NOZOMI NETWORKS

MAPPING GUIDE

How the Nozomi Networks Platform Supports CMMC 2.0 Compliance

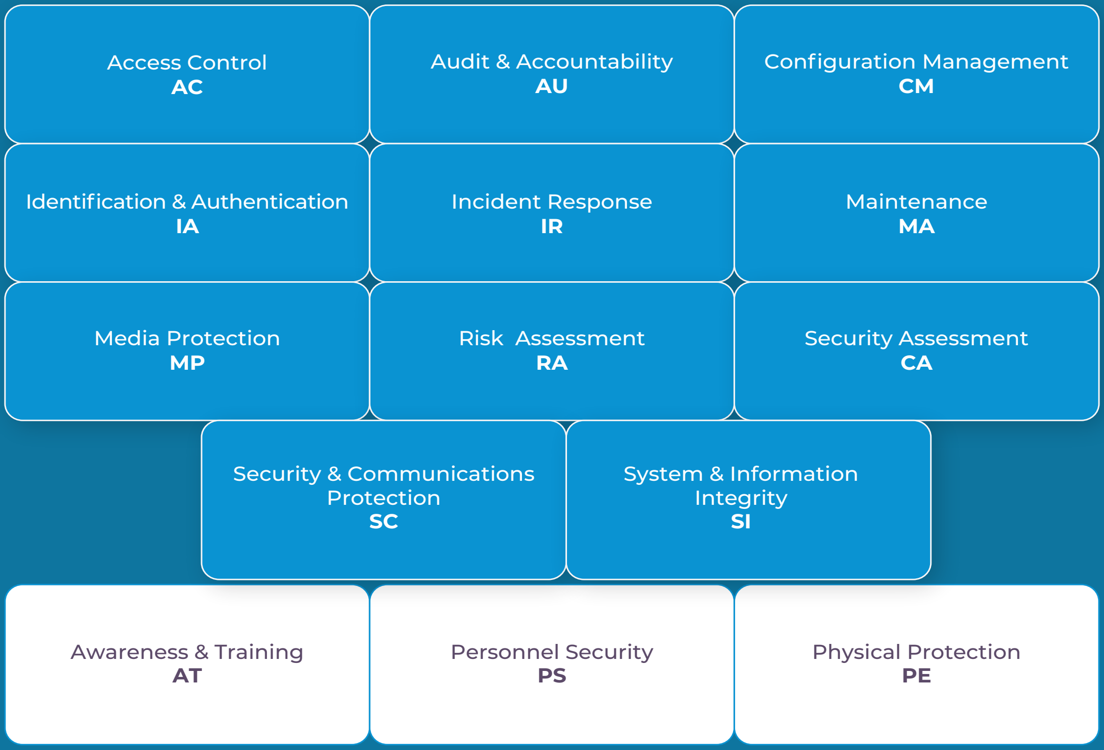
Table of Contents

The Cybersecurity Maturity Model Certification (CMMC) is the U.S Department of Defense's (DoD's) framework to ensure that that the companies in the Defense Industrial Base (DIB) supply chain adequately protect sensitive unclassified information shared with them through acquisition programs. It applies to prime contractors and their subcontractors.

CMMC 2.0 has a maximum of 134 requirements across 14 domains and offers three levels of maturity depending on the type of sensitive unclassified information to be handled per the contract.

Determining the scope of systems and networks covered under CMMC is a critical first step. **If your CMMC relevant environment includes OT and IoT devices (specialized assets), they must also be secured.**

Nozomi Networks is the leader in OT/IoT security and visibility. This guide describes how our platform helps you determine your relevant environment, automatically collect required data for certification and meet key Level 1, 2 and 3 requirements within 11 of the 14 CMMC 2.0 domains.



Access Control **AC**

Audit & Accountability **AU**

Configuration Management **CM**

Identification & Authentication **IA**

Incident Response **IR**

Maintenance **MA**

Media Protection **MP**

Risk Assessment **RA**

Security Assessment **CA**

Security & Communications Protection **SC**

System & Information Integrity **SI**

Awareness & Training **AT**

Personnel Security **PS**

Physical Protection **PE**

The Nozomi Networks platform can help you meet key Level 1, 2 and 3 requirements within 11 of the 14 CMMC 2.0 domains.

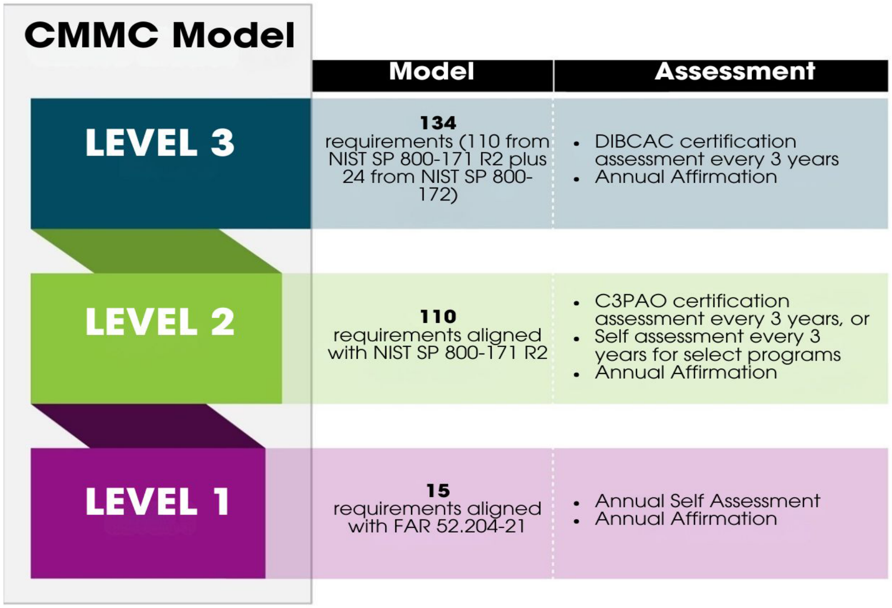
Introduction

The CMMC program is designed to ensure that DoD sensitive information shared with DIB contractors and subcontractors is handled securely during contract performance. Such information is labelled Federal Contract Information (FCI) or Controlled Unclassified information (CUI).

The CMMC framework is based on three levels of security maturity. Level 1 requirements are aligned with FAR 52.204-2. Level 2 is aligned with NIST SP 800-171, and Level 3 includes an additional 24 requirements from SP 800-172.

Before award, contracts are assigned one of the three CMMC levels, based on the type and sensitivity of unclassified information to be handled.

If you plan to bid (or be a sub-supplier in a bid) on a DoD contact after October 1, 2025, you must have achieved the required CMMC level specified in the contract to be eligible to bid.



CMMC Model

	Model	Assessment
LEVEL 3	**134** requirements (110 from NIST SP 800-171 R2 plus 24 from NIST SP 800-172)	• DIBCAC certification assessment every 3 years • Annual Affirmation
LEVEL 2	**110** requirements aligned with NIST SP 800-171 R2	• C3PAO certification assessment every 3 years, or • Self assessment every 3 years for select programs • Annual Affirmation
LEVEL 1	**15** requirements aligned with FAR 52.204-21	• Annual Self Assessment • Annual Affirmation

Source: DoD CIO

Background

Before CMMC, contracts were awarded to suppliers before they had details on security requirements, which led to excessive failed security audits and fines. This not only added risk to the supply chain but also drove up costs. Placing CMMC certification at the beginning of the contract process eliminates such waste.

The first version of CMMC was never fully rolled out due to the complexity, rigidity, and cost and compliance burden perceived by many contractors, who pushed back. CMMC 2.0 addresses those issues with fewer maturity levels (three instead of five), 14 domains instead of 17 (removes access management, recovery and situational awareness), closer alignment with NIST SP 800-711 (all 110 requirements for Levels 2 and 3) and fewer maximum requirements (from 171 to a total of 134 for Level 3).

Key Dates and Timeline

CMMC certification requirements will appear in most new DoD contracts beginning October 1, 2025. The program is being rolled out in phases beginning in 2025 and culminating with full implementation by 2028.

- **December 16, 2024:** CMMC 1.0 is superseded by CMMC 2.0, currently in effect (32 CFR CMMC Program Rule).
- **January 2025:** CMMC assessments for Level 2 and Level 3 begin.
- **July 23, 2025:** The rule requiring CMMC certification for most DoD contracts is finalized (48 CFR DFARS Rule).
- **October 1, 2025:** DoD contracts must include the CMMC certification clause (252.204-7021).
- **Four-phase implementation through 2028:**
  - Phase 1 - 2025: Level 1 or Level 2 self-assessments required for certain contracts
  - Phase 2 - 2026: Level 2 (C3PAO) assessments required for contractors handling CUI
  - Phase 3 - 2027: Level 3 (DIBCAC) l assessments required for relevant contracts
  - Phase 4 - 2028: Levels 1-3 compliance required for all relevant contracts.

Maturity Levels

- **Level 1: Foundational:** Aligns with FAR 52.204-21 and ensures that companies implement 15 basic cybersecurity hygiene practices to protect FCI. Requires an annual self-assessment.
- **Level 2: Advanced:** Aligns with NIST SP 800-171 Rev 2 and is designed for organizations handling CUI. Requires a third-party assessment (C3PAO) every three years.
- **Level 3: Expert:** Includes a subset of NIST SP 800-172 controls (24) for handling the most sensitive CUI, to protect against sophisticated threats. Organizations must first achieve Level 2. Requires a DoD assessment (DIBCAC) every three years.

During Level 2 and Level 3 assessments, contractors must also demonstrate how they protect their Security Protection Data (SPD), which is information about their own security tools, so a threat actor can't learn how to bypass your defenses.

CMMC 2.0 Required Controls by Domain

Domain	Level 1	Level 2	Level 3
Access Control (AC)	4	22	2
Awareness and Training (AT)	0	3	2
Audit and Accountability (AU)	0	9	0
Configuration Management (CM)	1	9	3
Identification and Authentication (IA)	2	11	2
Incident Response (IR)	0	3	2
Maintenance (MA)	0	6	0
Media Protection (MP)	1	9	0
Personal Security (PS)	0	2	1
Physical Protection (PE)	1	6	0
Risk Assessment (RA)	0	3	7
Security Assessment (RA)	0	4	1
System and Communications Protection (SC)	2	16	1
System and Information Integrity (SI)	4	7	3
Total	**15**	**110**	**24**

How the Nozomi Networks Platform Supports CMMC 2.0 Compliance

CMMC 2.0 requires DoD contractors to safeguard all assets in their relevant environments, including specialized assets[1] such as OT and IoT devices. These assets often operate on proprietary or legacy protocols, lack built-in security controls, and cannot be scanned or patched by traditional IT security tools without risking operational disruption.

For contractors whose relevant environments include OT and IoT assets, this creates a significant compliance challenge. CMMC practices — from asset identification to continuous monitoring and incident response — still apply, but most IT-centric solutions were never designed to address these unique systems. For starters, IT security tools can't read OT and IoT protocols, so they can't understand asset behavior and can't detect threats and anomalies.

The Nozomi Networks platform fills this gap. Purpose-built for critical infrastructure and industrial environments, it combines network and endpoint visibility, threat and anomaly detection and AI-powered analysis for faster, more effective response. Customers rely on us to minimize risk and complexity while maximizing operational resilience.

The summary below shows how the Nozomi Networks platform supports CMMC 2.0 at each level. Some of the required CMMC practices are a direct match for features found within the platform. For others, we provide key support for other tools or processes, significantly reducing the overall compliance challenge

[1] 32 CFR 170.19(c)(1) Specialized assets include IoT devices, Industrial IoT (IIoT) devices, OT, government furnished equipment (GFE), restricted information systems and test equipment.

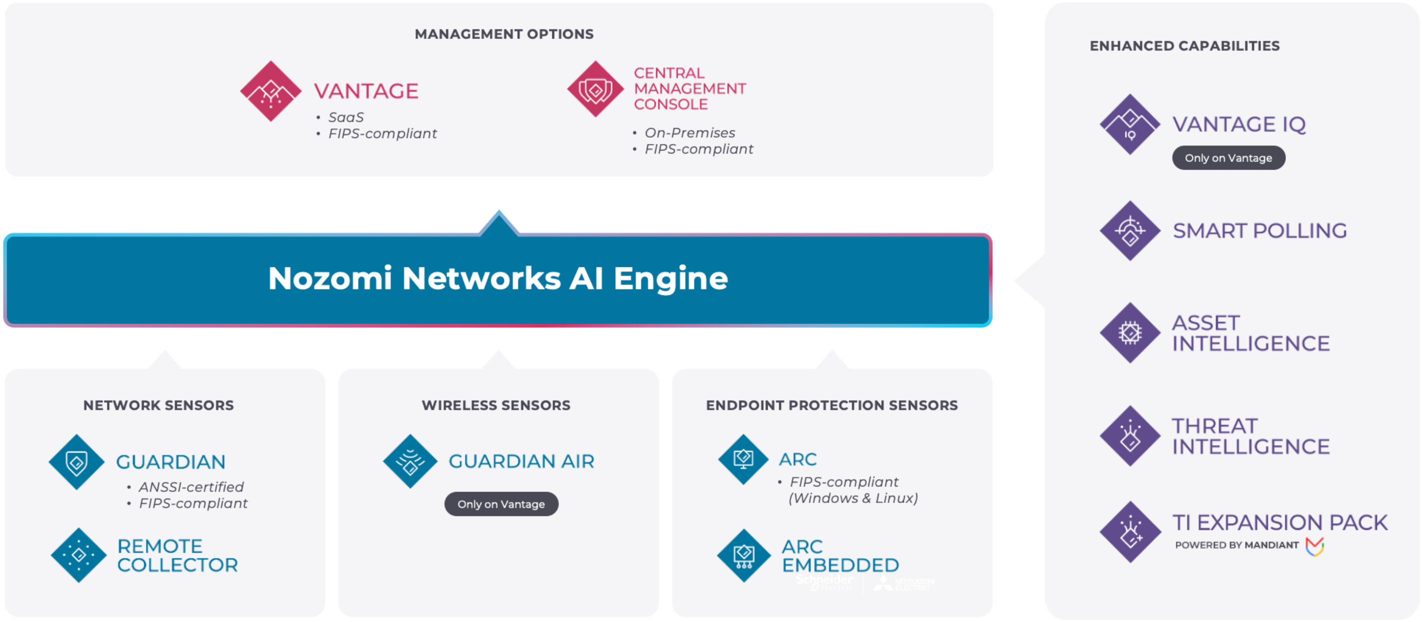
Domain	Level 1	Level 2	Level 3
Access Control (AC)	4	13	2
Awareness and Training (AT)	0	0	0
Audit and Accountability (AU)	0	5	-
Configuration Management (CM)	0	9	2
Identification and Authentication (IA)	2	1	0
Incident Response (IR)	0	2	0
Maintenance (MA)	0	4	-
Media Protection (MP)	0	1	-
Personal Security (PS)	0	0	0
Physical Protection (PE)	0	0	-
Risk Assessment (RA)	0	3	5
Security Assessment (RA)	0	3	0
System and Communications Protection (SC)	2	6	1
System and Information Integrity (SI)	3	2	2
Total	**11**	**49**	**12**

Nozomi Networks Platform Overview

Purpose built for complex industrial and critical infrastructure environments, the Nozomi Networks platform combines visibility from the endpoint to the air with continuous monitoring and AI-powered analysis to minimize cyber risk and maximize operational resilience. It helps you:

- See all OT, IoT and IT devices on your network and understand their behavior
- Detect and prioritize cyber threats, vulnerabilities and anomalies based on their risk
- Respond faster to critical breaches and process control issues with guided remediations.

The Nozomi Networks Platform



MANAGEMENT OPTIONS

VANTAGE
- SaaS
- FIPS-compliant

CENTRAL MANAGEMENT CONSOLE
- On-Premises
- FIPS-compliant

Nozomi Networks AI Engine

NETWORK SENSORS

GUARDIAN
- ANSSI-certified
- FIPS-compliant

REMOTE COLLECTOR

WIRELESS SENSORS

GUARDIAN AIR

Only on Vantage

ENDPOINT PROTECTION SENSORS

ARC
- FIPS-compliant (Windows & Linux)

ARC EMBEDDED

ENHANCED CAPABILITIES

VANTAGE IQ

Only on Vantage

SMART POLLING

ASSET INTELLIGENCE

THREAT INTELLIGENCE

TI EXPANSION PACK

POWERED BY MANDIANT

How the Nozomi Networks Platform Leverages AI/ML

Artificial intelligence (AI) and machine learning (ML) methodologies are everywhere today. For cybersecurity leaders, the challenge is to use the right AI/ML techniques in the right ways to at least keep pace with threat actors, who are using it to launch sophisticated attacks faster than ever.

Nozomi Networks is the leader in AI /ML for OT and IoT cybersecurity. Our R&D and lab teams have been building it into our platform and training our AI engine in-house since Day One — almost 13 years ago. That's more than a decade of real-world experience leveraging AI to defend some of the largest industrial and critical infrastructure organizations around the globe. In that time, we've learned which data matters, which is less important, and how to collect the maximal amount of right data and context to produce the right outcomes.

We use a variety of AI/ML methodologies throughout our platform, choosing the right tool (ML, predictive analysis, behavioral analytics, Bayesian Networks, LLMs) for the task at hand (asset inventory, vulnerability management, threat and anomaly detection, risk management) so you get actionable insights into your environment explaining what to do now to increase operational and cyber resilience.

Nozomi Networks Platform Features	
Asset Inventory	• Builds a comprehensive asset inventory via passive and active data collection, OT/IoT protocol support, third-party data ingestion and AI enrichment of asset profiles • Collects asset attributes including network, user, process, software, hardware, utilization, lifecycle, asset criticality and more
Communication Inventory	• Identifies and visualizes all OT/IoT network communications in east-west and north-south communications • Includes authorized and unauthorized wireless communications across at least the 800 MHz to 5895 MHz spectrum, covering Wi-Fi, Bluetooth, IEEE 802.15.4, LoRaWAN, Z-Wave, cellular and drones.
Vulnerability Identification and Prioritization	• Automates detection and assessment of firmware, operating system and software vulnerabilities in OT/IoT assets and communications. • Regularly updates vulnerability databases from community sources, integration partners and Nozomi Networks Labs • Prioritizes vulnerabilities based on criticality and exploitability, including CVSS, EPSS and KEV scores, and accounts for asset and environmental criticality.
Threat and Anomaly Detection	• Combines rule-based and behavior-based techniques to detect and limit the impact of threats and anomalies in your environment, from resource spikes to zero-days to living-off-the-land techniques to wireless attacks and malicious host activities • Leverages a continuously updated OT/IoT-focused threat intelligence feed to stay ahead of emerging malware and IOCs • Uses deep packet inspection to parse industrial protocols in network traffic and alert on suspicious behavior that deviates from baselines established with machine learning.
Risk Assessment and Prioritization	• Assigns a customizable weighted risk score for each asset and related entity (sensor, zone, site, enterprise) reflecting threat, vulnerability, controls effectiveness and impact • Calculates scores based on asset criticality, device risk, communication risk, vulnerability risk, alert risk and compensating controls.
Risk Remediation	• Prioritizes risk remediation actions based on hardware, software, communications/segmentation, team training and supply chain recommendations.
Incident Response	• Provides clear instructions the guide users through the appropriate actions to follow when an alert is triggered.

Determining the CMMC Relevant Environment

Properly determining the systems environment covered by CMMC is critical to obtaining compliance and keeping costs down. CUI is considered infectious under CMMC. If there is no clear boundary between the systems that process, store or transmit CUI and other systems, it is assumed that a compromise or infection in any CUI component could infect the entire environment. Without defined boundaries, the entire connected environment may fall within scope of CMMC.

The Nozomi Networks platform helps contractors establish and validate those boundaries and identify the assets within those boundaries – a crucial milestone in the road to compliance. Our wired, wireless and endpoint sensors identify all networks, assets and their communications flows, information that's used to model and baseline activity in your environment, regardless of their relevance to CMMC. This helps you:

- Understand actual network activity and communications
- Validate that network segmentation is operating as expected
- Monitor to ensure that CUI infections cannot propagate into systems that should remain out of scope

To eliminate ambiguities, CMMC defines to types of segmentation:

- **Isolated** assets have no logical access to an CMMC-regulated assets
- **Controlled Access** assets interact with CMMC-regulated assets in a controlled manner, typically through a firewall or other technology

Our security sensors validate communications between assets and ensure that systems are working in accordance with these CMMC definitions.

Extracting Relevant Reporting Information for Certification

CMMC 2.0 requires contractors not only to implement security controls, but to document and prove those controls are operating as intended. This means producing clear, defensible evidence for inclusion in Levels 1- Level 2 self-assessments, Level 2 C3PAO assessments and Level 3 DIBCAC assessments

The Nozomi Networks platform makes this simple. From a single interface, it continuously collects, correlates and stores security-relevant data across your OT, IoT and industrial networks. With powerful filtering, search and export capabilities, users can quickly extract:

- Asset inventories showing every device in the monitored environment, its role and current security posture
- Alert histories documenting detected threats, anomalies or policy violations and the corresponding response actions
- Configuration and segmentation validation records to demonstrate boundaries are intact and access controls are enforced
- Vulnerability and risk assessment reports highlighting discovered weaknesses, prioritization logic and remediation progress
- Anomaly and incident timelines for root-cause analysis and event reconstruction

The platform maintains a detailed historical record of network activity and security events, complete with time stamps, asset identities and contextual data, so generating compliance-ready reports is straightforward. This evidence can be exported in multiple formats and mapped directly to control requirements, saving time and reducing audit preparation costs.

Domain Requirements Mapping

Domain: Access Control (AC)

The Nozomi Networks platform continuously monitors network communications and the connections between devices and systems. Alerts are raised by abnormal behavior that could indicate an access control issue or weak cyber hygiene such as the use of cleartext passwords.

Monitoring also identifies suspicious remote access activity such as improperly used or stolen credentials, as well as behavior that typically evades detection by other tools. Examples include an unusually high number of remote connections, the use of uncommon protocols in those connections, portable device connections and atypical remote use behavior. Detailed visibility into each remote connection includes:

- The systems accessed by each remote user
- The protocols used and the network zones or VLANs traversed
- Any configuration or firmware changes made to any accessed system

In addition, the platform identifies anomalous asset activity due to a compromise. Fast detection and notification of access control incidents enable you to remediate before security or operations are disrupted.

The Nozomi Networks platform integrates with leading remote access management tools already in your security stack. This allows your cybersecurity and operations teams to secure almost any type of remote access to converged OT/IoT environments including VPNs, terminal servers, jump servers and clientless remote desktops. Additionally, because the Nozomi Networks platform shares its asset knowledge with other authorized applications, security teams can make better decisions around the granting of access privileges.

Level 1	Practice	How We Help
AC.L1-3.1.1	**Authorized Access Control** Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	Monitors and correlates device and user access paths, detecting unauthorized sessions and devices across the OT/IoT environment; validates segmentation and access policy enforcement via observed traffic.
AC L1-3.1.2	**Transaction & Function Control** Limit information system access to the types of transactions and functions that the authorized users are permitted to execute.	Uses DPI to observe allowed command/transaction types by asset and zone; alerts on out of policy operations or role inconsistent actions on OT/IoT devices and related communication channels.
AC L1-3.1.20	**External Connections** Verify and control/limit connections to and use of external information systems.	Discovers and inventories external connections to OT/IoT networks and flags unmanaged remote links, including wireless bridging, or cloud egress paths for review.
AC L1-3.1.22	**Control Public Information** Control information posted or processed on publicly accessible information systems.	Detects data flows from OT/IoT to public networks and alerts on unintended exposure, helping control information posted or processed on public systems..

Level 2	Practice	How We Help
AC L2-3.1.3	**Control CUI Flow** Control the flow of CUI in accordance with approved authorizations.	Monitors OT/IoT network traffic to identify, alert on, and log unauthorized transfers of sensitive data, ensuring flows comply with approved paths and authorizations.
AC L2-3.1.4	**Separation of Duties** Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	Correlates user activity with OT/IoT asset access to detect policy violations or unauthorized role combinations, supporting enforcement of separation of duties.
AC.L2-3.1.5	**Least Privilege** Employ the principle of least privilege, including for specific security functions and privileged accounts	Detects protocol/command misuse and lateral movement that indicate privilege overreach; highlights assets with excessive access across the OT/IoT environment.
AC.L2-3.1.6	**Non-Privileged Account Use** Use non-privileged accounts or roles when accessing nonsecurity functions.	Correlates user sessions and actions to endpoints; flags use of privileged tools from non privileged sessions on OT/IoT systems where telemetry is available.
AC.L2-3.1.7	**Privileged Functions** Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	Detects and logs execution of privileged functions (e.g., firmware/logic changes, configuration writes) on OT/IoT devices with time-stamped evidence.
AC.L2-3.1.8	**Unsuccessful Logon Attempts** Limit unsuccessful logion attempts.	Identifies failed/automated logon patterns at access gateways and wireless entry points; surfaces brute force or password spray behavior targeting OT/IoT assets.
AC.L2-3.1.12	**Control Remote Access** Monitor and control remote access sessions.	Monitors remote access sessions into OT/IoT networks, providing start/stop times, protocol used, and policy deviations for continuous oversight.
AC.L2-3.1.13	**Remote Access Confidentiality** Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	Flags plaintext or weakly protected remote sessions; identifies remote protocols lacking encryption to enforce cryptographic remote access policies.
AC.L2-3.1.14	**Remote Access Routing** Route remote access via managed access control points.	Verifies that remote access traverses managed control points by detecting direct peer to peer paths or bypass routes into OT/IoT segments.

Level 2	Practice	How We Help
AC.L2-3.1.15	**Privileged Remote Access** Authorize remote execution of privileged commands and remote access to security-relevant information.	Captures privileged remote command activity against OT/IoT assets and provides evidence for authorization review and approval workflows.
AC.L2-3.1.16	**Wireless Access Authorization** Authorize wireless access prior to allowing such connections.	Discovers wireless devices and attempts to connect; alerts on unauthorized wireless access to OT/IoT networks for prior authorization enforcement.
AC.L2-3.1.17	**Wireless Access Protection** Protect wireless access using authentication and encryption.	Evaluates wireless posture (auth/encryption), detects rogue APs and de auth/brute force activity; helps validate protection of wireless access.
AC.L2-3.1.21	**Portable Storage Use** Limit use of portable storage devices on external systems.	Detects and reports portable storage usage events on OT/IoT assets; correlates with policy and subsequent network activity.

Level 3	Practice	How We Help
AC.L3-3.1.2e	**Organizationally Controlled Assets** Restrict access to systems and system components to only those information resources that are owned, provisioned, or issued by the organization.	Identifies and monitors all assets in the environment, detecting unauthorized or unmanaged devices attempting to access organizational systems.
AC.L3-3.1.3e	**Secured Information Transfer** Employ secure information transfer solutions to control information flows between security domains on connected systems.	Monitors and validates information flows between network zones, helping enforce segmentation between security domains. Detects unauthorized communications or policy violations that may indicate improper data transfer paths across controlled system boundaries.

Domain: Audit and Accountability (AU)

The Nozomi Networks platform captures the audit details needed to identify changes made to assets and the OT/IoT environment via logs, reports and system snapshots taken at periodic intervals that can be drilled into to examine a rich information set.

Information captured by these methods includes:

- The identity of all devices communicating over the network
- Network traffic details such as throughput, protocols and open TCP connections
- The protocols used to communicate between nodes and zones
- Threat and vulnerability data by asset, with details that help remediation

This information also supports investigative and forensic activities as described under the Incident Response domain (IR).

Level 2	Practice	How We Help
AU.L2-3.3.1	**System Auditing** Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	Generates and retains audit telemetry for OT/IoT and wireless assets (events, flows, changes) with searchable timelines; integrates with SIEM for monitoring and reporting.
AU.L2-3.3.2	**User Accountability** Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions.	Correlates user identity (where available) with endpoint and network actions for per user accountability across OT/IoT environments.
AU.L2-3.3.5	**Audit Correlation** Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	Performs cross domain correlation (network, endpoint, wireless) to accelerate investigation and response to suspicious or unlawful activity.
AU.L2-3.3.6	**Reduction & Reporting** Provide audit record reduction and report generation to support on-demand analysis and reporting.	Reduces alert noise via deduplication and risk based prioritization; provides on demand reports for audits and investigations.
AU.L2-3.3.7	**Authoritative Time Source** Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	Normalizes telemetry with synchronized timestamps (authoritative time sources), preserving event ordering across OT/IoT and wireless domains.

Domain: Configuration Management (CM)

The Nozomi Networks platform uses machine learning to create a model of the OT/IoT environment. It learns and establishes baselines for:

- Assets
- Communications
- Hardware and OS types
- Processes
- Parameters and setpoints

Changes to configurations and devices, or new devices connected to the network, raise alerts. Programming changes can be examined to highlight differences, and if desired, trigger automated response actions. Built-in logging, reporting and system snapshots track changes and provide audit trails.

Level 2	Practice	How We Help
CM.L2-3.4.1	**System Baselining** Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	Builds and maintains an up to date inventory and baseline of OT/IoT assets, firmware, services, and communications; tracks deviations over time.
CM.L2-3.4.2	**Security Configuration Enforcement** Establish and enforce security configuration settings for information technology products employed in organizational systems.	Monitors for configuration drift and noncompliant settings on OT/IoT devices; provides evidence to support enforcement of secure configurations.
CM.L2-3.4.3	**System Change Management** Track, review, approve or disapprove, and log changes to organizational systems.	Detects, logs, and reports system changes (logic/firmware/config/flows) to support review and approval processes.
CM.L2-3.4.4	**Security Impact Analysis** Analyze the security impact of changes prior to implementation.	Assesses security impact by correlating changes with vulnerabilities, exposure, and asset criticality; adjusts risk accordingly.
CM.L2-3.4.5	**Access Restrictions for Change** Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	Observes access to change capable interfaces and records change activity, enabling verification of access restrictions for changes.

Level 2	Practice	How We Help
CM.L2-3.4.6	**Least Functionality** Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	Profiles OT/IoT devices to establish normal operational baselines and alerts on the activation or presence of unnecessary services, ports, or functions.
CM.L2-3.4.7	**Nonessential Functionality** Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	Highlights nonessential functions and unexpected protocols/ports in use, informing restriction or disablement decisions.
CM.L2-3.4.8	**Application Execution Policy** Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	Detects execution of unauthorized software or scripts on OT/IoT assets; supports deny all/permit by exception policies with evidence.
CM.L2-3.4.9	**User-Installed Software** Control and monitor user-installed software.	Monitors for user installed or newly present software on OT/IoT assets and flags deviations from baseline.

Level 3	Practice	How We Help
CM.L3-3.4.1e	**Authoritative Repository** Establish and maintain an authoritative source and repository to provide a trusted source and accountability for approved and implemented system components.	Continuously monitors OT/IoT systems for configuration changes and anomalies that could indicate integrity violations. Detects deviations from expected baselines and security policies, providing alerts and contextual data to validate and enforce secure configurations across managed environments.
CM.L3-3.4.2e	**Automated Detection & Remediation** Employ automated mechanisms to detect misconfigured or unauthorized system components; after detection, remove the components or place the components in a quarantine or remediation network to facilitate patching, re-configuration or other mitigations.	Automatically detects unauthorized or misconfigured assets or threats, then alerts security teams while the integration with enforcement tools isolates affected devices for remediation.
CM.L3-3.4.3e	**Automated Inventory** Employ automated discovery and management tools to maintain an up-to-data, complete, accurate and readily available inventory of system components.	Passive and active automatic discovery all OT, IoT and IT assets across the environment in a continuously updated, centralized inventory with detailed component attributes, enabling visibility, compliance reporting and rapid response to changes.

Domain: Identification and Authentication (IA)

The Nozomi Networks platform detects the use of cleartext passwords, as well as protocols that might expose credentials. Integrations with access management tools including LDAP, Aruba ClearPass (2x) and Cisco ISE provide control over user access and the authentication of ICS assets.

Level 1	Practice	How We Help
IA.L1-3.5.1	**Identification** Identify information system users, processes acting on behalf of users, or devices.	Identifies devices and sessions on OT/IoT networks; associates activity with specific assets to support user/device identification requirements.
IA.L1-3.5.2	**Authentication** Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	Detects use or absence of authentication on OT/IoT protocols; flags default or shared credentials and unauthenticated services for remediation.

Level 2	Practice	How We Help
IA.L2-3.5.10	**Cryptographically-Protected Passwords** Store and transmit only cryptographically-protected passwords.	Detects cleartext password exchange and weak authentication methods on OT/IoT links; highlights where cryptographic protection is required.

Level 3	Practice	How We Help
IA.L3-3.5.1e	**Bidirectional Authentication** Identify and authenticate systems and system components, where possible, before establishing a network connection using bidirectional authentication that is cryptographically based and replay resistant.	Monitors network traffic to identify when systems are not performing proper bidirectional authentication, detects anomalies such as unsecured communications or replay attempts, and validates use of cryptographic protocols during connection establishment.
IA.L3-3.5.3e	**Block Untrusted Assets** Employ automated or manual/procedural mechanisms to prohibit system components from connecting to organization systems unless the components are known, authenticated, in a properly configured stat, or in a trust profile.	Detects and alerts on unknown, misconfigured or untrusted assets attempting to connect to the network, enabling enforcement of asset trust profiles and integration with access controls to block unauthorized components.

Domain: Incident Response (IR)

The Nozomi Networks platform reduces forensic efforts and speeds response time. Its advanced wired, wireless and endpoint monitoring identifies security and reliability risks and generates detailed, accurate alerts. Each alert describes what happened, provides possible causes and recommends actions to take, reducing investigative efforts. In addition, through integrations with leading firewalls/UTMs, EDR tools and NACs, security responses to threats can be automated.

When further analysis is needed, additional tools are available.

Incident View of Grouped Alerts

Across the platform, alerts are grouped into Incidents that are related in time, asset or cause into a single view. When an operator sees that a critical incident is underway, via an alert they can examine the PCAP related to the alert and download it. With one click they can also access a diff report to compare times before and after the alert. Once changed parameters are identified, staff can take action to stop or mitigate an attack.

Time Machine Forensic Tool

Diff reports are an aspect of the platform's time machine feature, which takes snapshots of the system at periodic intervals so it can be explored and investigated at many moments in time. The snapshots are dynamic, allowing operators to drill down and examine a rich information set that accelerates response.

The platform further facilitates incident response with its powerful ad-hoc query tool that provides real-time responses to inquiries. The query tool can access the wide range of OT/IoT data such as alerts, assets, links, nodes, sessions, variables and zones. It can also use commands and functions to analyze the data.

AI-powered Analysis

Vantage IQ is Nozomi Networks' AI-powered analysis and response engine. It accelerates incident response in five key ways:

- **Alert correlation and prioritization:** Vantage IQ's Insights Dashboard automatically correlates numerous alerts into unified incidents, prioritizing them based on risk and providing root-cause context. This enables IR teams to focus on the most critical issues without getting overwhelmed by noise.
- **Root cause analysis:** Deep neural networks analyze network behavior patterns to support efficient root-cause identification.
- **Natural language queries:** Users can pose queries in plain language, such as "What are my high-risk vulnerabilities?" or "Which assets are most exposed?" They gain quick situational awareness that would otherwise require hours or days.
- **Predictive monitoring:** Vantage IQ applies machine learning to detect deviations from baseline network behavior. By alerting on unusual bandwidth and activity patterns, it can flag issues before they escalate into full-blown incidents.
- **Guided remediation:** Vantage IQ suggests actionable remediation steps. It can also highlight suboptimal sensor placements and recommend adjustments to enhance visibility, improving incident readiness and response accuracy.

Level 2	Practice	How We Help
IR.L2-3.6.1	**Incident Handling** Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	Provides continuous detection, evidence capture, and guided response workflows for OT/IoT incidents; supports preparation, analysis, containment and recovery.
IR.L2-3.6.2	**Incident Reporting** Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	Tracks and documents incidents with timestamps, artifacts and impact context; integrates with ticketing/SIEM to support internal/external reporting.

Domain: Maintenance (MA)

The Nozomi Networks platform provides operators with a comprehensive asset inventory, complete with the firmware and OS version of all devices and their subparts. This enables easy tracking of system updates and helps ensure that equipment is kept up to date.

The platform also identifies equipment that may be failing and alerts you about it so you can act before an outage occurs. For example, if a PLC starts to behave outside the normal range for its equipment type and baseline pattern in your operation, you will be warned. In diagnosing the problem, you will know the type of PLC, the type of cards it is running, its firmware and its serial number. Overall, your visibility to maintenance issues and ability to act before production outages is significantly improved.

To further enrich asset profiles, our Asset Intelligence feed uses advanced behavioral inference to fill in missing data from like data in our database. These enriched profiles enable teams to make informed decisions about the maintenance and security of your digital assets. Our AI engine learns from millions of assets that we monitor in customer environments across industries around the globe. This data trove is used to fill in gaps about identical devices across environments based on attributes such as MAC addresses, configuration, protocols, end-of-sale and -support dates, and more. When a match is found, those attributes and behaviors are added to your device profile.

Level 2	Practice	How We Help
MA.L2-3.7.1	**Perform Maintenance** Perform maintenance on organizational systems.	Logs maintenance windows and observed maintenance activity on OT/IoT assets; differentiates expected vs. anomalous behavior during service periods.
MA.L2-3.7.2	**System Maintenance Control** Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	Monitors the tools, techniques, and accounts used during maintenance; flags unauthorized utilities or personnel activity.
MA.L2-3.7.5	**Nonlocal Maintenance** Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	Detects nonlocal maintenance sessions into OT/IoT networks; provides evidence to validate MFA and terminates none—alerts when sessions persist beyond policy.
MA.L2-3.7.6	**Maintenance Personnel** Supervise the maintenance activities of maintenance personnel without required access authorization.	Captures maintenance personnel actions on systems for supervision and after action review, including remote work.

Domain: Media Protection (MP)

In IT security, USB use has drastically waned due to the ease of transferring files via the cloud. In OT environments, however, they are still commonly used to move files between restricted Purdue levels. While most file transfers are routine, the practice is risky. Worst case, a BadUSB attack can reprogram the USB to execute malicious commands on a victim's computer.

In 2023, Nozomi Networks introduce Nozomi Arc, the first endpoint security solution specifically designed for OT and IoT environments. Traditional endpoint security agents are too heavyweight and disruptive for OT devices and controllers, and they detect the wrong threats. Arc detects when and where a USB is plugged into an endpoint in the environment, along with any non-human behavior involving commands, scripts or data movement. In addition to detecting unauthorized USB connections, Arc identifies endpoints compromised by malware, rogue applications or suspicious user activity.

Level 2	Practice	How We Help
MP.L2-3.8.7	**Removable Media** Control the use of removable media on system components.	Detects removable media usage on OT/IoT assets and correlates file or process activity to enforce media policies.

Domain: Risk Assessment (RA)

Assessing risk in industrial and critical infrastructure environments is different from assessing traditional OT risk. Key differences include:

- **Cyber and operational risk:** You must account for both cyber and operational risk. If a server goes down in an operational environment, you have massive risk.
- **Consequence-based:** OT risk is consequence based. It must consider physical safety, environment harm and continuity or operations.
- **Interconnected risk:** Every component in an OT network is part of a larger process in a very distributed environment.
- **Multi-dimensional:** In IT, device risk is based solely on vulnerabilities, and you can practically eliminate risk with patching. In OT, patching must often be delayed until the next maintenance window, assuming patches exist at all. Other factors and controls must be weighed.

The Nozomi Networks platform assigns risk scores to each of your assets to help you prioritize security efforts, address the most critical risks first and take the correct actions to mitigate potential threats effectively. It calculates asset risk based on five factors: vulnerability risk, alert risk, communication risk, device risk, asset criticality and compensating controls. You can use our scores out of the box, or you can fully customize the weight of each variable until the calculation accurately reflects how your organization assigns risk.

Dashboards enable you to see at a glance what assets are riskiest by zone, site, vendor and other categories, and how individual risk scores contribute to higher-level scores. If your risk is trending in the wrong direction, you can drill down to see why and where you need to add controls. As you do, your risk score will change to reflect the impact your actions.

Level 2	Practice	How We Help
RA.L2-3.11.1	**Risk Assessments** Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	Continuously assesses asset and network risk and assigns a multi factor risk score at the asset, zone, site and enterprise level and dynamically recalculates scores based on changing conditions, including compensating controls.
RA.L2-3.11.2	**Vulnerability Scan** Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	Performs passive vulnerability discovery and maps newly disclosed CVEs to affected OT/IoT assets; supports safe scan alternatives.
RA.L2-3.11.3	**Vulnerability Remediation** Remediate vulnerabilities in accordance with risk assessments.	Prioritizes and tracks remediation based on exploitability, exposure, and operational criticality; validates risk reduction over time.

Level 3	Practice	How We Help
RA.L3-3.11.1e	**Threat-Informed Risk Assessment** Employ threat intelligence, at a minimum from open or commercial sources, and any DoD-provided sources, as part of a risk assessment to guide and inform the development of organizational systems, security architectures, selection of security solutions, monitoring, threat hunting, and response and recovery activities.	Ingests and correlates threat intelligence from multiple sources to inform risk assessments; guide security architecture decisions; and support monitoring, hunting, and incident response across OT and IoT systems.
RA.L3-3.11.2e	**Threat Hunting** Conduct cyber threat hunting activities on an on-going aperiodic basis or when indications warrant, to search for indicators of compromise in organizational systems and detect, track, and disrupt threats that evade existing controls.	Enables proactive threat hunting by continuously analyzing network and device behavior to detect indicators of compromise, track stealthy threats and uncover malicious activity that bypasses traditional defenses, with enriched context from integrated Mandiant threat intelligence.
RA.L3-3.11.3e	**Advanced Risk Identification** Employ advanced automation and analytics capabilities in support of analysts to predict and identify risks to organizations, systems, and system components.	Leverages AI-driven analytics, contextual asset intelligence, vulnerability exposure, wireless threat detection and configuration risk insights to help analysts proactively identify and prioritize risks across OT, IoT and cyber-physical environments, all within a unified platform.

Level 3	Practice	How We Help
RA.L3-3.11.5e	**Security Solution Effectiveness** Assess the effectiveness of security solutions at least annually or upon receipt of relevant cyber threat information, or in response to a relevant cyber incident, to address anticipated risk to organizational systems and the organization based on current and accumulated threat intelligence.	Continuously evaluates the performance of deployed security controls by correlating real-time threat activity, asset behavior and vulnerability data, while generating actionable metrics, reports and predictive trends. Provides contextual benchmarking against sector-wide risks and threat intelligence to help organizations assess control effectiveness and adapt defenses proactively in response to evolving threats or incidents.
RA.L3-3.11.6e	**Supply Chain Risk Response** Assess, respond to, and monitor supply chain risks associated with organizational systems and system components.	Monitors supply chain risk by tracking asset lifecycle status, including end-of-sale and end-of-support states, flagging communications with unsafe or high-risk countries, and identifying country-of-origin exposure across connected devices. Provides visibility into potentially untrusted components, integrates with threat intelligence for supply chain risk correlation, and supports remediation decisions with contextual asset history and behavioral data.

Domain: Security Assessment (CA)

The Nozomi Networks platform assesses the effectiveness of an organization's security controls by continuously monitoring the OT/IoT environment and correlating asset behavior with the intended design of those controls. It generates detailed asset inventories, vulnerability reports, logs and timelines that show actual control performance including network segmentation in practice, access violations detected, services disabled and more. Key capabilities include:

- **Security control validation:** Monitors network traffic to verify that segmentation and isolation policies are being enforced; flags unauthorized authentication and connection attempts; profiles devices to detect least-functionality violations.
- **Threat and anomaly correlation:** Uses machine learning, behavioral analytics and Bayesian correlation to detect anomalies that may indicate control failure (e.g., malware bypassing a firewall, unexpected data exfiltration); cross-references anomalies with known vulnerabilities, threat intelligence and behavior baselines to pinpoint where controls may be ineffective.
- **Metrics and risk scoring:** Assigns multi-factor risk scores that account for compensating controls, tracking changes in risk posture over time to provide measurable evidence of whether controls are reducing risk.
- **Incident and response validation:** Records all detected threats and policy violations and verifies that remediation steps taken (patching, access revocation, configuration changes, etc.) resolve the original issue and that similar activity is not recurring.

Level 2	Practice	How We Help
CA.L2-3.12.1	**Security Control Assessment** Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	Provides objective evidence (events, baselines, detections) to assess the effectiveness of security controls in OT/IoT environments.
CA.L2-3.12.2	**Plan of Action** Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	Supports creation and execution tracking of plans of action by tying tasks to assets, detections and measurable risk reduction.
CA.L2-3.12.3	**Security Control Monitoring** Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	Continuously monitors wired and wireless traffic and endpoints to verify that security controls are working as designed, alerting and providing evidence when violations or failures are detected.

Domain: System and Communications Protection (SC)

By monitoring network traffic across wired, wireless and endpoint-connected OT/IoT assets, the Nozomi Networks platform discovers every device, identifies communication pathways and validates that network segmentation is operating as intended. Deep packet inspection and protocol analysis confirm that only approved communications occur between in-scope assets and that those communications align with defined security policies. Unauthorized connections (such as covert wireless links, rogue access points or bypass routes around controlled boundaries) are identified and flagged for remediation.

The platform detects the use of insecure protocols, validating proper use of secure communication methods and alerting on deviations from established baselines. Continuous monitoring, asset profiling and cross-domain correlation provide real-time assurance that systems and communications remain within compliance parameters. This enables organizations to prove, with time-stamped and context-rich evidence, that protective measures for their OT/IoT environment are in place and functioning.

Level 1	Practice	How We Help
SC.L1-3.13.1	**Boundary Protection** Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	Monitors and validates boundary and internal segmentation, detecting cross zone violations and risky communications involving OT/IoT assets.
SC.L1-3.13.5	**Public-Access System Separation** Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	Watches for communications between public facing components and internal OT/IoT segments; alerts on mis segmentation.

Level 2	Practice	How We Help
SC.L2-3.13.2	**Security Engineering** Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	Supports secure architecture decisions by revealing real traffic flows, protocol use, and exposure in OT/IoT environments.
SC.L2-3.13.3	**Role Separation** Separate user functionality from system management functionality.	Correlates user and admin activities to ensure separation; flags management actions from user sessions on OT/IoT assets.

Level 2	Practice	How We Help
SC.L2-3.13.7	**Split Tunneling** Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).	Detects split tunnel behaviors and dual homed pathways that could bridge OT/IoT with external networks.
SC.L2-3.13.9	**Connections Termination** Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	Identifies long lived idle sessions and unexpected persistence; alerts so connections can be terminated per policy.
SC.L2-3.13.12	**Collaborative Device Control** Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	Detects remote activation or presence of collaboration tools on operator workstations/HMIs; provides user visible indicators via alerts.
SC.L2-3.13.14	**Voice over Internet Protocol** Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	Monitors for VoIP traffic within OT networks, ensuring it is segmented, approved and not interfering with control traffic.

Level 3	Practice	How We Help
SC.L3-3.13.4e	**Isolation** Employ physical isolation techniques or logical isolation techniques or both in organizational systems and system components.	Supports physical and logical isolation by performing real-time network mapping, triangulating asset locations and connections including physical network ports, and identifying segmentation gaps. Detects unauthorized lateral movement, validates enforcement of isolation policies, and integrates with infrastructure to monitor and control communication boundaries.

Domain: System and Information Integrity (SI)

The Nozomi Networks platform continuously monitors the operational environment to detect vulnerabilities, configuration weaknesses, malware indicators and anomalous behavior across OT, IoT and connected systems. AI-enriched asset profiles provide real-time awareness of system flaws and known vulnerabilities. Our OT/IoT-focused threat intelligence feed helps ensure sensors can detect emerging malware and IOCs, while multi-factor risk scoring prioritizes remediation efforts based on threat exposure and operational criticality. Threat intelligence, anomaly detection and behavioral analytics work together to identify potential compromises early, including sophisticated or low-and-slow attacks that could bypass traditional defenses.

By correlating events from wired, wireless and endpoint monitoring, the platform accelerates detection, investigation and response to integrity violations. Configurable alerting ensures that deviations from baselines above established thresholds are reported immediately, while historical logging supports root-cause analysis and incident reconstruction.

Level 1	Practice	How We Help
SI.L1-3.14.1	**Flaw Remediation** Identify, report, and correct information and information system flaws in a timely manner.	Maintains visibility of firmware/software versions and vulnerabilities on OT/IoT assets; provides evidence for timely flaw remediation.
SI.L1-3.14.2	**Malicious Code Protection** Provide protection from malicious code at appropriate locations within organizational information systems.	Detects malware like behavior and known indicators in OT network traffic and on OT/IoT assets; complements traditional AV.
SI.L1-3.14.4	**Update Malicious Code Protection** Update malicious code protection mechanisms when new releases are available.	Highlights outdated protection mechanisms and signatures where telemetry is available; alerts when updates are overdue.

Level 2	Practice	How We Help
SI.L2-3.14.6	**Monitor Communications for Attacks** Identify, report, and correct information and Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	Monitors inbound/outbound communications using DPI to detect attacks and indicators of compromise targeting OT/IoT devices.
SI.L2-3.14.7	**Identify Unauthorized Use** Identify unauthorized use of organizational systems.	Identifies unauthorized use via anomaly detection, policy violation monitoring and correlation across network, endpoint and wireless data.

Level 3	Practice	How We Help
SI.L3-3.14.3e	**Specialized Asset Security** Ensure that specialized assets including IoT, IIoT, OT, GFE, Restricted Information Systems, and test equipment are included in the scope of the specified enhanced security requirements or are segregated in purpose-specific networks.	Continuously discovers and monitors specialized assets across IoT, IIoT, OT and other non-traditional environments, ensuring they are included in security visibility and policy enforcement. Identifies assets that are improperly segmented or outside approved zones and supports isolation or control through integration with network infrastructure and security platforms.
SI.L3-3.14.6e	**Threat-Guided Intrusion Detection** Use threat indicator information and effective mitigations obtained from, at a minimum, open or commercial sources, and any DoD-provided sources, to guide and inform intrusion detection and threat hunting.	Correlates threat indicators from commercial, open source, and government feeds with real-time network and device activity to guide intrusion detection and threat hunting. Enriches detections with contextual intelligence to identify threats that match known indicators and supports targeted investigation across OT and IoT environments.

Conclusion

Nozomi Networks is the leader in OT/IoT security and visibility. If your CMMC relevant environment includes OT and IoT devices (specialized assets), our platform provides the protocol mastery, monitoring techniques, and threat and anomaly detection capabilities that IT-centric security tools don’t have. It helps you determine your CMMC 2.0 relevant environment, automatically collect required data for certification, and meet key Level 1, 2 and 3 requirements within 11 of the 14 domains, including those that apply to specialized assets.

Take the Next Step

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

Request a Demo

nozominetworks.com/demo

Cybersecurity for OT, IoT and Critical Infrastructure

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.

nozominetworks.com