VEDERE LABS

ATTACKING & DEFENDING CPS

Elisa Costante, PhD
VP of Research

1. About Forescout and Vedere Labs
2. The Evolution of Threats for CPS
3. CPS-specific Vulnerability Research
4. CPS-Specific Threats
5. Defense Mechanisms

Who is Forescout?

Over 20 years of cybersecurity expertise...

- *Headquartered in Dallas, Texas*
- *Employees in over 30 countries*
- *Leader in threat research and intelligence*

Over 3000 customers globally...

- *30% of Fortune 100, 20% of Global 2K*
- *Expertise across Financial, Insurance, Healthcare, Government, and Utilities industries*

Trusted and Proven...

- *Millions of end points deployed in US DoD Comply-to-Connect Program*
- *Completed Project Memoria, the most extensive study of TCP/IP stacks that uncovered 97 new vulnerabilities impacting over 400 vendors*
- *Diverse customer case studies and recognized by numerous industry awards*

Managing cyber risk through automation and data-powered insights.

VEDERE LABS

About me

- MSc in Software Engineering **@Unisannio**
- PhD. in Data Privacy & Security **@TU/e**
- 10+ years in cyber security with focus on industrial networks and critical infrastructures
- VP of Research **@Forescout**
  - Vulnerability research
  - Network monitoring and intrusion detection
  - Malware & Threat Analysis
  - Threat Intelligence

VEDERE LABS

ve·dé·re – *verb* (Italian)
meaning: to see, to view, to understand, to examine, to decide

Our Team








interns

4 **PhDs** in cyber security

8 **Languages**
(Russian, Ukrainian, Arabic, Portuguese, Italian, English, Spanish, French)

160+ **CVEs** in 18 months

Broad **skillset**
(penetration testing, threat hunting, intrusion detection, robotics, OT, IoT, IoMT, network security, protocols, ML)

Our Labs

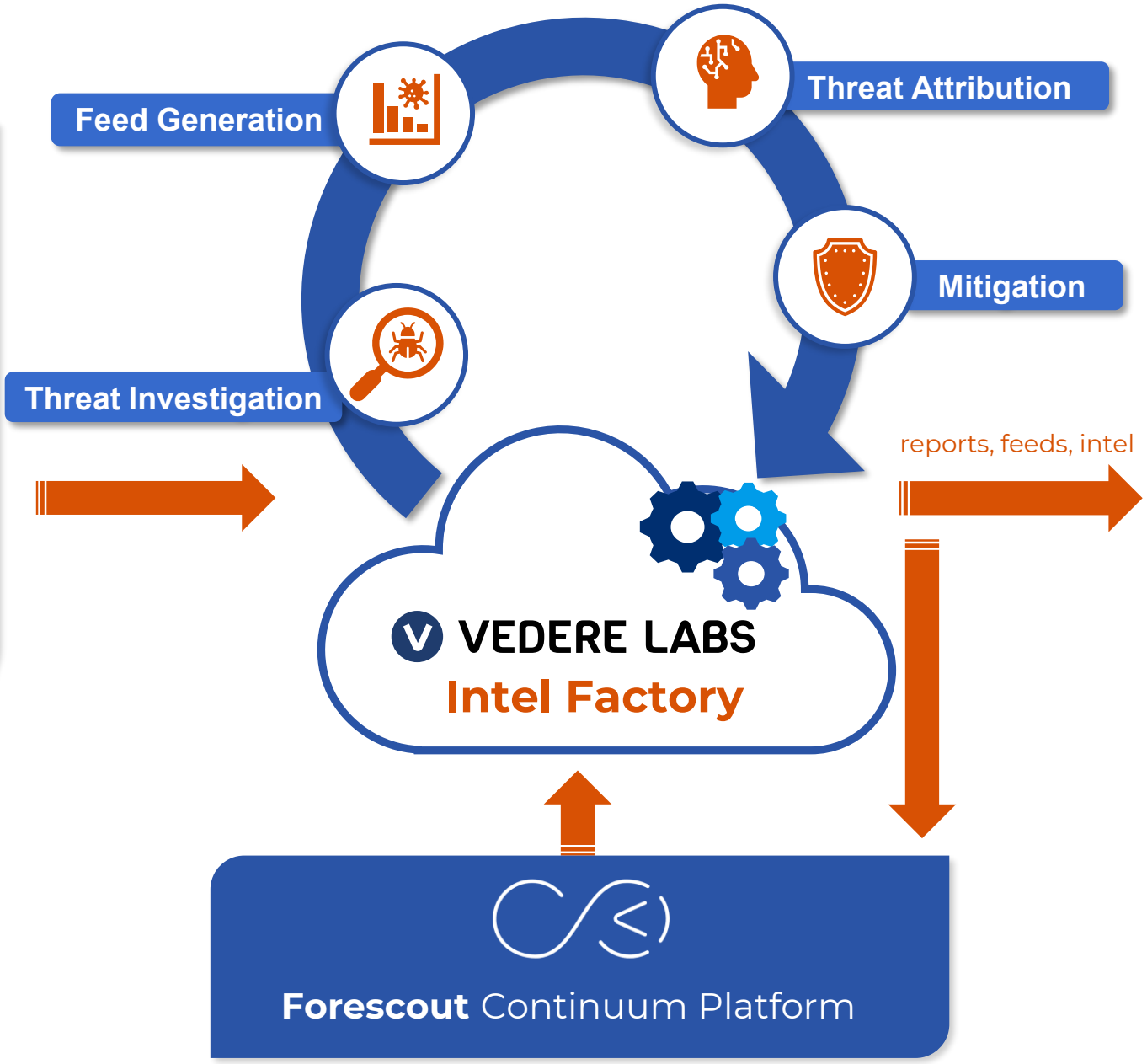

Industrial Control
Systems


Healthcare


Building Automation
Systems

How we work

- Forescout Frontline
- Third Party Threat Feeds
- Third Party Data Sources
- Vedere Labs Sandbox
- Darknet
- Vedere Labs Adversary Engagement Environment



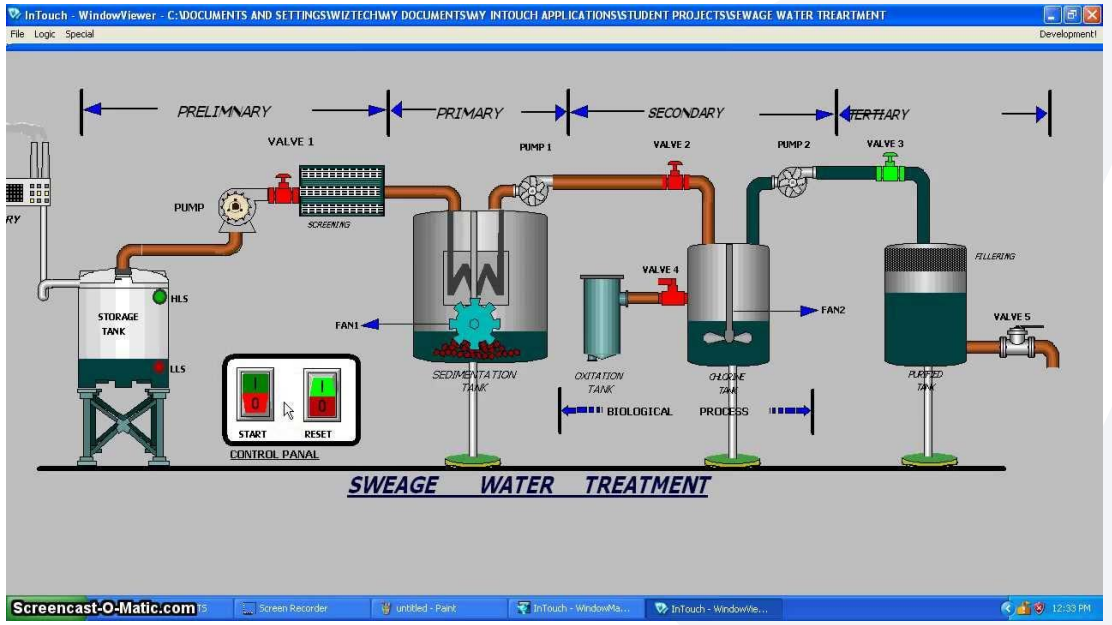
- Threat intel teams
- CERTs
- Cyber Threat Alliances
- ISACs
- Researchers
- Open-Source Platforms

The things we do

Some Definitions

Definitions

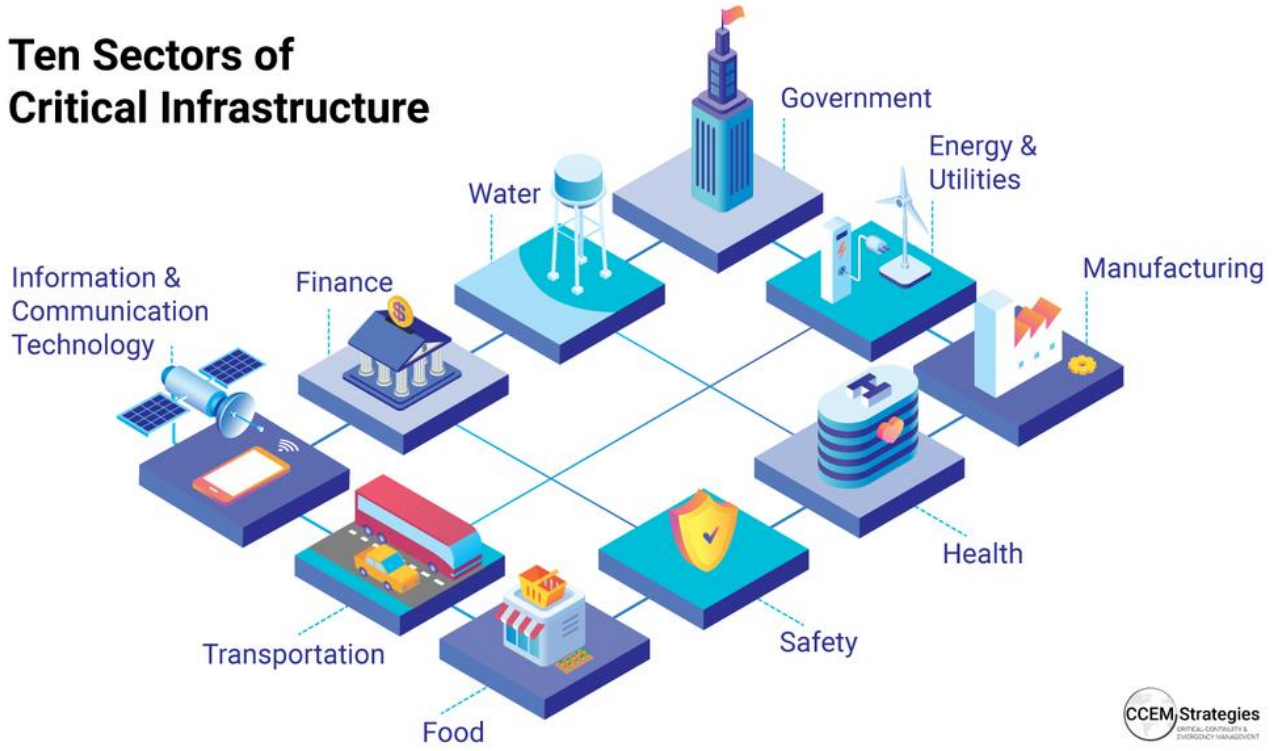
- **Cyber Physical Systems (CPS)**:
  - in cyber-physical systems, physical and software components are deeply intertwined,
  - Examples
    - Industrial Control Systems
    - Building Automation Systems
- **Operational Technology (OT)**:
  - Hardware and software dedicated to detecting or causing changes in physical processes through physical devices such as valves, pumps, etc.
  - Examples:
    - software: ladder logic,
    - hardware: PLC, RTU, SCADA



Definitions

- Critical Infrastructure:
  - Assets that are essential for the functioning of a society and economy

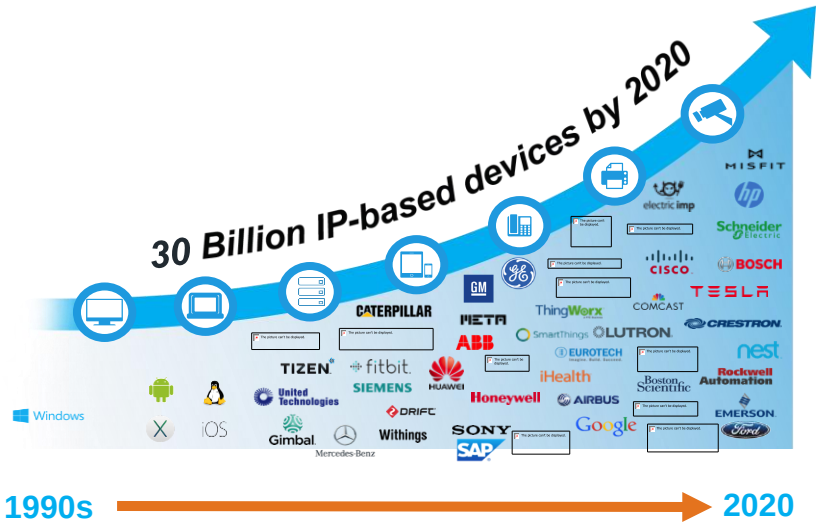
  - Examples:
    - Utilities (e.g., electricity, gas, water)
    - Transportation
    - Telecommunication
    - Hospitals
    - Airports



The Evolution of Threats for CPS

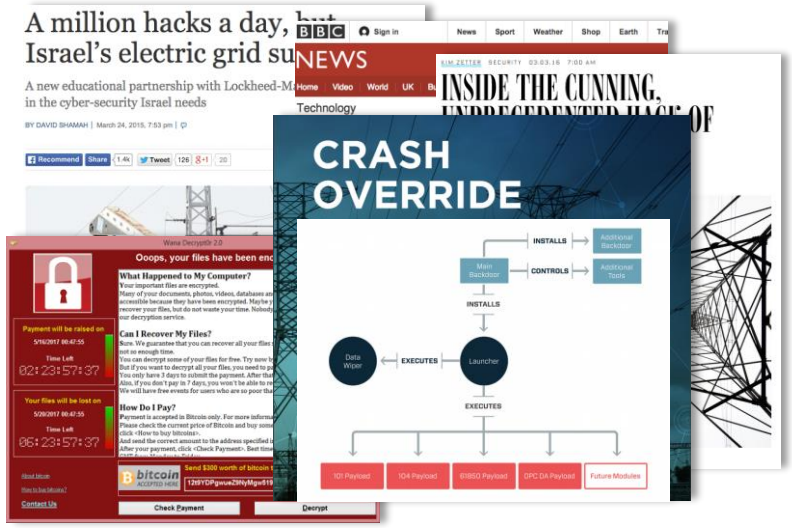
Three Trends That Make Breaches Difficult To Prevent

Growth of Devices & Platform Diversity



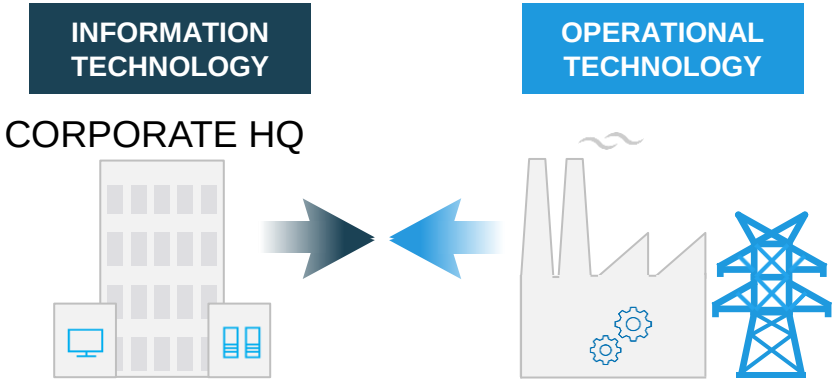
- Innumerable device-specific operating systems (OS)
- Cannot get agents onto new devices
- Cannot write agent-based software for every OS

New Threats



- Better funded actors (e.g., nation states)
- Advanced malware
- Malicious use of OT protocols and features

OT Convergence With IT Heightens Risk

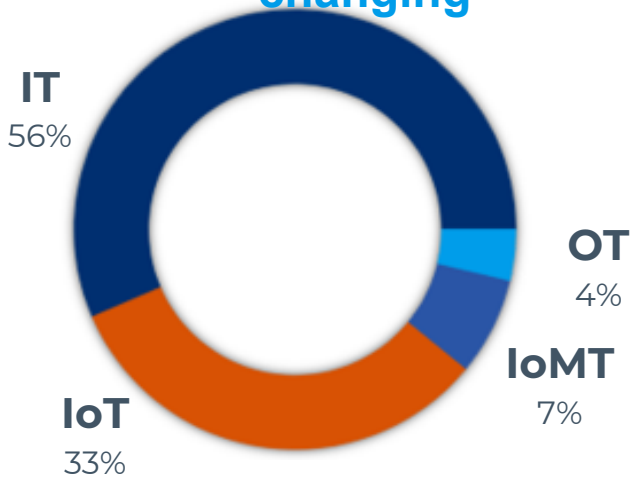


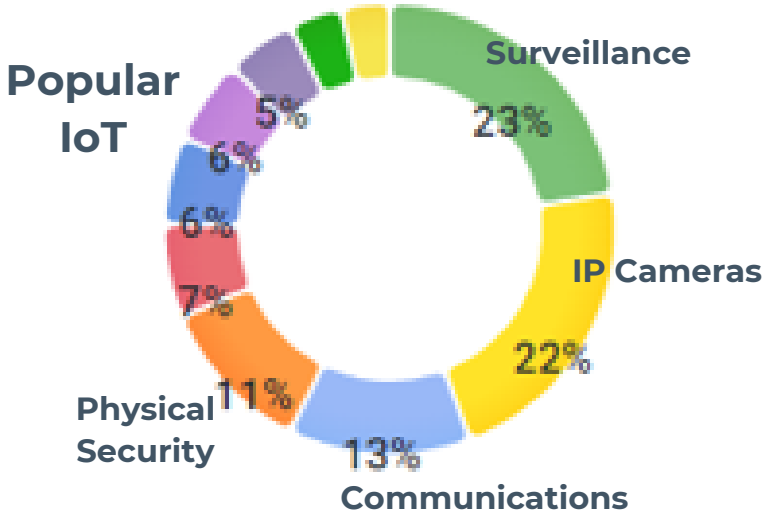
- INDUSTRIAL CONTROL SYSTEMS
- CRITICAL INFRASTRUCTURE

- OT networks are no longer physically separated
- Threats moving between cyber & physical dimensions
- Assets are highly vulnerable & rarely can be patched

Today's Device and Threat Landscape

1. The device landscape is changing





2. 10+ years of ICS attacks have shown some patterns

3. Attackers want money!

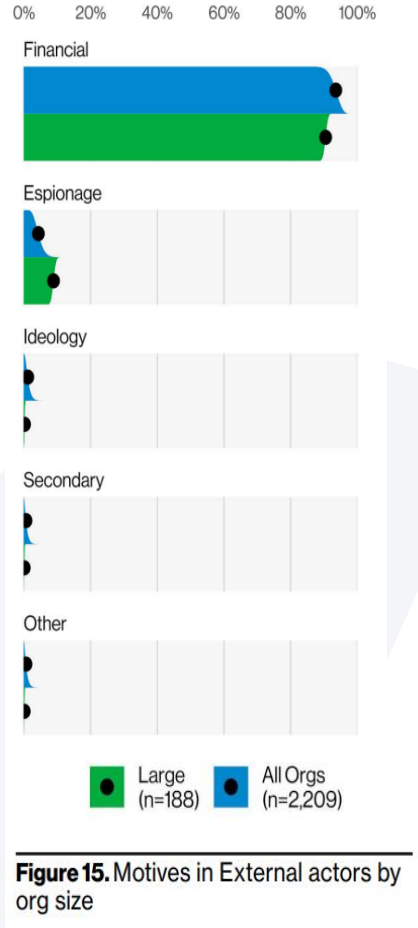
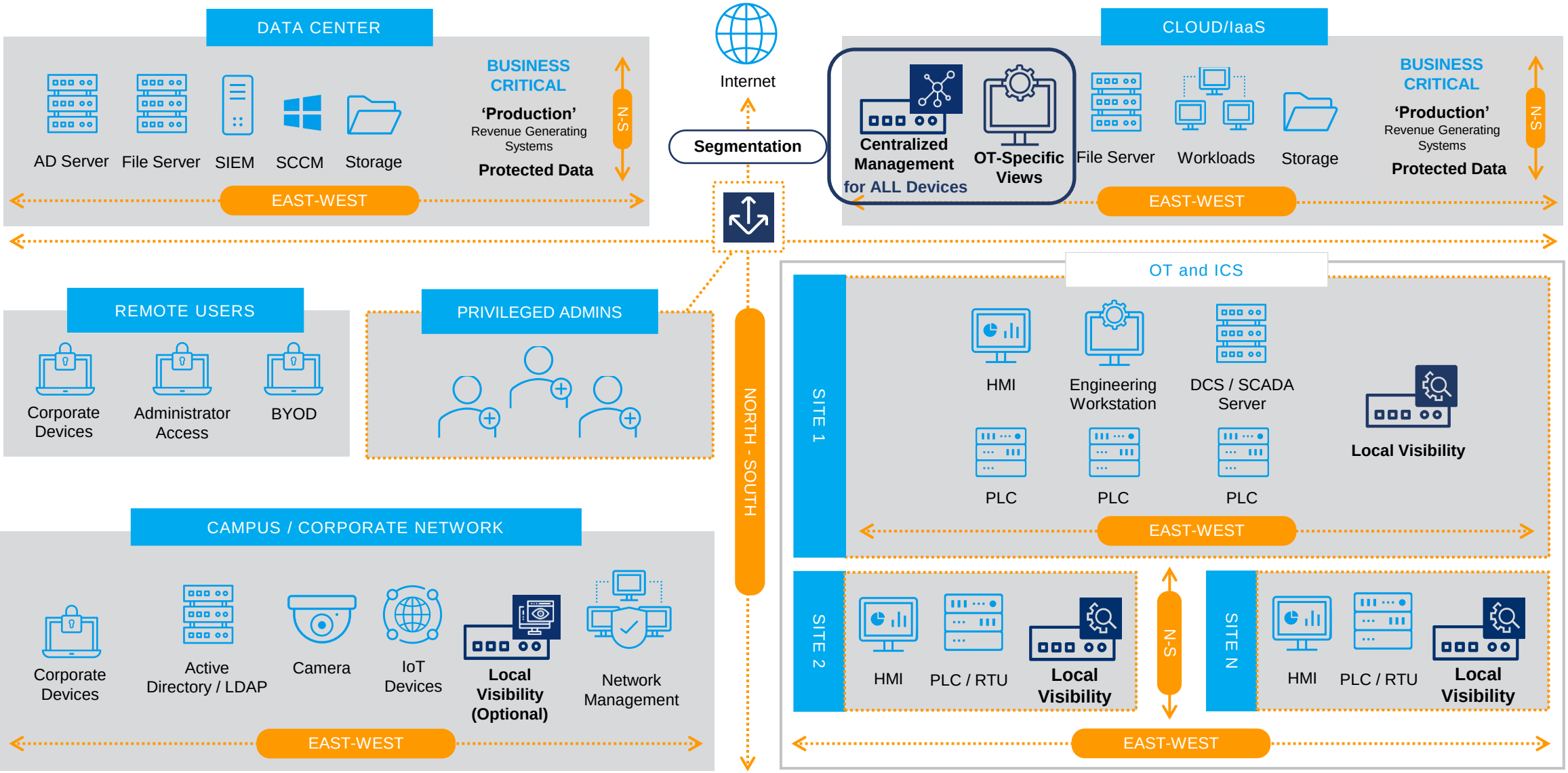


Figure 15. Motives in External actors by org size

https://www.verizon.com/business/resources/reports/dbir/

A Network Example



CPS-Specific Vulnerability Research

Vulnerability trends

01 Supply chain is a major concern

- Well-known supply chain attacks targeting **service providers**, such as SolarWinds, Kaseya VSA, NotPetya/M.E.Doc
- **Log4Shell** is representative of a growing number of vulnerabilities affecting software components used in wide range of devices
- These vulnerabilities are **“endemic” and “long-term”** – Cyber Security Review Board
- Examples: TCP/IP stacks, RTOS, IoT management platforms, applications
- https://forescout.com/research-labs/project-memoria

02 Insecurity by design remains very relevant in OT

- Past decade has shown that the **biggest security problem in OT continues to be the lack of basic controls (“insecure-by-design”)**
- Exploited by threat actors in several malware incidents
- Examples: insecure engineering protocols, broken authentication, insecure firmware updates
- https://forescout.com/research-labs/ot-icefall

Both these classes of vulnerabilities affect many vendors and device models at a time, which means that attackers can target not a single organization but entire industry verticals that rely on popular IoT or OT devices.

Recent Vedere Labs vulnerability research

OT:ICEFALL

- 56 CVEs affecting 10 major OT vendors
- Insecure-by-design issues, such as insecure engineering protocols and firmware updates or remote code execution
- Shows how proprietary nature of these devices complicate risk management
- **Devices affected: PLCs, Building Automation, Safety systems, DCS**

https://www.forescout.com/research-labs/ot-icefall/

Project Memoria

- 97 CVEs on 14 TCP/IP stack implementations
- Shows how a vulnerability in the software supply chain can impact hundreds of IoT/OT/IT products
- **Devices affected: everything from switches to VoIP phones, medical devices, etc**

https://www.forescout.com/research-labs/project-memoria/

PROJECT MEMORIA

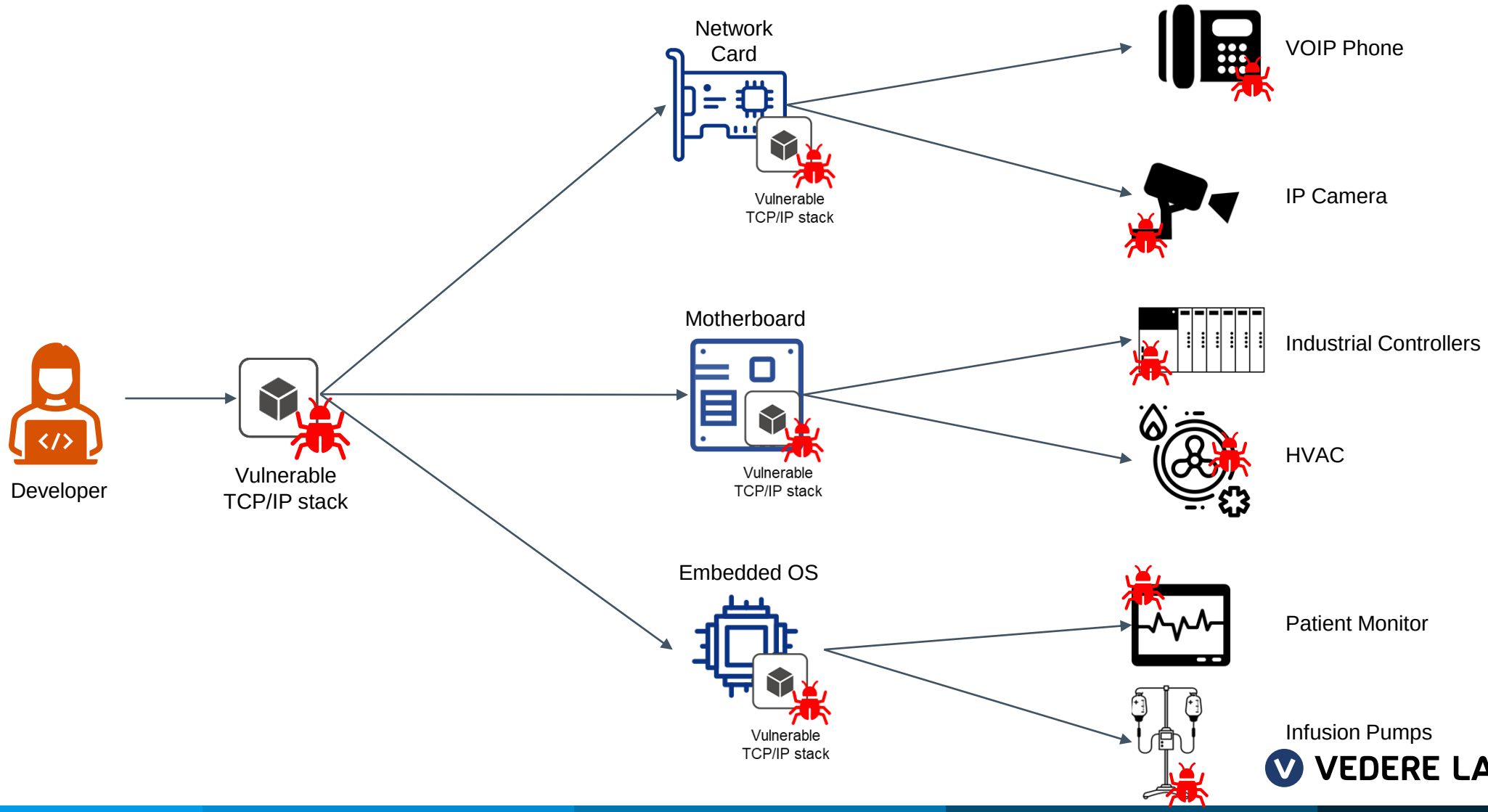
The most comprehensive study on the security of TCP/IP stacks by **Forescout Research Labs**

- **Analyze different TCP/IP stacks, open source and proprietary**
- **Dive into the intrinsic challenges of supply chain vulnerabilities**
- **Understand common mistakes behind the bugs**
- **Partner with universities and industry**
- **Educate the community & suggest mitigation**

Why It Matters

1. TCP/IP stacks **process *every* single network packet reaching a device.**
2. A single network packet can be used to crash a **device.**
3. Identifying vulnerable devices is **extremely challenging.**
4. Fixes might not be available and **large-scale patching might not be feasible**
5. There is **no silver bullet** to solve this, but it is possible to **mitigate the risk**

The Propagation of Supply Chain Vulnerabilities



The Challenges of Supply Chain Vulnerabilities

IoT and OT Devices
are the most vulnerable

400+
vendors affected

Billions+
of devices known to be vulnerable

Government, Healthcare and Manufacturing
are the most affected industries

unknown vulnerable devices

un-patchable devices

long & unknown supply chains

vendor out of business

unknown vulnerable vendors

publicly exposed devices

Project Memoria in Numbers

97
vulnerabilities

14
TCP/IP stacks analyzed

100+
impacted products

81
public advisories

422
impacted vendors

3 billion
vulnerable devices

18
months of research

15
partnerships

170 days
longest response time


VEDERE LABS
OT:ICEFALL

OT:ICEFALL Summary

Goals & Findings

- **Find and quantify** insecure-by-design vulnerabilities
- Discuss impact on OT **certification, risk management, supply chain, and offensive capabilities**
- **Public disclosure on June 21st:** 56 CVEs on 10 vendors

Impact & Mitigation

- Thousands of devices **exposed online**
- Devices often found on **critical infrastructure verticals** such as Oil & Gas, Power Generation & Distribution, Manufacturing, Water Treatment & Distribution, Building Automation
- Often no patches, but focus on **cyber hygiene**

Why Research Insecure-by-Design OT?

Past decade...

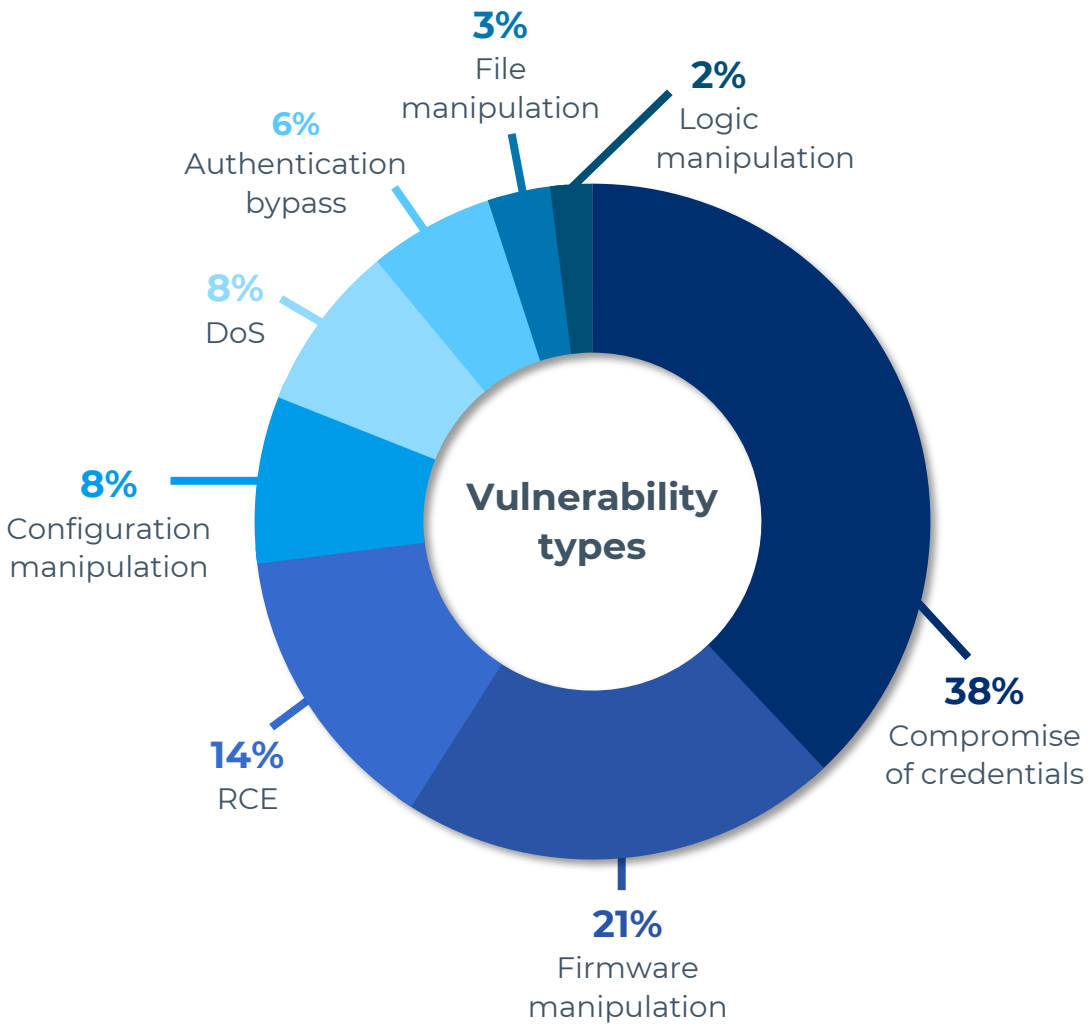
- Project Basecamp highlighted **insecure-by-design** critical OT devices and protocols

- **Real-world OT incidents** abusing insecure-by-design functionality such as:
  - Industroyer, TRITON, INCONTROLLER

Biggest issues facing OT security

- Persistent lack of **basic security controls**
- Opaque and proprietary nature of these systems

Vulnerabilities



Impact of vulnerabilities

- Set of 56 CVEs demonstrating insecure-by-design practices in OT

4 main categories of vulnerabilities:

- Insecure engineering protocols
- Weak cryptography or broken authentication
- Insecure firmware updates
- Remote code execution

Affecting 10 vendors:

OMRON, Bently Nevada, EMERSON, Honeywell, JTEKT 株式会社ジェイテクト, SIEMENS, PHOENIX CONTACT, motorola, YOKOGAWA

Vulnerable Products are Often Certified

74%

of the product families affected by the found vulnerabilities have some form of security certification

Factors contributing to this problem include:

- (Re)certification effort
- Limited targets for evaluations
- Opaque security definitions
- Focus on functional testing

Certifications among affected product families

Risk Management is Complicated by Lack of CVEs

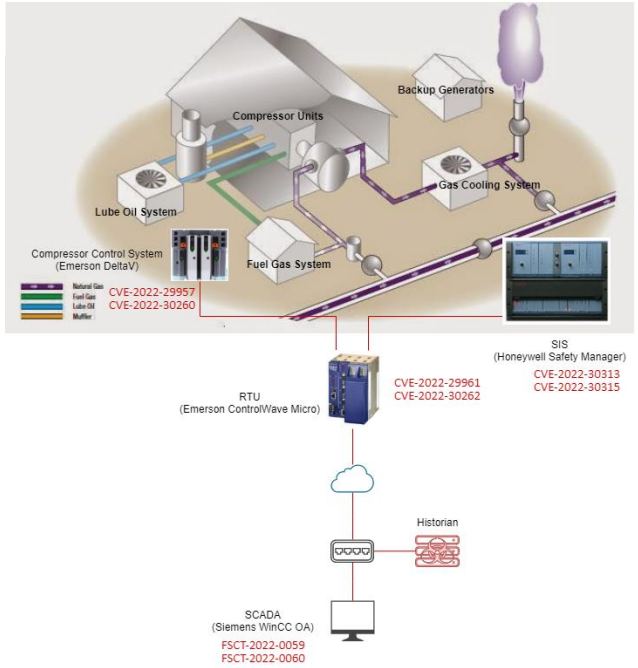
It is not enough to know that a device or protocol is insecure.

To make informed risk management decisions around segmentation, monitoring and hardening efforts, asset owners need to know *in what way* these components are insecure.

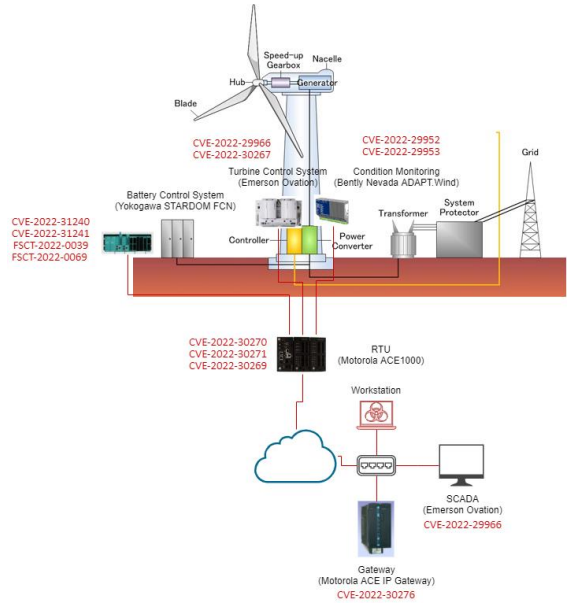
Issues considered the result of insecurity by design have not always been assigned CVEs, so they often remain less visible and actionable than they ought to be.

Attack Scenarios

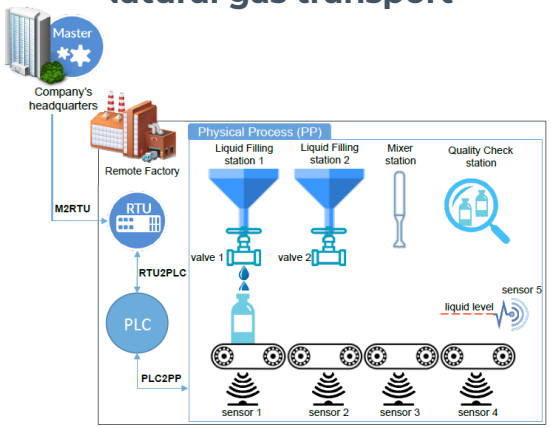
- **Manipulation of control / view**
  - Bypass authentication
  - Manipulate setpoints
  - Overwhelm operators with false alarms
  - Manipulate system configuration, operational settings and controller firmware
- **Denial of control / view**
  - Bypass authentication
  - Abuse unauthenticated communications
  - Issue commands
  - Deny operators ability to control and monitor
- **Loss of safety**
  - Gain code execution
  - Disable condition monitoring systems
  - Disable safety systems
- **Loss of productivity and revenue**
  - Degrade performance
  - Denial of service on PLCs



Natural gas transport



Wind power generation



Manufacturing

More details on our technical report

https://www.forescout.com/research-labs/ot-icefall/

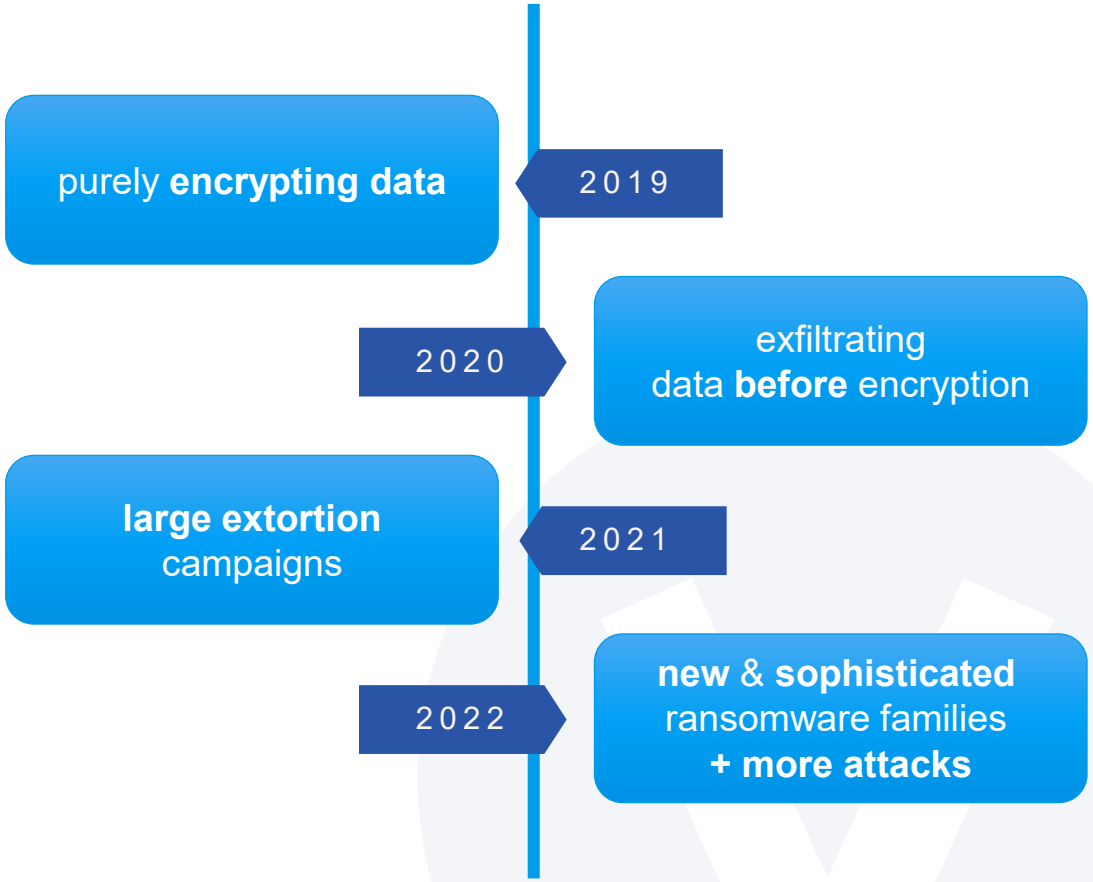
R4IoT – Ransomware for IoT

Introduction

RANSOMWARE

BIGGEST CYBERSECURITY THREAT OF 2021

- Ransomware has evolved **from data encryption to multi-faceted extortion attacks**
- The evolution of the ransomware threat landscape is far from over
- Ransomware can evolve in the coming years because:
  1. Proliferation of IoT devices
  2. Convergence of IT and OT networks



Overview

R4IoT

The first of its kind

Ransomware for IoT

proof of concept for next-generation ransomware

EXPLOITS IoT → **ENCRYPTS IT** → **DISRUPTS OT**

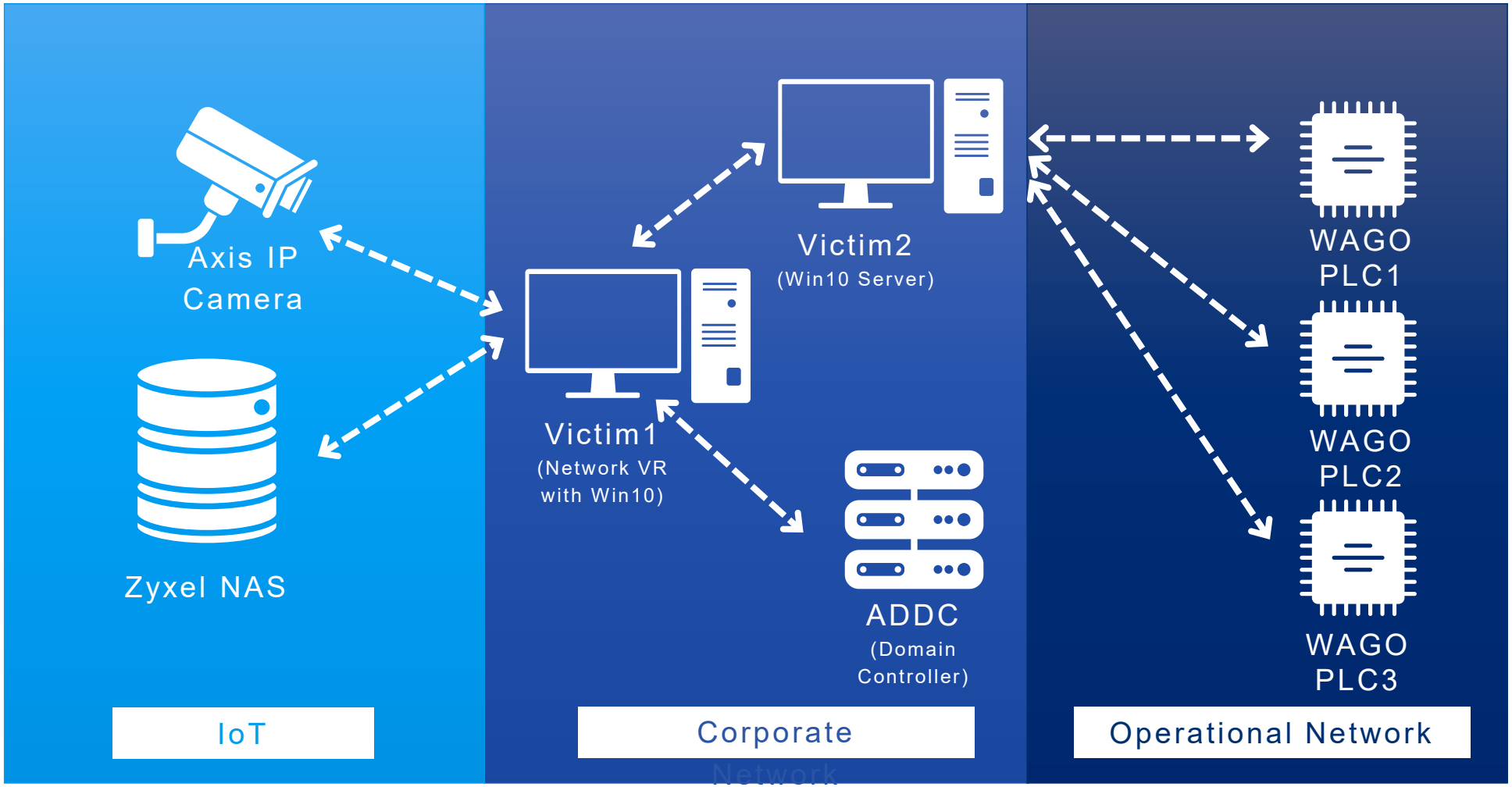
Why R4IoT, Why Now?

R4IoT novelty resides in the following *key contributions*:

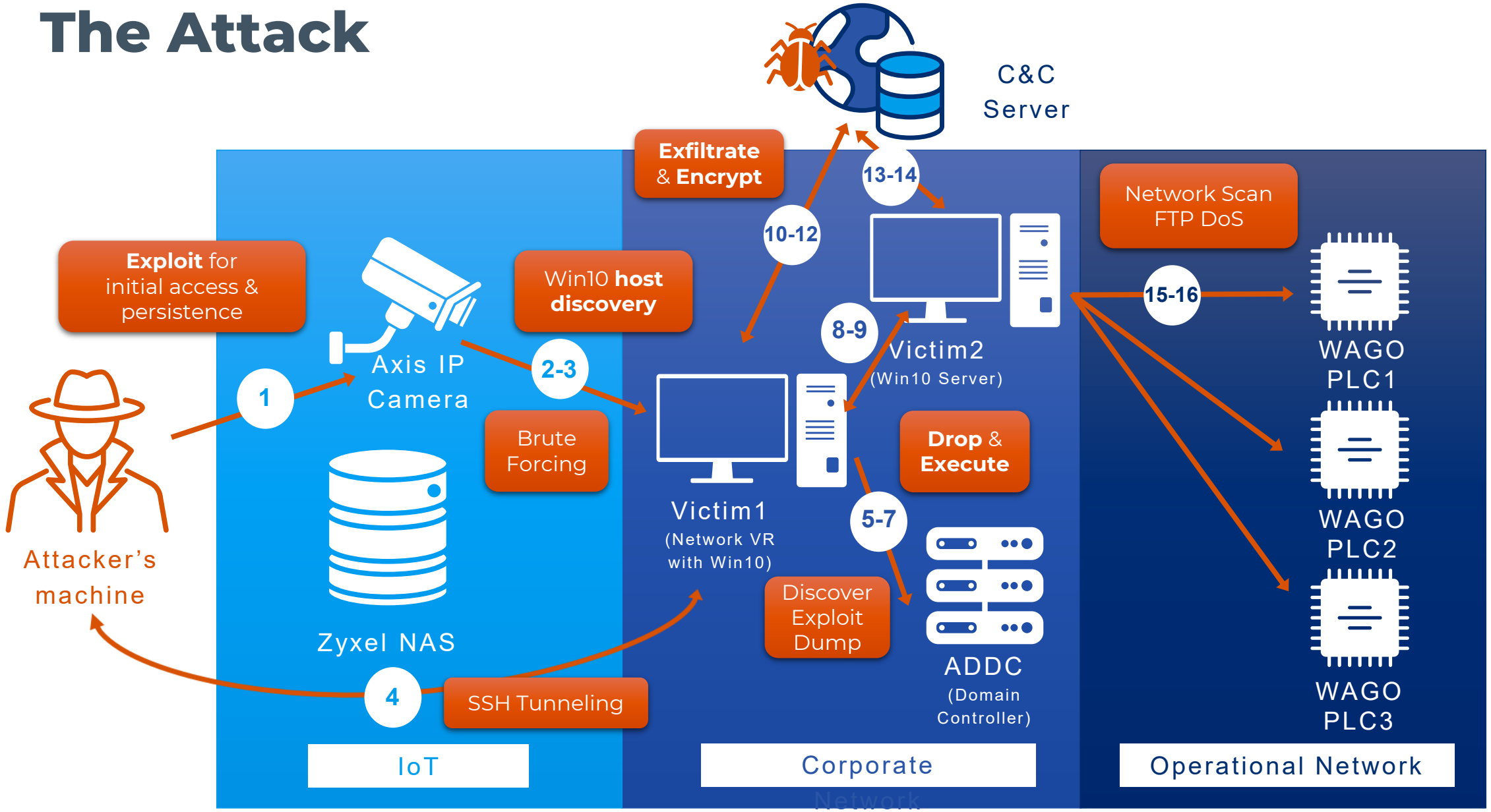
- This is the **first and only work to combine the worlds of IT, OT and IoT ransomware and to have a full proof-of-concept from initial access via IoT to lateral movement in the IT network and then impact in the OT network**.
  - Beyond just encryption, our proof of concept on IT equipment includes deployment of a crypto miner and data exfiltration (also known as **double extorsion)**.
- The impact we demonstrate on OT **is general purpose**:
  - It is not limited to standard operating systems (e.g., Linux) or device types
  - **Does not require** persistence or firmware modification on the targeted devices
  - W**orks at large-scale on a wide variety of devices impacted by TCP/IP stack vulnerabilities**.

We implemented detection & response actions for the attack that serve as a playbook for organizations looking to defend against both current and future threats.

The Victim Network



The Attack


C&C Server
Exfiltrate & Encrypt
13-14
10-12
Network Scan FTP DoS
Exploit for initial access & persistence
Win10 host discovery
15-16
8-9
Victim2 (Win10 Server)
Axis IP Camera
2-3
1
Brute Forcing
Drop & Execute
Victim1 (Network VR with Win10)
5-7
Attacker's machine
Discover Exploit Dump
ADDC (Domain Controller)
WAGO PLC1
WAGO PLC2
WAGO PLC3
Zyxel NAS
4
SSH Tunneling
IoT
Corporate Network
Operational Network

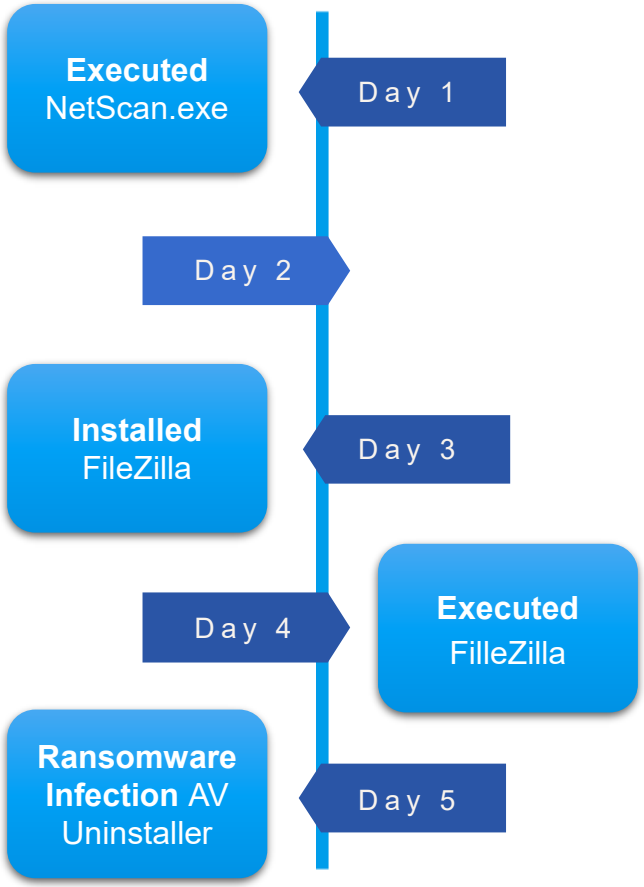
R4IoT Video

short version

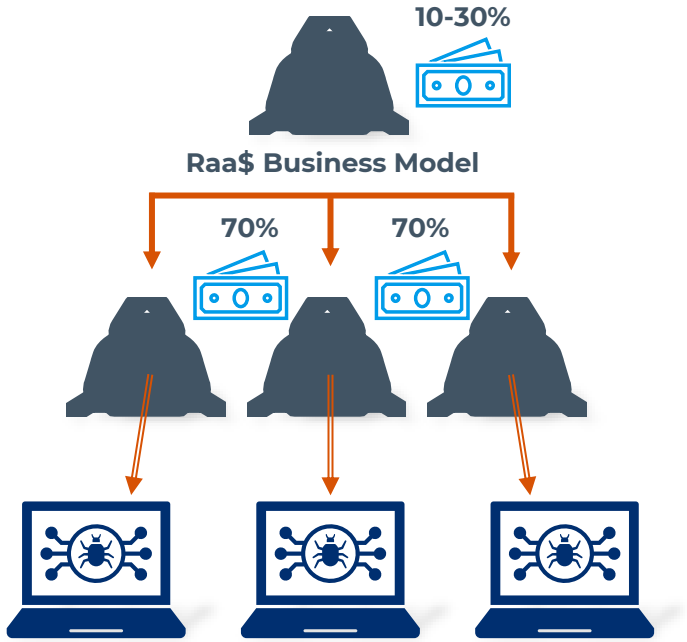
Defending from Attacks

How Mitigation is Possible: Three Important Observations

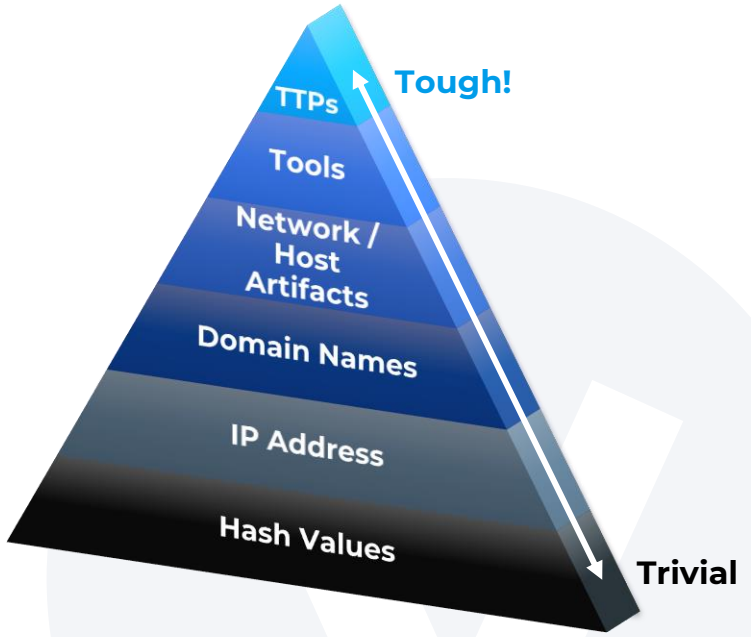
1. Attacks are *not* immediate and fully automated



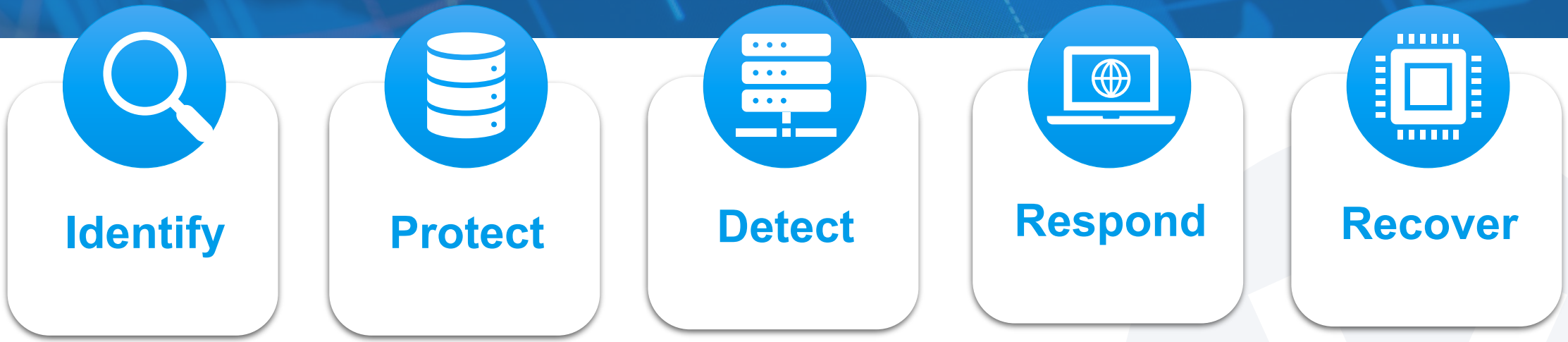
2. Cybercrime-as-a-service means that there are up to *hundreds* of very similar attacks happening



3. Most tools and techniques they use are well-known



NIST Cybersecurity Framework Functions:



- Implementing this mitigation strategy requires complete visibility and enhanced control of all assets in a network.

Implementing Policies with a Zero Trust Architecture

3 Key Pillars to Implement Zero Trust

1. Visibility

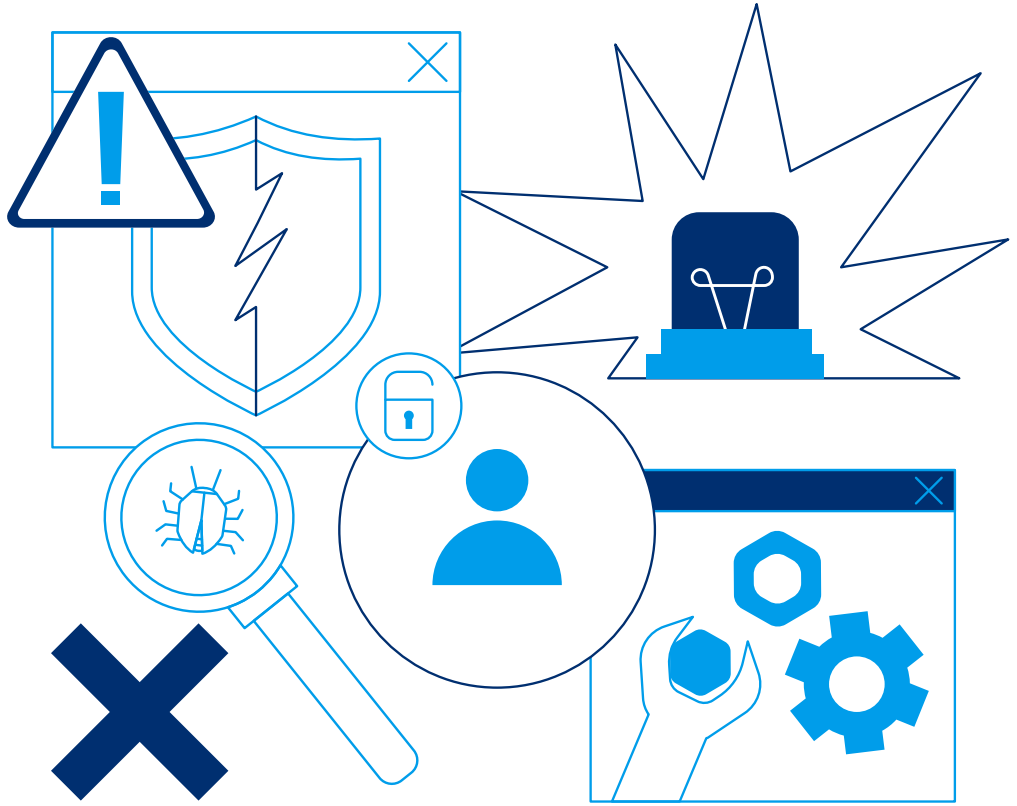
"You can't combat a threat you can't see or understand." Visibility must extend beyond devices to network communications where controls may detect anomalous behavior.

2. Compliance

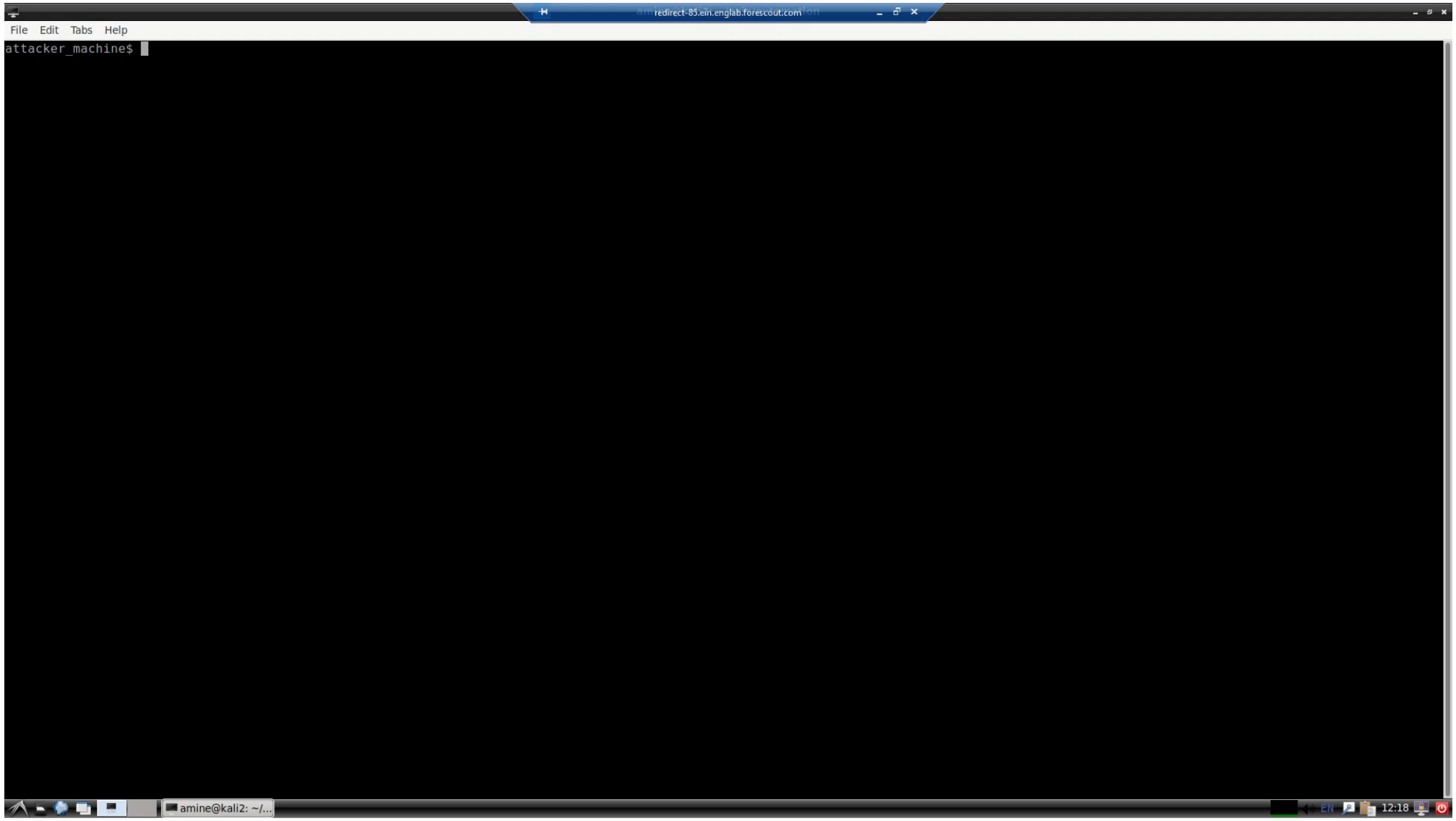
Establishes what should or should not be trusted in the network, making it possible to act on devices that do not meet compliance requirements.

3. Segmentation

Allows to enforce Zero Trust by limiting the allowed network communications of devices.



Example: Defending against R4IoT



References

- Project Memoria - https://www.forescout.com/research-labs/project-memoria/
- OT:ICEFALL - https://www.forescout.com/research-labs/ot-icefall/
- R4IoT - https://www.forescout.com/research-labs/r4iot/
- https://dashboard.vederelabs.com/
- https://www.forescout.com/threat-briefings/

Thank you.