The bridge to possible

Cisco Industrial IOT

Michał Małuszek
Cisco Industrial IOT EMEA Team

mmalusze@cisco.com

- **Unique portfolio capabilities**
- Market drivers
- OT Project examples and design considerations

Cisco solutions to accelerate IoT deployments

cisco Cisco Validated Design ✓

✓ Simplicity ✓ Security ✓ Scalability

Manufacturing

- Industrial Automation
- Industrial Security
- Industrial Wireless
- AGVs, AMRs

Power Utilities

- Substation Automation
- Distribution Automation
- Smart Metering
- Grid Security

Oil-&-Gas

- Industrial Automation
- Connected Pipeline
- Refinery/Processing Plants, Worker Safety

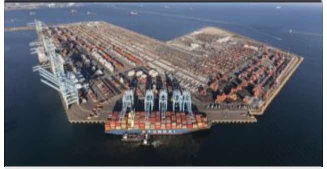
Roadways & Intersections

- Dynamic Road Signage
- Pedestrian Safety
- Signal/Camera connectivity

Smart Cities

- Smart & Connected Cities
- Digital Divide
- Video Surveillance

Ports & Terminals



- Terminal Automation
- Autonomous and Tele-Remote Operations
- OCR

Mining

- Surface Mining
- Underground Mining
- Fleet Management, Autonomous Vehicles

Renewables

- Off-shore / On-shore Windfarms
- Solar Farms
- EV Charging

Rail

- High-Speed Rail
- Urban / Light Rail
- CBTC, Passenger Wi-Fi, Train to Trackside

Mass Transit

- Fleet Management
- Passenger Wi-Fi
- Vehicle Telemetry

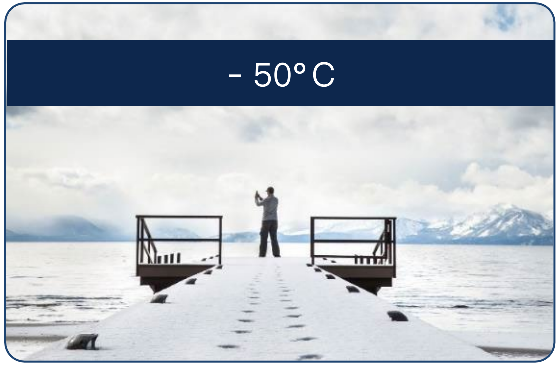
Proven Integrations

Rockwell Automation · Landis+Gyr · Itron · Schneider Electric · Cohda Wireless · energybox · Actility · ECONOLITE

SIEMENS · MITSUBISHI ELECTRIC · EXIMPROD Power Systems · EATON Powering Business Worldwide · SEL · CAT · SANDVIK · iteris · BECKWITH ELECTRIC CO. INC. · CIMCON Lighting · KLAS TELECOM · iOmniscient

Cisco IOT – most known use cases

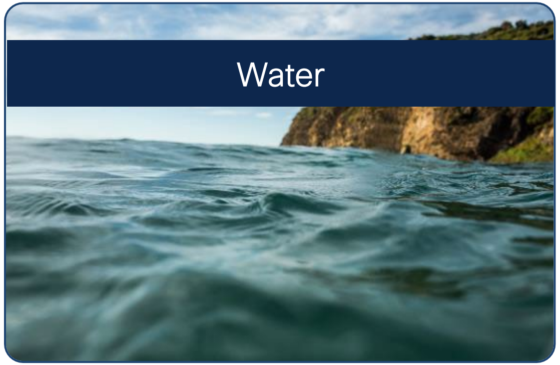
Your network goes wherever you need it



- 50° C

+75° C

Shock/vibration



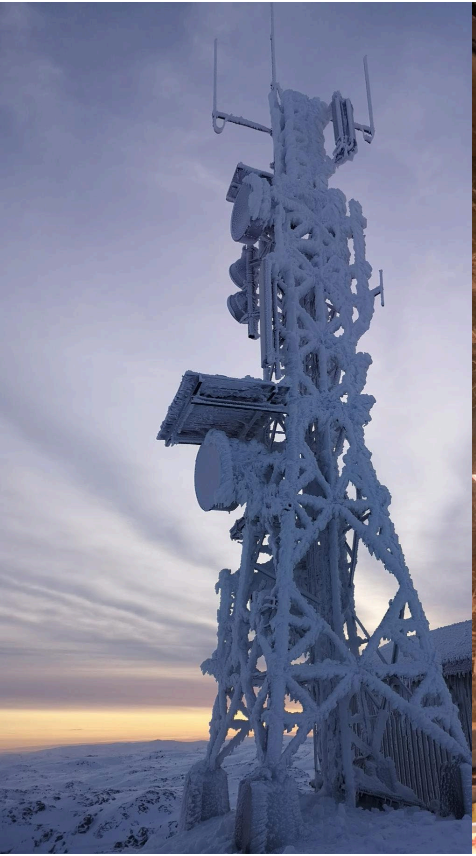
Water

Dust

Industrial certifications (e.g., EN50155)

Industrial protocols

Cisco IOT in production



Cisco IOT in production cont.

Cisco at Indy Autonomous Challenge
Helping build high-speed autonomous race cars

- 9 teams, 21 universities from 9 countries
- Students develop software to safely compete at high speeds on the Indianapolis Motor Speedway

LOXAM
0826 16 1234
DS2223RTP
4x4

Cisco IOT portfolio – 10 key considerations

IEC-62443-4
Part-1 & Part-2
Compliant Portfolio

1. Ruggedized, dust, humidity, temperature range
2. ARM
3. Longer product lifecycle
4. Software download possible without service contract
5. Fanless
6. Low power
7. Designed for air-gapped, isolated networks – no telemetry
8. Permanent, perpetual license unless centrally managed
9. Industrial protocol support e.g. Profinet
10. IOT Edge applications support

Comprehensive Industrial IoT Networking Portfolio

IEC-62443-4 Part-1 & Part-2 Compliant Portfolio

Industrial Switching

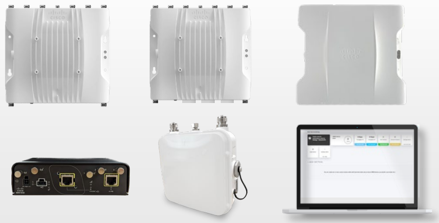
IE1000, IE3100, IE3200, IE3300, IE3400, IE4010, IE9300

Industrial Routing

IR1101, IR1800, IR8100, IR8300

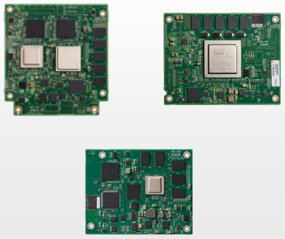
Industrial Wireless

IW9167E, IW9167E-HZ, IW9167I, IW9165E, IW9165D



Embedded Networking

ESS3300, ESS9300, ESR6300

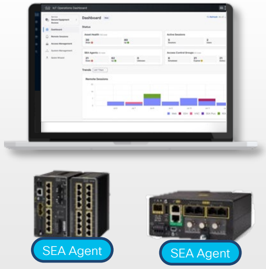


OT Visibility

Cyber Vision + Splunk SIEM and OT Security Add-on

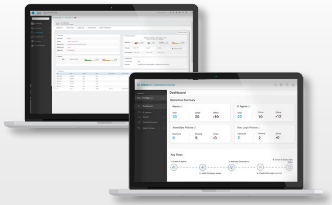
OT Remote Access

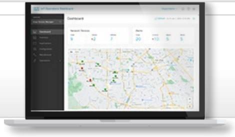
(Secure Equipment Access)



Data Control and Exchange

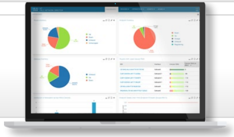
Edge Intelligence (Edge to multi-cloud data flow), Application Hosting, Splunk





Management & Automation

Cisco Catalyst Center, Cisco Catalyst SD-WAN, Field Network Director



The bridge to possible

- Unique portfolio capabilities
- **Market drivers**
- OT Project examples and design considerations

Industry Trends: Key Topics for Manufacturing

Advanced Manufacturing Operations

The future is a "manufacturing anywhere" model, where data is automated, simultaneously mobile, and controlled.

Manufacturing Supply Chain Operations

People, machines, and materials are in constant motion within a manufacturing warehouse operations. Proactively monitor and manage your supply chain.

Sustainability

Reduce operational expenses, improve the quality of production, and align to growing climate priorities.

Cybersecurity

The ongoing digitization of manufacturing will continue to elevate and introduce new security risks as the threat landscape becomes more complex.

The Rise of IT-OT Convergence

1980 - 2000

Two separate networks
Different technologies and approaches

Yesterday

Increased adoption and proliferation of IT based technologies in industrial information systems
IP based communication, software, hardware, cyber security

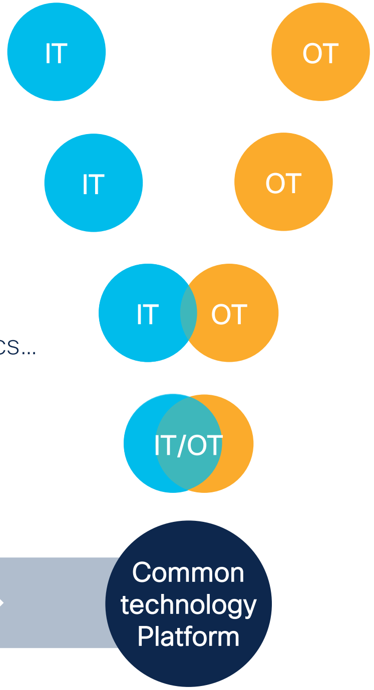
Today

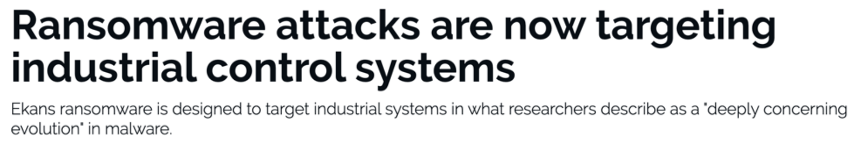
Strong need for integration of business and operational data to gain insights
Cloud, wireless, Big Data, smart sensors, Industrial IoT, predictive analytics…

Advent of Industry 4.0
Digital Twin, smart robots, cyber physical systems, prescriptive analytics, augmented reality, adaptive manufacturing

Tomorrow

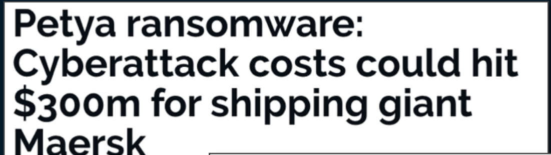
Fully connected enterprise and production
Vertical and horizontal integration of the entire value chain



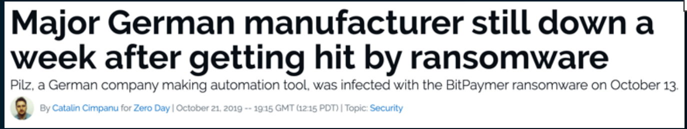


Ransomware attacks are now targeting industrial control systems

Ekans ransomware is designed to target industrial systems in what researchers describe as a 'deeply concerning evolution' in malware.



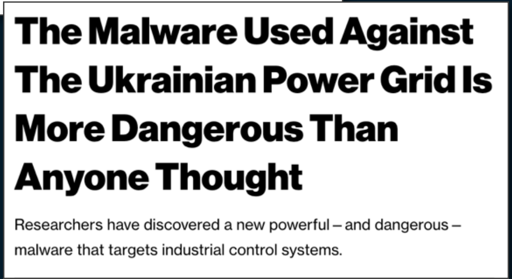
Petya ransomware: Cyberattack costs could hit $300m for shipping giant Maersk



Major German manufacturer still down a week after getting hit by ransomware

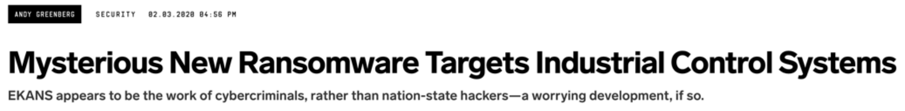
Pilz, a German company making automation tool, was infected with the BitPaymer ransomware on October 13.

By Catalin Cimpanu for Zero Day | October 21, 2019 -- 19:15 GMT (12:15 PDT) | Topic: Security



The Malware Used Against The Ukrainian Power Grid Is More Dangerous Than Anyone Thought

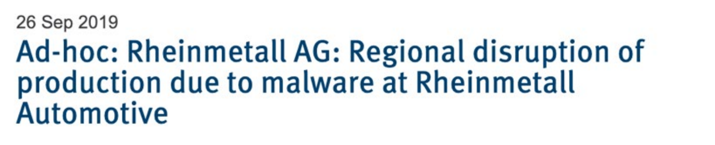
Researchers have discovered a new powerful – and dangerous – malware that targets industrial control systems.



ANDY GREENBERG SECURITY 02.03.2020 04:56 PM

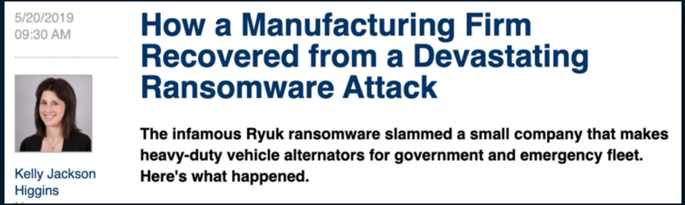
Mysterious New Ransomware Targets Industrial Control Systems

EKANS appears to be the work of cybercriminals, rather than nation-state hackers—a worrying development, if so.



26 Sep 2019

Ad-hoc: Rheinmetall AG: Regional disruption of production due to malware at Rheinmetall Automotive

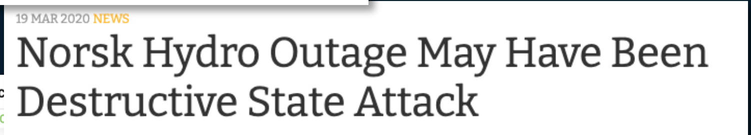


5/20/2019
09:30 AM

Kelly Jackson Higgins

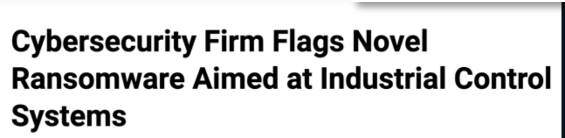
How a Manufacturing Firm Recovered from a Devastating Ransomware Attack

The infamous Ryuk ransomware slammed a small company that makes heavy-duty vehicle alternators for government and emergency fleet. Here's what happened.



19 MAR 2020 NEWS

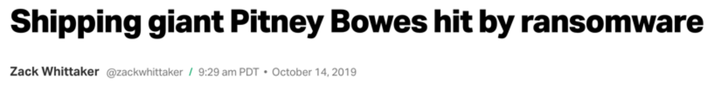
Norsk Hydro Outage May Have Been Destructive State Attack



Nextgov CYBERSECURITY EMERGING TEC

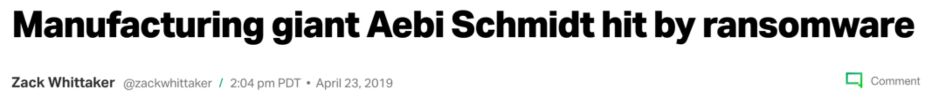
TRENDING // CLOUD // QUANTUM COMPUTING // ELECTION SEC

Cybersecurity Firm Flags Novel Ransomware Aimed at Industrial Control Systems



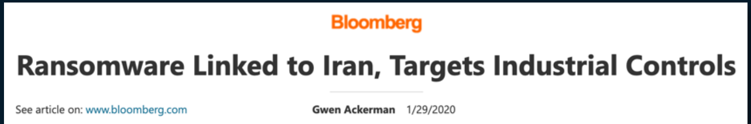
Shipping giant Pitney Bowes hit by ransomware

Zack Whittaker @zackwhittaker / 9:29 am PDT • October 14, 2019



Manufacturing giant Aebi Schmidt hit by ransomware

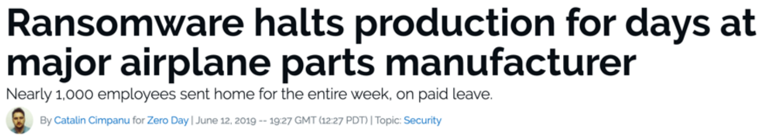
Zack Whittaker @zackwhittaker / 2:04 pm PDT • April 23, 2019 Comment



Bloomberg

Ransomware Linked to Iran, Targets Industrial Controls

See article on: www.bloomberg.com Gwen Ackerman 1/29/2020

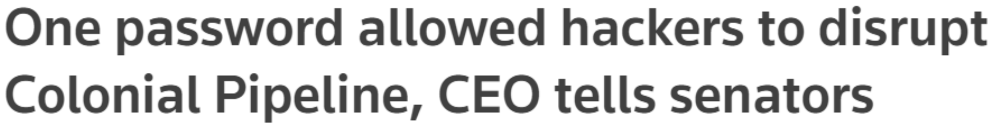


Ransomware halts production for days at major airplane parts manufacturer

Nearly 1,000 employees sent home for the entire week, on paid leave.

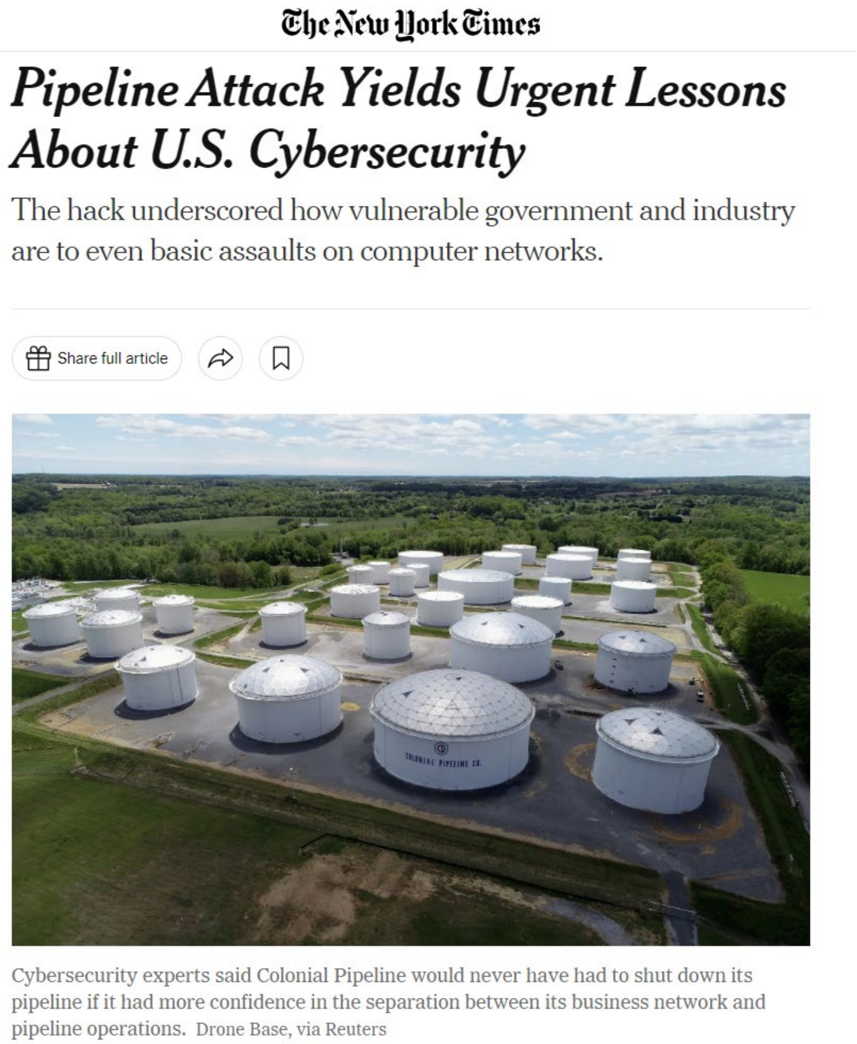
By Catalin Cimpanu for Zero Day | June 12, 2019 -- 19:27 GMT (12:27 PDT) | Topic: Security

Colonial Pipeline example



One password allowed hackers to disrupt Colonial Pipeline, CEO tells senators

… the attack occurred using a legacy Virtual Private Network (VPN) system that did not have multifactor authentication in place…



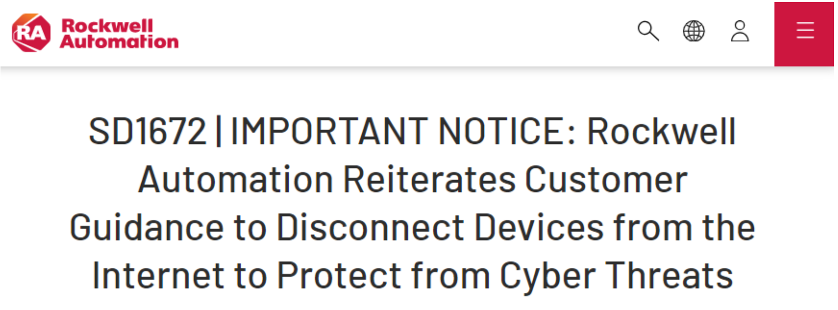
The New York Times

Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity

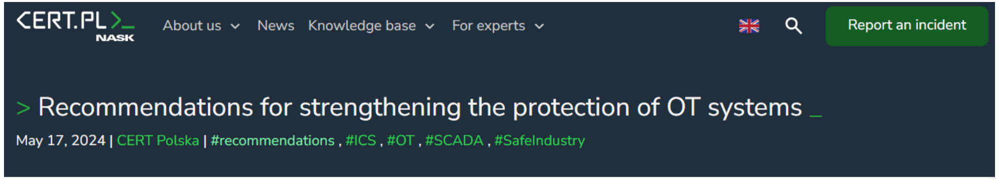
The hack underscored how vulnerable government and industry are to even basic assaults on computer networks.

Cybersecurity experts said Colonial Pipeline would never have had to shut down its pipeline if it had more confidence in the separation between its business network and pipeline operations. Drone Base, via Reuters

What are the IOT search engines Shodan and Censys?

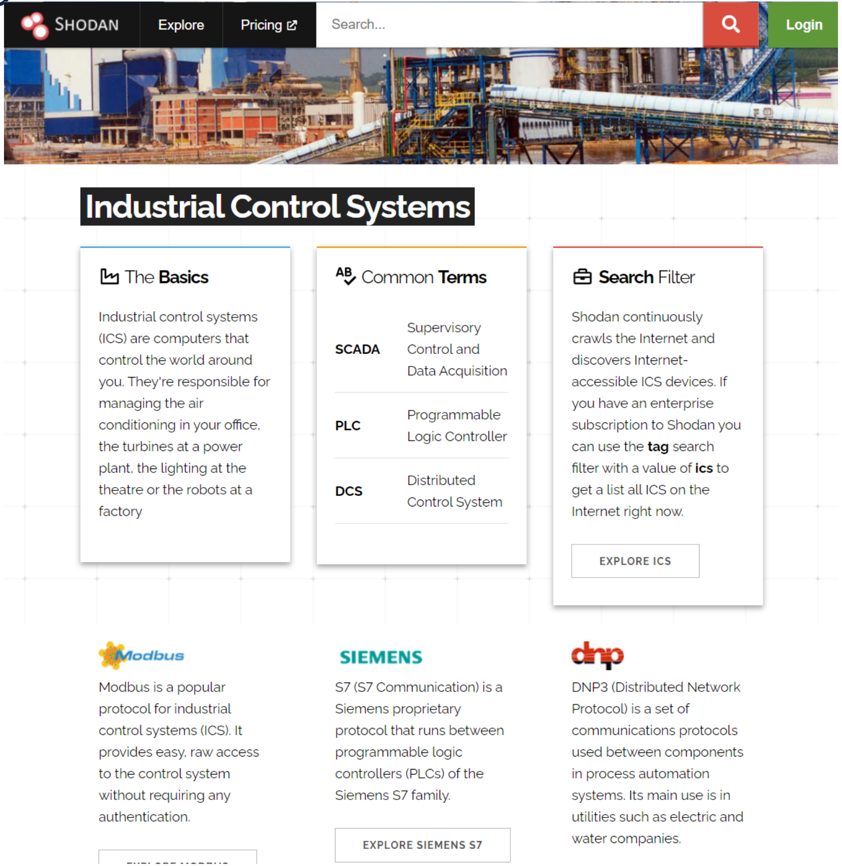


SD1672 | IMPORTANT NOTICE: Rockwell Automation Reiterates Customer Guidance to Disconnect Devices from the Internet to Protect from Cyber Threats



> Recommendations for strengthening the protection of OT systems _

May 17, 2024 | CERT Polska | #recommendations , #ICS , #OT , #SCADA , #SafeIndustry



Industrial Control Systems

The Basics

Industrial control systems (ICS) are computers that control the world around you. They're responsible for managing the air conditioning in your office, the turbines at a power plant, the lighting at the theatre or the robots at a factory

Common Terms

SCADA	Supervisory Control and Data Acquisition
PLC	Programmable Logic Controller
DCS	Distributed Control System

Search Filter

Shodan continuously crawls the Internet and discovers Internet-accessible ICS devices. If you have an enterprise subscription to Shodan you can use the **tag** search filter with a value of **ics** to get a list all ICS on the Internet right now.

EXPLORE ICS

Modbus

Modbus is a popular protocol for industrial control systems (ICS). It provides easy, raw access to the control system without requiring any authentication.

SIEMENS

S7 (S7 Communication) is a Siemens proprietary protocol that runs between programmable logic controllers (PLCs) of the Siemens S7 family.

EXPLORE SIEMENS S7

dnp

DNP3 (Distributed Network Protocol) is a set of communications protocols used between components in process automation systems. Its main use is in utilities such as electric and water companies.

Source:
https://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD1672.html
https://cert.pl/posts/2024/05/rekomendacje-ot/

The Landscape

Typical Issues Found in Industrial Networks

Unauthorized remote access by third parties

OT network fully connected to IT

Default credentials to log into systems

Security Patches not installed

Unknown devices

Bad Firewall or Switch configuration

Firmware uploaded over FTP without Signature

Multiple Time Servers

DNS queries to Amazon

Windows XP SMBv1

Unnecessary network communications

Decommissioned assets still connected

IPv6 traffic in IPv4 networks

Devices in the wrong VLAN

Malware or Virus activities

Program Upload over VPN during the night

What is ZTNA ? Why does it matter ?

> ZTNA provides controlled **identity and context-aware** access to resources. It starts with a **default deny** posture and **adaptively offers the appropriate trust** required at the time. A **trust broker** mediates connections between applications and users. The result **reduces risk** and offers **more flexible and responsive** ways to connect and collaborate.

Gartner®

Market Guide for Zero Trust Network Access,
August 2023

- Least privilege access
- Assets hidden from discovery
- No lateral movement possible
- Device posture compliance
- Time/date restricted access
- Reduced attack surface
- More flexible and responsive

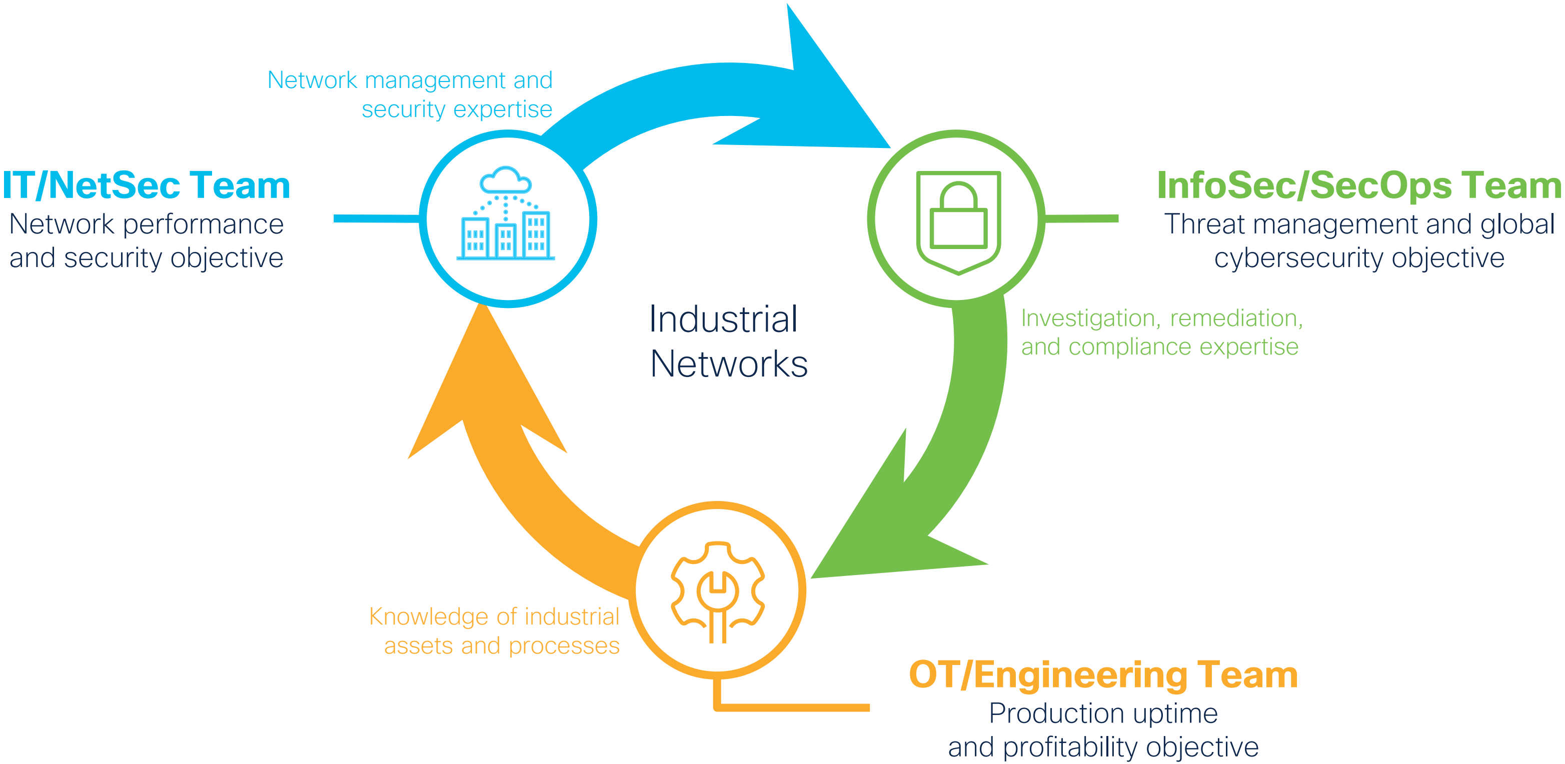
How Cisco OT visibility helps with NIS2 compliance

Required NIS2 Measures	OT Security Capabilities
Risk analysis	Risk scores, Security posture reports
Incident prevention	IEC62443 network segmentation with ISE
Incident detection & response	Snort IDS with Talos threat intelligence, Integration with Cisco XDR and Splunk
Vulnerability management	OT asset vulnerability, Cisco VM Risk scores
Cyber hygiene	Asset inventory, Activities, Security insights

Assess OT cyber risks with Cyber Vision to implement best practices

Who Manages Security in Operational Networks?

Hint: It must be a team effort!



IT/NetSec Team

Network performance
and security objective

Network management and
security expertise

InfoSec/SecOps Team

Threat management and global
cybersecurity objective

Investigation, remediation,
and compliance expertise

Industrial
Networks

OT/Engineering Team

Production uptime
and profitability objective

Knowledge of industrial
assets and processes

- Unique portfolio capabilities
- Market drivers
- **OT Project examples and design considerations**

Real-life OT Security project - simplified

Manufacturing

OT

- OT Asset visibility – 21 attributes
- Easy to read up to date **OT assets inventory** with filtering option for all locations, different asset attributes and OT protocols
- **CMDB** integration

IT

- **Solution and Performance Mgmt**. (HW+SW)
- Future proofed (cloud first strategy)

CSO

- **Setting security policies (N-S, W-E)**
- **Problem isolation**
- Security events

  (3rd party **SOC** integration)
- Vulnerability Mgmt. (3rd party integration)

Procurement

- **Effective licensing model** for all subsystems in the solution.
- Monitoring and pulling only the relevant information.

Question: if all of the 4 Teams are having a different objectives, who owns the project and who owns the budget?

Discrepancy in As-Built vs As-Is

As-Built Network Design

- ✓ Well defined VLANs per machine / process
- ✓ Port speeds set to prevent duplex mismatch
- ✓ QoS setting to prioritize time critical traffic
- ✓ Port security set for access control

As-Is Network State

- ⚠ Flat network with all devices in native VLAN
- ⚠ Devices in half-duplex due mismatch
- ⏲ Critical traffic treated as best-effort
- ☠ No port security settings

Compliance checks are important to ensure alignment to standards

How to Integrate Multiple Machines

Ethernet networks continue to grow

Each **machine** adds another

5-10

EtherNet / IP enabled devices

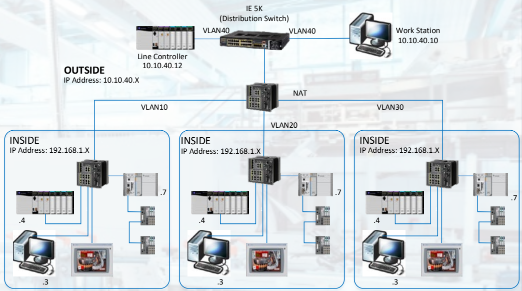
Every **line** adds another

250-1,000

EtherNet / IP enabled devices

How do I connect all these machines into a plant network to gain the advantages?

Layer 2 NAT Design



CUSTOMER STORY

Chemical

Smart Production

Manage the costs & ensure investments

Challenges

- Accelerate production automation to increase competitiveness
- Gain visibility into operational network to mitigate security threats

Solutions

- Cisco Cyber Vision on IE3400 Switches
- Cisco ISE, Cisco DNA Center

Outcomes

- Standardized network architectures to drive efficiency and lower costs
- Built comprehensive view of operational networks to improve production performance and security
- Created a collaborative workflow between IT and OT to drive secure industry 4.0 projects

CUSTOMER STORY

Automotive

Security and reliability on plant floor

Quality, Safety & Compliance

Challenges

- Utilize robots for automated processes on the factory floor

Solutions

- Cisco® Industrial Ethernet (IE) Switch Series
- Cisco Identity Services Engine (ISE)
- CURWB deployed at the 6m sq ft plant to enable mission critical applications in harmony with traditional WiFi access

Outcomes

- Customer has standardized its network design at the Plant and the e-powertrain production line is becoming fully automated
- Customer can now identify equipment failures, and assure production quality, improved efficiency

CUSTOMER STORY

Machine tool Producer

Optimizing production line

A leading manufacturer of machine tools, offering a broad range of products, including CNC (computer numerical control) turning centers, machining centers, and laser processing machines required help with their automation strategy and execution as well as the incorporation of IoT solutions.

Sustainability & Energy / Water

Challenges

- Optimizing production requires a system where production data can be visualized
- Understanding how much energy is consumed at which location
- Data-driven solutions for achieving carbon neutrality and innovation in production

Solutions

- Cisco Industrial Ethernet Switches
- Cisco Industrial Routers
- Cisco Wireless LAN Solutions

Outcomes

- Improved the plant utilization rate
- Energy-saving performance of machine tools
- Able to collect operation data of delivered machine tools in the cloud

CUSTOMER STORY

Automotive

Improving employee experiences

Webex and Augmented/Virtual Reality (AR/VR) are driving the new normal. See how an automotive company is using Webex Expert on Demand to communicate instantly across the globe with remote experts during times of travel restrictions and budgetary constraints.

Workforce management

Challenges

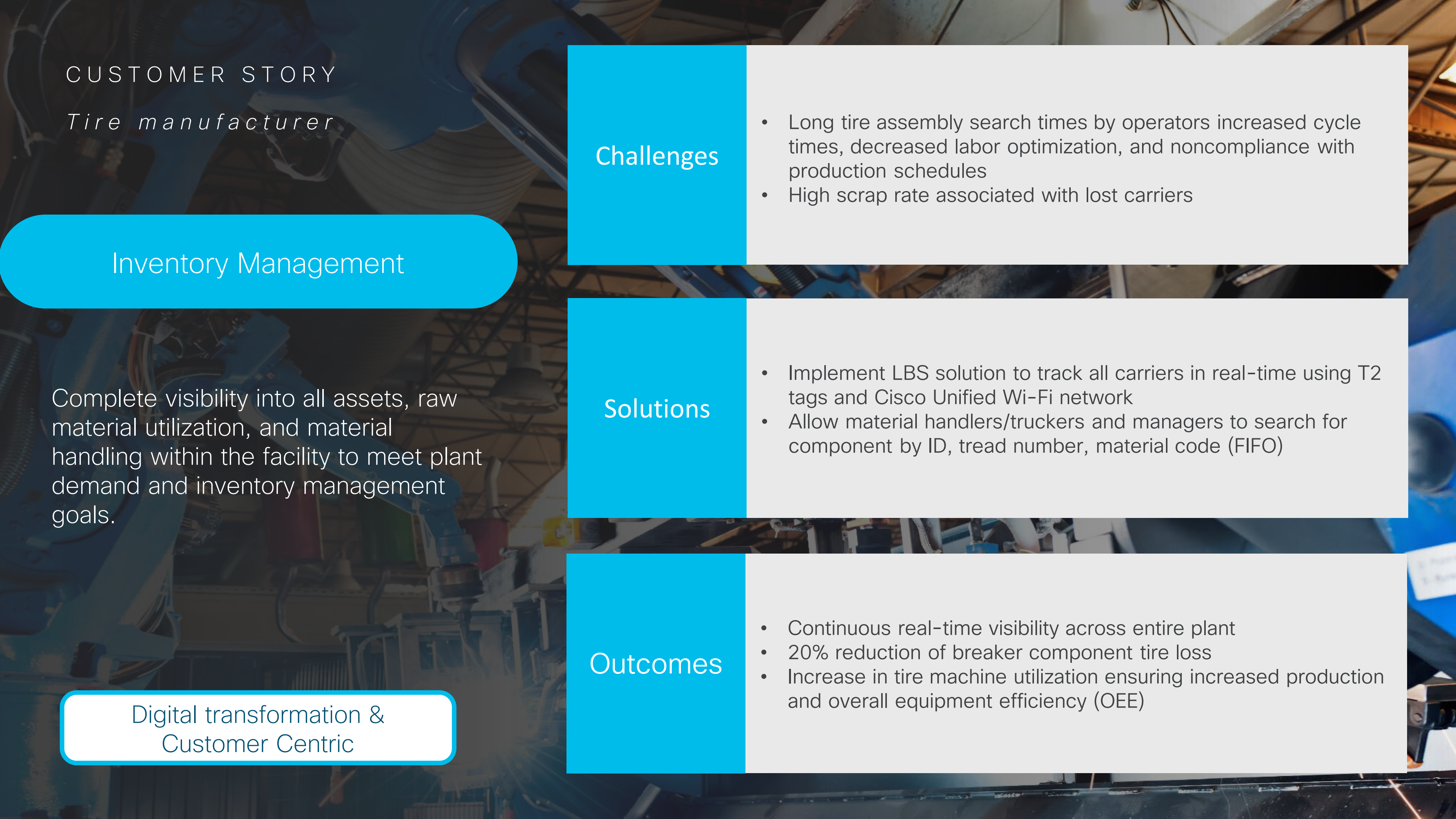
- Pandemic limited travel for training and in-person machinery maintenance and repair
- Downtime threatened to decrease productivity for seven plans located globally
- Needed a single, secure communications platform to call, message, meet, and file share

Solutions

- Webex Teams
- Webex Expert on Demand with RealWear integration
- Webex Teams Integration

Outcomes

- Frontline workers have access to instant help from experts any time, worldwide
- Remarkably increased the speed of first-time fix rates
- Saved on travel costs as well as training and education



CUSTOMER STORY

Tire manufacturer

Inventory Management

Complete visibility into all assets, raw material utilization, and material handling within the facility to meet plant demand and inventory management goals.

Digital transformation & Customer Centric

Challenges

- Long tire assembly search times by operators increased cycle times, decreased labor optimization, and noncompliance with production schedules
- High scrap rate associated with lost carriers

Solutions

- Implement LBS solution to track all carriers in real-time using T2 tags and Cisco Unified Wi-Fi network
- Allow material handlers/truckers and managers to search for component by ID, tread number, material code (FIFO)

Outcomes

- Continuous real-time visibility across entire plant
- 20% reduction of breaker component tire loss
- Increase in tire machine utilization ensuring increased production and overall equipment efficiency (OEE)

GO **BEYOND**