



The Emerging Cyber Threats to Industrial Control Systems (ICS) – Supply Chain Cybersecurity Threats

Camilo Gómez

Global Cybersecurity Strategist

YOKOGAWA | Co-Innovating tomorrow

<https://www.yokogawa.com/>

Agenda

- Threat Categorization
 - Indicators of Threat
 - Global Regulation
- End-to-end supply chain security
 - Role of organizations responding to threat
- What is most important
 - Strategies to prepare for, anticipate, and respond
 - Vulnerability Intel

Threat Categorization

Indicators of threat

Impact & Consequence

Headlines



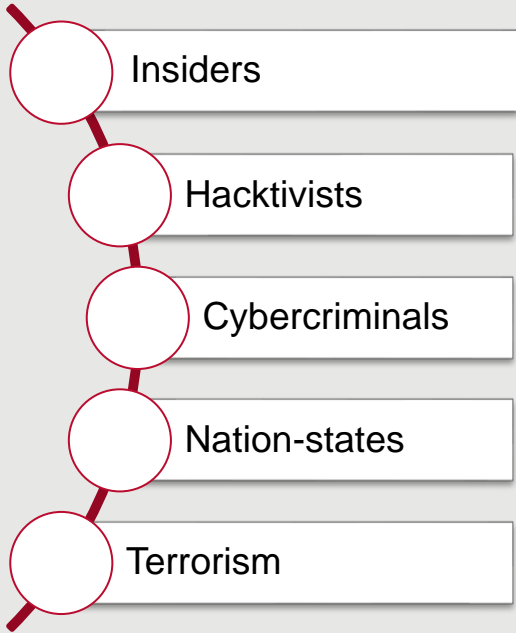
Consequences

- Ukrainian Electric grid (2016)
 - An hour-long blackout
 - 225,000 customers lost power
 - Shut down 1/5 of electric power
- SolarWinds (2020)
 - 100s Millions in reputational impact
 - 1000s organizations compromised
- Colonial Pipeline (2021)
 - Six-day shutdown (100M gallons of fuel/day) -
 - Gasoline, diesel fuel and jet fuel shortage panic
 - Communities, commerce, air travel and nation's security affected
 - Emergency declaration in D.C. and 17 states










Threat attribution

What is under your control?

Threat Agents



Most important

Why	How (the means)	What (the target)
<ul style="list-style-type: none">•Motive•Capability   	<ul style="list-style-type: none">•People•Technology Vulnerability   	<ul style="list-style-type: none">•Impact•Consequences   

Cyber attacks & Vulnerability

Preventable

Evolving attack methods & exploits: technical-flaw vs. backdoor

Vulnerability develops over time

SolarWinds → Supply chain attack

@ Product Supplier

Colonial Pipeline → Ransomware-as-a-Service (RaaS)

@ End User

Ukrainian Grid → CrashOverride

@ End user

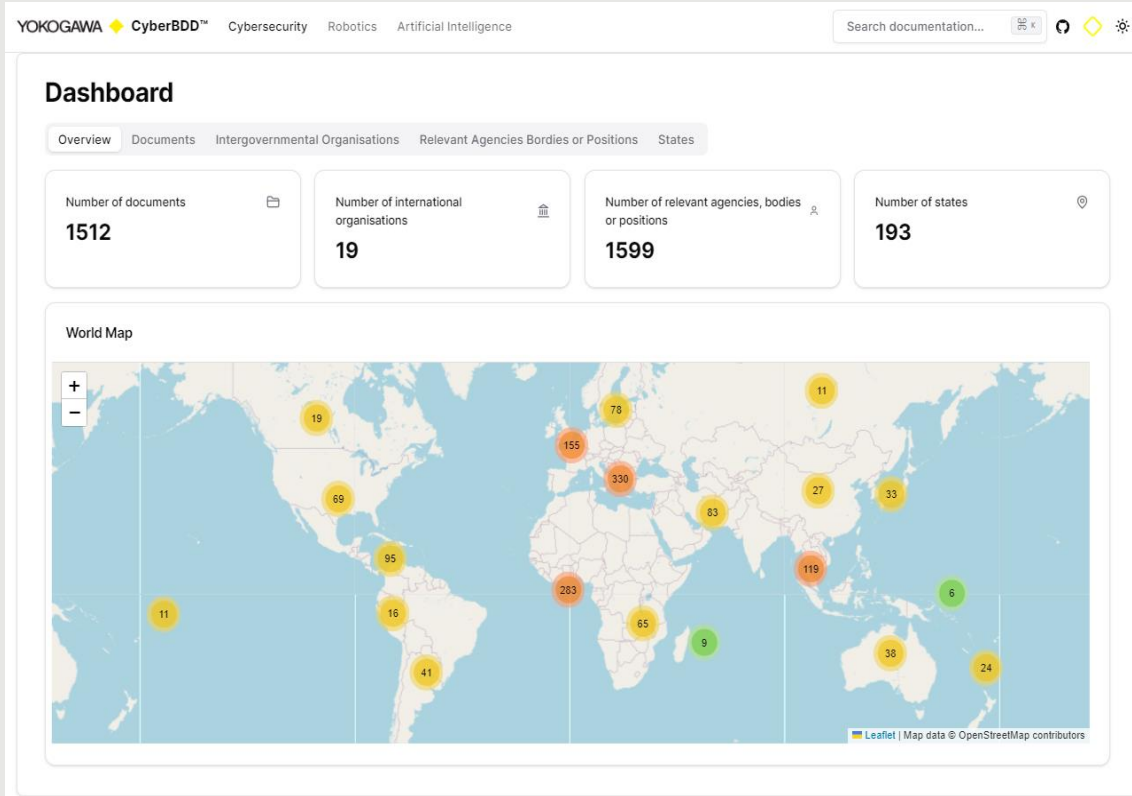
IT

OT



Global Cybersecurity Regulation

Threat is Real



Ranging: 2002 - 2021

Cyber
Crime

+

Data
Protection

Enacted

vs.

Enforced

TSA Pipeline Security Directive

Data Protection

Mandate



Establish and Implement

Cybersecurity Implementation Plan



Develop and Maintain

Cybersecurity Incident Response Plan



Establish

Cybersecurity Assessment Program

Scope

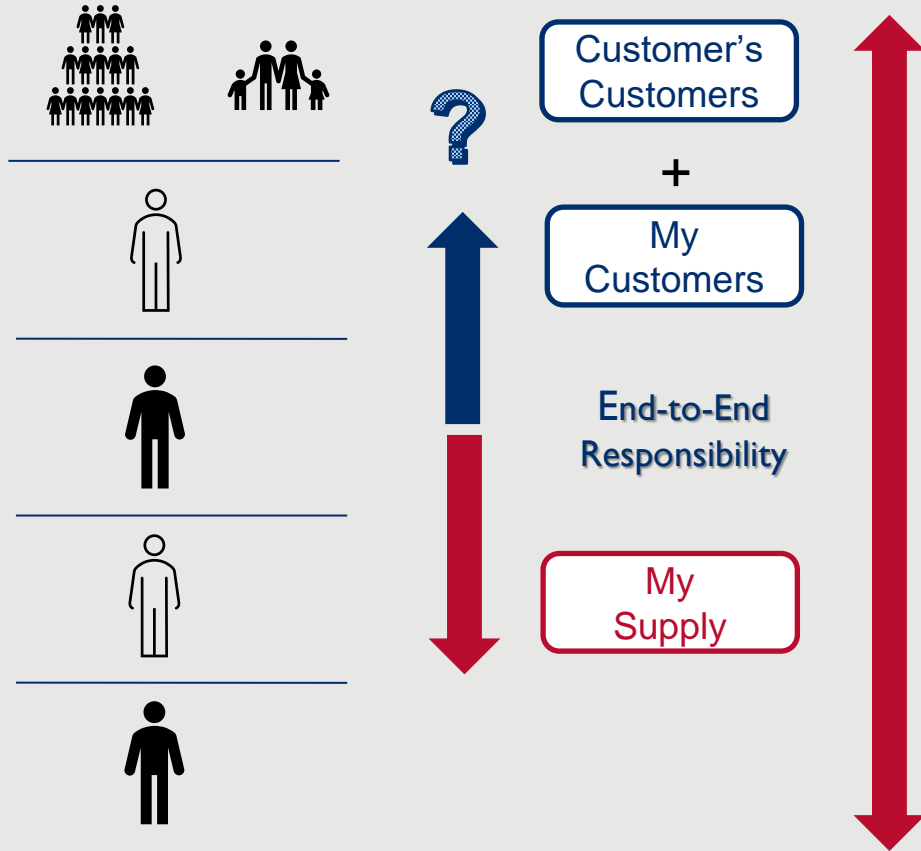
“Any” **IT and OT** system or data that, if compromised or exploited, **could result in operational disruption.**

Including business services that, if compromised or exploited, could result in operational disruption (e.g., billing system)

Supply Chain Cybersecurity

End-to-end supply chain cybersecurity

Persona & Roles

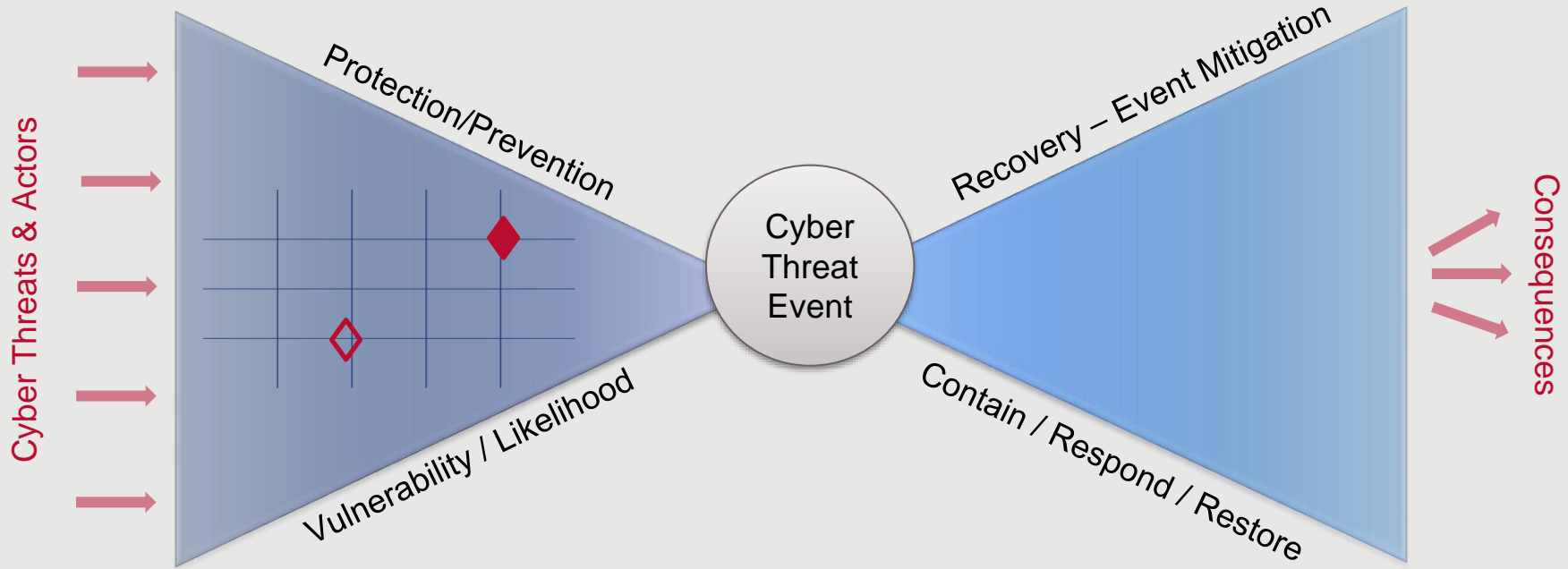


What can you do?

Why	How (the means)	What (the target)
<ul style="list-style-type: none"> •Motive •Capability 	<ul style="list-style-type: none"> •People •Technology Vulnerability 	<ul style="list-style-type: none"> •Impact •Consequences

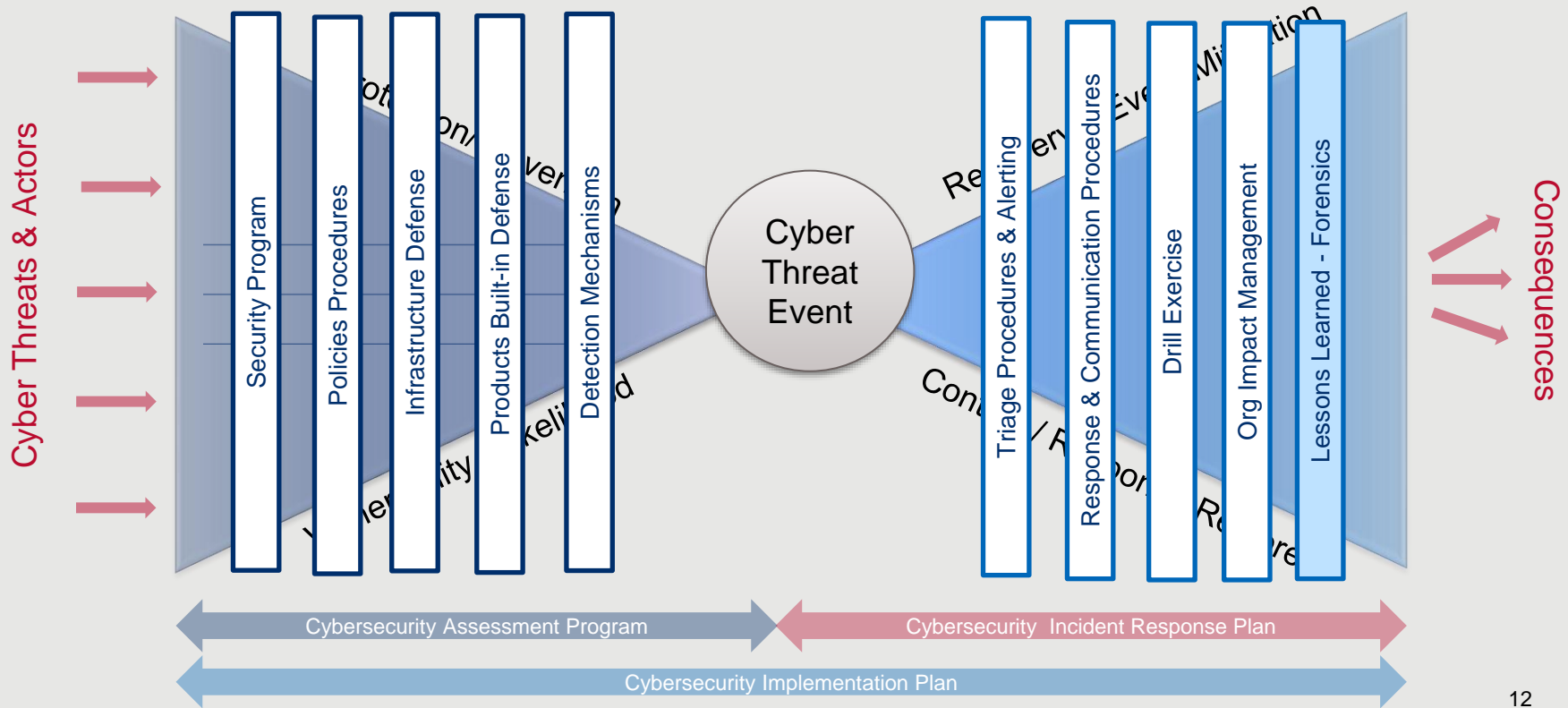
Security Risk Management

Risk Bowtie



Security Risk Management (cont.)

Lessen the Effect



OT & IT Supply Chain Distinctions

Understand

Challenges

- Technology refresh
 - IT: 2-5 years
 - OT: 5+ years
- Typical size of capital projects
 - IT: Millions
 - OT: Multimillion to Billions
- Weight of Budget (IT & OT)
 - Capital project: High
 - Operations: Low
- Built-in Capability of Legacy
 - IT: Somewhat capable
 - OT: Uncapable/Less capable

Strengths

- Standards
 - IT: ISO/IEC 27000
 - OT: ISA/IEC 62443 
- Product Certification
 - IT: Unpopular
 - OT: Prevalent
- Standards Supply Chain Assurance
 - IT: Product
 - OT: Both Product & Product Supplier organization

How to recommendations?

Strategies to prepare for, anticipate, and respond

Best Practices



Standards: ISA/IEC 62443 & Supply-Chain roles

OT Product Security Certification



Asset Owner

- 62443-2-1 Security Program
- 62443-3-1 Security Technologies
- 62443-3-2 Security Risk Assessment



Service Provider

- 62443-2-3 Path Management
- 62443-2-4 Service Providers
- 62443-3-1 Security Technologies



System Integrator

- 62443-2-3 Path Management
- 62443-2-4 Service Providers
- 62443-3-1 Security Technologies
- 62443-3-3 System Security



Product Supplier

- 62443-3-3 System Security
- 62443-4-2 Component Security
- 62443-4-1 Secure product development



Secured-by-design

- Security Capable (Built-in)
- Free of known vulnerabilities



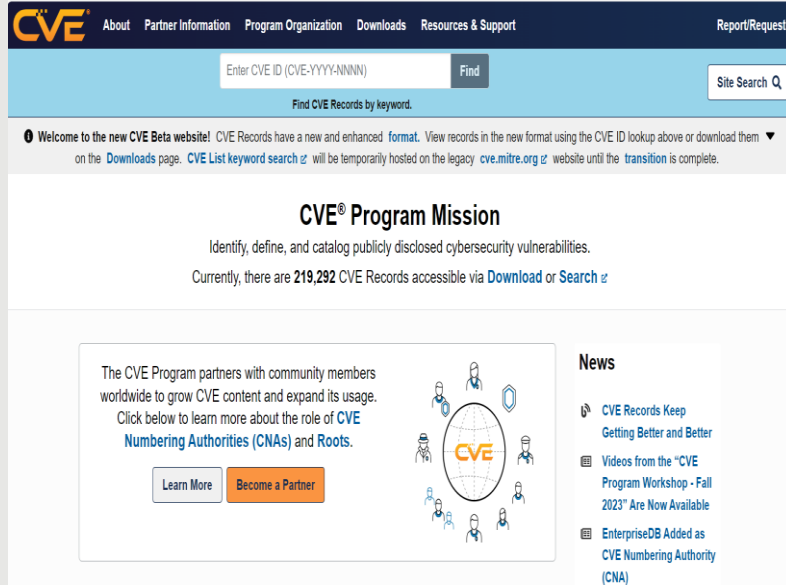
Product Lifecycle

- End-of-life Support
- Built-in Security Capability
- New Vulnerability

Vulnerability Intelligence & Management

For the more technical

IT - CVE



The screenshot shows the CVE website homepage. At the top, there is a navigation bar with links for 'About', 'Partner Information', 'Program Organization', 'Downloads', 'Resources & Support', and 'Report/Request'. Below the navigation bar is a search bar with the text 'Enter CVE ID (CVE-YYYY-NNNN)' and a 'Find' button. To the right of the search bar is a 'Site Search Q' button. Below the search bar, there is a message: 'Welcome to the new CVE Beta website! CVE Records have a new and enhanced format. View records in the new format using the CVE ID lookup above or download them on the Downloads page. CVE List keyword search will be temporarily hosted on the legacy cve.mitre.org website until the transition is complete.' Below this message is the 'CVE® Program Mission' section, which states: 'Identify, define, and catalog publicly disclosed cybersecurity vulnerabilities. Currently, there are 219,292 CVE Records accessible via Download or Search'. Below the mission statement is a 'News' section with a list of items: 'CVE Records Keep Getting Better and Better', 'Videos from the "CVE Program Workshop - Fall 2023" Are Now Available', and 'EnterpriseDB Added as CVE Numbering Authority (CNA)'. To the right of the news section is a 'Become a Partner' button.

Source: www.cve.org

OT - CISA



The screenshot shows the CISA website homepage. At the top, there is a navigation bar with links for 'Topics', 'Spotlight', 'Resources & Tools', 'News & Events', 'Careers', and 'About'. Below the navigation bar is a search bar with the text 'Search' and a search icon. To the right of the search bar is a 'REPORT A CYBER ISSUE' button. Below the search bar is the 'ShieldsUp' section, which states: 'Prepare for, respond to, and mitigate the impact of cyberattacks.' Below the ShieldsUp section is a 'WHITE PAPER' section with the title 'The Case for Memory Safe Roadmaps'. To the right of the white paper section is a 'LEARN MORE' button. Below the white paper section is a 'THE CASE FOR MEMORY SAFE ROADMAPS' section, which states: 'The Case for Memory Safe Roadmaps: Why Both C-Suite Executives and Technical Experts Need to Take Memory Safe Coding Seriously—explains how software manufacturers can eliminate memory safety vulnerabilities by transitioning to memory safe programming languages.' Below this section is another 'LEARN MORE' button.

Source: www.cisa.gov

Vulnerability Intelligence & Management (cont.)

Adversary Behavior

OT & IT – MITRE ATT&CK

What is ATT&CK?

A knowledge base of adversary behavior

- Based on real-world observations
- Free, open, and globally accessible
- A common language
- Community-driven

MITRE

Breaking Down ATT&CK

Tactics: the adversary's technical goals

Techniques: how the goals are achieved

Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Infection	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media			Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearghishing Attachment	Scripting					Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Vendorless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Information
								Program Download	Rootkit	
								System Firmware	Utilize/Change Operating Mode	

Specific Technique Implementation

Example
T883: Sandworm actors exploited vulnerabilities in GE's Cimplicity HMI and Advantech/Broadwin WebAccess HMI software which had been directly exposed to the internet.

MITRE

Source: <https://usea.org/sites/default/files/event-/Otis%20Alexander%20Presentation.pdf>

References

- Resilient Energy Platform: <https://www.nrel.gov/docs/fy20osti/76307.pdf>
- USEA Standards and Best Practices: <https://usea.org/event/cybersecurity-standards-and-best-practices-part-2-utilities-and-isoiec-27001-isms-20052013>
- TSA Pipeline Security Directive: https://www.tsa.gov/sites/default/files/sd_pipeline-2021-01b_05-29-2022.pdf
- ISO 27001: <https://usea.org/event/cybersecurity-standards-and-best-practices-part-2-utilities-and-isoiec-27001-isms-20052013>
- ISA Standards: <https://www.isa.org>
- IEC Standards: <https://www.iec.ch/homepage>
- ISASecure Certification: [ISASecure - IEC 62443 Conformance Certification - Official Site](#)
- IECEE CMC Certification: <https://www.iecee.org/certification/cb-test-certificates>
- CVE: <https://www.cve.org/>
- CISA: <https://www.cisa.gov/>
- MITRE ATT&CK: <https://attack.mitre.org/>

Thank You

YOKOGAWA | Co-Innovating tomorrow
<https://www.yokogawa.com/>