



TOP CYBERSECURITY RISKS FACING WATER & WASTEWATER UTILITIES



Our Speakers



Admiral (Ret.) Michael S. Rogers

Chairman, Board of Advisor



Grant Geyer

Chief Product and Strategy Officer



Andrew Nix

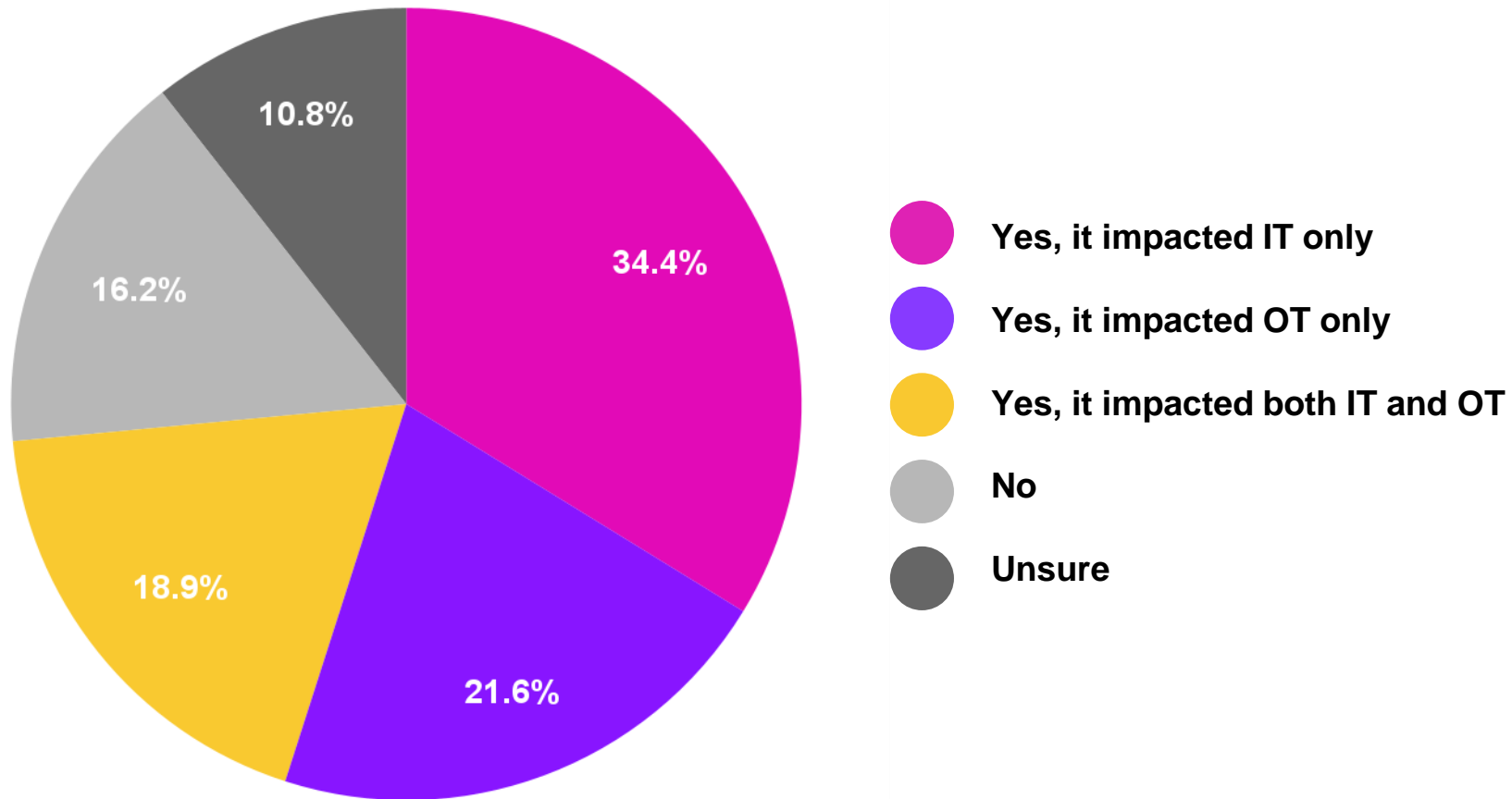
Operational Cybersecurity Solutions
& Services Manager - America



By the Numbers: The State of Water & Wastewater Cybersecurity

Sector Snapshot of Claroty's Global State of Industrial Cybersecurity Survey Report

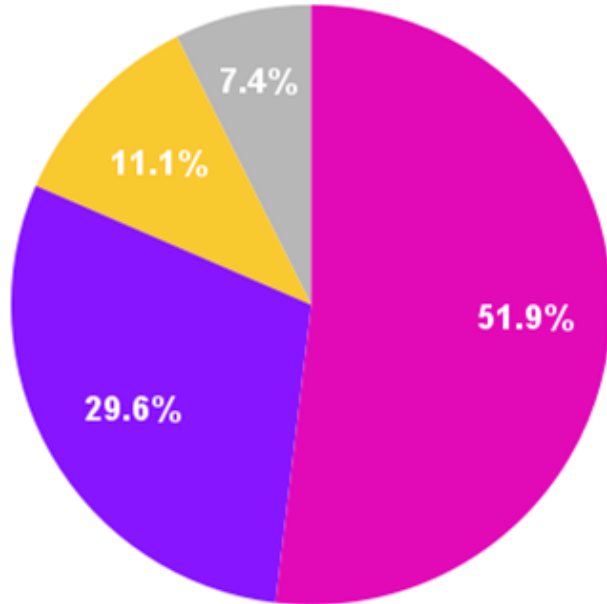
Has your organization experienced a ransomware attack in the past year?



By the Numbers: The State of Water & Wastewater Cybersecurity

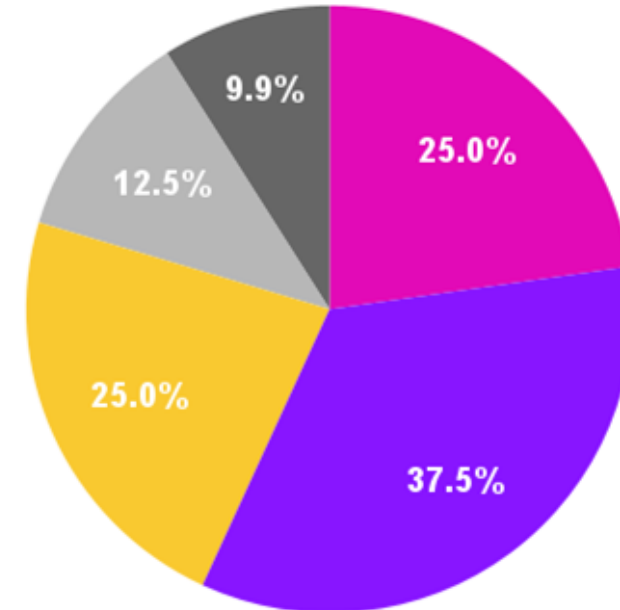
Sector Snapshot of Claroty's Global State of Industrial Cybersecurity Survey Report

What was the scope of impact on operations?



- Partial impact to one site
- Substantial impact to multiple sites for less than a week
- Substantial impact to multiple sites for more than a week
- Minimal impact

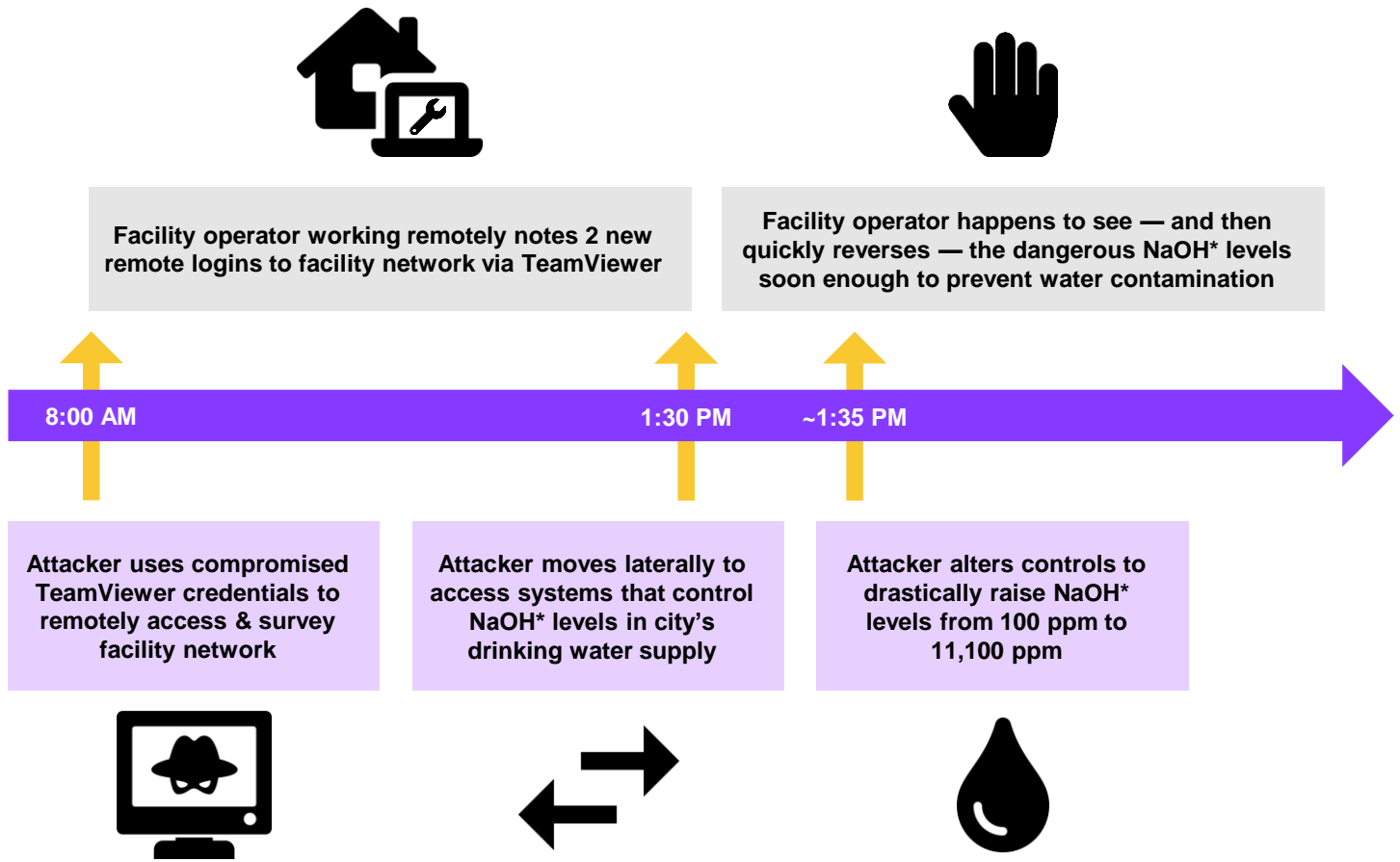
What does downtime cost your organization?



- Less than \$100k USD per hour
- \$100k - \$500k USD per hour
- \$500k - \$1M USD per hour
- \$1M - \$5M USD per hour
- Unsure

Anatomy of the Attack: Oldsmar Water Treatment Facility

Feb. 21' compromise underscores critical implications of sector's OT risk blind spots



Government & Regulatory: Sector Attacks Elicit Robust Response

U.S. EPA, NIST, CISA, and others take action following Oldsmar



CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Alerts and Tips Resources

National Cyber Awareness System > Alerts > Ongoing Cyber Threats to U.S. Water and Wastewater Systems

Alert (AA21-287A)

Ongoing Cyber Threats to U.S. Water and Wastewater Systems

Original release date: October 14, 2021 | Last revised: October 25, 2021

Print Tweet Send Share



EPA United States Environmental Protection Agency

Search EPA.gov

Environmental Topics Laws & Regulations Report a Violation About EPA

News Releases: [Headquarters](#) | [Water \(OW\)](#) CONTACT US

EPA Announces Action Plan to Accelerate Cyber-Resilience for the Water Sector

January 27, 2022


Contact Information
EPA Press Office (press@epa.gov)



BRIEFING ROOM

Fact Sheet: Biden-Harris Administration Expands Public-Private Cybersecurity Partnership to Water Sector

JANUARY 27, 2022 • STATEMENTS AND RELEASES



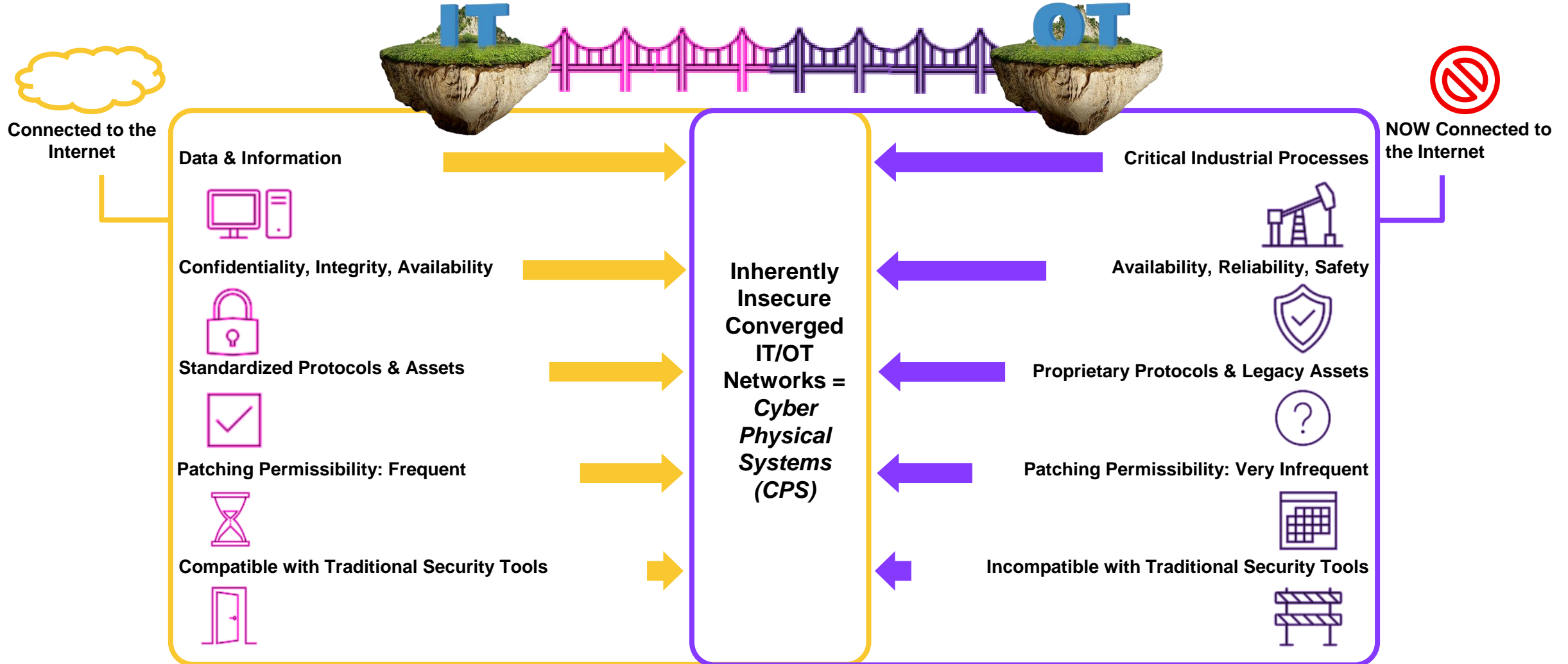
United States Government Accountability Office
Report to Congressional Committees

February 2022

CRITICAL INFRASTRUCTURE PROTECTION

Agencies Need to Assess Adoption of Cybersecurity Guidance

The Present: Cyber-Physical Systems Facing Escalating Risks

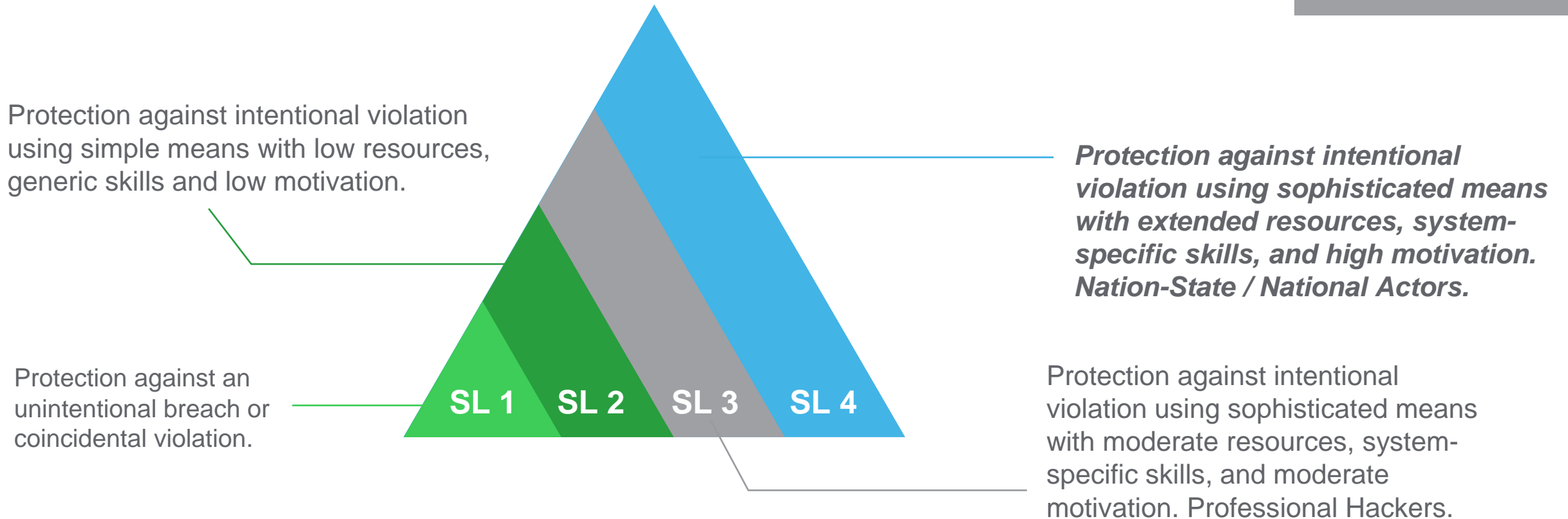


Recommendations

Using Your Standards: IEC 62443 Security Levels

A framework for addressing OT cybersecurity

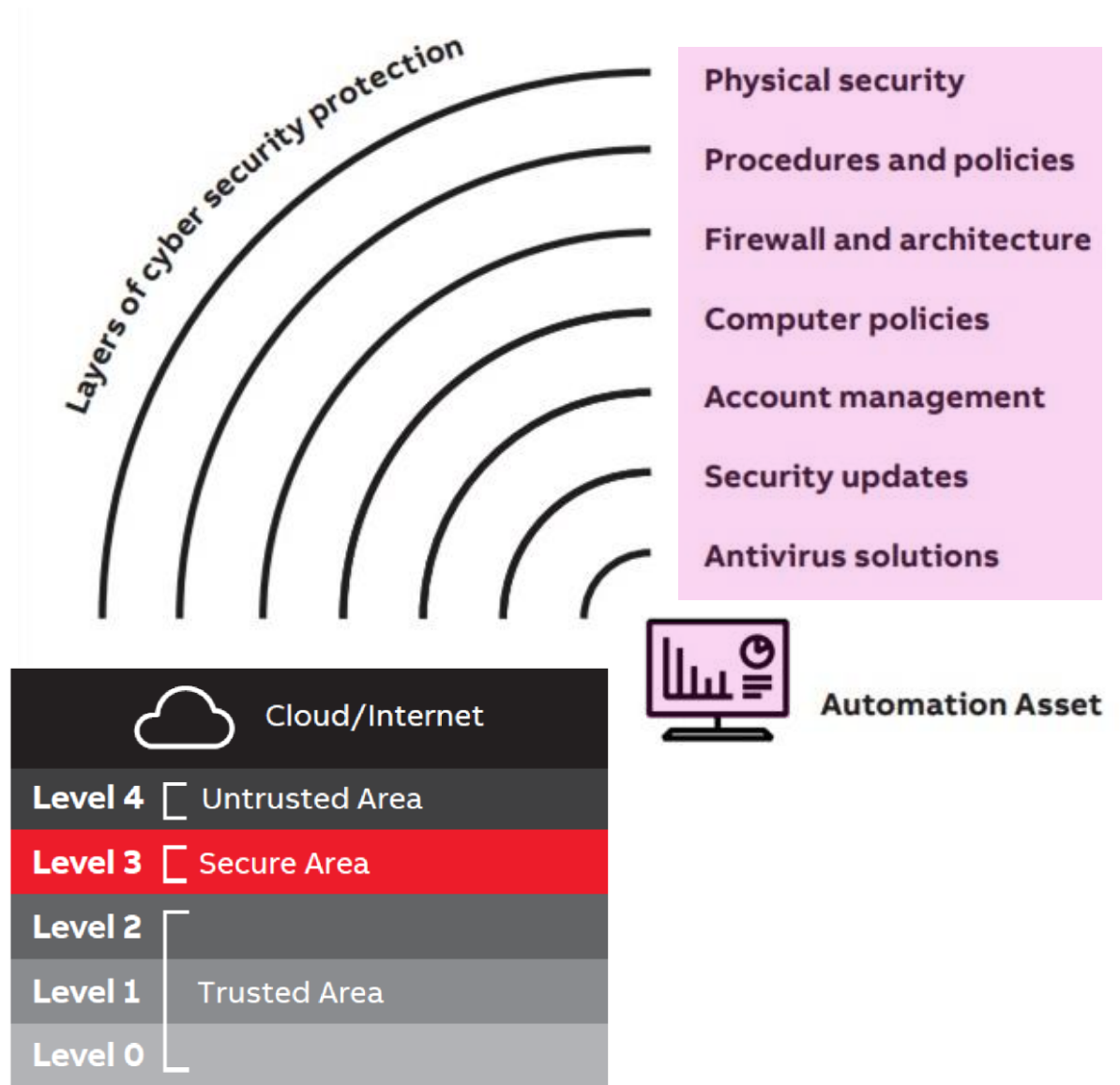
IEC62443-2-4



Water Organizations **MUST** aim for Security Level 4.

How Do I Defend Myself and My Organization?

- Conduct Regular **Cybersecurity Assessments**
- **Segment your OT network** from your IT network using a “Demilitarized Zone” (DMZ)
- Backup your Data (Automatically) – and **secure your backups!**
- Organize your assets into “zones”
- Store any supercritical configurations, source codes, etc.
- Just like a fire drill, **practice your cyber response plan.**
- Training, training, training! (Job Specific)
- Use **at least one** tool from each “Cybersecurity Pillar,” and *keep them up to date.*



Pathway to Cyber Confidence



Utilize your standards:

- IEC 62443, AWWA cyber risk tool provides high-level guidance and goals



Train and enforce a cybersecure culture:

- Go beyond the mandated minimum - role-based cybersecurity workshops



Follow the seven cybersecurity fundamentals for WWW:

- Perform asset inventories
- Assess risks
- Minimize control system exposure
- Enforce user access controls (UAC)
- Safeguard from unauthorized physical access
- Install independent cyber-physical safety systems
- Embrace vulnerability management



It's okay to ask for help:

- Seek insights and support from vendors and managed security services

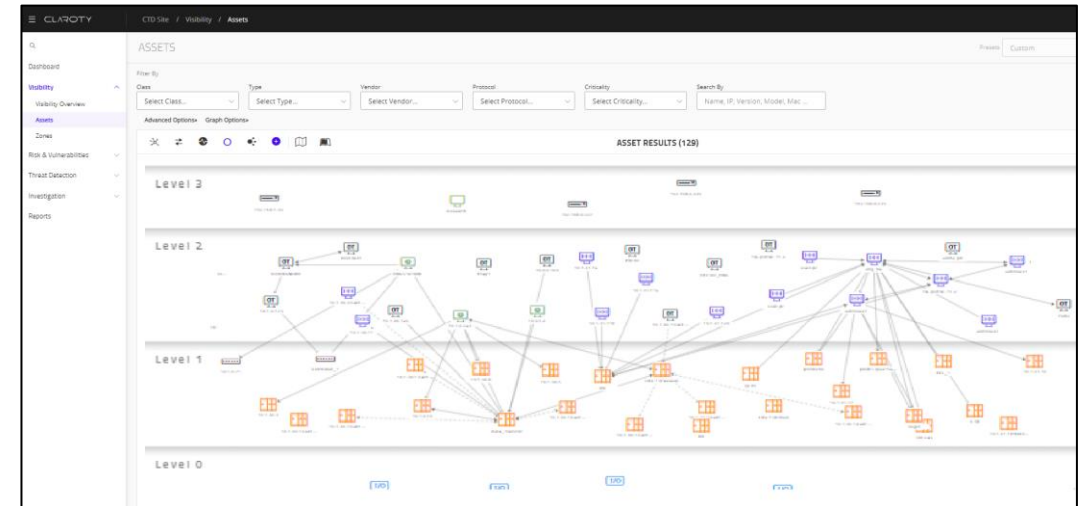
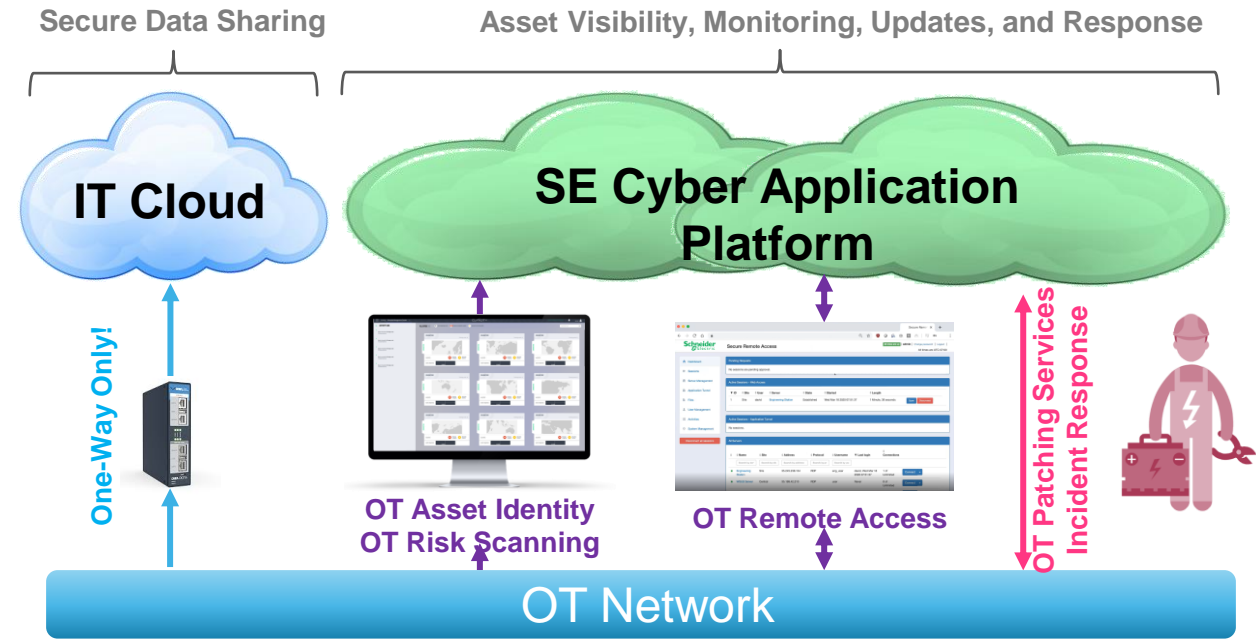


Success Story

Whether big or small, *it's okay* to need cyber help!

• Small Water / Waste Water Entity

- **The CHALLENGE:** How to secure Company's mixed vendor OT environment?
 - Yokogawa PLCs and GE controllers
 - Both Yokogawa and GE have their own Cyber consulting teams, however, only touch their own equipment
 - Cisco is the corporate standard for networking equipment
 - Interested in Anomaly detection, but don't know much about it
- **Solutions Provided:**
 - Assessment identified high priority needs
 - Engineering Svcs, Software, and ongoing Maintenance
 - Global deployment of Continuous Threat Detection platform, Advanced Analysis Services



The Claroty-Schneider Electric Difference for WWW



Be OT Cyber Safe

The Claroty Platform

Smart Water Digital Platform

OT Cybersecurity Services

Automated discovery & complete visibility into all WWWW assets

End-to-end management of all WWWW assets

Optimize WWWW assets & visibility across the lifecycle

Secure remote access to WWWW infrastructure

Remote & optimized WWWW operations

Minimize cybersecurity risks

Full protection & cybersecurity monitoring for WWWW infrastructure

Digital transformation of industrial automation & energy management

Develop Resource Singularity



If you need help with your organization's
Cybersecurity strategy, Let us know!



Q&A



Thank you

