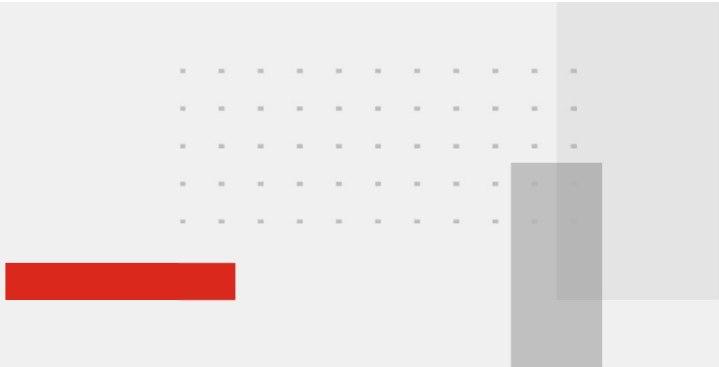




# Cyber Security in Operational Technology

Derek Wyss, Systems Engineer, CCIE#38238, NSE4

September 2024



# Welcome and Agenda

- Industry Trends
- Cybersecurity overview
- Being a human firewall
- Best Practices for Securing SCADA Systems
- Q&A

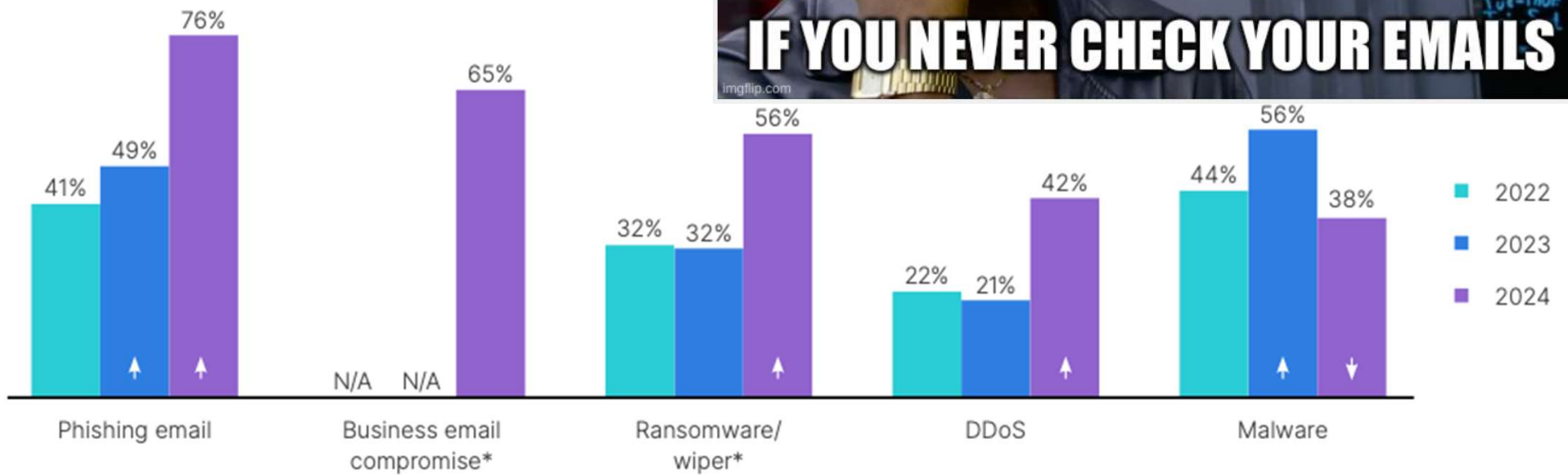
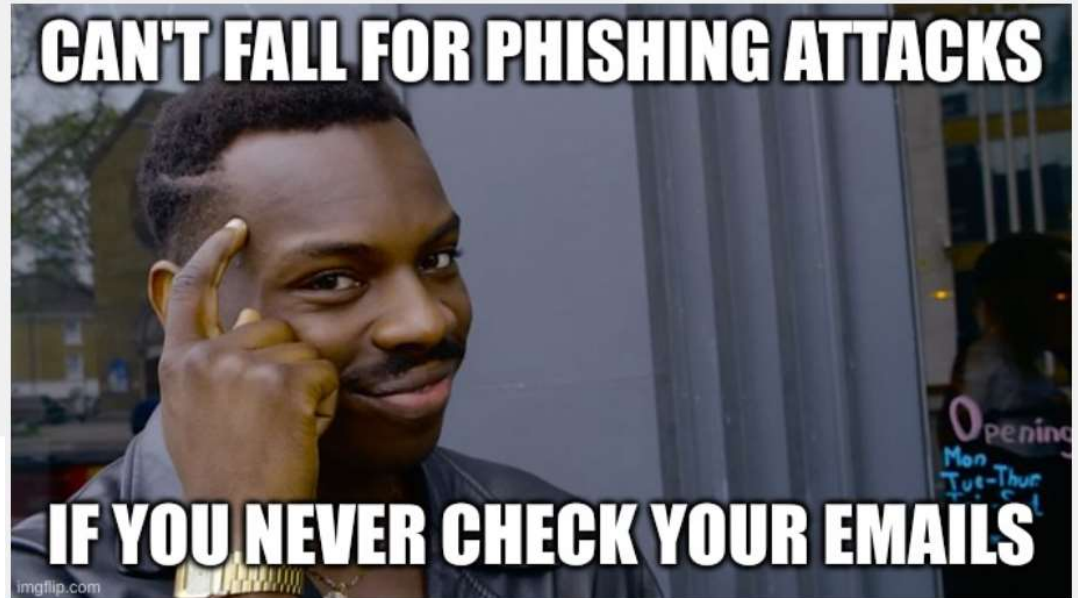


# The impact of intrusions

The negative effects caused by an OT intrusion are also getting worse across the board in all impact categories. More than half of respondents (52%) saw a steep increase in **degradation of brand awareness**, up from only 34% in 2023. **Loss of business-critical data and productivity** was another notable trend (increasing from 34% to 43% year-over-year).

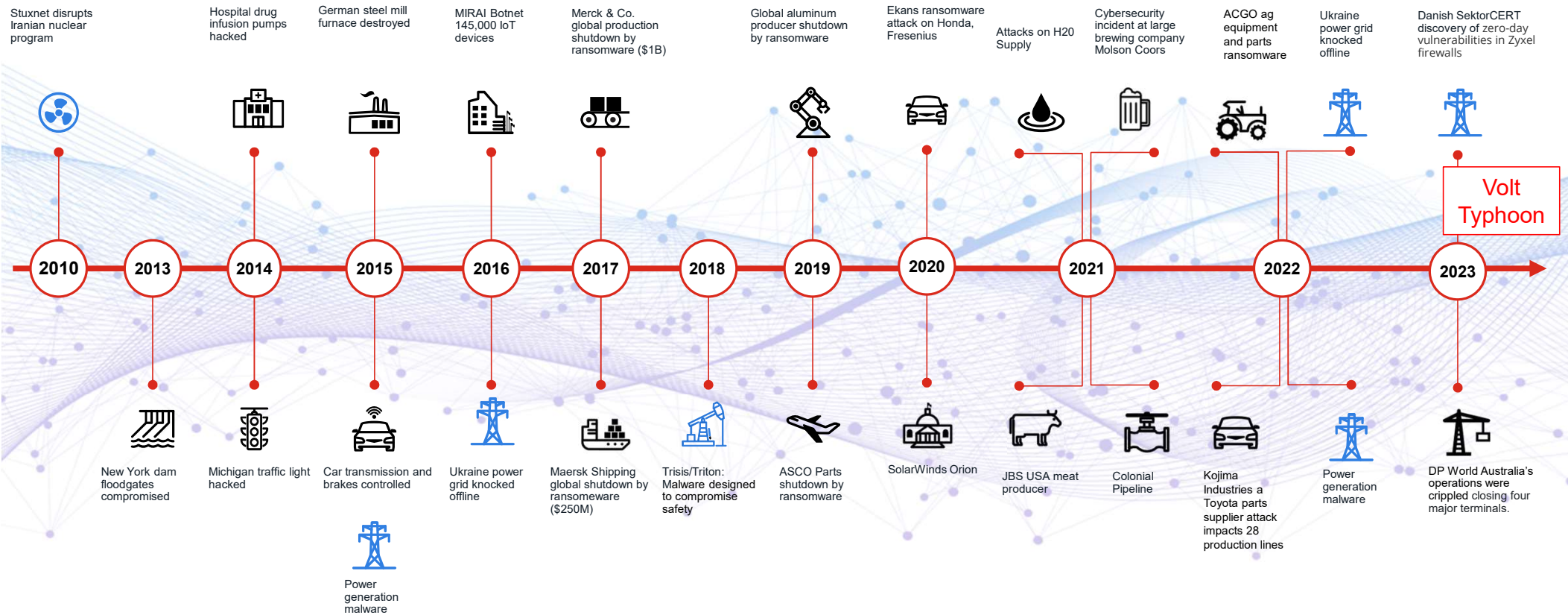


# What types of intrusion are most common in OT?



# OT attacks are getting worse...

Operational Technology incident history at a glance



OT targeted attacks

**CYBER SECURITY  
BUDGET BEFORE A BREACH**



**CYBER SECURITY  
BUDGET AFTER A BREACH**

 caniphish

**What is Cyber Security?**



# Cybersecurity and your safety

- Understanding when and how to share your personal information
- Having too much confidence can be a weakness
  - Accept that you might not know everything
- Think before you click
- Enable two-factor authentication for all critical accounts
- Use different passwords or a password manager for your accounts
- Use strong password phrases
- Keep software up to date
- Back up critical data
- Avoid public WiFi or at least use a VPN while connected
- Know who to contact if something does happen



**People**

**Processes**

**Technology**







# Phishing

- One of the most common attack vectors
- 9 out of 10 cyber attacks are launched using phishing emails
- Game of numbers for bad actors. They send out thousands of emails
- Statistically 1 in 20 people will fall for a phishing email.
- It only takes 1 and then malware can be deployed into the network
- Can be manipulative and very real looking



## How to spot a phishing email

- AI has made phishing attacks even harder to spot
- Personalization has become easier with information about you available online
- Is the message trying to get you to feel fear urgency or excitement
- Is the message trying to get you to take action by clicking a link, entering information, or opening an attachment?
- Do you know the sender, does it seem weird that they sent you this message?
- Were you expecting this message or was this request out of the blue?
- Bad writing, spelling, or grammar?
- Does the message ask for payment or money transfer?



## Phishing email example



**From:** sup00rt@middl!.school1.com  
**To:** KBaptis@middle.school.com  
**Subject:** Urgent: Reset your account

Dear Students ,

Your account has been deactivated due to the annual IT maintenance. We are strongly recommend you to reset your account to avoid missing any information.

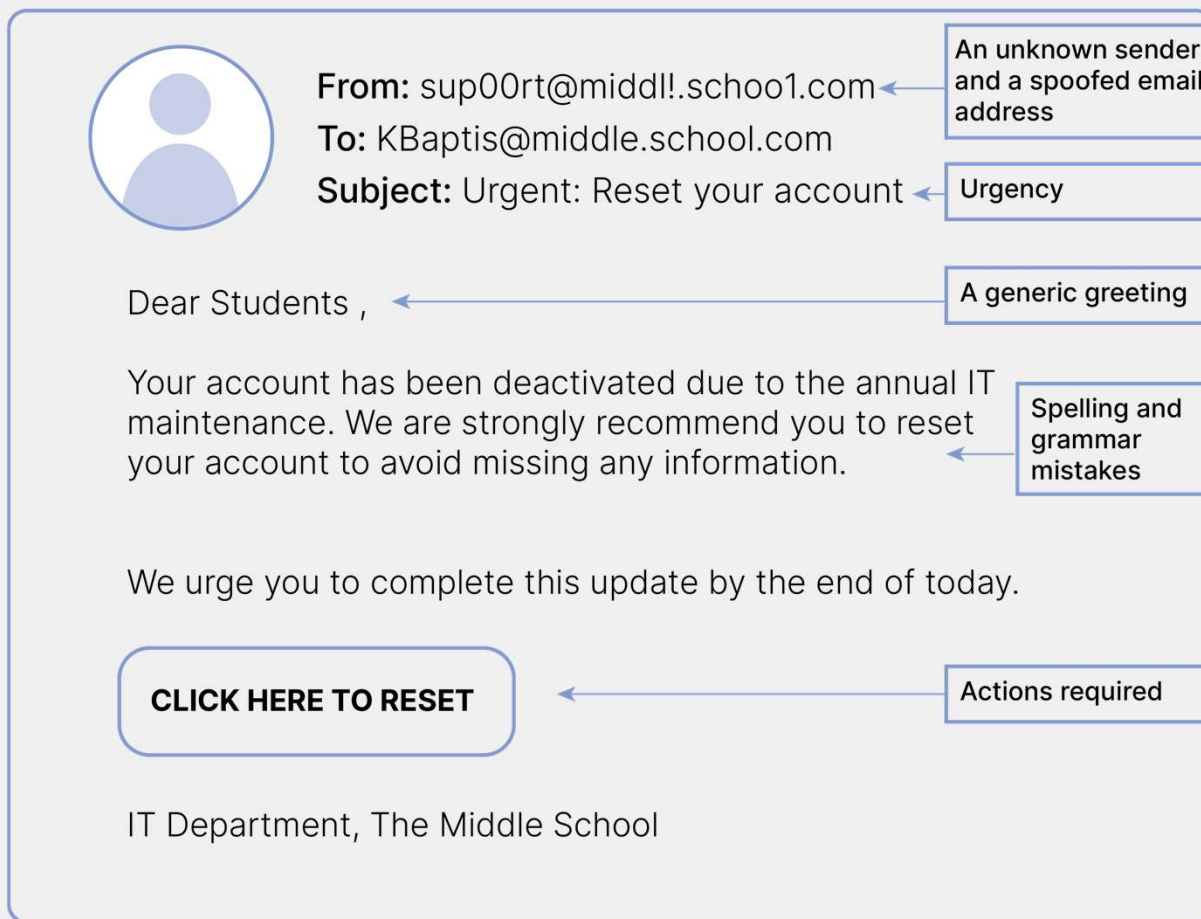
We urge you to complete this update by the end of today.


**CLICK HERE TO RESET**

IT Department, The Middle School



# Answers



 **From:** sup00rt@middl!.school1.com ← **An unknown sender and a spoofed email address**

**To:** KBaptis@middle.school.com

**Subject:** Urgent: Reset your account ← **Urgency**

Dear Students , ← **A generic greeting**

Your account has been deactivated due to the annual IT maintenance. We are strongly recommend you to reset your account to avoid missing any information. ← **Spelling and grammar mistakes**

We urge you to complete this update by the end of today.

**CLICK HERE TO RESET** ← **Actions required**

IT Department, The Middle School



# Malware

- Malicious Software
  - Program that runs on your devices and is meant to cause you harm
  - Spy on your activities
  - Expose your data
  - Trick you into giving away private information
  - Disrupt how your devices work
  - Spread to other devices
- Types of Malware
  - 350k new variants discovered every day
  - Trojan aka – Troy Trojan horse used by the Greeks. Installing a backdoor
  - Spyware gain info on you to steal/sell, or use to access your accounts
  - Worm – Make copies of itself and spreading to other devices
  - Ransomware – Encrypts your data and requests \$ to unlock



## Reminders! How to avoid phishing & malware

- Be smart and stay cautious online
- Don't click suspicious links
- Have AV installed
- Practice good password hygiene
  - all accounts use strong unique passwords
- Use VPN on public wifi
- Backup critical data



# Water and Wastewater Cybersecurity Principles



## Safety & Operations First

Safety-critical and operational-critical functions needs the highest protection



## Cohesive, Purpose-based Zoning

Zones impose security service requirements to the functions/devices/components



## Asset Assumed Vulnerable

Field digitalization will rise exponentially



# Basic Principles of the Cybersecurity Solution



## Protect Users

Security at the Edge to protect and secure all the infrastructure that runs the system from back office to laptops, SCADA and operators



## Protect the Network

Protect and secure all communication equipment from sensors to PLCs



## Protect the Servers

Protect and secure everything that serves employees and facilities





# Consequences

What happens if Water and Wastewater public providers do not act:



A Regional or National  
Emergency



Service Disruption



Customer Harm



Economic Impact

---

# Negative Media Exposure



# OT Security Focus Areas

Best Practices to Guide Strategy

## Asset Management

- Include offsite or remote devices
- Discover and profile OT devices
- Identify high and critical vulnerabilities (Virtual Patching)
- OT Protocol visibility (Modbus, DNP3, Ethernet IP)

## OT Network Segmentation

- Enabled secure communications through DMZ
- North-South network traffic monitoring and threat inspection (Inter VLAN)
- East-West traffic monitoring (intra VLAN inspect)

## Endpoint Security

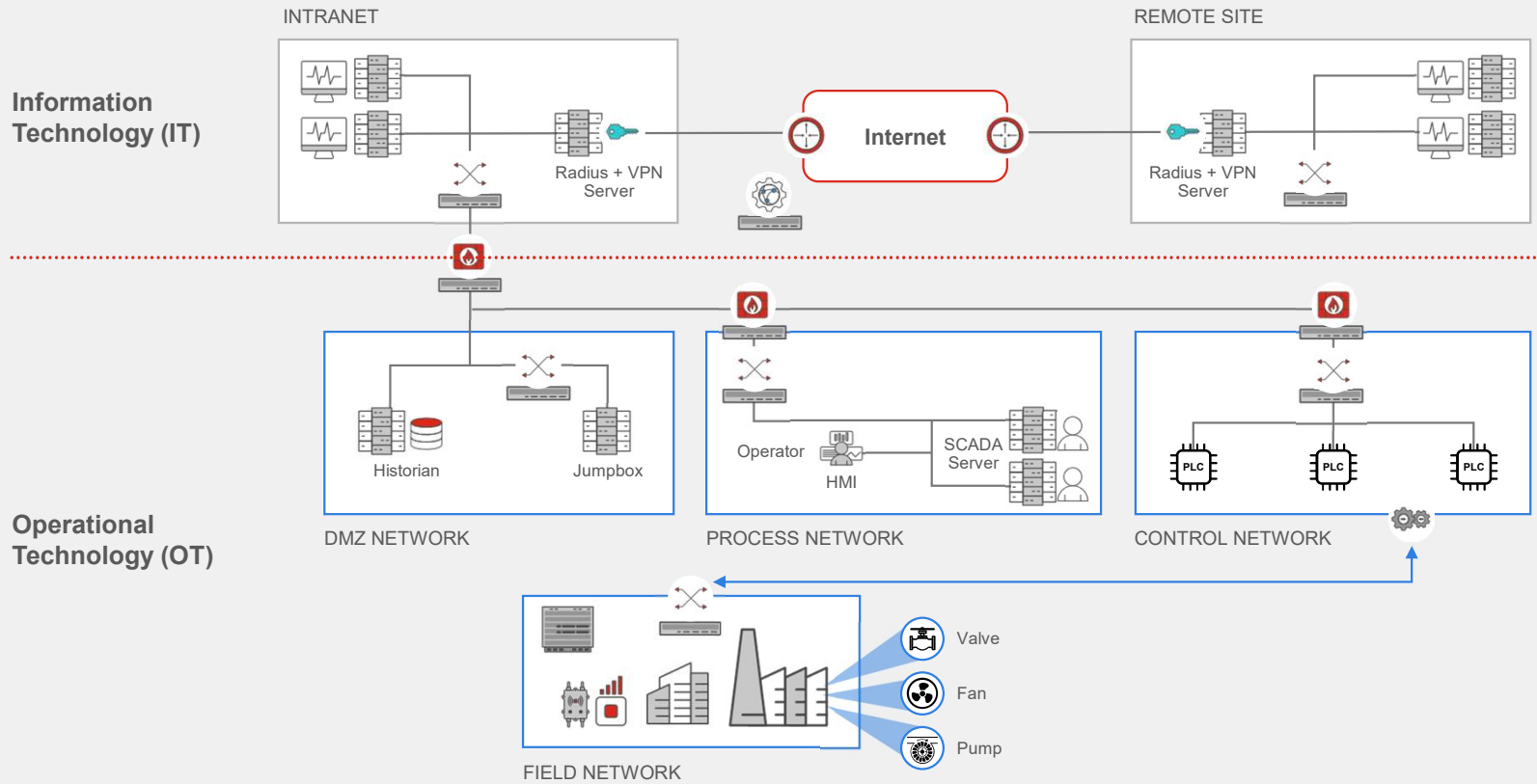
- Endpoint Detection & Response Solution
- Malware and Viruses Detection
- OT Application Whitelisting (Historian, SCADA, HMI)
- Integration with Incident Response
- Support Legacy & Modern Operating Systems (XP)

## Secure Remote Access

- Enable MFA and Role Based Access Control
- Provide access to required devices only
- Session Management (Start/Stop), MFA, Password Management, session recording and secure file transfer



# What and Where are IT and OT Networks?



# Funding for Cyber Resilience and Protection

- Clean Water State Revolving Fund (CWSRF) | US EPA
- Drinking Water State Revolving Fund (DWSRF) | US EPA
- State and Local Cybersecurity Grant Program (SLCGP) | CISA
- WaterSMART | USBR

**Over \$3B amongst these four programs**





**FORTINET®**

# Grants Support Program

Bringing Technology Funding Home for Public Sector Agencies

Get Started by emailing  
**[SLED@Fortinet.com](mailto:SLED@Fortinet.com)**



# Get the Report



Sponsored by



## 2024 Cybersecurity in Water Management Facilities Report

Addressing the growing  
threat of cyberattacks on  
America's water supply  
and wastewater utilities



# Q&A

