Cyber Threat Hunting Case Study using MISP

Meryem Ammi[1*] and Yusuf Mohamud Jama[2]

[1*]Department of Forensics, Criminal Justice College, Naif Arab University for Security Sciences, Riyadh, Kingdom of Saudi Arabia. mammi@nauss.edu.sa,
Orcid: https://orcid.org/0000-0001-6264-3720

[2]CEO of Managed Guard, Cybersecurity Researcher, Mogadishu, Somalia. yusuf3mj@gmail.com
Orcid : https://orcid.org/0009-0005-7696-8020

Received: February 04, 2023; Accepted: March 26, 2023; Published: May 30, 2023

Abstract

The growing frequency of cyberattacks invokes the need to develop and implement more efficient security strategies. Traditional preventive security measures are not able to counter incident threats effectively. These traditional approaches are usually based on heuristic, default or periodic signature rules that cannot efficiently prevent and repel more dynamic modern attacks. Threat hunting (TH) is gaining popularity because it helps to uncover the presence of attacker tactics, techniques and procedures (TTPs) within an environment that has not already been discovered by existing technologies. Threat hunting and threat intelligence are two distinct security disciplines, but they have the capacity to be complimentary. Hence, using cyber threat intelligence (CTI) to reinforce the traditional cybersecurity strategies by generating indicators of compromise (IoCs) feeds of the recent emerging cyberattacks can help the organisation mitigate the attacks more effectively and efficiently.

The primary aim of this paper is to design an approach that, based on cyber threat intelligence, will improve the cybersecurity defence strategies adopted by organisations. This goal will be achieved through the presentation of an architecture that collects threat information and feeds to security tools. This proposed architecture contains four main components: data aggregation, normalisation and enrichment, integration with the security operation centre (SOC) tools and real-time monitoring of security information and event management (SIEM).

After developing and implementing this architecture, we have conducted tests using Malware Information Sharing Platform (MISP) as a CTI platform to collect the threat information regarding the indicators and the Tactics, Techniques and Procedures (TTPs) of the known attack (Muddy Water threat actor). Subsequent tests were also conducted on emerging cyberattacks (SVBMv3 vulnerability and Covid19 themed cyberattacks campaign). The results obtained provide a defence of the in-depth approach of cybersecurity, which mitigates cyberattacks by efficiently using threat intelligence capabilities for emerging cyberattacks and when threat actors are targeting organisations, using the IoCs collected and the tactics, techniques and procedures.

Keywords: Cyber Threat Intelligence, Threat Hunting, Attack, MISP.

Journal of Internet Services and Information Security (JISIS), volume: 13, number: 2 (May), pp. 01-29.
DOI: *10.58346/JISIS.2023.I2.001*

*Corresponding author: Department of Forensics, Criminal Justice College, Naif Arab University for Security Sciences, Riyadh, Kingdom of Saudi Arabia.

1 Introduction

The ever-changing landscape of cyberthreats has brought about several key challenges in an increasingly large number of connected devices. According to the CROWDSTRIKE 2020 Global Threat Report, cyberattacks affect every sector and preventing these sophisticated attacks has become a considerably difficult task (Crowdstrike, 2020). The impact of cybercrime damage will hit $6 trillion annually by 2021, according to the Official Annual Cybercrime Report from Cybersecurity Ventures in 2019 (Cybersecurity Ventures, 2019). Another example stated by Marelli, M. (2022), the SolarWinds hack of 2021 revealed security flaws in the software supply chain, enabling hackers to penetrate several government agencies and private entities. Moreover, the lack of readiness in general security approaches has also led many organisations to turn their efforts towards CTI (Shin & Lowry, 2020).

To counter these advanced threats, cybersecurity systems must have the right data and priori-knowledge to detect and mitigate them. This process of acquiring the threat information ahead of time can also be referred to as Cyber Threat Intelligence (CTI). The activities of CTI are designed to recover threat information; including threat sources, actors, types, technologies and attack vectors. This information is directly relevant to a specific organisation, assisting in the engineering of more precise defence strategies (Shin & Lowry, 2020).

Furthermore, the frequency of cyber threats has increased; becoming more targeted and widespread. A new category of cyber threat has emerged, referred to as advanced persistent threats (APT). These groups are sophisticated and well-resourced adversaries that target specific information in high-profile organisations and governments using various methods and tools including zero-day vulnerabilities, new malware and sophisticated social engineering techniques like the phishing campaigns of coronavirus disease 2019 (COVID-19).

According to Recorded Future, threat actors are using COVID-19 as a theme for phishing lures to target victims around the world. They also observed that some of the cases related to the COVID-19 cyberattacks have been leveraged by possible nation-state actors. This situation shows how threat actors are ready to take advantage of global disruptions caused by COVID-19 to enhance their cyber threat activities. Furthermore, this accentuates the importance of tracing and monitoring the changing threat landscape to defend the critical infrastructure within public or private organisations and institutions (Recorded Future: Securing Our World with Intelligence, 2020).

Cyber threat hunting involves a proactive and iterative search for malicious actors and indicators in various types of logs. This proactive search process takes place in different environments such as networks and datasets, in order to detect and respond to progressive cyber threats that are not detected by rule- or signature-based security tools (Berndt & Ophoff, 2020). Threat hunting combines the use of threat intelligence, analytics, and automated security tools with experience, human intelligence and skills (Javeed et al., 2020). In fact, many efforts have been conducted by researchers and the industry but the current threat hunting process still faces the challenges of labor-intensive and error-prone approaches. Existing processes require non-trivial efforts of manual query construction and have overlooked the rich external knowledge of threat behaviors provided by open-source Cyber Threat Intelligence (OSCTI) (Gao et al., 2021).

Moreover, the process of acquiring the threat information ahead of time, known as Cyber Threat Intelligence (CTI), requires dutiful attention and prevention due to the fact that it entails actionable threat information customised to a specific organisation (Shin & Lowry, 2020). The primary aim of this process is to counter those advanced threats by feeding the conventional defence tools with the information required to detect and mitigate the threats. Using CTI capabilities indicates ‘what is bad’ to the defenders

or threat hunters so they know which threats to hunt by enforcing their defence strategies and feeding their cybersecurity tools with threat information from CTI platforms.

CTI implementation assists an organisation in performing threat detection and remediation in a more timely, proactive and preventive manner. This, in turn, enhances conventional risk-management which is built to improve general preparedness against a variety of threats (Shin & Lowry, 2020), (Kure, Islam, & Mouratidis, 2022). Thus, the purpose of CTI is to enable better security decision-making run relation to threats at different levels of the organisation, including strategic, tactical and operations. The National Institute of Standards and Technology (NIST), in 2016, defined this type of threat information as any useful knowledge that an organisation can use in its defence tools (e.g. security information and event management (SIEM)) to protect their data against threat actors (National Institute of Standards and Technology, 2014); this includes the following:

- Indicators of Compromise (IoCs)
- Tactics, techniques and procedures (TTPs)
- Security alerts
- Threat intelligence reports
- Tool configurations

This data can be categorised into Low-level cyber threat data and High-level cyber threat data:

1. Low level cyber threat data IoC includes IPs, network artefacts, hashes, keystroke, windows event log and several more of the most commonly used cyber threat data in CTI and intrusion detection systems (IDS). This low data yields an effective threat analysis because it helps to identify and profile threats. One of the main disadvantages of this type of data is that it is atomic in nature, insofar as the threat actor can change these IoCs dynamically so as to evade and bypass the detection and prevention techniques (Al-Taleb, N., Saqib, N. A., & Dash, S., 2020).
2. The high-level threat data includes techniques, tactics and procedures of the threat attackers: i.e., its behaviour, pattern and motivation. One main disadvantage is the need for human interference in order to extract knowledge. Due to the textual and unstructured nature of the threat data, human skills interference is needed to select the appropriate and accurate type of information to be fed into the machine. Extracting the targeted knowledge from different sources is a challenge. The selection of the keywords can affect the knowledge extraction from different sources by potentially discarding important and critical data. Consequently, it will affect the threat analysis and the profiling of threats and actors. These types of cyber threat data are provided by different sources that ensure to provide the relevant threat information on time, such as FireEye, IBM X-Force, and Threat Tracer (Al-Taleb, N., Saqib, N. A., & Dash, S., 2020).

Effective implementation of CTI (Cyber Threat Intelligence) within an organization can bring numerous benefits and advantages. One of the main advantages is that it enhances an organization's ability to predict and prevent potential threats by leveraging methodologies and techniques learned through CTI. This learning will also help the organisation to act proactively against these attacks and even prioritise them as risks. This rise in awareness level will undoubtedly allow the organisation to gain more visibility regarding threats that impact business. This will lead to an efficiency in decision making, the deployment of suitable countermeasures and enhance the collaboration between different entities and peers against cyberattacks through CTI sharing (Shin & Lowry, 2020).

The contribution of this paper is twofold. Firstly, this paper aims to design a cyber threat intelligence approach that enhances the work of threat hunting and provides enough threat intelligence to mitigate emerging cyberattacks. Secondly, the implementation of this approach through the use of collected threat intelligence and feeding it to security tools such as Network Intrusion Detection System (NIDS) and

Host Intrusion Detection System (HIDS) to detect attacks. For different threat detection levels such as indicators of compromise (IoCs), and Tactics, Techniques and Procedures (TTPs) this will augment their cyber defensive capabilities through situational awareness, prediction, and automated course of action.

The rest of the paper is organised as follows: Section 2 explains the related works concerning Cyber Threat Intelligence and cyber threat information sharing in security operations. Section 3 details the designed architecture of the cyber threat intelligence and explains the methodology for implementing the proposed approach. Section 4 presents a case study of the proposed approach, an analysis of the results and a discussion on the findings. Section 5 concludes the paper.

2 Related Work

Threat hunting is a proactive approach to cybersecurity that involves actively searching for and identifying potential threats and vulnerabilities within an organization's network. It has become an increasingly popular approach in recent years as traditional reactive security measures have proven to be inadequate in detecting and mitigating advanced persistent threats (APTs).

A significant amount of research has been conducted in the area of threat hunting, including the development of various frameworks, methodologies, and tools. Some of the popular frameworks and methodologies for threat hunting include the MITRE ATT&CK framework, the Diamond Model, and the Cyber Kill Chain. These frameworks provide a structured approach to threat hunting and help analysts identify potential threat actors, tactics, and techniques.

Given that this paper proposes a CTI model of how to incorporate CTI useful information into a conventional security strategy for an organisation, this section offers an overview of the use of CTI in general by the industry, the benefits of this approach and the grey areas between CTI and traditional cybersecurity research domains.

The use of CTI within organisations is growing from year to year. According to a survey conducted by SANS, the majority of organisations involved with CTI fall into one of these categories: those who produce intelligence, those who consume the produced intelligence and the hybrid category which produces and consumes intelligence. 72% of organisations reported that they consume or produce intelligence. This record has witnessed an increase since 2017, when it was 60%, and 2018, when it reached 68% (Brown & Lee, 2019).

One of the main aspects related to cyber threat intelligence sharing is automation (Wagner et al., 2019). This automation process is a necessity in order to cope with the considerable amount of information threats and vulnerability incidents. The process of sharing does involve some manual tasks like copying and pasting other ‘peers’ information. Data processing is also one the tasks that might be done manually because analysts have to evaluate the problem, implement the solution and share the information (Wagner et al., 2019).

The most important step is that of classification during the collection of data, a step which is vital for the effective discovery of threats and the documenting of incidents through statistics, data analytics and visualisation. Organisations need some form of standards to facilitate information sharing for CTI purposes. The US department and MITRE framework have developed protocols in the community: the Structured Threat Information Expression (STIX) and the Trusted Automated exchange of Indicator Information (TAXII), Cyber Observable Expression (CybOX) (Wagner et al., 2019) which act as a package to handle the different needs of CTI information sharing (Abu et al., 2018). These standards have been widely approved by international organisations as CTI sharing standard formats (Wagner et al., 2019) which solve the interoperability issue between sharing peers.

The CTI sharing collaboration between different stakeholders might be conducted through many methods; peer-to-peer, peer-to-hub, or a hybrid exchange (Wagner et al., 2019). These stakeholders belong to the same industry sector and share similar interests in attack patterns (Wagner et al., 2019). A threat sharing model, focussing on the collection, analysis and classification of CTI, has been presented for developing countries such as South Africa, as detailed by the research in (Mutemwa, Mtsweni, & Mkhonto, 2017). External tools such as anti-virus software and intrusion detection systems have been integrated into this model.

Sources for CTI collaboration can differ from one organisation to another and on a case-to-case basis as reported by an AlienVault survey at Black Hat 2016. The collaboration predominantly relies on the detection process of the organisation, paid subscriptions or government agencies as well as the community and open-source feeds (Lutf, 2018). For CTI to be effective, organisations need to cooperate by sharing threat information which may affect them all, however, this is not always possible due to confidentiality or reputation (Mohaisen et al., 2017). Moreover, the quality of the shared information or indicators is crucial for effective CTI (Asiri et al., 2023).

The different attributes offered by CTI turns this information into actual intelligence. The National Institute of Standards and Technology (NIST) defined the types of threat information as anything that and organisation can use in its defence tools (e.g. SIEM) to help protect their data against threat actors (National Institute of Standards and Technology, 2014)' this include indicators, tactics, techniques and procedures (TTPs), security alerts, threat intelligence reports and tool configurations. CTI indicators of compromise (IOCs) represent the forensic artefacts of an attack Liao et al. (2016). Therefore, these indicators can be used to investigate the attack once it occurs and eventually counter it during the execution. More specifically, an IOC incorporates not just individual data fingerprints associated with an explicit attack (such as the hash value of a detected malware), but also the setting of the attack and an examination of the behaviour of the adversary (such as the techniques used) Liao et al. (2016). Accordingly, the CTI gathering techniques incorporate the identification of the adversary TTPs, which, together with the threat fingerprints, help the cybersecurity and incident response teams of an organisation to understand their security posture, recognize early indications of attack and consistently enhance their security controls (Lacava, G., 2021).

NIST also defined the common characteristics of the efficient threat information that can be measured (National Institute of Standards and Technology, 2014) in terms of timeliness, relevance, accuracy, specificity and mitigating actions. The CTI process of gathering intelligence and converting it into actionable intelligence includes planning and requirement, collection and processing, analysis, production, dissemination and feedback (FireEye, 2020). As mentioned earlier, there are four CTI subdomains; strategic, operational, tactical and technical (Record Future, 2019).

CTI provides cyber defender early warning information of emerging cyberattacks that may target their organisation so that they can introduce the right measures to prevent the threat or minimize its impact. For instance, According to Hyslip and Burruss (2023), the most recent WannaCry ransomware attack managed to spread to more than 150 countries in only one day and infected more than 230,000 computers. Narayanan et al. (2018) explained that Microsoft batched the vulnerability used by WannaCry ransomware on March 14 2017, which limited the massive damage potential of this attack. The authors used this example to illustrate how critical it is to cyber threat intelligence to be aware of newly reported vulnerabilities. Lutf (2018) explained that many cyberattacks usually affect more than one organisation, often from the same sector. The authors also explored the need to share threat information and for collaboration between organisations. Miazi et al. (2017) discussed the game of threat hunting and the mindset behind effective hunting strategy using the CTI approach. Mavroeidis et

al. (2017) suggested a CTI model that can be used in the security operation of an organisation for its detective and preventive capabilities. The presented model evaluates and classifies taxonomies and shares standards and ontologies of relevant threat intelligence in order to mitigate emerging cyberattacks. Tounsi and Rais (2018) discussed emerging trends and standards of existing cyber threat intelligence types. The authors also conducted an evaluation of different threat intelligence platform (TIP) tools in order to start filtering and sharing information effectively.

Overall, improving security in an organisation may be done through a multitude of avenues. As stated in (Shackleford, 2018), the top three ways are:

- Improving the visibility of threats and attack methodologies impacting the environment
- Improving security operations
- Detecting unknown threats

Current trends indicate that CTI is being mainly aligned with the SOC, and operating alongside operational activities such as threat hunting, monitoring, and responses to incidents (Shackleford, 2018). This is reinforced by the top three methods mentioned above. Furthermore, according to the survey, CTI seems to be of maximum utility to those operations teams that are monitoring environmental events, proactively searching for threats and responding to incidents.

Wagner et al., (2016) described the threat intelligence sharing platform known as MISP (Malware Information Sharing Platform) along with its architecture and implementation. The authors outline the design and features of MISP, which offers a collaborative platform for sharing and correlating threat information among security practitioners, and discuss the difficulties associated with sharing threat data across enterprises. With insights about the evaluation of MISP's usefulness in enhancing collaboration and sharing of threat intelligence. The authors discussed also some insights into the planning and execution of a platform that can ease the sharing and disseminating of threat intelligence among various companies. Parmar and Domingo (2019) presented a study that aimed to evaluate the use of CTI in support of the commander understanding of the adversary. The result of this study suggested that the use of MISP platform and open source intelligence can provide valuable information by linking the indicators of compromise with the Adversarial Tactics, Techniques & Common Knowledge (ATT&CK) techniques deployed using MITRE ATT&CK framework (Qiang et al., 2018) also discussed and proposed a comprehensive evaluation architecture of CTI from a user perspective to measure the quality of threat intelligence feeds. The authors detailed the process of the proposed architecture as category, functions, properties, testing methods and items that decide the quality of the received threat information.

Mohaisen et al. (2017) discussed the use model of sharing information and communities to understand the various technical details involved, including security, privacy and functional issues. They concluded the research by emphasising the necessity of utilising the underlying community of trust, threat and use model, highlighting privacy through a measurable context in order to produce actionable threat intelligence within the community.

In (Skopik, Settanni, & Fiedler, 2016), a survey on collective cyber defence through security information discussed the overall issues of information sharing in the context of CTI. It concluded that the effectiveness of the threat intelligence platform could be increased with the presence of a strong active sector-oriented or region-oriented community.

One of the main challenges of CTI is its adaptation within an organisation, which requires efforts of technical implementation skills and use of the appropriate tools with regards to the available funds allocated to this process (Berndt & Ophoff, 2020), (Kotsias, Ahmad, & Scheepers, 2023).

To the best of the authors knowledge, this paper is the first to depict the challenge of adopting CTI through open-source tools and platforms. In this case, the novelty is the ability to integrate the CTI attributes (IoC and) effectively with SIEM tools, which are more or less commonly and conventionally used in many organisations. Regarding this, a case study of turning data into actionable intelligence will be shown.

Also, in our case study, we tackled six threat groups (APT33, APT34, APT35, APT39, TEMP. Zagros (Muddy Water) and Temp. Omega). In order to threat hunt the cyberattacks that might be caused by these groups effectively, two main attributes of the CTI (IoC and TTPs) will be used: the COVID-19 Cyber Threat Coalition - IOC and Muddy Water -TTPS.

3 Proposed Approach Architecture

The main objective of this paper is to add another layer of defence to protect any organisation against the type of sophisticated cyberattacks that traditional and conventional cybersecurity defence approaches cannot mitigate, as shown in Fig. 2. The proposed approach utilises cyber threat intelligence to obtain the data of attacks that are happening around the world and feed their artefacts to the defence tools used by the organisation so as to prevent cyberthreats.

This work intends to utilise the benefits of CTI for more than just focussing on internal intelligence data like anti-virus logs and threat feeds because this is considered as reactive approach. Instead, a more proactive stance will be adopted, implementing the CTI function through which more external threat feeds are analysed to discover threat actors and malware before an attack happens (Grisham et al., 2017).

Fig.2 shows a very simple conventional architecture of SIEM tools used by the majority of small organisations. In this case, the organisation is using its internal detection process to collect data. This data, after monitoring, is the main source that provides ‘higher visibility ’into its environment. Considering a government feed, or pulling data from a crowdsourced platform, could offer a clear perspective of the threat landscape overall. This perspective can greatly assist the organisation in the development, maintenance and fine-tuning of intelligence requirements that back-up business operations in the planning and direction phase of the Intelligence Lifecycle.

As a result, three categories of threat intelligence sources might be deduced as follows: internal source, external and community (Fig.1).

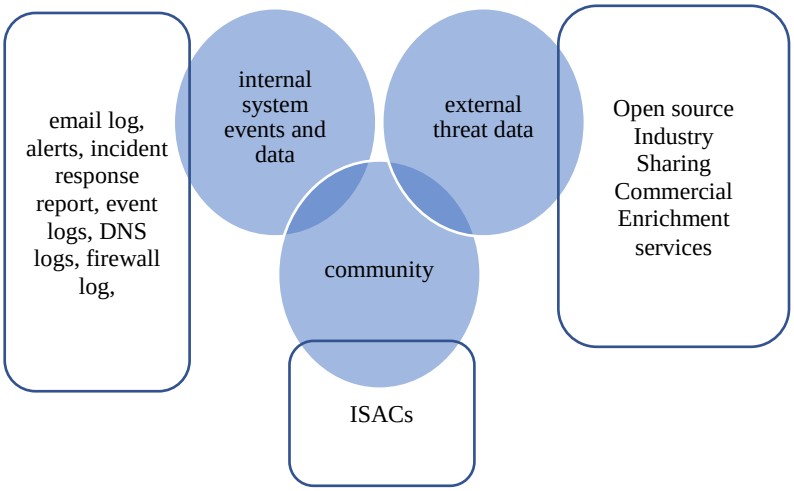


Figure 1: Source f Threat Intelligence

Internal sources are where the organisation depends on the threat data collected through its SIEM tools; such sources include email logs, alerts, incident response reports, event logs, DNS logs and firewall logs.

External sources can be obtained from open sources such as security researchers, vendor blogs, publicly available reputation and block lists which provide indicators for detection, most of the time, freely. The only issue related to open source data and feeds is the necessity for verification by the experts of the organisation in order to determine relevance.

Data quality is one of the main issues in open source intelligence (OSINT) (Schlette et al., 2021). Private sources of threat intelligence are accessible through a fee and offer threat intelligence feeds, structured data reports (such as STIX) and unstructured reports (such as PDF and Word documents). These paid feeds have a service level agreement (SLA) on data quality through a cyber threat intelligence update mechanism from the vendor.

Community based threat sources include any trusted channel CTI where the members have common interests. Information Sharing and Analysis Centers (ISACs) are organised under the National Council of ISACs (NCI) and specifically cover higher education or financial services. ETIS CERT-SOC Telco Network is another example where every member contributes threat information on telecommunication that they have detected through their infrastructure monitoring. This community uses MISP as their threat intelligence platform to collect and share threat information, including Malware indicators and vulnerabilities in the relevant telecommunication equipment (CERT-SOC, n.d.).

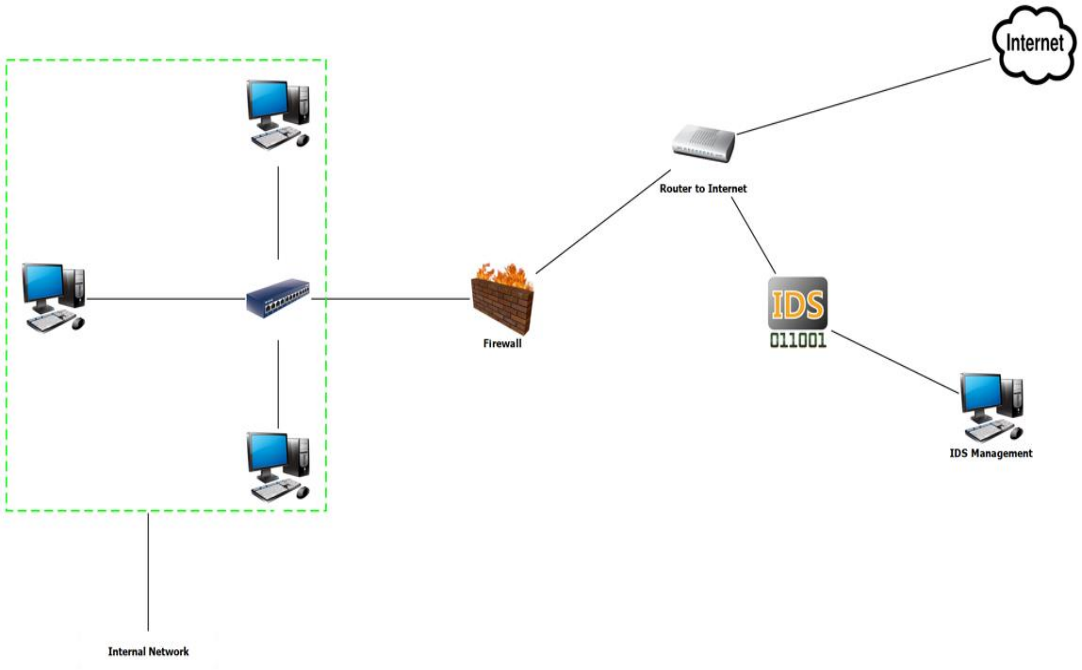


Figure 2: Traditional Cybersecurity Defence Approach

The proposed approach uses a Malware Information Sharing Platform (MISP) project as a platform to collect, analyse and disseminate threat intelligence information (MISP Project, n.d.). In the suggested model, as shown in Fig.3, the architecture consists of four layers, namely: open source intelligence (OSINT) feeds, MISP project, IDS/IPS tools and Elastic Stack as a SIEM tool is proposed. This section of the paper will describe the main components and processes of the proposed approach, as depicted in Fig.3(a and b).

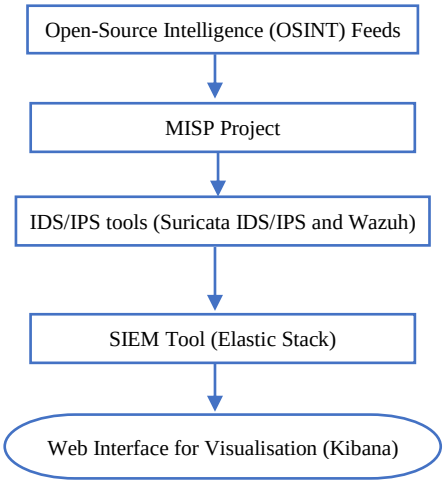


Figure 3(a): Flowchart of Proposed Architecture

Data aggregation and collection is conducted through the use of MISP, which is based on a hub-spoke model (TAXII) and represents an external threat data source.

The next step is Data Preprocessing; after normalising the format of the gathered data, the enrichment process turns it into actionable intelligence through the use of two main approaches: 'feedback and addition' and collaborative analysis. We used MITRE's ATT&CK Framework to gather TTPs. The study itself analysed the Cyber Threat APT.

After this, the intelligence is integrated with the security tools. In this case study, the basic conventional security tools used by our organisation is Suricata IDS/IPS and Wazuh HIDS.

Following this integration is the real time monitoring. The powerful Elastic Stack platform analyses machine data that has been organised. This data can be quickly searched and then visualized by Kibana, its web interface. Fig.3(b) explains the main four layers of the architecture proposed and the tools used.

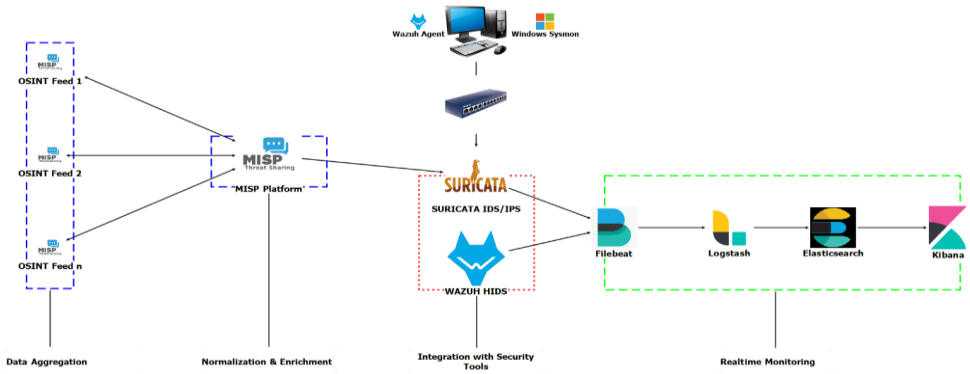


Figure 3(b): Proposed Approach Architecture

3.1. Data Collection (Data Aggregation)

In the proposed approach, we used the hub-spoke model infrastructure upon which the MISP is relying. This model is based on a hub and spoke sharing model (Trusted Automated exchange of Indicator of Information: TAXII). In this model, there is a central point called the hub, which is the server responsible for a MISP instance, where all data is kept. The spokes are the contributors that interact with the hub and share OSINT feeds, as shown in Fig. 4.

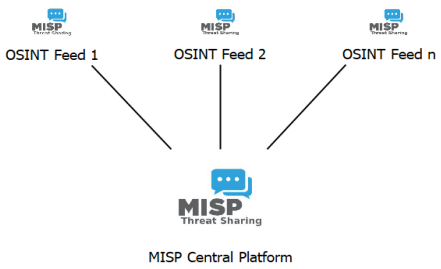


Figure 4: Hub-Spoke Model

In order to collect threat information from different open source feeds, we must first install MISP Project platform into our Ubuntu 18.04 server. For more information about installation and configuration refer to (MISP Project, n.d.). Once the installation is completed, a link will be provided that enables the user to access the platform https://192.168.227.129, as show in Fig. 5.

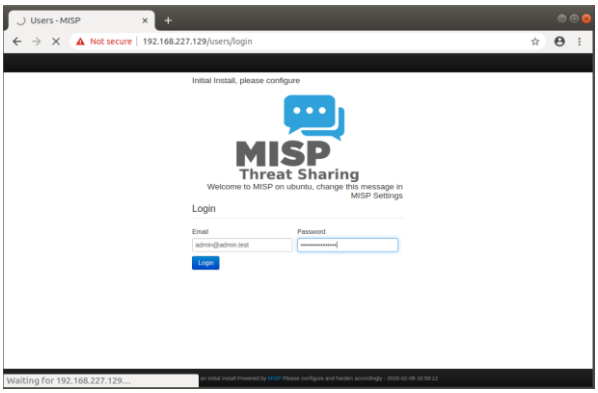


Figure 5: MISP Login

The second step is to enable the open source feeds to get threat information. In order to do so, the user has to operate a click Sync Action menu and then click on List Feeds, as shown in Fig. 6. The user will then see a list of feeds and should click the first check the feed_id box to select a list of all available feeds. After that, the user can click ‘Enable Selected’ to enable all the feeds and finally click Fetch and Store All Feed Data to obtain the data.

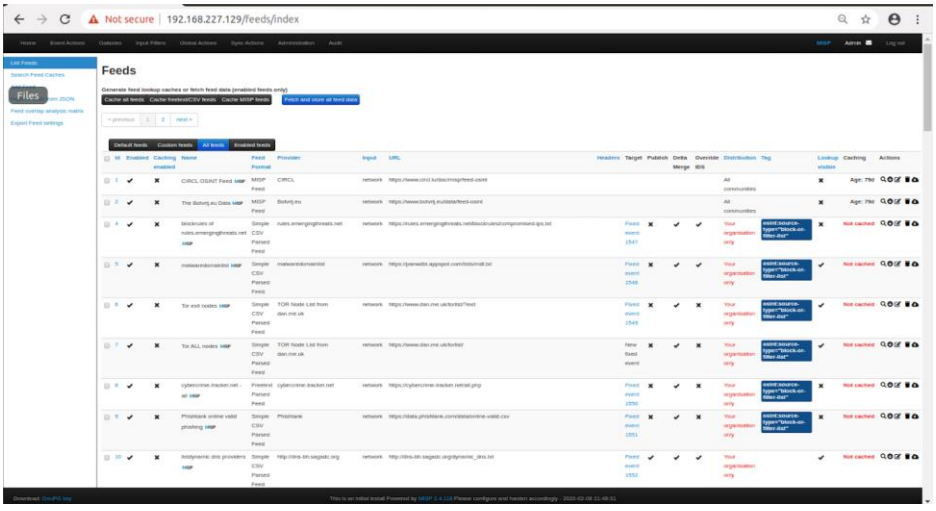


Figure 6: Feeds

Thirdly, the user will get the latest threat information shared within the community, including the local threat information that the user has created, as shown in Fig. 7.

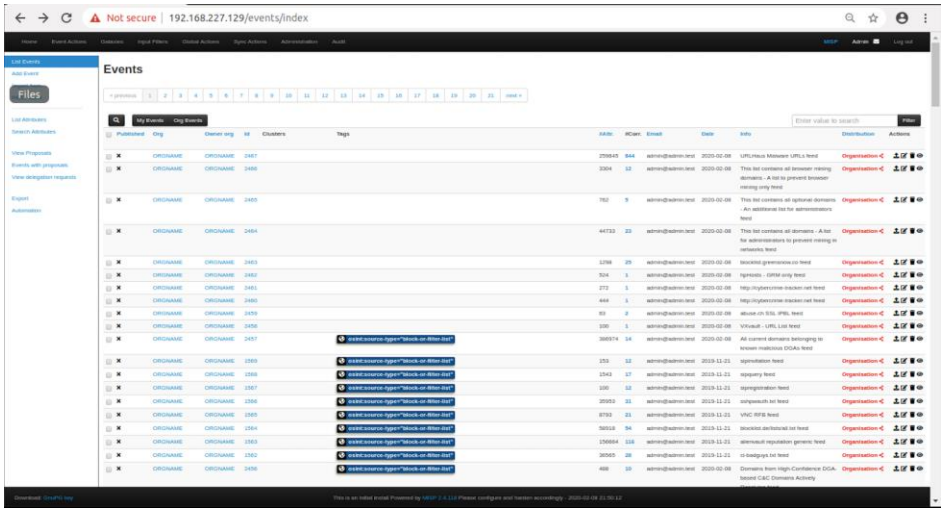


Figure 7: Events

3.2. Data Preprocessing (Normalisation and Enrichment)

To normalise the data that is coming from different feeds, MISP receives the data in a MISP event format and imports it in CSV file format. It is required to have a header which tells the MISP the starting point, in case the user wants to skip some records ("Logstash: Collect, Parse, Transform Logs," n.d.). MISP events will also be exported in a Common Event Format (CEF), which means each attribute matching with some predefined types is then exported in CEF format ("Export Modules," n.d.).

The most important part of the analysis stage is the enrichment process of the threat intelligence which adds another value to make it actionable threat intelligence. In order to enrich the data that we collected from open sources, we will use some of the community enrichment approaches: 'feedback and addition' or collaborative analysis.

a. Feedback and Addition

As we are collaborating to combat the kind of sophisticated cyberattacks that a single organisation or country cannot handle, after sharing threat information the easiest way is to give the community feedback if the shared threat information resulted in a successful detection of an attack or it is considered as false-positive; in MISP this is typically referred to as sighting.

This sighting contextualises the IoCs, giving the community more information about the threat information, such as the credibility or visibility of IoCs, as shown in Fig. 8. The sighting gives the event or attribute the validity of the indicator by the number of true positives detected within it, the number of times it has been marked as a false positive and the number of different expiration dates assigned to this attribute; all of which is valuable information for the community.

Figure 8: Sighting

Another approach to enrich the threat information is to propose the addition or update of an indicator into an existing event or threat when another community member detects one instead of creating and sharing a new event on basically the same threat.

b. Collaborative Analysis

Another useful approach to enrich threat intelligence is to promote community collaboration regarding the analysis of the tactics, techniques and procedures (TTPs) used by the adversaries. This collaboration gives members of the community the opportunity to take advantage of the available analysis to mitigate the emerging threats when there are not enough IoCs are available during the first emergence of an attack.

Moreover, Fig. 9 represents the Cyber Kill Chain which is the structure of an attack. This chain is used to analyse every step that the adversaries are using so as to understand what the organisation is missing in order to detect this emerging cyberattack. Cyber Kill Chain consists of PRE-ATTACK and ENTERPRISE ATTACK. The former aligns the first three phases and ENTERPRISE ATTACK aligns the rest (Bahrami et al., 2019).

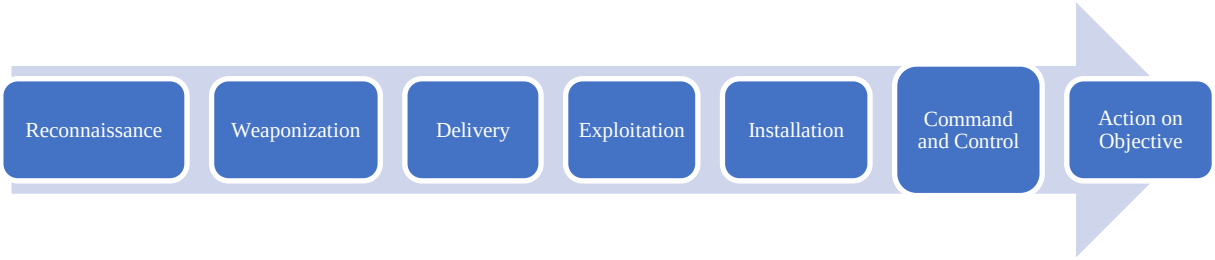


Figure 9: Cyber Kill Chain

To analyse threat information and subsequently map out adversary TTPs, we used MITRE's ATT&CK Framework tool, a collection of knowledge regarding adversary tactics, techniques and procedures, to model a specific threat (MITRE ATT&CK, n.d.).

The first step is to develop an organisational threat profile by reviewing the current threat landscape, understanding the motivation, methods and historical targeting of the actor and previous incidents. The final review will show the defenders which actors are posing the greatest and most likely threats (FireEye, 2020).

In our case, we will analyse specific Cyber Threats, also known as "Iranian threat actors".

FireEye company tracked the threat groups APT33, APT34, APT35, APT39, TEMP.Zagros (MuddyWater) and Temp.Omega, then combined those groups into one heat map, as shown in Fig.10. TTPs are colour-coded on a scale of 1 to 6, with "1" meaning this TTP (corresponding to the lightest shade of red) is used by one tracked threat group and "6" (bright red) meaning this TTP is used by 6 tracked groups. Combined TTPs will allow the defenders to identify higher priorities during threat hunts (Miazi et al. ,2017).

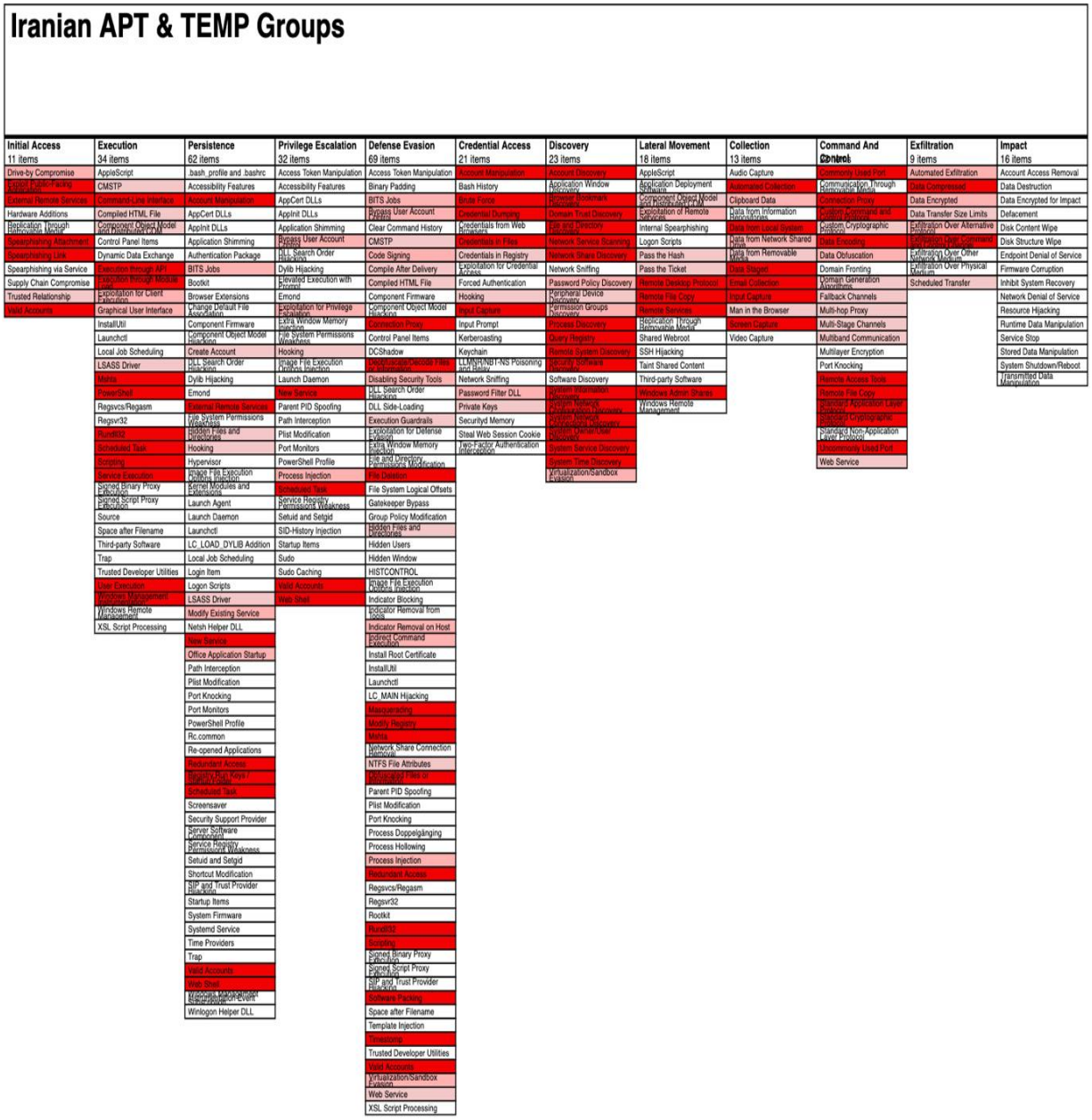


Figure 10: The APT & TEMP Group (FireEye, 2020).

Defenders such as Blue Team will compare the security controls that are in place while simultaneously mapping them to the MITRE Framework. This will help them to see the gaps in detection and mitigation.

By investigating the TTPs of the Threat Actors with the gaps of their security controls, the defenders can identify the vulnerability that the attacker is likely to target. Such knowledge provides the defenders with an opportunity to prioritise and hunt those attacks (Anomali, n.d.).

As shown in Fig.11, six threat groups have been mapped out against mitigations and detections to form an organisational heat map. Items in RED indicate a known adversary TTP for which the organisation lacks either mitigation and/or detection measures. Green indicates a TTP for which both mitigations and detections exist (Miazi et al. ,2017).

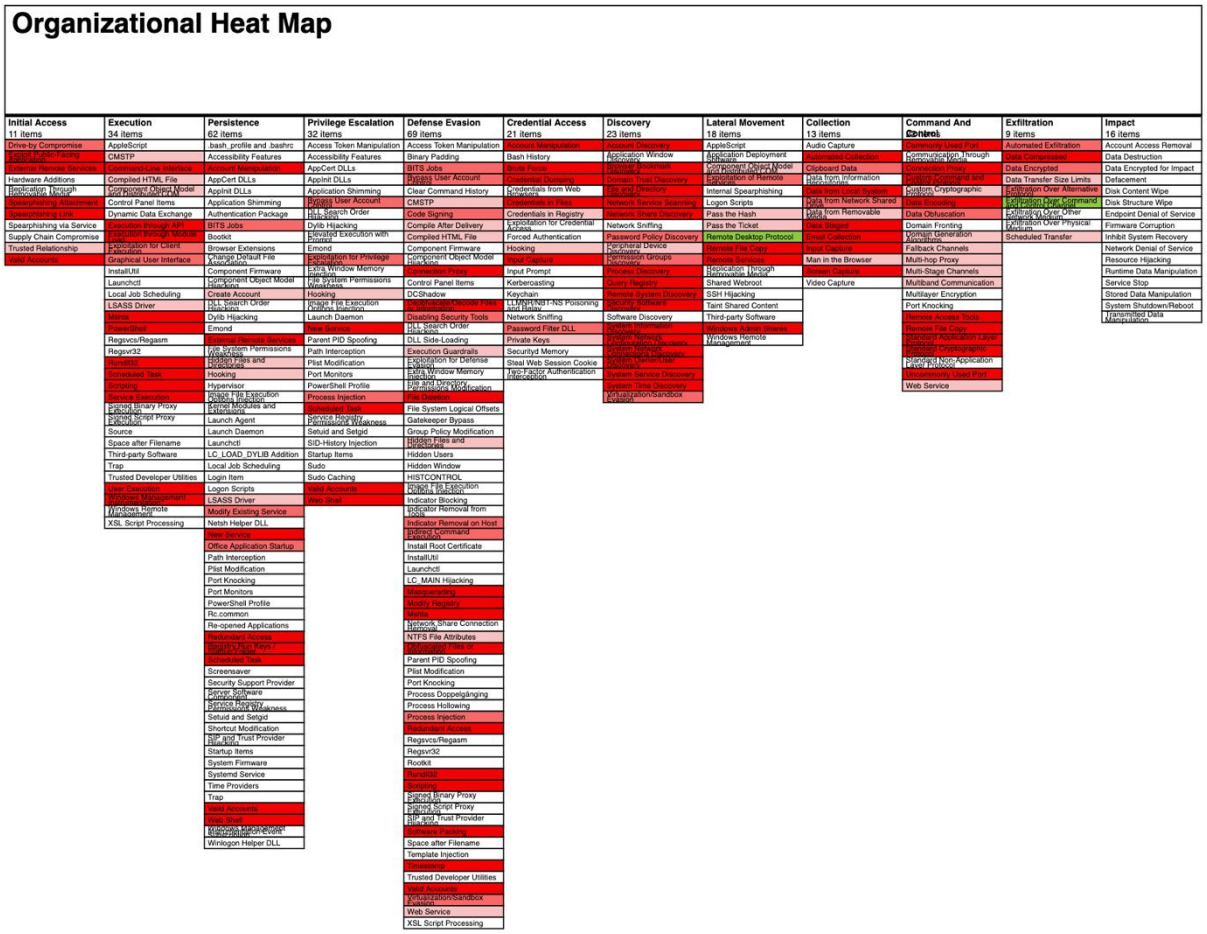


Figure 11: Organizational Heat Map (FireEye, 2020).

3.3. CTI Integration with SOC tools: Suricata Network IDS/IPS and Wazuh HIDS

In order to ingest the threat intelligence collected from the different source feeds with the security controls Suricata IDS/IPS and Wazuh HIDS *and* detect the emerging attacks, we will export threat information that has the IDS flag in MISP platform. Furthermore, we will integrate it with Suricata IDS/IPS by using curl to download all Suricata rules that are available in our instance and store it in a file format (.rules) in etc/suricata/MISPrules folder by the given misp file name, see Fig.12.

```
sam@ubuntu:~$ sudo curl -o /etc/suricata/MISPrules/misp.rules --insecure --header "Authorization:
 oNbCqpBcucD7M2t90GvaN5m9gYIn7a2TJkTlqKce" --header "Accept: application/json" --header "Content-
Type: application/json" https://192.168.227.129/events/nids/suricata/download
[sudo] password for sam:
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 55.1M  100 55.1M    0     0   289k      0  0:03:14  0:03:14 --:--:-- 16.8M
sam@ubuntu:~$
```

Figure 12: MISP Export Suricata Rules

After downloading the threat intelligence, we will feed it to the Suricata IDS/IPS to detect or prevent threats in real-time. As a result, this will load and enable the default Suricata rules within our threat intelligence news feed and test it if it is working properly. We will use suricata-update command to update the rules, see Fig.13.

Sudo suricata-update --local '/etc/suricata/MISPrules/misp.rules'

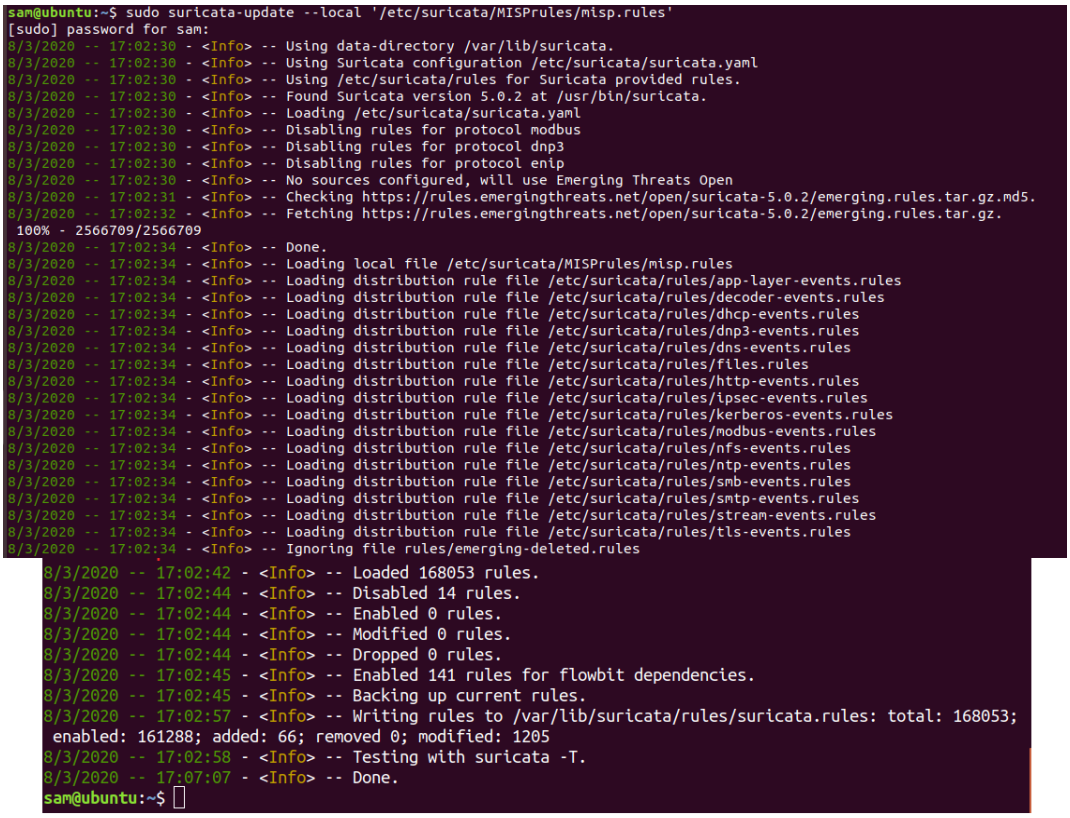


Figure 13: Updating Suricata Rules

To detect threats using this threat intelligence, we will run Suricata IDS/IPS to capture and match the traffic against the rules given. **sudo systemctl restart suricata.**

Wazuh was also utilised to monitor the system as a host intrusion detection and document the behaviour of the adversaries. First, Wazuh server manager and Wazuh agent were installed to analyse and detect intrusions, then the Wazuh agent sent the logs from the hosts. For more information about the installation and other dependencies, see Wazuh Documentation (WAZUH, 2020).

To register an agent, use the command line or later Elastic Stack. The agent key information must also be obtained from the Wazuh sever manager; this is an ID that authenticates the host, as shown in Fig. 14.

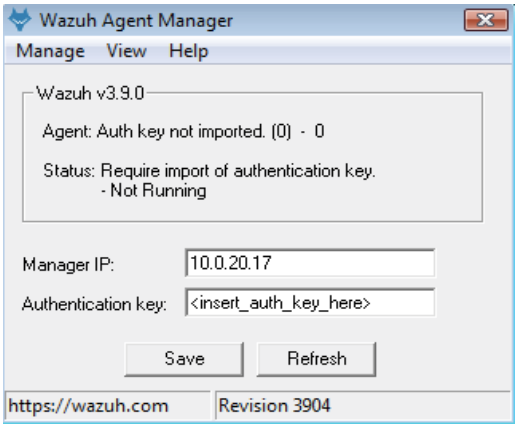


Figure 14: Wazuh Agent

One of the most useful capabilities of Wazuh is Virus Total integration, which we can scan the files if malicious content is present. Virus Total aggregates multiple antivirus products along with an online scanning engine. For more information on the integration Virus Total and the other capabilities of Wazuh, see Wazuh Documentation (WAZUH, 2020).

Finally, in order to obtain a detailed log from the Windows Operating System we will use the System Monitor (Sysmon) which stores logs about process creations, network connections and changes to file creation time (Mark Russinovich & Thomas Garnier, n.d.). To monitor, detect and analyse the TTPs of adversaries, it is necessary to install Sysmon and configure it with Swift On Security configuration. Wazuh agent and manager must also be configured (SwiftOnSecurity, 2020) (Brian Laskowski, n.d.).

3.4. Real Time Monitoring with Elastic Stack SIEM

In order to monitor all alerts generated from Suricata NIDS and Wazuh HIDS, an Elastic Stack server will be installed in the monitoring server as we are using single host architecture. Elastic Stack has been mentioned has already been described in this paper; for more information about the installation, configuration and integrating with IDS 'see Elastic Stack Documentation and Wazuh Documentation (WAZUH, 2020) (Beats: Data Shippers for Elasticsearch | Elastic, n.d.) (Logstash: Collect, Parse, Transform Logs| Elastic, n.d.) ("Elasticsearch," n.d.) (Kibana: Explore, Visualize, Discover Data | Elastic, n.d.).

After installing and configuring Elastic Stack, we are able to analyse and visualise the alerts from Suricata IDS/IPS and Wazuh HIDS using http://localhost:5601 . In order to view the agent, we are monitoring, using Wazuh HIDS, see Fig.15. To view the logs from Wazuh HIDS, see Fig.16 and to view logs from Suricata IDS/IPS, see Fig.17.

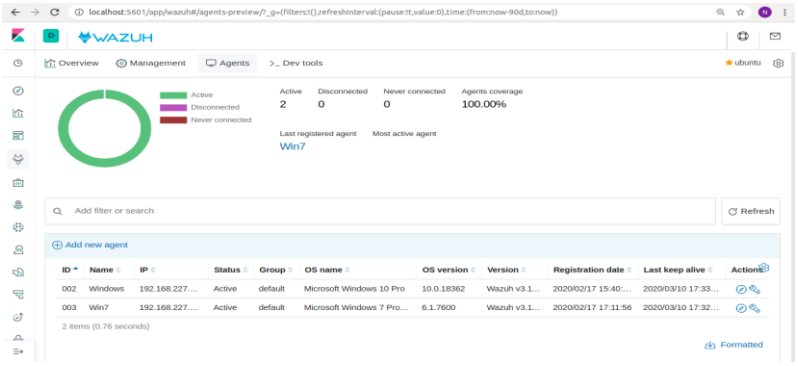


Figure 15: Registered Agents

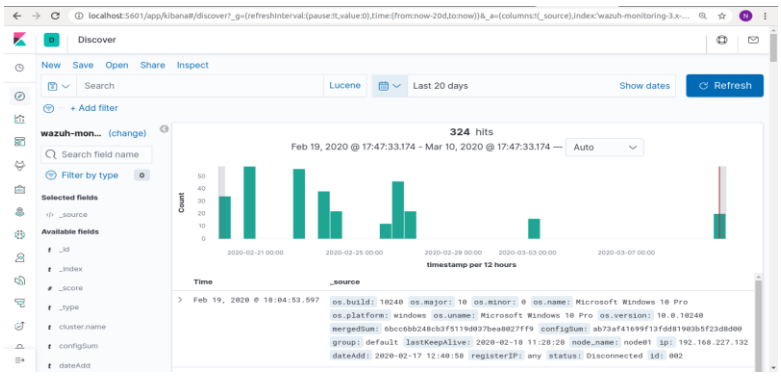


Figure 16: Wazuh HIDS Logs

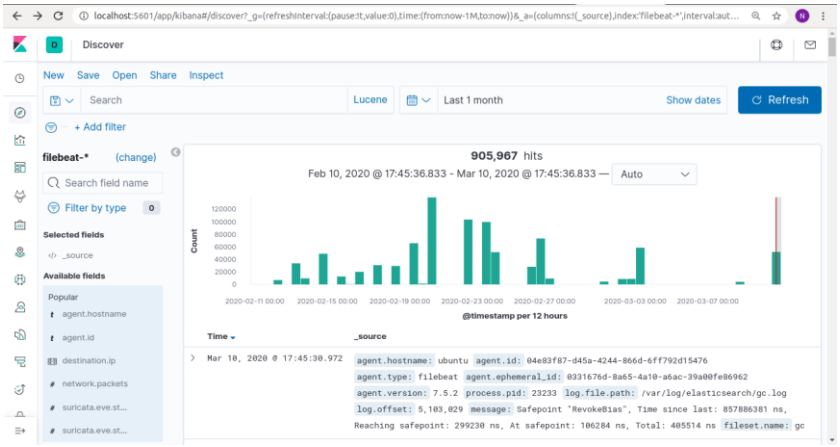


Figure 17: Suricata IDS/IPS Logs

4 Results and Discussions

This section will analyse the implementation of the proposed approach and the simulation scenario by firstly reviewing the current threat landscape in relation to the threat profile of the organisation. Furthermore, we will also focus on testing and measuring the effectiveness of our approach using Atomic Red Team library (developed by Red Canary) with some IoC's samples (Red Canary, n.d.). There will also be a discussion of the results from different perspectives, including the scope of an information source, actionability, detection capability and the integration of the CTI into defence tools.

In terms of the test environment, we utilized hardware with the following specifications: two servers equipped with Intel Core i7 CPUs and 16GB of RAM, accompanied by two network switches and four network cables. Each server was outfitted with a 512GB SSD storage drive and operated on Ubuntu Server. Additionally, we utilized VirtualBox, alongside other necessary virtualization software, to ensure a smooth and comprehensive testing experience.

4.1. Reviewing Threat Landscape to Identify the Adversaries

In order to test this approach, we will select the IoC's and TTPs of threat actor related to the threat profile of the organisation by reviewing the current threat landscape. The purpose of this selection is to detect attacks from this threat actor using known IoCs and TTPs.

Accordingly, the test will use the Muddy Water threat actor; one of the the APT groups that targets government agencies and companies in several countries, including the of Saudi Arabia, United Arab Emirates, Georgia, India, Israel, Pakistan, Turkey and USA (TOK & CELİKTAS, 2019). Muddy Water has been active since 2017, using macro malware to attack their targets. Additionally, they recently deployed an advanced attack vector to target governmental entities and the telecommunication sector (Clear Sky Cybersecurity, 2019).

4.2. Threat Hunting using IoC's

Detecting Muddy Water Threat Actor

Threat intelligence collected from MISP Platform consists of information from many feeds that may not be relevant in some cases. However, some of the threat intelligence *is* relevant to our test case, such as Event ID_398 in MISP Platform OSINT feed, which is related to Muddy Water, as shown in Fig.18.

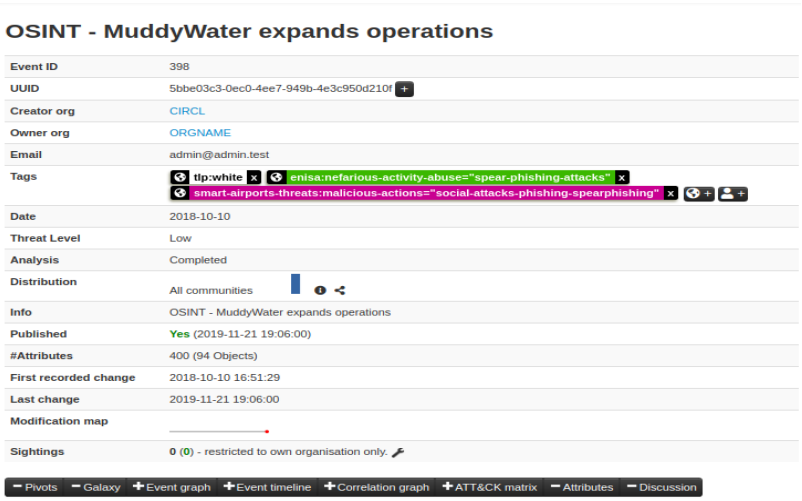


Figure 18: OSINT – Muddy Water Expands Operations

As seen in the attributes field in Fig.18, the event stores all known indicators that are related to this threat actor group (Table.1).

Table 1: Summary of the Categories of Event ID_398

Number of Indicators of Compromise	Types
400	IPs, Domains, URLs, Filenames, hashes

The first test will use the Muddy Water IoCs exported from MISP platform. They are flagged as network signatures and fed to Suricata IDS/IPS to detect traffic that matches those rules. After being tested to connect one of the commands and controls (c2) of this threat actor, an alert will be triggered such as the Suricata alert, shown in Fig.19.

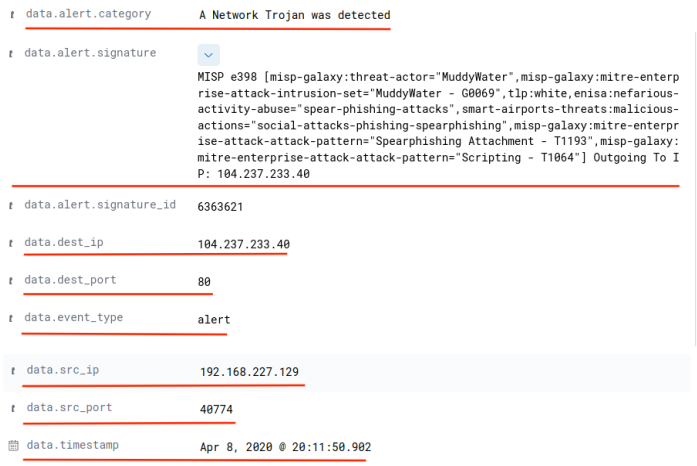


Figure 19: Suricata Alert

Moreover, this triggered alert describes the detection of c2 communication related to the Muddy Water threat actor and all the information related to this incident. Such information includes category, rule description, destination IP and port, event type and more about the effected host. This incident is detected by using the rule shown below in Fig.20, which will detect any outgoing traffic of a Muddy Water command and control (c2) IP which is IP: 104.237.233.40. The same method was used to detect other c2 IP's such as 104.237.233.60.

```
alert tcp any any -> any any (msg: "ATTACK [PTsecurity] CoronaBlue/SMBGhost DOS/RCE Attempt (CVE-2020-0796)"; flow: established; content: "|FC|SMB"; depth: 8; byte_test: 4, >, 0x800134, 8, relative, little; reference: url, www.mcafee.com/blogs/other-blogs/mcafee-labs/smbghost-analysis-of-cve-2020-0796; reference: cve, 2020-0796; reference: url, github.com/ptresearch/AttackDetection; metadata: Open Ptsecurity.com ruleset; classtype: attempted-admin; sid: 10005777; rev: 2;)

alert tcp any any -> any any (msg: "ATTACK [PTsecurity] CoronaBlue/SMBGhost DOS/RCE Attempt (CVE-2020-0796)"; flow: established; content: "|FC|SMB"; depth: 8; byte_test: 4, >, 0x800134, 0, relative, little; reference: url, www.mcafee.com/blogs/other-blogs/mcafee-labs/smbghost-analysis-of-cve-2020-0796; reference: cve, 2020-0796; reference: url, github.com/ptresearch/AttackDetection; metadata: Open Ptsecurity.com ruleset; classtype: attempted-admin; sid: 10005778; rev: 2;
```

Figure 20: The Triggered Alert

In addition, the rule detailed in Fig.20 gives the relevant alert information that is needed when investigating the triggered rule, such as MISP event id, the threat actor using this c2 and a reference link to search more information.

Detecting Emerging Cyberattacks

At the beginning of March 2020, emerging cyberattacks appeared that targeted unpatched CVE-2020-0796, also known as SMB Ghost or Corona Blue; a remote code execution that exists in Microsoft Server Message Block 3.1.1 (SMBv3). Microsoft suggested disabling SMBv3 to block this vulnerability (Microsoft, 2020) in order to mitigate this emerging attack without blocking SMBv3. We use Suricata PT Open Ruleset shared within the MISP community platform from Positive Technologies Security (PT Security), as shown in Fig. 21 (AttackDetection, n.d.).

```
alert ip $HOME_NET any -> 104.237.233.40 any (msg: "MISP e398 [misp-galaxy:threat-actor="MuddyWater",misp-galaxy:mitre-enterprise-attack-intrusion-set="MuddyWater - G0069",tlp:white,enisa:nefarious-activity-abuse="spear-phishing-attacks",smart-airports-threats:malicious-actions="social-attacks-phishing-spearphishing",misp-galaxy:mitre-enterprise-attack-attack-pattern="Spearphishing Attachment - T1193",misp-galaxy:mitre-enterprise-attack-attack-pattern="Scripting - T1064"] Outgoing To IP: 104.237.233.40";  classtype:trojan-activity; sid:6363621; rev:1; priority:3; reference:url,http://192.168.227.129/events/view/398;
```

Figure 21: CVE-2020-0796 Mitigation Rule

Using the rules in Fig.21, government agencies and organisations can mitigate cyberattacks using this vulnerability. This renders the organisation safe without disabling the functionality of SMBv3.

Another example of detecting an emerging cyber threat is the detection of cybercriminals that are using Covid-19 pandemic to exploit their targets. Cybercriminals are using COVID-19 as bait, in combination with spam and spear phishing campaigns, to increase the likelihood of a successful attack. Advanced Persistent Threat (APT) groups targeted China first and the cyberattacks spread in a similar manner to the virus itself (Krebs, 2020).

The Coronavirus has lead to a collaborative effort on the part of thousands of security professionals who have sought to tackle cybercriminals who seek to use this crisis for financial gain by volunteering their expertise. There have been a multitude of these potentially life-saving partnerships protecting

hospitals and taking down COVID-themed scam websites. (Malwarebytes, 2020). Major groups like the COVID-19 Cyber Threat Coalition (CTC) are working to protect against the latest cyber scams. This group consists of approximately 3,000 security professionals who are collecting, vetting and sharing new intelligence on cyber threats (CTC, 2020).

The shared threat information was fed to the defence tools IoC's related to Covid-19 cyber threats and tested in order to determine whether it was detecting those emerging cyberattacks.

As shown in Fig.22, Suricata IDS/IPS gave an alert that one of the organisation hosts accessed a domain that pretends to buy corona virus test kits.

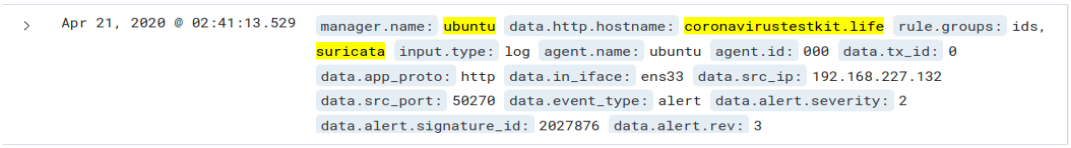


Figure 22: Alert Covid-19 Cyber Threats

Detailed information about the alert and the compromised host can be seen in Fig.23, while information about the detected domain from Virus Total and other tools detected this domain is contained in Fig.24.

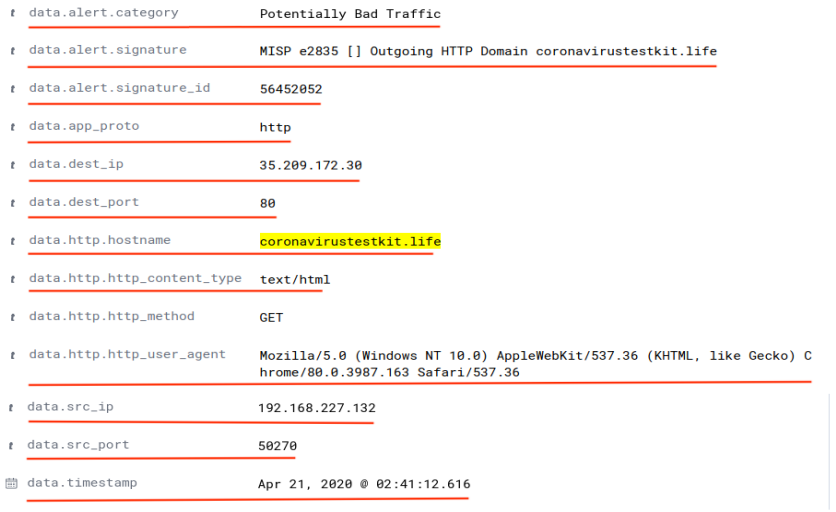


Figure 23: Detailed Information about the Alert

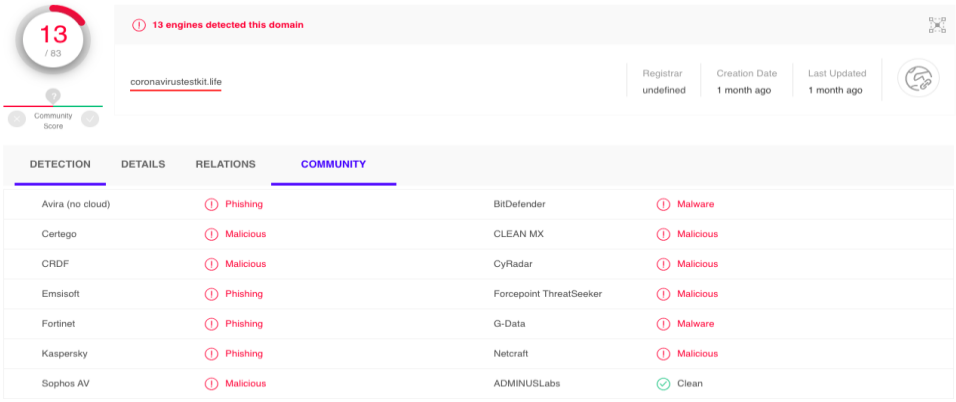
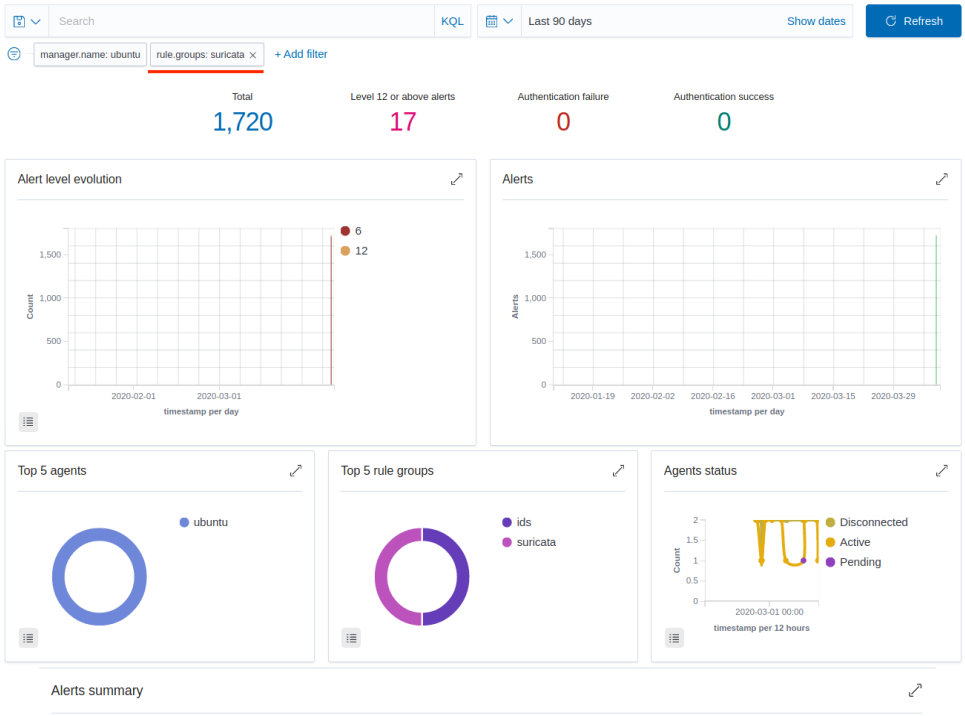


Figure 24: Virus Total Detection of this Domain

The summary of the test that used the IoCs of Muddy Water threat actor and searched for emerging cyberattacks matched or detected 17 critical incidents. In Fig.25, a Suricata Alerts Summary, the box highlighted in red shows the threat detected by Suricata IDS/IPS.



Alerts summary

Rule ID	Description	Level	Count
86600	Suricata messages.	6	1,703
86601	Suricata: Alert - MISP e398 [misp-galaxy:threat-actor="MuddyWater",misp-galaxy:mitre-enterprise-attack-intrusion-set="MuddyWater - G0069",tlp:white,enisa:nefarious-activity-abuse="spear-phishing-attacks",smart-airports-threats:malicious-actions="social-attacks-phishing-spearphishing",misp-galaxy:mitre-enterprise-attack-attack-pattern="Spearphishing Attachment - T1193",misp-galaxy:mitre-enterprise-attack-attack-pattern="Scripting - T1064"] Outgoing To IP: 104.237.233.40	12	4
86601	Suricata: Alert - ET INFO Observed DNS Query to .cloud TLD	12	3
86601	Suricata: Alert - MISP e2416 [tlp:white,source:DigitalSide.IT,source:urlhaus.abuse.ch,type:OSINT] Domain raw.githubusercontent.com	12	2

Figure 25: Suricata Alerts Summary

4.3. Threat Hunting using TTPs of Muddy Water Threat Actor

Using only network artefacts to detect advanced persistent threat (APT) will not prevent sophisticated attacks. Indeed, many intrusions start from the endpoint or host machine, such as client-side attacks. In order to prevent such attacks, we use Wazuh HIDS to monitor activities like logs and PowerShell commands on the host machine.

In this second test, we used Atomic Red Team library to emulate the attack behaviour of a Muddy Water threat actor to test our endpoint detection capabilities. Atomic Red Team gives us the capability to emulate an attack against the security endpoint tools the same way the attackers do, by using their tactics and techniques (Red Canary, n.d.). This information, related to the Muddy Water threat, was extracted by MITRE ATT&CK; see Table 2 (MITRE ATT&CK, n.d.).

Table 2: Techniques of Muddy Water Threat Actor

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
T1193 - Spearphishing Attachment	T1191 - CMSTP	T1060 - Registry Run Keys / Startup Folder	T1088 - Bypass User Account Control	T1088 - Bypass User Account Control	T1003 - Credential Dumping	T1083 - File and Directory Discovery	T1175 - Component Object Model and Distributed COM	Screen Capture	T1090 - Connection Proxy	T1002 - Data Compressed	
	T1059 - Command-Line Interface			T1191 - CMSTP	T1503 - Credentials from Web Browsers	T1057 - Process Discovery	T1105 - Remote File Copy		T1104 - Multi-Stage Channels		
	T1175 - Component Object Model and Distributed COM			T1500 - Compile After Delivery	T1081 - Credentials in Files	T1063 - Security Software Discovery			T1105 - Remote File Copy		
	T1173 - Dynamic Data Exchange			T1090 - Connection Proxy		T1082 - System Information Discovery					
	T1170 - Mshta			T1140 - Deobfuscate/ Decode Files or Information		T1016 - System Network Configuration Discovery					
	T1086 - PowerShell			T1036 - Masquerading		T1033 - System Owner/User Discovery					
	T1085 - Rundll32			T1170 - Mshta							
	T1064 - Scripting			T1027 - Obfuscated Files or Information							
	T1204 - User Execution			T1085 - Rundll32							
	T1047 - Windows Management Instrumentation			T1064 - Scripting							

Using Atomic Red Team Emulation, we will imitate the 31 techniques used by the Muddy Water threat actor, using PowerShell to see if our Wazuh HIDS is detects these them. Fig.26. is one such example of the test T1033. Notice how it describes the way in which the Muddy Water threat actor uses a malware that can collect the username of the victim.

```
PS C:\atomicredteam> Invoke-AtomicTest T1033 -ShowDetails
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

[********BEGIN TEST*******]
Technique: System Owner/User Discovery T1033
Atomic Test Name: System Owner/User Discovery
Atomic Test Number: 1
Description: Identify System owner or users on an endpoint.

Upon successful execution, cmd.exe will spawn multiple commands against a target host to identify usernames. Output will be v
ia stdout.
Additionally, two files will be written to disk - computers.txt and usernames.txt.
Attack Commands:
Executor: command_prompt
ElevationRequired: False
Command:
cmd.exe /C whoami
wmic useraccount get /ALL
quser /SERVER:"#{computer_name}"
qwinsta
qwinsta.exe" /server:#{computer_name}
qwinsta.exe
for /F "tokens=1,2" %i in ('qwinsta /server:#{computer_name} ^| findstr "Active Disc"') do @echo %i | find /v "#" | find /v "
console" || echo %j > usernames.txt
@FOR /F %n in (computers.txt) DO @FOR /F "tokens=1,2" %i in ('qwinsta /server:%n ^| findstr "Active Disc"') do @echo %i | fin
d /v "#" | find /v "console" || echo %j > usernames.txt
Command (with inputs):
cmd.exe /C whoami
wmic useraccount get /ALL
quser /SERVER:"localhost"
qwinsta
qwinsta.exe" /server:localhost
qwinsta.exe
for /F "tokens=1,2" %i in ('qwinsta /server:localhost ^| findstr "Active Disc"') do @echo %i | find /v "#" | find /v "console
" || echo %j > usernames.txt
@FOR /F %n in (computers.txt) DO @FOR /F "tokens=1,2" %i in ('qwinsta /server:%n ^| findstr "Active Disc"') do @echo %i | fin
d /v "#" | find /v "console" || echo %j > usernames.txt
[!!!!!!!!END TEST!!!!!!!]
```


Figure 26: Atomic Test T1033 (System Owner/ User Discovery)

The above test of the T1033 technique triggered an alert, as shown in Fig.27, which reveals that Wazuh detected an attacker trying to discover the current active user by executing a whoami command using PowerShell.

> Apr 8, 2020 @ 16:11:56.175 manager.name: ubuntu rule.groups: execution, MITRE, attack.t1033
> input.type: log agent.ip: 192.168.227.132 agent.name: Windows
> agent.id: 004 data.win.eventdata.originalFileName: whoami.exe
> data.win.eventdata.image: C:\\Windows\\System32\\whoami.exe
> data.win.eventdata.product: Microsoft® Windows® Operating System

Figure 27: Alert T1033 (System Owner/ User Discovery)

More information about the details of the above detected technique T1033 incident can be seen in Fig.28.

t input.type	log
t manager.name	ubuntu
t rule.description	Whoami ran as SYSTEM user, potential user recon after privelge escalation
t rule.groups	execution, MITRE, attack.t1033
# rule.level	12
timestamp	Apr 8, 2020 @ 16:11:56.175
t data.win.eventdata.user	DESKTOP-184F6CP\\cadeg
t data.win.system.channel	Microsoft-Windows-Sysmon/Operational
t data.win.system.computer	DESKTOP-184F6CP
t agent.id	004
t agent.ip	192.168.227.132
t agent.name	Windows
t data.win.eventdata.commandLine	\"C:\\WINDOWS\\system32\\whoami.exe\"
t data.win.eventdata.currentDirectory	C:\\atomicredteam\\
t data.win.eventdata.description	whoami - displays logged on user information
t data.win.eventdata.fileVersion	10.0.18362.1 (WinBuild.160101.0800)
t data.win.eventdata.hashes	SHA1=11E59C45DAB4B2B65884F043DB738D39574AAFBA,MD5=311EFED1B6336ED8DC5471FE58C88CB5,SHA256=AA1583D770C6774F8D8FCEC099CF7BDC05BEB0F08F6DB387F5B37CCA860771D7,IMPHASH=E91037BB26500603D5EE8666BA6C2510
t data.win.eventdata.image	C:\\Windows\\System32\\whoami.exe
t data.win.eventdata.originalFileName	whoami.exe
t data.win.eventdata.parentCommandLine	\"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe\"
t data.win.eventdata.parentImage	C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe
t data.win.eventdata.ruleName	technique_id=T1033,technique_name=System Owner/User Discovery

Figure 28: Detailed Incident T1033

The summary of the test which used TTPs of the Muddy Water threat actor matched or detected 121 critical incidents, as shown in Fig.29.

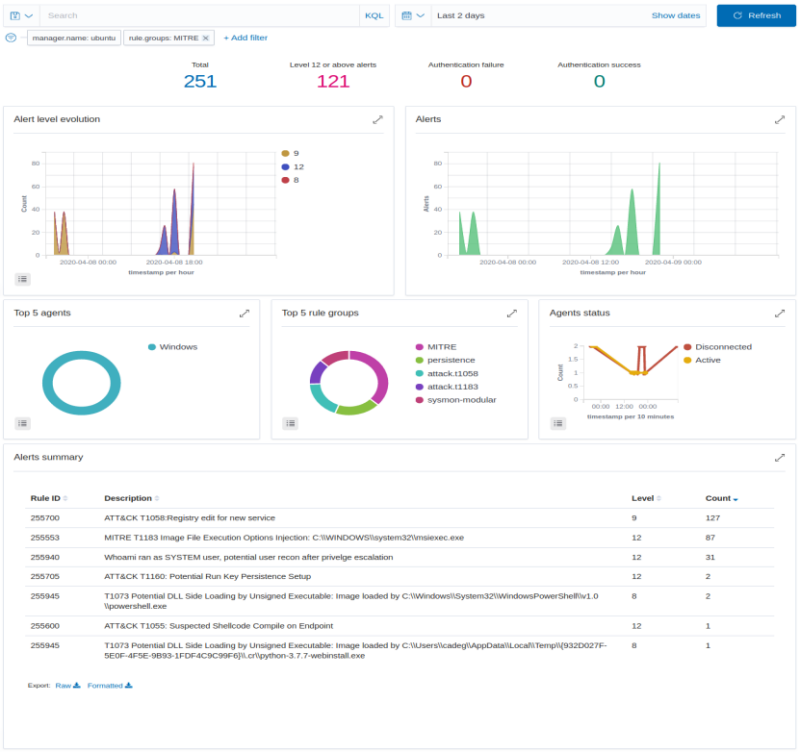


Figure 29: Wazuh HIDS TTPs Alerts Summary

The above alert summary section provides the techniques that enable effective prioritisation during the hunting of the Muddy Water threat actor. For example, MITRE Technique T1058, “Service Registry Permissions Weakness,” is the most observed technique from the emulated attack. MITRE’s T1058 is part of persistence and privilege escalation tactic and the attacker used this technique to accomplish their objective.

4.4. Findings and Insights

The threat intelligence we gathered from OSINT feeds has improved our cybersecurity defence strategy, enabling it to detect emerging cyberattacks and focus on the threat actors that pose a danger to our government agencies and organisations.

The MISP default feed consists of many international contributors that share valuable information in the OSINT community. Consequentially, the scope of the shared threat information in the community may not be relevant to us, but many of those indicators or the threat actors behind those attacks appeared in many countries, including Muddy Water and many other threat actors, which makes them relevant to us.

Both tests conducted have proved the efficiency of the proposed approach. The first one, which uses known indicators to detect the Muddy Water threat actor, detected all tests executed, as shown in section 4.3. The second test has highlighted the utility of using many types of security tools alongside the those that are already used. Indeed, by using threat actors TTPs, Suricata IDS/IPS was not able to detect the related intrusion activities and adversary behaviours but by combining with the Wazuh HIDS capabilities, the detection of theses malicious behaviours - based on the TTPs used - becomes effective. The results of both tests were illustrated in Fig. 30.

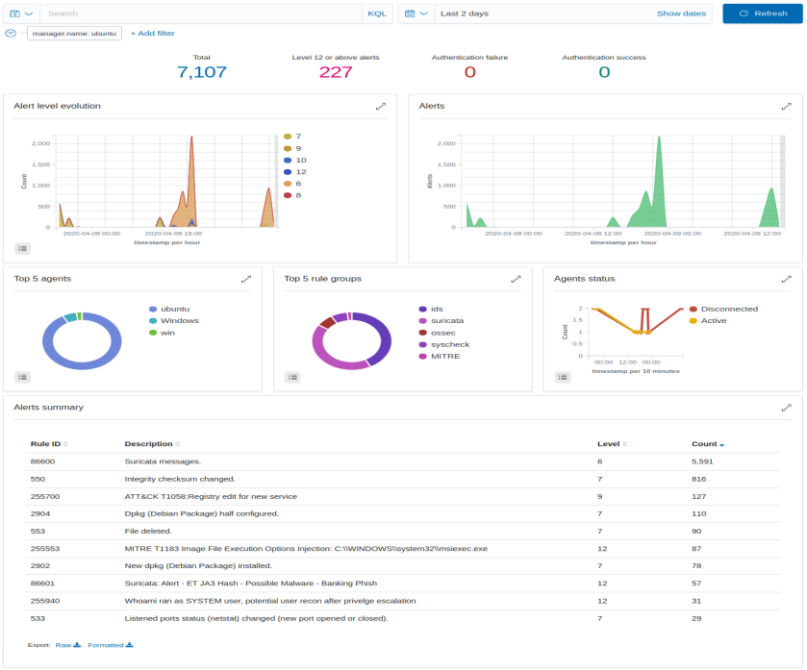


Figure 30: Summary of all Alerts

Comparing the detection of previous and current architecture, according to their design and the test, displays that traditional cyber defence architecture is not enough to prevent the current sophisticated cyberattacks; but the proposed architecture, as the result showed, can detect emerging cyberattacks using

cyber threat intelligence and determine whether the attacker bypassed NIDS by monitoring the TTPs of said adversary.

Fig.31, Proposed Approach Detection Heat Map, displays the scores of current visibility and detection coverage of the proposed approach measured against the techniques used by Muddy Water threat actor in the form of a heat map. The lightest shade of green indicates the strength of the visibility and detection coverage of the proposed approach, based on this actor, and the bright green colour indicates where the approach is not enough or weak according to the visibility and detection rules. The blue colour shows that the event is logged but the approach do not have a detection in place. Table 3 presents the input rules of the detection.

Table.3: The Input Rules of the Detection

Detection	Input Network Rules Used	Input Host Rules Used
Traditional Cyber Defense Architecture	Default Signature Rules.	Default Signature Rules.
New Proposed Architecture	Default Signature Rules with updated threat intelligence feeds from community.	Default Signature Rules with monitoring the TTPs of the criminals and using System Monitoring (Sysmon) tool to cover wide range of system and security logs.

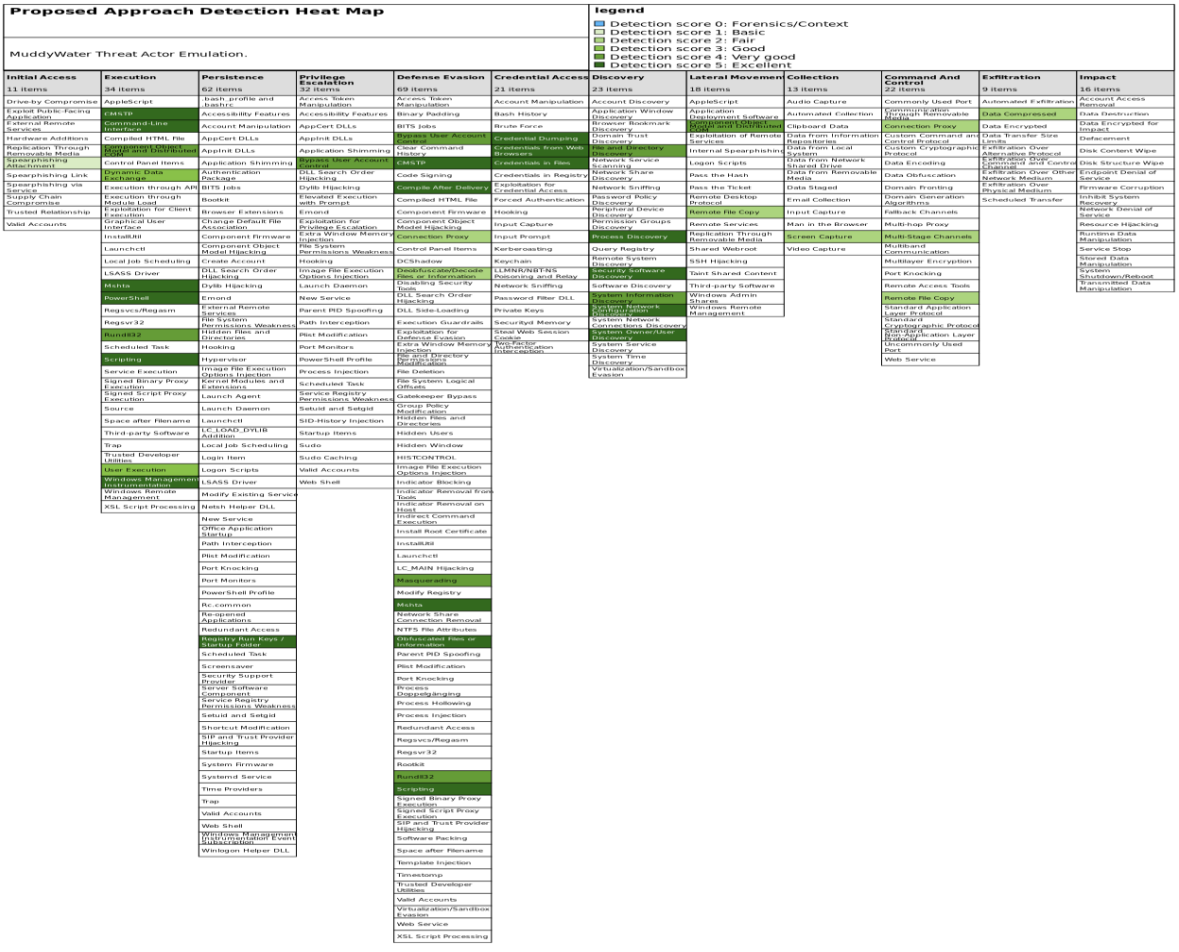


Figure 31: Proposed Approach Detection Heat Map

Finally, it is extremely necessary to highlight that the integration between threat intelligence and IDS tools needs deep configuration knowledge and many tests to ensure its proper detection or the match of data traffic against the rules given to detect attacks.

In summary, the results of the tests conducted show that CTI has improved and reinforced the cybersecurity defence strategy by adding another defensive layer. This will be used by the defenders to detect and prevent emerging cyberattacks and actors that are a threat to th organisation. Table 4 summarises the points discussed.

Table 4: Summary of Result Discussion

Key Points	**Using IoCs**	**Using TTPs**
Scope of an Information	Different Collection, some irrelevant.	Relevant.
Actionability	Actionable, ex. CVE-2020-0796 and Covid-19 themed cyberattack campaigns.	Actionable
Detection Capability	Detected know IoCs of Muddy Water and Covid-19 malicious domains.	All Detected
Integration of CTI	Need Hard Configuration.	Need Hard Configuration.

5 Conclusion

Threat hunting is a domain where organisations seek to proceed with a proactive defence mechanism by chasing the digital ‘fingerprints ’of the trending threats. After presenting the most important studies in this domain, we have proposed a way in which to shift from a conventional cybersecurity mechanism to an intelligent landscape. From a technical perspective, tests were conducted using the relevant threat information and known techniques of the Muddy Water threat actor. The first test was conducted using the IoC’s of the Muddy Water threat actor and emerging cyberattacks such as the Covid-19-themed campaigns that are targeting victims worldwide while the second test used the TTPs of the Muddy Water threat actor. Finally, we discussed the result obtained by the test through the evaluation of the collected and deployed threat information with the detection results. The use of Covid-19-themed campaigns by Muddy Water highlights the need for organizations to be vigilant and proactive in their defense against emerging threats, as attackers are constantly adapting and evolving their tactics. Overall, as key findings from the research conducted in this paper, the proposed approach of using threat intelligence combined with advanced cybersecurity mechanisms can help organizations stay ahead of emerging threats and respond more effectively to attacks. By conducting tests using threat information and techniques of known threat actors like Muddy Water, we were able to assess the effectiveness of our approach in detecting and responding to attacks. The use of IoCs and TTPs in our tests allowed us to identify potential attacks and proactively defend against them, rather than simply reacting after an attack has already occurred. The results of our tests demonstrate that by leveraging threat intelligence and advanced cybersecurity mechanisms, organizations can significantly improve their ability to detect and respond to emerging threats in a timely and effective manner.

References

[1] Abu, M.S., Selamat, S.R., Ariffin, A., & Yusof, R. (2018). Cyber threat intelligence–issue and challenges. *Indonesian Journal of Electrical Engineering and Computer Science*, *10*(1), 371-379.

[2] Al-Taleb, N., Saqib, N.A., & Dash, S. (2020). Cyber threat intelligence for secure smart city.

[3] Anomali. (n.d.). What Is MITRE ATT&CK and How Is It Useful. Available at: https://www.anomali.com/resources/what-mitre-attck-is-and-how-it-is-useful.

[4] Attack Detection. (n.d.). Attack Detection CVE-2020-079: https://github.com/ptresearch/Attack Detection/blob/master/CVE-2020-0796/cve-2020-0796.rules.

[5] Asiri, M., Saxena, N., Gjomemo, R., & Burnap, P. (2023). Understanding indicators of compromise against cyber-attacks in industrial control systems: a security perspective. *ACM transactions on cyber-physical systems*.

[6] Bahrami, P.N., Dehghantanha, A., Dargahi, T., Parizi, R.M., Choo, K.K.R., & Javadi, H.H. (2019). Cyber kill chain-based taxonomy of advanced persistent threat actors: Analogy of tactics, techniques, and procedures. *Journal of information processing systems*, *15*(4), 865-889.

[7] Beats: Data Shippers for Elasticsearch | Elastic Stack. (n.d.). Beats. Retrieved January 4, 2020, from https://www.elastic.co/beats

[8] Berndt, A., & Ophoff, J. (2020). Exploring the value of a cyber threat intelligence function in an organization. In *Information Security Education. Information Security in Action: 13th IFIP WG 11.8 World Conference, WISE 13, Maribor, Slovenia, Proceedings 13*, 96-109. Springer International Publishing.

[9] Brown, R., & Lee, R.M. (2019). The evolution of cyber threat intelligence (cti): 2019 sans cti survey. SANS Institute, 1-16.

[10] CERT-SOC. (n.d.). CERT-SOC TELCO NETWORK. Retrieved November 20, 2019, from https://www.etis.org/page/CERT_SOC.

[11] Clear Sky Cybersecurity. (2019). Iranian APT group 'Muddy Water' Adds Exploits to Their Arsenal: https://www.clearskysec.com/wpcontent/uploads/2019/06/Clearsky-Iranian-APT-group-%E2%80%98MuddyWater%E2%80%99-Adds-Exploits-to-Their-Arsenal.pdf.

[12] Crowdstrike. (2020). Crowdstrike 2020 Global Threat Report [PDF]. https://g o.crowdstrike.com/rs/281-OBQ266/images/Report2020CrowdStrikeGlobalThreatRe port.pdf.

[13] CTC. (n.d.). COVID-19 Cyber Threat Coalition. Retrieved April 27, 2020, from https://www.cyberthreatcoalition.org/

[14] Cybersecurity Ventures. (2019). 2019 Official Annual Cybercrime Report [PDF]. Retrieved from https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf. Accessed 15 march 2020

[15] Elasticsearch: The Official Distributed Search & Analytics Engine | Elastic. (n.d.). Elastic. Retrieved January 4, 2020 from https://www.elastic.co/elasticsearch

[16] FireEye. (2020). Operationalizing CTI: Using MITRE ATT&CK to Hunt for and Defend Against Iranian Cyber Threats [Online]. Available at: https://www.fireeye.com/blog/products-and-services/2020/01/operationalizing-cti-huntfor-defend-against-iranian-cyber-threats.html.

[17] Gao, P., Shao, F., Liu, X., Xiao, X., Qin, Z., Xu, F., & Song, D. (2021). Enabling efficient cyber threat hunting with cyber threat intelligence. *In IEEE 37th International Conference on Data Engineering (ICDE)*, 193-204.

[18] Grisham, J., Samtani, S., Patton, M., & Chen, H. (2017). Identifying mobile malware and key threat actors in online hacker forums for proactive cyber threat intelligence. *In IEEE international conference on intelligence and security informatics (ISI)*, 13-18.

[19] Javeed, D., Khan, M.T., Ahmad, I., Iqbal, T., Badamasi, U.M., Ndubuisi, C.O., & Umar, A. (2020). An efficient approach of threat hunting using memory forensics. *International Journal of Computer Networks and Communications Security*, *8*(5), 37-45.

[20] Hyslip, T.S., & Burruss, G.W. (2023). Ransomware. In *Handbook on Crime and Technology*, 86-104. Edward Elgar Publishing.

[21] Kibana: Explore, Visualize, Discover Data | Elastic. (n.d.). Elastic. Retrieved January 6, 2020 from https://www.elastic.co/kibana (Beats: Data Shippers for Elasticsearch | Elastic, n.d.)

[22] Kotsias, J., Ahmad, A., & Scheepers, R. (2023). Adopting and integrating cyber-threat intelligence in a commercial organisation. *European Journal of Information Systems*, *32*(1), 35-51.

[23] Krebs, B. (2020). COVID-19 Has United Cybersecurity Experts, But Will That Unity Survive the Pandemic? https://krebsonsecurity.com/2020/04/covid-19-has-unitedcybersecurity-experts-but-will-that-unity-survive-the-pandemic/.

[24] Kure, H.I., Islam, S., & Mouratidis, H. (2022). An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. *Neural Computing and Applications*, *34*(18), 15241-15271.
[25] Laskowski, B. (n.d.). Wazuh Manager MITRE Rules. https://github.com/Hestat/ossec-sysmon/blob/master/local_rules.xml
[26] Liao, X., Yuan, K., Wang, X., Li, Z., Xing, L., & Beyah, R. (2016). Acing the ioc game: Toward automatic discovery and analysis of open-source cyber threat intelligence. *In Proceedings of the ACM SIGSAC conference on computer and communications security*, 755-766.
[27] Logstash: Collect, Parse, Transform Logs | Elastic. (n.d.). Elastic. Retrieved January 4, 2020 from https://www.elastic.co/logstash
[28] Lutf, M. (2018). Threat intelligence sharing: a survey. *Journal of Applied Science and Computations*, *8*(11), 1811-1815.
[29] Lacava, G., Marotta, A., Martinelli, F., Saracino, A., La Marra, A., Gil-Uriarte, E., & Vilches, V.M. (2021). Cybersecurity Issues in Robotics. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 12*(3), 1-28
[30] Malwarebytes. (2020). APTs and COVID-19: How advanced persistent threats use the coronavirus as a lure. https://resources.malwarebytes.com/files/2020/04/200407-MWB-COVID-White-Paper_Final.pdf. Accessed 27 April 2020.
[31] Marelli, M. (2022). The SolarWinds hack: Lessons for international humanitarian organizations. *International Review of the Red Cross*, *104*(919), 1267-1284.
[32] Russinovich, M., & Garnier, T. (2021). Sysmon v12. 03.
[33] Mavroeidis, V., & Bromander, S. (2017). Cyber threat intelligence model: an evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. *In IEEE European Intelligence and Security Informatics Conference (EISIC)*, 91-98.
[34] Miazi, M.N.S., Pritom, M.M.A., Shehab, M., Chu, B., & Wei, J. (2017). The design of cyber threat hunting games: A case study. *In IEEE 26th International Conference on Computer Communication and Networks (ICCCN)*, 1-6.
[35] Microsoft. (2020, March 18). CVE-2020-0796 | Windows SMBv3 Client/Server Remote Code Execution Vulnerability [Online]. Microsoft Security Response Center. Available at: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0796.
[36] Miller, T., Staves, A., Maesschalck, S., Sturdee, M., & Green, B. (2021). Looking back to look forward: Lessons learnt from cyber-attacks on industrial control systems. *International Journal of Critical Infrastructure Protection*, *35*, 1-21.
[37] Platform, M.O.S.T.I. (2020). Open standards for threat information sharing. *MISP project: caŭm.*
[38] MITRE ATT&CK. (n.d.). Muddy Water Group. https://attack.mitre.org/groups/G0069/
[39] Mohaisen, A., Al-Ibrahim, O., Kamhoua, C., Kwiat, K., & Njilla, L. (2017). Rethinking information sharing for actionable threat intelligence.
[40] Mutemwa, M., Mtsweni, J., & Mkhonto, N. (2017). Developing a cyber threat intelligence sharing platform for South African organisations. *In IEEE Conference on Information Communication Technology and Society (ICTAS)*, 1-6.
[41] Narayanan, S., Ganesan, A., Joshi, K., Oates, T., Joshi, A., & Finin, T. (2018). Cognitive techniques for early detection of cybersecurity events.
[42] Parmar, M., & Domingo, A. (2019). On the Use of Cyber Threat Intelligence (CTI) in Support of Developing the Commander's Understanding of the Adversary. *In MILCOM IEEE Military Communications Conference (MILCOM)*, 1-6.
[43] Qiang, L., Zhengwei, J., Zeming, Y., Baoxu, L., Xin, W., & Yunan, Z. (2018). A quality evaluation method of cyber threat intelligence in user perspective. *In 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering*, 269-276.

[44] Record Future. (2019). How to Automate System Hardening with Technical Threat Intelligence. https://www.recordedfuture.com/technical-threat-intelligence/.
[45] Red Canary. (n.d.). Getting Started Testing with Atomic Tests. https://atomicredteam.io/testing.
[46] Sadique, F., Cheung, S., Vakilinia, I., Badsha, S., & Sengupta, S. (2018). Automated structured threat information expression (stix) document generation with privacy preservation. *In 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, 847-853.
[47] Schlette, D., Böhm, F., Caselli, M., & Pernul, G. (2021). Measuring and visualizing cyber threat intelligence quality. *International Journal of Information Security*, *20*, 21-38.
[48] Shackleford, D. (2018). CTI In security operations: SANS 2018 cyber threat intelligence survey. *SANS Institute*.
[49] Shin, B., & Lowry, P.B. (2020). A review and theoretical explanation of the 'Cyberthreat-Intelligence (CTI) capability' that needs to be fostered in information security practitioners and how this can be accomplished. *Computers & Security*, *92*, 1-40.
[50] Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security*, *60*, 154-176.
[51] Swift On Security. (n.d.). Swift on Security Sysmon Configuration. Retrieved from https://github.com/SwiftOnSecurity/sysmon-config.
[52] TOK, M.S., & CELİKTAS, B. (2019). Muddy water apt group and a methodology proposal for macro malware analysis. *Bilişim Teknolojileri Dergisi*, *12*(3), 253-263.
[53] Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber-attacks. *Computers & security*, *72*, 212-233.
[54] Wagner, T. D., Mahbub, K., Palomar, E., & Abdallah, A. E. (2019). Cyber threat intelligence sharing: Survey and research directions. *Computers & Security*, *87*, 1-27.
[55] WAZUH. (2020). WAZUH Documentation. https://documentation.wazuh.com/3.11/index.html

Authors Biography

Dr. Meryem is an accomplished assistant professor in the College of Criminal Justice at Naif Arab University for Security Sciences, where she serves as the Director of the Partnerships and International Cooperation Department. With a Ph.D. in Computer Science from the University of Constantine, 2-Algeria, and a Master's degree in information technology science from the same university, Meryem has built an impressive career focusing her research interests and publications on information security, cybersecurity, and artificial intelligence. Prior to her current role, Meryem worked as an advisor to the strategic projects department of the university, where she made significant contributions to the development of key initiatives. Her expertise and knowledge have been widely recognized, and she is a sought-after speaker and expert in her field.

Yusuf Mohamud Jama is a respected leader in the cybersecurity industry in East Africa. As the Co-Founder and CEO of Managed Guard, he is committed to advancing the industry through innovative cybersecurity solutions and the development of proprietary managed detection and response technology. Named one of the Top 10 IT Security Influencers in East Africa, Yusuf has over 12 years of experience in the security industry. He brings a wealth of expertise to his role, having previously worked as a cybersecurity consultant for the Djibouti and Somalia Governments. During his time there, he developed a comprehensive security program that covered all aspects of information security and risk management. Before entering the private sector, Yusuf served in the Ministry of Internal Security, specializing in intelligence and forensic analysis activities for the Somali Government. He has extensive experience in cyberwarfare and forensic analysis, making him a highly sought-after expert in the field.
Yusuf has earned a master's degree in information security from Naif Arab University for Security Science. He also holds several certifications in the cybersecurity industry.