IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received October 14, 2021, accepted November 21, 2021, date of publication December 6, 2021,
date of current version December 20, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3133260

A Threat Hunting Framework for Industrial Control Systems

ZAHRA JADIDI AND YI LU
Cyber Security Cooperative Research Centre, Queensland University of Technology (QUT), Brisbane, QLD 4000, Australia
Corresponding author: Zahra Jadidi (zahra.jadidi@qut.edu.au)

The work was supported by the Commonwealth of Australia and Cybersecurity Research Centre Limited.

ABSTRACT An Industrial Control System (ICS) adversary often takes different actions to exploit vulnerabilities, pass the border between Information Technology (IT) and Operational Technology (OT) networks, and launch a targeted attack against OT networks. Detecting these threat actions in early phases before the final stage of the attacks can be executed against industrial endpoints can help prevent adversaries from achieving their goals. Threat hunting in IT networks has been previously studied, and several hunting methods have been proposed. However, these methods are not sufficient for ICSs, as the integration of industrial legacy systems with advanced IT networks has introduced new types of vulnerabilities and changed the behaviour of attacks. The lack of a unified hunting solution for integrated IT and OT networks is the gap that is considered in our paper. The contribution of this paper is an ICS Threat Hunting Framework (ICS-THF) which focuses on detecting cyber threats against ICS devices in the earliest phases of the attack lifecycle. ICS-THF consists of three stages, threat hunting triggers, threat hunting, and cyber threat intelligence. The threat hunting trigger stage identifies events or external resources that can trigger the hunting stage. The hunting stage uses a combination of the MITRE ATT&CK Matrix and a Diamond model of intrusion analysis to generate a hunting hypothesis and to predict the future behaviour of the adversary. This hypothesis will be validated by analysing Diamond models of threat actions. Finally, the cyber threat intelligence stage is responsible for generating Indicators of Compromise (IoCs) to be used for future threat hunting. The Black Energy 3 malware, PLC-Blaster malware, and SWaT dataset are used in this paper to evaluate the efficiency of the proposed framework.

INDEX TERMS Threat hunting, industrial control systems, Diamond model, MITRE ATT&CK, cyber threat intelligence.

I. INTRODUCTION

Traditionally, industrial systems were isolated from external access, and security was not a primary design criterion. Many industrial control systems today are exposed to the Internet creating security vulnerabilities. The increasing number of threats to these vulnerabilities is a growing concern [1], [2], [42], [43]. Existing security mechanisms like firewalls, anti-malware, and security information and event management (SIEM) are reactive methods. Reactive security mechanisms can help networks to detect attacks and prevent repeat attacks by improving their protection strategies. For modern sophisticated attacks, it has been shown that proactive solutions are more efficient [45]. A proactive threat hunting solution can help to identify any potential attacks and respond to these attacks. While reactive approaches have been widely used, they are not capable of foreseeing threats and predicting their future attacks. High-skill attackers are well-aware of reactive methods and know how to bypass them. To combat the limitations of reactive methods, many organisations use cyber threat hunting to proactively search for threat actions that may be undetected and find them before they cause a major breach [45].

The goal of a hunting process is detecting threat actors early in the cyber kill chain by searching for signs of an intrusion and then, providing detection strategies for future use. Threat hunting is a proactive activity that starts with a hypothesis of a potential threat which should be validated during the hunting process. The validation process includes analysis of network and system data using the knowledge provided by Cyber Threat Intelligence (CTI). While threat hunting in conventional communication networks is not novel, Industrial

The associate editor coordinating the review of this manuscript and approving it for publication was Shafiqul Islam.

Control Systems (ICSs) need a hunting solution that can investigate adversarial capabilities in both Information Technology (IT) and Operational Technology (OT) networks.

Cybersecurity attacks do not always use pre-defined techniques, and organisations should not wait for alerts to detect security breaches. Threat hunters proactively search networks and devices to detect and investigate threats that cause unknown and malicious behaviours [1]. Different threat hunting methods have been proposed for IT networks. However, threat hunting in ICS networks is a research gap that has not been sufficiently investigated [44], [45]. To the best of the authors' knowledge, there is no framework available for threat hunting in ICS networks. In this paper, we address this gap by providing a framework for central threat hunting in an ICS network.

Although existing solutions have been proposed to facilitate the threat hunting process, there are three models which are widely used in the industry. These models are the Diamond model of intrusion analysis, cyber kill chain, and MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) which can model attack behaviour and predict future threat actions [3], [5]–[7]. Diamond models and the cyber kill chain model were used by some papers for threat hunting in IT and ICS networks [22], [3], [39]. However, our paper combines the Diamond model with the new MITRE ATT&CK for ICS.

MITRE ATT&CK is a model of cyber adversary behaviour, and it outlines different phases of attacks' lifecycle and the Tactics, Techniques, and Procedures (TTPs) of known attacks [41]. MITRE ATT&CK for ICS was released in 2020 [38], and it covered the TTPs of attackers targeting ICS networks. However, existing papers did not consider MITRE ATT&CK for ICS in generating Diamond models of the threat hunting process. In our paper, MITRE ATT&CK for ICS is used in conjunction with a Diamond model of an intrusion to visualise the attackers' routes in an ICS network.

The Diamond model, MITRE ATT&CK and other CTI sources help hunters to generate their initial hypothesis and contextualise and drive the hunt. Then, the outputs of the hunting process are used to generate intelligence. Different methods have been created to share cyber threat intelligence internally and externally. For example, MISP is an open-source threat intelligence platform that provides standards for CTI sharing [https://www.misp-project.org/]. Our paper shows how the threat hunting phase can be used to generate cyber threat intelligence.

Motivated by the above discussions, in this paper we address the lack of threat hunting framework in an ICS environment. We overcome this challenge by proposing a framework that categorises threat hunting into three phases. This framework called ICS-THF describes how collaboration with hunting triggers and cyber threat intelligence can help threat hunters in ICSs to detect adversarial activities in the early phases of the cyber kill chain. ICS-THF is a layered hunting solution that uses existing open-source resources. This framework combines, MITRE ATT&CK and a Diamond model, to provide more accurate details for a hunting hypothesis. This layered framework comprises three main phases which are:

- Phase 1, threat hunting triggers: A threat hunt will be initiated by outputs from analytics tools or notification from external resources. ICS-THF shows the required connections between the hunting trigger and threat hunting phases and feedback from the cyber threat intelligence to the hunting trigger phase.
- Phase 2, threat hunting: Threat hunters will utilise adversaries' TTPs provided by MITRE ATT&CK to conduct the threat hunt. They will also use the Diamond model to model the behavioural patterns of IT/OT adversaries. The Diamond model is used by hunters to manually cluster abnormal events in our network with similar events in well-known ICS attacks.
- Phase 3, cyber threat Intelligence: Threat hunters convert the detected adversary actions to actionable threat intelligence, to be disseminated using a platform like MISP.

Contribution. The novelty of this paper is:

- a central and unified threat hunting framework for ICS networks.
- using a combination of the Diamond model and MITRE ATT&CK for ICS in our framework for the first time in an ICS environment.
- providing a solution to use threat hunting outputs to generate cyber threat intelligence, and update security devices based on the threat actions detected.

Organisation. The rest of this paper is organised as follows. Section II presents a review of related works in threat hunting. Section III explains the threat hunting framework. Section IV discusses the threat hunting trigger stage. Section V describes the threat hunting stage. The cyber threat intelligence stage will be described in Section VI. ICS-THF will be evaluated in Section VII using three different scenarios, Black Energy 3 malware, Programmable Logic Controller (PLC)-Blaster malware, and an attack in the SWaT dataset. Section VIII concludes the paper.

II. RELATED WORKS

ICS networks contain integrated physical systems (OT networks) and IT systems data. Legacy ICS networks were isolated networks, and they were designed without consideration of cyber security. The isolated legacy ICS networks had little resemblance to IT systems, and they had systems running proprietary control protocols using specialised hardware and software. Now, the majority of old technologies have been replaced by low-cost Ethernet and Internet Protocol (IP)-based devices, and hence the possibility of cybersecurity incidents has been increased [48].

The connection of ICS networks to the Internet provides significantly less isolation for ICS devices from the outside world. Most security solutions have been designed to combat the security issues in IT networks. However, due to the different characteristics of IT and ICS networks, security

solutions should consider these differences when dealing with the security of an ICS environment.

Existing security mechanisms in ICS networks are reactive mechanisms, and they can detect and prevent threat actions. However, due to the weak security of ICS networks with heterogeneous devices and the sophisticated nature of attacks in ICS networks, we need proactive approaches such as threat hunting. Due to the lack of proactive monitoring of threat actions, many organisations are unaware that there may be some hidden intrusion in their networks as their security devices are bypassed or their confidential data may be compromised. In this paper, we present a framework to provide a proactive approach to monitoring an ICS network. It uses Diamond models in conjunction with MITRE ATT&CK Matrix to visualise threat actions to detect ICS attacks and mitigate future attacks. Diamond models can be used to visualise threat actions and track them as they evolve [44].

Different threat hunting methods have been proposed for IT networks. For example, a framework was proposed by [1] to improve collaboration between different operational units including a steering committee, control centre, threat intelligence, incident response, etc. The framework proposes using inputs from different sources such as SIEM tools, historical logs, and cyber intelligence. The authors [1] proposed a five-maturity-level threat hunting framework which are, no threat hunting, ad hoc level of threat hunting, use existing threat hunting procedure, create own threat hunting procedures, and automate threat hunting. To evaluate the proposed framework, the authors collected data from 500 industry professionals with a survey questionnaire on threat hunting.

Sequential pattern mining was used by Homayoun *et al.* [2] to perform threat hunting in IT networks. This method could find the patterns of activities in different ransomware families and provided a classification method to stop an attacker quickly and accurately [2]. Ransomware hunting is also studied in [8]. The authors presented a ransomware threat hunting and threat intelligence system to identify ransomware families. A machine learning method was used in their paper to automatically detect ransomware. Darabian *et al.* [4] proposed a Multiview learning method to provide multiple views for malware threat hunting on the Internet of Things platforms. While these threat hunting methods could improve the accuracy of detection in a specific kind of threat actions, they did not address the diversity of threat activities. Graph-based threat analysis is another method proposed for threat hunting [35]–[37]. All the above hunting solutions focused on IT networks, and threat hunting in ICS networks is the research gap that has not been sufficiently investigated [44], [45].

Three models which are widely used by threat hunters are the Diamond model of intrusion analysis, cyber kill chain and MITRE ATT&CK Matrix [3], [5]–[7]. While there are a few papers published in threat hunting in ICS networks [44], [45], they did not investigate how Diamond models and MITRE ATT&CK Matrix can be deployed in threat hunting in ICS networks.

The application of Diamond models and the cyber kill chain model in IT and ICS networks was reviewed by some papers [22], [3], [39]. The Diamond model of intrusion analysis was used by Cook *et al.* [3] to visualise behavioural patterns of ICS adversaries. The authors proposed a cyber defence triage process based on the Diamond model to identify adversarial behaviour in the Mandiant Attack Lifecycle, and they focused on the ICS operations which could be most impacted by an attacker. This triage process uses CARVER Matrix to prioritise ICS devices that need cyber defensive actions. There are different Advanced Persistent Threats (APTs) with advanced technical capabilities, and they spend significant time and resources to attack their target [9]. Potential targets of these groups can utilise the Diamond model of intrusion analysis to understand the patterns of previous attacks performed by the APT and implement an appropriate hunting process [5]. The Diamond model of intrusion analysis is also used by Mekdad *et al.* [39] to model threats in an ICS network. These papers employed Diamond models based on the cyber kill chain to understand threat actions.

The MITRE ATT&CK model is a hub that is constantly being updated to provide attacker tips, tactics, and techniques to network security teams to determine their organisation's risks and prioritise their protection efforts [12], [13]. Threat hunters can leverage the model to find specific techniques that adversaries use in conjunction with others. It is extremely advantageous in determining a system's level of visibility against targeted attacks by deploying tools across an organisations' endpoints and perimeter. The MITRE ATT&CK matrix consists of a set of techniques used by attackers to achieve an objective. These objectives are categorised as tactics in the matrix. The information provided by MITRE ATT&CK can also be used in threat hunting to identify resources that are affected by different ICS attacks. MITRE ATT&CK method was employed by Strom *et al.* [10] and Al-Shaer *et al.* [11] to find threats. Al-Shaer *et al.* [11] used statistical analysis based on MITRE ATT&CK to learn APT TTPs to predict the future techniques that may be performed by the adversary. MITRE ATT&CK for ICS was released in 2020 [38]. The novelty of our paper is combining this MITRE ATT&CK with Diamond models to perform threat hunting in ICS networks.

To have a proactive framework, the outputs of threat hunting can be used to generate CTI. Cyber threat intelligence is evidence-based knowledge that consists of tactics, techniques, and procedures of a threat and also indicators of compromise like file hashes, IP addresses, commands used by an attacker, domain name, website, and infrastructure used for launching attacks. CTI is beneficial for security operations to improve the efficiency of preventive and detective capabilities of an upcoming threat or a breach. This CTI information can also be used as triggers for future threat hunting activities. CTI can be extracted from the organisation's networks, or it may be received from external open-source threat intelligence resources. This information can be shared amongst trusted

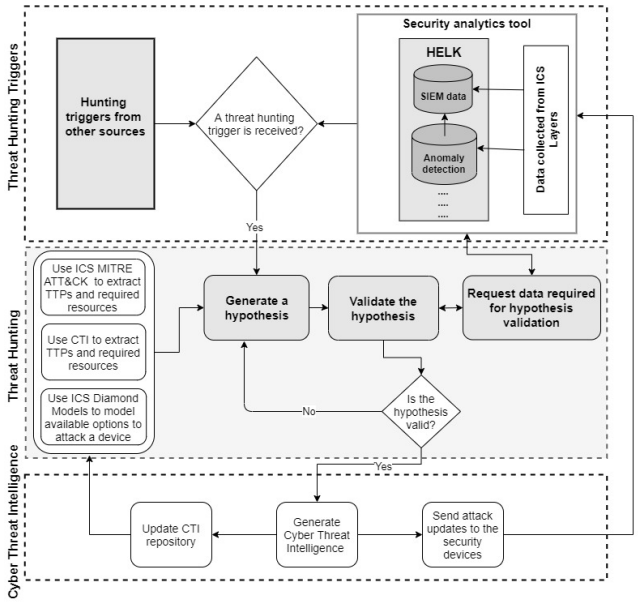


FIGURE 1. Proposed ICS threat hunting framework.

stakeholders [46]. Different CTI platforms were evaluated in [47]. According to this paper, MISP is a reliable platform for CTI sharing. MISP is a CTI platform utilised for sharing, storing, and comparing Indicators of Compromise (IoCs) in attacks. Using MISP, CTI information will be stored and shared, and it can be used to update the rules in security devices.

III. THREAT HUNTING FRAMEWORK

This paper proposes an ICS threat hunting framework called ICS-THF, Figure 1. ICS-THF consists of three phases, triggers, threat hunting, and cyber threat intelligence. Threat hunting may be triggered by events detected by security analysts. As shown in Figure 1, a security analytics tool is used by security analysts to capture data from ICS devices and monitor their traffic and logs. Unknown malicious behaviour in the input data may be a trigger for the threat hunting phase. Triggers can also be issued by external cyber threat intelligence sources such as new attacks in an organisation with similar infrastructure. The second phase of ICS-THF is the threat hunting phase which combines MITRE ATT&CK Matrix and the Diamond model of intrusion analysis. Adversarial TTPs provided by MITRE ATT&CK are used to generate a Diamond model. Information output from the MITRE ATT&CK framework is fed into the Diamond model and is used to visualise various actions available to an attacker, and it can be used by threat hunters to determine the characteristics of malicious behaviour and identify the attack [3], [12], [13], [14]. As shown in Figure 1, other threat intelligence sources, such as newly published articles about the actions of threat actors, may also be used by hunters to add more details to the Diamond model.

A repository of the Diamond models of well-known APTs can also be used by the hunters to generate a more accurate hypothesis based on known sets of TTPs. Hunters can also use this repository to cluster their identified Diamond Models to the similar models in the dataset. These methods provide further information to refine the existing hypothesis. A Diamond model can help analysts predict the next step the adversaries might take in their attack. Then, a threat hunter validates the generated hypothesis by the data requested from the security analytics tools and end devices. Hypothesis validation is manually performed by hunters by looking for the evidence and TTPs of the threat actions and comparing their identified events with Diamond models of expected threat actions. For well-known attacks, the hunter can validate the hypothesis by comparing their Diamond models with that of known ICS adversaries.

An unsupervised machine learning method can be used to learn possible hypotheses, and then, it can automate the validation of the hypothesis. This unsupervised machine learning method can be used by hunters to compare their identified Diamond model with existing Diamond models in the threat repository and cluster them to the similar APT Diamond model. Automation of hypothesis validation is beyond the scope of this paper. However, the challenging point in this automation is generating a comprehensive dataset of possible Diamond models of APT actions. MITRE ATT&CK matrix is a resource that can be used to generate this TTP dataset. This research gap will be studied in our future work.

The validated hypothesis will be sent to the CTI stage to extract important features and generate adversarial signatures. In this paper, a CTI sharing tool such as MISP is used to share standard IoCs generated by hunters for the detected threat. These IoCs will be added to the CTI repository to help hypothesis generation in the future. In addition, the outputs of MISP in the CTI phase can be pushed into the security analytics tool to update the detection rules. A CTI sharing tool such as MISP also has the capability to share the IoCs with other partners.

In addition to the three core ICS-THF phases, a preparation phase is required to provide inputs for the hunter. In the preparation phase, it is recommended to have a data collection and retention strategy that supports diverse data sources in a central location. Analysts should search, explore, and pivot different data sources to be able to hunt sophisticated adversaries. This paper aims to propose a suitable framework able to utilise low-cost tools to implement threat hunting in ICSs. Therefore, an open-source Hunting Elastic Stack (HELK) is used as a central data analytics tool. The outputs of the HELK feed hunting trigger phase.

Examples of security data that can be collected for threat hunting are [1], [15]–[19], [20], [21]:

a. Endpoint security logs: contain valuable information about the actions of users and malicious activities.
b. User Behaviour Analytics (UBA): Threat activities such as users accessing unexpected endpoints or executing unexpected applications can help to detect the threat.
c. Network and application threat analytics: Threat hunters use cyber intelligence from different vendors on the

network and application systems. This will help to identify high-risk applications and network systems.

Part of the challenge of threat hunting in ICSs is that the information sources might not be as available as in a normal network. In our framework, the hunting phase begins with available data sources in an organisation and the additional data sources required will be identified at the end of the hunting phase.

Analysing all available data and searching through all data will take a large amount of time and effort from hunters. Therefore, hunters need to carefully select their required data based on their hunting hypothesis [15], [21]. This requested data will be used to validate the hypothesis.

IV. THREAT HUNTING TRIGGERS

Normally, security analysts deal with well-known input data, and when there are well-defined signatures. However, hunters take over the task when there is poorly defined data that is vague and needs active investigation. Threat hunting is also triggered by external sources such as an article, a piece of news, etc. Some threat hunting triggers are [15], [17], [21]:

a) Cyber Threat Intelligence which provides information about new classes of vulnerabilities, or new actions of threat actors [15], [18], [21].
b) a new article that shows a new class of attack. This is a trigger for the threat hunting team to assess the risk of this attack against their network and determine tactics for defending against the attack.
c) notification from a third party, for example, law enforcement/intelligence organisations, national or subnational CERTs, or independent researchers.
d) data received from a security analyst. An analyst may detect a sudden spike in traffic created by an unknown port or protocol. At this stage, hunters take over the task. A hunting platform like HELK can be used by hunters to generate and evaluate their hypotheses.

HELK uses graph algorithms to find correlations between events and logs of ICS devices. Correlation analysis can help hunters to find connected components to the detected anomaly. In this paper, HELK is used to monitor network traffic and device logs, detect anomalies and their correlated components, detect MITRE ATT&CK TTPS, and trigger the threat hunting phase. Beats are open platforms used to send data from various machines and systems to HELK. Filebeat (https://www.elastic.co/beats/filebeat) is used for logs, Packetbeat (https://www.elastic.co/beats/packetbeat) is for capturing network data, and Winlogbeat is for Windows event logs. HELK is developed based on Elastic Stack which provides speed and scalability for distributed ICS networks.

V. THREAT HUNTING

At this stage, the hunter needs to create a hypothesis including the logistics of the hunt and defining the success criteria for the hunt [15], [21]. It should be a clear and falsifiable hypothesis. Initially, the hunter should assume that the hypothesis is correct and then, explain the indicators that should be used to investigate the hypothesis. The assets that may be impacted by these threat actions should also be reported. In addition, the list of data that the hunter needs to validate the hypothesis should be identified [15], [16], [21]. In this paper, Black Energy 3 malware, PLC-Blaster malware, and SWaT datasets will be used to evaluate the proposed framework. The hypothesis generated for these scenarios will be discussed in Section VII.

In the threat hunting phase of our proposed framework, two sources of data, MITRE ATT&CK and the Diamond model are combined to generate a hypothesis.

A. MITRE ATT&CK

ATT&CK is a model of cyber adversary behaviour, and it outlines different phases of attacks' lifecycle and the platforms they are known to target. The current version of MITRE ATT&CK for Enterprise categorises TTPs against multiple operating systems (Microsoft Windows™ systems, Linux and macOS), and it also covers pre-compromise tactics and techniques [12], [13]. The cyber-attack lifecycle initially developed by Lockheed Martin as a ''cyber kill chain'' has been used by MITRE ATT&CK to help defenders to learn about adversary techniques and find their detection gaps by mapping network defensive tools and the cyber-attack lifecycle.

Using this attack life cycle, MITRE ATT&CK provides a framework describing the actions that an adversary may take to compromise a network. This model can help to expand the knowledge of network defenders by outlining the TTPs which are used by adversaries to gain access to a remote system and execute their targeted attacks. MITRE ATT&CK for Enterprise which is for enterprise networks has 12 core tactics after Initial Access, shown in Table 1. For each tactic, a wide range of techniques used by threat actors are identified by the framework. Tactics show adversaries' technical goals. Techniques show how adversaries achieve their goals. The procedure of the techniques and the resources that should be used to detect that technique is also explained by the framework.

MITRE ATT&CK provides knowledge based on adversary behaviour which is created by real-world observation. Adversaries can easily change the value of a hash or their IP addresses if these indicators are discovered. However, it is very difficult for them to change their TTP behaviour upon being discovered. Therefore, MITRE ATT&CK has focused on TTPs. ATT&CK for ICS describes adversary behaviour and the actions that an adversary may take while operating within an ICS network. Although there is some overlap between the Enterprise and ICS ATT&CK, the focus of ATT&CK for ICS is on the actions that adversaries take against non-IT based systems of ICSs [12], [13].

ATT&CK for ICS has used public incident reports, research papers, conference presentations, blogs, and other available security reports to identify the existing techniques used by adversaries in OT networks. TTPs provided

TABLE 1. List of tactics in IT and ICS MITRE ATT&CK.

IT	ICS
Initial Access	Initial Access
Execution	Execution
Persistence	Persistence
Privilege Escalation	Privilege Escalation
Defence Evasion	Evasion
Credential Access	Discovery
Discovery	Lateral Movement
Lateral Movement	Collection
Collection	Command and Control
Command and Control	Inhibit Response Function
Exfiltration	Impair Process Control
Impact	Impact

for Enterprise ATT&CK is different from OT networks. Table 1 compares the tactics proposed for IT and OT networks [12], [13]. Both ATT&CK for Enterprise and ATT&CK for ICS are publicly available.

ATT&CK for enterprise and ATT&CK for ICS can be used together to show the behaviour of an adversary in the entire business network. In this paper, the MITRE ATT&CK Matrix is used because it provides a standardised and ever-evolving taxonomy of adversarial TTPs. These TTPs can be used to understand your environment and identify the resources that should be monitored to mitigate the risks of these adversaries. Using the MITRE ATT&CK framework, threat hunters can determine which TTPs to search for across their environment, create a contextual threat model relating to their networks, and identify threat groups who may try to attack their organisations and the tools and techniques they may use to achieve their goal. A threat hunting tool such as HELK can help to detect ATT&CK TTPs in an ICS network.

The threat hunting phase in our framework uses the combination of ATT&CK Enterprise and ATT&CK for ICS to feed a Diamond model and initiate a hypothesis about possible threats in an ICS network. The Diamond model in this paper is used to help visualise the information provided by MITRE ATT&CK.

B. DIAMOND MODEL

The Diamond model [23] is the framework used for the analysis of intrusion events. This model describes the four core features of an intrusion event, infrastructure, adversary, capability, and victim (Figure 2). The Adversary is the entity responsible for the intrusion. Capability shows the tools and methods which may be used in the event. Infrastructure means the resources used by the adversary to execute the event. The victim is the target of the intrusion event.

The core features in a Diamond model are connected by edges which show the relationship between features. A Diamond model also uses meta-features to be able to model further details of an intrusion event. In a Diamond model

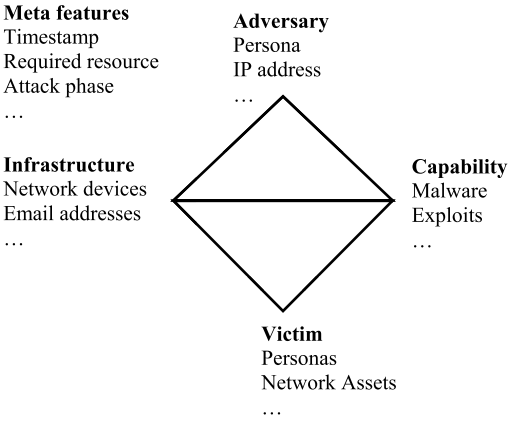


FIGURE 2. Diamond model.

created for a single intrusion event, each core feature is given a corresponding confidence value showing that how confident the analyst is that the feature is correct [3], [6], [7], [22], [23].

The Diamond model of intrusion analysis initially uses the Lockheed cyber kill chain to model the chain of detected events in an attack. The Diamond model is a two-dimensional representation of the attack shown in a directed phase ordered graph. This graph presents the cause-and-effect relationship between events [5].

In our framework, we integrate the MITRE ATT&CK with the Diamond model of intrusion analysis. A hunter receives information from MITRE ATT&CK and uses a Diamond model to visualise various actions available to an attacker [3]. Activity threads created by the Diamond model can develop potential attack paths before the detected intrusion. It can give an attacker's activity graph that shows various possible routes to the associated intrusions. Using this graph model, a threat hunter can understand the alternative paths that could be used by an attacker to get the same outcomes. This information can be used to improve defensive strategies. These graphs provide threat intelligence which can be stored in a threat intelligence repository. It is recommended that hunters keep the Diamond models of well-known ICS attacks, extracted from ATT&CK TTPs, in their cyber threat intelligence repository for future analysis. Diamond model-based threat intelligence can be used to:

- analyse publicised intrusions by different APT groups [5] to find indicators of the adversary at each cyber kill chain phase, create activity threads for the adversary, and understand the potential targets of these APT groups;
- predict the next step of the adversary;
- understand what alternative TTPs can cause the same impact on your ICS end devices;
- cluster intrusions to find the similarity between your network and other victims. In addition, you will be able to compare the vulnerabilities they might have.

The diamond model for each adversary can provide information about the capabilities and methods of the adversary, the infrastructure used by the adversary to deliver these

capabilities, and their target victim. Therefore, it can give insights into the types of adversarial capabilities you should protect against.

C. VALIDATION OF THE HYPOTHESIS

The next step of the threat hunting stage is the validation of the hypothesis. In this regard, a set of data required for this validation will be requested. Based on the collected data, the hunter should be able to prove or disprove the hypothesis. When the threat hunters receive the requested ICS data from the security analytics tool and other end devices, they evaluate the hypothesis by grouping their identified events with a Diamond model of the expected threat actions. For an incorrect hypothesis, the task will return to the hypothesis generation part to correct the hypothesis. A validated hypothesis will be sent to the CTI phase. If it is not feasible to collect the requested data, and available sources offer no evidence for the defined hypothesis, the hypothesis cannot be validated.

A machine learning classifier can be used in this section to automate the validation of the hypothesis. However, automation is beyond the scope of this paper, and it will be considered in our future work.

VI. CYBER THREAT INTELLIGENCE

CTI is the knowledge about a threat, and it includes threat indicators such as TTPs, IPs, etc. CTI can help organisations to learn about existing threats [2], [24], [25]. Cyber threat intelligence can be received from external open-source threat intelligence, or it can be extracted from adversarial activities in our networks.

The CTI phase in our framework is about extracting threat features from the actions of the identified adversary. These features will be used to build intelligence about threats against a given target. This intelligence will be stored in a CTI repository.

In the cyber threat intelligence stage, the generation of IoCs is performed by the hunters. These IoCs of the detected adversary are processed and distributed by MISP, and IoCs can be fed into the CTI repository. This repository will be used for future hypothesis generation.

MISP is a CTI platform utilised for sharing and storing IoCs of attacks. Cyber threat intelligence generation is a manual process in this manuscript. IoCs generated by hunters are shared via the MISP platform. MISP allows hunters to use CTI information from other companies and share back their IoCs with other partners.

Elastic in HELK has a module for handling threat information from MISP. Therefore, HELK can communicate with MISP APIs using a MISP Filebeat module. In addition, the IoCs shared by MISP can be pushed into security devices like firewalls and IDSs to update their rules. MISP is used by hunters to share CTI, and then, HELK can automatically receive CTI from MISP for future hunts. Evaluating the data provided by Cyber Threat Intelligence is not considered in this paper and will be done in our future works.

VII. EVALUATION OF THE PROPOSED FRAMEWORK

Three scenarios are used in this paper to evaluate the proposed framework. The first scenario is Black Energy 3 attack which was a sophisticated attack affecting both IT and OT networks. The next two scenarios are attacks targeting only OT networks. These scenarios are selected to show how the proposed framework can be used for threat hunting in both OT and the combination of IT and OT networks.

A. EVALUATION SCENARIO 1

In this section, we explore an attack against the Ukrainian power grid as a case study. The attackers caused significant disruption to the Ukrainian power grid in 2015 [15] utilising the Black Energy 3 malware toolkit. In 2014, attackers started deploying Supervisory Control and Data Acquisition (SCADA)-related plugins used in Black Energy 3 against victims in energy markets. Since 2015, spear-phishing emails with embedded malicious Excel or Word documents with macros have been used by the Black Energy APT group. These attachments contained macros to trigger Black Energy 3 malware infection [26]. Different plugins including various KillDisk were supported by Black Energy 3 malware. The Diamond models of the Ukrainian power grid attack are used for the evaluation of our ICS-THF [15].

This section evaluates the proposed ICS-THF framework in hunting Black Energy 3 malware. In this scenario, we assume that security analysts have detected unknown emails with malicious Microsoft Office attachments. There is also a new article about Black Energy 3 attack in another company. This information is sent to the threat hunting team for further analysis. Then, the threat hunters use MITRE ATT&CK for ICS, MITRE ATT&CK for Enterprise, and available Diamond models of ICS adversaries to generate an evidence-based hypothesis.

Ideally, threat hunters would have a Diamond model repository for well-known adversaries. Initially, industrial companies may not have this repository. In this case, they can start with an empty repository, and they can gradually fill in the repository with Diamond models that they generate for hypothesis validation.

In our scenario, checking the initial steps of well-known adversaries that used spear-phishing and comparing them with our evidence can give us ideas that what the adversary in our network is capable of. The knowledge about the similarity between our assets and other victims is very helpful for threat hunters to identify and request the data that they will need to validate the hunting hypothesis.

In our scenario, the hunter will form a hypothesis that the Black Energy group tends to send spear-phishing emails with malicious Microsoft Office attachments to employees from a legitimate email address to install Black Energy 3 malware. This is the hypothesis for the ''Delivery'' phase of the cyber kill chain [27] and it is driven by observed adversarial activities.

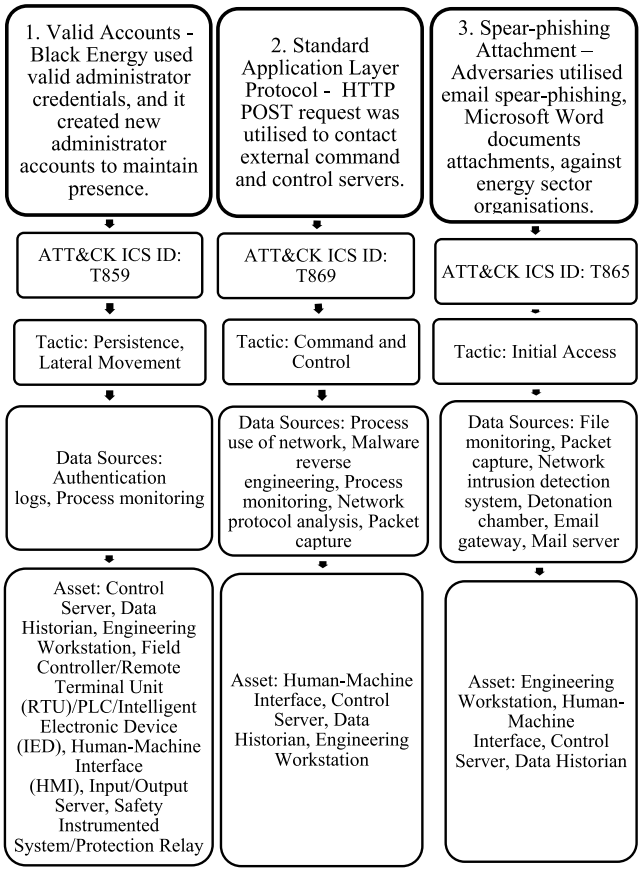


FIGURE 3. MITRE ATT&CK TTPs used by Ukrainian power grid attack.

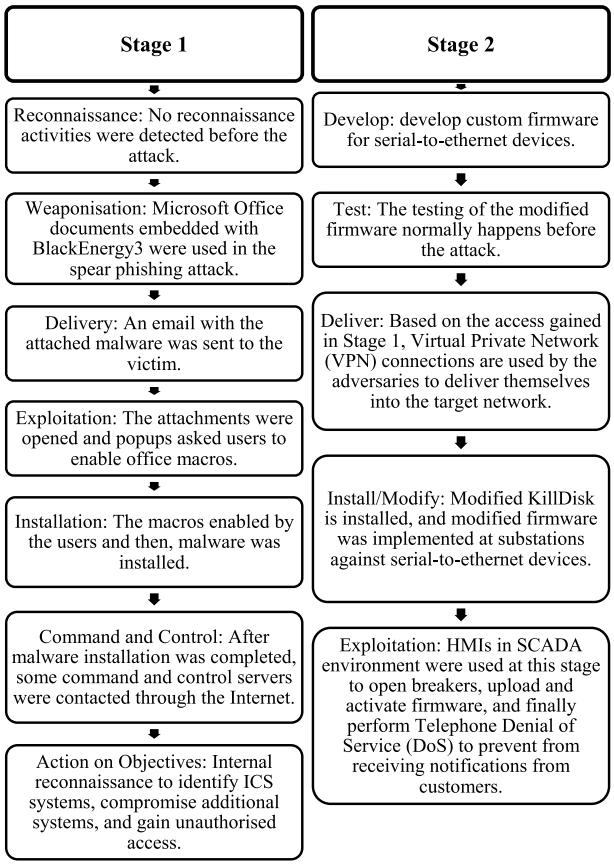


FIGURE 4. Cyber kill chain phases of Ukraine power grid attack—stages 1 and 2.

Using MITRE ATT&CK, you may be able to find the TTPs used by an adversary. Then, using the Diamond model, you can find more details about the victim and adversarial behaviour and predict future behaviour. MITRE ATT&CK and the Diamond model created to validate the hypothesis will be discussed in this section. According to MITRE ATT&CK for ICS, techniques used by Black Energy 3 are shown in Figure 3 [28], [29].

These TTPs are used to model Black Energy 3 events with the Diamond model of intrusion analysis [23]. In the Diamond model, we should also know the cyber kill chain phases of the malware [15]. SANS published a report [30] that divided ICS cyber kill chain into two stages:

- Stage 1: consists of reconnaissance, weaponisation, delivery, exploitation, installation, Command and Control (C2C), and action on objectives phases. These phases are similar to Lockheed Martin's Cyber Kill Chain, and it aims to gain access to information about the ICS.
- Stage 2: consists of the development, testing, delivery, install/modify, and execution phases. The knowledge gained in Stage 1 is used in stage 2 to develop, test and execute an attack against ICSs.

This two-stage ICS cyber kill chain is used in ICS-THF to create Diamond models of activity groups. Adversary activities in the Ukraine Power Grid attack based on different phases of the ICS cyber kill chain are shown in Figure 4 [15].

In the Diamond model, each adversary event is shown by four core features (adversary, capability, infrastructure, and victim) with their corresponding confidence values. These values show how confident the analyst is about the correctness of the feature [5]. The Diamond model may also use some meta-features such as timestamps, methodology and resources to present the event.

The Diamond model is combined with the MITRE ATT&CK matrix to provide a more comprehensive presentation of an adversary. A two-dimensional representation of the attack shows the relationships between events generated by the adversaries in different phases of the cyber kill chain.

Each event can be described as actual or hypothetical. An actual event means there is evidence for the occurrence of that event in the organisation's networks. Hypothetical means that the analyst uses some reasons to show the event has occurred.

Then, a confidence value is provided in the Diamond model for each event. Based on the knowledge provided by Figure 4, the Diamond model in Figure 5 is created for Black Energy 3 attack [15]. This Diamond model can be used by a machine learning classifier to automate the validation of the

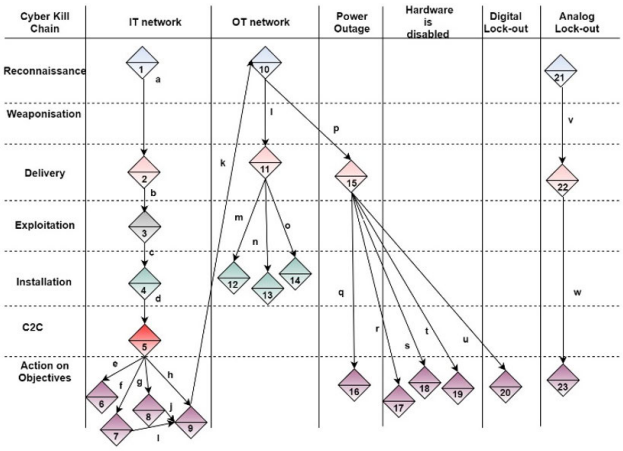


FIGURE 5. Diamond model based on adversary processes.

TABLE 2. Activity thread events in Ukrainian power grid attack.

Event No.	Verified	Description
1	Hypothesis	Open-source intelligence is conducted by the adversary.
2	Actual	A spear-phishing email is sent with a malicious attachment to employees.
3	Actual	Several employees opened the attachment which caused the unauthorised execution of Black Energy 3.
4	Actual	Black Energy 3 malware is installed.
5	Actual	C2C nodes are established.
6	Hypothesis	Lateral movement is performed for accessing active directories, creating account credentials, password grabs, etc.
7	Actual	Harvest valid VPN credentials.
8	Hypothesis	Identify business operations and ICS networks.
9	Actual	Gaining access to the ICS network using VPN credentials.
10	Hypothesis	Scan the ICS network to learn about its IT and OT networks and find field devices.
11	Actual	Use stolen credentials to gain access to ICS servers.
12	Actual	Install KillDisk software on target servers and RTUs.
13	Actual	Schedule disconnects for Uninterruptible Power server.
14	Actual	Install firmware to Serial-to-Ethernet devices.
15	Actual	Access the ICS network using VPN credentials
16	Actual	Compromised HMIs turned off breakers. This caused a power outage.
17	Actual	KillDisk wiping occurred.
18	Actual	Use windows-based HMIs in RTUs affected by KillDisk.
19	Actual	Serial-to-Ethernet substations become inoperative.
20	Actual	Lock administrator accounts
21	Hypothesis	Power plant call centre numbers are gathered.
22	Hypothesis	A dialling application made numerous calls to the call centre.
23	Actual	There was a Telephony Denial of Service (TDoS).

hypothesis. However, this is beyond the scope of our paper and will be studied in our future work. Figure 5 shows the activity thread created for Black Energy 3 intrusion events accompanied by the event description provided by Table 2. Table 3 describes the confidence values of each event [15].

The Diamond model of intrusion analysis in Figure 5 shows the Black Energy attack processes as an activity group. These adversary processes include IT network compromise, OT network compromise, execute power outage, use malware to attack computer systems (KillDisk) and power system hardware, remove administrator access from IT systems, and run a TDoS attack [15].

TABLE 3. Activity threads for Figure 5.

Arc	Confidence	Hypothesis/Actual
a	High	Hypothesis
b	High	Actual
c	High	Actual
d	High	Actual
e	High	Actual
f	High	Actual
g	High	Actual
h	High	Actual
i	High	Actual
j	High	Actual
k	High	Actual
l	High	Actual
m	High	Actual
n	High	Actual
o	High	Actual
p	High	Actual
q	High	Actual
r	High	Actual
s	High	Actual
t	High	Actual
u	High	Actual
v	High	Actual
w	High	Actual

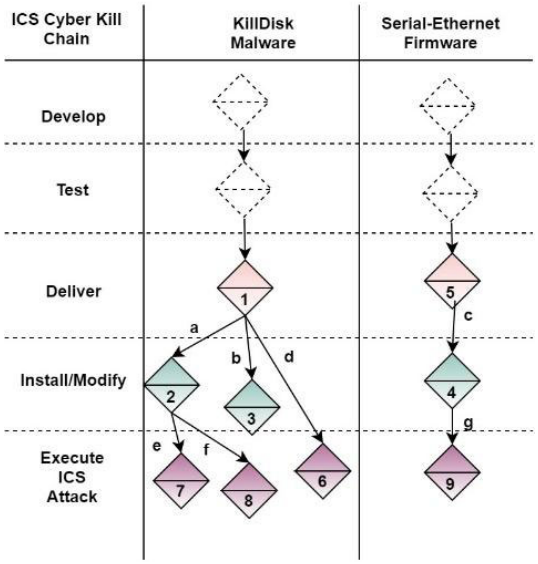


FIGURE 6. The Diamond model of black energy 3—ICS cyber kill chain—Stage 2.

The next step of analysing Black Energy 3 is creating the Diamond model of intrusion analysis based on the ICS cyber kill chain Stage 2, Figure 6 [15]. In the development and test phases, there are some dashed Diamonds, indicating that these activities occurred under the attackers' control and are not observable to the network defender.

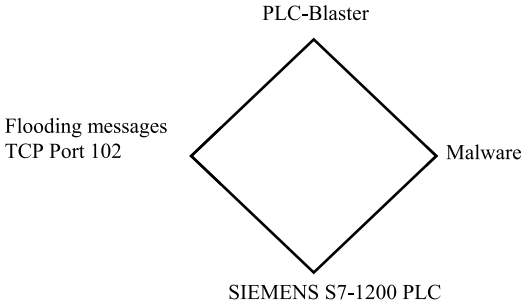


FIGURE 7. DoS attack to SIEMENS PLC.

At this stage, hunters can use the Diamond models of well-known ICS attacks extracted from ATT&CK TTPs. Therefore, any similarity between the historical behaviour of the activity thread in our network with existing adversary threads can be detected. We need to recognise the similarities between our equipment and the victims of well-known threat actions. This equipment includes components in our IT or OT networks such as hardware, software, and protocols. Then, the Diamond models of the attacks on these victims should be collected.

Activity thread in our network can be compared with these Diamond models to find possible future actions. After the adversary is detected, a MISP platform is used in the CTI stage to share extracted IoCs of the adversary and provide the adversary intelligence. These features will be stored in the CTI repository for future tasks.

B. EVALUATION SCENARIO 2

The PLC-Blaster attack is the second scenario used in this paper to evaluate the proposed framework. PLC-Blaster malware was designed to target Siemens SIMATIC S7-1200 PLCs. This malware lives and runs on PLCs. It scans the network to find and attack other targets (PLCs). PLC-Blaster can replicate itself onto the target PLCs. Once, it infects a target, it starts scanning for other targets [31].

This section discusses how ICS-THF can help to detect PLC-Blaster attacks. In this scenario, a flooding attack has happened to a PLC, and there is unknown traffic to port 102 of a SIEMENS PLC. Security analysts have sent this information to the threat hunting team. Based on the information provided by MITRE ATT&CK for ICS, attacks that use Denial of Service attacks are Backdoor. Oldrea, PLC-Blaster, and Industroyer. From the report sent by security analysts, threat hunters know that the source of the attack is another PLC in the network which shows the possibility of a PLC-Blaster attack. Therefore, the Diamond model created for this attack is as Figure 7.

In this scenario, the hunters will form a hypothesis that the PLC-Blaster group tends to send flooding messages to a PLC to infect other PLCs. Therefore, hunters now need to request data for the validation of the hypothesis. Based on the knowledge provided by MITRE ATT&CK for ICS, data sources that can be used to validate the hypothesis are shown

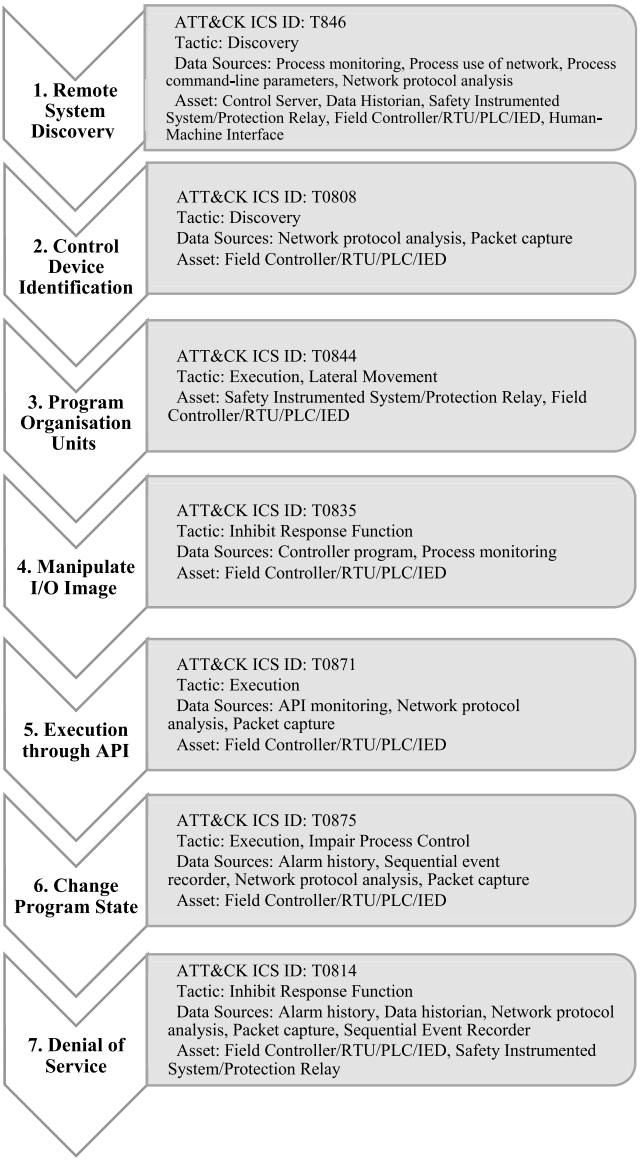


FIGURE 8. MITRE ATT&CK TTPs used by PLC-blaster attack.

in Figure 8. Different steps of the PLC-Blaster attack and their data sources are provided in Figure 8 [32].

These details are used to create Diamond models of a PLC-Blaster incident in Figure 9. The Diamond model in this figure is related to Stage 2 of the ICS cyber kill chain.

Figure 9 shows the activity thread created for PLC-Blaster intrusion events. The description of these events is provided in Table 4 [32].

The Diamond model in Figure 9 will be sent to the cyber threat intelligence phase to generate IoCs and share them using MISP.

C. EVALUATION SCENARIO 3

A six-stage Secure Water Treatment (SWaT) dataset is the third scenario used for the evaluation of the proposed framework. This dataset includes six main processes corresponding

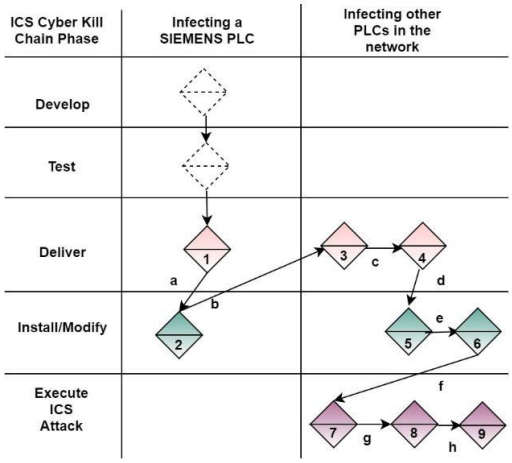


FIGURE 9. The Diamond model of PLC-blaster—ICS cyber kill chain—Stage 2.

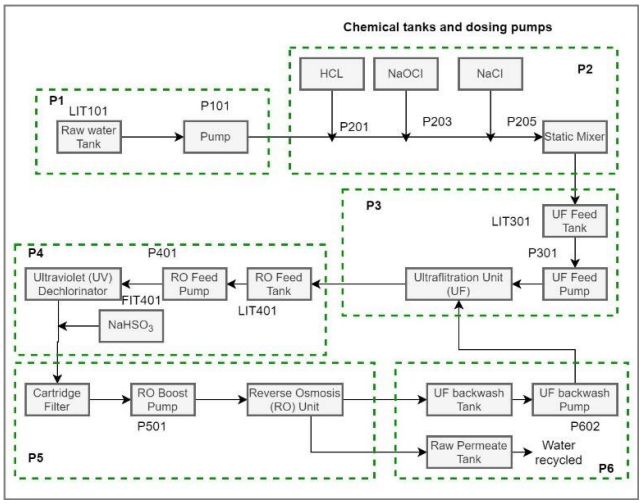


FIGURE 10. SWaT testbed processes.

TABLE 4. Activity thread event in PLC-blaster attack.

Event	Verified	Description
1	Actual	Gaining access to SIEMENS PLC
2	Actual	Install PLC-Blaster malware on the target PLC
3	Actual	Remote System Discovery: PLC-Blaster scans the network to find other Siemens S7 PLC devices to infect. It locates these devices by checking for a service listening on TCP port 102.
4	Actual	Control Device Identification: The PLC-Blaster worm starts by scanning for probable targets. Siemens SIMATIC PLCs may be identified by port 102/TCP.
5	Actual	Program Organisation Units: PLC-Blaster copies itself to various Program Organisation Units (POU) on the target device. The POUs include the Organisation Block, Data Block, Function, and Function Block.
6	Actual	Manipulate I/O Image: PLC-Blaster may manipulate any outputs of the PLC. Using the POU POKE any value within the process image may be modified.
7	Actual	Execution through Application Programming Interface (API): PLC-Blaster utilises the PLC communication and management API to load executable Program Organisation Units.
8	Hypothesis	Change Program State: After PLC-Blaster is transferred to a PLC, the PLC begins execution of PLC-Blaster.
9	Actual	Denial of Service: The execution of the PLC can be stopped by violating the cycle time limit. The PLC-Blaster implements an endless loop triggering an error condition within the PLC with the impact of a DoS.

to the physical and control components of a water treatment facility [33]. The six-stage filtration process of the SWaT testbed is shown in Figure 10.

The SWaT dataset is of a small-scale industrial water treatment process, which was generated by iTrust Cyber Security Research Centre [34]. The communication protocol used for automation was Modbus. The SWaT dataset includes APT activities, and it is collected from 11 days of continuous operation of a real testbed. The dataset consists of 7 days of normal traffic, containing no attack traffic, and 4 days containing attack traffic. The SWaT dataset consists of both network traffic and physical logs of the plant and water treatment process including 51 sensors and actuators data. There are four types of attacks in the SWaT datasets, Single Stage Single Point (SSSP) Attacks, Single Stage Multi-Point (SSMP) Attacks, Multi-Stage Single Point (MSSP) Attacks, and Multi-Stage Multi-Point (MSMP) Attacks.

The SWaT testbed consisted of a six-stage water treatment process including different sensors and actuators (Figure 10). MSMP attacks focus on one or two different attack points in the testbed which were from multiple stages of the process.

An MSMP attack in the SWaT dataset is used for the evaluation of the ICS-THF framework. This attack intends to underflow tank 101. To achieve this, the attacker:

- turns P-101 pump on continuously. P-101 pumps water from the raw water tank to the second stage of the treatment process;
- turns MV-101 actuator on continuously. MV-101 is a Motorized valve, and it controls water flow into the raw water tank;
- changes the value of the LIT-101 sensor which is a level transmitter; and
- P-102 which is a backup pump starts itself because the LIT301 level became low. P102 actuator pumps water from the raw water tank to the second stage. LIT301 sensor is a level transmitter.

Security analysts detect a changing pattern of traffic from an IP address, 192.168.1.60, and they identify a change with unknown reason in the value of the LIT-101 sensor. A request is sent to the threat hunting team to hunt the source of this malicious behaviour.

The hypothesis generated for this attack is ‘‘Tank 101 underflow’’. Using MITRE ATT&CK TTPs detected for this attack, hunters identify and request required data which is physical logs and network traffic. The Diamond model generated for the attack activity is as Figure 11. The description of these events is shown in Table 5. These events are Actual events meaning that there is evidence for the occurrence of

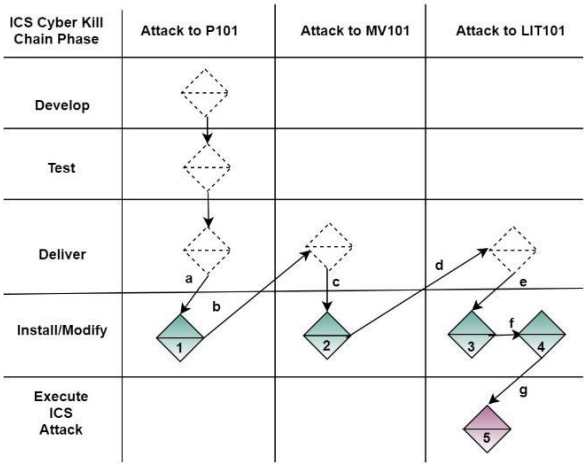


FIGURE 11. The Diamond model of the attack to tank 101.

TABLE 5. Activity thread events in the attack to tank 101.

Event	Verified	Description
1	Actual	Turn P-101 on continuously
2	Actual	Turn MV-101 on continuously
3	Actual	Change the value of LIT-101
4	Actual	P-102 starts itself because of LIT301 level
5	Actual	Tank 101 underflow; Tank 301 overflow

these events in the organisation's networks. The Diamond model in Figure 11 will be sent to the cyber threat intelligence phase to generate IoCs and store them in the CTI repository.

In this paper, we proposed a 3-layer method involving a trigger stage, the actual hunting, and a final treat intelligence layer. These concepts potentially benefit industrial control systems and/or other cyber-physical systems.

The goal of this hunting framework is to propose a solution to detect threat actors early in the cyber kill chain by searching for signs of an intrusion and then, updating detection strategies for future use.

VIII. CONCLUSION

A three-phase threat hunting framework was proposed in this paper to address the problem of hunting in ICS networks. The framework received triggers from security analysts and external sources. A combination of MITRE ATT&CK Matrix and Diamond models was used in the threat hunting phase to respectively identify adversarial TTPs and visualise attack routes towards its goals. This combination helps to understand activities in our network and compare them with possible attack routes to similar victims. A threat hunting hypothesis was proposed using the information received from hunting triggers. Then, the hypothesis was validated based on the data requested for threat hunting and using the Diamond model generated based on MITRE ATT&CK TTPs. Finally, the detected threat action was sent to a cyber threat intelligence stage in which hunters could generate CTI by extracting important features of the threat and store IoCs in a repository for future hunting. The generated CTI could also be fed into security analytics tools. The proposed framework was evaluated using three scenarios, Black Energy 3 malware, PLC-Blaster malware, and SWaT datasets. The evaluation outcomes showed that the proposed framework can be used by industrial companies to implement open-source threat hunting in their ICS networks.

In this paper, the process of hypothesis validation and threat intelligence generation are manual. The automation of these tasks can help to improve the response time. In addition, the quality and reliability of the hypothesis generated were not considered in this paper. Based on these limitations, some research gaps that should be considered in future works are:

- How can the reliability of the initial hypothesis be improved?
- How machine learning methods can be used to automate hypothesis validation and threat intelligence generation?
- How machine learning methods can be used to automatically cluster our Diamond models with known abnormal events?

ACKNOWLEDGMENT

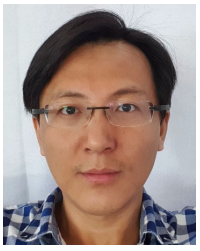
The authors acknowledge the support of the Commonwealth of Australia and Cybersecurity Research Centre Limited. The authors also acknowledge the Australian Cyber Security Centre (ACSC), and Dr. Rachel Mahncke and Daniel Meakins, from the Digital Government (DGov), Australia, for their supervision.

REFERENCES

[1] A. Bhardwaj and S. Goundar, "A framework for effective threat hunting," *Netw. Secur.*, vol. 2019, no. 6, pp. 15–19, Jun. 2019.
[2] S. Homayoun, A. Dehghantanha, M. Ahmadzadeh, S. Hashemi, and R. Khayami, "Know abnormal, find evil: Frequent pattern mining for ransomware threat hunting and intelligence," *IEEE Trans. Emerg. Topics Comput.*, vol. 8, no. 2, pp. 341–351, Apr. 2020.
[3] A. Cook, H. Janicke, R. Smith, and L. Maglaras, "The industrial control system cyber defence triage process," *Comput. Secur.*, vol. 70, pp. 467–481, Sep. 2017.
[4] H. Darabian, A. Dehghantanha, S. Hashemi, M. Taheri, A. Azmoodeh, S. Homayoun, K.-K.-R. Choo, and R. M. Parizi, "A multiview learning method for malware threat hunting: Windows, IoT and Android as case studies," *World Wide Web*, vol. 23, no. 2, pp. 1241–1260, Mar. 2020.
[5] S. Grooby, T. Dargahi, and A. Dehghantanha, "Protecting IoT and ICS platforms against advanced persistent threat actors: Analysis of APT1, silent chollima and molerats," in *Handbook of Big Data and IoT Security*. Cham, Switzerland: Springer, 2019, pp. 225–255.
[6] D. Ito, K. Nomura, M. Kamizono, Y. Shiraishi, Y. Takano, M. Mohri, and M. Morii, "Modeling attack activity for integrated analysis of threat information," *IEICE Trans. Inf. Syst.*, vol. E101.D, no. 11, pp. 2658–2664, Nov. 2018.
[7] J. Kotheimer, K. OMeara, and D. Shick, "Using honeynets and the diamond model for ICS threat analysis," Carnegie-Mellon Univ., Pittsburgh PA, USA, Tech. Rep. CMU/SEI-2016-TR-006, 2016.
[8] S. Homayoun, A. Dehghantanha, M. Ahmadzadeh, S. Hashemi, R. Khayami, K.-K.-R. Choo, and D. E. Newton, "DRTHIS: Deep ransomware threat hunting and intelligence system at the fog layer," *Future Gener. Comput. Syst.*, vol. 90, pp. 94–104, Jan. 2019.
[9] B. Stojanović, K. Hofer-Schmitz, and U. Kleb, "APT datasets and attack modeling for automated detection methods: A review," *Comput. Secur.*, vol. 92, May 2020, Art. no. 101734.
[10] B. E. Strom, J. A. Battaglia, M. S. Kemmerer, W. Kupersanin, D. P. Miller, C. Wampler, S. M. Whitley, and R. D. Wolf, "Finding cyber threats with ATT&CK-based analytics," MITRE Corp., Bedford, MA, USA, Tech. Rep. MTR170202, 2017.
[11] R. Al-Shaer, M. Ahmed, and E. Al-Shaer, "Statistical learning of APT TTP chains from MITRE ATT&CK," in *Proc. RSA Conf.*, 2018, pp. 1–2.

[12] *ATT&CK for Enterprise Introduction*. Accessed: Apr. 2021. [Online]. Available: https://attack.mitre.org/resources/enterprise-introduction/
[13] *ATT&CK for Industrial Control Systems*. Accessed: Apr. 2021. [Online]. Available: https://collaborate.mitre.org/attackics/index.php/Main_Page
[14] *Launching ATT&CK for ICS*. Accessed: May 2021. [Online]. Available: https://medium.com/mitre-attack/launching-attack-for-ics-2be4d2fb9b8
[15] D. L. Whyte, "Using a systems-theoretic approach to analyze cyber attacks on cyber-physical systems," Ph.D. dissertation, MIT, Cambridge, MA, USA, 2017.
[16] D. Gunter and M. Seitz, "A practical model for conducting cyber threat hunting," SANS White Paper 38710, Mar. 2019. [Online]. Available: https://www.sans.org/white-papers/38710/
[17] *SANS 2019 Threat Hunting Survey: The Differing Needs of New and Experienced Hunters*. Accessed: May 2021. [Online]. Available: https://www.sans.org/reading-room/whitepapers/bestprac/2019-threat-hunting-survey-differing-experienced-hunters_39220
[18] R. M. Lee and R. T. Lee, "SANS 2018 threat hunting survey results," SANS White Paper, Sep. 2018. Accessed: Jan. 20, 2021. [Online]. Available: https://www.sans.org/media/analyst-program/Multi-Sponsor-Survey-2018-Threat-Hunting-Survey.pdf
[19] B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington, and C. B. Thomas, "Mitre ATT&CK: Design and philosophy," MITRE, McLean, VA, USA, Tech. Rep. 18-0944, 2018.
[20] *The HELK*. Accessed: May 2021. [Online]. Available: https://thehelk.com/intro.html
[21] M. Collins, *Threat Hunting*, 1st ed. Newton, MA, USA: O'Reilly Media, 2018.
[22] L. Ertaul and M. Mousa, "Applying the kill chain and diamond models to Microsoft advanced threat analytics," in *Proc. Int. Conf. Secur. Manage. (SAM), World Congr. Comput. Sci., Comput. Eng. Appl. Comput. (World-Comp)*, 2018, pp. 252–258.
[23] S. Caltagirone, A. Pendergast, and C. Betz, "The diamond model of intrusion analysis," DTIC document, Southmoor, U.K., Tech. Rep., 2013.
[24] Y. Ghazi, Z. Anwar, R. Mumtaz, S. Saleem, and A. Tahir, "A supervised machine learning based approach for automatically extracting high-level threat intelligence from unstructured sources," in *Proc. Int. Conf. Frontiers Inf. Technol. (FIT)*, Dec. 2018, pp. 129–134.
[25] I. Deliu, C. Leichter, and K. Franke, "Extracting cyber threat intelligence from hacker forums: Support vector machines versus convolutional neural networks," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2017, pp. 3648–3656.
[26] *BlackEnergy APT Attacks in Ukraine*. Accessed: May 2021. [Online]. Available: https://www.kaspersky.com/resource-center/threats/blackenergy
[27] R. M. Lee and D. Bianco. (2016). *Generating Hypotheses for Successful Threat Hunting*. [Online]. Available: https://www.sans.org/readingroom/whitepapers/threathunting/generatinghypotheses-successful-threat-hunting-37172
[28] *BlackEnergy 3, MITRE*. Accessed: May 2021. [Online]. Available: https://collaborate.mitre.org/attackics/index.php/Software/S0004
[29] Booz Allen Hamilton. (2019). *When the Lights Went Out: Ukraine Cybersecurity Threat Briefing*. Accessed: May 19, 2021. [Online]. Available: http://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukrainereport-when-the-lights-wentout.pdf
[30] M. J. Assante and R. M. Lee, "The industrial control system cyber kill chain," SANS Inst., North Bethesda, MD, USA, Tech. Rep. 36297, Oct. 2015. Accessed: Sep. 21, 2021. [Online]. Available: https://www:sans:org/reading-room/whitepapers/ICS/industrial-controlsystem-cyber-kill-chain-36297
[31] R. Spenneberg, M. Brüggemann, and H. Schwartke, "PLC-blaster: A worm living solely in the PLC," in *Proc. Black Hat Asia*, vol. 16, 2016, pp. 1–16.
[32] *PLC-Blaster, MITRE*. Accessed: May 2021. [Online]. Available: https://collaborate.mitre.org/attackics/index.php/Software/S0009
[33] J. Goh, S. Adepu, K. N. Junejo, and A. Mathur, "A dataset to support research in the design of secure water treatment systems," in *Proc. Int. Conf. Crit. Inf. Infrastructures Secur.* Cham, Switzerland: Springer, Oct. 2016, pp. 88–99.
[34] *Secure Water Treatment Dataset, iTrust Centre for Research in Cyber Security*. Accessed: May 2021. [Online]. Available: https://itrust.sutd.edu.sg/itrust-labs_datasets/dataset_info/
[35] A. Berady, M. Jaume, V. V. T. Tong, and G. Guette, "From TTP to IoC: Advanced persistent graphs for threat hunting," *IEEE Trans. Netw. Service Manage.*, vol. 18, no. 2, pp. 1321–1333, Jun. 2021.
[36] B. Burr, S. Wang, G. Salmon, and H. Soliman, "On the detection of persistent attacks using alert graphs and event feature embeddings," in *Proc. IEEE/IFIP Netw. Oper. Manage. Symp. (NOMS)*, Apr. 2020, pp. 1–4.
[37] A. D. Raju, I. Y. Abualhaol, R. S. Giagone, Y. Zhou, and S. Huang, "A survey on cross-architectural IoT malware threat hunting," *IEEE Access*, vol. 9, pp. 91686–91709, 2021.
[38] O. Alexander, M. Belisle, and J. Steele, "MITRE ATT&CK for industrial control systems: Design and philosophy," MITRE Corp., 2020. Accessed: Mar. 1, 2021. [Online]. Available: https://collaborate.mitre.org/attackics/img_auth.php/3/37/ATT%26CK_for_ICS_-_Philosophy_Paper.pdf
[39] Y. Mekdad, G. Bernieri, M. Conti, and A. E. Fergougui, "A threat model method for ICS malware: The TRISIS case," in *Proc. 18th ACM Int. Conf. Comput. Frontiers*, May 2021, pp. 221–228.
[40] N. Mohamed and B. Belaton, "SBI model for the detection of advanced persistent threat based on strange behavior of using credential dumping technique," *IEEE Access*, vol. 9, pp. 42919–42932, 2021.
[41] E. C. Thompson, "Threat hunting," in *Designing a HIPAA-Compliant Security Operations Center*. Berkeley, CA, USA: Apress, 2020, pp. 205–212.
[42] R. Jhaveri, R. Sagar, G. Srivastava, T. R. Gadekallu, and V. Aggarwal, "Fault-resilience for bandwidth management in industrial software-defined networks," *IEEE Trans. Netw. Sci. Eng.*, early access, Aug. 12, 2021, doi: 10.1109/TNSE.2021.3104499.
[43] R. H. Jhaveri, N. M. Patel, Y. Zhong, and A. K. Sangaiah, "Sensitivity analysis of an attack-pattern discovery based trusted routing scheme for mobile ad-hoc networks in industrial IoT," *IEEE ACCESS*, vol. 6, pp. 20085–20103, 2018.
[44] A. B. Ajmal, M. Alam, A. A. Khaliq, S. Khan, Z. Qadir, and M. A. P. Mahmud, "Last line of defense: Reliability through inducing cyber threat hunting with deception in SCADA networks," *IEEE Access*, vol. 9, pp. 126789–126800, 2021.
[45] A. B. Ajmal, M. A. Shah, C. Maple, M. N. Asghar, and S. U. Islam, "Offensive security: Towards proactive threat hunting via adversary emulation," *IEEE Access*, vol. 9, pp. 126023–126033, 2021.
[46] V. Mavroeidis and S. Bromander, "Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence," in *Proc. Eur. Intell. Secur. Informat. Conf. (EISIC)*, Sep. 2017, pp. 91–98.
[47] A. de Melo e Silva, J. J. C. Gondim, R. de Oliveira Albuquerque, and L. J. G. Villalba, "A methodology to evaluate standards and platforms within cyber threat intelligence," *Future Internet*, vol. 12, no. 6, p. 108, Jun. 2020.
[48] K. Stouffer. (Jun. 3, 2015). *SP 800-82 Rev. 2, Guide to Industrial Control Systems (ICS) Security | CSRC. NIST*. Accessed: May 2021. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

ZAHRA JADIDI received the Ph.D. degree in network security from the ICT School, Griffith University. She is a Research Fellow at the Queensland University of Technology. Her research interests include the security of critical infrastructure, anomaly detection, and automation of security analysis.



YI LU received the Ph.D. degree in computer science from the University of New South Wales, in 2008. Since then, he worked as a Lecturer at the University of New South Wales and later as a Principal Researcher at Oracle Labs. He is a Senior Lecturer at the Queensland University of Technology. His research interests include the broad area of programming languages and information security, focusing on both theoretical and practical aspects of software security.