Cyber Attack Scenarios

WATER & WASTEWATER

Rowan Macfarlane
Principle Industrial Consultant

AGENDA

1 Threat landscape

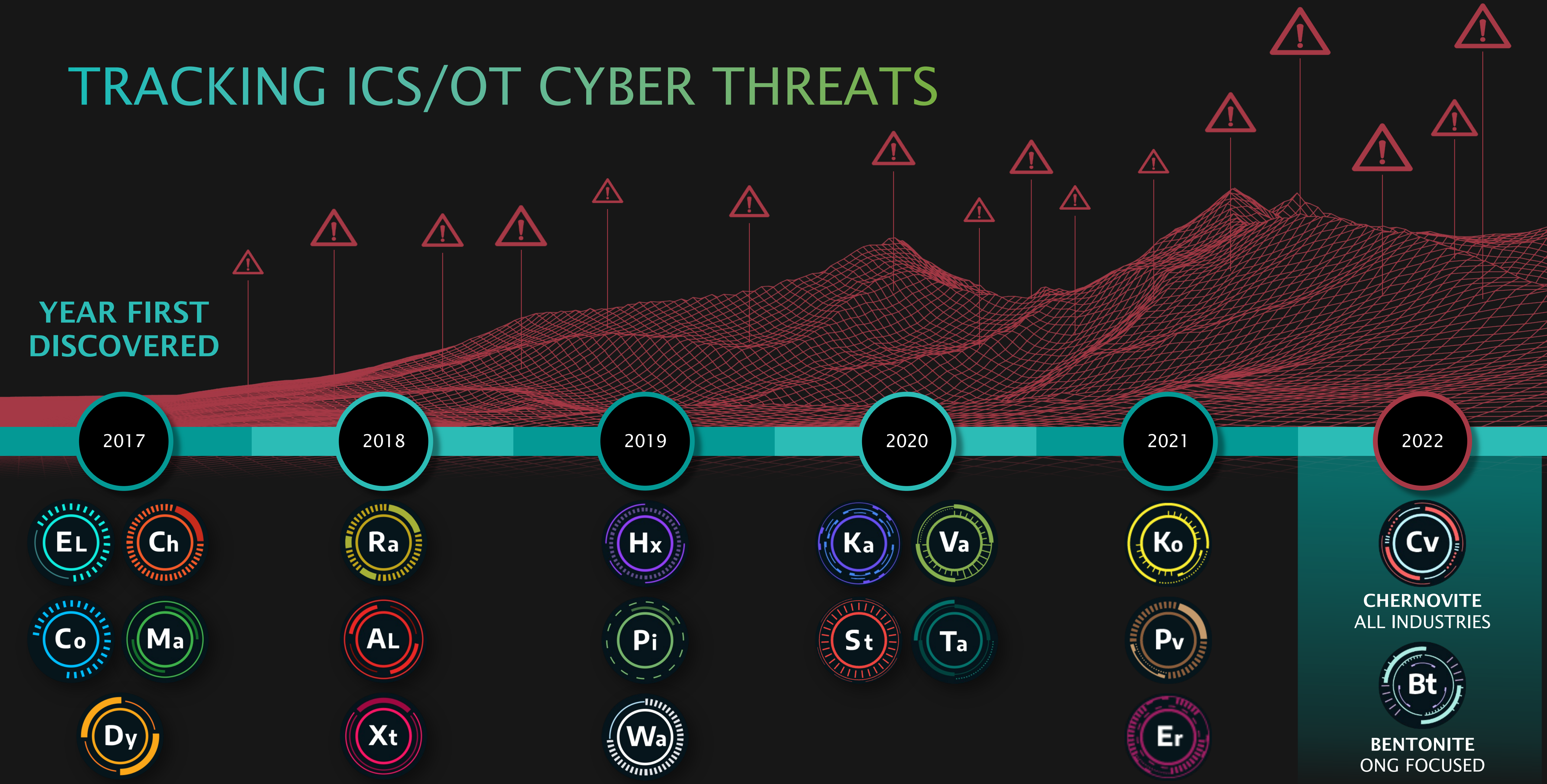
2 SOCI Act

3 Five Critical Controls

4 Defending against common attacks

5 OT-CERT

TRACKING ICS/OT CYBER THREATS



YEAR FIRST DISCOVERED

2017

2018

2019

2020

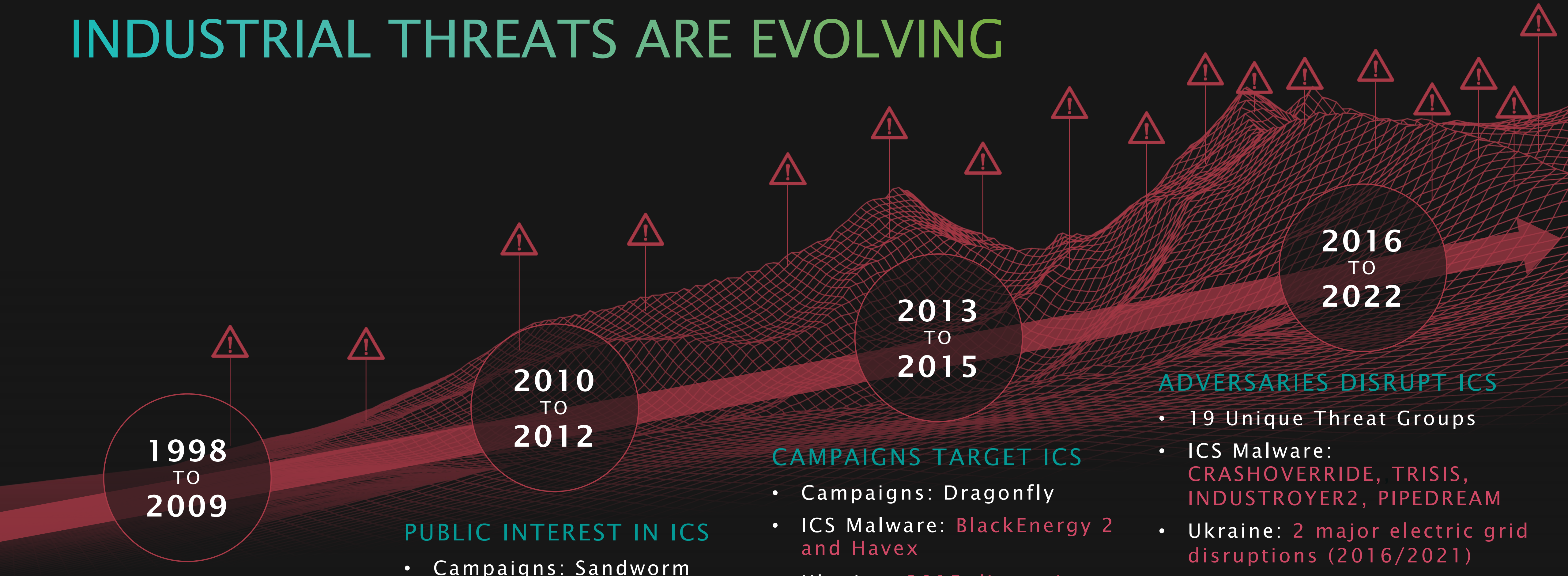
2021

2022

CHERNOVITE
ALL INDUSTRIES

BENTONITE
ONG FOCUSED

INDUSTRIAL THREATS ARE EVOLVING



1998 TO 2009

LACK OF COLLECTION

- Campaigns: APT1
- ICS Malware: None

2010 TO 2012

PUBLIC INTEREST IN ICS

- Campaigns: Sandworm
- ICS Malware: Stuxnet

2013 TO 2015

CAMPAIGNS TARGET ICS

- Campaigns: Dragonfly
- ICS Malware: BlackEnergy 2 and Havex
- Ukraine: 2015 disruption of electric power operations
- Germany: first attack to cause physical destruction on civilian infrastructure (steel)

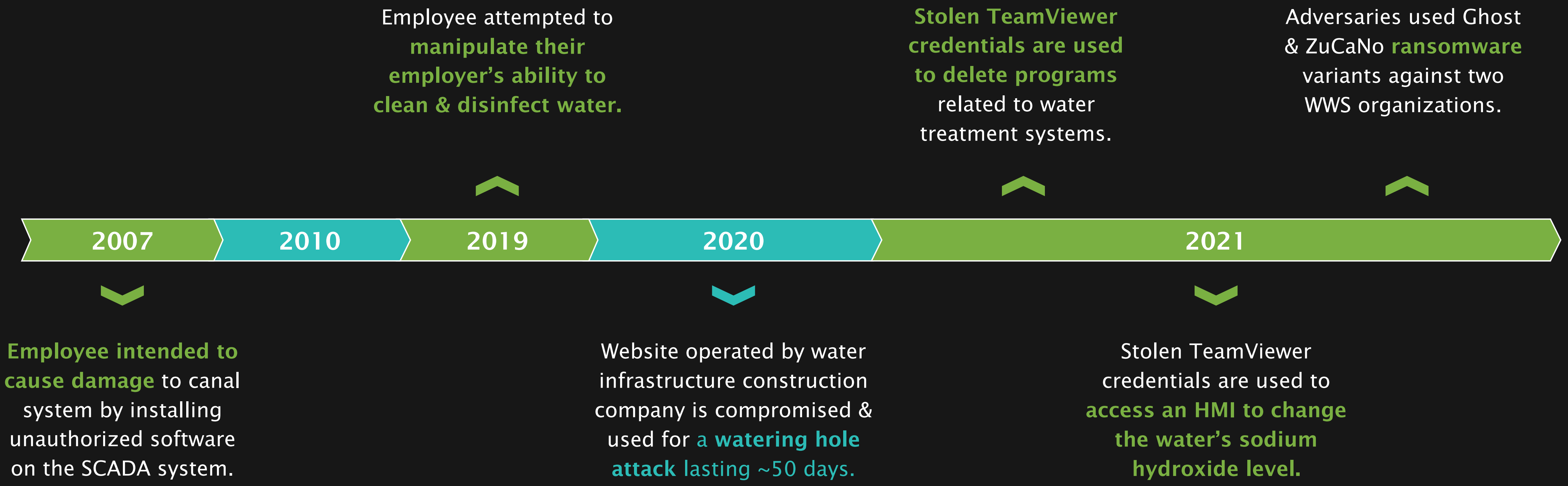
2016 TO 2022

ADVERSARIES DISRUPT ICS

- 19 Unique Threat Groups
- ICS Malware: CRASHOVERRIDE, TRISIS, INDUSTROYER2, PIPEDREAM
- Ukraine: 2 major electric grid disruptions (2016/2021)
- Saudi Arabia: first attack targeting human life (2017)
- Oldsmar, FL: Water Treatment attack
- Ransomware attacks: Colonial Pipeline, JBS Foods, Norsk Hydro

WATER & WASTEWATER CYBER EVENTS

BETWEEN 2006 AND 2023, THERE HAVE ONLY BEEN 27 PUBLICLY DISCLOSED CYBER EVENTS WITHIN THE WATER & WASTEWATER SECTOR IN THE U.S.



2007: **Employee intended to cause damage** to canal system by installing unauthorized software on the SCADA system.

2019: Employee attempted to **manipulate their employer's ability to clean & disinfect water.**

2020: Website operated by water infrastructure construction company is compromised & used for a **watering hole attack** lasting ~50 days.

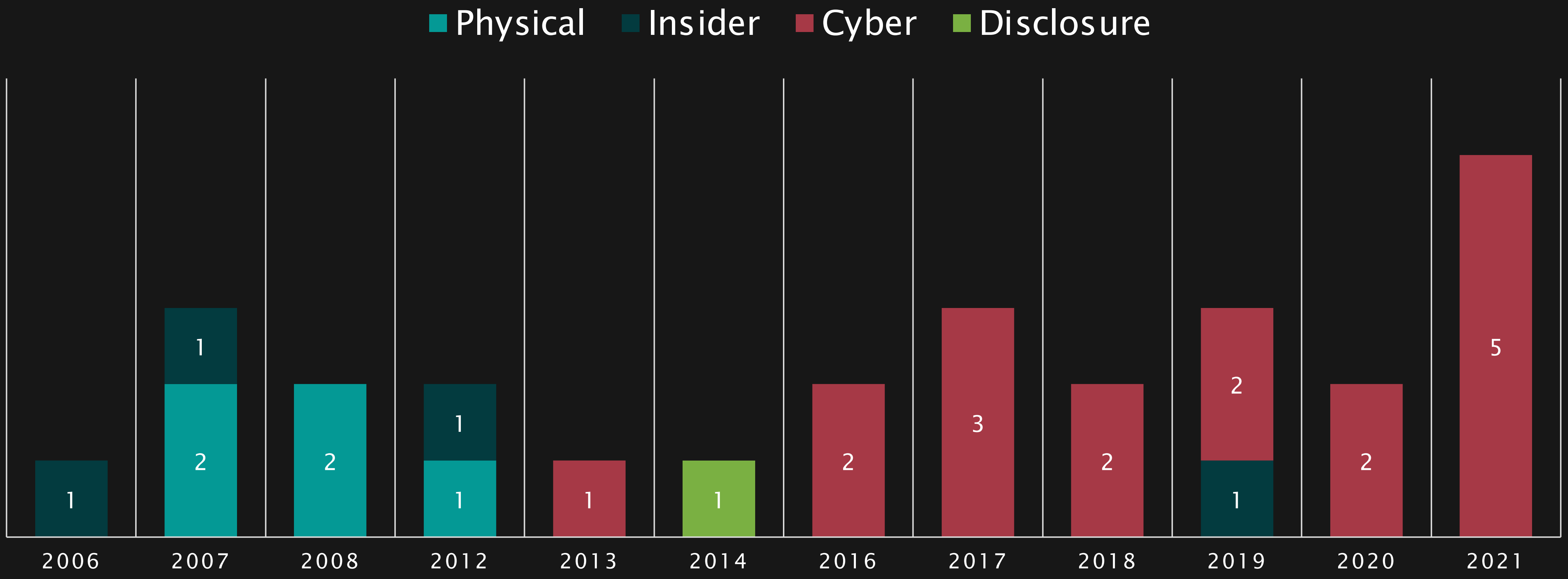
2021: **Stolen TeamViewer credentials are used to delete programs** related to water treatment systems.

2021: Stolen TeamViewer credentials are used to **access an HMI to change the water's sodium hydroxide level.**

2021: Adversaries used Ghost & ZuCaNo **ransomware** variants against two WWS organizations.

STEADY SHIFT TO CYBER THREATS

DIGITAL CONNECTIVITY CONVERGES WITH INCREASED RISK IN THE WATER & WASTEWATER SECTOR



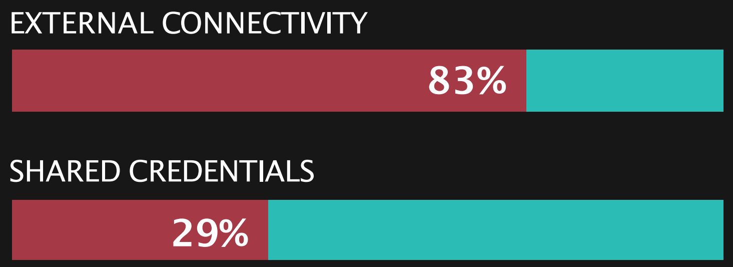
DRAGOS

EXPOSED ICS/OT ASSETS

INTERNET EXPOSED ASSETS & REMOTE ACCESS DEVICES ARE COMMONLY USED FOR INITIAL ACCESS.

Default or weak credentials on ICS/OT devices increases the risk of exposure & compromise.

BASED ON DRAGOS PROFESSIONAL SERVICES ENGAGEMENTS FOR THE WWS SECTOR IN 2022:



Bt

Exploits vulnerabilities in internet-facing assets for espionage, long-term persistence, & interactive operations.

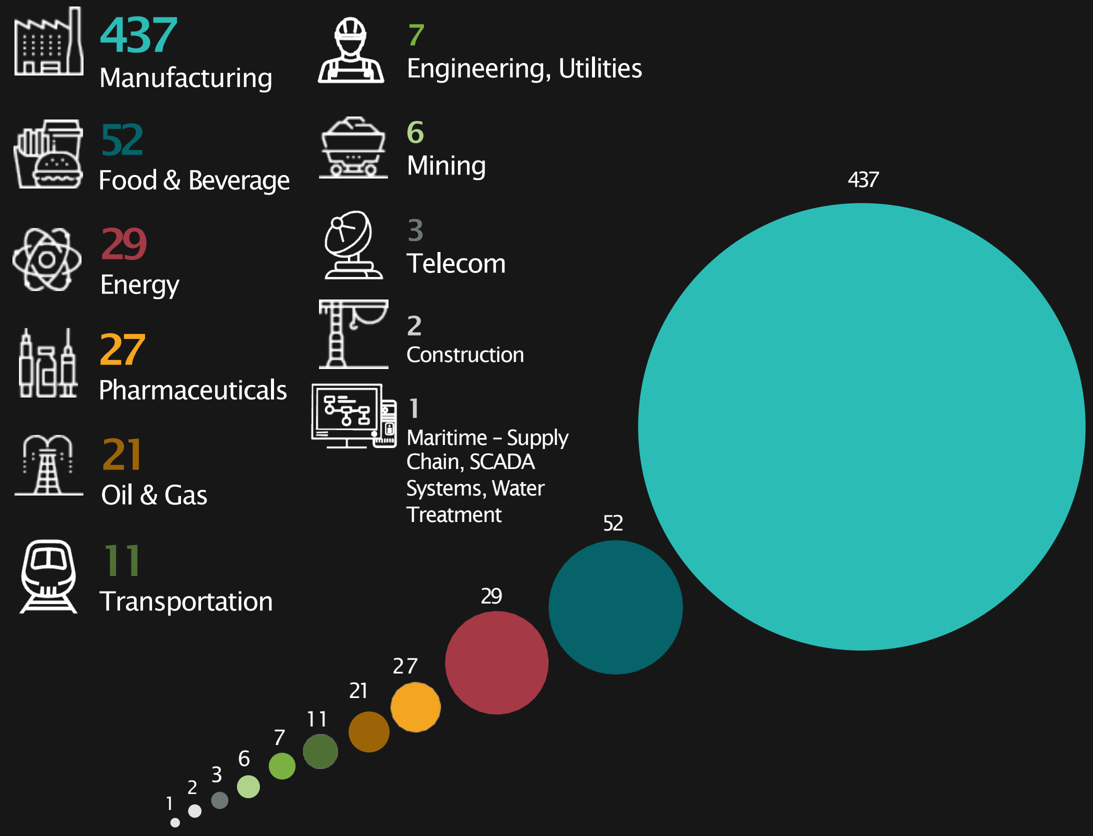
Ko

Compromises internet-exposed remote access devices. Capable of initial access to ICS/OT.

Ka

Exploits vulnerabilities in firewall & router devices. Has facilitated the execution of ICS/OT impact.

RANSOMWARE ATTACKS INCREASED BY 87%



Ransomware Attacks by ICS Sector

437	Manufacturing
52	Food & Beverage
29	Energy
27	Pharmaceuticals
21	Oil & Gas
11	Transportation
7	Engineering, Utilities
6	Mining
3	Telecom
2	Construction
1	Maritime – Supply Chain, SCADA Systems, Water Treatment

October 2022

Data exfiltration of transmission data and Critical Energy/Electric Infrastructure Information (CEII) from a global engineering firm. No known outages.

February 2023

During Royal ransomware attack, adversaries likely navigated to ICS/OT environment before detonating ransomware at a US-based energy company.

February 2023

Black Basta ransomware shut down operations of a food manufacturing company, with evidence of significant data exfiltration.

Security of Critical Infrastructure (SOCI) ACT

Water & Wastewater:

- Register your critical asset(s)
- Report cyber incidents
- Government intervention*
- Risk management program**

Enhanced Cyber Security Obligations***:

- Incident response plans
- Exercises
- Vulnerability assessments
- Provide system information

* during an active incident which has a material impact to society
** enforced from 18th July, supply 'annual report' at end of FY24
*** only applicable to 'Systems of National Significance' (SoNS)

FIVE CRITICAL CONTROLS

SANS

5 THE FIVE ICS CYBER SECURITY CRITICAL CONTROLS

01
ICS Incident Response Plan

02
Defensible Architecture

03
ICS Network Monitoring Visibility

04
Secure Remote Access

05
Risk-based Vulnerability Management

FIVE CRITICAL CONTROLS

SANS

5 THE FIVE ICS CYBER SECURITY CRITICAL CONTROLS

01
ICS Incident Response Plan — ECSO

02
Defensible Architecture — SOCI, ECSO

03
ICS Network Monitoring Visibility — SOCI

04
Secure Remote Access

05
Risk-based Vulnerability Management — SOCI

01 AN ICS-SPECIFIC INCIDENT RESPONSE PLAN

OT’s incident and response plan is distinct from IT’s.

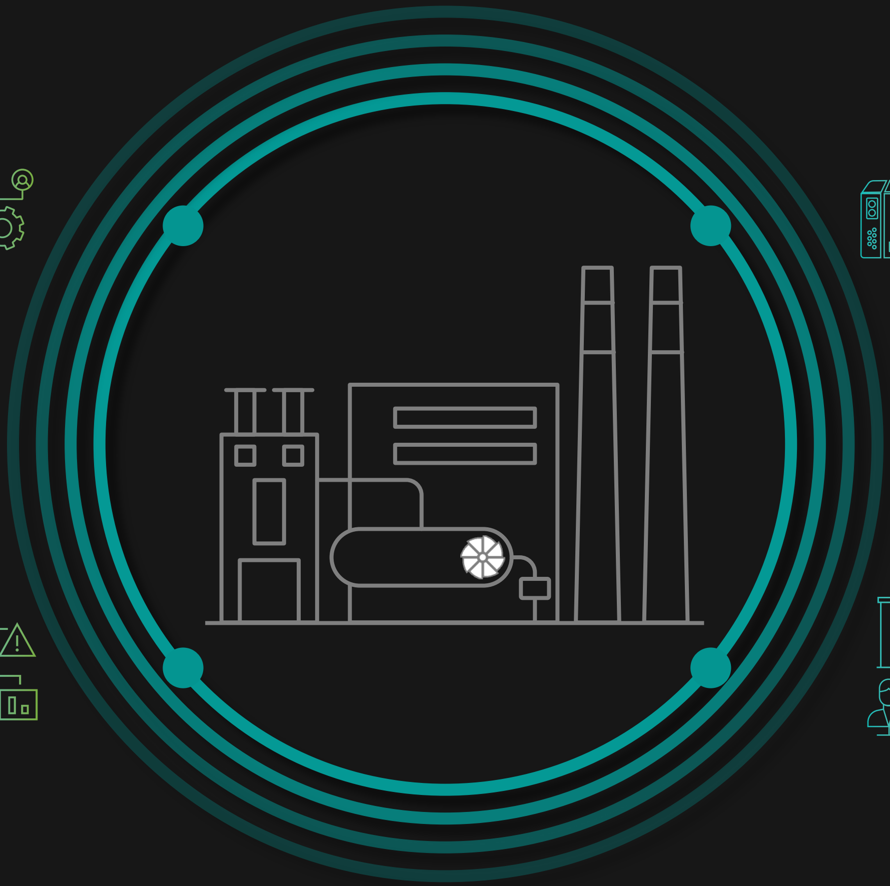
Different

People	Ops, HES & Maintenance
Consequence	Black start and recovery
Technology	Protocols, systems, logs

Managing the potential impact of an incident is different for OT’s. Create a dedicated plan as well as thought-out next steps for specific scenarios

02 A DEFENSIBLE ARCHITECTURE

The resources and technical skills required to adapt to new vulnerabilities and threats should not be underestimated.



Removing extraneous OT network access points

Mitigating high risk vulnerabilities

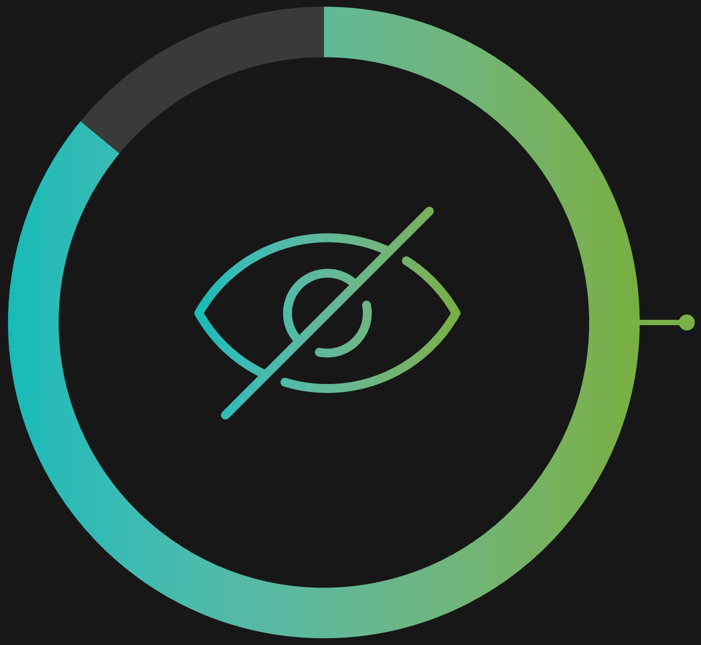
Maintaining strong policy control at IT/OT interface points

The people and processes to maintain it

02 A DEFENSIBLE ARCHITECTURE

03 OT VISIBILITY

You can't protect **what you can't see.**



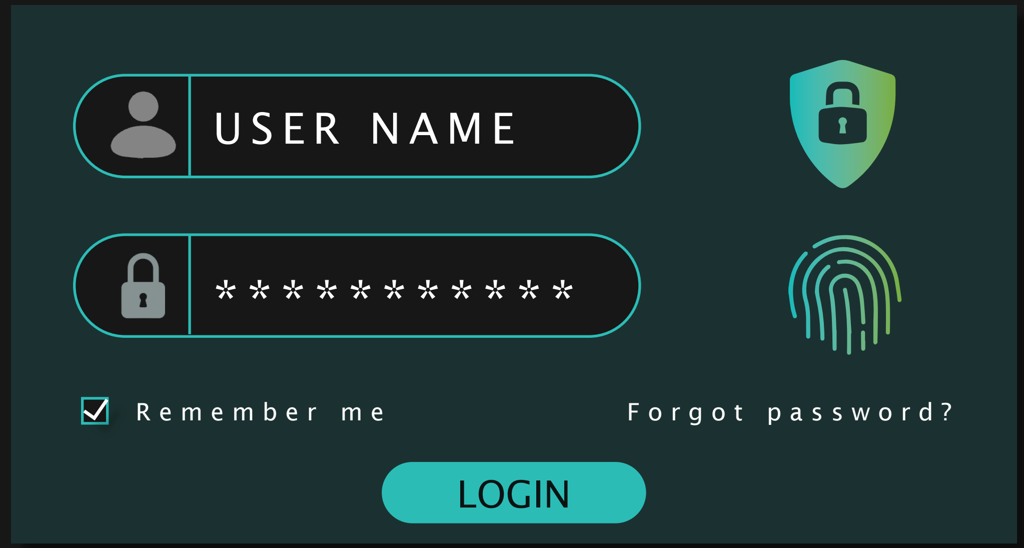
IN 2021
86%
of Dragos services customers had limited to no visibility in their OT environments

A Successful OT Security Posture

- ✓ Maintains an inventory of assets
- ✓ Maps vulnerabilities against those assets
- ✓ Actively monitors traffic for potential threats
- ✓ Validates the security controls implemented in a defensible architecture

04 Secure Remote Access

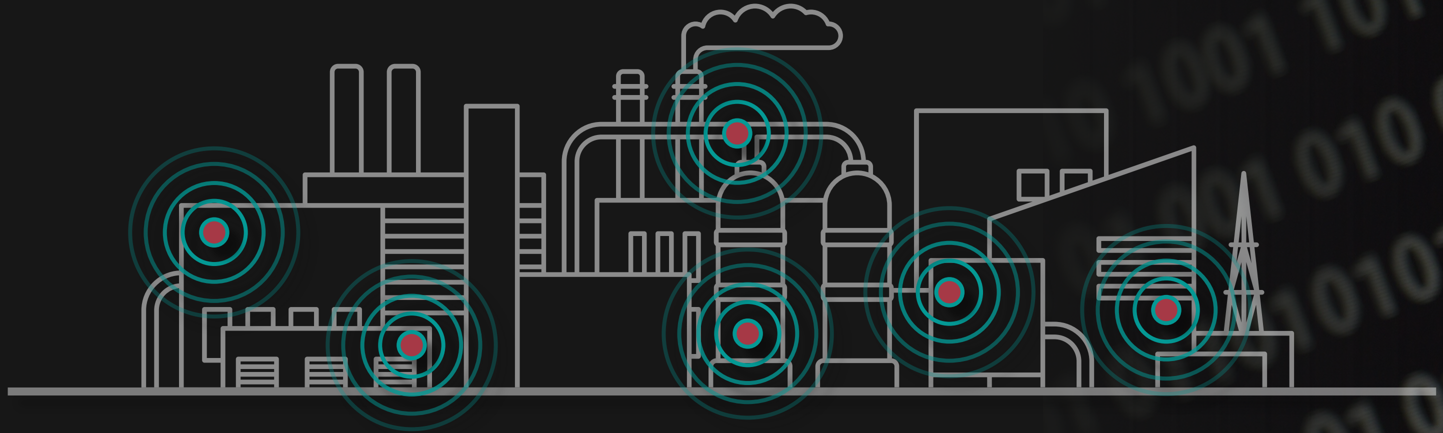
Multi-factor authentication (MFA)



MFA is a rare case of a classic IT control that can be appropriately applied to OT.

Implement MFA across your systems of systems to add an extra layer of security for a relatively small investment.

05 KEY VULNERABILITY MANAGEMENT PROGRAM

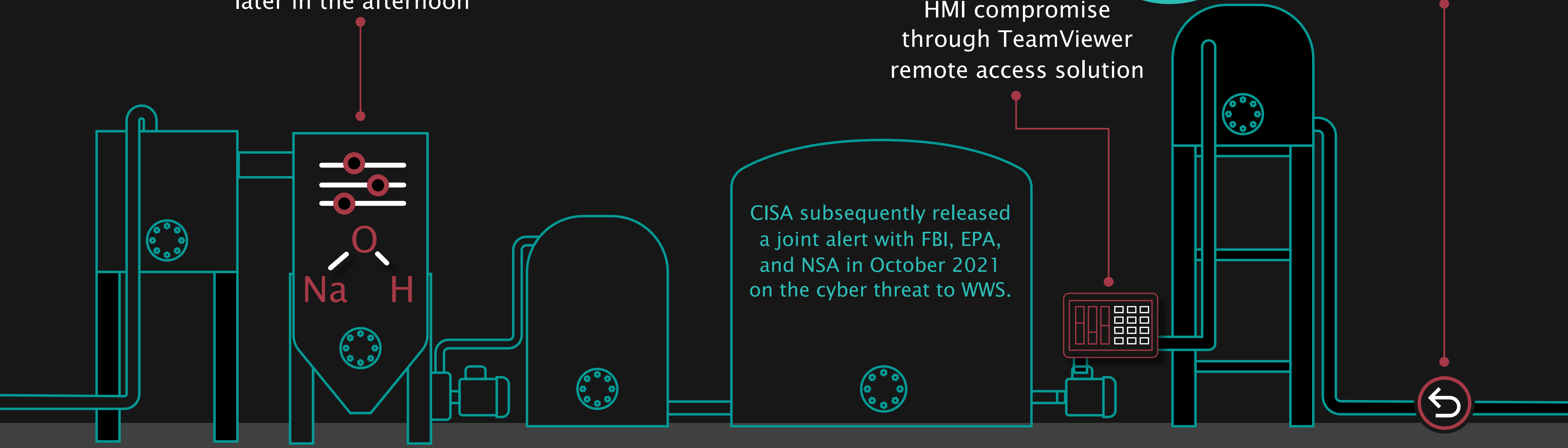


Knowing your vulnerabilities
and having a plan to manage them is a critical component to a defensible architecture.

*OLDSMAR REMOTE HMI ATTACK

04 Secure Remote Access

03 OT Visibility



Access on morning of 05 February 2021, followed by manipulation of NaOH levels later in the afternoon

CISA subsequently released a joint alert with FBI, EPA, and NSA in October 2021 on the cyber threat to WWS.

HMI compromise through TeamViewer remote access solution

Modifications noticed by operator and reversed. Physical safeguards also could have alerted on the change in PH

* May have not actually been a cyber attack!

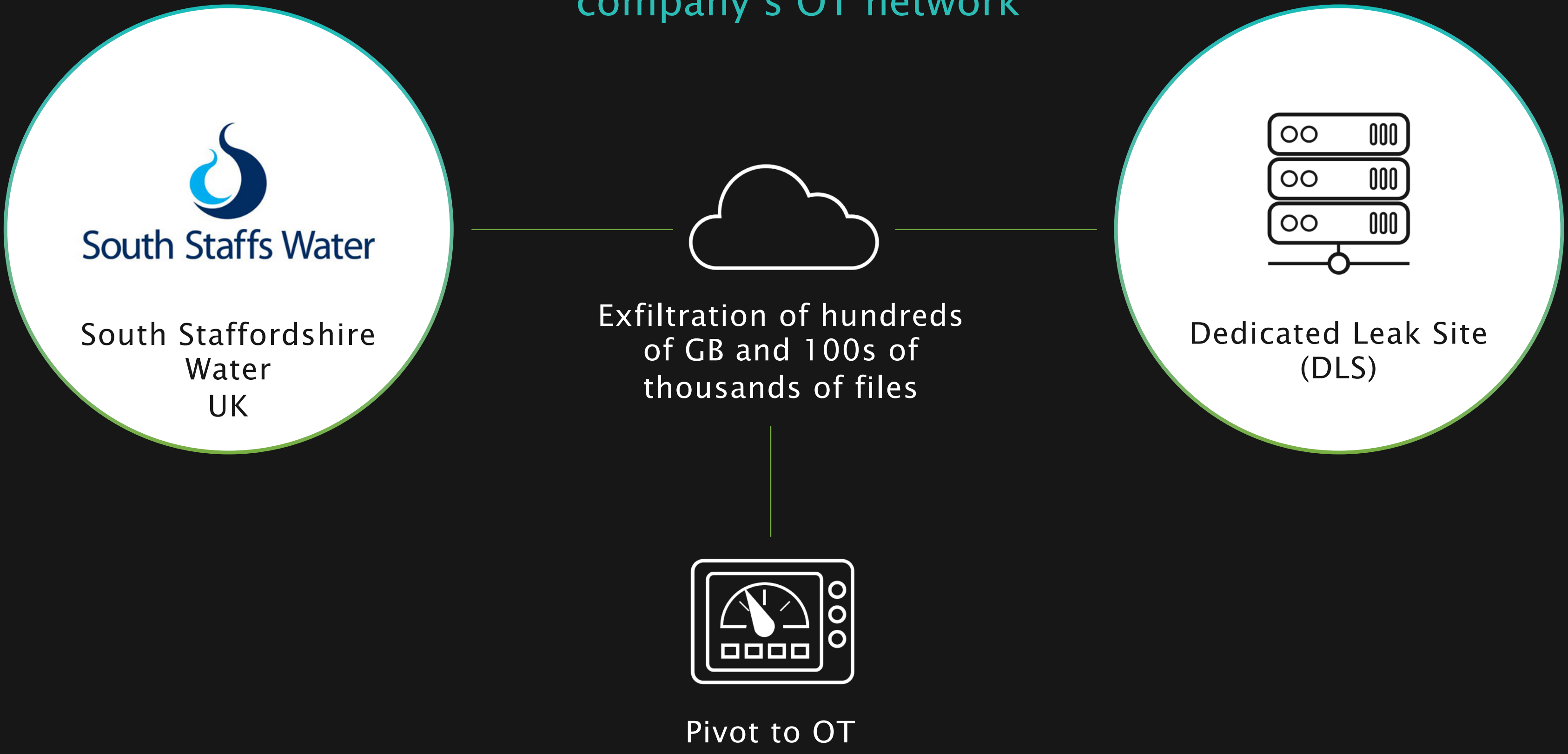
01
ICS IRP

02 CJA

RANSOMWARE: SOUTH STAFFORDSHIRE ATTACK

SOUTH STAFFORDSHIRE WATER SUPPLIES DRINKING WATER FOR 1.6M CONSUMERS

Cl0p gains access to corporate data and the water company's OT network



South Staffordshire
Water
UK

Exfiltration of hundreds of GB and 100s of thousands of files

Dedicated Leak Site
(DLS)

Pivot to OT

1. Cl0p claims compromise of Thames Water, servicing Greater London
2. Documents are shared by Cl0p that reference South Staffordshire Water
3. Multiple GB of data uploaded to their dedicated leak site
4. Includes leaked screenshots of an HMI taken by the adversary

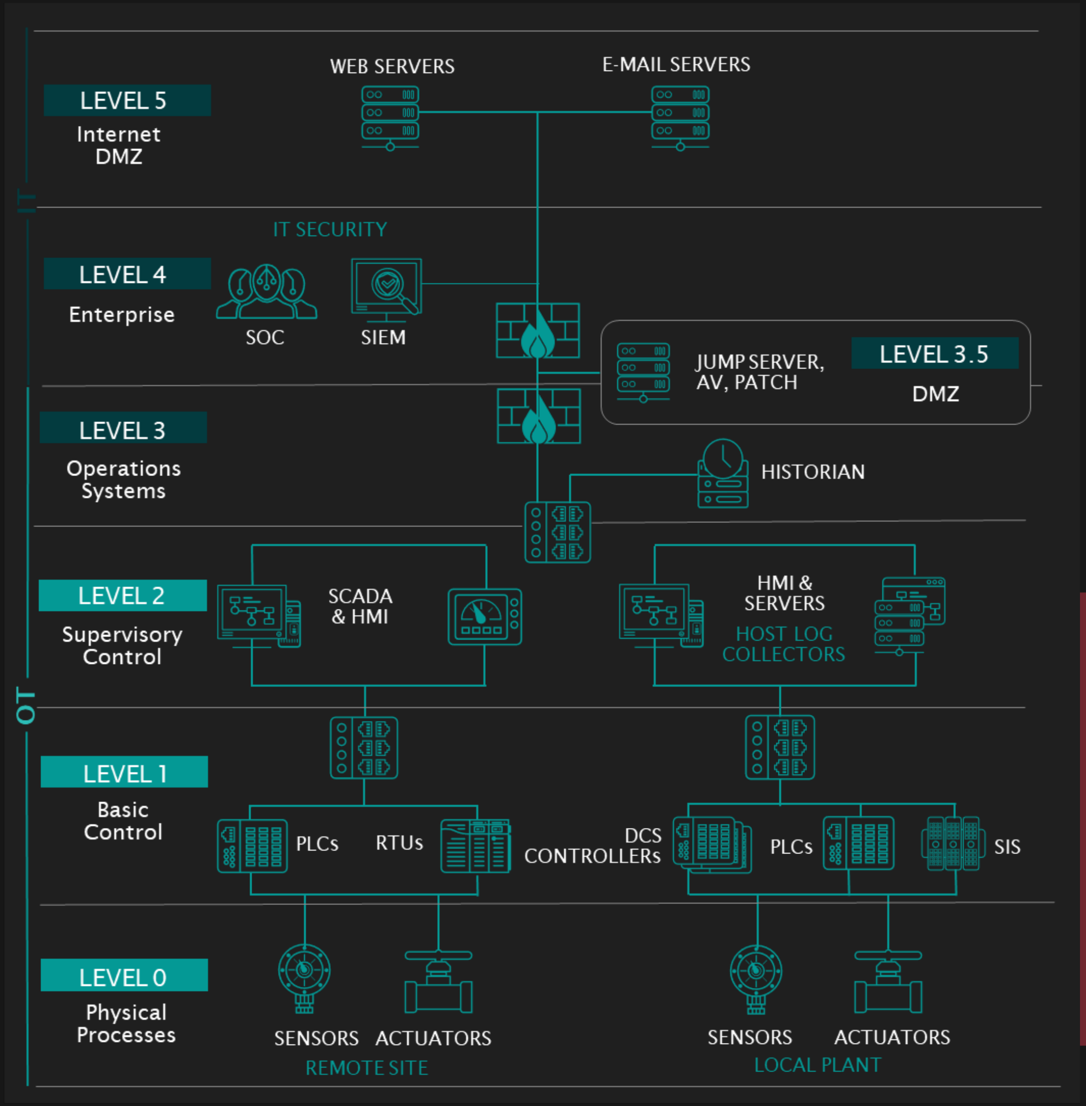
INSIDER THREATS & SUPPLY CHAIN ATTACKS

03 OT Visibility

05 Vuln. Mgmt.

04 Secure Remote Access

From the OT network, adversaries can exploit any number of vulnerabilities



IN THE WWS SECTOR, NEARLY 60% OF THE EXPLOITABLE VULNERABILITIES ARE ON CONTROLLERS

DRAGOS OT-CERT*

Industrial cybersecurity resources for the OT community

FREE CYBERSECURITY RESOURCES

Free content available for OT asset owners and operators, to help you build and maintain an effective OT cybersecurity program

OPEN TO GLOBAL ICS/OT COMMUNITY

Oriented toward Small and Medium businesses (SMBs) and resource-challenged organisations with OT environments that lack in-house expertise

NEW CONTENT MONTHLY

Members have access to a growing library of resources such as reports, webinars, training, best practice blogs, assessment toolkits, tabletop exercises and more, available from the OT-CERT portal

REGIONAL WORKSHOPS

Customised regional workshops to meet the needs of the community

VULNERABILITY DISCLOSURES

We take a coordinated approach to the disclosure of vulnerabilities, working with vendors to better protect our customers and the ICS/OT community

*Operational Technology –
Cyber Emergency Readiness Team

OT-CERT Resources available now

OT Cybersecurity Fundamentals Self-Assessment

Asset Management Toolkit
Collection Management Framework Toolkit
Host-Based Logging Toolkits
Incident Response Plan Toolkit
OT Backups Toolkit
Secure Remote Access Toolkit

Best Practices Blog Series

Self-Service OT Ransomware Tabletop Toolkit

ICS/OT Cybersecurity Introductory Training, Guides, and Videos

Joint Workshops with Partners

OT-CERT Working Sessions
Tips & Tricks from Members

ICS/OT Vulnerability Disclosures
Victim Notifications

THANK YOU

DRAGOS

ICS/OT CYBERSECURITY
YEAR IN REVIEW 2022

To download a copy of the
2022 Year In Review Report, visit:
www.dragos.com/year-in-review/