber Vision is an equipment inventory, network monitoring, and threat intelligence platform designed to secure industrial control systems (ICS) and supervisory control and data acquisition (SCADA) networks. It feeds the QRadar SIEM (Security Information and Event Management) platform with a detailed list of events, vulnerabilities, and asset information from the company's OT network. Security analysts now have a unified view to detect threats or attacks based on both IT and OT environments.

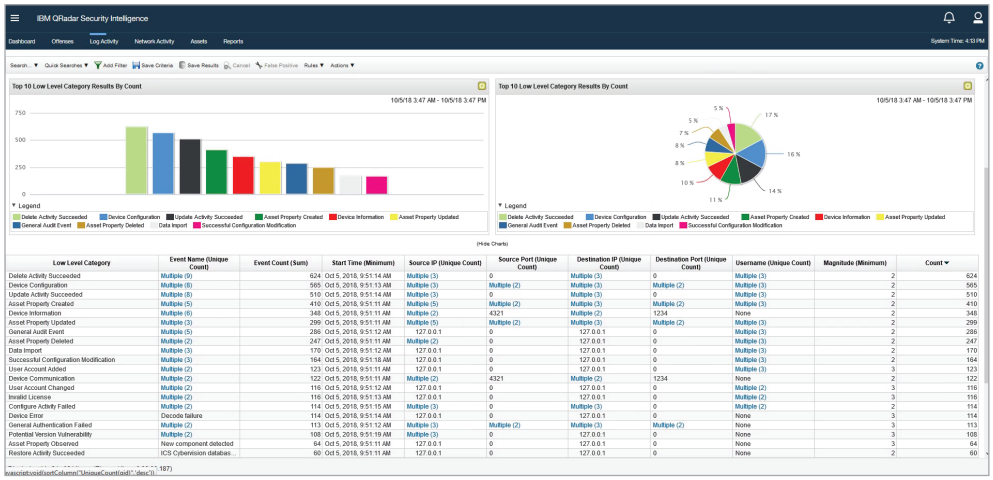
Add ICS-specific threat detection to QRadar

Attacks on ICS networks generally look like legitimate messages to OT devices. Cisco Cyber Vision offers comprehensive threat detection techniques, such as Snort® intrusion detection system (IDS) to identify known attacks and a behavioral analytics engine to detect abnormal behaviors and unknown attacks. It sends prioritized information to QRadar, so security analysts are not overwhelmed with false positives and can focus on high-risk events.

Actionable insights

The Cisco Cyber Vision QRadar app shows ICS events in tables, graphs and dashboards designed to help you analyze this wealth of previously unavailable information, such as:

- Abnormal OT/IT protocol behaviors
- Programmable logic controller (PLC) Stop/Start
- Firmware and Configuration downloads and uploads
- New and changed communications
- New assets on the network
- Asset vulnerabilities
- New and changed industrial properties
- Exceptions in industrial connections
- OT packet-decoding errors



Dashboards show events filtered by predefined analytics that QRadar users can customize and for which correlation rules can be easily added. Security analysts can drill down on any event to view the detailed list of actions and shorten investigation time or quickly remediate threats.

Download the Cisco app for QRadar

The Cisco Cyber Vision QRadar app is a free extension for the IBM QRadar Security Intelligence Platform. It is available for download on the IBM XForce App Exchange, the premier collaboration site for sharing software enhancements, applications and extensions that complement IBM Security solutions.

For more information

To learn more about the IBM Security App Exchange, please visit: apps.xforce.ibmcloud.com

For more information about Cisco Cyber Vision, please visit: www.cisco.com/go/cybervision

Cisco-IoT-CyberVision-SB-EN-20191121

© 2019 Cisco and its affiliates. All rights reserved.