WHITE PAPER

Indegy
Activate All Your Senses

Critical Infrastructure Cyber Security:

How to Actively Secure Your Industrial Environment In the New Era of Distrust

The Power of Hybrid Detection

By combining both passive network analysis and active monitoring, benefits include:

- Identify changes made to devices locally or over the network
- Trigger device integrity checks after suspicious network activity
- Provide added context for alerts
- Discover and track assets even if they are not communicating on the network
- Understand real network topology in instances of multiple network cards on devices
- Get complete and up-to-date backplane configuration for PLCs & server settings
- Compare firmware versions and hotfix lists to known CVEs
- Acquire list of open ports from devices that impact risk score
- Up-to-date risk data not based on 'last seen traffic'

The Industrial Cyber Security Challenge

Today's sophisticated Operations Technology (OT) environments have a large attack surface with numerous attack vectors. Without complete coverage, the likelihood of getting attacked is not a matter of 'if'; it's a matter of 'when'. Security for OT has gained significant attention due to a confluence of events.

Up until only recently the IT infrastructure played front and center in terms of ensuring complete visibility, security and control mostly because this was ground zero for where organizations were being attacked. For the better part of two decades this is what kept the CISO up at night; but the reality has changed. With our increasingly interconnected world through the adoption if IIoT, OT has quickly caught up as a lightning rod for new attacks and increased security concerns.

Because OT systems were traditionally segregated and isolated, controllers were not architected to address the security threats or the human errors we now experience. Outsiders, insiders, and outsiders masquerading as insiders are all possible actors that launch sophisticated attacks to take over machines for nefarious purposes. More recently hackers have changed from being rogue individuals to systematic programs launched by well-funded and highly motivated organizations and countries. A carefully executed attack can accomplish as much if not more than modern day warfare.

In addressing this relatively new security threat that is specifically targeting industrial operations, network monitoring is not enough. It is essential to gain visibility to the entire industrial control system (ICS) environment. This can only be accomplished by taking a forward leaning security posture. This paper will help you identify the key elements needed to progress beyond simple passive monitoring in order to secure your industrial organization from the clear and present threat.

Where Do ICS Threats Exist?

In ICS environments, questionable behaviors and activities can exist on the network as well as on devices. In fact, many operations may be conducted on a device and will never traverse the network. Critical asset inventory information like records of user log-ins and controller firmware versions, as well as changes to devices made via direct connections, don't typically present themselves in network traffic. If network monitoring misses an attack on a device, it can remain infected for days, weeks, or months without detection. In fact, network monitoring only provides operators with 50% visibility and coverage across the OT environment. As a result, an ICS security solution must address the threats that exist on the network as well as on devices that attack the network in order to achieve complete visibility, security and control.

Security Beyond The Network

Going beyond simple network monitoring to include Device Integrity security provides more complete solution for OT environments. Active security surveys devices in the ICS network to validate their status down to an extremely granular level. This capability enhances the ability to automatically discover and classify all the ICS assets from windows machines down to and including lower-level devices like PLCs and RTUs, even when they aren't active in the network. It also identifies local changes in the device's meta-data (e.g. firmware version, configuration details and state) as well as changes in each code/function block of the device's logic. It is essential however that the technology uses read only queries in the native controller communication protocols in order for it to be completely safe and having no impact on the devices being queried.

Device Integrity technology complements network monitoring by collecting information that is impossible to find in the network yet is crucial for all the benefits described earlier. It is also essential in order to provide additional context for security alerts. Finally, querying can save maintenance cost while allowing for more flexible deployments, since it eliminates the need to monitor every switch in the organization. If the environment is route-able, it is possible to get information on all the devices even with a single appliance.

Key Ingredients To Secure Your ICS Environment

Not all OT security vendors are created equal. Some do not provide any form of Device Integrity functionality because they believe it is “too dangerous”. Of course, anything done incorrectly can be dangerous, but executing Device Integrity properly is not only safe, but it leverages the technology that the PLC or DCS was built for.   Other vendors provide a method of device checks, but it can make the system unstable. In other cases, the checks do not provide the benefits you should be getting; thus, still leaving you vulnerable to risk.

In evaluating ICS security solutions there are some basic requirements that it should address not only at the network but down to the device level including visibility into what is happening, security against attacks, and control over the OT environment. We will briefly examine some of the requirements in each of these areas.

Visibility

In-Depth Enterprise Visibility

At the most basic level, information flows across the OT network, but this data is created by devices on the network. Thus, Asset Management is a key element for being in control of your ICS environment. Most importantly, asset data does not normally traverse the network. Details like the logged in user or latest hotfixes installed on PCs and Servers, or the firmware version and open port list of a PLC/DCS controller, are stored within the devices themselves and typically have no reason to be transmitted. Device Integrity solves that problem by querying the devices and automatically gathering the most comprehensive and critical information about every asset in the environment.

Capture of “Blind Spots”

Device Integrity discovers dormant industrial devices that are connected to the network but are not communicating. Most industrial control vendors support a “find me” mechanism built into their controllers that allows detecting them with a single broadcast of a unique packet. This is how engineering stations can find all controllers in the network automatically. Device Integrity uses that same built-in mechanism to make sure your asset inventory is complete and accurate.

Security

Safeguard from Malicious Insiders and Human Error

It is very common for employees, contractors and integrators to connect to control devices using a serial cable or USB. A malicious actor that has physical access to the network can also connect to controllers this way. Changes made to the controller code, firmware or configuration - whether authorized or not - cannot be detected by network monitoring. It is also plausible that an employee or contractor unknowingly exposed controllers to threats by using a compromised device, for example a laptop or USB drive infected with malware. By periodically capturing device snapshots and comparing them to previous baselines, you will be able to identify changes and validate that the integrity of the device is not compromised.

Insight into Vulnerability and Risk

By regularly querying the servers and controllers for details such as the OS & firmware version, open ports, latest software, hotfixes, hardware configuration, patch level and more, Device Integrity will proactively have complete awareness of the most current vulnerabilities that may put the industrial controllers at risk. This provides more accurate risk scoring which is augmented based on nonnetworked data. Rather than waiting for device information to be passed over the network, Device Integrity will have with the most updated and accurate information on the device, arresting attack propagation before it hits the network.

Control

Greater Efficiency for Incident Response

Alerts can be meaningless without added contextual information such as “who is the logged in user to the engineering station at a specific time” and “what was the impact of specific activity to the PLC ladder logic”. When detecting a suspicious network event, Device Integrity uses native protocols and automatically queries the relevant devices to gather further contextual details. This provides more meaningful alerts compared to a network-only solution and results in significantly improved situational awareness and quicker forensic and mitigation activity.

Lower Total Cost of Ownership (TCO)

A major disadvantage of network-only technologies is the necessity to deploy them at every intersection and switch of the network you want to monitor. This can turn out to be very expensive for a large environment with multiple subnets. The typical response to save hardware and maintenance cost is to deploy fewer appliances in the network. Too often, this results in a sacrifice of control and/or visibility when using a network-only approach. Device Integrity technology, however, provides the ability to monitor all routable sections of the network with one single appliance.

Operations Network Resiliency

Unless there is backup that traces the changes made to control devices, incident recovery can be very difficult. With Device Integrity, we enable you to simplify architecture and reduce costs at the same time. By capturing a complete snapshot of the device including firmware, configuration, complete ladder logic, diagnostic buffer and tag structure, you’ll be able to keep track of all versioning history of the controller and can help identify a previously known “good” state.

Safe, Smart Active Detection

In order to fulfill the requirements noted above, Indegy offers patent-pending technology as part of its Industrial Cyber Security Suite. It performs network based detection while also employing Device Integrity checks by using read-only queries in the native device communication protocols, so there is no impact on the devices being enquired. With Indegy, you can be assured that:

Devices are queried only in native language, when positively identified

Indegy’s Device Integrity never uses communication protocols that the device might not support or that are not native. It also never “blindly scans” the network looking for devices. Only after positively identifying a specific asset down to the vendor model and version, Device Integrity will activate and start querying that asset to gather information.

Industrial Controllers are accessed only as they are designed

Most of the industrial controllers use different electronic modules for different purposes. Consequently, ethernet based communication, with engineering station software are executed by the networking module and aren't part of the critical control loop. Additionally, mission critical I/O activity has its reserved processing resources, which prevents a network traffic overload. If the controllers aren't being exploited or maliciously scanned, an overload will not occur.

Schedules and policy settings are customizable to your business needs

Choose your query frequency: every 8 hours, only at specific times of day, for specific subnets, or only by manual activation. With Indegy, it is possible to customize policies to query only predefined set of IP ranges or asset types. It is also possible to check the network load and CPU load on the devices before surveying them.

Activity is Read-Only, Out of band

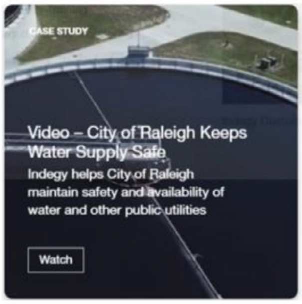
Indegy Device Integrity utilizes 100% read-only communication and by design, does not have the ability to change configurations and settings of any of the devices in the network

Our Approach is tailored to each vendor

Indegy works closely with controller vendors and performs extensive lab tests with physical devices to ensure that queries have no impact on the controllers and do not have the potential to cause any disruptions.

Practical Examples

Theory is always a little different than practice. What is easy to put in a white paper, may not be quite as simple in actuality. Below, you'll find three real customer case studies that are leveraging Indegy technology for their critical infrastructure.



Conclusion

When it comes to addressing the next generation of cyber attacks targeting the OT environment, network only monitoring will not be sufficient. By employing a solution that addresses both network based attacks as well as device active checking, you'll be able to see your entire industrial OT system, rather than just a portion. There are many vendors that are new to the OT field and may not offer device integrity checks because they believe it is “dangerous”. When performed in the right way, device checking is not only safe, but it is actually the only way to ensure complete visibility, security and control for your OT network both for today and also to scale into the future.

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 Suite 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.

For more information visit www.indegy.com, and follow us on Twitter and LinkedIn.
To schedule a demo contact us today.