Industrial Cybersecurity

5 Ways to Ensure the Integrity of Your Operations

Yariv Lenchner
Director of Product Management
June 2019
About the Presenter

Yariv Lenchner

- Director of Product Management
- 15 years of Product Management, Product Marketing and System Engineering in ICS and Networking
- Domain expertise across ICS, Security, Enterprise SW and IP Networking

Indegy provides situational awareness and real-time security for industrial control networks to ensure operational continuity and reliability.
Top Industrial Security Concerns

What’s missing in Industrial Control System (ICS) environments?

Top security gaps in an ICS network

1) Understanding what you have in your network
2) Threat Detection in OT environment
3) Blind spots of physical access to devices

To sum up – the 5 Ways
Why We’re Here Today

It’s happening more and more

The attack happened Monday morning and ETP reported a shutdown of the system because of the attack.

Government and Regulation taking notice

In March, U.S. officials issued a warning that Russian hackers were carrying out a broad attack on the nation’s electric grid.

Every infrastructure similarly vulnerable

Similar computer systems like the one at Energy Transfer are used by other pipeline operators including Tallgrass Energy Partners LP and Kinder Morgan Inc.
What Is Critical Infrastructure?

• It’s Not Just Grids.
Threats
To Your Industrial Control Systems

- **CYBER-ATTACK**
  - External targeted attacks
  - Collateral damage

- **MALICIOUS INSIDER**
  - Disgruntled employees
  - Dishonest 3rd Parties

- **HUMAN ERROR**
  - Unintentional mistakes
  - Compromised devices

---

**NOT JUST ABOUT DATA LOSS.**
Should any of these harm your industrial environment, major productivity and reputational damage, as well as loss of life, can result.
The Technical-Mental Gap Between IT and OT

- Data vs Operations
- PCs vs SCADA / DCS
- Standard vs Proprietary
- Secured vs Naïve Devices

“No, you can’t connect to the furnaces from your home”

“No, I can’t just restart the turbine”

Copyright © 2019 Indegy
Top Concerns as an ICS manager

What’s missing in ICS environments?

Top security gaps in an ICS network

1) Understanding what you have in your network
2) Threat Detection in OT environment
3) Blind spots of physical access to devices

To sum up – the 5 Ways
First of all, Is Security the Top Concern?
Or is it strictly the operations & safety aspect?

- How do I ensure my revenue generating process keeps running?
- How quickly will I discover a failure?
- How quickly can I pinpoint the source of the incident?
- How quickly can I recover?

Case Study:
When production is down, loss of revenue = £800 per minute per line
26 production lines - equals £48,000 per hour per line or £1,152,000 per day
Does not include mitigation costs
Vulnerabilities and Gaps
In Your Industrial Network

IT/OT Convergence

No Visibility into OT Networks

Outdated Equipment

Undocumented Protocols

No Configuration Tracking

Invisible Asset Inventory

Mail Server, PC, Firewall, Workstation, Historian, SCADA, DB, Switch, PLC

IT

OT

Indegy
Activates All Your Senses
Top Concerns as an ICS manager
What’s missing in ICS environments?

Top security gaps in an ICS network

1) Understanding what you have in your network
2) Threat Detection in OT environment
3) Blind spots of physical access to devices

To sum up – the 5 Ways
Security Gap #1 – Asset Inventory

Understand

what you have in your network
Implemented a long time ago

Recently inherited
And you know there were lots of changes over the years

No Documentation, Nobody knows anything

Even if there were an accurate list somewhere ...
Asset Discovery and Management

- The details I need:
  - IP / MAC / Serial address
  - OS / Firmware versions
  - When were they last updated? By who?
  - Associated risk of the device
  - List of potential vulnerabilities

- The details are constantly changing over time
  - Usually through a manual process
  - Error prone
  - Documentation-less
Ensure You Have Access to the ICS Data You Need

Manufacturer | Classification | Logged In User | Firmware Version | Software List | Configuration Control | Patch level | Traffic Volumes

**What to do?**

- **Identify**
  Assets communicating in the network

- **Discover**
  Devices which are not active

- **Classify**
  HMI, Historian, Router, PLC, Server, Switch...

- **Collect**
  Patch, Hotfix levels, Firmware, Users, PLC backplane

- **Track**
  Full configuration change control, including devices
Visibility for Risk Management

Continuously collect data from every source:
- Network traffic
- PCs & Servers
- Industrial devices

Analyze configurations, IOCs and threat intel from:

Guide mitigation of risk exposure:
- Pinpoint missing patches
- Risk score guide
- Integration with NAC or FW

Produce comprehensive or summarized reports with:
- Risky Postures Scoring
- Automated Insights
- Advanced Threat Modeling
Security Gap #2
Threat Detection Engines

Behavioral analytics to identify threats

And

Ability to enforce strict and granular policies
Network Behavior Patterns

- We have many elements in the ICS network that present challenges
  - Identifying rogue devices
  - Patterns of communication (ports, protocols, SCADA commands)
  - Malware scans

But some dangerous activities will never rise above the statistical baseline
Reprogramming ICS Devices

Unauthorized controller changes can cause significant damage!

Control Logic:

- If new_temp < MAX_TEMP
  - set furnace_temp = requested_temp
- else
  - ignore
  - Send Error Message

furnace_temp = 1000*MAX_TEMP
Why Anomaly + Policy Is Important

Think 1+1 = 3

Deep Packet Inspection tailored for industrial environments with unparalleled depth of analysis

• Anomaly detection against a baseline
  - Machine learning, no need to define custom policies
  - New device communication patterns
  - Not previously used protocols
  - Spikes in traffic volume and network scans

• Policy analysis of granular activities that don’t rise above the noise
  - Alert on any code/firmware download to a controller from engineering stations
  - Enforce compliance requirements by regulation & change management process
  - Whitelist protocols/commands used to communicate with each device
  - Configure permitted ranges for tags with data plane policies
Security Gap #3
Limitation of “Passive”

Addressing the #1 insider threat

Physical Access
More Food for Thought

The cyber-physical attack

• A cyber attack can happen on-site
• Hackers can physically access remote unmanned locations
• A System Integrator connects directly to controllers
• You need a device integrity module to provide ‘end point’ protection
Hybrid Detection Technology

Passive Monitoring + Querying Capabilities

Query Device Configuration

Analyze Real Time Network Traffic
Top Concerns as an ICS manager

What’s missing in ICS environments?

Top security gaps in an ICS network

1) Understanding what you have in your network
2) Threat Detection in OT environment
3) Blind spots of physical access to devices

To sum up – the 5 Ways
5 Key Areas To Address

- Threat Detection & Mitigation
- Asset Tracking
- Vulnerability Management
- Configuration Control
- Enterprise Visibility
Thank You

For more information, contact us at:

+1 (866) 801 5394  I  indegy.com
1460 Broadway St., New York, NY, 10036, USA
Welcome to SANS ICS Europe 2019 Summit & Training

#SANSICS EUROPE