# Central Security Incident Management Platform in Industry 4.0 with Threat Intelligence Interface

S.D. Cakmakci, K.-O. Detken (DECOIT®)

S. Catalkaya, E. Eren (University of Applied Sciences Bremen)

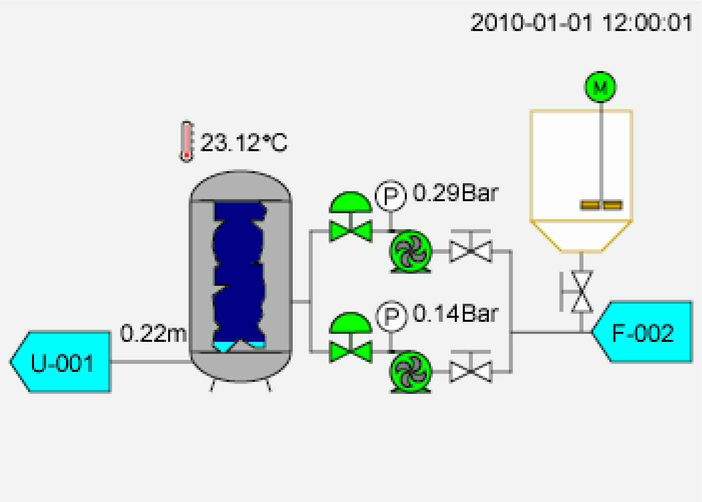
Dr. Salva Daneshgadeh Cakmakcı
DECOIT® GmbH & Co. KG
Fahrenheitstraße 9
D-28359 Bremen
https://www.decoit.de
daneshgadeh@decoit.de

# Agenda

- Industrial Control Systems (ICS)
- Research Questions
- ZenSIM 4.0 Project
- Common Security Advisory Framework (CSAF)
- Proposed System Architecture
- Attack Scenario
- Communication of Indicator of Compromise (IoC)
- Conclusions

# Industrial Control Systems (ICS)

- Information system used to control industrial processes such as manufacturing, production and distribution:
  - Supervisory Control and Data Acquisition (SCADA) system
  - Programmable Logic Controllers (PLC)
  - Human-Machine Interface (HMI)
  - Intelligent Electronic Devices (IED)



SCADA standard animation, Source: Wikipedia

# Vulnerability Surfaces

- Existence of outdated and unpatched assets in ICS environments.
- Communication over insecure ICS protocols such as PROFINET or Modbus (mostly in clear text).
- Direct access of ICS environments to internet via VNC or RDP protocols for remote maintenance services.
- Lateral movement from IT network.

# Attack history

- Stuxnet (2010)-Iran nuclear facility: (a malicious worm) Siemens Step7 software running on Windows systems
- Industroyer/CrashOverride malware(2016)-Ukraine's power grid
- Triton/Trisis (2017)- petrochemical plant in the Middle East, specifically Saudi Arabia: Triton malware targets Triconex Safety Instrumented System (SIS) controllers manufactured by Schneider Electric

# The project

ZenSIM Industrie 4.0

- ZenSIM4.0 : Central Security Incident Management for Small and Medium Enterprises in Industry 4.0
  - https://zensim-project.de
  - Cooperation project within the German BMBF
  - October 2021 - September 2024
- Partners:
  - DECOIT® GmbH & Co. KG: coordinator, developer, and SIEM specialist
  - University of Applied Sciences of Bremen: research and simulating specialist
  - VDE CERT: Association for Electrical, Electronic & Information Technologies. CSAF aggregator role in project

Federal Ministry
of Education
and Research

# Research questions

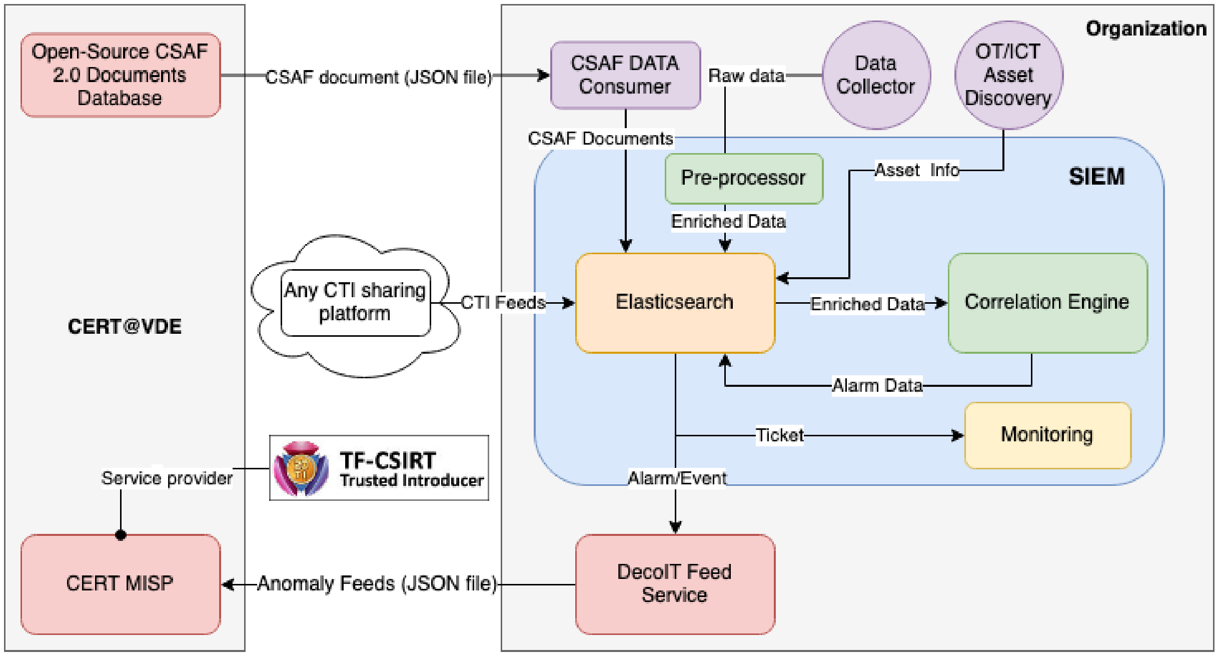
- Can SIEM protect ICS environments as well?
- How can a SIEM safely identify assets in the ICS environments?
- How can a SIEM protect the ICS environment against known vulnerabilities of assets and implement countermeasures?
- How can a SIEM produce and share information about detected attacks in the ICS environments?

# Focus of ZenSIM Industrie 4.0

- **Security Incident Management:**
  - Identifying, managing, recording and analyzing security threats or incidents in the product and production environment
- **Central Plattform:**
  - ZenSIM 4.0 develops a special central platform for SMEs operating in Industry 4.0 to support security incident management.

# ZenSIM 4.0 Framework

- ScanBox (SIEM)
- Asset discoverer
- Data collector: both It and OT protocols
- Common Security Advisory Framework (CSAF) consumer
- Correlation Engine

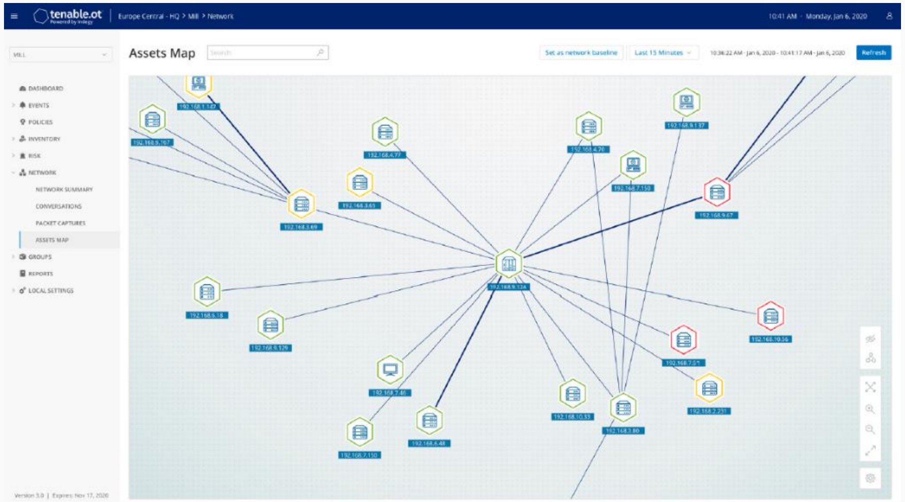


# Common Security Advisory Framework (CSAF)

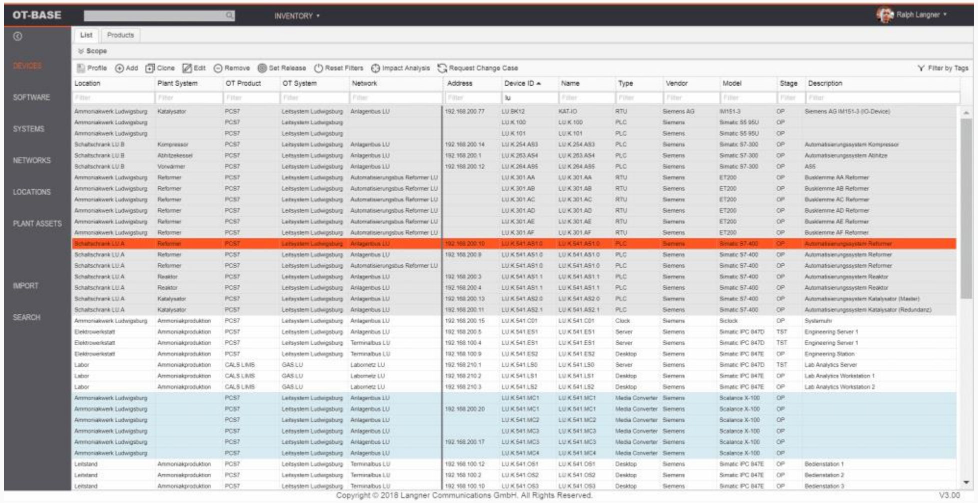
- Is a language to exchange Security Advisories.
- Is a human-readable security information (security advisories).
- Is a structured information on
  - Product
  - Vulnerabilities
  - The status of impact
  - Remediation
- Is published by the manufacturers or the coordinating bodies.
- CSAF aggregator: is an entity to collect and aggregate CSAF documents from trusted providers and provide a single point of contact for end users.

# Asset Discoverer

- Scan the ICS network and discover assets
- Create a topology of network
- Send asset information to the SIEM for storing



Solution overview: Tenable.ot Asset Inventory
(Source: de.tenable.com)



| Location | Plant System | OT Product | OT System | Network | Address | Device ID ▲ | Name | Type | Vendor | Model | Stage | Description |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Filter | Filter | Filter | Filter | Filter | Filter | lu | Filter | Filter | Filter | Filter | Filter | Filter |
| Ammoniakwerk Ludwigsburg | Katalysator | PCS7 | Leitsystem Ludwigsburg | Anlagenbus LU | 192.168.200.77 | LU.BK12 | KAT-IO | RTU | Siemens AG | IM151-3 | OP | Siemens AG IM151-3 (IO-Device) |
| Ammoniakwerk Ludwigsburg |  | PCS7 | Leitsystem Ludwigsburg |  |  | LU.K.100 | LU.K.100 | PLC | Siemens | Simatic S5 95U | OP |  |
| Ammoniakwerk Ludwigsburg |  | PCS7 | Leitsystem Ludwigsburg |  |  | LU.K.101 | LU.K.101 | PLC | Siemens | Simatic S5 95U | OP |  |
| Schaltschrank LU.B | Kompressor | PCS7 | Leitsystem Ludwigsburg | Anlagenbus LU | 192.168.200.14 | LU.K.254.AS3 | LU.K.254.AS3 | PLC | Siemens | Simatic S7-300 | OP | Automatisierungssystem Kompressor |
| Schaltschrank LU.B | Abhitzekessel | PCS7 | Leitsystem Ludwigsburg | Anlagenbus LU | 192.168.200.1 | LU.K.263.AS4 | LU.K.263.AS4 | PLC | Siemens | Simatic S7-300 | OP | Automatisierungssystem Abhitze |
| Schaltschrank LU.B | Vorwärmer | PCS7 | Leitsystem Ludwigsburg | Anlagenbus LU | 192.168.200.12 | LU.K.264.AS5 | LU.K.264.AS5 | PLC | Siemens | Simatic S7-300 | OP | AS5 |
| Ammoniakwerk Ludwigsburg | Reformer | PCS7 | Leitsystem Ludwigsburg | Automatisierungsbus Reformer LU |  | LU.K.301.AA | LU.K.301.AA | RTU | Siemens | ET200 | OP | Busklemme AA Reformer |
| Ammoniakwerk Ludwigsburg | Reformer | PCS7 | Leitsystem Ludwigsburg | Automatisierungsbus Reformer LU |  | LU.K.301.AB | LU.K.301.AB | RTU | Siemens | ET200 | OP | Busklemme AB Reformer |
| Ammoniakwerk Ludwigsburg | Reformer | PCS7 | Leitsystem Ludwigsburg | Automatisierungsbus Reformer LU |  | LU.K.301.AC | LU.K.301.AC | RTU | Siemens | ET200 | OP | Busklemme AC Reformer |
| Ammoniakwerk Ludwigsburg | Reformer | PCS7 | Leitsystem Ludwigsburg | Automatisierungsbus Reformer LU |  | LU.K.301.AD | LU.K.301.AD | RTU | Siemens | ET200 | OP | Busklemme AD Reformer |
| Ammoniakwerk Ludwigsburg | Reformer | PCS7 | Leitsystem Ludwigsburg | Automatisierungsbus Reformer LU |  | LU.K.301.AE | LU.K.301.AE | RTU | Siemens | ET200 | OP | Busklemme AE Reformer |
| Ammoniakwerk Ludwigsburg | Reformer | PCS7 | Leitsystem Ludwigsburg | Automatisierungsbus Reformer LU |  | LU.K.301.AF | LU.K.301.AF | RTU | Siemens | ET200 | OP | Busklemme AF Reformer |
| Schaltschrank LU.A | Reformer | PCS7 | Leitsystem Ludwigsburg | Anlagenbus LU | 192.168.200.10 | LU.K.541.AS1.0 | LU.K.541.AS1.0 | PLC | Siemens | Simatic S7-400 | OP | Automatisierungssystem Reformer |
| Schaltschrank LU.A | Reformer | PCS7 | Leitsystem Ludwigsburg | Anlagenbus LU | 192.168.200.9 | LU.K.541.AS1.0 | LU.K.541.AS1.0 | PLC | Siemens | Simatic S7-400 | OP | Automatisierungssystem Reformer |
| Schaltschrank LU.A | Reformer | PCS7 | Leitsystem Ludwigsburg | Automatisierungsbus Reformer LU |  | LU.K.541.AS1.0 | LU.K.541.AS1.0 | PLC | Siemens | Simatic S7-400 | OP | Automatisierungssystem Reformer |
| Schaltschrank LU.A | Reaktor | PCS7 | Leitsystem Ludwigsburg | Anlagenbus LU | 192.168.200.3 | LU.K.541.AS1.1 | LU.K.541.AS1.1 | PLC | Siemens | Simatic S7-400 | OP | Automatisierungssystem Reaktor |
| Schaltschrank LU.A | Reaktor | PCS7 | Leitsystem Ludwigsburg | Anlagenbus LU | 192.168.200.4 | LU.K.541.AS1.1 | LU.K.541.AS1.1 | PLC | Siemens | Simatic S7-400 | OP | Automatisierungssystem Reaktor |
| Schaltschrank LU.A | Katalysator | PCS7 | Leitsystem Ludwigsburg | Anlagenbus LU | 192.168.200.13 | LU.K.541.AS2.0 | LU.K.541.AS2.0 | PLC | Siemens | Simatic S7-400 | OP | Automatisierungssystem Katalysator (Master) |
| Schaltschrank LU.A | Katalysator | PCS7 | Leitsystem Ludwigsburg | Anlagenbus LU | 192.168.200.11 | LU.K.541.AS2.1 | LU.K.541.AS2.1 | PLC | Siemens | Simatic S7-400 | OP | Automatisierungssystem Katalysator (Redundanz) |
| Ammoniakwerk Ludwigsburg | Ammoniakproduktion | PCS7 | Leitsystem Ludwigsburg | Anlagenbus LU | 192.168.200.15 | LU.K.541.C01 | LU.K.541.C01 | Clock | Siemens | Siclock | OP | Systemuhr |
| Elektrowerkstatt | Ammoniakproduktion | PCS7 | Leitsystem Ludwigsburg | Anlagenbus LU | 192.168.200.5 | LU.K.541.ES1 | LU.K.541.ES1 | Server | Siemens | Simatic IPC 847D | TST | Engineering Server 1 |
| Elektrowerkstatt | Ammoniakproduktion | PCS7 | Leitsystem Ludwigsburg | Terminalbus LU | 192.168.100.4 | LU.K.541.ES1 | LU.K.541.ES1 | Server | Siemens | Simatic IPC 847D | TST | Engineering Server 1 |
| Elektrowerkstatt | Ammoniakproduktion | PCS7 | Leitsystem Ludwigsburg | Terminalbus LU | 192.168.100.9 | LU.K.541.ES2 | LU.K.541.ES2 | Desktop | Siemens | Simatic IPC 847E | OP | Engineering Station |
| Labor | Ammoniakproduktion | CALS LIMS | GAS.LU | Labornetz LU | 192.168.210.1 | LU.K.541.LS0 | LU.K.541.LS0 | Server | Siemens | Simatic IPC 847D | TST | Lab Analytics Server |
| Labor | Ammoniakproduktion | CALS LIMS | GAS.LU | Labornetz LU | 192.168.210.2 | LU.K.541.LS1 | LU.K.541.LS1 | Desktop | Siemens | Simatic IPC 847E | OP | Lab Analytics Workstation 1 |
| Labor | Ammoniakproduktion | CALS LIMS | GAS.LU | Labornetz LU | 192.168.210.3 | LU.K.541.LS2 | LU.K.541.LS2 | Desktop | Siemens | Simatic IPC 847E | OP | Lab Analytics Workstation 2 |
| Ammoniakwerk Ludwigsburg |  | PCS7 | Leitsystem Ludwigsburg | Anlagenbus LU |  | LU.K.541.MC1 | LU.K.541.MC1 | Media Converter | Siemens | Scalance X-100 | OP |  |
| Ammoniakwerk Ludwigsburg |  | PCS7 | Leitsystem Ludwigsburg | Anlagenbus LU | 192.168.200.20 | LU.K.541.MC1 | LU.K.541.MC1 | Media Converter | Siemens | Scalance X-100 | OP |  |
| Ammoniakwerk Ludwigsburg |  | PCS7 | Leitsystem Ludwigsburg | Anlagenbus LU |  | LU.K.541.MC2 | LU.K.541.MC2 | Media Converter | Siemens | Scalance X-100 | OP |  |
| Ammoniakwerk Ludwigsburg |  | PCS7 | Leitsystem Ludwigsburg | Anlagenbus LU |  | LU.K.541.MC3 | LU.K.541.MC3 | Media Converter | Siemens | Scalance X-100 | OP |  |
| Ammoniakwerk Ludwigsburg |  | PCS7 | Leitsystem Ludwigsburg | Anlagenbus LU | 192.168.200.17 | LU.K.541.MC3 | LU.K.541.MC3 | Media Converter | Siemens | Scalance X-100 | OP |  |
| Ammoniakwerk Ludwigsburg |  | PCS7 | Leitsystem Ludwigsburg | Anlagenbus LU |  | LU.K.541.MC4 | LU.K.541.MC4 | Media Converter | Siemens | Scalance X-100 | OP |  |
| Leitstand | Ammoniakproduktion | PCS7 | Leitsystem Ludwigsburg | Terminalbus LU | 192.168.100.12 | LU.K.541.OS1 | LU.K.541.OS1 | Desktop | Siemens | Simatic IPC 847E | OP | Bedienstation 1 |
| Leitstand | Ammoniakproduktion | PCS7 | Leitsystem Ludwigsburg | Terminalbus LU | 192.168.100.2 | LU.K.541.OS2 | LU.K.541.OS2 | Desktop | Siemens | Simatic IPC 847E | OP | Bedienstation 2 |
| Leitstand | Ammoniakproduktion | PCS7 | Leitsystem Ludwigsburg | Terminalbus LU | 192.168.100.10 | LU.K.541.OS3 | LU.K.541.OS3 | Desktop | Siemens | Simatic IPC 847E | OP | Bedienstation 3 |

Copyright © 2018 Langner Communications GmbH. All Rights Reserved. V3.00

Device inventory in the OT-BASE OT asset management system
(Source: https://www.langner.com)

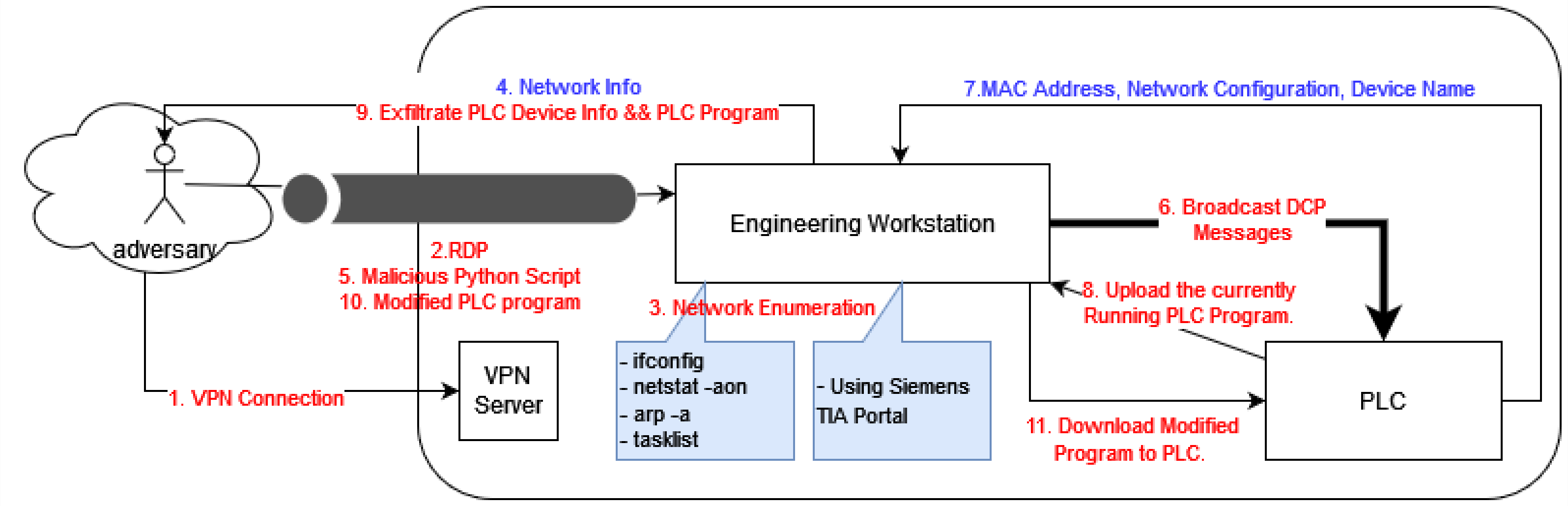
# ZenSIM 4.0 Framework (Correlation engine 1)

- Use Case 1:
  - Check organizational assets against CSAF documents.
  - If a match is found, it creats a ticket
    - Mach is based on name (Affected Product and Versions), brand, manufacturer, PURL, CPE, serial numbers and module numbers, file hashes, SBOM URL, and SKUs of assets.
- Use Case 2:
  - Check for attack signatures in the collected data, such suspicious use of netstat.exe via cmd.exe or PowerShell.
  - Detection of unusual events
    - Example: significant increase in the number of RDP connections between the Engineering workstation and PLC.

# ZenSIM Framework (Correlation engine 2)

- Use Case 3:
  - Check for multiple alerts on same machine.
    - Alert 1: Network enumeration from the engineering workstation EWS) (ipconfig, netstat, arp, and tasklist)
    - Alert 2: executable file transfer to EWS
    - Alert 3: DCP message broadcast.

# Attack Scenario (1)

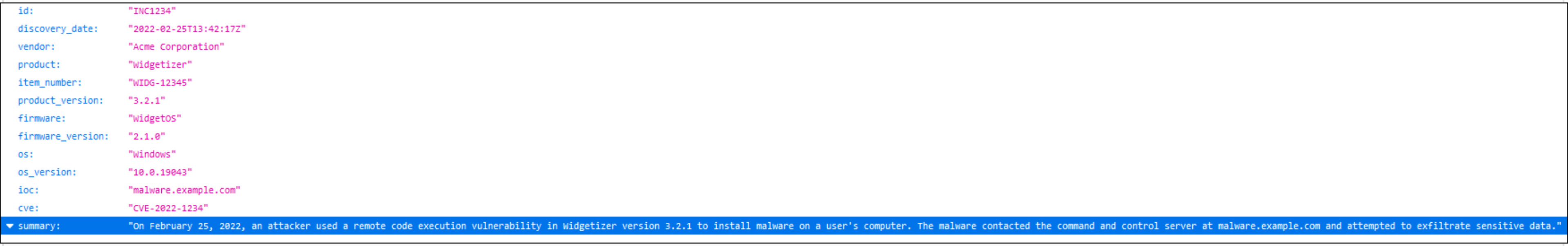

adversary
1. VPN Connection
VPN Server
2.RDP
5. Malicious Python Script
10. Modified PLC program
4. Network Info
9. Exfiltrate PLC Device Info && PLC Program
Engineering Workstation
3. Network Enumeration
- ifconfig
- netstat -aon
- arp -a
- tasklist
- Using Siemens TIA Portal
7.MAC Address, Network Configuration, Device Name
6. Broadcast DCP Messages
8. Upload the currently Running PLC Program.
11. Download Modified Program to PLC.
PLC

# Attack Scenario (2)

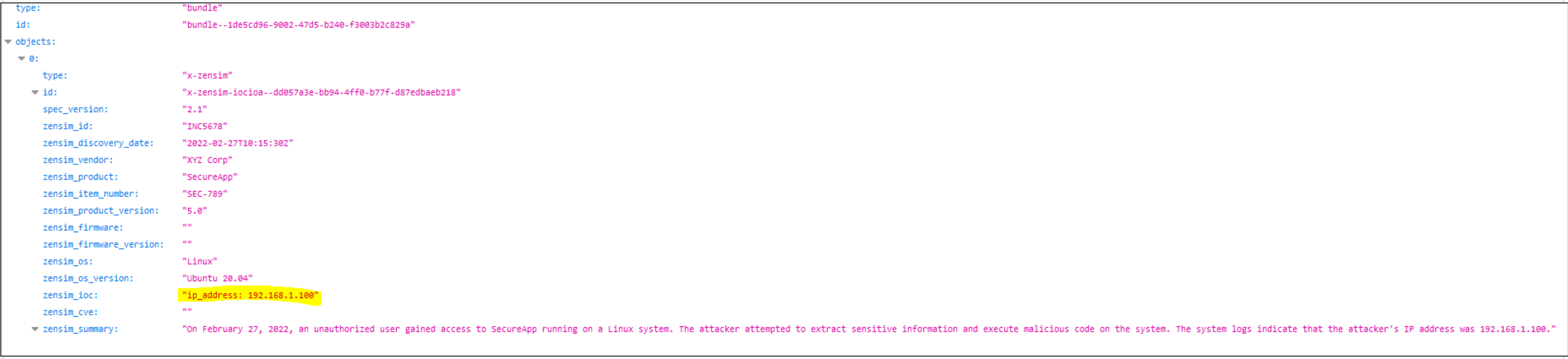
- Connection via VPN (Valid account) and then via RDP to EWS
- Network enumeration on EWS
  - IP addresses of PLC
  - Port 102/TCP is open → Siemens S7 protocols
  - Target network is utilizing Profinet protocol
- Malicious script (DCP.exe)
  - DCP broadcast is sent to the network
  - Profinet devices reply to MAC address, network configuration and device name
- Totally Integrated Automation Portal (TIA) from Siemens
  - PLC’s firmware version and article number and PLC program via the TIA Portal

# Attack IoCs

- Name of product, timestampt, OS version, Malware name and summary



```
  id:                 "INC1234"
  discovery_date:     "2022-02-25T13:42:17Z"
  vendor:             "Acme Corporation"
  product:            "Widgetizer"
  item_number:        "WIDG-12345"
  product_version:    "3.2.1"
  firmware:           "WidgetOS"
  firmware_version:   "2.1.0"
  os:                 "Windows"
  os_version:         "10.0.19043"
  ioc:                "malware.example.com"
  cve:                "CVE-2022-1234"
▼ summary:            "On February 25, 2022, an attacker used a remote code execution vulnerability in Widgetizer version 3.2.1 to install malware on a user's computer. The malware contacted the command and control server at malware.example.com and attempted to exfiltrate sensitive data."
```



```
  type:                          "bundle"
  id:                            "bundle--1de5cd96-9002-47d5-b240-f3003b2c829a"
▼ objects:
  ▼ 0:
        type:                    "x-zensim"
      ▼ id:                      "x-zensim-iocioa--dd057a3e-bb94-4ff0-b77f-d87edbaeb218"
        spec_version:            "2.1"
        zensim_id:               "INC5678"
        zensim_discovery_date:   "2022-02-27T10:15:30Z"
        zensim_vendor:           "XYZ Corp"
        zensim_product:          "SecureApp"
        zensim_item_number:      "SEC-789"
        zensim_product_version:  "5.0"
        zensim_firmware:         ""
        zensim_firmware_version: ""
        zensim_os:               "Linux"
        zensim_os_version:       "Ubuntu 20.04"
        zensim_ioc:              "ip_address: 192.168.1.100"
        zensim_cve:              ""
      ▼ zensim_summary:          "On February 27, 2022, an unauthorized user gained access to SecureApp running on a Linux system. The attacker attempted to extract sensitive information and execute malicious code on the system. The system logs indicate that the attacker's IP address was 192.168.1.100."
```

# Communication of IoCs

- IoC feed producer at operator part
- Mlaware Information Sharing Platform (MISP) server at CERT@VDE
- Trusted Automated Exchange of Intelligence Information (TAXII) server at CERT@VDE
- IoC files in JSON format or Structured Threat Information eXpression (STIX) format

# Conclusion

- Automated usage of CSAF adversary by SIEM
- Detect vulnerable assets and countermeasure them
- Detecting of attacks in ICS environment
- Construction of IoC files
- Communication of IoC with CERT@VDE
- On going project:
  - CSFA adversary matcher was implemented and tested
  - TAXII and MISP servers and feed producers developed and tested.
  - Attack detection rules was not tested yet.

# Thank you for your attention!

DECOIT GmbH & Co. KG
Fahrenheitstraße 9
D-28359 Bremen
https://www.decoit.de
info@decoit.de