



Information Services

# Intelligent automation

Cyber security and response management/automation internship  
Fontys Hogeschool ICT – Eindhoven / Information Services – Bulgaria, Sofia

Ivan Dimitrov Arbaliev  
20.11.2022 г.

Data student:	
Family name, initials:	Ivan Arbaliev - IA
Student number:	3883876
Assignment period: (from- till)	01.09.2022 – 01.03.2023
Data company:	
Name Company/ institution:	Information Services JSC
Department:	Security Operaiton Center
Address:	ul. "Lachezar Stanchev" 11, 1797 g.k. Iztok, Sofia
Company tutor:	
Family name, initials:	Simeon Kartselyanski
Position:	Manager Security Operation Center (SOC)
University tutor:	
Family name, initials:	Marc van Grootel
Final report:	
Title:	Intelligent automation
Date:	20.11.2022

Approved and signed by company tutor: Simeon Kartselyanski

Date: 05.01.2023

Signature:

 Възстановим подпис

X Simeon Kartselyanski

Подписано от: Simeon Pepov Kartselyanski

## Acknowledgment

I received a fantastic learning and professional development opportunity with the internship in Information Services. Therefore, I think of myself as a fortunate person because I was given the chance to participate. I appreciate the opportunity to interact with excellent people and experts who guided me through this internship term. Having first-hand experience in a governmental cybersecurity institution is a huge head start for my future career in that field. This section intends to express appreciation and gratitude to everyone who has implicitly contributed to the project's success.

I want to thank Marc Grootel for his insightful advice, insightful suggestions, constant encouragement, and timely support in getting the job done.

For my internship, Mr. Simeon Kartselyanski, a licensed cybersecurity expert and mentor, deserves my gratitude. Throughout the process, he has been a continual source of encouragement and support for me, and he has given me the self-confidence I needed to complete the project.

## Table of contents

Summary .....	4
Glossary .....	5
Chapter 1: Introduction .....	6
Chapter 2: About “Information Services” .....	7
Chapter 3: Assignment Overview .....	9
Chapter 4: Process .....	13
4.1: Research .....	13
4.1.1 Understanding the OSI model .....	13
4.1.2 Creating a virtual network .....	15
4.1.3 Network fragmentation and segmentation .....	18
4.2 Research questions .....	20
4.2.1 What is a SOC-Literature Study .....	20
4.2.2 What is the SOC operation and management process – literature and field study .....	21
4.2.3 What is a SIEM – Literature and A/B testing .....	23
4.2.4 What is a SOAR – Literature (design pattern) and Unique selling points .....	24
4.2.5 What is AV/EDR -Literature study .....	25
4.2.6 What is email security – literature study and risk analysis .....	26
4.2.7 What are the main attack vectors – Design pattern search .....	28
4.2.8 What are the incident response procedures- Best, good & bad practices .....	29
4.2.9 What is automation with Ansible .....	30
4.3 Working with QRADAR – investigating cases .....	31
4.4 Working with IBM Resilient .....	34
Chapter 5: Conclusion .....	39

## Summary

The internship I followed at the security operation center in Information services was beneficial for my personal and professional development. IS had a problem with late solving cyber security cases due to too analysis processes requiring too much human inputs. My assignment was to provide an automated solution to solve cases for them. I started by acquiring knowledge in cyber security (threat intelligence coordination, vulnerability management, Threat hunting, Incident response). After I received a company laptop and credentials I investigated cases in IBM QRADAR SIEM to determine best practices and most common time-wasting phases of the analysis process. After enough information was gathered I worked on the SOAR itself. I developed playbooks that solve cyber offences automatically as well as workflows for new employees to follow. The tool I worked on provided the SOC team with automation capabilities as well to teach someone with no experience in threat analysis (new employee) with a guide(workflow) that shows the steps he should take to come up with a verdict and close a case.

# Glossary

SOC – Security operation center

NOC – Network operation center

SOAR - Security orchestration, automation, and response

SIEM - Security information and event management

EDR - The Endpoint Detection and Response Solutions

AV – Antivirus

IOC - Indicators of compromise

SPF - Sender Policy Framework

## Chapter 1: Introduction

Cybercrime is a global problem that has been dominating the internet in the past few years. It poses a threat to individuals and an even bigger threat to big companies, governments, hospitals, and banks. Cyber attacks are past the time when lone hackers take down companies singlehandedly, nowadays large, organized rings employ highly educated developers who are constantly innovating online attacks. Enterprises use cyber security to protect against unauthorized access to crucial data and other systems. When talking about cyber security we are trying to protect ourselves from unauthorized access, deletion, and modification of data important to an individual or a company.

“Information services” is a state cyber security company that ensures the systems of strategic Bulgarian infrastructures remain operational and safe from online attacks. Some of the infrastructures that “Information services” protects are State Rails, Revenue management systems, the general labor inspectorate, Bulgarian posts, The secret service, the Central election commission, and others. They use various “tools” to provide information about everything happening on the strategic networks. The current way of examining cyber attacks involves too much human input and is usually taking days or sometimes up to several weeks for an online incident to be analyzed, documented, and closed. The tool we refer to as the “mother of tools” is IBM QRADAR SIEM (security information and event management). It collects data from other security equipment, sorts it according to the severity of each incident, and provides information to security analysts. My job as an intern in “Information services” is to find an automated solution to some parts of the typical security analyzing process. It will speed up the rate at which cases get closed and it will provide the company with a better workflow.

Chapter 2 provides more information about “Information services”, Chapter 3 gives all the details about the assignment, and Chapter 4 sheds light on the process and progress.

## Chapter 2: About “Information Services”

“Information services” was established in 1970 as a private company. In 1986 the Economic unit “Information services” was formed. In the years to come, the company was first transformed into a state-owned company, then into a single-member joint-stock company (EAD) with public participation, and in 1997 the organization became the “Information services” we know today. The company has a team of over 580 highly qualified developers, system administrators, security, and communication specialists. The company has a branch structure covering 26 regional centers in Bulgaria. It has been a key partner of the state institutions in the implementation of ICT projects with The National Revenue Agency, the Ministry of Finance, The ministry of regional development and public works, The Secret Service, etc. The company provides its employees with high- a tech work environment, different certification training, and practical professional development.

IS has 3 main operation centers – The network operation center (NOC), The security operation center (SOC), and a development team. The NOC is responsible for keeping the networks connected and operational as well as keeping the servers in good working condition. The dev team develops and implements websites and apps targeted at making the life of Bulgarian people easier. Some of their more notable projects are renewing the website of the Bulgarian Post Office, the Bulgarian Rail ticketing system, Revenue management for NRA, and Machine voting systems.





I am an intern at the SOC. The SOC team is made of 20 security specialists, working in day and night shift cycles. Our job is to catch, intercept and investigate cyber attacks aimed at our networks and the companies partnering with IS. This includes running scans on the networks and endpoints, analyzing potential threat requests to our servers, reverse engineering viruses found in a sandbox environment, and documenting my findings. We use IBM QRADAR SIEM as our main source of information as well as different tools reporting to the SIEM, (e.g., EDR, Malware detection tools, Web/email solutions, crisis communications, threat intelligence, vulnerability management, and ticketing alerts). Currently, every step throughout the investigation and response process requires human input. Usually, such a process can take days or up to several weeks depending on the severity and complexity. With the company's expansion, more and more cyber alerts are coming into the SOC each day and the security specialists can be overwhelmed by the amount of information they have to go through. My assignment as an intern is to find a solution to automate the analysis of the threats to speed up the conclusion for each alert.

## Chapter 3: Assignment Overview

The security operation center at IS services many companies of various scales and sizes. We receive cyber alerts daily. The current process of investigating each alert is mainly manual. The security analyst takes a case from IBM QRADAR and determines whether the alert is a false positive or a real cyber-attack. There are several ways he can do this. The easiest way to determine whether a sender's IP has malicious intents is to check its history in the Abuse DB database. It is a free website designed to make the security analyst's life easier by giving all IPs a trust score. If an IP is detected making illegal requests or launching scans it will be recorded in the database for future analysts to see.


This is an example of a clean IP according to Abuse DB

Check an IP Address, Domain Name, or Subnet  
e.g. 46.10.120.237, microsoft.com, or 5.188.10.0/24

46.10.120.237

CHECK

**46.10.120.237** was not found in our database

ISP	Vivacom Bulgaria Ead
Usage Type	Unknown
Hostname(s)	46-10-120-237.ip.btc-net.bg
Domain Name	vivacom.bg
Country	 Bulgaria
City	Sofia, Sofia (stolitsa)

IP info including ISP, Usage Type, and Location provided by IP2Location.  
Updated monthly.

REPORT 46.10.120.237

WHOIS 46.10.120.237

AbuseIPDB can use a lot of resources - our servers support millions of IP reports, checks, and whois lookups every week. See the [statistics](#). We use revenue from the advert being blocked here to pay our server bills. If AbuseIPDB is valuable to you, consider [chipping in!](#)

IP Abuse Reports for **46.10.120.237**:

*This IP address has not been reported. [File Report](#)*

This is an example of an IP that has been detected using brute force for cracking passwords.

Check an IP Address, Domain Name, or Subnet  
e.g. 46.10.120.237, microsoft.com, or 5.188.10.0/24

46.10.120.237

CHECK

**79.188.52.121 was found in our database!**

This IP was reported **4,268** times. Confidence of Abuse is **100%**: ?

100%

ISP

Orange Polska Spolka Akcyjna

Usage Type

Unknown


Hostname(s)

hma121.internetdsl.tpnet.pl

Domain Name

orange.pl

Country

 Poland

City

Legionowo, Mazowieckie

IP info including ISP, Usage Type, and Location provided by [IP2Location](#).  
Updated monthly.


REPORT 79.188.52.121



WHOIS 79.188.52.121

AbuseIPDB can use a lot of resources - our servers support millions of IP reports, checks, and whois lookups every week. See the [statistics](#). We use revenue from the advert being blocked here to pay our server bills. If AbuseIPDB is valuable to you, consider [chipping in!](#)

IP Abuse Reports for **79.188.52.121**:

This IP address has been reported a total of **4,268** times from 655 distinct sources. 79.188.52.121 was first reported on June 10th 2022, and the most recent report was **6 minutes ago**.

 **Recent Reports:** We have received reports of abusive activity from this IP address within the last week. It is potentially still actively engaged in abusive activities.

Reporter	Date	Comment	Categories
✓ Anonymous	6 minutes ago	Failed password for root from 79.188.52.121 port 42234 ssh2 Failed password for root from 79.1 ... <a href="#">show more</a>	<div>Brute-Force</div> <div>SSH</div>
✓  <a href="#">mahdielector</a>	7 minutes ago	Dec 4 18:16:11 Digitallogic sshd[34060]: Disconnected from authenticating user root 79.188.52.121 po ... <a href="#">show more</a>	<div>Brute-Force</div> <div>SSH</div>
✓ Anonymous	52 minutes ago	Unauthorized connection attempt detected, SSH Brute-Force	<div>Brute-Force</div> <div>SSH</div>
✓  <a href="#">Max la Menace</a>	6 hours ago	ssh brute force (P)	<div>Brute-Force</div> <div>SSH</div>

Another way of finding the sender's intentions is to check the country he is located. In IS we get activity from all over the globe, and we do not block users simply because of their geo-location, except for one country- North Korea. As you may know, people in North Korea do not have access to the internet, and every

communication coming from that geolocation is launched by the government. They tend to use whole subnets as attackers which might do different things, like scanning, web scraping, brute force, and attempting to launch man-in-the-middle attacks.

AbuseIPDB can use a lot of resources - our servers support millions of IP reports, checks, and whois lookups every week. See the <a href="#">statistics</a> . We use revenue from the advert being blocked here to pay our server bills. If AbuseIPDB is valuable to you, consider <a href="#">chipping in!</a>		
<b>IP Abuse Reports for 175.45.176.0/24:</b>		
<b>8 reported IPs</b> from this subnet for a total of <b>30 reports</b> . The most recently reported IP was <b>175.45.176.81 1 month ago</b> .		
175.45.176.0/24 is of the subnet 175.45.176.0/24. Hosts begin with address 175.45.176.1 and end with address 175.45.176.254, allowing for a space of 254 possible hosts.		
Address	Number of Reports	Time of Most Recent Report
 <a href="#">175.45.176.8</a>	2	2021-01-19 06:43:29
 <a href="#">175.45.176.15</a>	20	2021-04-11 16:36:20
 <a href="#">175.45.176.16</a>	2	2021-03-29 19:52:46
 <a href="#">175.45.176.20</a>	1	2021-10-14 22:21:36
 <a href="#">175.45.176.69</a>	1	2021-08-24 00:01:28
 <a href="#">175.45.176.76</a>	2	2022-01-26 15:55:31
 <a href="#">175.45.176.81</a>	1	2022-10-20 08:25:20
 <a href="#">175.45.176.131</a>	1	2021-04-28 13:16:02

The security analysts then read the log files of the communication between the sender and “Information Services” networks and document the findings in a report. This can take up to several days depending on the number of logs collected. If a malicious attack has been validated the security analyst escalates the case and if a virus/ trojan has been found on an endpoint, reverse engineering is the best practice.

The bottleneck in the analysis process is that our processes are reliant on individual excellence to achieve results. This showed during our national party elections. “Information service” was bombarded with alerts for two weeks. We were receiving up to several thousand daily alerts and could not handle them. The consequence of not being able to process cases fast was that we could miss a valid threat to our networks while investigating a false positive one. I am going to use Ansible in correlation with IBM Resilient SOAR for automating case responding and

creating workflows for new employees to follow. The goal of the project is to reduce the response time and investigation of cyber incidents related to alarms for the company's customers. After integrating the SOAR solution, a 25% drop in redundant investigations and actions by triage specialists is expected.

My job is to create workflows for different incident types and teach the IBM Resilient SOAR how to react to various threats in the form of playbooks. The SOAR tool will significantly enhance operations like threat detection and response by providing machine-powered assistance to analysts. I will use the waterfall methodology for configuring response actions in Resilient. For example, the response against malicious IPs (did the sender manage to get through the firewalls, did he manage to exfiltrate valuable data, was the data encrypted or he managed to get to it before encryption, are there any phishing emails, and who clicked on them)? Different scenarios should be handled according to the attack vectors. I will start with acquiring the necessary skills for working on the project – data transport protocols, networking layers, and working with SIEM. Once I get access to IBM QRADAR, I will start investigating offense cases on my own and think of an implementation to mitigate as many false positive alarms as possible. I will test the result with my internship mentor and change it according to his feedback if necessary.

For Resilient to be considered complete I must fulfill several requirements/constraints:

1. Implementation with SIEM. To visualize existing alarms from all SOC customer SIEMs
2. To process and close alarms centralized by SOAR
3. To integrate with an AV/EDR solution.
4. To integrate with SPFW.
5. To integrate with Email Gateway.

I divided my project into 4 phases.

1. Initial research (answer research questions, data transport protocols, networking layers, working with SIEM).
2. Investigating QRADAR cases to learn security analysts' workflow and best practices. Get to know the repetitive tasks executed in every case because they are most important for automation.
3. Implementation of SOAR and getting feedback from the internship mentor
4. Testing of working product

## Chapter 4: Process

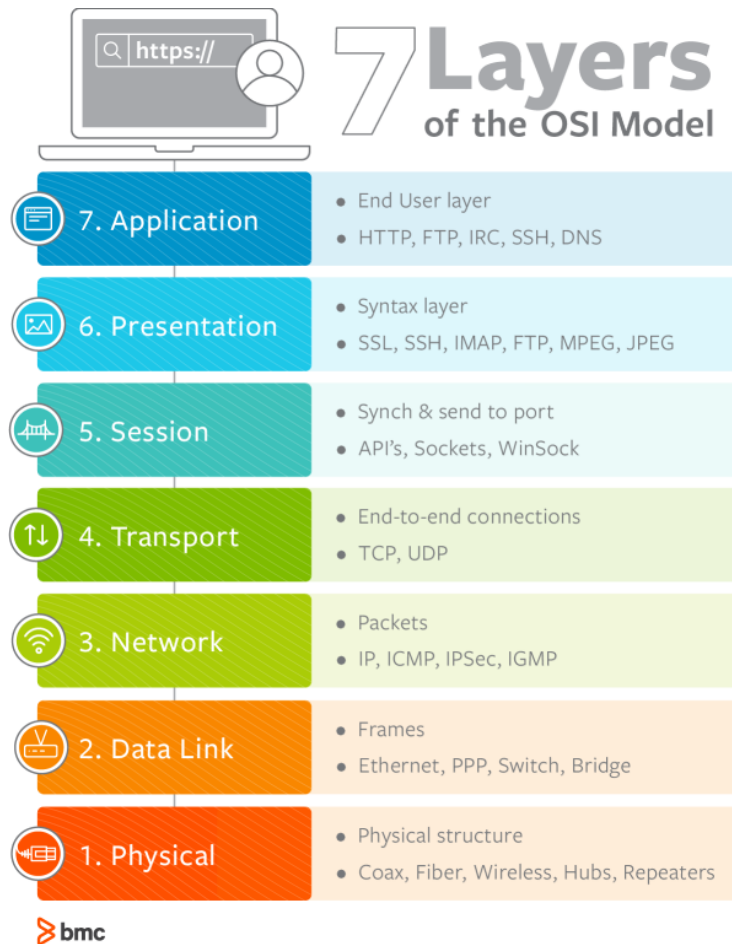
The first month and a half in “Information services” I spent acquiring the necessary skills needed to perform my tasks successfully. My internship mentor provided me with documentation for important topics I had to be familiar with before I started investigating cyber alerts. During that frame of time, I was not allowed to access the networks because I had to go through an extensive background check (providing proof that I haven't been convicted of any crimes and signing multiple non-disclosure agreements) due to the nature of the data I was going to work with. I dedicated that time to learning and conducting my research for the project as well as shoulder-surfing what my colleagues were working on. Thankfully they showed me the ropes and answered my questions if any occurred.

### 4.1: Research

#### 4.1.1 Understanding the OSI model

The open systems interconnection reference model is a way to describe the way that traffic is moving from one part of the network to another. It consists of seven

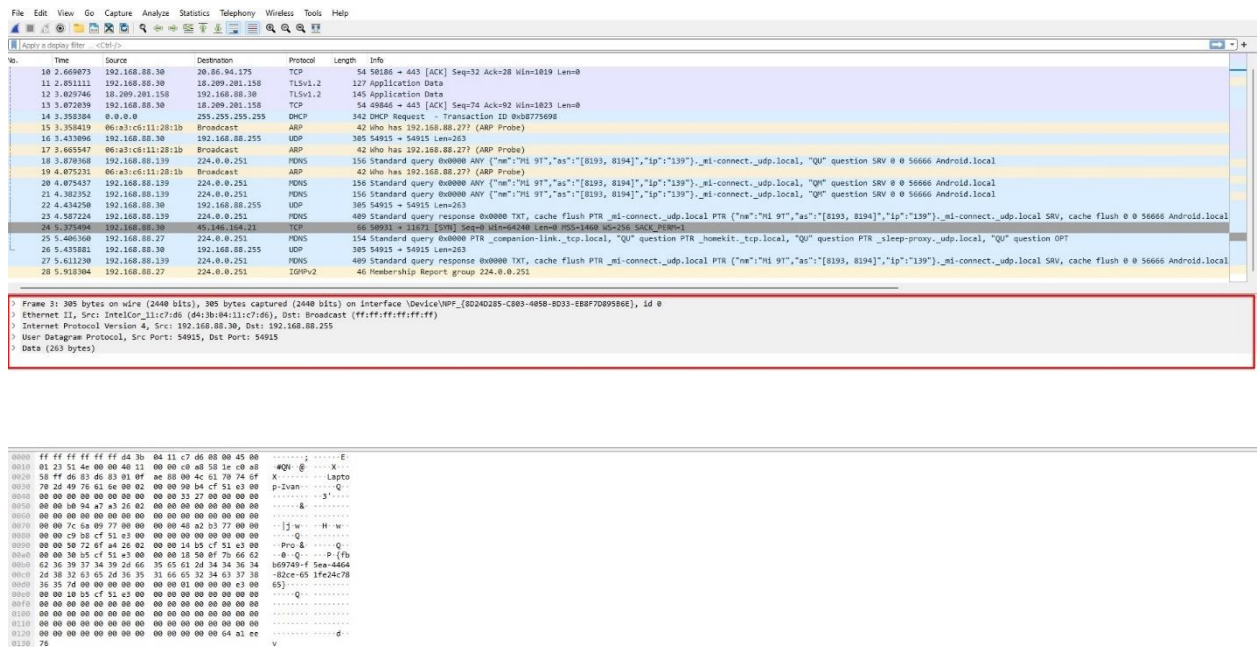
layers and each layer of the model is a set of protocols. Depending on the type of traffic going over the network different protocols are used.



Layer 1 is the physical part of the network. It is all about the signaling that is going over the network. Layer 2 is the foundational layer for the protocols that we stack on top of it. It is referred to as the “data link control” and is used for MAC address identification. Layer 3 is the network layer and is associated with IP addresses. Any device making forwarding decisions based on IP is using this layer. It is also used for data fragmentation if you are moving between different types of networks (Ethernet, WAN). Layer 4 is the transport layer. Its commonly referred to as the TCP/UDP layer. It describes how data is delivered and where it is delivered into a system. It is used when you are accessing a webpage but the webpage itself is so large that you can’t send all the data across the network into one frame. Instead, it is split into several frames that can be transported across the network and put together on the other side. Layer 5 is designed to start and stop communication



between one endpoint and another. Control and tunneling protocols are used to begin the communication of data between two devices. Layer 6 is the presentation layer. Character encoding and encryption occur at this layer. It is often combined with layer 7 because the functionality is so closely associated with our ability to use the applications. Layer 7 is the application layer, and it is what we see when we open a browser. Common protocols associated with that layer are HTTP, FTP, DNS, and SSH. One way of visualizing the OSI model layers is by using Wireshark



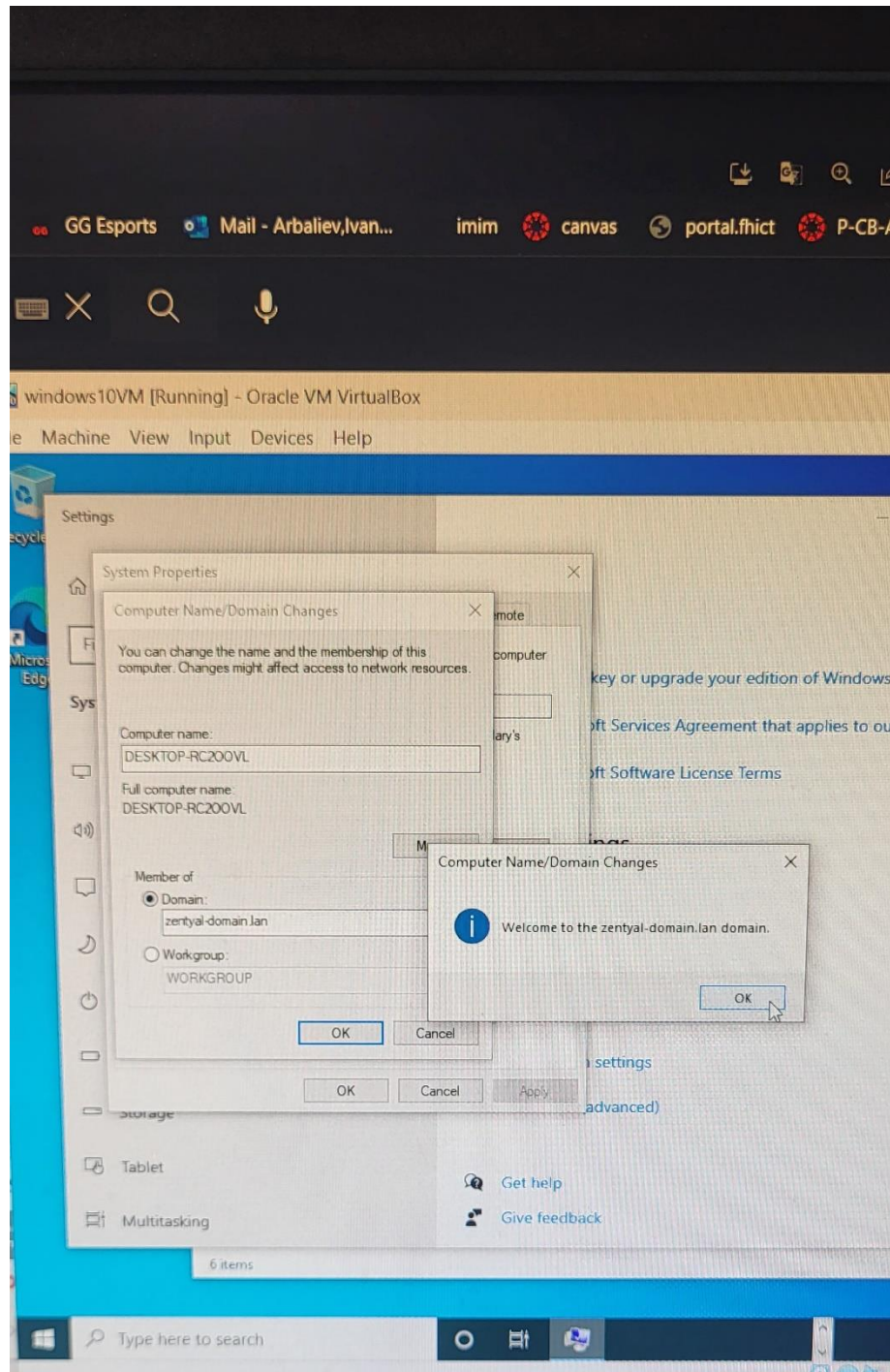
Layer 3,4,5 is most important for my internship because Cyber alerts most commonly occur on them.

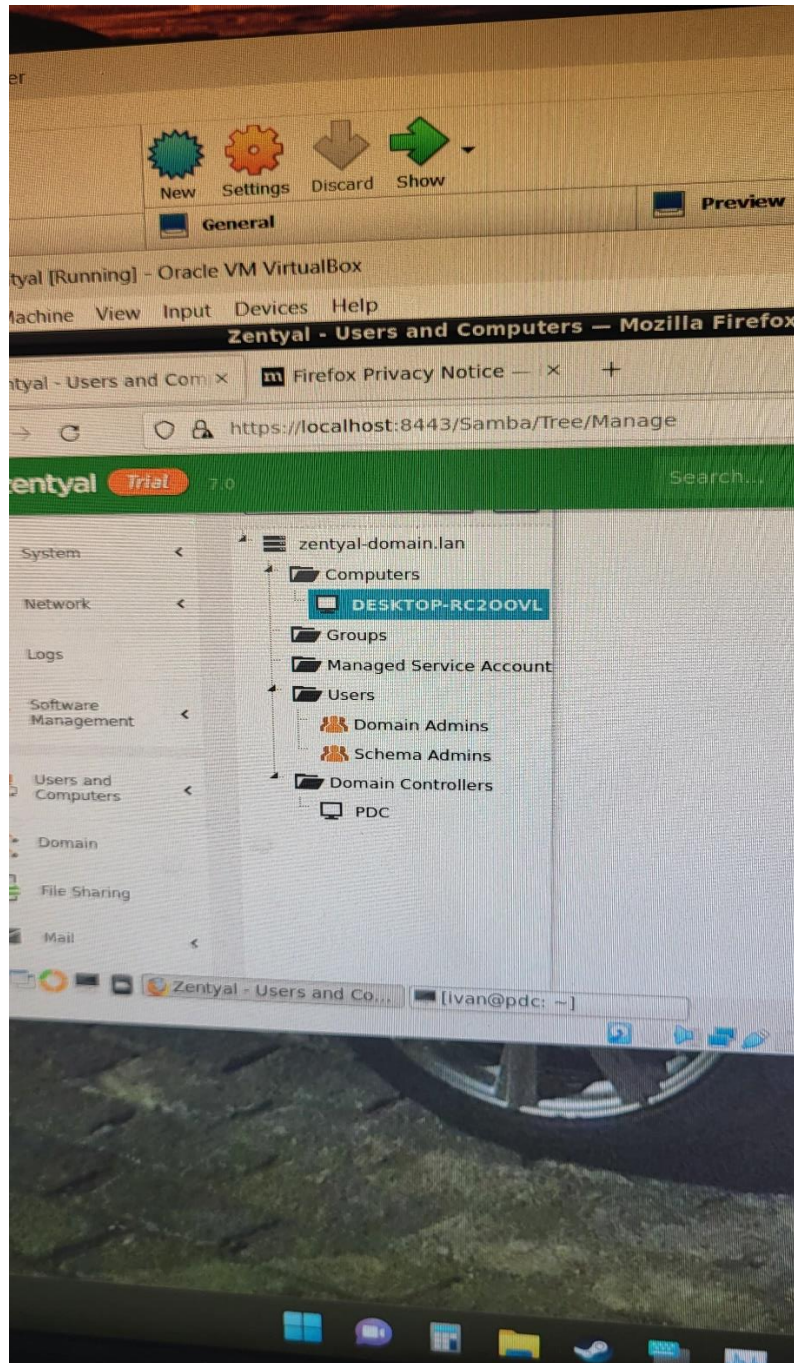
## 4.1.2 Creating a virtual network

One of the first tasks I got from my internship mentor was to create my own virtual environment. I chose VirtualBox as my hypervisor. For my server, I used Zentyal because it is a lightweight Linux distribution server based on Ubuntu. It provides a domain and directory server with native compatibility with Microsoft Active directory which worked well with the two windows 10 endpoints I created. Zentyal



served as my primary domain controller on the network. I set up the server's network card as "host only" and the endpoint as a NAT network. Doing so provided the endpoints with connectivity between each other as well as the server. I gave one of the endpoint administrators privileges.

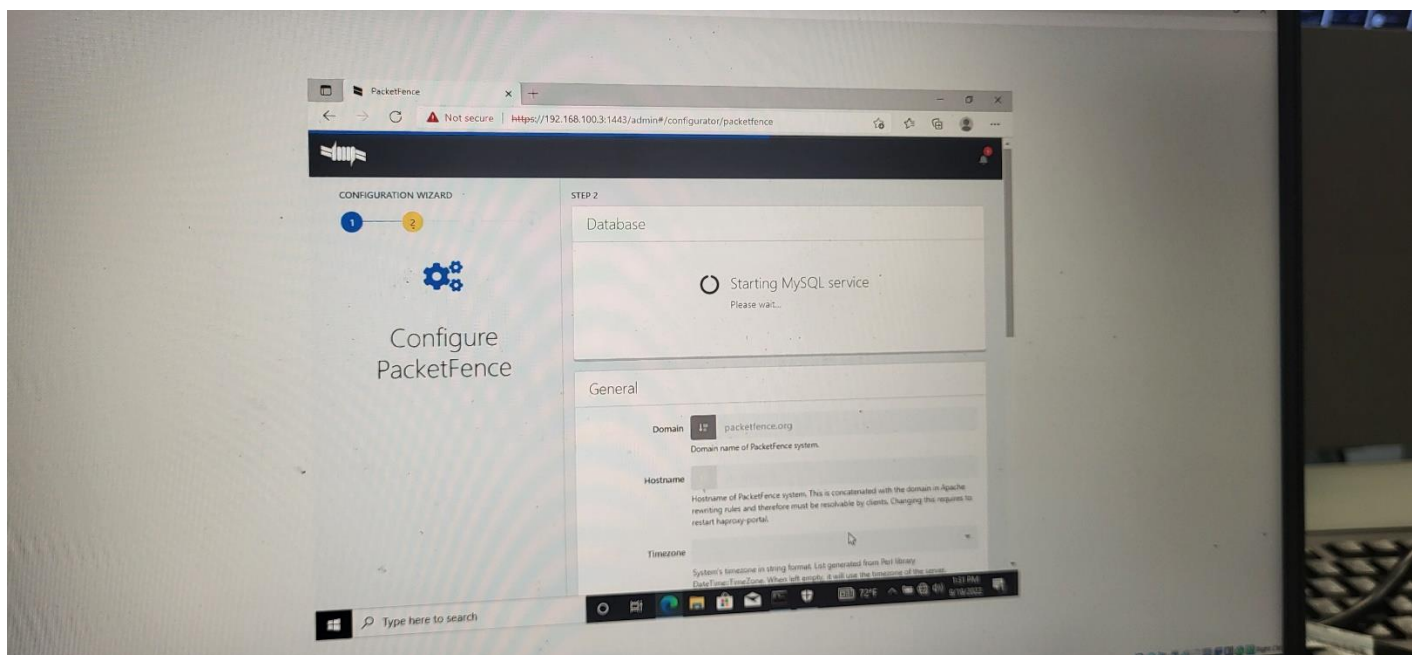




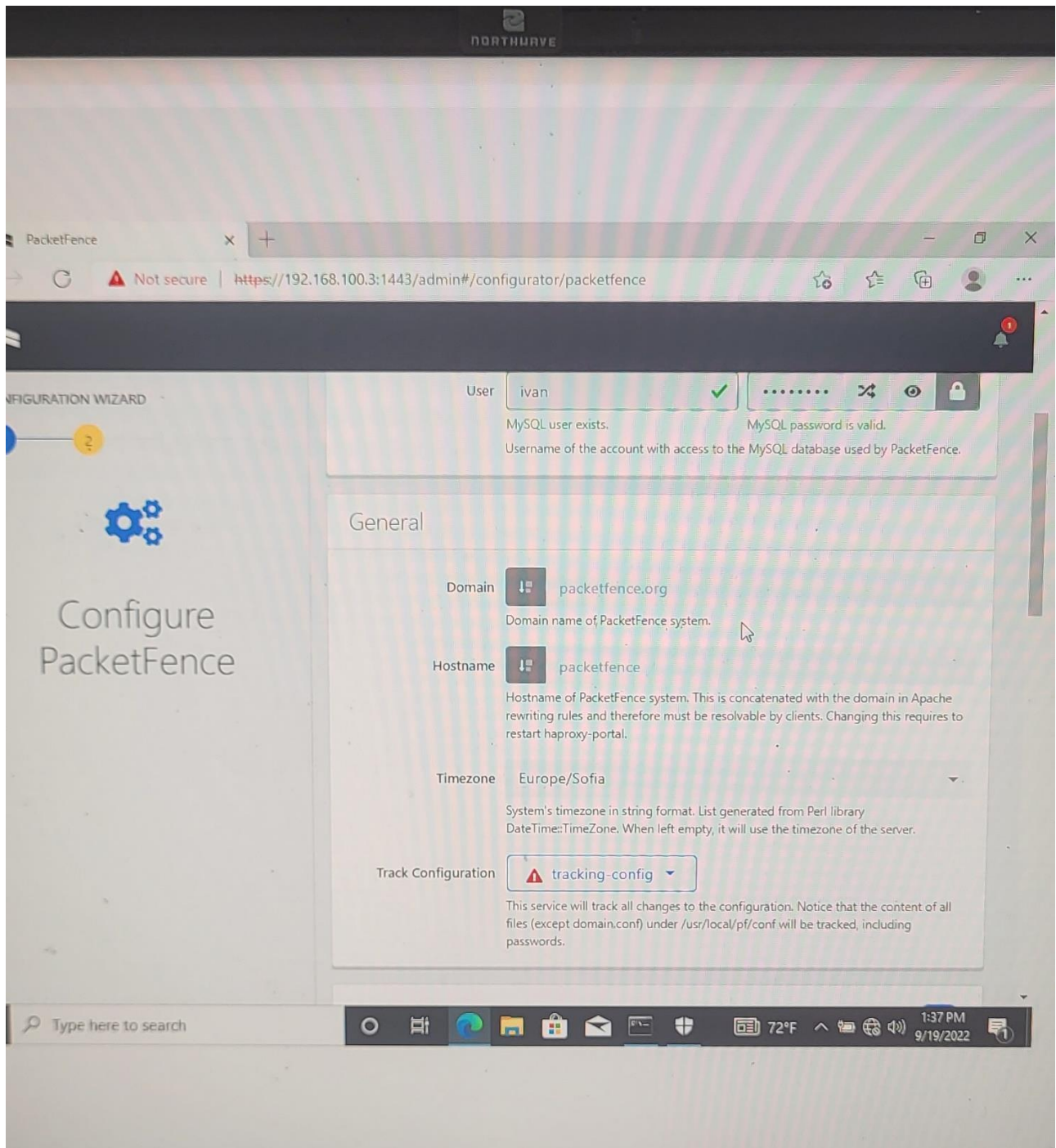
This task gave me knowledge in creating and managing networks and user privileges which is crucial for cyber security on network level.

### 4.1.3 Network fragmentation and segmentation

My next task was to learn network fragmentation and segmentation. The tool I used for is called Packet Fence. It is an open-source network access control tool. It is mainly used in university campuses as well as business buildings for providing network users with the detection of abnormal network activities, isolation of problematic devices, and a captive web portal. It works very well for detecting abnormal activity on the network and isolating the problematic device in a subnet of its own which ensures the stability and security of the main network. This feature makes it very useful for my virtual environment for testing viruses and other malicious software without putting the entire network at risk. It took me about two weeks to set it up but in the end, I got my network protected and ready for testing.







The reason my first screenshots are taken from a phone is that in the first three months of my internship I was not allowed to take screenshots. I was working on a stationary PC in the office and whenever I took a screenshot I triggered an offense

in QRADAR. When I got my work laptop, Its IP has been whitelisted so I could take screenshots without sending the entire team into panic mode.

## 4.2 Research questions

### 4.2.1 How does a SOC work? -Literature Study

The security operation center's function is to detect, analyze and respond to cybersecurity incidents. It acts like a central command post taking information from its infrastructures like devices, networks, and application tools. The SOC members decide how to handle, analyze, and report cyber security threats. The SOC's soul function is to improve the company's security posture. It can be in a company or outsourced to a separate building depending on the financial capabilities of the company. My internship company "Information services" serves as outsourced SOC for governmental companies. If a company does not have the financial capabilities to create a SOC on its own, its next best option is to outsource that function to a company that provides those services.

#### Basic team hierarchy

SOC teams tend to be separated into levels. Level 1, 2, 3, team leader and SOC manager. They have different permission rules and do different tasks. Level 1 security analysts investigate alerts coming in the SIEM and determine whether it is a false positive or a legitimate threat. If a case comes out as positive, he documents their findings and passes it to level 2. Level 2 security specialists make a verdict depending on the documentation coming from level 1 and investigate more if needed. If he cannot make a verdict the case is passed to level 3. Level one analysts have basic knowledge of how to work with the tools provided while level 3 know how the tools are working from in and out and have extensive knowledge in reverse engineering and programming. They can develop tools of their own to help them solve cases. Every action in the SOC is orchestrated by the team leader, including

scheduling meetings, organizing extra training courses, and managing the general health of the team. The picture below is showing a diagram of the team hierarchy.

---

# Basic Team Hierarchy



## 4.2.2 What is the SOC operation and management process – literature and field study

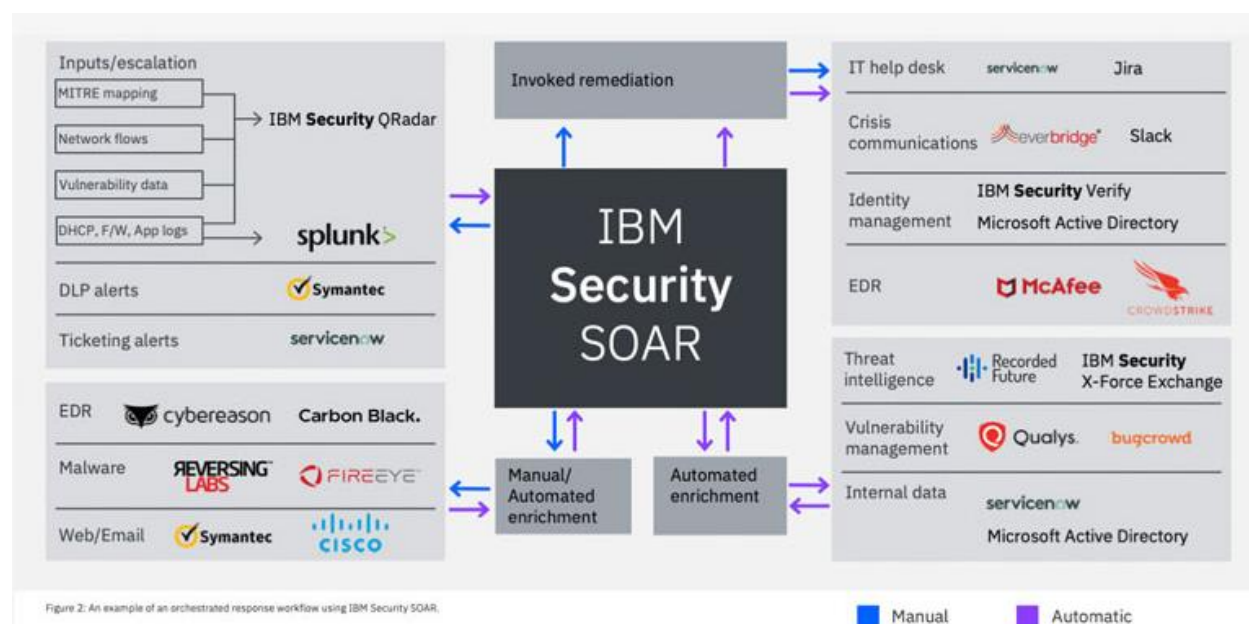
**Monitoring** – The security operation center monitors the networks, server activity, and endpoints nonstop. The core tool they use is called a SIEM (Security information and event management tool). The SIEM monitors alerts and telemetry on the network in real-time and flags potential threats. The SIEM that “Information services” use is provided by IBM, and it’s called QRADAR.

Log management – The collection and management of log files are very important when monitoring a network because they provide full insight into what action a given system has taken and whether it is acting abnormally. A good way to manage logs is a must because the telemetry information can become very extensive in just a couple of days. Many hackers count on the targeted company not analyzing their log data correctly which allows them to stay undetected for longer periods of time. Modern SIEMs have log collection and analysis solutions built in and strongly rely on artificial intelligence to filter out false positives.

Incident response – This is the steps SOC members take to limit the damage to their system which include:

- Shutting down compromised systems
- Isolating endpoints into sandbox networks where they can observe their actions
- Running antimalware software
- Finding and deleting malware
- Resetting compromised employee accounts

Lately, it has become the norm to automate those actions with XDR and SOAR solutions. In the picture below I have provided a diagram showing how IS's network is structured.



### 4.2.3 What is the functionality of a SIEM – Literature and A/B testing

SIEM stands for security information and event management. It centralizes all the security notifications from various security technologies like firewalls, intrusion detection systems, active directory servers, wireless access points. A full SIEM solution blends in threat feeds, blacklists, and geolocation data to further increase the accuracy and reduce false positives. Some people might say IDS/IPS solutions provide the same functionality as SIEM but that is not the case. IDS/IPS are littered with false positives, and they might work for a household or a very small company but in a big corporation with millions of critical alerts per day that can be challenging or straight impossible. SIEMS functions include:

- Data collection
- Aggregation
- Parsing
- Normalization
- Categorization
- Enrichment
- Indexing
- Storage

Collection happens in two different ways: agent-based or agentless. QRADAR is an agent-based SIEM which means that each system has a piece of software that reads the logs written and parses them to the next component. Agent-less SIEMs work well for smaller companies but on larger scales problems like buffer overflows can occur which can lead to log files getting corrupted irretrievably.

The process of collecting logs and presenting them as structured data is called aggregation. There are two methods for this: the PUSH and PULL methods. With the PUSH method, logs are pushed from the source to the server while with the PULL method logs are pulled from the server by the source.



Log files vary from system to system. Different operating systems (Linux, and Windows) have varying ways to display log data. Parsing is the function that brings the aggregated data into a structured form. Parsers are defined for systems.

Normalization merges events containing data into a reduced format that contains common even attributes.

Categorization adds meaning to events. This might be authentication, local/remote operations, identifying log data related to system events, etc.

Indexing is the function that provides security engineers with the ability to search and explore log data. Data query searches tend to be faster compared to a full scan of all the data.

#### 4.2.4 What is a SOAR – Literature (design pattern) and Unique selling points

SOAR stands for security orchestration and response. It is software that allows an organization to collect data about security incidents from multiple sources and respond to them without human assistance. SOAR technologies provide formalized workflows, reporting, and collaboration capabilities. They support the automation of processes, policy execution, and reporting. They can do this by integrating other security solutions/systems that allow them to pull data and push proactive actions. SOARs have a generic interface, allowing analysts to define actions on security tools and IT systems without being experts in their APIs.

An example of that is processing a suspicious email. The SOAR automatically checks the sender and compares its history to verify its legitimacy. Checks URLs by opening them in a sandbox environment determining their validation. Collects data on which company employee has clicked on the phishing link if any and takes actions like resetting their password to ensure no data leaks and breaches.

An example of orchestration can be the execution of a malware playbook. The malware file is scanned and opened in a sandbox environment. The recorded

actions are compared using external services like virus scanners. A security engineer is informed about the actions taken and malware remediation actions are performed.

I performed a benchmark creation on several SOAR looking for the best option for “Information services” including “Splunk phantom”, “IBM resilient”, “RespondX” and “ServiceNow”. They provided similar-looking UIs and functions differentiating slightly in the workflow and playbook creation. The key factor I considered was the price and compatibility. All the tools listed above are enterprise-level SOAR which means they cost upwards of a hundred thousand euros for a subscription. Information services are currently using the IBM QRADAR SIEM solution which includes IBM Resilient as an extension to its services. Since native support for Resilient is included in QRADAR that was the best option. It would save the team a lot of work by just enabling the extension and preventing headaches because of the native parsing of data between the tools. The only thing left for me to do was create custom workflows and playbooks.

#### 4.2.5 What is AV/EDR -Literature study

An AV or antivirus is software that scans and deletes viruses from a computer or a network. They use a dataset of known malware that is continuously updated. There are different techniques antiviruses use to detect malicious activity:

- Specific detection
- Generic detection
- Heuristic detection

Specific detection looks for known malware with a very specific set of characteristics. Patterns/ hashes are compared in a database and if a known threat has been found the virus is quarantined.

Heuristic detection looks for suspicious behavior that is coming out of a file.

EDR stores endpoint system-level behavior provides contextual information, blocks malicious activity, and provides remediation to restore the infected system to working conditions.

#### 4.2.6 Can emails be completely secure for cyber-attacks— literature study and risk analysis

Email gateway is sometimes called email security. It monitors and scans incoming and outgoing traffic. Email traffic uses the SMTP protocol using port 25. One of the big advantages of email gateways is spam filtering. About 80 % of internet traffic is spam. Spam detection work with proprietary algorithms where each email is rated with a spam score (between 1 and 10). Emails with higher spam scores are sent directly to the spam folder.

Anti-spoofing - Email gateways protect from email header forgery where the header of the email is spoofed to look like it came from sources other than the original.

Email gateways are also equipped with anti-spoofing features based on windows threat intelligence and machine learning algorithms. Another level of security provided by them is file filtering based on the extension of attachments, file names, and file size.

Email gateways are not totally secure. For example, our managers in IS send fake phishing emails from their computers to their employees to provide social engineering security against real threats. Later they check the SIEM to see which employee clicked on the phishing URL. Social engineering remains the biggest attack vector when it comes to email cyber-attacks In the picture below I show my inbox containing a phishing email sent from our manager.

**Favorites**

- Inbox 1
- Sent Items
- Deleted Items

---

**i.arbaliev@is-bg.net** 1

- Inbox
- Drafts
- Sent Items
- Deleted Items
- Archive
- Conversation History
- Junk Email
- Outbox
- RSS Feeds
- Search Folders

**> Groups**

Focused Other
 By Date ▾ ↑

**Today**

Вътрешна Комуникация  
Анкета в помощ на джуджет...  
Здравейте, колеги,

16:49

**Last Week**

Симеон Кърцелянски

Декларация  
По пълния е моля те да я

четв 10.11

Вътрешна Комуникация  
Профилактика климатици  
<https://intranet.is-bg.net/>

четв 10.11

IBM SOAR Incident

четв 10.11

Димитър Едрев

Qradar  
<https://qsaas.is-bg.net/console/>

четв 10.11

BK

To

Вътрешна Комуникация  
Служители в София

Translated from: Bulgarian

Show Original

Turn on automatic translation

← ↶ → ⋮

12:23

Hello, colleagues,

We would like to offer you to join a charity quiz and the funds raised to be donated to support The [Cedar Foundation](#).

You can read more about the activities of the charity below. \*

The minimum number of participants for such an event is **35**, as:

✓

The distribution is in teams between 4 and 6 people;

✓

the amount for participation / ticket / is **80 BGN** per person;

✓

the location may be on site in the office or in a restaurant with the possibility of food consumption;

✓

The winning team receives a prize in the amount of a voucher worth BGN 300. for experience/activity;

In this regard, we send a [short](#) survey about your desire to participate. Please note that those who have marked "Yes" in the survey confirm the purchase of a ticket, and the event will be held on a weekday, outside working hours.

The survey will be active until **Friday /18.11.2022/, 12:00** and we will contact the colleagues who have applied for participation.

#### 4.2.7 What are the main attack vectors – Design pattern search

A method used by an attacker to gain access or infect a target is called attack vector. Physical access to systems is significant attack vector. If an attacker has access to a system nothing stops him from sticking a malicious USB drive full of malware into it. That is the reason data centers are locked up and under constant surveillance with limited access. Old operating systems, lack of updates and old encryption technologies are the most common vulnerabilities hackers are looking for. Keeping systems up to date diminishes the possibility of attacks to a minimum. The most difficult attack vector to secure properly is social engineering.

Most companies consider attack vectors and do a good job of securing their systems against Bot attacks, malware, brute-forcing, and man-in-the-middle by installing It equipment to prevent them. Technology nowadays is smart, providing fewer vulnerabilities for hackers to enter, and thus hacking nowadays has shifted from trying to trick the system to trying to trick the user. A company that has secured its systems against a certain type of attack vector (e.g., DDOS) should focus on investigating cyber alerts triggered by other attack vectors. SIEMs help a lot with defining which attack vectors a company is prone to being attacked by simply filtering the cyber offenses by category.

#### 4.2.8 What are the incident response procedures- Best, good & bad practices

Cybersecurity is a cooperative work field. Cyber offenses and equivalent response procedures get posted on the internet to help combat cybercrime across the globe. Incident response can be broken into six main phases.

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons learned

Making sure you have well trained incident response team is a big factor for preparation. The identification phase includes investigation of the depth of compromise, its source, and its success/failure. It is typically done by reviewing log files. Evidence of the incident should not be damaged or erased and analysts should not miss any clear signs of misuse. Containment happens right after the identification phase and includes quarantining infected systems, and freezing compromised accounts, making sure there are no data leaks persisting in the company. Eradication includes removing malware from infected systems and restoring systems from backups. Recovery includes putting the now clean systems back into production, restoring user accounts, and resuming normal operations in the company. Many organizations tend to skip “lessons learned” but it is probably the most important phase to prevent future incidents of that sort. Security engineers should not rush to put the systems back into production without learning why they got attacked, patching the vulnerabilities, and documenting their findings for future awareness.

## 4.2.9 How useful is automation with Ansible

Ansible is an open-source tool that provides the ability to control multiple IT systems from one location. For example, if a company is working with a lot of Virtual machines and an outdated app is running on all of them, the security engineer must execute a single Ansible playbook to update it. Automation of processes saves a staggering number of working hours for both the company and the employees. Ansible is simpler to use than its counterparts because it is not agent-based and runs its communications with systems via SSH.

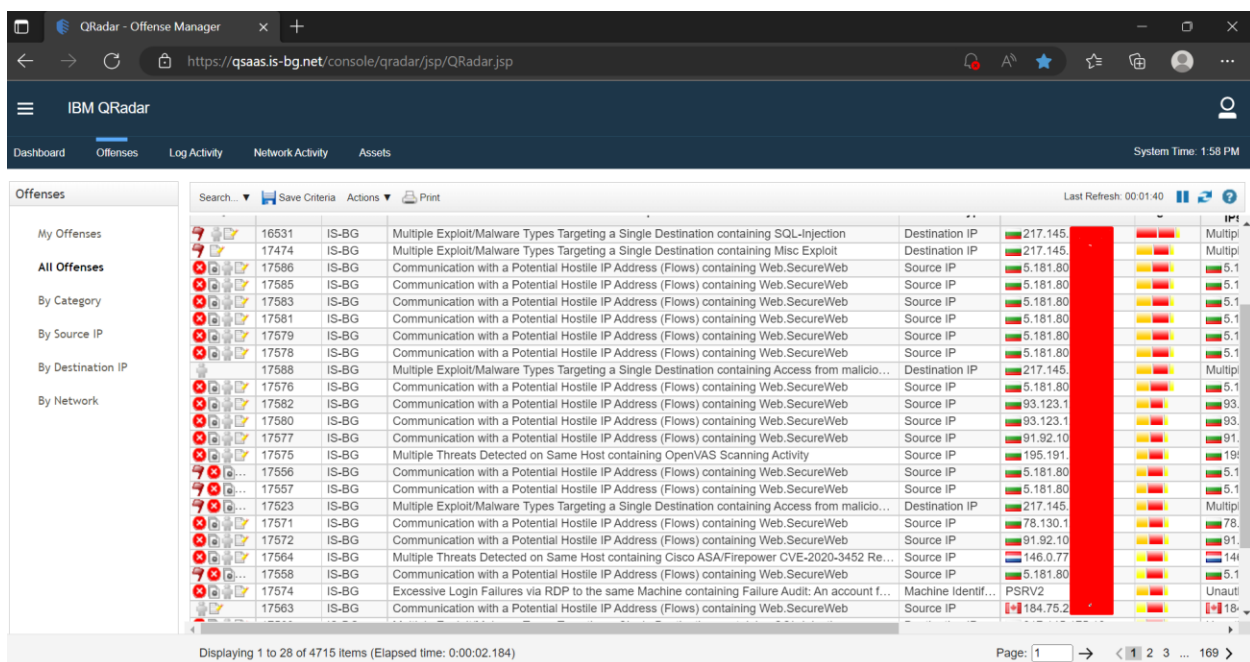
Ansible playbooks are the instructions that are passed to the nodes to execute. They are written in a language called YAML. It is a simply structured language used to describe data and tasks. In the picture below I have provided an example of blacklisting an IP with ansible looks.

```
1  ---
2  - hosts: Qradar
3    gather_facts: no
4    connection: network_cli
5    vars:
6      acl_name:
7  tasks:
8    - asa_acl:
9      lines:
10       - access-list ACL-ANSIBLE extended
11       deny ip host {{ 1.2.3.4 }} any log
12       match: strict
13       replace: block
```

Ansible works great for orchestrating large IT environments, but I did not use it extensively since I was not allowed permission to modify the network components. I focused mainly on investigating cases with QRADAR and creating playbooks/workflows in IBM Resilient UI. I will show you more about that in the next chapters.

## 4.3 Working with QRADAR – investigating cases

I investigated cyber offences in QRADAR to get an insight into which processes are most important for automation. The QRADAR console helps monitoring the entire activity on the network (top alarm signatures, attacked systems, most severe offences, most recent offences etc.). In the screenshot below I am showing the QRADAR offences dashboard. I have masked the sensitive information due to non-disclosure agreement.

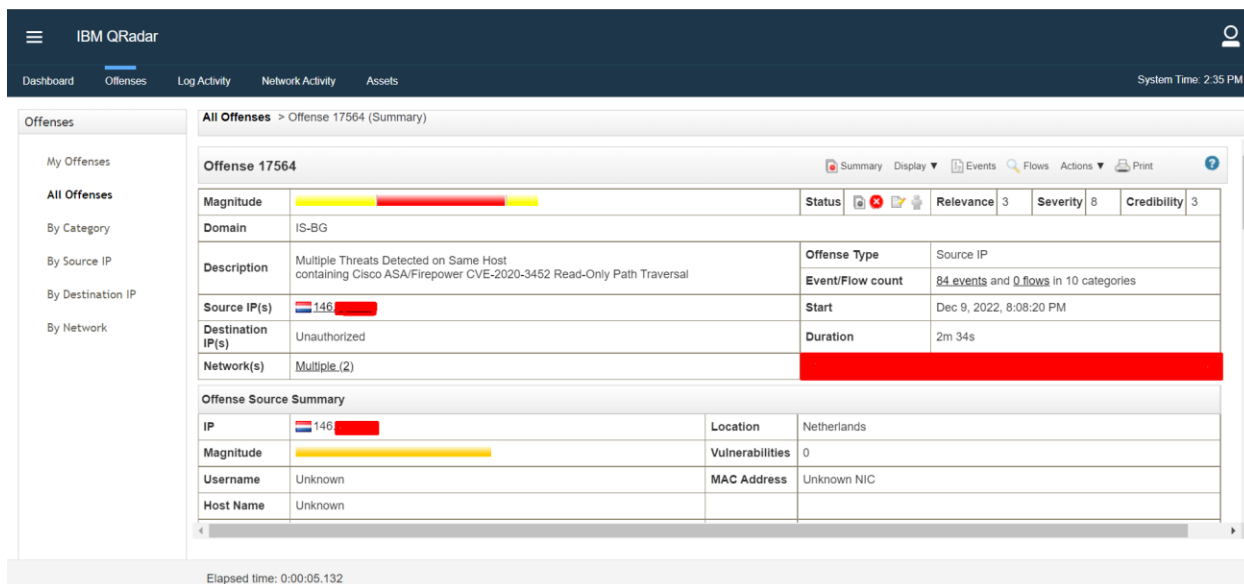


The screenshot displays the IBM QRadar Offense Manager interface. The top navigation bar includes 'Dashboard', 'Offenses', 'Log Activity', 'Network Activity', and 'Assets'. The 'Offenses' tab is active, showing a list of offenses. The table columns include 'Offense ID', 'Signature', 'Description', 'Source IP', 'Destination IP', 'Severity', 'Credibility', 'Relevance', and 'Magnitude'. A red vertical bar masks the 'Source IP' column for several rows. The offenses are sorted by relevance, with the most severe at the top. The bottom of the screen shows 'Displaying 1 to 28 of 4715 items (Elapsed time: 0:00:02.184)' and 'Page: 1'.

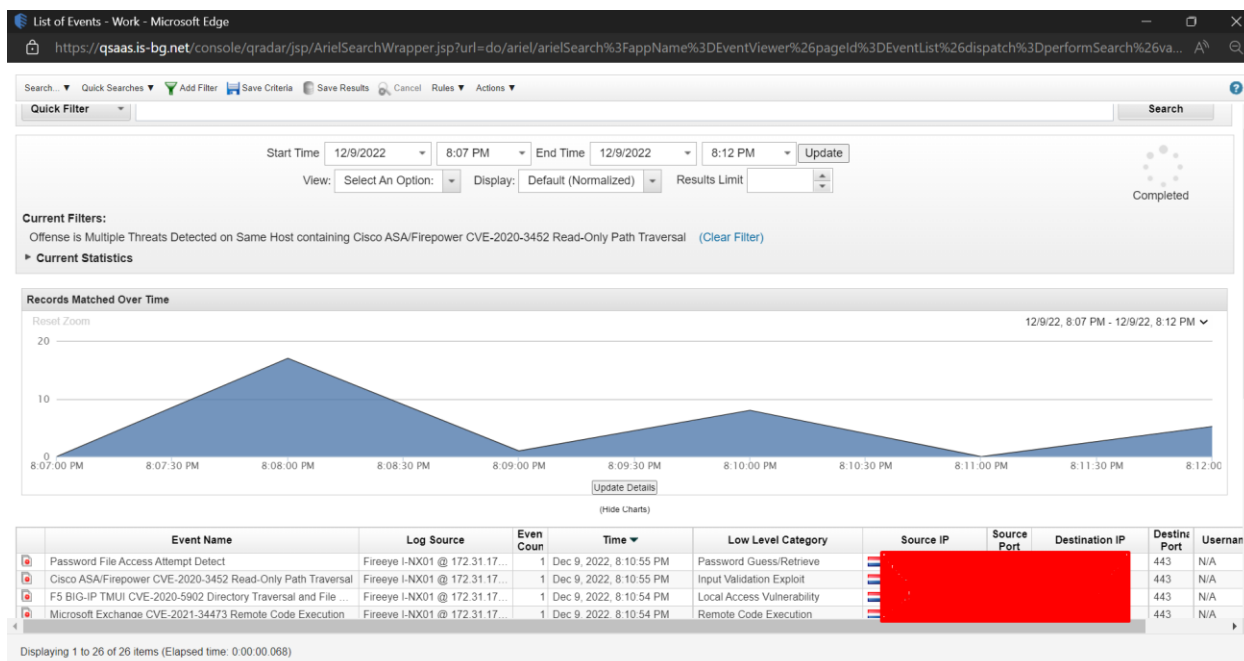
Offense ID	Signature	Description	Source IP	Destination IP	Severity	Credibility	Relevance	Magnitude
16531	IS-BG	Multiple Exploit/Malware Types Targeting a Single Destination containing SQL-Injection		217.145....	5.1	5.1	5.1	Multipl
17474	IS-BG	Multiple Exploit/Malware Types Targeting a Single Destination containing Misc Exploit		217.145....	5.1	5.1	5.1	Multipl
17586	IS-BG	Communication with a Potential Hostile IP Address (Flows) containing Web.SecureWeb	5.181.80		5.1	5.1	5.1	5.1
17585	IS-BG	Communication with a Potential Hostile IP Address (Flows) containing Web.SecureWeb	5.181.80		5.1	5.1	5.1	5.1
17583	IS-BG	Communication with a Potential Hostile IP Address (Flows) containing Web.SecureWeb	5.181.80		5.1	5.1	5.1	5.1
17581	IS-BG	Communication with a Potential Hostile IP Address (Flows) containing Web.SecureWeb	5.181.80		5.1	5.1	5.1	5.1
17579	IS-BG	Communication with a Potential Hostile IP Address (Flows) containing Web.SecureWeb	5.181.80		5.1	5.1	5.1	5.1
17578	IS-BG	Communication with a Potential Hostile IP Address (Flows) containing Web.SecureWeb	5.181.80		5.1	5.1	5.1	5.1
17588	IS-BG	Multiple Exploit/Malware Types Targeting a Single Destination containing Access from malicio...		217.145....	5.1	5.1	5.1	Multipl
17576	IS-BG	Communication with a Potential Hostile IP Address (Flows) containing Web.SecureWeb	5.181.80		5.1	5.1	5.1	5.1
17582	IS-BG	Communication with a Potential Hostile IP Address (Flows) containing Web.SecureWeb	93.123.1		93	93	93	93
17580	IS-BG	Communication with a Potential Hostile IP Address (Flows) containing Web.SecureWeb	93.123.1		93	93	93	93
17577	IS-BG	Communication with a Potential Hostile IP Address (Flows) containing Web.SecureWeb	91.92.10		91	91	91	91
17575	IS-BG	Multiple Threats Detected on Same Host containing OpenVAS Scanning Activity	195.191.		191	191	191	191
17556	IS-BG	Communication with a Potential Hostile IP Address (Flows) containing Web.SecureWeb	5.181.80		5.1	5.1	5.1	5.1
17557	IS-BG	Communication with a Potential Hostile IP Address (Flows) containing Web.SecureWeb	5.181.80		5.1	5.1	5.1	5.1
17523	IS-BG	Multiple Exploit/Malware Types Targeting a Single Destination containing Access from malicio...		217.145....	5.1	5.1	5.1	Multipl
17571	IS-BG	Communication with a Potential Hostile IP Address (Flows) containing Web.SecureWeb	78.130.1		78	78	78	78
17572	IS-BG	Communication with a Potential Hostile IP Address (Flows) containing Web.SecureWeb	91.92.10		91	91	91	91
17564	IS-BG	Multiple Threats Detected on Same Host containing Cisco ASA/Firepower CVE-2020-3452 Re...	146.0.77		141	141	141	141
17558	IS-BG	Communication with a Potential Hostile IP Address (Flows) containing Web.SecureWeb	5.181.80		5.1	5.1	5.1	5.1
17574	IS-BG	Excessive Login Failures via RDP to the same Machine containing Failure Audit: An account f...		PSRV2	Unaut	Unaut	Unaut	Unaut
17563	IS-BG	Communication with a Potential Hostile IP Address (Flows) containing Web.SecureWeb	184.75.2		18	18	18	18

In QRADAR cyber offences are given a score which is a combination of Relevance, Severity, Credibility and Magnitude. The most severe case will appear at the top because they can cause more damage than others. In the screenshot below I am showing a cyber offence coming from The Netherlands. It is a relatively simple case to investigate since our defensive IT structure has identified the problems for me.





If we take a look at the graph for offences over time we can see that there are several incidents appearing in the span of just a couple of minutes.



Looking at the most important log events we can see more information for what the sender was trying to achieve. With some research we can see that the sender was trying to request handshakes, but the firewall management center has denied access. After that he tried several exploits aimed at one our protected websites including (Remote code execution, Brute forcing, attempts at password

retrieval, malware injection and information leaks). Those attempts were stopped by a tool called FireEye NX

List of Events - Work - Microsoft Edge

https://qsas-is-bg.net/console/qadar/jsp/ArielSearchWrapper.jsp?url=do/arielSearch%3FappName%3DEventViewer%26pageId%3DEventList%26dispatch%3DperformSearch%26va...

Search Quick Searches Add Filter Save Criteria Save Results Cancel Rules Actions

(Hide Charts)

	Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP	Destination Port	Username
	Password File Access Attempt Detect	Fireeye I-NX01 @ 172.31.17...	1	Dec 9, 2022, 8:10:55 PM	Password Guess/Retrieve	146	33138	217.14	443	N/A
	Cisco ASA/Firepower CVE-2020-3452 Read-Only Path Traversal	Fireeye I-NX01 @ 172.31.17...	1	Dec 9, 2022, 8:10:55 PM	Input Validation Exploit	146	33132	217.14	443	N/A
	F5 BIG-IP TMUI CVE-2020-5902 Directory Traversal and File	Fireeye I-NX01 @ 172.31.17...	1	Dec 9, 2022, 8:10:54 PM	Local Access Vulnerability	146	33138	217.14	443	N/A
	Microsoft Exchange CVE-2021-34473 Remote Code Execution	Fireeye I-NX01 @ 172.31.17...	1	Dec 9, 2022, 8:10:54 PM	Remote Code Execution	146	33128	217.14	443	N/A
	SERVER-WEBAPP Microsoft Exchange autodiscover server si...	IS FMC	1	Dec 9, 2022, 8:10:07 PM	Potential Misc Exploit	146	33128	10.140	443	N/A
	Web Application Attack	IS FMC	1	Dec 9, 2022, 8:10:07 PM	Web Exploit	146	33132	10.140	443	N/A
	SERVER-OTHER Fortinet FortiOS and FortiProxy authenticati...	IS FMC	1	Dec 9, 2022, 8:10:07 PM	Potential Misc Exploit	146	33222	10.140	443	N/A
	SERVER-WEBAPP F5 BIG-IP Traffic Management User Interfa...	IS FMC	1	Dec 9, 2022, 8:10:07 PM	Remote Code Execution	146	33138	10.140	443	N/A
	SERVER-WEBAPP VMware vSphere Client remote code exec...	IS FMC	1	Dec 9, 2022, 8:09:53 PM	Remote Code Execution	146	33126	10.140	443	N/A
	VMware vSphere CVE-2021-21985 Remote Code Execution V...	Fireeye I-NX01 @ 172.31.17...	1	Dec 9, 2022, 8:08:43 PM	Remote Code Execution	146	33126	217.14	443	N/A
	Multiple Threats Detected on Same Host	Custom Rule Engine-126 : ...	1	Dec 9, 2022, 8:08:43 PM	Malware Infection	146	33132	217.14	443	N/A
	FortiOS SSL VPN Information Disclosure	Fireeye I-NX01 @ 172.31.17...	1	Dec 9, 2022, 8:08:43 PM	Information Leak	146	32962	217.14	443	N/A
	Suspicious Telnet UI Request	Fireeye I-NX01 @ 172.31.17...	1	Dec 9, 2022, 8:08:43 PM	Remote Code Execution	146	33140	217.14	443	N/A
	F5 BIG-IP TMUI CVE-2020-5902 Directory Traversal and File	Fireeye I-NX01 @ 172.31.17...	1	Dec 9, 2022, 8:08:43 PM	Local Access Vulnerability	146	33138	217.14	443	N/A
	Cisco ASA/Firepower CVE-2020-3452 Read-Only Path Traversal	Fireeye I-NX01 @ 172.31.17...	1	Dec 9, 2022, 8:08:43 PM	Input Validation Exploit	146	33132	217.14	443	N/A
	Microsoft Exchange CVE-2021-34473 Remote Code Execution	Fireeye I-NX01 @ 172.31.17...	1	Dec 9, 2022, 8:08:43 PM	Remote Code Execution	146	33128	217.14	443	N/A
	Password File Access Attempt Detect	Fireeye I-NX01 @ 172.31.17...	1	Dec 9, 2022, 8:08:43 PM	Password Guess/Retrieve	146	33138	217.14	443	N/A
	CONNECTION_STATISTICS - Deny	IS FMC	2	Dec 9, 2022, 8:08:37 PM	Firewall Deny	146	33222	10.140	443	No
	CONNECTION_STATISTICS - Deny	IS FMC	1	Dec 9, 2022, 8:08:37 PM	Firewall Deny	146	33138	10.140	443	No
	CONNECTION_STATISTICS - Deny	IS FMC	1	Dec 9, 2022, 8:08:37 PM	Firewall Deny	146	33128	10.140	443	No
	CONNECTION_STATISTICS - Deny	IS FMC	1	Dec 9, 2022, 8:08:37 PM	Firewall Deny	146	33132	10.140	443	No
	CONNECTION_STATISTICS - Allow	IS FMC	51	Dec 9, 2022, 8:08:35 PM	Firewall Permit	146	33866	10.140	443	No
	CONNECTION_STATISTICS - Allow	IS FMC	8	Dec 9, 2022, 8:08:25 PM	Firewall Permit	146	60770	10.140	443	No
	CONNECTION_STATISTICS - Allow	IS FMC	1	Dec 9, 2022, 8:08:25 PM	Firewall Permit	146	53576	10.140	443	No
	CONNECTION_STATISTICS - Allow	IS FMC	1	Dec 9, 2022, 8:08:20 PM	Firewall Permit	146	53576	10.140	443	No
	CONNECTION_STATISTICS - Allow	IS FMC	1	Dec 9, 2022, 8:08:20 PM	Firewall Permit	146	40127	10.140	443	No

Displaying 1 to 26 of 26 items (Elapsed time: 0 00 00 068)

The response to this attack is blacklisting the IP after we are sure that there are no successful data leaks.

## 4.4 Working with IBM Resilient

IBM Resilient is an extension to QRADAR. It provides automated threat responses to cyber security offences. It does so by determining the severity and activity of a given case and comparing it to a set of rules set up by the security team. In the picture below I have provided a screenshot of the activity dashboard. My work process was divided in setting up rules and then testing them with old offences to see if they worked.

IBM Security QRadar SOAR

Dashboards ▾

Artifacts

Incidents

Create incident ▾

2

Ivan Arbaliev

Information Services ▾

Activity Dashboard

News Feed

Show Types 

All ▾

Tasks Due Soon

You have no tasks due soon.

Generated Reports

You have no generated reports.

Need Help?

Documentation

All the information you need to get up and running.

?

Resource Library

Comprehensive resources for breach notification rules and security incident response best practices.

11/14/2022 05:24:49

System User modified Artifact **80.76.51.210** on incident **Test vito**

11/14/2022 05:24:41

System User modified Artifact **80.76.51.210** on incident **Test vito**

11/14/2022 04:24:49

System User modified Artifact **179.157.7.171** on incident **Test vito**

11/13/2022 08:46:54

fn\_virustotal wrote a note on the incident **Test vito**

Artifact: 80.76.51.212 detected\_urls

Positives: 1

First Seen Date: 2022-10-05 19:47:06

Last Seen Date: 2022-10-05 19:47:06...

11/12/2022 19:44:49

System User modified Artifact **80.76.51.210** on incident **Test vito**

11/12/2022 19:44:41

System User modified Artifact **80.76.51.210** on incident **Test vito**

11/12/2022 18:05:42

System User modified Artifact **1.2.3.4** on simulation QRadar ID 269 , SIM User Action preceded by SIM User Authentication - 1.2.3.4

11/12/2022 18:04:51

System User modified Artifact **1.2.3.4** on simulation QRadar ID 269 , SIM User Action preceded by SIM User Authentication - 1.2.3.4

11/12/2022 06:04:48

System User modified Artifact **80.76.51.210** on incident **Test vito**

11/12/2022 04:04:49

System User modified Artifact **179.157.7.171** on incident **Test vito**

The most common practice to determine whether an IP has malicious intents is to check it in Abuse DB (see chapter 3). That was the first function I added to Resilient but is probably the most crucial one for bringing a verdict to a case.

<input type="checkbox"/>	1.2.3.5	<b>IP Address</b>	~ AbuseIPDB Function hits added	11/02/2022 16:40	11/04/2022 16:46	1	11/02/2022 16:40 2258 / % Default Group	11/02/2022 16:40 2258 / % Default Group	—	On	On
<input type="checkbox"/>	1.2.3.4	<b>IP Address</b>	~ AbuseIPDB Function hits added ~ IBM X-Force Exchange ~ SANS Internet Storm Center	11/02/2022 16:40	11/02/2022 16:42	1	11/02/2022 16:40 2258 / % Default Group	11/02/2022 16:40 2258 / % Default Group	—	On	On

In the screenshot above I show the IP trust score function being added and in the screenshot below I show it working on an old QRADAR case that has been closed that I used for testing purposes.

Hits (1)

Filters

Added: 11/02/2022

AbuseIPDB Function hits added

Confidence Score

9

Number of Reports

2

Country

Australia

Most Recent Report

2022-10-13T11:59:45+00:00

Geolocation

Location

-33.494, 143.2104

Continent

OC

Country/Region

AU (Australia)

In the screenshots below I am showing what the creation of creating rules in Resilient looks like.

The screenshot shows the 'Create Incident' form in IBM Security QRadar SOAR. The top navigation bar includes 'Dashboards', 'Artifacts', 'Incidents', and 'Create Incident'. A yellow banner at the top states 'You are creating a simulation.' with a 'SIM' button. The left sidebar lists steps: 'Describe the Incident' (selected), 'Date and Location', 'Implications', 'Privacy', 'Team Formation', and 'Create'. The main form area is titled 'Describe and Name the Incident'. It contains the following fields:

- Incident Type:** Hostile IP
- NIST Attack Vectors:** Attrition (Denial-of-Service and Brute-Force Attacks), E-mail, Improper Usage
- Incident Disposition:** Unconfirmed
- Description:** A rich text editor with a toolbar showing 'Sans Serif', 'Normal', 'Bold', 'Italic', 'Underline', 'Link', 'Unlink', 'List', 'Unlist', 'Indent', 'Outdent', 'Text Color', 'Background Color', 'Image', and 'Table'.
- Name:** hostile ip test

A 'Next' button is located at the bottom right of the form. The footer indicates '© Copyright IBM Corporation 2022'.

The screenshot shows the 'Date and Location' step of the 'Create Incident' form. The left sidebar now shows 'Describe the Incident' as completed (checked) and 'Date and Location' as the current step. The main form area is titled 'Date and Location'. It contains the following fields:

- Date Occurred:** 11/14/2022 00:00:00 +02:00
- Date Discovered:** 11/14/2022 16:27:01 +02:00
- Address:** (empty field)
- City:** sofia
- Country/Region:** Bulgaria
- Postal Code:** 1235

'Previous' and 'Next' buttons are located at the bottom right of the form. The footer indicates '© Copyright IBM Corporation 2022'.

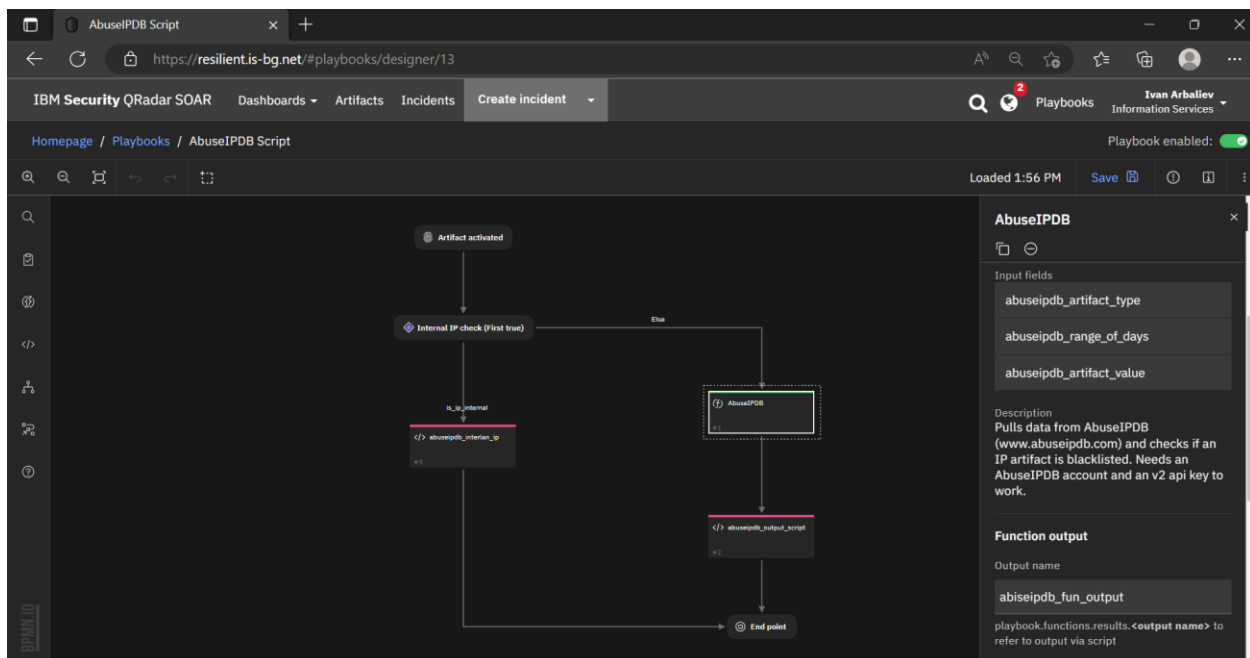
There are different vectors that should be considered for each case type. For example, was personal data involved? Did it leave the boundaries of the company? If so was it encrypted? Depending on these rules' cases are handled differently.

The screenshot shows the 'Create Incident' form in IBM Security QRadar SOAR. The 'Privacy' section is active, displaying a series of questions and input fields. A yellow banner at the top states 'You are creating a simulation.' The form includes a sidebar with navigation options: Describe the Incident, Date and Location, Implications, Privacy (selected), Team Formation, Regulators, Affected Individuals, Data Types, and Create. The 'Privacy' section contains the following fields:

- Was personal information or personal data involved? (Radio buttons: Yes, No, Unknown)
- Date Determined (Date picker: 11/14/2022 00:00:00 +02:00)
- Is harm/risk/misuse foreseeable? (Radio buttons: Yes, No, Unknown)
- Was the data encrypted? (Radio buttons: Yes, No, Unknown)
- Was the exposure resolved? (Radio buttons: Yes, No, Unknown)
- What was the source of the data? (Text input: Select Some Options)
- Data Format (Dropdown menu: Electronic)

Navigation buttons 'Previous' and 'Next' are located at the bottom right of the form.

In the screenshots below I am showing a playbook, workflow and scripts to the Ip validation and blacklisting functionality.



Security software comes with prebaked scripts. We just adapt the script to our network and databases.

Scripts / Abuseipdb API IP Check

Name \* Abuseipdb API IP Check

Description Script that checks a given IP in Abuseipdb using the API

Object Type \* Incident

---

Language Python 3 Mode Default Tab Size 2 - Font + Font

```
1 import requests
2 import json
3
4 URL_MAP = {
5     'incident': u"<a href='/#incidents/{0}'>{3}</a>",
6     'incident_element': u"<a href='/#incidents/{0}'>{0}</a>",
7     'task': u"<a href='/#incidents/{0}?taskId={1}&tabName=details&org_id={2}'>{3}</a>",
8     'artifact': u"<a href='/#incidents/{0}/artifact/{1}?org_id={2}'>{3}</a>",
9     'workflow': u"<a href='/#customize?tab=workflows&workflow={1}'>{3}</a>",
10    'playbook': u"<a href='/#playbooks/designer/{1}'>{3}</a>"
11 }
12
13 global apikey
14 apikey = '4a5442b285718b93f1b961059937bbe89a725281491176327bb0e1874bdfd511cbb6d75aea977f58' ##### ENTER API KEY HERE #####
15
16 ip_address = ### ENTER IP HERE ###
17
18 headers = {
19     'Key': apikey,
```

IBM Security QRadar SOAR Dashboards Artifacts Incidents Create incident

Layouts Rules Scripts Workflows Functions Destinations Phases & Tasks Incident Types

Workflows / AbuseIPDB Check IP Address Blocklist

Name \* AbuseIPDB Check IP Address Blocklist

API Name \* i abuseipdb\_check\_ip\_address\_blocklist

Description Pulls data from AbuseIPDB (www.abuseipdb.com) and checks if an IP artifact is blacklisted. Needs an AbuseIPDB account and an v2 api key to work. Default is reports from the last 30 days, but can be changed to as many as the last 365 days' reports.

Object Type \* Artifact

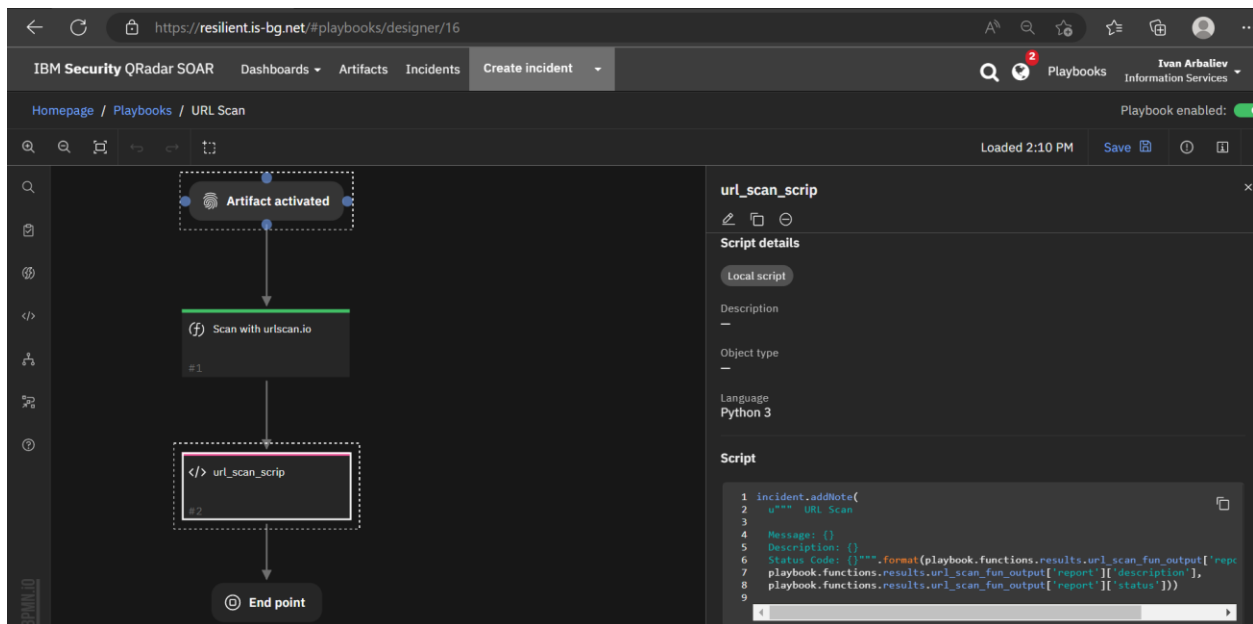
---

Start your workflow here

AbuseIPDB

Results are returned as a hit in the artifact

The screenshot below shows a function that scans URL and checks their validity. It can be used in email security scans to prevent phishing.



## Chapter 5: Conclusion

I used IBM QRADAR to analyze cyber threats and IBM Resilient to automate threat responses.

In the screenshot below I am showing a test of “Potential IP hosts” case executed automatically. The grey rows are not yet set up and the green ones with crossed text show that the process was executed successfully.



QRadar ID 13082 , Communication with a Potential Hostile IP ... closed

Description  
1 events in 2 categories: Communication with a Potential Hostile IP Address (Flows) containing Web.SecureWeb

Tasks Details Breach Notes Members News Feed Attachments Stats Timeline Artifacts Email Time tracking Tables

17% Complete Owner: 0 selected Status: Active Selected Add Task

Task Name	Owner	Due Date	Flags	Actions
<b>Engage</b>				
Initial Triage	Unassigned	No due date		
Determine if illegal activity is involved	Unassigned	No due date		
Determine if inappropriate internal involvement	Unassigned	No due date		
<b>Detect/Analyze</b>				
Collect volatile system data	Unassigned	No due date		
Select initial containment strategy	Unassigned	No due date		
Create backups of affected systems	Unassigned	No due date		
Disconnect compromised systems	Unassigned	No due date		
Analyze intruded systems	Unassigned	No due date		
Analyze network traffic for signs of intrusion	Unassigned	No due date		
Analyze application data for signs of intrusion	Unassigned	No due date		
Review the output and status of anti-virus software	Unassigned	No due date		

I learned a lot of new things concerning my future cybersecurity career. My initial assignment was to create an automated solution that makes decisions according to preset rules. I researched different problems using a variety of different CMD methods and I can say my research helped me come up with solution to my problems and answers to my questions. The final product should be operational for my demo in January 2023. The SOAR is expected to be in production in April 2023 according to my internship mentor.

# Learning outcomes

**Knowledge and insight** – In order to create a sufficient workflow/playbook for the cyber analyst I studied the process of analyzing cyber threats. Once I got access to the QRADAR SIEM I investigated cyber alerts using various methods for reaching a satisfactory final verdict. Being a cyber security analyst requires not only deep knowledge in the field of protection and security (how can a system network be as secure as possible without sacrificing functionality) but some knowledge in the offensive field as well (how are viruses distributed, how do they affect a given system, what are the latest and most vulnerable attack vectors). I learned a lot during my internship regarding pure knowledge in the cyber security field that I think will be beneficial for my future career.

**Analysis** – Analyzing the problem was intertwined with analyzing the process of reviewing and closing cyber alert tickets. This includes knowing why and where my internship company was receiving potential cyber-attacks, taking steps for mitigating the attack, checking for data leaks, and reverse engineering hostile executables in a controlled environment.

**Advise** – I would advise myself and everyone trying to implement automation into cyber security not to underestimate the difficulty and complexity of the project. It was harder than I initially expected but I managed to come up with a solution to the problem.

**Design** – Once I had enough knowledge and experience in analyzing cyber threats I knew which parts of the process can be automated reliably and which should be left partially automated with the supervision of the security specialist. I designed automation playbooks on my experience with insights into where the process can be sped up and when it will only tank the performance of the investigator. With that in mind I think I found the sweet spot for automation that blends automated repetitive processes and manual work.

**Realization** – At the start of my internship I wanted to develop full automation of existing cyber analyst processes. The moment of realization for me came when I was close to being done with the automation tool IBM Resilient, that not all processes are reliable when fully automated. Yes a lot of them can be but not everything should be automated. I created my fully automated playbook and immediately saw problems occur. The simpler stuff like checking the sender IP rating and checking for suspicious data movement/requests worked fine when automated, but pickier stuff like reverse engineering a virus and documenting its function often came with inconclusive results. That is why I decided to blend automation with partial automation for more severe cases of cyber-attacks.

**Manage and control** – It is safe to say that I never felt out of control during my internship regarding my progress on the project and my general ability to perform my work tasks. There were a couple of cases where I needed to ask for more access for working with specialized programs, but my team leader always granted it in just 2 or 3 days. I would not classify that as “being out of control” but more like “slight delay”. I managed to complete a large part of my research quite early into the semester and I was left with working on my project and enhancing my internship report along the way.

**Judgment** – Deciding which processes should be automated and which processes should be left partially automated was quite hard because I wanted to provide as much automatic functionality as possible. Every minute saved could be invested into another cyber alert potentially intercepting an incoming attack. I think I did a good job at judging that and I am happy with the results.

**Communication** – Communication between me and my colleagues was always smooth and hassle-free. They were with me in the office most of the time and never hesitated to answer my questions and help me if I got stuck on a case. My internship mentor is a busy person, but he was always there for me for advice and guidance both in person and on MS Teams. I am pleased that there was no language barrier between us which made things a little bit simpler when I wanted to ask a question.

**Learning ability** – When I finished my cyber security semester I was more inclined towards the “red hat” hackers. That changed when I started my internship in “Information services”. I learned a lot about the defensive mechanisms and structures behind big enterprises. This includes working with SIEM, setting up SOAR automation, developing playbooks/workflows for SOAR, investigating cyber security alerts, documenting my findings in a presentable and readable form, reverse engineering and examining viruses, and scanning networks for suspicious activity. Now that I am close to finishing my internship semester I am sure that “blue hat” (defensive cyber security) is my thing and I wish to improve in that.

# References

You tube security tutorials -

<https://www.youtube.com/watch?v=9NE33fpQuw8&list=PLG49S3nxzAnkL2uIFS3132mOVKuzzBxA8>

IBM documentation –

[https://www.ibm.com/docs/en/qsip/7.4?topic=SS42VS\\_7.4/com.ibm.qradar.doc/c\\_qradar\\_pdfs.htm](https://www.ibm.com/docs/en/qsip/7.4?topic=SS42VS_7.4/com.ibm.qradar.doc/c_qradar_pdfs.htm)

IBM SOAR documentation –

<https://www.ibm.com/support/pages/resilient-systems-user-guide-v34>

<https://docs.splunk.com/Documentation/SOAR/current/Admin/Intro>

# Evaluation

During my internship I met amazing new people, gained insight and knowledge on cyber security and threat hunting, as well as how to create and secure my own environment. I can say the time I spent in IS was beneficial for my future career as well as for my own personal development. In my research, I explored various tools and methods, and I gave advise on best practices for using them. I am happy to say my internship was a success. Communication with my internship mentor and student coach was helpful and always on time. In my opinion I have become part of the team and after I get my diploma from Fontys I will come back to work for IS again. I must express my gratitude towards my internship mentor, Simeon Kartselyanski for his fast communication, accurate and insightful advice and for taking me with him to extra investigations in other companies. I managed the problems that came along the way with his support and managed to come up with satisfactory solutions and results.

# Internship mentor assessment

Assessment form – Graduation and Internship, Portfolio and Thesis – v1.2

Student name	Ivan Arbaliev
Student number	3883876
Graduation Profile	
Date assessment	09.01.2023

U: Unsatisfactory/Onvoldoende, S: Satisfactory/Voldoende, G: Good/Goed, O: Outstanding/Uitmuntend

	Assessment dimensions	U	S	G	O	Feedback
1	Knowledge and Insight	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	I am happy that he had previous experience with cyber security and he managed to get to operational level very quickly.
	Application of Knowledge and Insight					
2a	Analysis	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	I am very happy with the way Ivan analyses problems and reacts to them.
2b	Advise	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	Ivan kept me well informed about his project progress and gave ideas for improving it further.
2c	Design	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	His design decisions were his biggest weakness but with time they improved to a sufficient level.
2d	Realisation	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	Ivan managed to complete all of the task given to him without much complications.
2e	Manage & Control	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	Ivan found ways to manage his tasks without requiring too much help.
3	Judgement	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	Ivan underestimated the vastness of the project but came up with good solutions that we can use to put the product into production soon.
4	Communication	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	Communicates well and doesn't hesitate to ask questions.
5	Learning ability	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	Fast learner, eager to read documentation and asked for extra materials on different topics.

Assessment form – Graduation and Internship, Portfolio and Thesis – v1.2

**Explanation**

My final assessment for the work is positive and good. Ivan copes well with the assigned tasks, as his strengths are the search and processing of information, its detailed understanding and analysis  
He has difficulties in the design of processes when working with multiple systems, but this is based on the little work experience he has and will improve with time.

**Final grade (U/S/G/O):**

G

**In case of Unsatisfactory ("U") result, advice to the Exam Commission about repair possibility:**

Assessment form – Graduation and Internship, Portfolio and Thesis – v1.2

Assessor 1:	Signature
Simeon Kartelyanski	<div> Simeon Pepov Kartelyan ski </div> <div> Digitally signed by Simeon Pepov Kartelyanski Date: 2023.01.09 14:43:52 +02'00' </div>
Assessor 2:	Signature
Date:	Place:
09.01.2023	Eindhoven