MANDIANT®

INCONTROLLER: Analysis and Implications of The New State-Sponsored Threat to ICS

Daniel Kapellmann Zafra
Senior Manager
@Kapellmann
www.kapell.tech

Ken Proska
Senior Analyst
@icsk3n

Who Are We?

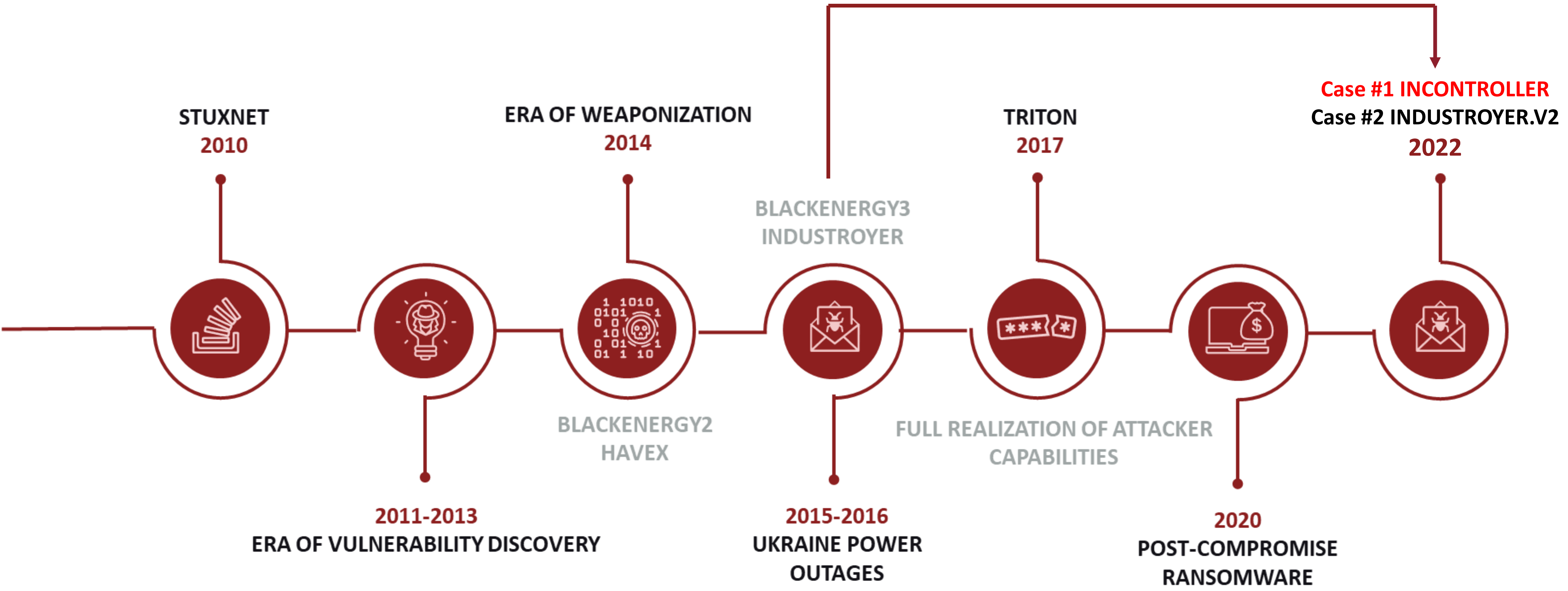
Daniel Kapellmann Zafra

Ken Proska

New Industrial Control Systems Malware?!

Icon by Freepik from Flaticon. Photo by Amber Kipp on Unsplash

Evolution of OT Malware



Background

We routinely find malicious capabilities via partnerships, incident response engagements, research, etc.

Mandiant analysis begun in early 2022 in collaboration with Schneider Electric and other entities

INCONTROLLER is related to:

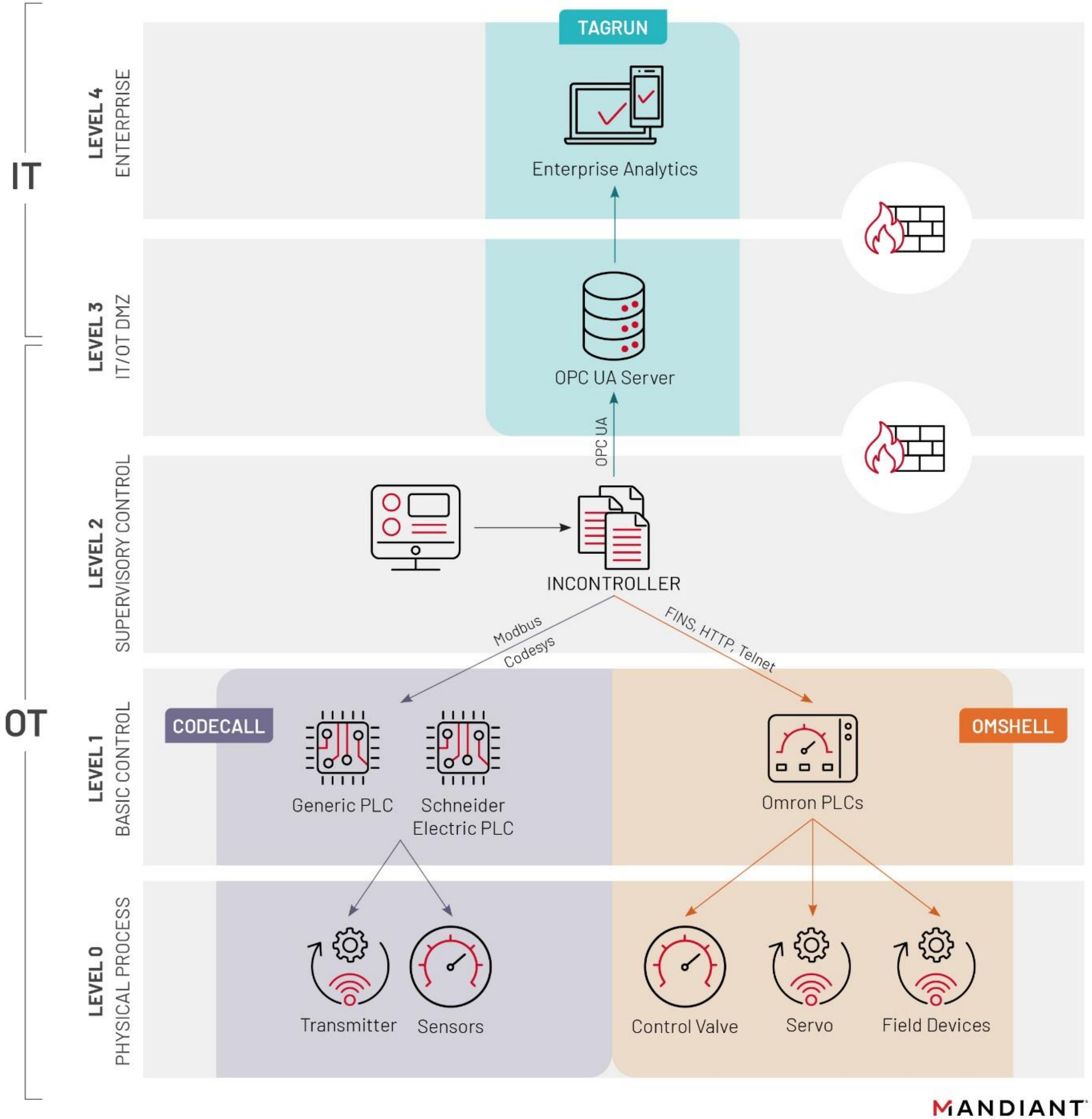
- CISA Alert (AA22-103A)
- Schneider Electric Bulletin SESB-2022-01
- CODESYS Advisory 2022-08
- PIPEDREAM reporting

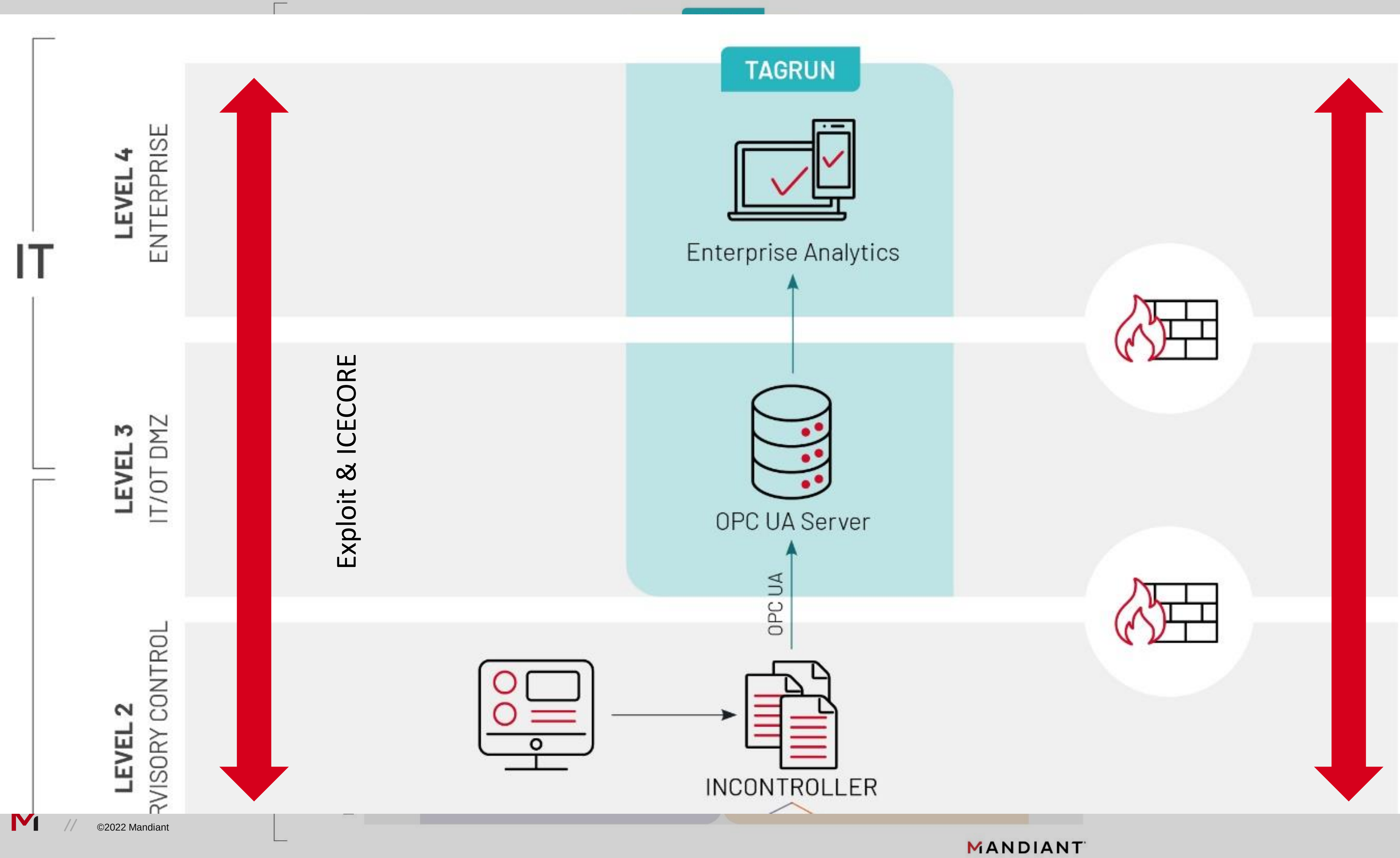
What is it?

INCONTROLLER	TAGRUN	ICS recon & attack support
	CODECALL	Schneider Electric disruption & attack
	OMSHELL	Omron attack

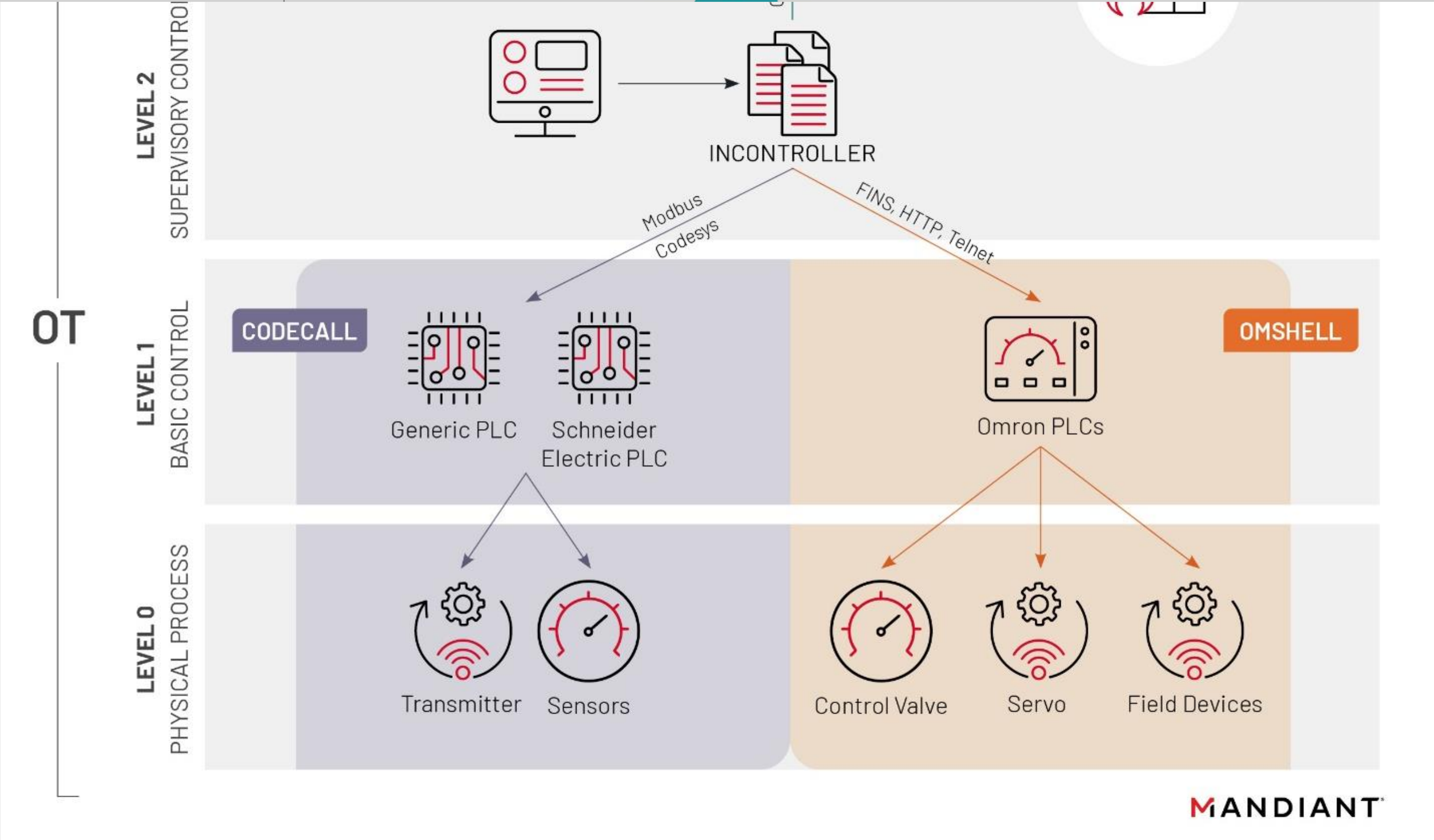
CVE-2020-15368 exploit	ASRock RGB Driver
ICECORE	C&C & IT/OT recon

Structure


IT
OT
LEVEL 4 ENTERPRISE
LEVEL 3 IT/OT DMZ
LEVEL 2 SUPERVISORY CONTROL
LEVEL 1 BASIC CONTROL
LEVEL 0 PHYSICAL PROCESS
TAGRUN
Enterprise Analytics
OPC UA Server
OPC UA
INCONTROLLER
Modbus
Codesys
FINS, HTTP, Telnet
CODECALL
Generic PLC
Schneider Electric PLC
OMSHELL
Omron PLCs
Transmitter
Sensors
Control Valve
Servo
Field Devices
MANDIANT



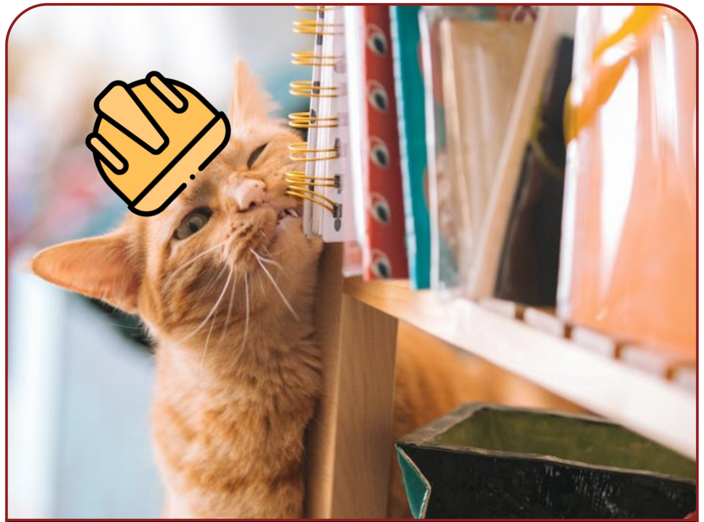
Exploit & ICECORE


OT
LEVEL 2
SUPERVISORY CONTROL
INCONTROLLER
Modbus
Codesys
FINS, HTTP, Telnet
LEVEL 1
BASIC CONTROL
CODECALL
Generic PLC
Schneider Electric PLC
Omron PLCs
OMSHELL
LEVEL 0
PHYSICAL PROCESS
Transmitter
Sensors
Control Valve
Servo
Field Devices
MANDIANT

Summary of INCONTROLLER

1. Large size and complex code
2. TAGRUN/OMSHELL/CODECALL → could be used independently or together
   - An attacker would likely leverage additional IT tooling
3. Targeted devices often in automation machinery across industries
   - Even without the users' knowledge – embedded systems
   - Possibly current modules were built to target a specific environment(s)
4. Very likely state sponsored – some evidence indicating Russia-nexus
5. Capabilities for to disruption, sabotage, and potential physical destruction

Summary of INCONTROLLER



Reusable

Extensible

Operated

As Seen in INCONTROLLER...

Icon by Freepik from Flaticon. Photo by Timo Volz on Unsplash, Photo by Tucker Good on Unsplash. "cat-typing" by graffiti living licensed CC BY-NC-ND 2.0.

Is INCONTROLLER Coming Back?

Icon by Freepik from Flaticon.

Photo by Harry Cunningham on Unsplash

INCONTROLLER: Tooling Overview

TAGRUN, CODECALL, OMSHELL and Potential Windows Tooling

TAGRUN

- ICS reconnaissance & attack tool targeting OPC UA servers and tags
  - OPC Unified Architecture (OPC UA) to centralize process data
  - Scanner, reader, and writer utility
- Scan IP addresses and ports via ICMP ping sweep
- Read server structure, read/write OPC tag values
- Login methods: credentials, certificates, brute force

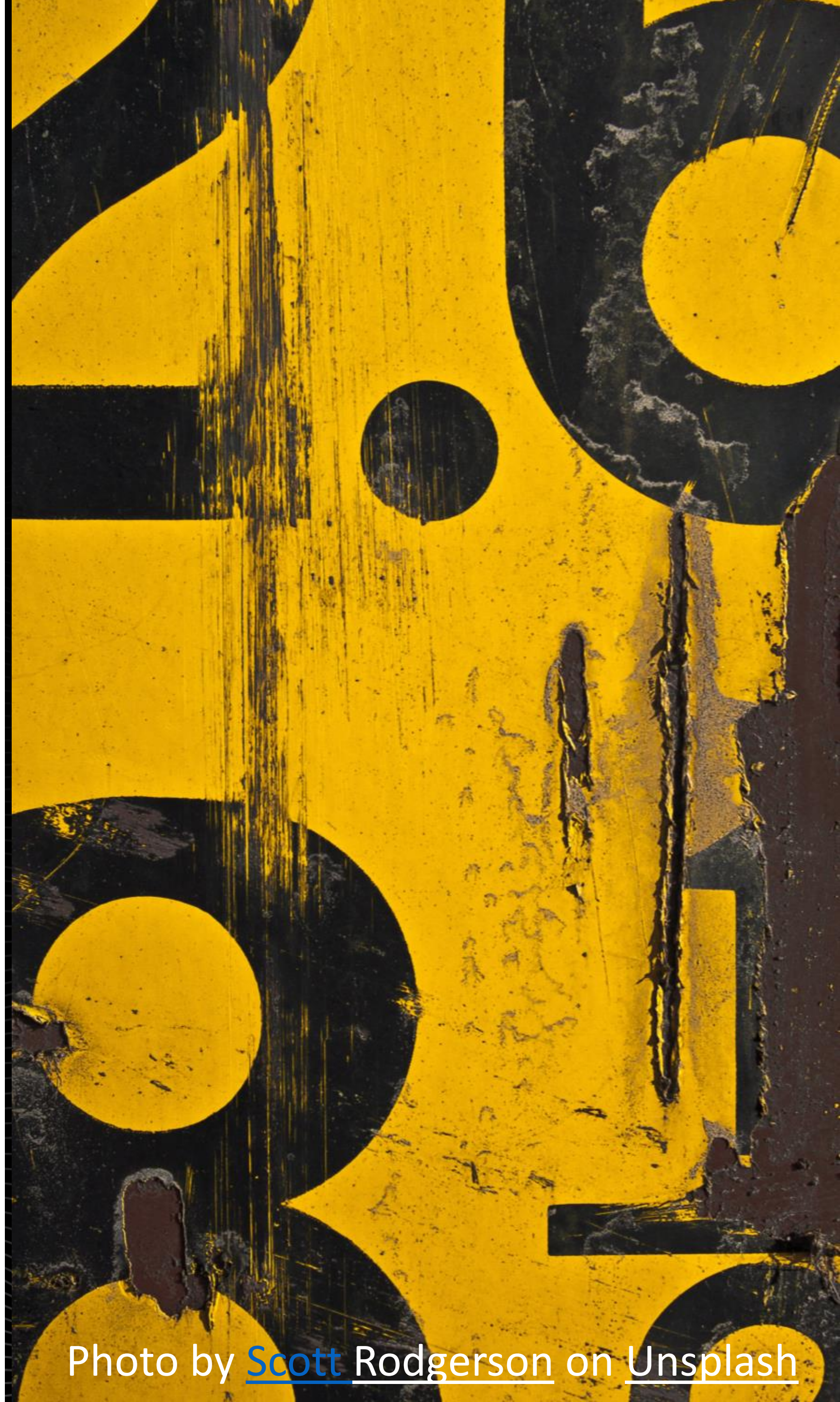
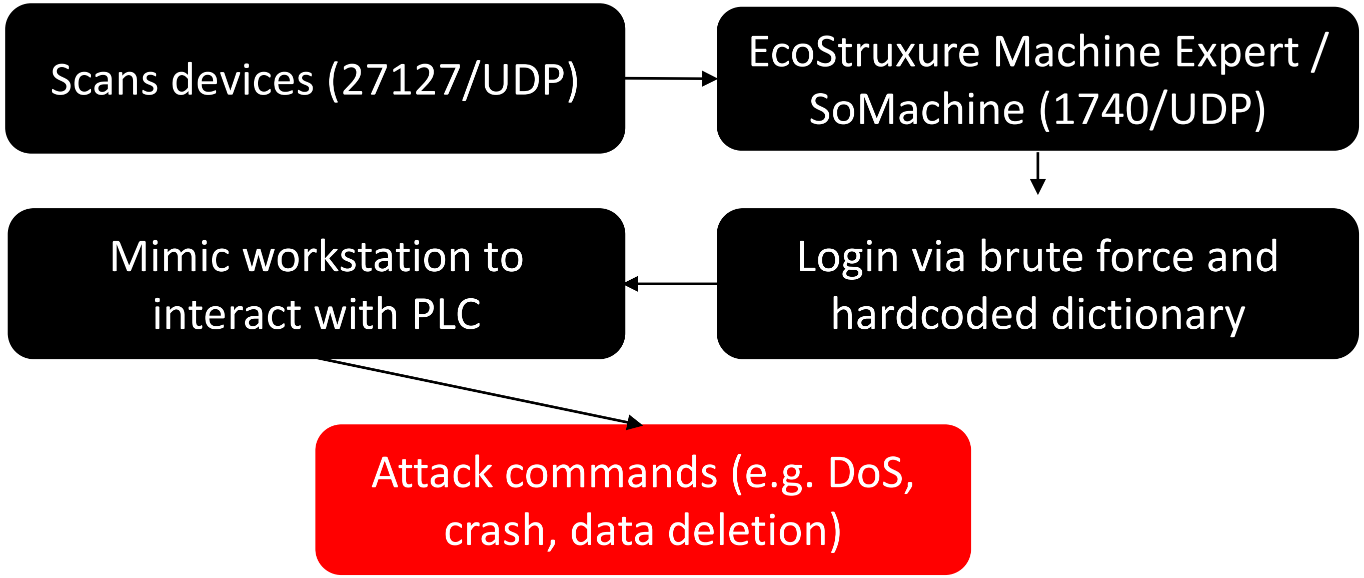


Photo by Scott Rodgerson on Unsplash

CODECALL

- CODECALL framework to interact with Modbus-enabled devices and specific PLCs
  - – Modbus is one of the most common ICS network protocols
- Scan/connect, and read/write device registers
- Schneider Electric TM251 PLC module:



Scans devices (27127/UDP)

EcoStruxure Machine Expert / SoMachine (1740/UDP)

Login via brute force and hardcoded dictionary

Mimic workstation to interact with PLC

Attack commands (e.g. DoS, crash, data deletion)

Photo by Paul Teysen on Unsplash

CODECALL – Target Device Modules

TM221

"Referenced"
/IO: Small (< 40 I/O)
Applications: repetitive machines

TM251

"Targeted"
I/O: Small – Large (>200 I/O)
Applications: modular, distributed machines

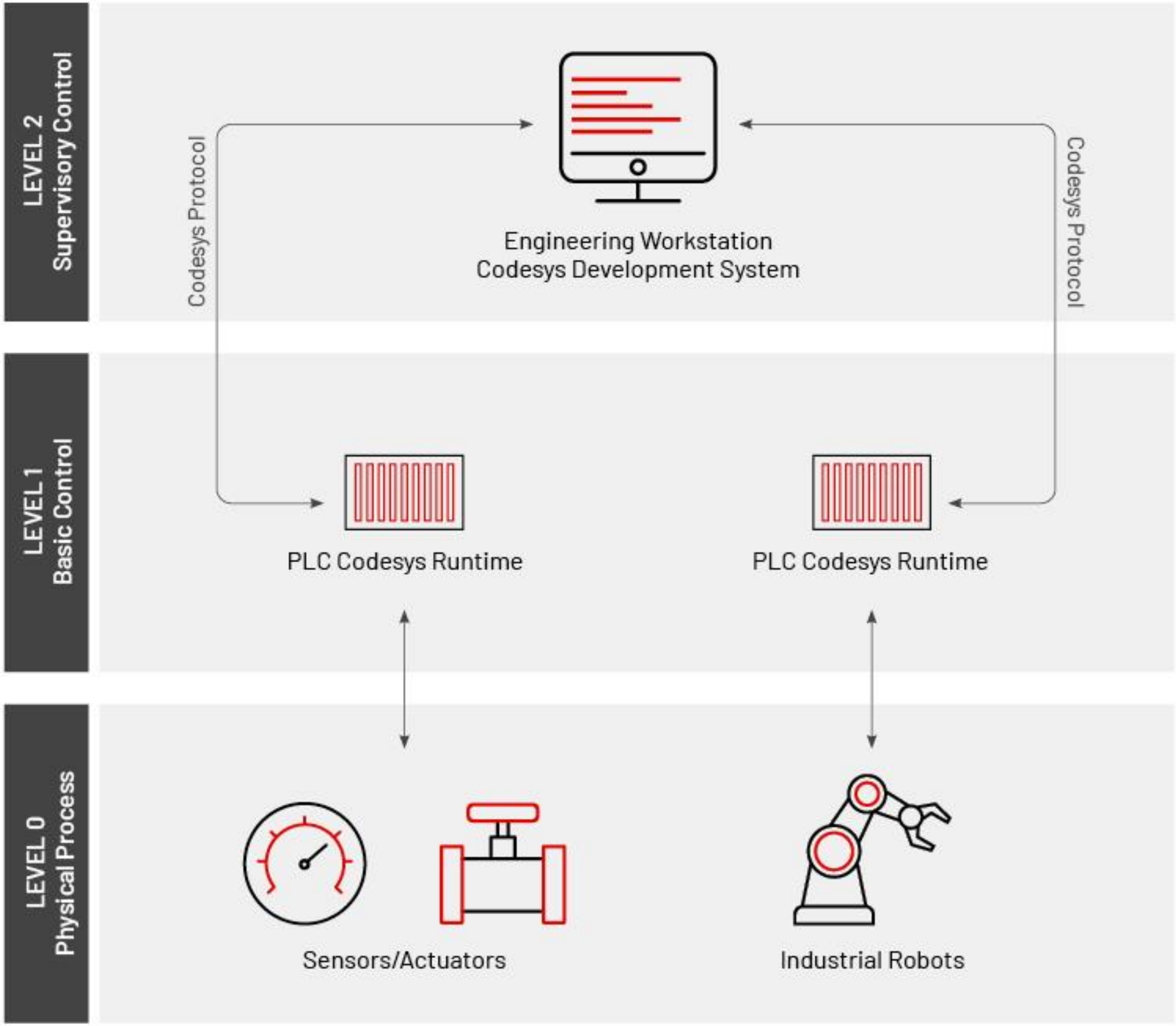
TM258

"Username:M258"
I/O: Small – Large (>200 I/O)
Applications: Packaging, conveying, hoisting

CODECALL – Other Impacted Devices

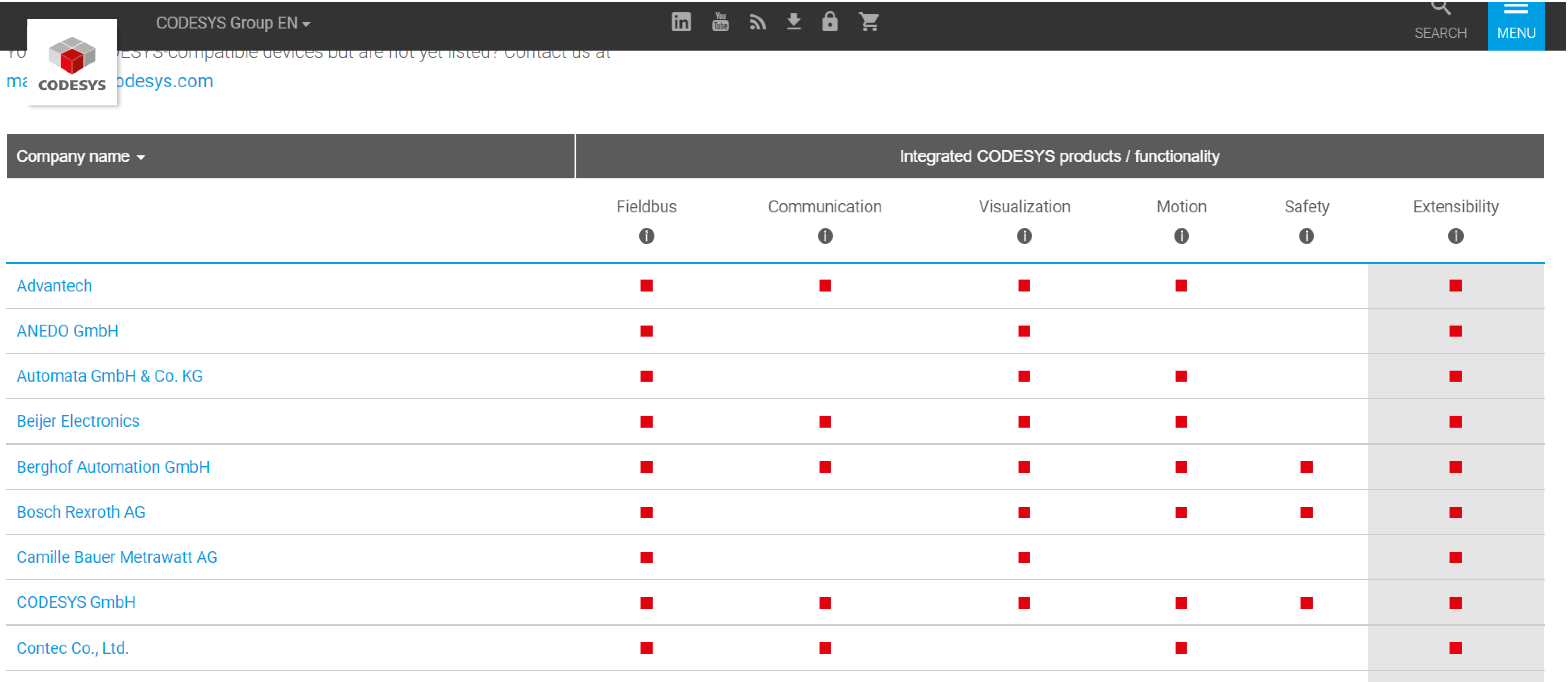
- No evidence interest in other specific devices, but can possibly be used in other Schneider electric controllers, or products with Codesys v3 and derived protocols
  - Some features (e.g., identification, dictionary list) potentially vendor/device-specific
- Modbus commands implemented outside of the device modules
  - Modbus is known to be vulnerable and easy to use for automation devices.

What's Up With Codesys?



“Several million CODESYS-compatible devices and approximately 1,000 different device types from over 500 manufacturers make CODESYS the leading manufacturer-independent IEC 61131-3 automation suite.”

[Quote from Codesys Website](#)



Yo ESYS-compatible devices but are not yet listed? Contact us at
ma odesys.com

Company name	Integrated CODESYS products / functionality					
	Fieldbus	Communication	Visualization	Motion	Safety	Extensibility
Advantech	🟥	🟥	🟥	🟥		🟥
ANEDO GmbH	🟥		🟥			🟥
Automata GmbH & Co. KG	🟥		🟥	🟥		🟥
Beijer Electronics	🟥	🟥	🟥	🟥		🟥
Berghof Automation GmbH	🟥	🟥	🟥	🟥	🟥	🟥
Bosch Rexroth AG	🟥		🟥	🟥	🟥	🟥
Camille Bauer Metrawatt AG	🟥		🟥			🟥
CODESYS GmbH	🟥	🟥	🟥	🟥	🟥	🟥
Contec Co., Ltd.	🟥	🟥		🟥		🟥

OMSHELL

- Scan/connect to Omron PLCs using MAC addresses, HTTP, and FINS protocol
  - Omron's proprietary Factory Interface Network Service (FINS) protocol (9600/UDP)
- Interact with Omron PLCs using HTTP
  - Query device information (model, device name, mode, user, CPU information, system config, etc.)
  - Transfer files, backup/load configurations
  - Read/write values of connected EtherCAT devices
  - Execute Telnet daemon on device to upload a payload
  - Some disruption capabilities (e.g. wipe memory)
- Contains servo module to read/write data
  - Convert electrical power into precision-controller motion

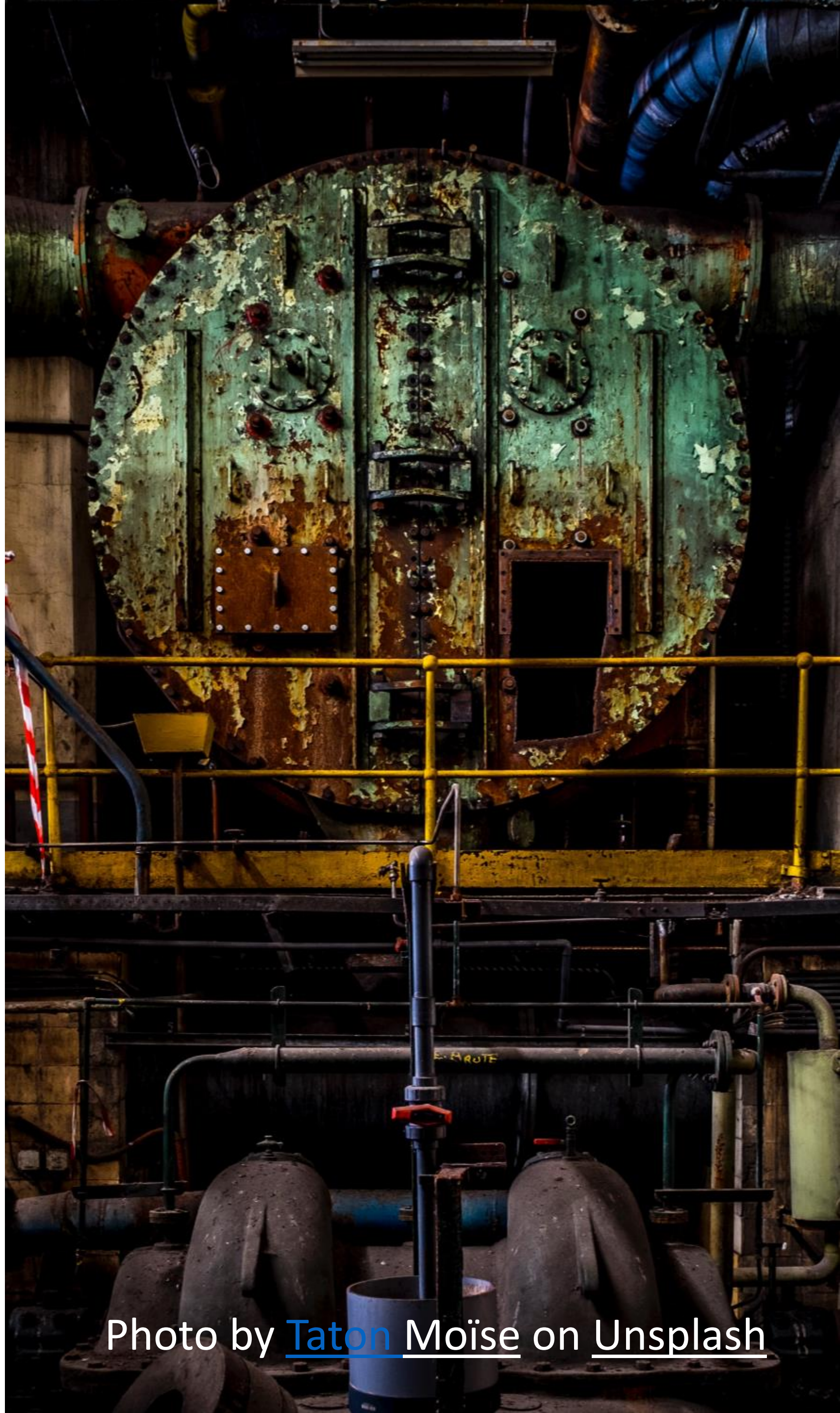


Photo by Taton Moïse on Unsplash

OMSHELL – Targeted Devices

NX1P2

Applications: advanced motion control, compact solutions

NJ501

Applications: advanced motion control, large/fast solutions

Servo

R88D-1SN10F-ECT
Applications: mid-high range

OMSHELL – Other Impacted Devices

- The primary protocol used by OMSHELL is HTTP

- Minimal documentation on HTTP protocol/API usage for Omron PLCs
  - Other NX/NJ PLC series devices appear to support HTTP, possibly more…

Potential Supporting Windows Tooling

- CVE-2020-15368 exploit
  - AsrDrv103.sys in the ASRock RGB Driver
  - Installation and exploitation of vulnerable driver
  - ASRock motherboards potentially used in HMIs and EWS
- ICECORE: C&C and IT/OT reconnaissance
  - Backdoor that performs command and control (C&C) over SSL
  - Malware capabilities:
    - Surveying system information using WMI
    - Executing arbitrary commands
    - Enumerating directories
    - Read/write file operations, registry entries

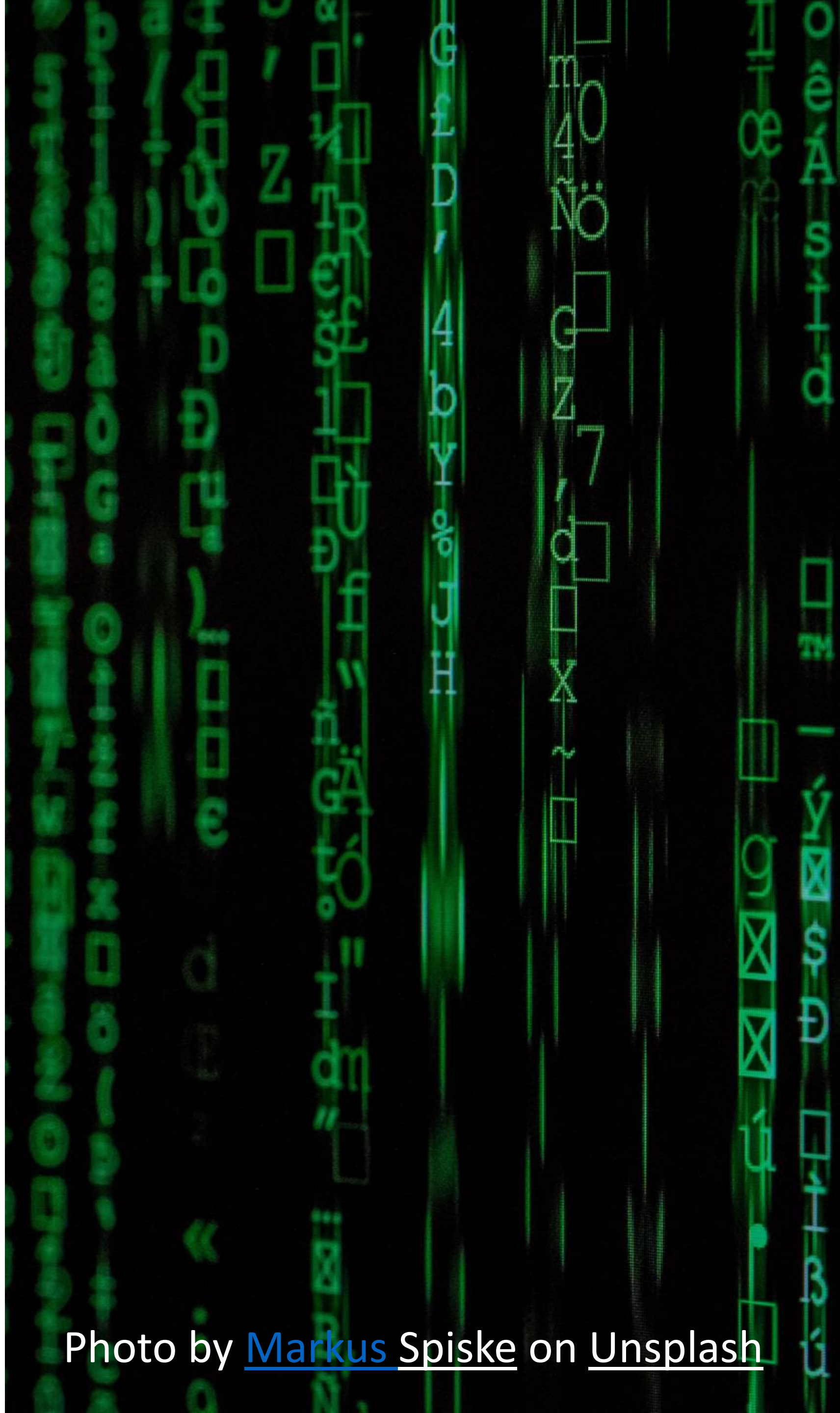


Photo by Markus Spiske on Unsplash

Attribution & Attack Scenarios

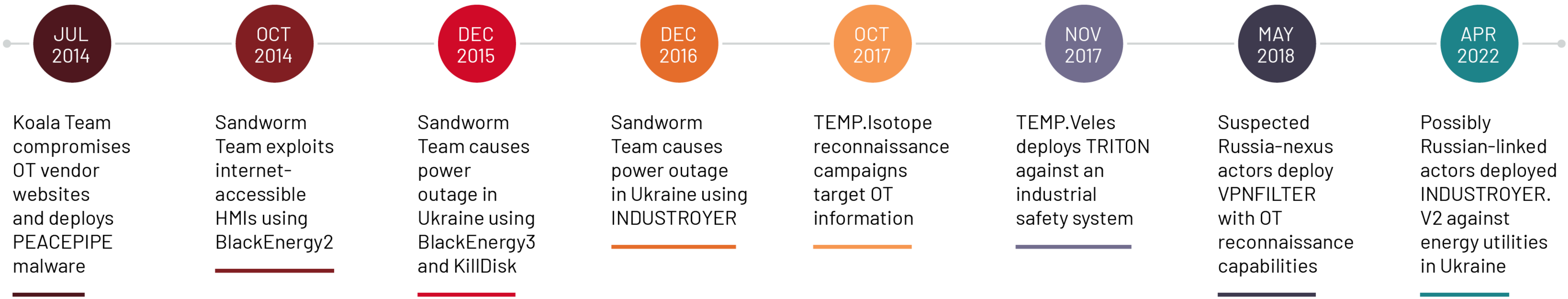
INCONTROLLER is Very Likely State-Sponsored Malware

- INCONTROLLER does not overlap with any previously tracked group
- Very likely state-sponsored given:
  - The tools complexity
  - Expertise and resources required to build it
  - Its limited utility in financially motivated operations
- Limited circumstantial evidence suggests a Russia-nexus
  - All we can share at this time is very circumstantial

Consistent With Russia’s Historical OT Threat Activity

2014
2022

HISTORICAL RUSSIA-NEXUS ACTIVITY IMPACTING ICS



JUL 2014

Koala Team compromises OT vendor websites and deploys PEACEPIPE malware

OCT 2014

Sandworm Team exploits internet-accessible HMIs using BlackEnergy2

DEC 2015

Sandworm Team causes power outage in Ukraine using BlackEnergy3 and KillDisk

DEC 2016

Sandworm Team causes power outage in Ukraine using INDUSTROYER

OCT 2017

TEMP.Isotope reconnaissance campaigns target OT information

NOV 2017

TEMP.Veles deploys TRITON against an industrial safety system

MAY 2018

Suspected Russia-nexus actors deploy VPNFILTER with OT reconnaissance capabilities

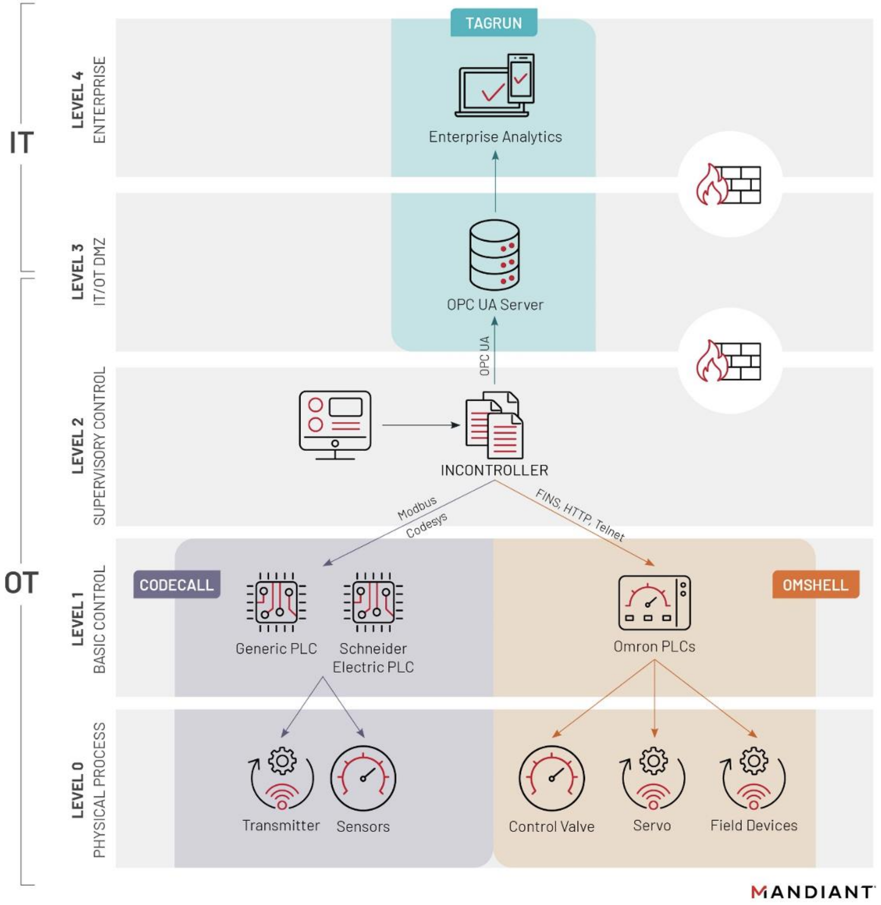
APR 2022

Possibly Russian-linked actors deployed INDUSTROYER. V2 against energy utilities in Ukraine

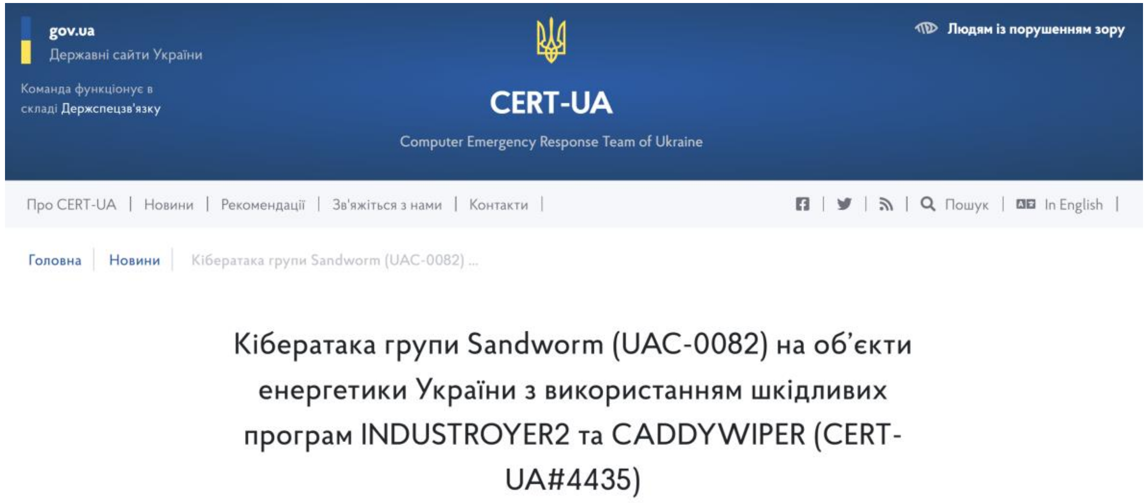
MANDIANT

2022: INCONTROLLER and INDUSTROYERv2

Case 1: INCONTROLLER



Case 2: INDUSTROYER.V2


gov.ua
Державні сайти України

Команда функціонує в складі Держспецзв'язку

CERT-UA
Computer Emergency Response Team of Ukraine

Людям із порушенням зору

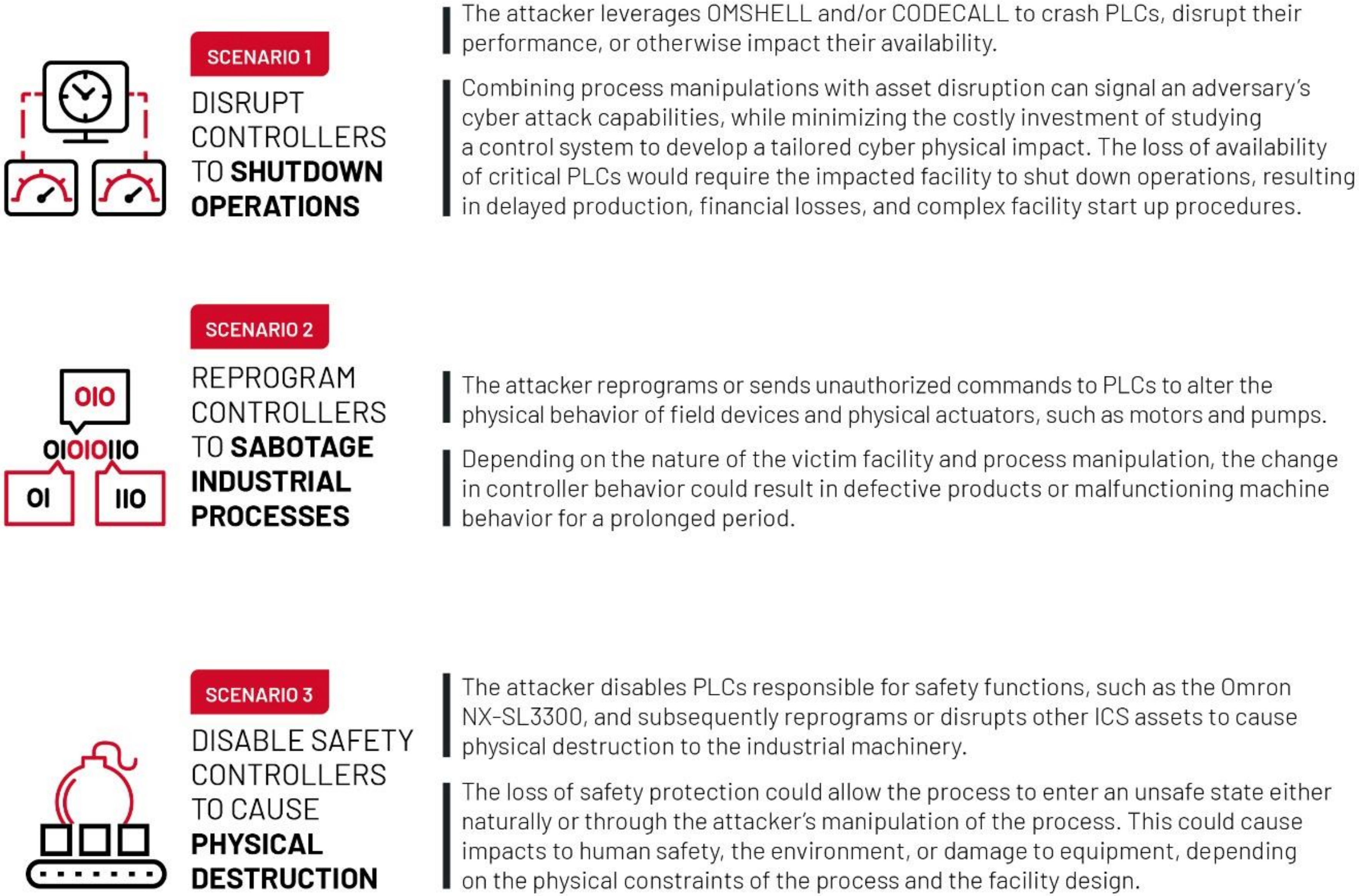
Про CERT-UA | Новини | Рекомендації | Зв'яжіться з нами | Контакти | Пошук | In English |

Головна | Новини | Кібератака групи Sandworm (UAC-0082) ...

Кібератака групи Sandworm (UAC-0082) на об'єкти енергетики України з використанням шкідливих програм INDUSTROYER2 та CADDYWIPER (CERT-UA#4435)

```
192.168.XXX.XXX 2404 2 0 1 1 Example StoppedProcess.exe 1 "Example PATH" 0 1 0 0 1
0 0 8 1104 0 0 0 1 1 1105 0 0 0 1 2 1106 0 0 0 1 3 1107 0 0 0 1 4 1108 0 0 0 1 5
1101 0 0 0 1 6 1102 0 0 0 1 7 1103 0 0 0 1 8
```

Attack Scenarios



SCENARIO 1

DISRUPT CONTROLLERS TO **SHUTDOWN OPERATIONS**

The attacker leverages OMSHELL and/or CODECALL to crash PLCs, disrupt their performance, or otherwise impact their availability.

Combining process manipulations with asset disruption can signal an adversary's cyber attack capabilities, while minimizing the costly investment of studying a control system to develop a tailored cyber physical impact. The loss of availability of critical PLCs would require the impacted facility to shut down operations, resulting in delayed production, financial losses, and complex facility start up procedures.

SCENARIO 2

REPROGRAM CONTROLLERS TO **SABOTAGE INDUSTRIAL PROCESSES**

The attacker reprograms or sends unauthorized commands to PLCs to alter the physical behavior of field devices and physical actuators, such as motors and pumps.

Depending on the nature of the victim facility and process manipulation, the change in controller behavior could result in defective products or malfunctioning machine behavior for a prolonged period.

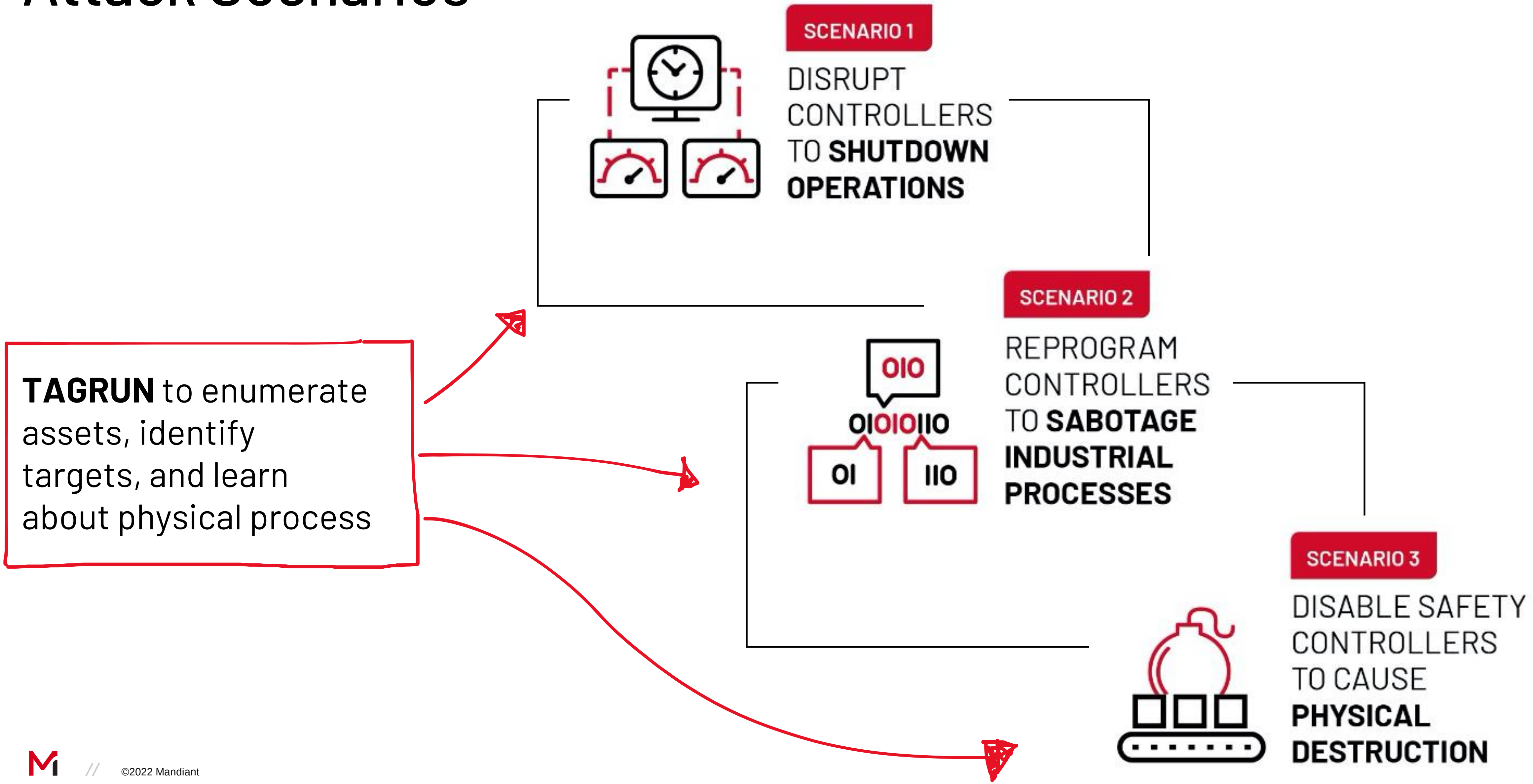
SCENARIO 3

DISABLE SAFETY CONTROLLERS TO CAUSE **PHYSICAL DESTRUCTION**

The attacker disables PLCs responsible for safety functions, such as the Omron NX-SL3300, and subsequently reprograms or disrupts other ICS assets to cause physical destruction to the industrial machinery.

The loss of safety protection could allow the process to enter an unsafe state either naturally or through the attacker's manipulation of the process. This could cause impacts to human safety, the environment, or damage to equipment, depending on the physical constraints of the process and the facility design.

Attack Scenarios



TAGRUN to enumerate assets, identify targets, and learn about physical process

SCENARIO 1

DISRUPT CONTROLLERS TO **SHUTDOWN OPERATIONS**

SCENARIO 2

REPROGRAM CONTROLLERS TO **SABOTAGE INDUSTRIAL PROCESSES**

SCENARIO 3

DISABLE SAFETY CONTROLLERS TO CAUSE **PHYSICAL DESTRUCTION**

Hunting and Detections

Icon by Freepik from Flaticon.

Who Should Take Action?

- Critical risk to organizations with compatible devices.
- Targeted devices are embedded in multiple types of machinery and different industrial sectors.
- Determine if targeted devices are in environments and apply vendor-specific countermeasures.
- Or if you are simply curious and have a good sample…

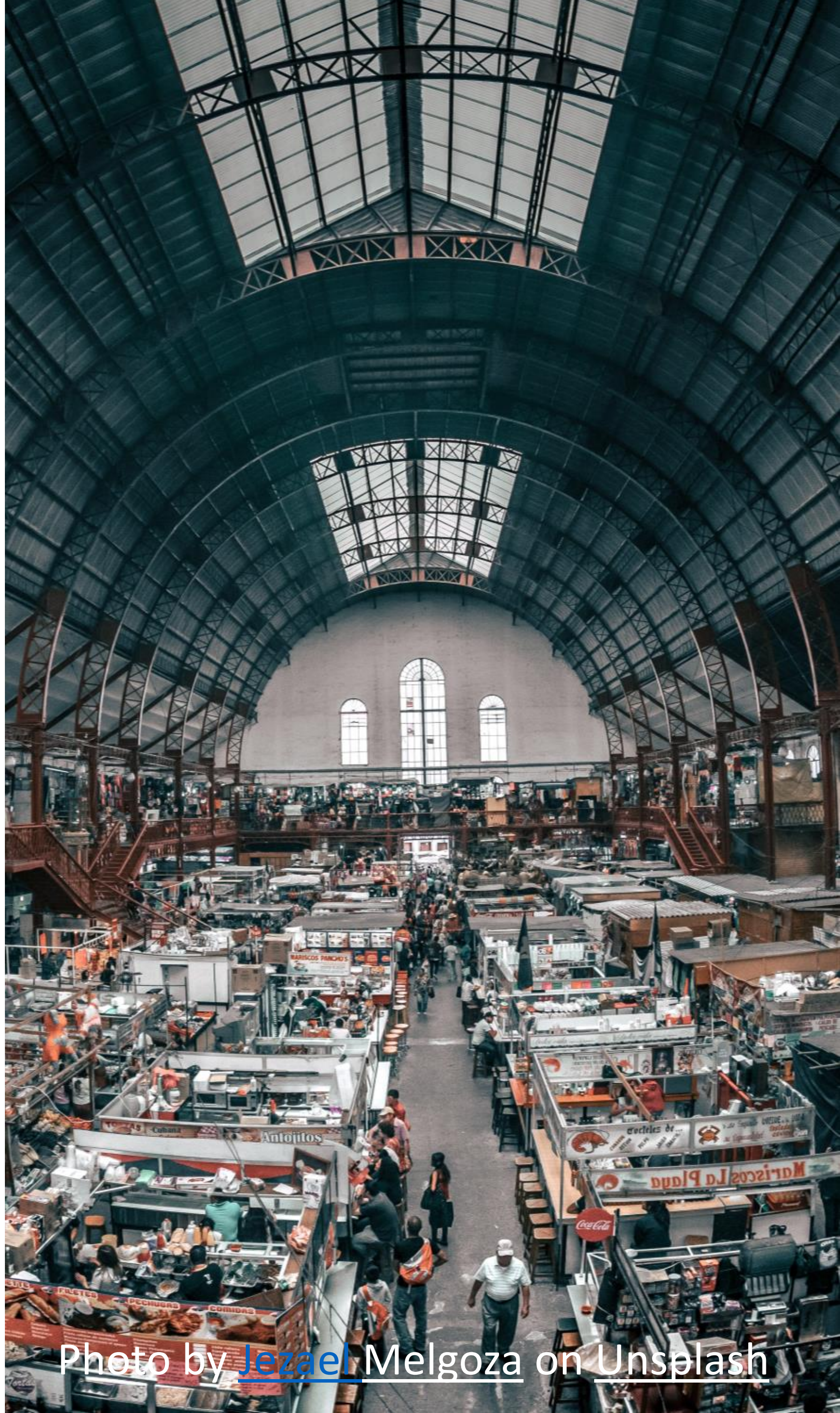


Photo by Jezael Melgoza on Unsplash

Challenges...

- Three separate tools with distinct capabilities.
- Presumably to be leveraged in different logical locations (IT vs. OT).
- Large amount of complex code - written in Python.
- Attacker would almost certainly modify or customize the tool(s).

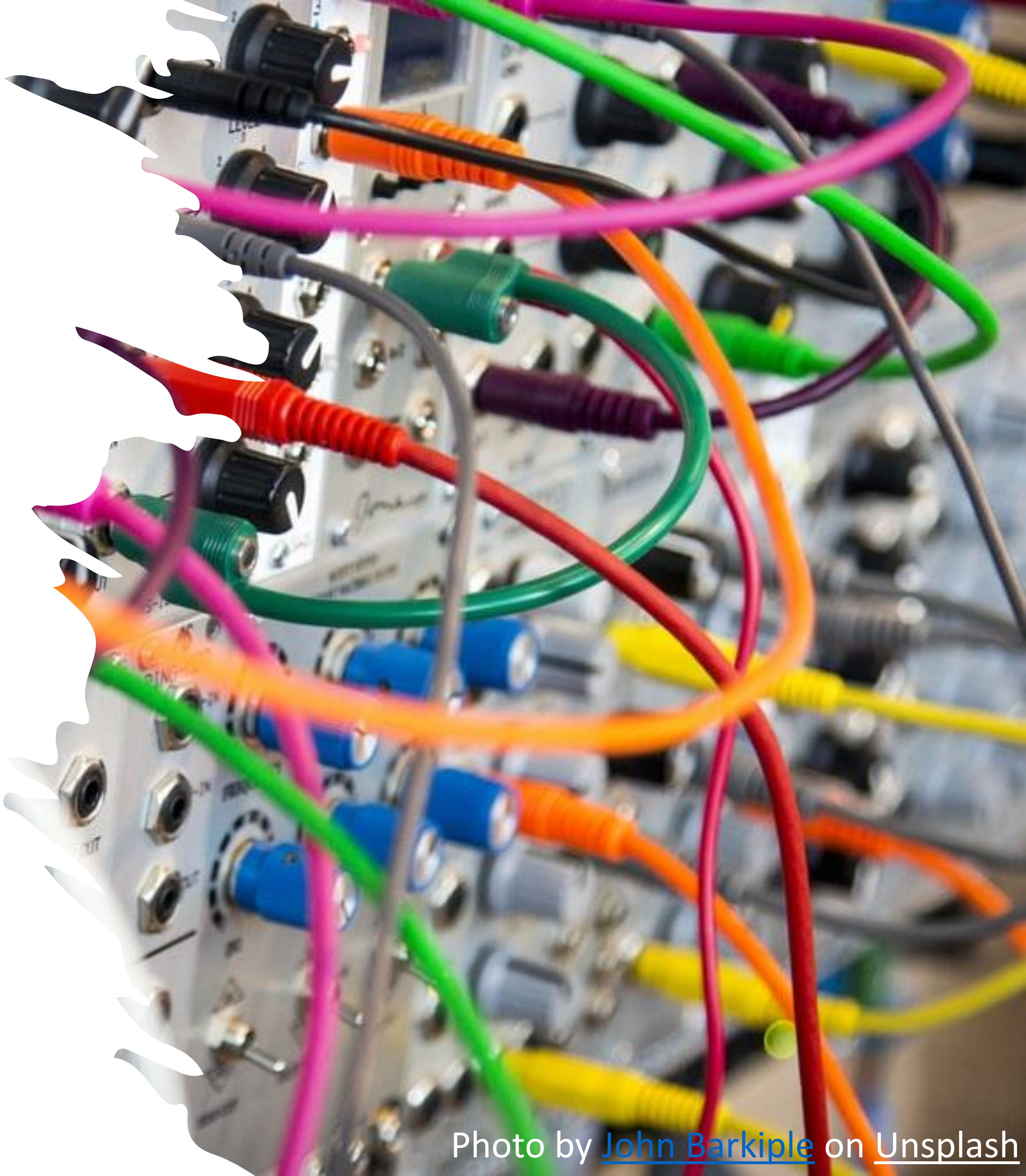


Photo by John Barkiple on Unsplash

What To Do?

Anchor on **behavior-based** hunting and detections

- Each tool has distinct behaviors/targets
- Develop signatures for normal/abnormal behaviors

Focus hunting efforts **on key systems**

- Crown jewels: EWS, HMI, and Historian servers/clients
- Know what "good" looks like for these systems
- Set "tripwires" to catch anomalies…and threats (YARA/Snort)

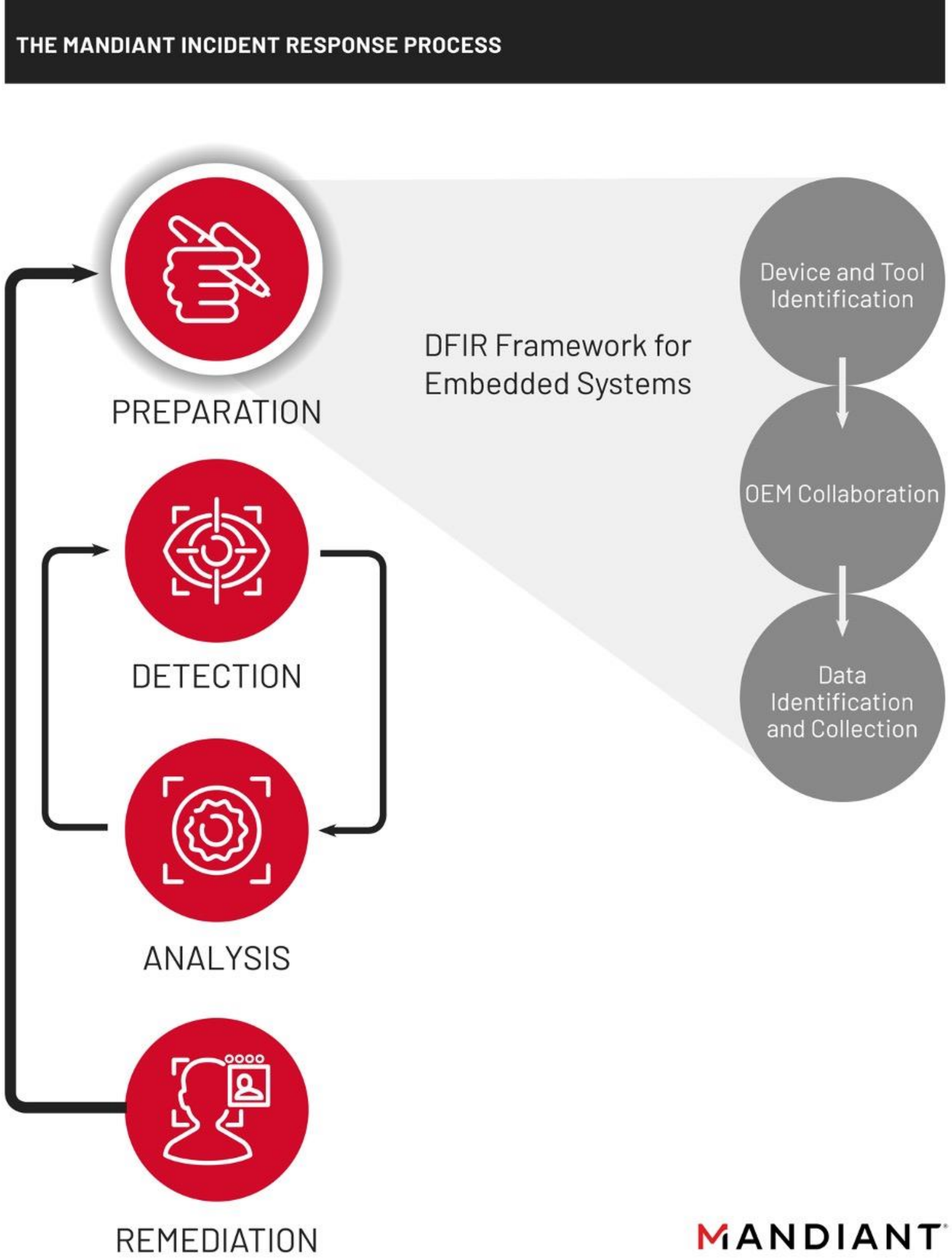
Ensure **collections** in place **for embedded devices**

- Enable logging for embedded devices AND their applications
- Centralize where feasible

"A well-understood ICS is a well-defendable ICS." – Ken

Photo by andré spilborghs on Unsplash

[Mandiant's Digital Forensics and Incident Response Framework for Embedded OT Systems]



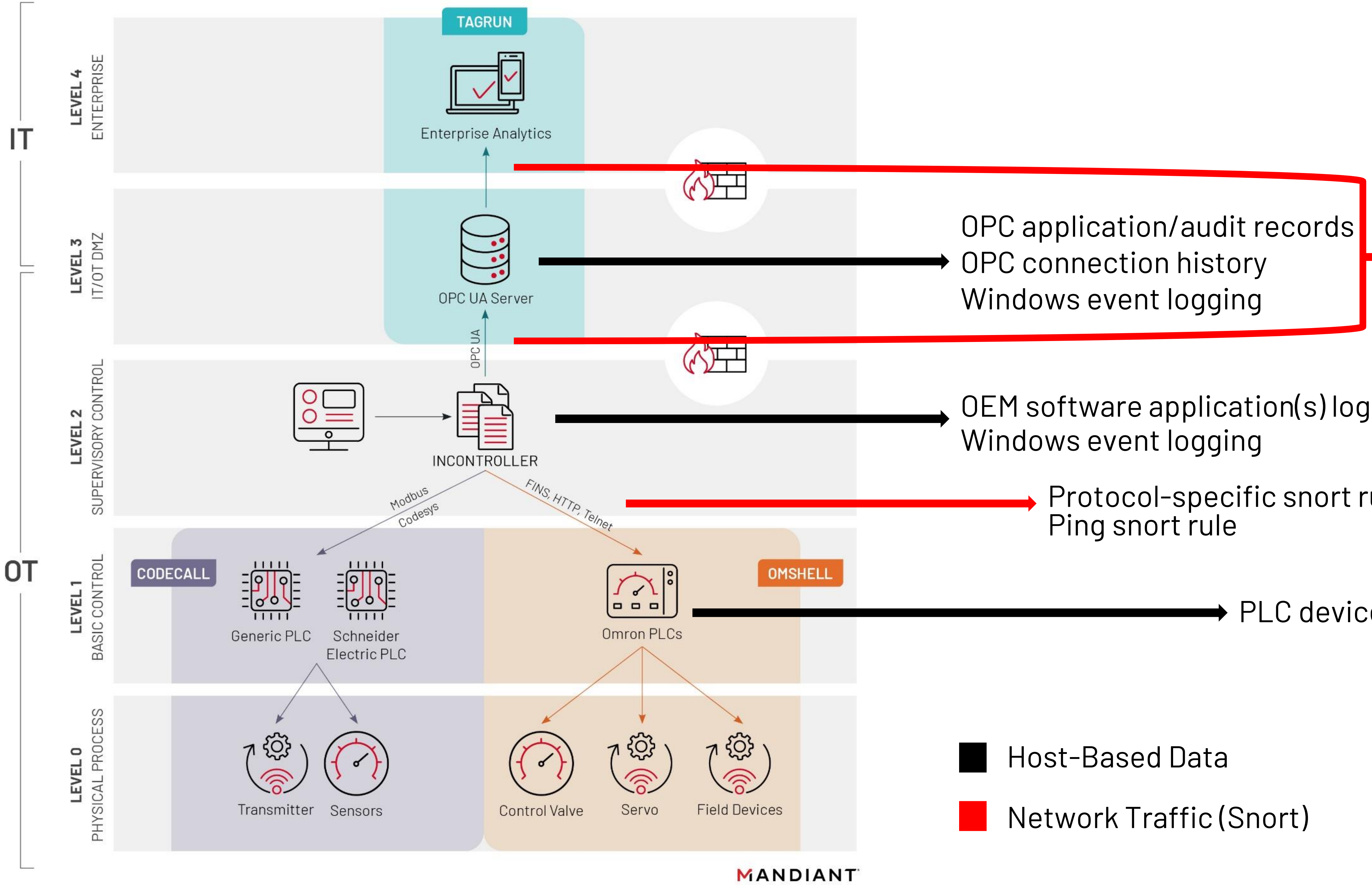
THE MANDIANT INCIDENT RESPONSE PROCESS

PREPARATION
DETECTION
ANALYSIS
REMEDIATION
DFIR Framework for Embedded Systems
Device and Tool Identification
OEM Collaboration
Data Identification and Collection

MANDIANT

Overview for Hunting and Detections

Code Family	Assets	Data	Tools & Methods
TAGRUN	• OPC servers • Clients with access to OPC resources	• OPC application/audit records • OPC connection history • Windows event logging • OPC client/server network traffic	• OPC software applications • Sysmon • YARA / Snort
CODECALL	• Devices with logical access to: • Modbus & Codesys enabled devices • Modicon M251 (TM251MESE) • Modicon M221 Nano PLC • Modicon M258 PLC	• PLC application/device logs • Windows event logging • EWS/HMI <-> PLC network traffic	• OEM software application(s) • Sysmon (event logging) • YARA / Snort
OMSHELL	• Devices with logical access to Omron devices: • NX1P2, NJ501, and R88D-1SN10F-ECT servo drive • Possibly other similar devices from the NJ/NX product lines.	• Omron application/device logs • Windows event logging • EWS/HMI <-> Omron network traffic	• Omron software application(s) • Sysmon (event logging) • YARA / Snort



OPC application/audit records
OPC connection history
Windows event logging

OPC snort rules
Ping snort rule

OEM software application(s) logging
Windows event logging

Protocol-specific snort rules
Ping snort rule

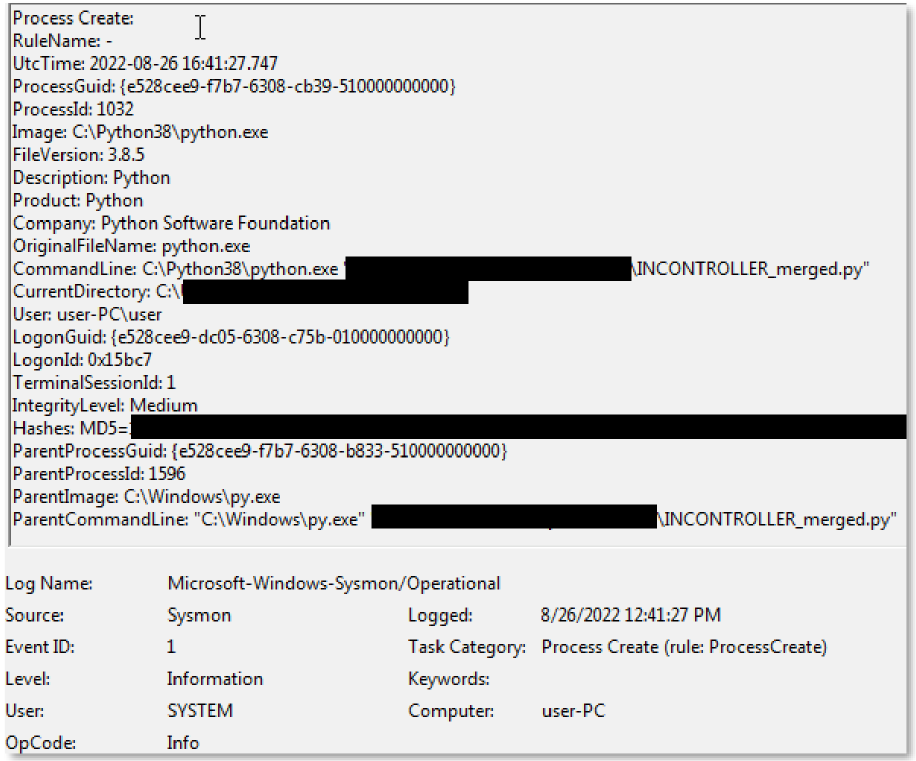
PLC device logs

■ Host-Based Data

🟥 Network Traffic (Snort)

1. ~~Snakes~~ Python on a ~~Plane~~ HMI

- Python script/code spawning and executing.
  - Process creation…Sysmon event ID 1
  - File creation…Sysmon event ID 11
  - Application whitelisting
  - YARA…compiled Python
- PIP/PyPI network traffic.
  - Should you ever see this traffic to/from OT assets?
  - Snort?

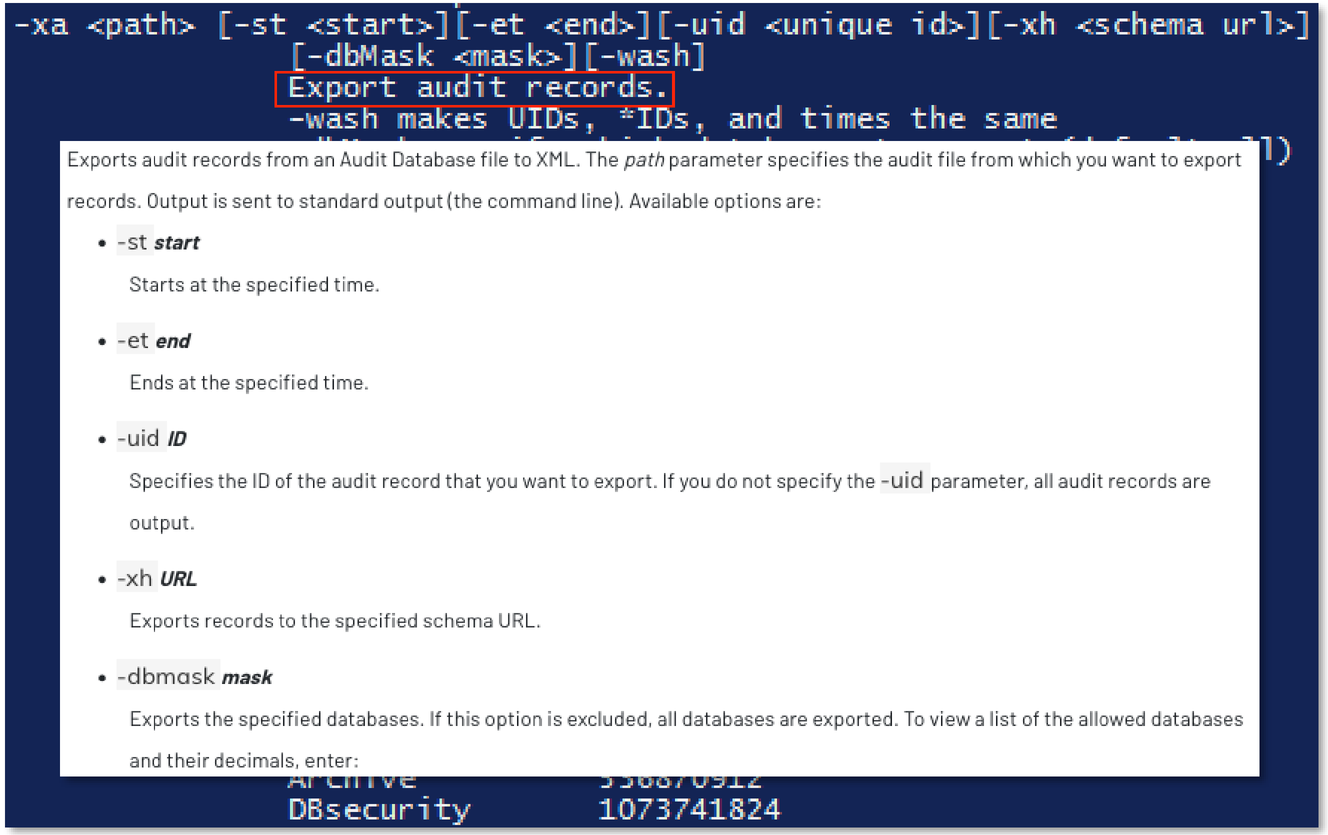


```
Process Create:
RuleName: -
UtcTime: 2022-08-26 16:41:27.747
ProcessGuid: {e528cee9-f7b7-6308-cb39-510000000000}
ProcessId: 1032
Image: C:\Python38\python.exe
FileVersion: 3.8.5
Description: Python
Product: Python
Company: Python Software Foundation
OriginalFileName: python.exe
CommandLine: C:\Python38\python.exe [redacted]\INCONTROLLER_merged.py"
CurrentDirectory: C:\[redacted]
User: user-PC\user
LogonGuid: {e528cee9-dc05-6308-c75b-010000000000}
LogonId: 0x15bc7
TerminalSessionId: 1
IntegrityLevel: Medium
Hashes: MD5=[redacted]
ParentProcessGuid: {e528cee9-f7b7-6308-b833-510000000000}
ParentProcessId: 1596
ParentImage: C:\Windows\py.exe
ParentCommandLine: "C:\Windows\py.exe" [redacted]\INCONTROLLER_merged.py"

Log Name:      Microsoft-Windows-Sysmon/Operational
Source:        Sysmon                      Logged:         8/26/2022 12:41:27 PM
Event ID:      1                           Task Category:  Process Create (rule: ProcessCreate)
Level:         Information                 Keywords:
User:          SYSTEM                      Computer:       user-PC
OpCode:        Info
```

```
alert udp $OT_PROD any -> any 53 (msg:"[OT/ICS Ruleset] - PyPI DNS Request from OT Host.";
content:"|03|www|0b|pypi|03|org|00|"; nocase; sid:1111115; rev:1; classtype:bad-unknown;)
```

2. TAGRUN

- Export/review OPC UA client/server audit records for evidence of:
  - credential brute forcing
  - nefarious certificate usage
  - explicit logins
  - configuration changes
  - changes to OPC tags
- Hunt for anomalous connections to OPC UA endpoints.



```
-xa <path> [-st <start>][-et <end>][-uid <unique id>][-xh <schema url>]
               [-dbMask <mask>][-wash]
               Export audit records.
               -wash makes UIDs, *IDs, and times the same
```

Exports audit records from an Audit Database file to XML. The *path* parameter specifies the audit file from which you want to export records. Output is sent to standard output (the command line). Available options are:

- -st ***start***

  Starts at the specified time.
- -et ***end***

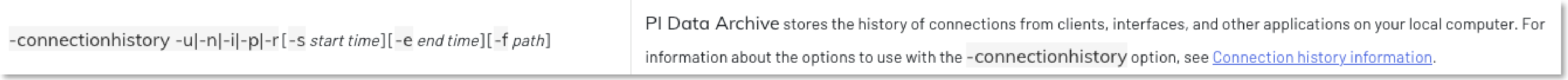
  Ends at the specified time.
- -uid ***ID***

  Specifies the ID of the audit record that you want to export. If you do not specify the -uid parameter, all audit records are output.
- -xh ***URL***

  Exports records to the specified schema URL.
- -dbmask ***mask***

  Exports the specified databases. If this option is excluded, all databases are exported. To view a list of the allowed databases and their decimals, enter:

```
               Archive          536870912
               DBsecurity       1073741824
```

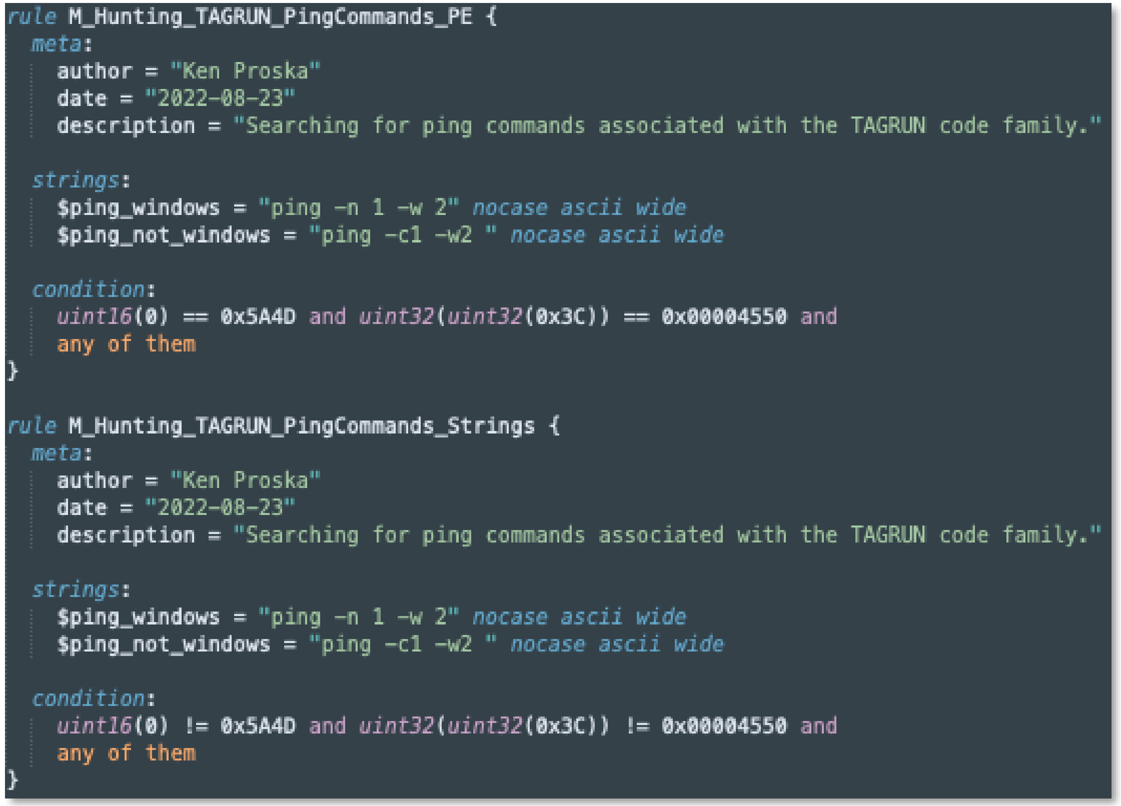


-connectionhistory -u|-n|-i|-p|-r [-s *start time*][-e *end time*][-f *path*]	PI Data Archive stores the history of connections from clients, interfaces, and other applications on your local computer. For information about the options to use with the -connectionhistory option, see Connection history information.

2. TAGRUN

- Search for and investigate TAGRUN ping command execution.
  - Windows OS: ping -n 1 -w 2 <IP>
  - Non-Windows OS: ping -c1 -w2 <IP>
  - Ping.exe....Sysmon event ID 1
- Review OT network traffic for evidence of pingsweep activity.
  - SNORT / IDS rules?

alert **icmp** any any **<> $OT_PROD** any (msg:"[OT/ICS Ruleset] - Suspicious ICMP/PING Traffic To/From OT Host."; sid:1111111; rev:1; classtype:icmp-event;)



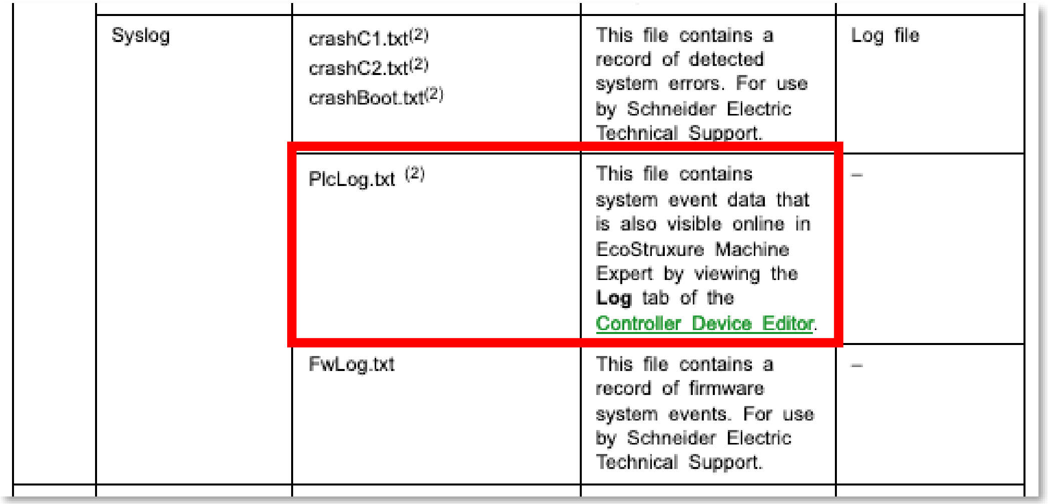
```
rule M_Hunting_TAGRUN_PingCommands_PE {
  meta:
    author = "Ken Proska"
    date = "2022-08-23"
    description = "Searching for ping commands associated with the TAGRUN code family."

  strings:
    $ping_windows = "ping -n 1 -w 2" nocase ascii wide
    $ping_not_windows = "ping -c1 -w2 " nocase ascii wide

  condition:
    uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550 and
    any of them
}

rule M_Hunting_TAGRUN_PingCommands_Strings {
  meta:
    author = "Ken Proska"
    date = "2022-08-23"
    description = "Searching for ping commands associated with the TAGRUN code family."

  strings:
    $ping_windows = "ping -n 1 -w 2" nocase ascii wide
    $ping_not_windows = "ping -c1 -w2 " nocase ascii wide

  condition:
    uint16(0) != 0x5A4D and uint32(uint32(0x3C)) != 0x00004550 and
    any of them
}
```

3. CODECALL

Collect, aggregate, and review embedded devices logs

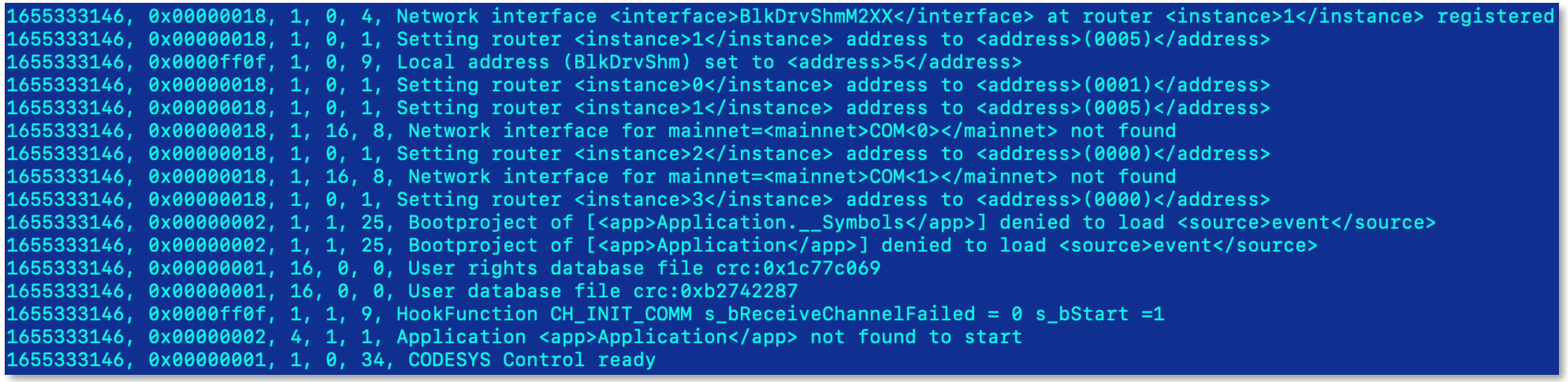
- Modicon M251 (TM251MESE) offers syslog

Work with operators/engineers/OEMs (who know how these devices work) to understand embedded devices' logs…



	Syslog	crashC1.txt(2)
		crashC2.txt(2)
		crashBoot.txt(2)
			This file contains a record of detected system errors. For use by Schneider Electric Technical Support.	Log file

		PlcLog.txt (2)	This file contains system event data that is also visible online in EcoStruxure Machine Expert by viewing the **Log** tab of the Controller Device Editor.	–
		FwLog.txt	This file contains a record of firmware system events. For use by Schneider Electric Technical Support.	–



```
1655333146, 0x00000018, 1, 0, 4, Network interface <interface>BlkDrvShmM2XX</interface> at router <instance>1</instance> registered
1655333146, 0x00000018, 1, 0, 1, Setting router <instance>1</instance> address to <address>(0005)</address>
1655333146, 0x0000ff0f, 1, 0, 9, Local address (BlkDrvShm) set to <address>5</address>
1655333146, 0x00000018, 1, 0, 1, Setting router <instance>0</instance> address to <address>(0001)</address>
1655333146, 0x00000018, 1, 0, 1, Setting router <instance>1</instance> address to <address>(0005)</address>
1655333146, 0x00000018, 1, 16, 8, Network interface for mainnet=<mainnet>COM<0></mainnet> not found
1655333146, 0x00000018, 1, 0, 1, Setting router <instance>2</instance> address to <address>(0000)</address>
1655333146, 0x00000018, 1, 16, 8, Network interface for mainnet=<mainnet>COM<1></mainnet> not found
1655333146, 0x00000018, 1, 0, 1, Setting router <instance>3</instance> address to <address>(0000)</address>
1655333146, 0x00000002, 1, 1, 25, Bootproject of [<app>Application.__Symbols</app>] denied to load <source>event</source>
1655333146, 0x00000002, 1, 1, 25, Bootproject of [<app>Application</app>] denied to load <source>event</source>
1655333146, 0x00000001, 16, 0, 0, User rights database file crc:0x1c77c069
1655333146, 0x00000001, 16, 0, 0, User database file crc:0xb2742287
1655333146, 0x0000ff0f, 1, 1, 9, HookFunction CH_INIT_COMM s_bReceiveChannelFailed = 0 s_bStart =1
1655333146, 0x00000002, 4, 1, 1, Application <app>Application</app> not found to start
1655333146, 0x00000001, 1, 0, 34, CODESYS Control ready
```

3. CODECALL

Develop Snort rule(s) to detect OT/ICS protocol activity from unauthorized devices

- Modbus over TCP on port 502
- "Machine Expert" protocol over UDP ports 1740, 1741, 1742 and 1743

```
alert udp !$CODESYS_CLIENTS any -> $CODESYS_SERVERS [1740,1741,1742,1743] (msg:"[OT/ICS Ruleset] - Unauthorized Codesys UDP Traffic."; sid:1111112; rev:1; classtype:bad-unknown;)
```

Develop Snort rules for risky/nefarious legitimate protocol functions

```
alert tcp !$MODBUS_CLIENTS any -> $MODBUS_SERVERS 502 (msg:"[OT/ICS Ruleset] - Unauthorized Modbus TCP Write Request."; flow:from_client,established; content:"|00 00|"; offset:2; depth:2; pcre:"/[Ss]{3}(x05|x06|x0F|x10|x15|x16)/iAR"; sid:1111113; rev:1; classtype:bad-unknown;)
```

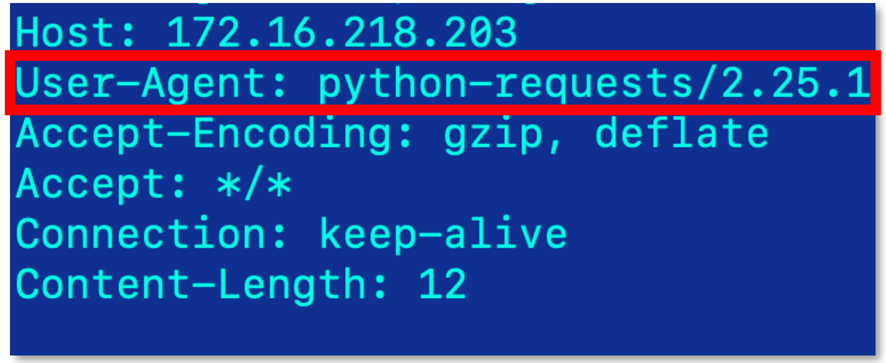
4. OMSHELL

Develop Snort signatures for protocols used by OMSHELL:

- udp://<omron_device>:9600 (omron FINS)
- http://<omron_device>:80 (primary protocol used by the framework)
- tcp://<omron_device>:23 (telnet)
- Undocumented ports communicating from OMRON servers

Ping sweep (same as TAGRUN).

POST:



```
Host: 172.16.218.203
User-Agent: python-requests/2.25.1
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Content-Length: 12
```

```
alert tcp any any -> $OMRON_SERVERS 80 (msg:"[OT/ICS Ruleset] - OMSHELL “python-requests” HTTP User-Agent."; content:"User-Agent: python-requests"; within:50; fast_pattern; sid:1111114; rev:1; classtype:web-application-activity;)
```

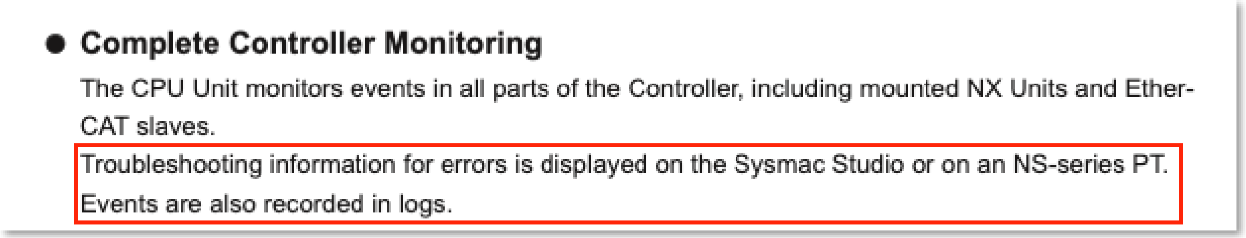
4. OMSHELL

FINS traffic

- Only used in identification…Snort?

Review Omron device logs for evidence of:

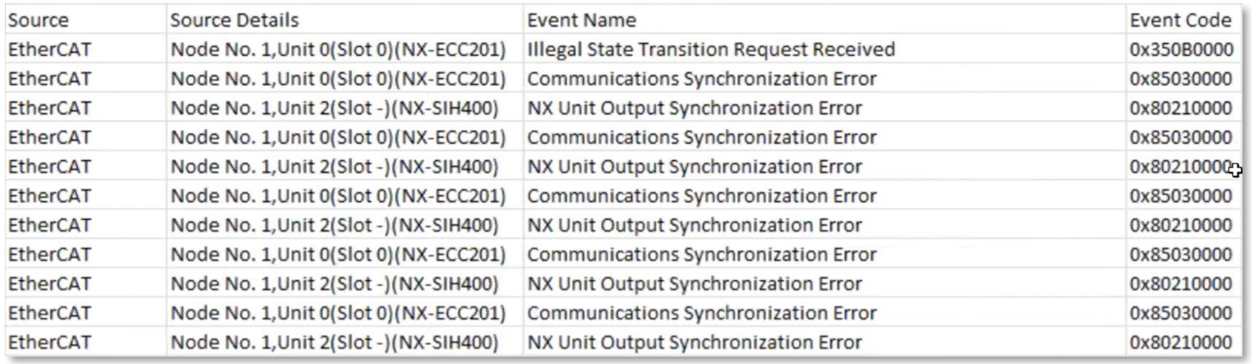
- Activation of Telnet daemon.
- Unauthorized Telnet connection attempts and use of default credentials.
- Wiping PROGRAM memory and device resets.
- Unauthorized changes in device configuration and command execution.
- Connections to devices outside environment norms.
- Downloaded/uploaded files



- **Complete Controller Monitoring**

  The CPU Unit monitors events in all parts of the Controller, including mounted NX Units and EtherCAT slaves.

  Troubleshooting information for errors is displayed on the Sysmac Studio or on an NS-series PT. Events are also recorded in logs.



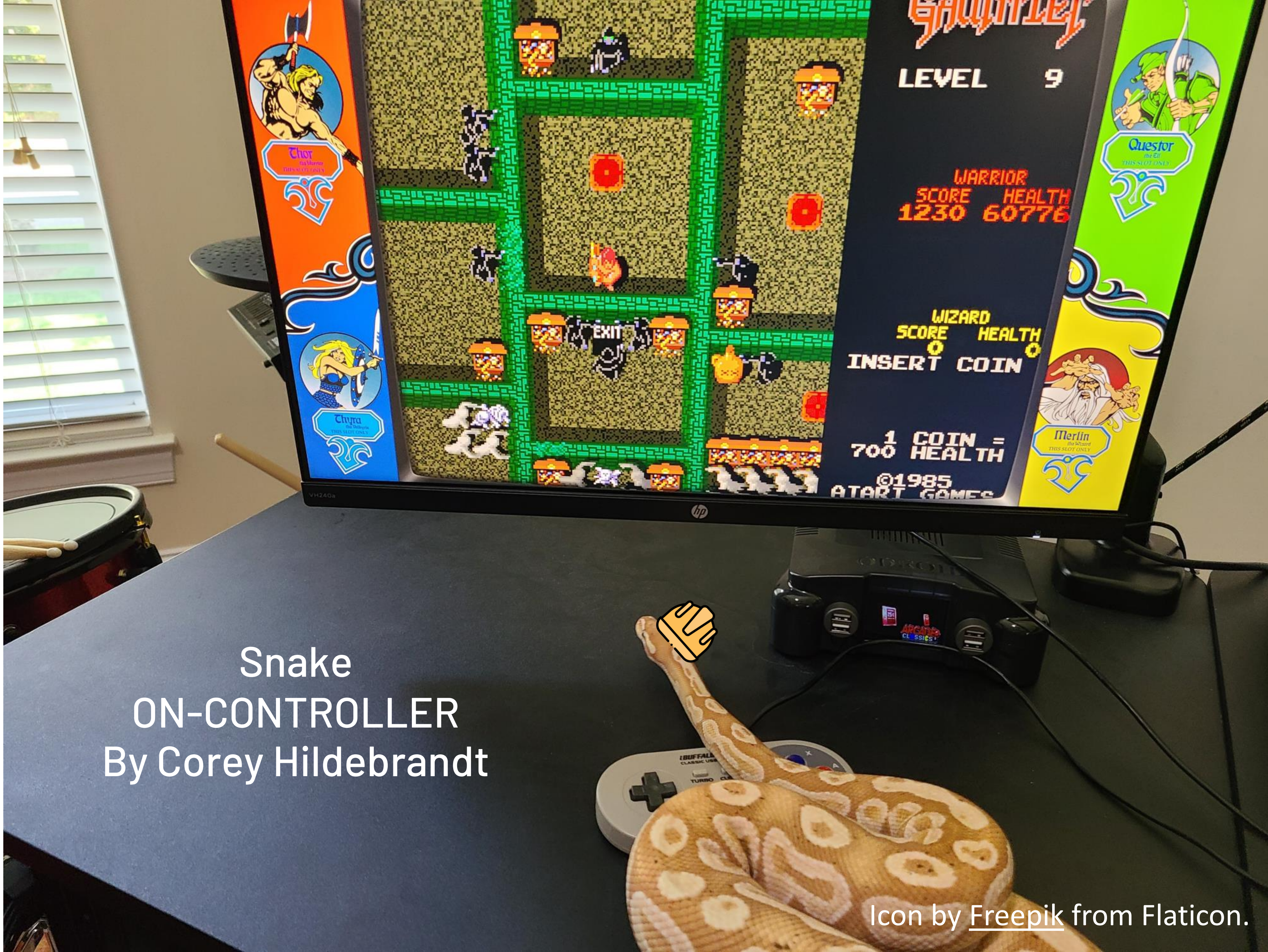
Source	Source Details	Event Name	Event Code
EtherCAT	Node No. 1,Unit 0(Slot 0)(NX-ECC201)	Illegal State Transition Request Received	0x350B0000
EtherCAT	Node No. 1,Unit 0(Slot 0)(NX-ECC201)	Communications Synchronization Error	0x85030000
EtherCAT	Node No. 1,Unit 2(Slot -)(NX-SIH400)	NX Unit Output Synchronization Error	0x80210000
EtherCAT	Node No. 1,Unit 0(Slot 0)(NX-ECC201)	Communications Synchronization Error	0x85030000
EtherCAT	Node No. 1,Unit 2(Slot -)(NX-SIH400)	NX Unit Output Synchronization Error	0x80210000
EtherCAT	Node No. 1,Unit 0(Slot 0)(NX-ECC201)	Communications Synchronization Error	0x85030000
EtherCAT	Node No. 1,Unit 2(Slot -)(NX-SIH400)	NX Unit Output Synchronization Error	0x80210000
EtherCAT	Node No. 1,Unit 0(Slot 0)(NX-ECC201)	Communications Synchronization Error	0x85030000
EtherCAT	Node No. 1,Unit 2(Slot -)(NX-SIH400)	NX Unit Output Synchronization Error	0x80210000
EtherCAT	Node No. 1,Unit 0(Slot 0)(NX-ECC201)	Communications Synchronization Error	0x85030000
EtherCAT	Node No. 1,Unit 2(Slot -)(NX-SIH400)	NX Unit Output Synchronization Error	0x80210000

General Mitigations

General Mitigations

- Segmentation of IT-OT networks to prevent attackers pivoting into OT environments.
- Enable logging for OPC UA applications, Schneider Electric and Omron PLC devices. (Aggregate logs to central location where applicable.)
- Allow listing primary/subordinate devices, behavior patterns, and commands to establish approved baselines and detect anomalies.
- Review vendor recommendations:
  - Recommended Cybersecurity Best Practices White paper | Schneider Electric
  - Cybersecurity Guidelines for EcoStruxure Machine Expert, Modicon and PacDrive Controllers and Associated Equipment, User Guide | Schneider Electric
  - Vulnerabilities in Omron CS and CJ series CPU PLCs
  - ICS Advisory (ICSA-19-346-02) - Omron PLC CJ and CS Series

Q & A



Snake
ON-CONTROLLER
By Corey Hildebrandt

Icon by Freepik from Flaticon.

MANDIANT®

YOUR CYBERSECURITY ADVANTAGE