Tampereen ammattikorkeakoulu

Exploring Network Detection and Response Technologies

Understanding the Role of Network Detection and Response and Comparing Features of Available Products

Aino Syrjälä

OPINNÄYTETYÖ
Elokuu 2023

Tietotekniikan tutkinto-ohjelma
Tietoliikennetekniikka ja tietoverkot

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietotekniikan tutkinto-ohjelma
Tietoliikennetekniikka ja tietoverkot

SYRJÄLÄ, AINO:
Katsaus verkon havainnointi- ja puolustusteknologioihin
NDR-teknologian tarpeen ymmärtäminen ja tuotevertailu

Opinnäytetyö 40 sivua, joista liitteitä 1 sivua
Elokuu 2023

Nykypäivänä monet tietoturvan uhkakuvat liittyvät tietoverkoissa tapahtuviin hyökkäyksiin. Vastauksena tähän markkinoille on tullut monia verkkoliikenteen valvontaan liittyviä tuotteita, jotka hyödyntävät tekoälyä ja koneoppimista perinteisten sääntöihin ja indikaattorien havainnointiin perustuvan valvonnan lisäksi. Tämän työn tarkoituksena oli selvittää, miten verkkoliikenteen valvontatyökalut (NDR) mahdollistavat paremman tilannekuvan kyberoperaatiokeskukselle ja miten eri tuotteita voi vertailla keskenään. Työ tehtiin Insta Advance Oy:n tilaamana.

Työssä selvitettiin, miten NDR-tuotteet toimivat ja luovat lisää informaatiota muiden tietoturvatyökalujen rinnalla. Lisäksi työssä käsiteltiin erilaisten verkkoympäristöjen tarpeita IT- ja OT-verkkoympäristöjen osalta. Työhön valikoitiin kaksi IT-verkkoihin erikoistunutta ja kaksi OT-verkkoihin erikoistunutta tuotetta. Tuotenimet on sensuroitu ja toimitettu ainoastaan Installe tilaajan toiveesta. Tässä työssä vertailu keskittyi tuotteiden toiminnallisuuksien vertailuun. NDR tuotteiden toiminta pohjautuu verkon tuntemiseen ja normaalista toiminnasta poikkeavan toiminnan havaitsemiseen. Tarpeeksi monipuolisen verkkoliikenteen tuottaminen laboratorioympäristössä olisi ollut haastavaa, joten tuotteiden käytännön vertailu jätettiin tämän työn ulkopuolella tuotantoympäristössä suoritettavalle testijaksolle.

Työn tuloksena todennettiin NDR-tuotteiden asema osana kattavaa kyberturvallisuusvalvontaa. Ratkaisut täydentävät omalta osaltaan tietoturvan tilannekuvaa luoden uusia havainnointi- ja reagoimismahdollisuuksia. Lisäksi työssä esitellään tapoja sopivan tuotteen valintaan.

Asiasanat: ndr, kyberturvallisuus, soc

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in ICT Engineering
Telecommunication and Networks

SYRJÄLÄ AINO:
Exploring Network Detection and Response Technologies
Understanding the Role of Network Detection and Response and Comparing Features of Available Products

Bachelor's thesis 40 pages, appendices 1 pages
August 2023

This work was done for Insta Advance Oy to explore available Network Detection and Response (NDR) solutions. First focus was on how NDR systems can provide broader visibility and new response options for the Security Operation Centers. This was done by evaluating how NDR system can provide additional information to existing security solutions. Considerations were also made on different requirements for IT and OT environments.

This work addresses the question of how to compare different NDR products. Two products focused on IT and two products focused on OT were chosen for comparison. Product names were censored in this work and provided only for Insta. This work concludes results from feature comparisons but unfortunately does not include proof of value evaluations of the products. NDR products working principles rely on learning the network they are monitoring which makes it hard to replicate a complex enough network reliably in lab environment. For this reason, products were not tested in lab environment and proof of value evaluations were left for later when they can be done in actual enterprise network.

As a result, this work shows the need for NDR solutions for providing better visibility over infrastructure for security operations. It also provides things to consider when looking for the right product for the environment.

Key words: ndr, soc visibility, cybersecurity

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

C2	Command and Control
EDR	Endpoint Detection and Response
ICS	Industrial Control System
IDS	Intrusion Detection System
IoT	Internet of Things
IPS	Intrusion Prevention System
IT	Information Technology
NDR	Network Detection and Response
NIDS	Network Intrusion Detection System
NTA	Network Traffic Analysis
OT	Operational Technology
SIEM	Security Information and Event Management
SOAR	Security Orchestration, Automation and Response
SOC	Security Operations Center
XDR	Extended Detection and Response

1 INTRODUCTION

As there are more and more interconnected devices and systems in today’s digital world, the importance of network security is ever increasing. The organizations need to act against the potential cyber threats and Network Detection and Response (NDR) systems are a crucial tool for the defenders in the fight against these threats.

NDR systems are used for monitoring the network traffic and to detect any anomalies that could be an indication of an attack. The traffic data is analyzed in real-time using machine learning algorithms and behavioral analytics that traditional signature-based tools or other security tools like Endpoint Detection and Response (EDR) systems working on the host may miss. Some NDR systems even offer the possibility to automatically respond and mitigate threats with integrations.

The need for better visibility and more capable tools has increased in recent years as the cyber threats have become more sophisticated and widespread. In addition to threats with known signatures, there are also unknown threats called zero-day attacks. With the right tools these can be recognized from the attack pattern or anomalous behavior. Attack surface is also increasing with more devices connected to networks. Bring your own device (BYOD) policies increase the variety of different devices being used. There are also increasing number of IoT devices connected to networks. With all this it is getting harder to monitor all the individual devices separately but monitoring the network can make it easier to notice when something is acting maliciously.

Considering these factors, NDR system could prove to be an essential component in every organization’s cybersecurity strategy by providing the additional layer of visibility and detection opportunities. When the right solutions are used the time to detect and respond to threats is minimal and the potential threats for data or processes are mitigated. In first part of this work, we will explore the current network threats and examine the role of NDR in mitigating them and on the second part we will go through how to compare different NDR products that are available.

2 BETTER VISIBILITY WITH NETWORK MONITORING

2.1 Detection

There are many things to consider when working with cyber security. Different frameworks and certifications guide on what and how to protect. National Institute of Standards and Technology (NIST) has developed one important framework. Their cybersecurity framework's core consists of five functions: Identify, Protect, Detect, Respond and Recover. [1] For this work two of these, Detect and Respond, will be considered. Defenders need to detect and identify the cybersecurity events as they occur and in order to do that they need to implement and maintain monitoring capabilities. When the event is detected, defenders need to act on the detected event and mitigate the damage that the event causes. This framework describes different aspects of implementation through categories and subcategories to consider.

For example, NIST Cybersecurity Framework there are three categories for detection. Anomalies and Events (DE.AE) is for detecting anomalous activity and understanding the impact of these events. First subcategory for this is DE.AE-1 is a requirement for baseline of network and expected dataflows. [1] NDR solutions are built to create a baseline of the network during the learning period and finding anomalies from baseline activities. Second detection category is Security Continuous Monitoring (DE.CM) and a subcategory for this is DE.CM-1 network monitoring to detect potential cybersecurity events. [1] This requirement can be fulfilled by deploying NDR solution. Another subcategory where NDR solution can be useful is DE.CM-7 which requires that there is monitoring for unauthorized personnel, connections, devices, and software. [1] Third category is Detection Processes (DE.DP) including a reason to deploy NDR as subcategory DE.DP-5 requires that detection processes are continuously improved.

2.2 SOC visibility triad

Gartner described the SOC visibility triad in 2019 and included network detection and response as one of the three main tools of a modern SOC [2]. There are three main components in the triad: SIEM/UEBA, NDR and EDR as presented in Figure 1.

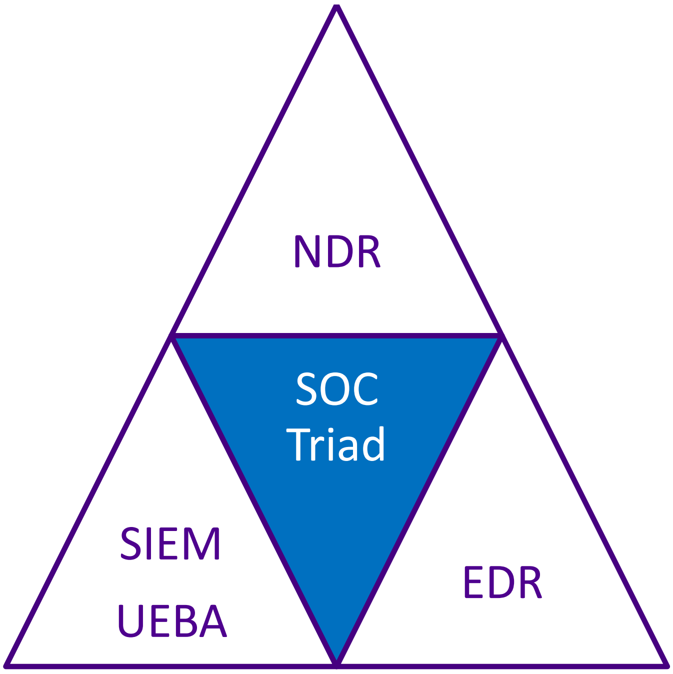


Figure 1. SOC Visibility Triad

Security Information and Event Management (SIEM) is the one of the main tools of the security operations center. The security related logs, like syslog or windows event logs, are collected across the organizations IT environment and fed to SIEM. SIEM is a tool for event analysis. The collected event data is normalized, categorized, and stored. SIEM detects the possible threats and informs the analyst of those events. Detections can be based on indicators of compromise in certain events or correlation rules that combine activity from several events such as multiple failed login attempts for same user or IP address. [3] On the same corner there is also User and Entity Behavior Analytics (UEBA). This is used to enhance the information gathered from logs by using machine learning to create a baseline and detect anomalies from it.

Second part of the triad is Endpoint Detection and Response (EDR) which is a technology for detecting malicious activity on endpoints such as user laptop or a server. EDR provides visibility to privileged access, accessed files and running processes on the endpoints. EDR can also be used for incident response to limit the impact of the malicious activity by isolating the host for example. Endpoints are important source for gaining visibility for cyber threats because they are a frequent entry point for an attacker. EDR differs from regular antivirus solution in a way that it focuses more on the behavior while antivirus relies on signatures of known attacks. [4] This aspect of behavioral analysis makes it possible to detect previously unknown threats as well. EDR solution can detect threats from all the stages of an attack lifecycle by continuously monitoring and correlating endpoint events. In addition to detection, EDR system provides response features such as isolating the endpoint or killing malicious processes.

Third part is the Network Detection and Response (NDR) which monitors network traffic in real time. One challenge related to monitoring logs and host activity is that they do not always reveal the malicious actions, or they might even be turned off or tampered by the attacker. Even if that happens there are very few attacks that would not need to communicate in any way via network and that is where NDR takes place. NDR system analyses network traffic and can recognize anomalous traffic by analyzing traffic patterns even if it uses encrypted tunnels. NDR can utilize signatures to identify malicious traffic, but the focus is on behavior based or machine learning solutions.

Together these are providing the defenders better visibility to the infrastructure than using only one or two of the three. Different tools can show attackers actions in different parts of the attack timeline. When malicious activity is detected with one of the tools, then analyst can correlate the events with other sources of telemetry.

2.3 Cyber threat landscape

The landscape of the cybercrime is in continuous change and identifying current and future threats can be hard. The European Union Agency for Cybersecurity (ENISA) has published yearly their Threat Landscape report where they try to identify the top threats, threat trends and attack techniques. ENISA’s report from year 2022 identifies eight prime threats and most of them can be linked to network traffic. One of the interesting ones for NDR is the supply chain attacks. In supply chain attack the first attack target is the organizations supplier. Then the second attack is done against the company using the supplied software. [5] These attacks are done with the certain final company in mind. There is also a similar exploitation method where there was no specific final victim, but the attacker uses a vulnerability for example in a developer library like in the Log4j case where the vulnerability was in widely used Apache logging library [6]. NDR can be used to detect these when there is attack activity over network.

The key trends show that use of zero-day exploits is on the rise, because there are better defense strategies against known vulnerabilities, which means that the attacker needs to find new ways to exploit systems. In 2021 the number of disclosed zero-day exploits was at all-time high reaching 66 cases. [5]

Both trends mentioned here are such that even though there is not known signatures or ways to prevent the unknown attacks. The NDR solutions are tackling these with machine learning and teaching it to learn what is normal traffic in the network and teaching what are the traces that certain attack types leave even when they are using previously unknown method.

2.4 Cyber kill chain

Cyber kill chain is a framework developed by Lockheed Martin that explains the steps that attackers take while moving through the network and identifying vulnerabilities to get to their targets [7]. The stages of the kill chain are shown in Figure 2. This tool can be used to identify the phases when NDR solutions can detect and prevent attacker activity.

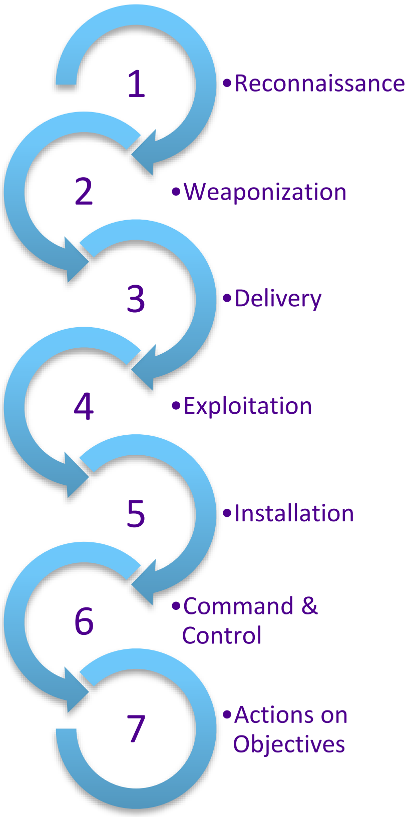


Figure 2. Cyber Kill Chain

Attacks begin with reconnaissance phase, when attacker collects information like email addresses and identifying potential targets or finding vulnerabilities. Then follows the weaponization stage where attacker prepares the weapons like modifying existing ransomware or creating malware for the attack. Third phase is delivery. In this stage attacker delivers the weapons via phishing email or uses a vulnerability to gain access into organizations network. After the initial access, the delivery the exploitation begins. In this stage attackers take advantage of their access and often proceed with lateral movement further into the network to reach their actual targets.

After the attacker gets access to their target, they start the installation phase. In this stage attacker tries to install their tools and take control of the system and exfiltrate data. Relating closely to the previous step the attack then continues with command and control when their malware on target communicates with the command and control (C2) server to receive commands what to do next. Last phase is actions and objectives. When attackers have their tools inside the network and they have control over it, they can execute their objectives that depend on their objectives like steal sensitive data, install ransomware for extortion or just use it as part of a botnet for DDoS attack.

During phases 3-7 NDR can be used to identify the malicious traffic related to the attack. In the model attackers succeed only if they get all the way through to the chain and reach their objectives in stage 7 [7]. Understanding the attacker's actions in different stages is the key for the defender's success by preparing proper detections and preventions through the chain. Adding the information about attack stage into the detected event can help to identify criticality of the event and help prioritizing events.

2.5 OT considerations

Main difference in monitoring IT and OT networks is that the devices use different protocols to communicate. OT or ICS network is partly shared with the IT network and that traffic could be monitored with the same processes and techniques for detecting threats and anomalies as in traditional IT network but going down the levels of Purdue model the protocols and requirements for detection and response change. Nowadays control systems could have ethernet or even IP connection and communicate with it but older devices will use process specific protocols. CAN bus or Modbus are some of the common communication protocols in industrial automation networks.

Another challenge is high availability requirement. These devices have limited resources only for their functionality and their lifespan is supposed to be very long: devices can be used in operation for decades. [8] For these reasons there is not resources to run anything extra and the risk of interruption is too high. The monitoring system cannot interfere with the systems or their network connectivity to keep the process going and real-time communications running. This means that only passive monitoring is a viable solution.

Then it comes to what is the main benefit from the NDR system in the OT: visibility, vulnerabilities, threats, or responses? Sometimes the starting point in OT security is getting information about all the assets and devices so that the information can be used to determine what are the most important systems and how they connect to other systems. Also knowing the assets allows determination of vulnerabilities related to those. In OT environment maintenance windows are limited and everything cannot be patched easily even when there is firmware update available. Knowing what is vulnerable and how it connects to other systems can help determine how to mitigate risk related to the vulnerability if it cannot be patched immediately. Detecting threats is one of the main reasons why to deploy NDR in OT environment, but sometimes the main benefit might come from learning the weaknesses of the environment when assessing the devices and systems in the environment, so the detections are done where they are needed.

The responses NDR can do in the OT environment are limited. The process should not be interrupted even when there is alert of suspicious activity. Locking an operator out of the system when the user account has several incorrect password attempts can create unsafe situation if they cannot access the systems. If there is a solution to block the malicious activity and keep the normal activities running it would be great, but most of the time responses need to be manual or they should require approval from the analyst to ensure the production will not be disturbed.

2.5.1 Purdue Model

Purdue model was developed in the 1990s [9] and the modified versions are still in use to describe the segmentation between layers of the OT network. The border between IT and OT may not be this distinct in all cases, but the model is still useful. One presentation of this model is available in appendix 1.

In this model the ICS network consists of IT and OT networks separated with a demilitarized zone (DMZ). On IT side there is Enterprise Zone that includes levels 4 and 5 of the model. Level 4 is the Business logistics consisting of systems like ERP that handles things like production schedule, inventory and shipping. Level 5 is the Enterprise network that is not really an ICS environment but data from the ICS systems is being collected and used for business decisions handled on enterprise network.

Below the demilitarized zone (DMZ) there is the OT network. Cell/Area zone can be presented as its separate zone below the manufacturing, or it could be included inside the manufacturing zone. Manufacturing zone consists of level 3 activities like managing and maintenance systems. Cell/Area zones are grouping ICS devices like different production lines can form their own cells. In this zone there are typically three levels of activity. On level 2 there are Engineering Workstations, systems for Human-Machine Interfaces (HMI) and for Supervisory Control and Data Acquisition (SCADA). Going down on level 1 there are programmable logic controllers (PLC) that direct the manufacturing process. Then on the bottom there is the physical processes on level 0 where the pumps or motors do the key functions of the manufacturing for example. [8]

2.5.2 ICS Cyber Kill Chain

The traditional Cyber kill chain from Lockheed Martin does not consider the details of the industrial networks and it needs to be extended for the ICS. One of the developed models extends the kill chain to have three layers where the External Kill Chain is used to invade the enterprise network, and this can be described with the Lockheed Martin's Cyber Kill Chain [7]. First addition to this is the Internal Kill Chain that describes the phases to reach the industrial control systems via internal reconnaissance, privilege escalations and lateral movement. This is common for most objectives of ICS attacks. Second addition is the ICS kill chain or target manipulation kill chain that is object specific and targets a specific ICS to launch attack on certain production process. [10]

To consider NDR from this perspective it can be deployed to the IT network side and the attacker's actions can be detected before the attack moves further into the internal kill chain or ICS kill chain. The probability of an attacker to do their attack from this route of first gaining access to company's enterprise network is higher than them getting physical access to site and the devices behind locked doors. This does not mean that the OT network should not be monitored, but assessing the risk related to these different ways of attacks is something to consider while choosing the defense solutions.

3 OPERATING PRINCIPLE OF NDR

3.1 From Signatures to Behavior Monitoring

Monitoring and analyzing network traffic is not a new idea. Different kinds of detection solutions have been around for decades, but only in the recent years term NDR has emerged. NDR is like the traditional signature-based intrusion detection and response systems, but there are some key differences.

Traditionally the detection and prevention solutions in the network relied on existing rules and indications of compromise (IOC) signatures. This method of detection is referred as Intrusion Detection System (IDS) or NIDS to emphasize the network. IDS products focus on detecting and alerting of potential threats and Intrusion Prevention System (IPS) products are designed to prevent and block threats. NDR systems try to do both, but the available respond methods vary between products and what other technologies are being used and how well the systems can integrate.

In 2020 Gartner defined the term Network Detection and Response as a product that detects abnormal system behaviors by applying behavioral analytics to network data. [11] Solutions can be physical or virtual sensors that continuously analyze the raw network packets or their metadata. They can be implemented to monitor traffic between internal networks (east-west) and traffic between internal and public networks (north-south). The response part of NDR should involve automated responses such as blocking the anomalous traffic or isolating the host from rest of the network as well as storing the packet capture for forensics.

NDR is mainly used to identify post breach activity such as lateral movement or C2 traffic, but it can also notice insider threat actions such as employee tries to exfiltrate data after receiving notice that their contract is being terminated. NDR complements the signature-based solutions but ideally it has the signature detection capabilities included. Signatures are still needed for compliance reasons. Customer may require that disclosed CVEs are detected and the fastest and cheapest way to detect is with signatures related to the CVE. Signatures can also be used for effective threat hunting.

3.2 Machine learning approaches

Different attacks require different models and algorithms for detection. Supervised learning can be used to train algorithms to recognize known threats from patterns in the network traffic. In this technique the training data has been labeled so that the outcome of the traffic is known. Packets are tagged as normal, malicious, or suspicious. They can also be tagged based on the used application or protocol. In the learning phase algorithm associates specific features and patterns with the corresponding labels. After that the algorithms can identify patterns and relationships related to normal traffic as well as the indicators of various types of threats such as malware or denial-of-service in real environments and packets they have not seen before. One technique that works like this is classification algorithms such as K-nearest Neighbor (KNN). Algorithm is trained with labeled data that can consist of labels for normal or attack events or there can be multiple classes for different attacks. [12] Visualization of these two types of classifications is presented in Figure 3.

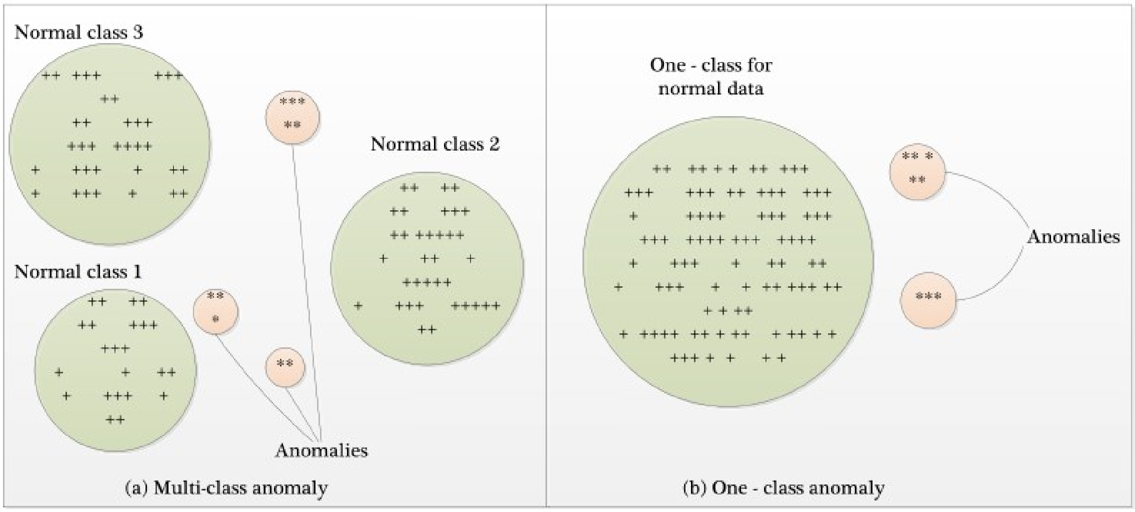


Figure 3. Classification algorithm visualization. [12]

Unsupervised learning is a machine learning technique in which the training data has not been labeled. Algorithms can use techniques to cluster packets based on similarities in their protocols, payloads, sources, or destinations. This can be used to identify patterns without the knowledge of attack patterns or labels. [12] Anomalies can also be found with unsupervised learning. If there is a deviation from the expected patterns of the normal behavior, it can be detected. These methods can be useful to identify anomalous network activity that could indicate a potential threat. This approach is useful for detecting unknown threats like zero-day attacks, because algorithms can find the anomalies in the traffic that could indicate a threat even when there is no existing signature or label related to that specific anomaly. There is still need of specialists to analyze and identify the clusters and anomalies unsupervised learning produces, but it makes it possible to find threats without prior knowledge of them.

Semi-supervised learning can be used to refine the detection results. This is a combination of the previous practices. In semi-supervised learning the algorithm is first trained with a small amount of labeled data. This is the supervised period. After that training is continued with unlabeled data like in unsupervised learning. The amount of labeled data needed is lower, because only part of the learning is supervised. This also means it can be more cost effective because less work is needed to produce the labeled dataset.

Deep learning uses neural networks to analyze complex patterns in large amounts of data. In NDR context this method can identify unique characteristics of the threats, even though deep learning cannot always point precisely to which feature in the data triggers detection. Still this approach can have a better recognition compared to statistical models. C2 traffic is one example where deep learning is useful. AI Behind Vectra AI describes the usage of LSTM (long short-term memory) to identifying the C2 attack behavior [13]. An example of this is described later in section 3.4.3.

NDR working principle is based on using multiple machine learning techniques to process network data. This can be visualized like in the Figure 4. [14] First network data is collected. This can differ from solution to solution, but data can include PCAP-files, collected flows and metadata. Then the data is fed to multiple machine learning algorithms for processing. Then it produces intel for the analysts like the detected anomalies and suspicious activities and offer some automated responses to mitigate the attack.

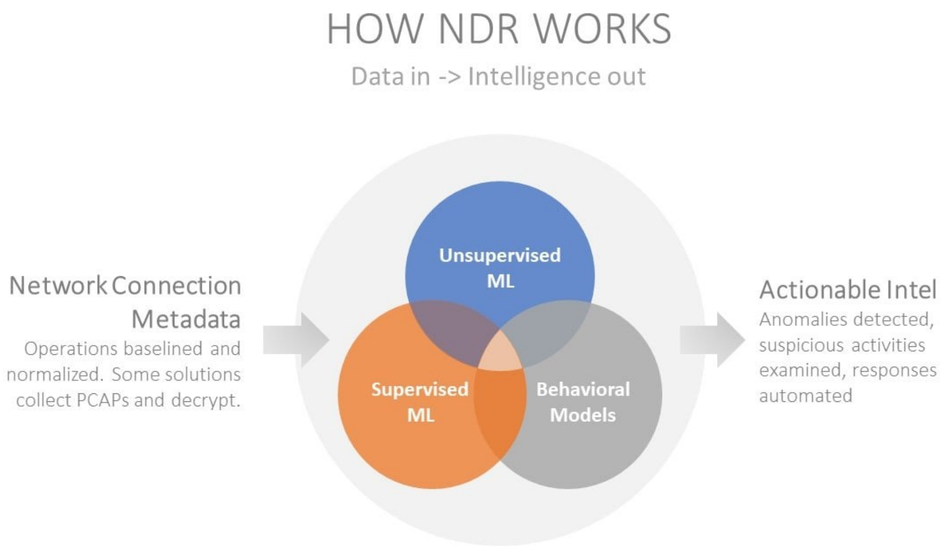

HOW NDR WORKS
Data in -> Intelligence out
Network Connection Metadata
Operations baselined and normalized. Some solutions collect PCAPs and decrypt.
Unsupervised ML
Supervised ML
Behavioral Models
Actionable Intel
Anomalies detected, suspicious activities examined, responses automated

Figure 4. NDR working principle [14]

.

3.3 NDR Sensor placement

To get the most out of NDR solution the network infrastructure especially the traffic paths need to be known and understood. It is not always necessary to capture all the traffic, but it is important to know what points in the network provide the critical traffic which will be monitored. One of the first deployment questions is: will NDR monitor only north-south or east-west traffic or will both be monitored. If east-west traffic is monitored, is it captured from all inter-VLAN routing points or only from datacenters ingress and egress points. Similar considerations are required for north-south traffic to cover all the needed egress points.

3.4 Types of threat that can be detected

The threat types that NDR detects can be divided to four main types. Unknown malware attacks are an external threat used to compromise and control hosts on the network. Targeted attacks are external attacks that are directly attacking the organization using different methods to gain access to endpoints, lateral movement and stealing data. Insider threats includes attacks done by employees or contractors and can include accessing or stealing data, installing malware etc. Fourth type identified is risky behavior. Employees do not mean to harm, but act in a way that exposes sensitive data or enables remote access etc.

3.4.1 Mapping to MITRE ATT&CK and D3FEND

MITRE ATT&CK is a knowledge base that covers different tactics and techniques that cyber adversaries' use. It is based on real-world observations and can be used for modeling threats. [15] ATT&CK matrix for enterprise covers techniques in 14 different categories: Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, and Impact. [16] This framework can be used as a reference to map the threats that NDR solution can cover.

As a counterpart for the ATT&CK there is MITRE D3FEND [17]. This knowledge base covers the countermeasures for the attack techniques and tactics in the ATT&CK matrix. D3FEND has five main categories of defend techniques: Harden, Detect, Isolate, Deceive, and Evict. The relationship between these two is presented in Figure 5.

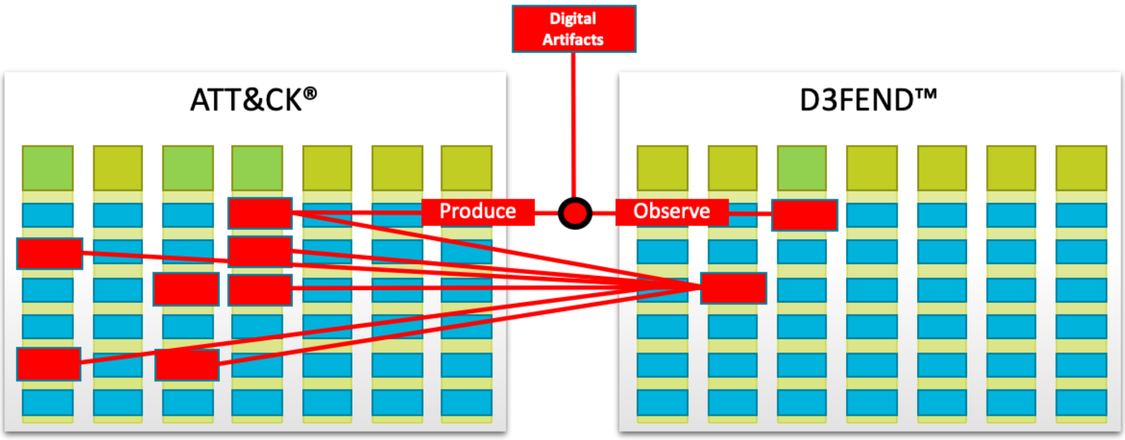


Figure 5. Relationship between offensive and defensive techniques in MITRE knowledgebases. [18]

MITRE D3FEND can also be used when evaluating NDR products. Products should cover countermeasures presented in detection category especially for Network traffic analysis parts and some of the User Behavior Analysis. There should also be options for techniques in Isolate category.

3.4.2 Case DNS tunneling

DNS tunneling is a technique to exchange information via DNS protocol. DNS is originally designed to convert human readable domain names to IP addresses using A records for IPv4 or AAAA records for IPv6 addresses. For example, the IP address for the mail.google.com is translated to the domain's IP address 172.217.16.133 using DNS. [19]

Attackers use DNS to receive commands or load malicious code via DNS protocol. When the local DNS server does not know the domain like getPayload001.evildomain.com, it must rely on the answer from evildomain.com that sends a CNAME record as reply dg59knca2rlpmnh98jdwyasdfer34.evil-domain.com. In this reply "dg59knca2rlpmnh98jdwyasdfer34" is the first part of the malware code that the stager interprets. Then several similar requests and replies follow until the entire malware code has been transferred. This kind of DNS traffic seems harmless, and firewalls or IDS systems do not interfere with it. This way of communication does not have any direct contact either between the infected device and the malicious domain because only DNS queries are made.

DNS tunneling is not encrypted traffic but identifying it can be challenging. Simple whitelists or blacklists are not working very well with DNS because restricting access to everything else than certain sites is not doable in many organizations and blacklisting does not affect new domains that attackers can register for their campaign. There are few ways to detect this kind of attack. First is investigating the size of the DNS requests. In order to optimize the data transfer via DNS request they use maximum number of characters. Then there is the character distribution of subdomains. These tend to be cryptic and not human-readable due to them containing the encrypted data instead of being a regular subdomain. Sometimes real domains can have non-human-readable domain names as well, but this could be indication of C2 channel. Another indication is missing benign traffic to follow like HTTP requests after DNS request. Normally the DNS request is done prior accessing something else and not just several DNS requests. Also, the distribution of different DNS requests is off. [19] All of these are things that machine learning can be trained to detect.

3.4.3 Case HTTPS tunnels

Network traffic is usually encrypted these days. There are ways to intercept the HTTPS traffic for example by using proxies to intercept and decrypt the traffic. This has some concerns about users right to privacy if the traffic is intercepted and decrypted. Another way is to use machine learning to analyze the patterns of the traffic data without decrypting it. Considering C2 traffic like in the previous example detections can be done from the shape of the traffic data. Benign beacons are used in communications to keep for example chatting apps in sync. These have regular levels of data bytes send and received. Beacons between infected host and C2 servers communicate differently. There are spikes in transferred bytes caused by the attacker's commands, which are followed by infected hosts response. [13] These shapes in the traffic can be used as detection patterns, which machine learning can identify without the need to decrypt the data.

3.5 NDR benefits

Main benefit for using NDR is having a broad visibility over the network. Attacker can try to hide on the endpoint, but it is harder to hide in the network. Attackers could use anti-forensics tools to hide or remove evidence of the attack. This means that the malicious activity may not get to SIEM from the endpoints. In these cases, there will still be traces in the network layer, because there are not many attacks that would be executed completely offline. [14] Compared to the possible thousands of endpoints to monitor with individual agents, network has fewer points where a sensor needs to be deployed to monitor important traffic flows. Another benefit is detection of activities that are not collected on endpoint like network scanning attempts, lateral movement, or data exfiltration. In the case of data exfiltration endpoint forensics might show what data was viewed, but it cannot confirm that it has been successfully exfiltrated by USB device unlike network traffic can show if data was exfiltrated through network.

3.6 Challenges

One challenge with NDR is the amount of data and problems related to it. Processing and storing data needs resources dedicated to this. Also, this data needs to be processed in a way that the analysts workload stays reasonable. This means that the AI should do some of the triaging and prioritizing so alerts are not flooding. Another thing is providing tools for the analyst to manage the alerts. If events are already linked together and put on timeline analyst does not need to use their time on that and instead, they can focus on investigating and mitigating the threats.

No single solution is perfect on its own. NDR should be implemented as a part of the security solution where data from various sources can be correlated to see the full picture of the incident from start to end. The trend is moving to Extended Detection and Response (XDR), which is a security strategy to use all available telemetry for handling detection and response. Components of XDR solution may vary, because it is not really another tool, but more of a collection of tools and integrations in one solution. [20]

In ideal scenario NDR alerts defenders in an early phase of the attack chain but finding the threshold for alerting baseline can be difficult and might need tuning to reduce the number of false positives. Also, IoT/OT networks have their own special cases, and it could be harder to install a solution so that it doesn’t interrupt production, which means that responses need to be mostly done or at least approved manually and the solutions need to be passive. Baselining the normal behavior differs from traditional IT networks and it can differ between different OT environments.

4 PRODUCT COMPARISON

4.1 Overview of selected NDR products

For this work a list of interesting vendors was collected. Then that was narrowed down for two products which are IT specific and two products that are OT specific. Rest of the products will be reviewed later internally after the process is assessed with these selected ones.

4.1.1 Product A

This product was chosen for the IT side of NDR solutions. This is a heavily AI and machine learning based solution for detection and for triage and prioritization, but they offer support for signature-based detection as well. Several machine learning approaches are used for detecting anomalies and attack patterns. Another thing that this product offers is response actions to contain and remediate attacks on systems.

4.1.2 Product B

Product B is the second product chosen for the IT NDR. It consists of two product subscriptions tied together where one is used for the detection side and the automated responses are provided via other subscription. Several detection engines with focus on unsupervised learning and anomaly detection. On the respond side they offer tools for automated incident investigation that apply ML techniques.

4.1.3 Product C

Product C is one of the OT side NDR solutions. They offer agentless device monitoring that can be deployed on-premises, cloud or for hybrid OT networks. Sensors are available either physical or virtual and there is a large support of OT protocols the sensors can detect including some custom and non-standard protocols.

4.1.4 Product D

This is another product that focuses on OT. Detections use known threats and custom rules, anomaly detection on communication patterns and behavioral analysis to detect known patterns of intrusion methods. They also offer asset profiling possibilities and wide protocol support of industrial vendor specific protocols. In addition to passive protocols, they have support for device specific active queries. The alerts are contextualized with their relation to Cyber kill chain and mapped to MITRE ATT&CK for ICS. Product provides root cause analysis and groups the related events together.

4.2 Considerations

There are several things to consider when deciding to implement NDR solution. First thing to consider should be how the NDR can complement the existing detection solution [21]. Solution should add value by adding capabilities for detection and post breach investigations. Adding to this is identifying gaps in current detection and response. Defenders should determine what are the most important detection gaps and consider is NDR able to fill those [21].

When evaluating vendors there are several factors to assess. These include solution type, detection methods, response methods, available integrations and is the solution for IT networks only or can it handle OT as well, or third is it OT specific. In addition to these the number of alerts should be considered as a metric. Supported protocols is a good way to evaluate is the NDR solution going to work for the use case. Also, if an important protocol is not directly supported, is there a way to write own parameters for detecting it. One important factor in the final decision making is the cost of the solution, but that is left out of this work.

4.3 Comparing core features

Core features could be described with the help of NIST Cybersecurity framework [1] and the MITRE ATT&CK [16] and D3FEND [17] frameworks. From the NIST Cybersecurity frameworks core functions Protect, Detect and Respond parts are needed from the NDR. These are not some specific features that the solution must have, but broader functionalities that are achieved with the NDR. How NDR can manage this was covered in the section 2.1 of this work.

MITRE ATT&CK is something that is used by the vendors, and it will be used in this work as well. Unfortunately, the products were not mapped to match the latest versions of this framework, so those previous versions will be used in this work as well.

4.3.1 MITRE ATT&CK for Enterprise

The product A and B are mapped against the Enterprise version of the framework. This version covers the attack vectors in the IT network, and it is suitable for showing the capabilities of IT specific NDR products. The latest version at the moment is version 13, but Product A provided mapping against version 12 and Product B did not mention the version they were using, but from the time and the tactics it seems to be against version 11. Versions 11 and 12 use same categories, but there are two added techniques. Serverless Execution was added to Execution category and Steal or Forge Authentication Certificates was added to Credential Access category. [22]

How products A and B cover the framework is shown in Table 1. Product A did not provide the mapping for all the categories, because it was argued that they mapped only the main areas of NDR. For this reason, the first two categories are marked as data not available (NA) for Product A. Product B listed their products coverage using sometimes the sub-techniques and sometimes the main technique so the data in this table was taken from the mentioned main techniques.

Table 1. Products coverage of MITRE ATT&CK for Enterprise

MITRE ATT&CK for Enterprise version 11 / 12	Product A mapped to v.12	Product B mapped to v.11
Reconnaissance	NA/10	2/10
Resource Development	NA/7	5/7
Initial Access	7/9	8/9
Execution *	8/13	7/12
Persistence	11/19	10/19
Privilege Escalation	4/13	4/13
Defense Evasion	13/42	13/42
Credential Access *	16/17	10/16
Discovery	14/30	16/30
Lateral Movement	9/9	9/9
Collection	16/17	13/17
Command and Control	16/16	13/16
Exfiltration	8/9	9/9
Impact	5/13	7/13
Total	**111/224**	**126/222**

*Added techniques in version 12

Overall Product B seems to cover more techniques than Product A. But as mentioned earlier all the techniques covered in the Enterprise matrix are not network specific so these should be looked more on the tactic level and decided which are the ones that NDR solution should be covering because some of the techniques here are better covered with an EDR solution instead. So, looking into C2 for example Product A covers all techniques while Product B covers only thirteen out of the 16. Lateral Movement is another tactic category that NDR should detect and on that both products cover it well.

4.3.2 MITRE ATT&CK for ICS

OT NDR solutions are mapped against the MITRE ATT&CK for ICS. This covers the tactics and techniques used in the industrial environments. Latest version of the ICS is also version 13, but the products provided mappings against version 8, which can be accessed with MITRE Attack Navigator [23]. Mappings were marked with direct detections and that can be achieved indirectly with correlations. Both products can achieve the full detection of the techniques and tactics shown in the framework when indirect detections are considered. When only direct detections are considered, Product D has a little better coverage as shown in the Table 2.

Table 2. Products coverage of MITRE ATT&CK for ICS

MITRE ATT&CK for ICS version 8	**Product C**		**Product D**	
	Direct	Total	Direct	Total
Initial Access	6/10	10/10	7/10	10/10
Execution	6/9	9/9	3/9	9/9
Persistence	3/6	6/6	5/6	6/6
Evasion	5/7	7/7	6/7	7/7
Discovery	7/7	7/7	6/7	7/7
Lateral Movement	5/6	6/6	5/6	6/6
Collection	7/11	11/11	8/11	11/11
Command and Control	3/3	3/3	3/3	3/3
Inhibit Response Function	13/15	15/15	15/15	15/15
Impair Process Control	8/11	11/11	11/11	11/11
Impact	2/11	11/11	0/11	11/11
Total	**65/96**	**96/96**	**69/96**	**96/96**

4.4 Deployment

It is important to consider how the product can be deployed. Is the collected event data and management console available on-premises and can that be air gapped, or is some of that handled in cloud? On-premises means that the solution is deployed on the customer's own infrastructure instead of having it managed through the vendor's cloud infrastructure. On-premises could be required for data confidentiality reasons. One step further into more confidential is air gapped environment where there is no traffic outside the environment. This means that all the updates need to be brought manually to the environment while on-premises solution might have connections outside like a lifeline to the vendor to receive product updates directly. Cloud managed solution might be more suitable for some organizations who do not have strict policies demanding data to remain inside their own network. Management of a SaaS solution is easy, and the deployment does not need as much effort compared to installing and handling everything inside company's own infrastructure. Available deployment possibilities for the products are shown in Table 3.

Table 3. Deployment possibilities

	Product A	Product B	Product C	Product D
Cloud	yes	yes	yes	yes
On-Premises	yes	yes	yes	yes
Air gapped	yes	yes	yes	yes
Virtual Sensor	yes	yes	yes	yes
Physical Sensor	yes	yes	yes	yes

Another thing to consider about the deployment is how the alerts and logs are handled. Depending on the existing environment there might be different needs for the NDR. In some cases, it could be more sensible to implement the NDR solution to an existing technology if there is a feature available that can handle network detection as well. Environment, which already has a solution for managing events and creating tickets with monitoring dashboards for the analyst, does not need another solution for this. Then a NDR solution that can be integrated into the existing system is all that is needed. Sometimes the use case might require a full-on solution that has its own console for alerting and handling the responses if there is not any existing infrastructure for that. Usually, the case is that even if the product has its own console, the events and logs are sent to centralized processing elsewhere so that SOC has all the information available from one place.

4.5 Detection types

In an ideal solution the detection is not based on single type but a combination of detection methods. Different techniques that are used consist of machine learning and behavior analysis, threat intelligence and signatures. Table 4 presents how products utilize different detection approaches. All the products use several machine learning methods. Main differences come in the threat intelligence. Most products offer some sort of signature-based detections, but Product B relies on their AI over signatures.

Table 4. Detection types

	Product A	Product B	Product C	Product D
ML	yes	yes	yes	yes
Signatures	Suricata, Threat Intel	no	Threat intelligence package (IOCs, CVEs, Asset profiles)	Snort, Yara
Deep Packet Inspection		yes	yes	yes

4.5.1 Response types

Response part of NDR seems to vary with different vendors. Some focus more on providing tools for manual responses and threat hunting and some have automated responses for remediation. Products offer data storing which can be the full PCAPs of the events or metadata. The type of stored data and storing periods vary depending on subscription types. One typical automated response is sending a command to a firewall via integration to drop the suspicious traffic. These different kind of definitions for response can be considered as what is needed and are the tools for handling incidents enough or should the analyst's workload be helped with automated responses. In both cases it makes sense to have integrations with other network protection solutions like firewalls and also EDR products to isolate the threat.

4.6 OT Protocol support

There is a wide range of different communication protocols used in industrial networks. This creates a challenge for the OT specific NDR systems to support all the specific protocols. Product C offers a shorter list of protocols that are supported out of the box for the OT and IoT device discovery, but there is opportunity to create own protocol support or look for community protocols. Product D offers wider range of passive protocols for real-time monitoring, and they also offer support for active protocols for device specific queries. Protocol support is presented below in Table 5.

Table 5. Protocol support

	Product C	Product D
Passive protocols	141	206
Active protocols	2	79
Support for protocol creation	yes	yes

Choosing the suitable product for the environment depends on what kind of devices there are and what protocols they use.

4.7 Performance comparison

For the performance testing we needed to define some metrics to measure during the assessment. Number of different kinds of alerts produced is one way to measure this. Another would be how long it takes to alert a critical event. This kind of comparison between products could provide information on which how fast different products can detect threats and how accurately they do it. One thing to investigate is the ratio and balance between false positives and false negatives. This means that the noise from the false positive alerts is low, but solution should not miss real threats either so false negatives should be low as well.

Accuracy is evaluation metric that describes what ratio of the detections were correct. Accuracy is defined as number of correctly classified events divided by total number of events. [24] This can be calculated using true positives (TP), false positives (FP), true negatives (TN) and false negatives (FN) as followed in equation 1:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{1}$$

In this case true positives are events that are correctly classified as alerts and true negatives are events that are correctly processed as benign. False positives are benign events classified as malicious and false negatives are real threats, which have not been noticed. Solution works well if the accuracy value is close to one. Two other parameters for evaluation of how well products perform in addition to accuracy are precision and recall. Precision tells how many of the positive results are correct:

$$Precision = \frac{TP}{TP + FP} \tag{2}$$

Recall answers how well the positives were identified correctly:

$$Recall = \frac{TP}{TP + FN} \tag{3}$$

Precision and recall can be used when defining the alerting threshold. Getting both high can be a challenge as because increasing precision by increasing threshold may lead to lower recall and vice versa. [25] This can be demonstrated in a simple linear example. In Figure 6 a linear presentation of threshold selection is presented with fifteen color coded events. Purple events present benign and yellow present malicious. Three different thresholds are proposed: one for high recall, two for balanced ratio and three for high precision. Events are also categorized to true and false positives and true and false negatives.

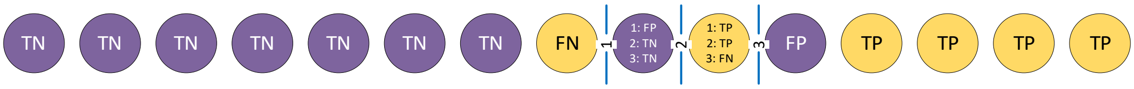


Figure 6. Linear example of threshold selection

Calculating accuracy, precision and recall for different thresholds we get following results for the first threshold:

$$Accuracy = \frac{5+7}{15} = 0{,}8$$

$$Precision = \frac{5}{5+2} = 0{,}71$$

$$Recall = \frac{5}{5+1} = 0{,}83$$

Similarly counting for the second threshold gives accuracy of 0.86, precision of 0,83 and recall of 0.83. For the third threshold accuracy of 0.8, precision of 0.8 and recall of 0.66.

Greater number of produced alerts is not a proof of better detection. Neither is too low number of alerts. It can be difficult to say what is the perfect amount, but the solution should correlate and prioritize events to make analysts life easier so that they can focus on the important events that require immediate action. In a way we could say that less is more when the important events are noticed but analysts don’t get alert fatigue if every anomaly is being alerted.

5 TESTING ENVIRONMENT

For the in-depth testing, a lab environment is needed. Also standardized test dataset needs to be defined for IT and OT use cases. There are few ways to do the testing. First is building own lab environment to simulate a company network, normal activities in it and attack on it. Another is using publicly available datasets and feed them to the products, which is not very suitable for a NDR that learns couple weeks what is the baseline and the normal activities in the network. Third way is testing with a proof of value trial in the actual environment or part of the company environment. The baseline will be the benign traffic that is present normally. After the learning period, a variety of attacks needs to be performed to see how the products handle them: at what point of time attacks are detected, how many events, alerts and critical alerts are generated.

5.1 Datasets and Test Cases

One problem with testing in lab environment is availability of datasets. This is a problem in the IT but especially for OT. There is only a few publicly available and complete enough datasets for this kind of use case. Privacy issues restrict how datasets can be shared and on the other hand anonymized datasets may lack some characteristics or be out of date. One solution could be dynamically generated datasets, which could be modified and extended for the use case. [26] There are few existing datasets for intrusion detection and Sharaldafin et. al generated a new dataset in 2017 to tackle the problems of the outdated datasets [27]. They created high security infrastructure for the victim network complete with firewall, router, switches, PCs and Servers with Linux, Windows, and Macintosh operating systems. These were used with an agent to create the naturalistic B-profile benign background data. [28]

Getting natural benign background data is a big challenge for testing NDR system in lab environment. These systems use machine learning approaches to create a baseline of the benign traffic over the learning period. If the dataset is not as excessive as a real corporate network environment, it should not be a challenge for the solution to detect the attacker traffic in the lab, because the anomalies are mostly related to the attacker actions instead of some human interaction that was not considered on creating the data. This means that the detection results in the lab environment could be significantly better than in real environment.

One thing that can be taken from these proposed datasets the variety of protocols used. And the second is the attack variety in M-profile or malicious profile [26]:

- Infiltration attacks
- DoS and DDoS Attacks
- Web application attacks
- Brute force attacks
- Unsuccessful infiltration from inside, unsuccessful privilege escalation
- Insider threats

Insider threats was not originally on the attack listing, but it is something many NDR providers say that they are able to detect, so it was added to the listing. Another thing to take from the attacks is not only successful attacks are listed. It is important to be able to detect unsuccessful attack attempts as well.

5.2 Proof of Value

As mentioned in the previous paragraphs, creating a suitable testing environment and datasets would be difficult. For this reason, instead of doing testing for various products in lab environment, it was decided that the work will be continued with proof of value cases with customers. Proof of value (PoV) testing means that the chosen product or competing products are setup in the company environment or into a section of their environment for a testing period. During this time, the learning period takes place first for baselining the network. After that there is the evaluation period which should include red teaming activities. This means that different attack attempts are made against the systems inside the network to see how the evaluated product is detecting and responding to these activities.

6 CONCLUSIONS

Main reason to deploy NDR solution is added visibility and filling the gaps in existing detection systems. NDR is not all-powerful tool for defenders. Instead, it is an important part of overall coverage of data sources for defenders to use every source of information available to build the full picture of what is happening in their systems, endpoints, and network in order to detect and respond to threats as fast as possible.

The products offer quite similar detection capabilities in their corresponding categories. In the OT category main differences comes from the supported protocols. Product D provides more passive and active protocols compared to Product C. On the IT side there is difference in included detection types. Product A has the added option to use signatures for threat detection when Product B relies only on their AI. Trend on deployment options seems to be providing the cloud managed versions, but the need for the on-premises option is taken into account in every product.

Unfortunately, testing of the products was left out of scope after realization of how difficult it would be to do realistic enough lab environment. Testing products that use AI to learn about the environment and anomalies in it need enough real events that make the baseline and in lab environment anomalies would be highly likely to show right away. So further testing was left for proof-of-value cases in real environments. Another thing that this work does not cover is money. Pricing of products will affect the final decision of the solution to choose, but it was left out of scope in this work.

REFERENCES

[1] NIST, "Framework for Improving Critical Infrastructure Cybersecurity," National Institute of Standards and Technology, 2018.

[2] A. Barros, A. Chuvakin and A. Belak, "Applying Network-Centric Approaches for Threat Detection and Response," Gartner, 2019.

[3] S. Bhatt, P. K. Manadhata and L. Zomlot, "The Operational Role of Security Information and Event Management Systems," *IEEE Security & Privacy,* vol. 12, no. 5, pp. 35-41, 2014.

[4] A. Arfeen, S. Ahmed, M. A. Khan and S. F. A. Jafri, "Endpoint Detection & Response: A Malware Identification Solution," in *2021 International Conference on Cyber Warfare and Security (ICCWS)*, Islamabad, 2021.

[5] ENISA, "ENISA Threat Landscape 2022," European Union Agency for Cybersecurity (ENISA), 2022.

[6] NIST, "NVD - CVE-2021-44228 Detail," 12 December 2021. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2021-44228. [Accessed 13 June 2023].

[7] Lockheed Martin, "Gaining the Advantage, Applying Cyber Kill Chain® Methodology to Network Defense," Lockheed Martin Corporation, 2015.

[8] P. Ackerman, "The Purdue Model and a Converged Plantwide Ethernet," in *Industrial Cybersecurity*, Birmingham, Packt Publishing, 2017.

[9] T. J. Williams, "A Reference Model for Computer Integrated Manufacturing from the Viewpoint of Industrial Automation," *IFAC Proceedings Volumes,* vol. 23, no. 8, pp. 281-291, August 1990.

[10] X. Zhou, Z. Xu, W. L. K. Chen, C. Chen and W. Zhang, "Kill Chain for Industrial Control System," *MATEC Web of Conferences,* vol. 173, p. 01013, 3 2018.

[11] Gartner, "2020 Gartner Market Guide for Network Detection & Response," Gartner, 2020.

[12] N. Moustafa, J. Hu and J. Slay, "A holistic review of Network Anomaly Detection Systems: A comprehensive survey," *Journal of Network and Computer Applications,* vol. Volume 128, pp. 33-55, 2019.

[13] Vectra, "White Paper: The AI Behind Vectra AI," 2022.

[14] J. Tolbert, "Network Detection and Response," Kuppingercole Analysts, 10 June 2020. [Online]. Available: https://www.kuppingercole.com/research/lc80126/network-detection-and-response. [Accessed 15 May 2023].

[15] B. E. Strom, A. Applebaum, D. P. Miller, N. K. C., A. G. Pennington and C. B. Thomas, "MITRE ATT&CK: Design and Philosophy," The MITRE Corporation, 2020.

[16] MITRE, "MITRE ATT&CK," 2023. [Online]. Available: https://attack.mitre.org/. [Accessed 12 4 2023].

[17] MITRE, "MITRE D3FEND," 2022. [Online]. Available: https://d3fend.mitre.org/. [Accessed 17 4 2023].

[18] P. E. Kaloroumakis and M. J. Smith, "Toward a Knowledge Graph of Cybersecurity Countermeasures," The MITRE Corporation, 2021.

[19] ENISA, "Encrypted Traffic Analysis," European Union Agency for Cybersecurity (ENISA), 2020.

[20] M. Chapple, J. M. Stewart and D. Gibson, "Secure Network Architecture and Securing Network Components," in *(ISC)2 CISSP® Certified Information Systems Security Professional: Official Study Guide*, John Wiley & Sons, Inc, 2018, pp. 439-520.

[21] J. D'Hoinne, N. Smith and T. Lintermuth, "Market Guide for Network Detection and Response," Gartner, 2022.

[22] MITRE, "Updates - October 2022," 25 10 2022. [Online]. Available: https://attack.mitre.org/resources/updates/updates-october-2022/. [Accessed 16 5 2023].

[23] MITRE, "MITRE ATT&CK® Navigator v4.8.1," 2023.

[24] Google for Developers, "Machine Learning Crash Course - Classification: Accuracy," [Online]. Available: https://developers.google.com/machine-learning/crash-course/classification/accuracy. [Accessed June 2023].

[25] Google for Developers, "Machine Learning Crash Course - Classification: Precision and Recall," [Online]. Available: https://developers.google.com/machine-learning/crash-course/classification/precision-and-recall. [Accessed June 2023].

[26] "CSE-CIC-IDS2018 on AWS," University of New Brunswick, 2018. [Online]. Available: https://www.unb.ca/cic/datasets/ids-2018.html. [Accessed April 2023].

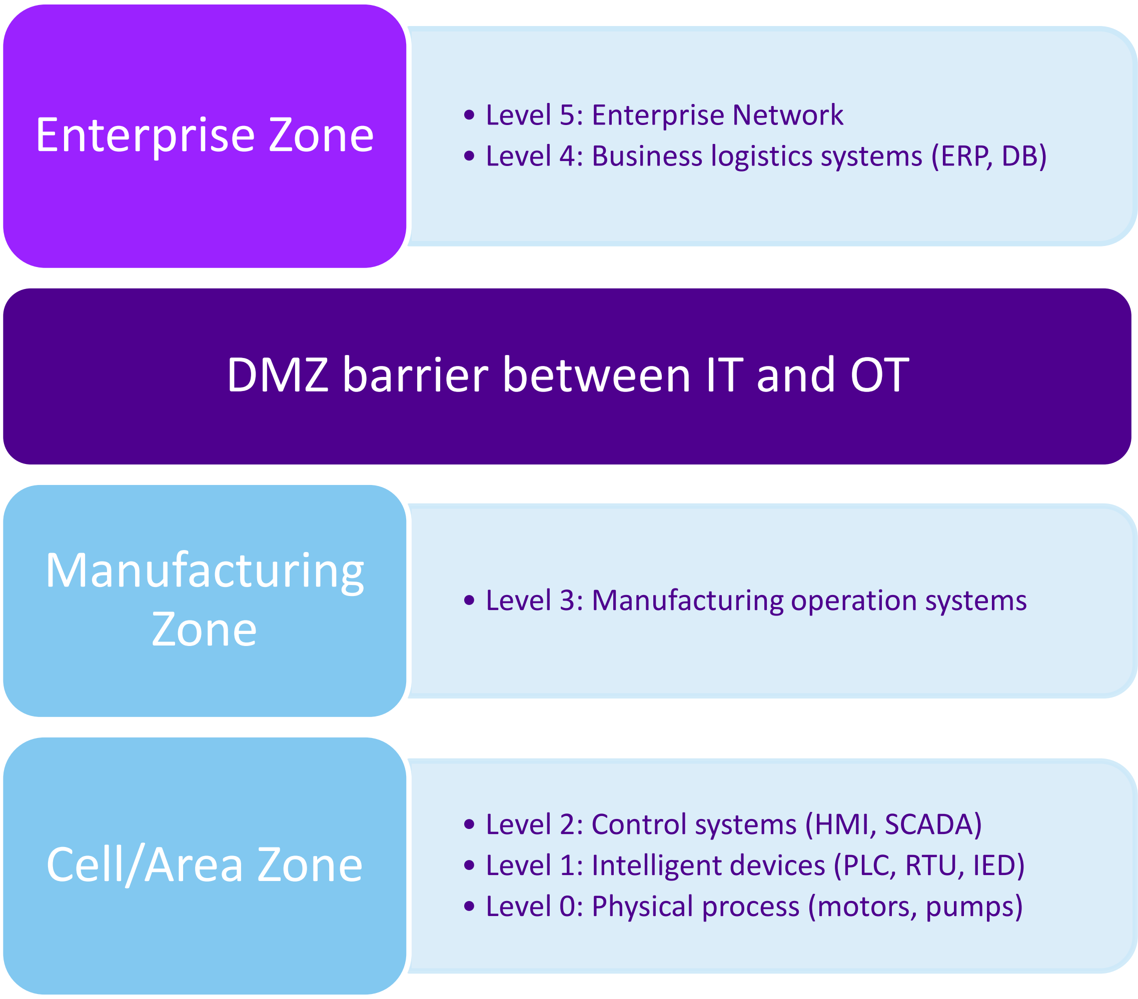
[27] I. Sharafaldin, A. Gharib, A. H. Lashkari and A. A. Ghorbani, "Towards a Reliable Intrusion Detection Benchmark Dataset," *Software Networking Journal,* pp. 177-200, 2018.

[28] I. Sharafaldin, A. H. Lashkari and A. A. Ghorbani, "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization.," in *4th International Conference on Information Systems Security and Privacy (ICISSP)*, Portugal, 2018.

[29] M. H. Bhuyan, D. K. Bhattacharyya and J. K. Kalita, "An effective unsupervised network anomaly detection method," in *ICACCI '12: Proceedings of the International Conference on Advances in Computing, Communications and Informatics*, 2012.

APPENDICES

Appendix 1. Purdue Model


Enterprise Zone
• Level 5: Enterprise Network
• Level 4: Business logistics systems (ERP, DB)
DMZ barrier between IT and OT
Manufacturing Zone
• Level 3: Manufacturing operation systems
Cell/Area Zone
• Level 2: Control systems (HMI, SCADA)
• Level 1: Intelligent devices (PLC, RTU, IED)
• Level 0: Physical process (motors, pumps)