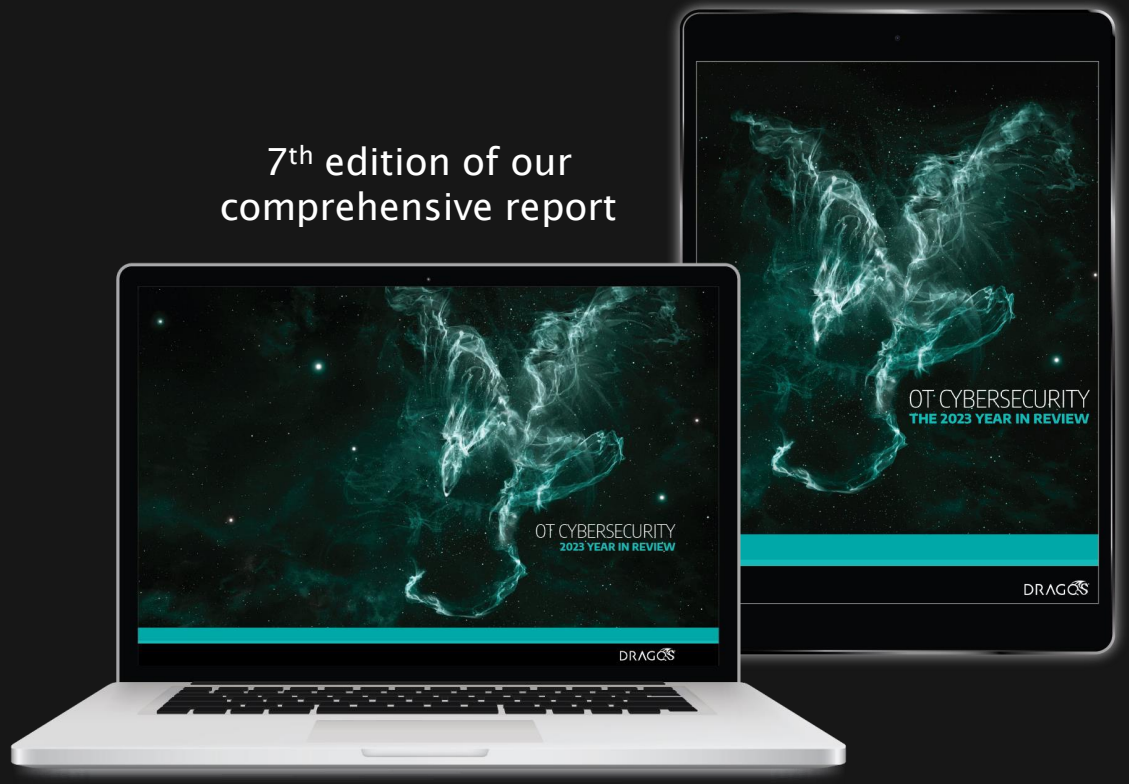
OT CYBERSECURITY

THE 2023 YEAR IN REVIEW

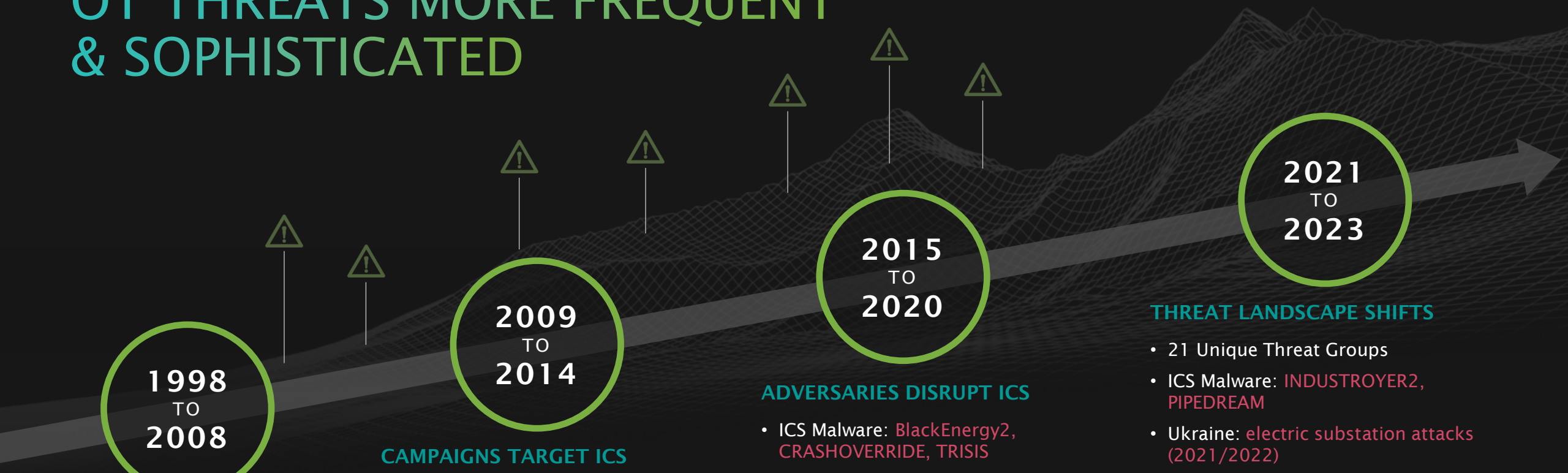
Robert M. Lee
Senior SANS Fellow
CEO & Co-Founder
Dragos, Inc.
@RobertMLee

WHAT IS THE YEAR IN REVIEW?

7th edition of our comprehensive report



OT THREATS MORE FREQUENT & SOPHISTICATED



1998 TO 2008

LACK OF COLLECTION

- Campaigns: APT1
- ICS Malware: None

2009 TO 2014

CAMPAIGNS TARGET ICS

- ICS Malware: Stuxnet, Havex
- Campaigns: Sandworm, Dragonfly
- Ukraine: Germany: 1st attack cause physical destruction on civilian infrastructure (steel)

2015 TO 2020

ADVERSARIES DISRUPT ICS

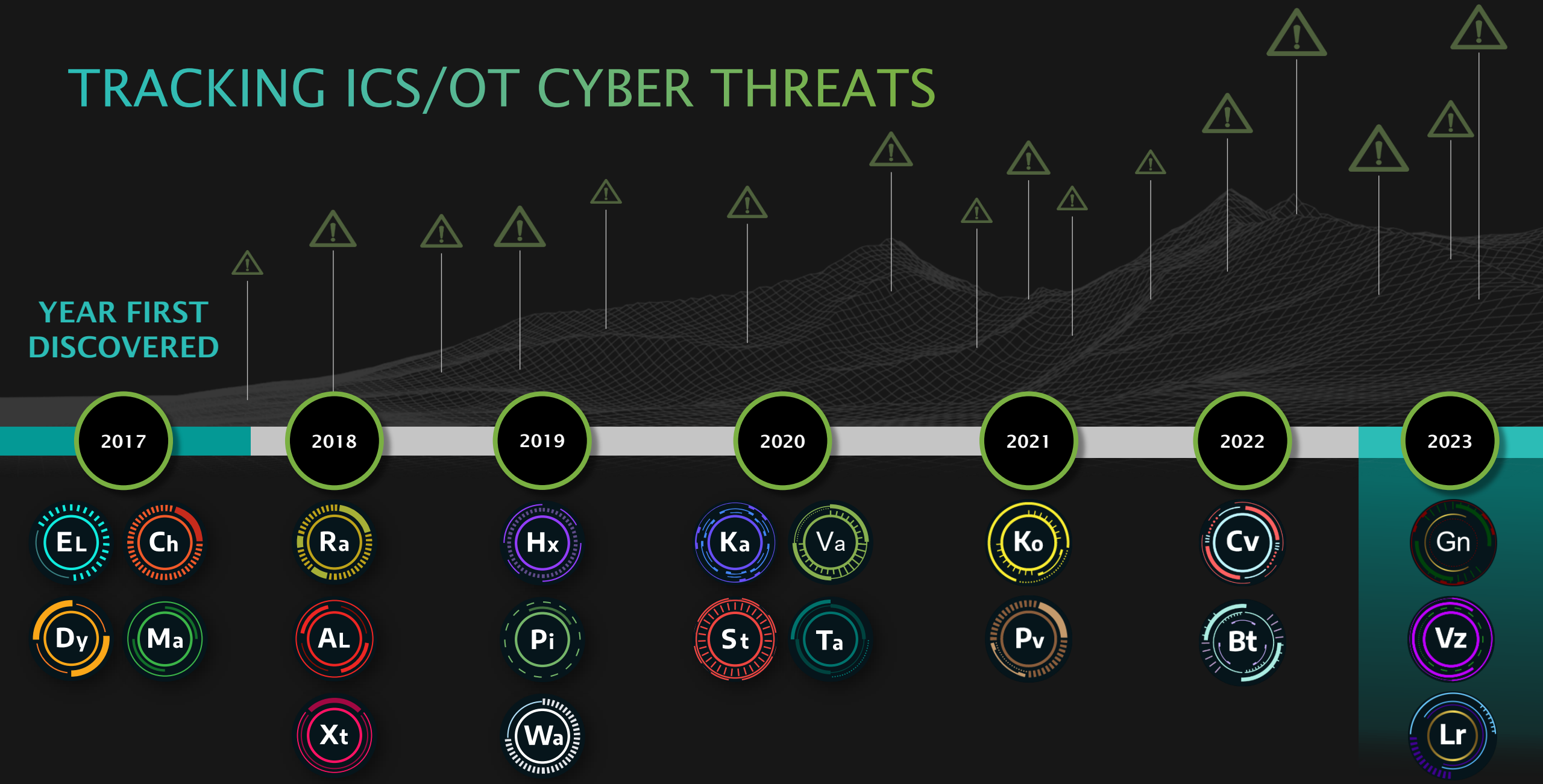
- ICS Malware: BlackEnergy2, CRASHOVERRIDE, TRISIS
- Campaigns: Dragonfly
- Ukraine: disruption of electric power operations (2015), major electric grid disruption (2016)
- Saudi Arabia: first attack targeting human life (2017)

2021 TO 2023

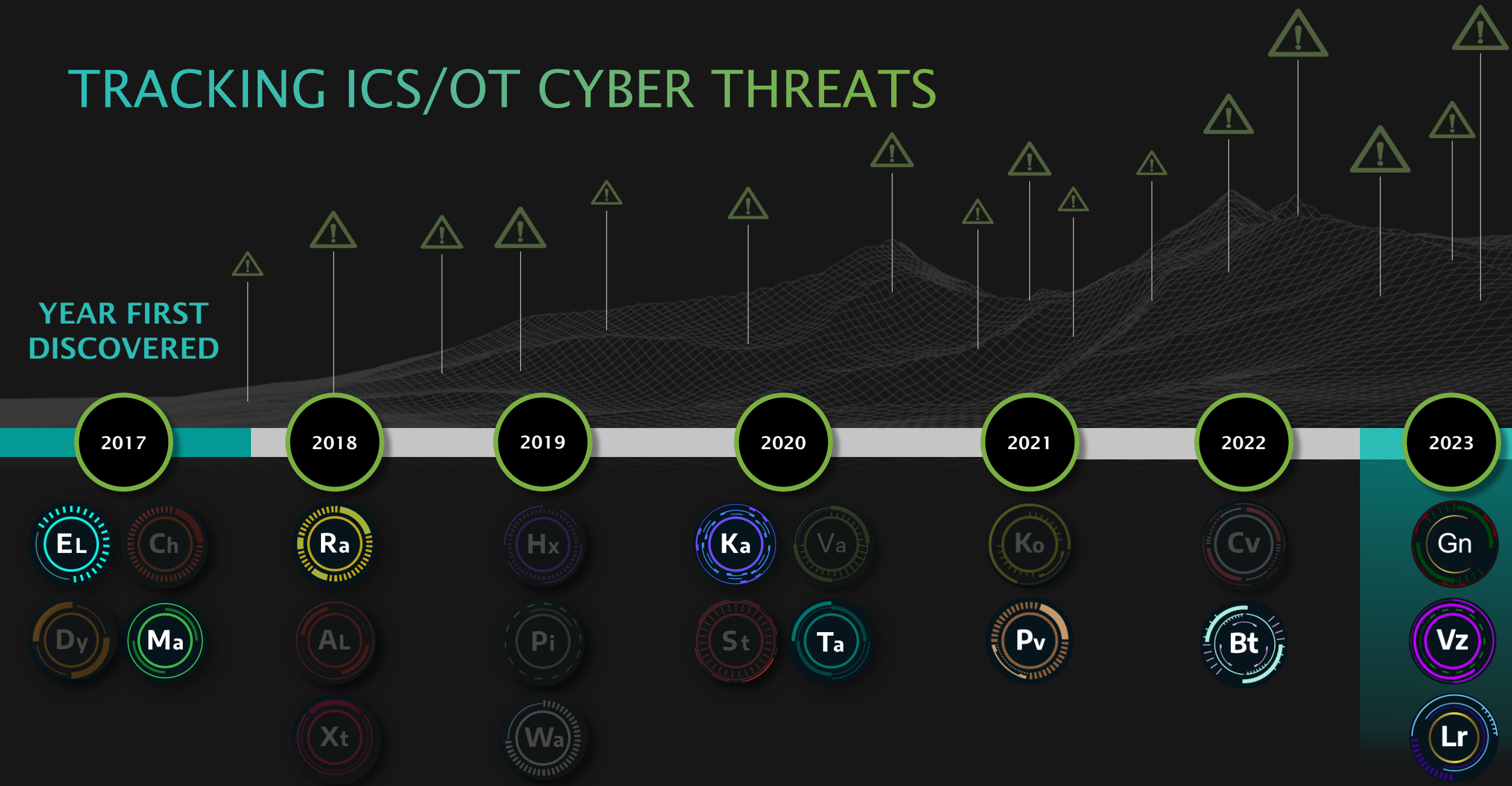
THREAT LANDSCAPE SHIFTS

- 21 Unique Threat Groups
- ICS Malware: INDUSTROYER2, PIPEDREAM
- Ukraine: electric substation attacks (2021/2022)
- Oldsmar, FL: Water Treatment attack
- Hacktivist Attacks: disruption of water utilities in U.S., Europe (2023)
- Ransomware attacks: Colonial Pipeline, JBS Foods, Norsk Hydro, Kojima, Foxconn, Dole, Yanfeng Automotive, Boeing

TRACKING ICS/OT CYBER THREATS



TRACKING ICS/OT CYBER THREATS



VOLTZITE

Heavy use of living off the land (LOTL) techniques. Evades detection with slow, steady reconnaissance.

TARGETS:

Electric Power Generation, Transmission & Distribution, Emergency Services, Telecommunications, Defense Industrial Bases, Satellite Services

INTENT/MOTIVATION:

Espionage & exfiltration, long-term persistent access.

VOLTZITE EXFILTRATION COULD FACILITATE FOLLOW-ON ACTIONS WITH PHYSICAL IMPACTS

KILLCHAIN ANALYSIS

		CAPABILITIES
Delivery	STAGE 01	Exploits internet accessible SOHO routers, uses them as intermediary hops back to ORB
Exploit	STAGE 01	Native Windows command line and PowerShell, Active Directory tools
Install/Modify	STAGE 01	Use of built-in proxy commands, open-source tools, & fast reverse proxy tool (frp
C2	STAGE 01	Initial access by exploiting edge network devices from Cisco, Ivanti, PRTG Network Monitor, Fortinet amongst others
Act	STAGE 01	Stages and exfiltrates sensitive operational data related to OT networks and processes

Overlaps with Volt Typhoon (Microsoft), BRONZE SILHOUETTE (Secureworks), Vanguard Panda (Crowdstrike), UNC3236 (Mandiant)

HUNTING FOR VOLTZITE

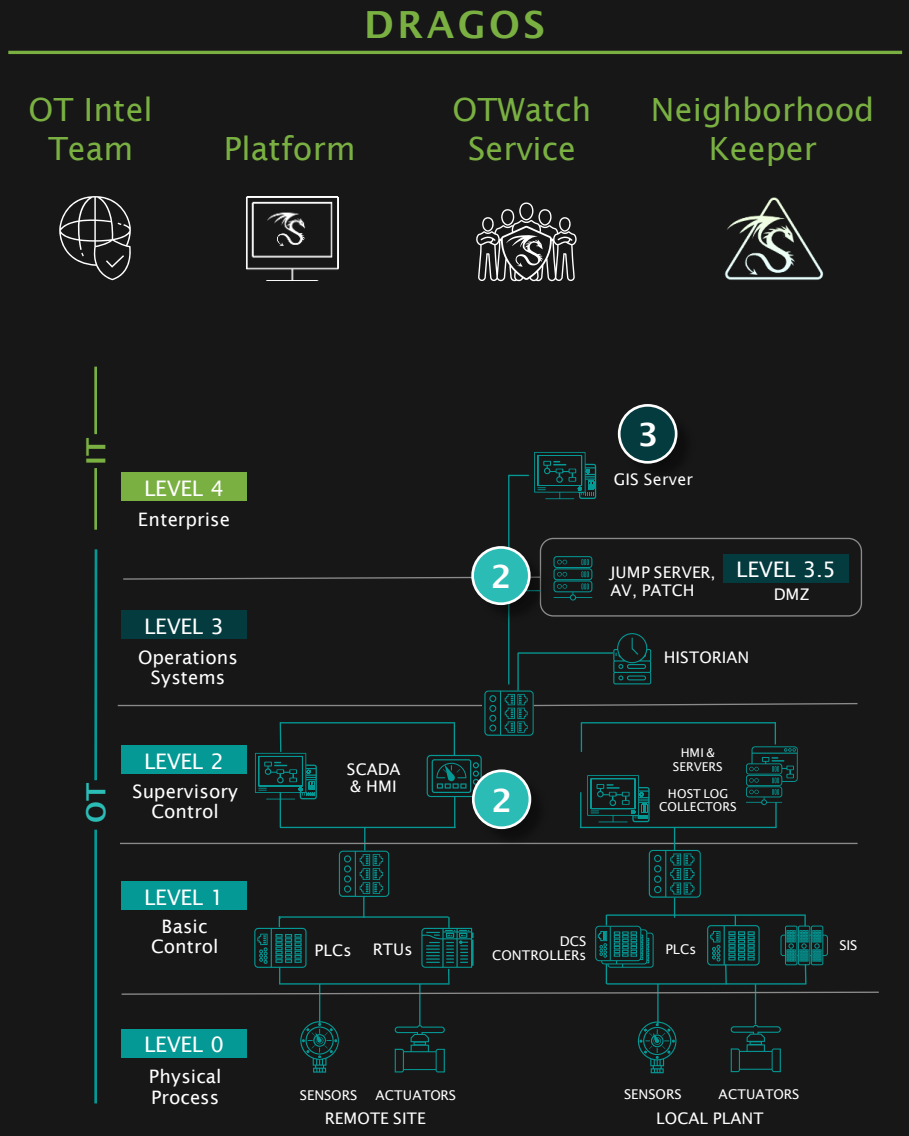
1. Dragos Intelligence VOLTZITE since early 2023 with regular behavioral detections codified in the Dragos Platform

2. New water & electric utility Customer deployed Dragos Platform at Level 3-4 (IT-OT traffic) & Level 2 (OT-OT traffic)

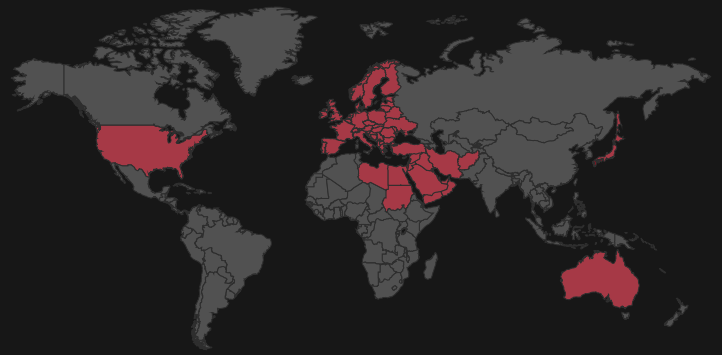
3. OTWatch conducted full hunt; Dragos Platform detected (Server Message Block) SMB traversal maneuvers in IT-OT network traffic.

4. OTWatch launches additional hunts across the fleet of subscribed customers; Intel analyzes Platform Neighborhood Keeper participants for indications of VOLTZITE behaviors, anonymously notifies impacted parties.

5. Intel works with detection engineering to develop high-fidelity detections for Platform deployed via Knowledge Packs.



LAURIONITE

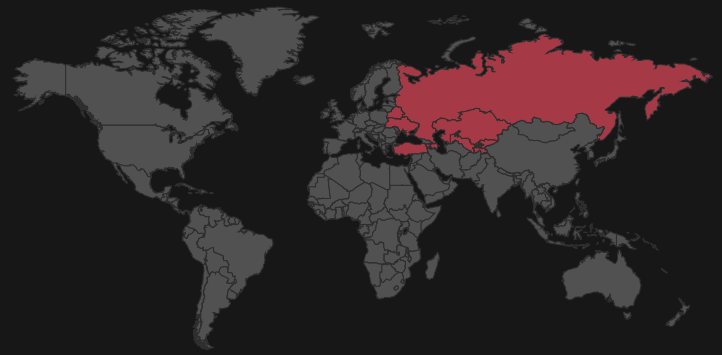


Observed exploiting internet-facing assets with Oracle E-Business with iSupplier exposed. Uses open-source tools, public POCs, known vulnerabilities.

TARGETS:
Air Transportation,
Professional Services,
Manufacturing Government

INTENT/MOTIVATION:
Espionage & exfiltration, long-term persistent access.

GANANITE



Credential phishing & domain masquerades, known exploits for initial access. Employs remote access trojans (RATs).

TARGETS:
Multiple industrial sectors: Electric,
Oil & Gas, Transport, Manufacturing,
Defense Organizations

INTENT/MOTIVATION:
Espionage & exfiltration

OTHER ACTIVE THREAT GROUPS IN 2023

KAMACITE

Used DarkCrystal remote access trojan (RAT) and LOTL techniques against electric entities in Ukraine

Facilitates initial access for ELECTRUM

Energy, Manufacturing
Europe, North America

ELECTRUM

CaddyWiper malware variants, also associated with the compromise of MicroSCADA software in a Ukraine substation in 2022

Electric
Ukraine

MAGNALLIUM

Password spraying operations against multiple industrial sectors

Multiple Industrial Sectors
Middle East, North America, APAC, Europe

RASPITE

Scanning for vulnerable SMB devices, password spraying operations

Multiple Industrial Sectors
US, Saudi Arabia, Europe, Japan

CYBERAV3NGERS HACKTIVIST GROUP

WEAK CREDENTIALS, INTERNET-FACING ASSETS ARE USED TO DISRUPT OT IN WATER UTILITIES IN U.S., EUROPE

November

Booster station belonging to the Municipal Water Authority of Aliquippa

25

26

CyberAven3gers posted the following message:

"Every Equipment
"Made In Israel" Is
CyberAv3ngers Legal Target!"

Images of compromised Unitronics Vision devices located in North America are shared online

27

28

The Full Pint Beer Brewery in Pittsburgh

29

December

30

Erris, Ireland water scheme

180 residents without running water for 2 days

1

Joint Cybersecurity Advisory warns of IRGC-affiliated actors exploiting PLCs in multiple sectors

LESSONS LEARNED FROM CUSTOMER ENGAGEMENTS

DRAGOS PROFESSIONAL SERVICES IDENTIFIED CRITICAL CYBERSECURITY WEAKNESSES IN OT IN 2023

Inadequately configured firewalls protecting OT

28%

Lacking or inadequate network segmentation

28%

1 in 10

Shared authentication domain architecture

20%

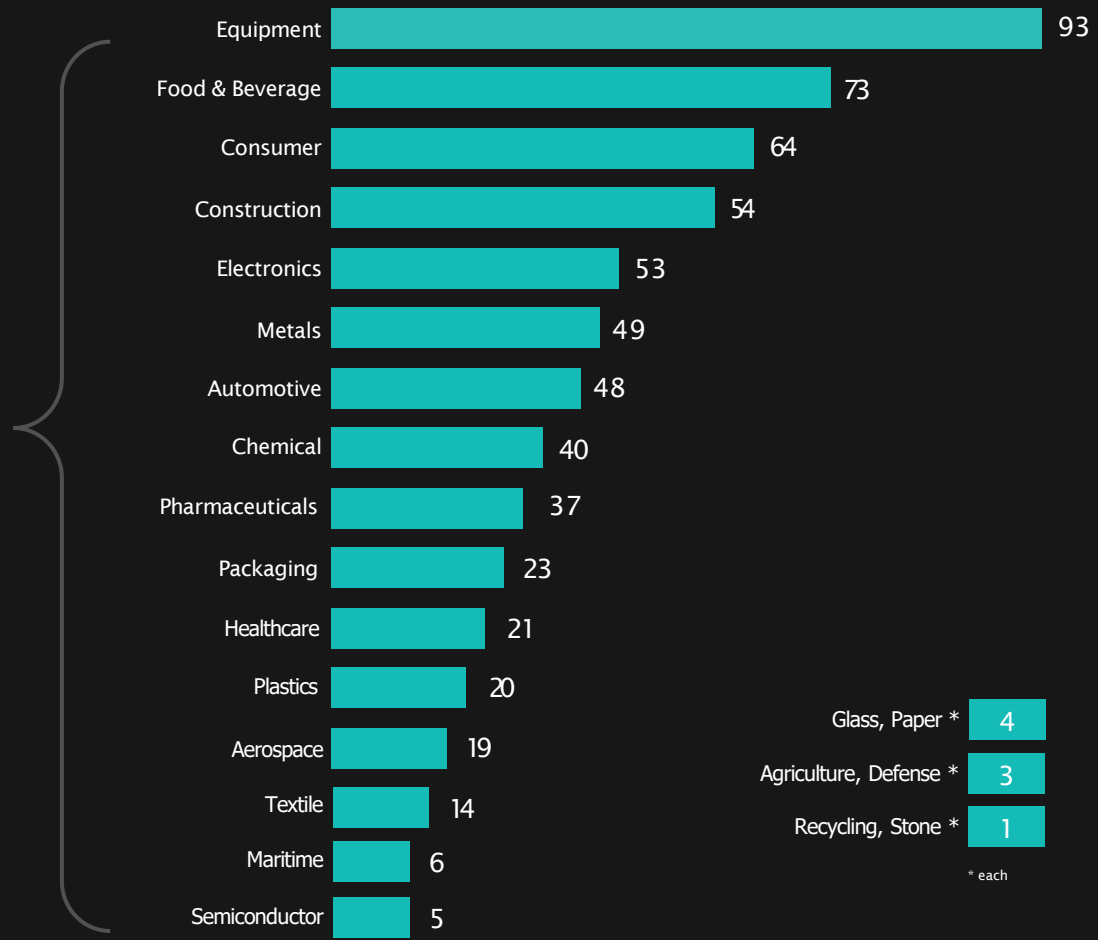
OT assets communicating with external addresses

RANSOMWARE ATTACKS INCREASED BY 50% IN 2023

RANSOMWARE IS CONSIDERED TO BE ONE OF THE TOP FINANCIAL & OPERATIONAL CYBER RISKS

RANSOMWARE BY ICS SECTOR

- **638** Manufacturing
- **115** Industrial Control Systems
- **65** Transportation
- **30** Oil & Gas
- **20** Electric
- **13** Mining
- **10** Water
- **10** Renewables
- **2** Government
- **2** Defense



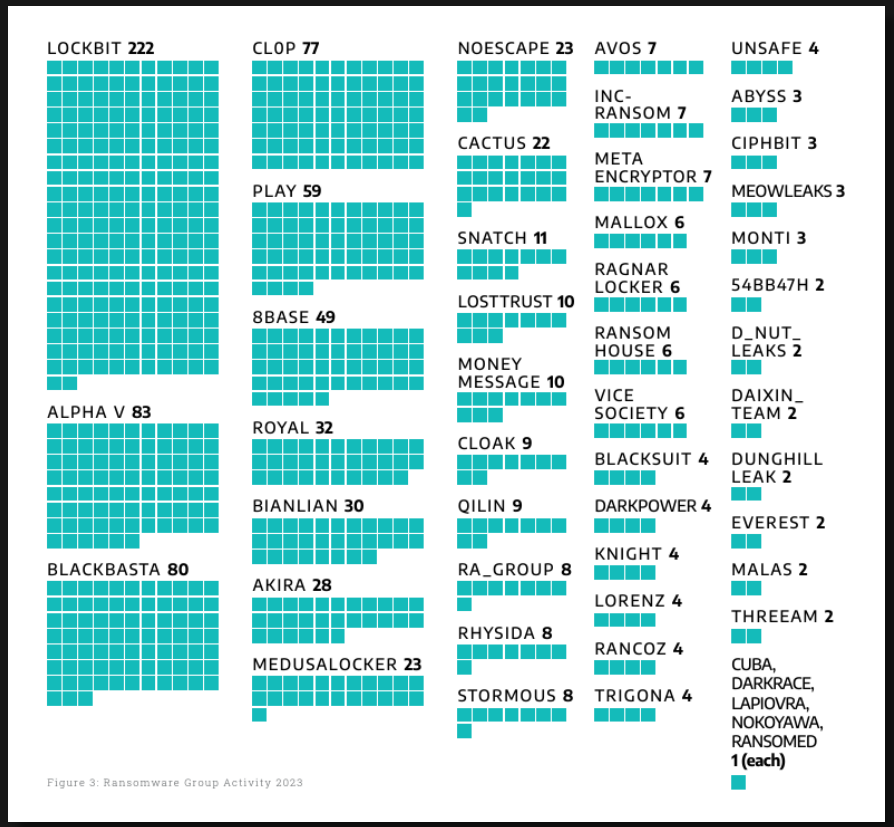
RANSOMWARE SPREADS IN FLAT NETWORKS

28% of customer engagements had findings of segmentation issues or improperly configured firewalls

RANSOMWARE GROUPS — MOVES AND CHANGES

25% OF RANSOMWARE ATTACKS INVOLVE LOCKBIT

ALPHAV + BLACKBASTA ACCOUNT FOR 9% EACH



= 1 RANSOMWARE ATTACK

50 ransomware variants

+ 28% / 2022

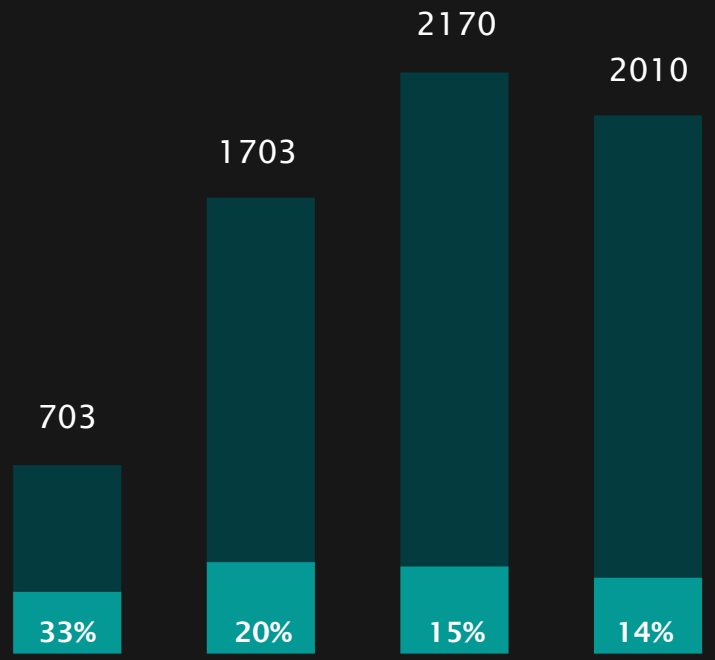
905 ransomware attacks

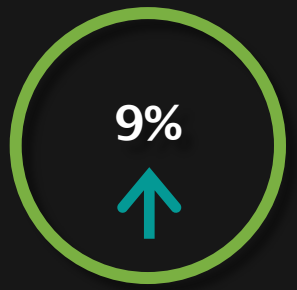
+ 49.5% / 2022

THE STATE OF ICS/OT VULNERABILITIES

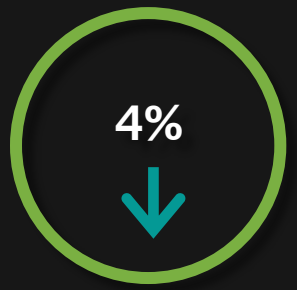
CVSS SCORES ARE OFTEN MISAPPLIED

TOTAL VULNERABILTIES ASSESSED ANNUALLY

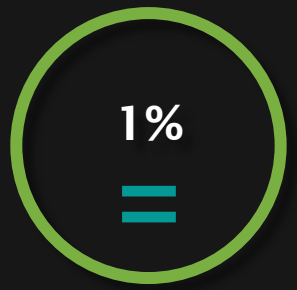




More Severe CVSS



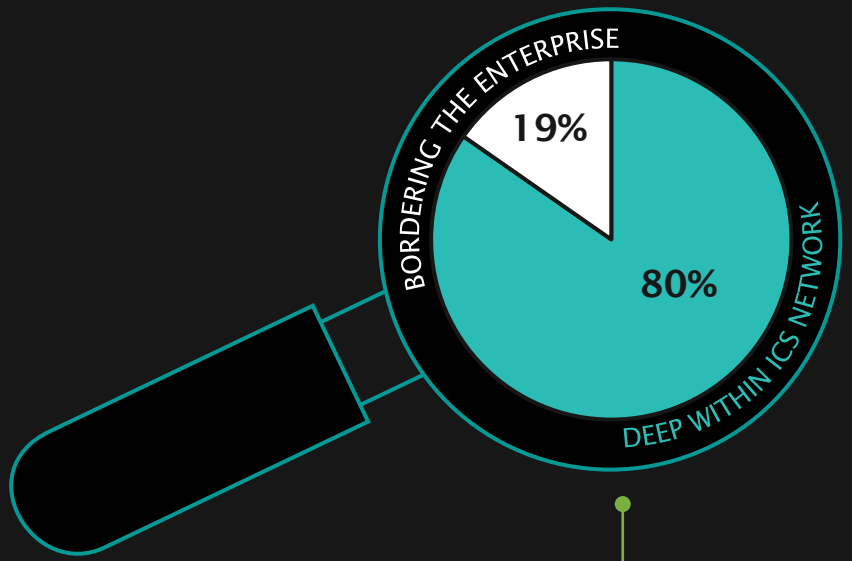
Less Severe CVSS

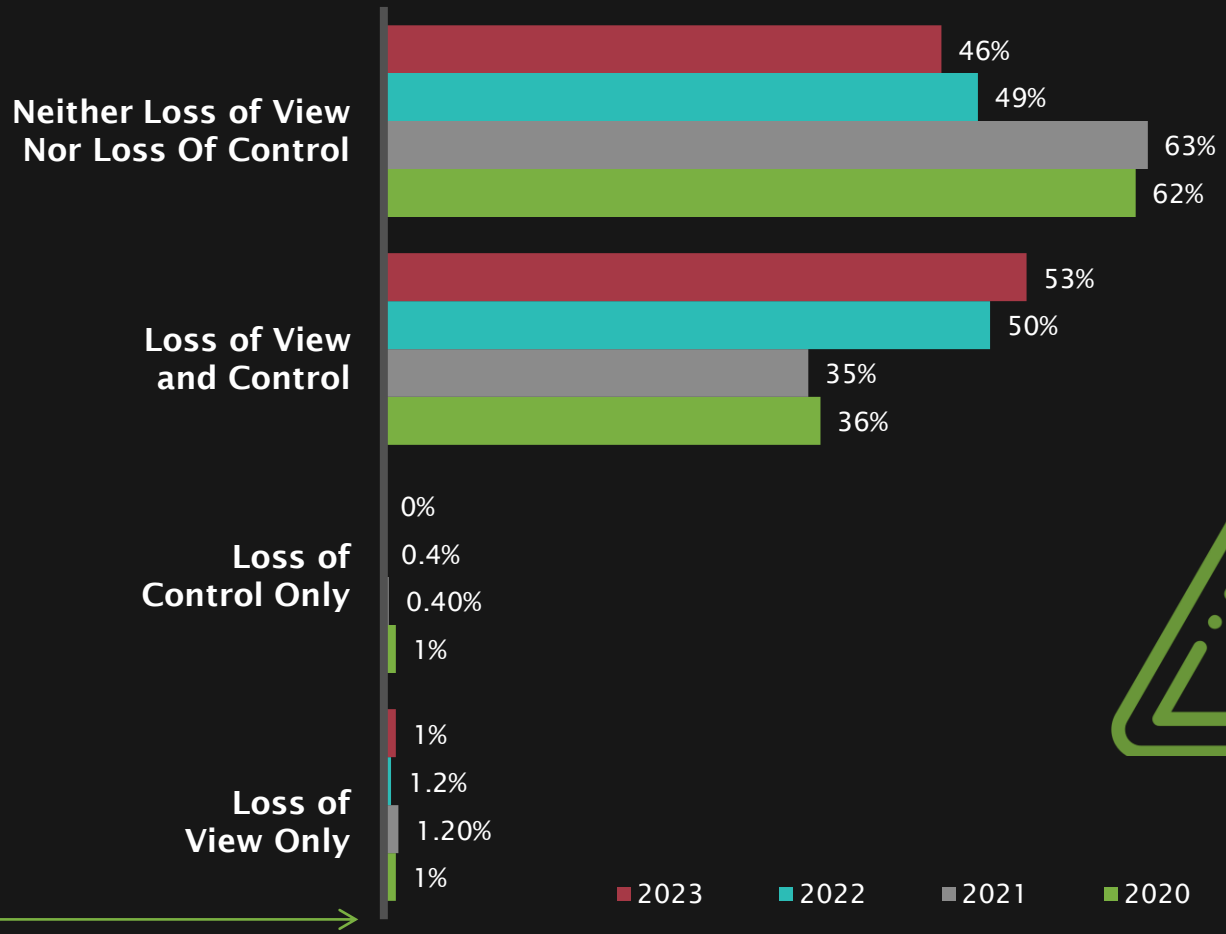


The Same

14% of vulnerabilities in 2023 had incorrect CVSS data

WHERE VULNERABILITIES EXIST





PRACTICAL RISK MITIGATION IN ICS/OT

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

72%
Advisories with a patch

28%
Advisories with no patch when announced

73%
CONTAIN NO PRACTICAL MITIGATION FROM THE VENDOR OR CNA

RISK-BASED VULNERABILITY MANAGEMENT

ONLY SOME VULNERABILITIES NEED IMMEDIATE ACTION

COLLECTIVE RESPONSE TO APT DEVELOPED EXPLOITS

APT DEVELOPED EXPLOITS

LOOK FOR ACTIVITY

DEPLOY ANALYTICS

The USG identified unknown vulnerabilities

Dragos worked with government agencies, Rockwell Automation, and other security vendors.

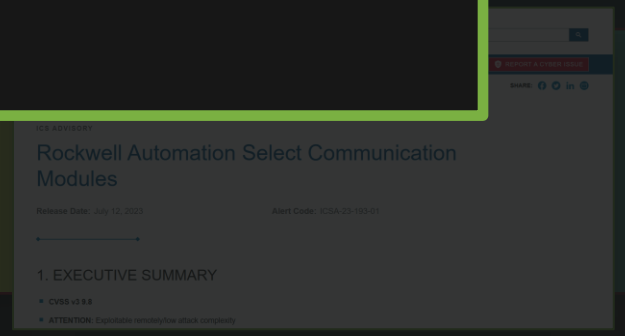
This collective response happened PRIOR to an attack taking place leading to a massive success.

WORKED WITH GOVERNMENT, ROCKWELL, OTHER SECURITY VENDORS

PCAP ANALYSIS

FIRMWARE REVERSE ENGINEERING

SIGNATURE/ ANALYTIC DEVELOPMENT



RELEASED JULY 12, 2023

OT WIN: COLLECTIVE RESPONSE TO VULNERABILITIES

VULNERABILITIES IDENTIFIED

USG identified unknown vulnerabilities

LOOK FOR ACTIVITY

*Leveraged **Neighborhood Keeper, OT Watch***

`# of assets + active exploitation`

DEPLOY ANALYTICS

Platform detections in KP-2023-004

NEIGHBORHOOD
Keeper Portal

Partner Intelligence Exchange

INDUSTRY Any | ORGANIZATION Any | ORG SIZE Any | REGION Any

Create Intel +

Proposed Detections	Approved Detections	Rejected	Occurences
2	106	2	13122

Date created	Organization	Intel type	Name	Description	Indicator	Status	Occurrences	Participants	First Seen
2023-07-12T 15:41	Dragos	Suricata-Rule	Rockwell Automation ControlLogix Vulnerabilities	ENIP CIP Vendor Specific Object Connected UCMM Parameter 2 With Unusual Length	See Rule	Approved			

DRAGOS INTELLIGENCE WORKED WITH GOVERNMENT, ROCKWELL, OTHER SECURITY VENDORS

100101001
010011010
101010101
100101011

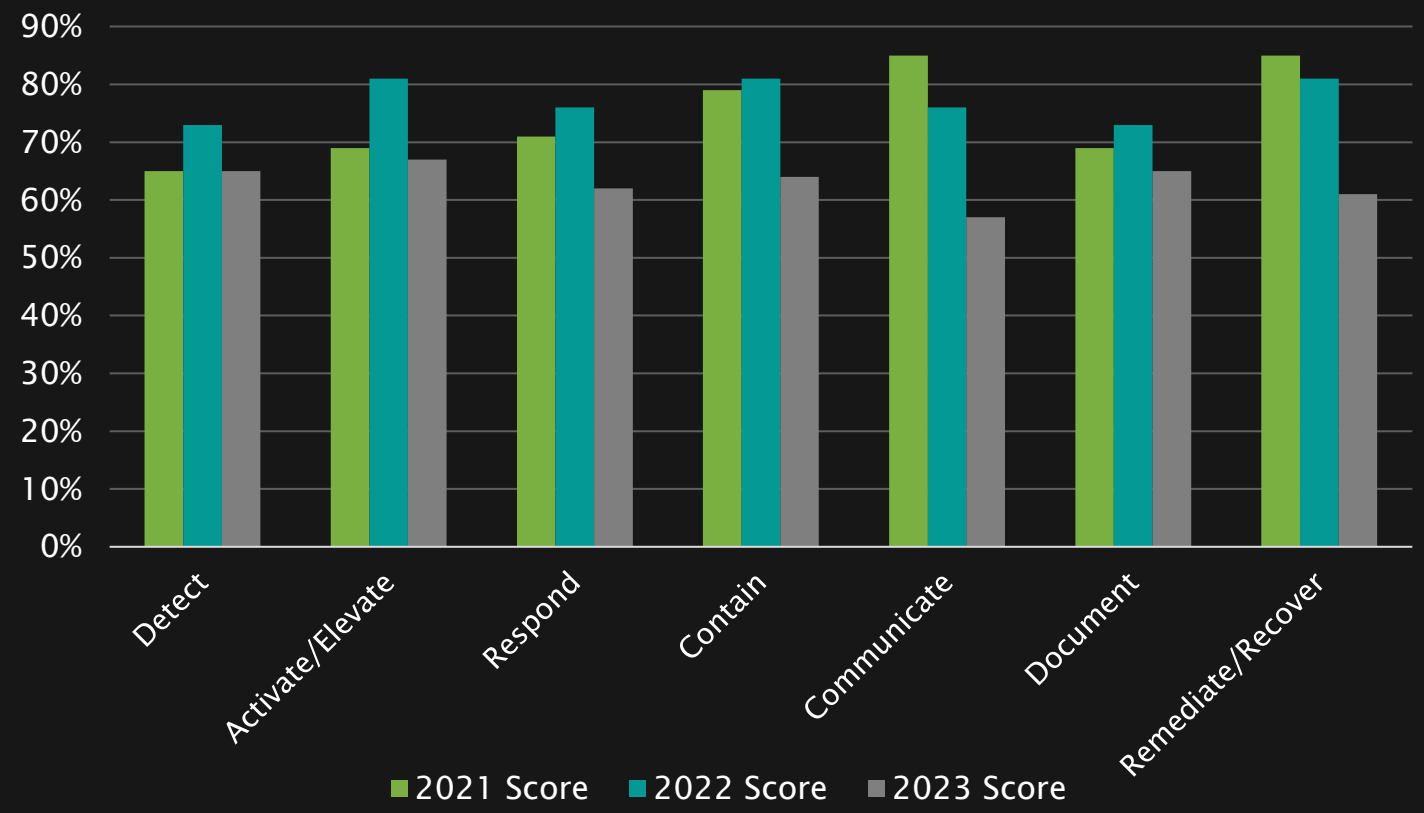
PCAP ANALYSIS

FIRMWARE REVERSE ENGINEERING

SIGNATURE/ ANALYTIC DEVELOPMENT

RELEASED JULY 12, 2023

ASSESSING IR READINESS WITH TABLETOP EXERCISES



- Detect saw an 8% decrease, continues to be a challenging core capability for asset owners
- Respond, Recover, & Communicate had the lowest aggregate scores, indicating they were the most challenging of all the core capabilities tested
- Performance drops across ALL core incident response capabilities

RECOMMENDATIONS

SANS

THE FIVE ICS CYBER SECURITY CRITICAL CONTROLS

	Reports with findings
01 ICS Incident Response Plan	38%
02 Defensible Architecture	46%
03 ICS Network Monitoring Visibility	61%
04 Secure Remote Access	29%
05 Risk-based Vulnerability Management	41%

QUESTIONS AND ANSWERS

ENHANCE YOUR OT THREAT PREPAREDNESS.

Download the Report:
dragos.com/year-in-review