Leveraging Digital Twins and SIEM Integration for Incident Response in OT Environments

Adei Arias, Cristobal Arellano, Aitor Urbieta
Ikerlan Technology Research Centre,
Basque Research and Technology Alliance (BRTA)
Arrasate-Mondragón, Spain
{aarias,carellano,aurbieta}@ikerlan.es

Urko Zurutuza
Department of Electronics and Computing
Mondragon Unibertsitatea
20500 Arrasate, Gipuzkoa
uzurutuza@mondragon.edu

***Abstract*—The Industrial Internet of Things (IIoT) has digitally transformed industrial processes albeit at the expense of increasing exposure to new security threats. System Information and Event Management (SIEM) systems, typically designed for Information Technology (IT), may struggle with the high data volume, specialized security needs, and real-time response requirements of IIoT environments. Digital Twins (DT), virtual replicas of physical devices, offer a solution to these challenges. By integrating SIEM with DT, incident response can be automated in Operational Technology (OT) environments. This integration enhances real-time threat detection, response coordination and post-incident tasks to ensure the security and continuity of industrial operations. A use case and prototype validate the effectiveness of this approach and highlight its potential to strengthen OT security in the face of evolving threats.**

***Index Terms*—IIoT, Digital Twins, Threat Detection, Incident Response, Attack Detection**

Type of contribution: *Original research*

I. Introduction

The IIoT has digitally transformed industrial processes, offering increased productivity, reduced downtime, and predictive maintenance capabilities. Leveraging on interconnected networks of devices and sensors, IIoT facilitates real-time insights and remote monitoring and control of industrial equipment and processes [1].

However, the advantages of IIoT are accompanied by significant security challenges. Firmware and software vulnerabilities, supply chain attacks, Zero-day exploits, and insider threats pose risks to IIoT systems [2]. Research indicates that a majority of organizations operating industrial systems have experienced damaging security events, underscoring the need for robust security measures [3].

The increasing complexity and scale of IIoT systems render manual incident response solutions impractical. There is an urgent need to automate incident response in IIoT environments to detect and respond to security threats in real-time, minimize operational disruptions, and ensure continuous industrial processes [4].

Recent literature suggests DT as an effective solution for automated incident response in IIoT environments [5], [6]. DT offer automated and efficient solution for incident response tasks while limiting the installation of external software. They provide a means to manage security incidents more efficiently, particularly for low-resource IIoT devices, by leveraging on greater computational capacity [7], [8].

DT also demonstrate effectiveness when integrated with SIEM systems for attack detection due to their real-time monitoring. This integration allows for efficient threat detection, analysis and response [9].

Moreover, DT can support security operations by providing a virtual environment for training and testing security measures, allowing security teams to simulate various attack scenarios and develop effective incident response plans [10].

SIEM systems aggregate, analyze, and correlate data from various IT infrastructure sources, providing real-time visibility into security events by collecting logs and alerts from devices. They detect potential incidents through pattern detection and anomaly analysis.

Despite research progress in automating incident response through DT and their integration with SIEM systems, there is a gap in applying this integration to OT environments. While SIEM systems are primarily designed for IT environments, there are specific systems for industrial settings, such as Splunk Enterprise Security [1], IBM QRadar [2], or Siemens Eos. However, applying these systems in OT environments faces challenges due to the limited computational resources of IIoT devices. This limitation often renders SIEM agents inoperable on many industrial devices. Therefore, a DT serves as essential middleware to facilitate communication with IIoT devices, enabling the execution of response scripts. This allows SIEM systems to concentrate on threat analysis while coordinating with firewalls or other DT solutions for attack response in OT environments.

The main contributions are summarized as follows:

- Definition of the requirements for designing and implementing a DT and SIEM integration solution customized for OT environments
- Implementation of both a use case and a prototypical implementation for validating the solution

The paper is organized as follows. Section II outlines IIoT networks, Threat Detection & Incident Response (TDIR) and DT foundations. Section III describes related work. Section IV depicts the general requirements of the proposed platform. A use case and a prototype are presented in section V. Then, different attack scenarios are emulated in order to evaluate the solution in section VI. Afterwards, the results of the evaluation are discussed in section VII. Section VIII concludes the work and presents the future work.

[1]https://www.splunk.com/en_us/products/enterprise-security.html
[2]https://www.ibm.com/es-es/qradar

II. Background

This section elaborates the background on IIoT networks, TDIR, and DT for cybersecurity.

A. IIoT Networks

IIoT networks refer to the utilization of smart devices such as sensors, actuators, and other connected devices to optimize manufacturing and industrial processes [11].

Despite their potential benefits, IIoT devices are inherently vulnerable due to factors deriving from their design, deployment, and management [12]. These vulnerabilities, which include weak authentication, lack of encryption, and inadequate physical security measures, expose IIoT networks to various threats [13] such as:

- Denial of Service (DoS): These attacks in IIoT environments aim to disrupt normal system operation by overwhelming critical resources. Traditionally, DoS attacks focused on saturating network bandwidth, making services unavailable. However, in IIoT, attackers can target a wider range of resources, including processing power, memory, storage capacity, and even a device's sleep cycle. Implementing firewalls or Intrusion Detection System (IDS) can mitigate such attacks.
- Man in The Middle (MiTM): Attackers intercept and modify data exchanged between devices. Encryption protocols or One Time Password (OTP) authentication can prevent unauthorized access in such scenarios.
- Replay attacks: Attackers capture and resend packets to mislead operators or compromise control systems. Adding timestamps to packets can prevent such attacks from occurring.
- Crafted packet injection: Malicious packets are sent to disrupt the normal operation of applications. Proper authentication and authorization mechanisms can mitigate the impact of such attacks.

It is important to address these vulnerabilities through robust cybersecurity practices and compliance with regulations, such as the Cyber Resilience Act (CRA), which aims to enhance cyber resilience in the European Union [14]. Additionally, the IEC 62443 standard provides specific guidelines for securing industrial automation and control networks, helping protect IIoT networks against threats and attacks [15].

B. Threat Detection and Incident Response (TDIR)

Threat detection along with prevention and incident response cover the three core cybersecurity functions [16]. It involves monitoring the threat landscape to identify and assess the risks that could potentially disrupt operational processes. This threat landscape changes daily due to multiple factors such as the emergence of new vulnerabilities or software changes. Therefore, a proactive analysis is essential to anticipate potential attacks [17]. Commonly employed technologies for facilitating threat detection include SIEM, IDS, and Machine Learning (ML) models [18].

Incident response aims to reduce cyber-attacks before they occur and to reduce their consequences. A general incident response plan outlines what steps should be taken whenever a specific type of cyberattack is detected [19]. This plan helps cybersecurity teams detect and contain threats, restore affected systems and reduce costs. According to the National Institute of Standards and Technology (NIST) [20], there are four steps that every response plan should follow:

- Preparation: Establishes an incident response team, defines roles, and develops incident response policies and procedures, ensuring the availability of necessary tools.
- Detection and Analysis: Monitors applications, systems, or networks for anomalies using technologies like IDS, SIEM, or Anomaly Detection System (ADS). Analyzes detected incidents to determine their nature and impact for an appropriate response.
- Containment, Eradication, and Recovery: Quickly contains incidents to prevent further damage or unauthorized access. Techniques include isolating affected systems, blocking malicious traffic, and disabling compromised accounts. Then, identifies the root cause and restores affected systems, followed by returning operations to normal.
- Post-Incident Activity: Involves lessons learned, documentation, and improvement. Organizations conduct post-incident reviews to assess response efficacy, identify areas for enhancement, and refine response plans accordingly.

C. Digital Twins for Cybersecurity

DT are virtual replicas of physical objects or systems that are continuously updated with data coming from their physical counterpart. They can be used to monitor performance, test scenarios, predict issues, and find optimization opportunities among many other applications. They leverage various technologies such as sensors, Internet of Things (IoT) devices, data analytics, and simulation models to create a digital counterpart of a physical entity [21].

Security professionals can also be supported by the use of DT. This technology enables replication, simulation, and historical data analytics security modes [10]. In replication, DT function as virtual replicas of physical assets, enabling real-time monitoring and analysis of their performance and security. Through simulation, security incidents like cyber-attacks can be replicated within a virtual environment, providing insights into potential vulnerabilities. Additionally, DT gather historical data for analysis, aiding in the identification of patterns and potential threats to enhance security posture. However, while DT offers significant benefits, it also increases the attack surface, as authors in [22] state. Notable risks include:

- Unauthorized physical access: DT could be compromised by gaining unauthorized access to the physical devices.
- Malicious data injection: Attackers could in an unauthorized way inject malicious data into the simulation process, leading to inaccurate results and bad decisions.
- Data exfiltration: Attackers could exploit a potential vulnerability to exfiltrate data and destroy services.

III. Related Work

The integration of DT into cybersecurity, particularly for enhancing incident response and security analytics in physical systems and IoT, has garnered significant attention in recent research. This section reviews existing studies that explore the

application of DT in cybersecurity and identifies the novel contribution of the proposed research.

Recent studies have explored various aspects of DTs' application in cybersecurity. For instance, authors in [23] examine the use of DT to support cybersecurity, specifically in Cyber-Physical System (CPS). The study provides a comprehensive analysis of how DT can be applied to enhance incident response playbooks for CPS cybersecurity, proposing a structured approach for incident response with DT.

Research has also demonstrated the viability of integrating DT security simulations into Security Operations Center (SOC) to enhance situational awareness and incident response capabilities [10]. Additionally, the literature covers the application of DT in anomaly detection within physical systems [23] and predictive maintenance [24].

Moreover, authors in [9] introduce a formal model for integrating DT with security analytics for IoT, emphasizing the need for additional research on implementing security monitoring and analytics utilizing DT. Additionally, the same authors introduce in [5] the SOAR4IoT framework, which adapts Security Orchestration, Automation, and Response (SOAR) to IoT by making IoT assets manageable via middleware to secure them. The research focuses on orchestrating incident response for IoT devices using DT. They demonstrate its feasibility through experimental setups that cope with Mirai and Sybil malware.

The proposed research aims to address the gap in integrating DT with SIEM systems to automate incident response in OT environments. While existing frameworks like SOAR4IoT utilize DT for incident response in IIoT devices, this work extends to enhance security specifically in OT settings by providing a comprehensive solution for automated threat detection and response.

The proposed integration of SIEM with DT allows direct communication with industrial devices to execute response scripts, freeing SIEM to prioritise threat analysis and communication with other network assets such as firewalls. This improves automation in OT environments, although SIEM systems were originally designed for IT environments. This synergy between SIEM and DT supports real-time threat detection and response, leading to improved security measures in industrial systems. The research aims to develop and implement an optimised integration framework that improves incident response capabilities and strengthens the cybersecurity posture in OT environments.

IV. Platform Requirements

This chapter introduces the identified requirements for the proposed platform. These requirements provide a clear understanding of the criteria guiding the platform's development. The platform requirements have been determined based on the excellent adaptability of DT both in managing security in IoT devices [25] and in integrating with tools such as SIEM or IDS [10]. Figure 1 depicts a general overview of the requirements of the platform.

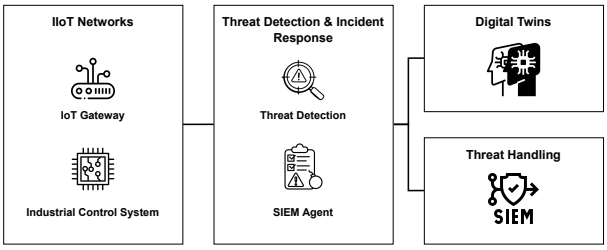

Figure 1. Platform requirements.

A. Operational Requirements

- *Communication with IIoT devices:* Given the critical importance of responding to attacks in OT environments, there is a need of communicating with IIoT to respond to attacks. DT replicate the lifecycle of IIoT devices and facilitate bidirectional communication with their physical counterparts, serving as essential conduits for incident response actions. The use of DT is shown more specifically in Figure 2.

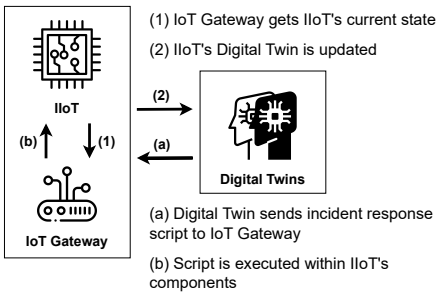

Figure 2. Digital Twins working flow.

- *Monitoring of IIoT networks:* The platform mandates continuous monitoring of IIoT networks, with each network asset associated with a DT. This ensures real-time monitoring and provides a channel for issuing commands to physical industrial devices. Simultaneously, robust threat detection mechanisms are imperative. These mechanisms utilize ADS or IDS to swiftly identify potential threats and anomalies, ensuring the security and integrity of IIoT networks. Additionally, monitoring networks is beneficial due to its low intrusiveness, a crucial aspect in maintaining system stability and minimizing disruptions in industrial operations.
- *Incident handling and integration of response agents:* The platform requires an incident handling process that facilitates seamless communication between incident response agents and enables thorough investigation into detected incidents. These agents must execute responses at the infrastructure level and seamlessly coordinate with DT to command responses to physical industrial devices. This process encompasses structured procedures for incident triage, investigation, containment, eradication, and recovery, ensuring efficient incident management and resolution.

B. Security Requirements

- *Network Segmentation and Packet Filtering:* It is required to segment the network to isolate critical components and implement packet filtering to control traffic flow between network segments.

- *Role-Based Access Control (RBAC):* Implement RBAC to define authorization and control at DT and threat handling platforms. Ensure proper assignment of roles and permissions to restrict unauthorized access and actions.

V. System Design and Implementation

This section presents the specific use case implemented to test the platform. Afterwards, the tools used to deploy the proposed prototype are presented. Finally, an incident response model is presented to assess the integration between the DT and the SIEM.

A. Use case design

An Industrial Control System (ICS) is required to test the proposed platform. This industrial system should resemble a real system as closely as possible in order to obtain meaningful results.

Specifically, it was decided to implement an industrial water tank, as this is one of the most common systems in OT [26] environments. This tank was designed according to the requirements defined by the authors in [27], [28], and its implementation is based on the water tank implemented in [29].

A general overview of the architecture of the use case is depicted in Figure 3. The industrial water tank comprises two actuators responsible for controlling the inflow and outflow and a sensor tasked with measuring the current water level. These components are governed by a Programmable logic controller (PLC), which adjusts the state of the actuators based on the liquid level readings.

In addition to the PLC, there is a Human Machine Interface (HMI) that visually represents the tank's current state (see Figure 4). Communication between the PLC and the actuators and sensors utilizes the ModBus network protocol, while communication between the PLC and HMI is facilitated through the Message Queuing Telemetry Transport (MQTT) protocol. Moreover, the PLC hosts a Secure Shell (SSH) service for administrative purposes, while the HMI's dashboard is accessible via an Hypertext Transfer Protocol (HTTP) server.

Furthermore, an IoT Gateway has been implemented to update the industrial tank's DT and to receive incident response commands from the DT in the event of an attack detection within the system.

B. Proposed Solution

The prototype of the solution has been deployed using Virtualbox [3] virtualization platform. Concerning the architecture of the proposed platform, Figure 5 describes its prototypical implementation.

Networks are segmented using VyoS [4] routers. These components have also firewall capabilities and primarily have been used to control how traffic flows between different segments of the network. There are three primary zones within the infrastructure (see Figure 5):

- OT zone: This zone hosts the emulated water tanks.
- OT Demilitarized Zone (DMZ): This zone serves two purposes. While it is used to establish a secure channel between the OT zone and the detection zone, it also hosts Suricata [5] for threat detection, the Wazuh [6] agent for executing response scripts, and the MQTT broker for communication with the DT.
- Detection zone: This zone hosts Eclipse Ditto as the DT management platform, Wazuh and TheHive as the threat management platforms.

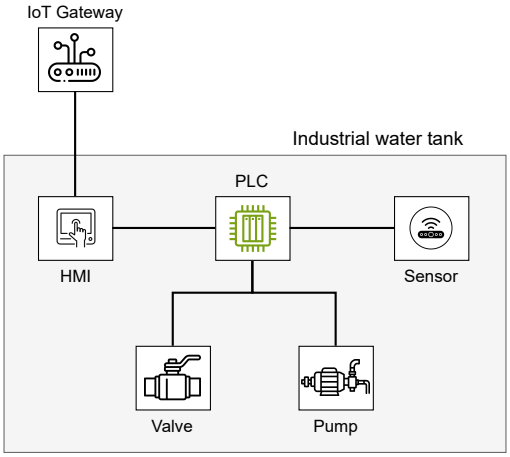

Figure 3. An industrial water tank.

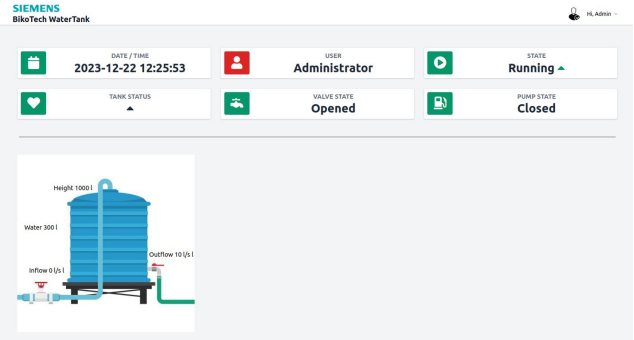

Figure 4. Industrial water tank's HMI.

Suricata IDS is set up to monitor the OT zone for potential threats. It achieves this by mirroring the network adapter and detecting attacks according to predefined rules. These rules were custom-created to focus on the principal attacks faced by industrial watertank systems, such as DoS, command injection, or brute force, as outlined in [30], [31]. Figure 6 shows an example rule aimed at uncovering unauthorized read requests on Modbus holding registers. Suricata is chosen due to its strong adaptability in OT environments [32].

Both network traffic and alerts generated by Suricata should be analyzed to respond to and mitigate potential threats. In the proposal, this network traffic is sent to the Wazuh platform for subsequent analysis. Wazuh, acting as a SIEM, meticulously collects and processes these alerts, allowing for a deeper understanding of network security by correlating and contextualizing the received data. Additionally, Wazuh

[3] https://www.virtualbox.org/
[4] https://vyos.io/
[5] https://suricata.io/
[6] https://wazuh.com/platform/overview/

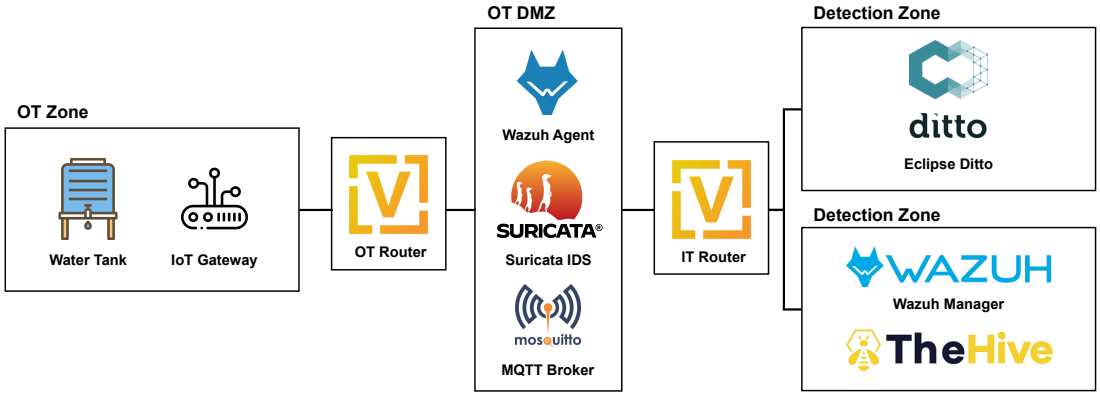

Figure 5. Proposed platform architecture.

is selected for its capability as a powerful open-source SIEM and incident response solution, automating actions to counter detected threats and ensuring timely remediation of security incidents.

Furthermore, the Wazuh agent is set up to run response scripts upon detecting attacks specified in Suricata rules. Specifically, two response scripts are configured: one for high-severity attacks and another for critical-severity attacks.

- High severity threats: These attacks may acquire sensitive information about the processes running in the application.
- Critical severity threats: These attacks represent a significant risk to the application, potentially halting or disrupting currently running processes.

This facilitates immediate action against potential threats and strengthens real-time response and risk mitigation capabilities. Following the execution of response scripts, these incidents can be further investigated to better understand the threat landscape and develop more effective countermeasures. TheHive [7] platform is deployed to manage this situation. This system empowers security professionals to handle and prioritize incidents, offering an efficient platform for enhancing overall security. TheHive is selected due to its centralized and collaborative environment for managing security incidents efficiently.

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $MODBUS_PORTS
(msg: "HIGH RISK. UNAUTHORIZED READ HOLDINGS DETECTED";
flow: established, to_server; modbus: access read holding;
classtype:potential-modbus-read; threshold: type both,
track by_src, count 10, seconds 20; sid: 17785; rev:2;)
```

Figure 6. Suricata rule to detect attacks on Modbus.

Eclipse Ditto [8] is chosen as the framework for establishing DT, with a specific focus on replicating the industrial water tank (see Figure 7). Eclipse Ditto enables message-oriented communication with IoT assets through their DT. Besides, it supports the definition of policies and the integration of specific brokers for several IoT protocols such as MQTT or Constrained Application Protocol (CoAP). Eclipse Ditto was selected due to its robustness, open-source nature, and widespread adoption in the industry.

Regarding the configuration of the DT for the water tank, policies are initially enforced. Specifically, these policies grant an admin user read and write access to the DT, its policies, and communication channels, while restricting a tank user to only have read and write access to the DT. Then, a DT is created within the platform. This mirrors the real-time status of the water tank, encapsulating vital data such as water level, pump, and valve statuses. Furthermore, messages are also defined. These messages allow users to interact directly with the digital of the tank. DT process all messages received from users separately and behave according to the message-defined function. Specifically, two types of messages have been defined. The first is used to send response scripts when critical risk attacks are detected, while the second is used to deal with high risk attacks. Last, Eclipse Ditto is connected to the Mosquitto [9] broker to establish bidirectional communication between the DT and the water tank. While data received from the DT broker updates the DT values, the DT can also send commands to the water tank.

C. Incident Response Model

The results of this research reflect the performance of the platform in detecting and mitigating the attacks in the industrial water tanks. To this end, a basic incident response plan has been created to detect and mitigate these attacks before they can disrupt tank operations. The solution has been tested by executing the attacks specified in subsection VI-A against the industrial tank. Figure 8 shows a general overview of this incident response plan.

Each arrow in the figure describes the steps involved in carrying out the process as follows:

- *(1) Incident response execution order:* The Wazuh manager initiates the incident response process upon detecting an alert from Suricata. Subsequently, it issues an order to the Wazuh agent to begin response actions to address the detected incident.
- *(2) Attacker's IP is blocked:* Wazuh agent adds a new rule to the firewall to block the attacker's IP address. This immediate action aims to halt the ongoing attack and prevent further unauthorized access.

[7] https://thehive-project.org/
[8] https://eclipse.dev/ditto
[9] https://mosquitto.org/

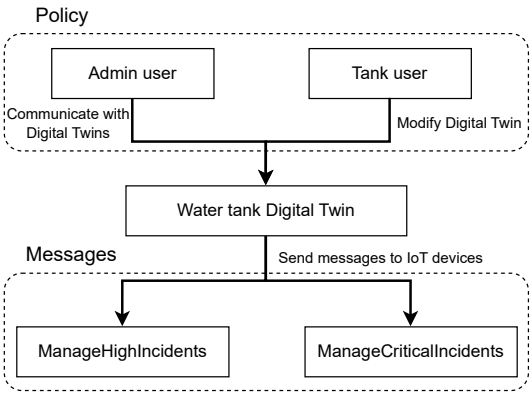

Figure 7. Digital Twins settings in Eclipse Ditto.

- *(3) Communication with DT:* Establishing communication with the tank's DT is paramount to initiating remediation commands promptly. This step ensures swift coordination between the security infrastructure and the digital representation of the industrial tank.
- *(4) Communication with the tank:* Leveraging the DT platform, such as Eclipse Ditto, facilitates seamless communication with the industrial device. Messages originating from the Wazuh agent are relayed to the tank, enabling swift execution of response commands.
- *(5) Response commands executed within the device:* The IoT gateway controlling the industrial tank receives and executes the response commands promptly. This proactive intervention aims to eradicate the threat and restore normal operations within the tank environment.
- *(6) DT's policy modification:* When it came to compromising the security of the tank, the attacker could have stolen the credentials of the communication with the twin. Therefore, usage policies are modified to limit the access of this tank to its DT until the incident has been investigated.
- *(7) Post-incident operations:* Subsequently, a comprehensive case is created within TheHive platform to facilitate in-depth investigation of the incident. Additionally, proactive measures are implemented to fortify the security posture and prevent the recurrence of similar threats.

VI. Evaluation

The performance of the proposed approach is assessed through an attack simulation on an emulated industrial water tank. Specifically, the platform's ability to detect and respond to network attacks against the virtual industrial system is tested.

A. Attack Setting

The first step is to define the attack scenario. A new virtual machine running Kali Linux [10] situated on the same network as the industrial water tank is used to simulate an internal attacker. Concerning the specific attacks executed, the following ones have been performed using various tools:

- **Modbus Register Read/Write Flood:** This attack overwhelms a Modbus system with excessive read or write requests to registers, potentially causing unresponsiveness .This attack was performed using *smod* [11].
- **Modbus Malformed Packets:** This attack involves crafting multiple requests with invalid or unexpected function codes. This can confuse the server and potentially lead to a DoS. This attack was executed using *smod*.
- **MQTT Publish/Subscribe Flood:** This attack involves overwhelming an MQTT broker with a massive amount of publish and subscribe requests, potentially causing the broker to become unresponsive and disrupting legitimate communication. This attack was executed using *mqttsa* [12].
- **Synchronize (SYN) DoS:** Sending numerous SYN packets to a target system to consume resources and render it unresponsive to legitimate traffic. This attack was launched using *hping* [13].
- **SSH Brute Force:** Systematic attempts to gain unauthorized access to a system via SSH by trying different combinations of usernames and passwords. This attack was performed using *hydra* [14].
- **HTTP Directory Brute Force:** Systematic requests for files and directories on a web server to discover hidden or unprotected resources. This attack was executed using *gobuster* [15].

These attacks have been selected based on several articles that illustrate the most likely attacks against industrial environments [30], [31].

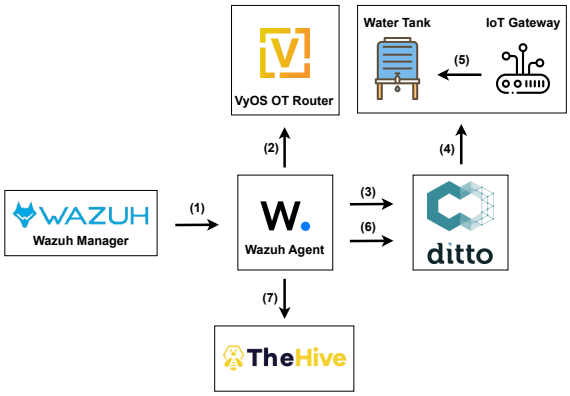

Figure 8. Incident response steps.

VII. Discussion

This section outlines the results obtained after conduction the simulations explained in subsection VI-A. Afterwards, the limitations regarding the proposed solutions are presented.

A. Discussion

The platform has demonstrated satisfactory results in detecting and responding to security threats. Specifically, the integration of a SIEM, Wazuh, with the DT, using Eclipse Ditto,

[10] http://kali.org/

[11] https://github.com/trouat/smod
[12] https://github.com/stfbk/mqttsa
[13] https://www.kali.org/tools/hping3/
[14] https://www.kali.org/tools/hydra/
[15] https://github.com/OJ/gobuster

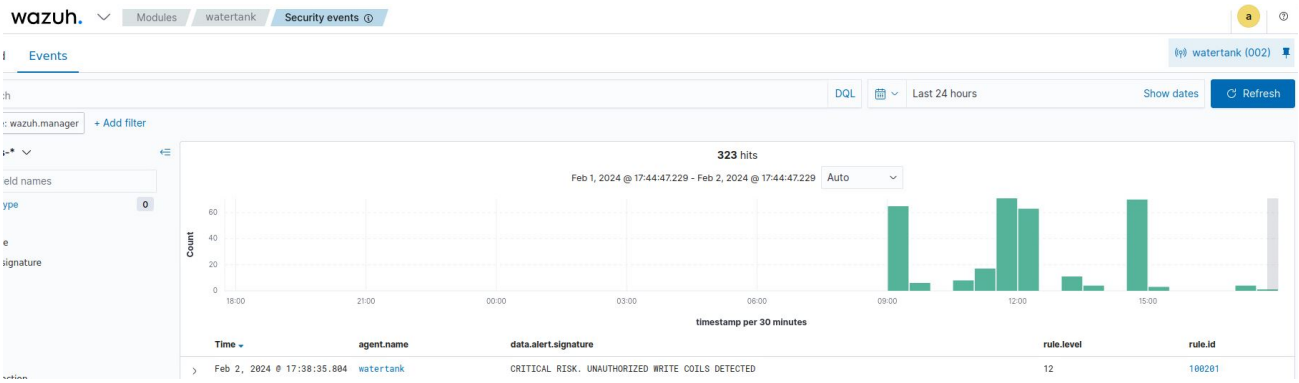

Figure 9. General overview of Wazuh dashboard.

has proven efficient in mitigating attacks on industrial devices. By promptly identifying incidents and executing predefined response plans, the system enhances overall security posture. Additionally, by using Suricata as a way to detect threats and TheHive to perform post-incident tasks, the entire incident response lifecycle as outlined by NIST is fulfilled [20].

The integration of SIEM with DT in IIoT environments presents substantial benefits. DT, by providing an abstraction and a unified interface for IIoT devices, it simplifies the process of monitoring and controlling these devices. Additionally, this abstraction allows for seamless scalability while maintaining efficient monitoring and management of IIoT devices and systems. Figure 9 shows a general overview of the dashboard provided by Wazuh SIEM. In this case, it displays a threat concerning an unauthorized Modbus write coils identified in the deployed industrial water tank.

By integrating SIEM's incident detection and response capabilities with DT's real-time representation of physical assets, IIoT devices can be centrally monitored and managed. This integration facilitates rapid response to security threats and automated mitigation actions at infrastructure and device levels. Furthermore, it enhances the resilience of IIoT networks against attacks by coordinating responses, thereby ensuring the continuity of operations.

Concerning the scientific impact, some academic works address automating incident response in IIoT devices using DT. This work is an attempt to leverage the integration of a SIEM and DT to automate incident response plans across IIoT environments. The solution has been tested using well-known technologies such as Wazuh and Eclipse Ditto.

B. Limitations

There are several limitations that this work does not address. First, threat detection has been carried out using an IDS. This approach may miss stealthy attacks. To address this limitation, it is necessary to include an ADS alongside the IDS. The combined approach would detect previously undetected threats, thus covering a larger attack surface.

Another limitation identified is that the proposed scenario may not be applicable to all industrial systems. While the industrial water tank emulation used to evaluate the proposed solution allowed for effective script execution and action-taking due to its composition with actuators, changes in these are immediately reflected in this setup. However, in more critical systems such as industrial furnaces, changes in the system itself, such as turning on or off, may not be reflected instantaneously. This discrepancy could hinder the ability for immediate response to attacks or anomalies in such systems, necessitating a more careful and tailored approach to the specific characteristics of each industrial system.

Concerning the implemented PoC, the IoT gateway, responsible for communicating with DT, exhibits a security limitation. An attacker could compromise the gateway, allowing interception and modification of response commands, as well as direct attacks that could prevent DT from being updated. This vulnerability must be addressed in future design iterations to ensure communication integrity.

Finally, although DT facilitate the execution of incident response in industrial environments, they also increase the attack surface [22]. Connecting these twins to industrial devices opens a new attack door, as these devices would be fully exposed if any of the twins were to be compromised. Attackers could take advantage of the bi-directional communication to send malicious commands to the IIoT devices.

VIII. Conclusions and Future Work

In this work, we have developed the integration of DT and SIEM. By implementing both a prototype of the solution and a use case for testing purposes, we demonstrate that the integration between these two technologies can efficiently automate incident response plans across IIoT environments.

Concerning future work, it is important to address the security implications of connecting an industrial environment with DT. This integration increases the attack surface [22], putting these industrial devices at serious risk if one of the twins is compromised. Additionally, we recommend testing the prototype in a real industrial system to validate the solution. Integrating additional threat detection systems, such as ADS, alongside the IDS, would enhance coverage of the larger attack surface. Lastly, while our platform has been tested using Wazuh and Eclipse Ditto, exploring additional tools could further enhance its capabilities and compatibility with a wider range of industrial environments.

Acknowledgments

This work has been financed by The European Commission through the Horizon Europe program under the IDUNN project (grant agreement number 101021911). It was also

partially supported by the Department of Economic Development, Sustainability and Environment of the Basque Government under the ELKARTEK 2023 program, project BEACON (with registration number KK-202300085).

References

[1] Cisco, "What is industrial iot (iiot)?" [Online]. Available: https://www.cisco.com/c/en/us/solutions/internet-of-things/what-is-industrial-iot.html

[2] Archon, "What are the risks associated with industrial iot (industrial internet of things)?" 2023. [Online]. Available: https://www.archonsecure.com/blog/what-are-the-risks-associated-with-industrial-iot

[3] Fortinet, "Information technology (it) vs. operational technology (ot) cybersecurity." [Online]. Available: https://www.fortinet.com/resources/cyberglossary/it-vs-ot-cybersecurity

[4] N. Hajdarbegovic, "Are we creating an insecure internet of things (iot)? security challenges and concerns." [Online]. Available: https://www.toptal.com/it/are-we-creating-an-insecure-internet-of-things

[5] P. Empl, D. Schlette, D. Zupfer, and G. Pernul, "Soar4iot: Securing iot assets with digital twins," *ARES '22: Proceedings of the 17th International Conference on Availability, Reliability and Security*, 2022.

[6] D. Allison, P. Smith, and K. Mclaughlin, "Digital twin-enhanced incident response for cyber-physical systems," *ARES '23: Proceedings of the 18th International Conference on Availability, Reliability and Security*, 2023.

[7] A. Akerele, W. Leppert, S. Somerville, and G.-A. Amoussou, "The digital twins incident response to improve the security of power system critical infrastructure," *J. Comput. Sci. Coll.*, vol. 39, no. 3, p. 86–99, oct 2023.

[8] K. Wolf, R. Dawson, J. Mills, P. Blythe, and J. Morley, "Towards a digital twin for supporting multi-agency incident management in a smart city," *Scientific Reports*, vol. 12, 09 2022.

[9] P. Empl and G. Pernul, "Digital-twin-based security analytics for the internet of things," *Information*, vol. 14, no. 2, 2023. [Online]. Available: https://www.mdpi.com/2078-2489/14/2/95

[10] M. Dietz, M. Vielberth, and G. Pernul, "Integrating digital twin security simulations in the security operations center," 2020. [Online]. Available: https://doi.org/10.1145/3407023.3407039

[11] "Industrial internet of things iiot." [Online]. Available: https://www.techtarget.com/iotagenda/definition/Industrial-Internet-of-Things-IIoT

[12] digiALERT, "Industrial iot (iiot) attacks," 2023. [Online]. Available: https://www.linkedin.com/pulse/industrial-iot-iiot-attacks-digialert/

[13] A. C. Panchal, V. M. Khadse, and P. N. Mahalle, "Security issues in iiot: A comprehensive survey of attacks on iiot and its countermeasures," pp. 124–130, 2018.

[14] E. Commission, "Commission welcomes political agreement on cyber resilience act," 2023. [Online]. Available: https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_23_6168/IP_23_6168_EN.pdf

[15] "Understanding iec 62443," 2021. [Online]. Available: https://www.iec.ch/blog/understanding-iec-62443

[16] R. M. Lee, "The four types of threat detection with cas e-studies in indus trial control sys tems (ics)," 2018. [Online]. Available: https://api.semanticscholar.org/CorpusID:212673566

[17] K. IT, "What's included in the threat landscape." [Online]. Available: https://encyclopedia.kaspersky.com/glossary/threat-landscape/

[18] R. Diaz, "Traditional and ai-powered threat detection in modern cybersecurity," 2023. [Online]. Available: https://threadfin.com/threat-detection-part-of-strong-cybersecurity-strategy/

[19] IBM, "What is incident response?" [Online]. Available: https://www.ibm.com/topics/incident-response

[20] NIST, "Computer security incident handling guide." [Online]. Available: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

[21] altexsoft, "Digital twins: Components, use cases, and implementation tips," 2021. [Online]. Available: https://www.altexsoft.com/blog/digital-twins/

[22] C. Alcaraz and J. Lopez, "Digital twin: A comprehensive survey of security threats," *IEEE Communications Surveys Tutorials*, vol. 24, no. 3, pp. 1475–1503, 2022.

[23] Q. Xu, S. Ali, and T. Yue, "Digital twin-based anomaly detection in cyber-physical systems," pp. 205–216, 2021.

[24] R. van Dinter, B. Tekinerdogan, and C. Catal, "Predictive maintenance using digital twins: A systematic literature review," *Information and Software Technology*, vol. 151, p. 107008, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0950584922001331

[25] P. Empl, H. Hager, and G. Pernul, "Digital twins for iot security management," pp. 141–149, 07 2023.

[26] S. Burge, "What is industrial control systems security?" 2023. [Online]. Available: https://internationalsecurityjournal.com/industrial-control-systems/

[27] M. M. Abdulwahid and N. Basil, "Design and implementation of water level tank model by using scada system," *Informatica : Journal of Applied Machines Electrical Electronics Computer Science and Communication Systems*, vol. 1, pp. 63–69, 12 2020.

[28] J. Mousdell, "Water storage tanks," 2023. [Online]. Available: https://www.h2xengineering.com/blogs/water-storage-tanks/

[29] "Icssim github repository." [Online]. Available: https://github.com/AlirezaDehlaghi/ICSSIM

[30] H. H. Addeen, Y. Xiao, J. Li, and M. Guizani, "A survey of cyber-physical attacks and detection methods in smart water distribution systems," *IEEE Access*, vol. 9, pp. 99 905–99 921, 2021.

[31] R. Taormina, S. Galelli, N. O. Tippenhauer, E. Salomons, and A. Ostfeld, "Characterizing cyber-physical attacks on water distribution systems," *Journal of Water Resources Planning and Management*, vol. 143, 02 2017.

[32] L. Jacobs, "Industrial control system (ics) cyber threat hunting using suricata," 2021. [Online]. Available: https://suricon.net/wp-content/uploads/2021/10/SURICON2021-Jacobs-ICS-Cyber-Threat-Hunting-Using-Suricata.pdf