ICS/OT CYBERSECURITY

YEAR IN REVIEW 2022

Ben Miller
Vice President of Services
Dragos, Inc.

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

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

TRACKING ICS/OT CYBER THREATS

YEAR FIRST DISCOVERED

2017
- EL
- Ch
- Co
- Ma
- Dy

2018
- Ra
- AL
- Xt

2019
- Hx
- Pi
- Wa

2020
- Ka
- Va
- St
- Ta

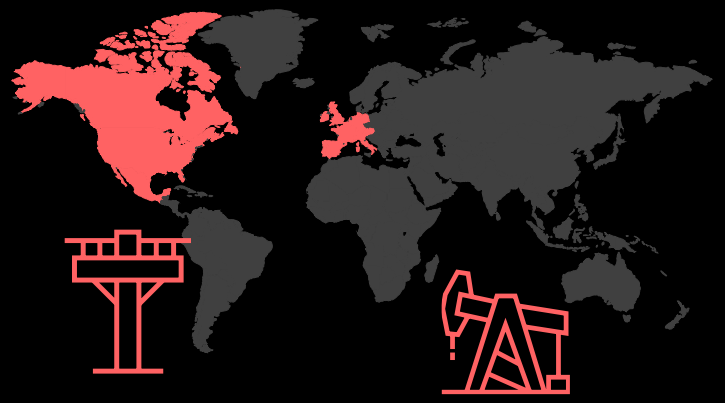
2021
- Ko
- Pv
- Er

2022
- Cv — **CHERNOVITE** ALL INDUSTRIES
- Bt — **BENTONITE** ONG FOCUSED

DRAGOS

CHERNOVITE: NEW IN 2022

ICS/OT SYSTEM SPECIALIST



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

Potential to impact all industries and regions

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

Capable of Stage 2 of the ICS Cyber Kill Chain

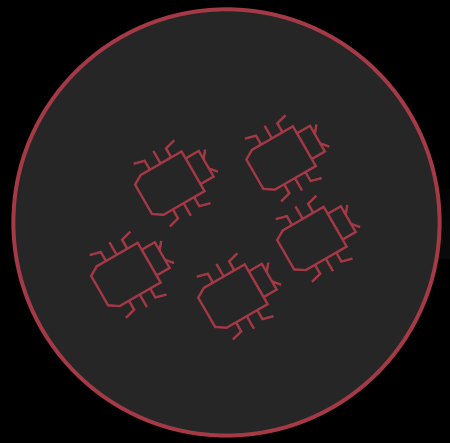
- STAGE 02 Develop
- STAGE 02 Test
- STAGE 02 Deliver
- STAGE 02 Install / Modify
- STAGE 02 **Execute ICS Attack**

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.

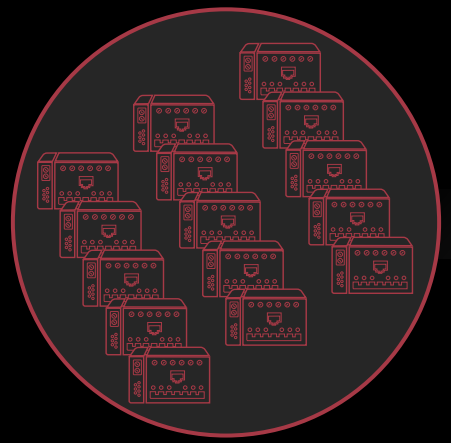
5



ICS PROTOCOLS ABUSED

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

100s



VENDORS IMPACTED

1000s

DEVICES POTENTIALLY IMPACTED

CAPABLE OF DISRUPTIVE & DESTRUCTIVE ICS CYBER ATTACKS

DRAGOS

PROTECTION AGAINST PIPEDREAM

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

100,000's

5

3-X

10K-X

ICS PROTOCOLS ABUSED
FINS, MODBUS, CODESYS, OPC UA,
Schneider Electric NetManage

ICS/OT
DEVICES TARGETED

ASSETS POTENTIALLY
IMPACTED

CAPABLE OF DISRUPTIVE & DESTRUCTIVE ICS CYBER ATTACKS

Detection

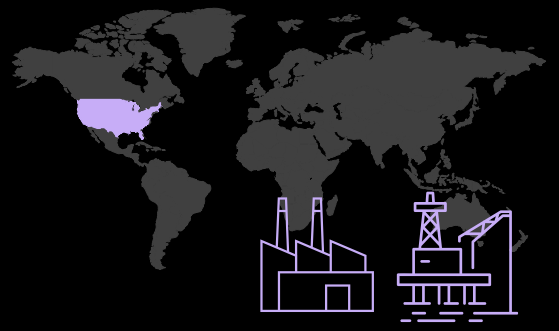
Monitor East-West OT networks with ICS protocol aware technologies. Look for modifications outside of maintenance periods.

Response

Have an ICS-focused Incident Response Plan (IRP) procedures for operating with a hampered or degraded control system.

BENTONITE: NEW IN 2022

OPPORTUNISTIC EXPLOITATION



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

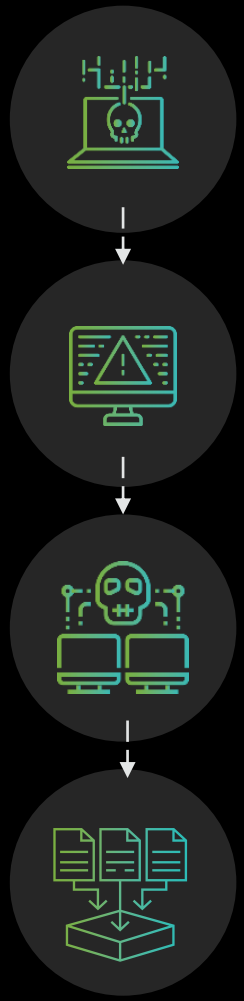
Targets **Oil & Gas, Manufacturing**

Highly opportunistic

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

BENTONITE: OPPORTUNISTIC EXPLOITATION

GETTING THROUGH THE OUTER DEFENSES



Exploits vulnerabilities in internet facing assets

Installs initial downloader implant

Implant retrieves malware from adversary Github account

Long-term persistence, reconnaissance, interactive operations

BENTONITE has in the past employed disruptive capabilities

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

Capable of deploying wiper malware

Capable of ransomware attack

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.

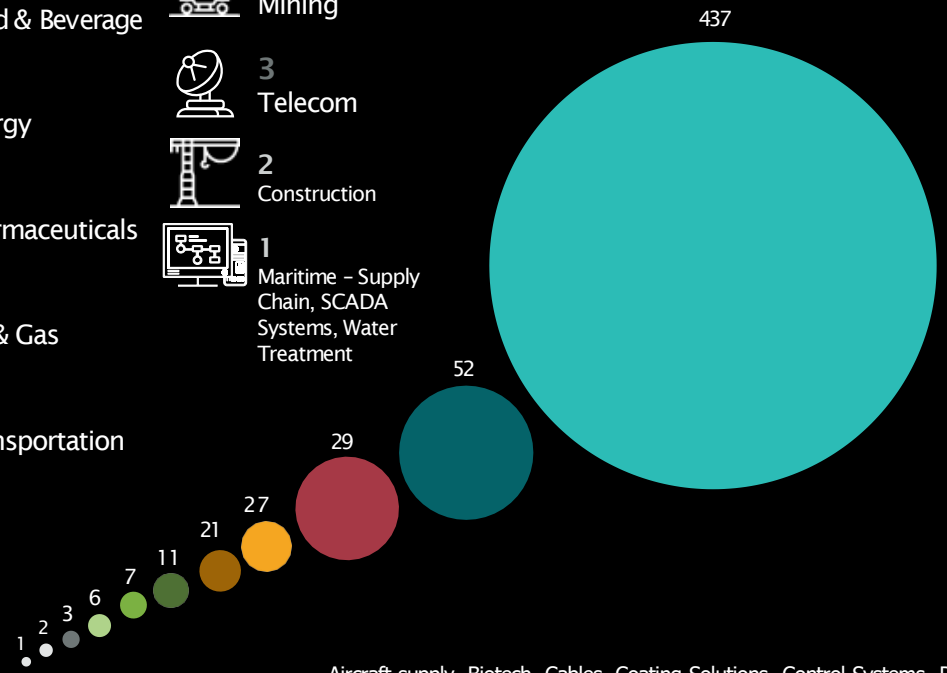
Multiple Industrial Sectors Targeted
South/East Asia, North America

RANSOMWARE ATTACKS INCREASED BY 87%

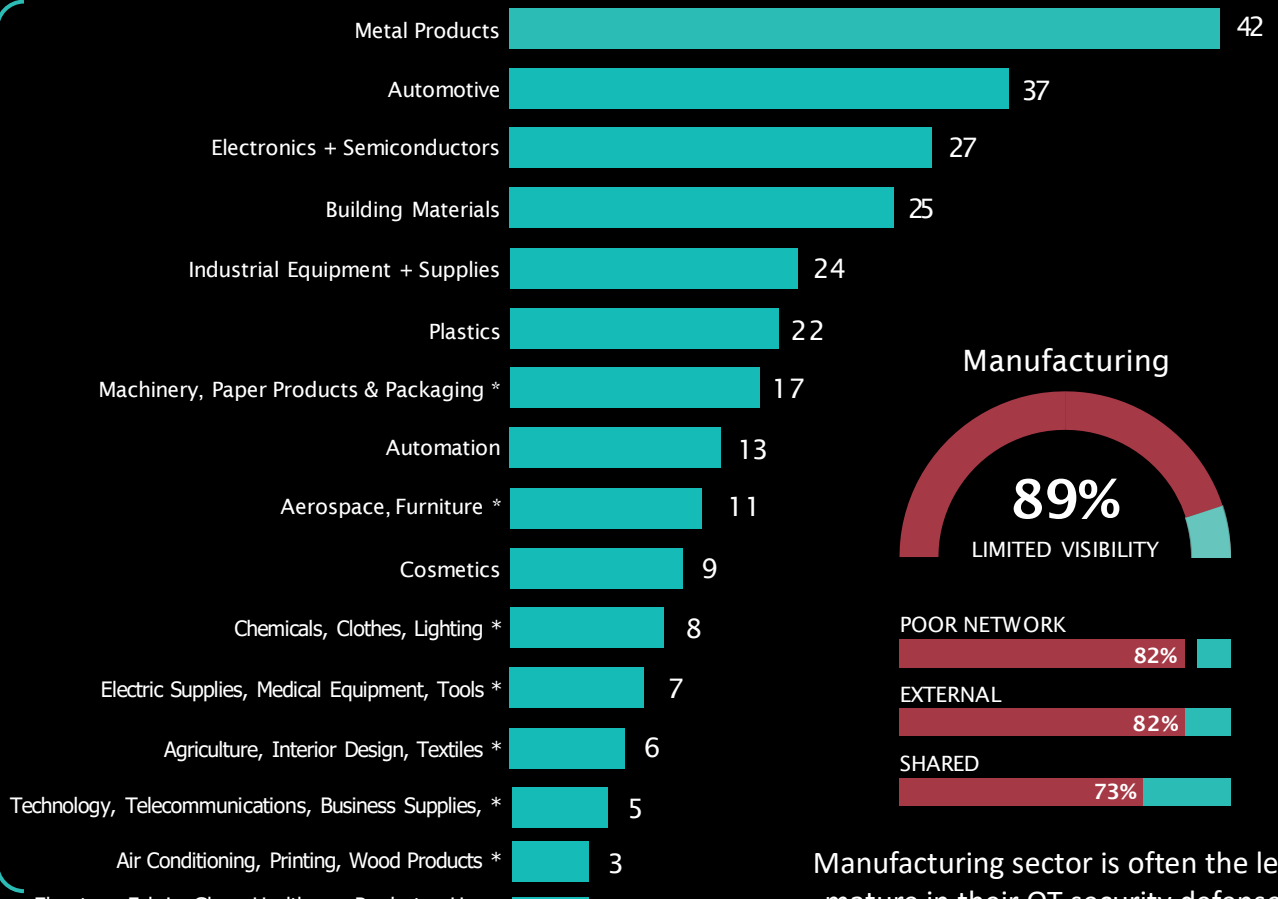
MANUFACTURING TARGETED IN 72% OF 2022 INCIDENTS

Ransomware 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



Ransomware by Manufacturing Subsector



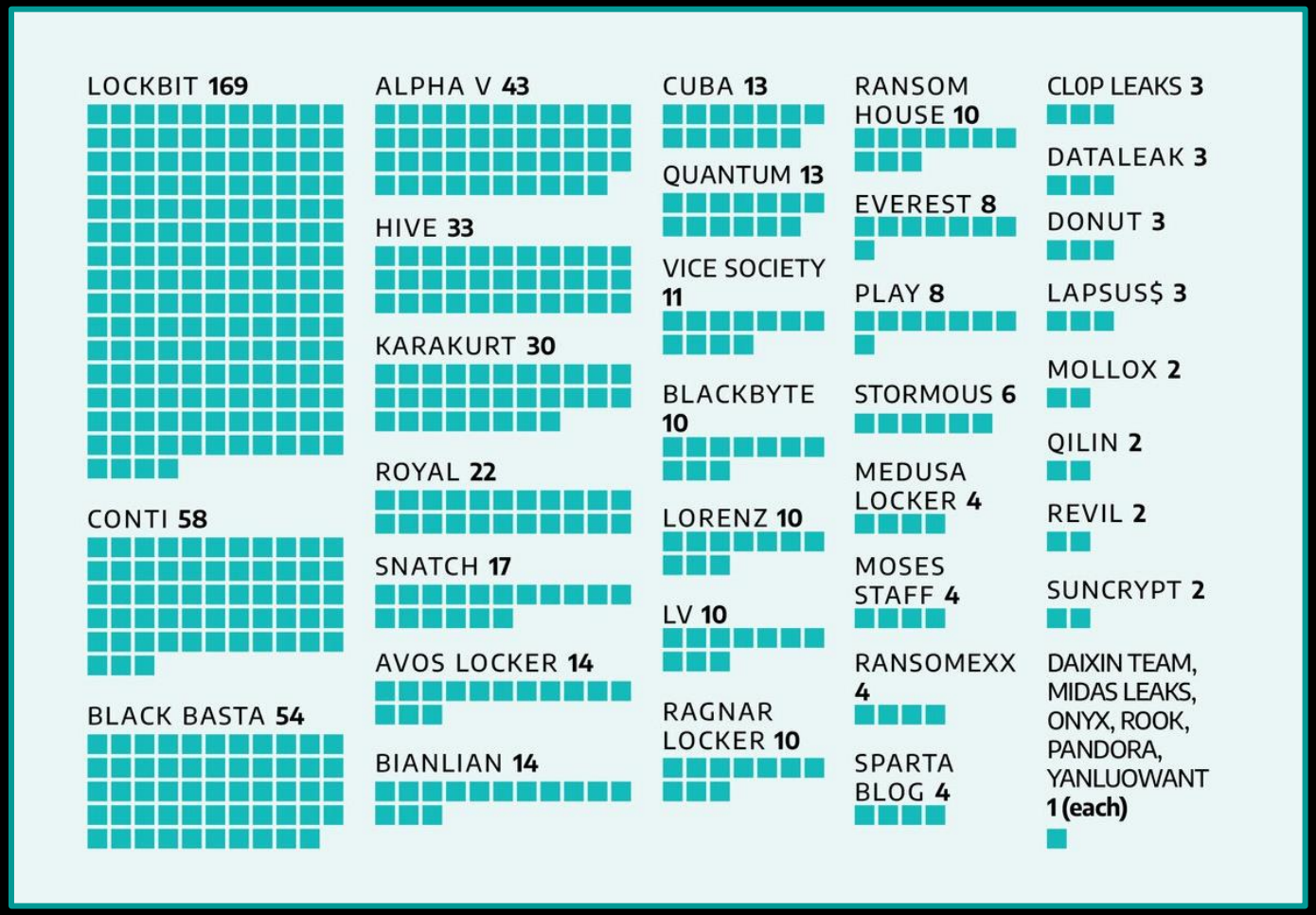
Manufacturing

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

RANSOMWARE GROUPS – MOVES AND CHANGES

LOCKBIT 2.0 + LOCKBIT 3.0 ACCOUNTED FOR 28% OF RANSOMWARE ATTACKS

CONTI SHUT DOWN OPERATIONS IN MAY



39 groups accounted for

605 ransomware attacks

THE RANSOMWARE KILL CHAIN

Does RANSOMWARE JUMP BETWEEN OT ZONES? FROM IT TO OT?

Remote Desktop Protocol (RDP) and Server Message Block (SMB) help tell the story…

RDP 40.0%
SMB 21.8%

Connections between OT zones

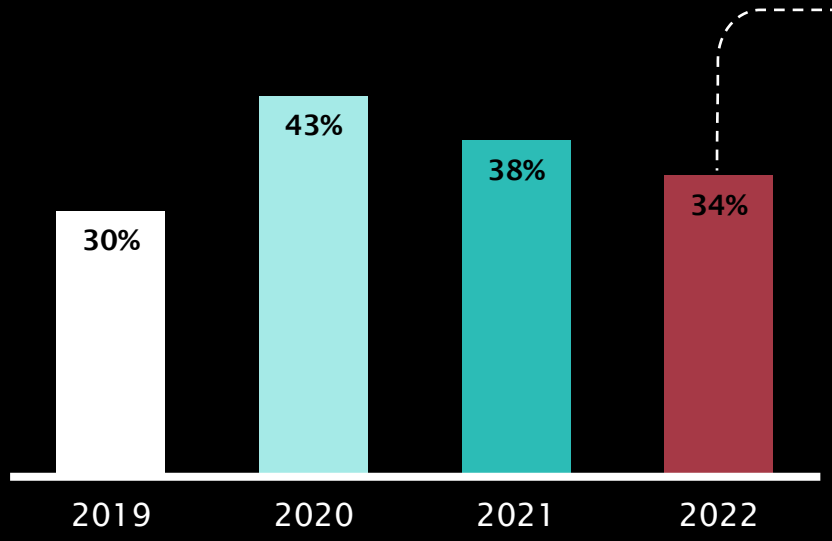
RDP 6.6%
SMB 3.6%

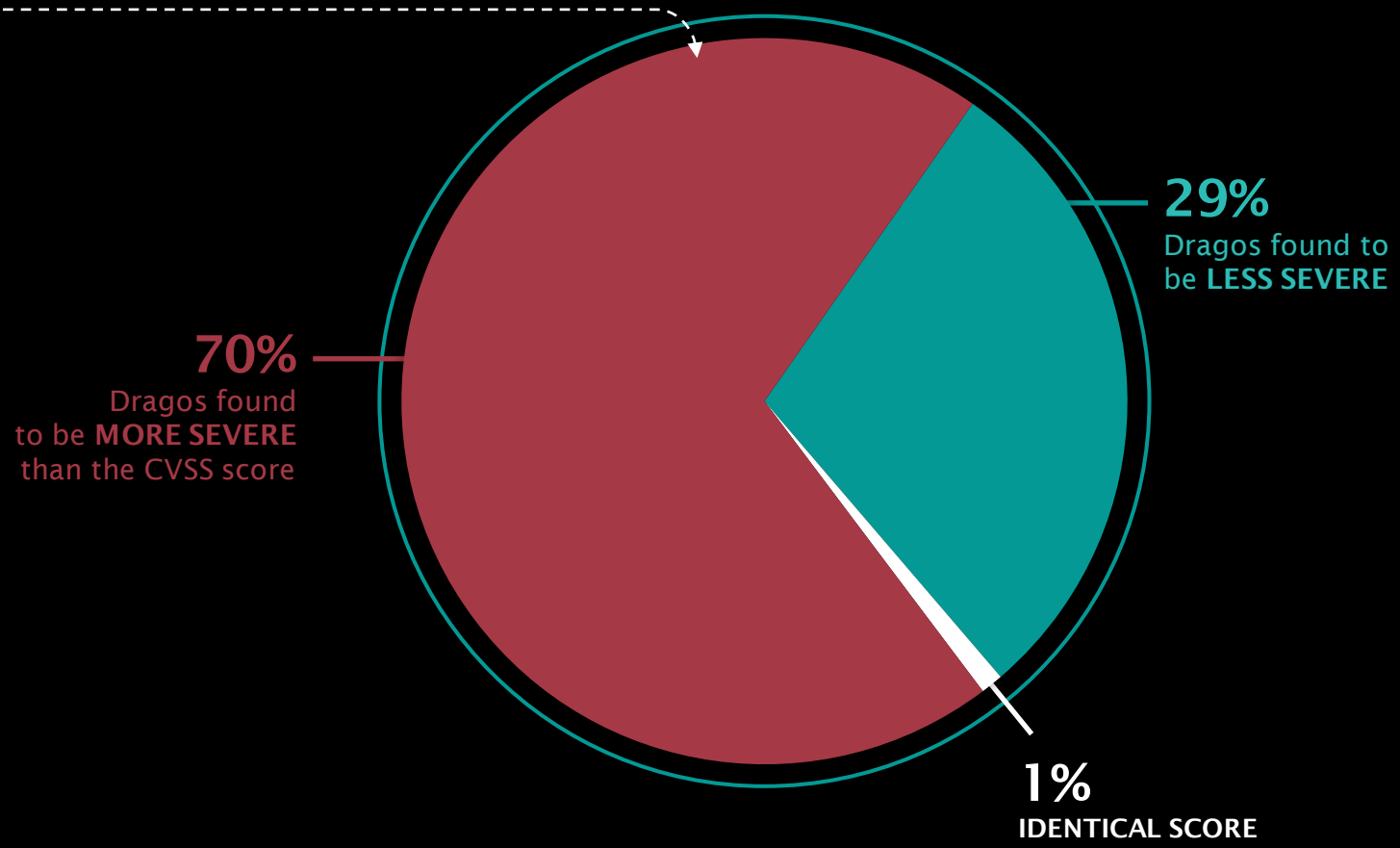
Connections existed between IT & OT zones

Even if an OT environment is not the target, ransomware can have an opportunistic impact due to these cross-zone network communication pathways.

THE STATE OF ICS/OT VULNERABILITIES

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



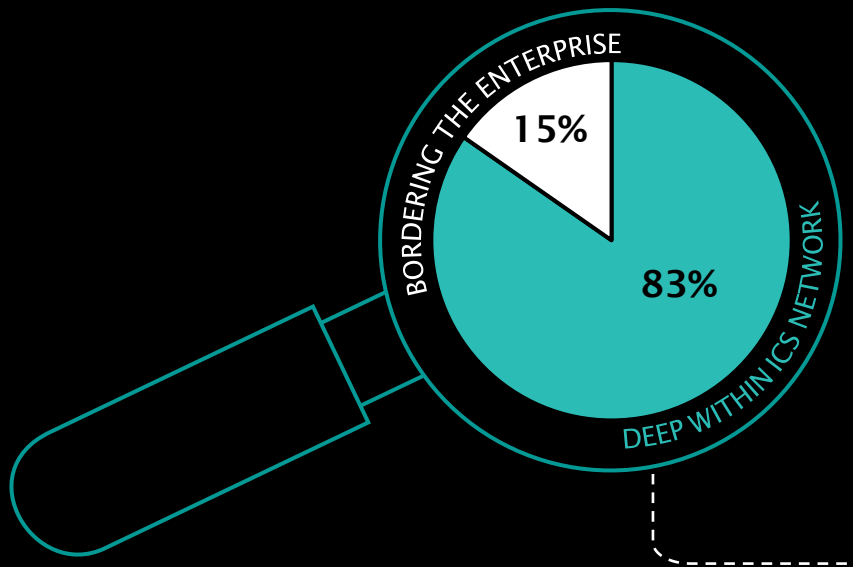


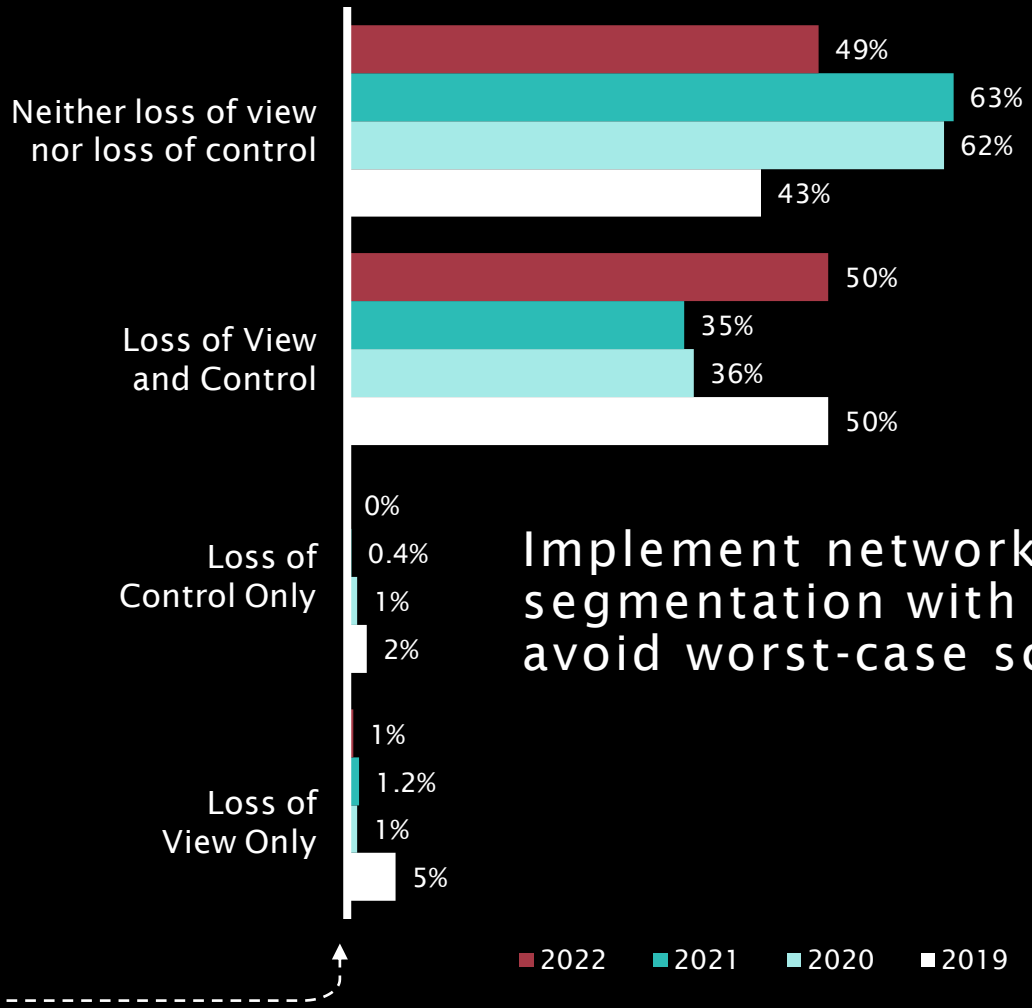
Dragos analyzed 465 advisories

34% had incorrect data

WHERE VULNERABILITIES EXIST

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





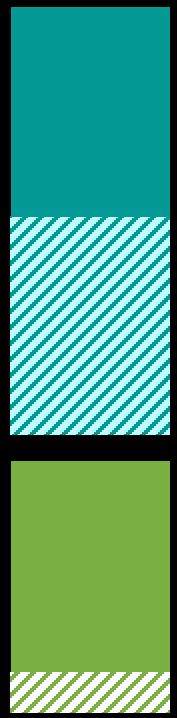
Implement network segmentation with MFA to avoid worst-case scenarios

PRACTICAL RISK MITIGATION IN ICS/OT

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

70%
Advisories with a patch

30%
Advisories with no patch when announced



51%
no practical mitigation

16%
no patch
no mitigation

77%
OVERALL NO PRACTICAL MITIGATION FOR ICS/OT FROM VENDOR OR CNA

CONSEQUENCE-BASED VULNERABILITY MANAGEMENT

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

ONLY 2%
OF ICS/OT VULNERABILITIES NEED TO BE ADDRESSED
NOW

68% of vulnerabilities
are network exploitable with no direct operational impact

Address these
NEXT

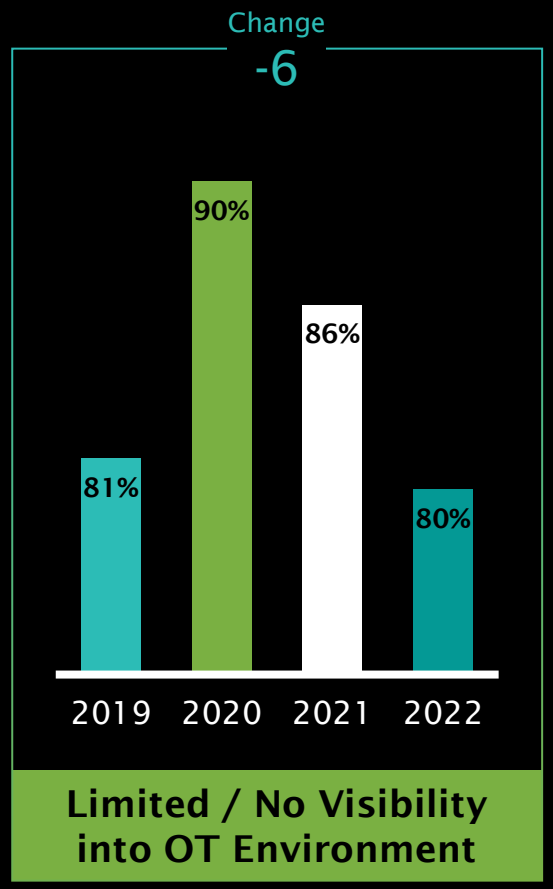
Mitigate through network monitoring, segmentation & MFA

30% of vulnerabilities
pose a possible threat but rarely require action

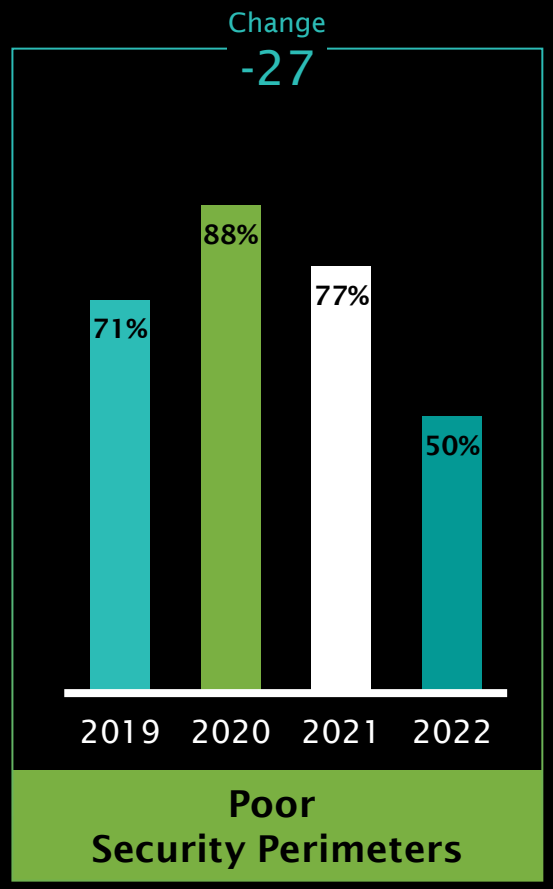
They likely NEVER need to be addressed

Monitor these for signs of exploitation

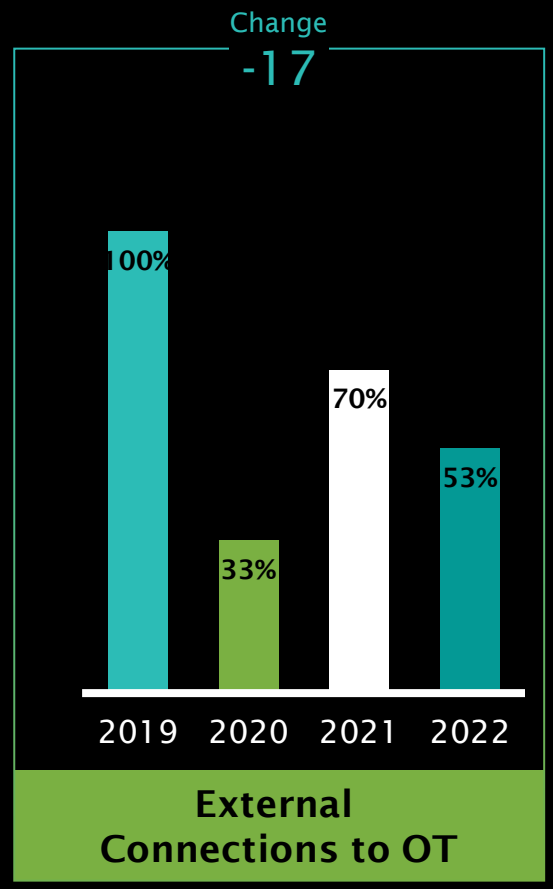
LESSONS LEARNED FROM CUSTOMER ENGAGEMENTS



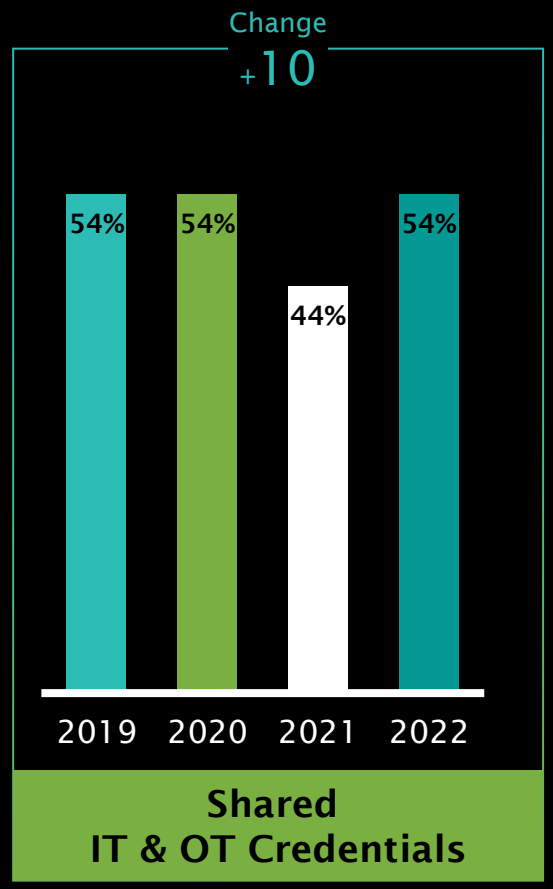
Limited / No Visibility into OT Environment



Poor Security Perimeters



External Connections to OT



Shared IT & OT Credentials

TSA* OIL & GAS PIPELINE REGULATIONS

REGULATIONS HAD A POSITIVE IMPACT TO RESILIENCE OF PIPELINE OWNERS & OPERATORS

In July, TSA released Security Directive Pipeline 2021-02C

Requirements include

- Creating a cybersecurity implementation plan
- Developing and maintaining a cybersecurity Incident Response plan
- Developing a cybersecurity assessment program

Dragos conducted Architecture Reviews for 20% of pipeline owners in scope of Pipeline-2021-02C and found:

- Asset visibility is still a challenge for pipeline owners & operators, but trends better than the OT industry average
- Network security perimeters are significantly better than the average OT industry
- Shared credentials are better than average
- External connections are on par with average

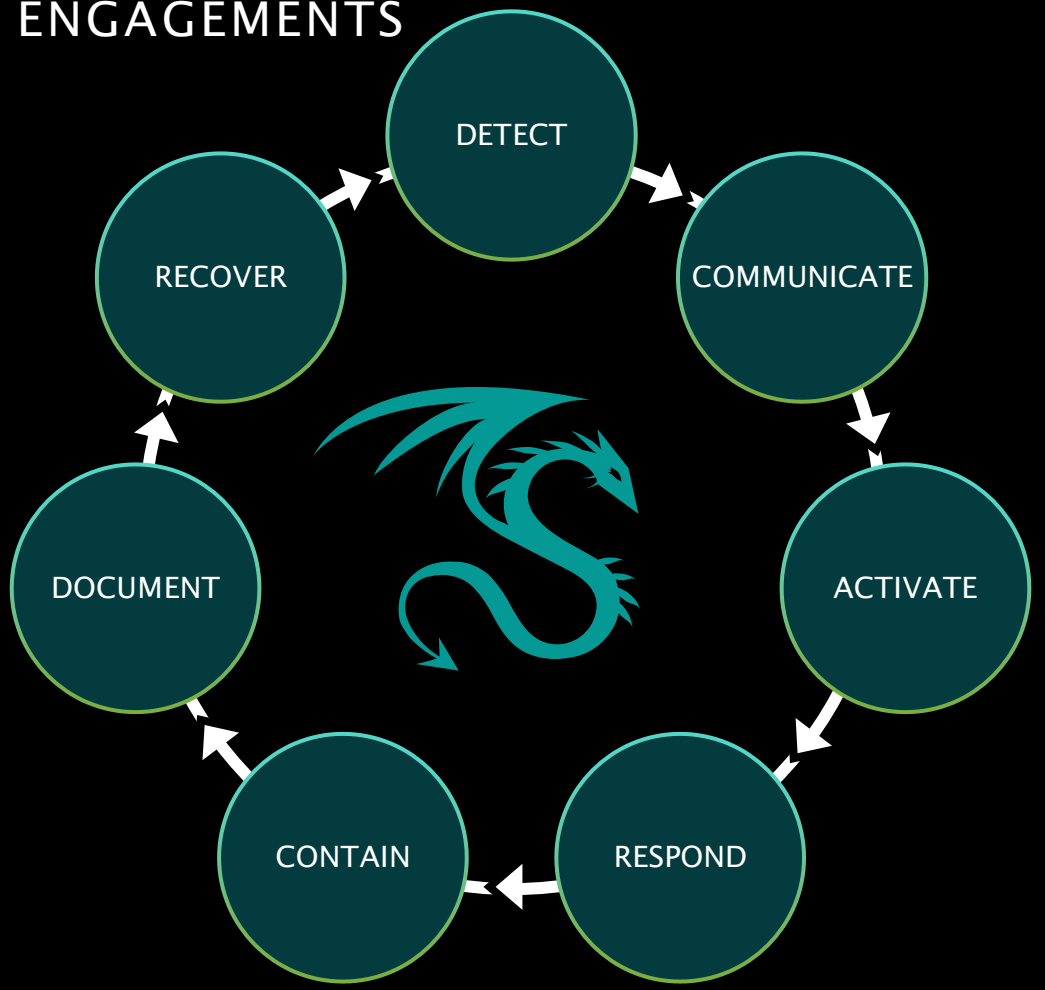
*U.S. Transportation Security Administration (TSA)

INCIDENT RESPONSE (IR) READINESS

300% INCREASE IN DRAGOS TABLETOP EXERCISE ENGAGEMENTS

Tabletop Exercises

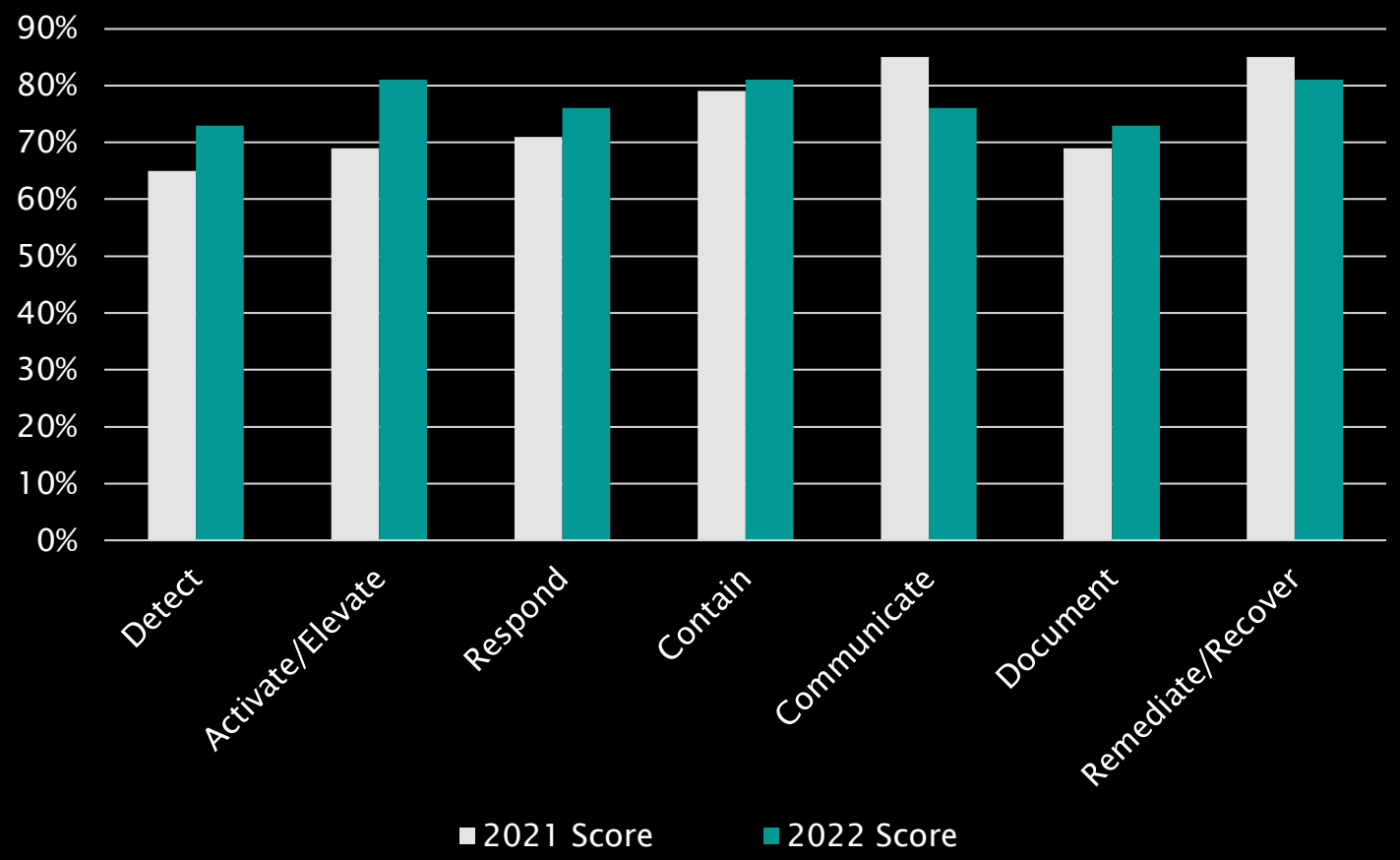
- Best way to test & refine IR plan
- Demonstrate how a realistic attack may occur in your OT environment
- Participants practice how they would respond using their current IR plans
- Evaluations are based on core capabilities for ICS/OT cybersecurity (see graphic)



CORE CAPABILITES FOR INCIDENT RESPONSE READINESS

ASSESSING IR READINESS WITH TABLETOP EXERCISES

Average Tabletop Exercise Scores Across Industries



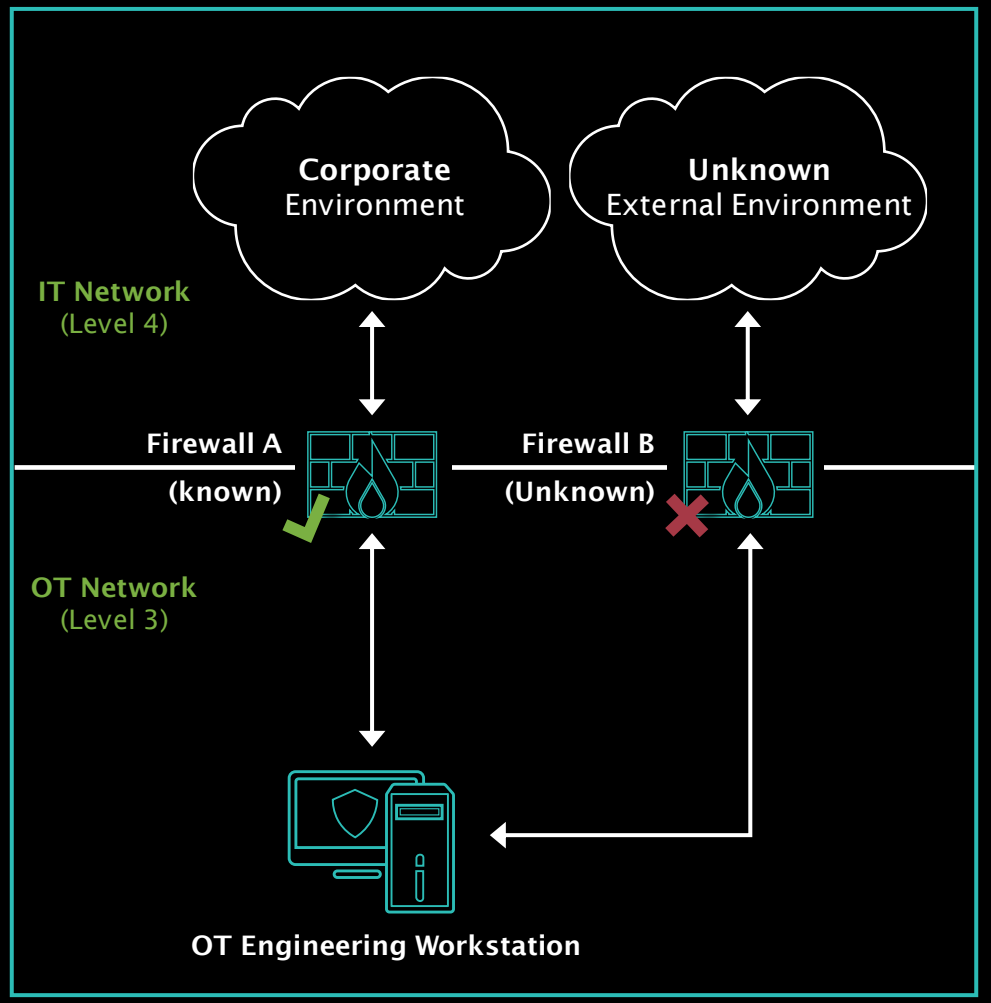
Key Takeaways

- While Detect saw an 8% increase, it remains the most challenging core capability for asset owners
- Detect and Document had the lowest aggregate scores, indicating they were the most challenging of all the core capabilities tested
- Activate/Elevate scores increased by 12% from 2021, leveling up from being performed with *some challenges* to being performed *without challenges*

RAIL INFRASTRUCTURE CASE STUDY

TAKING STEPS TO BUILD A SECURE OT ENVIRONMENT

- PCAP analysis during AR showed OT engineering workstation communicating externally with known IOC IP address
- Network Pen Test identified ‘known’ and ‘unknown’ external communications
- Client used IR plan to determine findings presented unacceptable risk, and hardened OT workstation as a result



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/