



OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

22 – 23 AUGUST 2023

The Industrial Cyberthreat Landscape
Robert M. Lee, CEO & Co-Founder, Dragos Inc.



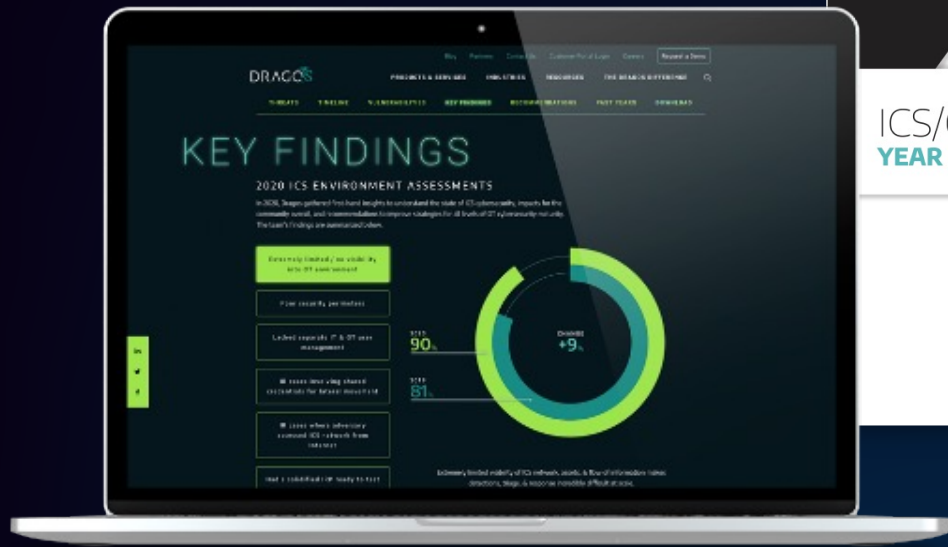
The Industrial Cyberthreat Landscape

Robert M. Lee, CEO & Co-Founder,
Dragos Inc.

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

WHAT IS THE YEAR IN REVIEW?

Sixth year
running!



Annual analysis of threats, vulnerabilities, & the state of industrial cybersecurity

Insights from OT threat intel researchers & incident responders

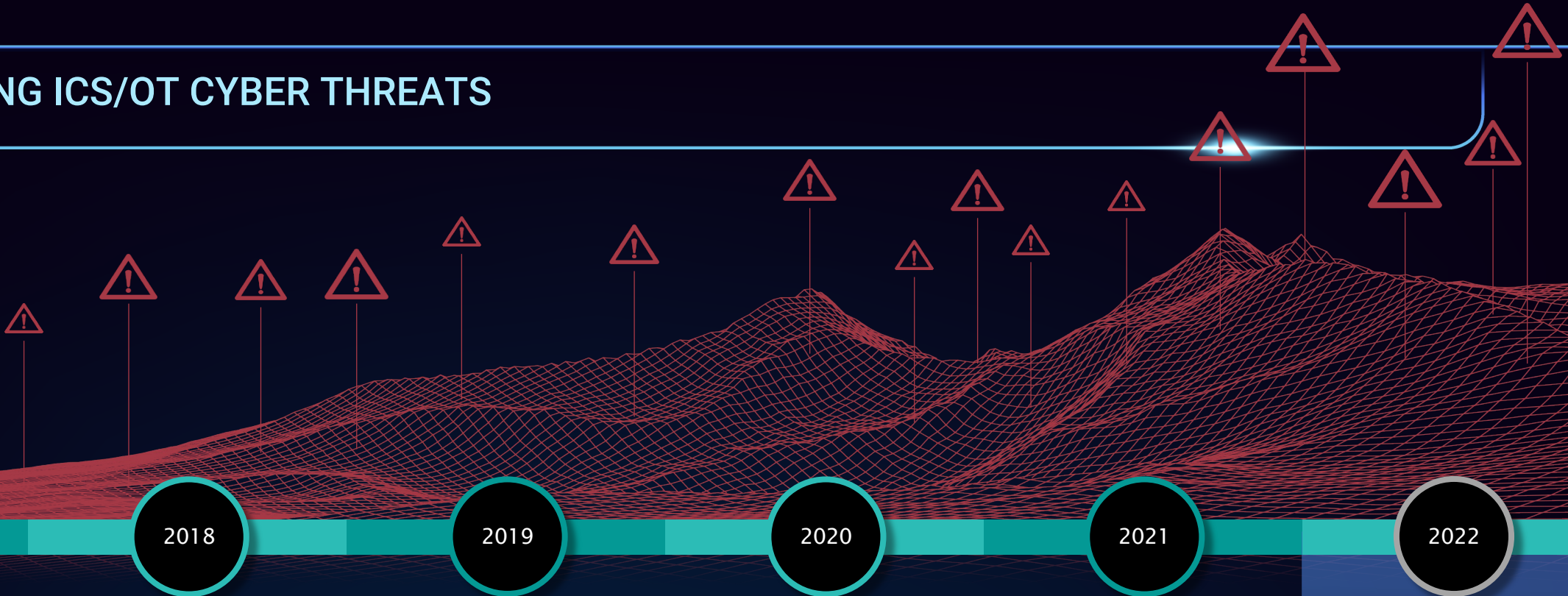
Promote awareness and community engagement



OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

TRACKING ICS/OT CYBER THREATS

YEAR FIRST DISCOVERED



2017

2018

2019

2020

2021

2022

EL

Ch

Ra

Hx

Ka

Va

Ko

Cv

Co

Ma

AL

Pi

St

Ta

Pv

Bt

Dy

Xt

Wa

Er

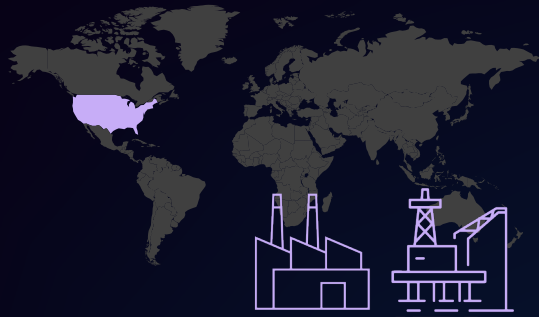
CHERNOVITE
ALL INDUSTRIES

BENTONITE
ONG FOCUSED

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

BENTONITE: NEW IN 2022

OPPORTUNISTIC EXPLOITATION



Targets Oil & Gas,
Manufacturing



BENTONITE SINCE 2021

ADVERSARY:

- + Associated with PHOSPHORUS
- + Able to run multiple, concurrent operations

CAPABILITIES:

- + Multi-stage downloaders, victim enumeration, reconnaissance and C2 capabilities
- + Vulnerability exploitation
- + Heavy use of Powershell to facilitate compromise
- + Disruptive Capabilities

VICTIM:

- + Highly Opportunistic
- + U.S. Oil and Gas, Manufacturing
- + State, Local, Tribal and Territorial organizations

INFRASTRUCTURE:

- + Credential harvesting
- + Separate domains for phishing and C2
- + Utilizes Github for delivery, SSH and HTTP for C2

ICS IMPACT:

- + Espionage, Data Exfiltration & IT Compromise
- + Disruptive Effects Possible

Delivery

STAGE
01

Exploit

STAGE
01

Install/Modify

STAGE
01

C2

STAGE
01

Act

STAGE
01

Highly
opportunistic

Demonstrated **Stage 1** of
the ICS Cyber Kill Chain

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

BENTONITE: OPPORTUNISTIC EXPLOITATION

GETTING THROUGH THE OUTER DEFENSES



BENTONITE has in the past employed disruptive capabilities

Compromises Maritime ONG, SLLT governments via vulnerabilities in remote access solution



Capable of deploying wiper malware

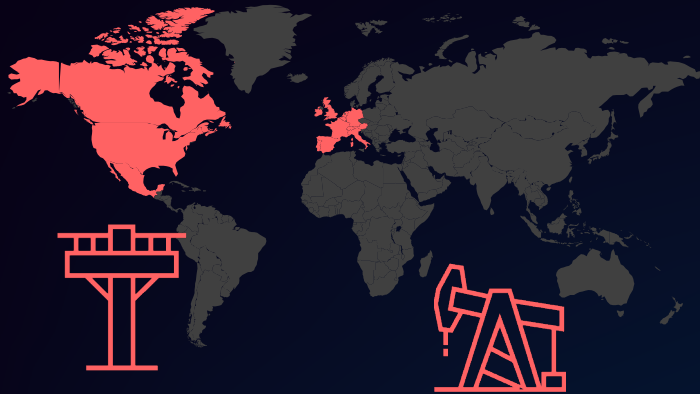


Capable of ransomware attack

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

CHERNOVITE: NEW IN 2022

ICS/OT SYSTEM SPECIALIST



Potential to impact **all industries and regions**



CHERNOVITE
SINCE 2021

ADVERSARY:

+ Development and effects team focused on ICS disruption

CAPABILITIES:

- + Unique tool development
- + Uses ICS-specific protocols for reconnaissance, manipulation, and disabling of PLCs
- + PLC Credential Capture. Password bruteforcing and denial of service

VICTIM:

- + Could impact all industries, initially targets electric, ONG
- + Companies with Schneider Electric, Omron, and CODESYS PLCs, as well as any OPC UA operations

INFRASTRUCTURE:

+ Unknown

ICS IMPACT:

- + Loss of safety, availability, and control; manipulation of control
- + ICS Kill Chain Stage 2 – Install/Modify, Execute ICS

STAGE 02

Develop

STAGE 02

Test

STAGE 02

Deliver

STAGE 02

Install / Modify

STAGE 02

Execute ICS Attack

Tens of thousands of ICS vendors use **CODESYS, Modbus, OPC UA**

Capable of **Stage 2** of the ICS Cyber Kill Chain

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

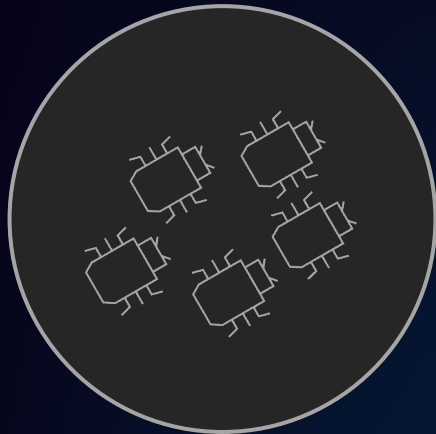
CHERNOVITE'S PIPEDREAM

EVOLUTION OF ICS/OT MALWARE



FIRST scalable, cross-industry OT attack framework (7TH overall ICS/OT specific)
Discovered before it was employed for destructive purposes.

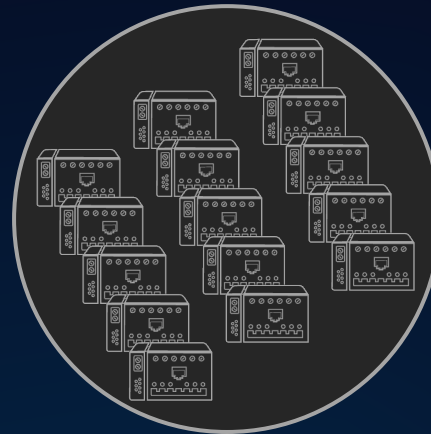
5



ICS PROTOCOLS ABUSED

FINS, MODBUS, CODESYS, OPC UA,
Schneider Electric NetManage

100s



VENDORS
IMPACTED

1000s



DEVICES POTENTIALLY
IMPACTED

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

CHERNOVITE'S PIPEDREAM MALWARE

CAPABLE OF DISRUPTIVE & DESTRUCTIVE ICS/OT IMPACT



1st scalable, cross-industry OT attack toolkit
7th ICS/OT targeting malware

Discovered before it was employed for destructive purposes



EVILSCHOLAR & BADOMEN are extensible – this is rare.

1000s of CODESYS devices across multiple sectors at risk



MOUSEHOLE manipulates OPC-UA server nodes & associated devices.

OPC-UA is a widely used communication protocol in ICS/OT



DUSTTUNNEL & LAZYCARGO demonstrate that CHERNOVITE can achieve an end-to-end attack.

INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	EVASION	DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND & CONTROL	INHIBIT RESPONSE FUNCTION	IMPAIR PROCESS CONTROL	IMPACT
Data Historian Compromise	Change Operating System	Modify Program	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	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	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Service
Engineering Workstation Compromise	Execution Through API	Project File Injection		Indicator Removal on Host	Remote System Discovery	Lateral Tool Transfer	Detect Operating System	Standard Application Layer Protocol	Block Command Response	Module Firmware	Denial of View
Exploit Public Facing Application	Graphical User Interface	System		Rootkit	System Discovery	Program Execution	Program Execution	Program Execution	Program Execution	Program Execution	Loss of Availability
Exploitation of Remote Services	Hooking			Rootkit	System Discovery	Program Execution	Program Execution	Program Execution	Program Execution	Program Execution	Loss of Control
Internet Accessible Device	Modify Computer Tasking			Special Repeating	Valid Accounts	Valid Accounts	Valid Accounts	Valid Accounts	Valid Accounts	Valid Accounts	Loss of Productivity & Revenue
Remote Services	Native API										Loss of Protection
Replication Through Removable Media	Scripting							Program Update	Detect		Loss of Safety
Rogue Master	User Execution							System Capture	Manipulate I/O Image		Loss of View
Speakeasy Attachment								Wireless Sniffing	Modify Alarm Settings		Manipulation of Control
Supply Chain Compromise									Roadkit		Manipulation of View
Wireless Compromise									Service Stop		Theft of Operational System
									System Firmware		

CHERNOVITE CAN EXECUTE 46% OF MITRE ATT&CK FOR ICS TECHNIQUES WITH PIPEDREAM

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

THREAT GROUPS INCREASE ACTIVITY IN 2022

RECON, CAPABILITY BUILDING, & INITIAL ACCESS ACTIVITY ACROSS ALL GLOBAL INDUSTRIAL SECTORS



KOSTOVITE

Dragos observed a possible link to multiple adversaries sharing common infrastructure with KOSTOVITE, with reports of exploitation of vulnerabilities by linked APT5.

Targeting Energy
North America, Australia



KAMACITE

Victims in multiple sectors are observed communicating with KAMACITE Cyclops Blink C2 infrastructure. Cyclops Blink malware is removed from firewall devices.

Many Industrial Sectors Targeted
Ukraine, Europe, U.S.



XENOTIME

Dragos observed reconnaissance and research activity focused on oil and gas entities in the U.S.

Targeting Oil & Gas, Electric
Middle East,
North America



ELECTRUM

INDUSTROYER2 malware and a set of wiper malware is discovered at a Ukraine energy provider.

Targeting Electric
Ukraine, Europe



ERYTHRITE

Continued targeting of industrial organizations with SEO poisoning techniques and custom, rapidly deployed malware.

Multiple Industrial Sectors Targeted
U.S, Canada



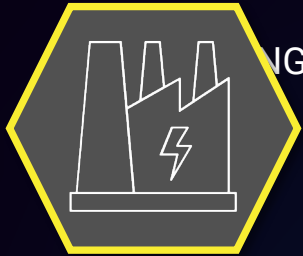
WASSONITE

Dragos observed ongoing deployment of nuclear energy themed spear phishing lures to deliver backdoor malware.

Multiple Industrial Sectors Targeted
South/East Asia,
North America

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

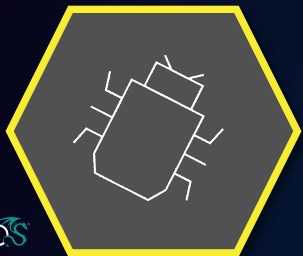
KOSTOVITE



ATTACKING ENERGY IN NORTH AMERICA, AUSTRALIA SINCE 2015
Compromise of an energy entity
& power generation facilities



Activity of multiple adversaries
sharing common infrastructure
with KOSTOVITE



KOSTOVITE-linked APT5 was
actively exploiting a zero-day in
Citrix perimeter access devices



Delivery	STAGE 1
Exploit	STAGE 1
Install/Modify	STAGE 1
C2	STAGE 1
Act	STAGE 1

COMPROMISES INTERNET-
EXPOSED REMOTE ACCESS
DEVICES

SKILLED LATERAL
MOVEMENT & INITIAL
ACCESS OPERATIONS
INTO ICS/OT

STAGE 2	Develop
STAGE 2	Test
STAGE 2	Deliver
STAGE 2	Install / Modify
STAGE 2	Execute ICS Attack

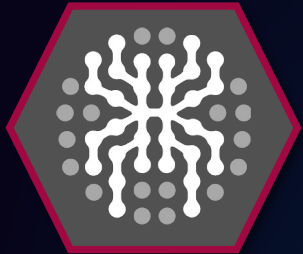
OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

XENOTIME

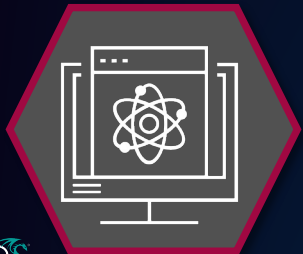
TARGETING THE OIL & GAS INDUSTRY IN THE U.S. & EUROPE SINCE 2014



Reconnaissance focused on oil & natural gas (ONG), liquified natural gas (LNG) industries



Heavy use of off-the-shelf tools & open-source information



Currently in the development phase, continues to target downstream & midstream ONG/LNG with a focus on pipeline, maritime, refining



ICS Malware: TRISIS

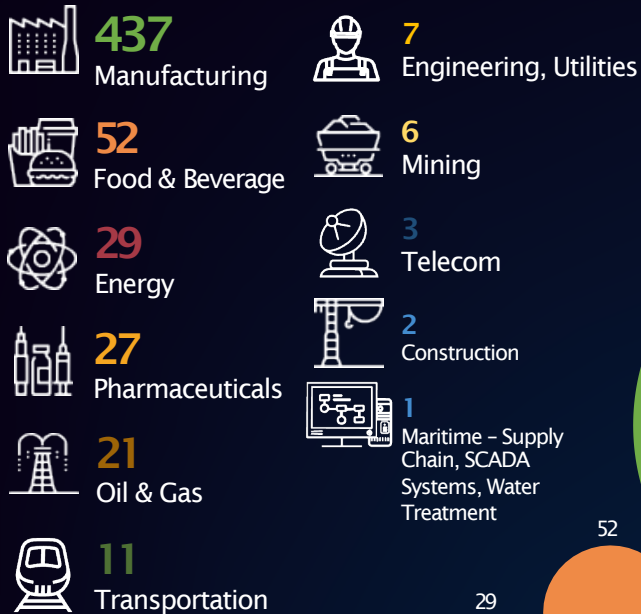
- Delivered in 2017 to an industrial facility in the Middle East by a well funded attack team
- Targeted Safety Instrumented System (SIS) and failed causing a stop in operations
- First malware to specifically target human life

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

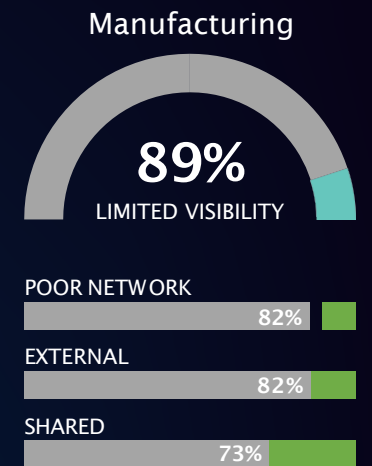
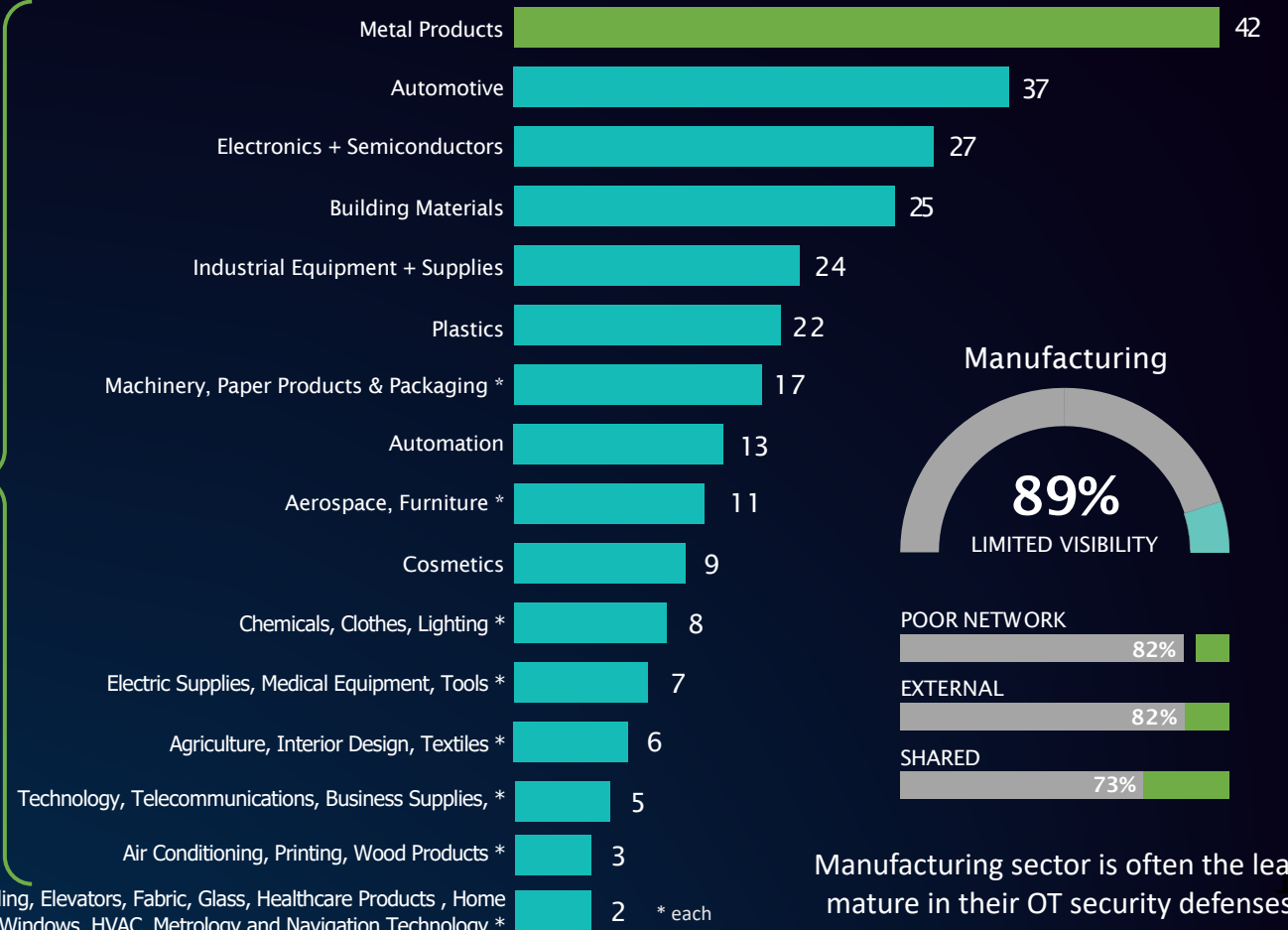
RANSOMWARE ATTACKS INCREASED BY 87%

MANUFACTURING TARGETED IN 72% OF 2022 INCIDENTS

Ransomware by ICS Sector



Ransomware by Manufacturing Subsector

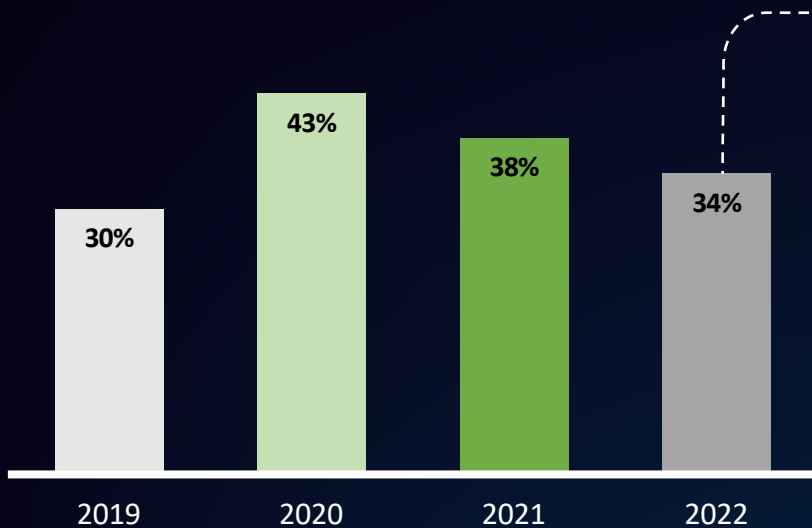


Manufacturing sector is often the least mature in their OT security defenses.

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

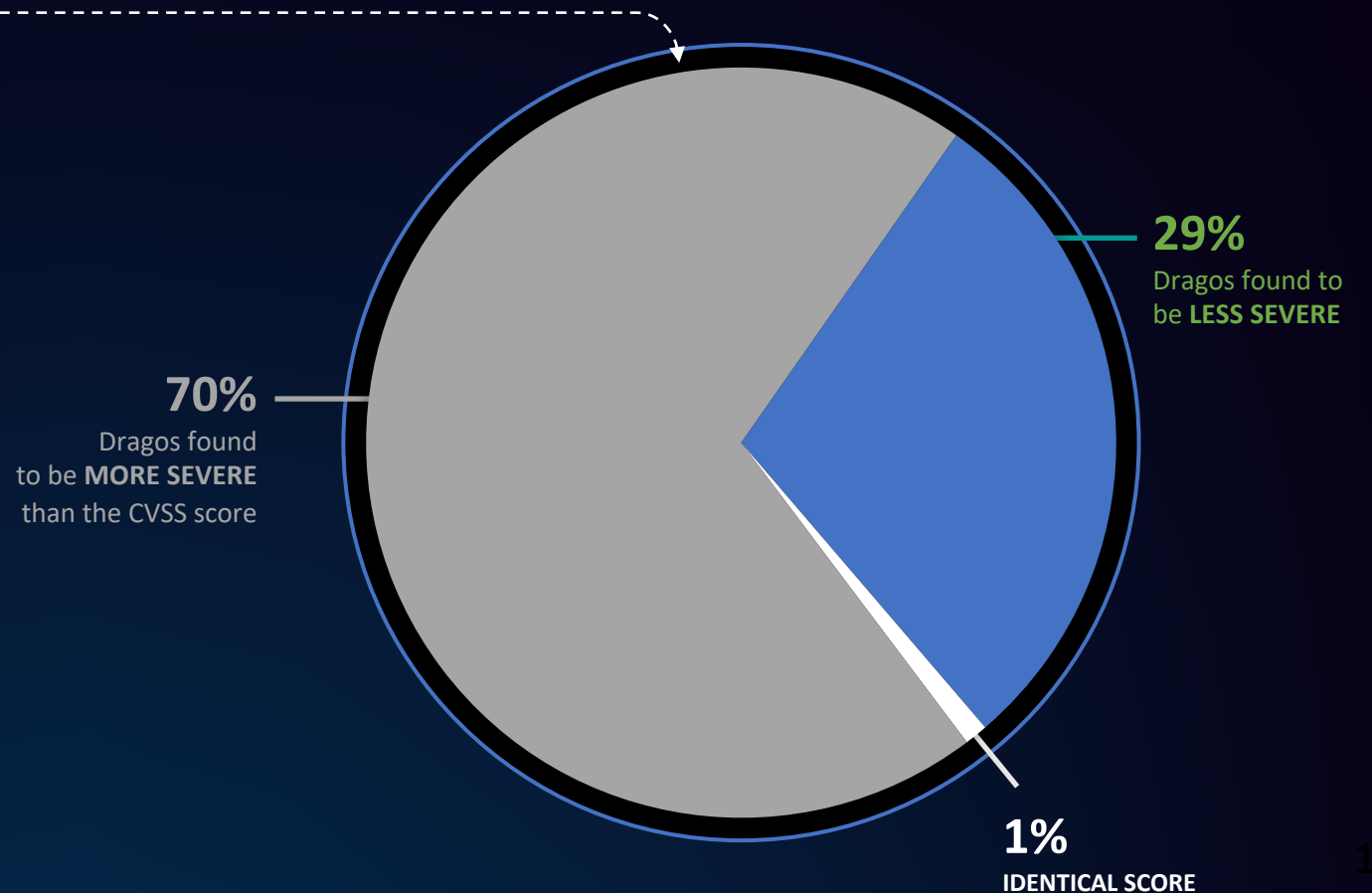
THE STATE OF ICS/OT VULNERABILITIES

ERRORS COULD CAUSE ASSET OWNERS AND OPERATORS TO WASTE RESOURCES ON LOW-RISK VULNERABILITIES OVER MORE SEVERE ONES.



Dragos analyzed 465 advisories

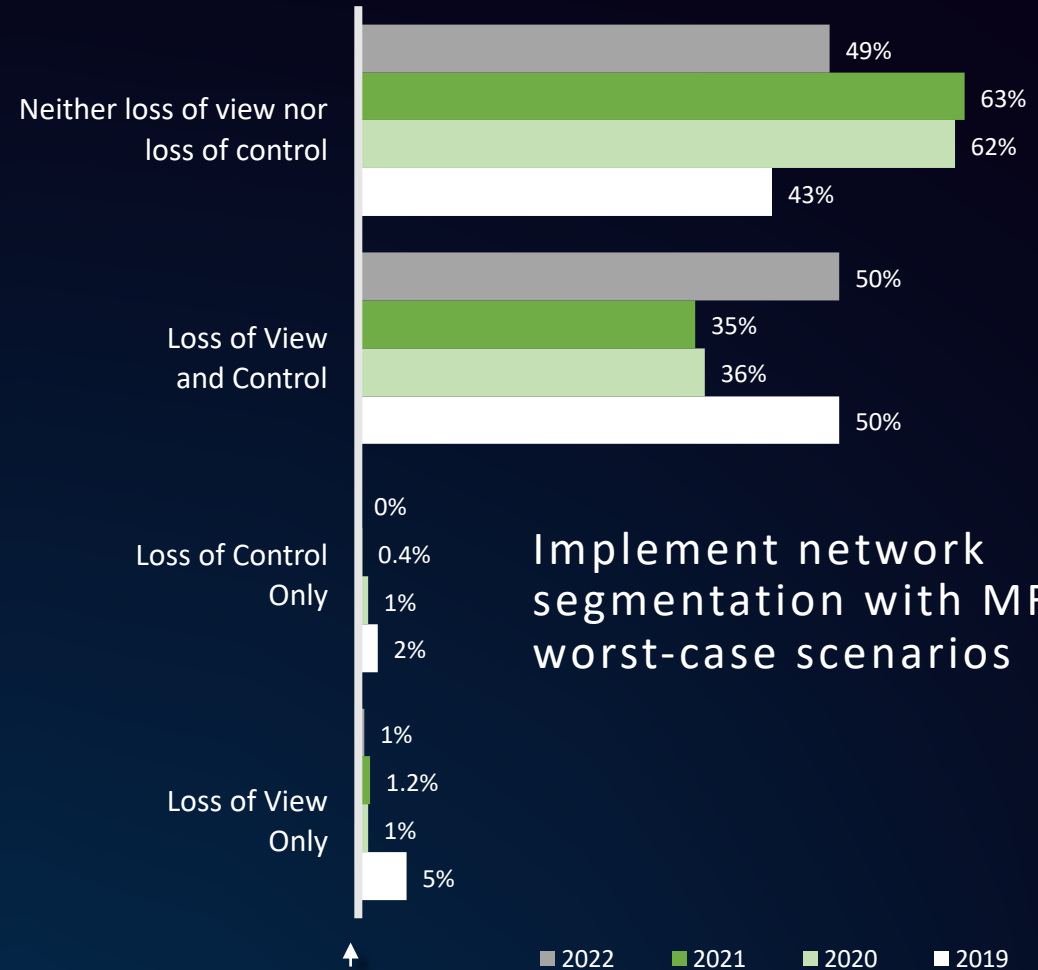
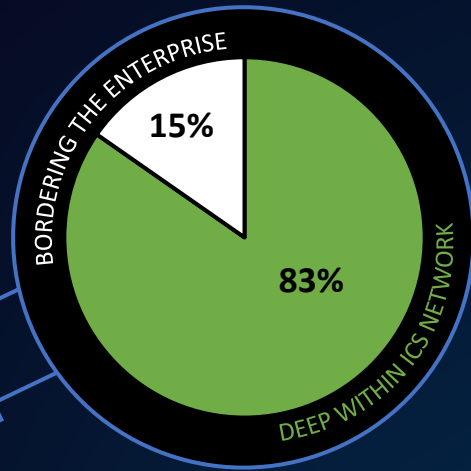
34% had incorrect data



OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

WHERE VULNERABILITIES EXIST

ADVERSARIES NEED INITIAL ACCESS TO OT NETWORKS TO COMPROMISE VULNERABILITIES DEEP WITHIN THE ICS NETWORK

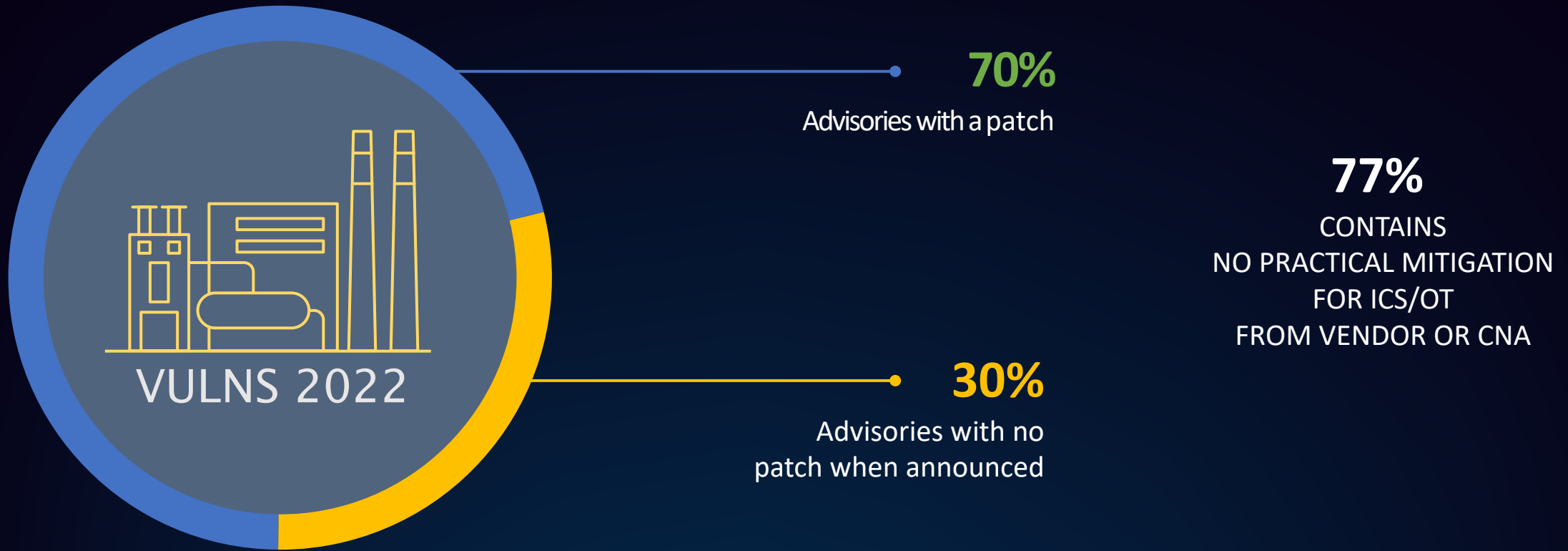


Implement network segmentation with MFA to avoid worst-case scenarios

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

PRACTICAL RISK MITIGATION IN ICS/OT

PATCHING CAN BE IMPRACTICAL IN ICS/OT DUE TO SAFETY & PRODUCTION REQUIREMENTS, ALTERNATIVE MITIGATION IS KEY



OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

CONSEQUENCE-BASED VULNERABILITY MANAGEMENT

FOCUS REMEDIATION EFFORTS ON VULNERABILITIES WITH OPERATIONAL IMPACT OR KNOWN TO BE ACTIVELY TARGETED BY ADVERSARIES.



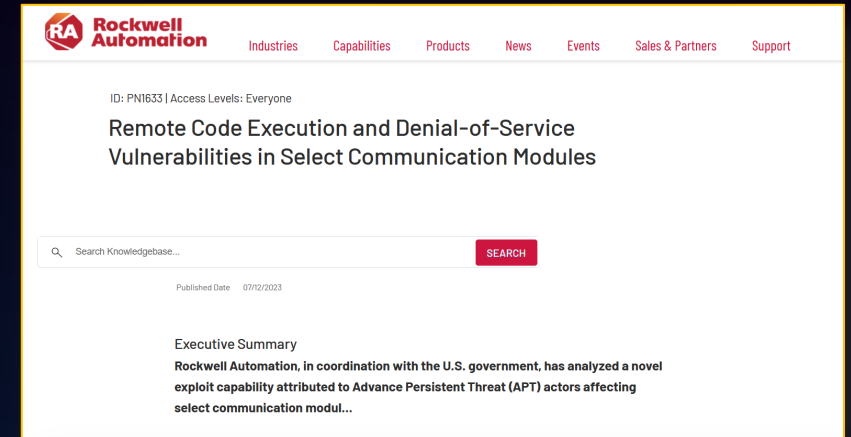
OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

JULY 2023: ROCKWELL AUTOMATION VULNERABILITY

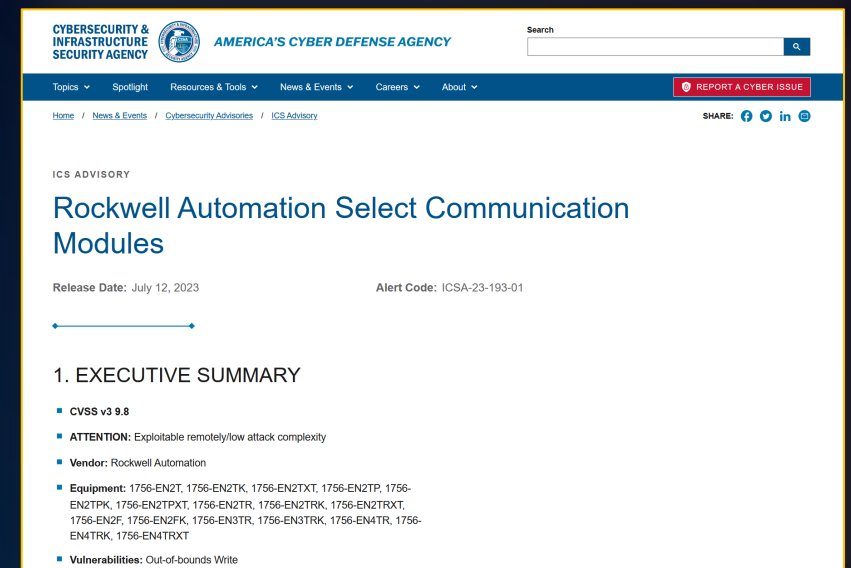
Rockwell Automation, in coordination with the U.S. government, released two vulnerabilities on 12 July 2023:

- **CVE-2023-3595:** RCE with persistence affecting 1756-EN2* and 1756-EN3* models of ControlLogix ENIP comms modules
- **CVE-2023-3596:** DOS affecting 1756 EN4* models of ControlLogix ENIP comms modules

These vulnerabilities are important because the USG identified a state actor developing exploits against these unknown vulnerabilities for use in attacks; this collective response was PRIOR to the attack leading to a massive success



The screenshot shows the Rockwell Automation Knowledgebase page for a security advisory. The title is "Remote Code Execution and Denial-of-Service Vulnerabilities in Select Communication Modules". The ID is PN1633 and the access level is Everyone. The page includes a search bar, a published date of 07/12/2023, and an executive summary stating that Rockwell Automation, in coordination with the U.S. government, has analyzed a novel exploit capability attributed to Advance Persistent Threat (APT) actors affecting select communication modules.



The screenshot shows the America's Cyber Defense Agency ICS Advisory page for "Rockwell Automation Select Communication Modules". The release date is July 12, 2023, and the alert code is ICSA-23-193-01. The advisory includes an executive summary with the following details:

- **CVSS v3 9.8**
- **ATTENTION:** Exploitable remotely/low attack complexity
- **Vendor:** Rockwell Automation
- **Equipment:** 1756-EN2T, 1756-EN2TK, 1756-EN2TXT, 1756-EN2TP, 1756-EN2TPK, 1756-EN2TPXT, 1756-EN2TR, 1756-EN2TRK, 1756-EN2TRXT, 1756-EN2F, 1756-EN2FK, 1756-EN3TR, 1756-EN3TRK, 1756-EN4TR, 1756-EN4TRK, 1756-EN4TRXT
- **Vulnerabilities:** Out-of-bounds Write

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

COLLABORATIVE WORK & COLLECTIVE DEFENSE

Critical Rockwell OT Bugs Fixed to Prevent Novel APT Exploit

Rockwell Automation: Urgent Attention Is Needed to Protect Critical Infrastructure

Mihir Bagwe (@MihirBagwe) · July 13, 2023

✉️ 🖨️ 📁 [f Share](#) [Tweet](#) [in Share](#) ⭐ Credit Eligible [Get Permission](#)



BIG CROSS-INDUSTRY LIFT

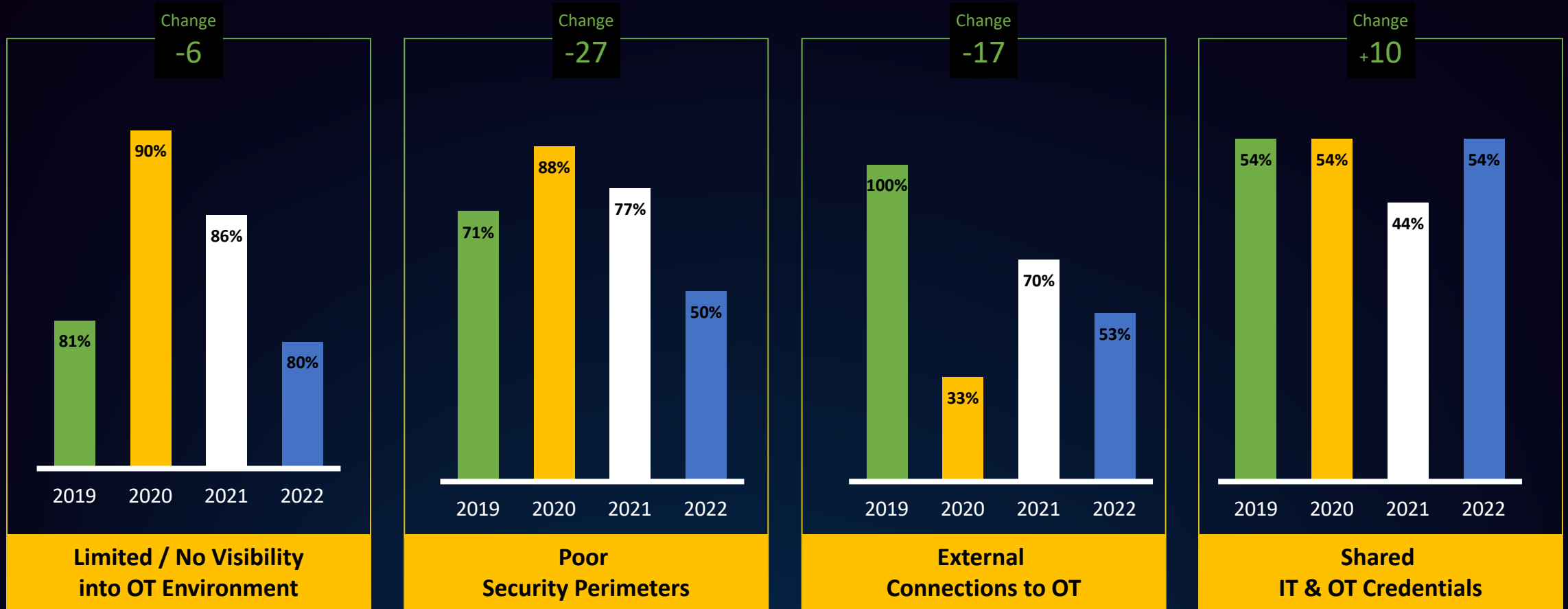
- US Government
- Rockwell Automation
- Dragos
- Other security vendors

COLLECTIVELY:

- Analyze vulnerabilities
- Test/Develop signatures
- Look for potential activity using respective telemetry

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

LESSONS LEARNED FROM CUSTOMER ENGAGEMENTS



OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

APPLYING THESE FINDINGS

Key takeaways for your teams:

- Attacks continue to increase for industrial infrastructure
- The tooling used by ICS-focused threat groups is growing more sophisticated
- The number of vulnerabilities found in OT environments continues to grow, while many advisories contain errors and offer limited advice for mitigation
- The industrial community is improving how they handle security perimeters and external connections. However, more work is needed around OT network visibility, segmentation, and controlling connections and credentials over ICS assets

Next steps to protect your organization:

- The SANS Institute identified five critical controls for ICS/OT cybersecurity. Implement these controls in your OT environments to improve your organization's security posture.

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

RECOMMENDATIONS

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

THANK YOU



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