WHITE PAPER

Indegy

Industrial Cyber Security

Top Three Use Cases for Automated OT Asset Discovery and Management

Introduction

Most Industrial Control Systems (ICS) networks were designed and implemented decades ago. Cyber security was not a concern at the time most ICS networks were built, which is reflected in the striking absence of basic security controls and the lack of automated asset management capabilities.

Today, however, as critical infrastructure and industrial organizations seek ways to defend their ICS networks against cyber attacks, the lack of automated asset discovery and management capabilities has come to the fore. Without an up-to-date and accurate inventory of ICS assets, including the automation controllers responsible for managing physical processes, it is virtually impossible to assess risk and apply effective defenses. Moreover, automated asset management is important for operational reliability and safety, as it enables OT managers to track changes made to devices, prioritize threat mitigation efforts, restore misconfigured devices to a “known good” state, and plan maintenance schedules.

As ICS networks grow, so does the need for effective asset management. The number and variety of different assets, models and firmware versions within a network, coupled with decades of consolidation and M&A activities, have added substantial complexity to asset management.

Use Cases

1. Understanding and Controlling the Cyber Security Resilience of ICS Assets

A decade ago, cyber security was a non-issue for OT environments, which were isolated from IT networks and considered invulnerable to cyber threats. Today, one of the biggest problems facing critical infrastructure providers is the lack of security controls in ICS environments. Protecting operational networks requires security professionals to understand and control the cyber resilience of ICS assets - a complex challenge yet to be addressed.

Eliminating Ineffective Manual Compilation of Asset Data

Unlike the world of IT networks, ICS environments lack automated asset discovery and management. The vast majority of industrial networks either don't track their assets at all, or use manual processes to track physical assets using bar codes and labels.

Using manual processes for inventory management is both time-consuming and prone to human error. It often results in information that is missing, outdated, or erroneous.

> The inability to automatically track detailed information and changes made to critical devices can leave an organization vulnerable to security threats.

As a result, most organizations don’t know what devices they have in different segments of the plant. Further complicating this scenario is the fact that many organizations include subsidiaries and remote branches, and work with third-party partners, contractors, temporary workers, and guests.

With new assets coming online and changes being made to these networks on a continuous basis, the only way to ensure a complete and accurate asset inventory is to implement an automated and continuous discovery process.

Prioritizing Vulnerable Assets and Scoping Security Projects

To build an effective security strategy, you need to know the manufacturers, models, firmware versions, latest patches, and current configuration for each and every asset in a network. Thus, a comprehensive asset inventory is crucial for both identifying vulnerable assets and implementing required mitigations to protect them.

Automated asset discovery and management helps organizations prioritize assets that require upgrades, maintenance, and other operational initiatives based on the asset's criticality and risk posture.

For example, let's say you've identified 20 PLCs on your production line that have vulnerabilities at different levels of severity. This information allows you to prioritize the deployment of security controls, ensuring that the most critical and vulnerable assets are handled first. Thus, prioritization becomes a safety and stability feature that enables organizations to minimize potential disruptions to production operations.

> Automated asset discovery is essential for meeting the security needs of ICS networks. After all, if you don't have visibility into the assets you have, how can you assess risk and apply the right defenses?

2. Improving Operational Incident Response, Shortening Resolution Time, and Ensuring Operational Continuity

Recover Faster from Cyber Incidents and Unauthorized Changes

In the event of a cyber-attack or a human error, the time it takes to restore a misconfigured device to a "known good" state is crucial for maintaining operational continuity. Fast recovery requires accurate and up-to-date information about the device in question, including a complete history of changes, in order to understand what happened, when and who was responsible.

> Detailed historical information about critical devices is critical for rapid incident resolution.

Automated asset inventory can provide much needed historical information required for device recovery, enabling organizations to recover faster from cyber-attacks and unauthorized device changes, and subsequently minimizing their impact on operations.

Avoid Operational Problems Due to Inaccurate Asset Data

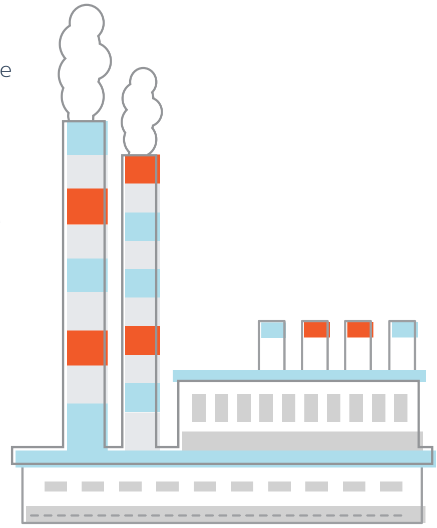
Inaccurate asset data maintained in a spreadsheet can easily snowball into a situation where one wrong piece of data can result in the disruption - and even shutdown - of operations.

Consider this real-world example from the manufacturing industry: a system integrator who arrived on site to perform a code change on PLCs that control an automated assembly line.

Due to the fact that the asset spreadsheet wasn't updated with recent changes made to the device IPs, the integrator modified the code on the wrong PLC.

This seemingly "simple" mistake triggered a chain of operational issues. In the time that it took to realize that the code on the designated PLC was not changed, defective units continued to be manufactured.

As a result, the entire assembly line had to be shut down for 24 hours. During this time the manufacturer's engineering staff had to determine which PLC's code was in fact changed, revert it back to its proper configuration, and upgrade the code of the correct PLC. Only after all of these steps were completed could the operations resume.



This entire chain of events could have been avoided by using an automated asset discovery and management solution. Such a solution would have kept a detailed asset inventory and tracked all changes, and raised real-time alerts each time an OT asset was changed.

At the same time, a comprehensive audit trail would have enabled the engineering staff to track the full chain of events that led to this incident. Lastly, by maintaining historical information about the PLC's configuration and code, the manufacturer could have quickly restored the PLC to a previously known good state rather than shutting down operations for 24 hours.

> Inaccurate asset data can trigger a chain of events that may result in severe operational disruptions.

Free Up Experts' Time to Let Them Focus on Work that Matters

Without an automated asset management solution, organizations are dependent on the availability of a limited number of personnel with the professional knowledge needed to restore a device to its proper state using the correct installation procedure, code and firmware. In many organizations, these experts are often overloaded with various tasks.

Given the shortage of skilled engineering resources across the industry, automated asset discovery and management is crucial for ensuring that historical information about devices remains available even for newer personnel joining the workforce. With an automated solution, senior professionals can devote their time and knowledge to more important tasks.

> Automated asset inventory management gives you the information needed to conduct predictive asset maintenance. It lets you plan which assets will need spare parts and when, and to prepare and maintain a spare parts inventory to ensure operational continuity.

Plan and Maintain a Spare Parts Inventory for Faster Repair Time

In critical infrastructure, manufacturing, and process industries, nothing is more important than operational reliability and continuity. Equipment uptime is critical for keeping production operations online, as a single failure can often impact the entire production process. The cost of shutting down a manufacturing production line, for example, can reach millions of dollars per day.

Thus, when a problem that jeopardizes continuity is encountered, it must be resolved quickly. Maintaining an up-to-date spare parts inventory is critical for ensuring fast repair times and preventing downtime. If your organization doesn't have an accurate inventory of assets, you won't know which spare parts to order and store on-site. If a piece of equipment breaks down, it might take a few days to receive the right part. In the meantime, your organization is losing money and orders may be backing up.

3. Complying with Industry Regulations Stipulating Identification and Inventory of Critical Assets

Given the growing number of cyber attacks against critical infrastructure, such as the attack against Ukraine's power grid and the Dragonfly campaigns targeting the energy sector and multiple government entities, new standards and regulations have been established to govern the cyber security measures that critical infrastructure must implement to minimize risk and ensure public safety.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), for example, provides a set of industry standards and best practices to help organizations manage and reduce cyber security risk to critical infrastructures and the ICS which they rely on.

NIST

To learn about Adhering to the NIST Cybersecurity Framework with the Indegy Platform

CLICK HERE >

NERC

To read Indegy's Compliance Guide for NERC CIP Standards

CLICK HERE >

In order to provide comprehensive visibility into critical control assets and activities associated with them, NIST requires that organizations implement an asset management function for the purpose of identifying, inventorying, and managing all physical devices and systems.

The NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection) plan is a set of requirements designed to secure the assets required for operating North America's bulk electric system. Similar to NIST, one of the most important elements spanning all NERC CIP regulations is the identification of Critical Assets (CA) and Critical Cyber Assets (CCA).

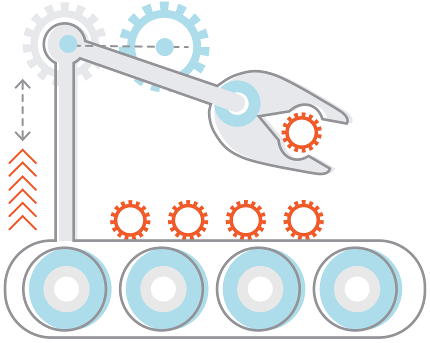
Compliance with NIST, NERC, and similar frameworks worldwide requires effective automated asset discovery and ongoing management of an asset inventory.

About Indegy’s Asset Management Solution

Indegy offers a comprehensive Industrial Cyber Security Platform that enables engineers and security personnel to secure and control ICS networks. Within this platform, the Asset Management component is responsible for asset discovery, classification, and management. It automatically maps all of the controllers on the network, documents their configuration, logs all activities and changes, and provides in-depth visibility into to their state.

By enabling organizations to understand what assets they have and what needs to be protected, Asset Management is the critical first step for ensuring operational continuity, reliability and safety. Real-time situational awareness lets you apply effective security and change management policies to prevent unauthorized activities. Asset Management also plays a key role in planning maintenance projects, prioritizing upgrades, patch deployments, incident response and mitigation efforts.

Using a patent-pending combination of both passive and active inspection technologies, Asset Management is uniquely able to discover all assets, gather details and monitor changes in the ICS environment. Indegy's breakthrough capabilities are based on the concurrent use of two core technologies:



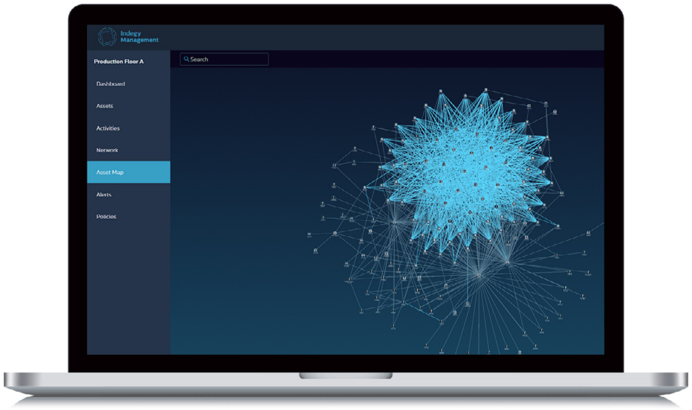
Control Plane Inspection (CPI)

This deep packet inspection engine was built specifically for the unique control-plane protocols used in ICS networks. It gathers asset details from network communications and provides organizations with full visibility into all OT activity. CPI allows Indegy to understand protocols, analyze network activity, report and raise alerts.

Agentless Controller Validation (ACV)

This patent-pending asset discovery technology enables Indegy to safely query devices using native commands and protocols, gather more in-depth details about an asset, and even find assets that are currently inactive. Safe use of native protocols means zero impact on controller operations and performance. ACV periodically validates controller integrity and components to ensure that the information displayed on a particular asset is always accurate.

Automated Asset Discovery and Management



Indegy's Interactive Asset Map

Indegy's automated asset discovery provides engineers and security managers with a complete picture of all the assets in an ICS network. As soon as the Indegy Platform is connected to the ICS network, it automatically discovers all of the devices in the network, including PLCs, RTUs, HMIs, engineering workstations, OPC servers, Historian and more.

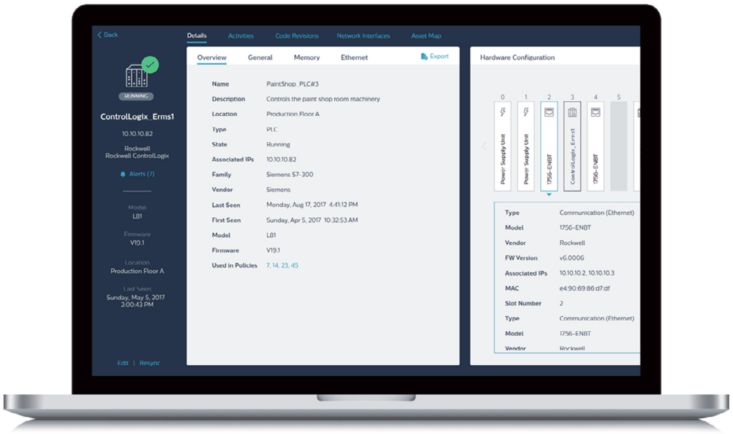
Indegy identifies new assets added to or disconnected from the network, and creates an asset map depicting the connections, protocols, and traffic patterns between assets.

To learn more about Indegy's Interactive Asset Map CLICK HERE >

Detailed Asset Classification

Indegy gathers asset information from the ICS network in a safe and comprehensive manner. Using native protocols for querying assets, Indegy collects the following set of highly detailed information about each asset on the network:

- Name and Location
- IP Address and MAC Address
- First and Last Time Seen
- Device Classification (PLC, RTU, HMI, Digital I/O, Analog I/O, Communications Card etc.)
- Device Maker and Model
- Part Number
- Firmware Version
- Serial Number
- State
- Memory Consumption
- Controller Scan Time
- Backplane/Chassis Configuration
- Open Network Ports



ControlLogix_Erms1

10.10.10.82

Rockwell
Rockwell ControlLogix

Alerts (7)

Model
L81

Firmware
V19.1

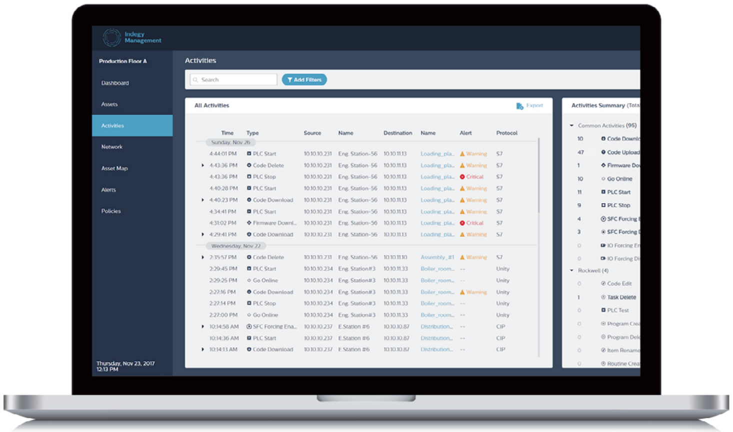
Location
Production Floor A

Last Seen
Sunday, May 5, 2017
2:00:43 PM

Name	PaintShop_PLC#3
Description	Controls the paint shop room machinery
Location	Production Floor A
Type	PLC
State	Running
Associated IPs	10.10.10.82
Family	Siemens S7-300
Vendor	Siemens
Last Seen	Monday, Aug 17, 2017 4:41:12 PM
First Seen	Sunday, Apr 5, 2017 10:32:53 AM
Model	L81
Firmware	V19.1
Used in Policies	7, 14, 23, 45

Type	Communication (Ethernet)
Model	1756-ENBT
Vendor	Rockwell
FW Version	v6.0006
Associated IPs	10.10.10.2, 10.10.10.3
MAC	e4:90:69:86:d7:df
Slot Number	2
Type	Communication (Ethernet)
Model	1756-ENBT
Vendor	Rockwell

Indegy asset classification and details



Thursday, Nov 23, 2017
12:13 PM

Activities

All Activities

Time	Type	Source	Name	Destination	Name	Alert	Protocol
Sunday, Nov 26							
4:44:01 PM	PLC Start	10.10.10.231	Eng. Station-56	10.10.11.13	Loading_pla...	Warning	S7
4:43:36 PM	Code Delete	10.10.10.231	Eng. Station-56	10.10.11.13	Loading_pla...	Warning	S7
4:43:36 PM	PLC Stop	10.10.10.231	Eng. Station-56	10.10.11.13	Loading_pla...	Critical	S7
4:40:28 PM	PLC Start	10.10.10.231	Eng. Station-56	10.10.11.13	Loading_pla...	Warning	S7
4:40:23 PM	Code Download	10.10.10.231	Eng. Station-56	10.10.11.13	Loading_pla...	Warning	S7
4:34:41 PM	PLC Start	10.10.10.231	Eng. Station-56	10.10.11.13	Loading_pla...	Warning	S7
4:31:02 PM	Firmware Downl...	10.10.10.231	Eng. Station-56	10.10.11.13	Loading_pla...	Critical	S7
4:29:41 PM	Code Download	10.10.10.231	Eng. Station-56	10.10.11.13	Loading_pla...	Warning	S7
Wednesday, Nov 22							
2:35:57 PM	Code Delete	10.10.10.231	Eng. Station-56	10.10.11.10	Assembly_#1	Warning	S7
2:29:45 PM	PLC Start	10.10.10.234	Eng. Station#3	10.10.11.33	Boiler_room...	--	Unity
2:29:25 PM	Go Online	10.10.10.234	Eng. Station#3	10.10.11.33	Boiler_room...	--	Unity
2:27:16 PM	Code Download	10.10.10.234	Eng. Station#3	10.10.11.33	Boiler_room...	Warning	Unity
2:27:14 PM	PLC Stop	10.10.10.234	Eng. Station#3	10.10.11.33	Boiler_room...	--	Unity
2:27:00 PM	Go Online	10.10.10.234	Eng. Station#3	10.10.11.33	Boiler_room...	--	Unity
10:14:58 AM	SFC Forcing Ena...	10.10.10.237	E.Station #6	10.10.10.87	Distribution...	--	CIP
10:14:36 AM	PLC Start	10.10.10.237	E.Station #6	10.10.10.87	Distribution...	--	CIP
10:14:13 AM	Code Download	10.10.10.237	E.Station #6	10.10.10.87	Distribution...	--	CIP

Activities Summary (Tota

Common Activities (95)

10	Code Downlo
47	Code Upload
1	Firmware Do
10	Go Online
11	PLC Start
9	PLC Stop
4	SFC Forcing E
3	SFC Forcing D
0	IO Forcing En
0	IO Forcing Di

Rockwell (4)

0	Code Edit
1	Task Delete
0	PLC Test
0	Program Crea
0	Program Dele
0	Item Renam
0	Routine Crea

Configuration control for critical automation controllers

Configuration Control for Automation Controllers

The Indegy Platform tracks and logs all configuration changes, whether executed by a human, malware, over the network, or physically on the device.

It provides a full history of changes made to device configuration over time, enabling users to quickly identify a previous "good configuration" and revert back to it.

Monitoring and Managing Changes to Critical Assets

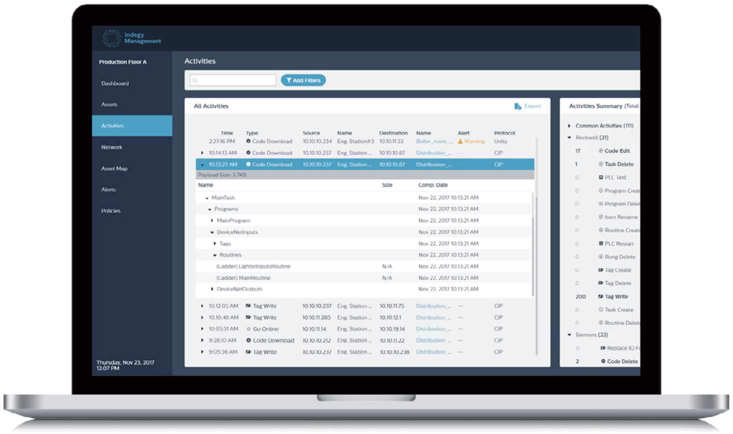
The Indegy Platform monitors all ICS activity, including HMI/SCADA activity, and engineering-level access to control devices. It provides full visibility into the critical control-plane activity, uniquely identifying changes made to firmware, logic, code and hardware configurations. Indegy tracks all changes made to controllers, whether performed over the network or directly on the device (via serial cable).

Real-time alerts enable engineering and security teams to track all engineering activities performed on controllers within the ICS network, shortening investigation and resolution times. Alerts are available via dashboard or email, and can also be exported to the enterprise SIEM.

Engineers can define and customize the policies for raising alerts in accordance with organizational procedures. These granular policies are based on real-time activities (not based on statistical calculations), which results in zero false positives and enables effective incident management.

All access and configuration changes made to devices are documented in a comprehensive audit log for compliance with industry regulations. This audit trail helps engineering staff ensure that maintenance was performed on schedule, while enabling security teams to identify unauthorized changes and determine root causes.

In addition, an asset configuration management database stores detailed information about control devices, including complete control logic, to facilitate backup and recovery in the event of a cyber-attack or human error.



Thursday, Nov 23, 2017
12:07 PM

Activities

All Activities

Time	Type	Source	Name	Destination	Name	Alert	Protocol
2:27:16 PM	Code Download	10.10.10.234	Eng. Station#3	10.10.11.33	Boiler_room_...	Warning	Unity
10:14:13 AM	Code Download	10.10.10.237	Eng. Station ...	10.10.10.87	Distribution_...	--	CIP
10:13:27 AM	Code Download	10.10.10.237	Eng. Station ...	10.10.10.87	Distribution_...	--	CIP

Payload Size: 3.7KB

Name	Size	Comp. Date
MainTask		Nov 22, 2017 10:13:21 AM
Programs		Nov 22, 2017 10:13:21 AM
MainProgram		Nov 22, 2017 10:13:21 AM
DeviceNetInputs		Nov 22, 2017 10:13:21 AM
Tags		Nov 22, 2017 10:13:21 AM
Routines		Nov 22, 2017 10:13:21 AM
(Ladder) LighterInputsRoutine	N/A	Nov 22, 2017 10:13:21 AM
(Ladder) MainRoutine	N/A	Nov 22, 2017 10:13:21 AM
DeviceNetOutputs		Nov 22, 2017 10:13:21 AM

Time	Type	Source	Name	Destination	Name	Alert	Protocol
10:12:05 AM	Tag Write	10.10.10.237	Eng. Station ...	10.10.11.75	Distribution_...	--	CIP
10:10:48 AM	Tag Write	10.10.11.285	Eng. Station ...	10.10.12.1	Distribution_...	--	CIP
10:05:51 AM	Go Online	10.10.11.14	Eng. Station ...	10.10.19.14	Distribution_...	--	CIP
9:28:10 AM	Code Download	10.10.10.212	Eng. Station ...	10.10.11.22	Distribution_...	--	CIP
9:05:36 AM	Tag Write	10.10.10.237	Eng. Station ...	10.10.10.238	Distribution_...	--	CIP

Activities Summary (Total

Common Activities (111)

Rockwell (21)

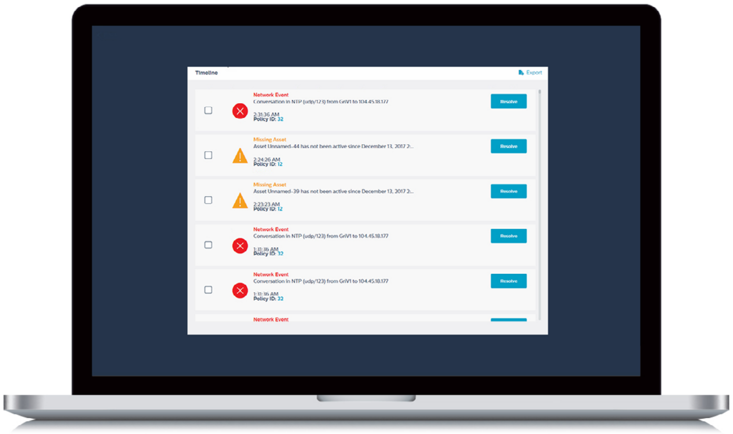
17	Code Edit
1	Task Delete
0	PLC Test
0	Program Creat
0	Program Delet
0	Item Rename
0	Routine Create
0	PLC Restart
0	Rung Delete
0	Tag Create
0	Tag Delete
200	Tag Write
0	Task Create
0	Routine Delete

Siemens (22)

0	Replace IO Fo
2	Code Delete

Tracking changes to critical control assets

Real Time Notifications on Changes to Critical Assets



Network Event
Conversation in NTP (udp/123) from GriV1 to 104.45.18.177
2:31:36 AM
Policy ID: 32

Missing Asset
Asset Unnamed-44 has not been active since December 13, 2017 2:...
2:24:26 AM
Policy ID: 12

Missing Asset
Asset Unnamed-39 has not been active since December 13, 2017 2:...
2:23:23 AM
Policy ID: 12

Network Event
Conversation in NTP (udp/123) from GriV1 to 104.45.18.177
1:31:36 AM
Policy ID: 32

Network Event
Conversation in NTP (udp/123) from GriV1 to 104.45.18.177
1:31:36 AM
Policy ID: 32

Network Event

Indegy alerts on missing assets that have been inactive for a while

The Indegy Platform automatically alerts on changes to assets that require attention. This includes new assets appearing in the network, missing assets that have been inactive for a while, as well as changes to asset configuration, firmware, and code.

The platform provides granular security and change management policies. Out-of-the-box policies are included to alert on various events, such as new assets discovered in the network. Custom policies can easily be generated to alert on specific events. For example, organizations can define a policy to alert on unauthorized users accessing a specific group of assets.

About Indegy

Indegy, the leader in industrial cyber security, protects Industrial Control Systems (ICS) used in critical infrastructure, utilities and manufacturing industries against operational disruptions caused by external and internal threats.

By providing comprehensive visibility into the control-plane engineering activities performed in operational technology networks, Indegy's Industrial Cyber Security Platform automatically discovers all controllers (PLCs, RTUs, DCSs) on ICS networks, monitors all access and changes in real-time, and validates their integrity ensuring no unauthorized changes go undetected.

Indegy enables advanced detection and response to threats that place the safety, reliability and security of industrial networks at risk before damage occurs.

The company has been named a Gartner "Cool Vendor" for Industrie 4.0, one of the 10 Most Promising Cyber Security Startups by Forbes Israel, is a TiE50 winner, Network World Hot Security Startup to Watch and Product Leader in Industrial Cyber Security by Frost & Sullivan.

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

For more information about the Indegy Platform visit www.Indegy.com

To schedule a demo contact us today.