DRAGOS

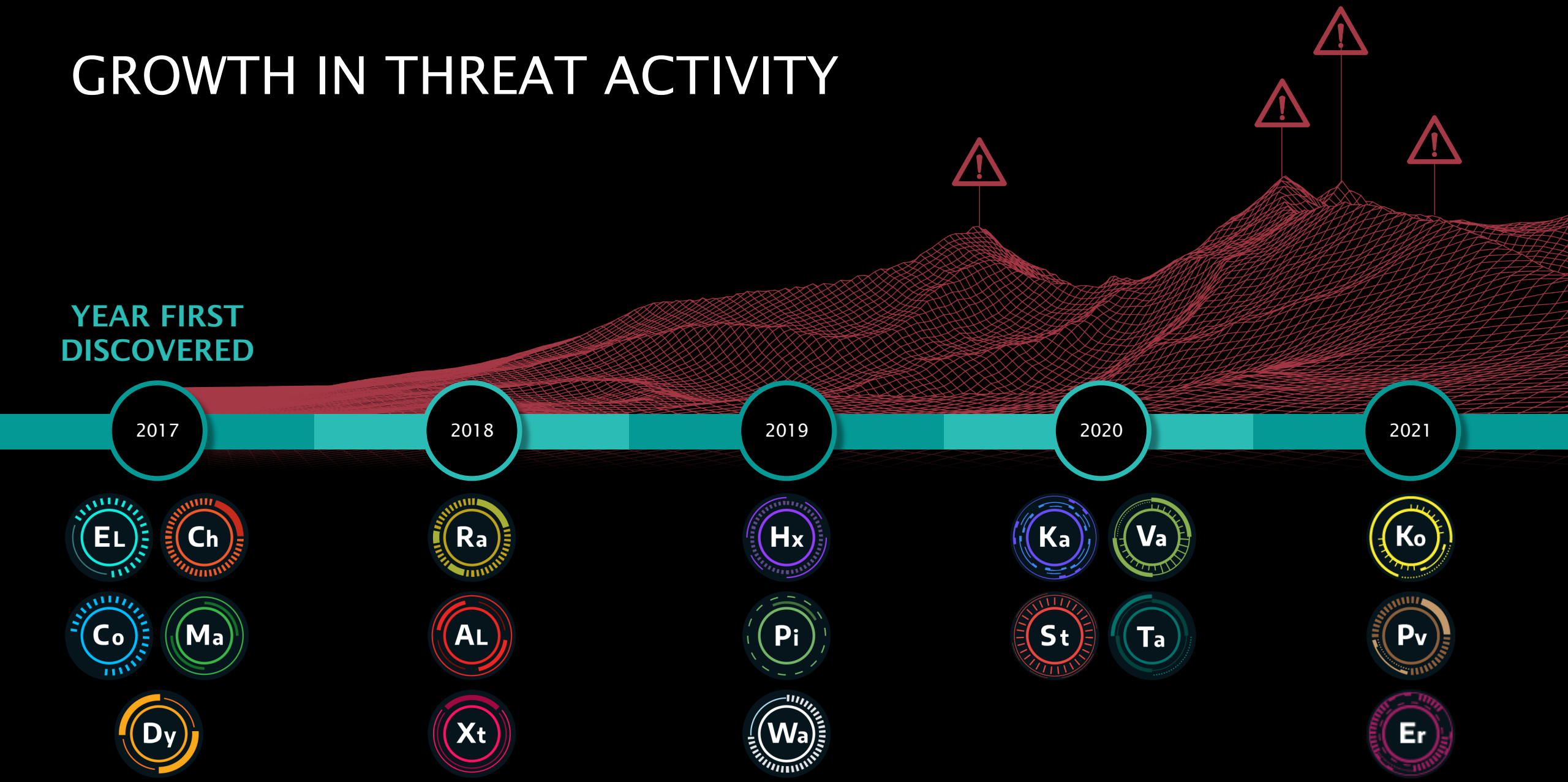
THREAT LANDSCAPE

YEAR IN REVIEW 2021

Anna Skelton
Senior Intelligence Analyst
Dragos, Inc.

Seth Lacy
Principal Adversary Hunter
Dragos, Inc.

GROWTH IN THREAT ACTIVITY



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

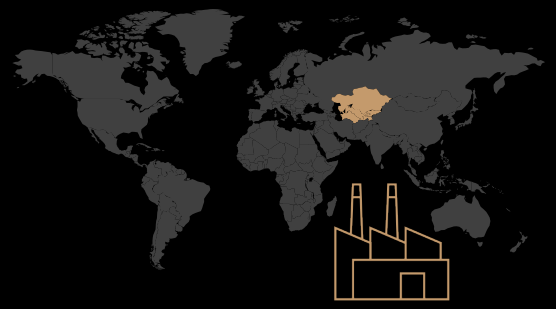
INFRASTRUCTURE:
+ Dedicated per target
+ Compromised home and small business QNAP NAS devices exposed to internet
+ Commercial Ivanti VPN appliances

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

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

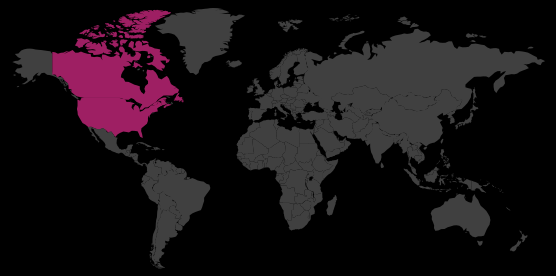
ICS IMPACT:
+ Stage 1 of ICS Kill Chain
+ Delivery, Installation, Command and Control, Action on Objectives

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 environments across many industrial sectors, we estimate they have compromised **~20% of Fortune 500 companies**

UPDATE ON EXISTING ACTIVITY GROUPS

STIBNITE

FEB

Spear-phishing emails targeting Azerbaijani wind renewable resource linked firms

KAMACITE

MAR

New GREYENERGY files discovered in the wild

WASSONITE

JUN

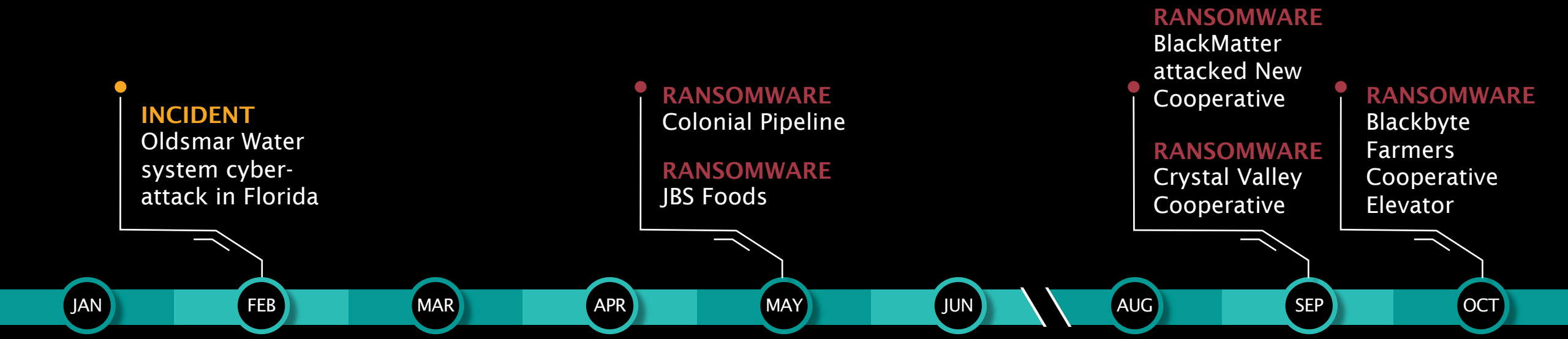
Continued targeting of Electric, ONG, and Manufacturing sites (previously compromised the IT network of an Indian nuclear power company)

KAMACITE

AUG

New GREYENERGY files discovered in the wild

NOTABLE EVENTS IN 2021

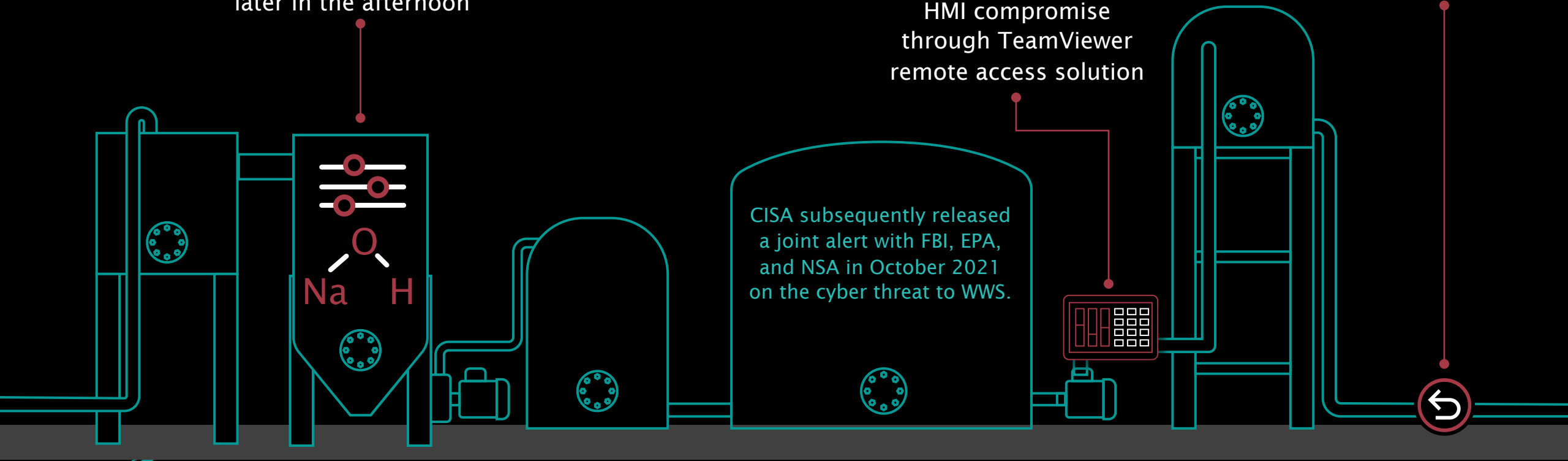


CASE STUDY – OLDSMAR WATER INCIDENT

Access on morning of 05 February 2021, followed by manipulation of NaOH levels later in the afternoon

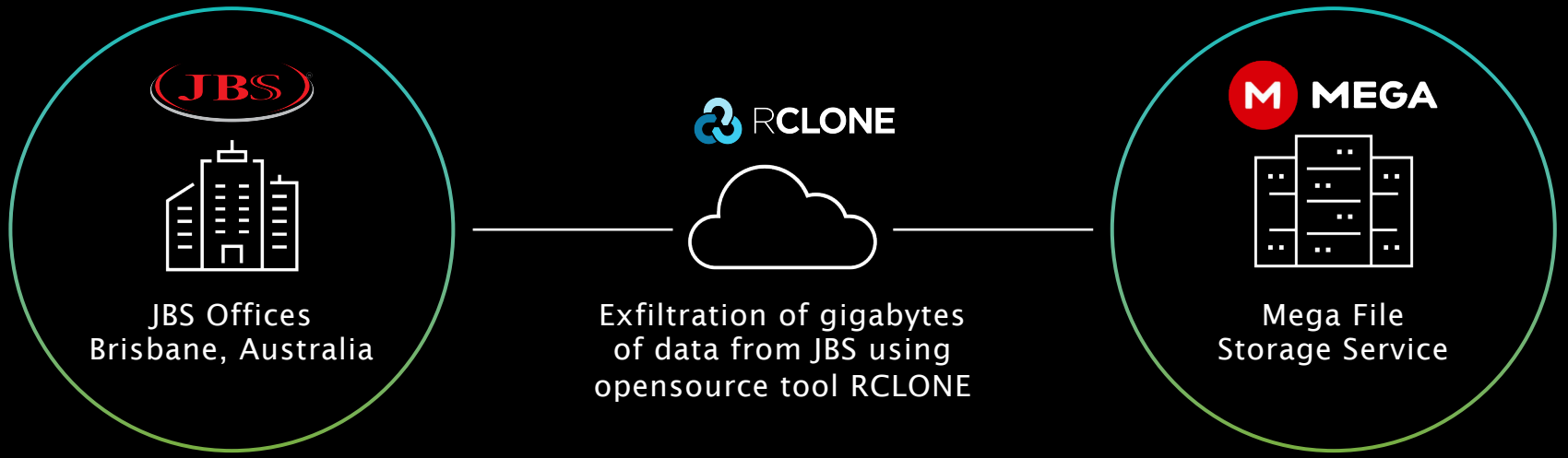
HMI compromise through TeamViewer remote access solution

Modifications noticed by operator and reversed. Physical safeguards also could have alerted on the change in PH



CASE STUDY – JBS FOODS

REvil RANSOMWARE



JBS Global meat supplier with facilities in the U.S., UK, Australia, Canada, Mexico, and Brazil

REvil gains initial access and exploits public facing applications

1. **March 4 & 5**
   Test connections to Mega
2. **March 7**
   Large data upload
3. **April 9**
   Multiple GB of data uploaded
4. **May 30**
   Final Upload, Day the attack was reported

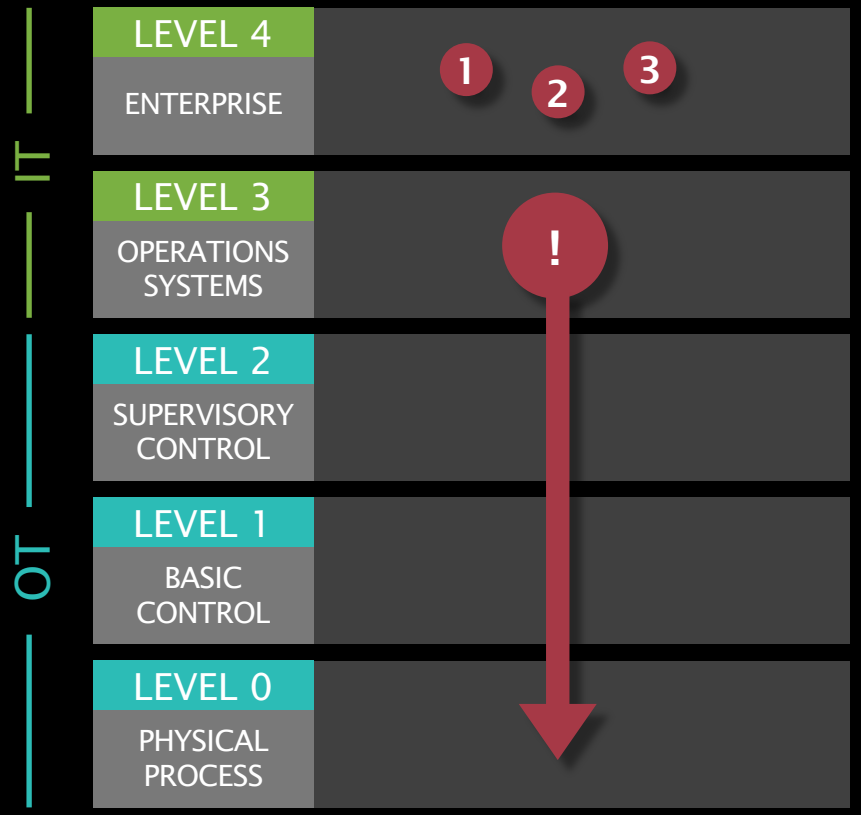
CASE STUDY – COLONIAL PIPELINE RANSOMWARE

Lack of OT Visibility Leads to Precautionary Operations Shutdown To Avoid Catastrophic Impact From Successful IT Ransom Attack

55% of the gasoline, diesel, & jet fuel used on US East Coast

$4.4 million ransom paid, $2.3 million later recovered

DarkSide Ransomware Attack



1 Initial Access
Compromised Credential, no MFA
Likely Phish attack, leading to credential use to gain VPN access into IT systems remote desktop protocol. PowerShell to download tools and install malware.

2 Lateral Movement & Escalation
Access Active Directory to escalate privileges, acquire additional credentials and other data.

3 Exfiltration of Data, Encryption of IT System Files
Data transferred to TOR site.
Locks file systems.
Deletes tools and shadow copies.

4 Precautionary OT Shutdown
Final Upload, Day the attack was reported

RANSOMWARE USE CASE: SEASONAL TARGETING OF AGRICULTURAL COMPANIES

Mid-September 2021
the ransomware group BlackMatter attacked New Cooperative, an association of Iowa corn and soybean farmers, and demanded a $5.9 million ransom payment for a decryptor.

September 19
the Minnesota-based Crystal Valley Cooperative announced it was also hit with ransomware, which forced the company offline and disrupted its business operations.

Later in October
the ransomware group BlackByte allegedly attacked a second Iowa cooperative called Farmer's Cooperative Elevator Co.

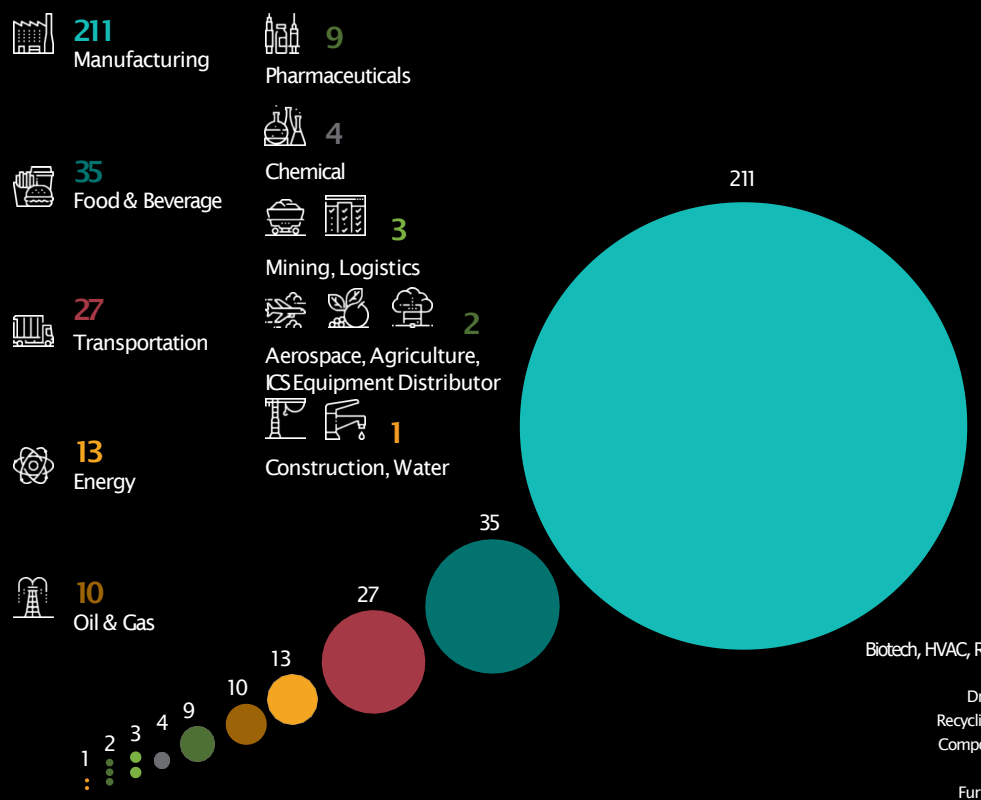
GLOBAL VICTIM MAP

RANSOMWARE TRENDS

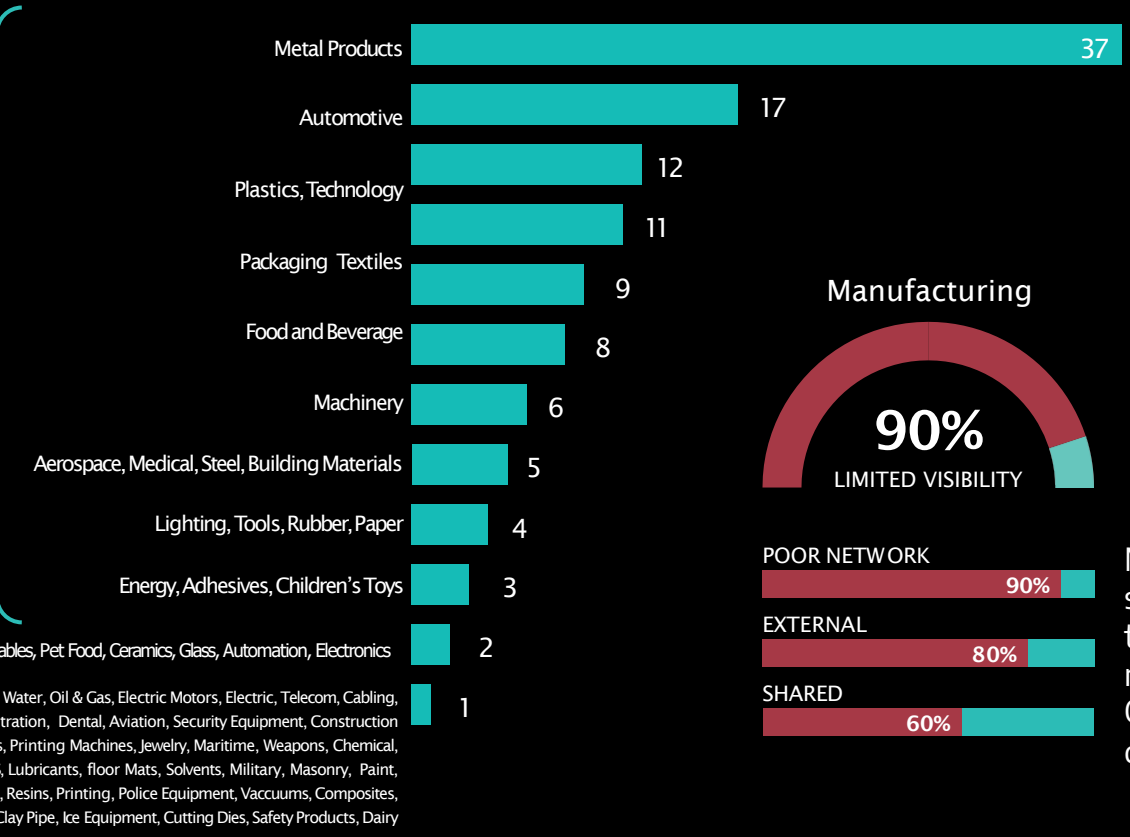
Ransomware became the number one attack vector in the industrial sector.

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

Ransomware by ICS Sector



Ransomware by Manufacturing Subsector



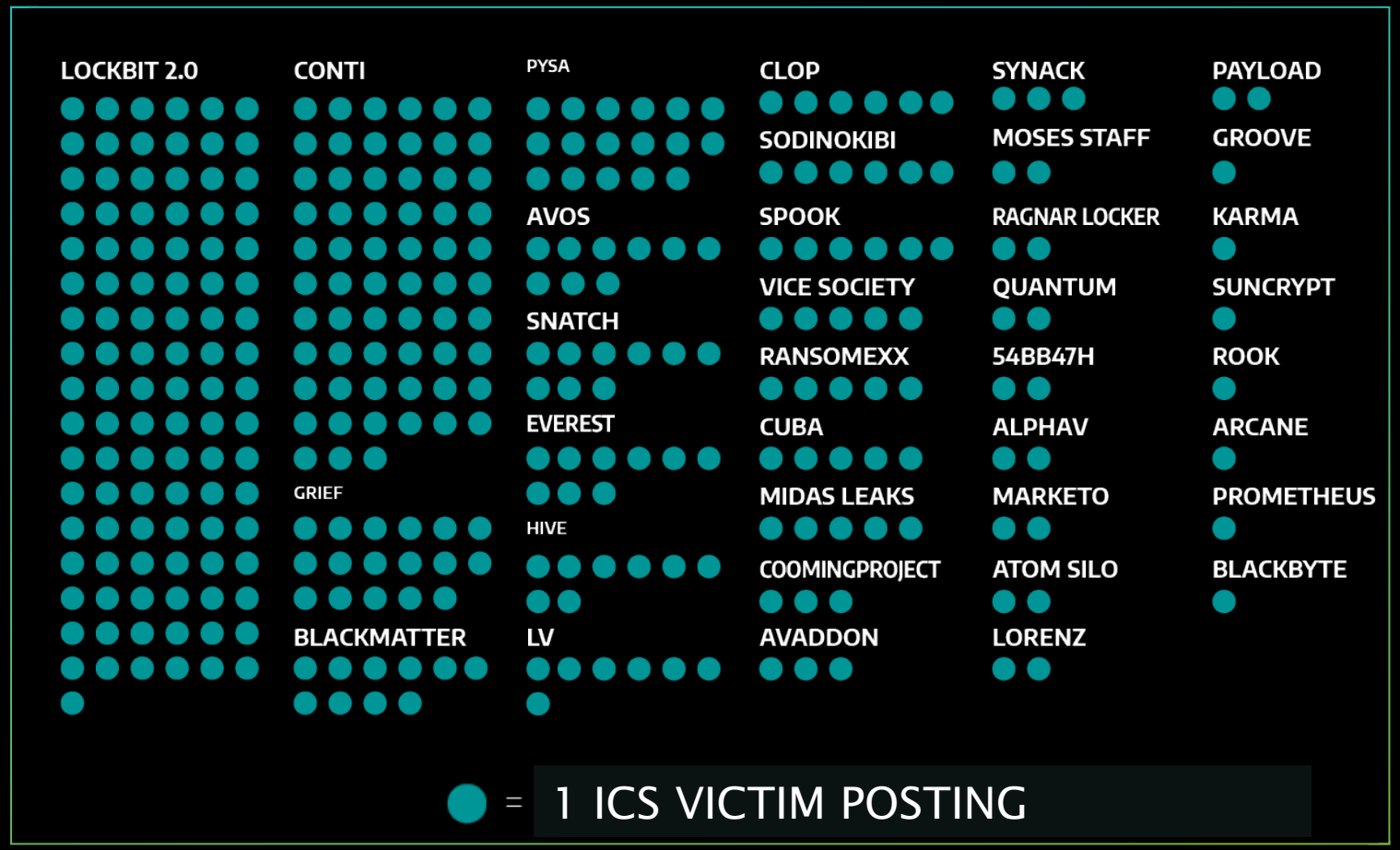
Manufacturing sector is often the least mature in their OT security defenses.

RANSOMWARE INCIDENTS by GROUP/STRAIN

Lockbit 2.0 and Conti account for:

51% of the total ransomware attacks

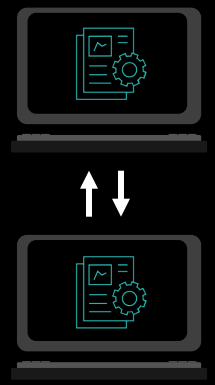
70% of their malicious activity targeted manufacturing



DEEP DIVE: LOCKBIT 2.0 AND CONTI

Ransomware gangs like Conti and Lockbit 2.0 have mobilized an underground marketplace where their developers **outsource operations to affiliates who execute the attacks**

Conti, active since 2020, is often volatile and offers low levels of support for victims; prone to leaks, a disgruntled affiliate leaked the “Conti playbook” in August 2021.



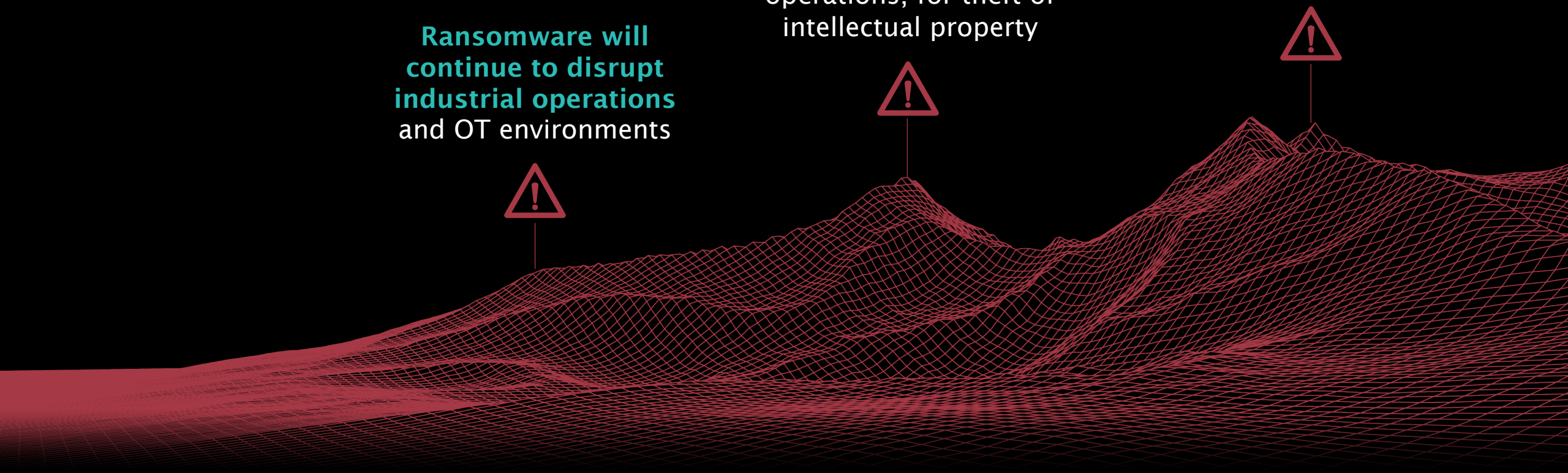
In June of 2021, Lockbit 2.0 retooled and now focuses on stealing data and extorting victims for financial gain by threatening publication of exfiltrated data if victims do not pay the ransom.

DRAGOS 2022 ASSESSMENTS

Ransomware will continue to disrupt industrial operations and OT environments

State-sponsored adversaries may leverage ransomware to mask their alternate operations, for theft of intellectual property

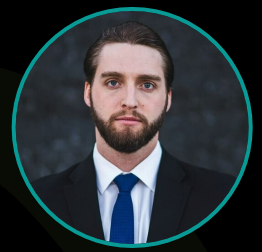
Ransomware actors' **extortion techniques will continue to grow in severity and intensity** as adversaries deploy any means available to pursue their ransom payments



QUESTIONS AND ANSWERS

THANK YOU

Anna Skelton
Senior Intelligence Analyst
Dragos, Inc.



Seth Lacy
Principal Adversary Hunter
Dragos, Inc.

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