CSA SINGAPORE | SG Passion Made Possible

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

22 – 23 AUGUST 2023

Preventing Unintentional or Collateral Cyber Disasters

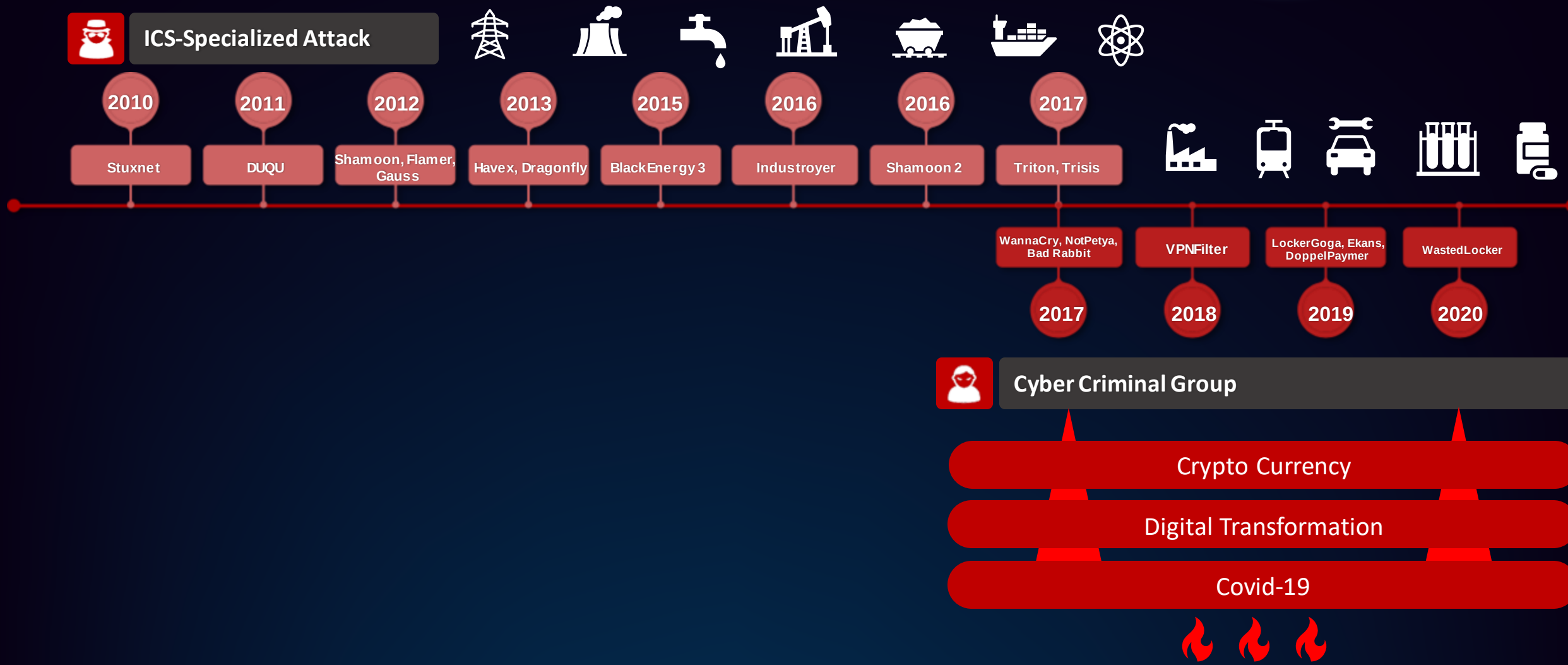
Dr. Terence Liu

CEO, TXOne Networks

OT Cyber Breaches are happening

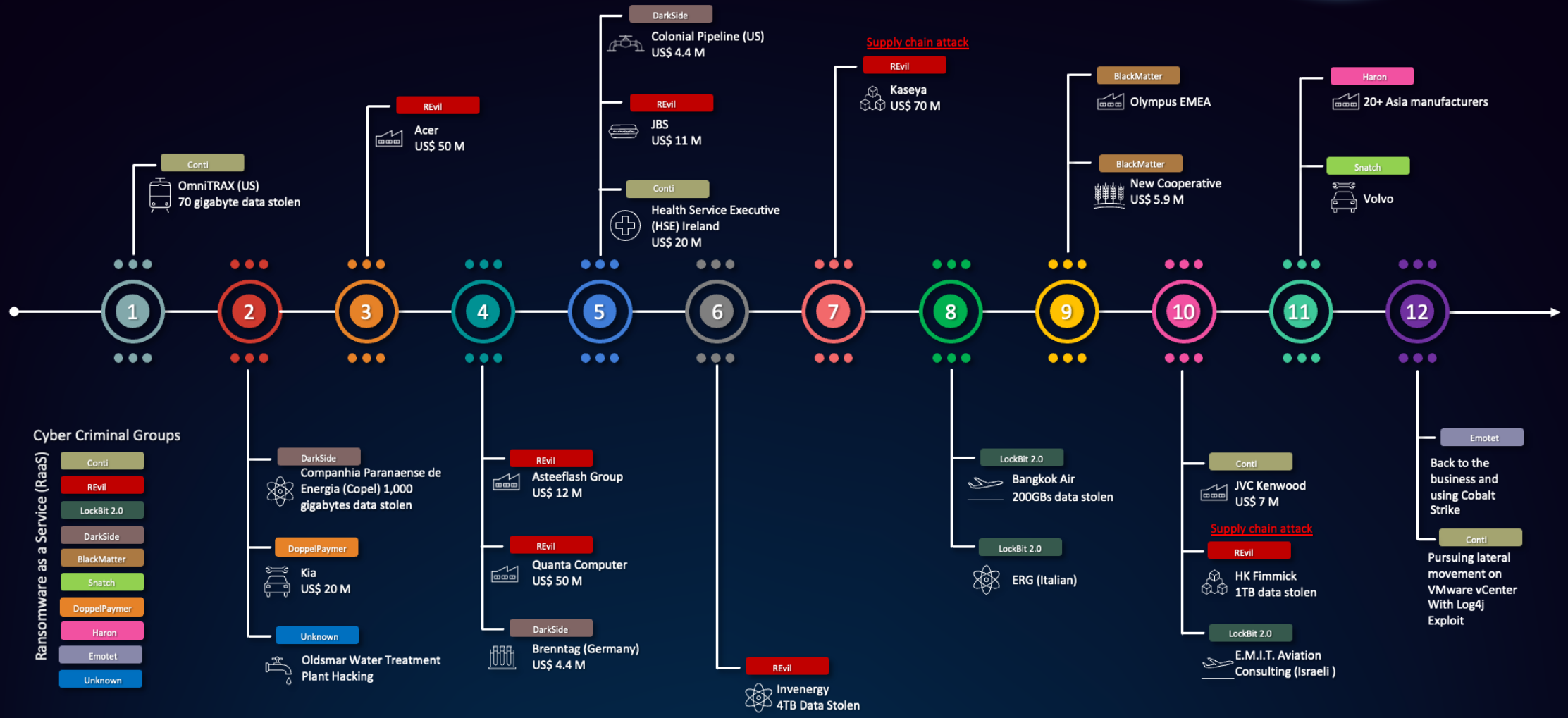
OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

The Paradigm Shift of OT Threats



OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

OT Cybersecurity Issues in 2021 – Mainly ransomware attack



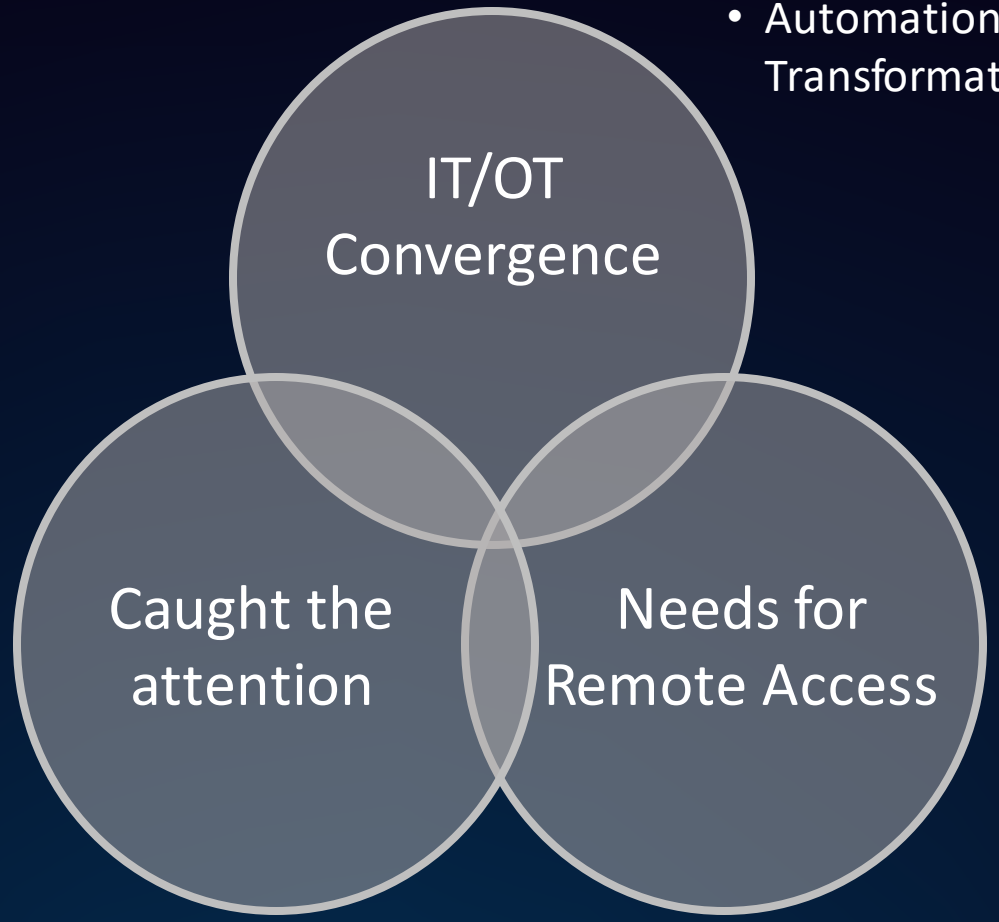
OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

Diversified OT Attack Techniques in 2022

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

Perfect Storm for OT Cybersecurity Threats

- Automation, Digitalization, Digital Transformation

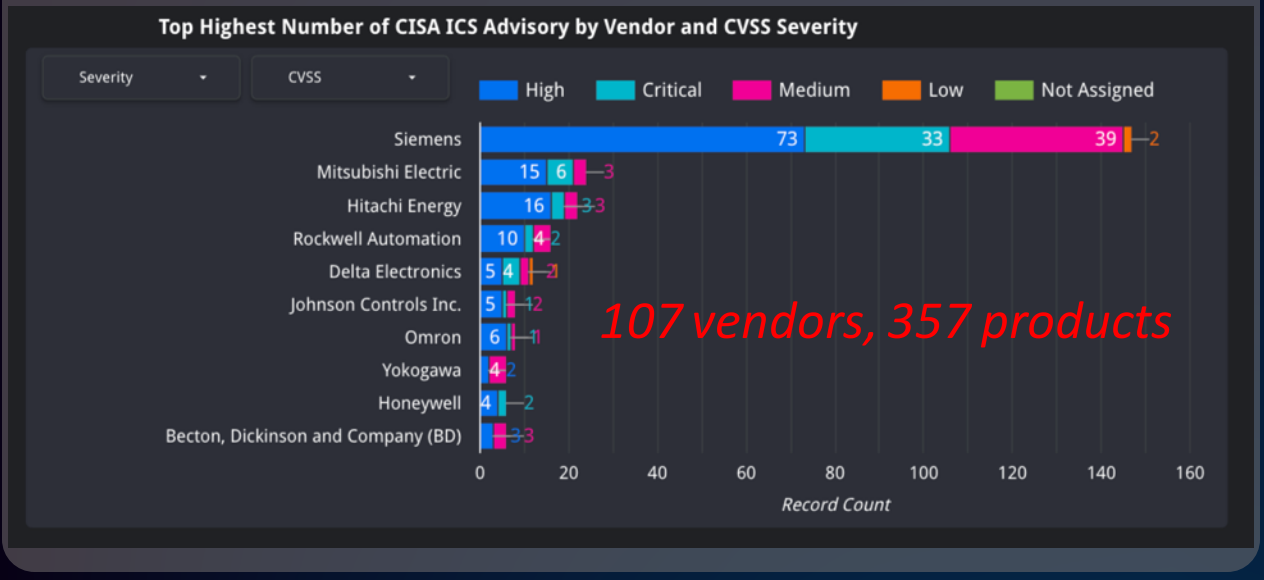


- Cyber criminals are aware that manufacturers are the soft spot
- Geopolitical tension

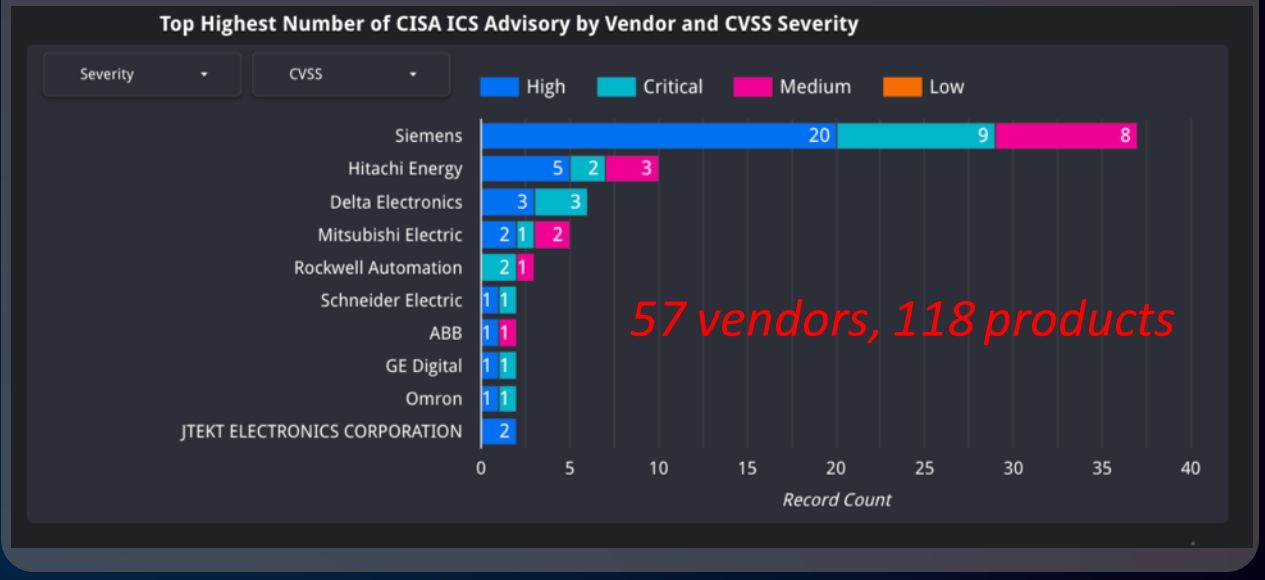
- Pandemic results in the shift of work culture
- Remote Access introduces more risks

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

2022.01–2022.12



2023.01 – 2023.04



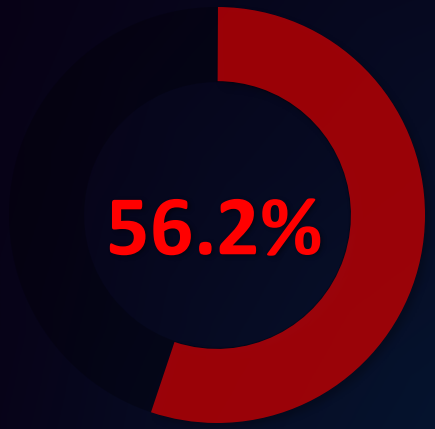
Source: ICS Advisory Project

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

OT Vulnerabilities are Critical

Source: TXOne Networks 2022 Annual Report

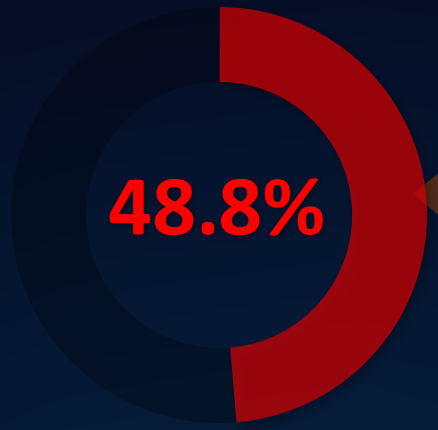
ICS-CERT ADVISORIES



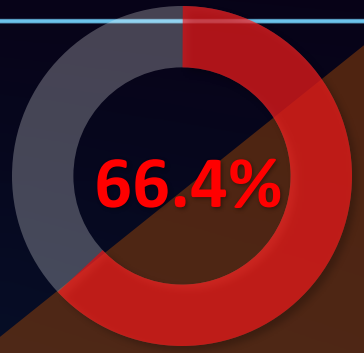
The number of ICS-CERT advisories increased by 56.2% from 2020 to 2021.

CRITICAL MANUFACTURING

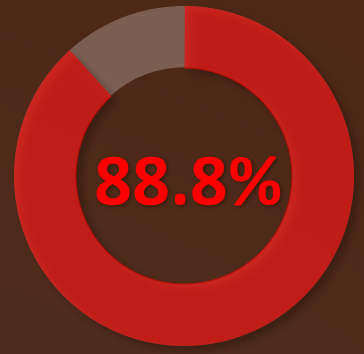
Report focused on ICS-CERT advisories listed vertical – "Critical Manufacturing"



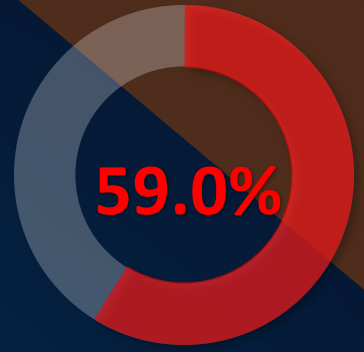
of CVEs identified in ICS-CERT advisories in 2021 can be used to affect Critical Manufacturing.



of 2021's ICS-related vulnerabilities may be used by attackers to accomplish Initial Access and compromise a system.



of 2021's CVEs affecting the Critical Manufacturing sector can be used to cause an Impact.



of 2021's CVEs can be used to cause damage to property, productivity, or revenue.

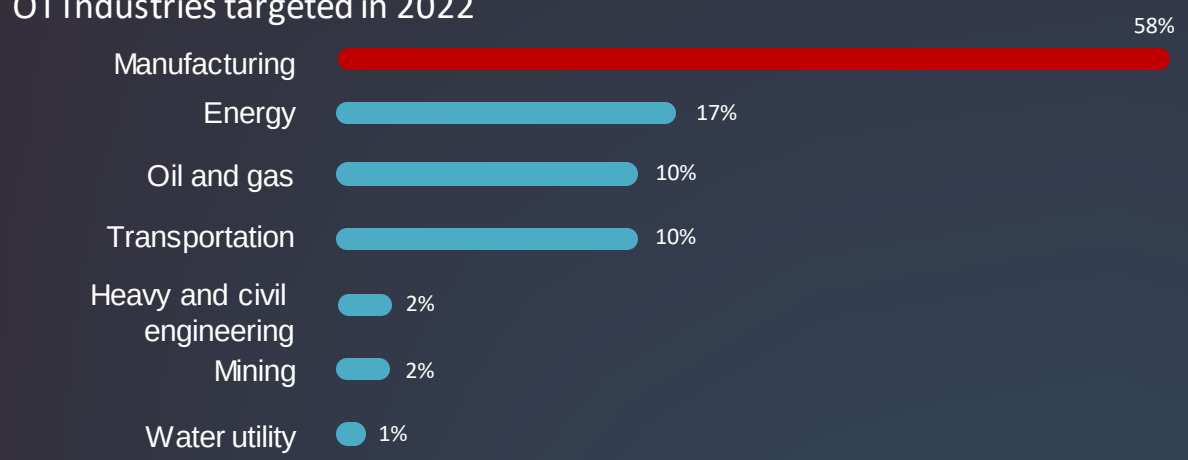
OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

Manufacturing becomes the world's most attacked industry

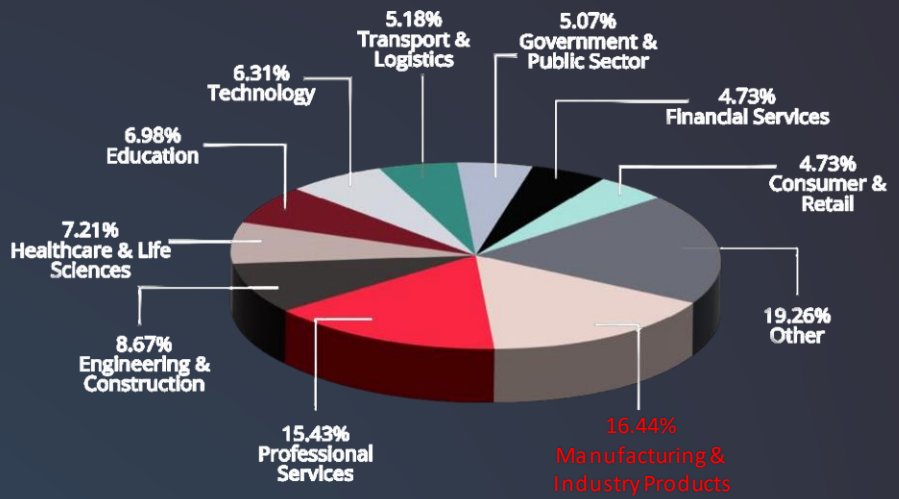
Manufacturing replaced financial services as the top attacked industry in 2021 - representing 23.2 percent of the attacks… (IBM X-Force Threat Intelligence Index 2022)

Manufacturing was the most targeted sector for ransomware cyber-attacks and the most extorted industry in 2022… victimized in 30 percent of incidents… (IBM X-Force Threat Intelligence Index 2023)

KELA disclosed that the manufacturing and industrial sectors were most targeted by ransomware attackers and data leak actors during the first quarter of 2023 (KELA 2023Q1 Ransomware Report)



Proportion of IR cases by OT-related industry to which X-Force responded in 2022.

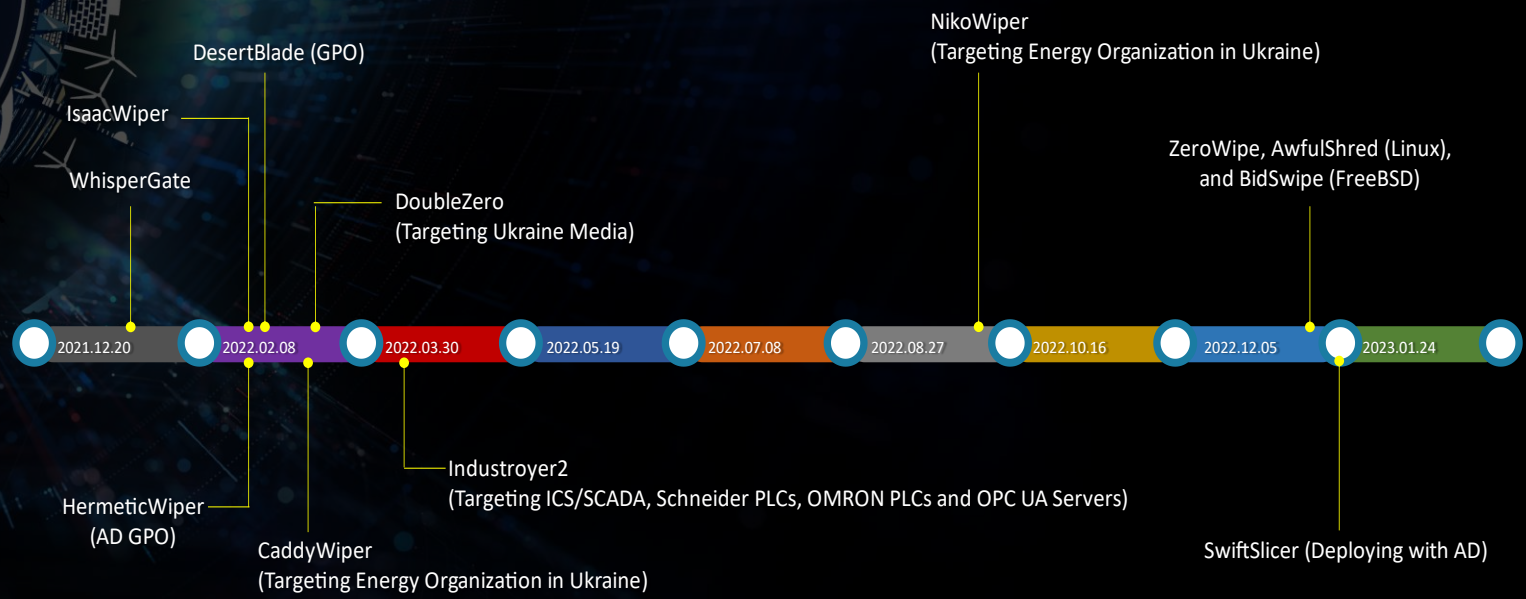


KELA ransomware victims and network access sales in Q1 2023

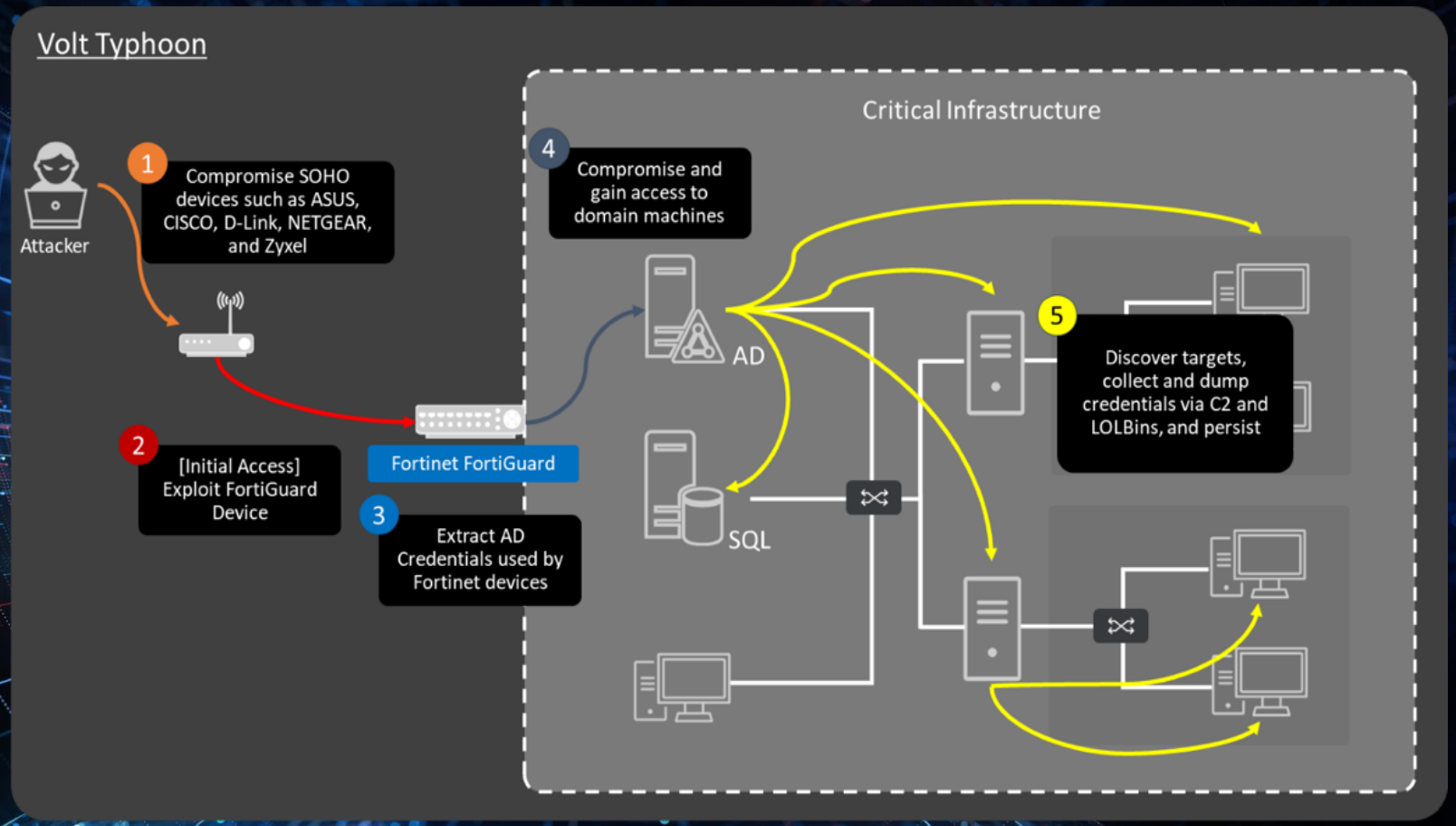
Geopolitics lead to an increase in malicious disruptions in 2023

Wiper Attacks

- Unprecedented Data Destruction Attack on Critical Infrastructure in Ukraine
- In addition to Ukraine, as many as 25 other countries were also affected
- Over 16 different families of Wiper malware have been discovered in the past year



Volt Typhoon targets US critical infrastructure



This TTP allows the actor to evade detection by blending in with normal Windows system and network activities, avoid endpoint detection and response (EDR) products that would alert on the introduction of third-party applications to the host, and limit the amount of activity that is captured in default logging configurations.

The attackers exploit zero-day vulnerabilities in Fortinet FortiGuard devices, and gain access to a device that allows them to connect directly to the internal network of critical infrastructure.

Obstacles and Challenges

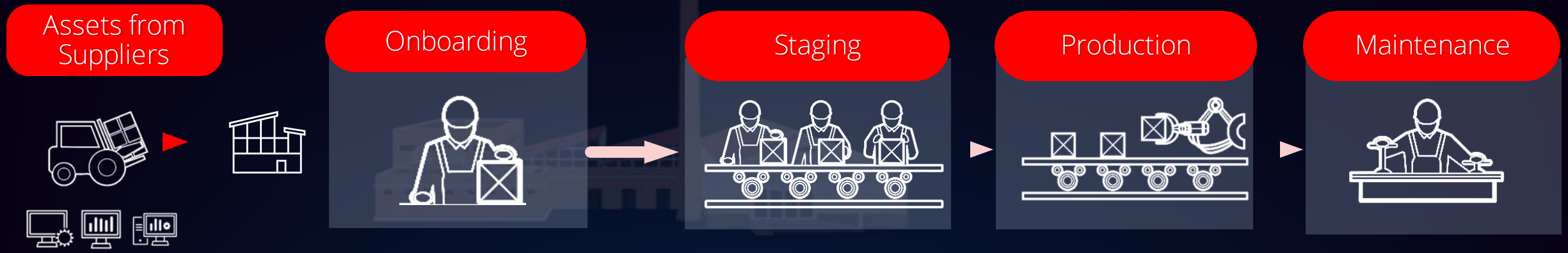
OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

IoT-OT Attacking Vectors

	Worm and Virus	Ransomware	Cyber Sabotage
Root Cause	• Internet Scanning (IoT) • Unintentional infection • Compromised equipment	• Targeted attack. IT Protection fails, and hackers manage to find a path to penetrate OT	• Any possible way including insider threats
Impact	• Trojan/Backdoors • Malfunctional devices • Worm propagates to interrupt the operation	• Mission-Critical assets are locked/encrypted so that operation will be interrupted • Impact to business reputation and possibly the trade value for public companies	• Mission-Critical assets are manipulated • Loss of Safety and Availability

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

The collateral damage of IT security incidents impacting the OT environment for the business continuity



47%

OT/ICS attack come from new assets

6%

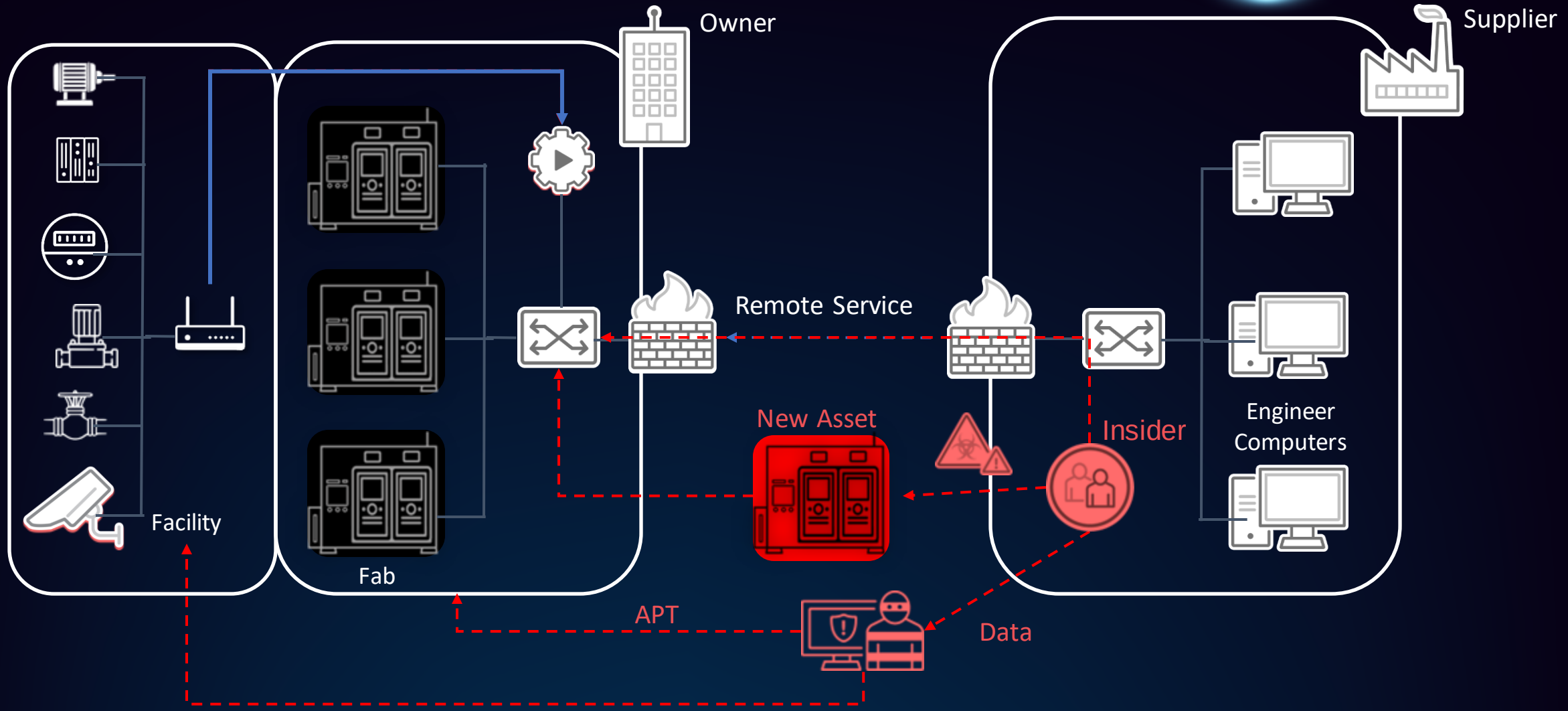
of organizations have 100% of their Windows devices protected by endpoint security solutions

94%

of IT security incidents affect the organization's OT environment

Source: TXOne Networks 2022 Annual Report

Supply Chain Cybersecurity has been a real issue



OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

Enterprise IoT-OT Security Challenges

Continuous cybersecurity threats

- Multiple Extortion Ransomware
- Supply Chain Attacks
- Critical Infrastructure on the target List

Geopolitics and Regulations

- Nation regulation focus on the level up the critical infrastructure cyber and physical security

Collateral Damage to OT

- OT operation impacted by IT cybersecurity incidents in data and operation hostage

Lack of even Basic Protection

- Insiders and supply chain threat
- Lack of protection in the OT environment

Shortage of Cyber Talents

- Globally, the shortage is estimated to be 2.72 Million
- The difficulty of hiring qualified security professionals from a limited talent pool

Best Practices in Cybersecurity for Manufacturers

Step-by-step from Within to Without

With support from top management,

define R&R, build a (small) team,

extend your security guideline from IT to OT,

in order to

1. Strengthening Perimeter Security to Reduce Attack Vectors
2. Elevating OT Defense for Enhanced Resilience
3. Strengthening Ecosystem Cybersecurity Preparedness

Strengthening Perimeter Security to Reduce Attack Vectors

- Build the OT DMZ
  - A Zone, Not a Wall
- Remote Access
  - Meet each other in the cloud
- Inspection of inbound devices
  - newly delivered or refurbished equipment
  - computers and storage medias tool of visitors
- Inspection of Outbound traffic
  - More restricted destination for OT servers

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

Elevating OT Defense for Enhanced Resilience

Endpoint

- GOOD
  - Endpoint protection
    - Anti-Malware
    - Whitelisting for legacy machines
  - Secure file transfer
- UGLY
  - System performance
  - Diversity of Legacy and Modern systems
  - SaaS vs On-Prem
  - Alert fatigue
  - Lifecycle gap
  - High Roll Out Costs

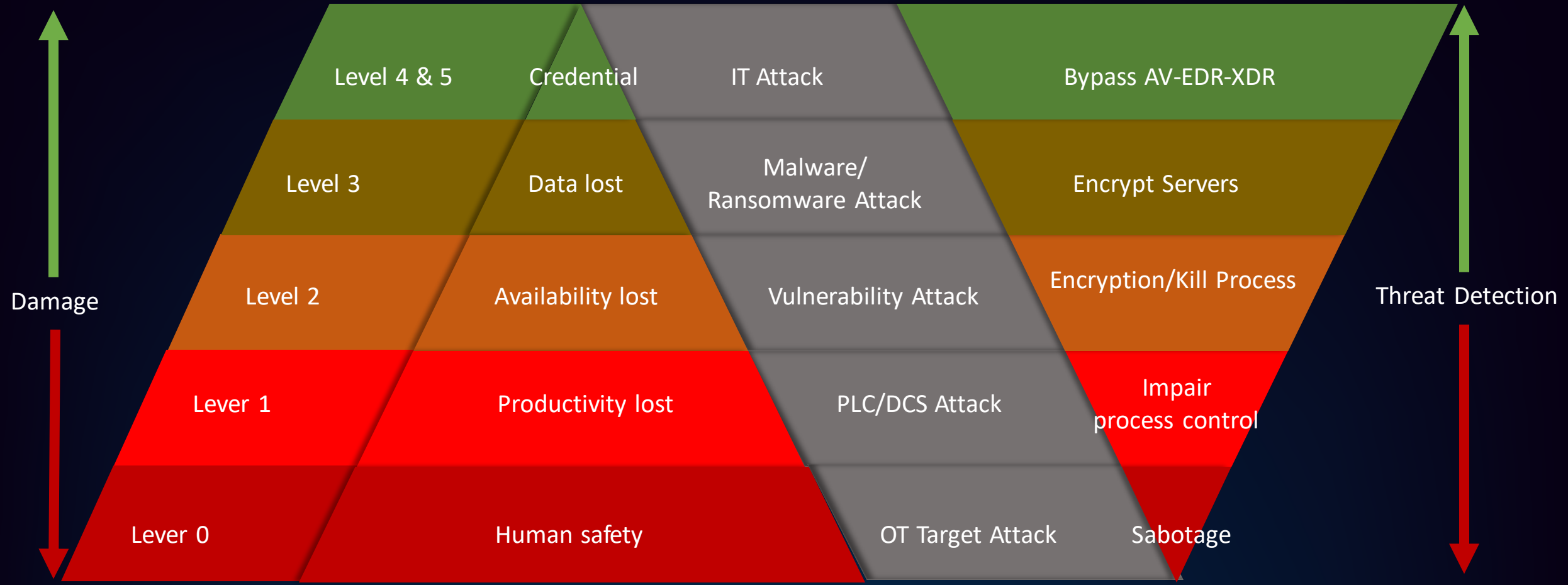
Network

- GOOD
  - Micro Segmentation
  - Virtual Patching
  - OP Whitelisting
- UGLY
  - Network performance
  - HW/SW failure of Security products
  - High Roll Out Costs

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

Elevating OT Defense for Enhanced Resilience: Visibility ▸ Cyber Hygiene ▸ Detection & Response

OT is the last line of defense for the corporate



OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

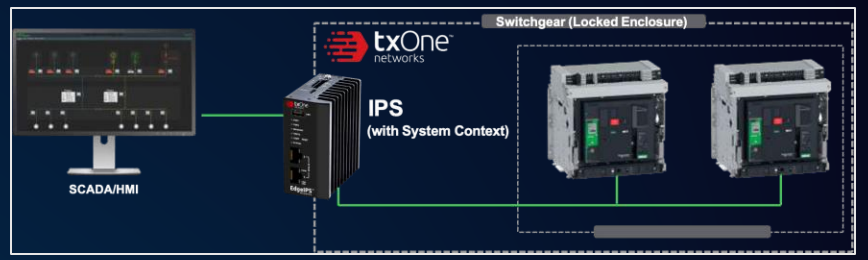
Strengthening Ecosystem Cybersecurity Preparedness

As a buyer

- Request legitimate products
  - Correct configuration
  - Without Trojans and malwares
- Request better cybersecurity posture to suppliers
  - External Assessment
  - Questionnaire Assessment
- Develop cybersecurity standard, guidelines, or reference architecture
  - e.g. SEMI E187, GISAX

As a Supplier

- Security by design
  - Secure SDLC
  - Software components
  - Certificate and Credential
  - Pentest
- Secure your products (and watch it)
  - Perimeter gateway
  - Application whitelisting



Summary

- Incorporating OT and IoT into Cybersecurity Blueprint for Digitalization and Automation Journey
- Urgent Resilience Enhancement for Manufacturers and Critical Infrastructure Targeted by Digital Crimes
- Securing OT Boundaries with Zero Trust: Comprehensive Examination of All Ingress and Egress
- Strengthening Internal OT Networks and Endpoints for Enhanced Operational Resilience
- Collaborative Efforts for Rising Supply Chain Cybersecurity Significance among Owners and Suppliers

Thanks for Listening

Dr. Terence Liu

Terence_Liu@txone.com