WHITEPAPER

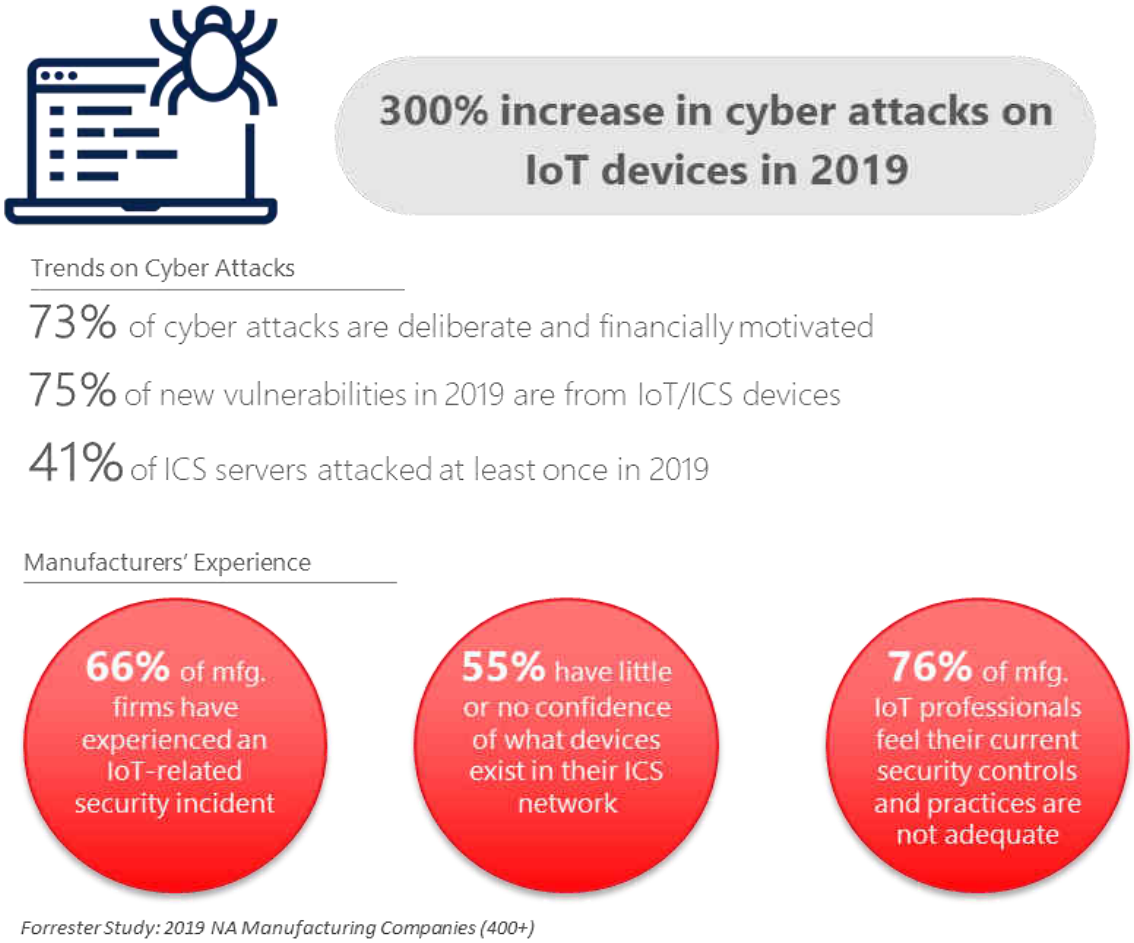
A Ground up approach to securing the plant floor

Introduction

Back in 2004, the Department of Homeland security officially named October, National Cyber Security awareness month after several attacks like *Code Red* and the *I Love You* worm took the attention of the public. Those were the good old days of basement hacks with the intent of notoriety in, what was then, a small and very tight knit community.

Cyber threats have always kept pace with technology changes, and today present the most clear and present danger with the potential to paralyze life and business as usual. In September 2020, the first known death from a cyberattack was reported after cybercriminals hit a hospital in Düsseldorf, Germany with ransomware. The notion that there is money to be made from cyberattacks has skyrocketed the number of incidents and hackers have a new favorite target, industrial control systems.

Since 2019, the US has seen a 300% increase in cyber-attacks on IoT devices. 73% of those are carried out deliberately and are financially motivated. 75% of all the new vulnerabilities discovered in 2019 are from IoT or ICS devices.



The financial impact can be astronomical. Let's look at an all too common ransomware attack scenario on the plant floor.

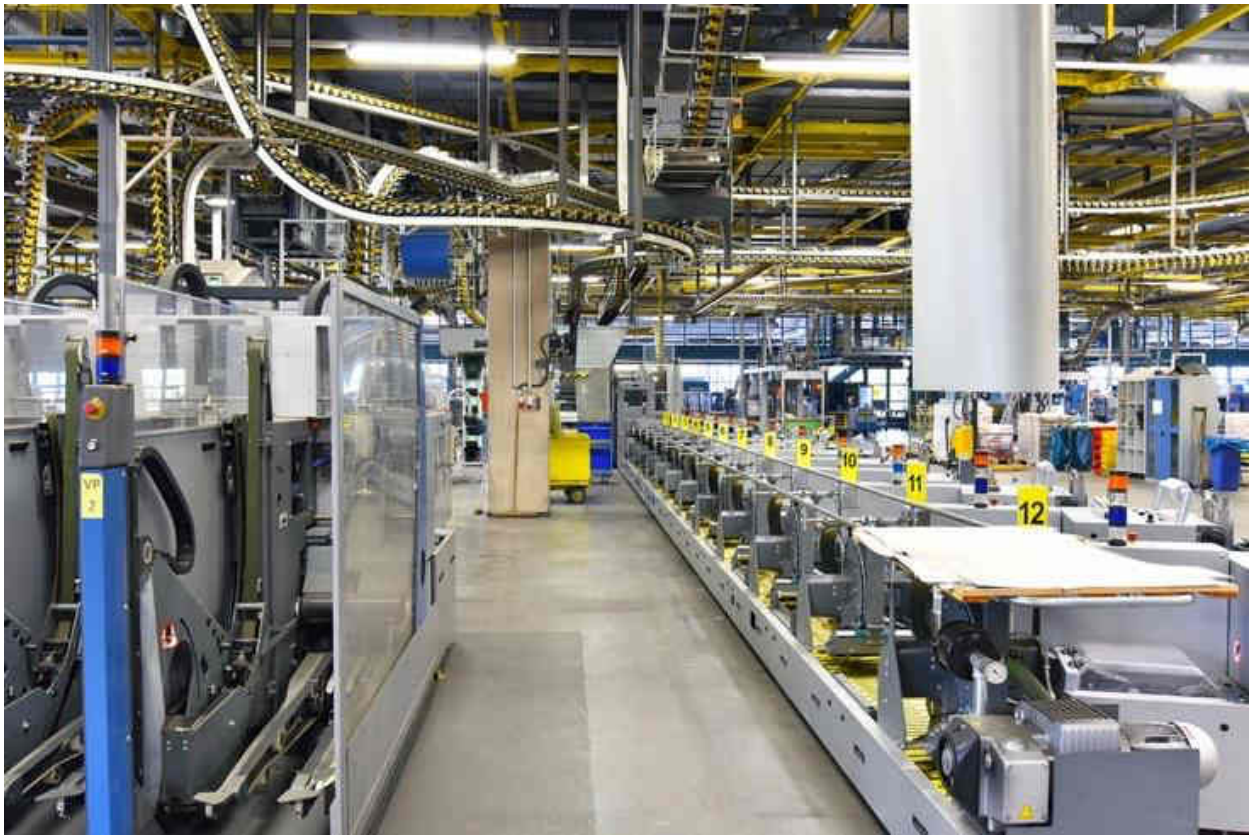
> *An engineer Googling for technical information from a connected engineering workstation on the plant floor accidentally downloads ransomware. The malware exploits known vulnerabilities that have not yet been patched on the industrial network, encrypts the engineering workstation, and spreads to the SCADA servers in the plant. The SCADA servers in the industrial network are encrypted, shutting down the control system. The impaired control system is unable to follow a normal shutdown procedure. Noticing this, the plant operator triggers an ESTOP. The emergency shutdown procedure damages important equipment at the plant, impairing production for months.*

The good news is that the methods to prevent these types of attacks in your plant isn't as prohibitive or complex as one may think. In this whitepaper, we'll discuss some best practices and different ways to secure your ICS architecture. These follow the same principles as the NIST (National Institute of Standards and Technology) Cybersecurity Framework.

Common Challenges to Industrial Networks

Visibility

The most critical issue in an ICS is the simple concept of knowing what or who is connected to you ICS. Tools or control systems might have been installed by an integrator or come along with a factory acquisition. Unless you are lucky enough to have a single plant, you have assets dispersed through the field or remote locations. Unconnected network segments are common.



Think in terms of not only the remote production site you oversee, but the automation contractor assigned to upgrade a line. It's a common practice for engineers to have some means of remote diagnostics and troubleshooting. TeamViewer or VNC have become common tools for remote access and uses connection methods not usually blocked by traditional means.

- If you don't know exactly what assets are on the plant floor, how do you know they are not reachable from the internet?
- How do you know that your plant devices don't have any vulnerability that could potentially be used by hackers to access your operations?

Age

It's not uncommon for plant assets and equipment to be 20-30 years old. Industrial plant machines and controls are designed for reliability and longevity. Since these devices are part of the business-critical processes, there is little or no downtime. IT maintenance procedures like "patch Tuesdays" can't happen in OT.

Also, ICS systems have never been designed to fend off cybersecurity attacks. Vendors today are trying to secure select firmware but older system that have reached a vendor's end of life are not updated and left vulnerable.

IT and OT Convergence

The NIST states that industrial control systems

"have many characteristics that differ from traditional IT systems, including different risks and priorities. Some of these include significant risk to the health and safety of human lives, serious damage to the

environment, and financial issues such as production losses, and negative impact to a nation's economy. ICS have different performance and reliability requirements and use operating systems and applications that may be considered unconventional in a typical IT network environment. Security protections must be implemented in a way that maintains system integrity during normal operations as well as during times of cyber attack."

ICS protocols are mostly closed and proprietary. It's not feasible for some common IT conformance checks to be used here. A better way to look at this, is that you can't apply IT rules, or tools for that matter, to OT. This is exactly what drives the apprehension of IT security managers stepping on the plant floor. To compound this problem, OT and production managers fear the seemingly endless details of IT centric security policies and procedures. Both teams are apprehensive about each other and have historically, not worked together.

This is the key to securing your industrial operations.

IT SOC has the responsibility of securing the entire enterprise. OT managers have the responsibility of reliability, safety, and uptime. To effectively secure a plant floor, IT needs a holistic view of all connected devices. However, the goals of these entities do overlap. Both are committed to securing the organization, minimizing risk, maximizing uptime, and ensuring that the organization can continue to safely generate revenue. To ensure that security measures are implemented successfully, IT and OT teams must work in harmony through each phase of the cybersecurity process. Collaboration early in the process is a key factor in success.

Phase One

ELIMINATE DOUBT WITH ASSET VISIBILITY

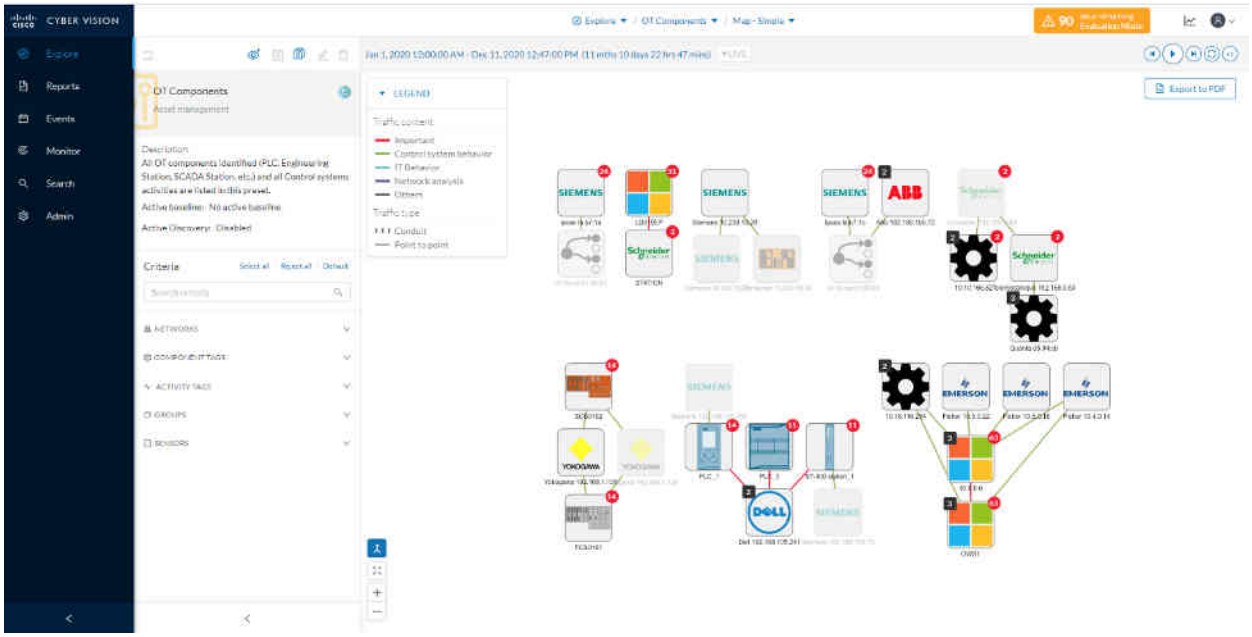
Gaining visibility to what you have on your network is the first step to understand what needs to be done: An accurate and up to date inventory of all the assets in your facility addresses this need.

Securing industrial environments requires continuous visibility into every device within the environment at every stage, from the moment it enters the environment to the time that it is removed. This helps organizations keep track of vulnerabilities, remote access for vendors, and decommissioned assets.

Other than what you know of OT assets, this list should also include any engineering stations, development laptops that may not be connected full time, and disconnected work cells like a palletizing robot. Just because these aren't currently connected to a central ICS network, doesn't mean they will stay that way.

The discovery process includes building an automated asset inventory that identifies the makes and models of devices, firmware, antivirus software, and other system factors to assess asset vulnerability. This step also includes a network discovery process to build a real-time view of the network's application flows and communication protocols.

Cisco Cyber Vision provides visibility into all industrial assets and creates inventories that have relevant details such as device type, firmware version, etc. Cyber Vision Center is deployed as a sitewide application. Cyber Vision sensors are embedded into the cell/area network equipment to discover devices, monitor communications, and pass security telemetry to Microland's iSOC team.



ACHIEVING IT/OT CONVERGENCE

The key finding from gaining the OT asset visibility is a risk analysis into the business process on the plant floor. OT now has a map of processes, devices, and flows. IT has a contextual list of process groups that are critical to plant operations. Now the two can work together with this information to define logical groups that need to share data or have specific access. They can also prioritize these groups by process criticality to define alert and detection strategizes that doesn't impact business processes. IT now has some tangible intelligence to what was once viewed as just an IP address on the plant floor.

Phase Two

Now that you have a single, detailed view of your ICS architecture, IT and OT can work together to create a joint strategy for protecting it.

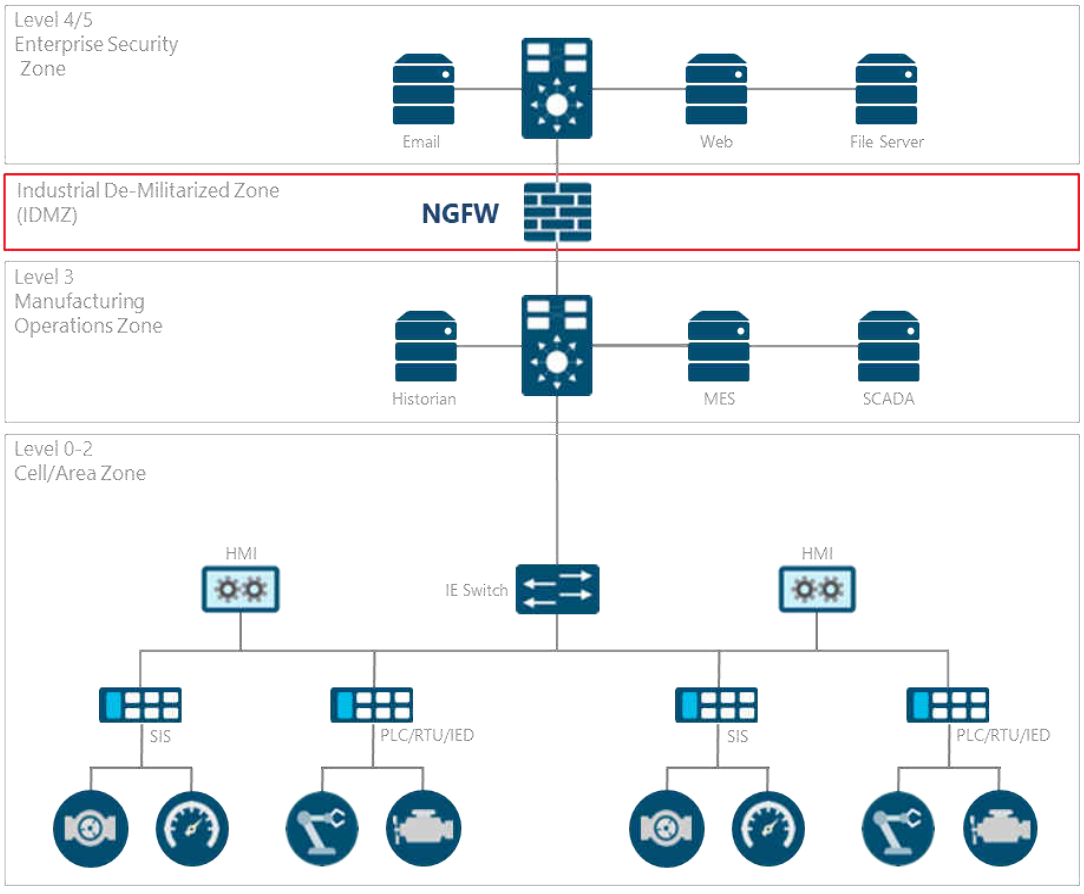
PROTECT YOUR ICS WITH NETWORK SEGMENTATION

Cyber criminals study ways to infiltrate the ICS network by looking at the most vulnerable point. Segmentation helps to prevent the spread of the infection and limits it only to those endpoints that an infected host can reach. The intent behind network segmentation is two sided: to logically group assets that you want data shared and to logically disconnect those you don't. Unlike consumer-based networks, in which the main threat vectors involve the internet, in an ICS, the fear is that malicious programs will be inserted through USB keys or by the lateral movement of malware to the stations that pilot the ICS.

Segmentation serves as a stop gap. If an ICS is broken into smaller, manageable pieces, a potential threat is contained within that piece and is easier to remedy. If you take the opening story as an example, the same malware would have only affected one line instead of spreading through the entire facility. In the reference diagram, we use the Cisco next generation firewall (NGFW) and an ISA3000 to create and manage these segments easily.

CREATE AN INDUSTRIAL ZONE

An "I" DMZ (industrial de-militarized zone) creates a secure gap between the plant and office minimizing the potential threats that could be introduced from non-production assets.



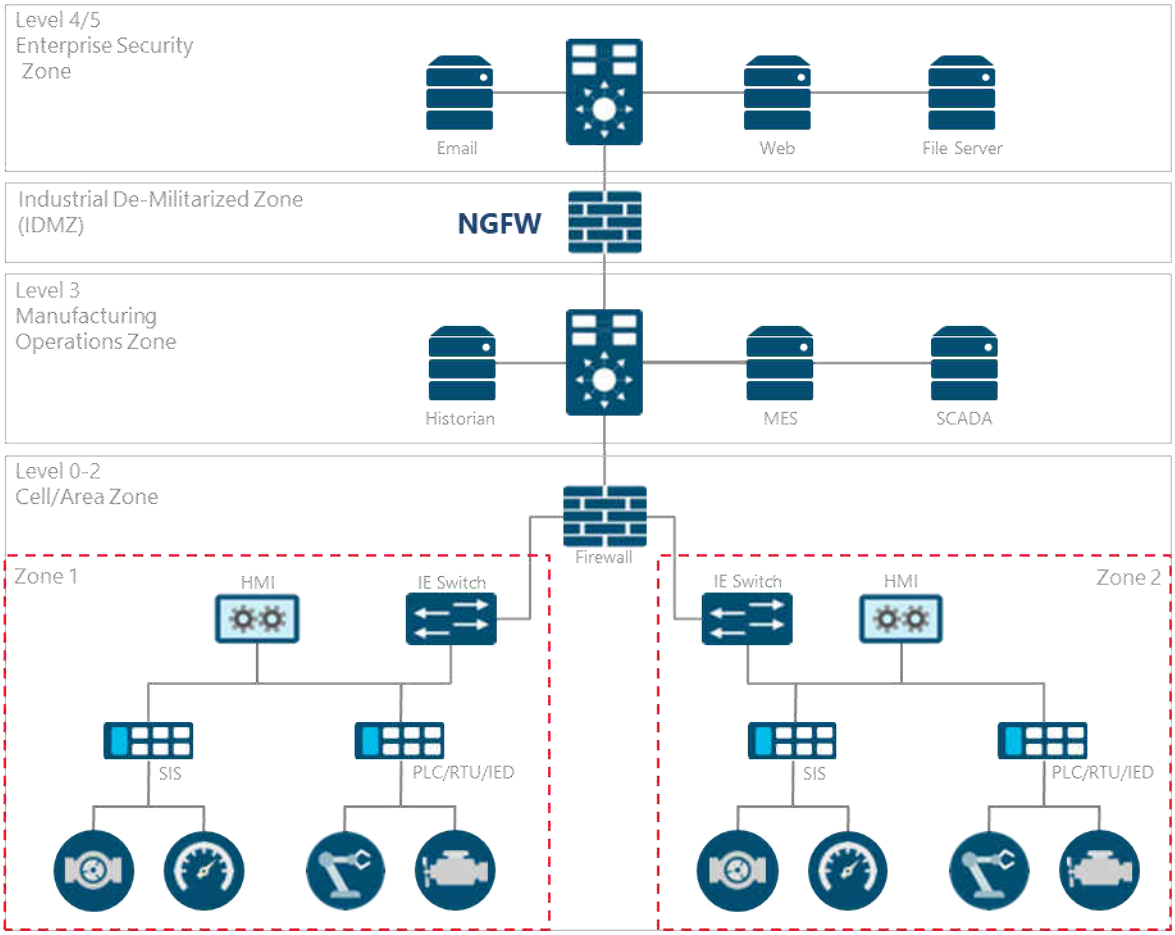
ZONING

A "zone" can be defined as a production cell, line, area, building or whatever defines a group of assets that need to communicate. The asset inventory that you completed enables you to now think about how your plant network can be organized into these zones.

These groups that you define could be based on:

- **Physical location:** All assets in building three or on the welding line.
- **Process type:** All security cameras on the floor or AGVs
- **Process flow:** All devices in the chassis line

These are some examples, but all should be considered when organizing your groups. The goal is to make small segments that doesn't impact processes or performance while minimizing the impact and spread of a potential threat.



Zones are established by having separate LANs and/or VLANs, with conduits between zones enforced by the Cisco 3000 Series Industrial Security Appliances (ISA3000). The ISA3000 provides the access and communication control, as well as intrusion detection capabilities. The ISA3000 and Cisco NGFW can also include Cisco Advanced Malware Protection (AMP) to provide protection against malware.

Now that you have your network organized, you can now easily manage IT security policies, internet access, and VPN vendor connectivity.

DETECT

It's a common practice for IT SOC engineers to implement security monitoring capabilities that monitor data integrity for IT. While commonly associated with IT security, data integrity is also applicable to OT security when it comes to checking for process anomalies by decoding industrial network traffic and determining the integrity and legitimacy of the commands within such traffic.

Organizations need a solution that understands the protocols used in these industrial environments and knows the OT processes, environment, assets, and correct use of protocols.
IT and OT personnel must work together to define what should be considered an anomaly. This includes defining what the normal industrial process should be, understanding the potential impact of an anomaly to set criticality levels, and enabling effective communications between IT and OT teams so that SecOps doesn't drown in false alarms during OT maintenance, for instance.

During their day-to-day activities, each side of the organization will need different kinds of data and insight to assess, investigate, and respond to OT security events. OT teams will be monitoring for process modifications and changes to devices. IT/SecOps teams will be monitoring vulnerabilities and IDS events. And SOC managers will need detailed asset information to simplify the investigation process and policy configurations.

Phase Three

Monitoring and Management

With full visibility to your ICS and a well segmented network, the next step is leveraging the insights available at your fingertips to run secure operations with confidence. It is imperative to stay ahead of the curve, proactively introducing new policies, or identifying anomalous behavior and new threats introduced into the environment.

How Can Microland Help?

Unlocking the full potential of Industry 4.0 requires a common, connected, and standardized infrastructure in which people, processes and technologies can be seamlessly connected. Microland's Industrial Site Monitoring & Management solution offers a turnkey approach to engineer, monitor, and secure the industrial network landscape, managed by a remote 24x7 OT/IT Operations Team, letting customers focus on core business operations.

The solution gives full visibility into your ICS, including dynamic asset inventory, real-time monitoring of control networks and process data, and comprehensive threat intelligence, so you can build secure infrastructures and enforce security policies to control risk.

Combining a unique edge monitoring architecture and deep integration with Cisco's leading security portfolio, this solution can be easily deployed at scale so you can ensure the continuity, resilience, and safety of your industrial operations. Our 24x7 SOC operations utilize this cutting-edge software paired with three decades of network and SOC operational excellence to secure industrial networks and operations.

The Industrial Monitoring Solution comprises:

Industrial Security Assessments

Securing OT infrastructure starts with having a precise view of asset inventory, communication patterns, network topologies and a sound understanding of the industrial protocols and ecosystem. Security assessments evaluate your landscape to identify security issues and architectural risks across the network, application, firmware, and hardware.

Industrial Security Implementations

We can deploy the security services by implementing Cisco's Cyber Vision at scale across factories and sites following a planned roadmap and our time-tested methodology. This factors in provisions for a diverse OT asset landscape including different OEMs. Bringing our expertise, we deploy a robust security framework while simplifying OT security implementation, thereby taking off the load from clients.

24 x 7 i-SOC Monitoring/Managed Services

Live Industrial Asset Discovery & Monitoring along with network topology discovery provides immediate notifications of new devices or people connected to your plant floor. Our IT/OT engineers deploy specialized traditional and machine learning based OT network & security tools for cyber security threat monitoring and management specific to OT networks.

The i-SOC services are designed to provide a security, purpose and performance focused OT network to a production environment. Our simplified and best-in-class approach enables your site teams to focus on production and innovation.

References

ISA-62443: https://www.isa.org/products/ansi-isa-62443-3-2-2020-security-for-industrial-a

Cisco: https://www.cisco.com/c/en/us/products/security/cyber-vision/index.html

Forbes: Cyberattacks On IOT Devices Surge 300% In 2019, 'Measured In Billions', Report Claims

About the author

Robert Rash
Principal Industrial Architect (IIoT), Microland

RobertRO@microland.com

@robertmrash

Rob is an experienced industrial architect with over 19 years of experience and a demonstrated history of working in the industrial automation industry.

About Microland

Microland's delivery of digital and "Making Digital Happen" allows technology to do more and intrude less. We make it easier for enterprises to adopt nextGen Digital infrastructure. We enable this using our expertise in Cloud and Data Centers, Networks, Digital Workplace, Cybersecurity and Industrial IoT, ensuring the embrace of brilliance is predictable, reliable, and stable.

Incorporated in 1989 and headquartered in Bengaluru, India, Microland has more than 4,500 digital specialists across offices and delivery centers in Asia, Australia, Europe, Middle East and North America.