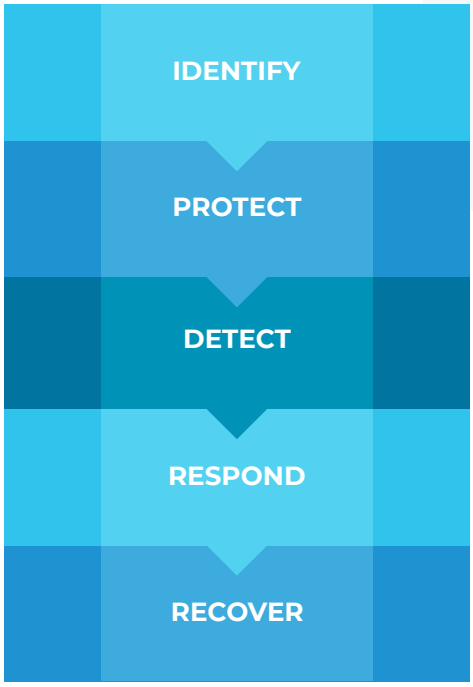
NOZOMI NETWORKS

COMPLIANCE MAPPING GUIDE

NIST

How the Nozomi Networks Solution Supports the NIST Cybersecurity Framework



Understanding the need for reliable critical infrastructure, the U.S. president issued an Executive Order in 2013 for the U.S. National Institute of Standards and Technology (NIST) to develop a new voluntary Cybersecurity Framework for reducing cyber risk to critical infrastructure. Within a year, the NIST Cybersecurity Framework (NIST CSF) was published. The framework identified 16 critical infrastructure sectors whose assets, systems and networks are vital to the country.

NIST CSF helps critical infrastructure organizations document and implement controls for information technology systems that support their operations and assets, including access control, audit and accountability, incident response, and system and information integrity. The framework is organized into five core functions: Identify, Protect, Detect, Respond, and Recover.

Simplify NIST CSF Compliance with Nozomi Networks

The Nozomi Networks Solution aligns with the NIST Cybersecurity Framework's primary directive of enabling critical infrastructure operations to effectively identify, manage, and reduce cyber risk. By combining the core security controls into a single solution, you can manage security in a more holistic and efficient way.

Identify

Purpose

Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

Examples of functions under this category include: asset management, business environment management, governance, risk assessment, and risk management strategy.

How Nozomi Networks Helps You Identify

As soon as it's deployed, the Nozomi Networks solution uses machine learning and a behavior-based analytics engine to develop a detailed asset inventory of the devices and connections in the network. By providing a detailed view of assets and connections, you will have an accurate picture of your network, how assets are communicating, and the vulnerabilities that exist.

Protect

Purpose

Develop and implement the appropriate preventative actions to ensure delivery of critical infrastructure services.

Examples of functions under this category include: access control, awareness and training, data security, information protection processes and procedures, maintenance, and protective technology.

How Nozomi Networks Helps You Protect

The Nozomi Networks solution integrates seamlessly with existing IT and security tools including SIEMs, firewalls, UTM devices, EDR tools, ticketing management systems, access control systems, and more. These integrations provide full visibility of all your IT, OT and IoT assets. Additionally, this visibility can help you reduce your time to incident response and even automate some processes.

Detect

Purpose

Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. The detect function enables timely discovery of cybersecurity events.

Examples of functions under this category include: anomalies and events, security continuous monitoring, and detection processes.

How Nozomi Networks Helps You Detect

By combining artificial intelligence with traditional threat detection technologies, the Nozomi Networks solution helps you quickly detect and respond to threats. This hybrid approach reduces false positives and provides additional context on the behavior on your network. The solution also uses machine learning to detect changes to the environment that, if left unattended, could lead to equipment failure or critical system downtime. Integrated threat intelligence can be accessed through Nozomi Networks Labs, which uses rules and signatures to help identify emerging threats and zero-days in your network.

Simplify NIST CSF Compliance with Nozomi Networks

Respond

Purpose

Develop and implement the appropriate activities to mitigate a detected cybersecurity event. The respond function supports the ability to contain the impact of a potential cybersecurity event.

Examples of functions under this category include: response planning, communications, analysis, mitigation, and improvements.

How Nozomi Networks Helps You Respond

Beyond detection, the solution supports rapid threat remediation and response. By using queries and rules, you can automatically kick off investigations by triggering actions like “create a TimeMachine snapshot” or “send email alerts to an SNMP trap” to speed up forensics. It also integrates with tools such as firewalls, UTM devices, EDR devices, and ticketing systems that automate responses such as “block this IP” or “create a ticket for the security team.”

Recover

Purpose

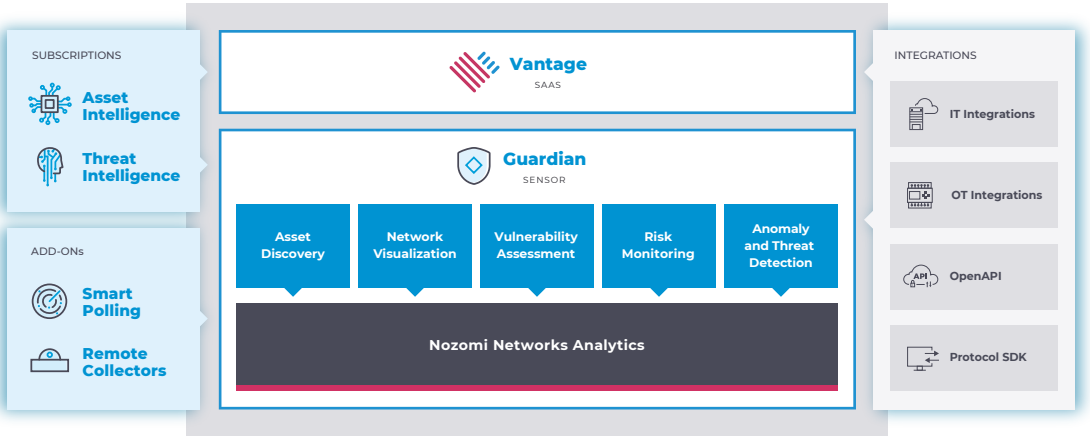
Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

Examples of functions under this category include: recovery planning, improvements, and communications.

How Nozomi Networks Helps You Recover

The Nozomi Networks solution provides built-in governance features such as a rich historian, network snapshot comparison functionality (Time Machine™), custom queries, and more. This data can be used for postmortem analysis to reevaluate security policy decisions and complete the cyclical process of constant improvement.

Nozomi Networks Solution Architecture



Nozomi Networks Mapping to NIST Cybersecurity Framework

Function	NIST CIS Category	NIST CIS Sections that Nozomi Networks Covers	How Nozomi Networks Helps
Identify (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	ID.AM-1, ID.AM-2, ID.AM-3, ID.AM-4	• Built-in asset discovery provides a dynamically updated inventory of assets across your entire OT and IoT environment
	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	ID.BE-5	• Redundant and high availability architecture can be provided to maintain continuous risk monitoring and threat detection for your infrastructure
	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	ID.RA-1, ID.RA-2, ID.RA-3, ID.RA-4, ID.RA-5	• Identify systems susceptible to known vulnerabilities, with devices ranked from low to high risk vulnerabilities • Identify patches or workaround available to vulnerable systems • Integrated threat and asset intelligence provide up-to-date information on threats, vulnerabilities and anomalies • Alerts are generated for new threats and anomalous behavior, with risk scores included to demonstrate which alerts should be prioritized • Suggested remediation steps are included in the threat knowledgebase for each alert

Nozomi Networks Mapping to NIST Cybersecurity Framework

Function	NIST CIS Category	NIST CIS Sections that Nozomi Networks Covers	How Nozomi Networks Helps
Protect (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	PR.AC-1	• Seamless integrations, with access management tools like LDAP, Aruba Clearpass, CISCO ISE and more, provide control over user access and authentication of OT and IoT assets
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-1, PR.AT-2	• Nozomi Networks Certified Engineer Training Course provides a 3-day hands-on instruction that covers basics in cybersecurity, OT infrastructure, and how to leverage the Nozomi Networks solution for OT and IoT cybersecurity and operational intelligence
	Information Protection Processes and Procedures (PR.IP): Security policies (which address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-1, PR.IP-3, PR.IP-5, PR.IP-7, PR.IP-8, PR.IP-12	• Machine learning creates a baseline of the environment, systems, and processes running • Changes in configurations can be alerted on, with automated response actions to manage the changes • Integrated threat intelligence from Nozomi Networks Labs is updated regularly to provide continuous improvements to threat detection and vulnerability assessment capabilities • Email alerts, SMS, and seamless integrations with ticketing systems ensure that information is properly shared with the right people • Continuous vulnerability assessments of assets in the OT and IoT environment provide the foundations for a thorough vulnerability management plan
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	PR.PT-1	• Built-in logging and reporting capabilities, plus a rich historian and network snapshotcapabilities provide audit details needed to identify changes made to systems

Nozomi Networks Mapping to NIST Cybersecurity Framework

Function	NIST CIS Category	NIST CIS Sections that Nozomi Networks Covers	How Nozomi Networks Helps
Detect (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5	• As soon as it's deployed, Nozomi Networks uses machine learning to create a baseline of the environment • Through the Threat and Asset Intelligence services, threats and vulnerabilities, anomalies, data, events, and communications are monitored in real-time for potential threats • Nozomi Networks uses a hybrid approach to threat detection by combining both anomaly detection to alert on changes in the environment with traditional threat detection technologies to identify known malicious activities • All events in the Nozomi Networks solution are scored based on risk - the risk score takes into account vulnerabilities that exist on the asset, the severity of threats detected, and more
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-1, DE.CM-3, DE.CM-4, DE.CM-5, DE.CM-6, DE.CM-7, DE.CM-8	• Nozomi Networks combines both continuous passive monitoring with active discovery approaches to collect comprehensive data about the network • When changes are made to devices in the network or new devices connect to the network, alerts are raised • Malicious code, such as malware, ransomware, etc. are identifed by the Threat Intelligence service • Vulnerability assessment is provided in real-time. And as new and emerging threats (like zero-days) are announced, Nozomi Networks immediately checks your network for indicators by using the Threat Intelligence and Asset Intelligence services
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	DE.DP-4, DE.DP-5	• Built-in alerts for email and SMS, plus seamless integrations with IT tools such as ticketing systems help to make sure that the appropriate parties are alerted when there is an incident • The Nozomi Networks platform undergoes regular monthly updates to improve the quality of our machine learning and anomaly detection capabilities. Additionally, the Asset Intelligence service is updated on a regular basis with rules and signatures to detect new and emerging threats

Nozomi Networks Mapping to NIST Cybersecurity Framework

Function	NIST CIS Category	NIST CIS Sections that Nozomi Networks Covers	How Nozomi Networks Helps
Respond (RS)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	RS.RP-1	• The moment a security incident is detected, rapid communications and detailed information are key to success for incident response teams. The Nozomi Networks solution provides real-time alerts to administrators that include all the contextual information they need to respond quickly and accurately.
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cyber security awareness education and are trained to perform their ybersecurity for both instances duties and responsibilities consistent with related policies, procedures, and agreements.	RS.CO-2	• The Nozomi Networks solution provides consistent reporting of threat data to customers, which includes details on the threat, which assets are affected, any applicable vulnerabilities, and more
	Information Protection Processes and Procedures (PR.IP): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	RS.AN-3	• Nozomi Networks helps customers through the first steps of response by providing access to PCAPs that can be used in the forensic investigation • The Time Machine capability allows customers to compare changes in the network and analyze alerts at the time of the incident • Response actions can be automated to gather forensic details any time a certain event occurs in the network
	Mitigation (RS.MI): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	RS.MI-1	• Through integrations with firewalls/ UTMs, EDR tools, and NACs, Nozomi Networks helps customers contain threats by automating response actions for threats
Recover (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	RC.RP-1	• Using the forensic data and pcaps collected in Nozomi Networks, security teams can scan the entire network for indicators of compromise to identify remaining pockets of infection. Teams can use post-mortem analysis to reevaluate security policy decisions and improve processes

Products and Services

SAAS

Vantage accelerates security response with unmatched threat detection and visibility across your OT, IoT and IT networks. Its scalable SaaS platform enables you to protect any number of assets, anywhere. You can respond faster and more effectively to cyber threats, ensuring operational resilience.

Requires Guardian sensors.

EDGE OR PUBLIC CLOUD

The **Central Management Console** (CMC) consolidates OT and IoT risk monitoring and visibility across your distributed sites, at the edge or in the public cloud. It integrates with your IT security infrastructure for streamlined workflows and faster response to threats and anomalies.

SUBSCRIPTION

The **Threat Intelligence** service delivers ongoing OT and IoT threat and vulnerability intelligence. It helps you stay on top of emerging threats and new vulnerabilities, and reduce your mean-time-to-detect (MTTD).

GUARDIAN ADD-ON

Remote Collectors are low-resource sensors that capture data from your distributed locations and send it to Guardian for analysis. They improve visibility while reducing deployment costs.

EDGE OR PUBLIC CLOUD

Guardian provides industrial strength OT and IoT security and visibility. It combines asset discovery, network visualization, vulnerability assessment, risk monitoring and threat detection in a single application. Guardian shares data with both Vantage and the CMC.

SUBSCRIPTION

The **Asset Intelligence** service delivers regular profile updates for faster and more accurate anomaly detection. It helps you focus efforts and reduce your mean-time-to-respond (MTTR).

GUARDIAN ADD-ON

Smart Polling adds low-volume active polling to Guardian's passive asset discovery, enhancing your asset tracking, vulnerability assessment and security monitoring.

Nozomi Networks

The Leading Solution for OT and IoT Security and Visibility

Nozomi Networks accelerates digital transformation by protecting the world's critical infrastructure, industrial and government organizations from cyber threats. Our solution delivers exceptional network and asset visibility, threat detection, and insights for OT and IoT environments. Customers rely on us to minimize risk and complexity while maximizing operational resilience.

NIST-8.5x11-005

nozominetworks.com