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 Oliver Detken[1] , Evren Eren[2]
[1] DECOIT GmbH & Co. KG, Bremen, Germany,
daneshgadeh@decoit.de, detken@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 has tightly integrated Information Technologies (IT) and Operational Technologies (OT), enabling enhanced manufacturing capabilities and cost reduction. However, this integration also expands the attack surface and introduces new cyber vulnerabilities and threats, often with more significant impacts than before. Consequently, there is a pressing need for a comprehensive approach that ensures the security of both IT infrastructures and products. In response to this challenge, the ZenSIM project was initiated, aiming to develop a platform-based solution for identifying security vulnerabilities in the product and production environments of manufacturers. The project's objectives include detecting cyber-attacks and anomalies, generating Cyber Threat Intelligence (CTI), and sharing it with relevant stakeholders for further investigation and the creation of publicly available CTI and security advisories.This paper only addresses the architectural design of the proposed solution for protecting Industry 4.0-enabled manufacturing environment by utilizing 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. These systems utilize SelfX technologies, such as self-configuration, self-healing, and 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, Profinet, Modbus). Industrial Control Systems (ICS) communicate 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 convergence of office IT and production processes through the use of Operational Technology (OT) has introduced vulnerabilities. Traditional proprietary systems are being replaced by standard IT components such as hardware, operating systems, and networks, alongside specialized systems like SCADA, PLC, HMI, Historian, and Engineering Station. As a result, automation systems are exposed to both familiar 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 that are connected to the internet are susceptible to network-based cyberattacks. The MITRE ATTCK® ICS Matrix[1] provides insights into 12 techniques that adversaries may employ to target ICS networks. These techniques include 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 multifactor 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 involves exploiting an IT asset that directly communicates with the ICS network (MITRE-TA0109).
- Phishing/spear-phishing emails with malware attachments can potentially provide direct access to the ICS network, depending on the location from which

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

979-8-3503-5805-6/23/$31.00 ©2023 IEEE

the email attachment is accessed (MITRE-TA0108).
- Removable media, such as USB drives, phones, or laptops, can pose a risk of infection if they have been exposed to a compromised host or network (MITRE-TA0108).

A notable example of such a compromise is the BlackEnergy 3 cyberattack on the Ukrainian power grid system. In this attack, the perpetrators employed spear-phishing emails containing malware attachments to gain unauthorized access to the enterprise network and compromise VPN credentials. With these compromised credentials, the attackers were able to infiltrate the ICS network, leading to the successful disruption of the power grid system [5].

II. Background

In this section, we provide an overview of existing approaches used for generating and utilizing cyber threat knowledge. Additionally, we present a glossary of key stakeholders involved in the project and outline the state-of-the-art tools and protocols employed within the proposed framework.

A. Related Cyber Security Players and Concepts

Cyber Threat Intelligence (CTI) refers to the analyzed and organized information about an adversary. It seems as best practice to protect IT and OT environments from well-defined and replicated 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 ICS/ OT devices) and use-cases with adequate Course-of Action (CoA) are still challenging aspects.

The **Computer Emergency Response Team (CERT)** is an organization that dedicated to 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 cyber-security of their products inside the embedded software area (e.g. Industrial Control Systems, ICS).

The **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 those vulnerabilities, and recommended remediation. The CSAF document is a JSON file that has three properties: ”document,” ”product-tree,” and ”vulnerabilities.” The product-tree provides information about the products such as name, manufacturer, Common Platform Enumeration (CPE). The ”vulnerabilities” property includes information about 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 A **Security Information Event Management (SIEM)** tool is responsible for collecting logs and events from various sources such as network traffic and security solutions. Subsequently, SIEM analyzes the collected data to detect and alert 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.

B. Related Work

Shingo et al. proposed a solution called the Traceback Honeypot System (THS) [6] to enhance the early detection of incidents in ICS networks. THS employs a machine learning method to learn normal network communication and detects malicious ones. When THS finds a suspicious communication, it 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 their followup 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 [3] format from different IMS. ICSEMW provides a SIEM function to analyze received information, 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 highlighted the need for defining new ICS exploits within the honeypot networks. Because, 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 in the form of 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 can a SIEM safely identify assets in the ICS environments?

[2]https://docs.oasis-open.org/csaf/csaf/v2.0/csaf-v2.0.html
[3]https://oasis-open.github.io/cti-documentation/stix/intro.html

2) How can a SIEM protect the ICS environment against cyber attacks which target known vulnerabilities of assets and implement countermeasures?
3) How can a SIEM automatically share information about detected attacks and their associated assets in the ICS environments?

III. Methodology

This paper aims to investigate the architectural design of a cyber incident platform for an ICS environment. It includes identifying the systems, sub-systems, parties and their roles and communication protocol among parties.

A. Framework

Figure 1 displays our proposed platform. The central security incident management platform for SMEs in Industry 4.0 is built upon an OT-supported SIEM. The SIEM is equipped with dedicated sensors that monitor the ICS network and collect relevant data regarding 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 such as name, version, serial number, manufacturer and operating system to the SIEM.

The data collector is responsible for collecting network traffic. Elasticsearch, a distributed data store, is employed to store all the collected data and offers full-text query capabilities. In the proposed platform, there are four types of indices (a logical partition of documents that is similar to a database in the relational databases) in Elasticsearch. These indices include the network traffic index, asset index, adversary index, and CTI index. The CSAF consumer component is responsible for downloading CSAF documents based on the asset inventory data stored in the asset index on a regular-base or when a new version is available. In this platform, CERT@VDE plays as a CSAF aggregator who aggregates and stores CSAF documents from trusted third parties and manufacturers themselves and serves a consolidated set of CSAF documents for manufacturers, integrators, plant constructors and operators from the industrial automation sector. The correlation engine serves as the core component of the SIEM, responsible for detecting incidents and supporting incident response activities. 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 within rule conditions.

The correlation engine is also responsible for generating tickets when an attack is detected. A ticket is a comprehensive record that includes information such as alerts, the history of alerts (including timestamps, affected assets, IP addresses, users, etc.), and a specific tag. Furthermore, each ticket is associated with at least one playbook which includes countermeasures for a detected attack or vulnerability. A tag is used to specify how an alert should be treated in the future. Specifically, an ”Internal” tag indicates that the alert should be handled internally. For example, if an alert is created for a known vulnerability of an asset. On the other hand, an “External” tag means that the alert includes attack information (e.g., Malware, Phishing Campaign, etc.) against the ICS network and should be communicated with CERT. A ”Zero-day” tag indicates that the alert contains information about a potential vulnerability in an ICS asset that has not been previously reported in the CSAF documents by CERT@DVE. Organizations are encouraged to inform CERT@VDE about this kind of vulnerabilities, typically via email, providing enriched alert data that makes the case reproducible by the asset vendor.

B. 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 and 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.
   - IPSec Client, OpenVPN Client
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), WinCC-HMI
5) level 3-2: OPNsense Stage2 Firewall
6) level 2: Industry network
   - Win7-Admin-OPNsense, TIA Portal Engineering Workstation, PLCSIM Advanced S7-1516, OpenPLC (Modbus), Win7-ScadaBR, Win7-ModbusTool (Master), Debian-ModbusPal (Slave).
7) level 1: Process control network (not used).

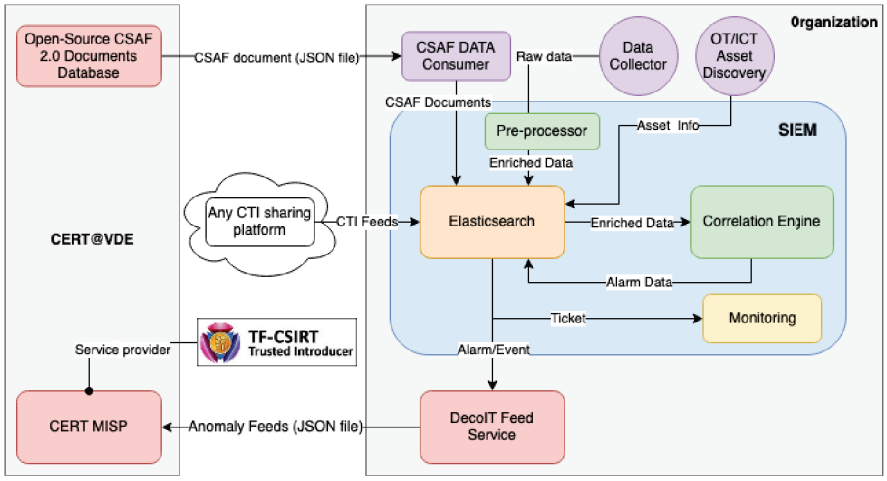

Figure 1. Architecture of the central security incident management platform for SMEs in industry 4.0

8) Monitoring zone: Isolated zone for monitoring appliances (SIEM appliance)

Our experiment disclosed that passive scans cannot provide accurate and comprehensive information about assets, which is essential for effective matching with CSAF documents. For instance, it was often not possible to obtain the full product name, serial number, module number, version, and Operating System (OS) for most assets. The most comprehensive results have been achieved by the numerous Nmap scripts from Redpoint. Nmap is an active scanner and could potentially disrupt sensitive ICS devices even with a reduced speed. However, it provided the more detailed information about the assets compared to other open-source tools used in our experiments. Consequently, Nmap was utilized to demonstrate the proof of concept within the project's scope.

C. Asset Matching

The more detailed information we access during asset discovery, the higher the likelihood of making a more accurate 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 a unique match is not found, additional asset information is included in the matching query to enhance the accuracy of the match.

D. Playbook

A playbook maintains predefined procedures to handle a specific type of incident. In the proposed platform, customized playbooks can be created for each asset and different types of attacks. Moreover, when assets are matched, the information within the remediation field of the corresponding CSAF document (such as mitigation, vendor_fix, and workaround values) are copied into the respective asset playbook.

IV. Application of Proposed Framework

A. Attack Scenario

This attack scenario was inspired by [11] and it utilizes different steps of the Cyber Kill Chain that an adversary must follow to achieve its objective [12]. It is assumed that the Enterprise and ICS networks are physically separated, and there is only remote maintenance VPN access available for engineers to access the Engineering Workstations in the ICS network via RDP. In the following scenario, the adversary has already compromised the enterprise network and obtained valid credentials for VPN and Engineering Workstation RDP access. Therefore, the adversary uses the valid account credential to access the ICS network via a VPN connection and then connects via RDP to the Engineering Workstation. The adversary enumerates the network to gather information about ICS assets in the network using the following commands.

- IPconfig: Basic network enumeration.
- Netstat: Port 102/TCP is open, which is used by the Siemens S7 protocols.
- Arp: The adversary takes notes on the IP addresses as well as MAC addresses in the Arp cache.
- Tasklist: Checking for Siemens services.

The adversary discovers that the target network is utilizing the open international standard Profinet protocol, which is an Ethernet-based industrial protocol used by field devices. The adversary forges the DCP "identify all request" with an executable "DCP.exe" which is written in Python and uses the Scapy library. Then the adversary transfers "DCP.exe" to the Engineering Workstation and executes it. As a result, a DCP broadcast is sent to the network. Single DCP scan is enough, because the result of IPconfig command revealed that the system is not multi-homed. The Profinet devices then reply to this broadcast message with their MAC address, network configuration and device name. The adversary exfiltrates

this information and uses it to locate the PLC in the network.

Subsequently, the adversary locates the vendor Software (TIA Portal) on the workstation to program the PLC. The Adversary uploads the running program from the PLC into the Engineering Workstation without the need of providing a password. According to [13] the security measures for read/write access on the PLCs are generally disabled in practice. Furthermore, the adversary gains access to the PLC's firmware version and article number via the TIA Portal. This information can potentially be used to identify PLC vulnerabilities. With this information, the adversary exfiltrates the program through the RDP connection and investigates it. Subsequently, the adversary can modify the PLC program in a way that causes disruption to the plant. Following this, the adversary reconnects to the Engineering Workstation via RDP and transfers the modified program to the workstation. The final step in the adversary's mission to disrupt the plant is completed by downloading the modified program into the PLC from the workstation using the TIA Portal.

B. Attack Detection

The correlation engine utilizes three different types of rules. First, simple rules are used to search for matches between asset data and CSAF documents. These rules also check for attack signatures in the system, such as identifying suspicious use of netstat.exe via cmd.exe or PowerShell. Second, threshold rules are employed to track abnormal events, such as unusual VPN and RDP connection times or a significant increase in the number of RDP connections between the Engineering workstation and PLC. Third, correlation rules are utilized to correlate various security events (alerts) across the entire ICS network. These rules support the correlation engine at different levels:

- Correlation of low-level alerts for each host.
- Only alerts that have the potential to belong to the same attack kill-chain should be correlated.
- Correlation of previously correlated alerts. Correlation is done based on shared identifiers such as host IP or identifiers of pre-defined use cases (e.g., username).

Algorithm 1 displays the high level notation of the Correlation Engine. Furthermore, it is crucial to correlate the malicious internal IP address, which serves as the initial point of access to the ICS network, with the data at the VPN gateway in order to map the internal malicious private IP address to the corresponding external IP address before generating IoCs.

C. Attack Feeds

The SIEM should notify CERT@VDE about any detected external attacks. Like to any data exchange between computers, the transmitted data has to be in a structural format that is readable and potentially actionable by machines. As mentioned in [14], a CTI schema that provides information about vulnerabilities, detailed data about malware, comprehensive details about attacker trends, and specific Indicators of Compromise (IoCs) to integrate into IT and security infrastructure are considered highly valuable features. Ramsdale et al. [15] discussed that the format of CTI data closely depends on the use case. He even recommended the use of a custom user-defined JSON format to improve the quality of CTI data. Therefore, we have adopted the data schema (JSON format) proposed by ACDC [4] as it aligns with the criteria outlined in [14] and [15]. Based on the principles outlined in the ACDC schema, the reported attack should have information about the attacking host and should belong to one of the categories including abuse, compromise, data, Denial of Service (DoS), login, malware, scan and others. An attack report can also refer to other attack reports using the source_value (e.g., URL, IP address,

Algorithm 1: Pseudocode for the Correlation Engine

```
Input  : alert
Output: alert/ticket
correlate_alerts(alerts)
Perform correlation among retrived alerts based on
  2 criterias: shared host IP or when alerts have a
  potentiality to belong to the same attack
  kill-chain;
return correlated_alerts
calculate_risk_score(alerts)
Update the risk score based on the information in
  the alerts (asset criticalities, impacts of risk,
  severaity level of alerts);
return risk_score
create_ticket(correlated_alerts)
Create a ticket which encompasses information
  from the correlated alerts;
receive_alert(alert)
store_alert (alerts);
correlated_alerts ← correlate_alerts
  (alert);
// capturing correlated_alerts for
   checking its risk score
if calculate_risk_score (correlated_alerts)
  > pre-defined_critical_threshold then
    create_ticket (correlated_alerts);
end
```

[4] https://www.acdc-project.eu/

hash value) of the system performing the attack. Consequently, source_value is a must for all reports. However, in addition to the mandatory fields of the report, the optional fields can assist better identification of attackers by Clearinghouse. ACDC has introduced various schemas to address distinct features of different categories and sub-categories of attack. Each schema encompasses the Indicator of Compromises (IoC), serving as a resource for identifying attacks. For example, a DoS attack report includes IoCs such as IP address and port number of the attacker, the application protocol (e.g., DNS), traffic volume information such as bits/packets per second and so on. It is also important to take into account that, personalized and private information (e.g., IP address of victim) should be removed or anonymized from the report to protect individuals' privacy [16]. Consequently, we proposed the implementation of Trusted Automated Exchange of Intelligence Information (TAXII) [5] and Malware Information Sharing Platform (MISP) [6] as extra interfaces for transmitting data to CERT@VDE. According to [17] Structured Threat Information Expression (STIX™) is the most used standard for CTI feed integration, analysis and reporting. STIX utilizes a Channel-based communication between a TAXII Client and TAXII Server, and the request-and-response fashion is employed to exchange information.

V. Discussion

This paper presents an architectural design of a central platform for Industry 4.0 which automates the ingestion and application of security advisories on products. The security advisories were received from CERT@DVE's API in the form of CSAF documents. Each document is a JSON file that encompasses information about vulnerabilities in software or hardware, the status of impact and remediation of vulnerabilities for a given ICS asset. On the other hand, this platform enables the automatic transfer of indicator of compromised regarding attacks which detected by SIEM to CERT@DVE. The Operators of large ICS infrastructures will be the intended consumers of the IoC data. They are required to subscribe to MISP/TAXII instance of CERT@DVE in order to push or pull new IoCs. This paper is based on an ongoing project and only focuses on conceptualizing the proposed framework without presenting any experimental results. For future work, it is necessary to integrate the independent components of the system (SIEM, CSAF Data Connector, asset discovery, asset matcher, TAXII client and server), which are currently in a functional state, and evaluate the operational effectiveness of the system. This system represents a novel approach, it is not feasible to directly compare it with other existing systems. However, in the future, the individual components of the system can be compared to known approaches in the literature and market.

Acknowledgment

The authors would like to thank the German Federal Ministry of Education and Research (BMBF) [7] for the financial support, as well as all other partners involved in the research project ZenSIM4.0 [8] for their great collaborations.

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.

[11] A. Scott and B. Miller, "Generating labelled network datasets of apt with the mitre caldera framework," Whitepaper, Dragos, Inc., 2021, available at https://www.dragos.com/resource/mitre-engenuity-attack-evaluations-for-ics-whitepaper-2021/.

[12] L. Martin, "Cyber kill chain framework," 2023.

[13] E. Biham, S. Bitan, A. Carmel, A. Dankner, U. Malin, and A. Wool, "Rogue7: Rogue engineering-station attacks on s7 simatic plcs," *Black Hat USA*, vol. 2019, 2019.

[14] R. Brown and R. M. Lee, "2021 sans cyber threat intelligence (cti) survey," in *Tech. Rep*. SANS Institute, 2021.

[15] A. Ramsdale, S. Shiaeles, and N. Kolokotronis, "A comparative analysis of cyber-threat intelligence sources, formats and languages," *Electronics*, vol. 9, no. 5, p. 824, 2020.

[16] A. P. Consortium, "Data format specification," ACDC Project, Deliverable Report D1.7.2, July 2015. [Online]. Available: https://acdc-project.eu/wp-content/uploads/2015/11/ACDC_D1.7.2_Data_Format.pdf

[17] D. Shackleford, "Cyber threat intelligence uses, successes and failures: The sans 2017 cti survey," *SANS Institute*, 2017.

[5] https://oasis-open.github.io/cti-documentation/taxii/intro.html

[6] https://www.misp-project.org/l

[7] https://www.bmbf.de

[8] https://www.zensim-project.de