

Tatu Eskelinen

DEVELOPMENT OF OPEN-SOURCE SIEM AND SECURITY OPERATION CENTRE IN A COMPANY

Bachelor's thesis

Information Technology

2022



South-Eastern Finland
University of Applied Sciences

Author	Degree title	Time
Tatu Eskelinen	Bachelor of Engineering	February 2022
Thesis title		53 pages
Development of SIEM & SOC		
Commissioned by		
MPY Telecom OY		
Supervisors		
Reijo Vuohelainen (Senior Lecturer / XAMK) & Aapo Sormunen (Production Manager / MPY Telecom Oyj)		
<p>The goal of this thesis was to study and deploy an open-source SIEM for MPY Telecom Oyj, which they wanted to use it for the company and productize for its customers. At the start of this thesis, I will introduce the history of cybersecurity, clarify the differences between information security and cybersecurity, and present the current state of cybersecurity in Finland. This thesis was requested for research by MPY Telecom Oyj.</p> <p>The main point of this thesis was to create a product family about OSSIM and SOC. The Theoretical part is based on my understanding of OSSIM and SOC, and cybersecurity. I also introduce the tools of OSSIM, a sensor and plugin, that are deployed during the project. This thesis also includes a business point of view because, in the end, the products are used in the company and added in the product knapsack for preparing to put in the product shelves for customers.</p> <p>Cybersecurity is one of the most important things for companies in order protect their valuable data. Data contains sensitive information, including important data about staff, partners, company's R&Ds or next of kin; shareholders, business partners and clients et cetera.</p>		
Keywords		
SIEM, SOC, OSSIM, Cybersecurity		

OPENING WORDS

To begin with, I want to thank my supervisor, Aapo Sormunen, who convinced me to take a jump into an unknown subject and take it as a challenge without having any conversance which was new for both of us. I want to thank my family and friends who supported me during my thesis project. In addition, special thanks and credits go to my thesis instructor, Reijo Vuohelainen, who showed me the way during the challenges I encountered during this thesis, and also over the last four years.

4G	The fourth generation of cellular broadband
5G	The fifth generation of cellular broadband
AI	Artificial Intelligence
APARNET	The Advanced Research Projects Agency Network
AT&T	American Telephone and Telegraph Company
BYOB	Bring Your Own Device
CLI	Command-Line Interface
DDoS	Distributed Denial-of-Service
DNS	Domain Name System
EDVAC	Electronic Discrete Variable Automatic Computer
HIDS	Host-Based Intrusion Detection System
ID	Identify Document
IoT	Internet of Things
IP	Internet Protocol
IRC	Internet Relay Chat
ISP	Internet Service Provider
KGB	Committee for State Security in Soviet Union
LAN	Local Area Network
ML	Machine Learning
NDA	Non-Disclosure Agreement
NOD	A Slovakian Antivirus Company
OSSIM	Open-Source SIEM
PC	Personal Computer
R&D	Research and Development
RDC	Remote Desktop Connection
SEM	Security Event Management
SIEM	Security Information Event Management

SIM	Security Information Management
SOC	Security Operation Centre
SSH	Secure Shell
UCLA	University of California, Los Angeles
UI	User Interface
USM	Unified Security Management

CONTENTS

1	INTRODUCTION.....	1
2	CYBERSECURITY IS FOR EVERYONE	1
2.1	Information security or cybersecurity	2
2.2	The price without cybersecurity	3
2.3	Campaign between attack and defense	3
3	‘THE ART OF WAR’ IN CYBERSECURITY	4
3.1	Sun Tzu’s methods.....	5
3.1.1	There is always human	5
3.1.2	Don’t overthink	5
3.1.3	Adapt to the environment	6
3.1.4	Basic things come first.....	6
3.1.5	Know your enemy.....	6
4	THE BEGINNING OF CYBERSECURITY.....	7
4.1	Before it all started	7
4.2	How it all began.....	8
4.3	The beginning of the commercial antivirus	8
4.4	Advanced criminals	10
4.5	Threats diversify and multiply	11
4.6	Meaning of cybersecurity increases	11
4.7	Next generation and new challenges	12
4.8	Upcoming challenges	14
5	PRESENT STATE OF THE CYBERSECURITY IN FINLAND	15
6	PROBLEMS DURING RESEARCH PROCESS.....	17
6.1	Research questions.....	17
6.2	Research objectives	17

7	LOG DATA AS SUPPORT OF INFORMATION SECURITY IN MPY	18
8	IDEOLOGY OF SOC SIEM	19
8.1	SIEM	19
8.2	SIEM in business and future	21
8.3	SOC – Security Operation Center	21
8.4	SOC in business and future	22
9	ALIENVAULT & AT&T CYBERSECURITY	22
10	ALIENVAULT OSSIM.....	23
11	ALIENVAULT ARCHITECTURE AND COMPONENTS	24
11.1	An easy method to explain OSSIM.....	26
12	ALIENVAULT OSSIM INSTALLATION PROCESS.....	28
13	TOOLS	29
13.1	Sensor.....	29
13.2	Plugin	31
14	THE VIEW OF PRODUCTIZATION	35
15	FURTHER MEASURES AND FURTHER RESEARCH PROPOSAL.....	36
16	CONCLUSION	36
	REFERENCES.....	38

1 INTRODUCTION

MPY Telecom Oyj is a Finnish ICT company. MPY was founded by the name of Telefooniyhdistys in 1888, but many decades later, in 1938, the name was changed to MPY, which is an abbreviation for Mikkelin Puhelinyhdistys. The company provides SMA information management and consultant services, both cloud and information network services for small and medium-sized enterprises and directly to consumers. MPY Group has been separated into three spheres of responsibilities: MPY Osuuskunta, MPY Yrityspalvelut and Telecom Oyj, which was where I worked. The board of MPY Palvelut Oyj and MPY Osuuskunta is divided to separate businesses, networking and the group as their own companies in 2019. MPY Osuuskunta owns of both 100 percent. Just a sphere of responsibilities has been shared. MPY has set up several new branches during the last decade, which include old ones: Mikkeli, Vantaa, Oulu, Tampere, Ylivieska, Kuopio, Kouvola and Joensuu. (Wikipedia, 2021)

When I did my internship at MPY, I worked on several different projects to improve the company's network security and its network devices, which is why this became my thesis topic after having a conversation with my supervisor. The purpose of this thesis purpose is to improve MPY's cybersecurity. MPY acknowledges that cybersecurity has become more critical nowadays because it protects all categories of data from theft and damage. From the enterprises' point of view, this protects sensitive data which MPY's customers, mostly SMEs, want their data covered from espionage. Without cybersecurity, the customers of MPY cannot defend themselves against a data breach campaign. That is why MPY wants to protect their customers from data breaches and increase the company's imago (Tunggal, 2021).

2 CYBERSECURITY IS FOR EVERYONE

We are living in the world among bits, where we are enjoying the digitalization possibilities that are provided for us all, trusting that the world is safe. Cyberworld

and cybersecurity have become part of our daily lives. Economy, society's security, the operations of companies and our lifestyles, regardless of where people are around the world are dependent on data. There is a two-edged sword: our dependency on security and the vulnerability increases besides the security. Security is a basic need for humans, companies, society, and nations (Limnell, 2014, 13).

Many people make the assumption that cybersecurity is only about technology, but it is also related to people, companies, and politics.

2.1 Information security or cybersecurity

It is not always easy to tell the difference between cyber and information security ideas. Cybersecurity is often used to refer to information security that is also linked to the outside world of computers, for example, social engineering (Suomen Automaatioseura, 2021, 23).

Cybersecurity has been gaining a lot of attention in the previous few years (5-10) and it is a relatively new phenomenon. On the other hand, information security has existed since the 1970s, with the introduction of PCs, LANs, and the Internet's precursors. Perhaps the easiest way to understand the distinction between these concepts when it comes to define the data security, it's best to think of it as the protection of information as it travels, like the company's files, emails or bank IDs. Poor physical security in the office or inadequate network security can expose to data breaches. (Puro, 2017)

When it comes to hacking computers and networking devices, it is not the same thing as picking up a computer by its arm with a crowbar. As a result, cybersecurity is special importance to the security of information systems (Puro, 2017). On the other hand, the term "information security" usually refers to the protection of existing, and stored data, and disorganized raw data (Limnell, 2014, 31).

Many people use the term “cyber” to refer to a variety of different things around the world. The term “cyber” became so popular at the end of the 1990s, particularly in the military, as all information technology was developed by the military. During that decade, it was used for information warfare. The term has taken root in society step by step. Cyber was needed to define the altered operational environments because information technology has rapidly been changing, especially networks and PCs. It successfully refers to interaction between the physical and digital worlds. It combines the strategic idea of data, information and knowledge, and directs that in our desired direction. That is why it is used to describe the world we live in. Our modern lives and companies, as well as our society, rely heavily on the use of the word “cyber” and “cyber” has taken root in international languages (Limnéll, 2014, 30-31).

2.2 The price without cybersecurity

Cybersecurity is a perfect illustration of why the society and businesses need to think about security holistically. Cybersecurity exists, and it has access to all levels of protection. Cybersecurity is not like a layered cake where you merely put a cherry on top of the cream that has already been applied. It should be known right from the start while baking a cake with its ingredients (Limnéll, 2014, 15).

When it comes to cybersecurity, there are two things to bear in mind. First and foremost, cyberthreats are real and they may be pretty dangerous. The cost of being irresponsible will rise. Second, there is a positive side to cybersecurity in the form of opportunities that we may take advantage of on a daily basis, both at work and in our spare time. It allows us, businesses, and other organizations to extend their services and operations while also producing new products and lowering expenses. (Limnéll, 2014, 15)

2.3 Campaign between attack and defense

At the moment, the world is divided into two races for the cyber security. Similarly, the battle between the cyber defence and the cyber assault is

intensifying. To ensure safety of the internet, governments, companies, the militaries, and information security firms are all working on to develop the most effective defenses. Simultaneously, on the opposite side, cybercriminals, foreign nations, and hacktivists are continually conducting innumerable assaults on the defender's systems, looking for weaknesses and holes in the protection. The attacker's methods become more sophisticated and devious. Simultaneously, the defence side makes every effort to prevent the attacker from succeeding. There are now two races taking place throughout the globe for dominance in the cyber realm. In addition, the battle between cyber defense and cyber-attack is becoming more intense (Limnéll, 2014, 21).

For example, the same logic has been used in the creation of weapons and counter-weapons throughout history. As an example, the armoured tanks first appeared on the French Somme battlefield in 1916. The armoured tanks seemed to be a stronger opponent at first until an armored assault weapon was produced. Since then, for over a century, there has been a constant race between the tank development and anti-tank weapon development, with various interests on both sides. The defenders are always being targeted by cybercriminals and other nations, as well hacktivists, who are continually looking for weaknesses and holes in the defense (Limnéll, 2014, 21). There is a similarity in the business world as well.

3 'THE ART OF WAR' IN CYBERSECURITY

Cybersecurity is like a war and military leadership that are the first structured forms of human civilization (Limnéll, 2014, 75). The ancient Chinese military strategist, Sun Tzu, would agree: "The best defence is to avoid attack in the first place." Sun Tzu's "The Art of War" has been adopted by some of the world's most successful cybersecurity experts and professionals for its guidance and advice on how to prepare for and handle battle. Much of it is devoted to outwitting adversaries without engaging in combat (Securitymagazine, 2021). The work of Sun Tzu is the cultural heritage's oldest and most dazzling piece. His work has

gained popularity in recent years as society and businesses scramble to comprehend today's prospects and difficulties (Limnéll, 2014, 76).

3.1 Sun Tzu's methods

The work, although, it was written almost 3,000 years ago, the teachings contained may help nowadays security professionals in establishing key security concepts. In cybersecurity, by approaching Sun Tzu's methods provide businesses with an understanding of what to look for, what vulnerabilities pose the most danger, and how to build suitable incident response processes (Securitymagazine, 2021). Focusing on these five methods will have a huge influence on the "battlefield".

3.1.1 There is always human

First and foremost, Sun Tzu's teachings have a psychological and leadership aspect. To sum it up, Sun Tzu's psychological leadership consists of guiding his own troops and participating in psychological warfare against the opponent. Consider the fact that cyber security is always a human endeavor. Somebody somewhere has chosen to act via the cyber world before any cyber assault happens or a defensive mechanism is established. (Limnéll, 2014, 76)

3.1.2 Don't overthink

Second, Sun Tzu advises that we should focus on our own preparation to meet enemy assaults rather than on the possibility of an enemy attack. It is critical to have a self-contained operating capability that can be depended upon in all circumstances. At the same time, it must be recognized that everyone is a target of cyberattack (Limnéll, 2014, 76). It is good to know that attackers will be educated to recognize their victims and would have conducted research on all possible routes and vulnerabilities. Organizations should analyze all possible points of entry and potential risks. (Madsen, 2017)

3.1.3 Adapt to the environment

Third, to keep up with the continual vigilance in the cyber environment, both defensive and security system must be constantly evolving. Like Sun Tzu once said, “Therefore, just water retains no constant shape, so in warfare there are no constant conditions” (Limnéll, 2014, 76). This happens all the time in any other branches. That’s why we need to keep an eye on the future and try to predict it. In this situation, all areas of a company’s cyber security need to be improved constantly.

3.1.4 Basic things come first

Fourth, “Appear weak when you are strong, and strong when you are weak” works quite well (Limnéll, 2014, 76). Putting the basics in order improves the company and society’s cybersecurity without requiring too many complicated things. When new subjects need a different way to approach to understand how it generally works, the most difficult step has been taken. After keeping one’s eye open, it is much simpler to have a better understanding of the subject. (Suomen Automaatioseura, 2021, 72)

3.1.5 Know your enemy

Fifth, while developing a plan, every creator should examine objectives as well as seek a balance between goals and available resources. However, the beginning point for anything is always being aware of one’s own vulnerabilities and risks. It is critical to identify the dangers while designing cyber strategies and selecting the required degree of protection. In order to achieve, one must be aware of one’s own capabilities, limitations and strengths. This is true for both human and technological processes. Everything is needed to succeed in safety in a cyber environment. “If you know the enemy and know yourself, you need not fear the result of hundred battles. If you know yourself but not the enemy, for every victory gained, you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle” (Limnéll, 2014, 77).

Even Sun Tzu taught battle tactics thousands of years ago. These notions are not just timeless but also adaptable to cybersecurity. The person who understands how to apply these concepts in the cyber environment is vital.

4 THE BEGINNING OF CYBERSECURITY

When the Internet and wireless network standards such as Bluetooth and Wi-Fi, a significant growth of smart devices and the different devices of Internet of Things became in this world by mankind, cybersecurity is still growing considerably due to the increased dependence on a computer system. Cybersecurity is still one of the major challenges in business and technology in the modern world. A natural question is, where did it all begin? Let's take a look at the brief history of cybersecurity from its inception to nowadays. (Danes, 2021)

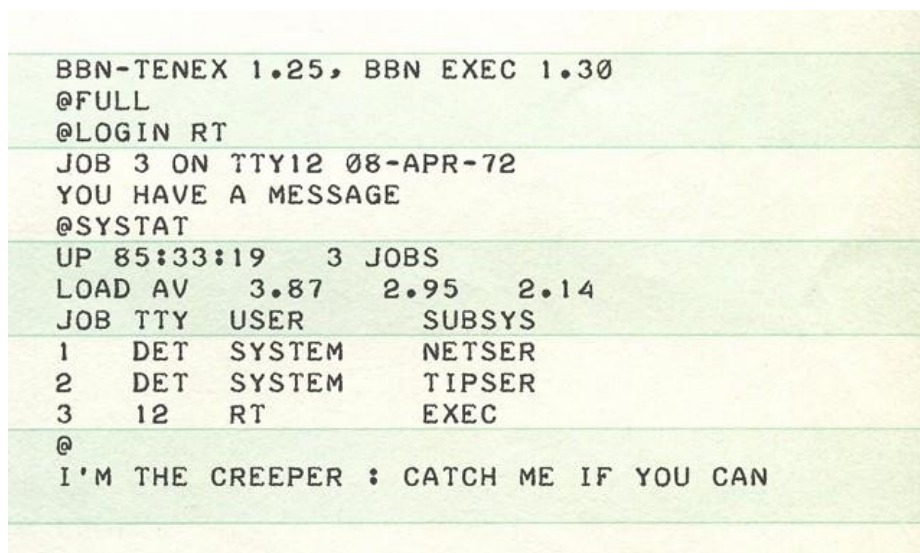
4.1 Before it all started

The world's first operational storage-program computer was designed by Sir Maurice Vincent Wilkes in 1946, who read Hungarian-American mathematician Jon Von Neumann's draft of report and machine description that led to the construction of the EDVAC in 1945 after World War II. The following year, Maurice Wilkes, helped design in Cambridge University a machine called Electronic Delay Storage Automatic Calculator (EDSAC) that would officially become the world's first operational stored-program computer (Lemelson, n.d.).

In 1969, the router was connected to the network, and it was the sole device on the whole network. It was unable to transmit any data until researchers from UNCLA and Stanford University tested the new connection. The first data packed moved online (Hyppönen, 2021, 22). However, the real cybersecurity started 30 years later in the 1970s when the Creeper worm was coded.

4.2 How it all began

It all began in the 1970s, to be precise in 1971 when a researcher, by the name of Bob Thomas, created a computer program called Creeper that was able to move across an experimental ARPANET's (The Advanced Research Project Agency Network) network, leaving a small trail wherever it went. Creeper was the world's first example of the virus and a computer worm (Danes, 2021). The computer screens displayed the phrase: "I'm the Creeper, catch me if you can!". (Matthews, 2019)



```
BBN-TENEX 1.25, BBN EXEC 1.30
@FULL
@LOGIN RT
JOB 3 ON TTY12 08-APR-72
YOU HAVE A MESSAGE
@SYSTAT
UP 85:33:19 3 JOBS
LOAD AV 3.87 2.95 2.14
JOB TTY USER SUBSYS
1 DET SYSTEM NETSER
2 DET SYSTEM TIPSER
3 12 RT EXEC
@
I'M THE CREEPER : CATCH ME IF YOU CAN
```

Figure 1 - Printing message "I'M CREEPER CATCH ME IF YOU CAN" (SentinelOne, 2019)

Ray Tomlinson, who invented email also wrote the program Reaper, by redesigning Creeper, which identified and deleted the malware Creeper. Reaper was the world's first anti-virus software and the first self-replicating program which created the first-ever computer worm. He took Creeper to the next step, making it self-replicating and the world's second worm was born. (History Computer, 2021)

4.3 The beginning of the commercial antivirus

During 1980s, the world still lived in the Cold War time. East and West's computers started to be become more and more connected, in other words

computers were started to be used for military purposes, and so computer viruses also became more advanced. Both sides did the steady assaults of innovative hacking techniques which was too much for information security system to handle.

Here are some examples of what has happened in real life. The Soviets first used cyberpower as a weapon in 1986 when they hired a German computer hacker, Marcus Hess, to acquire US military secrets. He hacked into nearly 400 military systems, including Pentagon mainframes, with the intention of selling their secrets to the KBG. His mission failed because he was prevented. (Murphey, 2019)

Two years after the incident, in 1988, the Morris Worm was born, marking one of the most significant turning points in the history of cybersecurity. The network's use began to rapidly spread, with more and more colleges, militaries, and governments becoming linked to it (Murphey, 2019). As a result, the requisite security measures had to gradually grow more expensive, giving rise to the Morris Worm.

The Morris Worm, named after its creator, Robert Morris, was designed to spread over networks, penetrate terminals using a known bug, and then duplicate itself. Its purpose was to find a weak point in a network intrusion prevention system (Murphey, 2019).

There was one bright thing during the 1980s: although there were conflicting for the inventor of the first antivirus product, 1987 was the birth year of commercial antivirus. Two young computer science students, Kai Figge and Andreas Lüning, who met each other in a copy shop developed their first antivirus program for the Atari ST in 1987 because both were minded and had a soft spot for it, the same year that Ultimate Virus Killer was introduced (AG, 2018). During the same year, two Slovakian students, Miroslav Trnka and Peter Pako, who founded an antivirus program NOD (ESET nowadays). NOD obtained an award which aided

the firm in establishing subsidiaries in the United States, Argentina and Singapore, as well as development facilities in Poland and the Czech Republic (Wikipedia, 2021).

John McAfee sensed a financial opportunity and he set up about developing anti-virus software that could identify and eliminate computer viruses automatically. McAfee decided to found McAfee Associates Inc. In the same year like a couple of Slovakian guys did in 1987 to offer this program, which he named VirusScan. This was the first anti-virus software to be released in public, as well as one of the first software products to be distributed through the Internet. (Wikipedia, 2020)

Some understanding on people's motivation and mindset while utilizing malware: back in the 1980, people used malware as a joke with no malicious intent to cause confusion. 1990s, people's attitudes started to change toward malware (Lin, 2019). By the end of the 1980s, it was rare for a home to be without a PC. People used them for work, playing games and a variety of other activities, such as communicating with others on the workplace network and using other business-related applications. As more individuals bought computers in the 1980s, they also became more appealing and user-friendly. (The People History, n.d.)

4.4 Advanced criminals

With the general availability of the Internet, more people began posting their personal information online. Organized criminal groups views this as a possible source of cash and began stealing enterprises, people, and government's data over the Internet. By the mid-1990s, network security risks had grown tremendously, necessitating the mass production of firewalls and antivirus software to safeguard the public (Danes, 2021). The number of new viruses and malware skyrocketed in the 1990s, rising from tens of thousands in the decade to 5 million every year by 2007. By the mid-1990s, it was obvious that cybersecurity

needed to be mass-produced in order to safeguard the public. There was one researcher of NASA who created the first firewall program. As a result of the increasing need of data protection, a new area known as ethical hacking has evolved.

4.5 Threats diversify and multiply

Cyberattacks began to be widely funded by crime syndicates in the early 2000s, which resulted in harsher penalties for those who were found guilty. In addition to the advancement of information security, viruses also arose as the Internet expanded in popularity among people (Danes, 2021).

Cybercriminals were able to take advantage of more gadgets and software vulnerabilities than ever before because of the widespread availability of the Internet. Plundering became easier as more and more information was being stored online (Chadd, 2020).

Hackers began replacing clean pages with infected ones of hiding malware on legal websites in 2001, a new infection tactic emerged: users no longer needed to download files but just browsing an infected website as well was enough. Viruses intended to spread over IRC (Internet Chat Relay) also started to appear, and instant messaging services were also targeted.

4.6 Meaning of cybersecurity increases

At a rate of knots, the cybersecurity sector is expanding at an exponential rate. According to Statista (Statista, 2017), the worldwide cybersecurity industry is expected to rise to USD 345.5 billion by 2026. Ransomware is one of the most prevalent dangers to any organization's data security, and it is expected to continue to grow in popularity. In other words, hackers are doing it for money, fame or even ideologies.

Over the last decade, we have seen the fast expansion and evolution of cybercrime. What was once a cottage industry, has now evolved into a multibillion-dollar enterprise. As we know, attackers have created new harmful programs and methodologies, which resulted in a rise in both the rate of cybercrime and the number of cyberattacks each day. We are talking about billions of dollars that were lost. Major corporations began to hire more cybersecurity professionals to combat the danger of threats. Cybercrime has been expanded over the last ten years, so cybersecurity business has expended so much. (Arctic Wolf, 2020)

During the 2010s, we have had massive data breaches, for example WannaCry ransomware happened in 2017 and was a pretty big issue for Windows users, years of prolific hacktivism, cyber-espionage by the nations and industry and malware that has made systems inoperable. We could say that the most significant event was the Snowden revelation. Snowden's disclosures started the creation of surveillance programs in China, Russia, and other countries, as well as an increase in cyber espionage (Cimpanu, 2019).

4.7 Next generation and new challenges

Despite the COVID-19 pandemic's effects, according to International Data Corporation that IT Security expenditure is predicted to climb 8.3 % year by year in 2021. (IDC, 2021) As the influence of Covid-19 has affected towards telecommunication on a worldwide basis, this fact has become more clear. More and more people are using their home Wi-Fi networks to connect to corporate servers for the first time. Taking advantage of the Covid-19 fear and social engineering, many sophisticated assaults have been already made against crucial healthcare infrastructure, as well as government communication channels. (Discoverpc, n.d.)

At this point, we might need a new fresh viewpoint at this moment. Society, firms, and nations are going to face many things to diversify their cybersecurity to fill up

as many gaps as possible. We have to invest in a wide range of point solutions to achieve a complex defense ecosystem.

Participants at this year's World Economy Forum annual meeting, which brings together the world's top academics, politicians, business, youth and civil society leaders to discuss the most important global challenges. One of them is cybersecurity.

Internet users will face the same problems of misinformation and cyberattacks in developing countries as those that are more technologically advanced.

Successful business leaders will require a strong culture of cybersecurity within their organizations. In order to secure the best possible cybersecurity and digital trust, leaders need to adapt and adopt the proper methods and develop successful alliances. In 2020, cyber-risks have undergone significant changes as a result of the emergences of new technologies and new users. 5G has opened up a wide range of new possibilities. (World Economic Forum, 2020)

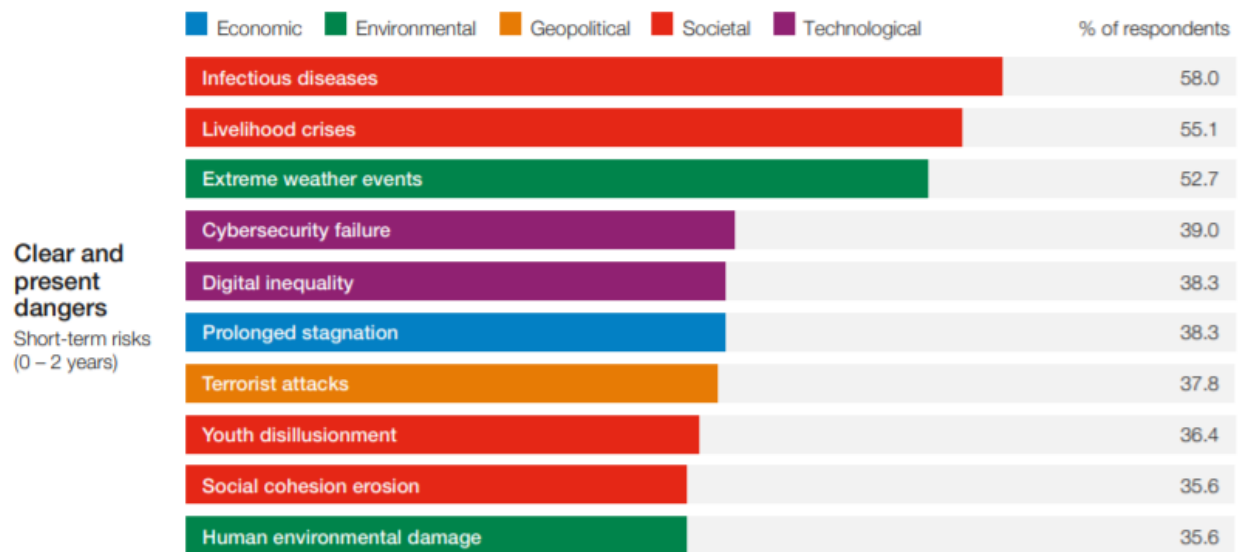


Figure 2 – Global Risks Horizon Report 2021 (McLennan, 2021)

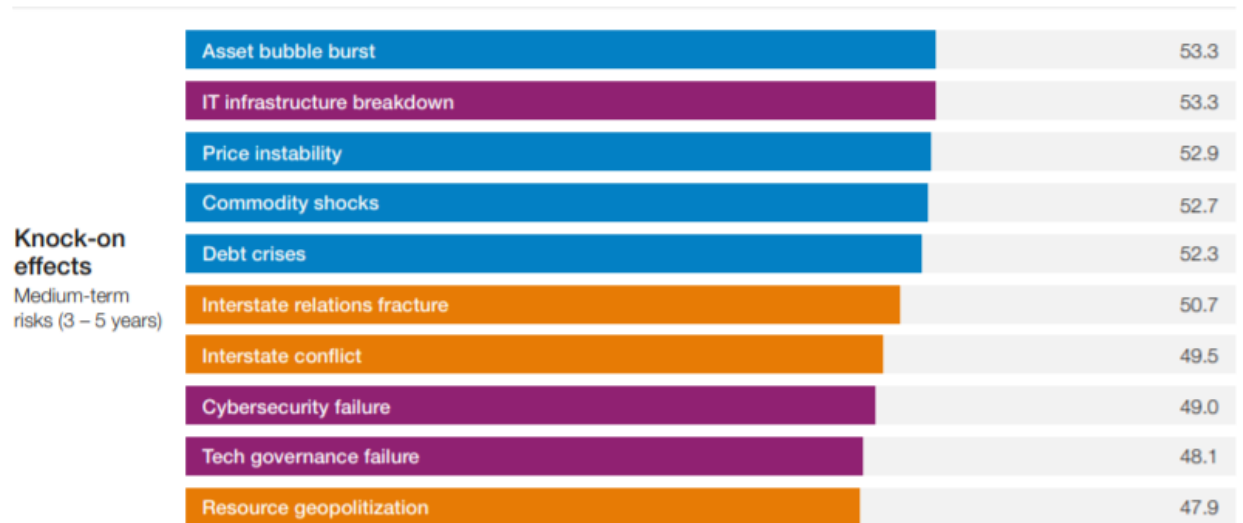


Figure 3 - Global Risks Horizon Report 2021 (McLennan, 2021)

According to the Cybersecurity Guide for Leaders in Today's Digital World (World Economic Forum, 2019, 5): in the next decade, cyberattacks are expected to cost USD 90 trillion if cybersecurity measures do not keep pace with technological advancement. A lack of executions of recommended actions are continuing to fall short of what is necessary to provide effective defense against cyberattacks. Nowadays, in this technologically advanced world, cybersecurity is no longer only the duty of a single Chief Security Officer, rather it's a responsible for everyone in a company. (World Economic Forum, 2020)

4.8 Upcoming challenges

After 2020, we have developed 5G which has better dependability, better lighting speed and reduced latency which is welcomed by both business and people in telecommunication. However, there are some risks of 5G. These demonstrations the promise of 5G, we are still long way from being there. 5G network will connect much more devices than 4G network, the security risks that are existed on the latter network will likely be amplified much more on the former. ISPs might be the first point of failure during a cyberattack if current security vulnerabilities are not addressed and carried over into 5G era, from baking to healthcare might suffer because 5G issues are still being researched.

IoT will link billions of devices, which opens up several entry points into a business if it is left unprotected. Why are they called “a minefield”? A potential minefield of security outbreak awaits many enterprises, industries and especially healthcare IT systems where cyber hygiene, software patches and upgrades will be temporarily neglected. Many corporations are already taking steps toward that end to approach IoT devices to keep them as secure as necessary. (Discoverpc, n.d)

5 PRESENT STATE OF THE CYBERSECURITY IN FINLAND

At this point nowadays, cybersecurity is one of the most rapidly growing sectors and a constantly changing environment of dangers that are threats on state economies, private companies, and people. Cyber threats are becoming sophisticated, which is involving all of state’s operations, as well as its security and defensive systems. Cyber techniques are used to sway democratic elections in several nations and the military has to make an effort to defend against assaults. These cyber tactics can be deployed against foreign nations in an effort to weaken them or to act as a deterrent against perceived threat (Antczak, 2018, 6). EU has a remarkable role to play in the sphere of cybersecurity, but instead we will focus on Finland’s cybersecurity strategy.

Table 1 - Thematic Scope of National Security Strategy (Antczak, 2018, 10)

Country	Addressing cybercrime	Keeping balance between security and private	Developing national cyber contingency plans	Establishing a public-private partnership	Establishing baseline security requirements	Holding cybersecurity exercises
Denmark	x	-	x	-	-	x
Finland	x	x	x	x	-	x
Italy	x	x	x	x	x	x
Ireland	-	-	x	-	-	x

Finland has been taking seriously to achieve the goals of national cybersecurity strategies. According to Table 1, Finland has its own cybersecurity plans, which should be noted. This is for respecting people to process of personal data and on the free movement (Antczak, 2018, 19). Finland takes seriously the risk evaluation of networking communication, purchases and manufacturers into consideration national security to subject to cyber security measures (Suomen Automaatioseura, 2021). Generally Finland humbly accepts the directives of the EU of cybersecurity strategies because Finland is a role model in the EU, regardless the directives the EU commission gives.

Most concerning things for Finland are data breaches and theft, but cybercriminals are undoubtedly the single largest danger category, those who aim to steal money via hacking. Finland has experienced assaults on ordinary life by the states, for example, Russian and Chinese espionage assaults are prevalent in Finland (Yle, 2017).

Cybersecurity is being tested every day by the Defence Forces, who have increased their cyber capacity so much. Cybersecurity has also become an essential aspect of the society's ability to operate because digital systems are becoming more and more important in our daily lives and in the workplace. Finland is one of the world-class levels of cybersecurity as a model student of EU, but there is always a room for improvement. (Yle, 2017)

Finland's National Coordination Center for cyber security matters was established by the Finnish government on 30 September 2021. The new duty would increase the Cyber Security Centre's role in aiding Finnish business and industry. Its function would be strengthened by collaboration with European Cybersecurity Competence Centre and the network of national coordination centers created by EU Regulation. (Valtioneuvosto, 2021)

6 PROBLEMS DURING RESEARCH PROCESS

The relationship between questions and objectives were faced during the internship and thesis that this thesis will be presented. The objectives were discussed with my supervisor. The first issue occurred during the project time was my lack of knowledge in the field at the beginning. Looking the project by multi-perspective was challenging; therefore, it was difficult for me to have the overview of the project. Furthermore, the project was accomplished by self-effort resulting in longer time on researching.

6.1 Research questions

During the meeting with my supervisor, we listed the goals that we wanted to achieve. The problems occurred during the project leading to some questions:

- What kind of model of SIEM will be?
- What are the tools and how to get it?
- How theoretically does it detect, prevent, and handle an incident?
- How does it support in MPY?
- Will there be any expenses?
- Is it possible to productize the model?
- Is it possible to get support from AT&T?

6.2 Research objectives

The objectives of this thesis are to achieve the goals of building an open-source tool model and get answers for the research questions:

- A model of SIEM & SOC will be built by using AlienVault OSSIM.
- The tools that will be used are a sensor and plugin.
- The model will use a sensor to detects the incidents
- The model would be very useful for MPY
- There aren't any expenses because it is open-source.
- This might be possible when the model has been deployed, operated and usage. At this stage it is only for deployment.
- It is not possible. OSSIM is open-source, and no one really looks after it. Must do it on our own.

7 LOG DATA AS SUPPORT OF INFORMATION SECURITY IN MPY

Cybersecurity and information security are part of corporate security. The company's most valuable assets, such as people, information, reputation and the environment, are safeguarded from threats. The company's main goal is to increase competitiveness and productivity which is part of the company's management strategy. MPY wants to achieve a high level of corporate security and risk management, which is the best interest of business. As a result, to achieve to be positively different in the market.

People, information, reputation, property, and environment are all protected by security measures. Corporate's primary goal is to boost the company's competitiveness and productivity as high-quality corporate security and risk management are also a way for companies to stand out positively in the market. (Elinkeinoelämän keskusliitto, n.d.)

The process of developing and constructing a log management could be separated into many stages. This stage focuses on development of the log management. This development project is performed for MPY itself. To begin with, the first step is to discuss and do a research of the development's resources. After that a roadmap and the project's goals will be decided. The final step of the project is practical - implementation and maintenance are not included in the project.

The first step is to understand what is log data. A log is a kind of event log, a type of journal. A good example for this is a voyager's events are all documented (Wikipedia, 2019). In other words, the log files are used to keep track of the operating systems, applications and softwares. In this case, SIEM is used. You may use any endpoint in a workstation as a primary device for tasks. A local log is created by the operating system and several applications on a device. In this case, for example domain controllers, BYOB, servers, network devices and more (Petters, 2019). When it comes to the log management, sometimes it is

hard to define what is the right amount of logs but at least the most important thing is that a log including following information: users' actions, where, when, who, from where and was the operation successful (Suomen Automaatioseura, 2021, 183).

8 IDEOLOGY OF SOC SIEM

Two important terms in this project are SIEM and SOC that are important concepts in cybersecurity. What are the solutions and difference between SIEM and SOC?

8.1 SIEM

SIEM stands for Security Information and Event Management which is a subfield of cybersecurity in which software products and services integrate SIM (Security Information Management) with SEM (Security Event Management), and it is provided by vendors. According to Figure 4, it analyzes and gathers historical security events issued by, for example, software, applications, network devices in real time to support threat detection, compliance, record security, and create reports. It also normalizes and aggregates data from a wide range of sources across the whole IT infrastructure. When we are talking about unknown threats, they could be possible insider threats, phishing attacks and DDoS attacks (37). SIEM was invented by Gartner's Mark Nicolett and Amrit Williams. (Wikipedia, 2019)

SIEM has grown to be a \$2 billion market, yet only 21,9 % of those companies are gaining value from their SIEM (Petters, 2019). But SIEM is not like a 'plug-and-play' product. SIEM can be bought or built by yourself by using open source SIEM which we have used it for this project to build our own "product".



Figure 4 – SIEM process, made by Varonis (Petters, 2019)

SIEM is beneficial because it reports and investigate the security breaches, and it collects massive amounts of data from your whole network and presents data in a way that is understandable for humans. Giving an example to see a whole picture how SIEM works: SIEM classifies the data into many categories, such as successful and unsuccessful logins to see, for example, if it is potential harmful behavior or other malware. For example, there is an employee who came from a long summer holiday and after returning back to work with empty mind he creates 15 unsuccessful login attempts in 15 minutes. SIEM keeps it as low priority because it is mostly done by an employee who has forgotten his login details.

Another example is that there is a user who creates 100 unsuccessful login attempts in 6 minutes that would be classified as a high-priority event because it might be a bruce-force attack that is in process (Rosencrance, 2020). SIEM provides an additional beneficial for improving system by allowing the security team to discover the path of an attack that travels throughout the company's

network, identify the sources that have been compromised and also gives automated measures to block the assaults in the first place.

8.2 SIEM in business and future

SIEM is a tool that helps businesses identify and mitigate possible threats and vulnerabilities before they change to affect to company operations. SIEM is still evolving after many years to become more than just a log management tool. Whatever the size of a company is, SIEM system provides a wide range of advantages for business, and they will become an important part of optimizing security processes/projects.

AI is expected to take a huge part in the future in SIEM, since cognitive capabilities are making systems able to make better decisions. Other endpoints as IoT, cloud, mobile and other technologies will produce more log data that SIEM can handle (Rosencrance, 2020). In this case MPY is trying to develop a SIEM solution to strengthen the company's security posture. Without SIEM, it would be time-consuming that the login data are collected manually and analysis reports conducted by an employee.

8.3 SOC – Security Operation Center

As mentioned, that SIEM system is related and managed within a SOC. What is SOC? When it comes to protecting business from cyberattacks, SOC is a command center facility for a team of IT specialists who have experiences in information technology (Lewis, 2020).

SOC all the time monitors the signals that are implemented all of these systems including internet traffics as well as the networks that connect them. SOC is its own department with SOC staff members, could be in-house or a vendor service provider with advanced IT skills and cybersecurity expertise. Basically, SOC works for 24 hours and seven days a week for reducing and tracking risks with work shifts and trained staff. (Lewis, 2020)

8.4 SOC in business and future

SOC plays a critical role in reducing the financial impact of data breaches in companies and many different organizations. The company has to identify its own cybersecurity strategy in order to connect it with its present business objectives and concerns before building a SOC. The company needs to accomplish those objectives to fulfill those goals as well as what infrastructure and tooling is needed, as well as staffing is needed to accomplish them (Lewis, 2020). A good SOC is well-structured and is very useful.

What is the future role for SOC? SOC will face the expanding technological scenery and also the increasing threat scenery. AI, ML, cloud, edge computing, IoT etc. are all functions that could lead to the exponential expansion of assaults. To stay ahead, companies need to make better analyzes and decision-making for building a SOC (Aria 2020).

Covid-19 has created a significant impact on any company's SOC, but there has been a SOC trend before the epidemic. It is expected that the future of SOC's might need automation for new and evolving threats which COVID-19 speeds up (Wikipedia, 2019).

9 ALIENVAULT & AT&T CYBERSECURITY

A Spanish company was founded in 2007 and named AlienVault and it obtained USD 116 million in funding. In 2018, an American company AT&T finalized its acquisition of AlienVault, making it a fully owned subsidiary and was rebranded AT&T Cybersecurity. This company is the world's biggest crowd sourced computer security platform that has created commercial and open-source services to handle cyber-attacks (Wikipedia, 2019). There are other companies AlienVault competes in the SIEM and network security market with, such as Microfocus ArcSight, IBM QRadar, and LogRhythm.

10 ALIENVAULT OSSIM

MPY ended up with AlienVault because OSSIM is an open-source product of AlienVault that offers to build its own SIEM regardless to be depended on other vendors. AlienVault OSSIM stands for Open-Source Security Information and Event Management which is an open source SIEM. Once again, a SIEM gathers event data from a company's numerous security logs as I mentioned in SIEM chapter. SIEM translates the event data to a format that is understandable, analyzes it, alerts for any questionable events, and generates off the reports on the events. (Scartone, 2015)

When it becomes a product, there is just one version of AlienVault OSSIM and it is server-based only. AlienVault provides two commercial SIEMs: USM Appliance and USM Anywhere but Anywhere is not within this thesis. In short, USM Anywhere product availability is focused on a cloud-based host which focuses on more SaaS services, and USM Appliance is focused on On-Premises and virtual environments. For instance, USM Appliance Logger doesn't include in AlienVault OSSIM (AT&T Cybersecurity, n.d).

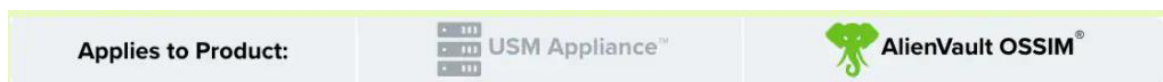


Figure 5 - Applies to OSSIM (AT&T Cybersecurity, n.d)

One disadvantage of this AlienVault OSSIM is the limitation of features due to subset of USM. The main task is to install a sensor and a plugin for a switch, without mentioning the brand. AlienVault OSSIM emblem, an elephant, can be seen on each page in green when a subject applies to AlienVault OSSIM, according to Figure 5. When the feature is grey, it doesn't apply to AlienVault OSSIM. (AT&T Cybersecurity, n.d)

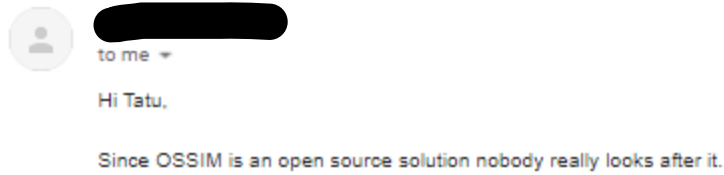


Figure 6 - Email from AlienVault

According to Figure 6, I asked AlienVault staff to help me figure out how to deploy a plugin and sensor but when it is open-source, they won't help you until you have purchased a commercial SIEM.

11 ALIENVAULT ARCHITECTURE AND COMPONENTS

In this chapter, a few basic concepts of AlienVault Appliance will be explained. So, in the first place, USM (Unified Security Management) Appliance system is designed to keep an eye on your assets, such any equipment that is used and has a monetary or functional value to the business. It monitors and collects data about assets' health, availability, configuration, activities and most importantly, events. It is valuable because data is stored, and it travels through the infrastructure. In network world, IP addresses are considered to be assets because they are unique, they are connected to different assets and located in different locations. (AT&T Cybersecurity, n.d, 9-10)

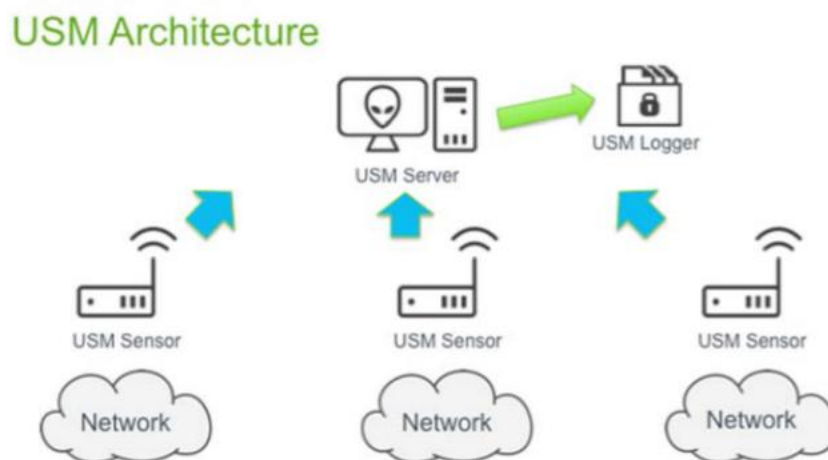


Figure 7 - USM Architecture (AT&T Cybersecurity, n.d)

In this project, we use two different components: a sensor and plugin. According to Figure 8, in Appliance USM sensor is used to monitor a certain geographical area. The sensor transmits information to the USM Appliance Server that represents one certain area. For example, at the XAMK campus each building could basically have one sensor that collects all building's assets which are configured to the certain sensor. The sensor has also other tasks than just delivering data to the server. The Sensor is like in the front line of defense against threats. It normalizes raw log data that will standardize format event and the normalized events are then sent to the server (AT&T Cybersecurity, n.d, 20).

USM Appliance plugins collect and standardize the data from various sources into normal format events, which are sent to the sensor. Plugin is like a sensor's little brother. One asset may have up to 10 plugins enabled and a sensor can have up to 100 plugins enabled (AT&T Cybersecurity, n.d, 11).

According to the Figure 8, USM Logger is the platform's secure data archiving component where it copies event data and is utilized for reporting. (AT&T Cybersecurity, n.d, 20)

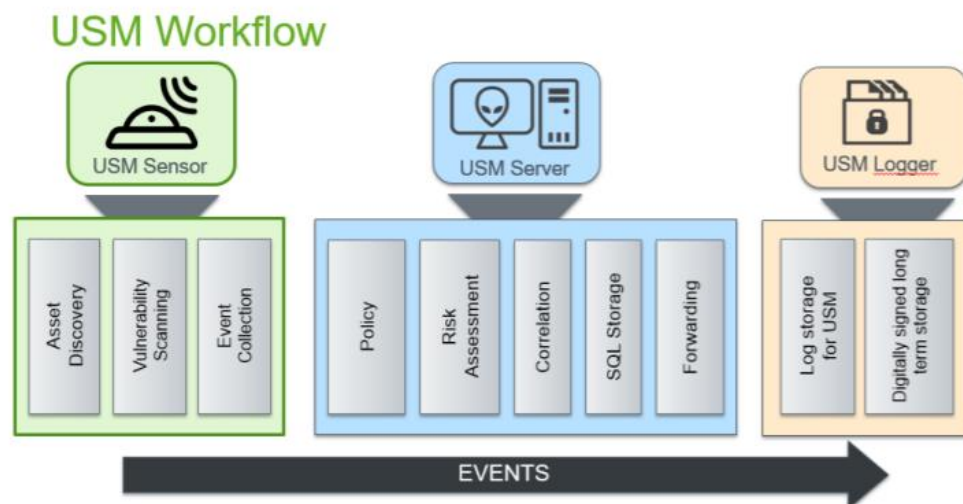


Figure 8 - High level view of events (AT&T Cybersecurity, n.d)

As soon as USM Appliance is installed, it begins to collect data on the many assets that make up the network, including firewalls, routers, switches, servers

and applications. Again, it is collected by a sensor and sent to the server (AT&T Cybersecurity, n.d, 20).

11.1 An easy method to explain OSSIM

- 1) Install AlienVault OSSIM to the virtual machine.

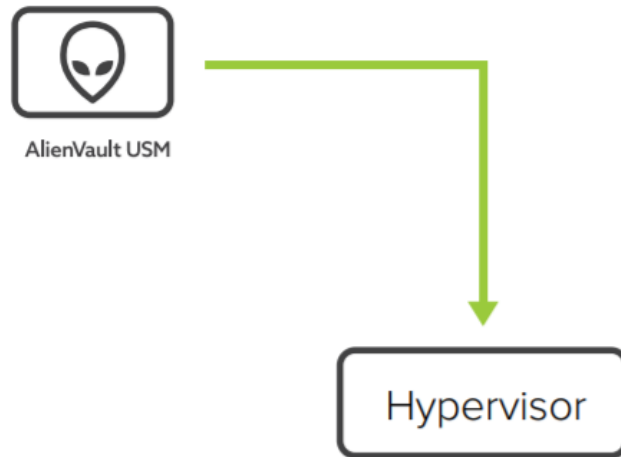


Figure 9 - First step (AT&T Cybersecurity, n.d)

- 2) Configure an interface and deploy sensors and plugins.

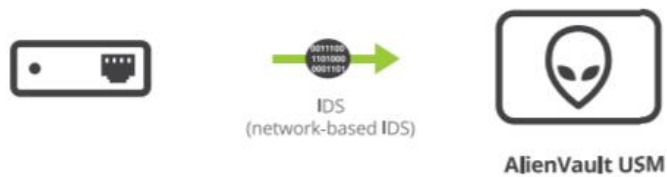


Figure 10 - Second step (AT&T Cybersecurity, n.d)

- 3) Perform a discovery scan to detect assets.



Figure 11 - Third step (AT&T Cybersecurity, n.d)

4) Collect assets' log events and make alarms if suspicious occur.

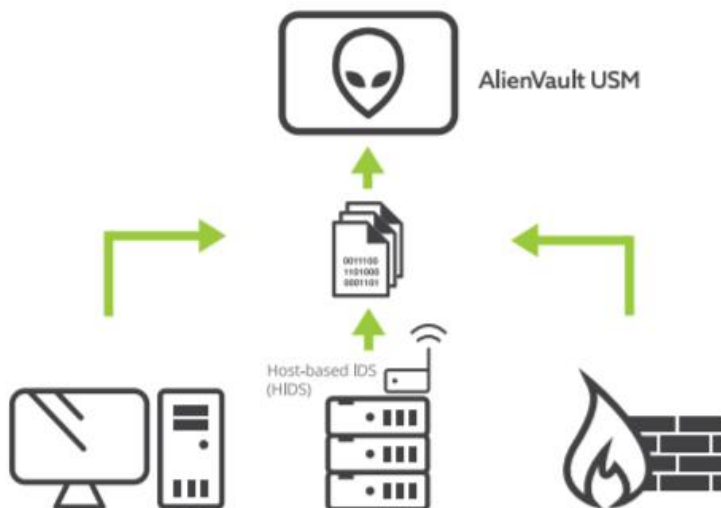


Figure 12 - Fourth step (AT&T Cybersecurity, n.d)

5) Identify threats and investigate incidents and check reports.



Figure 13 - Fifth step (AT&T Cybersecurity, n.d)

12 ALIENVAULT OSSIM INSTALLATION PROCESS

AlienVault OSSIM ISO file is available for free and can be found on the AlienVault OSSIM product webpage. The installation was done in the other sector which handles networking and servers where I don't have access. The reason for this is the company policy that only limited staff has access to the networking sector. There are the recommended system requirements to a PC's hard drive as follows (AT&T Cybersecurity, n.d):

- 8 CPU cores
- 16 - 24 GB RAM
- 500 GB – 1 TB HDD
- 1000 – 2000 EPS compatible network card

You will have to choose from a variety of settings as you go through the installation procedure, including the network configurations like IP Address, netmask, Gateway and DNS Server Address. Then you have to set up a root password that will be used for the AlienVault OSSIM console.

It was installed in a virtual machine where I logged in by using RDC. Then to begin using AlienVault OSSIM is to open the web browser and type the configured IP address that was used in the setup process.

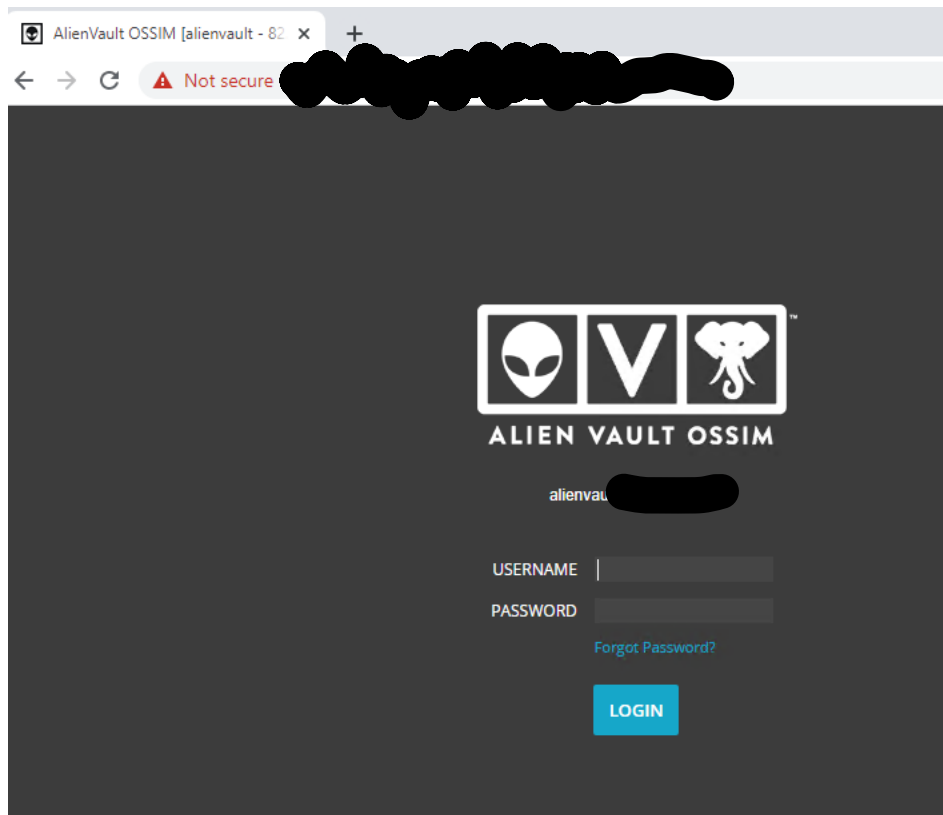


Figure 14 - WEB UI access

13 TOOLS

As it was mentioned, OSSIM is an open-source solution. The staff of AlienVault doesn't help process further because the 'introductions' are very approximate, not step-by-step introductions, and you have to figure it out by yourself how to manage to install plugins and sensors. OSSIM includes self-developed tools. I'm allowed to show some screenshots from my work but I can't show the whole dashboard of the AlienVault OSSIM because I have a NDA. It includes sensitive data. Instead, some other screenshots will be shown in following chapters.

13.1 Sensor

When the installation is done, we want to configure an AlienVault OSSIM sensor using AlienVault Console through SSH and the credential to log in.



Figure 15 - AlienVault Console

When the console is open, the AlienVault Setup menu displays.

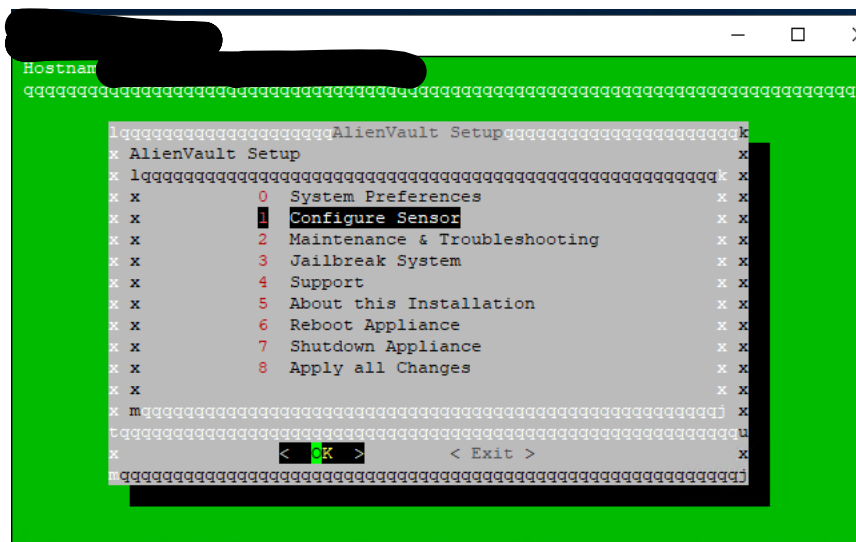


Figure 16 - Setup menu

We select “**Configure Sensor**” and then “**Configure AlienVault Server IP**” by adding the server IP that you used for installing AlienVault OSSIM. The configure sensor menu pops up again and select ‘**Configure AlienVault Framework IP**’ where you type the same IP address you did for the server and in the end, you confirm the changes.

We go back to the Web UI to check if the sensor is there. The path is:

Configuration > Deployment > Components > Sensors. There you can add a

specific description for the sensor and check its status. (AT&T Cybersecurity, n.d)
In some cases the sensor can be automatically installed during AlienVault OSSIM installation process.

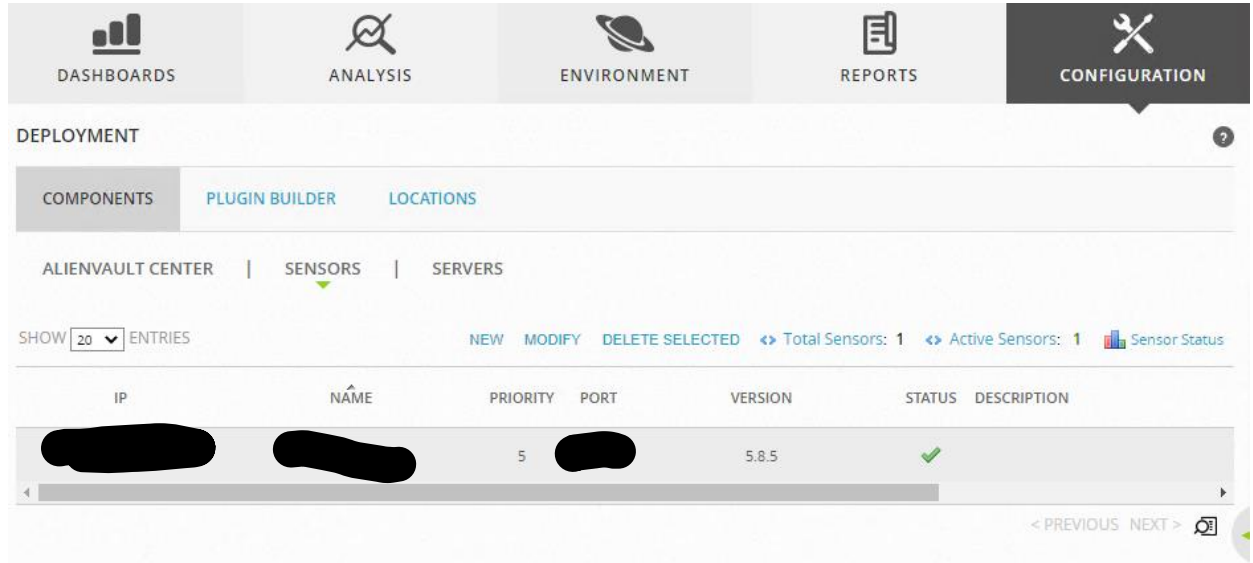


Figure 17 - Sensor

13.2 Plugin

Plugin was the hardest part. Using AlienVault OSSIM, the Plugin Builder is a limited feature. Instead, we must use the AlienVault console to configure a plugin. It can be created from a scratch to modify it or use an existing plugin. This case requires some Linux command skills. There are two ways: select a suitable plugin from a various number of plugins or build it from scratch from an existing plugin. The company chose to use the simplest way, to use an existing plugin because the network device that they use is suitable for it.

First, we open the console and choose 'Jailbreak System'. We type a command **cd /etc/ossim/agent/plugins** and we type **ls**, and after that we get a huge selection of plugins.

```

barracuda-ng.cfg      crushftp.cfg          fortimail.cfg
barracuda-spam.cfg    cryptospot.cfg        fortinet-fortidb.cfg
barracuda-sslvpn.cfg  custom_functions      fortiproxy.cfg
barracuda-waf.cfg     cyberark.cfg          fortisandbox.cfg
barracuda-webfilter.cfg cyberguard.cfg         fortiweb.cfg
baruwa.cfg            cyberoam.cfg          freeipa.cfg
bind.cfg              cyberx-xsense.cfg     freeradius.cfg
bit9.cfg              cylance.cfg           fw1-alt.cfg
bit9_v7.cfg           cyphort.cfg           fw1-cef.cfg
bitdefender-gravityzone.cfg darktrace.cfg         gajproactive.cfg
bitdefender-ntsa.cfg  date_config           gajshield-firewall.cfg
blackboard-learn.cfg  datto-siris.cfg       geist-watchdog.cfg
bluecoat-packetshaper.cfg ddi-frontline.cfg    gfi.cfg
bluecoat.cfg          deepsec-agent.cfg     glastopng.cfg
bomgar.cfg            deepsec-manager.cfg   gta-firewall.cfg
bro-ids.cfg           defender-tokengo.cfg  h3c-ap.cfg
brocade.cfg           dell-chassis.cfg       h3c-switch.cfg
bromium-vsentry.cfg   dell-equallogic.cfg   ha-proxy.cfg
buffalo.cfg           dell-force.cfg         harpp-ddos.cfg
alienvault:/etc/ossim/agent/plugins# █

```

Figure 18 - Existing plugins

As you can see in Figure 18, there are different plugins for different brands of routers, switches and firewalls etc. To choose any plugin, use command **less *the plugin name***, for example, **less byffalo.cfg**.

The next step is to enable a plugin from the sensor configuration in the web UI, which is the fastest way to enable plugins on the sensor. We go to the AlienVault Center.

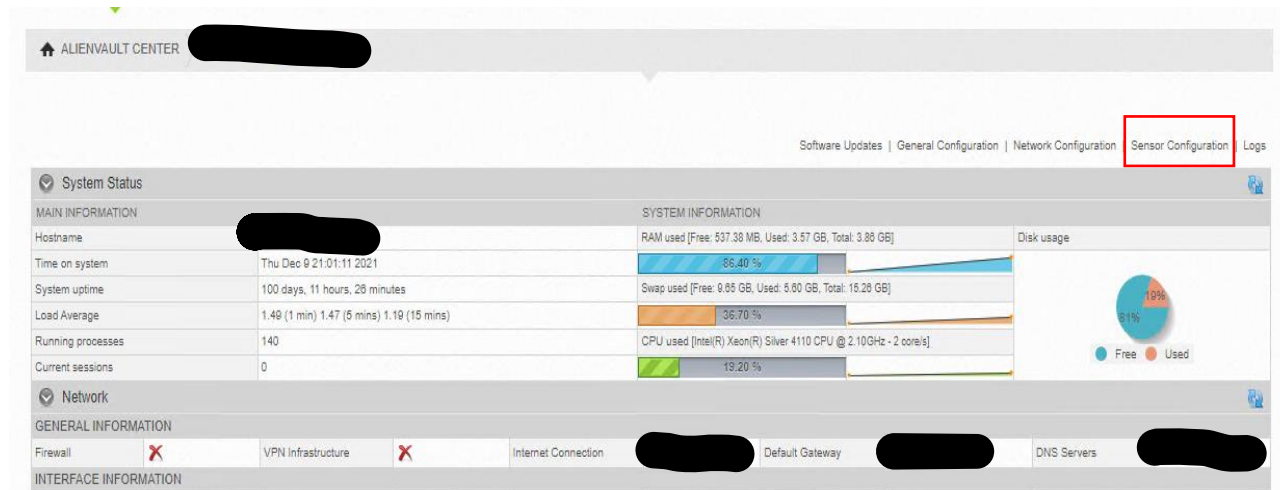


Figure 19 - AlienVault Center

According to Figure 19, we choose Server Configuration and Collection (AT&T Cybersecurity, n.d)

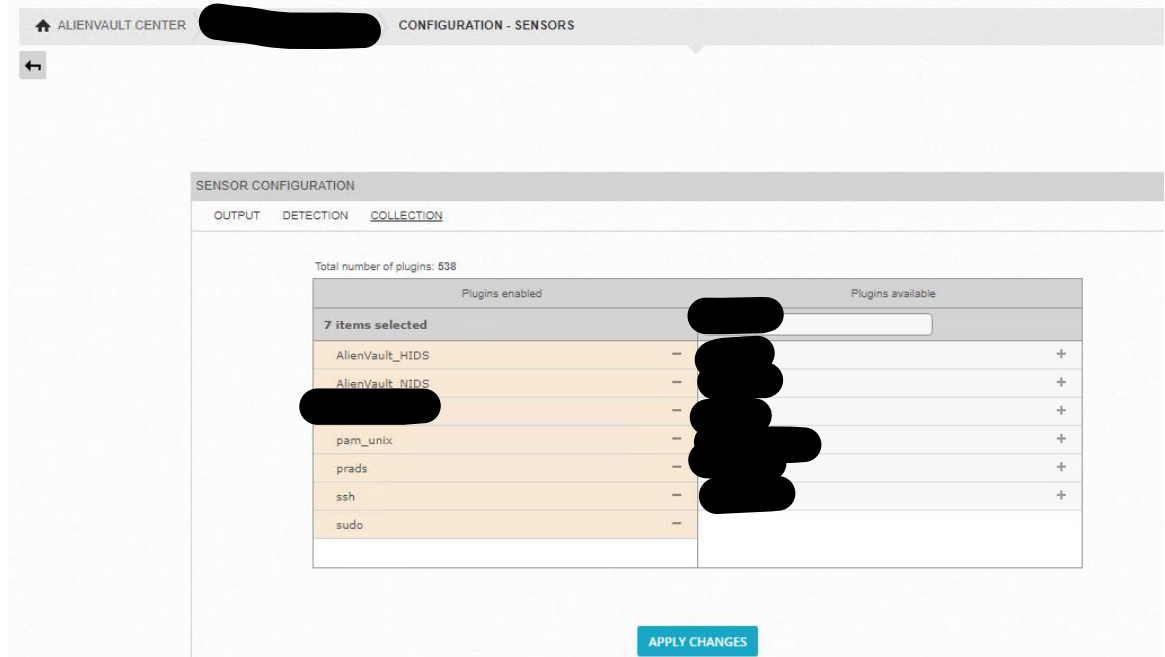


Figure 20 - Enable a Plugin from the Sensor Configuration

On AlienVault console we can check if the plugin is already configured. We select **'Configure Data Source Plugins'**.

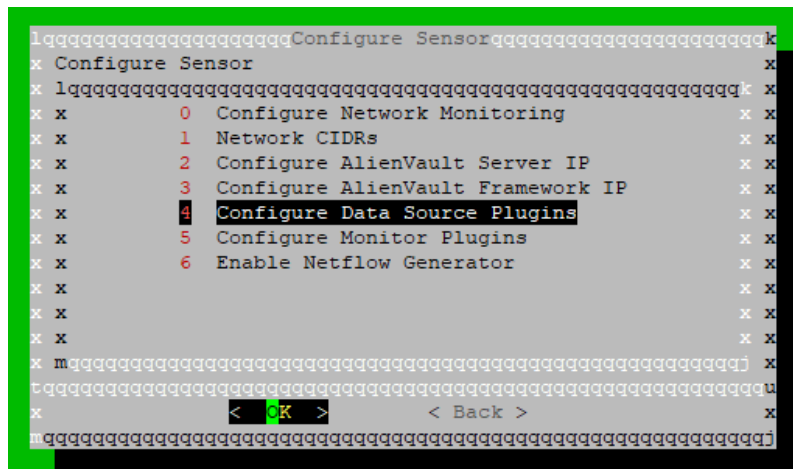


Figure 21 - Configure Data Source Plugins

We can see in Figure 22 that it is already there.

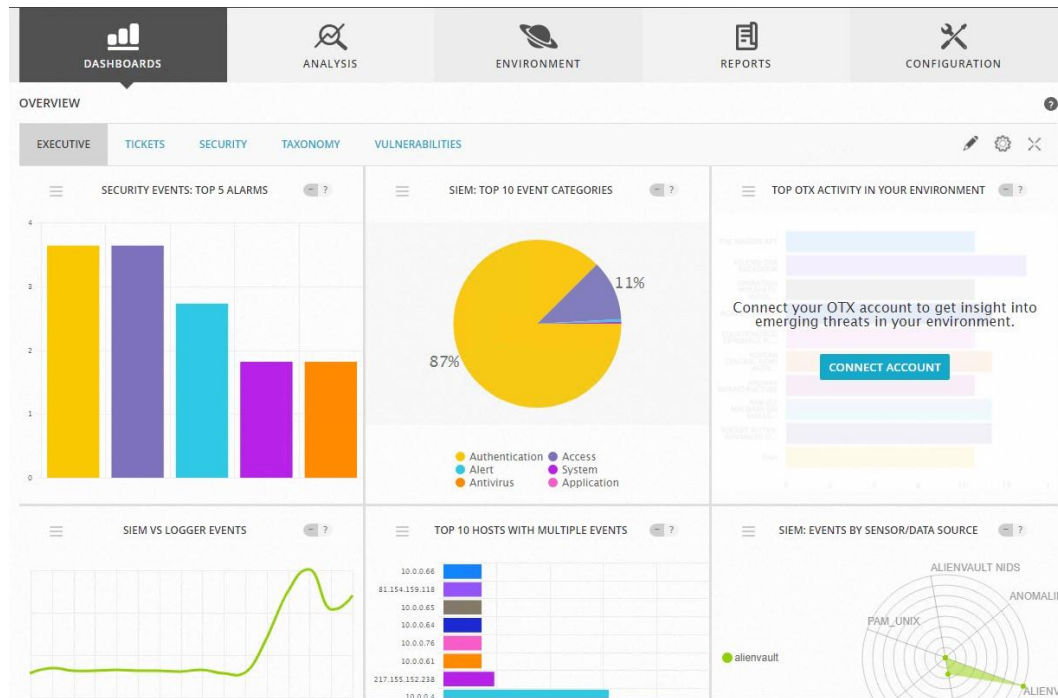


Figure 23 - Example General OSSIM Application Dashboard (Garth, 2018)

The last step is to perform a discovery scan to detect assets. When scanning assets is done, the dashboard would look like in Figure 23. You can see, for instance, alerts, top 5 security events and top 10 hosts with multiple events. (Garth, 2018) Following the NDA, I can't show the real dashboard, instead I show an example.

14 THE VIEW OF PRODUCTIZATION

When we think about productization for this SIEM & SOC product for MPY and maybe in the future for upcoming customers. Many branches have almost the same approaches to productization. Nevertheless, what is productization? Productization refers to the process of making an idea, expertise, or service to find a niche in the market for a particular audience. In this case, MPY tries to sell an IT security program. We must remember that producing a thing is not the same thing as productization (AT&T Cybersecurity, n.d). When we think about the productization from an IT point of view, there are several components working at once.

We have got a restricted amounts of resources to work with. There are a lot of moving elements that affect the future of the company, such as the market situation and other projects in the company (Lynn, 2019). In terms of resources, it could refer to raw material, but it is not like that. Resources can be non-material and harder to control: workers' knowledge, skills, time, and energy (AT&T Cybersecurity, n.d).

Making an IT security product, it follows a multi-staged lifecycle of any other IT service: Architecture -> Deployment -> Operation -> Usage (AT&T Cybersecurity, n.d, 4). In my thesis, we are at the deployment stage. At this stage, employees need to jump into an unknown subject, which takes time and resources to educate themselves. Even if there are setbacks during the project, it is normal, and we proceed smarter.

15 FURTHER MEASURES AND FURTHER RESEARCH PROPOSAL

After having a discussion with my supervisor, as we acknowledged that this project is challenging and remarkable for MPY, it was decided to take it for further development. This upcoming product is useful for MPY and its customers who, can get benefit from it.

R&D can still be done at the deployment stage. In my opinion, OSSEC, which is widely used as a free open-source HIDS, could be crowned the product by installing an AlienVault HIDS agent and making the SIEM stronger.

16 CONCLUSION

This thesis was done at MPY by request to explain what cybersecurity is nowadays, how to approach SIEM and SOC, and how to deploy OSSIM. My work included research work, the basic building of OSSIM, its plugin and sensor. I found OSSIM very challenging, but at the same time it was rewarding to find a way to go forward with the project. The different abbreviations, like SIEM and

OSSIM and the difference between AlienVault OSSIM and AlienVault Appliance are not straightforward to understand.

Even though this project and thesis were huge, it was managed successfully. The sources that were used for this project were selected carefully with updated materials.

REFERENCES

AG, G.D.C. (2018). Inventor of Antivirus. WWW document. Available at: <https://www.inventorofantivirus.com/en/> [Accessed 30 November 2021].

Antczak, J. and Kamiński, K. (2018). Cybersecurity expenditure in the EU member states. PDF document. Available at: <https://newdirection.online/2018-publications-pdf/CYBERSECURITY.pdf> [Accessed 5 December 2021].

AT&T Cybersecurity. (n.d.). About USM Appliance. WWW document. Available at: <https://cybersecurity.att.com/documentation/usm-appliance/system-overview/about-usm-solution.htm?tocpath=Documentation%7CUSM%20Appliance%E2%84%A2%7CDeployment%20Guide%7CSystem%20Overview%7CAbout%20USM%C2%A0Appliance%7C> 0 [Accessed 9 December 2021].

AT&T Cybersecurity. (n.d.). AlienVault USM Virtual Appliance Quick Start Guide. PDF document. Available at: <https://cybersecurity.att.com/documentation/resources/pdf/usm-appliance-quick-start-guide.pdf> [Accessed 12 December 2021].

AT&T Cybersecurity. (n.d.). Configuring a USM Appliance Sensor in AlienVault USM Appliance. WWW document. Available at: <https://cybersecurity.att.com/documentation/usm-appliance/initial-setup/configuring-usm-sensor.htm?tocpath=Documentation%7CUSM%20Appliance%E2%84%A2%7CDeployment%20Guide%7CUSM%C2%A0Appliance%20Deployments%7C> 9 [Accessed 8 December 2021].

AT&T Cybersecurity. (n.d.). Developing ITIL -Mature Security Incident Response With SIEM A Plan for CSIRT Maturity Models via monitoring-driven Kanban Part

1 of 3. PDF document. Available at: <https://cdn-cybersecurity.att.com/blog-content/2011/11/SIEM-for-ITIL-Incident-Response-Part-1.pdf> [Accessed 9 December 2021].

AT&T Cybersecurity. (n.d.). Enabling Plugins from the Sensor Configuration in AlienVault USM Appliance. WWW document. Available at: https://cybersecurity.att.com/documentation/usm-appliance/plugin-management/enabling-plugins-from-sensor-config.htm?tocpath=Documentation%7CUSM%20Appliance%E2%84%A2%7CDeployment%20Guide%7CPlugin%20Management%7CEnable%20Plugins%7C___2 [Accessed 9 December 2021].

AT&T Cybersecurity. (n.d.). Installation of AlienVault OSSIM®. WWW document Available at: https://cybersecurity.att.com/documentation/usm-appliance/initial-setup/ossim-installation.htm?tocpath=Documentation%7CUSM%20Appliance%E2%84%A2%7CDeployment%20Guide%7CUSM%C2%A0Appliance%20Deployments%7C___8 [Accessed 8 December 2021].

AT&T Cybersecurity. (n.d.). USM Appliance Documentation. WWW document. Available at: <https://cybersecurity.att.com/documentation/usm-appliance.htm> [Accessed 8 December 2021].

AT&T Cybersecurity. (n.d.). USM Appliance™ User Guide. PDF document. Available at: <https://cybersecurity.att.com/documentation/resources/pdf/usm-appliance-user-guide.pdf> [Accessed 9 Dec. 2021].

Arctic Wolf. (2020). The Fascinating Decade in Cybercrime: 2010 to 2020. WWW document. Available at: <https://arcticwolf.com/resources/blog/decade-of-cybercrime>. [Accessed 1 December 2021].

Aria (2020). 3 SOC Trends Shaping the Future of Security. WWW document. Available at: <https://blog.ariacybersecurity.com/blog/3-soc-trends-shaping-the-future-of-security> [Accessed 8 December 2021].

Britannica. (2021). Maurice Wilkes. WWW document. Available at: <https://www.britannica.com/biography/Maurice-Wilkes> [Accessed 29 November 2021].

Chadd K. (2020). The History of Cybersecurity. WWW document. Available at: <https://blog.avast.com/history-of-cybersecurity-avast#the-1990s> [Accessed 1 December 2021].

Cimpanu C. (2019). A decade of hacking: The most notable cyber-security events of the 2010s. WWW document. Available at: <https://www.zdnet.com/article/a-decade-of-hacking-the-most-notable-cyber-security-events-of-the-2010s/> [Accessed 2 December 2021].

Danes V. (2021). *The history of cybersecurity*. WWW document. Available at: <https://cybermagazine.com/cyber-security/history-cybersecurity> [Accessed 28 November 2021].

Discoverpc (n.d.). discoverpc.NET - How cybersecurity is changing in the 2020s. WWW document. Available at: <https://www.discoverpc.net/blog/37-how-cybersecurity-is-changing-in-the-2020s> [Accessed 3 December 2021].

Elinkeinoelämän keskusliitto. (n.d.). Yritysturvallisuus. WWW document. Available at: <https://ek.fi/tavoitteemme/yrityslainsaadanto/yritysturvallisuus/> [Accessed 5 December 2021].

Garth, C. (2018). What is OSSIM? WWW document. Available at: <https://espprojects.co.uk/general/what-is-ossim/> [Accessed 12 December 2021].

History Computer. (2021). The First Computer Virus of Bob Thomas Explained: Everything You Need to Know. [online] Available at: <https://history-computer.com/the-first-computer-virus-of-bob-thomas/> [Accessed 29 November 2021].

Hyppönen, M. (2021). Internet. Helsinki: Werner Söderström Osakeyhtiö.

IDC: The premier global market intelligence company. (2021). Europe IT Security Spending to Jump 8.3% in 2021, According to IDC. WWW. document Available at: <https://www.idc.com/getdoc.jsp?containerId=prEUR248131621#:~:text=IDC> [Accessed 2 December 2021].

Lemelson-Mit (n.d.). John von Neumann. WWW document. Available at: <https://lemelson.mit.edu/resources/john-von-neumann> [Accessed 29 November 2021].

Lewis S. (2020). What is a Security Operations Center (SOC)? WWW document Available at: <https://www.techtarget.com/searchsecurity/definition/Security-Operations-Center-SOC> [Accessed 7 December 2021].

Limnell J., Majewski K. and Salminen M. (2014). Kyberturvallisuus. Jyväskylä: Docendo.

Lin, P. (2019). Cyber Security for Normal People. WWW document. Available at: <https://medium.com/@peterlin5301997/cyber-security-for-normal-people-3621caf25444> [Accessed 10 December 2021].

Lynn, R. (2019). Lean Business Development: How 7 Lean Principles Guide Sustainable Growth. WWW document. Available at: <https://www.planview.com/resources/articles/lean-business-development/> [Accessed 9 December 2021].

Madsen, T. (2017). Sun Tzu's "The Art of War" for Cybersecurity. WWW document. Available at: <https://www.infosecurity-magazine.com/opinions/sun-tzus-art-of-war-cybersecurity/> [Accessed 1 December 2021].

Matthews, T. (2019). Creeper: The World's First Computer Virus. WWW document. Available at: <https://www.exabeam.com/information-security/creeper-computer-virus/> [Accessed 29 November 2021].

McLennan, M. SK Group. Zurich Insurance Group. 2021. The Global Risks Report 2021, 16th Edition. PDF document. Available at: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf [Accessed 12 December 2021].

Murphey, D. (2019). *A history of information security*. WWW document. Available at: <https://www.ifsecglobal.com/cyber-security/a-history-of-information-security/> [Accessed 29 November 2021].

Petters J. (2019). What is SIEM? A Complete Beginner's Guide - Varonis. WWW document. Available at: <https://www.varonis.com/blog/what-is-siem/> [Accessed 6 December 2021].

Puro J. (2017). Mikä on tietoturvan ja kyberturvallisuuden ero? WWW document. Available at: <https://www.itewiki.fi/blog/2017/03/mika-on-tietoturvan-ja-kyberturvallisuuden-ero/> [Accessed 5 December 2021].

Rantala O.-P. and Kievari T. (2016). Information Security Strategy for Finland The World's Most Trusted Digital Business Environment. PDF document Available at: <https://julkaisut.valtioneuvosto.fi/handle/10024/75353> [Accessed 5 December 2021].

Rosencrance L. (2020). What is SIEM and Why is it Important? WWW document Available at: <https://www.techtarget.com/searchsecurity/definition/security-information-and-event-management-SIEM>. [Accessed 6 December 2021].

Scartone K. (2015). AlienVault OSSIM: SIEM Product overview. WWW document Available at: <https://www.techtarget.com/searchsecurity/feature/AlienVault-OSSIM-SIEM-Product-overview> [Accessed 8 December 2021].

Securitymagazine. (2021). *How to apply Sun Tzu's "The Art of War" to cybersecurity*. WWW document. Available at: <https://www.securitymagazine.com/articles/96072-how-to-apply-sun-tzus-the-art-of-war-to-cybersecurity> [Accessed 1 December 2021].

SentinelOne. (2019). The history of Cyber Security – Everything You Ever Wanted to Know. WWW document. Available at: <https://www.sentinelone.com/blog/history-of-cyber-security/> [Accessed 29 November 2021].

Statista. (2017). Global cybersecurity market forecast 2017-2023. WWW document. Available at: <https://www.statista.com/statistics/595182/worldwide-security-as-a-service-market-size/> [Accessed 30 November 2021].

Suomen Automaatioseura ry. (2021). Automaatien Tietoturva – Kriittisen tuotannon turvaaminen. Helsinki: Grano.

The People History (n.d.). 1980's Computers from The People History Site. WWW document. Available at: <https://www.thepeoplehistory.com/80scomputers.html> [Accessed 30 November 2021].

Tunggal A. (2021). Why is Cybersecurity Important? WWW document. Available at: <https://www.upguard.com/blog/cybersecurity->

[important#:~:text=Cybersecurity%20is%20important%20because%20it](#)
[Accessed 28 November.2021].

Valtioneuvosto. (2021). National Cyber Security Centre to be designated as Finland's National Coordination Centre for cyber security matters. WWW document. Available at: https://valtioneuvosto.fi/en/-/national-cyber-security-centre-to-be-designated-as-finland-s-national-coordination-centre-for-cyber-security-matters?languageId=fi_FI [Accessed 5 December 2021].

Wikipedia. (2019). AT&T Cybersecurity. WWW document. Available at: https://en.wikipedia.org/wiki/AT%26T_Cybersecurity [Accessed 8 December 2021].

Wikipedia. (2019). Loki (rekisteri). WWW document. Available at: [https://fi.wikipedia.org/wiki/Loki_\(rekisteri\)](https://fi.wikipedia.org/wiki/Loki_(rekisteri)) [Accessed 6 December 2021].

Wikipedia. (2019). Security information and event management. WWW document. Available at: https://en.wikipedia.org/wiki/Security_Information_and_Event_Management [Access 6 December 2021].

Wikipedia. (2020). John McAfee. WWW document. Available at: https://en.wikipedia.org/wiki/John_McAfee [Accessed 30 November 2021].

Wikipedia. (2021). ESET. WWW document. Available at: <https://en.wikipedia.org/wiki/ESET> [Accessed 30 November 2021].

Wikipedia. (2021). MPY Palvelut. WWW document. Available at: https://fi.wikipedia.org/wiki/MPY_Palvelut [Accessed 27 November 2021].

World Economic Forum. (2019). The Cybersecurity Guide for Leaders in Today's Digital World Shaping the Future of Cybersecurity and Digital Trust. PDF

document. Available at:

https://www3.weforum.org/docs/WEF_Cybersecurity_Guide_for_Leaders.pdf

[Accessed 13 December 2021].

World Economic Forum. (2020). Why 2020 is a turning point for cybersecurity.

WWW document Available at: <https://www.weforum.org/agenda/2020/01/what-are-the-cybersecurity-trends-for-2020/> [Accessed 4 December 2021].

Ylätalo A. (2019). Development of process and tools for vulnerability management. WWW document. Available at:

https://www.theseus.fi/bitstream/handle/10024/262440/YI%E4talo_Anssi.pdf?sequence=2 [Accessed 27 November 2021].

Yle. (2017). *Suomi on kyberturvallisuudessa "tarkkailuluokan mallioppilas."* WWW

document Available at: <https://yle.fi/uutiset/3-9440404> [Accessed 5 December 2021].

List of Figures and Tables

Figure 1 - Printing message "I'M CREEPER CATCH ME IF YOU CAN" (SentinelOne, 2019)	8
Figure 2 – Global Risks Horizon Report 2021 (McLennan, 2021)	13
Figure 3 - Global Risks Horizon Report 2021 (McLennan, 2021)	14
Table 1 - Thematic Scope of National Security Strategy (Antczak, 2018, 10)	15
Figure 4 – SIEM process, made by Varonis (Petters, 2019).....	20
Figure 5 - Applies to OSSIM (AT&T Cybersecurity, n.d)	23
Figure 6 - Email from AlienVault.....	24
Figure 7 - USM Architecture (AT&T Cybersecurity, n.d).....	24
Figure 8 - High level view of events (AT&T Cybersecurity, n.d)	25
Figure 9 - First step (AT&T Cybersecurity, n.d)	26
Figure 10 - Second step (AT&T Cybersecurity, n.d).....	26
Figure 11 - Third step (AT&T Cybersecurity, n.d).....	27
Figure 12 - Fourth step (AT&T Cybersecurity, n.d).....	27
Figure 13 - Fifth step (AT&T Cybersecurity, n.d)	28
Figure 14 - WEB UI access	29
Figure 15 - AlienVault Console.....	30
Figure 16 - Setup menu.....	30
Figure 17 - Sensor.....	31
Figure 18 - Existing plugins	32
Figure 19 - AlienVault Center	32
Figure 20 - Enable a Plugin from the Sensor Configuration	33
Figure 21 - Configure Data Source Plugins.....	33
Figure 22 - Select a Plugin	34
Figure 23 - Example General OSSIM Application Dashboard (Garth, 2018).....	35