Value of Anomaly and Threat Detection in Industrial Control Systems

Patrick McBride
Chief Marketing Officer, Claroty
About Myself

- **Current:** Chief Marketing Officer, Claroty
- **Past:** Over 25 Years in Cybersecurity
  (All Seats - Customer, Research Analyst, Vendor)
  - iSIGHT Partners
  - Xceedium
  - META Security Group (Security Consultancy)
  - META Group (Gartner)
  - Travelers Insurance
About Claroty - Our Mission

Secure the safety and reliability of industrial control networks that run the world from cyber attacks
Agenda

- ICS Cyber Risk Summary
- Key ICS Cybersecurity Measures
- How can Anomaly Detection Help?
- Case Study: Triton Chemical Plant Attack
IT

- Designed to be connected
- Updated / replaced regularly
- Designed to be open and collaborative

OT

- Designed to be stand alone
- Lifetime of decades
- Designed to be closed and siloed
An ideal world scenario – “individual islands”

**IT**

“Running the Business”

- Connected to the INTERNET

**OT**

“Managing the Process”

- **DCS**: Safely controls a process during normal operation
- **SIS**: Moves a process to a safe state when an emergency or other abnormal condition occurs

Control

Monitoring & Safe Operation

Process

Not Normally Connected to the Internet
Meanwhile, in the real world…

- Remote Maintenance
- “Shop Floor to Top Floor” KPIs
- ERP Integration
- Predictive Analytics
Very Active ICS Threat Landscape Over Last 18 Months

Aggressive Nation State Activity
(Russia, Iran, North Korea)

“Collateral Damage” Causes Billions in Losses
(WannaCry/NoPetya)

Repeated Warnings DHS/FBI
(energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors)

Advanced Safety System Attacks
(Triton/Triss)
What have we learned?

Threat actors are actively targeting ICS/OT systems

&

You don’t have to be the target to be a victim
Where To Start With ICS Cybersecurity?

Speed (Time to Value)

- Fast
- Slow

Visibility/Monitoring
- Comprehensive

Network Segmentation
- Secure Remote Access
- Vulnerability/Patch Mgmt.
- Advance Endpoint Protection
- Comprehensive Network Segmentation
- Traditional Virus Protection
- Risk Mitigation

Low

High
What can “Anomaly Detection” systems do?

- Provide Visibility into Industrial Networks
- Enhance Asset Management, Compliance, Segmentation
- Provide Threat Detection (malicious and accidental)
- Case Study
Why Visibility? You Can’t Protect What You Can’t See
Visibility - Using Safe/Passive DPI

Level 4: Enterprise Zone (IT Domain)
Level 3: Operations & Control
Level 2: Supervisory Control DCS/SCADA
Level 1: Basic Control
Level 0: Process Device I/O
Automatically Discover Asset Details & Communication Patterns
Understanding “Extreme Visibility”
Continuous Threat Detection

SWITCH SPAN Port

Automatically Discover Assets

Profile All Network Communications

Generate High-Fidelity Baseline Model

Monitor: Anomalies/Changes/Intrusions

Generate Actionable Alerts

Production Mode

Training Mode

Alerts:
Security Threats
Process Integrity Issues
Changes to Environment
New Vulnerabilities

Insights:
Network Hygiene Issues
Known Vulnerabilities (CVEs)

Safely Detect Known and Unknown Threats

Behavior-Based Anomaly/Threat Detection
Behavior-Based Anomaly/Threat Detection

Early Warning | Detect Threats Across Cyber Kill Chain
Actionable Alerts

Clear | Consolidated | Context-Rich Alerts = Reduced Time to Remediate
Continuous Vulnerability Monitoring

Pinpoint Matching of CVEs with ICS Assets

- Curated Feed by Claroty Research Team
- CVEs from different sources (US Cert, ICS Vendors, Threat Intelligence providers...)
- Remediation Steps
Continuous Vulnerability Monitoring

Network Hygiene Issues

- Real-Time detection of network configuration issues
- “Network Hygiene” weaknesses that can leave industrial networks exposed

- **8 assets** have unpatched vulnerabilities
- **170 assets** are communicating with external IPs
- **206 assets** are using unsecured protocols
- **2 assets** have data acquisition write operations performed on them
- **43 assets** are configured with dynamic IP addresses (DHCP)
- **4 assets** are acting as DHCP servers
- **197 assets** are performing DNS queries
Case Study: Triton (aka TriSis/HatMan)

The Basics

- Malware designed to install a Remote Access Trojan (RAT) that allow read/write/execute over SIS in run/remote mode
- Memory-based attack, No payload
- “Very well written”, very few bugs
- 0-day for privilege elevation to read/write the firmware memory
S4 2018: Paul Forney (Schneider Electric) Testimonial
Out-of-the-box reporting

Actionable real-time alerts and intelligence
Modified reporting
What can “Anomaly Detection” systems do?

- Provide Visibility into Industrial Networks
- Enhance Asset Management, Compliance, Segmentation
- Provide Threat Detection (malicious and accidental)
- Case Study
Thank You!

Questions/Comments? patrick.m@claroty.com