Industry 4.0

THE CURRENT STATE OF SECURITY FOR THE INTERNET OF THINGS

Cadre
information security

Contents

Introduction

A QUICK RUN THROUGH THE INDUSTRIAL REVOLUTION

INTRODUCTION

The production industry has seen incredible changes over the last few centuries, and emerging technologies such as the Internet of Things provide an abundance of previously unimaginable opportunities, yet these advantages also make the industry vulnerable on the cyber landscape.

A Quick Run Through the Industrial Revolution

In the last 336 years, the production industry has evolved from mechanical production powered by steam and water, to assembly lines and electricity, to computer automated distribution control systems, to today's cyber-physical systems and the internet – known as the next industrial revolution, or Industry 4.0.

Today's industrial operations are managed by an array of computing systems known as operational technology (OT). Industrial control systems (ICS) are a major segment within the operational technology sector. These systems are used to monitor and control industrial processes, which are typically managed by programmable logic controllers (PLC) and supervisory control and data acquisition (SCADA) systems.

SCADA was first implemented in 1969 (Industry 3.0), and although it has evolved into Industry 4.0, it has limited capabilities. Simply put, it is a computer system that lacks many technical and security controls that are critical in today's industrial environment.

The Internet of Things (IoT), on the other hand, comprises of modern technologies that work together to create a network of devices that are constantly connected and exchange data across different networking infrastructures.

Both IoT and SCADA platforms involve sensors and data acquisition, and they are intended to optimize operational control of devices and processes. However, the integration of these platforms would provide the most optimal industrial network security ecosystem.

1 | The Current State of Operational Technology and Internet of Things

SECTION ONE

The Current State of Operational Technology and Internet of Things

There are more IoT devices today than there are users on the internet. In fact, it is predicted that by this year (2020), there will be 50 billion devices or things connected to the internet. That's just going to explode and keep growing. This is very top-of-mind with C-level execs we talk to and the network operators that we work with daily.

A significant shift is happening in the industry as new technologies forge dynamic internet-based control systems. Government compliance regulations are also becoming more robust with these emerging technologies. For example, we've recently seen the release of new CISA and information security guidelines for OT controls and ICS, as well as the new NIST Software Development Framework.

As a reaction to these new standards, there has been a lot of new startups coming out of stealth mode in the last few years as well as a few players that've been around a bit longer. They are IoT discovery engines. They're basically sitting quietly, listening on those segments where you have an ICS network or IoT devices. They're discovering devices on the network, discovering who these machines are talking to over the network, identifying firmware revisions and other things that can only be extrapolated by listening in on the conversation. These startups are very specialized. They hire engineering resources from the market they cover and they're very good at deciphering the proprietary protocols that these devices speak. This, of course, is in the ICS realm. There's also enterprise IoT, such as standard devices in your home, TVs in the conference room, IP cams in your facility, and physical entry type devices, etc.

2 | Flying Blind in a Vulnerable Network Security Ecosystem

Flying Blind in a Vulnerable Network Security Ecosystem

While operational technology and the Internet of Things offer an abundance of advantages to the industry, they're also vulnerable on the cyber landscape as we've seen in daily headlines of organizations falling prey to cybercrime.

There are many challenges with OT, SCADA systems, and IoT devices. In the case of ICS networks and SCADA systems, our customers try to follow the Purdue Model, which is a network architecture consisting of a nicely segmented hierarchy of systems within the ICS network that allows levels of separation between devices that require externalized access all the way down to devices doing the actual work. Any connection between them is highly controlled, sometimes by unidirectional gateways, or Next-Gen gateways with specific policies for each layer in the model.

Today, as IT and OT converge, we're faced with new types of sensors, such as conveyor belt sensors that may send production rates directly to a business partner via a cloud monitoring component. This turns the Purdue model on its head as these sensors need direct access to the Internet. The desire for more real-time operational data in manufacturing environments is growing, thus requiring new approaches to the Purdue Model. Some have suggested a "Level 6" Zone to cover the new IoT devices which require direct to cloud connectivity, leaving the original Purdue Model intact.

We also see challenges with validating the identity of limited function OT devices to allow them on the network. For example, if you're going to have a default deny policy for allowing new devices on the network, are you going to have a manual process to onboard those devices? If so, that fits a static environment and the Purdue Model very well. But if you want a dynamic insertion into the network, then the device has to be capable of presenting an authenticator in some way or be front-ended by functionality that can provide an authenticator that can be interrogated by the network intelligence. It would be phenomenal if devices could present the appropriate certificate for an insertion into the network, but that's absolutely not possible in a lot of our programmable logic controllers. The new ICS/IoT discovery sensors can quickly identify the new device on the network, determine if it's at an authorized device with the proper firmware level, gather details on where it's attempting to communicate and relay all that information to a Network Access Control (NAC) solution.

3 | Leverage Network Access Control Solutions

SECTION THREE

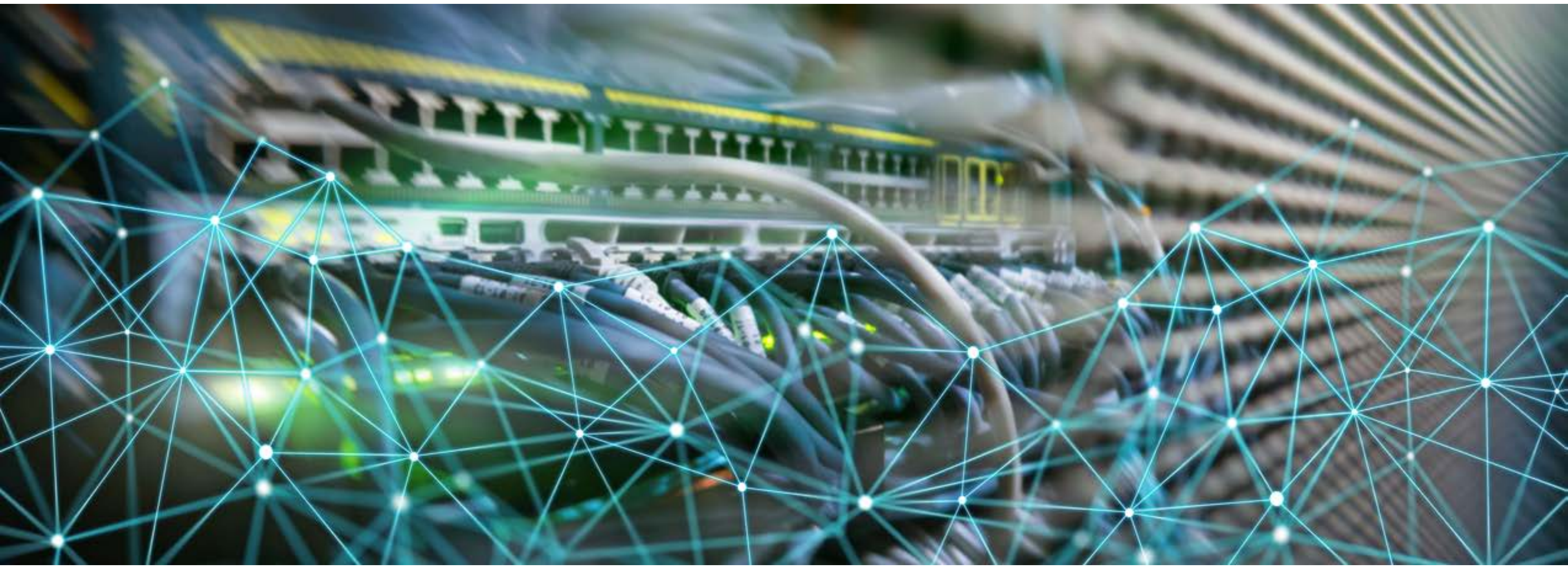
Leverage Network Access Control Solutions

Fortunately, we can leverage NACs to protect dumb devices that are critical to business and security operations. Dumb devices will not only interface with firewalls to dynamically block traffic that's not expected or not allowed, but they can also interface with NAC devices.

There are many NAC solutions to help determine a new device's health and whether or not it should be allowed on the network.

Layer 2 level solutions can work very well, and allow you to contact your vulnerability scanner and say, "Hey, there's a new device on the network, scan it for me, please." You can then assess the results to better understand what the device is.

So, at the very least you're alerted when a new device pops up on the network. That visibility sensor will tell you when a new device is plugged in, when it starts talking on the network, this is the device, this is the firmware revision of that device, and you'll have workflows in place to decide whether to automatically allow it based on those parameters or escalate it up to someone to make that decision.



At the layer 3 level, you need to decide what VLAN to place the device in. If there's a preliminary check or something that interferes with the NAC solution's ability to determine whether or not it's allowed on the network, then it might be put in a guest VLAN or a quarantine VLAN for manual inspection.

If the vulnerability scan comes back fairly clean and the IoT discovery device says, "Yes, this is a XYZ type of device, it's running on X version software or operating system, etc." Then you can configure those parameters into the NAC solutions to determine if it's allowed to be placed in production network.

If you don't have a NAC solution, you can simply leverage layer 3 controls to keep it from communicating outside the network. But having a NAC solution in combination with a Next-Gen Firewall and IoT sensor will give you the best visibility and best means to automate workflows to determine if it belongs on the network, or if it should be quarantined for further assessment.

This is hugely important because of the pervasiveness of ransomware attacks these days. Now you have another attack vector, and you're bringing something into your system that may already have been compromised. So, you want to have those protocols before you let that device phone home to get the ransomware keys.

4 | Break Shop Floor Barriers

SECTION FOUR

Break Shop Floor Barriers

There is often a breakdown in communication between non-IT folks, such as shop floor managers, and security folks. On the surface, this may appear as a turf war, because shop managers don't want security folks walking the floor, disrupting equipment and operations.

Neutralize the shop floor turf war

The reality is that both shop managers and security folks have a unique base of knowledge that is critical to both operations and security. So, it's important that they bring their expertise to the table, and collectively map out the best solutions.

Perhaps the most effective way to earn the shop manager's trust and cooperation is to begin by simply sitting down with open ears. Allow them to educate you about the operational environment and any concerns they may have about the functionality of equipment, etc.

Shop managers know how their machines operate, the protocols used within their shop, and they understand what breaks if the line of communications between one device and another is broken. They see the symptoms on the shop floor and can recognize those things very quickly.

Elevate your customer's cooperation

By allowing your customer to tell their story first, you're immediately letting them know that you value their experience, expertise and concerns. They'll be less likely to take a guarded stance and be more receptive to the expertise that you bring to the table.

This approach will improve communications and cooperation. It may also organically address concerns that you've identified while doing your homework to better understand your customer and it will allow you to further identify and focus on the most critical issues.

Now that your customer understands that you're genuinely invested in the plant, you can ask the unanswered questions and address concerns on the security side of plant operations that you've identified while doing your homework.

This is where you review the complete inventory of systems you see on the network, and even out of the network in some situations. A complete inventory of what devices are seen on the network, and the flows actually occurring on the network between those devices.

Come bearing gifts

Maintaining production and uptime is one of a customer's highest priorities. Bring solutions to the table and show your customers how these solutions will improve production and uptime, and how you can help them do it securely.

Show them how an IoT sensor can act as an early warning system, and how they can detect if a device is starting to post errors. Perhaps it just started posting errors but hasn't quite failed, or perhaps a network condition is causing the sensor to error out.

Show them the benefits of having an ICS Discovery Sensor in place, how it will help them follow best practices in populating a configuration management database (CMDB) inventory system with firmware revisions and specific device identifiers. You can also show them network flows, and alerts to problematic communications between devices or to the Internet, all of which will improve operational security.

5 | Network Segmentation Guidance

SECTION FIVE

Network Segmentation Guidance

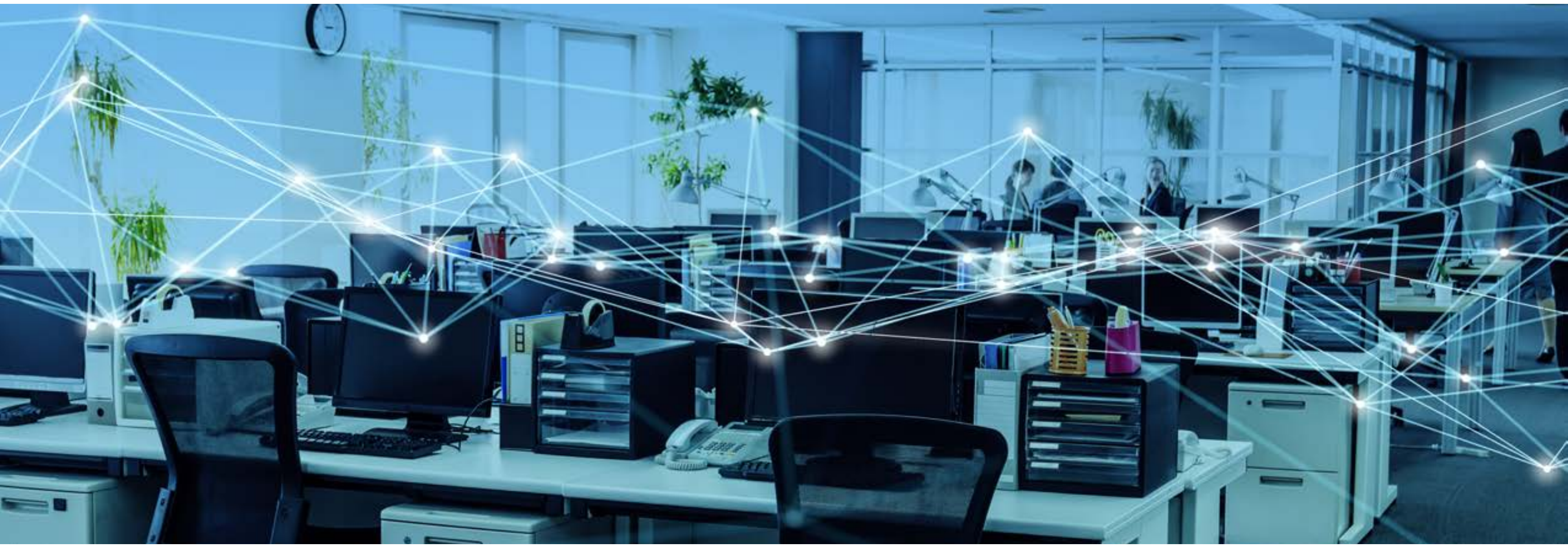
Government compliance regulations are moving more towards some of the best practices that IT organizations have been doing for a very long time. They simply bring us closer to understanding each other and are moving the industry towards a more secure environment.

While the needs of IT are to maintain secure communications, the operators of these manufacturing plants have an obligation to keep things running and keep production going. Doing that securely is something that can't be ignored these days.

There have been too many plants shutdown by ransomware because they haven't applied the same types of controls and processes that they do on their information and data security, so segmenting your networks is basic best practice to help prevent spread of malicious activities.

Applying threat intelligence to the information flows that you discover through these devices is critical. Modern threat intelligence can spot malicious activity way before you notice anything going wrong on the shop floor or within your office environment.

So, it's extremely important to apply modern security processes and techniques. Maintaining regular vulnerability assessment programs will allow you to track changes over time and see what progress you've made and patch vulnerabilities in your systems.



6 | The Future of IoT Threat Intelligence

SECTION SIX

The Future of IoT Threat Intelligence

Modern IoT discovery devices are implementing machine learning and AI to spot anomalous behavior in ICS and enterprise IoT devices. They’re sending their data to a cloud-based server where that meta information from the packets that are flowing across the network can be analyzed by an AI engine.

DHS and the shared community within ICS are tracking some of the more modern attacks and putting together full Indicators of Compromise (IoCs) in the MITRE Attack Framework. So, devices can actually look for tactics, techniques and procedures that are used by malicious actors against industrial and medical type environments.

“Threat intelligence is becoming less proprietary. In fact, there is a very large shared threat intelligence initiative underway.”

Threat intelligence is becoming less proprietary. In fact, there is a very large shared threat intelligence initiative underway. The Department of Homeland Security (DHS) shares threat intelligence with critical infrastructure across the country. Other organizations are also leveraging shared intelligence to prevent many of the attacks we see in other countries.

Conclusion

BUILD A ROBUST CYBERSECURITY SOLUTION FROM THE BOTTOM-UP

CONCLUSION

Build a Robust Cybersecurity Solution from the Bottom-UP

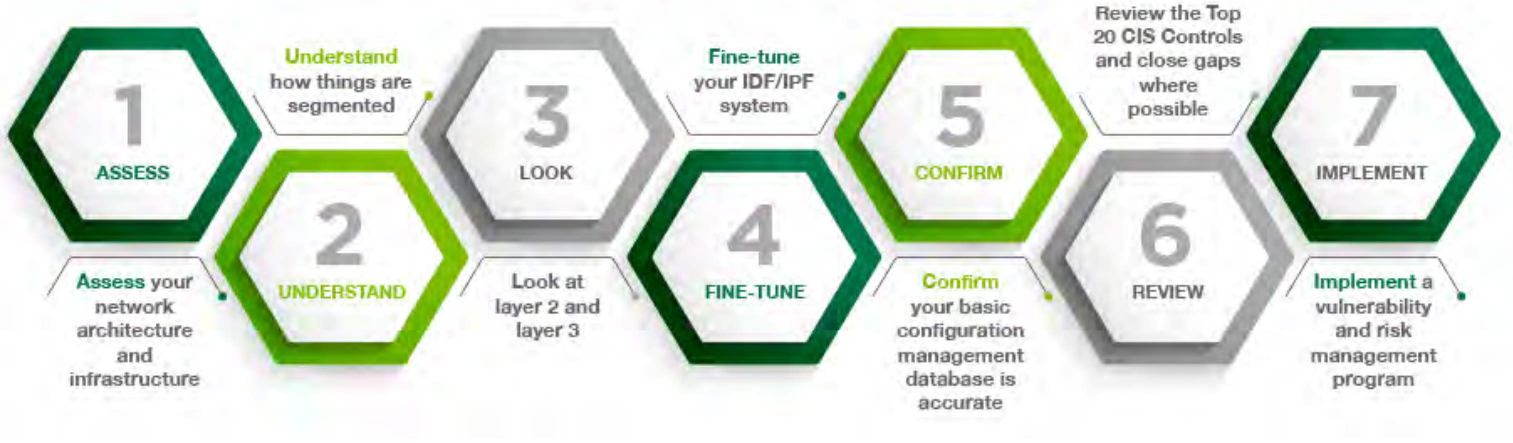
There are a whole lot of companies that treat East-West traffic as if it is untouchable. That's not the case. It's how companies get infected with ransomware and it spreads like wildfire.

It's very important to start with the basics. You must know your network, devices on the network, and versions of software and operating systems running on those devices to effectively protect your network security ecosystem.

Remember, visibility is everything. Make sure you know where your weaknesses are, and how to configure your controls to protect yourself from people who would take advantage of those weaknesses.

If you would like to learn how Cadre can help you implement a vulnerability and risk management program, please contact us. We'd love to be part of your cybersecurity solution.

Critical Steps to Fortify Your Organization



1 ASSESS: Assess your network architecture and infrastructure

2 UNDERSTAND: Understand how things are segmented

3 LOOK: Look at layer 2 and layer 3

4 FINE-TUNE: Fine-tune your IDF/IPF system

5 CONFIRM: Confirm your basic configuration management database is accurate

6 REVIEW: Review the Top 20 CIS Controls and close gaps where possible

7 IMPLEMENT: Implement a vulnerability and risk management program

How Can Cadre Help You?

For more information on the current state of security for the internet of things and how Cadre can help you, reach out to start a conversation today!

cadre.net

cadre
information security