Indegy

Adhering to the NIST Cybersecurity Framework with the Indegy Platform

Indegy's Industrial Cyber Security Platform supports the implementation of the NIST cybersecurity framework

US national security depends on the reliability and continuous operations of the nation's critical infrastructure. The increasing complexity and connectivity of critical infrastructure systems exposes them to cybersecurity threats which put their safety and reliability at risk.

The National Institute of Standards and Technology (NIST) Framework was created through the collaboration of the government and the private sector in response to Executive Order (EO) 13636: Improving Critical Infrastructure Cybersecurity, which called for the development of a risk-based Cybersecurity Framework. It provides a set of industry standards and best practices to help organizations manage and reduce cybersecurity risk to critical infrastructures.

According to a recent survey conducted by SANS on securing industrial networks, NIST is the most popular standard - 48% of respondents claim they map their cybersecurity standards to the NIST Cybersecurity Framework (CSF).

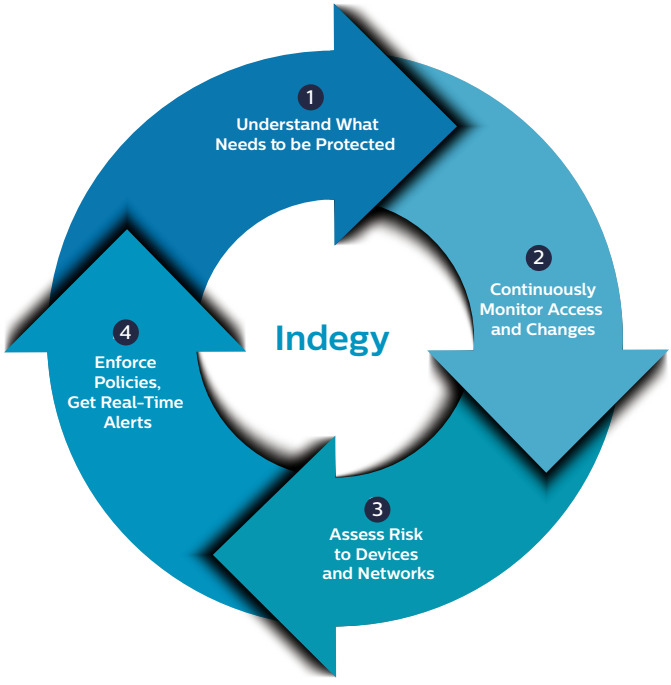
Indegy's Industrial Cyber Security Platform aligns with the CSF primary directive of identifying, managing and reducing the cyber risk of critical infrastructures and the Industrial Control Systems (ICS) on which they rely, by providing comprehensive visibility into critical control assets and activities associated with them.

Managing and Reducing Risk to Critical Infrastructure with the Indegy Platform

To address threats to ICS, whether external cyber attacks, malicious insiders or human error, there needs to be a way to track all devices and activities and alert on anomalies and unauthorized activities.

At the heart of ICS networks, the industrial controllers (e.g. PLCs, RTUs, DCS controllers) are ultimately the most critical devices, and are in charge of process automation, safety and control. Any unauthorized access or changes to these devices, whether malicious or unintentional, can put industrial and critical infrastructure at risk, and lead to severe disruptions.

The Indegy Platform provides comprehensive real-time visibility into ICS to identify threats that place the safety, reliability and security of operational infrastructure at risk. By detecting anomalous activities, unauthorized access and changes to controllers, Indegy provides advanced protection against cyber attacks, insider threats and human error, enabling operators to ensure operational safety and continuity.



IDENTIFY (ID)

Category	Subcategory	Indegy Industrial Cyber Security Platform
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 business objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	The Indegy Platform automatically discovers and maps all ICS devices and keeps an up-to-date inventory of these assets. This includes the operator and engineering workstations, the controllers (PLCs,RTUs and DCS controllers), and I/Os. Indegy's patent-pending Agentless Controller Validation (ACV) enables the discovery of devices even if they aren't actively communicating over the network. Indegy collects highly granular information on each device, including the firmware versions and serial numbers of the devices. The asset inventory is continuously updated with any changes made to ICS devices or when devices are added/removed.
	ID.AM-2: Software platforms and applications within the organization are inventoried	The Indegy Platform automatically identifies the configuration settings and the control code on the industrial controllers themselves, facilitating configuration management of these devices. It also classifies ICS specific MS-Windows stations, such as HMIs and engineering stations.
Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	The Indegy Platform supports the implementation of out-of-the-box and custom security policies, providing real-time alerts on every cyber event that takes place within the ICS network. Alerts can be exported to SIEM systems and SOCs, or sent via email, to any internal or external stakeholder.
Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-1: Asset vulnerabilities are identified and documented	The Indegy Platform identifies and alerts on vulnerabilities of ICS devices.

Protect (PR)

Category	Subcategory	Indegy Industrial Cyber Security Platform
Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	PR.AC-1: Identities and credentials are managed for authorized devices and users	Since industrial controllers usually don't support authentication of any sort, Indegy serves as a compensating control by auditing successful and unsuccessful access attempts made by users and applications alerting in real-time on unauthorized access and anomalies.
	PR.AC-2: Physical access to assets is managed and protected	Since most industrial controllers can be easily accessed physically, and such access can't be monitored over the network, Indegy's Agentless Controller Validation technology (ACV) is used to monitor all physical access and assure no unauthorized changes were made to controller configurations, code, firmware and settings.

.Protect (PR) cont

Category	Subcategory	Indegy Industrial Cyber Security Platform
	PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	Since industrial controllers usually don't support authentication of any sort, Indegy serves as a compensating control by auditing successful and unsuccessful access attempts made by users or applications and alerting in real-time on unauthorized access and anomalies.
Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-1: Data-at-rest is protected	Since data-at-rest on industrial controllers isn't protected, Indegy is used as a compensating control to monitor all access and changes to this data and alert in real-time on suspicious and unauthorized access and changes.
	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	All assets within the ICS networks are automatically mapped and inventoried. The user is alerted in real-time on all changes made to the inventory, including devices that are being connected or disconnected from the network. Formal asset removal procedure is facilitated by the system as well.
Information Protection Processes and Procedures (PR.IP): Security policies (that 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: A baseline configuration of information technology/industrial control systems is created and maintained	Indegy's Agentless Controllers Validation technology (ACV) is used to automatically build a baseline of the industrial controllers' firmware, code and hardware configurations. This information is backed up per asset, and is used to perform periodic controller integrity checks. Users can set the identified configuration as the baseline.
	PR.IP-3: Configuration change control processes are in place	Every configuration change made is automatically identified and flagged, regardless of whether it's done over the network or via physical access to the controllers. User defined policies are used to distinguish authorized changes from unauthorized/malicious ones. Users can resolve alerts through the system and set new configuration baselines as needed.
Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	Any remote access to the network, whether authorized or not, is automatically identified, flagged and logged. The system issues alerts when unauthorized/malicious access occurs.
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: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	Indegy produces and stores a very comprehensive system log, facilitating the consumption of this information by SIEM systems.
	PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	Since industrial controllers usually don't support authentication of any sort, Indegy serves as a compensating control by auditing successful and unsuccessful access attempts made by users and applications, providing real-time alerts on suspicious and unauthorized access.

Detect (DE)		
Category	**Subcategory**	**Indegy Industrial Cyber Security Platform**
Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	Indegy maps all the net-flows and allows the user to search, filter and analyze them. A set of policies on network traffic alerts on any anomalies and unauthorized communications in real-time based on parameters such as the source, the destination, the time, and the protocol used.
	DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	Indegy's alerts are exported by default to SIEM systems, where they are utilized for data correlation between multiple sources.
	DE.AE-5: Incident alert thresholds are established	Indegy offers very granular customizable policies allowing users to set custom thresholds and customize incident alerts.
Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-1: The network is monitored to detect potential cybersecurity events	The Indegy Platform continuously monitors all ICS activities, including activities taking place over proprietary control-plane protocols, identifying in real-time anomalies, suspicious and unauthorized activities, to detect and alert on cybersecurity events.
	DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	Since industrial controllers can be easily accessed physically, Indegy's agentless controller validation technology (ACV) is used to monitor physical access and ensure such access wasn't used for unauthorized or malicious changes of controller configurations, code, firmware and settings.
	DE.CM-4: Malicious code is detected	Malicious code is detected in 3 different ways: 1. By monitoring control plane engineering activities which are used for updating control code 2. By periodically verifying the controllers' code and validating its integrity 3. By flagging anomalous net-flows that may be caused by the existence of malicious code
	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	Any access by an external service provider to the network, whether authorized or not, is automatically identified, flagged and logged. The comprehensive audit trail tracks all the service provider's activities and ensures services were delivered as planned. Real-time alerts are sent on any unauthorized/suspicious activity.
	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	Indegy detects and alerts on all ICS access and activities including unauthorized network connections, new devices that are being connected and on any changes made to the software of the industrial controllers.

Detect (DE) cont.

Category	Subcategory	Indegy Industrial Cyber Security Platform
Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	DE.DP-4: Event detection information is communicated to appropriate parties	The user is provided with various methods to consume event information: • Via the Indegy Platform user interface • Sending a syslog message to a SIEM system • Via email Each alert contains detailed information, relevant to that specific event, including the who, what, when, where and how for each event.

Respond (RS)

Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	RS.CO-2: Events are reported consistent with established criteria	Indegy offers very granular, customizable policies to alert on specific events based on predefined criteria. Criteria include source device, user, destination device, protocols used and time of the event.
Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	RS.AN-3: Forensics are performed	Indegy is a key source of forensics information, such as: raw network traffic, audit trail of configuration and code changes. The Platform also provides comprehensive details about the assets inventory.

Recover (RC)

Category	Subcategory	Indegy Industrial Cyber Security Platform
Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	RC.RP-1: Recovery plan is executed during or after an event	Indegy helps simplify and accelerate recovery processes, as it stores historical information about controller configuration and settings, and supports asset backup and recovery.

International Headquarters
1460 Broadway
New York, NY, 10036
Tel: +1 (866) 801 5394

Research and Development Center
126 Yigal Alon St., Building C
Tel Aviv, Israel, 6744332
Tel: +972 (3) 530 1783

For support contact:
Support@indegy.com
+1 (866) 801 5394

www.indegy.com