GUIDE

Indegy
Activate All Your Senses

Adhering to NIST Cyber Security Framework with Indegy Security Suite

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

The NIST Framework was created through collaboration between government and the private sector, in response to the Executive Order (EO) 13636: Improving Critical Infrastructure Cybersecurity, which calls 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 infrastructure. NIST is considered to be the authoritative standard to which organizations both in the US and overseas map their cyber security standard.

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 and control into critical control assets and activities associated with them.

Indegy's Industrial Cyber Security Suite supports the implementation of the updated NIST Cybersecurity Framework (V1.1 released April 2018)

Managing and Reducing Risk to Critical Infrastructure with Indegy's Cyber Security Suite

Indegy protects industrial networks from cyber threats, malicious insiders and human error by providing visibility and control. Our solution offers the most advanced Industrial Cyber Security Suite, leveraging a hybrid of policy-based monitoring and network anomaly detection combined with unique device integrity checks for full visibility into ICS activities and threats.

- Threat Detection & Mitigation that combines behavioral anomalies with policy based rules.
- Asset Tracking that goes as far as dormant devices and as deep as PLC backplane configurations.
- Vulnerability Management that can track and score patch & risk levels of ICS devices.
- Configuration Control that tracks all changes to code, OS & firmware, whether done through the network or locally.
- Enterprise Visibility that ensures all data collected by Indegy integrates to your single pane of glass.

Indegy Industrial Cyber Security Suite Alignment to the NIST Framework Core Functions*

The table below maps the functionality of the Indegy Cyber Security Suite to the five pillars of the CSF and relevant categories:

Identify (ID)

Category	Subcategory	Indegy Cyber Security Suite
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	Indegy Cyber Security Suite automatically discovers and maps all ICS devices and keeps an up-to-date inventory of these assets. This includes the operator and engineering workstations and controllers (PLCs, RTUs and DCS controllers), and I/Os. Indegy's patent-pending Device Integrity technology 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, PLC backplane configurations and serial numbers of the devices. The asset inventory is continuously updated with any changes made to ICS devices, as well as when devices are added/removed.
	ID.AM-2: Software platforms and applications within the organization are inventoried	Indegy Cyber Security Suite 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.
	ID.AM-3: Organizational communication and data flows are mapped	Indegy Cyber Security Suite automatically maps communication links and data flows between all of the assets in the organization's network. Indegy's baseline deviation capabilities will also alert on changes in these data flows.

*The following does not represent the NIST Framework guidelines in its entirety. For the full NIST Framework Guidelines, visit: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Identify (ID) Continued

Category	Subcategory	Indegy Cyber Security Suite
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	Indegy Cyber Security Suite 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.
	ID.GV-4: Governance and risk management processes address cybersecurity risks	Indegy support the governance and risk management processes by providing a Risk Assessment report that provides a unique, full and detailed analysis on the industrial environment, network behavior, asset inventory and risk posture.
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	Indegy's Risk Assessment report includes a vulnerability drill down chapter that dives into vulnerabilities that exist in the environment. Full details are provided for each vulnerability, including description, affected assets, severity and mitigation steps. A clear view of the most common and severe vulnerabilities helps prioritize patching and software updates for purposes of reducing the environment's overall risk.
	ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	Indegy's Risk Assessment report takes into account alerts in the environment, existing known vulnerabilities and specific aspects in the configuration of controllers that may expose them to potentially malicious threats.

Protect (RR)

Category	Subcategory	Indegy
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 alerting in real-time on unauthorized access and anomalies.
	PR.AC-2: Physical access to assets is managed and protected	Since industrial controllers usually can be easily accessed physically, and such access can't be monitored over the network, Indegy's Device Integrity technology is used to monitor all physical access and assure no unauthorized changes were made to controller configurations, code, firmware and settings.
	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 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 and data-in-transit 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-2: Data-in-transit is protected	
	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.
	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	Indegy's Device Integrity technology verifies that industrial PLCs' code, firmware and setting integrity are secured.

Protect (RR) Continued

Category	Subcategory	Indegy
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 Device Integrity technology 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. Indegy's Cyber Security Suite extracts the names and module numbers of all the modules on the controller's backplane. The user can be alerted on changes identified in either of the modules on the backplane.
	PR.IP-3: Configuration change control processes are in place	Every configuration change is automatically identified and flagged, regardless of whether it's done over the network or via physical access to the device. 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.
	PR.IP-12: A vulnerability management plan is developed and implemented	Indegy recognizes and alerts on vulnerabilities to industrial controllers based on known vulnerabilities issued in the CVE list.
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 alerts on unauthorized/malicious access.
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 providing real-time alerts on suspicious and unauthorized access.

Detect (DE)

Category	Subcategory	Indegy
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's Cyber Security Suite enables the user to define a baseline based on existing network traffic and receive alerts in the event of any deviations. The baseline can be updated at any time.
	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 and customizable policies, allowing administrators to set custom thresholds and customize incident alerts. Using Indegy's policies system, administrators can configure alerts based on specific parameters. It is also possible to define the allowed ranges for them. Users are alerted in the event of deviations.
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 Security Suite continuously monitors all ICS activities, including activities taking place over proprietary control-plane protocols. Indegy identifies real-time anomalies, suspicious and unauthorized activities, enabling it to detect and alert on cyber security events.
	DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	Since industrial controllers can be easily accessed physically, Indegy's Device Integrity capability 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. Indegy also monitors abnormal changes of set-points. Using the policies system, the user can configure Indegy to alert on changes made to specific parameters, as well as defining the allowed ranges and deviations for alerts. This can be used to alert on changes resulting from physical access/ manipulation of sensor information.
	DE.CM-4: Malicious code is detected	Malicious code is detected in three different ways: 1. by monitoring engineering activities which are used for updating control code. 2. by periodically verifying controllers' code and validating its integrity. 3. by flagging anomalous net-flows that may be caused by the existence of malicious code.

Detect (DE) Continued

Category	Subcategory	Indegy
	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. A comprehensive audit trail tracks all service provider 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, deviations from the network traffic baseline, and all changes made to the industrial controllers' software.
	DE.CM-8: Vulnerability scans are performed	Indegy's Risk Assessment report provides detailed information on the vulnerabilities that exist in the environment. Full details are provided for each vulnerability, including description, affected assets, severity and mitigation steps. A clear view of the most common and severe vulnerabilities helps prioritize patching and software updates for purposes of reducing the environment's overall risk.
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	Indegy provides users with various methods to receive event information: • via Indegy's Cyber Security Suite userinterface • via 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. Indegy Cyber Security Suite also supports retaining of full packet captures for forensic analysis. This allows the user to download a copy of the traffic in PCAP format to further investigate alerts and network events.

Respond (RS)

Category	Subcategory	Indegy
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. This includes 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: raw network traffic, audit trail of configuration and code changes, as well as comprehensive details about the assets inventory. This information provides unparalleled forensic support. Indegy also retains full packet captures for forensic analysis, allowing users to download a copy of the traffic in PCAP format to further investigate alerts and network events.
	RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	Indegy recognizes and alerts on vulnerabilities to industrial controllers, based on known vulnerabilities listed in the CVE list. Exact matching of vulnerabilities to controllers is performed based on Indegy's detailed knowledge of controller models and firmware versions. Indegy also offers the option of raising an alert whenever a new vulnerability is identified.

Recover (RC)

Category	Subcategory	Indegy
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 configurations and settings. This directly supports asset backup and recovery.

About Indegy

Indegy, is a leader in industrial cyber security, protects industrial control system (ICS) networks from cyber threats, malicious insiders and human error. The Indegy Industrial Cyber Security Suite arms security and operations teams with full visibility, security and control of ICS activity and threats by combining hybrid, policy-based monitoring and network anomaly detection with unique device integrity checks.

For more information visit indegy.com, and follow us on Twitter and LinkedIn.

To schedule a demo contact us today.