MITRE ICS Attack Simulation and Detection on EtherCAT Based Drinking Water System

2021 9th International Symposium on Digital Forensics and Security (ISDFS) | 978-1-6654-4481-1/21/$31.00 ©2021 IEEE | DOI: 10.1109/ISDFS52919.2021.9486331

Firdevs Sevde TOKER
Computer Eng.Dep.
Sakarya University
Sakarya, Turkey
firdevstoker@sakarya.edu.tr

Kevser OVAZ AKPINAR
Computer Eng.Dep.
Sakarya University
Sakarya, Turkey
kovaz@sakarya.edu.tr

İbrahim ÖZÇELİK
Computer Eng.Dep.
Sakarya University
Sakarya, Turkey
ozcelik@sakarya.edu.tr

***Abstract*— Industrial control systems (ICSs) are complex systems due to the technology and protocol diversity they contain. Operational Technology (OT), an ICS operating structure, has different performance and security requirements than the standard IT infrastructure. ICS systems consist of field devices where operational processes take place and control systems that provide management of these devices. Attackers are involved in the whole process after gaining access from the control layer. As a result, critical infrastructure systems are threatened by cyber-attacks. Therefore, continuous monitoring and security audits are also necessary processes for critical infrastructures. In this study, studies on the cyberattack and detection system were carried out on the critical infrastructures of the water management process. On the EtherCAT-based water management process, six different attack vectors for field devices were developed by the techniques in the MITRE ICS ATT&CK matrix, and these attacks were separated by data obtained from network traffic and determined by the SVM algorithm. Attack scenarios were created by selecting seven different MITRE ICS ATT&CK matrix techniques for attacks on the SCADA system in the control center via the engineering computer on the same process. Wazuh HIDS was used for the intrusion detection system for the SCADA system. Visualization of both attacks was done on ELK.**

Keywords*— *critical infrastructures, cyber security, MITRE ICS, EtherCAT, intrusion detection, water management

I. INTRODUCTION

ICS is the intersection of the physical world and the cyber world. Therefore, the system requirements and the operation of the processes are a little more complicated than the standard informatics infrastructure. To give an example to industrial control systems, systems that have an essential place in daily life, such as energy distribution systems, water management systems, intelligent transportation systems, natural gas distribution systems, are the main ones. Especially in recent times, the risk has increased substantially with the enabling of remote use and control of industrial control devices. In other words, while the systems were previously operated in isolation, the cyber-physical structure has now become integrated. In a study conducted by IBM [1], cyber attacks on the OT side where critical infrastructures are running indicate an increase of 2,000 percent. This increase is one of the main reasons for the expansion of attack surfaces for cyber attackers due to decreasing controls as institutions and industrial structures grow. Therefore, it has become necessary to operate cybersecurity processes such as security controls in critical infrastructures, continuous system monitoring, periodic penetration tests, and follow-up of related systems tightening.

When literature studies are analyzed, there are different approaches for attack detection systems. Machine learning-based detection systems [2], [3], [4] detection system development by open source IDS tools [5], and detection with categorical based classification [6], [7] are some of these approaches. As can be seen from the literature examples, although intrusion detection methods in ICS are carried out with various tools, new methods continue to be developed. We used two different detection systems in this study. (1) SVM algorithm for attacks on field devices in drinking water systems, (2) Wazuh HIDS [8] for attacks on the SCADA system via the engineering workstation. The attack vectors were created using the techniques in the MITRE ICS ATT&CK matrix [9]. The detection system has been visualized in the ELK environment. The organizational structure of the study is as follows: In Section 2, theoretical information about MITRE ICS ATT&CK, EtherCAT protocol within the experimental method; Attack vectors for field devices and engineering computers, and application information for detection are included. The rest of this paper is organized as follows: in Section II, some background information is briefly described; in Section III, methodology about attack vectors Section IV, conclusions are given.

II. BACKGROUND

A. MITRE ATT&CK Matrix

MITRE ATT&CK Matrix [10] is database consists of tactics and techniques based on known cyber-attacks. This open and accessible structure is open to continuous improvement. It significantly contributes to the systematic performance of various tests for red and blue teams. MITRE ATT&CK techniques and procedures provide behavioral observability to detect attacks by analyzing the network and end systems [7]. MITRE ATT&CK Matrix is improved continuously, and there are three types of MITRE Matrix:

This work was supported by the Scientific and Technological Research Council of Turkey (TÜBİTAK) (Project no.118E263).

Enterprise [10], Mobile [11], and ICS [12]. We used the MITRE ICS ATT&CK Matrix type for our study. Due to the diversity of assets in industrial control systems, the ICS ATT&CK matrix was created focusing on the functional levels of the Purdue architecture and asset classes to make the correct classification [9]. While each title in the matrix defines a tactical name, techniques used for the relevant tactic are described under each heading. A technique can be classified under more than one tactic according to its intended use. There are 11 tactics and 81 techniques in the existing ICS Matrix. The matrix shows us which method APT attacks like Stuxnet, BlackEnergy, Havex, Etc—followed for damage to the critical infrastructure by APT groups. We used ICS Matrix in our study to create the Attack scenario in Section III.

B. *WAZUH Host-Based IDS and Sysmon*

Wazuh [13] is an open-source host-based intrusion detection system. It provides multiple functionalities like integrity monitoring, security monitoring, incident response, vulnerability management, etc. With the triggering of relevant events in the system, alarms are created, and potential threats are detected early, preventing severe attacks. Additional alarm rules can be written to the default alarm rules. Wazuh can be used in various architectures [14] depending on the intended use and system size. System Monitor (Sysmon) is the Windows system service and device driver for monitoring system activity and logging system events in the Windows event log. Provides detailed information about process creation processes, network connections, and changes in the file creation time [15]. We located this tool on the engineering workstation the collect critical events.

III. METHODOLOGY

In this section, we describe our methodology to attacks and detection techniques on EtherCAT-based Water Management System. Our study consist of two main approaches: making an attack by MITRE techniques and detection methods for these attack techniques. The detection system includes two particular solutions for end point (Engineering Workstation) systems and field device (PLC) systems.

A. *Testbed Environment*

The test environment topology includes managing a total of 4 stations, including one treatment station, two pumping stations, and one warehouse. Each station has PLC and I/O equipment for control (Fig 1). There are also key devices, an engineering station for configuration and programming, ET2000 probe devices for passive network listening, and an HMI panel (Fig 2) for management/monitoring. Our study was carried out in real devices and modeled water process in Sakarya University Critical Infrastructure National Testbed [16] center.

B. *Attack Vectors for ICS Network*

This section discusses the safety aspect of using the EtherCAT protocol at the factory level. The Ethercat protocol does not contain basic security parameters such as standard authentication, encryption, and authorization used in information technologies. Therefore, media access control has been vulnerable to leaks, remote data acquisition, and other advanced attacks requiring advanced information. There are various EtherCAT protocol-based anomaly detection methods in the literature: machine learning for device level [4], periodicity-based [17], and fuzzing methods [18]. However, we analyze AMS and EAP sub-protocols that enable EtherCAT to communicate at factory level, which is not in other studies.

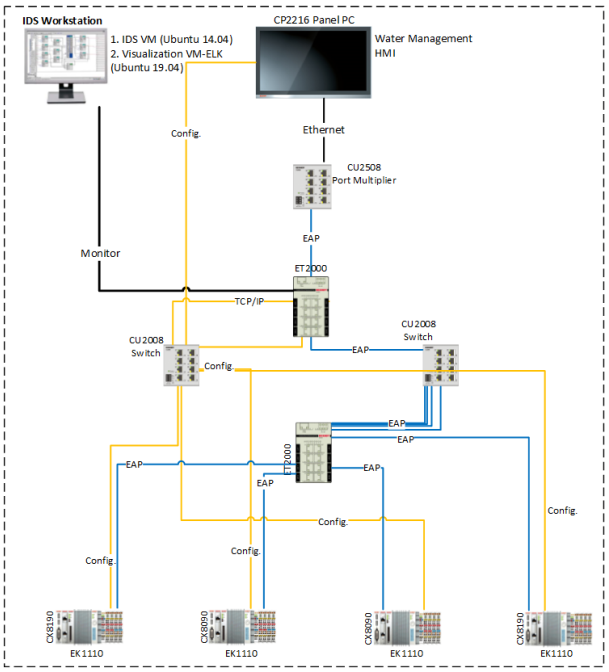

Fig. 1. Testbed environment

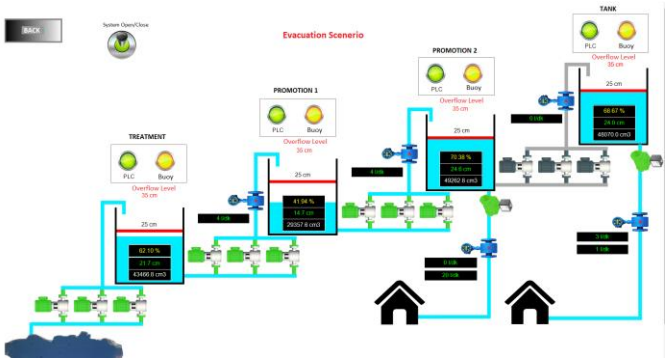

Fig. 2. Evacuation scenerio control screen

TABLE I. MITRE ICS ATT&CK Tecnhiques

Tactic Name	Technique ID - Name	Our Method
Impair Process Control	T0855- Unauthorized Command Message	The water level information was changed unauthorized, so the PLC changed the working state of the motors.
Inhibit Response Function	T0858- Utilize/Change Operating Mode	Putting the PLC device into config/reconfig mode
	T0816- Device Restart/Shutdown	Restarting and shutdown PLC Devices
	T0814- Denial of Service	The water process was disabled by making a DDOS attack on the PLC device.

- T0855 attack in Table I, EAP communication, which carries the data information between PLC devices, rested from the Probe (ET2000) device in the test environment. The water level was changed, and the water was pumped into the filled water container as if there was a small amount of water. The system has been manipulated by running the motors that should not work in the same way.
- T0816 and T0858 attacks in Table I, PLC configuration statuses are transmitted via AMS protocol. With the TwinCAT program running on the engineering computer for AMS communication, during the transition of PLCs from working to configuration state, network registration was recorded with ET2000 device. When the saved AMS PCAP file is examined, the ADS State field has been changed for PLC devices to switch from working to configuration. C++ code developed to make for these attack vectors in the testbed.
- T0814 attack in Table I, With high network traffic over a single source, the running system has been able to stop the water treatment process. The PCAP file received from the system was stopped by creating a large number of network flows by giving the loop parameter 5000000 of the *tcpreplay* tool in the Kali operating system.

C. *Attack Vectors for End Point Systems*

Many APT attacks on natural systems have been carried out by taking advantage of the lack of security controls such as misconfiguration, no security tightening, or lack of authentication. There are various social engineering methods to provide initial access to the system. In this study, assuming the attacker is in Layer 3 of the Purdue architecture, possible APT scenarios have been implemented on the existing water process. The scenarios realized were created according to the tactics and techniques in the MITRE ICS ATT&CK matrix. In our study, we create two attacks scenario for simulating APT behaviors. We selected techniques from the MITRE ICS ATT&CK matrix step by step for two attack scenarios (Fig 3).

1) Attack Scenario 1

There are three different scenarios in the water process based on the various working principles of motors and valves, namely evacuation, circulation, and treatment. In the evacuation scenario, the motors of the dam in the system do not work typically. The attack vector aims to make the motors in the dam run when the evacuation scenario is selected.

Step 1: Initial Access/ Replication Through Removable Media (T0847), A USB device that includes reverse shell exe to attacker machine is attached to engineering workstation.

Step 2: Initial Access/ Engineering Workstation Compromise (T0818), The previous technique provides that attacker access to engineering workstation persistently. The "Migrate" process has been done to continue in privileged mode on the engineering computer. While performing the "*migrate*" process, "*RtkAudioService64.exe*", a process belonging to the system user, was made according to the process number.

Step 3: Discovery/ Remote System Discovery (T0846), Using the MAC addresses in the ARP table of the engineering computer, the model of Ethernet cards was determined to be Beckhoff PLC.

Step 4: Lateral Movement / Program Organization Units (T0844), The TwinCAT development environment of the program required for the development and installation of the program that enables the control of Beckhoff PLC devices has been found in the internet environment. The processes running on the target computer are listed, and the POU file containing the PLC codes has been found on the engineering workstation machine. The POU file was downloaded from the engineering workstation to the attacker machine via injected malicious exe file. Dam motors have been changed to TRUE in the condition of *scenario_secim=3* in Fig 4.

Step 5: Execution/ Project File Infection (T0873), PLC logic control code changed in the previous step. However, this change in the attacker machine, not in the engineering workstation. The changed POU file was uploaded to the same directory in the engineering workstation.

Step 6: Impair Process Control/ Modify Control Logic (T0833); for the logical change made in the previous technique to be effective in PLCs, the "Activate Configuration" process must be done by the TwinCAT program. An attacker machine caused this process.

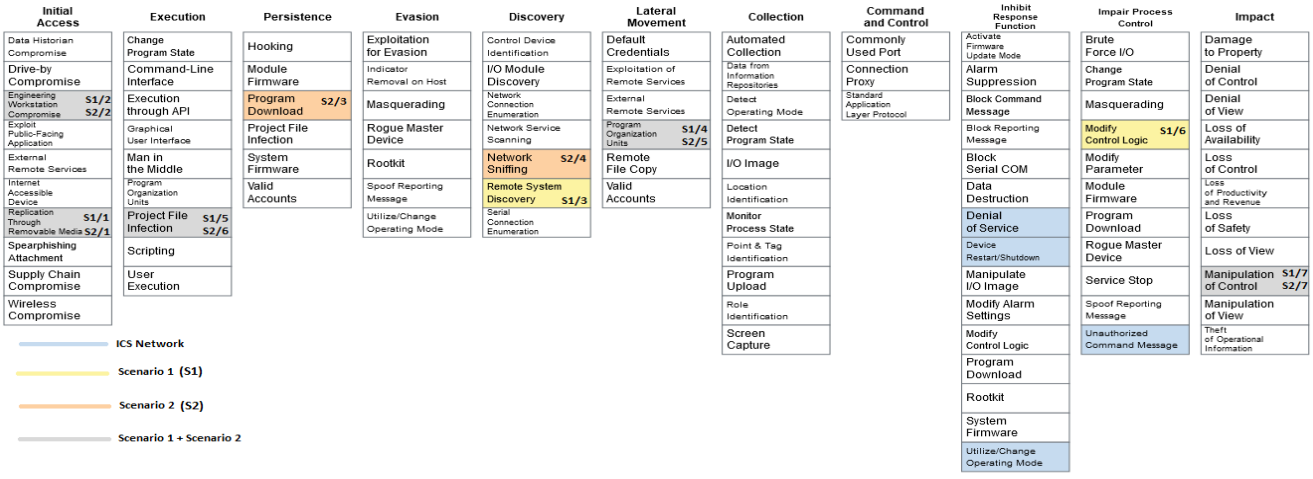

Fig.3. MITRE ICS ATT&CK techniques

```
IF senaryo_secim=3 THEN
    baraj_veri.motor1:=TRUE;
    baraj_veri.motor2:=TRUE;
    baraj_veri.motor3:=TRUE;
    IF su_yeterli THEN
        IF terfi_1_suSeviyesi<24 THEN
            aritma_veri.motor1:=TRUE;
            aritma_veri.motor2:=TRUE;
            aritma_veri.motor3:=TRUE;
        END_IF
        IF terfi_1_suSeviyesi>25 THEN
            aritma_veri.motor1:=FALSE;
            aritma_veri.motor2:=FALSE;
            aritma_veri.motor3:=FALSE;
        END_IF
        ELSE //su yeterli else
            aritma_veri.motor1:=FALSE;
            aritma_veri.motor2:=FALSE;
            aritma_veri.motor3:=FALSE;
    END_IF
END_IF
```

Fig.4. PLC POU file

Step 7: *Impact/ Manipulation of Control (T0831),* As a result of all steps, when the "Evacuation Scenario" is selected from the HMI interface in the water process, the control has been changed to unauthorized by ensuring that the motors that should not work for the dam will run.

2) Attack Scenario 2

In the water process, attack vectors have been applied to the PLC device that controls the treatment tank to perform the same operations regardless of the scenario selection. An essential step in this attack, different from the previous one, is to ensure persistence through routing the engineering computer to the C&C server (Fig 5).

Step 1 and *Step 2* are performed by applying the same method as specified in Attack scenario 1.

Step 3: Persistence/ Program Download(T0843), Although this technique in the ICS matrix is not defined for the engineering computer, it has been interpreted in this technique because it has a similar effect. The *.vbs* code connected from the Kali virtual machine to the Ubuntu 19.10 virtual machine has been created on the engineering computer. Thus, it was transferred to the C&C server, where the commands to continue the attack will be executed. Since the *.vbs* code created in the engineering workstation can communicate with C&C when the computer is turned off and on again, persistence has been achieved on the system.

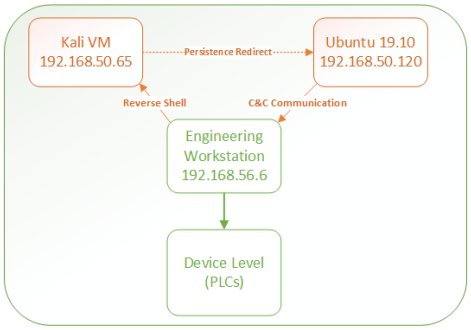

Fig.5. Attack flow of Attack scenario 2

Step 4: Discovery/ Network Sniffing (T0842) and Network Connection Enumeration (T0840), Packages sniffed from the engineering computer were examined. The AMS sub-protocol of the EtherCAT protocol was detected from the network traffic.

Step 5: Lateral Movement/ Program Organization Units (T0844), same as Step5 in attack scenario 1.

Step 6: Execution/ Project File Infection(T0873), same as Step 5 in attack scenario 1.

Step 7: Impact/ Manipulation of Control (T0831), As a result of this attack, the working principle of the PLC device, which controls the water process in the water treatment tank, did not change regardless of the scenario selected on the HMI screen. Manipulation occurred in the control center.

D. Anomaly Detection and Visualization for ICS Network

SVM algorithm was used to detect the attack vectors created in the previous section. According to the detection program of the attacks carried out at the factory level, learning is carried out from the traffic flowing in real-time. The parameters to be used to detect attacks from this learning are parsed and saved in the CSV file. The model formed as a result of the learning has been kept in a file. Subsequent attacks were evaluated according to this model, and the states of PLC devices were classified. Classified attacks were transferred to the ELK system and visualized.

The flow given in Fig 6 was realized on Ubuntu 19 with Python3 programming language. A linear SVM algorithm is used. In the learning part of the SVM algorithm, five attributes are used as features. These are defined in Table II according to their intended use.

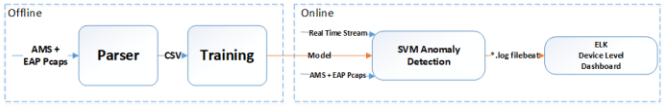

Fig.6. Anomaly detection for ICS Network

TABLE II. Features for SVM Algorithm

Features	Purpose of Usage
CMD ID	It determines the command types of packets sent and received in communication between PLCs.
ADS State	It is a variable that keeps the instant status of PLC devices.
Protocol	It represents a protocol-based definition, as many sub-protocols are used at the factory level.
Data Length	The EtherCAT factory-level process data is carried in the data area. In the topology used, data such as the level information of the stations are transmitted in this area.
Packet Count	It is chosen for situations where the number of packages is decisive, such as DoS. The attribute value is determined by looking at the time between arrivals between 2 consecutive packets.

An open-source ELK Stack is used to visualize the attacks. The log files resulting from the SVM attacks were transferred to the ELK machine with filebeat. Dashboard screens, where

detailed data of attacks are displayed graphically, have been created in Kibana (Fig 7).

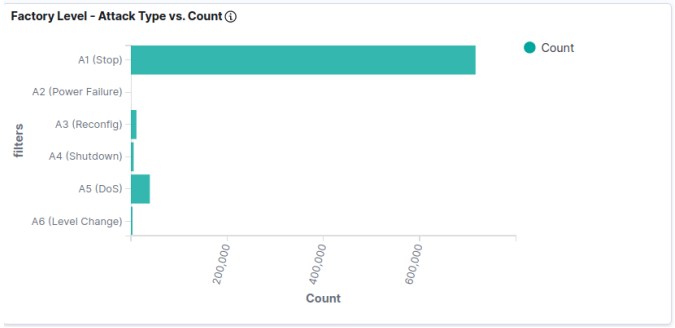

Fig.7. Anomaly detection dashboard

E. *Anomaly Detection and Visualization for End Point Systems*

Wazuh open source HIDS was used to detect the attacks carried out in section C. The ossec-agent component that sends events to the Wazuh tool is installed in the engineering computer. The agent sends its logs to the central server (Fig 9). The alarms on the main server will be displayed on the Kibana interface thanks to the Wazuh extension installed on Kibana.

Sysmon tool is also included in Wazuh alarms to monitor logs that do not generate default, such as process create/delete, WMI Event. The rule file has been reconfigured for the Sysmon tool to classify techniques [19] in the MITRE ATT&CK Enterprise matrix.

The analysis of the attacks in the C part according to the events that took place in the engineering computer was made as follows:

As a result of the "*migrate*" process of both attack scenarios in Step 2, a new process operating under the same process is formed. This situation causes a "*File Create*" type log to be created in Sysmon with Event ID = 11 value. The "*File Create*" event is significant as it detects newly created suspicious files. The alarm of this event is indicated in Fig 8.

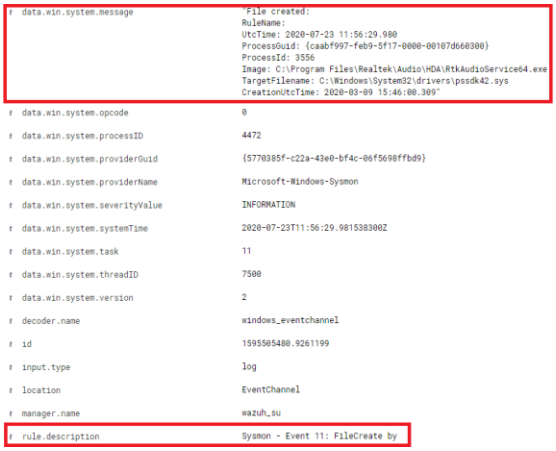

Fig.8. Wazuh file create alarm

In Step 3 of the attack scenario 2, a file consisting of random letters is created in the engineering computer to direct the *.vbs* code to the C&C server and provide persistence. C&C server and engineering computer communicate by accessing this file. Therefore, the alarm similar to specified in Fig 8 occurs.

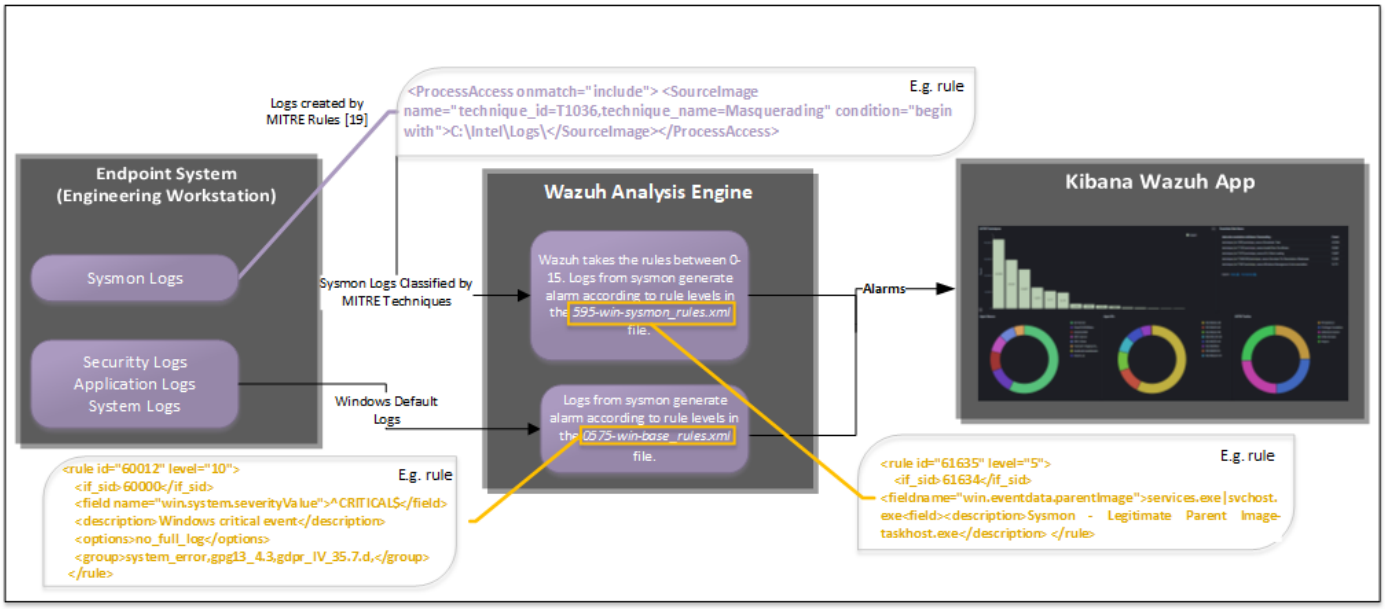

Fig.9. Wazuh HIDS Workflow

Various graphs have been created in the Kibana tool to analyze alarms with appropriate filters quickly. These graphs are collected in a dashboard structure. For example, in attack scenarios, a continuous connection is provided during the sending of commands. Therefore, since the connection process is accessed chiefly (185) (Fig 10), the "*Process Access*" rule is unified.

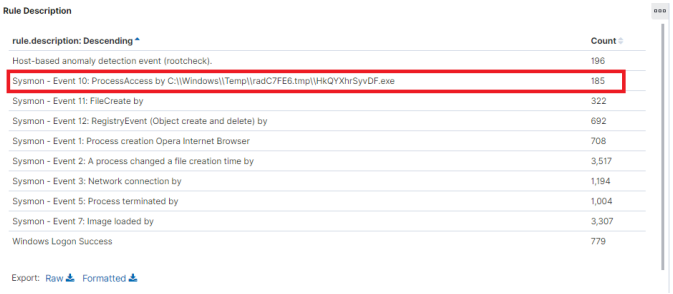

Fig. 10. Process access count by event log count

IV. CONCLUSIONS

In industrial control systems, existing and new attacks continue to threaten organizations. Due to its critical impact on both financial and human life, it is crucial to manage, detect and prevent security vulnerabilities to prevent these attacks. In our study, a solution proposal has been developed that provides possible attacks and detection of both end point devices and SCADA system in an EtherCAT-based water process. The attacks and detection system do not offer a solution for zero-day vulnerabilities. With this study, the machine learning algorithm for the field level for detecting cyber attacks that may occur at the factory level against the EtherCAT protocol; An intrusion detection system with Wazuh HIDS was developed for the control center.

The monitoring of devices is facilitated with the ELK system, which is integrated to monitor the system. It was ensured that information about essential criteria such as analysis of attacks over time and tracking system vulnerabilities was obtained through both visual and numerical ratios. If it is desired to get instant information from the operations performed in the test environment, it is possible to add visuals.

In future studies, solutions for both attack and detection can be diversified on this matrix. Periodic up-to-date studies of this matrix can also provide continuous traceability of the system. When the logs generated by the Wazuh server are generated at certain levels, they direct them to the SIEM product, allowing a more comprehensive correlation. Network-based monitoring can be done by setting up NIDS in water process communication and sending network-based events to the Wazuh server for analysis.

REFERENCES

[1] J. Wheeler, "Modernizing Threat Management for the Evolving Attack Surfaces of OT, IoT and IoMT," 2019. https://securityintelligence.com/posts/modernizing-threat-management-for-the-evolving-attack-surfaces-of-ot-iot-and-iomt/ (accessed Jun. 07, 2020).

[2] J. Inoue, Y. Yamagata, Y. Chen, C. M. Poskitt, and J. Sun, "Anomaly detection for a water treatment system using unsupervised machine learning," *IEEE Int. Conf. Data Min. Work. ICDMW*, vol. 2017-Novem, pp. 1058–1065, 2017, doi: 10.1109/ICDMW.2017.149.

[3] F. A. Alhaidari and E. M. Al-Dahasi, "New approach to determine DDoS attack patterns on SCADA system using machine learning," *2019 Int. Conf. Comput. Inf. Sci. ICCIS 2019*, pp. 2–7, 2019, doi: 10.1109/ICCISci.2019.8716432.

[4] K. O. Akpinar and I. Ozcelik, "Analysis of Machine Learning Methods in EtherCAT-Based Anomaly Detection," *IEEE Access*, vol. 7, pp. 184365–184374, 2019, doi: 10.1109/ACCESS.2019.2960497.

[5] A. GRANAT, H. HÖFKEN, and M. SCHUBA, "Intrusion Detection of the ICS Protocol EtherCAT," *DEStech Trans. Comput. Sci. Eng.*, no. cnsce, 2017, doi: 10.12783/dtcse/cnsce2017/8885.

[6] J. Zhang, S. Gan, X. Liu, and P. Zhu, "Intrusion detection in SCADA systems by traffic periodicity and telemetry analysis," *Proc. - IEEE Symp. Comput. Commun.*, vol. 2016-Augus, pp. 318–325, 2016, doi: 10.1109/ISCC.2016.7543760.

[7] R. Al-Shaer, J. M. Spring, and E. Christou, "Learning the Associations of MITRE ATT&CK Adversarial Techniques," 2020, [Online]. Available: http://arxiv.org/abs/2005.01654.

[8] "Wazuh Anomaly and Malware Detection." https://documentation.wazuh.com/3.13/user-manual/capabilities/anomalies-detection/how-it-works.html (accessed Jul. 05, 2020).

[9] J. Steele, "MITRE ATT & CK ® for Industrial Control Systems : Design and Philosophy Authors : Otis Alexander Misha Belisle," no. March, 2020.

[10] "ATT&CK Matrix for Enterprise." https://attack.mitre.org/ (accessed Jun. 28, 2020).

[11] T. M. Corporation, "Mobile Matrices." https://attack.mitre.org/matrices/mobile/.

[12] "ATT&CK® for Industrial Control Systems." https://collaborate.mitre.org/attackics/index.php/Main_Page (accessed Apr. 20, 2020).

[13] "WAZUH." https://wazuh.com/.

[14] "WAZUH Architecture." https://documentation.wazuh.com/3.12/getting-started/architecture.html (accessed Jun. 10, 2020).

[15] T. G. Mark Russinovich, "Sysmon." https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon.

[16] "Critical Infrastructures National Testbed Center." https://center.sakarya.edu.tr/.

[17] K. O. Akpinar and I. Ozcelik, "Methodology to Determine the Device-Level Periodicity for Anomaly Detection in EtherCAT-Based Industrial Control Networks," *IEEE Trans. Netw. Serv. Manag.*, vol. 4537, no. c, 2020, doi: 10.1109/TNSM.2020.3037050.

[18] K. O. Akpinar and I. Ozcelik, "A Standalone Gray-Box EtherCAT Fuzzer," in *2018 2nd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*, Oct. 2018, pp. 1–4, doi: 10.1109/ISMSIT.2018.8566695.

[19] O. Hartong, "A Sysmon configuration repository for everybody to customise." https://github.com/olafhartong/sysmon-modular/blob/master/sysmonconfig.xml (accessed May 04, 2020).