nviso

Red Team Operations in OT

A peek behind the curtains of hacking industrial systems

RuhrSec – February 2025

ADVERSARIAL RISK EMULATION & SIMULATION

NVISO ARES

ADVERSARIAL RISK
EMULATION &
SIMULATION

Sarah Mader

IT Security Consultant,
Red Team

Sarah.mader@nviso.eu

Operational Technology (OT)?

ICS and OT

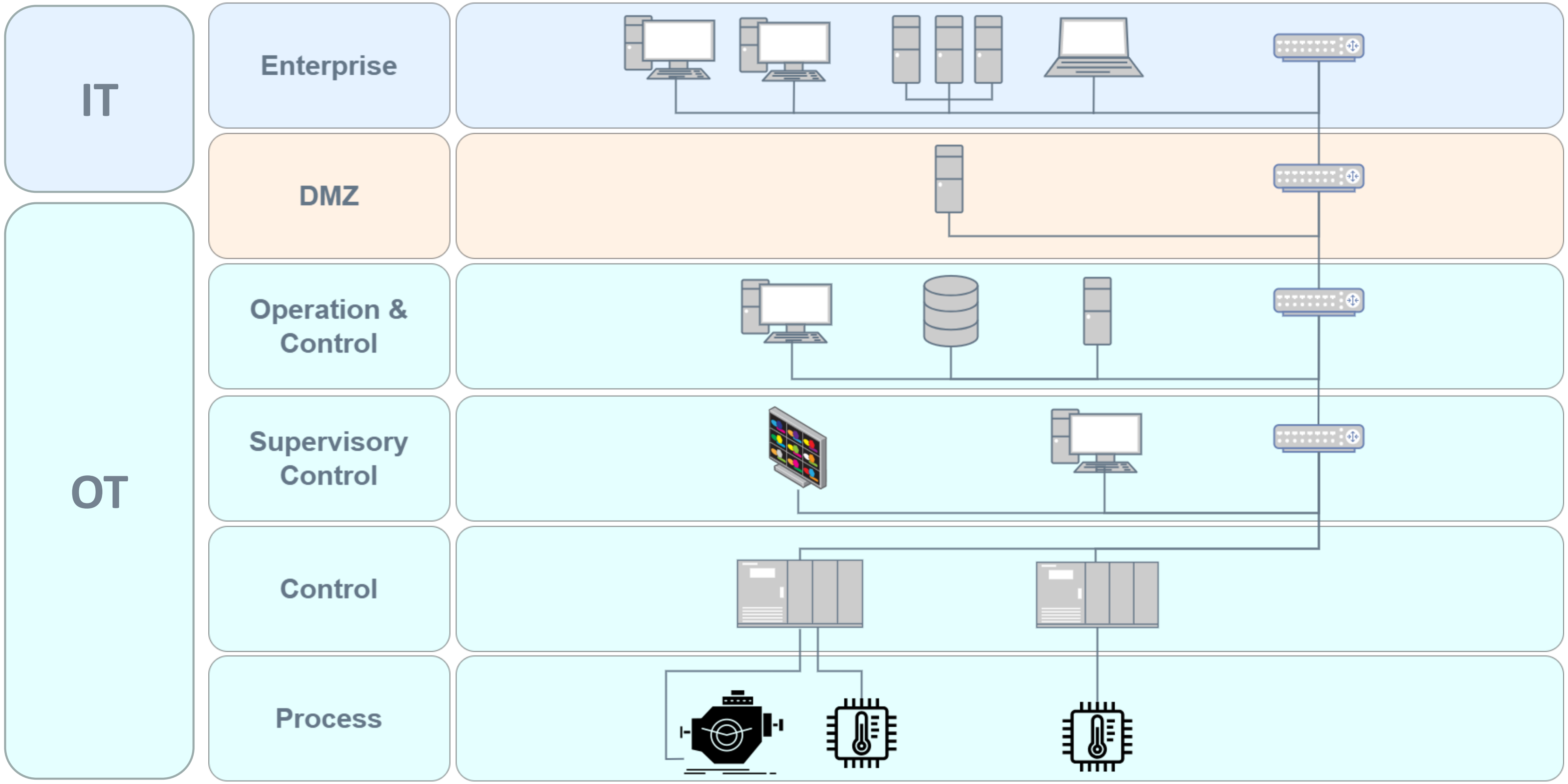
The NIST Computer Security Resource Center defines Operational Technology (OT) as "**Programmable systems or devices that interact with the physical environment** (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms.“

Industrial Control Systems (ICS) are further defined as "An **information system used to control industrial processes** such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems used to control geographically dispersed assets, as well as **distributed control systems** and smaller control systems using **programmable logic controllers** to control localized processes."

https://csrc.nist.gov/glossary/term/operational_technology

https://csrc.nist.gov/glossary/term/industrial_control_system

Company = IT + OT



OT Security?

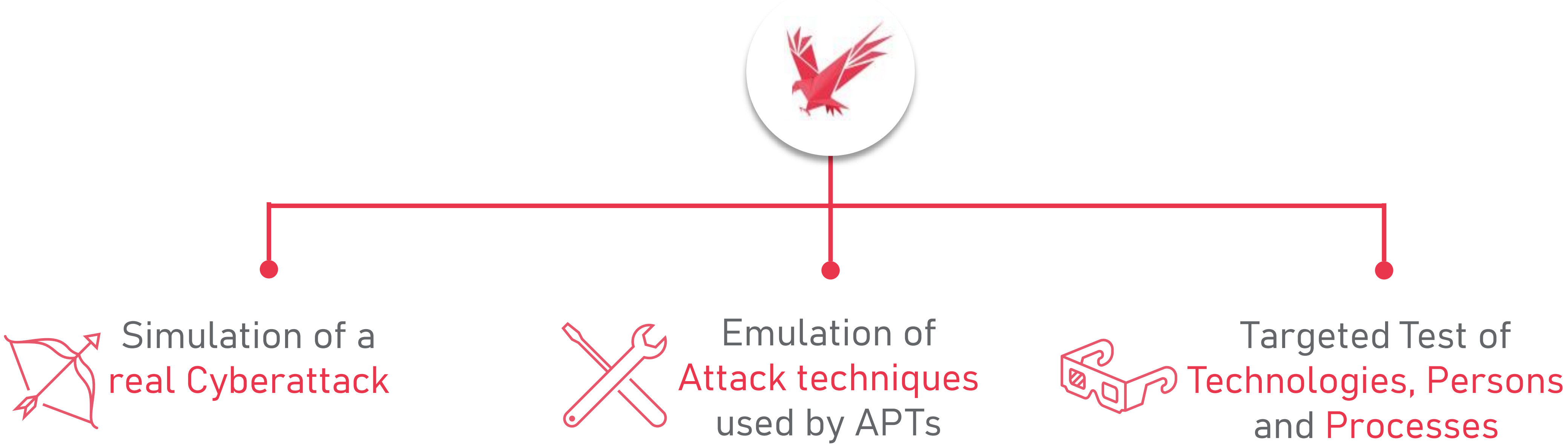
OT Security

- Increased Connectivity
- Surge in global tension led to increased cyber threat activity (Ukraine-Russia, Israel-Hamas, and South China Sea regions)
- Rise in Ransomware Attacks
- Regulations (NIS2, ISA/IEC-62443, etc.)

Introduction to Red Teaming

nviso

Red Teaming



Simulation of a real Cyberattack

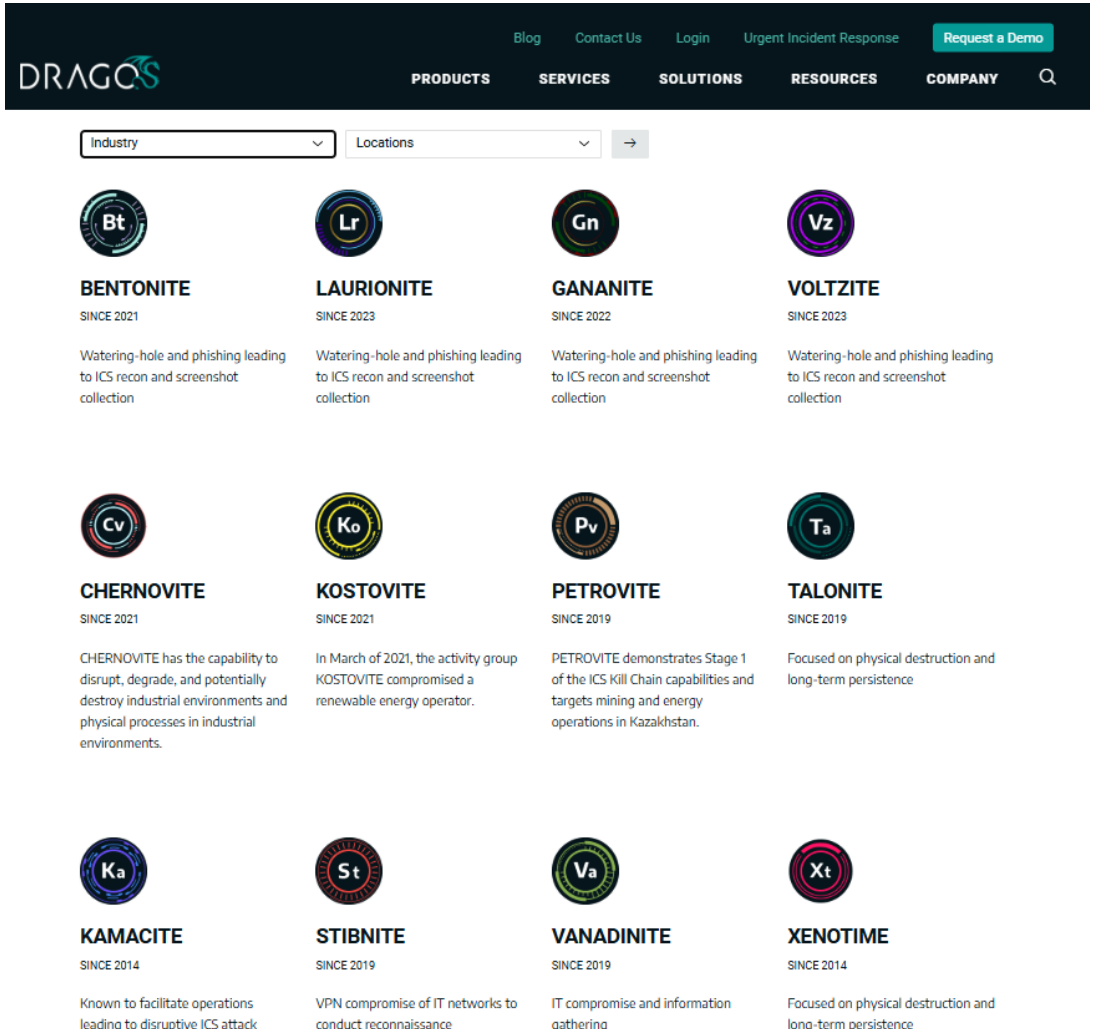
Emulation of Attack techniques used by APTs

Targeted Test of Technologies, Persons and Processes

„APT (Advanced Persistent Threat) is a ***complex, targeted*** *and* ***effective*** *attack on* ***critical IT infrastructures****."*

Introduction to Red Teaming

Advanced Persistent Threat



BENTONITE
SINCE 2021
Watering-hole and phishing leading to ICS recon and screenshot collection

LAURIONITE
SINCE 2023
Watering-hole and phishing leading to ICS recon and screenshot collection

GANANITE
SINCE 2022
Watering-hole and phishing leading to ICS recon and screenshot collection

VOLTZITE
SINCE 2023
Watering-hole and phishing leading to ICS recon and screenshot collection

CHERNOVITE
SINCE 2021
CHERNOVITE has the capability to disrupt, degrade, and potentially destroy industrial environments and physical processes in industrial environments.

KOSTOVITE
SINCE 2021
In March of 2021, the activity group KOSTOVITE compromised a renewable energy operator.

PETROVITE
SINCE 2019
PETROVITE demonstrates Stage 1 of the ICS Kill Chain capabilities and targets mining and energy operations in Kazakhstan.

TALONITE
SINCE 2019
Focused on physical destruction and long-term persistence

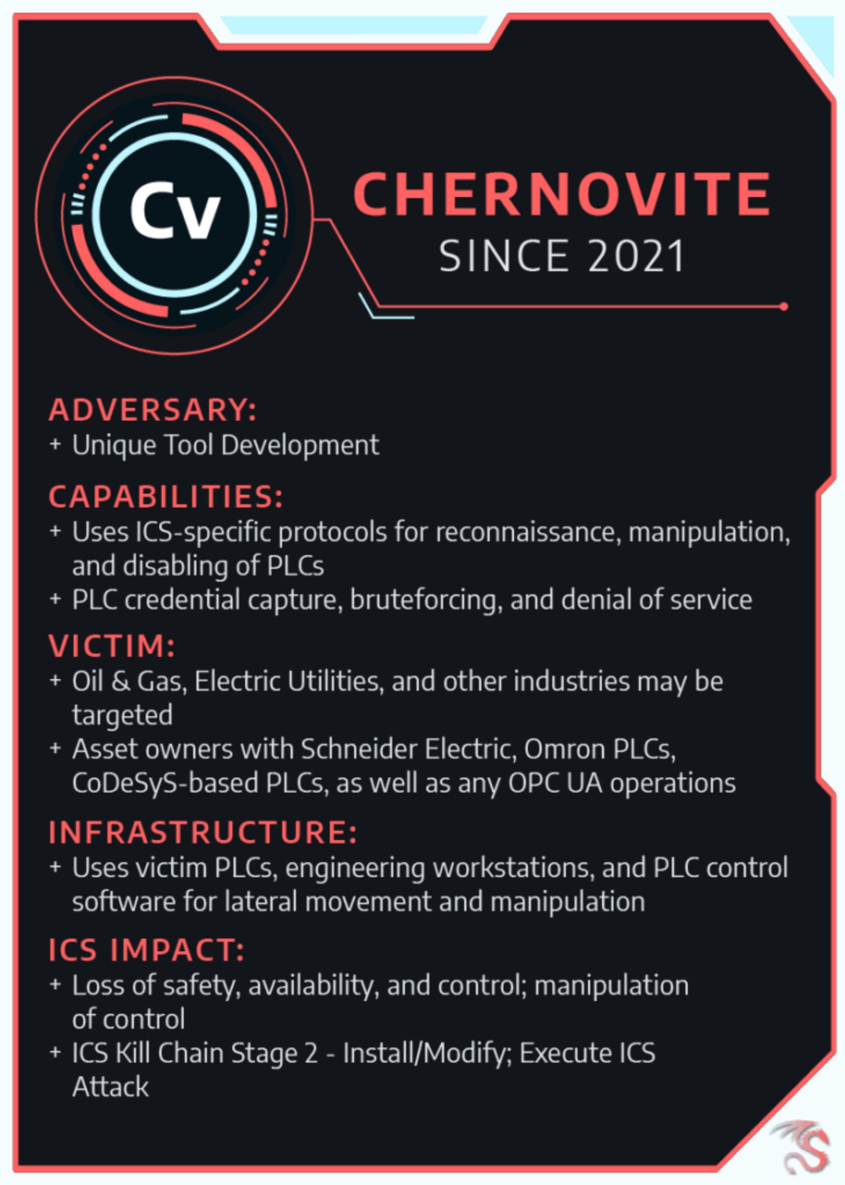
KAMACITE
SINCE 2014
Known to facilitate operations leading to disruptive ICS attack

STIBNITE
SINCE 2019
VPN compromise of IT networks to conduct reconnaissance

VANADINITE
SINCE 2019
IT compromise and information gathering

XENOTIME
SINCE 2014
Focused on physical destruction and long-term persistence

https://www.dragos.com/threat-groups/



CHERNOVITE
SINCE 2021

ADVERSARY:
- Unique Tool Development

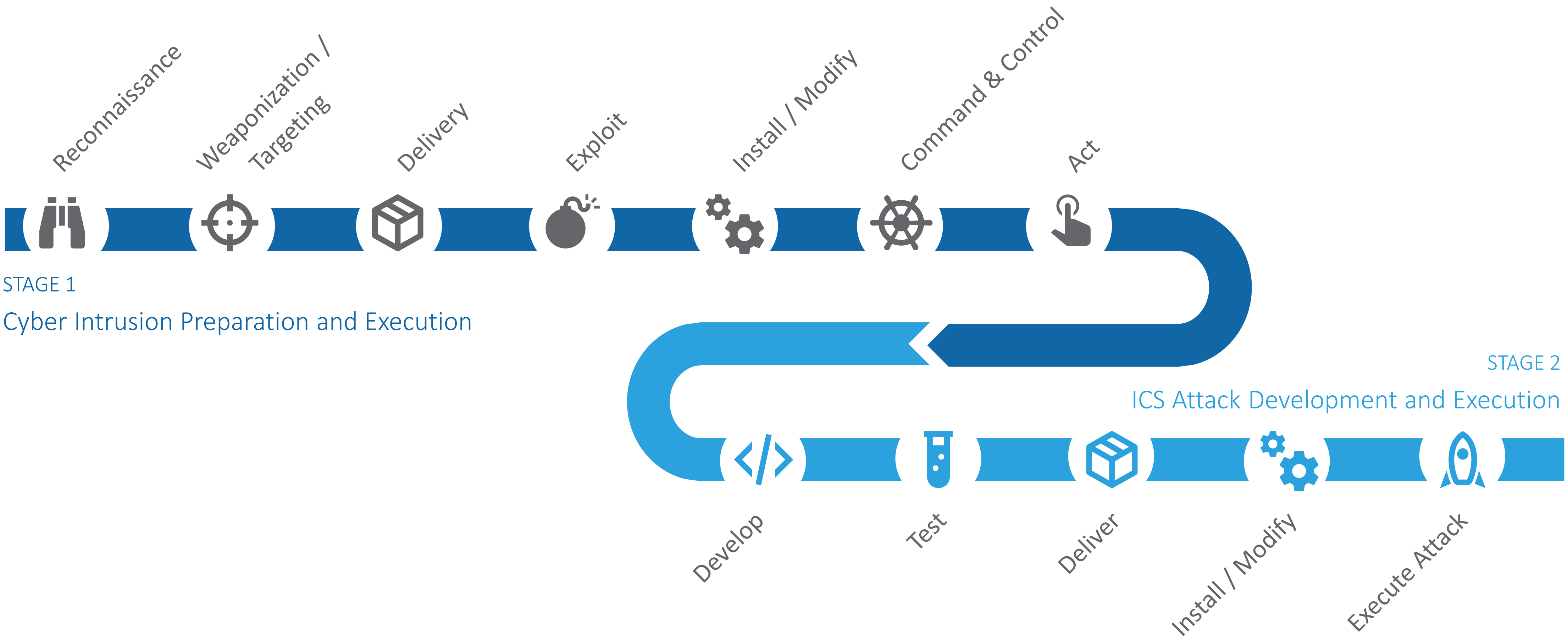
CAPABILITIES:
- Uses ICS-specific protocols for reconnaissance, manipulation, and disabling of PLCs
- PLC credential capture, bruteforcing, and denial of service

VICTIM:
- Oil & Gas, Electric Utilities, and other industries may be targeted
- Asset owners with Schneider Electric, Omron PLCs, CoDeSyS-based PLCs, as well as any OPC UA operations

INFRASTRUCTURE:
- Uses victim PLCs, engineering workstations, and PLC control software for lateral movement and manipulation

ICS IMPACT:
- Loss of safety, availability, and control; manipulation of control
- ICS Kill Chain Stage 2 - Install/Modify; Execute ICS Attack

https://www.dragos.com/threat/chernovite/



STAGE 1

Cyber Intrusion Preparation and Execution

STAGE 2

ICS Attack Development and Execution

But OT is not IT

OT vs. IT

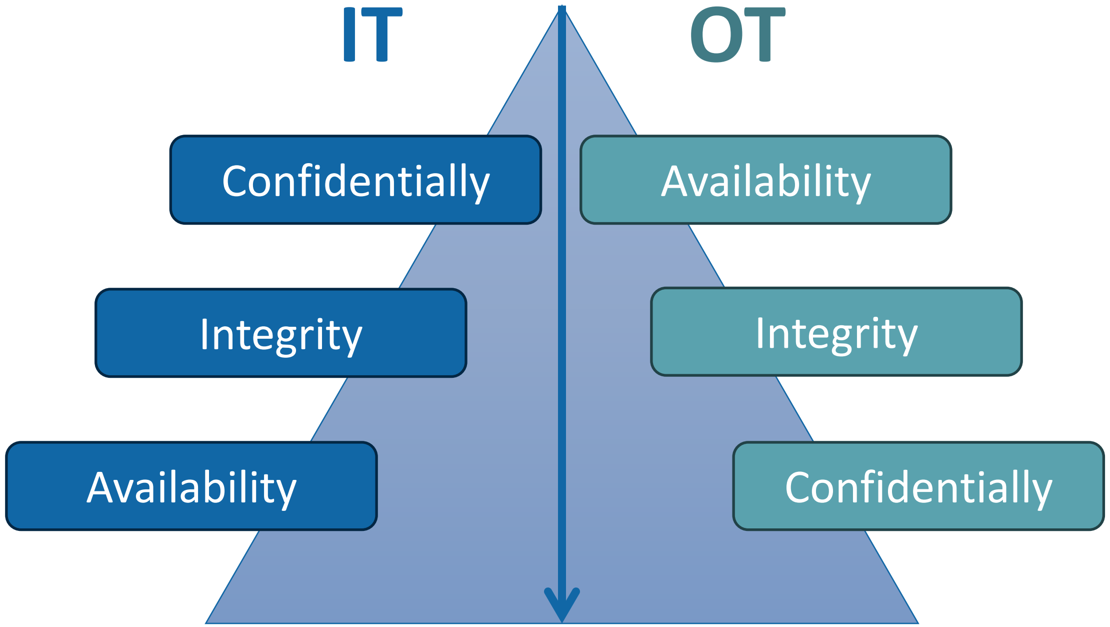
True but…

- 38% of compromises to ICS environments in 2023 come from compromises in IT networks

OT vs. IT

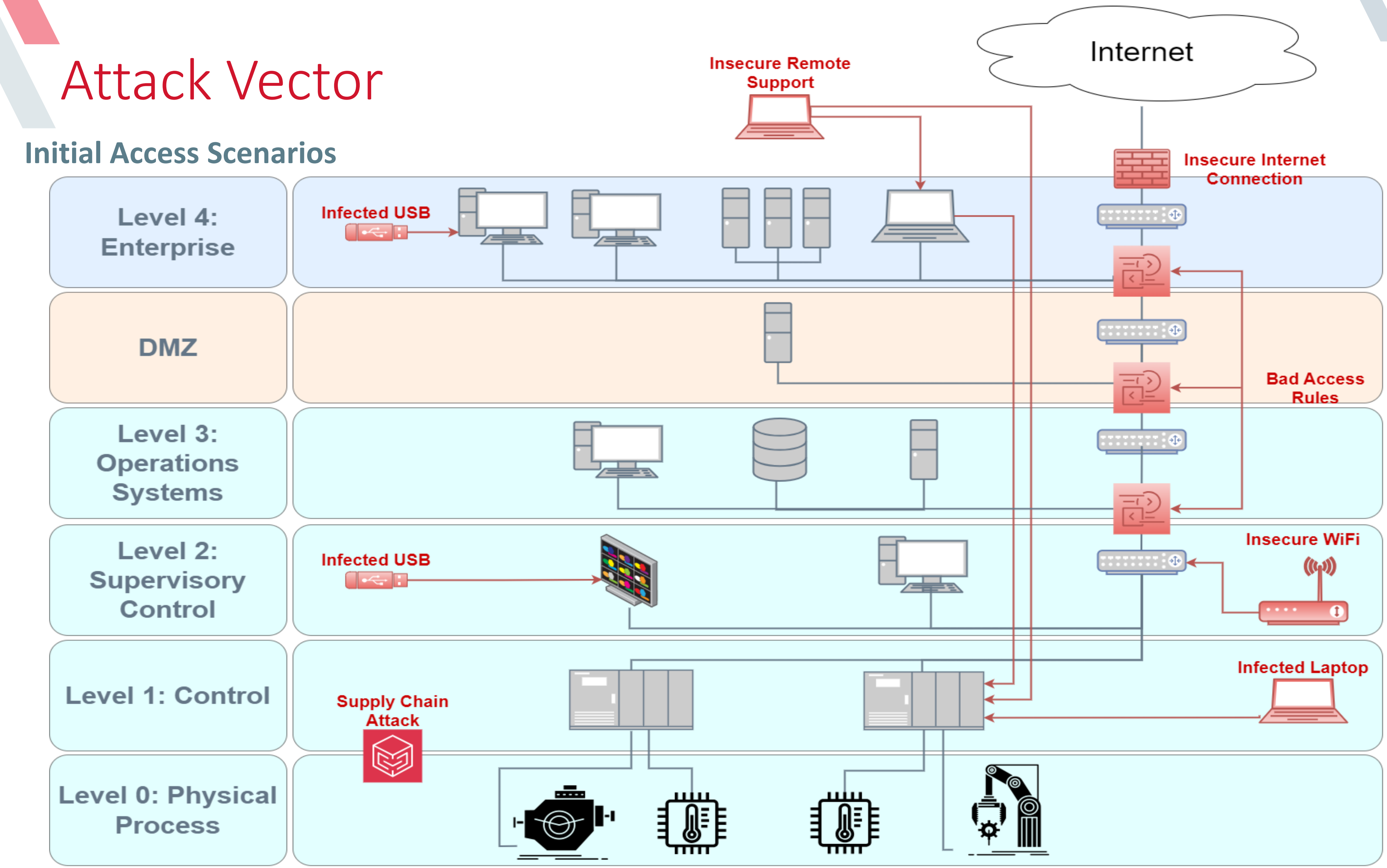
Key Difference

- Safety is always first in ICS environments



Attack Vector

Initial Access Scenarios



Case Story

Case-Story

OT Red Team Assessment

Initial Access:	Physical
Objectives:	Compromise OT network & takeover control
Temperature:	0° down to -20°
Success:	True

www.nviso.eu

Case-Story

Physical Assessments

Case-Story

SL

Lomier
Humans lowern 20;
Allowad
Allowed
Not Allhow|Lerne
239°
2:23°
↑ 22

Brainstorm Location #1

- Pick locks at night
- Social engineering: visitors' tour

Case-Story

- Lockpicking, sure…
- Visitor tour

Case-Story

- Lockpicking,
- Visitor tour

Brainstorm Location #2

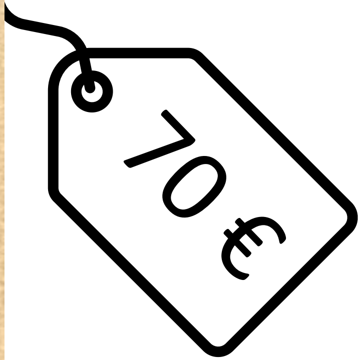
Break into facility at night

- Lots of security measures, What to do once inside?

Social engineering: cleaning service

- Bypass security measures, Ask for assistance once inside!

Case-Story



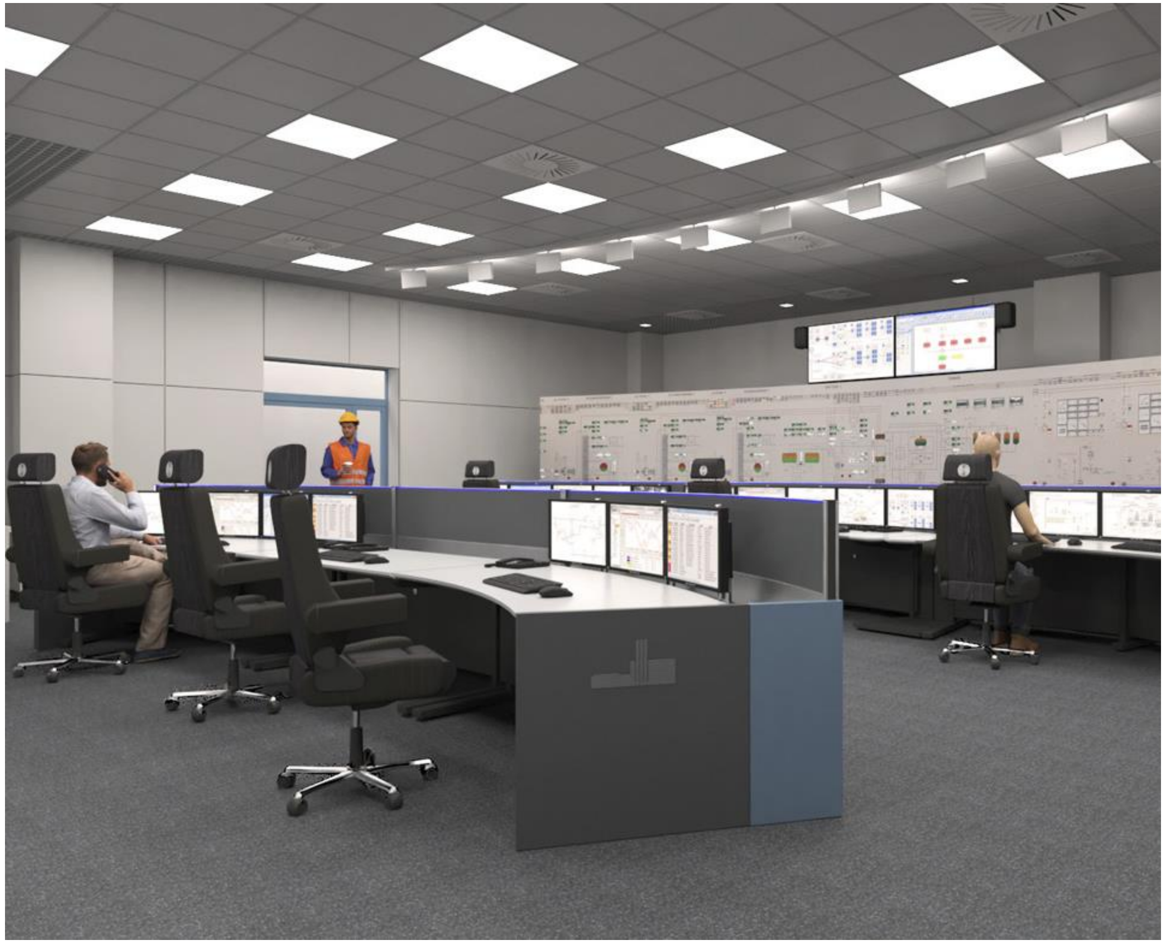
Case-Story

Problem: Control Room still locked!

Case-Story

Problem: Co
still locked!

Case-Story



Thank you!