DRAGOS

ICS/OT CYBERSECURITY
YEAR IN REVIEW 2021

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

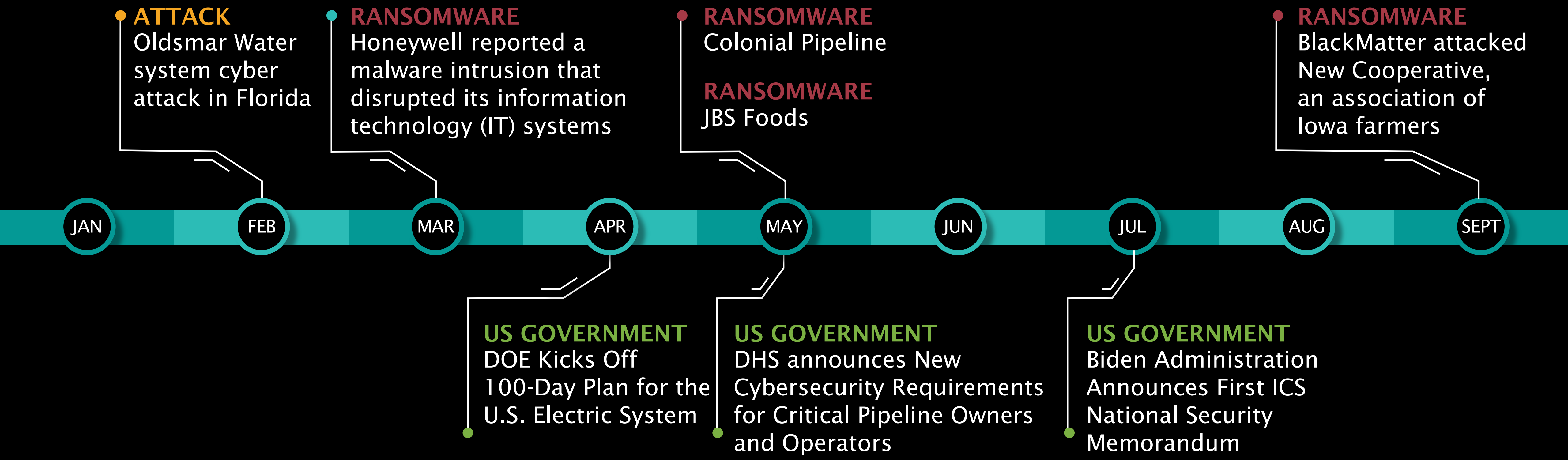
WHAT IS THE YEAR IN REVIEW?

Annual analysis of threats, vulnerabilities, assessments, insights

Fifth year running

Purpose is to help accelerate learning on how to address the challenges

A LOOK BACK AT 2021



ATTACK
Oldsmar Water system cyber attack in Florida

RANSOMWARE
Honeywell reported a malware intrusion that disrupted its information technology (IT) systems

US GOVERNMENT
DOE Kicks Off 100-Day Plan for the U.S. Electric System

RANSOMWARE
Colonial Pipeline

RANSOMWARE
JBS Foods

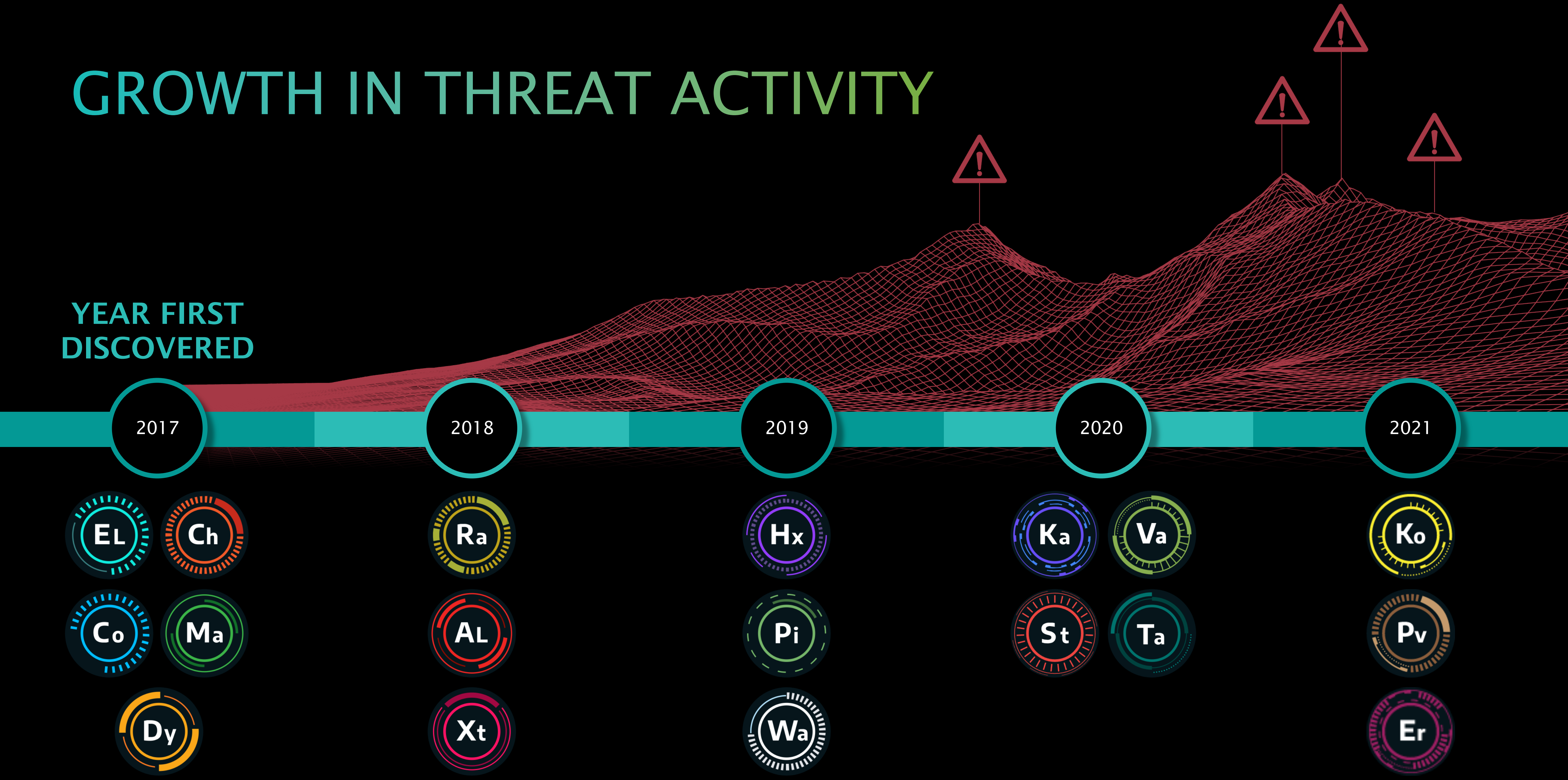
US GOVERNMENT
DHS announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators

US GOVERNMENT
Biden Administration Announces First ICS National Security Memorandum

RANSOMWARE
BlackMatter attacked New Cooperative, an association of Iowa farmers

GROWTH IN THREAT ACTIVITY

YEAR FIRST DISCOVERED



2017

EL Ch

Co Ma

Dy

2018

Ra

AL

Xt

2019

Hx

Pi

Wa

2020

Ka Va

St Ta

2021

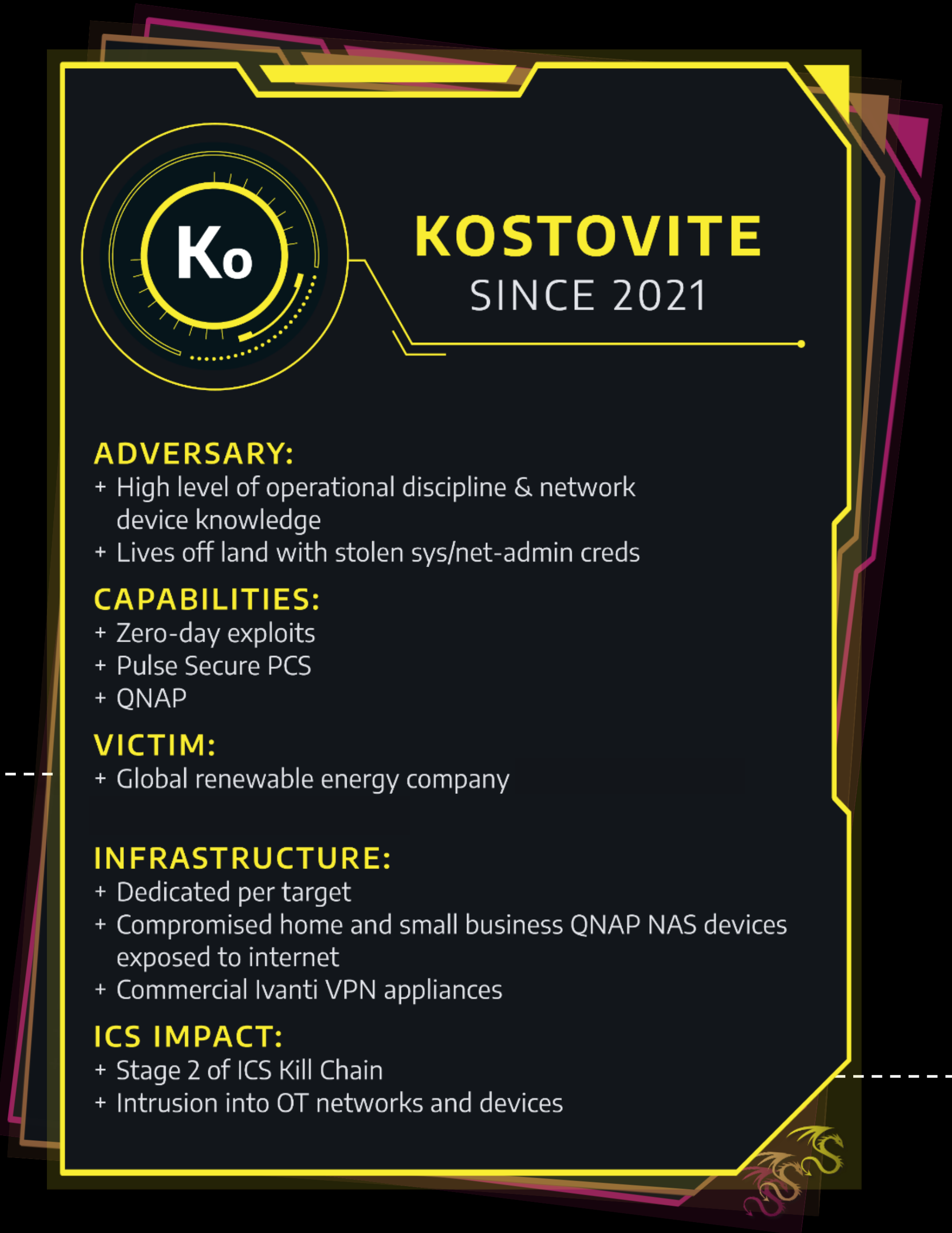
Ko

Pv

Er

KOSTOVITE

Targets **renewable energy operations**



KOSTOVITE

SINCE 2021

ADVERSARY:

- High level of operational discipline & network device knowledge
- Lives off land with stolen sys/net-admin creds

CAPABILITIES:

- Zero-day exploits
- Pulse Secure PCS
- QNAP

VICTIM:

- Global renewable energy company

INFRASTRUCTURE:

- Dedicated per target
- Compromised home and small business QNAP NAS devices exposed to internet
- Commercial Ivanti VPN appliances

ICS IMPACT:

- Stage 2 of ICS Kill Chain
- Intrusion into OT networks and devices

STAGE 02 Develop

STAGE 02 Test

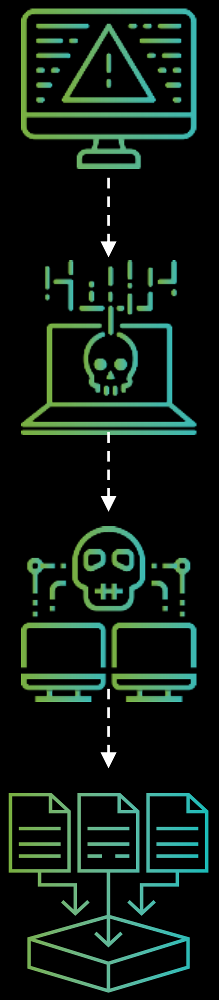
STAGE 02 Deliver

STAGE 02 Install / Modify

STAGE 02 Execute ICS Attack

Reached Stage **2 of ICS Kill Chain capabilities** with a confirmed intrusion into an operations and maintenance (O&M) firm’s OT networks and devices

KOSTOVITE IN ACTION

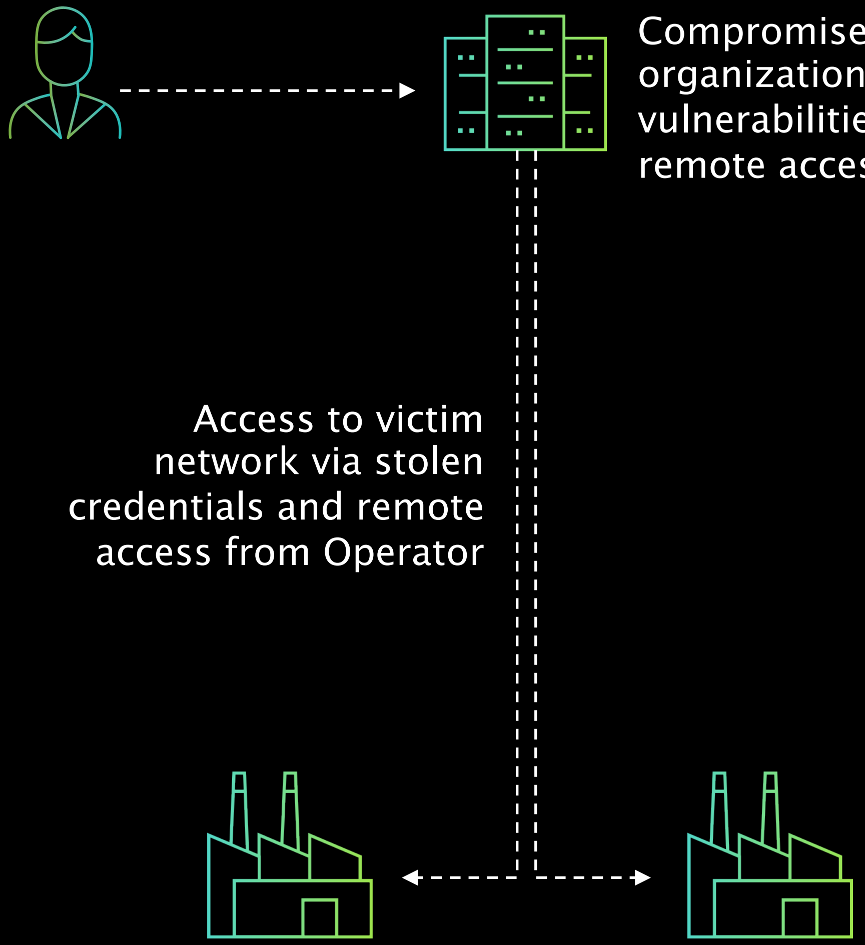


Compromises Energy Organization

Steals Credentials

Moves Laterally to gain access to OT networks

Living off the land: once inside uses native tools to target technical environment



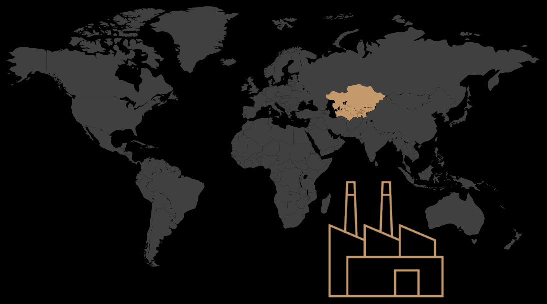
Compromises Energy organization via vulnerabilities in remote access solution

Access to victim network via stolen credentials and remote access from Operator

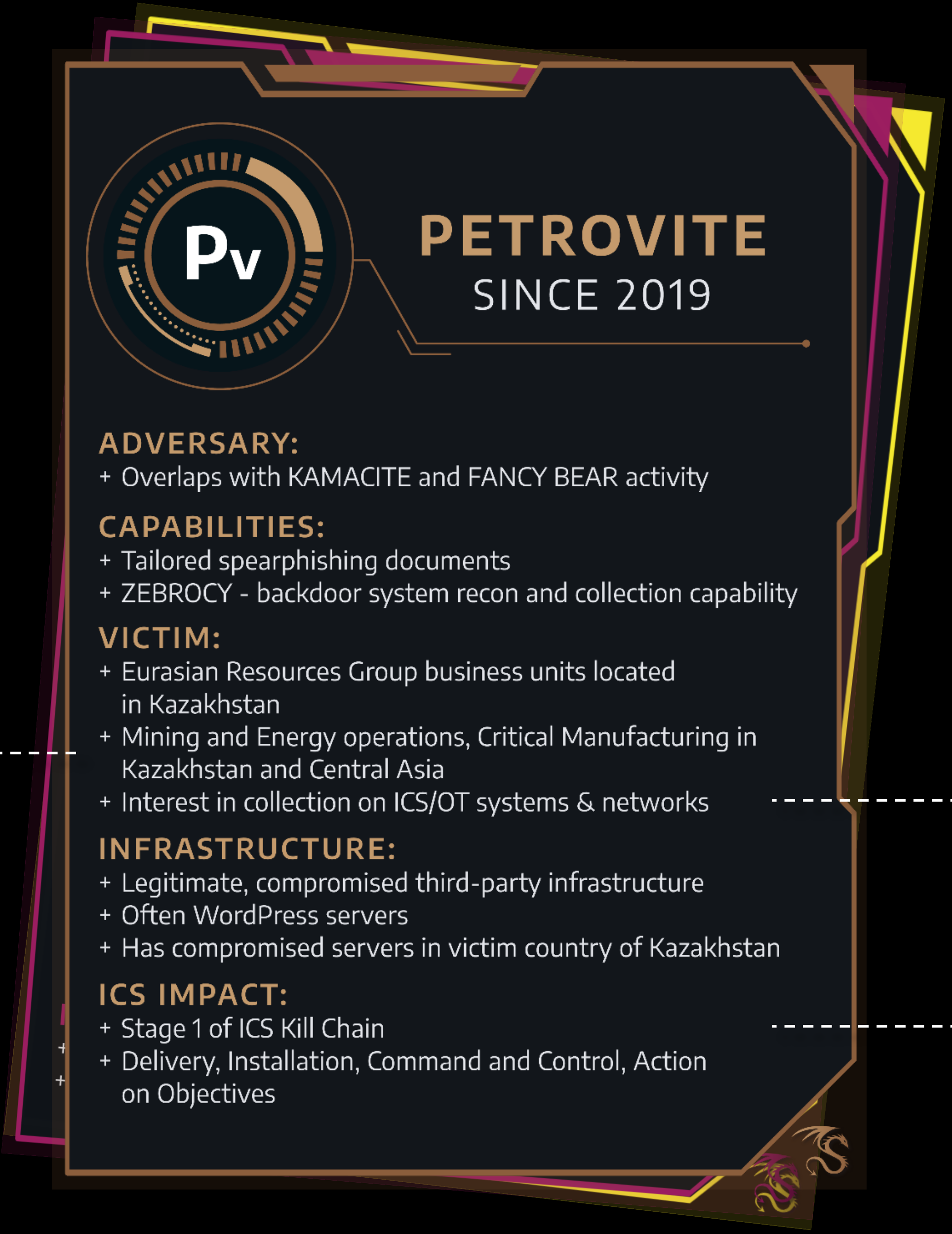
Generation Facility 1

Generation Facility 2

PETROVITE



Targets **critical manufacturing** and energy in Central Asia



PETROVITE

SINCE 2019

ADVERSARY:

+ Overlaps with KAMACITE and FANCY BEAR activity

CAPABILITIES:

+ Tailored spearphishing documents
+ ZEBROCY - backdoor system recon and collection capability

VICTIM:

+ Eurasian Resources Group business units located in Kazakhstan
+ Mining and Energy operations, Critical Manufacturing in Kazakhstan and Central Asia
+ Interest in collection on ICS/OT systems & networks

INFRASTRUCTURE:

+ Legitimate, compromised third-party infrastructure
+ Often WordPress servers
+ Has compromised servers in victim country of Kazakhstan

ICS IMPACT:

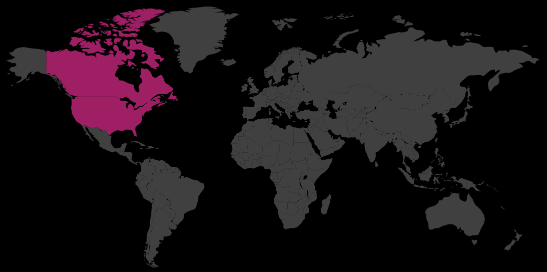
+ Stage 1 of ICS Kill Chain
+ Delivery, Installation, Command and Control, Action on Objectives

Delivery	STAGE 01
Exploit	STAGE 01
Install/Modify	STAGE 01
C2	STAGE 01
Act	STAGE 01

The group is active and displays an interest in collection on **ICS/OT systems and networks**

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

ERYTHRITE



Broadly targets organizations in the **US and Canada**

ERYTHRITE

SINCE 2020

ADVERSARY:

+ No links to tracked activity groups; overlaps with Solarmarker

CAPABILITIES:

+ Bespoke credential stealing malware and SEO poisoning
+ Rapid Release and recrafting to evade AV
+ Possible affiliate-based operation model
+ Exploits 100k+ WordPress Sites, Formidable Forms, PDF documents, Google Groups, Shopify Sites

VICTIM:

+ C2 Filtering for USA and Canada
+ Compromised ~20% of F500 including: Mfg., Electric Utilities
+ Risk to victims using common credentials in IT & OT

INFRASTRUCTURE:

+ C2 and affiliate/panel mgmt. hosts in St. Petersburg & Moscow, Russian Federation
+ Reverse proxies/load balancers in France, Germany, Switzerland, Denmark, Romania, Canada, & USA

ICS IMPACT:

+ Stage 2 of ICS Kill Chain
+ Possible initial access brokery to 3rd party actors

Has technical **overlaps to another group** labeled by multiple IT security organizations as Solarmarker

Pursues OT environme nts across many industrialsectors, we estimate they have compromised **~20% of Fortune 500 companies**

ACTIVITY GROUP UPDATES

STIBNITE

FEB

Spear-phishing emails targeting Azerbaijani wind renewable resource linked firms

KAMACITE

MAR

New GREYENERGY files discovered in the wild

KAMACITE

AUG

New GREYENERGY files discovered in the wild

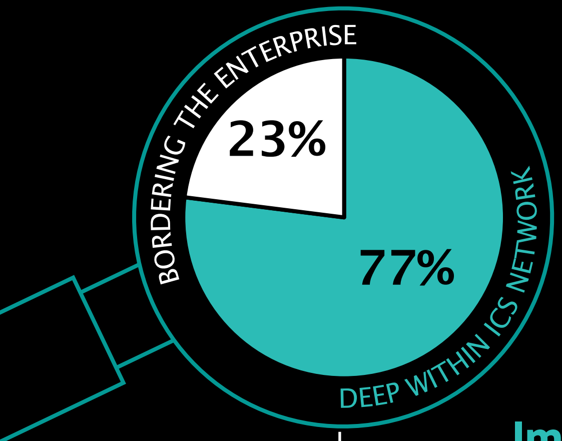
WASSONITE

OCT

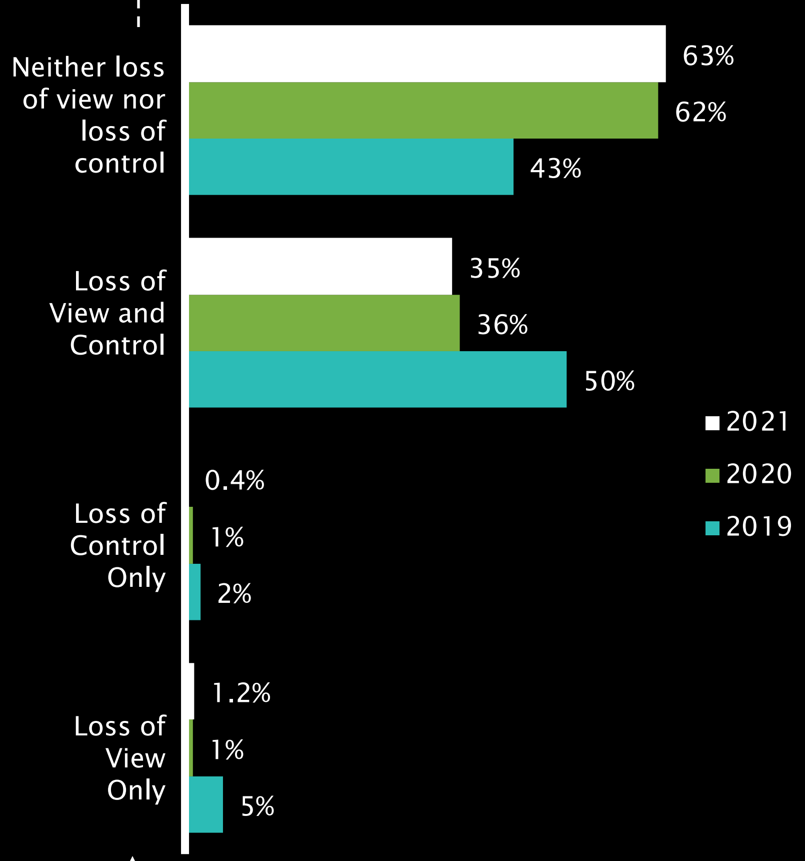
Continued targeting of nuclear power and electric sites (previously compromised the IT network of an Indian nuclear power company)

STATE OF ICS VULNERABILITIES

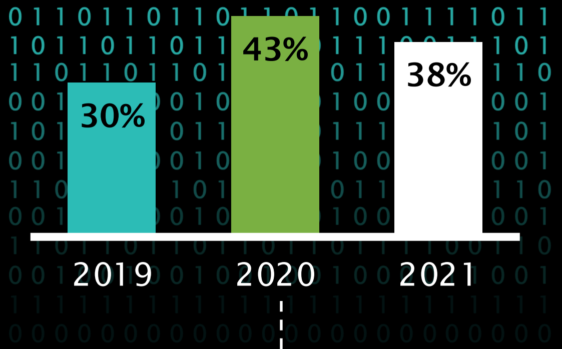
Where Vulnerabilities Reside

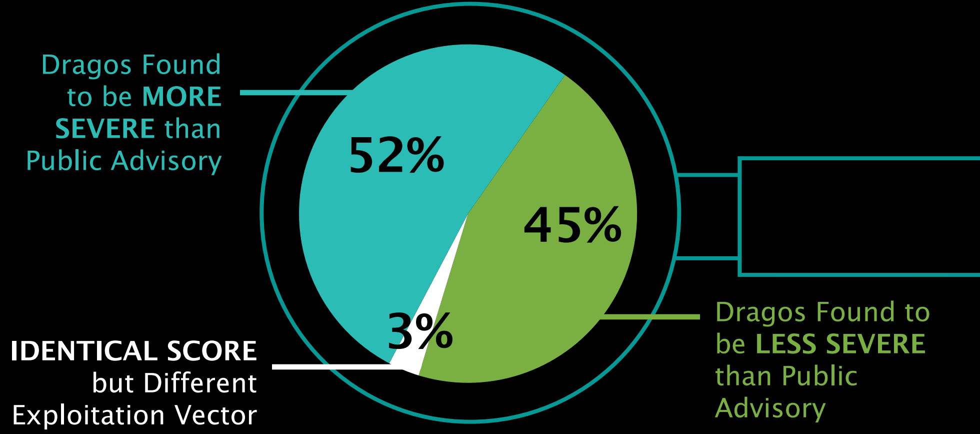


Impact of Disclosed Flaws

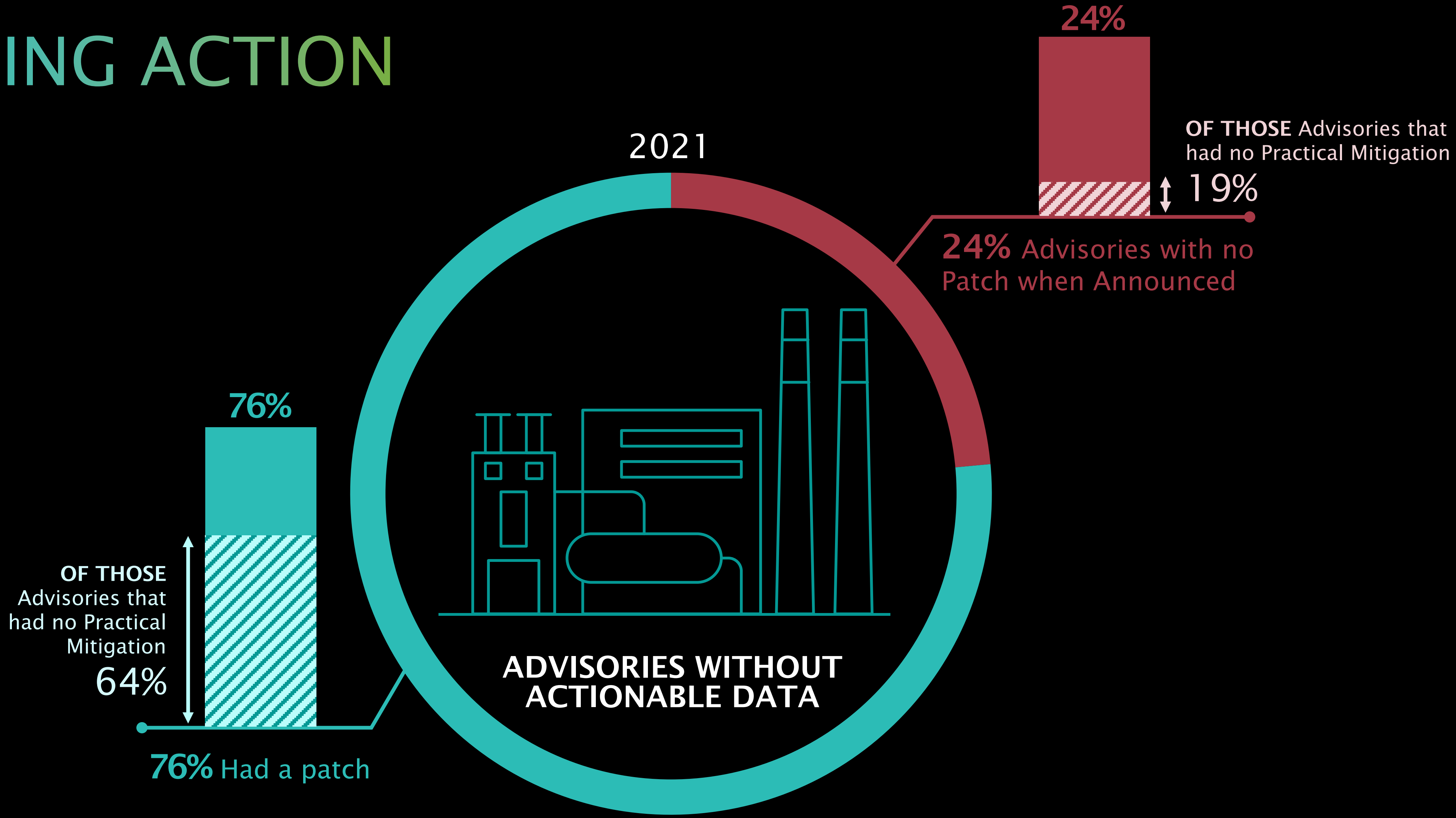


Advisories with Incorrect Data





TAKING ACTION



2021

ADVISORIES WITHOUT ACTIONABLE DATA

24%

OF THOSE Advisories that had no Practical Mitigation

19%

24% Advisories with no Patch when Announced

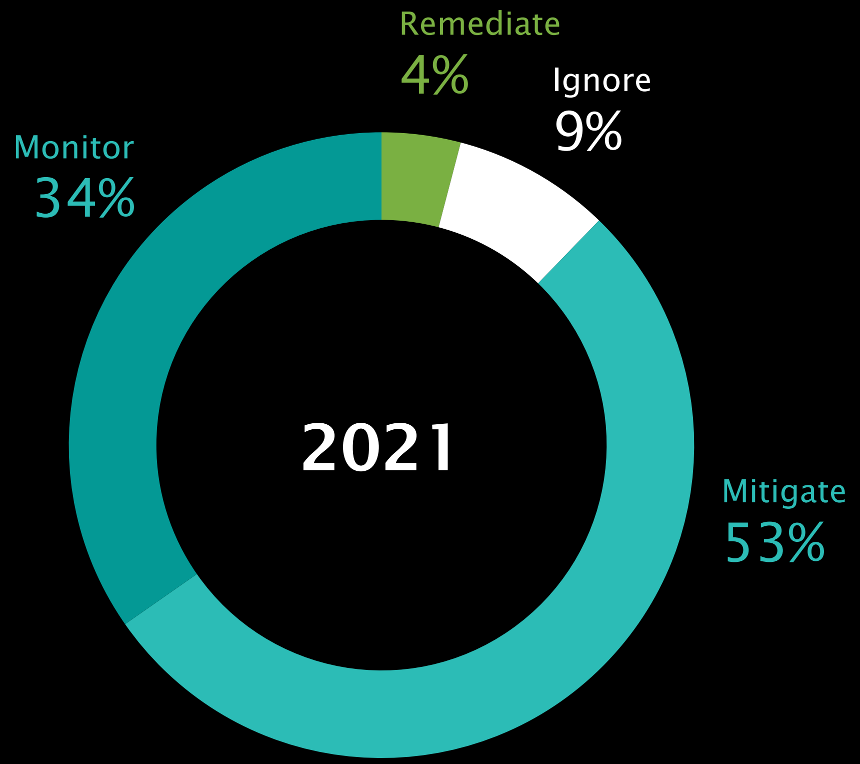
76%

OF THOSE Advisories that had no Practical Mitigation

64%

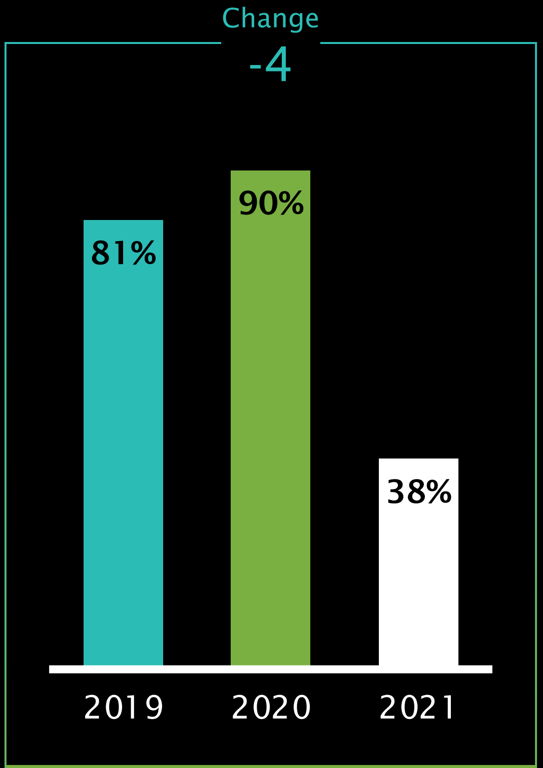
76% Had a patch

TAKING ACTION

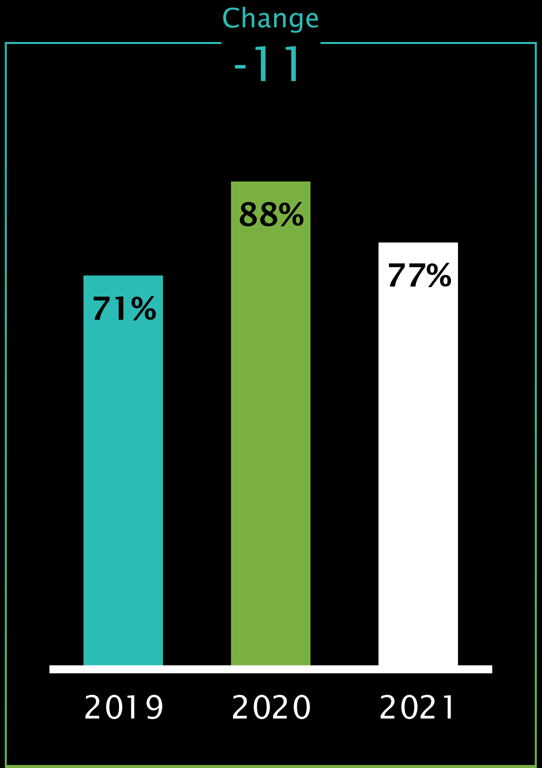


```
    height: 100%;
}

.block {
width: 100%;
height: 500px;
margin: 0 auto !important;
padding: 0 auto;
line-height: 0;
}

h2 {
    font-family: 'Montserrat', sans-serif;
    font-weight: 900;
    text-align: left;
    font-size: 3000%;
    z-index: 1;
    transform: scale(-1, 1);}
}
```

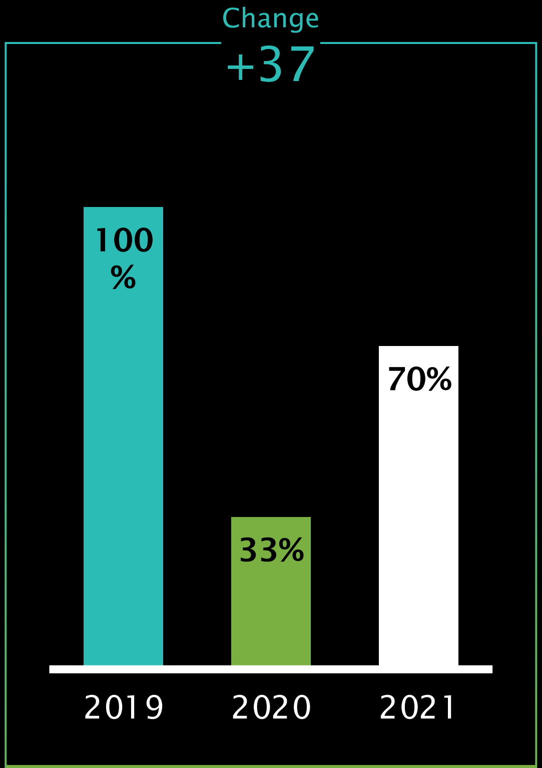
LESSONS LEARNED FROM CUSTOMER ENGAGEMENTS



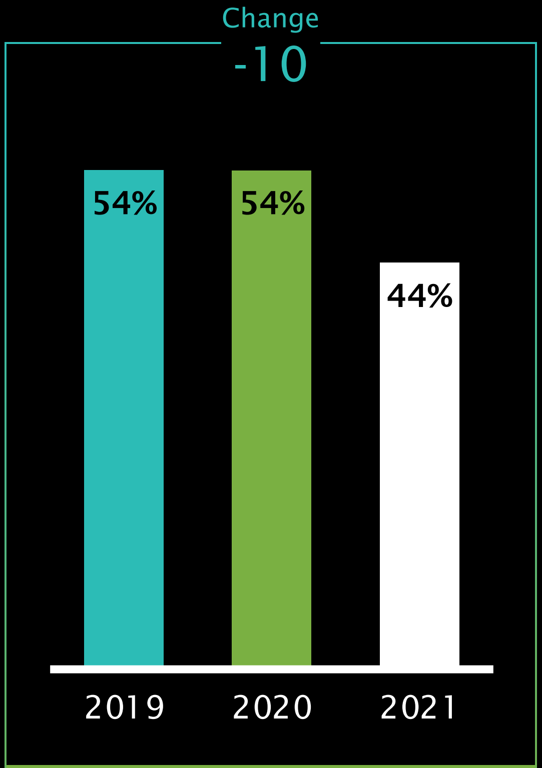
Limited / No Visibility into OT Environment



Poor Security Perimeters



External Connections to OT



Shared IT & OT Credentials

DRAGOS INCIDENT RESPONSE CASE
GHOST IN THE GENERATOR

Gas Turbine Suddenly & Mysteriously Turns On

Out of the Box Investigation Leads to HMI in Remote Shed

Incident Resolved – Moisture Triggered Control Loop

ICS monitoring would have accelerated alert,
eliminated external connections as a cause, & simplified root cause analysis

LESSONS LEARNED FROM CUSTOMER ENGAGEMENTS

Limited visibility

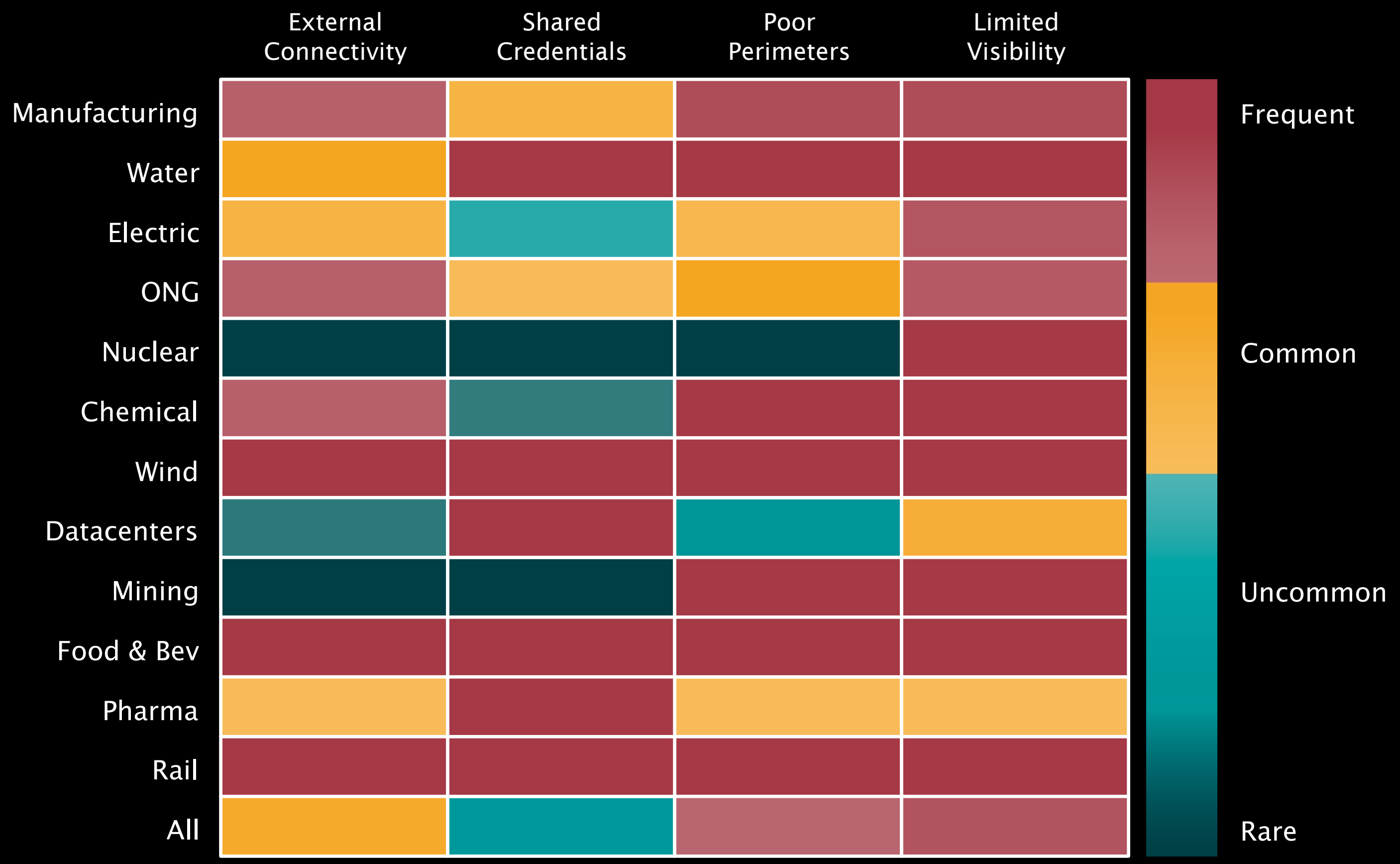
At least 50% of customers in all verticals have significant issues with network perimeters and visibility.

Common Findings

The four findings are prevalent and exist in more than 70% of the Water, Food & Beverage and Wind industries.

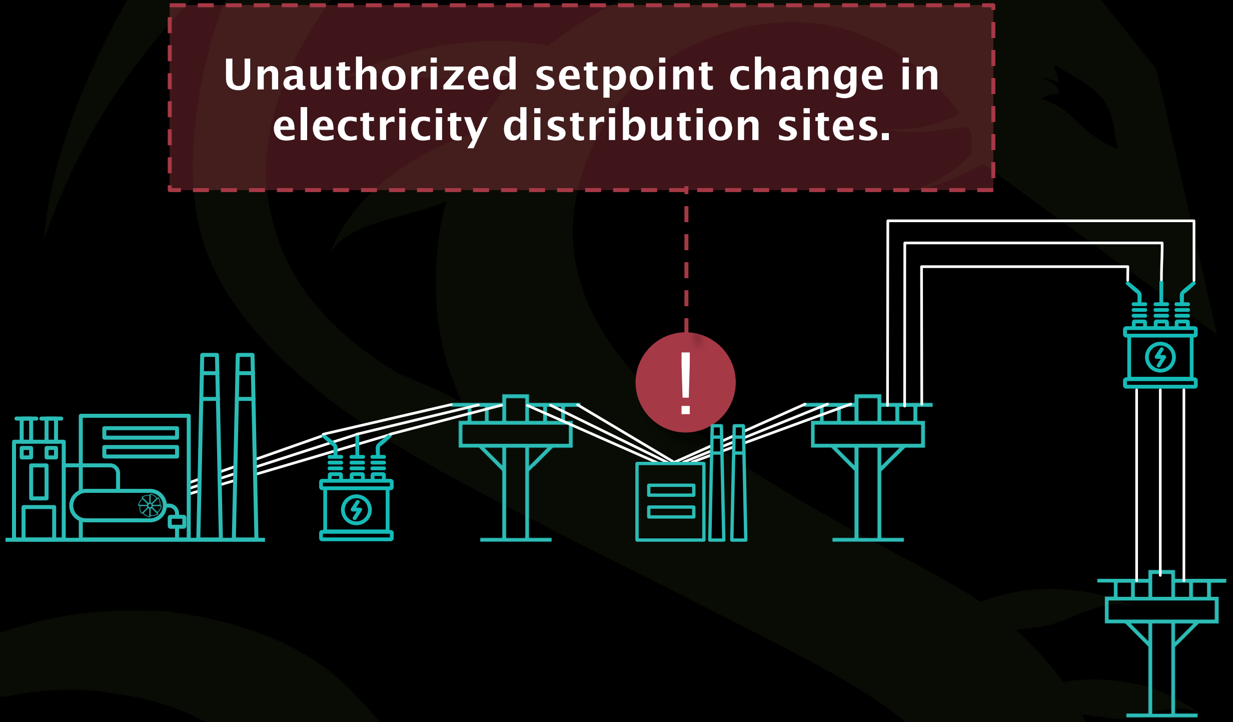
Shared credentials between IT and OT

Is the least consistent finding across verticals, and is widespread in only a few of the verticals



Common Findings by Industry Sector

DRAGOS IR - ICS VISIBILITY RULES OUT MALICIOUS ACTS, ISOLATE SYSTEM BUGS


Unauthorized setpoint change in electricity distribution sites.
!

Dragos IR team
Deploy Dragos Platform, Collect Telemetry

- ✓ Identified commands, host, & collected forensic data
- ✓ Analysis shows command issued by control software
- ✓ Resolved with OT Vendor; programming error fixed in two weeks

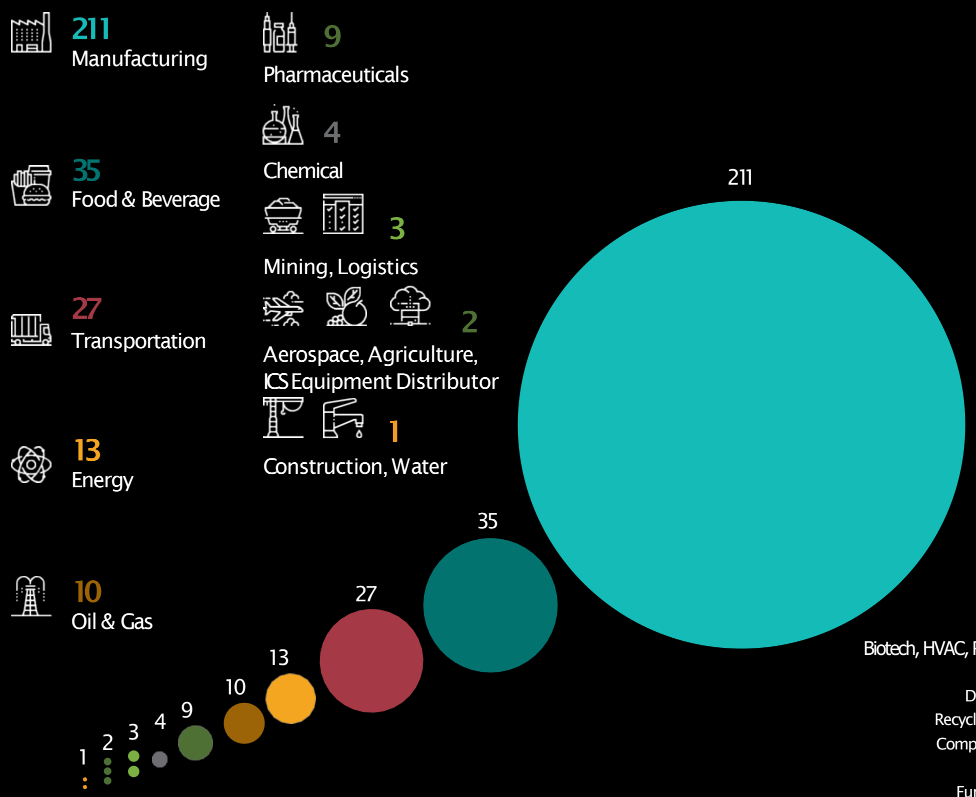
Dragos IR ruled out malicious activity and isolated the cause of the operational issue.
Demonstrates value of visibility and relationships with of OT system vendors

RANSOMWARE TRENDS

Ransomware became the number one attack vector in the industrial sector.

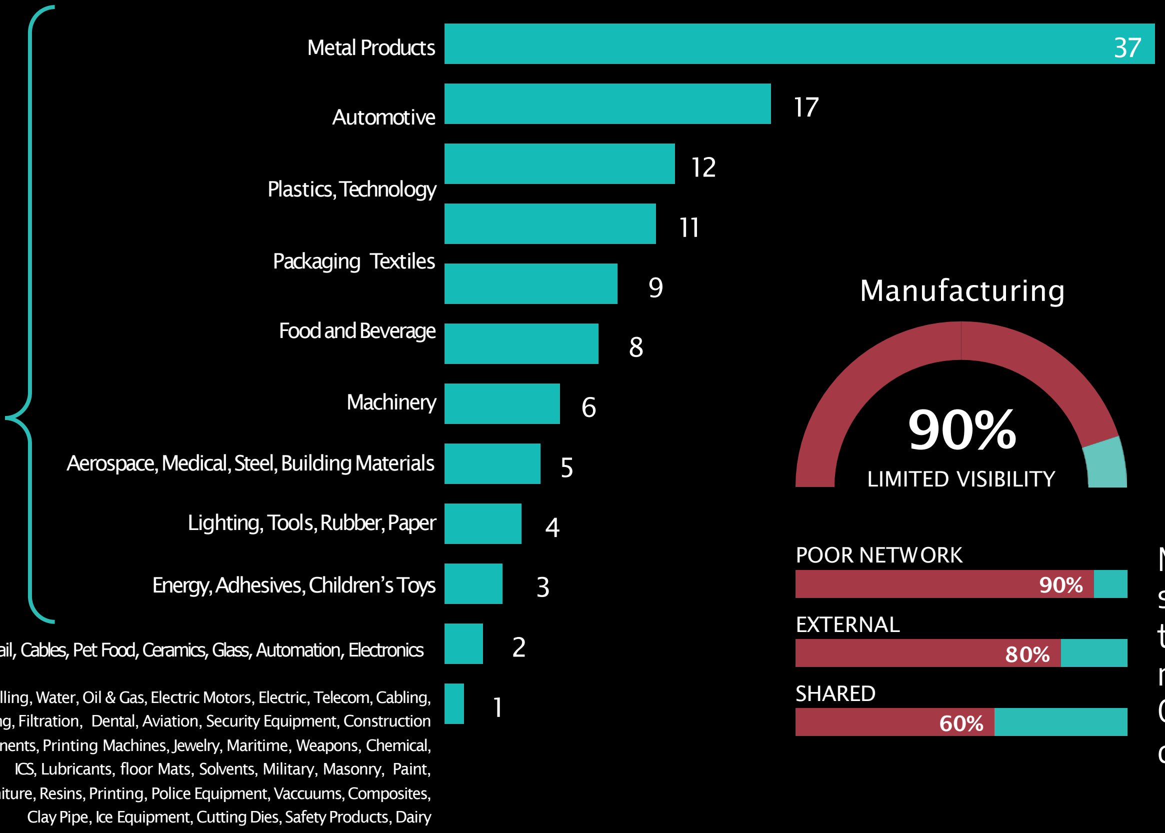
In industrial sector attacks, Ransomware groups targeted Manufacturing more than any other industrial sector accounting for 65%

Ransomware by ICS Sector

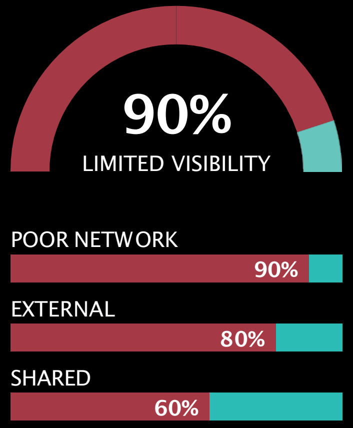


211	Manufacturing
35	Food & Beverage
27	Transportation
13	Energy
10	Oil & Gas
9	Pharmaceuticals
4	Chemical
3	Mining, Logistics
2	Aerospace, Agriculture, ICS Equipment Distributor
1	Construction, Water

Ransomware by Manufacturing Subsector



Manufacturing



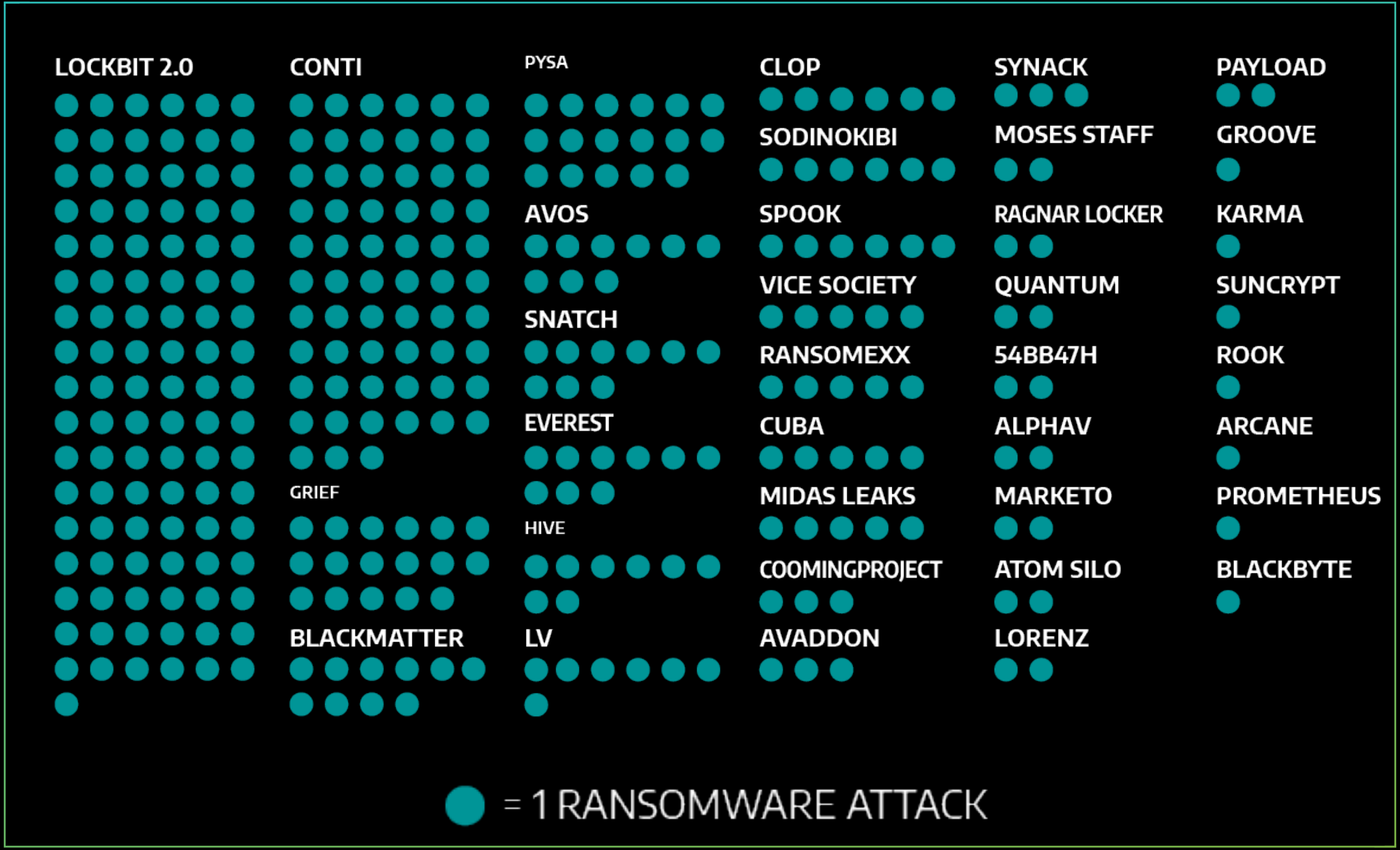
Manufacturing sector is often the least mature in their OT security defenses.

RANSOMWARE INCIDENTS by GROUP/STRAIN

Lockbit 2.0 and Conti account for:

51% of the total ransomware attacks

70% of their malicious activity targeted manufacturing



RECOMMENDATIONS

5 Security Controls for a World-Class OT Cybersecurity Program

1
A DEFENSIBLE ARCHITECTURE

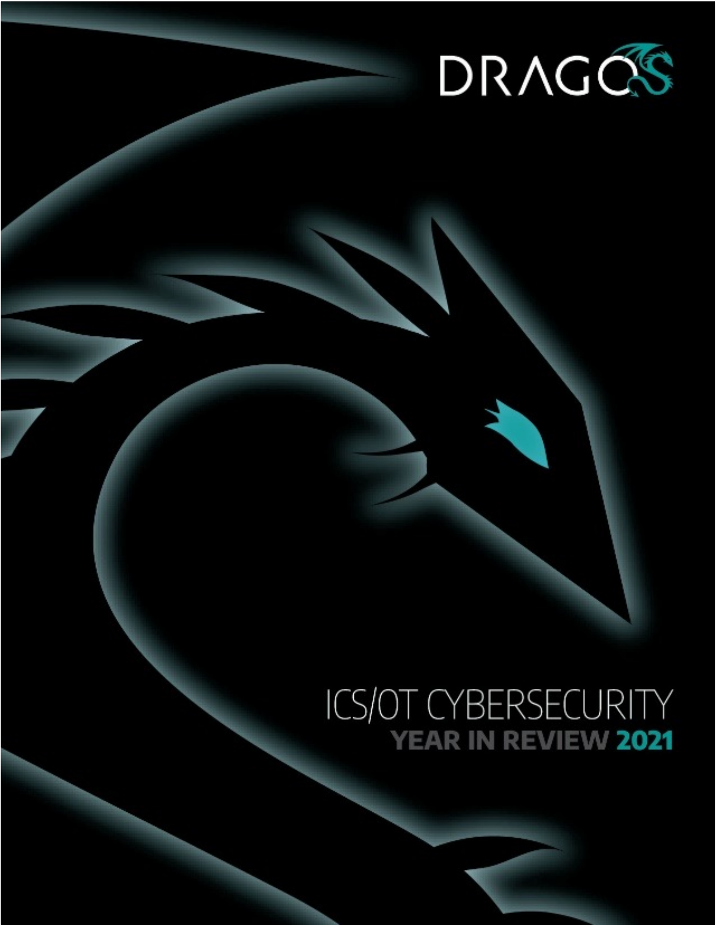
2
ICS NETWORK MONITORING

3
REMOTE ACCESS AUTHENTICATION

4
KEY VULN MANAGEMENT

5
ICS/OT IR PLAN

THANK YOU



To download a copy of the
2021 Year In Review Report,
Visit: dragos.com/yir