NOZOMI NETWORKS

MAPPING GUIDE

How the Nozomi Networks Platform Supports the U.S. DoW Zero Trust for OT Activities and Outcomes

Table of Contents

1. Executive Summary

Zero trust for OT is inherently an ecosystem strategy. Purpose-built for OT environments, the Nozomi Networks platform acts as the central OT intelligence layer, powering enterprise controls through tight integration with the zero-trust ecosystem including ICAM, PAM, NAC, EDR/DR and SIEM/SOAR systems.

Independently, the Nozomi Networks platform addresses 33 of the 84 Target Activities and eight of the 21 Advanced Activities, or 41 of the total 105 activities across six of the seven pillars.

In November 2025 the U.S. Department of War (DoW) published guidance for the adoption of zero- trust (ZT) cybersecurity principles for operational technology (OT) systems. The ZT for OT guidance adapts ZT principles to industrial environments and organizes requirements into activities and outcomes across seven pillars: User, Device, Applications & Workload, Data, Network, Visibility & Analytics, and Automation & Orchestration. It specifies 105 activities and capability outcomes to implement in OT environments, including:

- **84 Target Activities:** The minimum set of ZT capability outcomes and activities intended to collectively prevent lateral movement in the environment
- **21 Advanced Activities:** Additional long-term goals that provide adaptive responses and comprehensive ZT functionality but will not be held to the Target timeline.

Overview: Nozomi Networks Platform Support for ZT for OT Pillars and Activities

Pillars	Activities and Outcomes					
	Target		Advanced		Total	
	Nozomi Supported	All	Nozomi Supported	All	Nozomi Supported	All
User	12	13	5	5	17	18
Device	5	13	2	3	7	16
Applications & Workload	3	9	0	3	3	12
Data	1	17	0	2	1	19
Network & Environment	2	10	0	0	2	10
Automation & Orchestration	0	10	0	6	0	16
Visibility & Analytics	10	12	1	2	11	14
Total	33	84	8	21	41	105

2. Why ZT for OT Compliance Matters for DoW Components

Complying with the ZT for OT requirements is not a checkbox exercise; it's a foundational shift in how DoW Components protect their OT environments against modern threats. OT systems increasingly face nation-state actors, ransomware operators, supply chain attacks and insider risks. These systems differ significantly from IT: they include legacy equipment, proprietary protocols, safety critical functions and environments where downtime is unacceptable. As the ZT for OT guidance explains, applying traditional IT controls blindly can disrupt operations and even endanger physical processes. It provides an OT-specific roadmap that ensures:

- **Operational continuity:** The framework explicitly accounts for safety and reliability as primary constraints in design and deployment.
- **Risk reduction:** It mitigates threats to infrastructure that could lead to outages, environmental hazards or compromised mission execution.
- **Interoperability with enterprise IT:** It ensures OT is safely integrated with enterprise identity, analytics and response services, improving readiness and reducing blind spots.
- **Future-proofing:** As OT environments modernize, compliance provides a scalable architecture that reduces technical debt and prevents fragmentation.

Failure to comply increases exposure to cyber-physical disruptions, regulatory penalties, operational losses and reputational damage, especially as zero trust expectations become mandatory across government and critical infrastructure sectors.

3. How Nozomi Networks Supports the ZT for OT Pillars

Nozomi Networks aligns well with the ZT for OT guidance because our platform was built **specifically for operational technology**, not retrofitted from an enterprise IT security solution. This gives it several decisive advantages:

3.1 Deep, OT-native visibility across the entire environment

The ZT for OT guidance requires accurate inventories of users, devices, applications, workloads, data flows and behaviors. Nozomi delivers:

- Passive and safe active discovery of OT assets and Non-Person Entities (NPEs)
- Detailed network flow mapping and operational baselining to support segmentation, policy creation, and access governance
- Continuous monitoring of controller logic changes, remote configuration attempts and process critical activity

These features support large portions of the Device, Network, Application and Visibility & Analytics pillars.

3.2 OT-focused behavioral analytics and anomaly detection

The ZT for OT guidance places heavy emphasis on user and entity behavior analytics (UEBA), user access management (UAM), anomaly detection and environmental baselining to identify threats early, before they escalate.

The Nozomi platform provides:

- OT-aware AI/ML that learns normal behaviors and flags deviations
- Event correlation tied to specific Person Entities (PEs) and NPEs to accelerate incident triage
- Integration of data flows, asset context, threat intelligence and baselines to create precise threat profiles aligned with ZT for OT expectations

This gives organizations the analytics depth required by the guidance while avoiding alert fatigue.

3.3 Tight integration with the zero-trust ecosystem (ICAM, PAM, NAC, EDR/XDR, SIEM/SOAR)

Zero trust is inherently an ecosystem strategy. Nozomi acts as the central OT intelligence layer powering enterprise controls by integrating with:

- **Active Directory,** multi-factor authorization (MFA) and credentialing services (User pillar)
- **Cisco ISE/Aruba ClearPass** for dynamic network access control and Identity, credential and access management (NAC/ICAM) and isolation (User/Device/Network pillars).
- **Dispel** and other privileged access management (PAM) and secure remote access (SRA) solutions
- **Tanium, Carbon Black, Microsoft Defender** and our own Arc sensor for OT-optimized endpoint detection and response and extended detection and response (EDR/XDR)
- **SIEM/SOAR platforms** (security information and event management/security orchestration, automation and response) to orchestrate response with human-in-the-loop safety

These integrations make Nozomi the connective tissue that turns zero trust policy into actionable enforcement in OT environments.

3.4 Safety-centric design built for OT constraints

The ZT for OT guidance stresses that OT environments require careful, risk-aware rollouts and must avoid operational disruption. Nozomi meets this requirement through:

- A **passive-first approach** to monitoring
- Safe active scanning engineered to avoid process impact
- Architecture that functions even in isolated or air-gapped systems
- Features built specifically around programmable logic controllers (PLCs), remote terminal units (RTUs), historians, operator workstations and industrial protocols

This ensures zero trust implementation enhances mission operations rather than jeopardizing them.

3.5 Coverage across the mandate

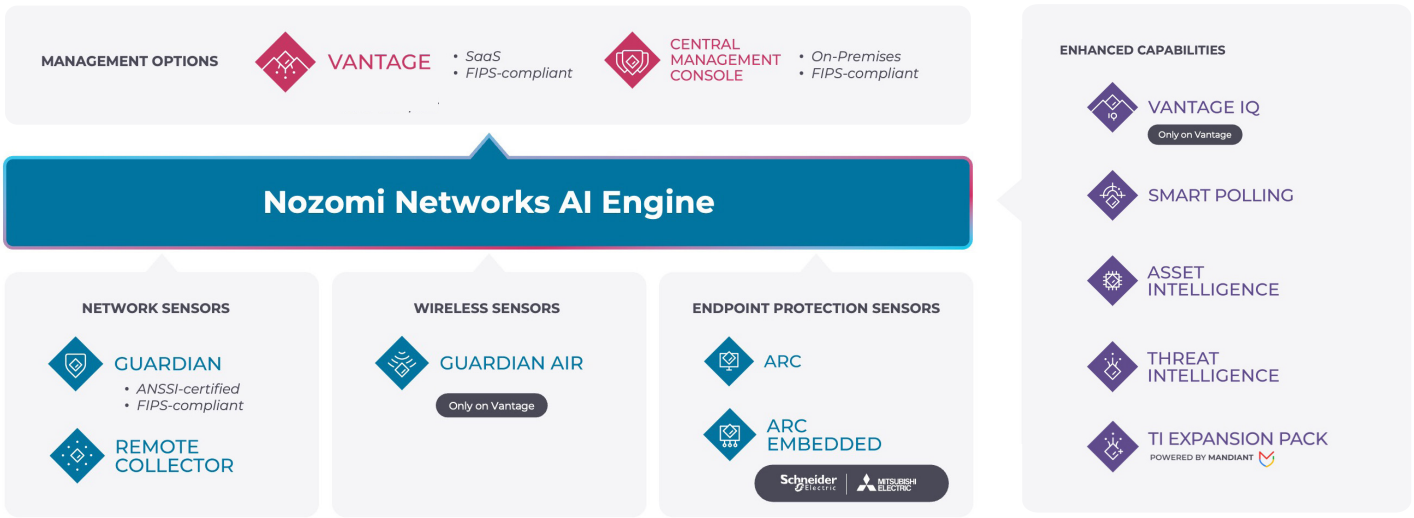
Per the pillar-specific tables later in this document that map ZT Activities to Nozomi platform capabilities, Nozomi provides strong, moderate or supportive coverage across all seven pillars. Where Nozomi is not the enforcement tool [e.g., public key infrastructure (PKI), attribute-based access control (ABAC), digital rights management/digital loss prevention (DRM/DLP) and software-defined networking (SDN) policy engines], it still provides the critical telemetry and analytics these controls depend on.

Nozomi Platform Coverage by Pillar

Pillars	Coverage
User	Moderate–Strong (via integrations). ICAM/MFA/PAM hooks, UEBA/UAM, session controls; not a user inventory tool.
Device	Strong. Passive/active discovery, config change detection, vulnerability/patch posture, EDR/XDR via Arc & partners.
Applications & Workload	Moderate. Integrity signals for controllers and vuln program inputs; ABAC enforcement is external.
Data	Supportive. Detects exfil/ransomware patterns; file/DB monitoring/DRM/DLP are external but benefit from Nozomi context.
Network & Environment	Strong as enabler. Ground truth of assets/flows driving micro-segmentation with partner enforcement.
Automation & Orchestration	Supportive. Extensive API/SIEM/SOAR integrations; not a SOAR/orchestration product.
Visibility & Analytics	Strong. Native AI/ML, baselining, SIEM integrations, asset alert correlation, IR isolation support.

Strong Moderate Supportive

The Nozomi Networks Platform



4. Requirements Mapping by Pillar

4.1 Pillar 1: User

Intent of the pillar: Centralize credentialing, enforce strong authentication, reduce privileges and monitor user/entity behavior in OT with safe, operations-aware enforcement.

How Nozomi helps:

- **ICAM/RBAC enablement via integrations.** Nozomi integrates with enterprise credentialing (e.g., Active Directory) to support role-based access and dynamic policy decisions for remote/third-party access (Activities 1.2.1.OT, 1.2.2.OT).
- **MFA support.** The platform can require MFA for administrative access using common authenticator apps (Activity 1.3.1.OT).
- **Alternative credentialing & interoperability.** Nozomi leverages **RADIUS** with NAC platforms (Cisco ISE, Ivanti Policy Secure) and interoperates with a broad range of credentialing services (Activities 1.3.2.OT, 1.3.3.OT).
- **PAM ecosystem.** Nozomi integrates with PAM/SRA partners (e.g., Dispel) to cover critical privileged use cases (Activities 1.4.1.OT, 1.4.2.OT).
- **Identity lifecycle management (ILM).** While Nozomi is not an ILM system, it signals to ISE/ClearPass to quarantine or revoke access based on anomalous identity/device behavior (Activities 1.5.1.OT, 1.5.2.OT).
- **UEBA/UAM for OT.** Nozomi provides OT-tuned UEBA/UAM capabilities including network-level and endpoint-user events (e.g., keystroke/macro detection, USB insertion via Arc) (Activity 1.6.1.OT).
- **Deny by default posture.** Via NAC integrations, Nozomi helps automate revocation and least privilege enforcement (Activity 1.7.1.OT).
- **Session authentication controls.** Automated session re-authentication and inactivity/expiration controls support initial/periodic authentication (Activities 1.8.1.OT, 1.8.2.OT); continuous authentication signals flow through NAC integrations (Activity 1.8.3.OT).
- **Enterprise credentialing alignment.** Nozomi interoperates with approved credentialing authorities to extend strong, federated authorization to OT assets (Activities 1.9.1 OT, 1.9.3.OT).

OT Activity ID	OT Activity Name	Description	How Nozomi Helps
Target Activities			
1.2.1.OT	**Implement Authorization and Access Management for OT Environments**	DoW Components implement OT or Enterprise ICAM governance, or other authorized credentialing services, in accordance with applicable policies and regulations. The authorized credentialing service establishes a set of attributes for authentication and authorization within the OT environment. Attributes are integrated with the 2.1.3. OT activity process for a complete IdP process. The OT credentialing service is enabled for adding and updating attributes for users. OT privileged access and authorization are approved and tailored as specified by the roles. For OT systems on which it is technically capable, any shared group, must-run, and service OT accounts are migrated to proper identities or are decommissioned. Any OT systems identified that cannot be migrated and/or decommissioned are tracked using a risk-based methodology for future migration and/or decommission.	Integrates with credentialing services like Active Directory.

OT Activity ID	OT Activity Name	Description	How Nozomi Helps
Target Activities			
1.2.2.OT	**Role Based Dynamic Access for OT Environments**	DoW Components develop rules, both technical and procedural, for remote and third-party access into the OT environment. All users must have strict role-based access controls prior to access or connection into the OT environment. Remote and third-party access should be limited to the account of least privilege required to perform work. OT privileged accounts required for operations are accessed through the Authorized Credentialing Service. Identify high-privileged accounts and require these use dynamic access control.	Integrates with credentialing services like Active Directory in order to implement RBAC.
1.3.1.OT	**MFA for OT Environments**	DoW Components enable or integrate the Authorized Credentialing Service with Multifactor Authentication (MFA), or an approved alternative authoritative credentialing solution, either technical or procedural, for access within the OT Environment.	Enables MFA using well known authenticator apps.
1.4.1.OT	**Implement PAM for OT Environments Pt. 1**	DoW Components procure and implement an OT Privileged Access Management (PAM) solution that supports all critical privileged use cases, as appropriate in the OT environment. Integration points for applications, services, and/or devices are identified to determine the status of support for the PAM solution. Applications, services, and/or devices that are able to integrate with the PAM solution are transitioned to using the solution.	Integrates with several PAM solutions, like Dispel, and SRA solutions to enhance security in OT and IoT environments.
1.4.2.OT	**Implement PAM for OT Environments Pt. 2**	DoW Components extend integrations with the OT PAM Solution to all use cases, inclusive of all critical use cases. Applications, services, and devices that cannot integrate with the PAM solution shall be managed in a risk-based methodical approach to be migrated and/or decommissioned where operationally possible in the OT Environment.	Integrates with several PAM solutions, like Dispel, and SRA solutions to enhance security in OT and IoT environments.
1.5.1.OT	**Life-Cycle Management for OT Environments Pt. 1**	DoW Components develop and document an Identity Life-Cycle Management (ILM) process for the OT Environment. The process is implemented for all users that access, connect, and operate with the OT Environment.	Integrates with tools like Cisco ISE and Aruba ClearPass to dynamically enforce access policies. If Nozomi detects an identity (user or device) behaving maliciously, it can trigger these systems to quarantine the user or revoke access.
1.6.1.OT	**Implement User & Entity Behavior Activity (UEBA) and User Activity Monitoring (UAM) Tooling for OT Environments**	DoW Components procure and implement UEBA and UAM solutions that are designed specifically for OT environments for all users, PEs and NPEs, as appropriate. UEBA and UAM solutions are integrated with the Authorized Credentialing Service and configured actions prioritize safety, reliability, and resilience within the OT environment.	Incorporates UEBA and UAM functionalities as embedded features within the platform to protect critical infrastructure. Provides UEBA-like capabilities focused on "entities" (devices and systems) and their interactions, rather than just human users. Nozomi's UAM is focused on network-level and endpoint user events within industrial environments, including keystroke, macro detection and USB insertion using Arc.

OT Activity ID	OT Activity Name	Description	How Nozomi Helps
Target Activities			
1.7.1.OT	**Deny by Default Policy in OT Environments**	DoW Components conduct a comprehensive review of all user accounts and their assigned permissions, applying the principle of least privilege to revoke unnecessary access rights while maintaining the safety and reliability of OT processes. Identify and decommission static privileged accounts where possible, or reduce their permissions to the minimum required. Automate audit logging and governance processes to continuously monitor access and prepare for the implementation of more granular, attribute-based or dynamic access control mechanisms.	Integrates with tools like Cisco ISE and Aruba ClearPass to dynamically enforce access policies.
1.8.1.OT	**Initial Authentication in OT Environments**	DoW Components implement authentication processes to authenticate users at the start of every session in the Operational IT environment, in the Enterprise IT environment when it interoperates with the OT environment, and in the Process Control environment via technical or procedural means, as appropriate.	Implements automated session & re-authentication controls. Includes native controls to enforce periodic re-authentication based on inactivity or predefined limits: Inactivity timeouts, Mandatory token expiration and inactive user expiration.
1.8.2.OT	**Programmable Periodic Authentication in OT Environments**	DoW Components enable programmable periodic authentication requirements in the Operational IT environment, in the Enterprise IT environment when it interoperates with the OT environment, and in the Process Control environment, as appropriate on a session basis. Alternative mitigating controls, technical or procedural, must be deployed and documented when OT devices do not support periodic authentication.	Achieves the required results through automated session & re-authentication controls, programmable API security and compliance-driven identity policies.
1.9.1.OT	**Enterprise Credentialing Services Pt. 1**	The DoW Enterprise works with DoW Components to implement DoW approved Credentialing Services in a centralized and/or federated fashion in the Operational IT environment, in the Enterprise IT environment when it interoperates with the OT environment, and in the Process Control environment, as appropriate. DoW Components credentialing services interoperate with the DoW Enterprise, while also ensuring all risks involving communications between Process Control and Operational IT environments are mitigated beforehand. DoW Component local credentialing solutions are identified for future migration and decommissioning.	Integrates with a wide variety of credentialing services from well-known vendors.
1.9.2.OT	**Enterprise Credentialing Services Pt. 2**	DoW Component local credentialing solution is decommissioned and users are migrated to the DoW Approved Credentialing Authority as appropriate. All systems are assessed for compliance with this directive. Systems unable to comply due to technical or operational constraints, including Stand-Alone systems, where migration may be delayed due to inherent limitations, are subject to a documented risk assessment process to be migrated and decommissioned in the future, and compensating controls are implemented to maintain equivalent security posture. Any users that are in violation are escalated for review and remediated.	Integrates with a wide variety of credentialing services from well-known vendors.

OT Activity ID	OT Activity Name	Description	How Nozomi Helps
Advanced Activities			
1.3.2.OT	**Alternative Flexible Credentialing**	DoW Components shall support alternative methods of authentication that can be managed using a self-service approach. The solution will be approved and implemented following DoW Enterprise policy recommendations and guidance.	Leverages RADIUS within integrations with NAC platforms like Cisco ISE and Ivanti Policy Secure to exchange device attribute.
1.3.3.OT	**Interoperate Credentialing Services**	DoW Component Authentication solution is extended to interoperate with DoW Approved Credentialing services.	Integrates with a wide variety of credentialing services from well-known vendors.
1.5.2.OT	**Life-Cycle Management for OT Environments Pt. 2**	DoW Components works with the DoW Enterprise to review and align the OT Environment ILM process with existing ILM processes, policies, and standards. Exceptions are identified and are managed in a risk-based methodical approach.	Integrates with tools like Cisco ISE and Aruba ClearPass to dynamically enforce access policies. If Nozomi detects an identity (user or device) behaving maliciously, it can trigger these systems to quarantine the user or revoke access.
1.8.3.OT	**Continuous Authentication**	DoW Components monitor transaction-based authentications for Policy Violations. Any violations are escalated for response to the incident response process.	Integrates with tools like Cisco ISE and Aruba ClearPass to dynamically enforce access policies. If Nozomi detects an identity (user or device) behaving maliciously, it can trigger these systems to quarantine the user or revoke access.
1.9.3.OT	**Enterprise Credentialing Services Pt. 3**	DoW Components shall apply authentication from DoW Approved Credentialing Authority to all OT Assets.	Integrates with a wide variety of credentialing services from well-known vendors.

4.2 Pillar 2: Device

Intent of the pillar: Establish authoritative device inventory, configuration/patch governance, endpoint detection and risk-based control for NPEs.

How Nozomi helps:

- **Authoritative NPE inventory.** Employs passive discovery by default, with safe active discovery options where appropriate (Activities 2.1.1.OT, 2.1.4.OT).
- **Configuration monitoring & control.** Detects remote configuration attempts, operational state changes and PLC configuration changes (Activity 2.3.1.OT).
- **Vulnerability & patch posture.** Asset risk management surfaces firmware/software versions, vulnerability assessments and patch recommendations, supporting compliance with reassessments (Activities 2.5.1.OT, 2.6.2.OT).
- **EDR/XDR for OT. Nozomi Arc** brings OT-optimized EDR to endpoints and integrates with CrowdStrike, Tanium, VMware Carbon Black and Microsoft Defender. XDR coverage is achieved by unifying Nozomi sensors and integrating with Secureworks Taegis, Vectra AI and MDR stacks (Activities 2.7.1.OT, 2.7.2.OT).

OT Activity ID	OT Activity Name	Description	How Nozomi Helps
Target Activities			
2.1.1.OT	**Inventory NPEs in OT Environment**	DoW Components develop a centralized inventory for NPEs in the Operational IT and Process Control environments. Existing inventories are identified and manual and/or passive discovery-based automated solutions shall be used to update the centralized inventory. Automated inventories must be manually verified and audited periodically for accuracy as new equipment is deployed in the environment.	Uses passive network asset discovery by default.
2.3.1.OT	**Configuration Monitoring and Control Tools for OT Environments**	DoW Components procure and implement configuration monitoring and control solutions for the Operational IT environment. Configuration control should ensure configuration files (e.g., ladder logic) for the Process Control environment are not altered, downloaded, or uploaded except by authorized individuals.	Identifies and generate alerts when remote configuration attempts; operational state changes and configuration changes in select critical OT devices like PLCs are detected.
2.5.1.OT	**Implement Vulnerability and Patch Management Tools for OT Environments**	OT Environments must maintain minimum government approved compliance standards and patching as well as be maintained to current approved configuration profiles. Any systems outside of these standards require authorization from the DoW Component through a risk based assessment approach. Periodic reassessments for compliance are performed for all devices in use. At the Process Control level, special care must be given to mitigate vulnerabilities without a patch source, while protecting safety, operational functionality, and process reliability. Similarly, risk-based testing must be performed and accepted prior to patching.	Nozomi asset risk management system helps provide visibility of asset software and firmware versions and provides patch recommendations as well as vulnerability assessments for each analyzed asset.
2.6.2.OT	**OT Device Configuration Management**	DoW Components sets standards and policies for the device inventory and secure configuration, in conjunction with the UEDM solution and asset management tools, to enable automated configuration management control. Automated solutions for configuring devices are used only after analyzing the risk to operations.	Nozomi asset risk management system helps provide visibility of asset software and firmware versions and provides patch recommendations as well as vulnerability assessments for each analyzed asset.
2.7.1.OT	**Implement Endpoint Detection & Response (EDR) Tools for OT Environments**	DoW Components procure and implement EDR solution(s) within the Operational IT, and Process Control environments as appropriate. DoW Components conduct system analysis to determine the potential automated responses within both the Operational IT and Process Control environments prioritizing safety, process reliability, and mission.	Implements OT-optimized EDR through its Nozomi Arc sensor and deep integrations with leading IT EDR vendors like CrowdStrike, Tanium, VMware Carbon Black and Microsoft Defender.
Advanced Activities			
2.1.4.OT	**Automated NPE Discovery**	DoW Components automate OT network NPE discovery through the OT environment, limiting access to NPEs based on risk-based methods. OT network asset discovery shall utilize active discovery methods that are optimized to mitigate operational disturbances through configurations that avoid aggressive network scans, especially for equipment in the Process Control environment. In addition, SIEM, SOAR, and IDS solutions shall be configured to permit traffic from authorized active discovery tools to reduce false alarms.	Utilizes active network discovery to discover network devices that are online but not actively communicating.

OT Activity ID	OT Activity Name	Description	How Nozomi Helps
Advanced Activities			
2.7.2.OT	**Implement Extended Detection & Response (XDR) Tools for OT Environments**	DoW Components procure and implement XDR solution(s) to all possible devices, and integration with other solutions where possible. EDR continues coverage to include the maximum number of services and applications as part of the XDR implementation. Basic analytics are sent from the XDR solution stack to the OT and/or Enterprise SIEM solution.	Helps achieve Extended Detection and Response (XDR) capabilities by unifying its native network, endpoint, and wireless sensors into a single AI-powered platform, by implementing the Nozomi Arc Endpoint sensor and through deep integrations with third-party IT XDR vendors like Secureworks Taegis, Vectra AI and various MDR solutions.

4.3 Pillar 3: Applications & Workload

Intent of the pillar: Inventory OT apps, enforce application integrity and run an OT-aware vulnerability program aligned with enterprise processes.

How Nozomi helps:

- **Application integrity signals.** For inventoried apps (e.g., SCADA/controller IDEs), Nozomi flags unauthorized/remote configuration activity on critical controllers (Activity 3.1.2.OT).
- **OT vulnerability management program inputs.** Nozomi provides a comprehensive vulnerability console with affected assets, available patches, workarounds and lifecycle context, supporting Component and Enterprise programs (Activities 3.3.1.OT, 3.3.2.OT).

OT Activity ID	OT Activity Name	Description	How Nozomi Helps
Advanced Activities			
3.1.2.OT	**OT Application Control**	Application control solutions are applied to inventoried applications (e.g., SCADA software, control software, controller IDEs, etc.), to prevent unauthorized modifications.	Identifies and generate alerts when remote configuration attempts, operational state changes and configuration changes in select critical OT devices like PLCs are detected.
3.3.1.OT	**OT Vulnerability Management Program Pt. 1**	DoW Components work with the DoW Enterprise to establish and manage an OT Vulnerability Management program. OT Vulnerability Management teams shall collaborate with a related Enterprise IT Vulnerability Management team. Vulnerability management for the OT environment shall incorporate vulnerability scope and risk to mission in prioritization decisions. Vulnerability sources can be delivered from any trusted agent, and must be consumed as an interoperable product.	Provides a comprehensive vulnerability management console, with extensive information about affected assets, patches available, workarounds and equipment lifecycle.

OT Activity ID	OT Activity Name	Description	How Nozomi Helps
Advanced Activities			
3.3.2.OT	**OT Vulnerability Management Program Pt. 2**	Standard processes are established at the DoW Enterprise level for reporting and managing the disclosure of vulnerabilities in DoW maintained or operated OT environments, for disclosure both publicly and privately. DoW Components expand the OT Vulnerability Management program to track and manage open public, controlled public, PAI and CAI, and DoW internally derived vulnerability sources.	Helps achieve this goal by integrating extensively with SIEM (Security Information and Event Management), SOAR (Security Orchestration, Automation and Response), and other enterprise security consoles to provide a unified view of IT, OT, and IoT threats.

4.4 Pillar 4: Data

Intent of the pillar: Tag/classify OT data, implement DLP/DRM controls, monitor high value files and databases, and enforce data protection at/beyond the formal boundary.

How Nozomi helps:

- **DLP analytics & exfiltration detection.** By baselining industrial communications — including cross Purdue and external traffic — Nozomi detects anomalous flows suggesting data exfiltration or ransomware activity, feeding SIEM for triage (Activity 4.4.1.OT).
- **File/database monitoring interoperability.** While file/database monitoring tools are separate, Nozomi's telemetry enhances SIEM analytics that correlate with file integrity/database monitor events (Activities 4.4.3 OT, 4.4.6.OT).

OT Activity ID	OT Activity Name	Description	How Nozomi Helps
Target Activities			
4.4.1.OT	**DLP Analytics**	DoW Components establish DLP types (e.g., Network, Endpoint, On-Premises, etc.) and recognition patterns based on data tagging solution in Activity 4.3.1.OT. A DLP analytics process is established to investigate loss type from logs, and determine severity, impact, policy enforcement, and mitigation response.	Detects unusual communications between devices, across the Purdue levels and to the external world, potentially identifying data exfiltration or ransomware attempts.

4.5 Pillar 5: Network & Environment

Intent of the pillar: Define granular access rules, map/segment flows across planes, implement micro-segmentation and protect data in transit.

How Nozomi helps:

- **Access policy inputs (asset/flow intelligence).** Nozomi Guardian discovers assets and maps data flows, providing the factual details needed to write granular rules and ConOps (Activities 5.1.1.OT, 5.1.2. OT, 5.2.3.OT).
- **Segmentation enablement.** Nozomi's visibility supports plane segmentation and micro-segmentation; the tables also reference ecosystem partners (e.g., Blastwave) where policy enforcement is applied (Activities 5.3.1.OT, 5.4.1.OT, 5.4.2.OT).

OT Activity ID	OT Activity Name	Description	How Nozomi Helps
Target Activities			
5.1.1.OT	**OT Granular Access Rules and Policies Pt. 1**	The DoW Enterprise works with DoW Components to create granular access rules and policies, technical and procedural, in the Operational IT environment, and within the Enterprise IT environment when services are provided to the OT environment. Associated ConOps shall be developed to align with the access rules and policies. DoW Components will implement these access rules and policies into existing solutions to improve initial risk levels and ensure future interoperability.	Used in conjunction with micro-segmentation tools, Nozomi Networks Guardian discovers the assets in the Operational & Enterprise IT environment which access rules and policies will be applied.
5.1.2.OT	**OT Granular Access Rules and Policies Pt. 2**	Data flow patterns are defined. DoW Components apply data tagging patterns to enable granular access to the OT environment, as appropriate.	Used in conjunction with micro-segmentation tools, Nozomi Networks Guardian discovers the network data flows and communications.

4.6 Pillar 6: Automation & Orchestration

Intent of the pillar: Normalize policy artifacts, define API patterns, integrate SOAR/SIEM and automate response with "human in the loop" safety for OT.

How Nozomi helps:

- **Standards-based integrations.** Nozomi integrates broadly with SIEM/SOAR and policy services via APIs, feeding alerts, context and asset identities to orchestrated workflows. However, Nozomi is not an orchestration tool itself.

4.7 Pillar 7: Visibility & Analytics

Intent of the pillar: Achieve full-fidelity OT monitoring, parse/analyze logs, baseline behavior, expand threat alerting and correlate alerts to asset identity to drive safe isolation and response.

How Nozomi helps:

- **SIEM integration & alerting.** The platform integrates deeply with multiple SIEMs; develops OT rules/alerts and continuously ingests CTI-aligned data streams (Activities 7.2.2.OT, 7.2.3.OT).
- **Anomaly detection (AI/ML).** The platform uses advanced AI-powered analytics to detect trends, attack vectors and anomalous behaviors; establishes baseline and generate threat profiles based on assessed risk to prioritize events (Activities 7.1.3.OT, 7.2.6.OT, 7.3.1.OT, 7.3.2.OT, 7.4.1.OT).
- **Asset ID correlation.** Alerts are correlated to specific PEs/NPEs to accelerate triage and enable targeted responses (Activity 7.2.5.OT).
- **IR isolation support.** By detecting abnormal interconnections across Enterprise, Operational and Process Control layers, Nozomi informs safe logical/physical isolation and controlled recovery testing (Activity 7.2.1.OT).

OT Activity ID	OT Activity Name	Description	How Nozomi Helps
Target Activities			
7.1.2.OT	**Log Parsing in OT Environments**	DoW Components identify and prioritize collection of all log, event, alert, and flow sources in the Operational IT and Process Control environments within the OT environment, and for data flow to the Enterprise IT and external environments. DoW Components and DoW Enterprise, with vendor support, map existing vendor log content and create a DoW Enterprise machine consumable pattern. The established DoW Enterprise pattern is provided as a contract element for vendor capability alignment.	Integrates extensively with SIEM, SOAR other enterprise security consoles to provide a unified view of IT, OT and IoT threats and via API integration.
7.1.3.OT	**Log Analysis in OT Environments**	DoW Components work with DoW Enterprise to develop common behaviors, and identifies and prioritizes behaviors based on all relevant documented processes, including distinct operating modes. Ensure log data has sufficient attributes to analyze the behavior model.	Integrates extensively with SIEM, SOAR other enterprise security consoles to provide a unified view of IT, OT and IoT threats and via API integration.
7.2.1.OT	**OT Infrastructure Incident Response Isolation**	DoW Components will ensure that the interconnections between Enterprise IT, Operational IT, and Process Control infrastructure are designed to be disconnected physically or logically during a detected incident to prevent any further intrusion or damage. The infrastructure must prevent reconnection until the incident is cleared. A controlled recovery procedure for testing and validation is used during reconnection to maintain system integrity and reduce the risk of recurring issues.	Detects unusual communications between devices across the Purdue levels and to the external world, potentially identifying data exfiltration, ransomware attempts or unauthorized communications between infrastructures.
7.2.2.OT	**Threat Alerting for OT Environments Pt. 1**	DoW Components procure and implement a SIEM solution, or integrate, with an Enterprise SIEM. Data feeds are ingested, identified from the CTI program established in 7.5.1.OT, to develop rules and alerts for the OT environment.	Integrates extensively with SIEM, SOAR other enterprise security consoles to provide a unified view of IT, OT and IoT threats and via API integration.
7.2.3.OT	**Threat Alerting for OT Environments Pt. 2**	DoW Components expand threat alerting and develop deviation anomaly rules to detect advanced threats utilizing the data feeds established in 7.2.2.OT.	Implements an alert management system that keeps track of events and uses advanced AI/ ML algorithms to detect trends and attack vectors. Integrates deeply with SIEMs to deliver information for immediate remediation.
7.2.5.OT	**OT Asset ID and Alert Correlation**	All PEs and NPEs in SIEM are identified and correlated to alerts in order to provide security teams with accurately detailed information and asset IDs. Event visualization indicates which asset ID is affected by detected event.	Integrates deeply with multiple SIEMs to provide comprehensive data about alerts and associated assets.
7.2.6.OT	**OT Baselines**	DoW Components develop a subject/attribute baseline approach based off of typical patterns and behaviors from activity 7.3.2.OT.	Implements an alert management system that keeps track of events and uses advanced AI / ML algorithms to detect trends, attack vectors and anomalous behaviors.
7.3.1.OT	**Implement Analytics Tools for OT Environments**	DoW Enterprise works with DoW Components to develop and provide minimum requirements for Analytics Tools capabilities to analyze all data. Any analytic tools under consideration by DoW Components for implementation shall be subject to these requirements.	Uses advanced AI/ML algorithms to detect trends, attack vectors and anomalous behaviors while reducing alert fatigue to enhance focus on important tasks.

OT Activity ID	OT Activity Name	Description	How Nozomi Helps
Target Activities			
7.3.2.OT	**Establish OT Baseline Behavior**	DoW Components utilize analytics tools developed for OT environments to analyze baseline operational behavior patterns across the entire OT environment, and to identify patterns and deviations from the normal baseline.	Implements advanced AI and ML algorithms to detect trends, attack vectors and anomalous behaviors based on a previously built baseline that is used as a reference.
7.4.1.OT	**OT Environment Baseline and Profiling**	DoW Components, utilizing the developed OT baselines, create to assess the level of risk of deviations from normal baseline. Threat profiles should be used for prioritization of events and integrated into access profile rules developed for system triage.	Implements advanced AI and ML algorithms to detect trends, attack vectors and anomalous behaviors based on a previously built baseline that is used as a reference to activate future alerts.
Advanced Activities			
7.2.4.OT	**Threat Alerting for OT Environments Pt. 3**	Threat Alerting is expanded to include advanced data sources, such as UEBA and UAM. These advanced data sources are used to develop and improve anomalous and pattern activity detections and event triggers.	Implements an alert management system that keeps track of events and uses advanced AI/ML algorithms to detect trends, attack vectors and anomalous behaviors. Integrates deeply with SIEMs to deliver information for immediate remediation.

5. Conclusion

Complying with the ZT for OT mandate requires deep visibility, precise monitoring and seamless integration across identity, device, network and analytics controls. Nozomi Networks is uniquely positioned to support this journey because it provides the OT-native visibility, behavior analytics and threat detection that zero trust relies on, without disrupting industrial operations. It integrates tightly with key zero trust ecosystem components such as AD, MFA, PAM, NAC, EDR/XDR and SIEM/SOAR — ensuring that OT insights translate into real, enforceable security outcomes.

Take the next step.

Contact one of our federal government solution specialists to learn more.

Book a demo

nozominetworks.com/demo

Nozomi Networks protects the world's critical infrastructure from cyber threats. Our platform uniquely combines network and endpoint visibility, threat detection, and AI-powered analysis for faster, more effective incident response. Customers rely on us to minimize risk and complexity while maximizing operational resilience.

NOZOMI NETWORKS

nozominetworks.com