OT ThreatFeed

ICS Threat and Vulnerability Feed for Up-to-Date Risk Monitoring

Regularly Receive OT Threat and Vulnerability Updates

Quickly Identify New Risks to Your Industrial Systems

Rapidly Respond with Actionable Insights

The **Nozomi Networks OT ThreatFeed™** subscription provides threat updates to Nozomi Networks products, making it easy for IT/OT professionals to stay on top of current ICS risks.

Our team of ICS security experts curates and adapts threat and vulnerability information from multiple sources, ensuring that threat information is accurate, concise and actionable. Updates include vulnerabilities and malware discovered by the Nozomi Networks research team, which makes significant contributions to ICS-CERT advisories and provides malware tools and other resources to the ICS community.

When new information is received, SCADAguardian™ or SCADAguardian Advanced™ rapidly checks your industrial network for the presence of new malware or vulnerabilities. If a threat is found, you are immediately notified, and can utilize the time-saving, ICS specific forensic tools available in our products to prevent consequences or remediate the situation.

The OT ThreatFeed is available from the Nozomi Networks Customer Portal, or it can be automatically sent to designated Central Management Consoles™.

Timely Threat Updates

- Provides indicators of known and emerging threats and vulnerabilities
- Curates, tests and adapts ICS threat information from multiple sources
  - Threat signatures, Indicators of Compromise and zero-days discovered by Nozomi Networks
  - Yara Rules and Packet Rules from the ICS Community
  - Vulnerability updates from the U.S. government's National Vulnerability Database (NVD)
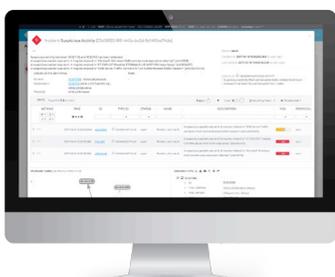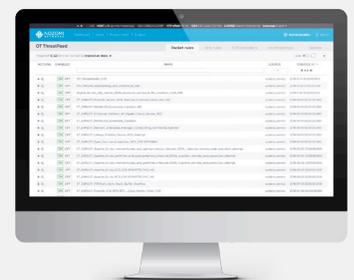
Actionable Threat Remediation Insights

- Identifies threats present in the industrial network, significantly reducing the Mean Time to Detection (MTTD)
- Decreases the Mean Time to Respond (MTTR) with Smart Incident™, which correlates alerts, provides ICS operational context and delivers automatic packet captures
- Decodes incidents with Time Machine™ system snapshots and diff reports

Nozomi Networks Solution Architecture
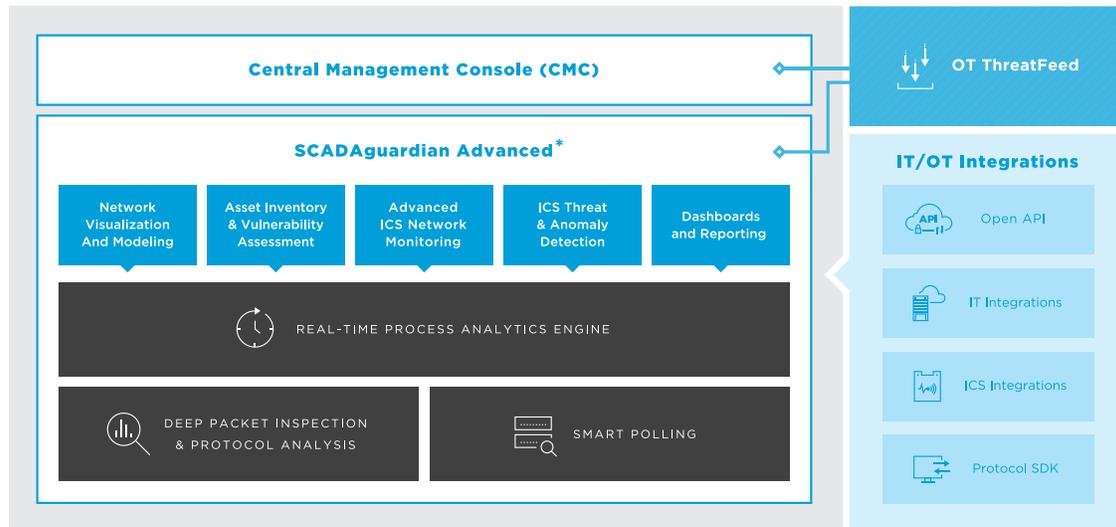
A separate, completely passive product, SCADAguardian is also available. It does not include Smart Polling.

The award winning Nozomi Networks solution improves cyber resiliency and reliability via a modular, extensible and scalable architecture.

Nozomi Networks Products and Services

SCADAguardian protects control networks from cyberattacks and operational disruptions. It provides superior operational visibility and rapid detection of cyber threats plus process risks through passive network traffic analysis.

SCADAguardian Advanced extends the significant value obtained from passive network analysis with the use of Smart Polling. This precise, low volume, active technique provides a full asset inventory, exact vulnerability assessment and advanced ICS network monitoring.

The Central Management Console (CMC) aggregates ICS data from hundreds of facilities, providing centralized and remote OT monitoring and cyber security management.

OT ThreatFeed is an optional subscription that delivers threat updates curated, adapted and discovered by Nozomi Networks. It ensures rapid detection of emerging threats and vulnerabilities and makes it easy for IT/OT teams to stay on top of current ICS risks.

About Nozomi Networks

Nozomi Networks is the leader of industrial cyber security, delivering the best solution for real-time visibility to manage cyber risk and improve resilience for industrial operations. With one solution, customers gain advanced cyber security, improved operational reliability and easy IT/OT integration. Innovating the use of artificial intelligence, the company helps the largest industrial facilities around the world See and Secure™ their critical industrial control networks. Today Nozomi Networks supports over a quarter of a million devices in sectors such as critical infrastructure, energy, manufacturing, mining, transportation and utilities, making it possible to tackle escalating cyber risks to operational networks (OT).