SEC Consult

an Eviden business

Challenges of Digital Forensics and Incident Response (DFIR) in OT Environments

Or „Who cares about breaches if my process is still running“

Stephan Mikiss
Gerhard Hechenberger
IT-S NOW 2024

an Eviden business

Who We Are

Senior Security Consultants @ SEC Consult

Stephan Mikiss

Head of SEC Defence
DFIR Specialist

Focus topics:

- Team management
- Incident management
- Incident response
- Proactive workshops

Gerhard Hechenberger

OT/IoT and Embedded
Security Specialist

Focus topics:

- Device hardware assessments
- Device firmware assessments
- OT infrastructure assessments
- SCADA assessments
- Research

Who We Are

Trusted partners for 360° digital security.

SEC Consult

an Eviden business

20+ years of consulting

8 countries

140+ white-hat hackers

80+ certificates

10+ years ISO 27001 certified

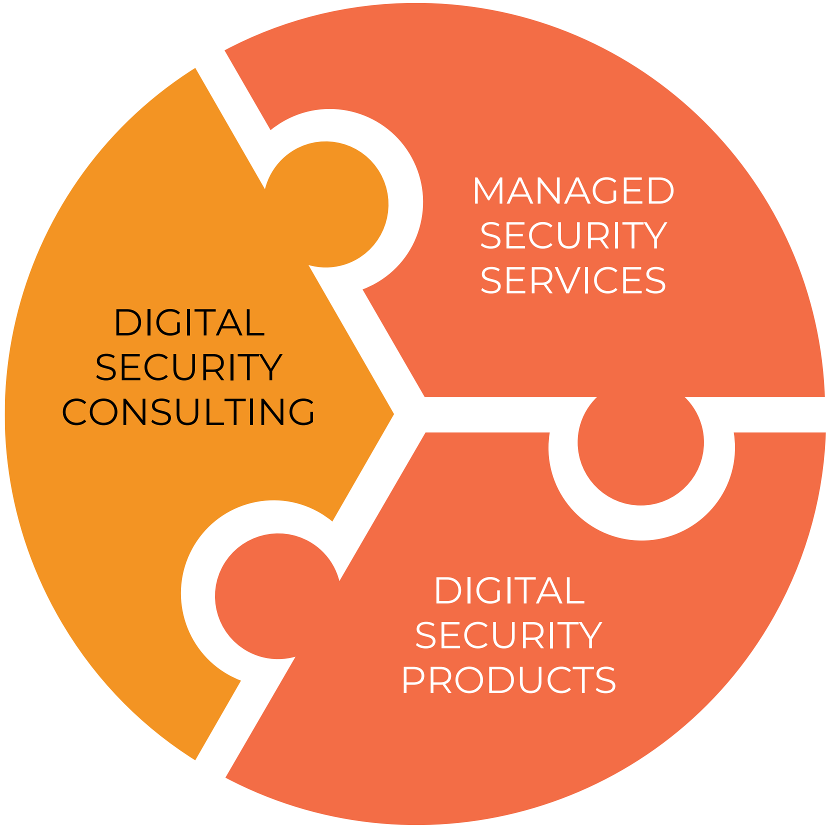
400+ advisories

r.sec-consult.com/advisories

bsi. ISO/IEC 27001 Information Security Management

IS 524814

CREST


MANAGED SECURITY SERVICES
DIGITAL SECURITY CONSULTING
DIGITAL SECURITY PRODUCTS

EVIDEN

5 SOC locations

6.000+ security experts

World's **# 1** in managed security services

2.100 patents

50.000 digital certificates

SEC Consult

an Eviden business

Agenda

01
Attack Landscape

02
Operational Technology (OT)

03
Incident Response Process

04
Anomalies, Visibility and Detection

05
Digital Forensics

06
Preparation

IT

OT

SEC Consult
an Eviden business

01 Attack Landscape

https://imgflip.com/

Attack Landscape for IT

Vectors of Compromise

Exploits

- Exploitation of vulnerabilities that are externally accessible.
- Example: Microsoft Exchange "ProxyLogon“

Phishing

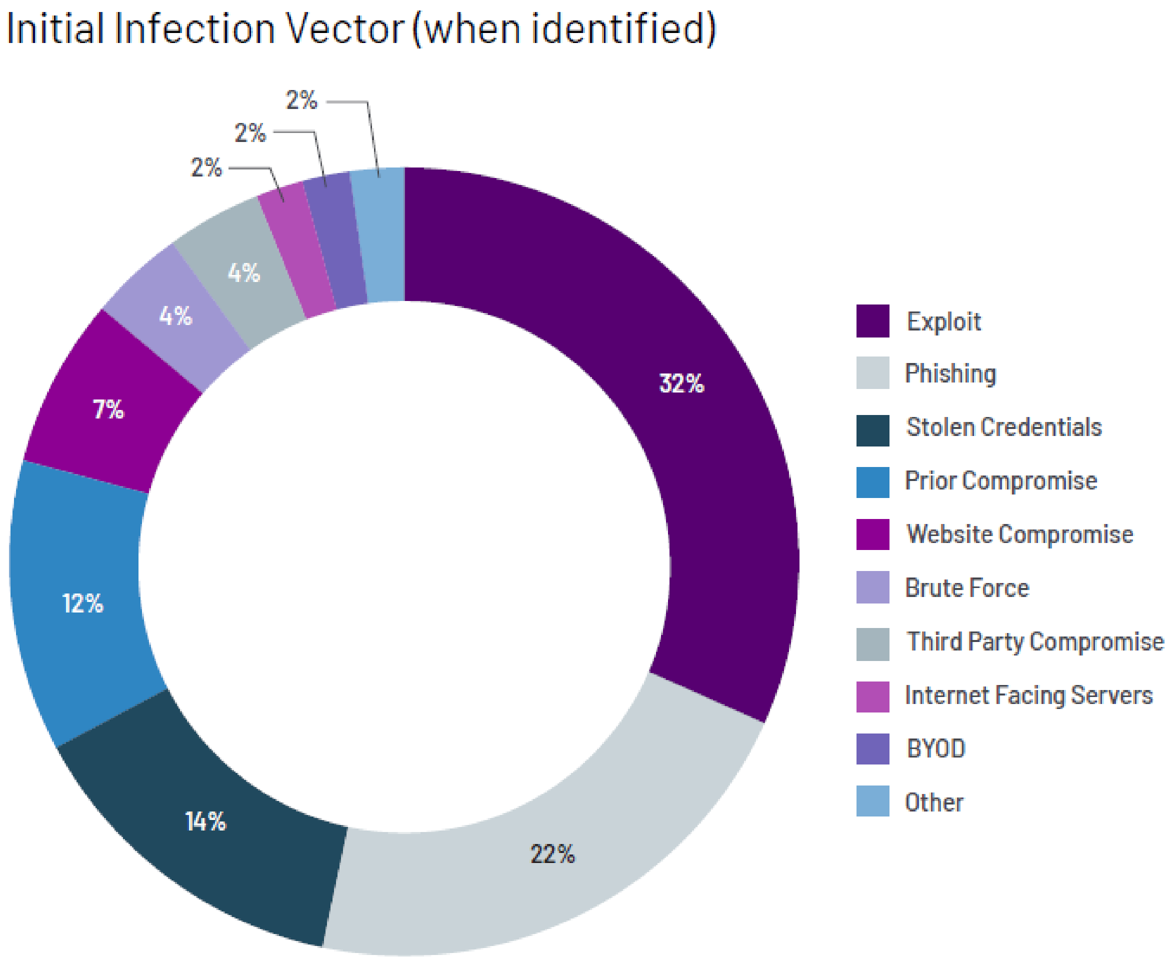
- Convincing employees to open malicious attachments from E-mails.
- Example: Emotet, Squirrelwaffle

Stolen Creds

- Utilize reused credentials from other breaches
- Example: Password reuse

Prior Compromise

- Active compromises are not sufficiently cleaned up
- Example: No pw change after ransomware attack

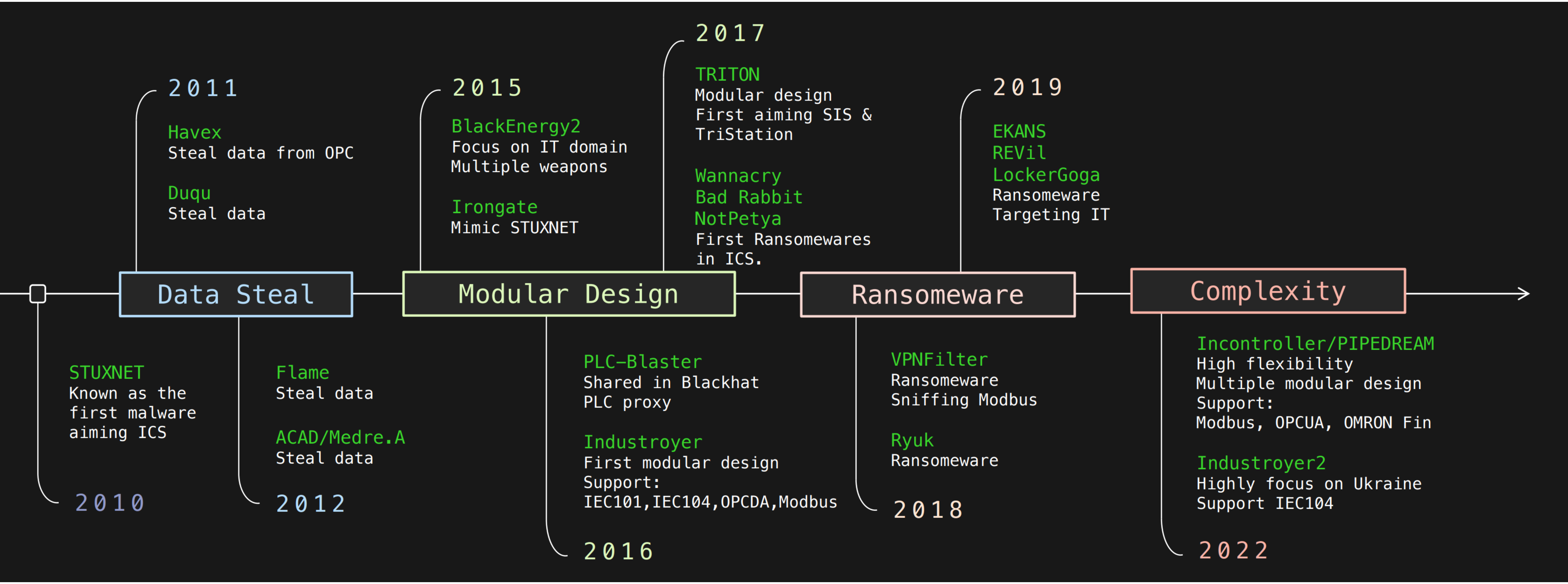


Initial Infection Vector (when identified)

Source: Mandiant M-Trends 2023

Attack Landscape for OT

ICS Malware Evolution



Data Steal

2010

STUXNET
Known as the first malware aiming ICS

2011

Havex
Steal data from OPC

Duqu
Steal data

2012

Flame
Steal data

ACAD/Medre.A
Steal data

Modular Design

2015

BlackEnergy2
Focus on IT domain
Multiple weapons

Irongate
Mimic STUXNET

2016

PLC-Blaster
Shared in Blackhat
PLC proxy

Industroyer
First modular design
Support:
IEC101,IEC104,OPCDA,Modbus

2017

TRITON
Modular design
First aiming SIS & TriStation

Wannacry
Bad Rabbit
NotPetya
First Ransomewares in ICS.

Ransomeware

2018

VPNFilter
Ransomeware
Sniffing Modbus

Ryuk
Ransomeware

2019

EKANS
REVil
LockerGoga
Ransomeware
Targeting IT

Complexity

2022

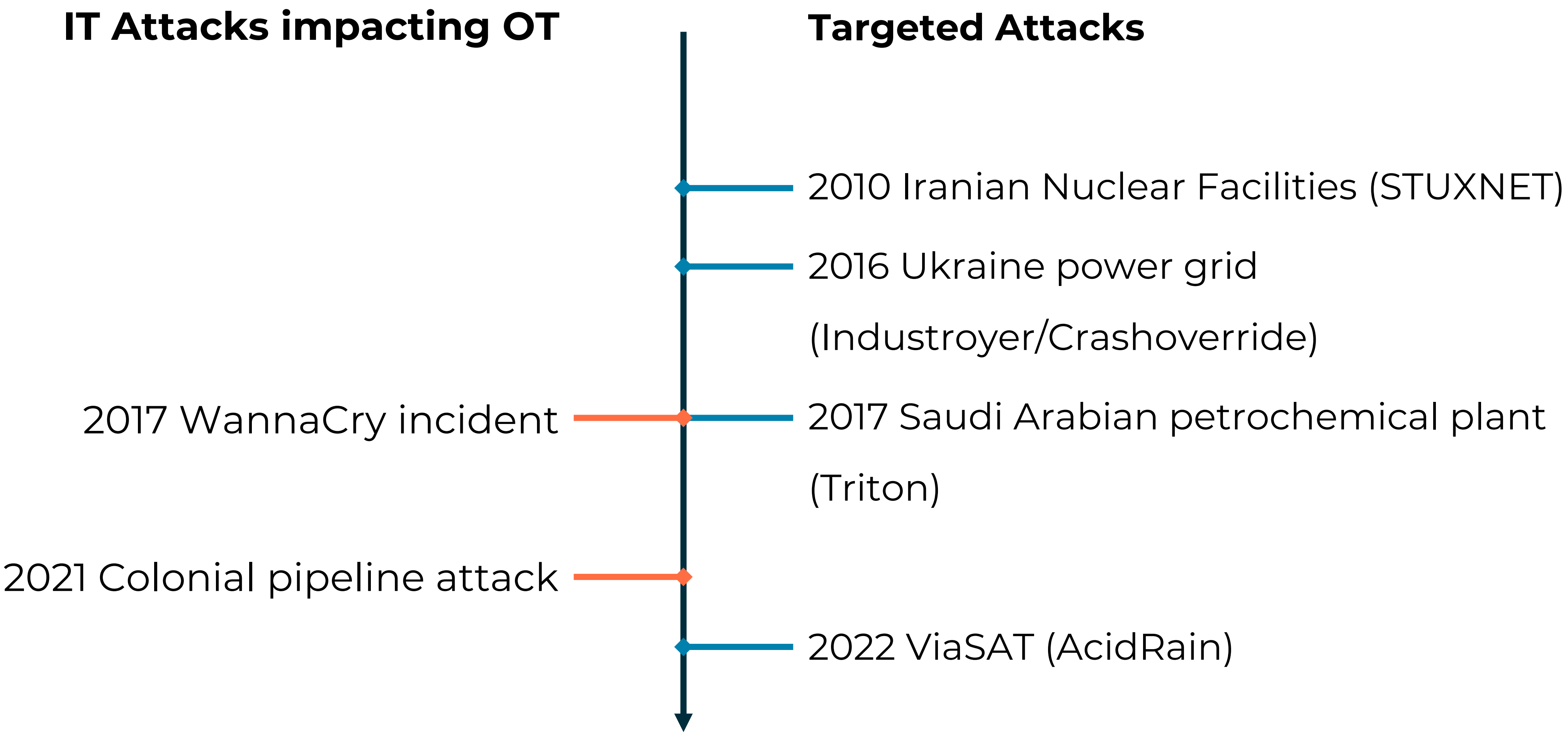
Incontroller/PIPEDREAM
High flexibility
Multiple modular design
Support:
Modbus, OPCUA, OMRON Fin

Industroyer2
Highly focus on Ukraine
Support IEC104

Source: Scarlet OT, HITBSecConf2023 – Phuket, https://conference.hitb.org/hitbsecconf2023hkt/materials/D2T1%20-%20Scarlet%20OT%20%e2%80%93%20OT%20Adversary%20Emulation%20for%20Fun%20and%20Profit-%20Vic%20Huang%20&%20Sol%20Yang.pdf

Attack Landscape for OT

Notable Events



IT Attacks impacting OT

Targeted Attacks

2010 Iranian Nuclear Facilities (STUXNET)

2016 Ukraine power grid (Industroyer/Crashoverride)

2017 WannaCry incident

2017 Saudi Arabian petrochemical plant (Triton)

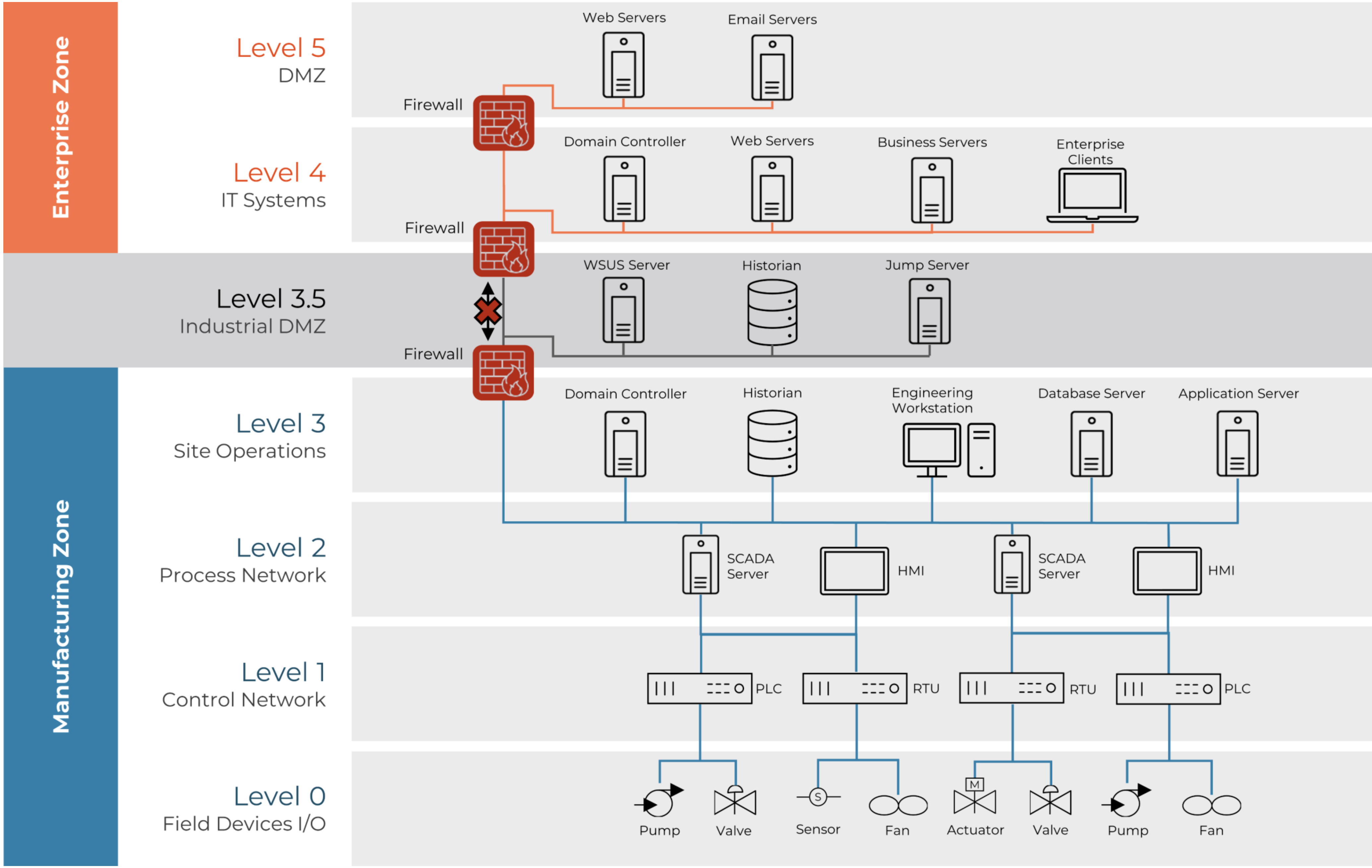
2021 Colonial pipeline attack

2022 ViaSAT (AcidRain)

an Eviden business

02 Operational Technology (OT)

https://imgflip.com/



Enterprise Zone

Level 5
DMZ

Level 4
IT Systems

Level 3.5
Industrial DMZ

Manufacturing Zone

Level 3
Site Operations

Level 2
Process Network

Level 1
Control Network

Level 0
Field Devices I/O

SEC Consult
an Eviden business

Operational Technology (OT)

Comparing Priorities

	IT Network	OT Network
Focus	Data	Process
Priorities	CIA	Safety AIC
Data Traffic	High throughput, dynamic	Low throughput, deterministic
Access Control	Many gateways	Few gateways
Device Failure Implications	Marginal	Severe
Threat Protection	Block data access	Keep operating
Patch Management	Patch Tuesday	Patch ... decade?

Operational Technology (OT)

Attack Surface of OT Process

Enterprise Network

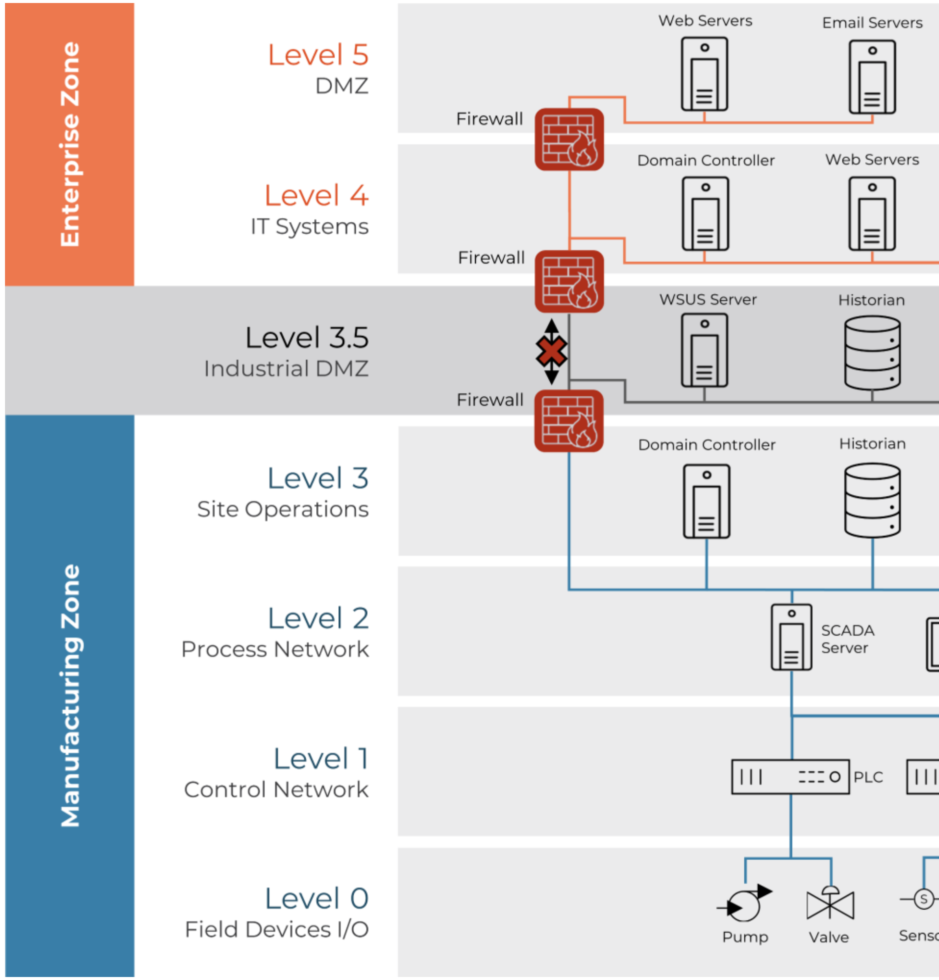
- Breaching the enterprise network
- Exploiting bad segmentation, passwords, …

Operations/Process Network

- Exploiting physical access
- Dual-use of PCs

Supplier

- Brought in hardware (notebook)
- Support access for machines



SEC Consult

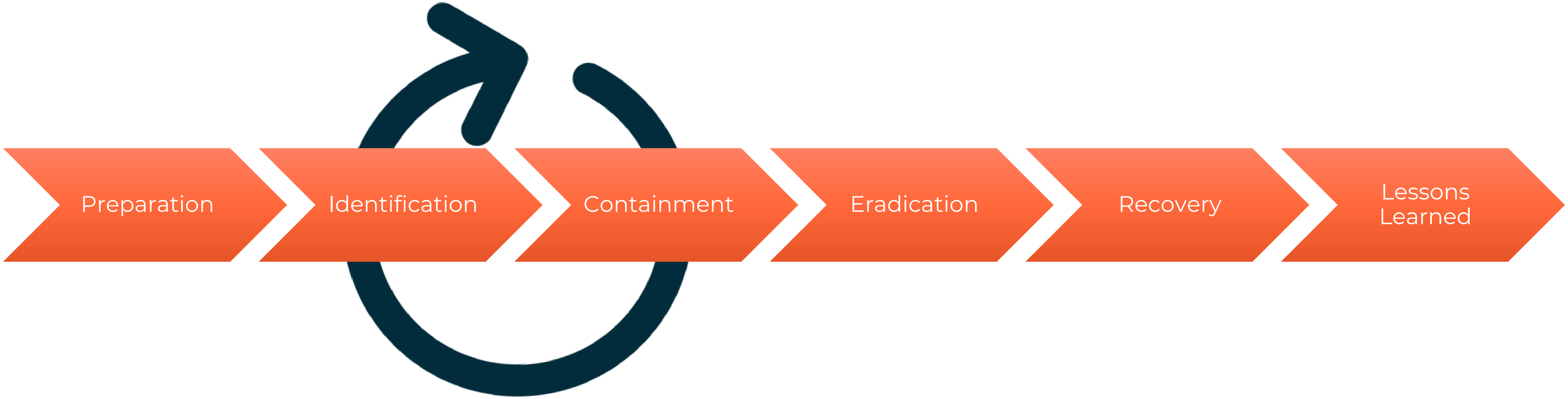
an Eviden business

03 Incident Response Process

https://imgflip.com/

Incident Response Lifecycle

„Incident handling is the process of detecting and analyzing incidents and limiting the incident‘s effect“ - NIST 800-61r2



Preparation

Identification

Containment

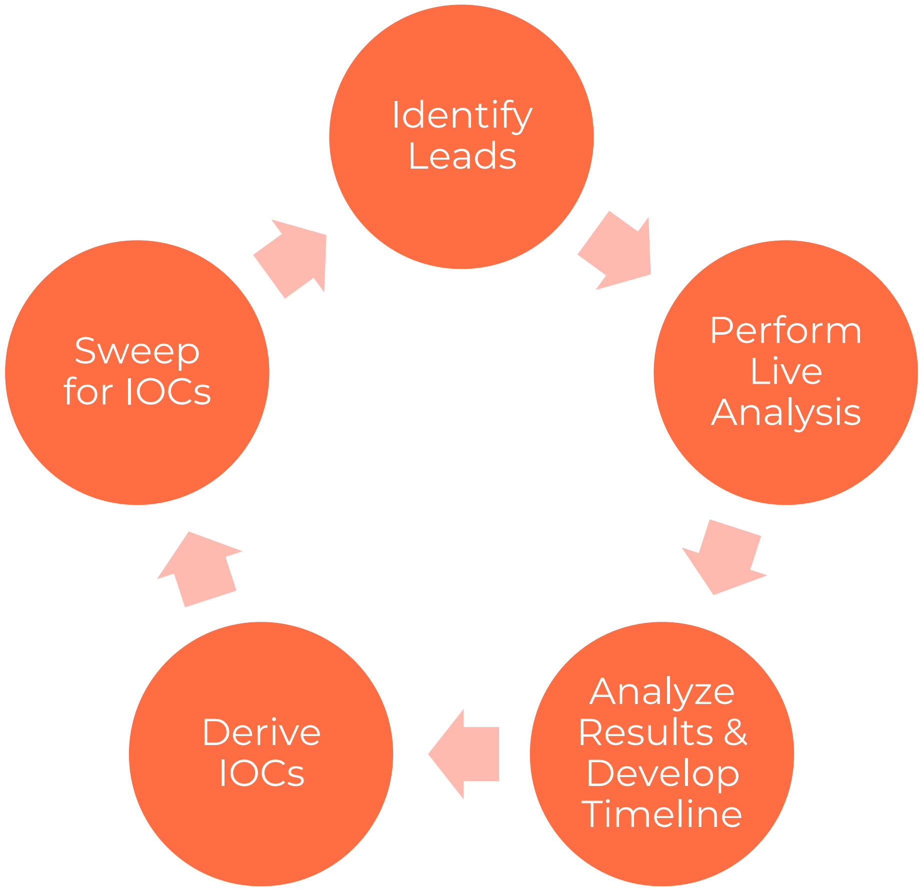
Eradication

Recovery

Lessons Learned

Incident Response Process in IT Environments

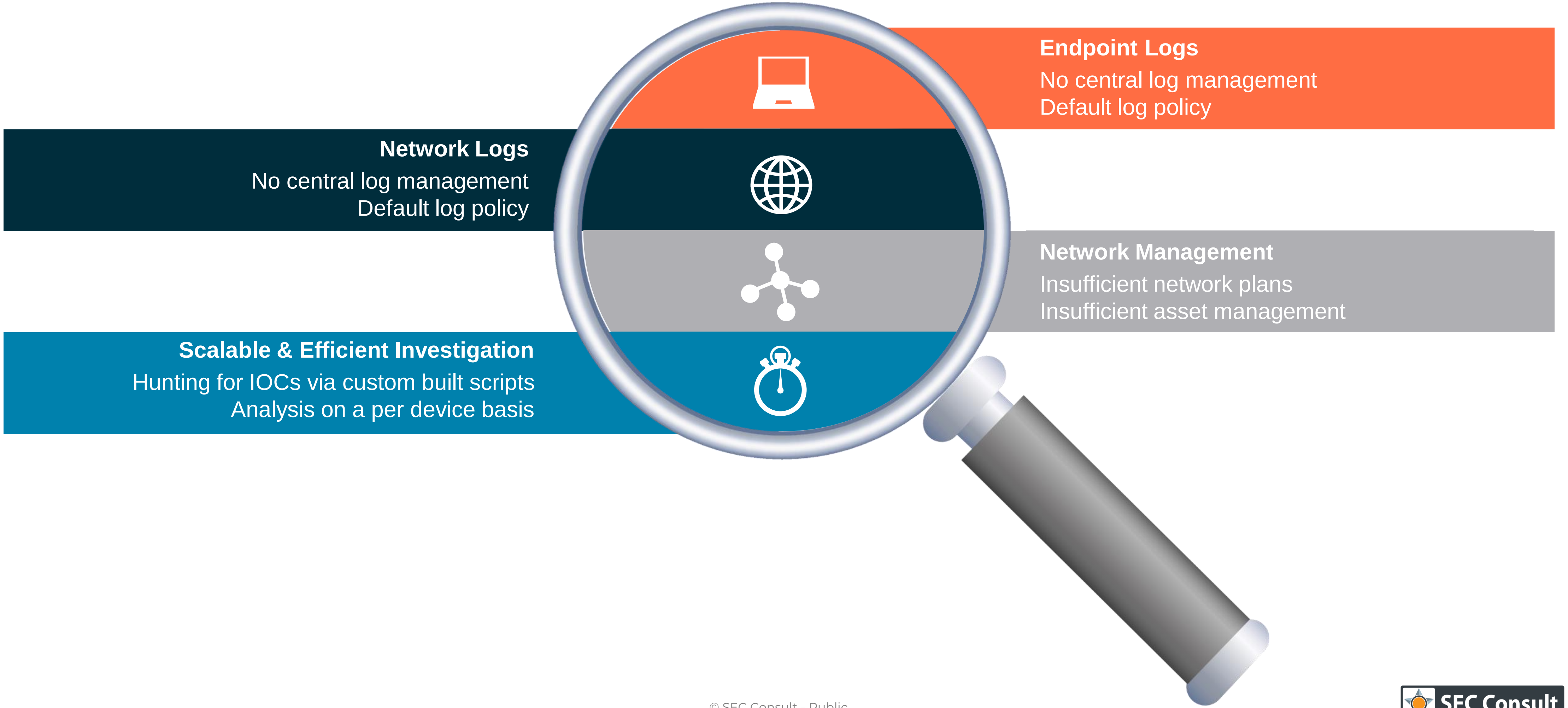
Identification Cycle



- Today: Endpoint centric investigations
- Fast response
- Scaling through the entire network
- Understanding the attack flow
- Reducing investigation overhead
- Identifying multiple patient zeroes
- Forensic investigations in the aftermath

Incident Response Process in IT Environments

Visibility Challenges



Endpoint Logs
No central log management
Default log policy

Network Logs
No central log management
Default log policy

Network Management
Insufficient network plans
Insufficient asset management

Scalable & Efficient Investigation
Hunting for IOCs via custom built scripts
Analysis on a per device basis

Incident Response Process

Incident Response Team in IT/OT

Internal

- Incident Manager
- Operations Leadership
- On-call IT personnel
- Physical security personnel
- Procurement
- Public relations and legal personnel

External

- Incident Response team

Internal OT

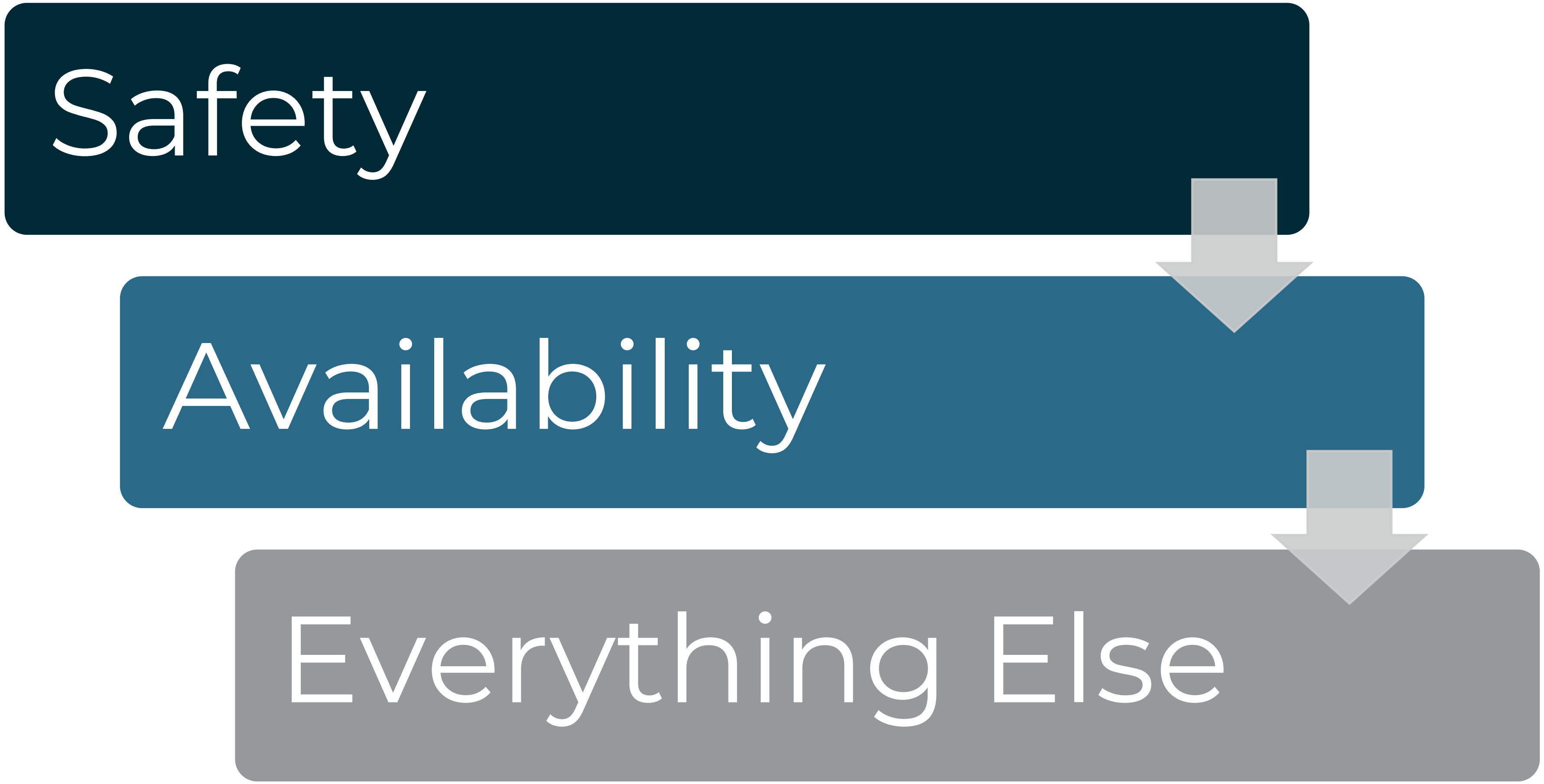
- Safety personnel
- On-call OT systems personnel

External OT

- OT technical support
  (vendors, integrators)
- Operational supply chain
  (e.g., suppliers, customers, distributors, business partners)
- Impacted community
  (e.g., facility neighbors)

Incident Response Process in OT Environments

Challenge: Safety and Availability



Safety

Availability

Everything Else

Incident Response Process in OT Environments

Challenge: Environment

Heterogeneous Software Environment

- Windows (XP+, CE Embedded, …)
- Linux (RHEL/SUSE, Embedded variants, …)
- Real-Time Operating Systems (RTOS)
- Industry software

Heterogeneous Hardware Environment

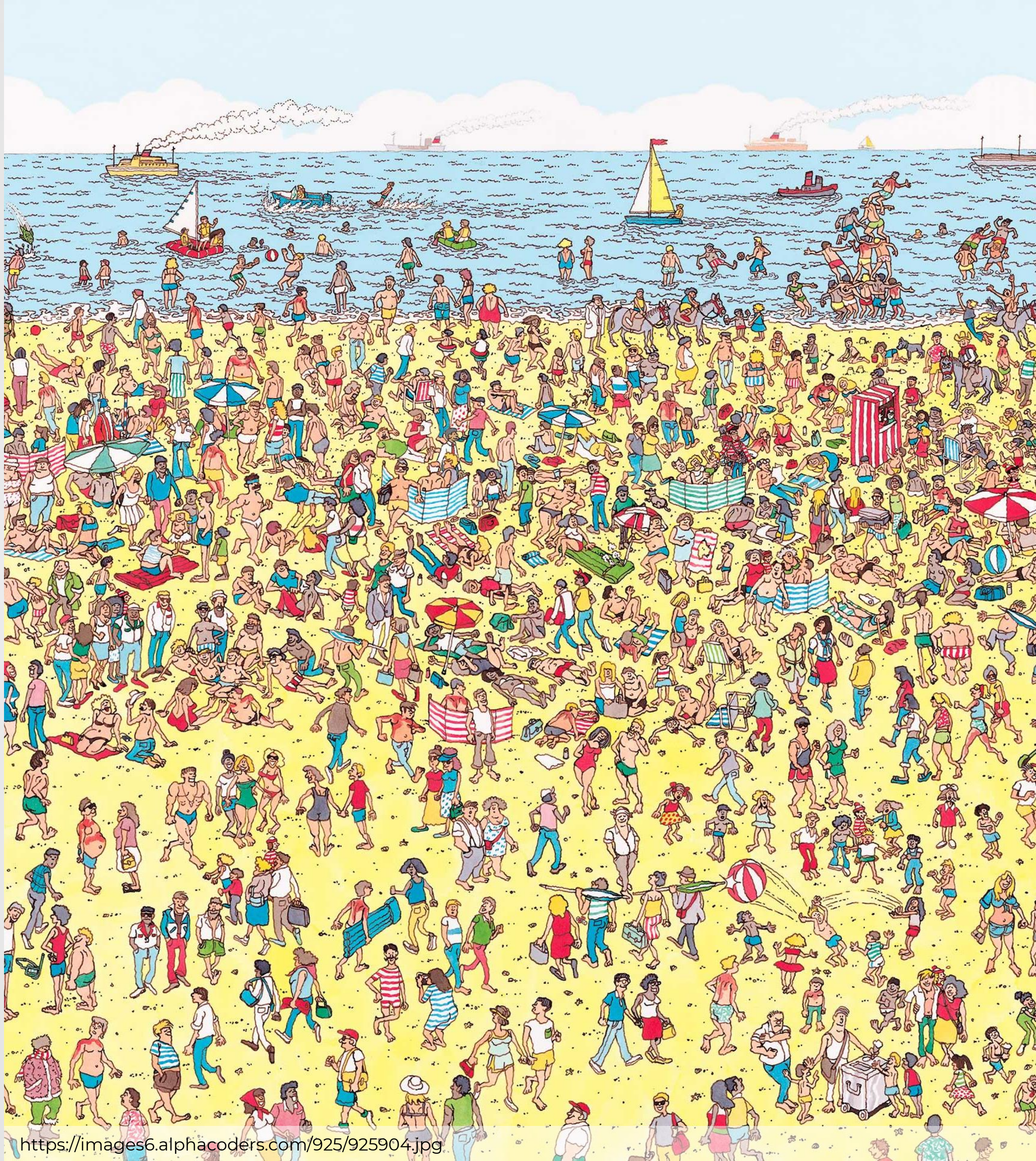
- Standard client PCs
- Embedded Systems: Firewall, TAPs, …
- Embedded Systems: PLC, RTU, HMI, …
- Embedded Systems: Smart sensors/actors

That may mean

- Less/No logging
- No root access
- Imaging is hard
- Need for specialists
- Destructive forensics
- Impossible forensics

an Eviden business

04 Anomalies, Visibility and Detection



https://images6.alphacoders.com/925/925904.jpg

Anomalies, Visibility and Detection

Incident Detection

Alert from an in-house technology (Reactive)

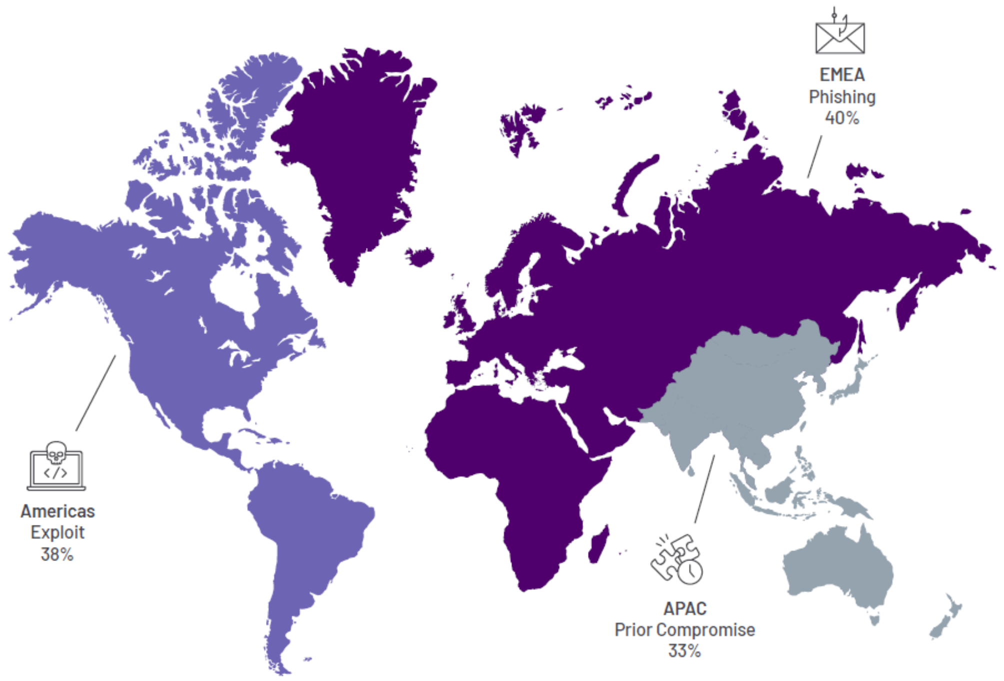
Threat Hunting (Proactive)

External notification

Anomalies, Visibility and Detection in IT Environments

Dwell Time

Most Prevalent Initial Intrusion Vector by Region



Global Dwell Time

16 Days

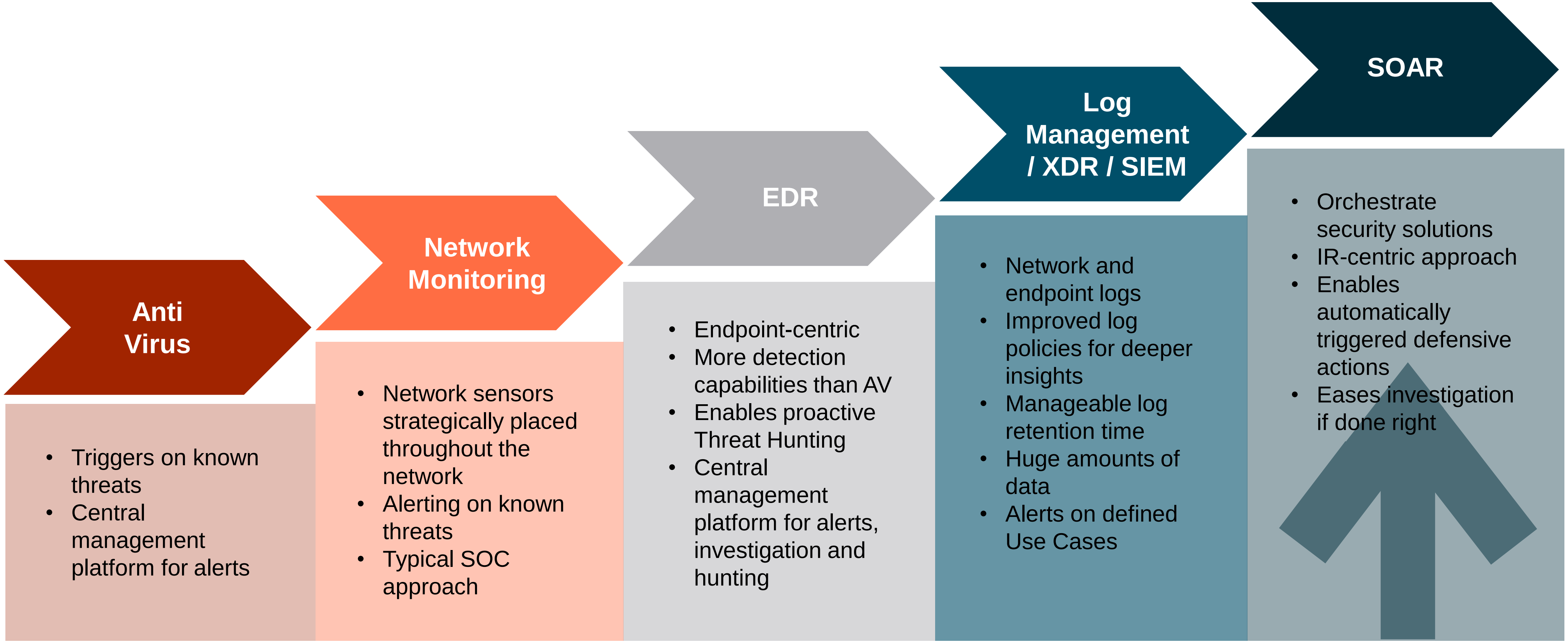
Ransomware Dwell Time

9 Days

Source: [Mandiant M-Trends 2023]()

Anomalies, Visibility and Detection in IT Environments

Visibility and Maturity



Anti Virus

- Triggers on known threats
- Central management platform for alerts

Network Monitoring

- Network sensors strategically placed throughout the network
- Alerting on known threats
- Typical SOC approach

EDR

- Endpoint-centric
- More detection capabilities than AV
- Enables proactive Threat Hunting
- Central management platform for alerts, investigation and hunting

Log Management / XDR / SIEM

- Network and endpoint logs
- Improved log policies for deeper insights
- Manageable log retention time
- Huge amounts of data
- Alerts on defined Use Cases

SOAR

- Orchestrate security solutions
- IR-centric approach
- Enables automatically triggered defensive actions
- Eases investigation if done right

Anomalies, Visibility and Detection

Forensic Artifacts

Forensic Artifact?

- Anything that helps you reconstruct attacker related events
- Depends on OS, configuration and attacker‘s TTPs of course

Basic Artifacts

- Logs
- Processes
- Executables
- Network Connections

There are multiple more advanced artifacts like

- Prefetch
- Shimcaches
- Registry Keys …

What do we look for?

- Network Behavior
- Processes
- File/Directory
- Locations
- Strange User Pattern
- Privileged Account Abuse
- Depending on organization

What is normal? Know your system! Create a baseline

Alerting thresholds

- Normal network traffic
- Normal data flows
- Normal human behavior
- Normal OT process behavior

Keep response time in mind (remote/unstaffed components)

Anomalies, Visibility and Detection in OT Environments

Challenge: Forensic Artifacts & Detection

Forensic Artifacts

- Events similar to IT
  - Windows
  - Linux
  - RTOS?
- Videos of status lights, HMIs, …
- Time variations (if not synchronized)
- Device memory captures
- Running program captures
- Firmware captures/documentation

Monitoring

Network

- Switched Port Analyzers (SPAN)
- Network Taps
- Strategic placement

System Use

- Combine with control log management system (SIEM)

Testing

- Performance testing
- Load testing
- Penetration testing

Vulnerability Scanning

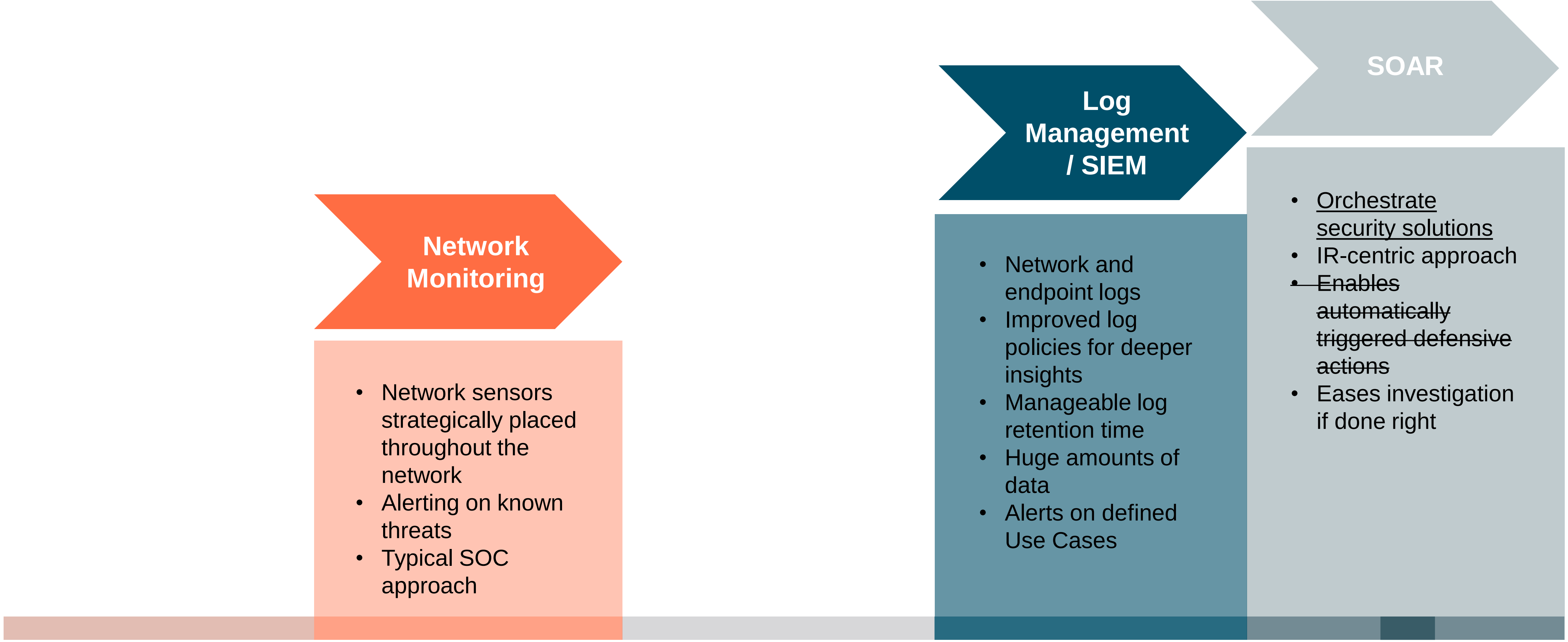
- Passive: Network traffic
- Active: Agent queries

Malicious Code Detection

- Antivirus is challenging

Anomalies, Visibility and Detection in OT Environments

Challenge: Visibility and Maturity



Network Monitoring

- Network sensors strategically placed throughout the network
- Alerting on known threats
- Typical SOC approach

Log Management / SIEM

- Network and endpoint logs
- Improved log policies for deeper insights
- Manageable log retention time
- Huge amounts of data
- Alerts on defined Use Cases

SOAR

- Orchestrate security solutions
- IR-centric approach
- ~~Enables automatically triggered defensive actions~~
- Eases investigation if done right

SEC Consult

an Eviden business

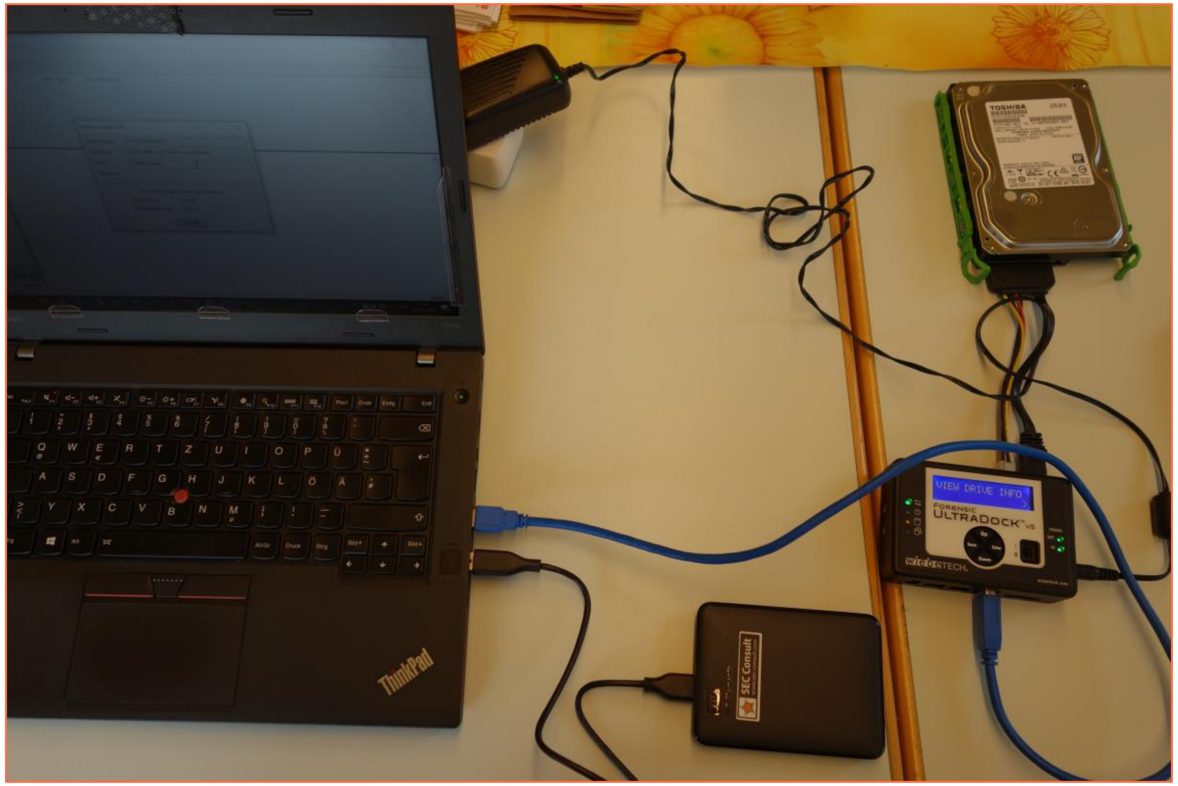
05 Digital Forensics

https://imgflip.com/

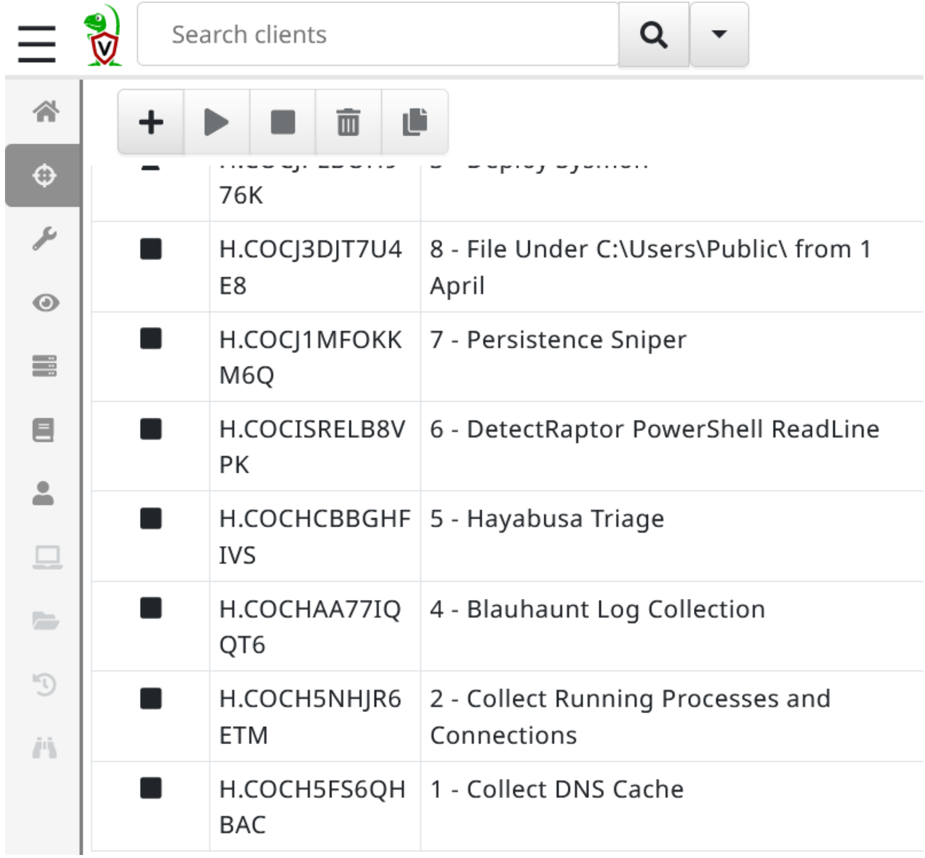
Digital Forensics in IT Environments

Data Acquisition

Physical Images



Velociraptor



	76K	
■	H.COCJ3DJT7U4 E8	8 - File Under C:\Users\Public\ from 1 April
■	H.COCJ1MFOKK M6Q	7 - Persistence Sniper
■	H.COCISRELB8V PK	6 - DetectRaptor PowerShell ReadLine
■	H.COCHCBBGHF IVS	5 - Hayabusa Triage
■	H.COCHAA77IQ QT6	4 - Blauhaunt Log Collection
■	H.COCH5NHJR6 ETM	2 - Collect Running Processes and Connections
■	H.COCH5FS6QH BAC	1 - Collect DNS Cache

Digital Forensics in OT Environments

Challenge: Environment

Heterogeneous Software Environment

- Windows (XP+, CE Embedded, …)
- Linux (RHEL/SUSE, Embedded variants, …)
- Real-Time Operating Systems (RTOS)
- Industry software

Heterogeneous Hardware Environment

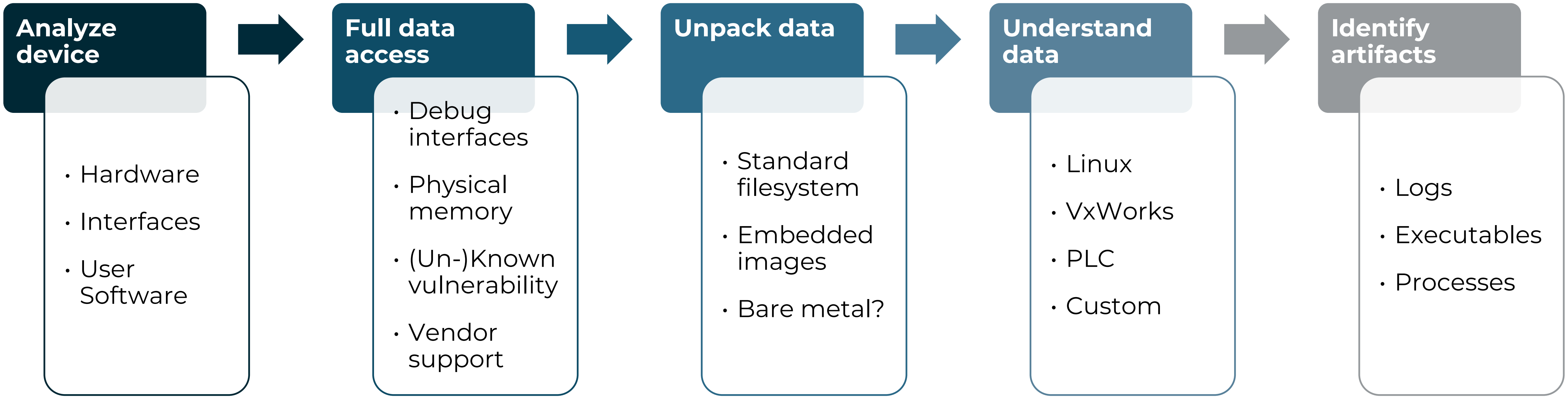
- Standard client PCs
- Embedded Systems: Firewall, TAPs, …
- Embedded Systems: PLC, RTU, HMI, …
- Embedded Systems: Smart sensors/actors

That may mean

- Less/No logging
- No root access
- Imaging is hard
- Need for specialists
- Destructive forensics
- Impossible forensics

Digital Forensics in OT Environments

Embedded Systems Lab



Analyze device

- Hardware
- Interfaces
- User Software

Full data access

- Debug interfaces
- Physical memory
- (Un-)Known vulnerability
- Vendor support

Unpack data

- Standard filesystem
- Embedded images
- Bare metal?

Understand data

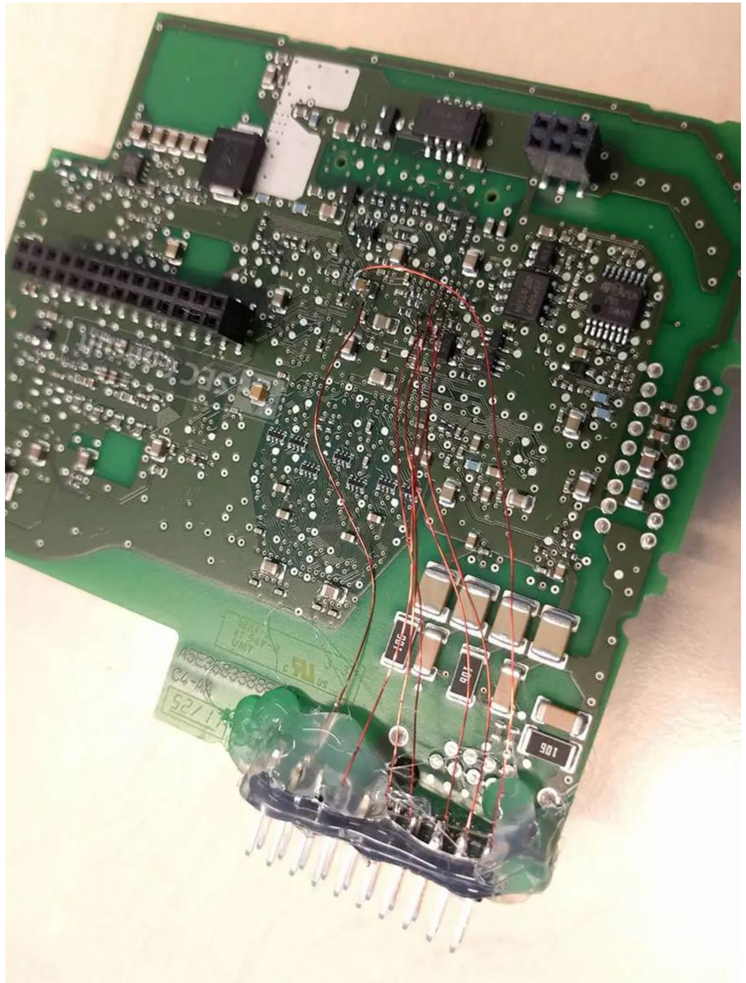
- Linux
- VxWorks
- PLC
- Custom

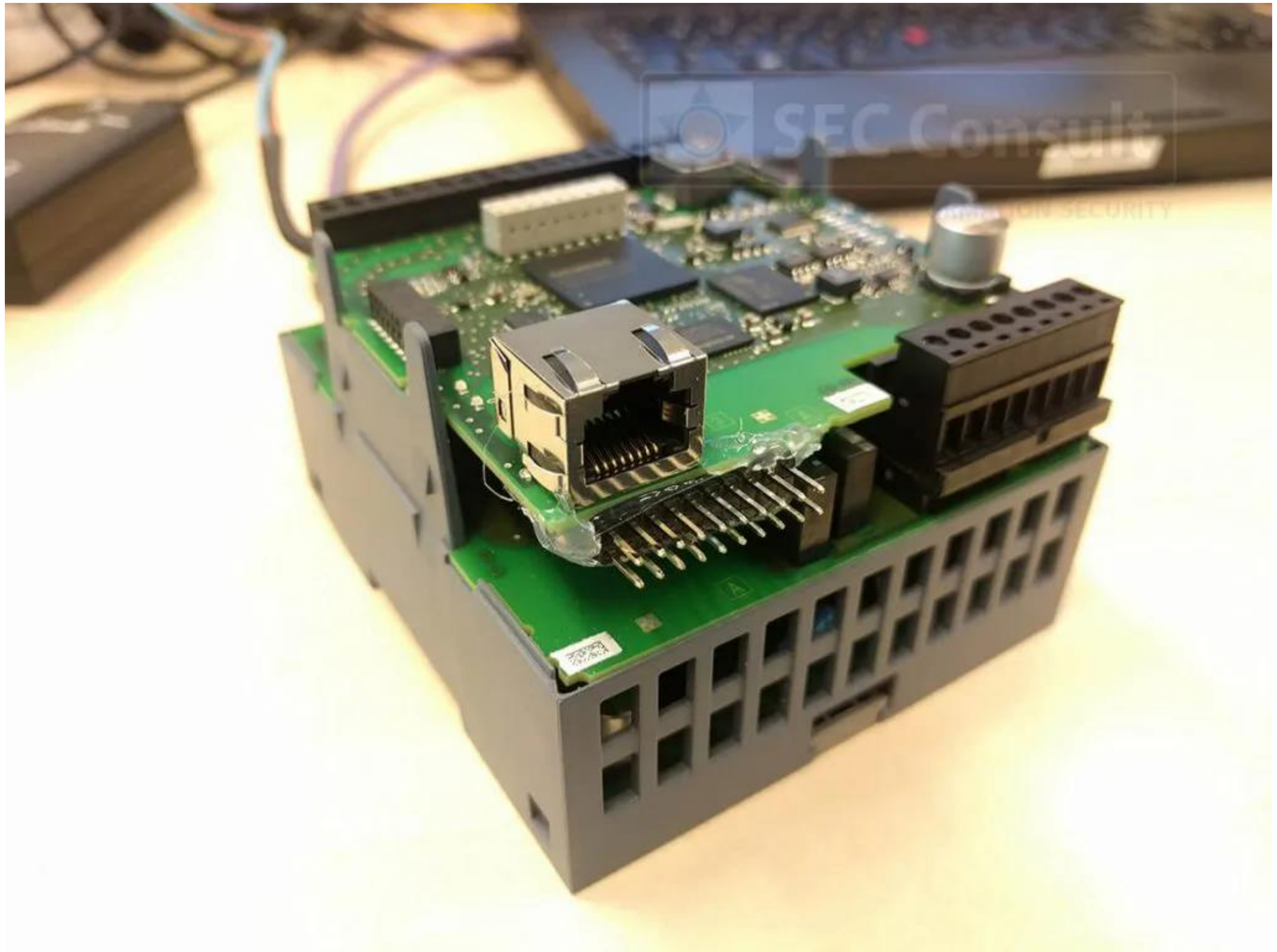
Identify artifacts

- Logs
- Executables
- Processes

Digital Forensics in OT Environments

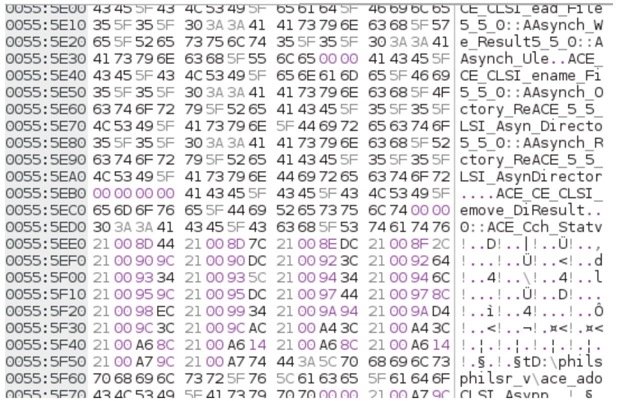
Embedded Systems Lab





Digital Forensics in OT Environments

Embedded Systems Lab



```
0055:5E00 43 45 5F 43  4C 53 49 5F  65 61 64 5F  46 69 6C 65  CE_CLSI_ead_File
0055:5E10 35 5F 35 5F  30 3A 3A 41  41 73 79 6E  63 68 5F 57  5_5_0::AAsynch_W
0055:5E20 65 5F 52 65  73 75 6C 74  35 5F 35 5F  30 3A 3A 41  e_Result5_5_0::A
0055:5E30 41 73 79 6E  63 68 5F 55  6C 65 00 00  41 43 45 5F  Asynch_Ule..ACE_
0055:5E40 43 45 5F 43  4C 53 49 5F  65 6E 61 6D  65 5F 46 69  CE_CLSI_ename_Fi
0055:5E50 35 5F 35 5F  30 3A 3A 41  41 73 79 6E  63 68 5F 4F  5_5_0::AAsynch_O
0055:5E60 63 74 6F 72  79 5F 52 65  41 43 45 5F  35 5F 35 5F  ctory_ReACE_5_5_
0055:5E70 4C 53 49 5F  41 73 79 6E  5F 44 69 72  65 63 74 6F  LSI_Asyn_Directo
0055:5E80 35 5F 35 5F  30 3A 3A 41  41 73 79 6E  63 68 5F 52  5_5_0::AAsynch_R
0055:5E90 63 74 6F 72  79 5F 52 65  41 43 45 5F  35 5F 35 5F  ctory_ReACE_5_5_
0055:5EA0 4C 53 49 5F  41 73 79 6E  44 69 72 65  63 74 6F 72  LSI_AsynDirector
0055:5EB0 00 00 00 00  41 43 45 5F  43 45 5F 43  4C 53 49 5F  ....ACE_CE_CLSI_
0055:5EC0 65 6D 6F 76  65 5F 44 69  52 65 73 75  6C 74 00 00  emove_DiResult..
0055:5ED0 30 3A 3A 41  43 45 5F 43  63 68 5F 53  74 61 74 76  0::ACE_Cch_Statv
0055:5EE0 21 00 8D 44  21 00 8D 7C  21 00 8E DC  21 00 8F 2C  !..D!..|!..Ü!..,
0055:5EF0 21 00 90 9C  21 00 90 DC  21 00 92 3C  21 00 92 64  !...!..Ü!..<!..d
0055:5F00 21 00 93 34  21 00 93 5C  21 00 94 34  21 00 94 6C  !..4!..\!..4!..l
0055:5F10 21 00 95 9C  21 00 95 DC  21 00 97 44  21 00 97 8C  !...!..Ü!..D!...
0055:5F20 21 00 98 EC  21 00 99 34  21 00 9A 94  21 00 9A D4  !..ì!..4!...!..Ô
0055:5F30 21 00 9C 3C  21 00 9C AC  21 00 A4 3C  21 00 A4 3C  !..<!..¬!.¤<!.¤<
0055:5F40 21 00 A6 8C  21 00 A6 14  21 00 A6 8C  21 00 A6 14  !.¦.!.¦.!.¦.!.¦.
0055:5F50 21 00 A7 9C  21 00 A7 74  44 3A 5C 70  68 69 6C 73  !.§.!.§tD:\phils
0055:5F60 70 68 69 6C  73 72 5F 76  5C 61 63 65  5F 61 64 6F  philsr_v\ace_ado
0055:5F70 43 4C 53 49  5F 41 73 79  70 70 00 00  21 00 A7 9C  CLSI_Asypp..!.§.
```

SEC Consult

an Eviden business

06 Preparation

https://imgflip.com/

Preparation

Incident Response Preparation in IT/OT Environments

Incident Preparation

- Incident classification and escalation paths
- Out-of-band communication mechanisms
- Investigation and analysis infrastructure
- BCM / Disaster Recovery plans

Backups

- Separate infrastructure
- Validate integrity
- Test restoration (time!)
- Documentation

Additionally for OT

- Backup control system configuration workstation
  - Portable
  - Programming software for all systems
- Isolated examination environment

- Proprietary software, media & license keys
- Documentation & wiring diagrams
- Spare parts

SEC Consult

an Eviden business

Summary

Summary

Challenges of DFIR in OT Environments

Past Attacks are executed from highly sophisticated groups over lengthy periods

Coming Attacks move towards the current IT ransomware state

OT Technology gets more connected and exposed

Security Level in OT environments is still low

Summary

Challenges of DFIR in OT Environments

- Baseline Creation is easier but takes effort
- Visibility Maturity is low and limited
- Universal Tools are scarce due to heterogeneous environment
- Forensic Artifacts are limited, and acquisition takes more effort
- Device Forensic is limited, expensive and destructive

SEC Consult

an Eviden business

Questions?

SEC Consult

an Eviden business

Thank you!

Dou you have any further questions?
For more information please contact:

Stephan Mikiss
Head of SEC Defense
s.mikiss@sec-consult.com

Gerhard Hechenberger
Senior Security Consultant
g.hechenberger@sec-consult.com