
13TH ANNUAL LEADERSHIP EVENT
CYBER SECURITY SUMMIT
cybersecuritysummit.org
RESILIENCE UNLOCKED
TITLE SPONSOR
Island
#cybersecuritysummit #css13

FORESCOUT

TODAY'S THREAT LANDSCAPE REQUIRES A UNIQUE CAPABILITY

Shawn Taylor
Regional Technology Officer

Twitter: @smtaylor12

Including research and findings from

VEDERE LABS

AGENDA

01 Threat Landscape

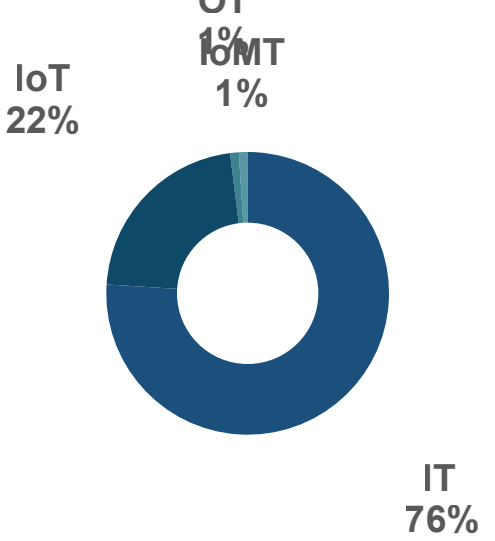
02 Impacts

03 What can be done?

04 Required Capabilities

Threat Landscape

The device landscape has changed



01 More than 24% of devices are not traditional IT

- Data from **18+ million devices** on customer networks
- 8000+ unique **device vendors**, 2000+ unique **OS flavors**

02 Not all devices are equally risky

- **IT: network infrastructure** (e.g., routers and firewalls), one of the main initial access points for ransomware and other actors
- **IoT: surveillance** (e.g., IP cameras and NVR) and **VoIP**, lots of easily exploitable vulnerabilities and Internet exposure
- **OT: PLCs, DCS** and building automation (e.g., HVAC and access control), critical impact and (increasingly) often Internet connectivity

This major attack surface is being targeted by threat actors in many industries

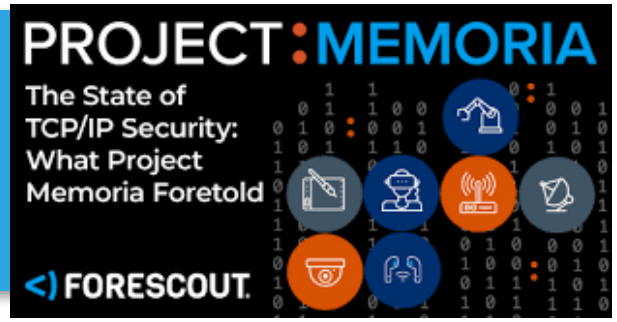
- Example: Chinese state-sponsored actor exploiting vulnerable web servers in IP cameras for initial access into Indian power grid operators

The risks are becoming more widespread and complex

VEDERE LABS

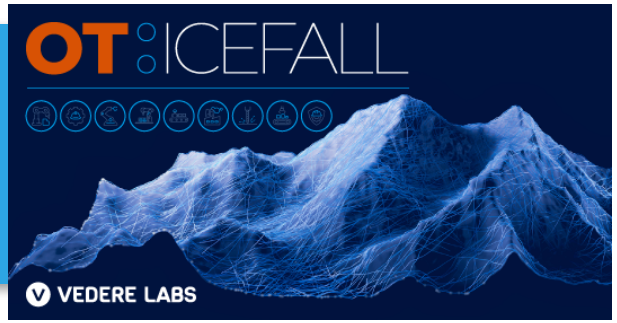
01 Supply chain is a major concern

- **Log4Shell** represents a growing number of **“endemic” and “long-term”** vulnerabilities affecting software components used in wide range of devices
- Examples relevant for OT: TCP/IP stacks, RTOS, web servers



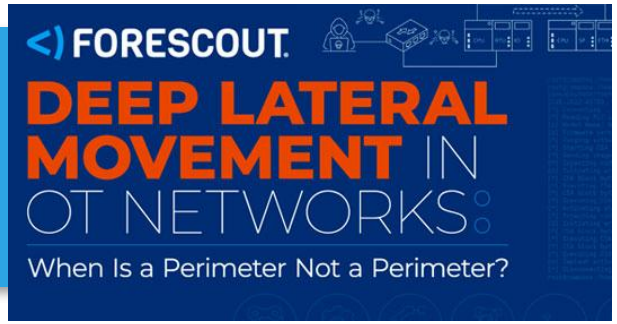
02 Insecurity by design remains very relevant in OT

- 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



03 These vulnerabilities can be chained in complex attacks

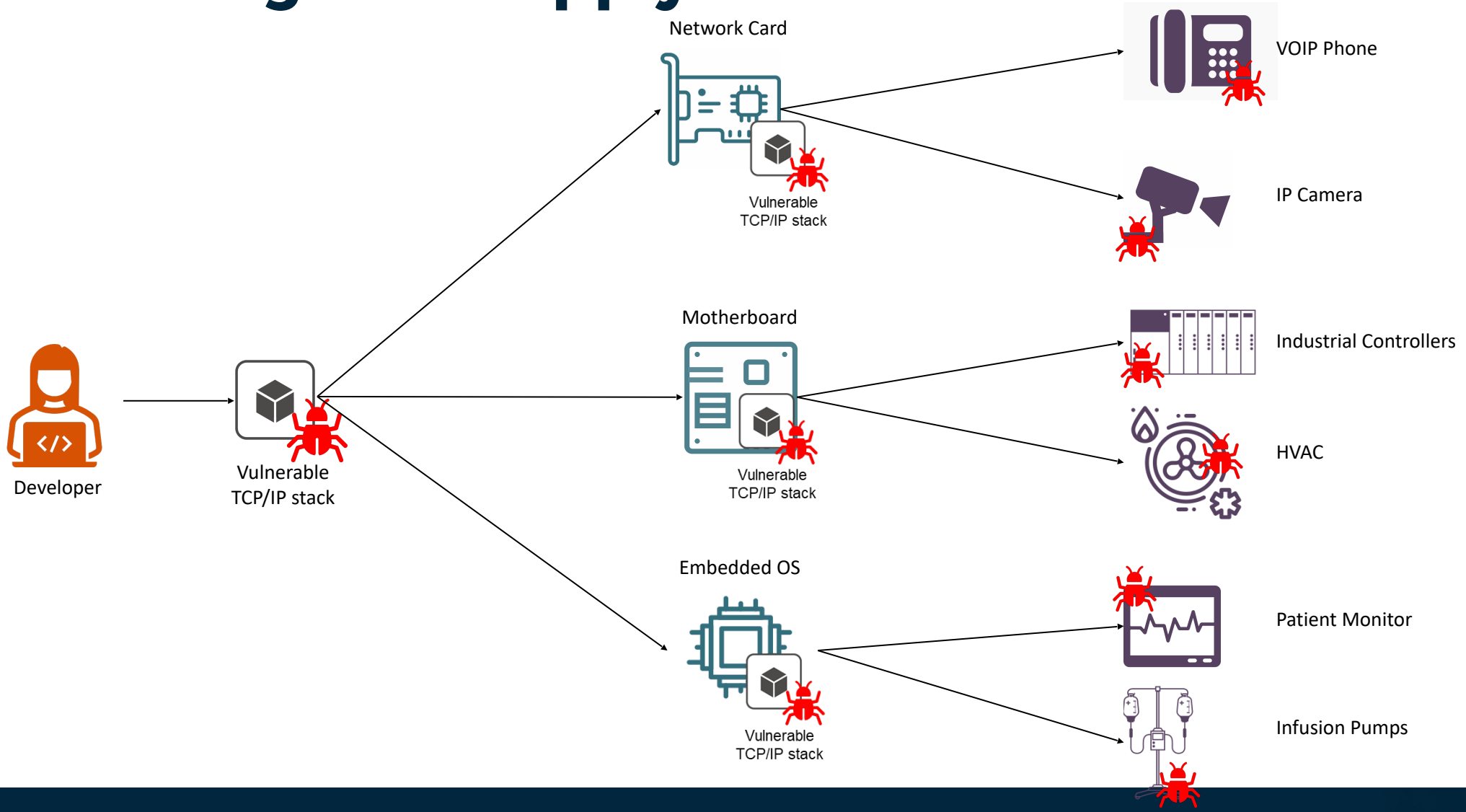
- OT attacks are becoming more commonplace and sophisticated actors can do increasingly more damage



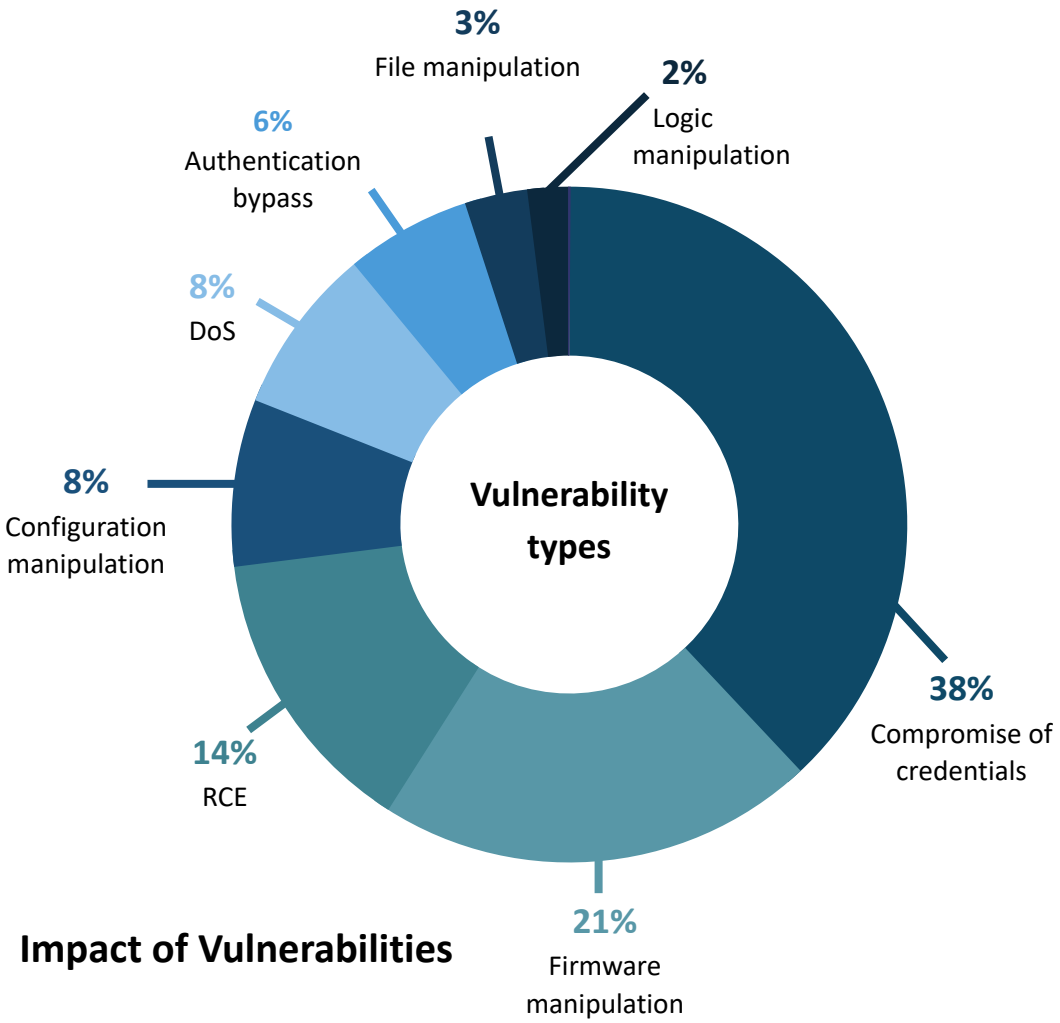
Project Memoria: Why It Matters

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 take a long time to 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 Challenges of Supply Chain Vulnerabilities



Vulnerabilities



Impact of Vulnerabilities

Set of 59 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 12 vendors:

OMRON, Bently Nevada a Baker Hughes business, EMERSON, Honeywell, JTEKT 株式会社ジェイテクト, SIEMENS, PHOENIX CONTACT, motorola, FESTO, YOKOGAWA, CODESYS, Schneider Electric

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.

Insecure-by-Design Supply Chain Components

Vulnerabilities in OT supply chain components tend to not be reported by every affected manufacturer

- Not immediately clear what runtime a particular PLC uses
  - Lack of **Software Bill of Materials (SBOM)** and the complexity of product supply chains

Vulnerabilities on an important supply chain component of OT devices:

ProConOs runtime / protocols

Phoenix Contact	CVE-2014-9195	CVE-2019-9201
Other vendors	▶ Unlikely aware of security issues	

Impacts

It’s about dollars and cents…

RANSOMWARE

R4IoT, an Overview

R4IoT

The first of its kind

Ransomware for IoT

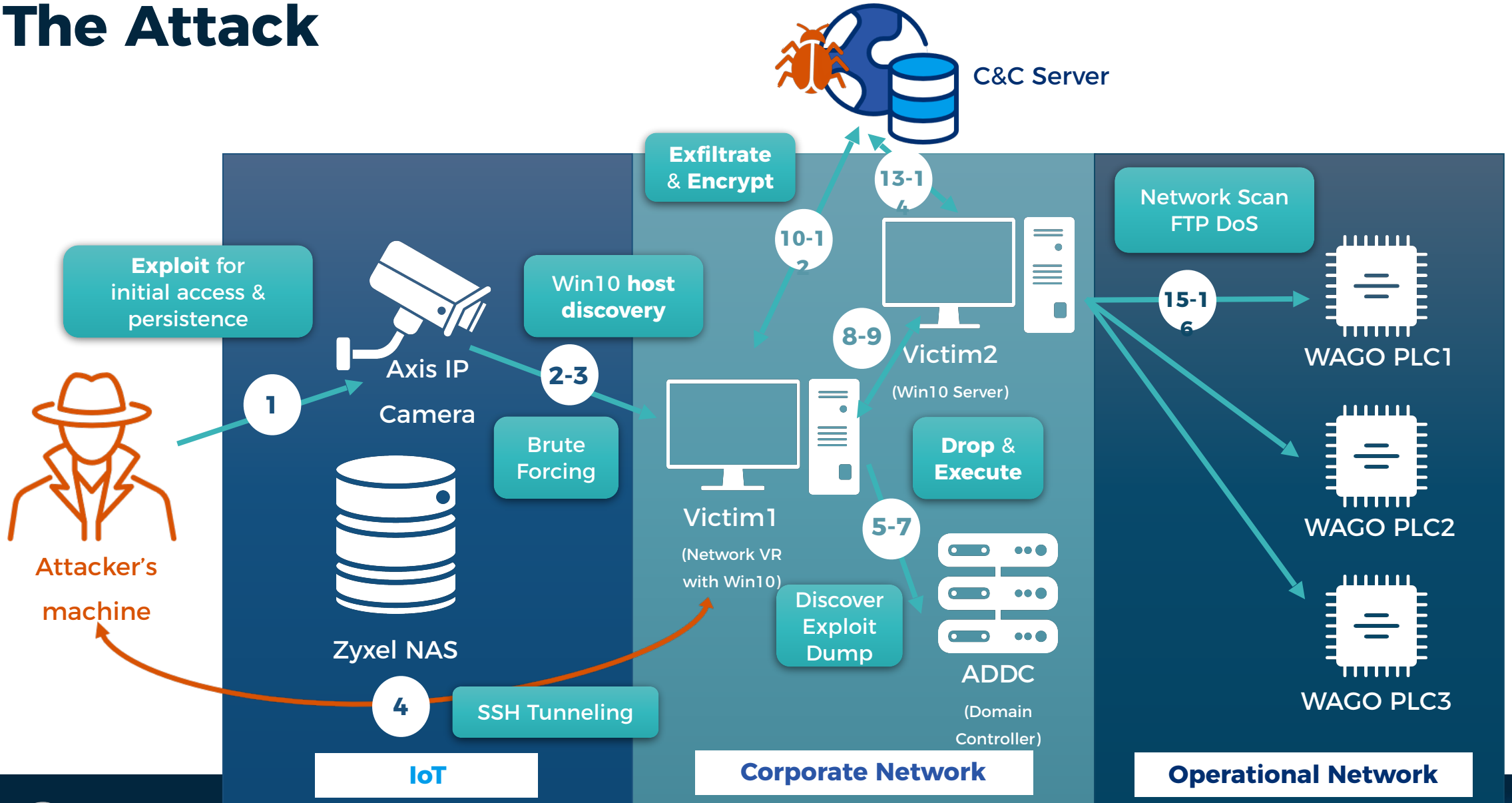
proof of concept for next-generation ransomware

EXPLOITS IoT

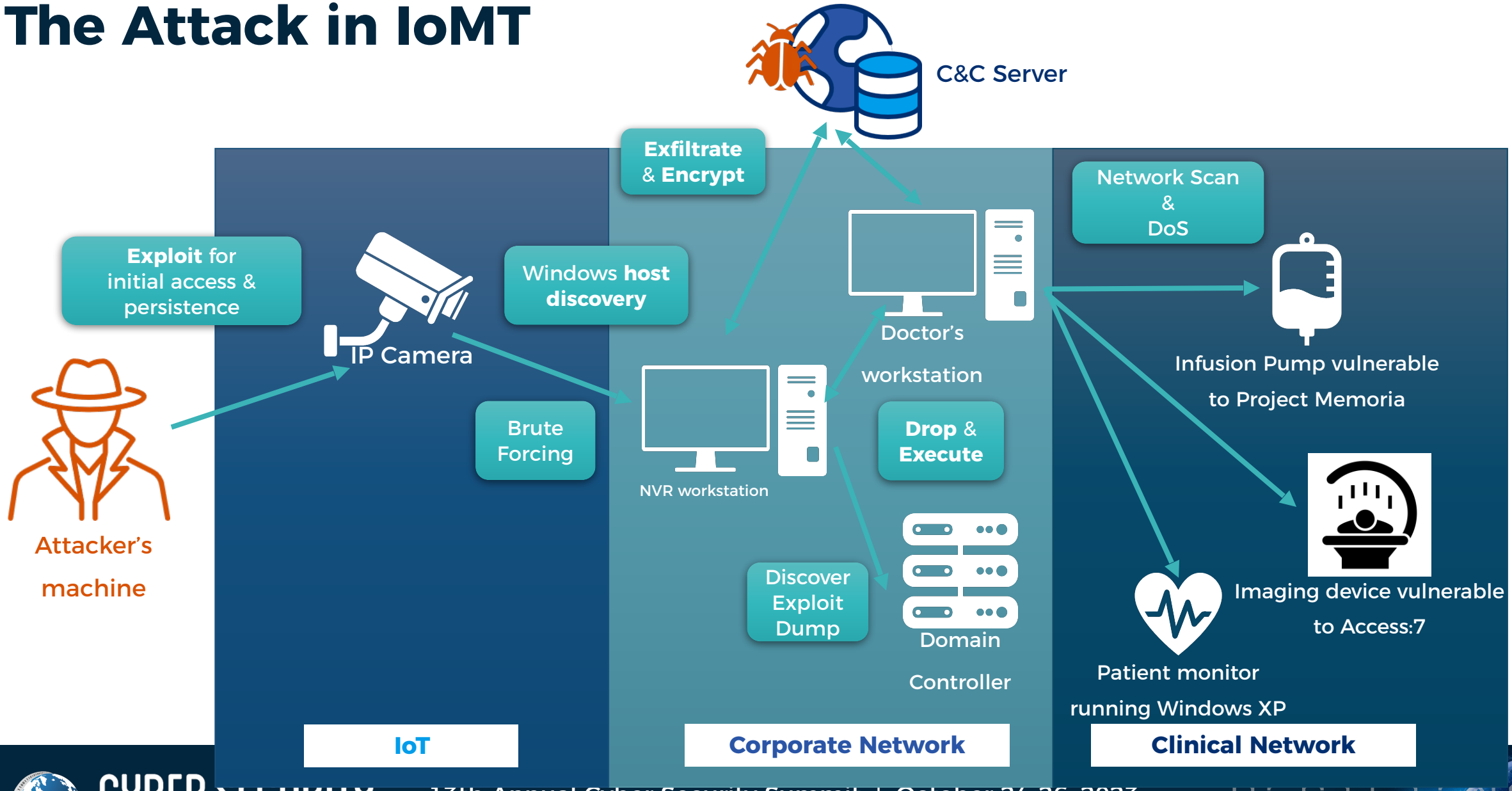
ENCRYPTS IT

DISRUPTS OT

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)
WAGO PLC1
Axis IP Camera
1
2-3
Brute Forcing
Drop & Execute
WAGO PLC2
Victim1
(Network VR with Win10)
5-7
Discover Exploit Dump
ADDC
(Domain Controller)
WAGO PLC3
Attacker's machine
Zyxel NAS
4
SSH Tunneling
IoT
Corporate Network
Operational Network

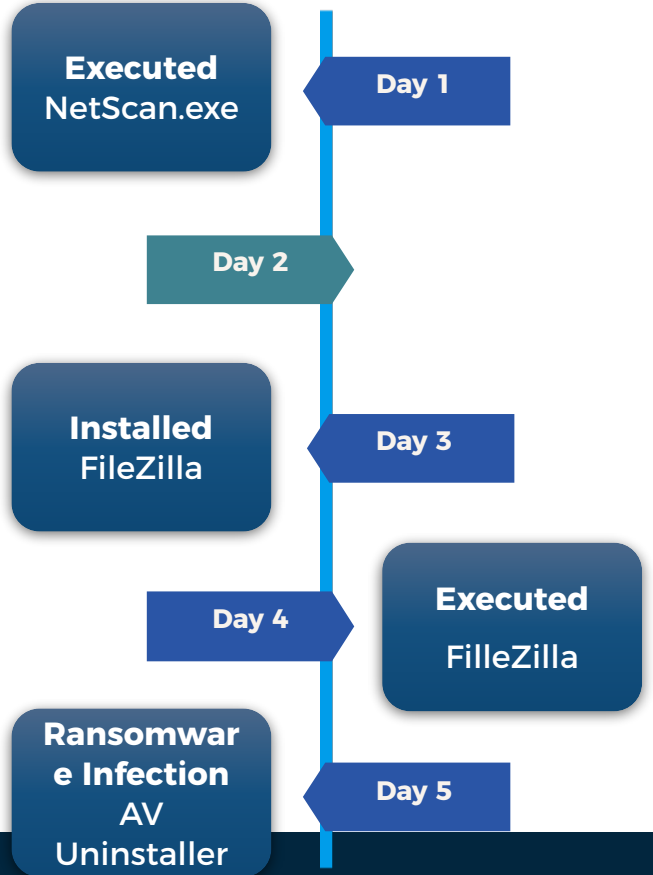
The Attack in IoMT



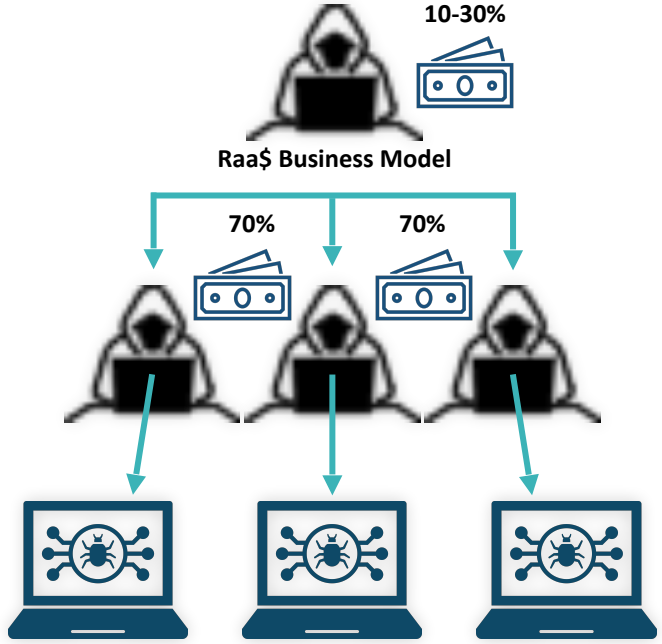

So...what can be done?

How Mitigation is Possible: Three Important Observations

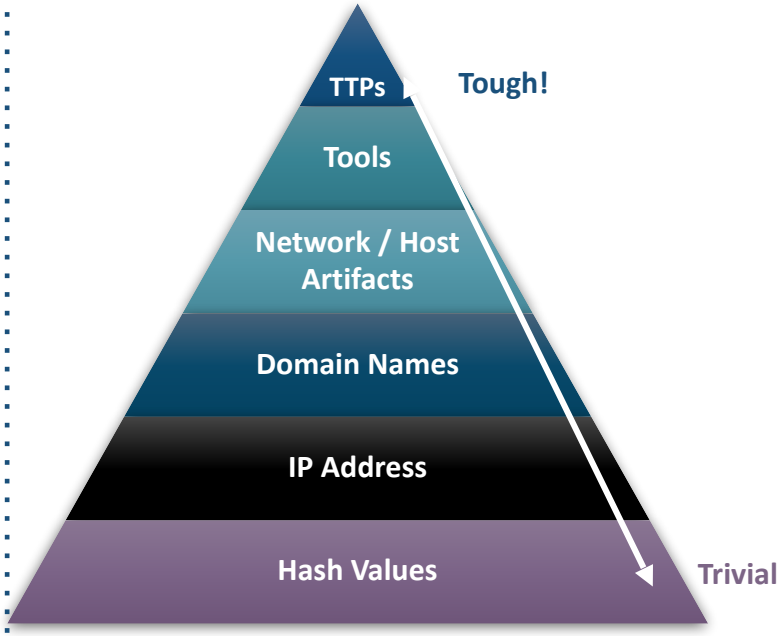
1. Attacks are not immediate and fully automated



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

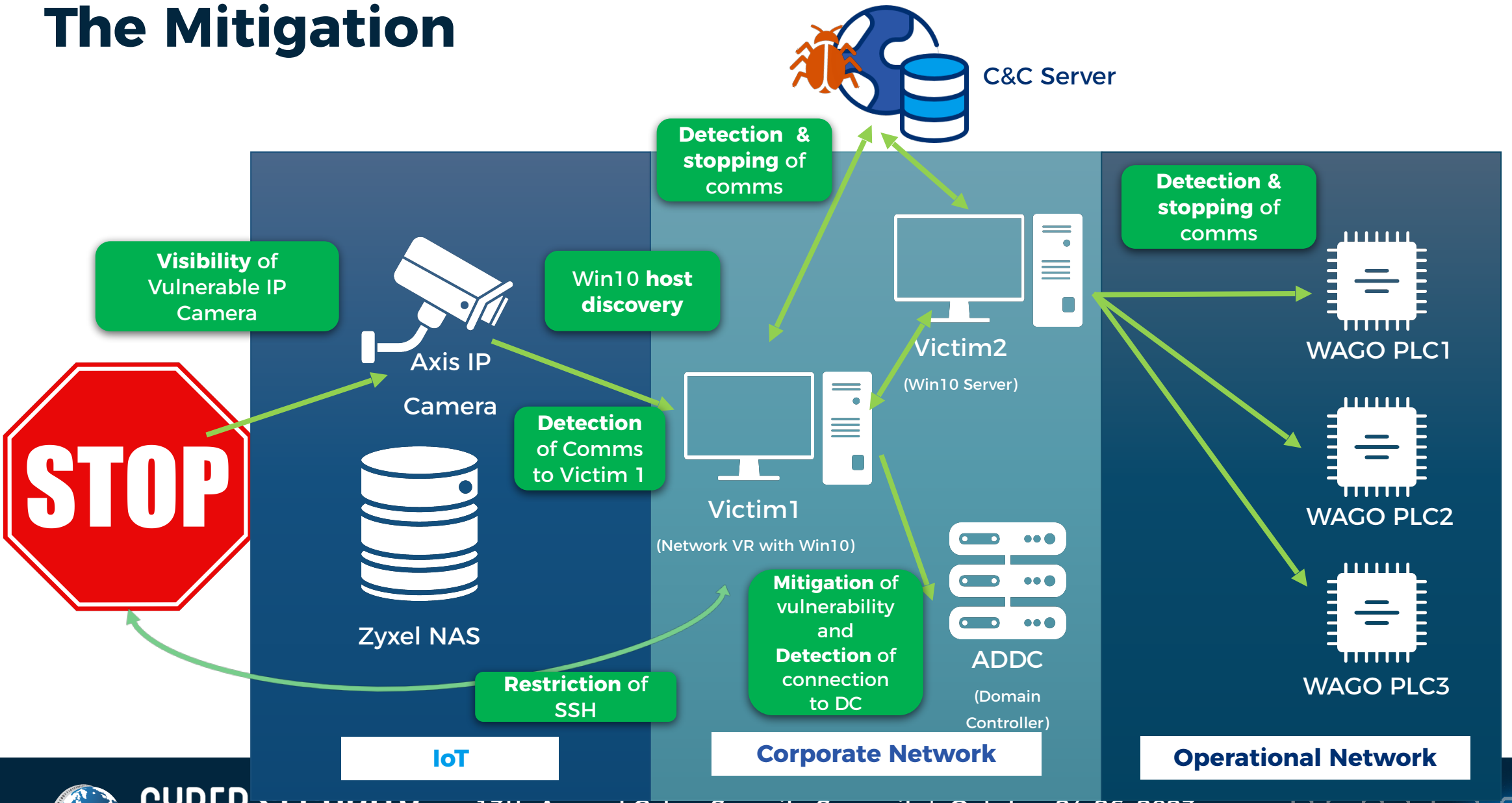


3. Most tools and techniques they use are well-known

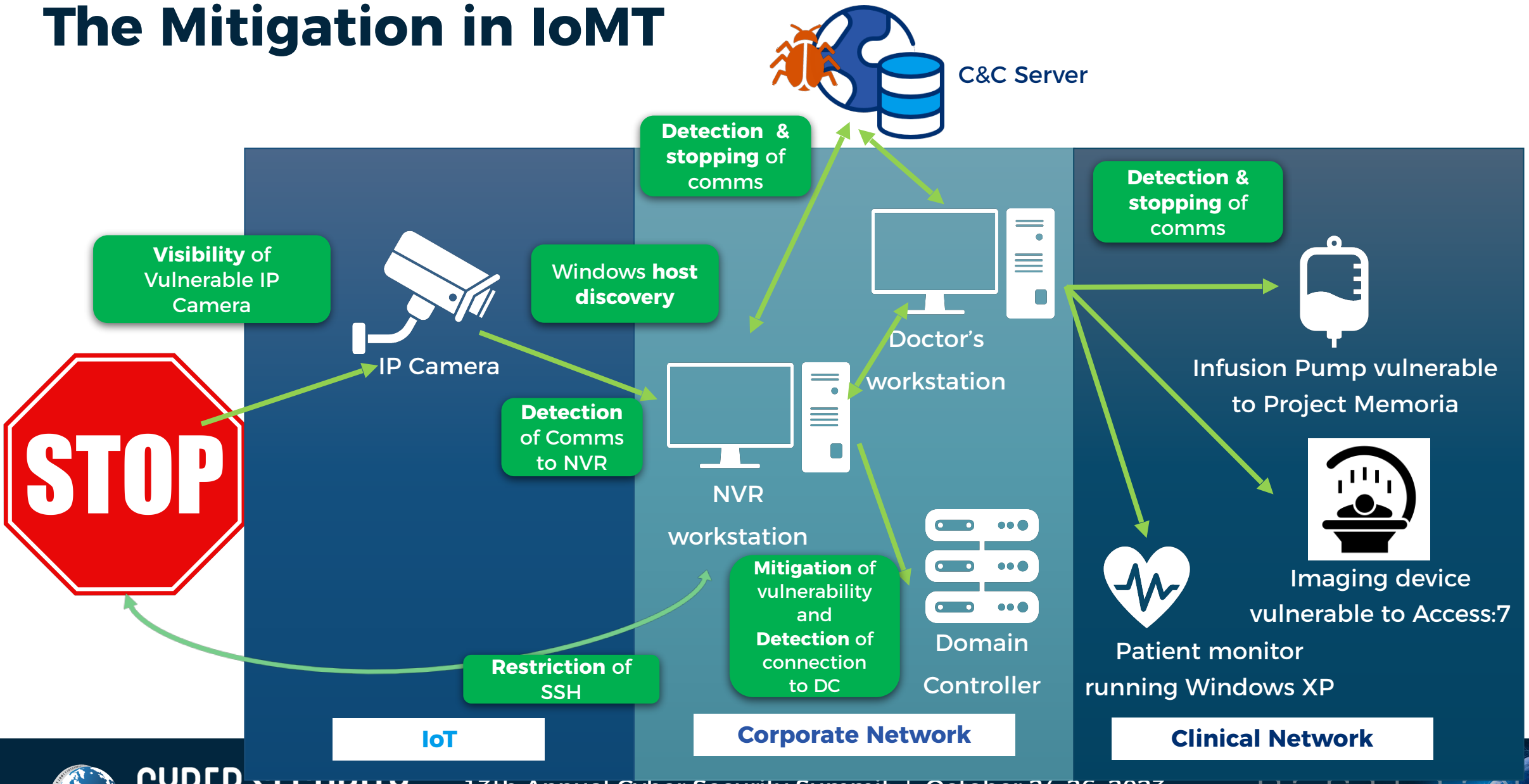


FORESCOUT

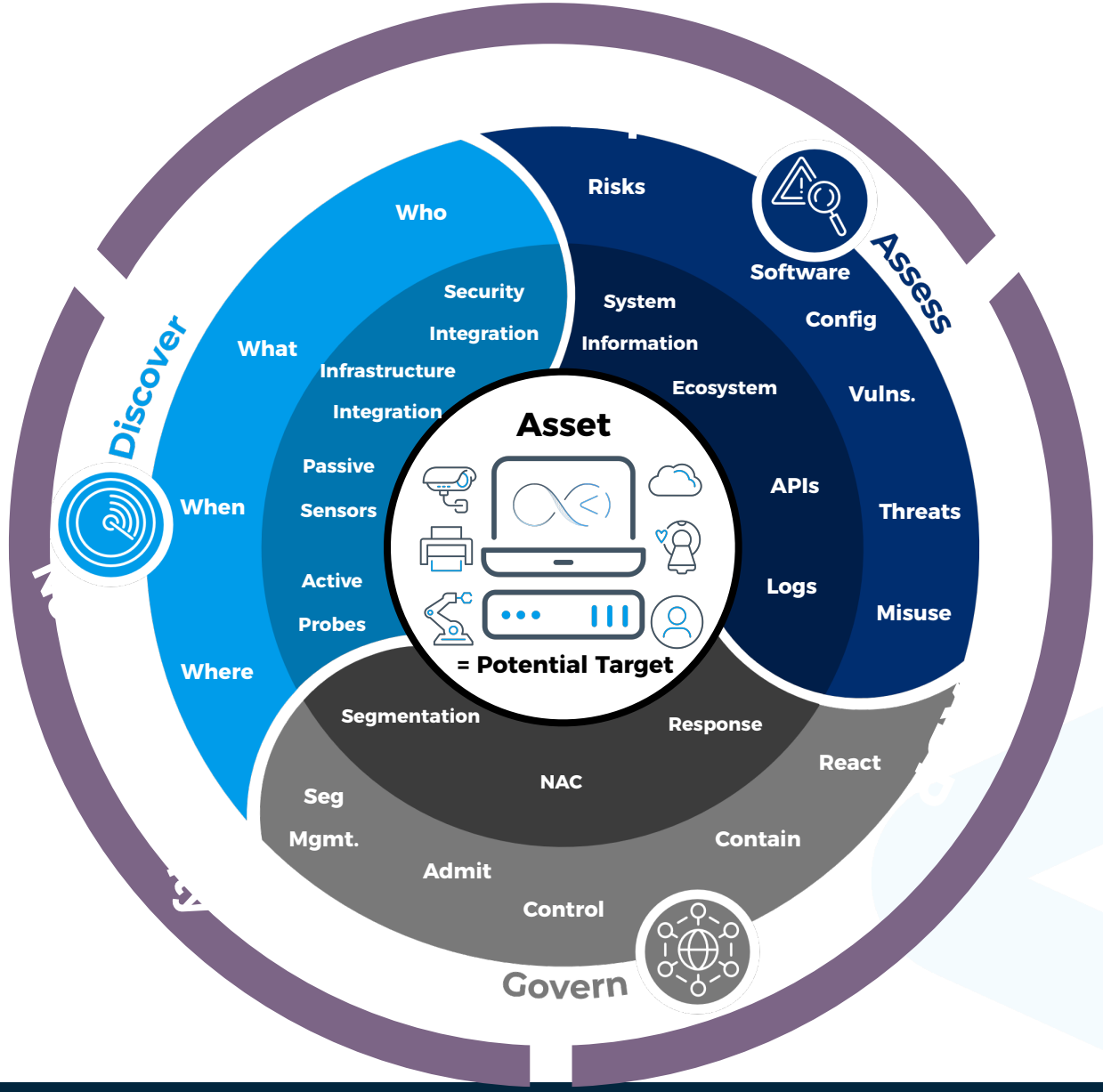
The Mitigation



The Mitigation in IoMT



Required Capabilities


Discover
Who
What
When
Where
Security
Integration
Infrastructure
Integration
Passive
Sensors
Active
Probes
Assess
Risks
Software
System
Information
Config
Ecosystem
Vulns.
APIs
Threats
Logs
Misuse
Asset
= Potential Target
Govern
Segmentation
Response
React
NAC
Seg
Mgmt.
Contain
Admit
Control

CAASM
Attack Surface Management
Asset Inventory
Asset Visibility
Risk Prioritization
Device Compliance

Network Access Control
Segmentation Management
Zero Trust
OT / IoT Security
Medical Device Security
Risk & Threat Containment

Threat Detection & Response
Managed Detection & Response (MDR)
SIEM Modernization / Next-gen SIEM
SOC Consolidation (SOAR, UEBA, TIP)
Log Storage / Compliance
Threat Hunting

Forescout Mission: Continuously identify, protect and ensure the compliance of all cyber assets across the modern organization.


Thank you