IBM Security

IBM

IBM QRadar and Nozomi Networks SCADAguardian

Providing integrated security visibility for Operational Technology (OT) and Information Technology (IT) environments

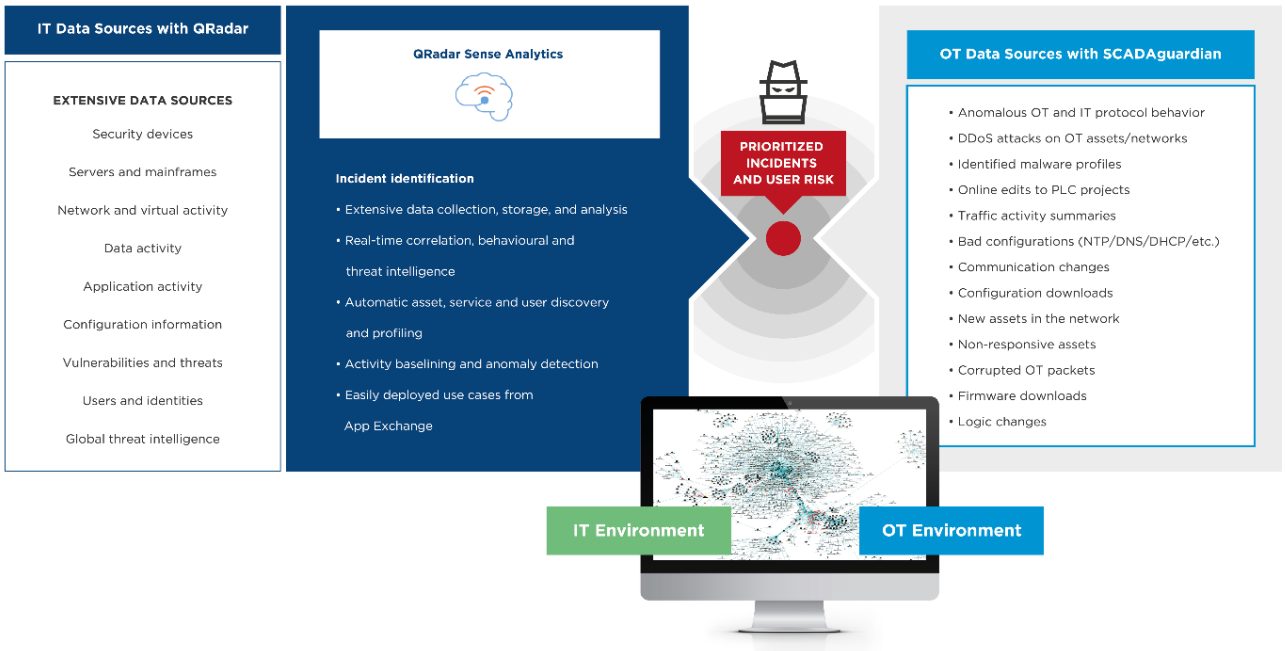
Highlights

- Rapidly discovers and monitors OT infrastructure, vulnerabilities and traffic
- Feeds detailed OT network visibility into the IBM QRadar Platform to identify and analyze IT/OT cyber risks
- Provides complete ICS (Industrial Control System) asset inventories for improved reporting and forensic analysis
- Quickly identifies and prioritizes vulnerabilities .
- AI-enabled hybrid threat detection combines signature-based and process anomalies for superior OT threat detection
- Empowers security analysts to rapidly respond to and remediate threats with alert aggregation
- Free application from the IBM X-Force App Exchange

The QRadar and SCADAguardian solution provides Information Security, OT and IT teams with real time visibility into the current state of their environments, and any potentially malicious activity within it, in one platform. After discovering and creating an inventory of the OT environment, SCADAguardian begins assessing vulnerabilities and monitoring traffic. This wealth of previously unavailable information, from multiple sources, in multiple formats, is then “normalized” and passed to the QRadar SIEM (Security Information and Event Management) platform.

Security teams that were previously only able to look for risks, vulnerabilities and attacks in their IT infrastructure, now get a single point of view across both OT and IT environments.

QRadar with SCADAguardian



Discover IT and OT environments
Create baseline traffic mapping
Identify malicious activity and vulnerabilities

Download the Nozomi Networks App

Nozomi Networks QRadar App, available in the IBM X-Force App Exchange, is a free extension for the IBM QRadar Security Intelligence Platform. The app delivers out-of-the-box rules and algorithms that plug directly into the QRadar advanced analytics engine. This fully integrated solution provides real-time visibility and threat detection for OT networks, as well as alert aggregation and prioritization for coordinated IT/OT threat management. By extending the QRadar Security Intelligence Platform with Nozomi Networks, security analysts can achieve deeper OT network visibility and continuous threat intelligence across the entire ICS and OT environments.

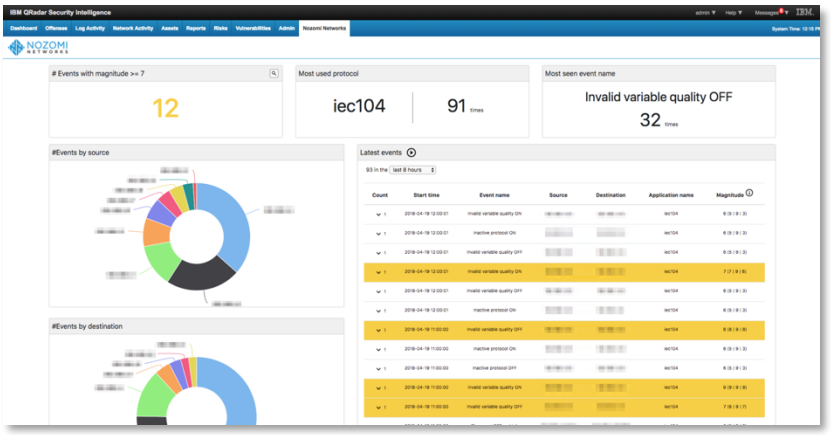
Integrated IT/OT Cybersecurity

Typical OT and industrial networks are large and include many diverse assets. They also change frequently, with devices being added, updated and removed all the time. That's why it is so critical for integrated security information and event management (SIEM) solutions to consider OT assets and network behavior.

The Nozomi Networks QRadar integrated solution allows IBM customers to identify devices and node end-points from all common automation vendors, protocols, associated MAC and IP address, as well as other key data via the QRadar interface. By identifying and generating alerts, incidents and local logs, Nozomi Networks is able to inform QRadar for further analysis.

With an Artificial Intelligence-enabled analytics engine, Nozomi Networks extends visibility into the OT domain to provide unprecedented context to identified anomalies. Together with QRadar, the app quickly exposes and prioritizes high-risk OT alerts.

When high-risk anomalous activity is discovered, analysts can drill down on any user, application, node or violation. Users can obtain a detailed view of the actions that contributed to the high risk score. This centralized view of multitenant user and network activity helps shorten investigation time and enables faster response to Indicators of Compromise (IoC).



The Nozomi Networks QRadar app dashboard displays actionable data insights to SOC analysts, including (but not limited to):

- Anomalous OT and IT protocol behavior
- DDoS attacks on OT assets/networks
- Identified malware profiles
- Online edits to PLC projects
- Traffic activity summaries
- Bad configurations (NTP / DNS / DHCP/ etc.)
- Communication changes
- Configuration downloads
- New assets on the network
- Non-responsive assets
- Corrupted OT packets
- Firmware downloads
- Logic changes

In conclusion

The explosion of ICS vulnerabilities created by increased connectivity and digitization, combined with the rise in ICS-targeted malware make cybersecurity solutions that bridge the IT/OT divide an absolute must.

IBM and Nozomi Networks have teamed up to address this growing need for effective, integrated IT/OT cybersecurity.

IBM QRadar and the IBM Security Platform leverages Nozomi Networks QRadar App's AI-enabled hybrid threat detection and OT visibility capabilities to help security teams quickly identify and remediate cyber and operational OT risks.

For more information

To learn more about this offering contact your IBM or Nozomi Networks representative or go to IBM X-Force App Exchange at: exchange.xforce.ibmcloud.com

IBM Corporation
Software Group
Route 100
Somers, NY 10589

In coordination with:

Nozomi Networks
120 2nd Street
San Francisco, CA 94105

Produced in the United States of America
August 2018

Please Recycle