The 12th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications
7-9 September, 2023, Dortmund, Germany

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

Salva Daneshgadeh Çakmakçı[1] , Sercan Catalkaya[2] , Kai Olver Detken[1] , Evren Eren[2]
[1] DECOIT GmbH & Co. KG, Bremen, Germany,
daneshgadeh@decoit.de, deltkan@decoit.de, www.decoit.de
[2] University of Applied Sciences, Bremen, Germany,
sercan.catalkaya@hs-bremen.de, evren.eren@hs-bremen.de, www.hs-bremen.de

***Abstract* — The emergence of Industry 4.0 inextricably tied together Information Technologies (IT) and Operational technologies (OT). It fosters manufacturing while reducing costs. On the other hand, it broadens the vulnerability surfaces of operations. It defines new cyber vulnerabilities and attacks even with more extensive effects than previous ones. Therefore, there is a need for a holistic approach that supports the security of both IT infrastructures and products. The ZenSIM project was initialized to fill in the gap by developing a platform-based solution tool to identify security vulnerabilities in the product and production environment for manufacturers, detect cyber-attacks (anomalies), create a form of Cyber Threat Intelligence (CTI) and finally share it with corresponding parties for extended investigation and creation of publicly available CTI and/or security advisories. This paper only addresses the architectural design of the proposed tool to protect Industry 4.0-enabled manufacturing environment by consuming open-source knowledge about known asset vulnerabilities and exchanging incident information. The experimental validation of the platform is beyond the scope of this paper.**

Keywords* — *SIEM; CTI; CSAF; CERT; CVE

I. Introduction

Today, production plants with increasing automation are characterized by a high degree of networking computers, measurement and control systems, agents and sensors that are networked usage of SelfX technologies (self-configuration, self-healing, self-optimization). This creates a diversity of complex, dynamic, and heterogeneous IT landscapes (operating systems, communication protocols, data formats), accompanied by increased usage of standard hardware and software (COTS: Commercial-Off-The-Shelf solutions) and open standards for communication (such as TCP/IP; e.g. Profinet, Modbus). ICS communicates with the office IT, so that classic boundaries between production and the business world dissolve. Sensitive data is transferred across organizational boundaries and technology areas which were previously autonomous are merging [1].

In industrial plants, the existing office IT and production processes (via the usage of OT) are becoming vulnerable. Standard IT components (hardware, operating systems, networks) and special systems like SCADA, PLC, HMI, Historian and Engineering Station are replacing traditional proprietary systems. Automation systems are exposed to similar and new threats. By using standardized protocols, special knowledge is no longer needed for classical attacks. Standardization and networking increase the risk of accessing production processes, even remotely controlling equipment and systems. New attack vectors are emerging (e.g. machine-specific malware) [2].
There is a broad range of attack vectors to compromise ICS networks as follows:

- ICS devices being exposed to the internet. Therefore, they also remain vulnerable to network-based cyber-attacks. MITRE ATT&CK® ICS Matrix[1] contains 12 techniques that can be used by adversaries to target ICS networks such as Initial Access, Execution, Persistence, Privilege Escalation, Evasion, Discovery, Lateral Movement, Collection, Command and Control, Inhibit Response Function, Impair Process Control and Impact [3].
- ICS devices communication over insecure ICS protocols such as PROFINET or Modbus (mostly in clear text) [4].
- Widespread existence of Outdated and unpatched assets in ICS environments [2].
- Weak password/reuse of passwords or no multi-factor authentication on remote maintenance services, such as VPN (MITRE-TA0108).
- Exposing an unintended service through a public-facing application, such as VNC or RDP access on a web application (MITRE-TA0108).
- Leveraging a compromise on the enterprise network to pivot into the ICS network, like exploiting an IT asset directly communicating with the ICS network (MITRE-TA0109).
- Phishing/spearfishing emails with malware attachments. This could lead to direct access into the ICS network, depending on where the email attachment is accessed from (MITRE-TA0108).
- Removable media like USB drives, phones or laptops that are likely to be infected from being exposed to

[1] https://attack.mitre.org/matrices/ics/

a compromised host/network (MITRE-TA0108).

A relatively well-known example of such a compromise is the BlackEnergy 3 cyberattack on the Ukrainian power grid system. The adversaries utilized spearfishing emails with malware attachments to access the enterprise network and compromise VPN credentials. With those, the adversaries were able to access the ICS network and ultimately take down the power grid system. [5]

II. BACKGROUND

In this section, we summarize similar approaches available for producing and consuming cyber threat knowledge. We also present a glossary of project shareholders and employed state-of-the-art tools and protocols in the proposed framework.

A. Related Cyber Security Players and Concepts

Cyber Threat Intelligence (CTI) is analyzed and organized information about an adversary. It seems as best practice to protect IT and OT environments from well-defined and duplicated cyber-attacks. Regardless of improvement in the availability and adoption of CTI materials and practices in recent years, specialized CTI for various sectors (especially, critical infrastructures with industrial control systems (ICS)/ OT devices and software) and use-cases with adequate Course-of Action (CoA) are still challenging aspects.

Computer Emergency Response Team (CERT) is an organization that specializes in responding to and preventing cyber attacks. CERT@VDE is a coordinating product CERT (PSIRT) in Germany that focuses on delivering cyber security services to European companies and organizations. It is a one-stop shop for companies and organizations that need support in improving the cybersecurity of their products inside the embedded software area (e.g. Industrial Control Systems, ICS).

Common Security Advisory Framework (CSAF) is a specific machine-readable language for the creation, update and communication of security advisories. It compasses structural information on products, their known vulnerabilities, the impact of the vulnerability, and remediation. The CSAF document is a JSON file that has three properties: document, product-tree (e.g., name, manufacturer, Common Platform Enumeration (CPE)) and vulnerabilities (e.g., Vulnerabilities and Exposures(CVE), Common Weakness Enumeration (CWE)). The document property contains document-level metadata such as the CSAF document version and its publisher[2].

SIEM Security Information Event Management (SIEM) tool collects logs/events from network traffic and security solutions and stores them in a centralized location. Subsequently, it detects and alerts on security events. In recent years, Security Orchestration and Response (SOAR) was designed to prioritize and manage alerts from SIEM and help security operations teams to respond to alerts by means of prebuilt remediation steps called playbook.

[2]https://docs.oasis-open.org/csaf/csaf/v2.0/csaf-v2.0.html

B. Related Work

Shingo et al. [6] proposed the installation of a Traceback Honeypot System (THS) in the ICS network for early detection of incidents. THS employs a machine learning method to learn normal network communication and detects malicious ones. When THS finds a suspicious communication, starts a counter-scan and collects information about the source device. Then collected data are compared with Indicators of Compromise (IoCs) provided by US-CERT to spot the attack. In the follow-up paper [7], Shingo et al. proposed the implementation of a THS in each network segment of the ICS environment and a central Integrated Management System (IMS) to integrate and analyze information gathered from each THS. The authors also proposed setting up a shared platform called Early Warning Management System (ICSEWM). ICSEWM receives information about attacks in STIX format from different IMS. ICSEMW provides a SIEM function to analyze sent information from IMSs, creates IoCs, and finally shares them with all IMSs. Dodson et al. [8] also proposed the integration of high-interaction ICS honeypots to identify and profile targeted ICS attacks. They discussed that it requires the definition of new ICS exploits by the honeypot networks. Unfortunately, the current ICS honeypots can not be used in detecting deliberately modified ICS behaviors and new ICS exploits. Additionally, they can not model attackers' behaviors (e.g., modify any PLC code written by an engineer) because they are not able to emulate the device state.

C. Our Contribution

To the best of our knowledge, there is not any SIEM that directly ingests and consumes asset vulnerability information (via CSAF documents) and automatically creates ICS asset-related feeds. We investigate the following research questions in this study to realize such a platform.

1) How SIEM can identify assets in the ICS environments in a safe manner?
2) How SIEM can protect the ICS environment against cyber attacks which target known vulnerabilities of assets and countermeasure them?
3) How SIEM can automatically share information about detected attacks and their associated assets in the ICS environments?

III. METHODOLOGY

This paper aims to investigate an architectural design for identifying the systems, sub-systems and communication among them to build up a cyber incident platform for an ICS environment. Our methodology explores required systems, external parties and their roles and communication protocol among parties.

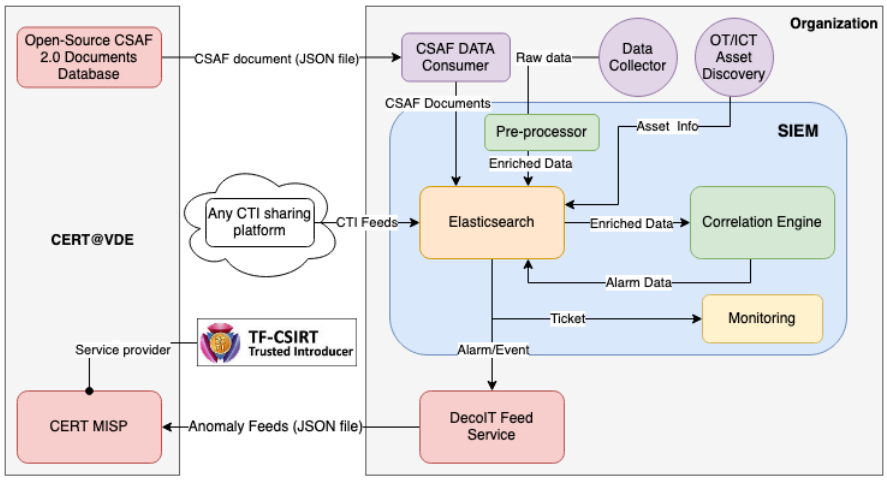

Figure 1. Architecture of the central security incident management platform for SMEs in industry 4.0.

A. *Framework*

Figure 1 displays our proposed platform. This section elaborates on each component of the platform. An OT-supported SIEM is the backbone of the central security incident management platform for SMEs in industry 4.0. We use an OT-supported SIEM with dedicated sensors to monitor the OT network and collect data about assets and their communications. It uses an agent-less OT/ICS asset scanner that discovers IP-enabled devices in the network and sends detailed information about them to the SIEM. It could be an integrated open-source tool like Nmap or any other commercial or open-source ICS assessment and inventory tool which can provide at least information about an asset such as name, version, serial number and manufacturer. The data collector is responsible for collecting network traffic. Elasticsearch is a distributed datastore that stores all collected data and it provides the full-text query. There are four types of indices (a logical partition of documents that is similar to a database in the relational databases) in Elasticearch in this platform 1) network traffic index, 2) asset index, 3) adversary index, and 4) CTI index. The CSAF consumer is responsible for downloading CSAF documents based on asset data on regular-base or when a new version is available. in the platform, CERT@VDE plays as a CSAF aggregator who aggregators and stores CSAF documents from trusted third parties and manufacturers themselves and serves a collective set of CSAF documents for manufacturers, integrators, plant constructors and operators from the industrial automation sector. The correlation engine is the brain of the SIEM. It detects incidents and assists in incident response. It consists of a rule engine that utilizes rules, and knowledge to protect industries against known vulnerabilities and attack patterns. Rules compare events or network traffic against predefined condition(s) and trigger an alert when a match is found. Knowledge about threats or vulnerabilities (e.g., CSAF documents) is used as a rule condition.

The correlation engine creates an alarm for a detected attack or an anomaly. An alarm is a combination of low-level alerts and a tag. Each alarm should have a corresponding **Ticket** in the system. A ticket includes detailed information about an alarm (timestamp, affected assets, users and etc.) and one or more attached playbooks (if there is a countermeasure for a detected attack or vulnerability). A tag differentiates the way an alarm should be treated later. A “Internal” tag means that the alarm should be handled internally. For example, if an alarm is created for a known vulnerability of an asset. A “External” tag means that the alarm includes attack information (e.g., Malware, Phishing Campaign, etc.) against the ICS network and should be communicated with CERT. This type of alarm will be processed and converted into a format recognizable by the CERT MISP. In this project, Trusted-Introducer-Network (TF-CSIRT/TI). [3] will operate MISP server and provide an Information Sharing Platform (ISP) called **Clearinghouse** which is operated by. A “Zero-day” tag means that the alarm includes information about a potential vulnerability in an ICS asset that was not reported in the CSAF documents. Organizations are encouraged to inform CERT@VDE about an alarm with a Zero-day tag via email whenever they enrich the alarm with enough information that makes the case reproducible by the asset vendor.

B. *Data Collection*

The data collector collects flow-based network traffic via Zeek then raw data is normalized and enriched through the pre-processor and written in the network traffic index in Elasticsearch. The CTI data is collected by means of

[3]https://tf-csirt.org/trusted-introducer/

the Threat Intel module [4]of Elastic.

C. OT/ICS Asset Discovery

According to [9], asset discovery is a challenging process in ICS environments. First, it is almost not possible to install an agent on the asset to perform an agent-based asset discovery. Second, active scanning causes service disruption, performance degradation or costly downtime in critical infrastructures. Third, passive scanning (only targeting specific protocols) usually can't provide enough information for accurate asset identification. We constructed a virtual lab to test the performance of the different asset discovery tools including Nmap, S7-info, Grassmarlin, PLCScan, Redpoint, Modbusdiscover, ICS-Hunter, Scadascan, SCADACIP, Scada-tools, Unicornscan, Cyberlens, PLCScanner, Networkminer, S7scan to gather useful asset information [10]. Additionally, we evaluated if ICS assets can withstand active scanning with configured IP ranges and specific ports. We used the Purdue 5-level reference model with some extensions to construct the architecture of an ICS network as follows:

1) Level 5: Public Internet as well as external networks.
2) Level 4: Corporate network, intranet or office network (office IT)
3) Level 3-4: Industrial DMZ
   - Ubuntu Jump Host, OPNSENSE VPN Server, IPSEC VPN Gateway
4) Level 3: Automation network
   - Active Directory Server (2019)
   - Above systems communicates with the systems in Level 4, usually via an appropriate DMZ in between. Direct communication may not occur. In addition, Level 3 systems may communicate with systems in Levels 2 and 1.
5) level 3-2: OPNsense Stage2 Firewall
6) level 2: Industry network
   - Win7-Admin-OPNsense, PLCSIM Advanced S7-1516, WinCC-HMI, OpenPLC (Modbus), Win7-ScadaBR, Win7-ModbusTool (Master), Debian-ModbusPal (Slave).
7) level 1: Process control network (not used).
8) Monitoring zone: Isolated zone for monitoring appliances (SIEM appliance)

Our experiment disclosed that passive scans cannot deliver accurate and comprehensive information about assets which is essential for effective matching with CSAF documents. For example, for most assets, it was not possible to find out the full product name, serial number, module number, version and Operating System (OS). Most comprehensive results have been achieved by the numerous Nmap scripts from Redpoint.

[4]https://www.elastic.co/guide/en/beats/filebeat/7.17/filebeat-module-threatintel.html

D. Asset Matching

The more detailed information we access during asset discovery, the more likely we make a better match. We limit our asset matching to name, brand, manufacturer, PURL, CPE, serial numbers and module numbers, file hashes, SBOM URL, and SKUs of assets. To accelerate the matching process, we initially correlate only the product name and version. If we do not find a unique result we will include other attributes to the matching query.

E. Playbook

A playbook maintains predefined procedures to handle a specific type of incident. In the proposed platform, customized playbooks are created for each identified asset in the asset index. The information inside the remediation field of the CSAF document (e.g., mitigation, vendor_fix and workaround values) will be copied into the respective asset playbook.

IV. Application of Proposed Framework

V. Anomaly Feeds

VI. Discussion

A. Limitations and Future Work

VII. Summary

Acknowledgment

References

[1] E. Eren, "Cyber security in smart manufacturing: Status and challenges," *ACHEMA Pulse*, pp. 16–18, Juni 2021. [Online]. Available: www.achema.de

[2] E. Eren, "Sicherheitsaspekte bei industrie 4.0," *NET (Zeitschrift für Kommunikationsmanagement*, vol. 9, pp. 39–41, 2017.

[3] "the tactics and techniques representing the mitre att&ck® matrix for ics." [Online]. Available: https://attack.mitre.org/matrices/ics/

[4] S. Mehner and H. König, "No need to marry to change your name! attacking profinet io automation networks using dcp," in *Detection of Intrusions and Malware, and Vulnerability Assessment: 16th International Conference, DIMVA 2019, Gothenburg, Sweden, June 19–20, 2019, Proceedings 16*. Springer, 2019, pp. 396–414.

[5] D. U. Case, "Analysis of the cyber attack on the ukrainian power grid," *Electricity Information Sharing and Analysis Center (E-ISAC)*, vol. 388, pp. 1–29, 2016.

[6] S. Abe, Y. Tanaka, Y. Uchida, and S. Horata, "Tracking attack sources based on traceback honeypot for ics network," in *2017 56th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE)*. IEEE, 2017, pp. 717–723.

[7] S. Abe, Y. Uchida, M. Hori, Y. Hiraoka, and S. Horata, "Cyber threat information sharing system for industrial control system (ics)," in *2018 57th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE)*. IEEE, 2018, pp. 374–379.

[8] M. Dodson, A. R. Beresford, and M. Vingaard, "Using global honeypot networks to detect targeted ics attacks," in *2020 12th International Conference on Cyber Conflict (CyCon)*, vol. 1300. IEEE, 2020, pp. 275–291.

[9] P. Kelley, "Asset discovery challenges in ot and ics environments," 2020. [Online]. Available: https://www.axonius.com/blog/asset-discovery-challenges-ot-ics-environments

[10] E. Samanis, J. Gardiner, and A. Rashid, "Sok: A taxonomy for contrasting industrial control systems asset discovery tools," in *Proceedings of the 17th International Conference on Availability, Reliability and Security*, 2022, pp. 1–12.