Detect threats faster in IT and OT networks with Vectra and Nozomi

CHALLENGE

The rise of IoT and the convergence of information technology and operational technology networks.

SOLUTION

Nozomi Networks and the Cognito network-detection and response platform from Vectra eliminate blind spots that allow attackers to hide in IT and OT network traffic.

BENEFITS

- **Complete visibility into cyberattacks inside the industrial network** – Critical insight into threats and progression of attacks enable security teams to quickly identify targeted attacks and take action.
- **Pinpoint hosts with the highest risk to the industrial network** – Automatically associate malicious behaviors to the physical host across IT and OT devices.
- **Automated mapping of Nozomi and Cognito detections to SIEMs** – Quickly and accurately correlate and track all behaviors and events across IT and OT devices.

Solution

Nozomi Networks, the leader in industrial control system (ICS) cybersecurity, and the Cognito® network-detection and response platform from Vectra® work together to provide organizations with total visibility into their information technology (IT) and operational technology (OT) networks.

Nozomi and Vectra eliminate the blind spots in IT and OT networks, empowering security analysts with complete threat hunting and leaving attackers nowhere to hide.

Nozomi's AI-driven solution provides real-time visibility and cybersecurity for ICS networks, delivering superior operational visibility and advanced industrial control system (ICS) threat detection through passive network traffic analysis.

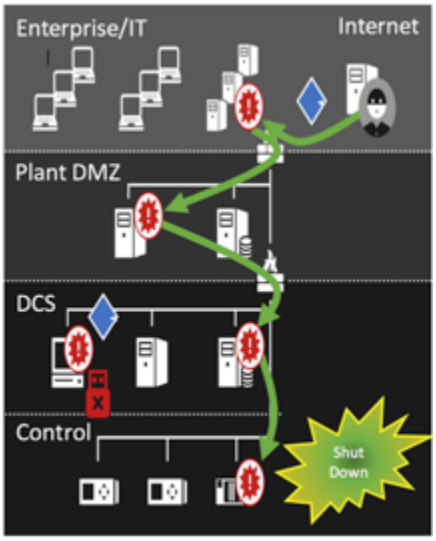
Powered by AI, Vectra and its Cognito platform enable organizations to detect hidden cyberattacks in real time in IT networks and enriches threat investigations with a conclusive chain of evidence.

Rising threats to industrial networks

At one time, the ICS used across manufacturing, transportation, utilities, energy and critical infrastructure were thought to be impervious to cyberattacks because the computers used to operate them did not access the internet and were separate from the corporate network.

This is no longer true. The risk of nation-state threats, espionage and internal exposure is rising.

Systems and network administrators, third-party vendors, industrial system developers and integrators have different levels of internet and ICS management access. This broader access has unwittingly created a way in for attackers. For example, an infected laptop can be brought in by a contractor, connect to the network and the attack can spread to the controlled ICS environment.



Attack #1

Attack from internet or third party to IT network

Compromise host in DMZ

Compromise host in ICS

Perform attack payload

Attack #2

Infected media

ICS malware
TRITON
Ransomware
Cryptominer
Windows
Malware
Conficker
Palevo/Mariposa

Mitigations

System backups
System spares
Incident response plan

The growing prevalence of IoT-connected industrial devices has dramatically increased the ICS attack surface. More than one million ICS devices were remotely accessible on the internet between 2012 and 2014, according to the Project SHINE (SHodan INtelligence Extraction) study.

Beyond the risks of internet connectivity, more ICS devices are running commercial operating systems, exposing the ICS to a wider variety of known vulnerabilities.

The connectivity and integration of traditional information technology with operational technology – IT/OT convergence – is increasing exponentially. IoT adoption and IT/OT convergence are accelerated by a fast-changing business environment and the use of AI to drive decisions and actions in ICS environments.

A lack of visibility into threats

Lack of visibility is a primary impediment to securing ICS. Security teams need full knowledge of all connected and interconnected assets, configurations and the integrity of communications to successfully protect critical infrastructure.

Manually monitoring ICS, network devices and system administrators presents a significant challenge to resource-constrained organizations. Large teams of security analysts must perform time-consuming manual analysis to identify attacks or unapproved behaviors within an ICS-regulated environment. A manual approach is simply not a scalable, efficient or effective way forward.

Visibility inside IT and OT networks that adapts to the dynamics of growth and change is critical. Organizations need technology that automates the real-time analysis of communications, devices, administrators and human behaviors on a converged IT/OT network to detect intentional attacks or unintentional consequences.

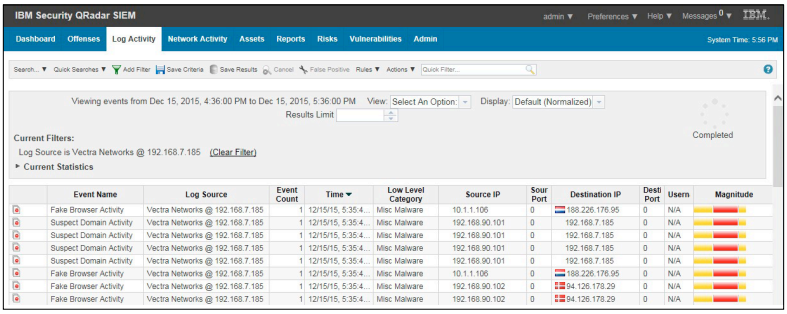
Real-time visibility and threat hunting for industrial networks

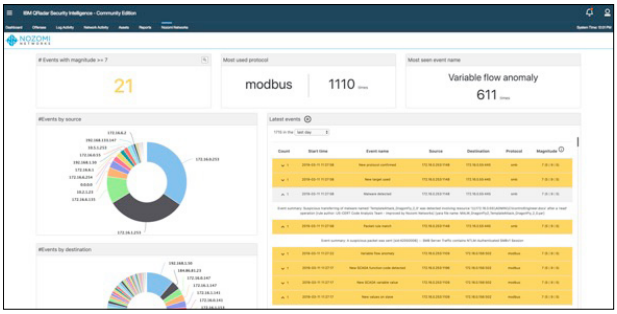
Because of the specialized nature of ICS and the differences in how IT and OT networks work, the right answer for complete visibility in an IT/OT environment is best-in-class technology that understands the inner workings of each environment – not a generic solution that is adapted to work across both.

This is why Vectra and Nozomi are working together to provide organizations total visibility into all their assets, enabling comprehensive threat hunting across IT and OT assets.

Together, Nozomi and Cognito provide real-time threat information on the behavior of every device in an IT/OT network, with the ability to roll-up this information to a central point, so network behaviors can be correlated for a complete picture of the attack lifecycle.

A common dashboard provides a full spectrum of information, enabling security operations teams to observe information across both IT and OT networks to respond faster to threats.





In the IBM QRadar UI, Vectra threat detections show suspicious domain activity, which occurs in the early stages of an attack on user desktops. From there, attacks spread to critical systems, where Nozomi detects deviations from normal OT traffic behaviors. By leveraging a SIEM, security analysts can stitch together the entire attack – from IT to OT – as a single incident.

Strengthen your existing security infrastructure

Whether providing the intelligence to block a new class of threat with firewalls, endpoint security, NAC and other enforcement points, or providing a clear starting point for a more extensive search with SIEMs and forensic tools, Cognito and Nozomi give you more value from existing security technologies.

Robust APIs in Cognito and Nozomi automate response and enforcement with virtually any security solution. Both generate syslog messages and CEF logs for all detections as well as prioritized host scores. This makes Cognito and Nozomi much more than just another source of logs and provides an ideal trigger for investigations and workflows within your SIEM.

Key benefits of integration

Together, Nozomi and Vectra reduce ICS cyber-risks:

- **Complete visibility into threats across the attack lifecycle** – The Cognito and Nozomi integration provides critical insight into specific threats as well as the progression of attacks across the attack lifecycle. This visibility allows security teams to quickly distinguish opportunistic botnet behaviors from more serious targeted threats and take action before data is stolen or damaged.
- **Pinpoint hosts with the highest risk to the network** – Cognito and Nozomi automatically associate all malicious behaviors to the physical network and hosts across IT and OT to present a comprehensive view of overall organizational risk.
- **Automated mapping of Cognito and Nozomi detections to SIEMs** – Cognito and Nozomi detections can be correlated in your SIEM, permitting security analysts to immediately see Cognito and Nozomi events. Now, security teams can properly correlate and track all behaviors and events across both IT and OT devices.

Manufacturers, transportation, utilities, energy and critical infrastructure operators can use Nozomi and Vectra to eliminate the blind spots in their industrial networks. Organizations can stay ahead of the ever-increasing malware threats that impact both IT and OT devices and mitigate the risk of operational disruption, data theft or other damage due to cyberattack.

About Vectra

Vectra is the leader in network detection and response – from cloud and data center workloads to user and IoT devices. Its Cognito platform accelerates threat detection and investigation using artificial intelligence to enrich network metadata it collects and stores with the right context to detect, hunt and investigate known and unknown threats in real time. Vectra offers three applications on the Cognito platform to address high-priority use cases. Cognito Stream™ sends security-enriched metadata to data lakes and SIEMs. Cognito Recall™ is a cloud-based application to store and investigate threats in enriched metadata. And Cognito Detect™ uses AI to reveal and prioritize hidden and unknown attackers at speed. For more information, visit vectra.ai.

About Nozomi Networks

Nozomi Networks is the leader of industrial cybersecurity, delivering the best solution for real-time visibility to manage cyber risk and improve resilience for industrial operations. With one solution, customers gain advanced cybersecurity, 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). For more information, visit nozominetworks.com.

VECTRA®
Security that thinks®

Email info@vectra.ai **Phone** +1 408-326-2020
vectra.ai