Industrial AI and Digitization

What It Means to the Cyber Threat Landscape

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


Digitization and AI:
Productivity, Safety, Sustainability
DRAGOS

Digitization and AI:

But Also Threats

DRAGOS

OT Heritage:
Heterogeneous Environments

DRAGOS

The Move to Homogeneous Environments

DRAGOS


2017: First OT Attack to
Threaten Human Life

2022: CHERNOVITE

First Scalable, Repeatable Malware

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

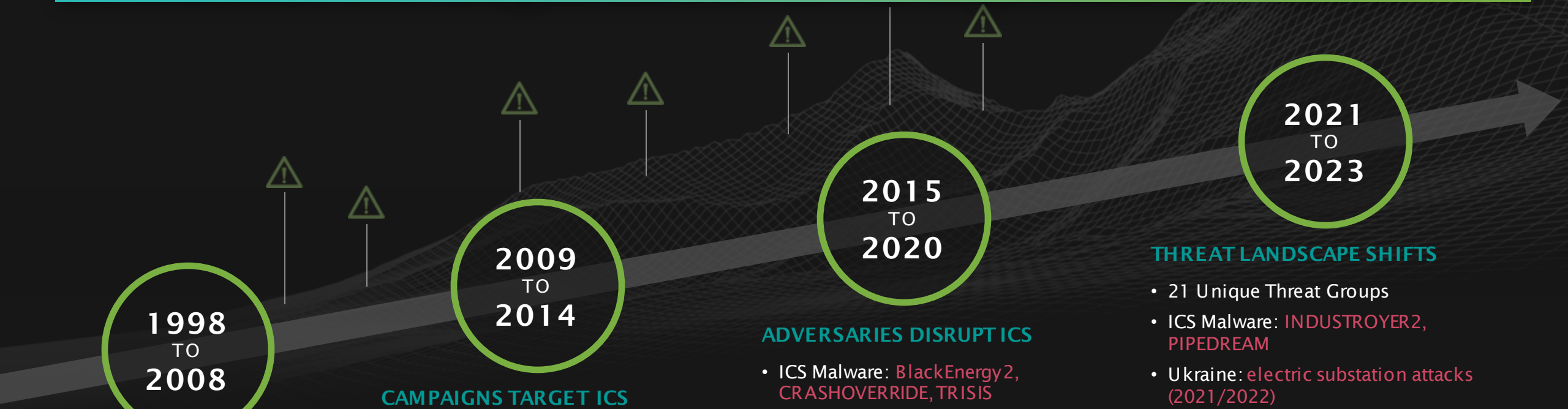
Tens of thousands of ICS vendors use CODESYS, Modbus, OPC UA

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

Threats Becoming

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)

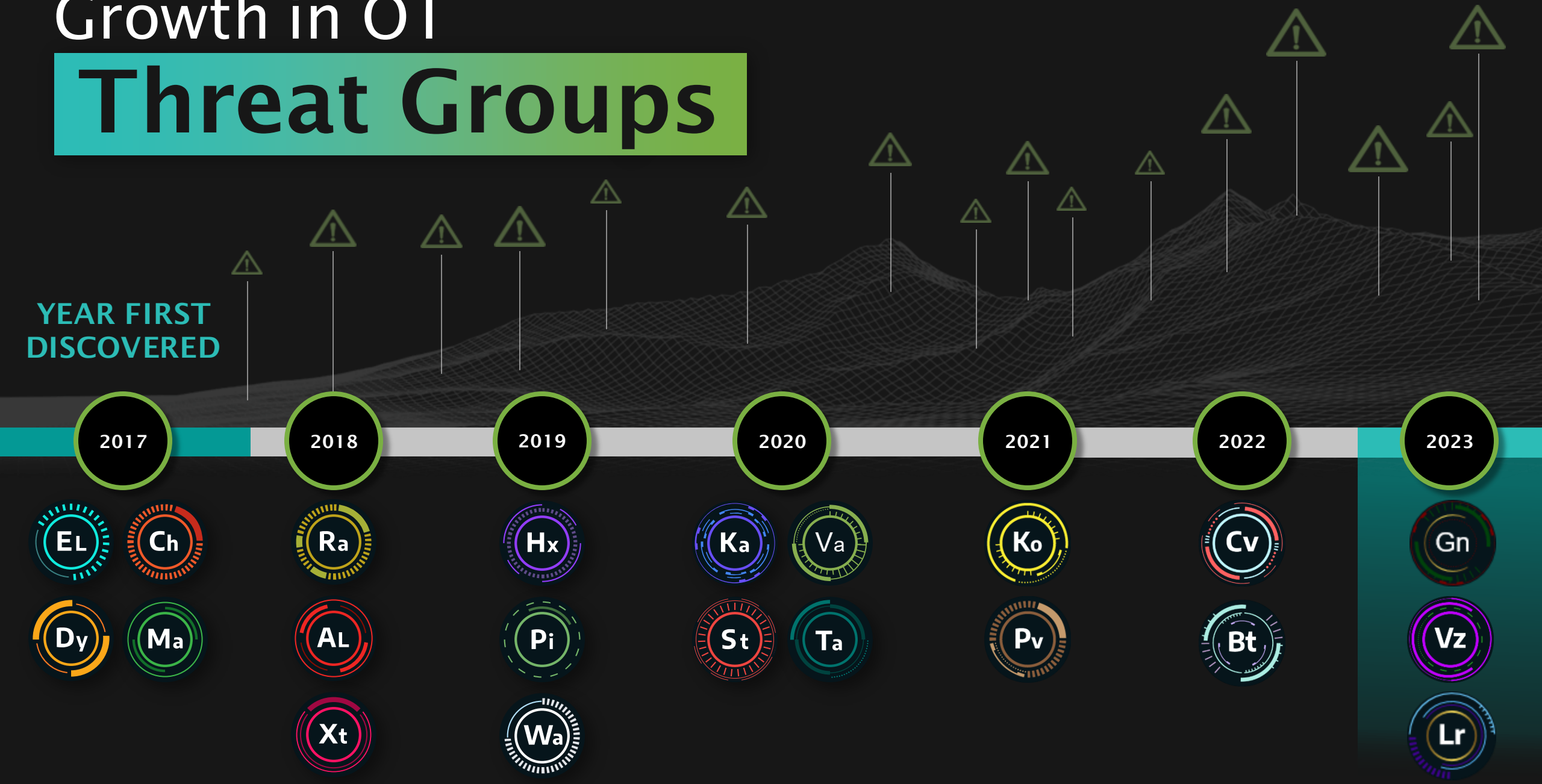
2021 TO 2023

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

Growth in OT

Threat Groups



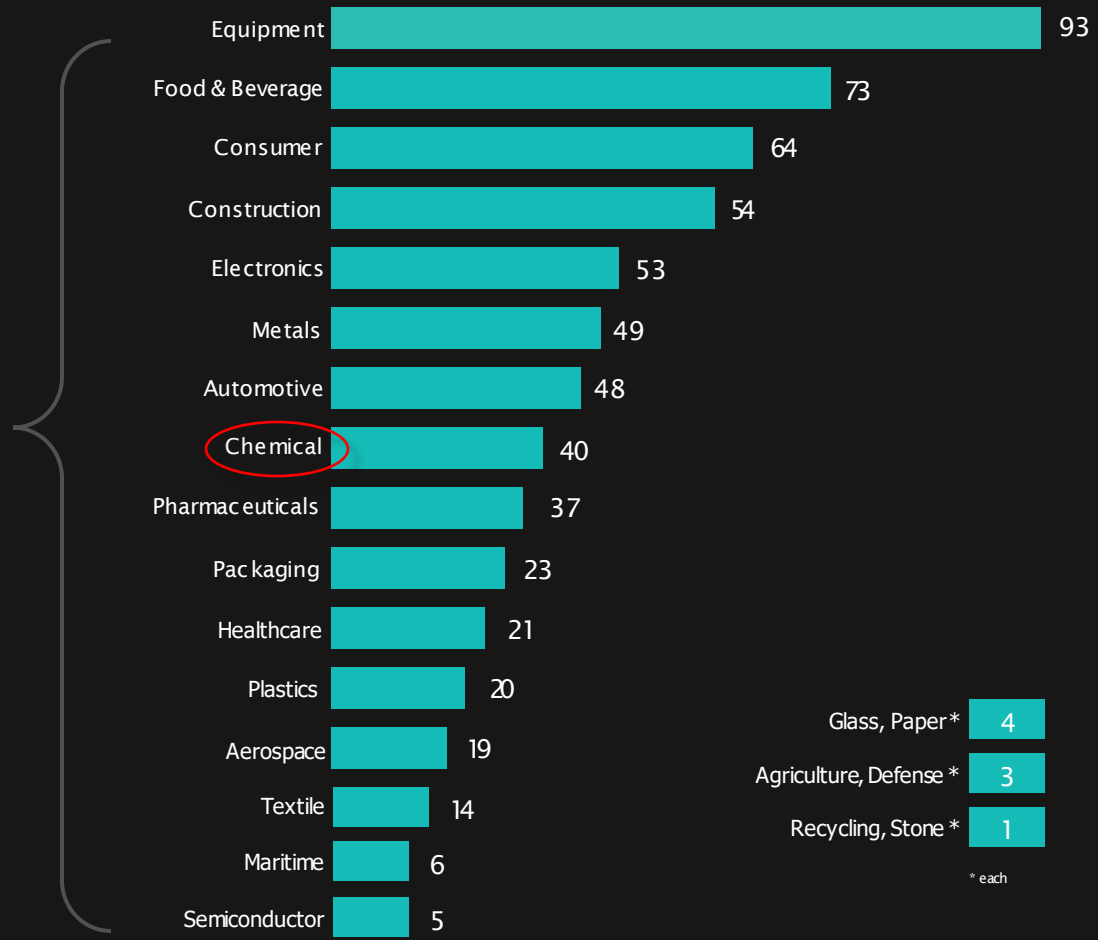
Ransomware

Targeting Manufacturing

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

Effective
OT Security

SANS

5

THE FIVE ICS CYBER SECURITY CRITICAL CONTROLS

01
ICS Incident Response Plan

02
Defensible Architecture

03
ICS Network Monitoring Visibility

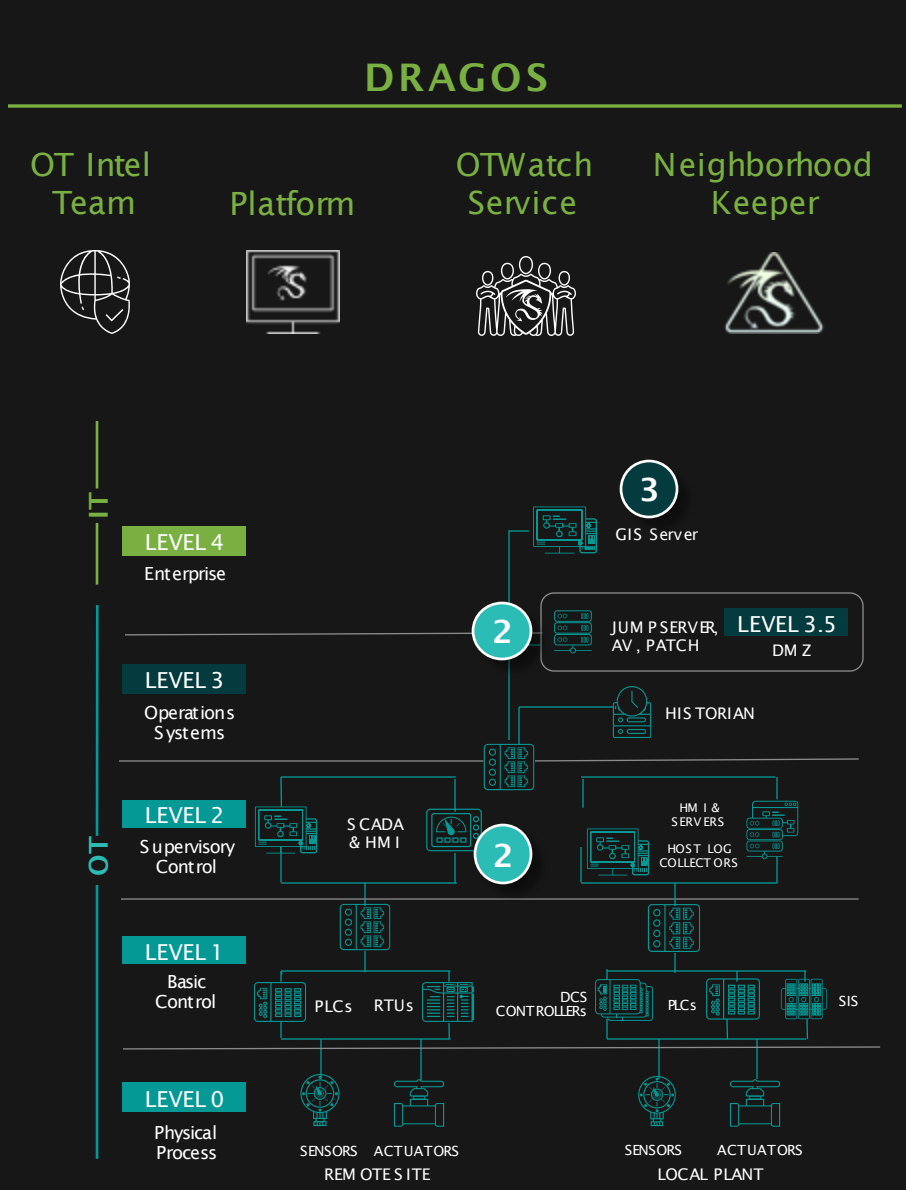
04
Secure Remote Access

05
Risk-based Vulnerability Management

DRAGOS

OT Cybersecurity in Action: 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.




Thank You!