DRAGOS

ICS/OT CYBERSECURITY

YEAR IN REVIEW 2022

LESSONS LEARNED

Chrissy Grove
Curtis Chmilar
Eric Brown
Sumeet Jauhar
Markus Mueller
Hussain Virani

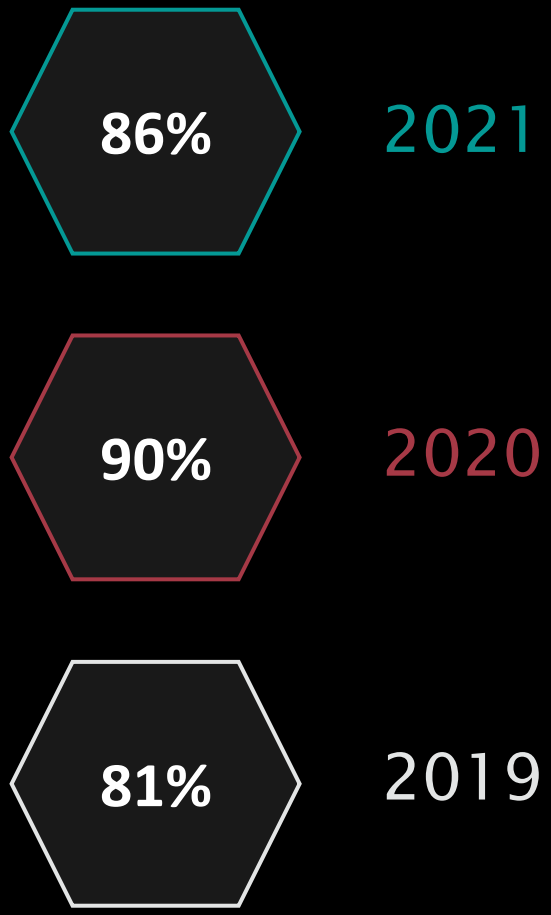
WHAT IS THE YEAR IN REVIEW?

Sixth year running!

LESSONS LEARNED FROM CUSTOMER ENGAGEMENTS

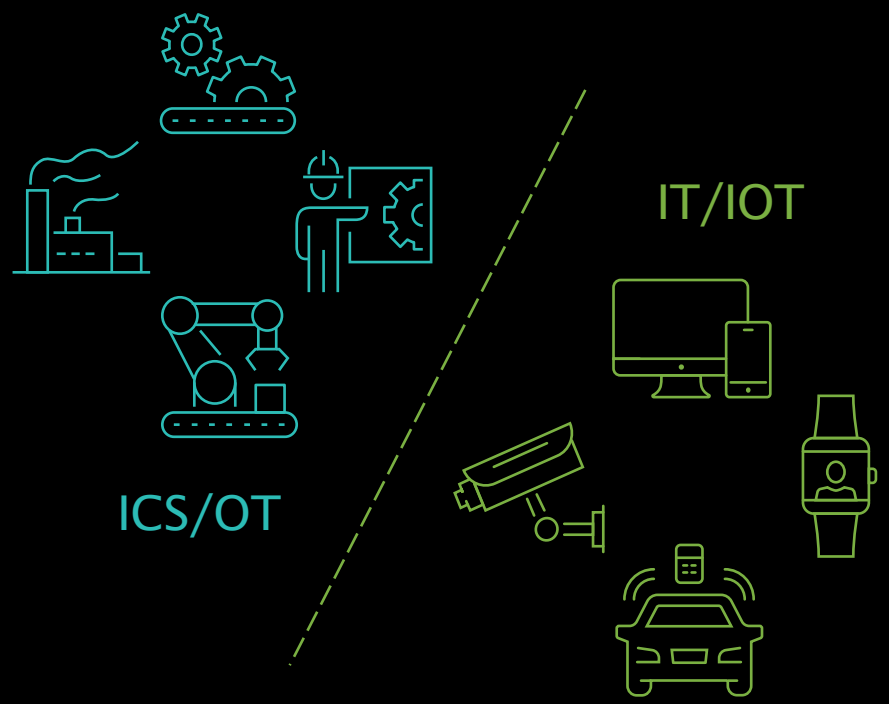
Limited or No Network Visibility

80% OF SERVICE ENGAGEMENTS IN 2022 HAD LIMITED TO NO VISIBILITY INTO THEIR ICS ENVIRONMENT



LESSONS LEARNED FROM CUSTOMER ENGAGEMENTS

Poor Security Perimeters



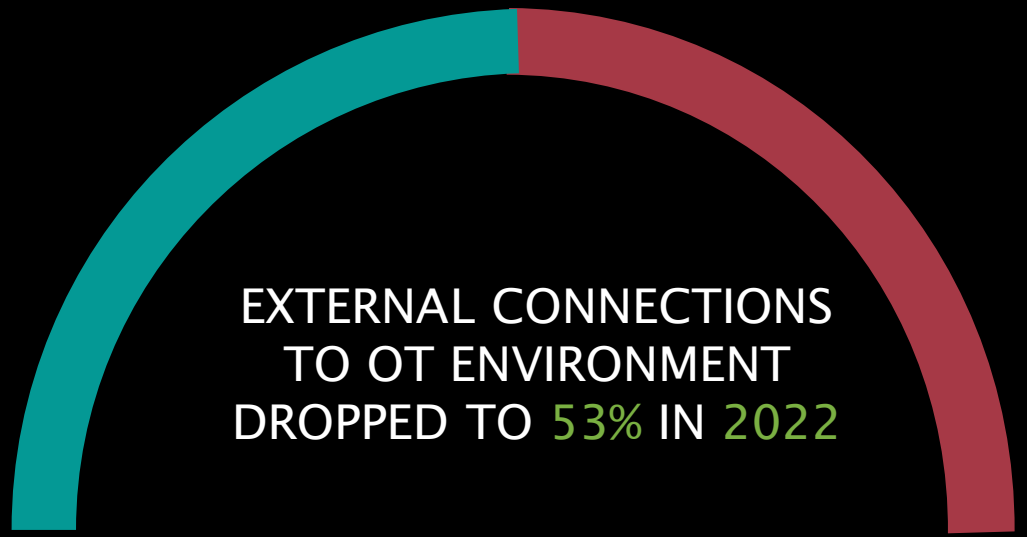
50% of SERVICE ENGAGEMENTS IN **2022** IDENTIFIED ISSUES WITH NETWORK SEGEMENTATION

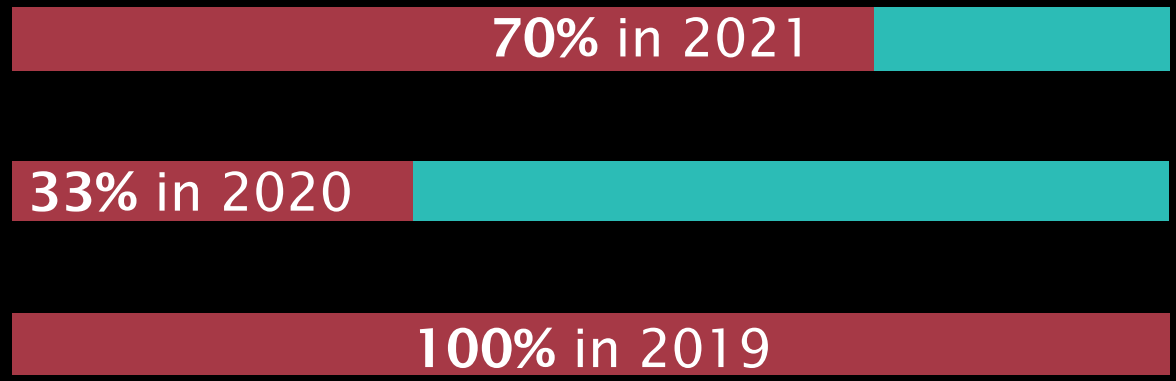
77%	88%	71%
2021	2020	2019

LESSONS LEARNED FROM CUSTOMER ENGAGEMENTS

External Connections to OT Environments

AN EXTERNAL CONNECTION IS ANY INTERNET PROTOCOL (IP) AND / OR ASSET THAT COMMUNICATED BEYOND A PRE-DEFINED SECURITY PERIMETER



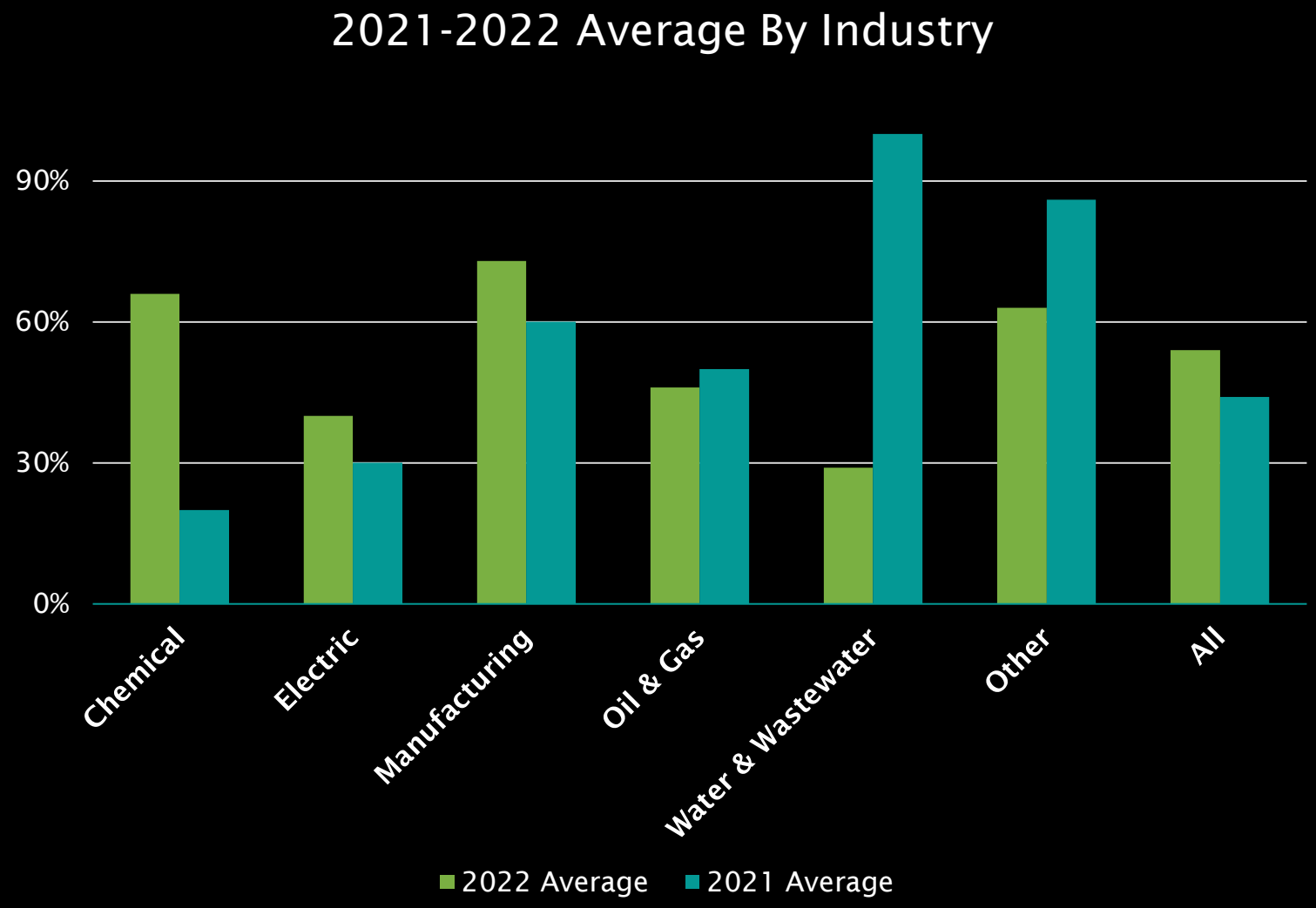


LESSONS LEARNED FROM CUSTOMER ENGAGEMENTS

Shared Credentials

IN 2022, 54% OF SERVICE ENGAGEMENTS INCLUDED FINDNGS RELATED TO SHARED CREDENTIALS

SHARED CREDENTIALS HAS REMAINED A CONSISTENT TREND OVER THE PAST 4 YEARS, STAYING AROUND 50%



INDUSTRY REGULATIONS

REGULATION CHANGES HAD A POSITIVE IMPACT

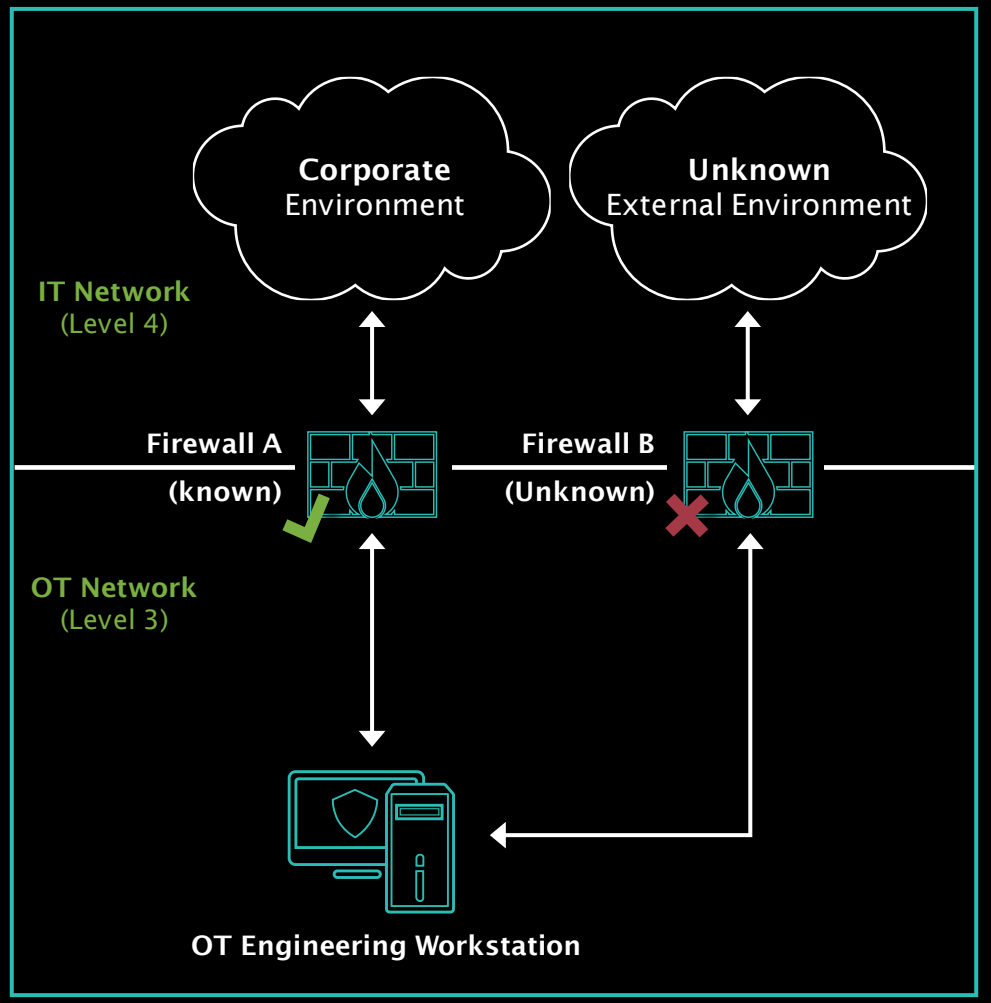
TSA released Pipeline-2021-02C in July 2022 shifting from a prescriptive, compliance-based standard to a functional, performance-based standard

SD-1580/82 was released for rail infrastructure in October 2022 using the SD 2021-02C as a foundation. Rail Operators identified to comply with this directive delivered Cybersecurity Implementation Plans for approval in February 2023

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

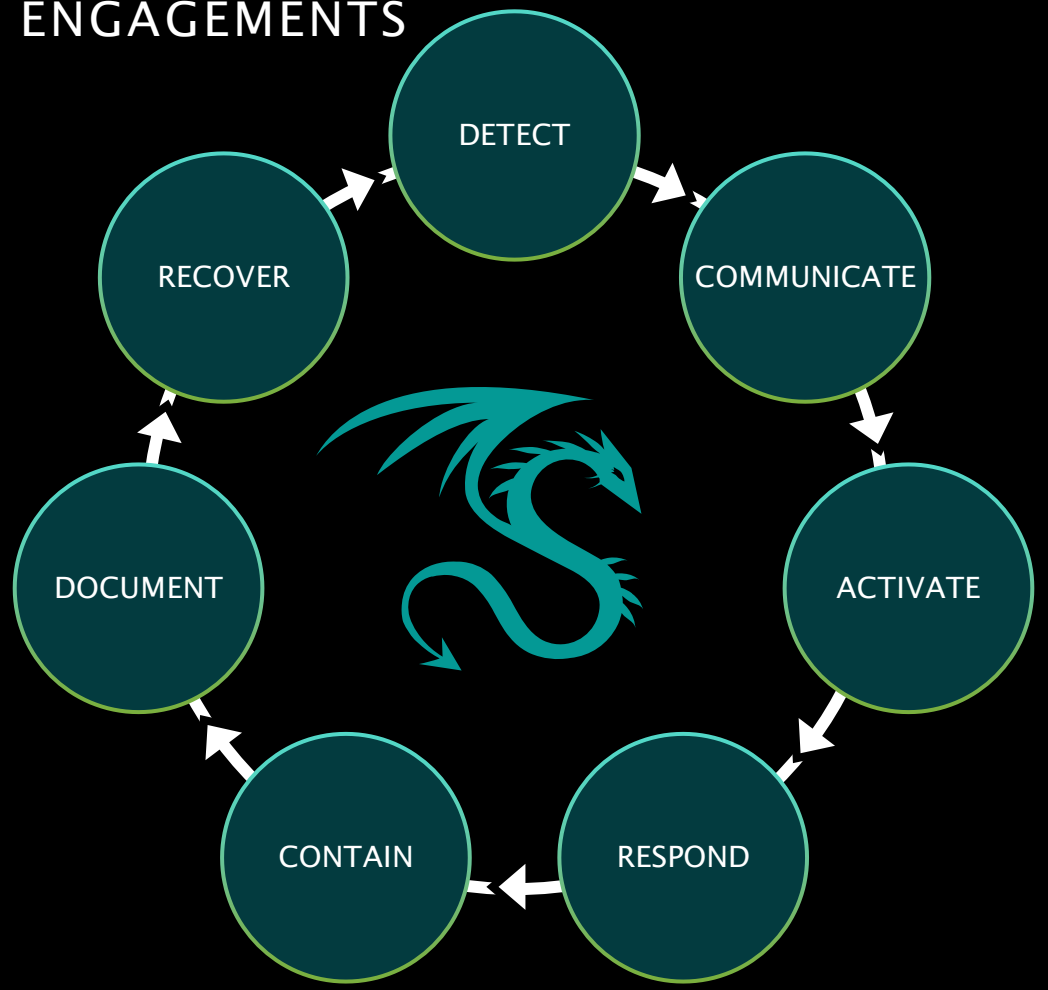


INCIDENT RESPONSE (IR) READINESS

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



CORE CAPABILITES FOR INCIDENT RESPONSE READINESS

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

QUESTIONS AND ANSWERS

THANK YOU

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