jamk

Overview for capabilities of OT network monitoring tools

Tommi Ollila

Master's thesis
April 2024
Technology
Master's Degree Programme in Cyber Security

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Description

Ollila, Tommi

Overview for capabilities of OT network monitoring tools

Jyväskylä: JAMK University of Applied Sciences, April 2024, 63 pages.

Master's Degree Program in Information Technology, Cyber Security. Master's thesis.

Permission for open access publication: Yes

Language of publication: English

Abstract

Key objective for this research was to identify modern, current-day network monitoring tools' capabilities, which are designed for industrial customers. Organizations which want to improve their cyber security maturity and increase preparedness level, one development area is implementing a network monitoring system.

Research consisted of identifying and analyzing network monitoring tools, which are purpose built towards industrial applications. The preliminary research and suggestions directed this research towards different software vendors.

Operational side of this research consisted of evaluating functionalities of the tools. The following functionalities were evaluated: what kind of first impression does the tool provide, how available the tool is, how does the tool compare to established evaluation criteria. Based on the established evaluation criteria, a single tool was selected and assessed in a laboratory environment with exploratory testing.

The research implies that even though there are tools available to increase capability in general network monitoring, path to increasing it in an industrial environment is not as straightforward. The root cause is mainly due to tools not supporting vendor-specific industrial protocols. In addition, scarcity of available technical information regarding industrial environments should be taken into account.

Keywords/tags (subjects)

operational technology, industrial, network monitoring, cyber security

Miscellaneous (Confidential information)

-

jamk

Kuvailulehti

Ollila, Tommi

OT verkkomonitorointityökalujen kyvykkyyskatselmointi

Jyväskylä: Jyväskylän ammattikorkeakoulu, Huhtikuu 2024, 63 sivua.

Master’s Degree Program in Information Technology, Cyber Security. Master’s thesis

Verkkojulkaisulupa myönnetty: Kyllä

Julkaisun kieli: Englanti

Tiivistelmä

Tutkimuksen päätavoitteena oli selvittää nykyaikaisten, teollisuuden asiakkaille suunnattujen verkkomonitorointityökalujen toimintakykyä. Yritykset, jotka haluavat kehittää kyberturvallisuutensa kypsyystasoa ja parantaa varautumisastettansa, yksi kehityksen osa-alueista on verkkomonitorointijärjestelmän käyttöönotto.

Tutkimus koostui verkkomonitorointityökalujen löytämisestä sekä analysoimisesta, jotka ovat tarkoitettu sekä suunniteltu teollisen ympäristön vaatimuksia ajatellen. Alustava selvitys ja käytännön ohjeistus antoi suuntaa tälle tutkimukselle eri ohjelmistotoimittajien osalta.

Tutkimuksen käytännön osuus muodostui eri työkalujen kyvykkyyksien arvioinnista. Nämä kohdistuivat seuraaviin aihealueisiin: minkälaisen ensivaikutelman työkalu antaa, miten hyvin se on saatavilla, sekä miten työkalun ominaisuudet sopivat ennalta määriteltyihin arviointikriteereihin. Kriteeristön perusteella valittiin yksi työkalu, jota arvioitiin laboratorioympäristössä tutkivan testauksen menetelmillä.

Tutkimuksesta voidaan päätellä, että vaikka on olemassa erilaisia työkaluja yleisen verkkomonitoroinnin kyvykkyyden kasvattamiseen, se ei ole yhtä suoraviivaista teollisessa ympäristössä. Juurisyy tähän on se, että työkalut eivät välttämättä tue teollisuuden laitetoimittajakohtaisia protokollia. Lisäksi on otettava myös huomioon teollisen ympäristön saatavilla olevan teknisen tiedon niukkuus.

Avainsanat (asiasanat)

operaatioteknologia, teollisuus, verkkomonitorointi, kyberturvallisuus

Muut tiedot (salassa pidettävät liitteet)

-

Contents

1 Introduction 6
1.1 Motivation 7
1.2 Research questions and objectives 8
2 Research methodology 10
2.1 Qualitative research 10
2.2 Initial scoping 10
2.3 Exploratory research 10
2.4 Research ethicality and reliability considerations 11
3 OT enviroment in general 12
3.1 Typical OT environment 12
3.2 Challenges in OT environments 13
3.2.1 Criticality 13
3.2.2 Availability 13
4 Network monitoring 14
4.1 Performing network monitoring 14
4.2 Value adding methodologies 14
4.2.1 Visibility to the network itself 14
4.2.2 Detecting malicious activity 15
4.2.3 Vulnerability and version management 15
4.2.4 Configuration management 15
4.2.5 Asset inventory 15
4.2.6 Monitoring remote access 15
5 IEC 62443 – Standard for OT enviroments 17
5.1 IEC 62443: 1-1 to 1-4 17
5.2 IEC 62443: 2-1 to 2-5 17
5.3 IEC 62443: 3-1 to 3-3 18
5.4 IEC 62443: 4-1 to 4-2 18
5.5 Network layout in OT environments 18
5.6 Purdue model 19
6 Network monitoring implementation process 20
6.1 Improvement on visibility 20
6.2 Iterative proof-of-value approach 20
6.2.1 One-time network scan 20

6.2.2 Permanent installation 21
6.3 Resource allocation 21
7 Evaluation of tool vendors 22
7.1 Armis 22
7.2 Barracuda: CloudGen Firewall 22
7.3 Check Point 22
7.4 Cisco: Cyber Vision 23
7.5 Cisco: Secure Network Analytics 23
7.6 Claroty 23
7.7 Darktrace: Industrial Immune System 23
7.8 Dragos 23
7.9 Forescout: eyeInspect 24
7.10 Kaspersky: Industrial Cyber Security 24
7.11 Microsoft Defender for IoT 24
7.12 Nozomi Networks: Guardian 24
7.13 Ordr 24
7.14 Palo Alto Networks 24
7.15 SCADAfence 25
7.16 Smokescreen: IllusionBLACK 25
7.17 Tenable OT Security 25
7.18 Verve: Security Center 25
7.19 VMware: Carbon Black 25
8 Comparison of features between identified tools 26
8.1 Evaluation criteria 26
8.2 Comparison based on criteria 26
8.3 Comparison results 29
8.4 Additional evaluation criteria 30
8.5 Comparison based on additional criteria 31
8.6 Final results on comparison 33
9 Evaluation: Microsoft Defender for IoT 34
9.1 Tools on network traffic recording 34
9.1.1 Tcpdump 34
9.1.2 Plunder bug 34
9.1.3 Wireshark 35
9.2 Technique on network sample data collection 36

9.3 Laboratory environment setup overview for evaluation 38
9.4 Network capture locations 38
9.5 Network capture files 38
9.6 Setting up evaluation environment 41
9.6.1 Obtaining installation media 41
9.6.2 Installation of Microsoft Defender for IoT 43
9.6.3 Replaying network capture files 48
9.7 Review of the tool's features and outputs methods 50
9.7.1 Asset inventory 50
9.7.2 Integrations to third party systems 51
9.8 Results on network traffic captures 52
10 Results 54
10.1 Functionality areas of Microsoft Defender for IoT 54
10.2 Summary of value-adding functionalities 56
11 Conclusions 57
11.1 Evaluation of research questions 57
11.2 Further improvements, research, and evaluation 58
11.3 Afterthoughts 59
References 60

Figures

Figure 1. Example of purdue model (Dolezilek et al., 2020) 19
Figure 2. Pie chart displaying distribution of initial evaluation criteria fullfillment 29
Figure 3. Pie chart displaying distribution of additional evaluation criteria fullfillment 33
Figure 4. Plunder bug network tap device (Hak5 LLC, n.d.) 35
Figure 5. Screenshot about inspecting a single network packet within Wireshark 36
Figure 6. Port mirroring illustration in a lab enviroment network traffic capture scenario 37
Figure 7. Network port passive capture illustration 38
Figure 8. Screenshot after logging into Microsoft Defender For IoT dashboard in Azure 41
Figure 9. Screenshot of setting up OT/ICS security in Microsoft Azure 42
Figure 10. Screenshot about generating MD5 checksum from the downloaded file 42
Figure 11. Screenshot of VMware Workstation version information 43
Figure 12. Screenshot of VMware Workstation virtual machine settings 43
Figure 13. Screenshot of booting the installer image inside the virtual machine 44
Figure 14. Screenshot of selecting network management interface 44
Figure 15. Screenshot about a successful installation login prompt 45
Figure 16. Screenshot of Microsoft Defender for IoT local login webpage 46
Figure 17. Screenshot of license verification after installation 46
Figure 18. Screenshot of SSL certificate options during configuration phase 47
Figure 19. Screenshot about the sensor main webpage 48
Figure 20. Screenshot about Play PCAP feature 49
Figure 21. Screenshot of network traffic analysis in progress 49
Figure 22. Screenshot of main overview page of the IoT sensor after ingesting network data 50
Figure 23. Screenshot listing seen devices on the network 51
Figure 24. Screenshot illustrating forwarding configuration 51
Figure 25. Screenshot about integration of forward options to different systems 52

Tables

Table 1. Evaluation criteria 26
Table 2. OT network monitoring tool functionality comparison matrix 27
Table 3. Potential OT network monitoring tool candidates for further evaluation 30
Table 4. Additional evaluation criteria 31
Table 5. Additional comparison of network monitoring tools 32
Table 6. Capture methods by number 39

Table 7. Network traffic capture file matrix 39
Table 8. Value-adding matrix 54

1 Introduction

A general rule of thumb towards Cyber Security is the principle “defense in depth.” In order to best secure an environment, multiple different controls needs to be implemented with different protection angles, which affect different areas on the system as a whole. (Knapp & Samani, 2013)

Typically, an organizations’ IT assets have been the first and most visible target towards bad actors. Therefore, businesses have had inherent driving factors on protecting IT related assets. Unfortunately, the same cannot be stated from operational technology’s point of view. Operational technology in recent years has matured to a point, in which devices in the area have become more interconnected and smarter. Such things as Industrial IoT or Industry 4.0 have developed in the background in increasing productivity and effectiveness of production lines. However, the same maturing has not applied on general outlook of OT related cyber security areas. Still, in the industry attitude towards OT is that the devices are not at risk and are “offline only.” (Renaud & Ophoff, 2021)

The lifespan of an OT device is generally extremely long compared to an IT device, and therefore it inherently creates risk in lifecycle management. Depending on vendor support, the device might not have mitigation measures available towards different cyber security threats. Replacing specific components cannot be done unless a larger system is replaced. (Jung et al., 2023)

This creates excessive cost on mitigation procedures and therefore usually risks related towards OT devices on cyber security are accepted instead of mitigated. One alternative mitigation measure for substantial number of devices is network monitoring. Since OT devices are becoming more interconnected, they have a common control plane that can be monitored. (Cheung et al., 2006)

Typically, businesses do not have actual visibility to the OT networks themselves. The mitigation control focus has been on enterprise IT networks. OT devices are typically provided and configured by their respective vendors. Business responsible IT personnel might not even be aware of the devices, networks, procedures, and responsibilities on the OT side of network. (Kapoor et al., 2023)

Networked OT devices communicate between each other and affect real world, based on parameters received over the network. Even if an organization would have IT network monitoring in-place, and by extension SOC procedures in place, any OT related devices could fall outside of this monitoring scope. Operational technology related alarms are generally related to the process itself and are generated by a production control system and directed towards on-site operators. (Chen et al., 2022)

Network monitoring implementation can help businesses to report on potential malicious activity within their environments. If unusual activity is detected that deviates from established baseline, an alert can be sent out to relevant responsible persons. In addition, network monitoring solution could be used as a type of system health monitor. As an example, it can generate events based on different availability metrics. In a case where a device drops out of the network, an alert can be generated, and the issue can be addressed accordingly. Historical usage data, trends and device communication patterns can also be generated from network activity. (Etalle, 2019)

1.1 Motivation

The topic for this research was heavily motivated by the author's own subjective experiences from operating within OT technology field. An unfortunate but very real lacking attitude towards cyber security elements within industrial environments still persists even to this day. Since industrial environments provide critically necessary functions to societies, they present themselves as an attractive target for bad actors. This fact combined with lacking or outdated security control measures, the potential impact on a successful attack cannot be understated.

This research's aim is in the recognition of untapped potential on implementing network monitoring solutions to pre-existing industrial environments. While the prospect of integrating such systems may initially seem daunting, advancements in tool maturity have made it increasingly feasible to deploy robust monitoring solutions without imposing prohibitive costs or risks.

Reflecting on these key motivations, this research endeavors to shed light on the imperative need for heightened cyber security measures within industrial environment, while also exploring a practical avenue for implementing a network monitoring solution. Contribution on recommendation in enhancing resiliency and security posture of industrial infrastructures in an increasingly digital age

is pivotal objective of this research, with the goal of giving guidance on increasing cyber security maturity level and bringing forward security knowledge.

1.2 Research questions and objectives

The first research question can be stated as follows:

What tools currently exist that are viable for network monitoring in OT environments?

The information gathered during preliminary search directed this research towards well-known software suppliers and their software catalogs. A first-stage evaluation will be done in order to assess whether the tool itself is suitable for our research's secondary and tertiary objectives.

The secondary research question can be stated as follows:

How does the existing tools suit specifically for OT network monitoring?

The question focuses in on the perceived functionalities different tools have. Functionality offering has the potential to differentiate tools between each other. Assessment criteria will be crafted with different operating areas in mind. Qualitative research method will be used on publicly available information sources during assessment for the secondary research question.

The tertiary research question can be stated as follows:

Perform exploratory testing to one screened tool and verify its operational capabilities. What value-adding functionalities does the tool have? How does the tool improve organizations' cyber security maturity?

Evaluation criteria should include cost-benefit assessment towards the organizations which could benefit from integrating such tool into their environment. Depending on the maturity level of an organization and their processes in place, it should be reflected if an organization can benefit from

the tertiary research's objective results. As an example, in the case that the tool can generate reports which help in businesses-making decisions, the report's visibility and practicality towards these criteria should be evaluated.

2 Research methodology

2.1 Qualitative research

Qualitative research method has been used in conducting this research due to the nature of the research questions (Patton, 2015). Availability of the information in which the tool evaluation has been based on, is qualitative in nature. In addition, it is assumed that the tool evaluation will provide data which could be also considered qualitative in nature. However, it should be noted that the comparison based on the evaluation criteria could be thought as partly quantitative.

2.2 Initial scoping

Preliminary research from publicly available sources have been used to gather information about the current state of network monitoring tools suitable for OT environments. The initial research implies that there exists potential candidates for network monitoring solutions, but no concrete evidence has been presented on how effective these kinds of tools are in tackling real-world problems. The effectiveness typically is only backed by the supplier organization's own material and could be considered biased. Another variable is the possibility, that a tool has been purpose-built towards IT environments. In this research, even if a tool is clearly designed to be operated within IT environment, the tool must be evaluated from operational technology standpoint. This kind of evaluation can also bring forward potential incompatibilities among different business priorities between IT and OT environments.

2.3 Exploratory research

Qualitative comparison of the different tool vendors was based on publicly available information. Limiting information source to only publicly available data was done due to time and resource constraints. It should be acknowledged that there exists margin for error depending on the investigated material (Patton, 2015). Considering that the research's information was obtained mainly on first-hand software catalog brochures, the information obtained is potentially biased towards highlighting wanted traits and not mentioning negative ones. In addition, it should be stated that due to the nature of software catalogs, all of the relevant information for this research might not be present which could have affected the end results during tool evaluation phase. On the other hand, material

was obtained directly from the vendor and not from a third party, which could have affected negatively on the credibility of the evaluation.

2.4 Research ethicality and reliability considerations

This research follows JAMK University of Applied Science's published ethical guidelines (JAMK University of Applied Sciences, 2018). Used sources have been cited accordingly and have been selected with consideration in mind, based on "SIFT & PICK" procedure (Carey, 2023). This guideline presents key characteristics in which to consider when selecting credible sources for research. The approach is similar to a slightly older "P.R.O.V.E.N" process (Carey, 2021).

This research conducts comparison between different potentially commercially competing products. It is crucial to highlight that this research is conducted with objectivity in mind without affiliations to any of the identified software vendors. In addition, it should be stated that no financial transactions, goods, endorsements, or incentives of any kind were received from the identified vendors. Furthermore, it should be declared that no attempts were made by any of the identified vendors in this research to influence the findings or end-results of this research.

Information on which the comparison of different tools is based on, is obtained from direct source of the software vendor. This eliminates potential bias of a third-party skew of feature highlights. However, since the information is based on different commercial products, it should be noted that vendors typically would like to present their own product in favorable light. Therefore, any evaluation criteria needs to be objectively selected.

3 OT enviroment in general

3.1 Typical OT environment

Operational technology as a concept could be described as technology affecting real world applications. As an example, a PLC could control a motor, which in turn would rotate an axle. These types of technologies are not typically marketed towards non-business consumers and instead marketing focuses on industrial clients. Operational technology is not just limited to traditional computers or software that runs within, but it also encompasses, for example, PLCs, protection relays, engine controllers, measurement devices, smart buttons or building automation systems. The concept of operational technology is quite wide, and it is everywhere around us. (Radvanovsky, 2013)

It is observed that attitude and technological implementations towards Cyber Security in operational technology field is behind information technology applications. This can be observed for example, as shared administrator accounts, lack of cryptographic implementations between endpoints and relaxed attitude towards good cyber security related best-practices. (Assenza et al., 2020)

As an example, operational technology can be considered to be in the following kinds of fields:

- Buildings (building automation, e.g., air conditioning and heating)
- Electrical grids
- Factories
- Logistic centers
- Marine vessels
- Medical field, hospitals, clinics
- Offshore wind turbines
- Oil drilling platforms
- Power plants

3.2 Challenges in OT environments

3.2.1 Criticality

Operational technology assets typically run real-life value affecting processes. If this process was to be disrupted, direct loss of revenue and profitability can be seen (Weiss et al., 2022). Via this context, the outlook to changes, modifications and updates is stricter and slower. Depending on the criticality of the system, one method is to perform upgrade testing. By performing this cautionary measure, it is verified that the intended changes can be done in a non-production environment successfully, and that no unintended downtime will be caused by unforeseen setbacks. (Staves et al., 2023)

3.2.2 Availability

In operational technology, another key characteristic is availability. During risk assessments, any availability affecting risks compared to confidentiality, usually the method which ensures availability better is selected. This preference can lead to prolonged periods of time between security related or general software lifecycle control improvements. (Garimella, 2018)

Vendors which operate within industrial environments over extended periods of time are typically offering lifecycle management services (ABB Oy, 2022). With this kind of approach, the expected lifetime of the system is known beforehand, and it increases predictability to managing cost and downtime of the system.

4 Network monitoring

As organizations grow, communication networks tend to grow and become more complex. Network administrators often fail to keep up with the growth and therefore the growth is inverse to visibility of the network. Operational models which have performed well on small scale networks do not scale well into enterprise sized networks. One solution for this is network monitoring implementation. Network monitoring is essentially bringing forward visibility to events happening in an organization's communication network. In short, monitoring enables network administrators to get a better overall understanding of what they are responsible of. Therefore, network monitoring can increase enterprises' cyber security capability in different areas. (Weiss et al., 2022)

4.1 Performing network monitoring

Network monitoring is typically performed by collecting data from multiple network traffic conjunction points from multiple different devices. The data is then delivered to a central monitoring location. The monitoring location has capability and methods for ingesting, processing, and displaying collected data. Various kinds of information can be deducted from network activity. This information can then be used in pre- or post-processing tasks in security or non-security related matters. These tasks should be delegated. Follow ups and monitoring should have a designated named responsible person available. Reporting policies and procedures should be established in order to bring visibility to decision-making level, since organizational, budget-level decisions can be affected by conclusions based on network monitoring data. (Mukherjee, 2020)

4.2 Value adding methodologies

4.2.1 Visibility to the network itself

If an organizations network grows enough, it becomes unsustainable to keep track of it manually. Therefore, automated tools have been developed which bring visibility to the contents of communication networks. Dashboards and user interfaces have been developed which aggregate data from all over the network, in order to give network administrators better general information about the status of the whole network. (Mukherjee, 2020)

4.2.2 Detecting malicious activity

Network activity can show attempted access to malicious or otherwise undesired domain names. Depending on company policy, such sites can be pre-emptively blocked. For example, firewalls can block access to such sites and create logs if those sites are attempted to be accessed. In a modern environment with constantly updating access lists, suspicious machine-to-machine activity could for example, trigger an alert. (Mukherjee, 2020)

4.2.3 Vulnerability and version management

By processing network traffic data with modern tools and by collecting and evaluating metadata, organizational level vulnerability information can be obtained. An application can potentially announce its version number within its network traffic. This version number can then be matched against known public vulnerability databases, in order to obtain device specific vulnerability information. (Mukherjee, 2020)

4.2.4 Configuration management

Network monitoring can also help deduct configuration errors within networks. If a networked device is seen on monitoring doing something it should not do, then deducting its location and reason for possible misconfiguration is made more straightforward. As an example, a type of misconfiguration could be that a device is trying to reach an Internet based address for automatically updating its software or firmware. (Mukherjee, 2020)

4.2.5 Asset inventory

In addition, network monitoring can be used to gather an asset inventory list. Devices seen on the network can be logged, collected, recorded, and categorized by their network behavior. In addition, if unknown devices are seen on the network, they can be investigated further, and an evaluation could be made if the device is an indicator of compromise. (Mukherjee, 2020)

4.2.6 Monitoring remote access

A typical remote support procedure in OT environments is that a remote connection is established over the Internet towards OT vendor’s device. This is due to having support capability, without the

need of support engineer having to be physically present on-site. For example, a permanent VPN connection can be built into the end-customer premises. Therefore, a risk exists that this type of connection has not been approved or communicated for end-customers IT, or even OT department. Typically, this kind of scenario can become reality when a vendor offers lifecycle, support, or update services. Remote support does not have travel costs, and it is therefore seen generally as the more preferred option. In addition, response time to support is faster due to no on-site presence requirement by the supporting engineer. (Mukherjee, 2020)

Network monitoring solution in an OT network can provide assurance that common agreed operational methods are being adhered to by all parties. Typical procedures could be, for example calling the customer first and verifying that using remote connection is approved for that specific time, or making sure that personnel on-site are aware that changes are being made to the system which can cause unintentional alarms and can therefore be ignored. Network monitoring could reveal authorized-but-unapproved remote connections within the network towards different devices. (Mukherjee, 2020)

5 IEC 62443 – Standard for OT enviroments

The IEC 62443 standard has been created for the purpose of addressing industrial cyber security and operational technology related areas. The standard has been divided into four different sections of focus, from component level to organizational level, utilized by the following categories:

- General
- Policies & Procedures
- System
- Component

Since the definition of operational technology is not limited to just factories or critical infrastructure, it is utmost essential to take cyber security into account when considering if the current objective belongs to realm of operational technology. The amount of interconnected operational technology hidden in plain sight in modern-day world can be surprising. (Franceschett et al., 2019)

5.1 IEC 62443: 1-1 to 1-4

The IEC 62443 1-1, 1-2, 1-3 and 1-4 addresses general terms and gives an overview of the terminology, models, and concepts behind the standard. A reader which is not familiar with automation or cyber security concepts beforehand, can familiarize themselves with these sections. It brings forward knowledge which is essential in understanding the concept of defense in depth. (Leander et al., 2019)

5.2 IEC 62443: 2-1 to 2-5

The “level 2” of IEC 62443 addresses cyber security requirements, methods, policies, and ways of working on an organizational level. These sections focus on the non-concrete and abstract line of policies for the executive and managerial levels since usually in most organizations that level has the power to address and deploy changes to operational models. (Leander et al., 2019)

5.3 IEC 62443: 3-1 to 3-3

The “level 3” of the standard focuses on component level details. It is directed first and foremost to system creators and gives input on the proper way of building and securing operational technology networks and systems. The standard gives guidance for system builders on using already-developed tools on design, configuration, and integration. As an example, one target group would be system engineers building a new power plant project (IEC 62443-3-3:2013, 11-13).

5.4 IEC 62443: 4-1 to 4-2

The “level 4” of the standard is directed towards developers and gives guidance on best practices related to development processes. The key focus area is towards secure product development lifecycle and component level requirements for industrial automation cyber security elements. The target group for this standard is for example, software developers working with new features on an already existing distributed control system product. (Leander et al., 2019)

5.5 Network layout in OT environments

The network layout can be vastly different in industrial applications than in regular enterprise networks for general organizational level use. Typically, the differentiating network requirement is availability and in general, networks with OT devices have longer lifecycle than their IT counterparts. The procurement and maintenance responsibility of aforementioned OT networks can also be fragmented across different vendors. Distributed control systems can have their own networks supplied by the vendor, and its control and maintenance is potentially not transparent to the organizational IT level. In addition, typically any changes done to the network after commissioning could cause downtime in the industrial environment which could be unacceptable. For these reasons, maintenance could be neglected, since the risk of old or degraded versions has been accepted in favor of keeping downtime to a minimum. (Leander et al., 2019)

5.6 Purdue model

Current recommended network layout for industrial applications can be found within IEC 62443 3-3 standard. The fundamental is based on “defense in depth” principle, which sets out to apply multiple defense mechanisms and controls in order to avoid a single point of failure in terms of protecting an environment.

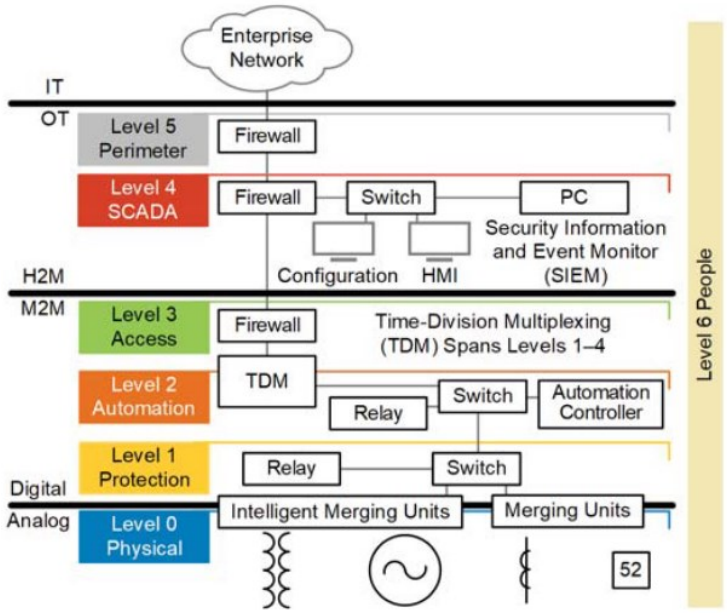


Figure 1. Example of purdue model (Dolezilek et al., 2020)

The general design model is that all network traffic must pass through a DMZ network which has control mechanisms in place. This can be, for example a virtual machine which has application layer controls in place, in order to disallow direct connections from upper levels to lower control levels. The virtual machine can for example, accept a remote connection originating from upstream and check for privileges according to set policies. In addition, the connection itself should not be directly forwarded. In practice depending on the software and use-case required, a mirror of the data from lower levels can reside in DMZ, which itself forwards the data to upper levels. This methodology removes the need for direct upstream connection to the low levels. (Santiago Robles Durazno, 2021)

6 Network monitoring implementation process

6.1 Improvement on visibility

”You cannot protect what you cannot see” (Quade, 2018).

In security industry, the above-mentioned quote has been thought out to be one foundation of security related viewpoint. If a network-connected asset has remained undetected and therefore not maintained, over an extended period of time it becomes more vulnerable to exploitation. These kinds of devices then can be potentially used as a pivoting point in creating an attack vector towards more critical systems. If a potentially vulnerable device is connected to two or more networks, this could for example, bypass firewall controls or access networked resources which have been built with the assumption, that any traffic into them can be considered as trusted. (Quade, 2018)

6.2 Iterative proof-of-value approach

Before committing large amount of time and resources, an iterative proof-of-value approach could be taken about the benefits of network monitoring, with either a small-scale deployment, or in a non-invasive way by collecting network data from on-site locations and inserting captured data into a network monitoring tool.

An organization which wants to improve its own network security posture could approach the implementation in a similar way as this research demonstrates in the exploratory research chapter. Depending on the implementing organization’s maturity level on cyber security, the effective usage of conclusions, visibility, and alerts that a network monitoring tool provides, can have drastic differences in proof-of-value outcomes. If the organization does not have the capability to act on the provided results, the proof-of-value effectiveness can be reduced.

6.2.1 One-time network scan

Instead of immediately going forward with a permanent installation of network monitoring solution, an alternative way would be to perform one-time network scan. This can keep the initial investment low with minimal modifications to the existing infrastructure. Afterwards, when the network traffic

has been captured, the data can then be forwarded to a similar laboratory environment in order to evaluate different network monitoring tools for their specific requirements and devices.

6.2.2 Permanent installation

Permanent network monitoring solution installation to on-site locations could be performed, after an initial proof-of-value assessment shows indicators of value-adding functions. Therefore, making the installation permanent could be a natural next step. Compared to an initial assessment, a permanent installation would require separate hardware and licensing investment, and permanent network modifications. Depending on which party is responsible for OT networks, lead time to acquire suitable modifications to the network could be extended. For example, in a case, where a third-party hardware vendor has procured and commissioned an industrial network, the modifications and change requests must be perhaps done via the original supplier. If the responsibility areas are not clear, the implementation time can experience a snowball effect within a network monitoring implementation project. Another key obstacle could be the lack of comprehensive network diagrams which express different third-party device interconnectivities, and the connectivity towards business IT networks.

6.3 Resource allocation

If an organization decides to implement network monitoring solution within their network by outsourcing the installation and integration project, knowledge must be transferred in order to fully utilize all potential the solution offers. If training and knowledge-acquirement has been outsourced, then the implementing organization will most likely be dependent on a 3rd party provided service model. Therefore, it should be imperative to evaluate if resourcing and training could be allocated to persons within the implementing organization.

7 Evaluation of tool vendors

Information gathering within this research focused on well-known software vendors' product portfolios. Analysis was conducted on the availability of tools suitable for OT specific network monitoring purposes. Criteria was established about which features are required within OT environment. As a precautionary measure, if multiple different tools would have similar qualities, additional evaluation criteria needs to be established, in order to single out one tool for exploratory laboratory testing.

The following tools are presented, which at a first glance, fulfill criteria to be included in this research. The common qualities which evaluation was based on with these tools were marketing material and first impression. These features indicate purpose towards network monitoring, but not necessarily towards OT environments. The following subchapters include a brief overview of the selected tools. A quantitative based, established feature criteria evaluation has been conducted in chapter 8.

7.1 Armis

The tool seems to have an extensive OT and IoT device database. Connectivity to cloud seems to be required. The functionality of the tool seems to be more of an asset inventory and not necessarily a traffic analysis toolset. (Armis, 2020)

7.2 Barracuda: CloudGen Firewall

The tool itself seems to be firewall and enforcement type of control software. At first glance, the tool itself is possibly not suitable for passive or active network traffic analysis. In addition, the tool itself seems to have limited protocol database available. (Barracuda Networks Inc., 2023)

7.3 Check Point

The tool itself seems not to be suitable as a pure network analysis tool and seems to be more of a firewall type in nature. Therefore, the tool seems to be designed to be an enforcement control software in nature. The tool itself seems not to have active scanning functionality built in. (Check Point Software Technologies Ltd, 2023)

7.4 Cisco: Cyber Vision

Cisco Cyber Vision's marketing material seems to indicate that the tool is purpose-built towards OT environments. However, the tool seems to require a proprietary Cisco network infrastructure to already be in-place. (Cisco, 2022)

7.5 Cisco: Secure Network Analytics

The tool seems to be purpose-built towards collecting information from existing networks devices. In addition, the tool seems to be built towards general IT infrastructure, and not specifically for OT environments. (Cisco, 2021)

7.6 Claroty

The tool at first glance seems promising. It seems to include the possibility to replay PCAPs into the software. In addition, it seems to be possible to be installed in a local virtual machine on the user's premises. It seems that no mandatory cloud connectivity is required. The tool seems to be capable of generating current-state reports about the network status. (Claroty, 2023)

7.7 Darktrace: Industrial Immune System

The tool seems to rely heavily on machine learning in order to raise alerts or deviations from baseline network traffic. Therefore, it is seeming that the tool does not have protocol analyzer per se and relies on long-term installations. In addition, the tool does not seem to support active scanning. (Darktrace, n.d.)

7.8 Dragos

Marketing material of the tool seems to indicate that it is designed to be integrated within OT environments. The software itself seems to be oriented towards incident response. Software itself seems to be possible to be installed within a physical device or to a virtual machine. In addition, it seems that importing PCAPs is a possibility. (Dragos, Inc., n.d.)

7.9 Forescout: eyeInspect

The tool seems to be designed with OT environments in mind. An active or passive network monitoring seems to be possible. (Forescout, n.d.)

7.10 Kaspersky: Industrial Cyber Security

The tool seems to be designed towards OT networks. Threat management seems to be done with real-time passive monitoring. The seems to have intrusion detection features available. (AO Kaspersky Lab, 2020)

7.11 Microsoft Defender for IoT

The tool seems to be purpose-built towards OT environments. Cloud connectivity seems to be required for an initial setup, but not mandatory for an actual deployment. Threat intelligence seems to be displayed within cloud environment. Air-gapped installation and local dashboard seems to be available. (Microsoft Corporation, n.d.)

7.12 Nozomi Networks: Guardian

Nozomi seems to offer Software-as-a-Service type model for organizations. The tool seems to be purpose built towards OT environments. Reports seem to be able to be generated and exported to PDFs or CSVs for better machine readability and integrations to other systems. The tool seems to have capability for passive monitoring on mirrored network ports. (Nozomi Networks Inc., 2020)

7.13 Ordr

From marketing material viewpoint, the tool seems to be focused on asset inventory and non-Industrial Internet of Things. (Ordr, n.d.)

7.14 Palo Alto Networks

Palo Alto is typically known for their firewall products. The software seems to be general-built in its usage environment, and not OT-specific in nature. In addition, the software seems to be enforcement type in nature. (Palo Alto Networks, 2022)

7.15 SCADAfence

Scadafence's target audience seems to be industrial environments and protecting critical infrastructure. The tool seems to have built-in risk analysis feature, which helps the user in further decision-making processes. It seems that reports can be generated and exported for later use. In addition, it seems that an analysis report regarding compliance to IEC 62443 is available. Installation procedure seems manual in Linux environment. Cloud-based environment seems to be available. (SCADAfence, n.d.)

7.16 Smokescreen: IllusionBLACK

This tool differentiates from the rest of the offerings due to its seeming honeypot like solution. The core functionality seems to be presenting itself as a vulnerable device within a network, which would then attract potential bad actors and generate alerts if the vulnerabilities inside the honeypot are targeted for exploitation. No active scanning functionality seems to be presented. (Smokescreen, n.d.)

7.17 Tenable OT Security

Tenable seems to offer wide category of different toolsets for different purposes. Their offering also seems to include a tool for handling OT security as a whole. From publicly available material, the feature-set seems to offer vulnerability management, asset inventory and report generation. (Tenable Inc., 2022)

7.18 Verve: Security Center

The toolset seems to be focused on OT technology field. However, no information seemed to be available to the underlying technology itself which empowers the software. The concept seems to be advertised as Software-as-a-Service and most likely is subscription based. (Verve, 2020)

7.19 VMware: Carbon Black

Vmware's offering seems to focus on endpoint protection. Therefore, it seems not to be suitable as a network monitoring tool. (VMware Inc, 2023)

8 Comparison of features between identified tools

8.1 Evaluation criteria

Evaluation criteria was established in order to select a tool for further exploratory testing. The functionality criteria are based on real-world requirements. The information in which the evaluation results have been based on, is the information vendors have publicly made available. The evaluation takes into consideration value-adding functionalities which are key focus areas for an organization. The criteria are designed based on multiple different use-cases. It was established that the network monitoring tool would need to perform the following functions by minimum:

Table 1. Evaluation criteria

Criteria number	Evaluation criteria
#1	Designed for OT network environments first
#2	Packet capture file replays (PCAP files)
#3	Report generation
#4	Active scanning

8.2 Comparison based on criteria

By establishing the mandatory functionalities an OT network monitoring tool should have, an evaluation on these functionalities can be performed. A table which consolidates the tools and functionalities compared to evaluation criteria can then be formed. A checkmark “X” indicates that the tool has that specific functionality or feature. The first-stage comparison can be observed in Table 2:

Table 2. OT network monitoring tool functionality comparison matrix

Tool to be evaluated	**#1 Designed only for OT networks**	**#2 PCAP replay**	**#3 Report generation**	**#4 Active scanning**
Armis	**X**		**X**	
Barracuda: CloudGen Firewall				
Check Point				
Cisco: Cyber Vision	**X**			
Cisco: Secure Network Analytics				
Claroty	**X**	**X**	**X**	**X**
Darktrace: Industrial Immune System	**X**			
Dragos	**X**	**X**		
Forescout: eyeInspect	**X**	**X**		**X**
Kaspersky: Industrial Cyber Security	**X**			
Microsoft Defender for IoT	**X**	**X**	**X**	**X**

Tool to be evaluated	#1 Designed only for OT networks	#2 PCAP re-play	#3 Report generation	#4 Active scan-ning
Nozomi Networks: Guardian	**X**	**X**	**X**	**X**
Ordr				
Palo Alto Networks				
SCADAfence	**X**		**X**	
Smokescreen: IllusionBLACK				
Tenable OT Security	**X**	**X**	**X**	**X**
Verve: Security Center	**X**			
VMware: Carbon Black				

As visualization, the distribution of initial different feature requirement fulfillment can be observed in Figure 2.

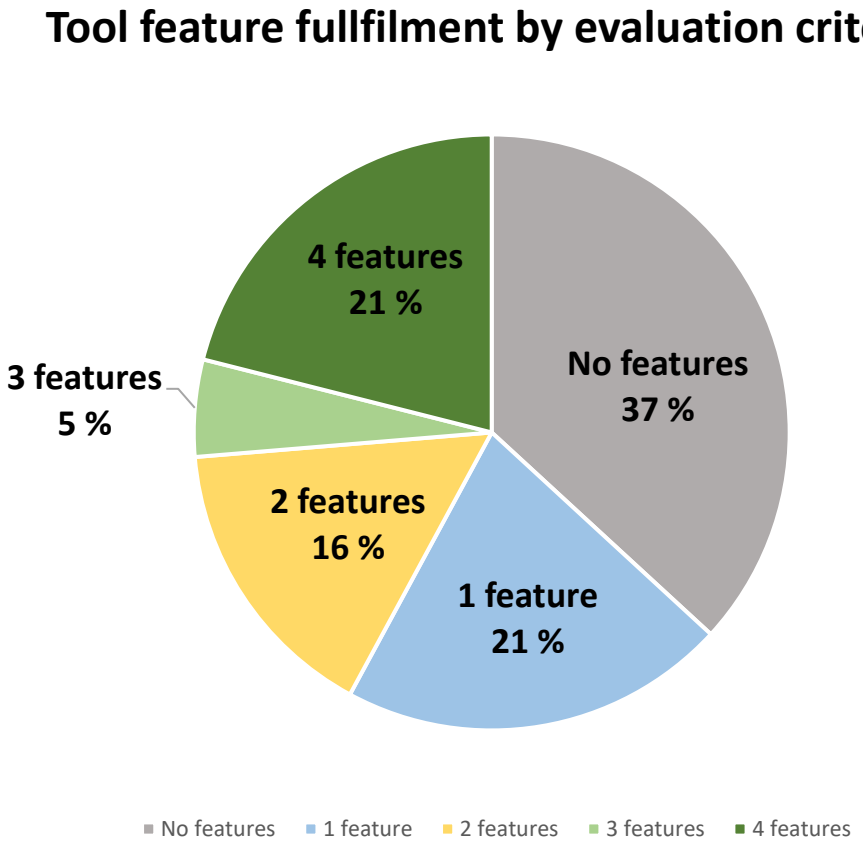


Figure 2. Pie chart displaying distribution of initial evaluation criteria fullfillment

8.3 Comparison results

By combining the tools which fulfill all of the initial criteria, a new table can be formed which displays a consolidated view of the potential OT network monitoring tools. The tools which fulfill all requirements set in Table 1 are presented in Table 3.

Table 3. Potential OT network monitoring tool candidates for further evaluation

Tool	**#1 Ad-hoc capability**	**#2 PCAP replay**	**#3 Report generation**	**#4 Vulnerability listing**
Claroty	**X**	**X**	**X**	**X**
Microsoft Defender for IoT	**X**	**X**	**X**	**X**
Nozomi Networks: Guardian	**X**	**X**	**X**	**X**
Tenable OT Security	**X**	**X**	**X**	**X**

Due to the evaluation resulting in multiple different tools from different vendors which fulfill the necessary requirements, additional criteria needs to be established in order to single out one tool for further exploratory testing.

8.4 Additional evaluation criteria

Additional evaluation criteria have been designed with end-user perspective in mind. An evaluation should be done on the ease of information available in a scenario, where the end-user is considering implementing network monitoring. Therefore, additional evaluation criteria are required and can be observed in the following table.

Table 4. Additional evaluation criteria

Criteria number	Evaluation criteria
#1	Public demo available (video or interactive website, not still images or brochures)
#2	Private demo available upon request
#3	Software files available for download without additional monetary or NDA commitment

8.5 Comparison based on additional criteria

By applying the criteria in Table 4 to the remaining tools in Table 3, the following comparison can be made in Table 5:

Table 5. Additional comparison of network monitoring tools

Tool	**#1 Public demo available (video or interactive website, not still images or brochures)**	**#2 Private demo available upon request**	**#3 Software files available for download without additional monetary or NDA commitment**
Claroty		**X**	
Microsoft Defender for IoT	**X**	**X**	**X**
Nozomi Networks: Guardian	**X**	**X**	
Tenable OT Security		**X**	

As previously done in chapter 8.2, additional criteria can be plotted in order to visualize distribution.

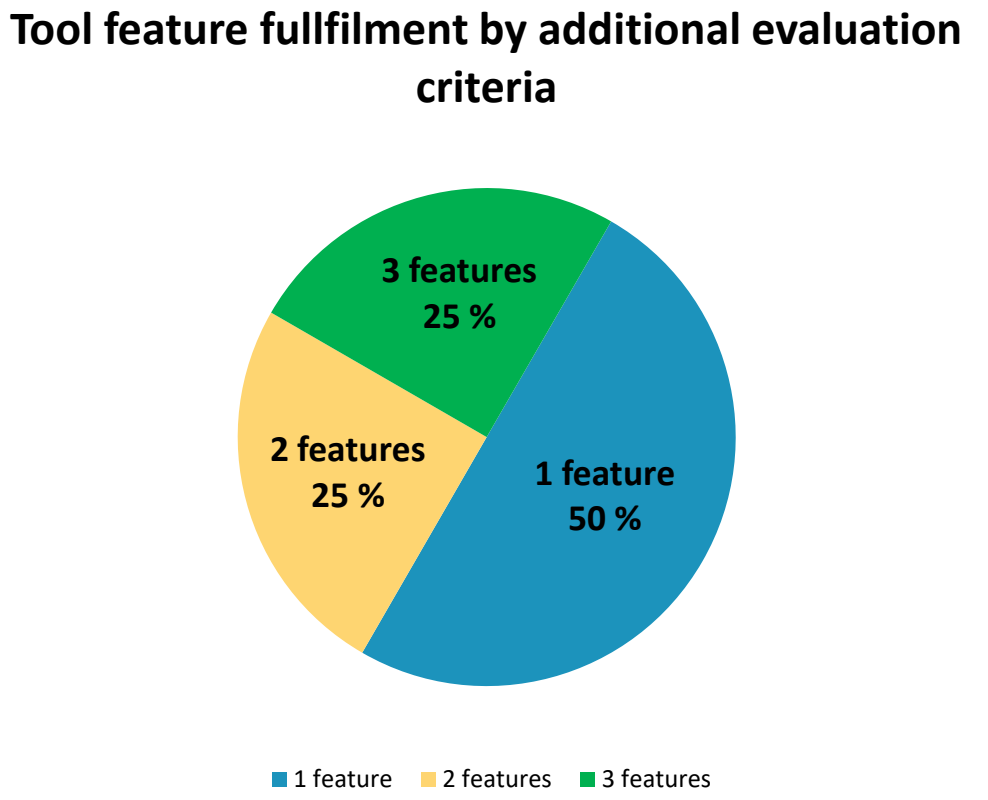


Figure 3. Pie chart displaying distribution of additional evaluation criteria fullfillment

8.6 Final results on comparison

By applying multiple evaluation criteria to the tools, one tool can be singled out which fulfills all the requirements presented in Table 1 & Table 4. The solution that will be evaluated in a laboratory environment in this research is Microsoft's Defender for IoT.

The tiebreaker requirement "#3 Software files available for download without additional monetary or NDA commitment" is fulfilled by Microsoft Defender for IoT due to Microsoft Azure Dev Tools for Teaching program (formerly known as Microsoft Imagine). It provides JAMK University of Applied Sciences members a limited free access to Microsoft Azure tool offerings. It should also be noted that Microsoft Defender for IoT offers at the time of writing a free 60-day trial period (Microsoft Corporation, 2023).

9 Evaluation: Microsoft Defender for IoT

Process of elimination resulted in Microsoft's Defender for IoT to be selected as the OT network monitoring tool for exploratory laboratory testing. In order to perform exploratory testing in a laboratory environment, real-world network traffic data capture is a prerequisite. The following chapters present methodologies and tools used in capturing network traffic and the evaluation of Microsoft Defender for IoT.

9.1 Tools on network traffic recording

Microsoft Defender for IoT is designed to be a cloud-based application first. On-site installations have sensors which collect network traffic data by monitoring mirrored ports on the network and then the sensors forward this data to Microsoft Azure cloud environment. Alternatively, an on-site installation can function in standalone mode, since network monitoring tools which operate in OT environments, need to take air gapped networks into account. Air gapped networks, by definition can be large, but they are not connected to any other network in the IEC 62443's purdue model or to the Internet (Microsoft Corporation, 2023).

9.1.1 Tcpdump

The core software in capturing network traffic data was tcpdump. It is an open-source command line software built for multiple platforms. Its designed purpose is to record network traffic data. (Sandler, 2008)

9.1.2 Plunder bug

The hardware which was used to capture network traffic data was the company Hak5's commercial Plunder bug hardware. The network TAP plugs either in-between two devices communicating or into a mirrored network switch port. In both cases the device captures network data passively. The network tap itself is connected to a laptop via an USB-C cable. The network tap is then identified within the operating system as a normal Ethernet device. (Hak5 LLC, n.d.)

Figure 4. Plunder bug network tap device (Hak5 LLC, n.d.)

9.1.3 Wireshark

Wireshark is a network packet analysis tool (Wireshark, n.d.). This software was used to evaluate network traffic captures in the field and to evaluate, if the collected data samples were valid. The tool was used in giving a first-stage assessment, in order to see if the network data was viable and if it would be usable in the exploratory testing phase.

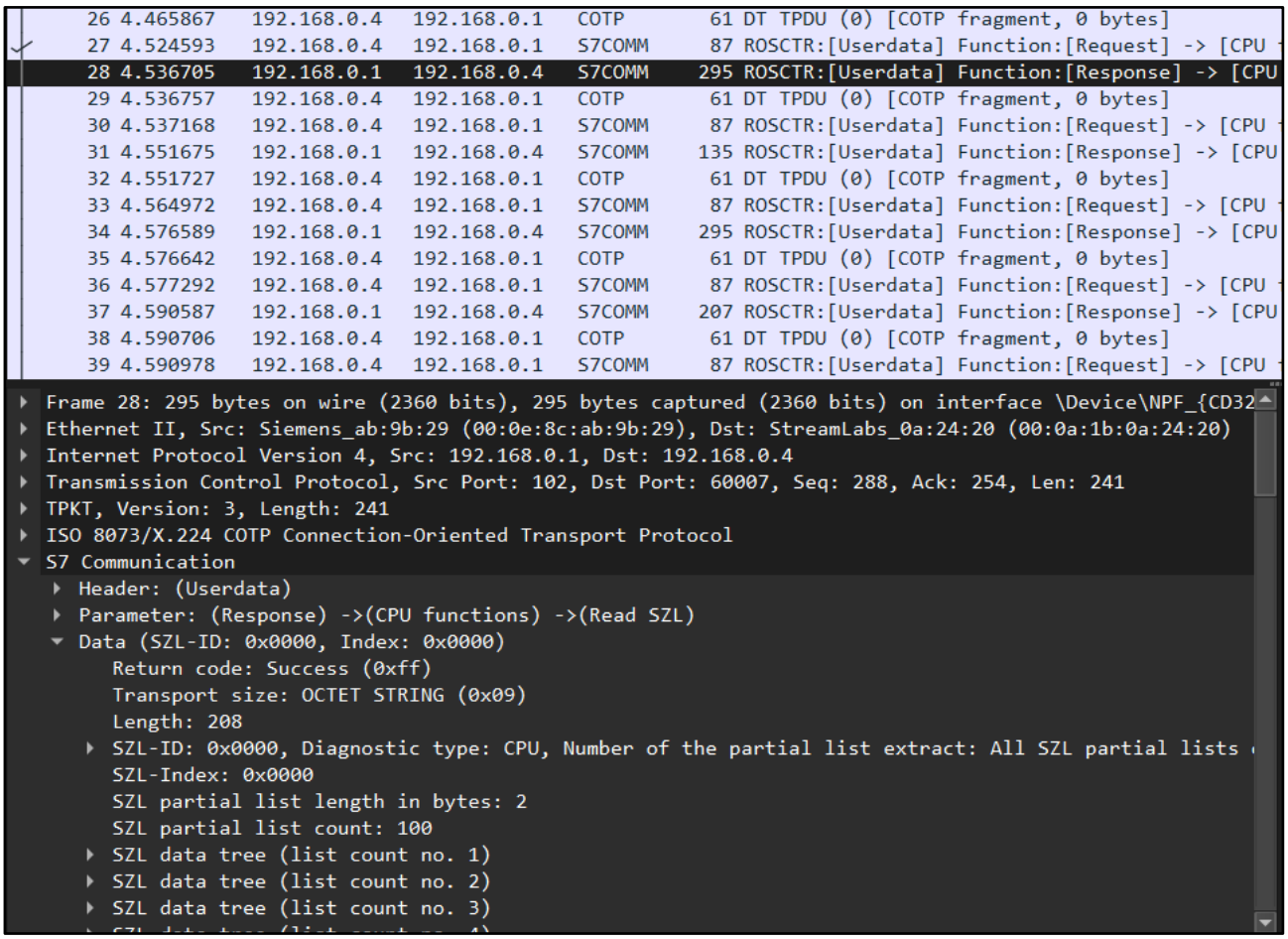


Figure 5. Screenshot about inspecting a single network packet within Wireshark

Wireshark capability to analyze packets is demonstrated in Figure 5. It shows contents of a single network packet. Figure 5 displays a specific network packet containing Siemens S7 communication data. Conclusion can be made that the network data which has been captured is beneficial in further line of testing and contains traffic which could be seen in an OT network.

9.2 Technique on network sample data collection

Network sample data was collected via two methods. The first was by using a network port mirroring method. The mirroring is achieved by the network device duplicating network packets passing through it and sending the duplicated packets into a designated and pre-configured Ethernet port. The device which has been connected to the mirrored port, receives duplication of all the traversing packets in the network switch. (Cisco, 2023)

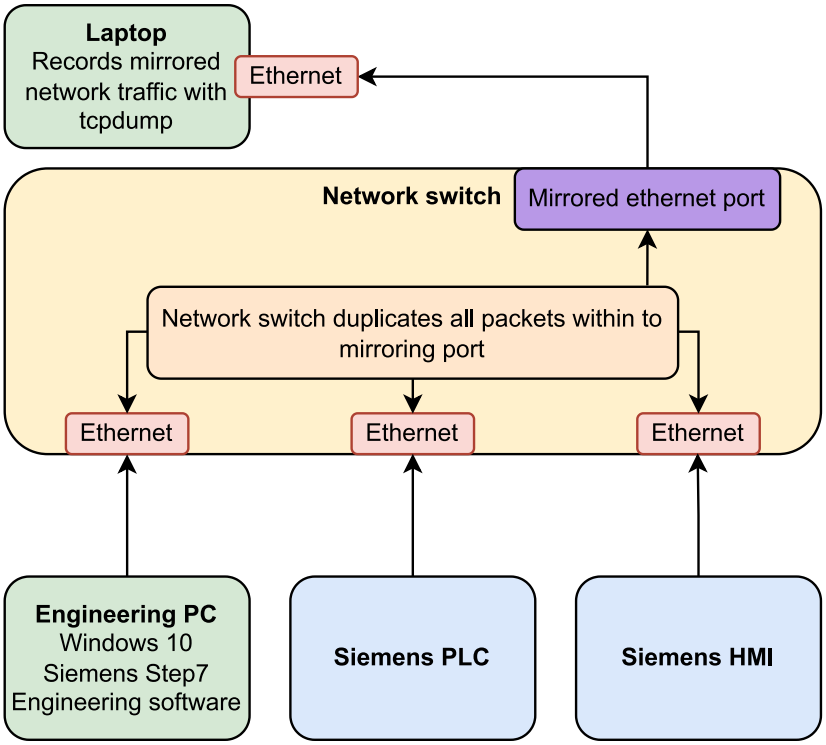


Figure 6. Port mirroring illustration in a lab enviroment network traffic capture scenario

The secondary method involved using the Plunder bug tool. The tool is attached between two devices, in this scenario, between a PLC and an engineering PC which communicate over the network. Plunder bug then copies any packets passing through it while remaining invisible to the devices. (Hak5 LLC, n.d.)

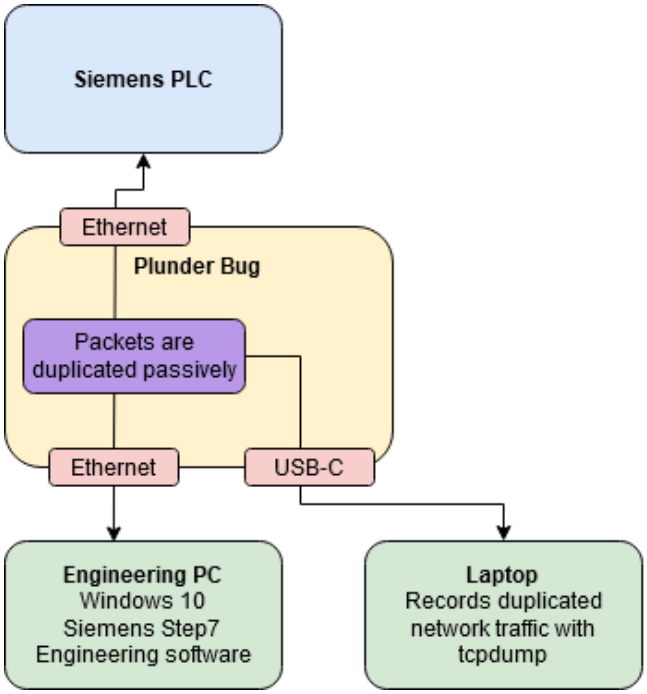


Figure 7. Network port passive capture illustration

9.3 Laboratory environment setup overview for evaluation

Laboratory test environment setup consisted of running Microsoft Defender for IoT sensor within a local virtual machine. Network packet captures are then replayed into the tool and output result will be observed. VMware Workstation 17 has been selected as the hypervisor, which has the capability of running Ubuntu 18.04 Linux virtual machines.

9.4 Network capture locations

Collected network traffic samples were uploaded into the tool from different types of laboratory setup networks and OT devices. Microsoft Defender for IoT results will be observed from this traffic. Network capture was performed on multiple separate networks by using tcpdump software in conjunction with Plunder Bug device, either passively or by connecting the device into mirrored network switch's Ethernet port.

9.5 Network capture files

The network traffic capture methods used in this research can be divided into two types.

Table 6. Capture methods by number

Capture method number	Capture method
#1	Network traffic captured with passive network TAP
#2	Network traffic captured via mirrored switch port

The following Table 7 presents collected network traffic samples and their contents. The first column presents the number of the capture method which is displayed in Table 6.

Table 7. Network traffic capture file matrix

Capture method number	Actions performed with engineering tool	Filename	OT devices
#1	No actions performed. Engineering tool failed to detect PLC with Plunder Bug plugged in before Siemens engineering tool discovery phase.	1_fail.pcapng	PLC: Siemens S7-1500

Capture method number	Actions performed with engineering tool	Filename	OT devices
#2	No actions performed.	2_On-lyFromPLC_to_Switch.pcapng	PLC: Siemens S7-1500 HMI: Siemens Simatic HMI TP700
#1	Uploading incomplete program to PLC, commanding master reset to PLC's CPU.	3_KindofFail_Run-MonitorMRES_com-mands.pcapng	PLC: Siemens S7-1500 HMI: Siemens Simatic HMI TP700
#1	Uploading program to PLC, monitoring and toggling variables, commanding CPU to start & stop.	4_S7_300_traf-fic.pcapng	PLC: Siemens S7-300 HMI: Siemens Simatic HMI TP700
#1	Uploading program to PLC, monitoring and toggling variables, commanding CPU to start & stop.	5_Si-matic_HMI_TP700_Comfort.pcapng	PLC: Siemens S7-1500 HMI: Siemens Simatic HMI

During the traffic capture, a few obstacles were encountered. The procedure was not as straight-forward as initially thought. It was discovered that the engineering tools require an initial discovery

and connection to the PLC before network traffic could be intercepted. The second difficulty was in incomplete PLC software projects available in the environment. This led to only having basic commands such as, variable monitoring and program upload available in the network traffic capture samples. The collected traffic is assumed to be normal traffic between Siemens PLC and HMI. In addition, PLC software upload has been captured during the network traffic collection.

9.6 Setting up evaluation environment

9.6.1 Obtaining installation media

Installation of Microsoft Defender for IoT begins by downloading an installation .iso image file distributed by Microsoft Azure. This image file contains a Linux based installer image which has been heavily customized by Microsoft. Access to this image requires a Microsoft Azure subscription to be in place. The installation guidance was followed, which is available from Microsoft's website (Microsoft Corporation, 2023).

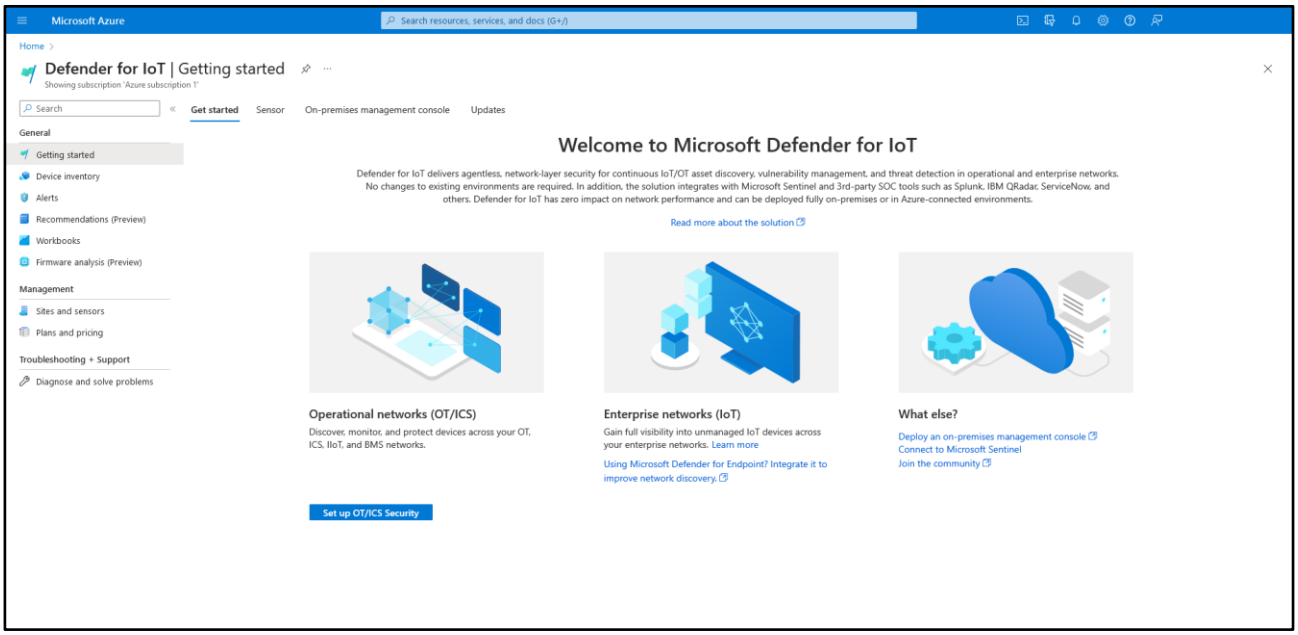


Figure 8. Screenshot after logging into Microsoft Defender For IoT dashboard in Azure

The overall experience has been designed to be user friendly with guidance and links to supporting documentation from Microsoft. The "Set up OT/ICS Security" which starts the process, includes a verification for subscription before granting access to any installation files or further steps. It should

be noted that obtaining such subscription in the viewpoint of research was not straightforward. The Microsoft Defender for IoT is not included in the default free-tier subscription for students and instead requires a payment method to be added before access to a free 60-day trial is granted.

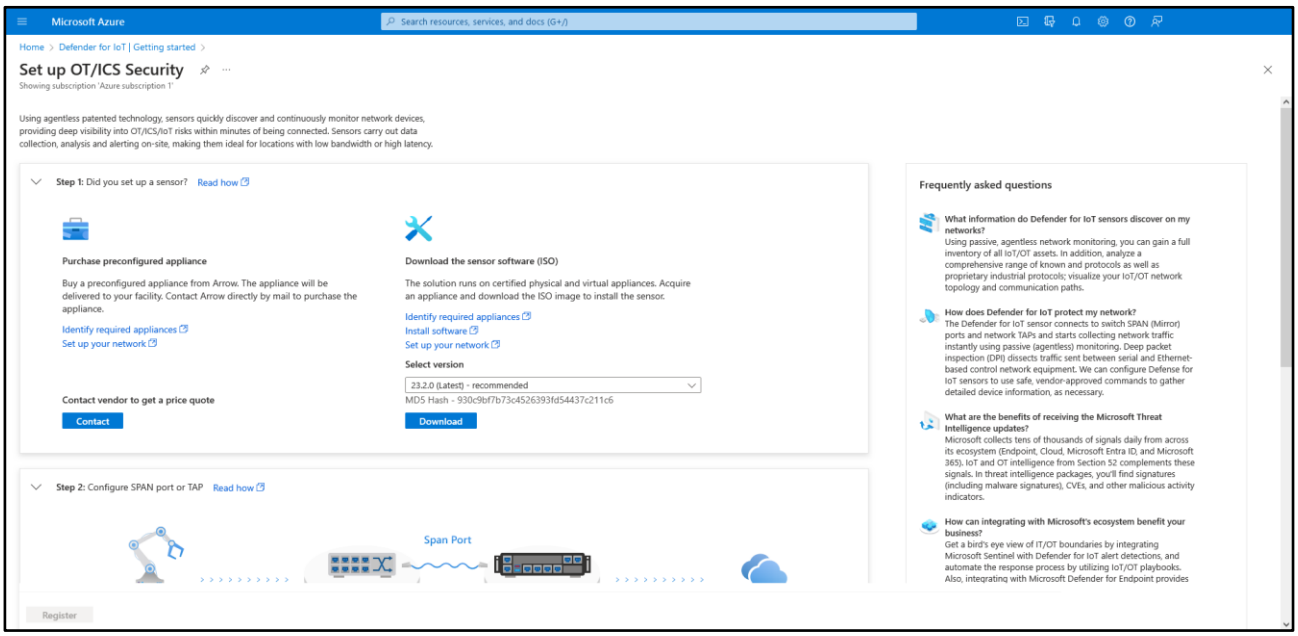


Figure 9. Screenshot of setting up OT/ICS security in Microsoft Azure

After subscription checks have been passed, Defender for IoT website then guides the user to either purchase a preconfigured appliance or as performed in this research, to download a software image file. As a precautionary measure, after downloading the installer, a MD5 checksum was generated from the downloaded file. The MD5 checksum matched between the downloaded local file and the checksum provided on the website.

```
PS C:\Users\[redacted]\Downloads> Get-FileHash .\iot-sensor_23.2.0.84583901.iso -Algorithm MD5

Algorithm       Hash
---------       ----
MD5             930C9BF7B73C4526393FD54437C211C6
```

Figure 10. Screenshot about generating MD5 checksum from the downloaded file

Powershell command “Get-FileHash .\iot-sensor_23.2.0.84583901.iso -Algorithm MD5” outputs the correct checksum.

9.6.2 Installation of Microsoft Defender for IoT

Installation was performed into a VMware Workstation 17 virtual machine. However, Microsoft's official documentation only imply support for VMware's ESXi or Microsoft's Hyper-V hypervisor platforms (Microsoft Corporation, 2023). However, in this research VMware Workstation 17 was used due to technological constraints.

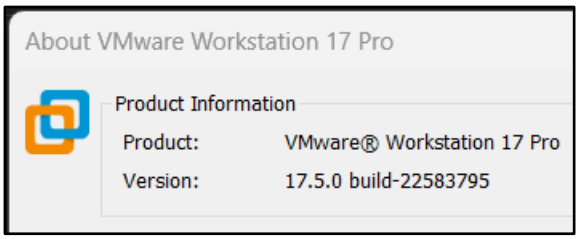


Figure 11. Screenshot of VMware Workstation version information

The virtual machine itself was configured with Ubuntu 18.04 template, with only a few modifications to the default suggested resource allocations.

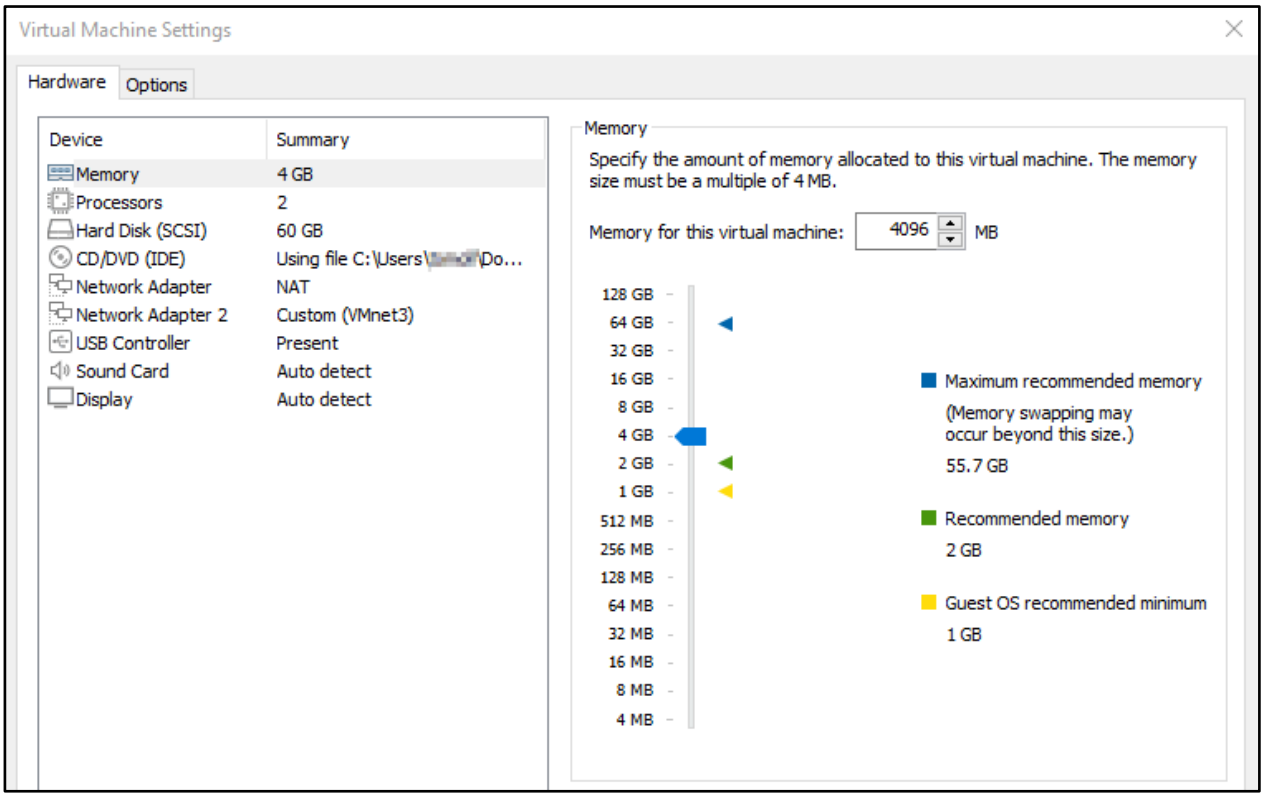


Figure 12. Screenshot of VMware Workstation virtual machine settings

The downloaded image was mounted into the virtual machine's DVD-drive, from which the virtual machine could boot the Defender for IoT sensor installer.

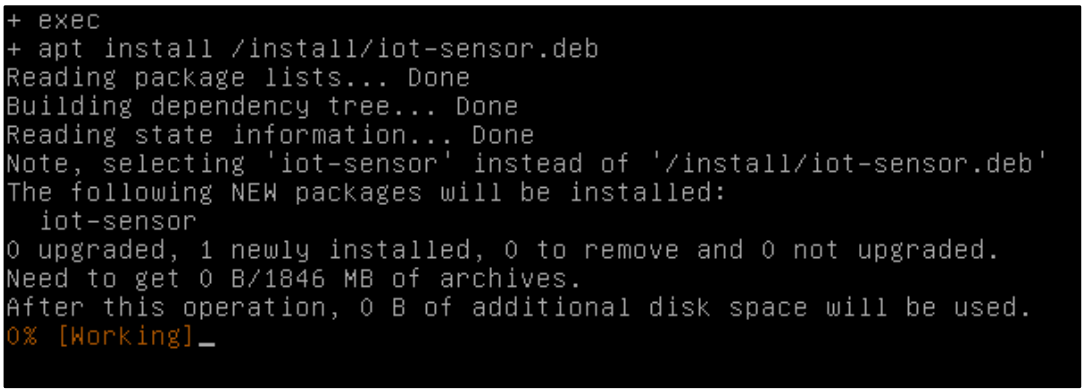


Figure 13. Screenshot of booting the installer image inside the virtual machine

The process is fully automated, requiring little to no user interaction during the installation process. The virtual machine automatically asks which attached network interface should be used for management interface and which interfaces are designated for ingesting network traffic. In a similar fashion, manual IP-address configuration needs to be set for the management interface.

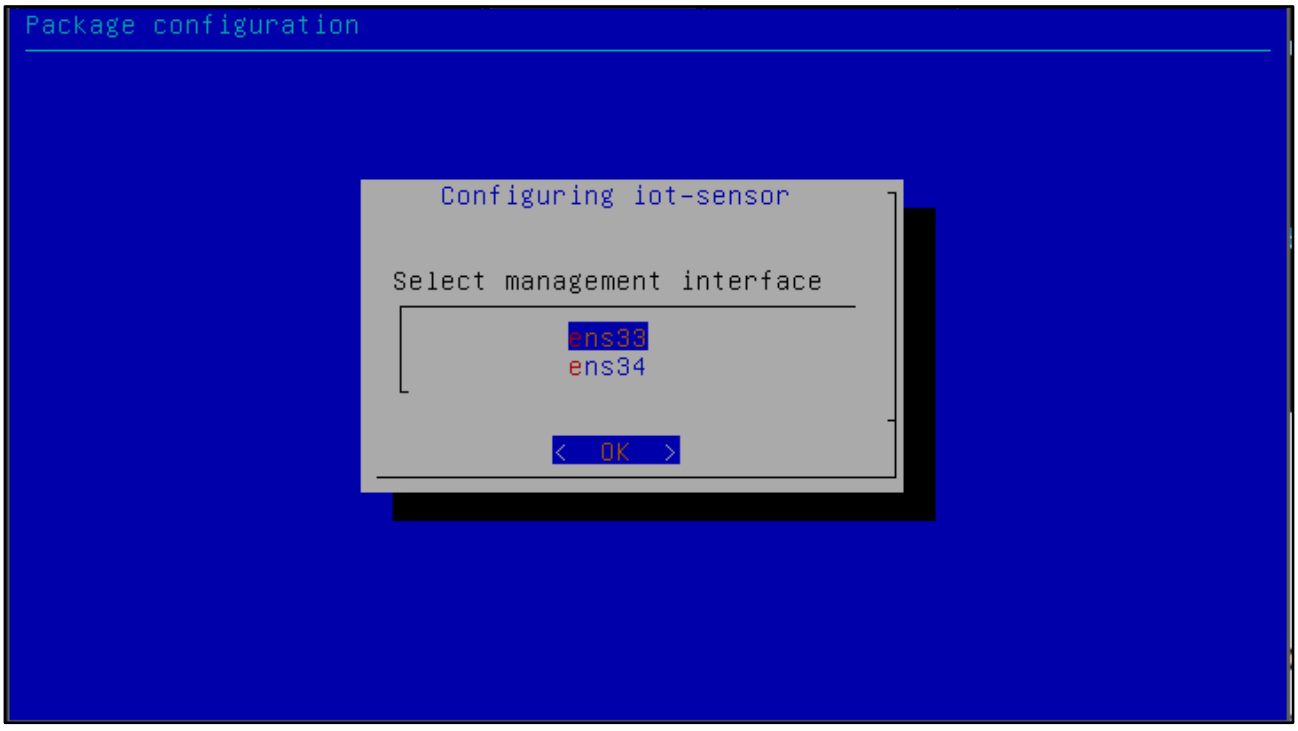


Figure 14. Screenshot of selecting network management interface

After successful installation, the virtual machine display indicates its management IP-address, subnet and gateway.

Figure 15. Screenshot about a successful installation login prompt

The workflow includes a mandatory change of administrator password which is prompted after first successful login. This is the last step of the virtual machine installation part. Further installations and configurations are done via host operating system web browser on the management IP-address displayed on the virtual machine. In this case, the IP-address is “172.16.1.21”.

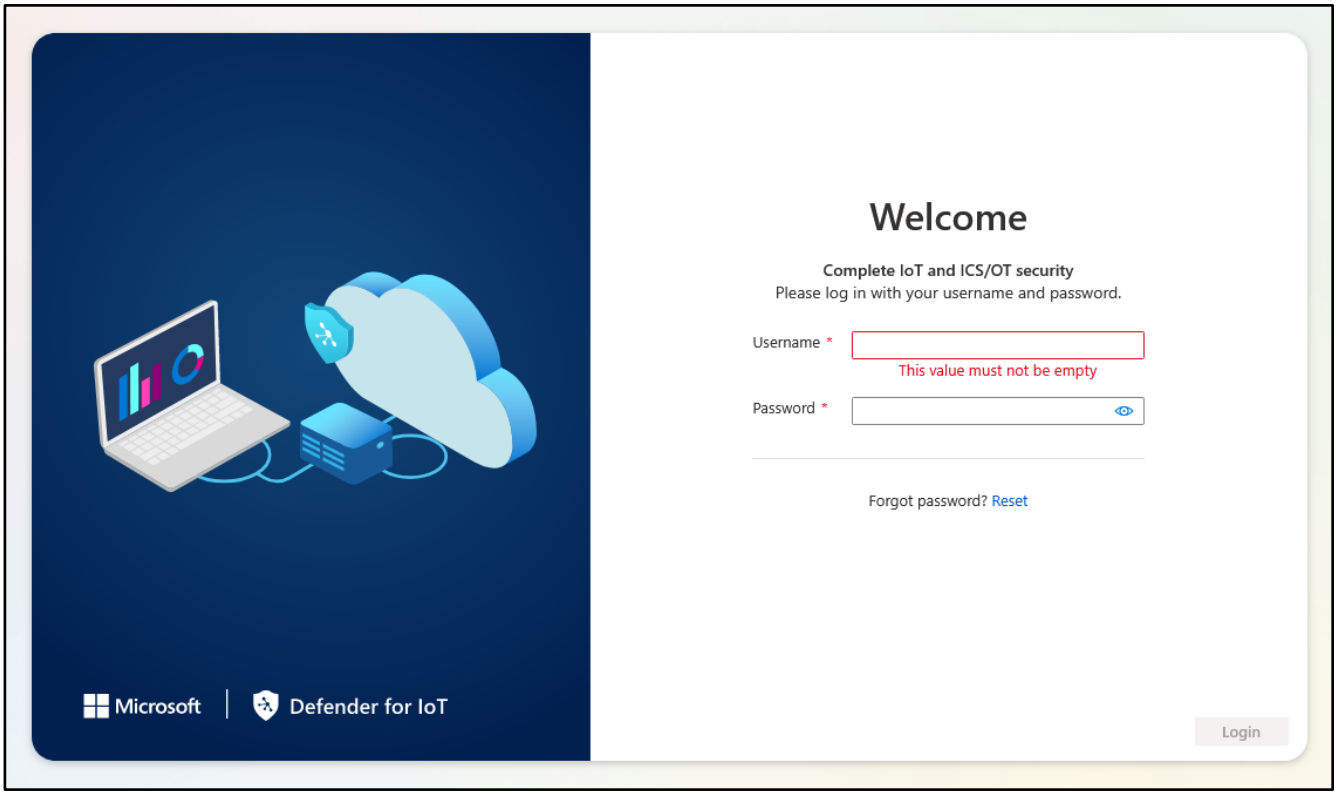


Figure 16. Screenshot of Microsoft Defender for IoT local login webpage

After logging into the website with the address “172.16.1.21”, a license activation file is requested. The license file is obtained from Microsoft Azure website.

Figure 17. Screenshot of license verification after installation

Securing communication channels between multiple sensors and Azure is typically done with certificates. In our laboratory exploratory use-case, it was decided not to use certificates.

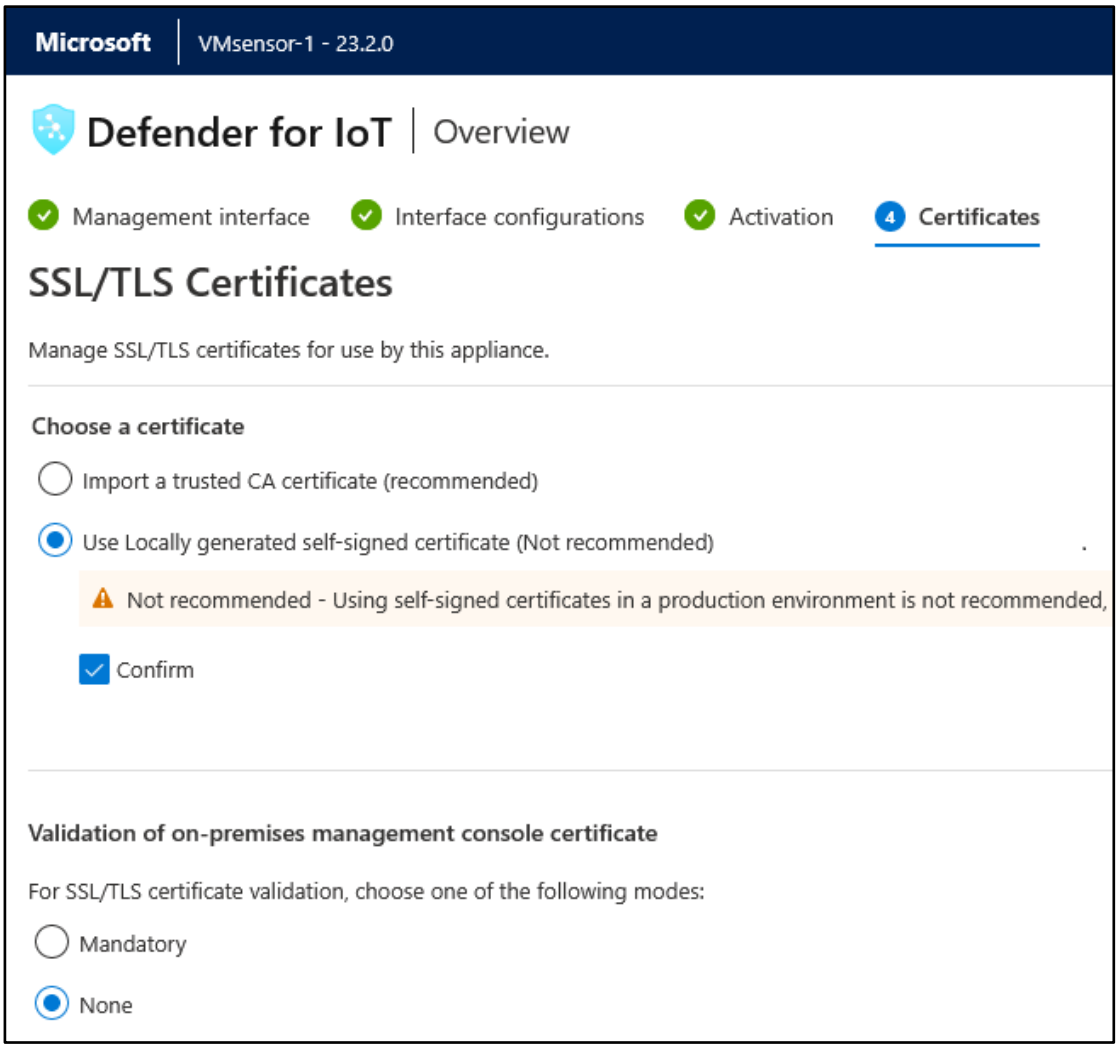


Figure 18. Screenshot of SSL certificate options during configuration phase

After the installation instance has been fully completed and configured, the user is prompted view of the main page.

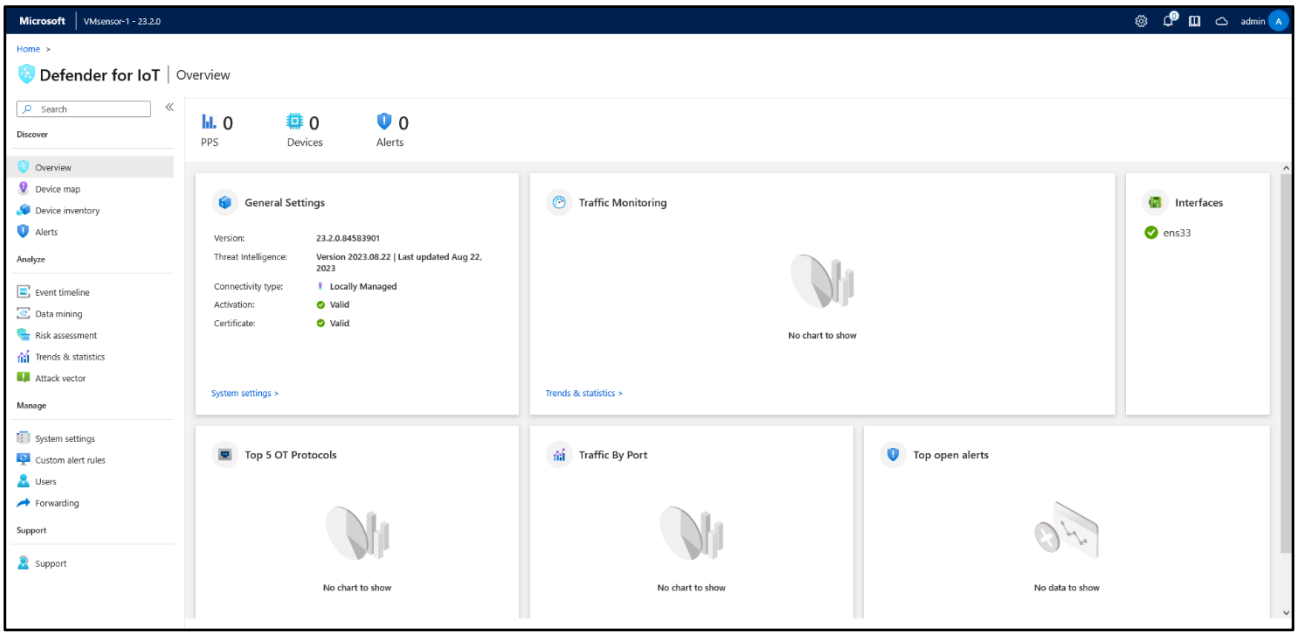


Figure 19. Screenshot about the sensor main webpage

This page should be considered to be the default starting point for any integrator when implementing the tool. This also serves as the baseline dashboard layer without any alerts or configurations. The next steps include exploratory testing of its capabilities and what the tool has to offer.

9.6.3 Replaying network capture files

The Defender for IoT has the capability to replay previously captured network packets and analyze them as if they were part of the network installation. This is specifically useful if the environment has separate, air gapped networks which have been deviated out from integrating to the network monitoring tool.

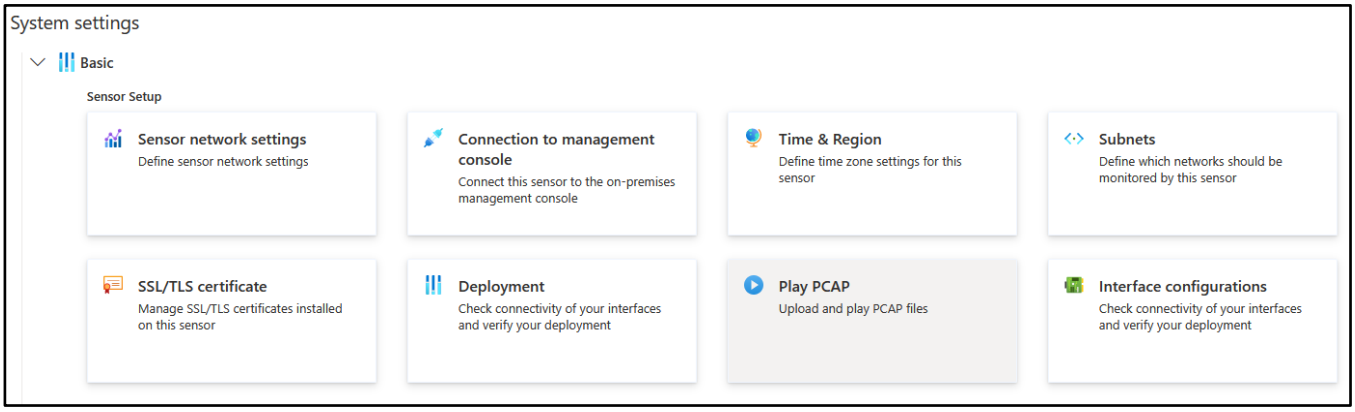


Figure 20. Screenshot about Play PCAP feature

Clicking the “Play PCAP” button opens a menu to the webpage sidebar which has the option to upload PCAP files with a maximum file size of 2 GB. After uploading the network samples, the PCAPs can be analyzed with “Play All” button. This can take surprising amount of time depending on the size of the network traffic capture. In this use case, it took approximately 40 minutes. It should be noted that virtual machine resource allocation can affect the speed of the PCAP replays.

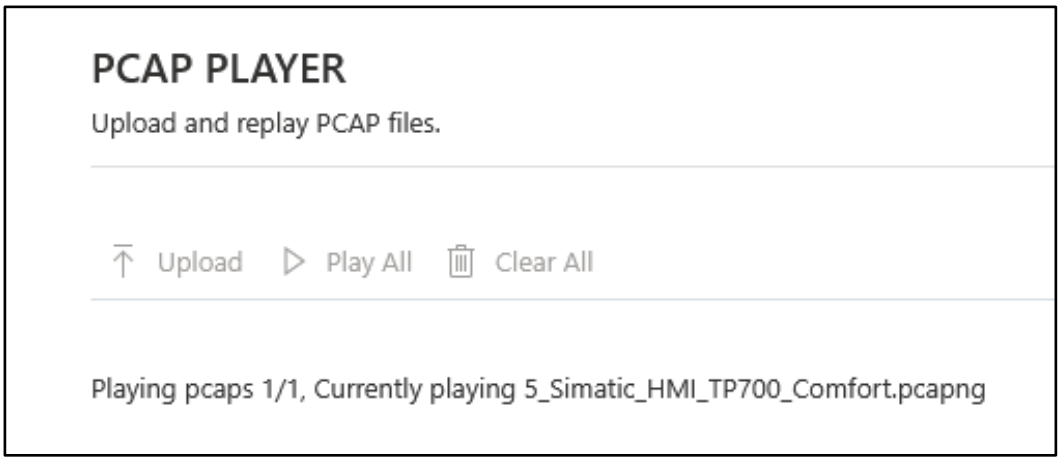


Figure 21. Screenshot of network traffic analysis in progress

After the PCAP replay has been completed, the tool is now in a ready state for performing exploratory testing. This signifies that the tool has ingested network data and is in a state which would simulate a real-world setting. The next step in this research is to perform exploratory testing of the tools capabilities and evaluate value-adding functionalities.

9.7 Review of the tool's features and outputs methods

Main dashboard indicates changes from base installation state after replaying the network traffic capture files. This view has been designed with user accessibility in mind and to include information also for non-technical persons. This view also shows alerts from baseline status to users in the network, which has been displayed in Figure 22. This overview allows for quick overview glance of the state of the environment. The view is useful for preliminary analysis. For example, in a case of a network failure, or in the event of a non-functional PLC.

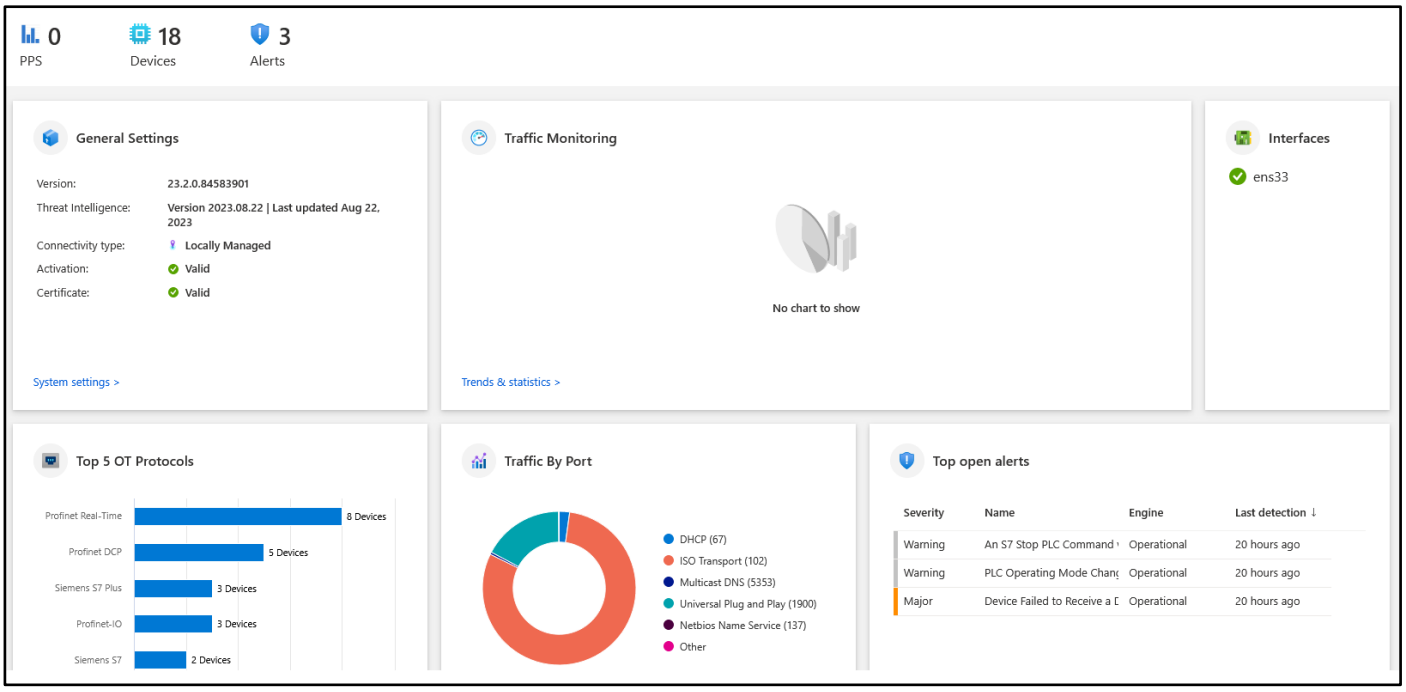
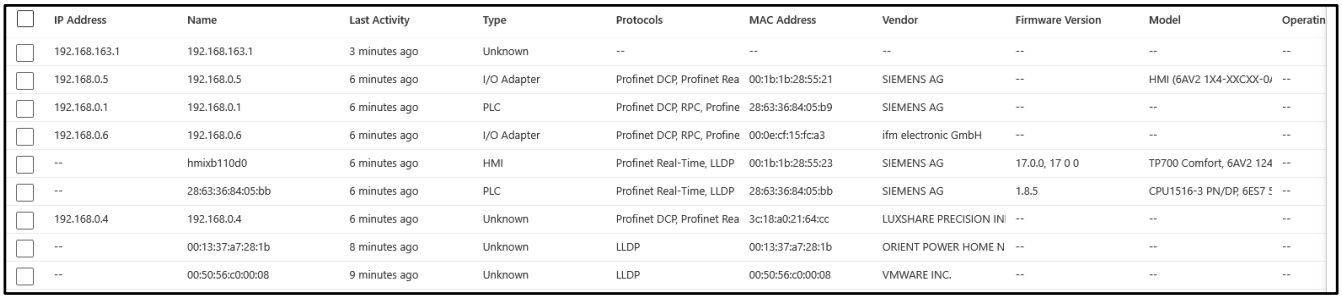


Figure 22. Screenshot of main overview page of the IoT sensor after ingesting network data

9.7.1 Asset inventory

The Microsoft Defender for IoT can function in a supportive asset inventory role. The discovered assets on the network are displayed on a separate page.



IP Address	Name	Last Activity	Type	Protocols	MAC Address	Vendor	Firmware Version	Model	Operatin
192.168.163.1	192.168.163.1	3 minutes ago	Unknown	--	--	--	--	--	--
192.168.0.5	192.168.0.5	6 minutes ago	I/O Adapter	Profinet DCP, Profinet Rea	00:1b:1b:28:55:21	SIEMENS AG	--	HMI (6AV2 1X4-XXCXX-0/	--
192.168.0.1	192.168.0.1	6 minutes ago	PLC	Profinet DCP, RPC, Profine	28:63:36:84:05:b9	SIEMENS AG	--	--	--
192.168.0.6	192.168.0.6	6 minutes ago	I/O Adapter	Profinet DCP, RPC, Profine	00:0e:cf:15:fc:a3	ifm electronic GmbH	--	--	--
--	hmixb110d0	6 minutes ago	HMI	Profinet Real-Time, LLDP	00:1b:1b:28:55:23	SIEMENS AG	17.0.0, 17 0 0	TP700 Comfort, 6AV2 124	--
--	28:63:36:84:05:bb	6 minutes ago	PLC	Profinet Real-Time, LLDP	28:63:36:84:05:bb	SIEMENS AG	1.8.5	CPU1516-3 PN/DP, 6ES7 5	--
192.168.0.4	192.168.0.4	6 minutes ago	Unknown	Profinet DCP, Profinet Rea	3c:18:a0:21:64:cc	LUXSHARE PRECISION INI	--	--	--
--	00:13:37:a7:28:1b	8 minutes ago	Unknown	LLDP	00:13:37:a7:28:1b	ORIENT POWER HOME N	--	--	--
--	00:50:56:c0:00:08	9 minutes ago	Unknown	LLDP	00:50:56:c0:00:08	VMWARE INC.	--	--	--

Figure 23. Screenshot listing seen devices on the network

Relevant information, such as IP-address, DNS names, MAC addresses and protocols that the asset has used, can be observed from the presented asset list. An approximation made by the Defender for IoT about the device type is shown at the “Model” column. This is based on device-specific network traffic metadata.

9.7.2 Integrations to third party systems

The tool has capability to forward its alerts to third party SOC or SIEM systems. The alerts can be forwarded based on the alerts severity.

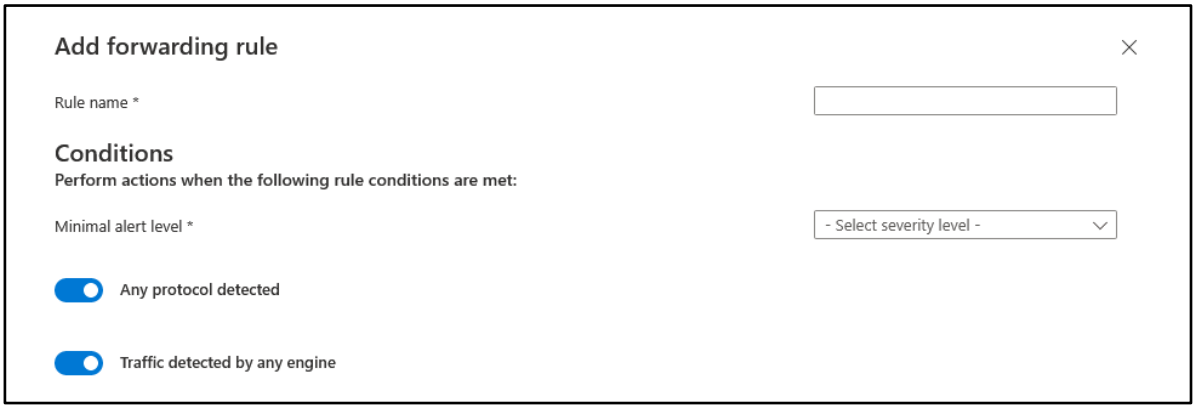


Figure 24. Screenshot illustrating forwarding configuration

In addition, custom forwarding rules can be set towards third party systems based on configurable log levels.

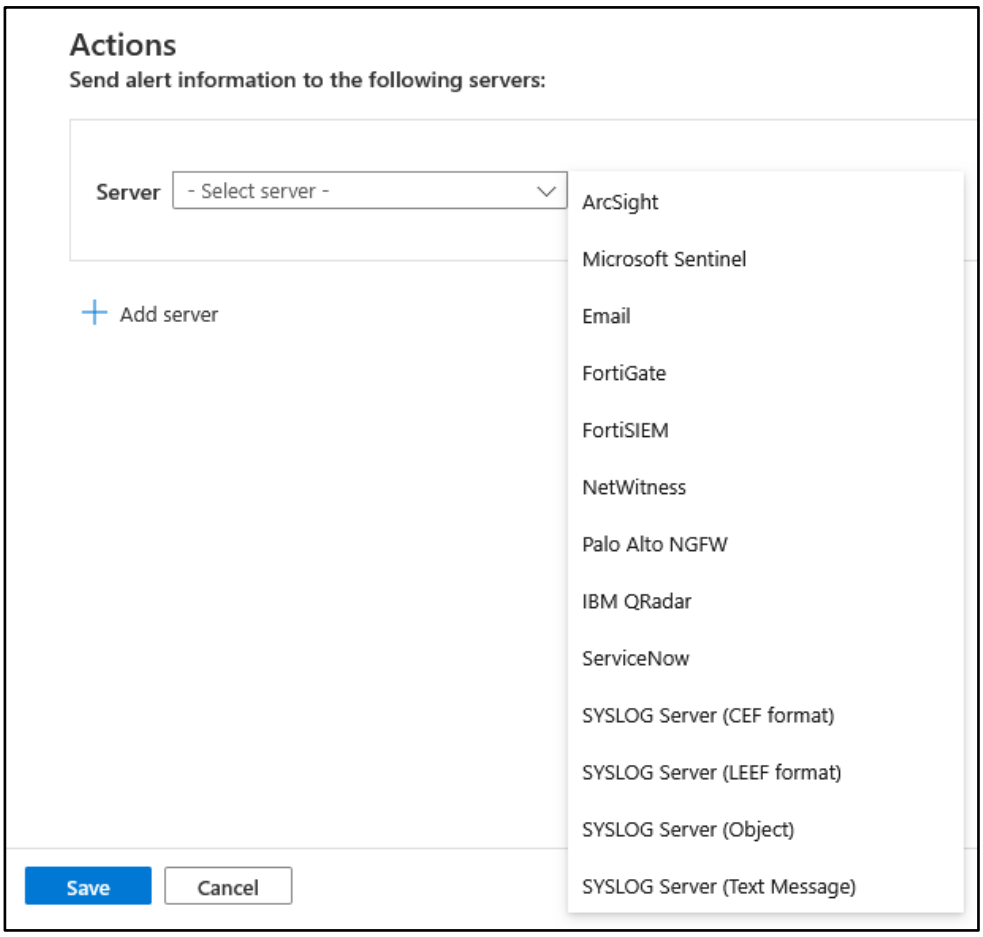


Figure 25. Screenshot about integration of forward options to different systems

Currently supported integrations to third-party systems suggests development weight behind the Defender for IoT platform. In addition, an integration to ServiceNow (an IT ticketing platform) implies that the full process in addressing any security deviations has been thought out at a business decision-making level, instead of focusing only on technical, component-level workflows.

9.8 Results on network traffic captures

The findings indicate that Microsoft Defender for IoT is a capable tool in improving an organization's cyber security resilience within network monitoring aspects. However, the tool is still clearly in the maturation phase, and all the functions were not as polished as expected. Nevertheless, the as-is state is sufficient in providing threat intelligence and visibility to assets. A remark however must be made: the tool does not provide reactive countermeasures against intrusion and is only intended to be a passive monitoring tool. Any reactive actions could potentially be configured by a proxy. For example, if a severe alert has been detected, the alert could then be forwarded to a third-party

system or a firewall, which in turn could perform automatic network-affecting actions based on its configuration. This could include for instance, shutting down Internet access at firewall level before the alert has been manually addressed.

10 Results

10.1 Functionality areas of Microsoft Defender for IoT

Results which were observed in this research in chapter 9 can be consolidated into the following Table 8. The methodologies have been separated as pages in the tool.

Table 8. Value-adding matrix

Area in Cyber Security	**Microsoft Defender for IoT specific area**	**Value-adding methodology**
- Incident response	Overview dashboard of current status.	A simple “one-stop-shop” for checking current status of OT network.
- Incident response - Disaster recovery	Integration to third party monitoring solutions.	If an organization already has SOC or alternative procedures established, the tool can then be integrated into those – no need to create tool-specific procedure.
- Asset inventory - Incident response - Disaster recovery	Integration to Microsoft Azure.	This integration option heavily targets towards using Microsoft’s cloud-based Defender. This allows visibility and a single point of view of security status for IT and OT environments alike.

Area in Cyber Security	**Microsoft Defender for IoT specific area**	**Value-adding methodology**
- Network security - Intrusion detection	Monitoring network against changes to baseline traffic.	Typically, an OT network is immutable, and no significant changes to predetermined traffic baseline is observed. Therefore, a type of whitelisting approach can be taken, and a baseline can be learned. After sufficient time, the network baseline learning mode can be turned off and any network activity that deviates from the known baseline can be configured to raise an alert.
- Asset inventory - Vulnerability management	Combining and extracting asset information seen on the network.	Microsoft Defender for IoT can extract vital information from OT field devices, such as firmware versions. This information can then further be processed when planning maintenance sessions and for example, during hardware lifecycle management. Firmware versions usually have specific Common Vulnerabilities and Exposures (CVEs) tied into them.
- Attack vectors	Identifying potentially unsafe communication pathways.	The attack vector simulation helps to identify weak links with securing network perimeter and additionally adding or modifying security controls.

10.2 Summary of value-adding functionalities

A summarized conclusion can be drawn from Table 8; Microsoft Defender for IoT succeeds in improving OT network cyber security resiliency within various different areas. However, there are some limitations which can be observed. The tool is not yet fully mature in terms of proprietary protocol support. Implementing or developing organization's own protocol support is not possible at the time of writing.

The amount of real-world value-adding functionality ultimately depends on the implementing organization. The tool has a good coverage on technical controls, but it does not provide a set of premade procedures or guidance on integrating follow-up actions within different organizational hierarchies. In addition, if budget or personnel resource allocations are not being made, the full potential of the tool can be left underutilized. The nonexistent entry cost with a 60-day trial period lowers the barrier to do exploratory testing. Comparing this to the other products on the market, Microsoft Defender for IoT did not require a monetary or NDA commitment before granting access to the tool. This was observed in Table 5 additional evaluation criteria. In a scenario where security responsible persons are tight on time and resources, the self-service approach to obtaining access to installation files can be the most enticing feature.

11 Conclusions

11.1 Evaluation of research questions

Exploratory testing produced promising results, but has the results addressed original research questions?

What tools currently exist that are viable for network monitoring in OT environments?

Current day market has tools available to address challenges in the OT network monitoring field. From the tools which are presented in chapter 7, a conclusion can be drawn that some of the initially promising tools were not in fact, network monitoring solutions. Secondary observation is that some of these tools were cloud-only based. When operating in OT environment, a mandatory Internet connectivity is not feasible for air gapped networks. These kinds of networks are not uncommon occurrence in OT field. As a note, all of the evaluated and available tools are commercial and require a license. This in turn affects the availability of information in terms of installation manuals or system requirements. These types of manuals would have been useful by providing a more comprehensive view of the tool's technical capabilities and installation procedures. Furthermore, restricted access to technical material could potentially lessen interest in a specific tool.

How does the existing tools suit specifically for OT network monitoring?

An analysis of the identified tools was conducted in order to establish a single candidate for exploratory testing. Fundamental purpose was to differentiate information technology from operational technology tools. A key observation was that only a surprisingly small number of tools were only OT focused. Majority of the identified tools focused on securing business IT related areas. Furthermore, during evaluation, some of the tools revealed to be not intended for network monitoring applications. In a single case, this manifested as an incident response first approach with the help of AI powered detection methods. During research, the core functionality of AI based detection was not well established and perhaps this can be attested to being a corporate secret. Since this research focused on tools which are purely made for network monitoring, any deviating core functionalities were left out from further investigations.

Despite the narrowing sample set, a small number of tools existed which looked promising for OT network monitoring use-cases. Since multiple tools met the initial assessment criteria, additional criteria had to be established. This enabled the focus on a single tool, which could be assessed furthermore. Overall, the tools which could be considered as OT network monitoring tools are consolidated into Table 3, since all of them met the initial assessment criteria.

Perform exploratory testing to one screened tool and verify its operational capabilities. What value-adding functionalities does the tool have? How does the tool improve organizations' cyber security maturity?

As the additional evaluation criteria defined in Table 4 singled out one potential candidate over others, exploratory testing was performed in order to obtain first-hand knowledge about the tool. The areas in which the tool improves was described in chapter 10. To summarize, the Microsoft Defender for IoT demonstrated promising capabilities with which an organization could increase their own cyber security maturity without excessive investment or overhaul of their operational technology ecosystem.

It should however be noted that in order to fully benefit from the tool provided functionalities, the information generated by the tool should be actively monitored and actions should be performed. The tool should be considered only a part of defense in depth strategy, and it should not be assumed that the OT environment is secure only by implementing a network monitoring tool. Nevertheless, it is a good step towards increasing cyber security maturity and gaining insight on what happens inside operational technology networks.

11.2 Further improvements, research, and evaluation

In order to fully establish the tools capabilities, the evaluation should be done in a real-world setting with real-world traffic outside of a laboratory environment. In addition, integration towards Microsoft organization-level tool "Microsoft Defender for Business" could be explored, in order to include alerts towards already pre-existing organizational IT workflows.

11.3 Afterthoughts

In the beginning of this research journey, it was unclear how well the tools and software could be obtained and how viable this research provided results would eventually turn out. Since operational technology is an industrial field, the availability of information is scarce by default. Network data for testing was also hard to come by due to the nature of industrial devices. Potentially procuring equipment permanently would have also been too expensive (Santiago Robles Durazno, 2021).

In retrospect, this research has indicated surprising results about available tools. During operational phase of the research, many unforeseen technical obstacles were encountered in which support was not always available. The results indicate that even though many tools advertised themselves as network monitoring tools, they are not suitable for OT-specific use-cases. Careful consideration needs to be performed on a case-by-case basis on the required functionalities. Despite these difficulties, the research questions brought forward insight into the methodology in improving network monitoring maturity level. I hope that this research can bring direction to individuals keen on improving their own cyber security capabilities.

References

ABB Oy. (2022). *Product Life Cycle Management*. https://new.abb.com/ev-charging/connected-services/product-life-cycle-management

AO Kaspersky Lab. (2020). *Kaspersky Industrial CyberSecurity: Solution overview*. https://media.kaspersky.com/en/business-security/enterprise/KICS_Solution_overview_A5_EN.pdf

Armis. (2020). *Armis Threat Detection*. https://media.armis.com/pdfs/sb-armis-threat-detection-unmanged-devices-en.pdf

Assenza, G., Cozzani, V., Flammini, F., Gotcheva, N., Gustafsson, T., Hansson, A., Heikkila, J., Iaiani, M., Katsikas, S., Nissilä, M., Oliva, G., Richter, E., Roelofs, M., Azari, M. S., Setola, R., Stejin, W., Tugnoli, A., Vanderbeek, D., Westerdahl, L., … Young, H. (2020). *White Paper on Industry Experiences in Critical Information Infrastructure Security: A Special Session at CRITIS 2019*. In S. Nadjm-Tehrani (Ed.), Critical Information Infrastructures Security (Vol. 11777, pp. 197–207). Springer International Publishing. https://doi.org/10.1007/978-3-030-37670-3_18

Barracuda Networks Inc. (2023). *Barracuda CloudGen Firewall: Datasheet*. https://assets.barracuda.com/assets/docs/dms/DS_CloudGen-Firewall_US.pdf

Carey, E. (2021). *P.R.O.V.E.N. Source Evaluation Process*. https://libguides.sbcc.edu/ld.php?content_id=51820702

Carey, E. (2023). *Fact Checking & Source Evaluation SIFT & PICK*. https://libguides.sbcc.edu/ld.php?content_id=71256269

Check Point Software Technologies Ltd. (2023, June 14). *Check Point Quantum*. https://www.checkpoint.com/downloads/products/check-point-appliances-brochure.pdf

Chen, G., Qu, Y., & Jin, D. (2022). *Cyber-Physical Simulation Testbed for MadIoT Attack Detection and Mitigation*. Proceedings of the 2022 ACM SIGSIM Conference on Principles of Advanced Discrete Simulation, 59–60. https://doi.org/10.1145/3518997.3534995

Cheung, S., Dutertre, B., Fong, M., Lindqvist, U., Skinner, K., & Valdes, A. (2006*). Using Model-based Intrusion Detection for SCADA Networks*. 12.

Cisco. (2021). *Cisco Secure Network Analytics: Scalable visibility and security analytics*. https://www.cisco.com/c/en/us/products/collateral/security/stealthwatch/secure-network-analytics-aag.pdf

Cisco. (2022, August). *Cisco Cyber Vision: Bringing unprecedented scale and simplicity to industrial security*. https://www.cisco.com/c/en/us/products/collateral/security/cyber-vision/cyber-vision-aag.pdf

Cisco. (2023, November 17). *Configuring Traffic Mirroring*. https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/en/us/td/docs/iosxr/cisco8000/Interfaces/75x/configuration/guide/b-interfaces-config-guide-cisco8k-r75x/m-configuring-traffic-mirroring-8k.html.xml

Claroty. (2023). *Data sheet: Claroty Continuous Threat Detection*. https://web-assets.claroty.com/resource-downloads/ctd-ds.pdf?external_link=true

Darktrace. (n.d.). *Industrial Immune System: Product Overview*. https://assets-global.website-files.com/626ff4d25aca2edf4325ff97/62a2996dd3dee0a0e845667c_ds-iis.pdf

Dolezilek, D., Gammel, D., & Fernandes, W. (2020). *Cybersecurity based on IEC 62351 and IEC 62443 for IEC 61850 systems*. 15th International Conference on Developments in Power System Protection (DPSP 2020), 6 pp.-6 pp. https://doi.org/10.1049/cp.2020.0016

Dragos, Inc. (n.d.). *Dragos Platform: Datasheet*. https://www.dragos.com/wp-content/uploads/Dragos-Platform-Datasheet.pdf

Etalle, S. (2019). *Network Monitoring of Industrial Control Systems: The Lessons of SecurityMatters*. Proceedings of the ACM Workshop on Cyber-Physical Systems Security & Privacy - CPS-SPC'19, 1–1. https://doi.org/10.1145/3338499.3357354

Forescout. (n.d.). *Forescout eyeInspect Data Sheet 2022*. https://www.forescout.com/resources/forescout-eyeinspect-datasheet/

Franceschett, A. L., Souza, P. R. A. D., Pereira De Barros, F. L., & De Carvalho, V. R. (2019). *A Holistic Approach—How to Achieve the State-of-art in Cybersecurity for a Secondary Distribution Automation Energy System Applying the IEC 62443 Standard*. 2019 IEEE PES Innovative Smart Grid Technologies Conference - Latin America (ISGT Latin America), 1–5. https://doi.org/10.1109/ISGT-LA.2019.8895368

Garimella, P. K. (2018). *IT-OT Integration Challenges in Utilities*. 2018 IEEE 3rd International Conference on Computing, Communication and Security (ICCCS), 199–204. https://doi.org/10.1109/CCCS.2018.8586807

Hak5 LLC. (n.d.). *Plunder Bug Lan Tap*. Retrieved February 14, 2024, from https://shop.hak5.org/products/bug

International Electrotechnical Commission (Ed.). (2013). *Industrial communication networks: Network and system security*. Pt. 3,3: System security requirements and security levels (Ed. 1.0, 2013-08). IEC Central Office.

JAMK University of Applied Sciences. (2018). *Ethical Principles for JAMK University of Applied Sciences*. https://www.jamk.fi/en/media/34826

Jung, D., Shin, J., Lee, C., Kwon, K., & Seo, J. T. (2023). *Cyber Security Controls in Nuclear Power Plant by Technical Assessment Methodology*. IEEE Access, 11, 15229–15241. https://doi.org/10.1109/ACCESS.2023.3244991

Kapoor, S., Priyanka, R., Agarwal, S., & Pradish, M. (2023). *Security Implementation Testing of Remote Terminal Unit for Power Utility*. Power Research - A Journal of CPRI, 77–82. https://doi.org/10.33686/pwj.v19i1.1126

Knapp, E. D., & Samani, R. (2013). *Applied Cyber Security and the Smart Grid: Implementing Security Controls Into the Modern Power Infrastructure*. Elsevier, Syngress.

Leander, B., Čaušević, A., & Hansson, H. (2019). *Applicability of the IEC 62443 standard in Industry 4.0 / IIoT*. Proceedings of the 14th International Conference on Availability, Reliability and Security, 1–8. https://doi.org/10.1145/3339252.3341481

Microsoft Corporation. (2023, August 2). *Install OT monitoring software on OT sensors*. https://learn.microsoft.com/en-us/azure/defender-for-iot/organizations/ot-deploy/install-software-ot-sensor

Microsoft Corporation. (2023, December 17). *Deploy hybrid or air-gapped OT sensor management*. https://learn.microsoft.com/en-us/azure/defender-for-iot/organizations/ot-deploy/air-gapped-deploy

Microsoft Corporation. (2023, February 14). *OT monitoring with virtual appliances*. https://learn.microsoft.com/en-us/azure/defender-for-iot/organizations/ot-virtual-appliances

Microsoft Corporation. (2023, November 7). *Defender for IoT billing*. https://learn.microsoft.com/en-us/azure/defender-for-iot/organizations/billing

Microsoft Corporation. (n.d.). *Microsoft Defender for IoT: Agentless IoT and OT security, integrated with Microsoft SIEM and XDR*. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWWsxj

Mukherjee, A. (2020). *Network Security Strategies Protect Your Network and Enterprise Against Advanced Cybersecurity Attacks and Threats*. Packt Publishing, Limited.

Nozomi Networks Inc. (2020). *Guardian: Industrial Strength OT and IoT Security and Visibility*. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vq2k

Ordr. (n.d.). *Solution Brief: Ordr Overview*. https://resources.ordr.net/resource-center/ordr-overview

Palo Alto Networks. (2022). *Realizing Cybersecurity Value: The Business Benefits of Palo Alto Networks Platforms*. https://start.paloaltonetworks.com/rs/531-OCS-018/images/platform-approach.pdf

Patton, M. Q. (2015). *Qualitative research & evaluation methods: Integrating theory and practice*. SAGE Publications, Inc.

Quade, P. (2018, February 19). *You Can't Protect What You Can't See*. https://www.csoonline.com/article/564627/you-cant-protect-what-you-cant-see.html

Radvanovsky, R. (2013). *Handbook of SCADA/control systems security*. CRC Press.

Renaud, K., & Ophoff, J. (2021). *A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs*. Organizational Cybersecurity Journal: Practice, Process and People, 1(1), 24–46. https://doi.org/10.1108/OCJ-03-2021-0004

Sandler, A. (2008, May 18). *Tcpdump for Dummies*. http://www.alexonlinux.com/tcpdump-for-dummies

Santiago Robles Durazno, A. (2021). *Industrial Control Systems Cybersecurity Analysis and Countermeasures* [Edinburgh Napier University]. https://napier-repository.worktribe.com/output/2848612/industrial-control-systems-cybersecurity-analysis-and-countermeasures

SCADAfence. (n.d.). *OT Security. At Scale.: Securing Your Industrial Digital Transformation Journey*. https://www.scadafence.com/wp-content/uploads/2020/04/SCADAfence_CO_Overview_Web_ENG.pdf

Smokescreen. (n.d.). *Deception Defence Platform: Solution Document*. https://spiresolutions.com/wp-content/uploads/2020/08/Smokescreen-Network-Endpoint-Deception-Solution.pdf

Staves, A., Maesschalck, S., Derbyshire, R., Green, B., & Hutchison, D. (2023). *Learning to Walk: Towards Assessing the Maturity of OT Security Control Standards and Guidelines*. 2023 IFIP Networking Conference (IFIP Networking), 1–6. https://doi.org/10.23919/IFIPNetworking57963.2023.10186424

Tenable Inc. (2022). *Tenable OT Security 3.13 User Guide*. https://docs.tenable.com/PDFs/OT-Security/Tenable_OT_Security-User_Guide_3_13.pdf

Verve. (2020, November). *Verve Security Center*. https://verveindustrial.com/wp-content/uploads/2020/11/Verve-Security-Center-data-sheet-Verve-Industrial.pdf

VMware Inc. (2023). *VMware Carbon Black XDR™: Strengthen lateral security and unify security tools to see more and stop more*. https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/support/vmw-carbon-black-cloud-service-description.pdf

Weiss, J., Stephens, R., & Miller, N. (2022). *Changing the Paradigm of Control System Cybersecurity*. Computer, 55(3), 106–116. https://doi.org/10.1109/MC.2021.3138231

Wireshark. (n.d.). *Chapter 1. Introduction*. Retrieved February 14, 2024, from https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html

Yiapanis, A., & Mazzola, A. (2023). *Opinion of the European Economic and Social Committee on the Joint Communication to the European Parliament and the Council: EU Policy on Cyber Defence*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022IE5106