DRAGOS

Intelligence-First Approach to OT Cybersecurity

Understanding the critical role of OT threat intelligence

Josh Hanrahan
Principal Adversary Hunter

Josh Hanrahan

Principal Adversary Hunter

Global Electric Industry Focused Adversary Hunter

Previous:

- Lead Threat Hunter @ Commonwealth Bank
- Threat Intelligence Analyst @ Australian Energy Market Operator (AEMO)

Certs:

- GIAC Certified Forensic Analyst (GCFA)
- GIAC Reverse Engineering Malware (GREM)
- GIAC Cyber Threat Intelligence (GCTI)
- Bachelor of Information Technology (BInfoTech)
- Graduate Certificate in Cyber Security (GradCertCyberSec)

Contact:

- jhanrahan@dragos.com
- @cyberbubblez
- www.nocht.org

AGENDA

1. Dragos Threat Discovery
2. Defining Cyber Threat Intelligence
3. Industrial Threat Landscape
4. Case study: KAMACITE/ELECTRUM
5. Operationalizing OT Threat Intel

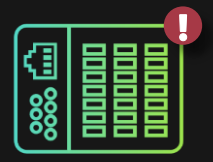
CYBER THREAT INTELLIGENCE FOR OT

Largest private cyber threat intelligence team focused entirely on ICS/OT threats

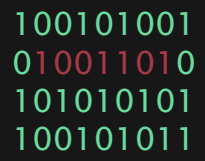
DRAGOS THREAT INTELLIGENCE TEAM

WHAT WE DO

Threat Discovery



Vulnerability Analysis



Malware Analysis

Detection Engineering

DRAGOS WORLDVIEW

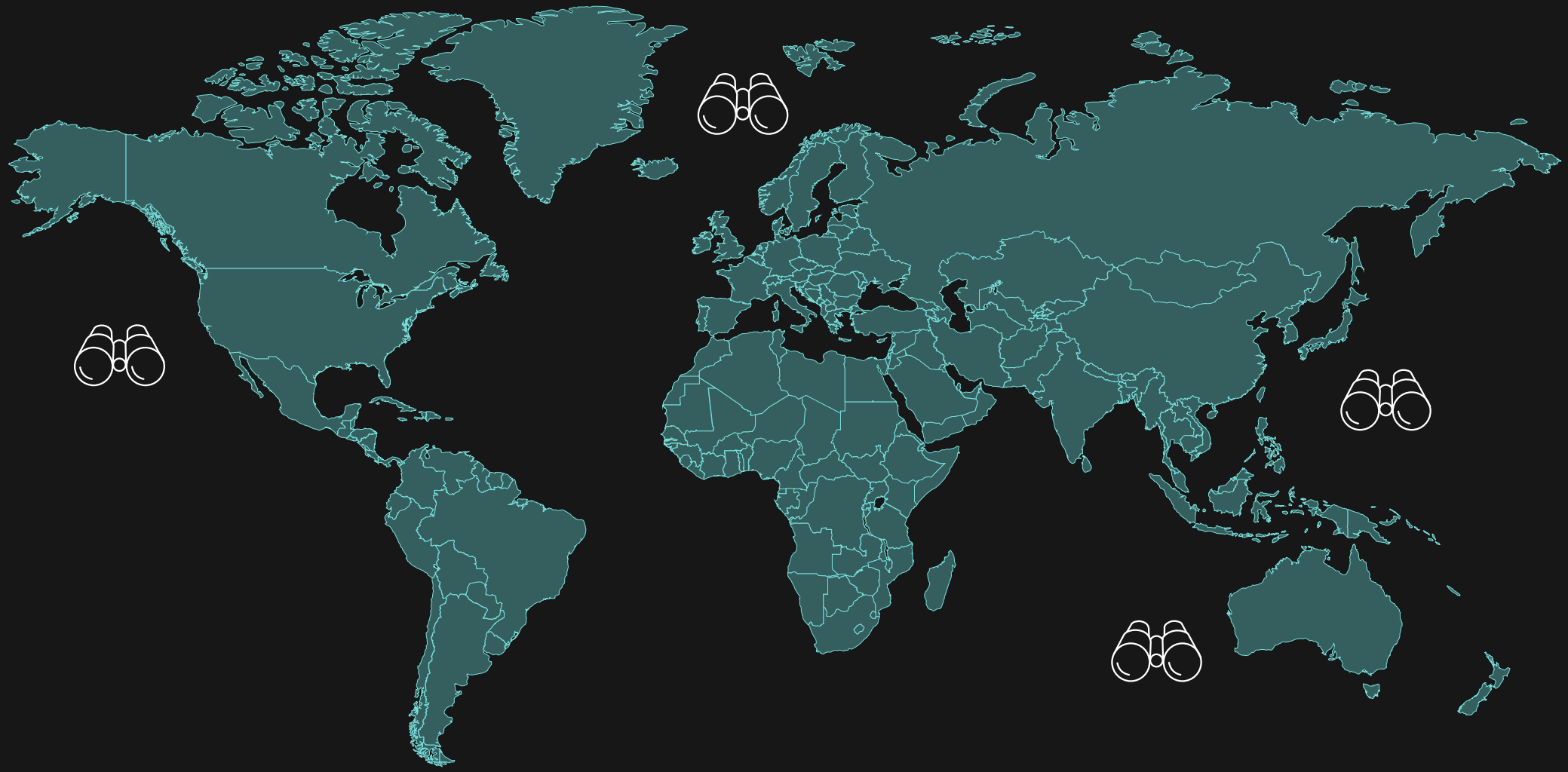
CONCIERGE ANALYST

THREAT DETECTIONS, VULNERABILITY DATA & INDICATORS ARE CODIFIED IN THE **DRAGOS PLATFORM**

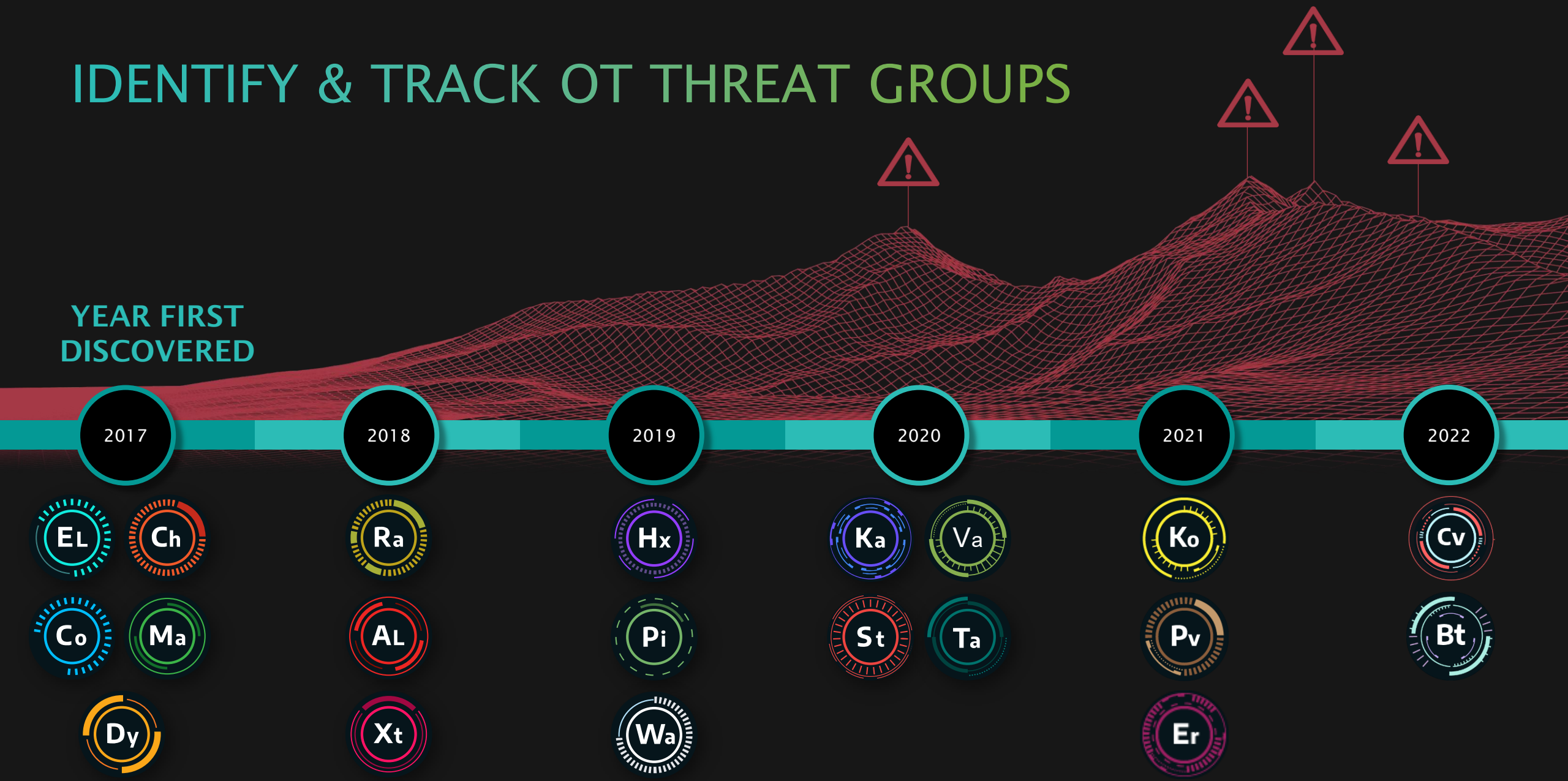
THREAT DISCOVERY TEAM

- We detect, track, and report on global threats to operational technology and industrial control systems
- We use open-source intelligence, exclusive telemetry, shared intelligence, vendors/OEMs, government advisories, ISACs

GLOBAL COVERAGE, REGIONAL FOCUS



IDENTIFY & TRACK OT THREAT GROUPS



THREAT DISCOVERY METHODS

Industry &
Region

Victim

Threat Group

Defining CTI

GOOD THREAT INTELLIGENCE – QUALITY VS. QUANTITY

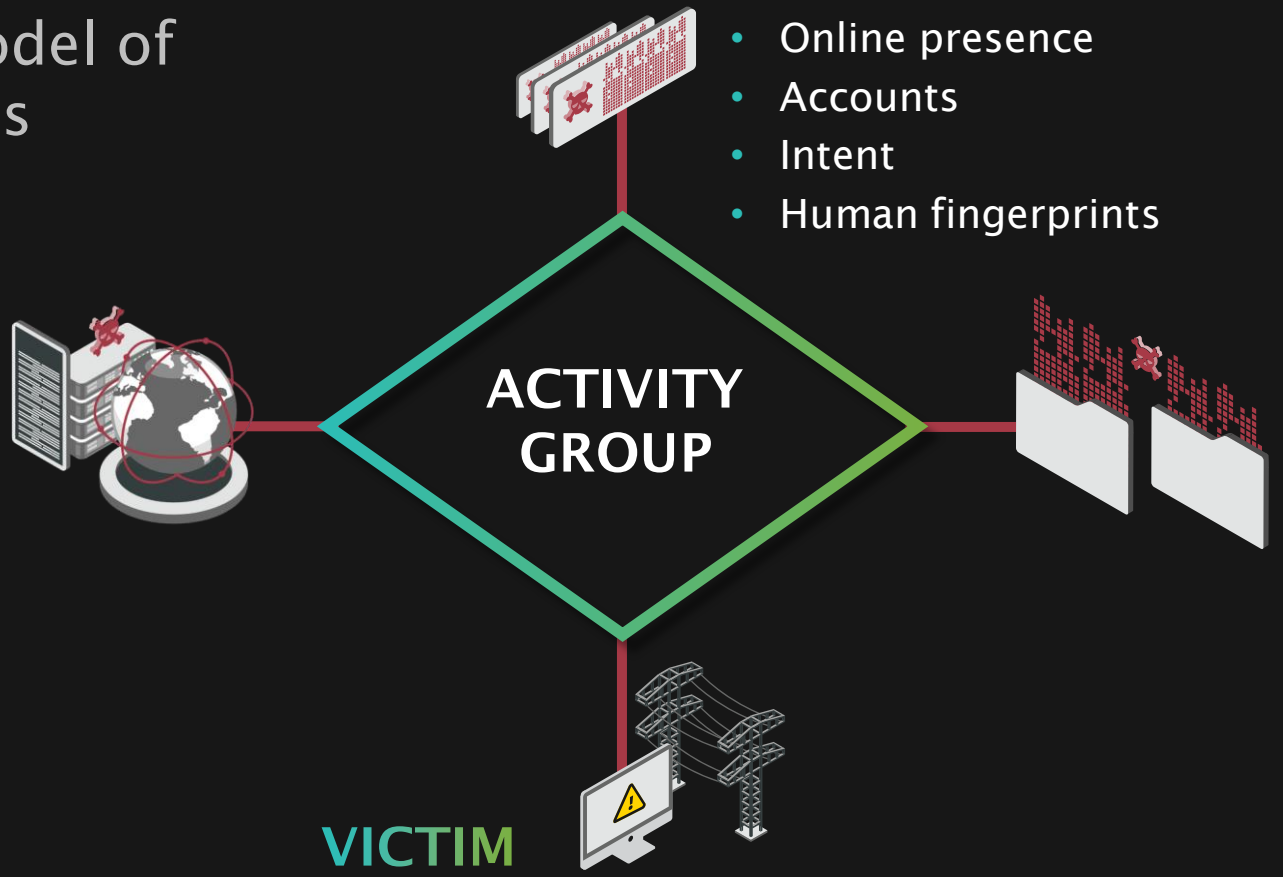
- ✓ Contextualized, finished cyber threat intelligence
- ✓ Evidence-based, uses multiple sources
- ✓ Follows a structured intelligence lifecycle & process
- ✓ Actionable guidance to mitigate and preempt threats
- ✓ Made relevant to a specific industry, a specific business
- ✓ Timely updates on changes to the threat landscape
- ✓ Used as part of an overall OT cybersecurity strategy

GOOD THREAT INTELLIGENCE – QUALITY VS. QUANTITY

- ✓ Contextualized, finished cyber threat intelligence
- ✓ Evidence-based, uses multiple sources
- ✓ Follows a structured intelligence lifecycle & process
- ✓ Actionable guidance to mitigate and preempt threats
- ✓ Made relevant to a specific industry, a specific business
- ✓ Timely updates on changes to the threat landscape
- ✓ Used as part of an overall OT cybersecurity strategy

Dragos Threat Groups

The Diamond Model of Intrusion Analysis



ADVERSARY

- Online presence
- Accounts
- Intent
- Human fingerprints

INFRASTRUCTURE

- C2 nodes
- Domains
- Hosting
- Service accounts

CAPABILITIES

- Tools and techniques
- Expertise
- Malware usage: operational, open source, custom
- Exploit development
- Methods of staging data
- Operational discipline

VICTIM

- Recipient of the capabilities:
  - Networks, systems, people, companies
- Apparent target objectives
- At Dragos, a TG is only named if the adversary aims for or purposefully affects ICS and/or OT of its target

WHERE TO FIND OT THREAT INTEL

1st Party Data

THIS IS YOUR DATA

Network and Endpoint Traffic Data, Security Logs, Incident Reports, Any information that is generated internally

Dragos Platform

2nd Party Data

THIS IS YOUR PARTNER'S 1st PARTY DATA

Peer-to-Peer Sharing Networks, Joint Cybersecurity Operations, Partner Agreements

Neighborhood Keeper

3rd & 4th Party Data

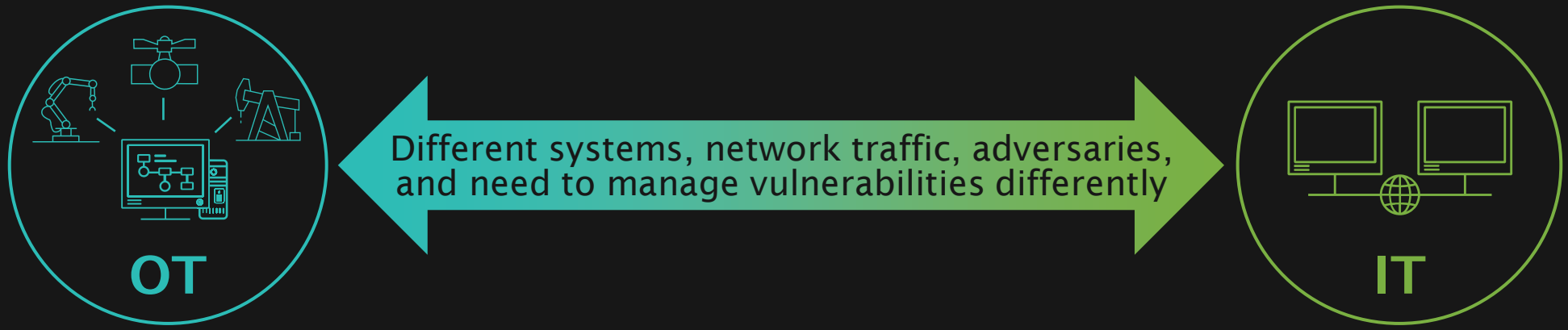
FROM EXTERNAL SOURCES

Commercial Cyber Threat Intelligence Providers, ISACs, Government Advisories, OSINT

Dragos Threat Intelligence

Why is OT CTI Different?

FILL THE OT THREAT INTEL GAP



OT

- Loss of electrical grid, water systems, safety systems, pipeline, or plant operations
- Loss of revenue generating operations for industrial companies

Impact From A Major Cyber Security Incident

IT

- Loss of data, intellectual property, network services
- Loss of revenue generation for services, financial, & technology companies

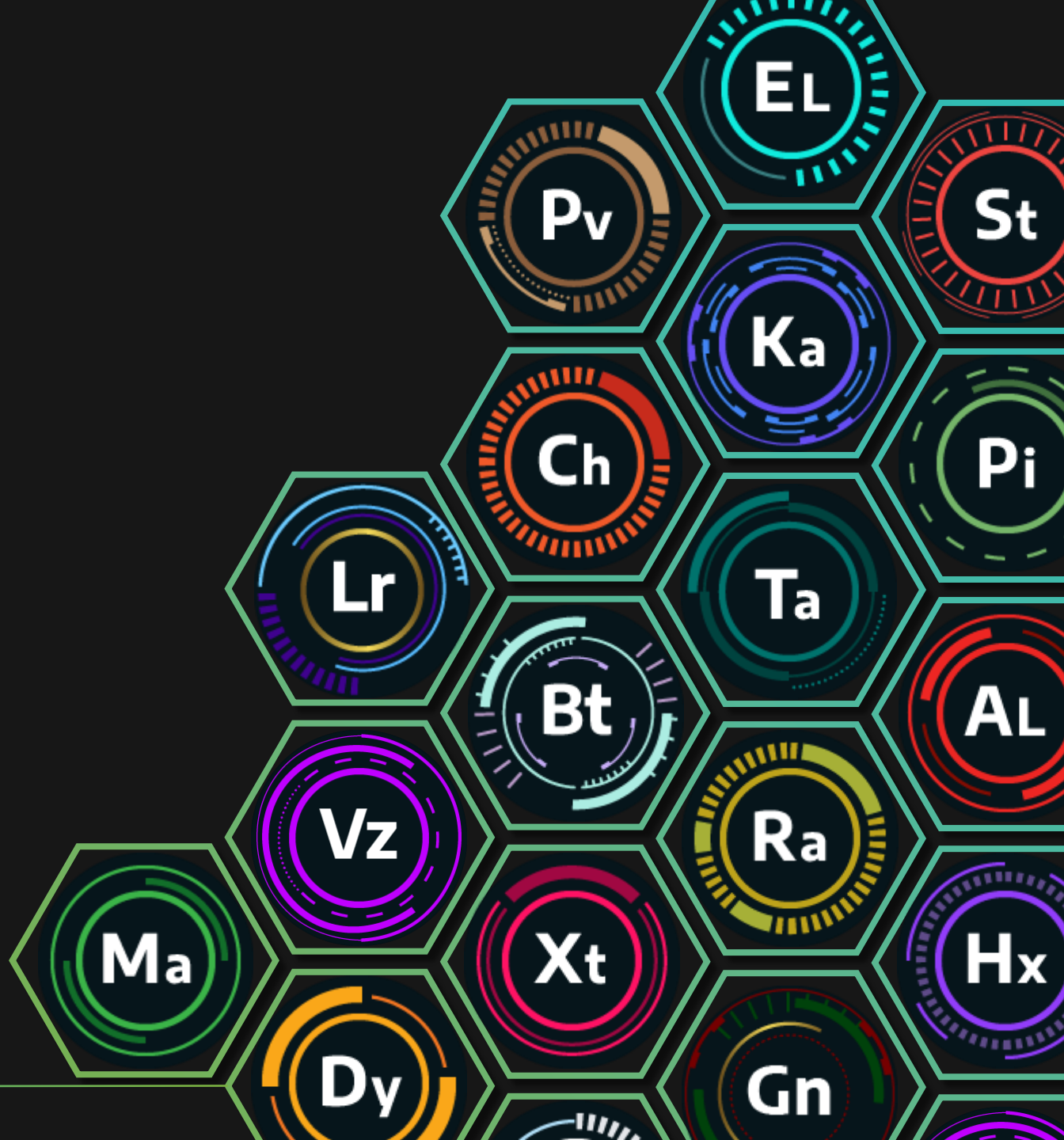
CLASSES OF ICS THREATS

ICS Curious	Adversaries known to have an interest in industrial organizations, industrial control systems, and operational technology networks. *Example: KAMACITE*
ICS Capable	Threats directly impacting the operation of industrial control systems. *Example: ELECTRUM*
ICS Adjacent	Threats not associated with industrial control systems but have a high likelihood of disrupting their operations. *Example: Ransomware*

ICS Threat Landscape

THREAT LANDSCAPE

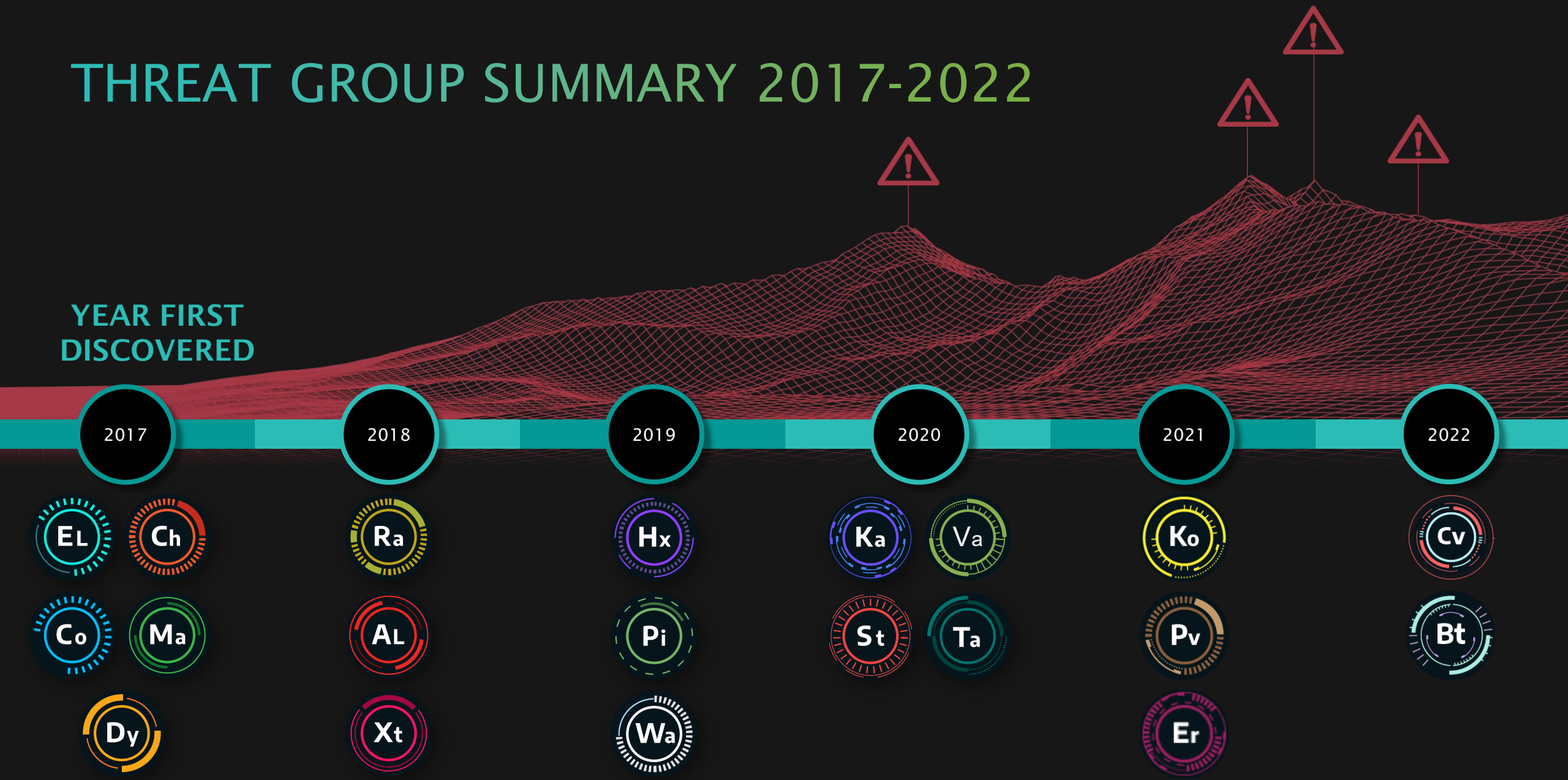
- 20 public threat groups targeting ICS/OT
- ICS-specific malware
- Supply chain – OEMs, telecommunications, data centers
- Remote access, vendor access
- Vulnerability exploitation to enable process disruption



INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	EVASION	DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND & CONTROL	INHIBIT RESPONSE FUNCTION	IMPAIR PROCESS CONTROL	IMPACT
Drive-by 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
Engineering Workstation 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 Control
Exploit Public-Facing Application	Execution Through API	Project File Infection		Indicator Removal on Host	Remote System Discovery	Lateral Tool Transfer	Detect Operating System	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
Exploitation of Remote Services	Graphical User Interface	System Firmware		Masquerading	Remote System Information Discovery	Program Download	I/O Image		Block Reporting Message	Spoof Reporting Message	Loss of Availability
External Remote Services	Hooking	Valid Accounts		Rootkit	Wireless Sniffing	Remote Services	Man in the Middle		Block Serial COM	Unauthorized Command Message	Loss of Control
Internet Accessible Device	Modify Controller Tasking			Spoof Reporting Message		Valid Accounts	Monitor Process State		Data Destruction		Loss of Productivity & Revenue
Remote Services	Native API						Point & Tag Identification		Denial of Service		Loss of Protection
Replication Through Removable Media	Scripting						Program Upload		Detect Restart/ Shutdown		Loss of Safety
Rogue Master	User Execution								e I/O		Loss of View
Spearfishing Attachment									arm Settings		Manipulation of Control
Supply Chain Compromise									Rootkit		Manipulation of View
Transient Cyber Asset									Service Stop		Theft of Operational System
Wireless Compromise									System Firmware		

MITRE ATT&CK FOR INDUSTRIAL CONTROL SYSTEMS

THREAT GROUP SUMMARY 2017-2022



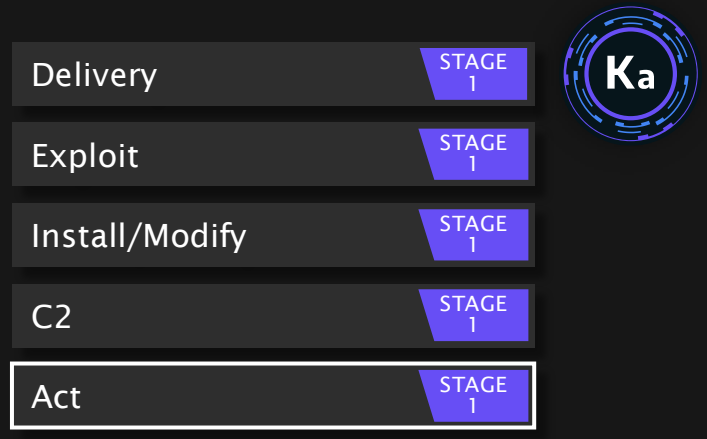
CASE STUDY: KAMACITE/ELECTRUM

THREAT ACTIVITY GROUPS SPECIALIZE IN ICS/OT

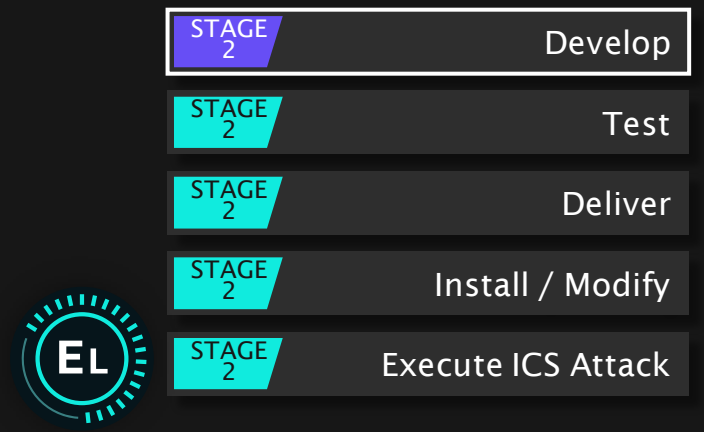
CRASHOVERRIDE

Attack Impacted ¼ million homes in Ukraine

KAMACITE CAN ACHIEVE INITIAL ACCESS INTO IT NETWORKS & PIVOT TO OT



ELECTRUM DEPLOYED CRASHOVERRIDE OT MALWARE



KAMACITE

GAIN INITIAL ACCESS, PIVOT TO OT

February 2022	March	April	May	June
CYCLOPS BLINK targeting vulnerabilities in small/home office devices	 WatchGuard firewall & router devices  ASUS firewall & router devices	Malware removed from vulnerable firewall devices used for C2 CYCLOPS BLINK operations	Targets another set of routers & IP cameras for initial network access (outside of CYCLOPS BLINK operations)	Communication with the same oblenergo targeted in a 2015 Ukraine cyber attack

Observed utilizing DarkCrystal malware to conduct reconnaissance in 2023

WIPER MALWARE

There have been at least 7 wipers deployed in Ukraine since the beginning of the Russian invasion:

1. WhisperKill/WhisperGate
2. DesertBlade
3. HermeticWiper/FoxBlade
4. IsaacWiper/Lasainraw
5. CaddyWiper
6. DoubleZero/FiberLake
7. Prestige
8. *AcidRain*

Microsoft reported a new wiper used by Cadet Blizzard that targets the Master Boot Record (MBR) when the device is powered down that includes a fake ransomware note with no mechanism for data recovery.

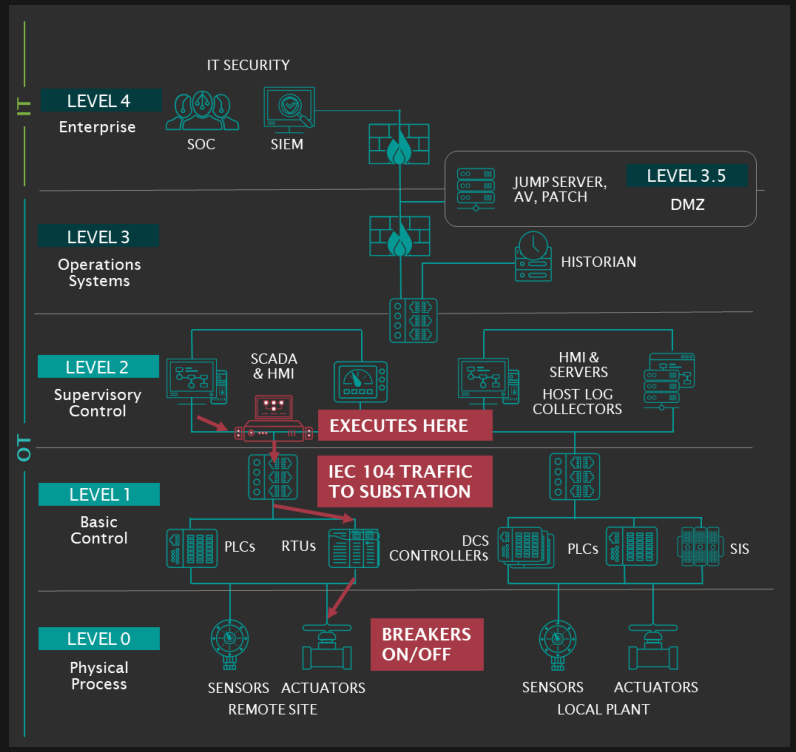
Wiper malware that has a demonstrated history of spreading to or having cascading impacts into neighboring EU countries (NotPetya, Shamoon Wiper)

ELECTRUM
EXECUTING ICS ATTACKS

In April 2022, ESET reports malware is uncovered at a Ukrainian utility provider

INDUSTROYER2 overlaps with CRASHOVERRIDE, with fewer components

Wiper malware is deployed with INDUSTROYER2: CADDYWIPER, ORCSHRED, SOLOSHRED, & AWFULSHRED



ADVERSARIES & TOOLS EVOLVE
INDUSTROYER2
A VARIANT OF CRASHOVERRIDE
DISCOVERED IN 2022

OPERATIONALIZE OT THREAT INTEL

Internal/external visibility

- Acquire sufficient data sources and visibility into your OT network
- Understanding of outside facto

OT intel for IT

- Help IT cybersecurity contextualize threats to OT

Operational factors, maturity/capabilities

- Understand the impediments to response

EVOLVING YOUR INTERNAL CTI CAPABILITIES

	CTI CAPABILITIES	OUTCOMES
BASELINE ASSESS, PLAN, & ORGANIZE	Organization has few processes in place to action on cyber threat intelligence. Low visibility into company's networks & assets.	✓ Integrate IOCs with IT SOC ✓ Know your top threats & critical points of weakness ✓ Identify OT cybersecurity requirements
OPERATIONALIZE OT SECURITY CONTROLS	Dedicated cyber threat intelligence analyst. Responding to trends, informed security posture decisions. Increased visibility of networks & assets.	✓ Report on industry-specific threat landscape developments ✓ Management of OT vulnerabilities ✓ Validate defensive controls
OPTIMIZE PROACTIVE RISK REDUCTION	Prioritized intelligence requirements & defines new capabilities to stay ahead of security trends. Leveraging metrics, playbooks, & red teaming exercises. Full visibility of networks & assets.	✓ Plan & test response to active threat ✓ Hunt for malicious activity impacting your OT network ✓ Develop custom detections

Thank You!

DRAGOS