Aalto University
School of Science
Master's programme in ICT innovation – Human-Computer Interaction and Design

Cîmpan Andra

Applying design system in cybersecurity dashboard development

Master's Thesis
Espoo, July 20, 2019

Supervisor: Marko Nieminen, Professor of Usability and User Interfaces
Thesis advisor(s): Virág Benke, MA (Sociology)

AALTO UNIVERSITY
School of Science
Master’s programme in ICT innovation

ABSTRACT OF THE
MASTER´S THESIS

Author: Cîmpan Andra

Title of the thesis: Applying design system in cybersecurity dashboard development

Degree programme: Master of Science (Technology) Master's Programme in ICT Innovation	**Major:** Human-Computer Interaction and Design	
Number of pages: 83+8	**Date**: 26.07.2019	**Language:** English
Supervisor: Marko Nieminen	**Advisor:** Virág Benke	

Abstract:

This thesis evaluates the applicability of a particular Design System in the development of a dashboard that addresses the needs of cybersecurity teams. This work is motivated by the reduced knowledge of the specific needs that a dashboard for cyber security products could encounter and by the narrow understanding of the limitations and challenges that the applicability of a design system on such a targeted system could encounter. The context of research, development and testing is the multinational Ericsson which offer the opportunity to gain access to not only to experts from Finland but worldwide.

The initial efforts were directed towards identifying and understanding the users, their needs and tasks, and the environment in which they operate. This qualitative data is obtained by performing a literature review on the state of the art and multiple interviews with experts from Security Operation Centres. After the requirements have been collected and by utilising the Design System, a design for the dashboard is presented and tested with experts.

The primary outcome of this thesis comes in the form of a user-centred methodology for the extraction of expert knowledge and its conversion into requirements. The proposed solution constitutes a baseline approach towards identifying the needs of professionals in an environment in which the access to users is limited.

Keywords: User-centered design, Design System, Cyber security, Dashboard

Preface

Throughout the writing of this master's thesis I have received a great deal of support and assistance for which I am deeply grateful.

I would first like to thank my supervisor, Marko Nieminen, whose expertise was invaluable in the formulating of the research topic and methodology in particular.

I would like to acknowledge my colleagues from Ericsson Finland for their wonderful collaboration and support. I would particularly like to thank to my advisor Virág Benke for the excellent cooperation and for all of the support I was given to conduct my research.

Finally, I would like to thank my family for their wise counsel and for their great support.

Without your support, this journey would not have been possible.

Thank you.

Table of Contents

List of Figures

List of Tables

1. Introduction

1.1 Background

The engine behind this dynamic era of accelerating possibility is software. As more innovative products that aimed for more life-improving breakthroughs were launched on the market, software became ubiquitous and essential in every aspect of our modern lives. The development of new software system is one of the drivers behind the economic growth and the software is predicted to magnify and exponentially expand opportunities throughout other sectors too. (BSA The Software Alliance, 2016)

The rise in the importance of the software industry led to an increase in the complexity of the developed digital products. In order to reduce the complexity, to validate the needs, and to evaluate the core business assumptions early in the product development process, the modern organisations proceeds the product development and design on user research. Following a user-centred approach and a continuous feedback loop with customers during the course of product development, a superior solution can be achieved which offers a competitive advantage for the organisation. (Maurya, 2012)(Bohemia, Liedtka and Rieple, 2012) The benefits of following a user-centred or human-centred process can be measured by analysing the costs during the entire lifecycle of the product, from conception and design to implementation to maintenance and finally, disposal.(Enanv *et al.*, 2010)

The user-centred design approach consists of a set of activities that are performed throughout the entire lifecycle of the development of the product. The iterative process contains three main phases which are research, design and evaluation. According to the ISO 9241-210:2010, the design should be built on a steady research and on the "understanding of users, tasks and environments"(Enanv *et al.*, 2010), the users should be consulted during the design and development process as their insights are a "a valuable source of knowledge about the context of use, the tasks, and how users are likely to work with the future product, system or service"(Enanv *et al.*, 2010). The design of the product should also be "refined by user-centred evaluation". The feedback provided by users is an essential source of inspiration and is a crucial method of reducing the risk of the final result not corresponding to the organizational needs. For the final acceptance of the product, user-centred evaluation should be performed to validate that requirements have been met.

One of the obstacles that is encountered by the design teams while using the user-centred design approach for products that are dedicated to experts is the limited contact with the users. In order to overcome this impediment, multiple methods have been developed with the scope of maximising the information collected and designing considering the users and their cognitive principles.

A problem that is faced when developing digital products at a large scale is maintaining consistency. Due to the increased demand for content velocity, in recent years, companies started their quest for a faster way of designing and building the customer experience. A solution to this problem that has increased in popularity and is implemented by many organisations such as Airbnb, Audi, Polaris, IBM and Yelp is design systems. By developing a design system that incorporates and illustrates the values of the company and by integrating this framework into the product development process they hope to reduce the design debt, to accelerate the design process and increase the collaboration within the team. (Adobe XD, 2019) The promise behind the utilization of a design system is that it will save time in the design and implementation phases as it provides elements that can be reused, it will facilitate a faster launch of the product on the market, it will assure a brand unity across a product or a line of products and it will be a shared language that will enable collaboration within the team.(Alla-Kholmatova, 2017)(Pyrhönen, 2019)

A challenge that was identified from the beginning regarding the topic of design systems is that little research on this matter has been performed in the academic field and the majority of the information available today is provided from the industry. Large organisations present their experiences on implementing such a system and then utilizing it as a tool for building their product but more research on the applicability should be performed in the academic world. (Alla-Kholmatova, 2017; Pyrhönen, 2019)

1.2 Purpose and Context of the Study

The aim of this masters thesis is to discover and highlight the specific needs that a dashboard for cyber security products could encounter. The starting hypothesis is that in the case of security experts, the dashboard should provide immediate, “at-a-glance” monitoring of the network and of the events that are taking place on it, in order to help analysts make key decisions on how that should proceed in their work. In order to validate this hypothesis and to achieve the goal of offering a tailored experience, the design process has to focus on user needs and preferences, but also identify which are the most appropriate visual encodings to be used, to enable a better interpretation of the data and to improve the ability of making sense of the information. It is crucial to perform a user research in order to grasp a firm understanding of the users of the product and to determine the level of expertise, the environment in which they operate and the tasks that have to be performed.

The thesis aims to also tackle the implementation of the product, based on a defined design system and what the challenges and limitations of it could be, when it comes to such a targeted product. Design system adoption has increased in the past few years as their ability to enable teams to build digital products faster, improve company collaboration, increase productivity, saving time and money, has been proven by successful products from leaders in the tech business. As the tech industry evolves and user-centred design becomes the core of building products, implementing a design system across the enterprise suites of applications becomes crucial in unifying the brand experience, creating consistency, a visual harmony and improving the usability.

The context of study for this thesis has been Ericsson - a multinational telecommunication company. The company’s portfolio covers four main topics: “Networks, Digital Services, Managed Services and Emerging Business”. (Ericsson, 2018a)

With a multitude of products under their umbrella, some of the challenges that the company face, especially concerning the design is the consistency of the look and feel across the product and the development of a customer development approach where the product development is focused on the customer needs. This thesis aims to implement the

Design system developed in the company to a section of the product – the Dashboard while consulting the users for the validation of the results.

The thesis will consist of three parts, one of them being the discovery of the user requirements and needs for the dashboard of the cyber security product. The results of the research that has been performed in phase one will not only add value to the business but would also provide information that can be used during the design and development phase to identify needs and emphasize the team with the users. The second phase will focus on implementing the findings according to the design system and complying to the brand guidelines that the design system has put into place. The third step will validate the decisions that were made and will identify problems that should be solved in the future.

1.3 Research Questions

Drawing on the challenges presented in the previous chapter, the following research questions are addressed in this work:

- What is the role of a dashboard for cybersecurity professionals?
    - What are Dashboards?
    - What are the needs of cybersecurity experts in regards to a dashboard?
    - How to study the needs? What are the user-centred design methods that can be applied for studying these needs? Is the Persona a valid method to use for the development of tools for experts, in cases where the contact with users is limited?

- How does the Design System approach support cybersecurity dashboard development?
    - Is the Design System in the case company suitable for such a product and can it cover all of the defined needs?

In order to answer these questions, the first phase of inquiry is to pose the initial research questions, followed by a literature review on the following three topics: Cybersecurity, focusing on Security Operation Centre scope and organizational structure, Dashboards and Design Systems in order to gain an understanding of the state of the art. By examining previous research, the first sub-question:" What are dashboards?" will be answered, and a classification of the elements that belong to a dashboard will be conceived.

Once this base understanding is attained, the second phase of action starts: the user research, based on interviews with security experts. In this phase, the persona method is applied and the requirements for the dashboard design are defined, responding to the sub-question: "What are the needs of cybersecurity experts in regard, to a dashboard?".

This step is followed by deciding on the requirements and by implementing the dashboard. At this point, the research question "How does the Design System approach support cybersecurity dashboard development?", concerning the suitability of the design system is answered. The last phase of action is the usability test, which has the goal of validating the relevance of the usage of persona method in the context of professionals, providing an answer for "Is the Persona a valid method to use for the development of tools for experts, in cases where the contact with users is limited?" and validating the relevance of the content accommodated in the dashboard. Following these phases, all the research questions have been answered and the desired outcome has been achieved. Once all of this is attained, the conclusion and the further work are formulated.

2. Related Research

2.1 Cyber Security

In the recent years, the number of connected devices increased at a fast pace, exceeding 17 billion in 2018. The vast diffusion and increase of connected devices grew the complexity of cyber infrastructure exponentially, which led to a higher number of vulnerable devices.(Dawson and Thomson, 2018). The likelihood of experiencing a security breach has risen substantially in the last few years according to a recent IBM study (Ponemon, 2017) and the attacks have escalated both in number and complexity. The growing size of the network is not the only factor that influences the total of potential attackers, but also the tools that are available to the attackers are becoming more complex, sophisticated, capable, and powerful.

Companies realize that, as technology represents a consistent part of the way they run their business, they are vulnerable and present a high risk to cyber security threats. In order to protect sensitive information about their clients, partners or internal operations from the rising sophistication of cybercriminals and hacking software, both big and small business started to explore new methods to protect themselves against potential attacks. Some of the strategies that they follow are either purchasing digital products that scan their networks, outsourcing their cybersecurity entirely to external service providers or the most effective approach that is starting to get a multitude of supporters among the strategy-focused organizations is creating a Security Operation Centre team. (Blackstratus, 2019)

Before addressing the utility that a Security Operation Centre brings in the organization, a clear definition of security has to be established. Security is considered as "a process to protect an object against physical damage, unauthorized access, theft, or loss, by maintaining high confidentiality and integrity of information about the object and making information about that object available whenever needed"(Abomhara and Køien, 2015). From this definition it can be extrapolated that cybersecurity is concerned with the comprehending of cyber-attacks and creating defence strategies in order to maintain the availability, confidentiality, and integrity of a digital system. These three attributes that are used in the industry to characterise the cyber security space indicate that "a secure system is available for normal use even in the face of an attack" (James Waldo , Herbert S . Lin, 2007) ; that a secure system guarantees that the information that is received by the user has not been modified after it has been sent – integrity , and that a secure system will preserve your confidentiality by denying non-authenticated party to access or examine your data.

The most common terms found at the base of cyber security are assets, vulnerabilities, exploits, threats and risks.

The first step in the process is to identify the system assets of the network and to make an inventory of the system components. An asset refers to any resource that is part of a network. The assets can be divided into two categories: "soft" which would include software programs and "hard", which would include host computers, servers, desktops, and laptops. Network assets are interconnected assets that rely on each other to provide a service. In order to effectively operate and maintain a network infrastructure, network assets must be efficiently managed and stored. (Roca and Cited, 2006)

The term “vulnerability” covers all the weaknesses found in the system or in the design of a system that may be exploited by allowing attackers to execute commands, access unauthorized data, or conduct denial-of-service attacks. These weaknesses can be found in hardware, software, firmware, operating systems, networks, or policies and procedures used in the systems. Some of the most common software security vulnerabilities are buffer overflow, missing data encryption, cross-site scripting and forgery, OS command injection, and URL redirection to untrusted sites.

The potential for a vulnerability to be exploited is called a threat. Threats can be divided into two categories based on their sources: nature and humans. The nature category covers events such as natural disasters that would affect the hardware of the computer systems. This type of disaster is impossible to prevent from happening and only minor safeguards can be arranged. On the other side, the human category covers threats produced by people or organizations, or by someone internal, that has the authorized access, either by someone external that is working outside the network and can be performed in a structured or unstructured manner (Abomhara and Køien, 2015).The likelihood of a threat to occur is found in the risk measurement which should be taken into consideration when prioritising vulnerabilities and their threat levels. A visual representation of the risk probability is presented below in Figure 1.

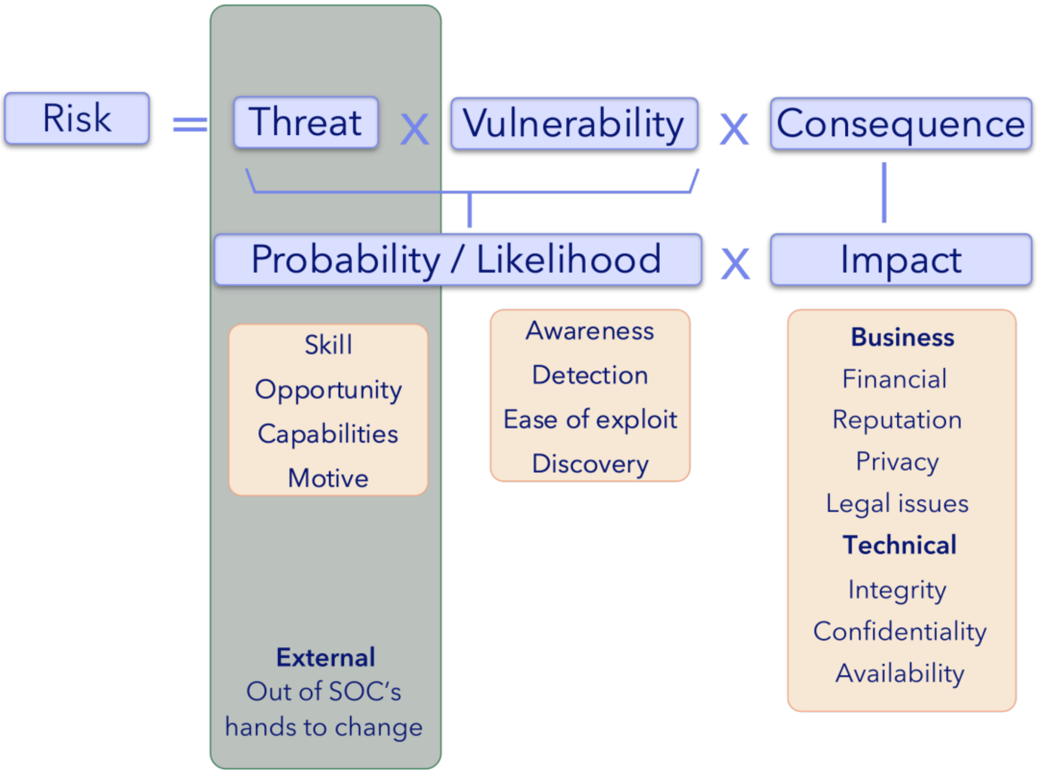


Figure 1: Risk formula

Exploiting vulnerabilities by using advanced tools and techniques, attackers can perform actions in order to harm a system or disrupt their behaviour.(Abomhara and Køien, 2015) Attacks can come in a multitude of forms, but they can be classified into two main categories:

- “ active ” – the attacker “ initiates commands to disrupt the network's normal operation ” (Pawar and Anuradha, 2015)

- “ passive ” – the attacker “ intercepts data traveling through the network ” (Pawar and Anuradha, 2015)

Some of the most common active attacks are:

- Spoofing
  The spoofing attack refers to the act of impersonating a trusted source (user or device) in the network in order to gain access to information, spread malware or bypass access controls. There are different types of spoofing, the most common ones being Website spoofing, IP address spoofing, ARP (Address Resolution Protocol) spoofing, and DNS (Domain Name System) server spoofing.

- Denial of services
  The denial of service attack refers to the act of flooding the network to prevent legitimate users of accessing the service.

- Wormhole
  The wormhole attack can be found in the literature also under the name of “tunnelling attack” and it implies that the attacker receives a package at a certain point in the network and it forwards it to another point from which point they are replayed into the network.

Some of the most well-known passive attacks consist of the following examples:

- Eavesdropping
  The eavesdropping, also known as man-in-the-middle attack, refers to the act of listening to the communication that operates through the network in order to gain access to confidential information. The standard defence for eavesdropping attacks is cryptography.

- Traffic Analysis
  The traffic analysis attack refers to the act of intercepting and examining the network traffic to identify patterns and behaviour in order to obtain information. This attack is performed when the traffic is encrypted.

The figure that is found below illustrates the relationship among these terms, the way they interact with each other, and the phases that they follow.

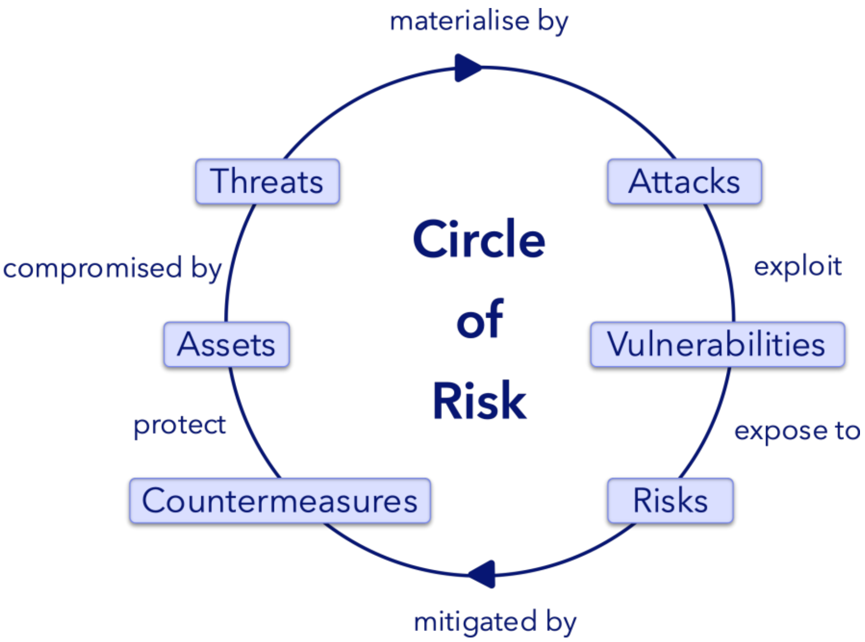


Figure 2: Circle of Risk

These are some of the most common terms that are used in the cybersecurity world. In today's world, cyber-attacks are enhancing their complexity and they feature sophisticated competences. Due to the increasing capabilities of the attacks and the evolving security landscape that offers new automated offensive tools, the chances of experiencing a security breach have risen incrementally in the last years. According to a study from IBM performed in 2017 (Ponemon, 2017), in one year period, in the US, one out of four organization will find themselves under a cyber-attack. Concluding from this number, and analysing the market that has to offer "well-organized libraries of offensive tools that are packaged on free-to-download-and-use Linux distributions such as Backtrack and Kali "(Muniz, McIntyre and AlFardan, 2015) cyber threats are no longer an exception but more of a daily reality in this technology driven age. As a response, businesses are developing new methods to protect themselves against potential cyber-attack such as investing in advanced tools that scan their networks, by outsourcing their cybersecurity to a third-party organization, or by creating in-house security operation centres.

The incorporation of Security Operation Centre (SOC) within the organization is starting to grow in popularity among strategy-focused companies. Having a SOC team has a paramount significance in the identification and defence against cyber-crime. The key responsibilities associated with the team are improvement of security incident detection through continuous monitoring and analysis of data activity, minimizing losses by preventing breaches that are considerably costly to businesses, increasing control and maintaining trust.

McAfee, one of the influential players in the security industry, states that the SOC responsibility is "monitoring, detecting, and isolating incidents and the management of the organization's security products, network devices, end-user devices, and systems". This function is performed around the clock (24/7), defending against intrusion any time of the day regardless of the attack type or source. The technology arsenal that helps them in the process is a suite of firewalls, probes, event management systems, and setup that collects data and monitors the network.

After reviewing and analysing a mixture of scientific and industry literature, the process of establishing a new SOC team within the organization could follow the steps presented in the scheme below:

Table 1: Scheme for SOC team development

Values	Establish the mission, vision & objectives		
	Define methodology & operating model		
Process	Identify	Understand the Environment	
		Business Environment	
		Risk Management & Strategy	
	Protect	Awareness & Training	
		Maintenance	
	Detect	Anomalies and Events	
		Detection Process & Monitoring	
	Respond	Response Planning	
		Analysis & Mitigation	
	Recover	Recovery Planning	
		Improvement	
Team	Roles & Responsibilities		
	Escalation Process		
	Human Factors & Mental Model		
	Schedule		

2.1.1 Establish the Mission, Vision & Objectives

At the core of effective detection is a well-functioning SOC. The pillars of a successful and excellence driven SOC are capable and skilled individuals, well defined and applied processes, and “a constant drive for continuous improvement to stay ahead of the cyber adversaries”.(EY, 2014)
Their mission, vision, and objectives should prioritise the following three main points:

- Support the business goals
- Comply with mandatory information security or privacy standards required in the industry
- Align with the overall risk posture (EY, 2014)

2.1.2 Define Methodology and Operating Model

In the case of cybersecurity, a methodology can be explained as a collection of procedures aimed to discover and prevent potential attacks in a way that minimizes the impact and provides fast recovery. The two frameworks for addressing cybersecurity that we are going to analyse are OODA loop and NIST.

Table 2: Comparison between OODA Loop and NIST framework

OODA Loop	Observe	Orient	Decide	Act
NIST	Monitor	Frame	Assess	Respond

The OODA loop was developed in the military context by the strategist Colonel John Boyd.(Gray *et al.*, 2015) The OODA Loop is particularly well-suited for cybersecurity. The four-step approach designed to determine the appropriate response to a problem acknowledges the complex environment in which it operates and offers a solution for effective effort prioritization. Translated to the cybersecurity field, the four steps are the following:

- Observe – collect and store data, continuously monitor the network
- Orient – analyse the collected data and search for suspicious events and activities
- Decide – categorise the event and evaluate it
- Act – execute the step determined by the analysis

One of the keys of the framework is integrating continuous improvement in the process, always implementing the lessons learned from the previous experiences into the system. By feeding new knowledge to the loop a better performance can be achieved in time. Working with the OODA Loop framework allows the team to treat emerging challenges and threats in an agile manner.

The NIST framework developed by the National Institute of Standards and Technology U.S. sets a guideline for businesses on how they should identify, detect and respond to cyber-attacks. According to the official documentation, the cybersecurity framework consists of three main components:

- Core – defines a set of activities used to achieve a certain cybersecurity result. The core can be divided into the following parts: functional – the outlined functions consisting in identify, detect, protect, respond and recover, categories and subcategories.
- Implementation Tiers – describes the degree to which an organization complies to the rules and characteristics presented in the framework.
- Profile - "the organization alignment of the requirements, objectives, risk appetite and resources against the desired outcomes of the framework's core"(National Institute of Standards and Technology, 2013)

The five functions are considered to act as the backbone of the framework core, and they are the pillars of a strong and successful cybersecurity procedure.

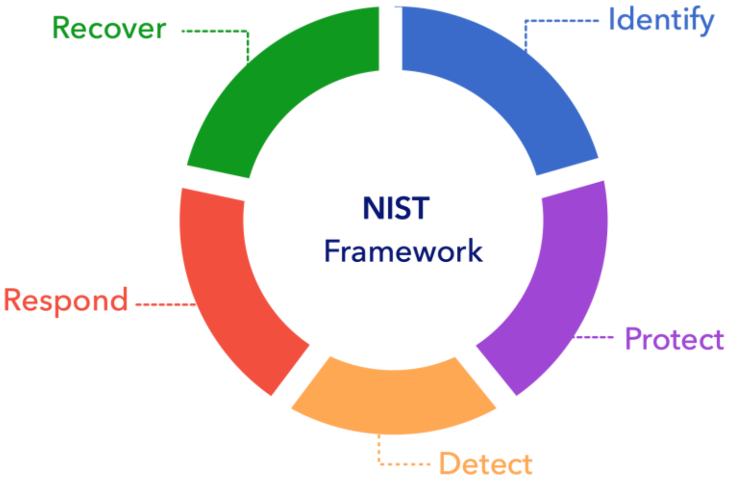


Figure 3: NIST Framework, figure adjusted from (National Institute of Standards and Technology, 2013)

2.1.3 Establish a Process

A well-established process enables the team to work with “consistent operations and repeatable outcomes” (EY, 2014). The process will follow the NIST framework, so all the steps fall in one of the five functional components. In order to obtain the best results, the SOC team should effectively document and implement the process and incrementally update and improve it.

The first step under the core functionality – “identify” is to understand the environment. From the beginning, the SOC team should determine the domain that needs to be monitored, to write the “use cases”, and to decide on the format of the data that will be collected. Establishing awareness of the assets as well as the hardware and the software that is running on the network should be a priority, followed by centralizing the display of assets in a tool that provides a real-time, comprehensive view of the activities that maximizes the chances of detecting threats as they occur or sooner. In the category of understanding the environment, we can also find the requirement of learning about the business needs, objectives and the value associated with specific decisions in order to prioritize and craft the most appropriate response.(EY, 2014) In the scope of enabling the business and offering security, the SOC needs an asset management system that will manage the events evaluating their risk and repercussions to the organization. Without understanding the “organization specific threat landscape and vulnerability status” (Muniz, McIntyre and AlFardan, 2015), dealing with risk cannot be achieved.

In the identify phase, the team is responsible to develop or set up with the available tools an intrusion detection system that monitors the network and automatically detects intrusion behaviour exploitation by matching signatures, which are patterns of known attacks against the network activity and triggers alerts. This detection is performed based on the defined use cases. A use case can be described as an event that requires the SOC monitoring or intervention and may include the involvement of a rule or alarm to meet the organization requirement.(McAfee and Intel Security, 2016) The use cases can be defined only after the environment is understood and the team has a deep knowledge of the assets and the company policies.

The SOC team has a limited amount of resources, so a prioritization of use cases definition should be defined. For the ranking and resource allocation a risk management process should be considered. As previously defined, a risk consists of the probability of a threat exploiting a vulnerability to arise and the impact of that execution. By performing a risk assessment, the team can take better informed decisions , decisions that can be categorised into one of the following activities: mitigate, transfer, accept or avoid. (Muniz, McIntyre and AlFardan, 2015)

A critical part of an efficient operation is the training of the team members. Proper education and continuous training ensure that the skills and knowledge of the team members is up to date and evolves with the changing threat landscape. The SOC will constantly evaluate their rules and use cases to assess their relevance and capabilities against advanced threats.

The core functionality – "detect" is based on events from different assets and systems. Monitoring the organization's assets and the activity on the network the team is expected to identify the incidents- events that must be acted upon and to react accordingly. The first step is to certify the validity of the incident and verify that the incident is enclosed within the scope assigned by the security operations team.

The scheme presented below presents a typical incident handling process by presenting the steps that have to be followed.(Muniz, McIntyre and AlFardan, 2015)

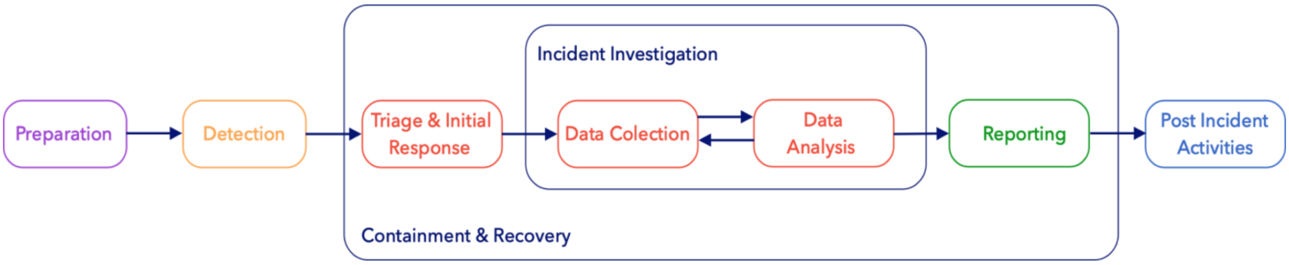


Figure 4: Incident handling process, figure adjusted from (McAfee and Intel Security, 2016)

In the detection phase, an incident is observed, and it is reported in the ticketing system available. The main purpose of the ticketing system is to ensure the assignment of the ticket and the continuity of the incident from a work shift to another. Some requirements that should be covered by the system are that it should provide a level of security, ensuring that sensitive data can be accessed only by authorised personnel, and should provide a structuring of incidents based on priority. A ticket reporting an incident must document the following aspects: source, channels, steps, and requirements.

The next step in the process is incident triage, which represents the initial actions that are performed on a detected event. The triage phase can be split into three sections: verification, classification, and assignment. For the categorization of events and incidents, a standard is available in the "organization's Governance Risk and Compliance System and metrics can be tracked accordingly for each category"(McAfee and Intel Security, 2016). The ten categories are:

- Training and Exercises

Event:

- Unsuccessful Activity Attempt
- Non-Compliance Activity
- Reconnaissance
- Investigating
- Explained Anomaly

Incident:

- Root Level Intrusion
- User Level Intrusion
- Denial of Service
- Malicious Logic

The triage process will prioritize the incident severity. The severity levels evaluate the impact of an incident. According to the category value that has been assigned to the incident, the appropriate resources will be allocated.

The lifecycle of a registered incident should conclude in some form of resolution. The objective of the incident resolution phase is to contain the incident as early as possible and to determine the root cause of the incident. In the containment step the team should stop an incident from escalating and prevent it from spreading to other systems. The analysis and investigation phase that is running in parallel with the containment has the purpose of identifying the assets that have been compromised, understanding the repercussions of the incident, and finding the succession of events that led to the incident.

The last phase in the process is incident closure which refers to eradicating and closing the vulnerabilities that led to the incident. In this step, the team has to assure that the traces of the incident have been cleaned and to test that eradication was effective.

After the incident closure, with the "lesson learned", the team goes through the post-incident phase, in which they use the knowledge gained to improve their process in order to prevent future incidents " in the form of proactive services such as enhancing the security features of functions within defences".(Muniz, McIntyre and AlFardan, 2015)

2.1.4 SOC Roles and Responsibilities

The following structure and division of tasks is recommended. As we can see from the structure part, an individual starts from the bottom – Security Analyst Level 1 and escalades in time and after gaining more skills, knowledge and experience within the team. The Security Analyst Level 2 and Security Analyst Level 3 are more experienced individuals that can handle more complex events. They are able to establish remediation and recovery strategies and to perform a continuous optimization of the security monitoring tools.

Table 3: Distribution of Roles and Responsibilities among the team

Structure	Role	Skills	Responsibilities
Level 1 Security Analyst 	**Triage specialist** The main responsibility is to monitor the "situational awareness and automation systems for security events" (SANDOVAL, 2018) and deciding how to act – either closing or escalating that event.	The skill set can be divided in the categories: - **System Administration** - **Programming** - **Security**	The L1 Security analyst identifies, categorizes and investigates events and performs the incident triage. Based on the alarms, they create tickets in the system and assign relevancy and urgency. Another responsibility of the L1 is to run vulnerability scans and to manage and configure security monitoring tools. (Tom D'Aquino, 2018)
Level 2 Security Analyst 	**Incident responder** The main responsibility is to perform a long-term analysis and investigation on the network activity.	The L2 possesses all of the L1 skill set plus an ability to handle stressful events and a curiosity to find the root cause of the incident.	Investigates tickets escalated from L1 and determine the remediation and recovery strategy. Another responsibility of the L2 is to "leverage emerging threat intelligence to identify impacted systems and the scope of the attack."(Tom D'Aquino, 2018)

Structure	Role	Skills	Responsibilities
Expert Security 	**Threat Hunter** The main responsibility is to research ways to determine “stealthy threats” using the latest threat intelligence.	Apart from the skill set, the Security Expert is familiar with penetration testing tools and visualization tools that are used in the process.	Improves and optimizes the security monitoring tools based on previous finds from the threat hunting. Identifies weaknesses and validates.
SOC Manager 	**Operations & Management** The main responsibility is to supervise the SOC team and to achieve the set goals through implementation of the process and procedures.	The SOC manager passed through all of the above phases before. An important skill that is needed in this position is strong leadership and good communication skills.	Responsible for maintaining smooth operations, for running compliance reports and supporting the audit process. Other key responsibilities are measuring the team performance and informing business leaders about the value of security operations.

2.1.5 Escalation Process of the Incidents Within the Team

The team and incident solving are based on intense collaboration within the team. A well-defined set of processes and procedures empower the team to operate in a manner that is sustainable and measurable. The escalation within the tiers in the organisation should follow the scheme:

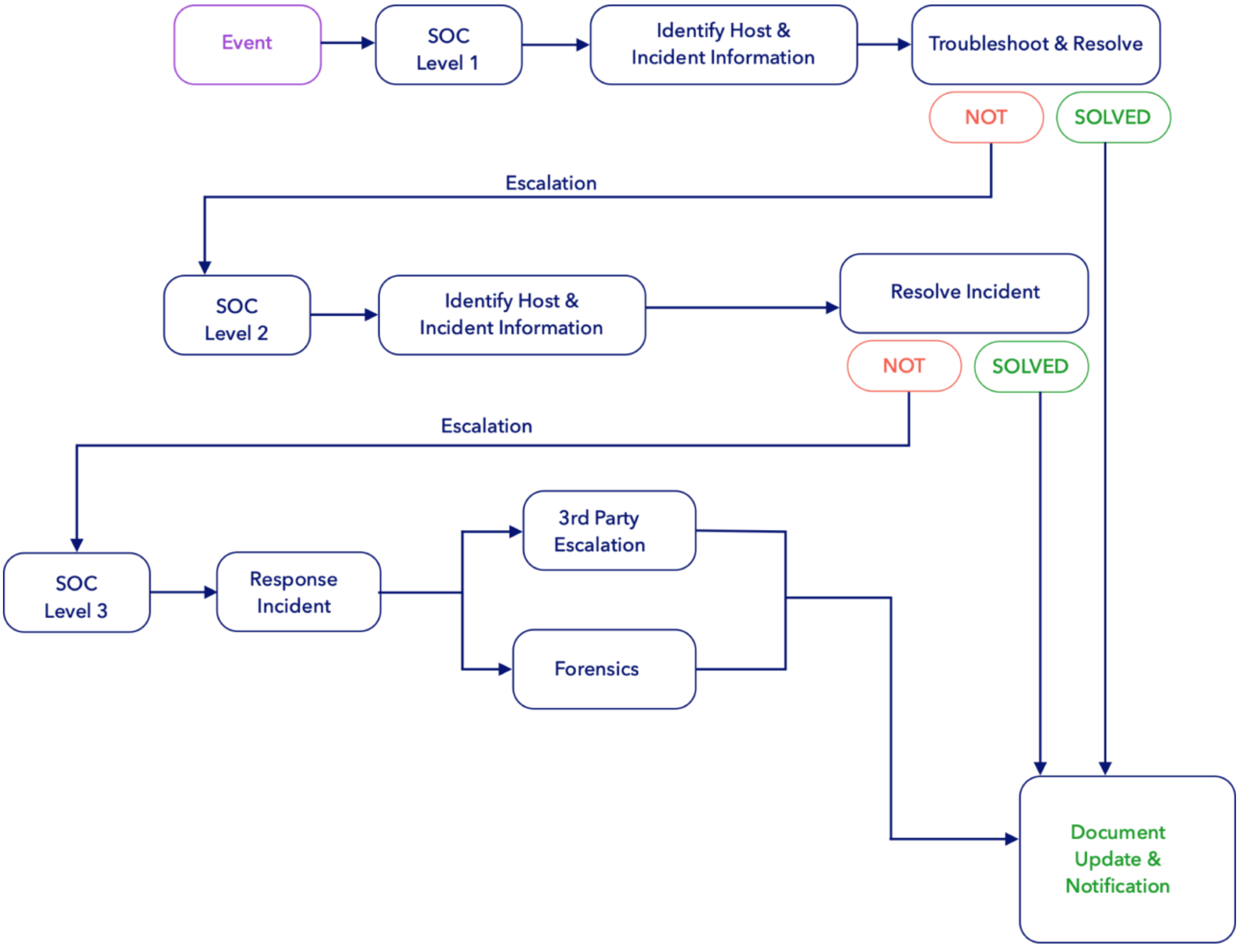


Figure 5: Escalation process, figure adjusted from (McAfee and Intel Security, 2016)

The Level 1 Analyst is the first layer in the process. His main responsibilities are identification, categorization, event identification and incident triage. The L1 Analyst documents data regarding new host infections, creates cases or files tickets to locate the infected devices or systems. If an issue cannot be resolved by the L1, the escalation process is performed, the issue being raised to the next tier, the incident being assigned to a Level 2 Analyst which will perform an in-depth investigation on this event. The most advanced experts are doing forensics.

2.1.6 Human Factors and Mental Model

The collaboration and communication within the team is crucial as the performance and contribution of each member sums up in the success of the team. Collaboration can come also from the community, a community which consists of "geographically dispersed experts who communicate through a host of structured mailing lists and informal contacts".(Goodall, Lutters and Komlodi, 2004) Experts and novices consult the community for emergency problems and novel attacks.

The mental model of the team consists of the shared knowledge that they possess. (Hámornik and Krasznay, 2018) This mental model consists of an "up-to-date representation of the internal and external reality" (Hámornik and Krasznay, 2018), the basic sysadmin, programming, and security skills, and the lessons learned from previous common experiences. The common education that they own contains the values and objectives of the team, problems that need to be solved, tools used, and the process that has to be followed. The mental model offers a shared language within the team members, acts as an interpretative frame, and enables them to react to challenges in an effective manner, especially during the high pressure times when there is no time to discuss and "to explain the background of actions or the context".(Hámornik and Krasznay, 2018)

Solid background in computer technologies focused on networks and reverse engineering are the key skills that are needed for the team members. All of the team members should also share a genuine interest in learning about security, a self-motivated attitude, and self-taught, hands-on approach.

2.1.7 Schedule

A fully-functional should provide permanent monitoring, 24/7 coverage which requires a team of minimum 10 employees in the team. In order to maintain high quality through the shifts and changing personnel, the mental model has to be developed and kept up-to-date. As the common understanding within the team is such an important aspect, the recruitment, selection, and retention of employees has to be performed laboriously.

A global skill-set shortage can be identified in the field as the SOC is pushed by the complex cyber-attacks to constantly apply new technologies and move from a reactive way of working to a proactive one.   As a consequence of the 24/7 schedule, the work-life balance can be impacted negatively, and it can induce stress and exhaustion in their life. The time pressure and high-risk task could classify this under the high-risk professions.

2.2 Dashboards

Dashboards have become a standard tool over the last decade, a term which evolved from the automobile dashboard where the driver was responsible for tracking the major functions based on summarised information to a business tool that helps in making strategic decisions for corporations, teams, or even one individual. In the modern context, a dashboard can be defined as a visual display of valuable information used to monitor conditions and facilitate understanding. They improve the “span of control” over the data and help people to visually identify trends, patterns and anomalies, guiding them towards effective decisions. The concept developed from single-view reporting screens to interactive interfaces with multiple views and various objectives additional to the conventional purposes of decision support and monitoring. (Alper Sarikaya, Michael Correll, Lyn Bartram, Melanie Tory, 2015)

The benefit of a dashboard is that it reduces information overload and improves the performance of the users by displaying visualizations from the gathered data, offering an overview image and trends and patterns in the data. Another advantage is that it has the potential of reducing excessive reporting and favours the allocation of working time on relevant tasks and shifting the focus to significant information that is used in the decision-making process. In order to serve their purpose and fulfil their true potential, dashboards have to communicate efficiently and effectively which requires leveraging the power of visualization to process and aggregate large amounts of information.(Few, 2006)

Dashboards can provide unique and powerful methods of presenting information. (Few, 2006) For that, the material is displayed visually, combining graphical and text elements. The emphasis is on the graphical elements as they can facilitate superior decision making by shifting the focus to the relevant portions of information in the data set. In order to build a dashboard that fulfils this requirement and that can be analysed quickly by the human brain, the following fundamentals should be respected:

- **The dashboard should have clear and well-defined goals**
  The intended use of a dashboard drives the choice in design, technology and scope. The first step is to define the goals of the dashboard, a decision that will influence the choice of data that has to be collected and the visualizations that will be used.

- **The correct visualization elements should be integrated into the dashboards**
  Graphical elements convey information, provide an approach to explore data and are essential in result presentations. It is important to choose the right type of visualization from the start, and the decision should be made taking into account the data that will be displayed and the goal that has to be achieved. One elementary rule to consider is: “Visualization is effective if the maximum amount of data is perceived in a minimum amount of time”(Yigitbasioglu and Velcu, 2010)

- **The content of the dashboard should fit one single screen**
  The dashboard should be contained in one screen outline, to be available within the viewer's eye, to be monitored at a glance. The goal is to render the most important information in a readily manner that can be absorbed effortlessly. The

dashboard should be kept minimal, so any additional information that is not relevant and creates a cluttered space should be eliminated.

- **The dashboard should integrate into the context of the application**
  The purpose of the dashboard is to convey information but it is always part of a larger whole, “a context that provides relevance.”(Chen, Hrdle and Unwin, 2008) Taking that into account, the dashboard should fit in terms of content, style, and layout with the rest of the application.

Dashboards are used to support a broad spectrum of information needs, so each dashboard should be tailored to the specific needs that it serves and to the defined purpose. The following categories have been defined to structure the decision of the dashboard design.

Table 4: Classification of Dashboard attributes

Category	Dimensions	Description
Purpose	Strategic	Provide a quick overview for the decision makers on actionability combining multiple high-level metrics to report the activity over a longer a longer period of time. The strategic dashboard concentrates on high-level measures of performance, including forecasts to light the path into the future.(Few, 2006) As the goal is to provide a long-term strategic direction the data is not required to be displayed in real-time; the strategic dashboard is rather a static snapshots taken at a given interval of time. It is also not intended for further analysis, which means that it is not necessary to be interactive.
	Analytical	Dashboards for analytical purposes demand to paying attention to the greater context, “such as rich comparisons, more extensive history, and subtler performance evaluators”(Few, 2006). For the benefit of the analysis, the dashboard is a static snapshot of data, but in comparison to the strategic dashboard, the analytical dashboard contains graphics with high visualization literacy, graphics with higher complexity that help the analysts to examine complex data and relationships. The dashboard allows interactions like drilling down into the underlying details in order to explore and examine the causes.
	Operational	Dashboards for operational purposes support monitoring of the operations and present the near past state in terms of “immediate quantifiable metrics that can be correlated to their responsible entity.” The nature of the immediate and dynamic actions that have to be performed shapes the design of the dashboard. The content should enable the user to monitor operations and it should maintain awareness on the constantly changing events and it

		should provide a method to respond at a moment's notice. The design should be minimal, without redundant elements and distractions from the fundamental activity. In the case of an incident or emergency requiring an immediate response, the system should have a notification mechanism to raise the awareness of the user when an operation falls outside the acceptable threshold of performance. Also, the meaning of the situation and the process to be followed should be presented in a clear and simple way to prevent mistakes.
Time horizon	Historical	A dashboard that provides an overview of the previous events in order to identify and track trends.
	Snapshot	The content of the dashboard presents performance at a given point in time.
	Real Time	In the real time dashboard, the content is automatically updated with the most current data available.
	Predictive	Analysing past performance predicts future performances.
Interactivity	Static display	Static display provides consistent information for a defined period, creating a unified perspective. The dashboard displays statistics and data on a certain period in order to gain an understanding of what has occurred. The outcomes of the examined data from the past can provide an insight into how the process has improved and which are the points that need extra efforts for improvements. This approach supports a single version of the truth, collaborated conclusions and facilitates future decision-making process.
	Interactive display	Interactivity at the display level allows the user to focus the analysis on the items that are relevant at a given point by faceting the data with filters and slicers, selecting certain items within the views and accessing data in a lower or higher level of a hierarchically structured database. The tasks that have higher uncertainty require a more disaggregated data. The in-depth details should be available "on request", by accessing data through roll-up or drill-down and filtering because having all the data available on display would lead to information overload and inaccuracy.
Point of view	Prescriptive	The dashboard presents the data in an explicit way and advises the user on the steps that have to be performed next.

	Exploratory	The exploratory approach offers to the user the possibility of interpreting and analysing the results.
Span of data	Enterprise-wide	The data is collected at the enterprise level and the dashboard offers an overview of the whole organization.
	Departmental	The data is collected at the department level and the dashboard offers an overview of only that department.
	Individual	The data is collected at an individual level, offering information only about the performance of one particular individual.
Data acquisition	Manual	The data can be introduced into the system manually by the stakeholders or employees.
	Automated	The data can be imported into the tool in an automated manner from other systems in different types of formats.
Control	One-size-fits all / Universal	One dashboard is defined, and it is used by all users, without the feature of customization or personalization. All users have access to the same features and controls.
	Role based personalization	In role-based personalization, certain users are grouped together according to predefined characteristics. The dashboard addressed to a certain role contains an identical set of elements for the users that are found in that category.
	Individualized personalization	Based on previous interactions with the application, a model is automatically created for each individual user and a dashboard is built according to that model.
	Customizable	The dashboard enables the user to have the capability of modifying the construction and composition of views. The user has the flexibility to make their own selections, to set their preferences on the way information is organised and displayed, to modify the placement and visual representation of the views and to select particular measures to be visualised.
Triggers	Pull scenario	In the pull scenario, the user queries the dashboards for a specific information.
	Push scenario/ Alert Notification	In the push scenario, the important information is pushed to the user, informing about problems, anomalies, or unexpected situations. The dashboard maintains a real-time connection with the database and raises alerts to the user indicating warnings and dangerous events that require the user's immediate action in order to remedy the issue.(Alper Sarikaya, Michael Correll, Lyn Bartram, Melanie Tory, 2015)

The goal of dashboards in security is to assist the analysts in their work to increase the safety and integrity of digital networks by providing an effective workspace. When it comes to cyber security, there are plenty of challenges that have to be overcome:

- The dashboard should enable "multiple, simultaneous investigations and foraging"(Fink *et al.*, 2009) and be able to organise the data.

- The system should be able to handle enormous amounts of data in the analysis. In the design process of the visualizations, key points such as the amount of data that has to be stored, the time period for which it will be stored and how to provide timely access to this information should be carefully considered. (Fink *et al.*, 2009)

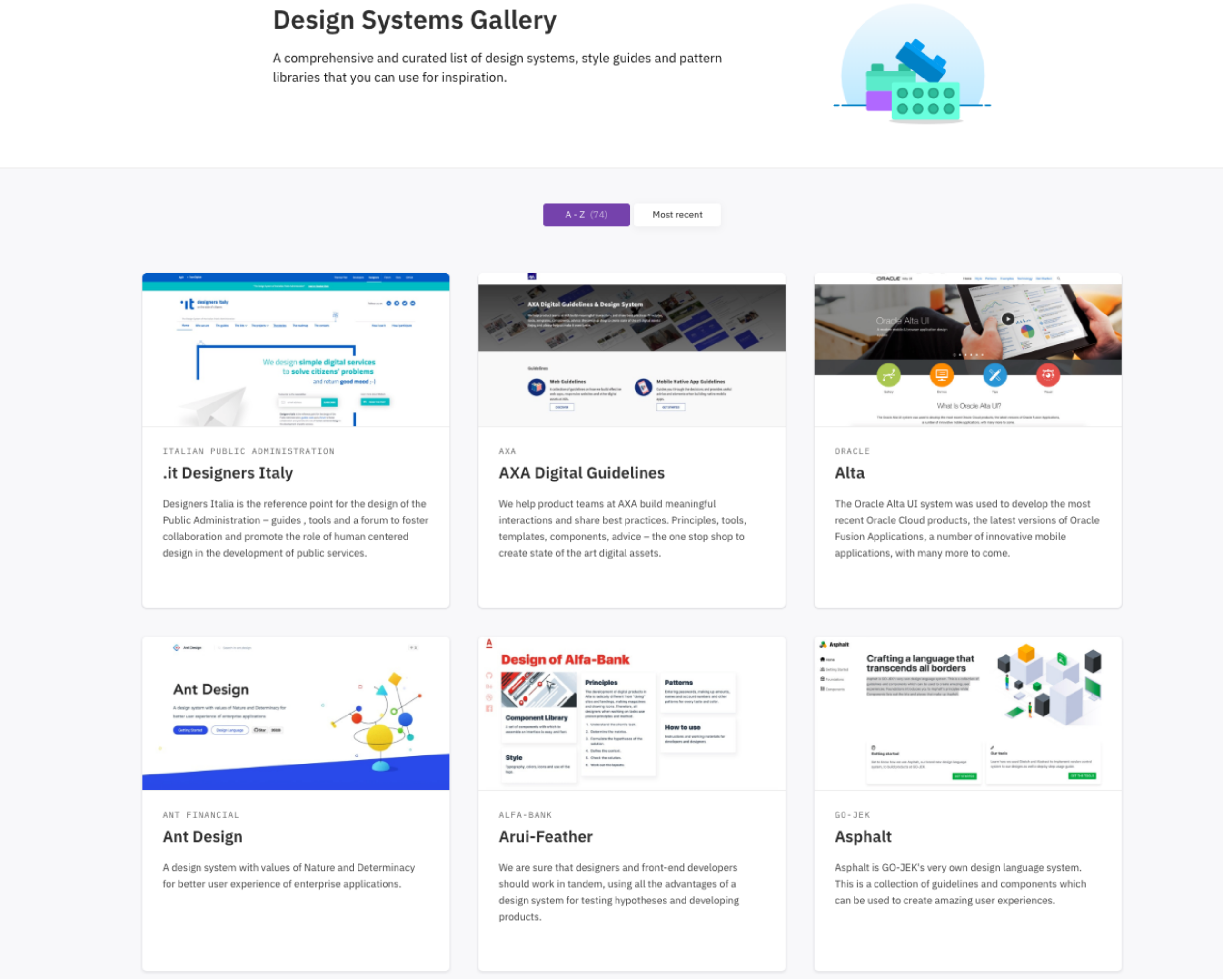
- The tool should support with other applications and utilities that are used in the industry.

- The tool should provide the functionalities of filtering, joining and "transforming the data without altering the original"(Fink *et al.*, 2009). Also, the "detail on demand" feature should be available as well as access to the source data, as it is critical in the investigation process.

The majority of cyber security professionals prefer the command line because of its "unparalleled flexibility and expressive power"(Fink *et al.*, 2009). Considering this preference, their pain points, their challenge to identify connections that locate the source of threats in the defended system the designers should create a more usable and compelling dashboard. The dashboard should not simplify the data by over aggregation or smoothing the "noisy" data, should keep the context of the investigation and should allow the users to "drill down" and get more details, especially for critical requirements.

2.3 Design Systems

In recent years, design systems gained popularity not only in the world of digital design but in the whole world of digital products, with the biggest players on the market, such as Google, Audi, Atlassian, Dropbox, Shopify, Airbnb and many others investing in the development of their personal design systems. In this space, we can identify not only private companies, like the ones mentioned, but we can also identify public entities, such as the U.S. government, Indiana University, the Australian government, Italian public administration and many others. This design systems can be open, available for everyone to use, or they can be closed, available only within the organization and applied to the products that are branded by the company. One repository of the open to use design systems available on the market is Design Systems Repo (https://designsystemsrepo.com) and it hosts in its gallery more than 70 references.



Design Systems Gallery

A comprehensive and curated list of design systems, style guides and pattern libraries that you can use for inspiration.

ITALIAN PUBLIC ADMINISTRATION
.it Designers Italy
Designers Italia is the reference point for the design of the Public Administration – guides , tools and a forum to foster collaboration and promote the role of human centered design in the development of public services.

AXA
AXA Digital Guidelines
We help product teams at AXA build meaningful interactions and share best practices. Principles, tools, templates, components, advice – the one stop shop to create state of the art digital assets.

ORACLE
Alta
The Oracle Alta UI system was used to develop the most recent Oracle Cloud products, the latest versions of Oracle Fusion Applications, a number of innovative mobile applications, with many more to come.

ANT FINANCIAL
Ant Design
A design system with values of Nature and Determinacy for better user experience of enterprise applications.

ALFA-BANK
Arui-Feather
We are sure that designers and front-end developers should work in tandem, using all the advantages of a design system for testing hypotheses and developing products.

GO-JEK
Asphalt
Asphalt is GO-JEK's very own design language system. This is a collection of guidelines and components which can be used to create amazing user experiences.

Figure 6: Design system gallery (Limcaco, 2019)

Before addressing the utility and the benefits of the design system, the first step is to define the concept. According to Alla Kholmatova, a design system consists of a set of "interconnected patterns and shared practices coherently organized to serve the purpose of a digital product"(Alla-Kholmatova, 2017). In this case patterns are considered to be repeating elements such as buttons, text fields, typography, and colours, interactions that are used to create an interface. Practices are rules, guidelines that describe the way in which the team should use the defined patterns to assemble the application. The design system can be considered as a "system that is the single source of truth which groups all elements that will allow teams to design, realize, and develop a product."(*UX Collective*, 2019)

The foundation of the design system consists of the **style guide** that gathers the styles, patterns, the best practices and principles related to a company or brand. A style guide can include elements such as typography schemes – clear instructions regarding the typeface font sizes, weights and styles for titles, subtitles, headings and all the other elements, responsive layouts, colour palettes, spacing and positioning. Especially for digital style guides, additional UI components such as iconography, and basic elements such as buttons or input texts can be found in the style guide.

One of the most iconic style guides is the NASA Graphics Standards Manual released in 1976 which defined the way in which the design standards of Nasa would be implemented on everything, from documents, magazines, and billboards to uniforms, airplanes, and spaceships.(NASA, 1976)The decision to adopt the style guide was explained by the company in the following way:

"We have adopted a new system of graphics-the visual communications system by which we are known to those who read our publications, see our vehicle markings and signboards and the logotype that unmistakably brands them as NASA's."(NASA, 1976)

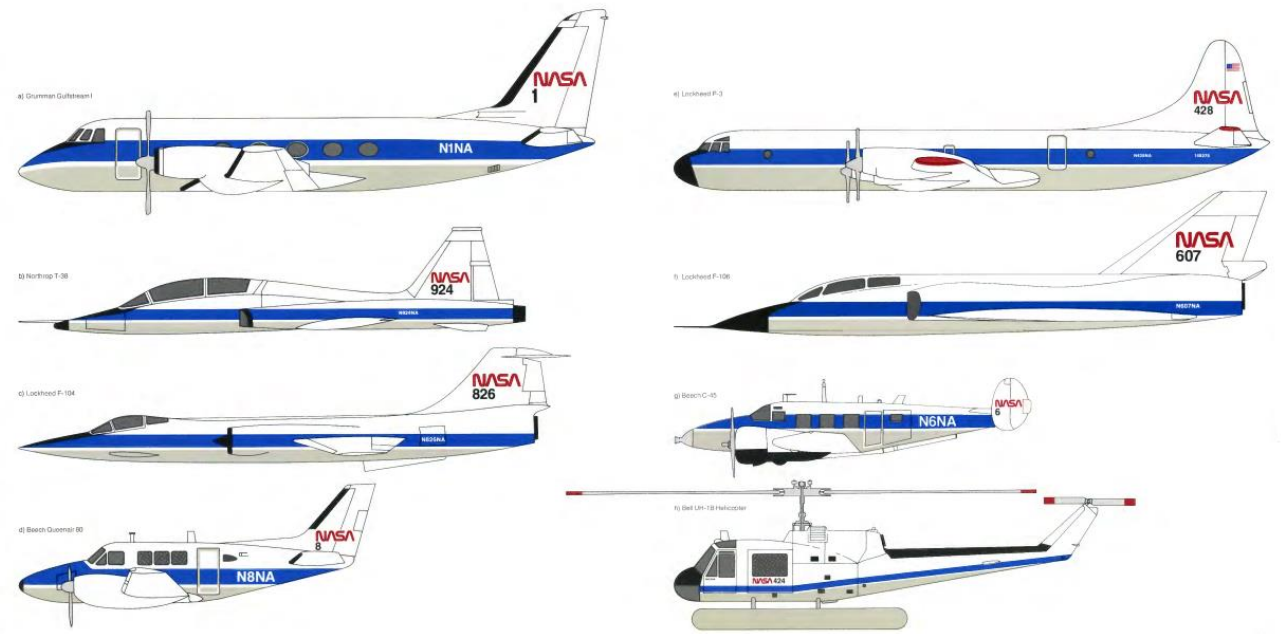


Figure 7: Example from NASA Graphics Standards Manual (NASA, 1976)

The concepts that integrates style guide and extends its capabilities is the **pattern library**, which can be defined as a set of reusable and complementary components.

The concept of design patterns was introduced by the architect Christopher Alexander in the books The Timeless Way of Building and A Pattern Language. It was defined as a recurring pattern or a reusable solution that solves a design problem.

"A pattern is a recurring, reusable solution that can be applied to solve a design problem solution to that problem" - *Christopher Alexander* (Christopher Alexander, Sara Ishikawa, 1977)

Similar to architecture, when creating interfaces, the design patterns are used to solve common problems. The design patterns will usually include code snippets or live documentation and they will contain components such as navigation menus, charts and data visualization, images, sliders, switches, micro interactions, and many more others. The majority of the design patterns are well-established and recognizable to the user and they utilize the mental model of the user to create an intuitive design. The novelty occurs in the way that the patterns are applied and how they interconnect to achieve a design purpose. A design language is formed by the set of interconnected patterns and when the design language is articulated, it becomes actionable and reproducible.

In the digital world, one of the most popular digital pattern libraries is Bootstrap which is an open-source framework for creating websites and web applications. It is a collection of reusable code written in HTML, CSS, and JavaScript used by front-end developers and designers to build responsive applications. Some of the components that are available in the library are alerts, breadcrumbs, buttons, cards, carousels, dropdowns, navbars, paginations, spinners, and many more.

A **design system** accommodates the style guide and the pattern library and the relationship between them is illustrated in the image below.

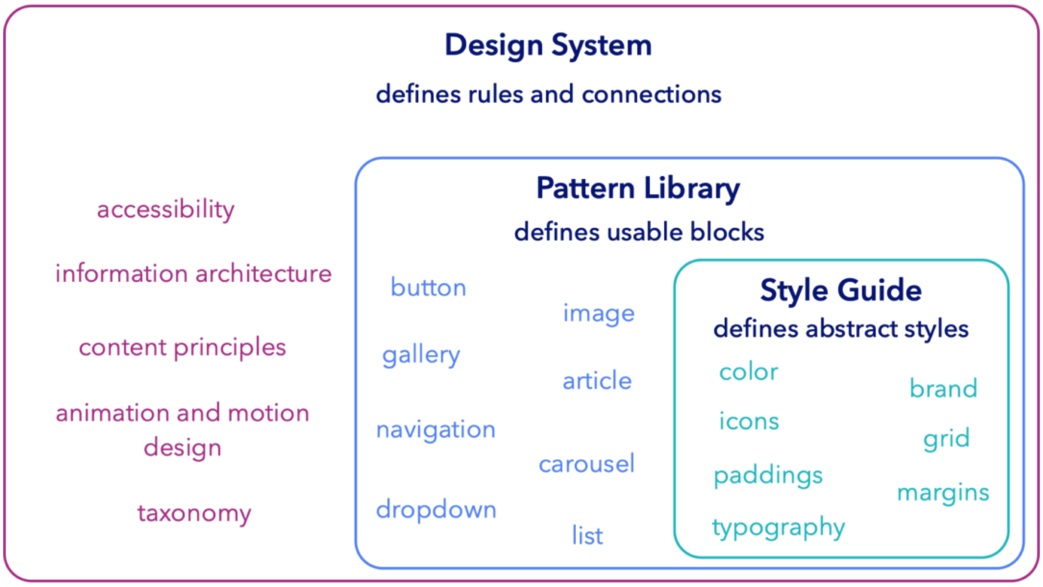


Figure 8: Design system representation

The design system acts like a blueprint for the development of the product and it encompasses the value, purpose, design principles but also the functional and perceptual pattern that are contained by the style guide and pattern library. The functional patterns, represented in the patterns library, consist of concrete modules of the interface such as buttons, list, and menus. The perceptual patterns are descriptive styles that express the visual personality of the product incorporating aspects such as colour, typography, and animations. Looking from the perspective of front-end development, the modules are coded in HTML while the perceptual patterns are CSS properties. (Alla-Kholmatova, 2017)

The design system also defines the principles by which the components work together, by presenting the purpose and values, design principles, behavioural and functional patterns and aesthetics and perceptual patterns. By establishing these grounding values and principles a measuring tool to measure if the purpose is reflected in the final design of the product is established.

- Purpose and shared values are the essential step that has to be established among the team. The shared goals enable the team to build a common vision regarding the final product.

- Design principles create a set of general principles that support a coherent experience and can be the focus on the brand, team culture or the design process. For example, in the case of Mozilla, the design principles, the guiding principles that support their design decisions are meaningful, flexible, accessible to all, global and useful. In the case of Atlassian, the design principles that are reflected on their digital products are: "build trust in every interaction, connect people to collaborate better, match purpose and feel familiar and drive momentum from end to end."(Atlassian, 2019) The design principles can be used as review heuristics for new proposed patterns in the design system.

- Behavioural and functional patterns are the "tangible building blocks of the interface" and their goal is to encourage a desired user behaviour. Determining the purpose of the patterns in the early stages of the design process prevent duplication in the later stages, when the product develops and grows.

- Aesthetics and perceptual patterns help modular systems to achieve visual coherence and seamlessness. Perceptual patterns for digital products are all the elements that are combined and used in an interface such as tone of voice, typography, colour palette, layouts, shapes and textures, spacing, etc.

The design system establishes a common shared language among team members that facilitates a more efficient collaboration among the team. As the objective is to construct "a single source of truth" to be considered in the product design, it also represents a shared language among team members that is used in the development of the product. Other benefits that the usage of a well-constructed and kept up-to-date design system are the following:

- Product consistency – the lack of consistency across a product or a range of product of a company can lead to user confusion -different patterns responsible for the same actions confuse the user -, slow design process, slow development and difficult onboarding. Also, the design should feel like a consistent experience in regard to behaviour and interaction across all platforms. A well-defined design system not only helps maintain consistency across different teams and products but also reduces the cognitive load.

- Clear guidelines – the design system is the blueprint of the product development and that is why all the design principles, patterns, and visual assets are meticulously documented. Code snippets and references accompany each piece of design. As a result, the design scales alongside development.

- Product scalability and increased product value – the consistent look, feel and behaviour of the product are utilizing the reusable components built upon each other. The increase in consistency is followed by an increase in user efficiency.

- Increased productivity – a regularly updated design and code repository accompanied by exhaustive documentation enhances the collaboration and reduces friction in the process.

- Saves time and resources – the design system frees up time for the developers and designers by removing redundant and repetitive work, time that can be used for projects that deliver more business value. By having the component-based toolkit available in one place the team can have a more agile process, speeding up releases without compromising quality.

- Increase collaboration, communication and knowledge sharing. The designers and developers are more autonomous due to the already approved assets and conventions. The design system can act as a bridge between teams by making it easier to reuse existing work.

3. Methodology

This chapter covers the methodology and the research approach that were used in this thesis. Due to the nature of the research and the industry that the topic is addressed to, the mixed methods research approach along with qualitative and quantitative data collection and analysis methodology are used in the thesis.

In the scientific field, the approaches that are used are divided into two categories: quantitative and qualitative research. Qualitative research focuses on producing insights and meaning, while quantitative research is focused on measuring the effect based on counts and measurements.

Due to the multifaceted nature of the results of the design process, in the case of this project – a user interface, the decision made was to use predominantly the qualitative methods, as they were the most suitable in the given context. In the final steps of the process, one quantitative method was used also, in order to measure two attributes of usability, that is why the decision to use a mixed-method research approach was made.

The data that has been collected can be divided into two categories, which is done based purely on the phase of the project in which they were collected. The first category covers qualitative data, gathered from the interviews performed in the research phase, while the second category consists of both quantitative and qualitative data gathered from the user testing phase.

For the first category, the process of gathering the data consisted of semi-structured interviews. The semi-structured interviews method consists of a combination of open-ended predefined questions and is accompanied with additional unstructured questions that might arise from the discussion. The “interview guide” that was followed can be found in the 7.1 Appendix 1: Interview with SOC experts. The goal of the interview was to validate the information that was collected in the literature review phase and to gather additional information about the Security Operation Centre work while allowing some additional explorations on the topic. The reason behind the decision to use this type of interview was that it provides the opportunity to uncover previously unknown issues and it provides flexibility for the discussion while still ensuring that the same main points are covered. (Chauncey Wilson, 2014)

More information regarding the process of gathering the data belonging to the first category has been covered in the chapter “ 4.1 Modelling Users: Personas”, while the methods that were used for gathering the data corresponding to the second category is described in detail in the chapter “ 4.5 Usability Test Planning”.

The data analysis methods are divided into the same two categories, due to the nature of the data and also depending on what the aim of the research is. In the first category, the method that is used is Persona, which was preceded by qualitative coding performed on the data. The qualitative coding is used to filter and categorise the raw data and to extract ideas, behavioural patterns, and quotes, things that will help in the construction of the final personas.

The Persona is a powerful tool for communicating about different types of users and their goals and needs, and for prioritizing which are the most important user types to target in the design from the form and behaviour point of view. The persona helps the team overcome several problems such as:

- Determine – the goals and tasks of the persona provide the foundation of "what the product should do".

- Communicate – persona promotes a "common language for discussing design decisions"(Cooper, Reinmann and Cronin, 2007) that is used by designers, developers and stakeholders.

- Build consensus and commitment – the common language is used to build a common understanding and empathy.

- Measure – the persona is used to measure the effectiveness of the design as it is considered a powerful reality-check tool for designers.

- Contribute – the persona can be used also by other product-related activities such as marketing and sales plans.

One of the most critical aspects that is covered by the persona is building empathy, which is essential for the design decisions. As the persona is a user model that is a specific individual human being, both cognitive and emotional dimensions should be taken into account. The implications of design in human terms can be materialised into goals, which outlines the context and structure of the tasks presenting how the culture, environment and workflow shape the behaviour. The framework that was chosen in order to offer a template or a standard of the process is the technique developed by Alan Cooper who created the persona in 1999.(Cooper, Reinmann and Cronin, 2007) The process is further explained and applied in the next chapter, titled "Modelling users: Personas".

In the second category, the data was collected and analysed in the usability test. The test was performed in order to ensure that the product is suitable for the purpose for which it was designed and for the target audience. The main goal of the usability test is to validate the relevance of the content and ease of use of the new designed dashboard.

According to the International Organization for Standardization, a definition for the usability is the following:

> *"the effectiveness, efficiency and satisfaction with which specified users can achieve specific goals in particular environments" ISO DIS 9241-11* (Faulkner, 2000)

In the definition it is clearly stated that in order to consider a product usable and to fit into the criteria for usability, it should be:

- Effective – defined by the ISO as "*the accuracy and completeness with which users achieve specific goals*"(Faulkner, 2000) , the degree to which a task or a subtask can be carried out to completion in a certain environment, with a particular tool by a specific individual. In order to evaluate the effectiveness of the system, the success to failure ratio of the results, the problems experienced, and the use of commands should be taken into account.

- Efficient – defined by the ISO as "*the accuracy and completeness of goals in relation to resources expected*"(Faulkner, 2000). In this case, on a simple level, the resources can be seen as the time that it takes for the user to complete the task, but they could also contain more complex concepts such as effort, such as the number of actions required in order to reach the desired result, the time spent with help or documentation and the time spent dealing with an error.

- Satisfying – defined by the ISO as "*the comfort and acceptability of the system*"(Faulkner, 2000). This attribute of usability measures the satisfaction that the user feels while using the system. The measurements of this metric can be done by observing the user and the user attitudes towards the system. Another method that can be used to measure if the user has a positive feeling towards the system is by using a questionnaire with open ended questions or, by using a standardized usability questionnaire with a Likert scale. They are designed to determine the perceived satisfaction and usability as a whole in some cases by computing a result from the score-based answers of the respondents. The standardised usability questionnaires that are commonly used by the professionals can be classified by the moment in which they are performed during the test and they are divided into two categories:
    - the questionnaire is performed after each task of the test and some of the most notable in the industry are: ASQ, SEQ, and SMEQ.
    - the questionnaire is performed at the end of the test and some of the most notable in the industry are: QUIS, SUMI, SUS, and UMUX.

In order to evaluate the proposed design of a system, an empirical method was used, consisting of an analysis of the user performance in relation to the suggested dashboard. In the empirical method, data is gathered and analysed, data collected from the interaction with the users. Some of the procedures that are used are observations, questionnaires, experiments, interviews and standard surveys. In the usability test performed on the dashboard designs the following strategy and methodology were decided on:

- Effectiveness – in order to measure the effectiveness, the completeness of the tasks and the success to failure ratio will be measures that will be recorded.

- Efficiency – in the case of this test, as it is an early exploratory test and a think aloud method will be used, the time on task measurement is not advisable. Some of the things that would influence the results are that the fact that the novelty of the interface and the fact that users have to describe their thoughts regarding the task will slow them down and will lead to decreased performance. Other benchmarks that were considered are the error rates, the ideal case consisting in the performance of a task with no errors of any kind. Due to the complexity of the system and that the primary goal of this test is validating the relevance of the information on the dashboard, this metric was not considered in the analysis of the results. As a conclusion, the efficiency will not be measured by the usability test.

- Satisfaction – the satisfaction of the user in regard to the product will be measured using a standardized survey. The advantages of using a standardized test consist of objectivity – it allows independent verification of the measurements, replicability, scientific generalization, and quantification – the standardized measurements enable the usage of mathematical and statistical methods for a better understanding of the results.(Sauro and Lewis, 2016)

The standardized survey that was chosen is the SUS-Software Usability Scale a popular questionnaire for end-of-test that offers a global view of the subjective evaluation of usability. The test consists of ten questions about the system that can be evaluated by the participant on a Likert scale on a range from 1 (Strongly disagree) to 5 (Strongly agree) after the tasks were performed. The final score of the SUS, representing a synthesized measure of the overall usability of the system, ranges from 0 to 100. The benchmark that has been reached based on previous research is 68, the number 68 reflecting a standard average for the SUS.

The structure of the usability test is based on the following main points:

- Determine the target group – the target group of this project has been defined from the beginning and consists of Security Experts

- Recruiting users – the system is developed in-house, and that is the reason behind the decision to test with users within the organisation. Another constraint is that the field of security implies extra care regarding the confidentiality of the work, so obtaining permission to test with users outside of the organisation is problematic.

- Establishing the goals and the tasks – the main goals are validating the design and content of the dashboard while testing also the usability of the new design. A list of tasks is created, tasks which are considered for the evaluation of usability.

- Performing the evaluation – before conducting the evaluation, the user has to be introduced to the system. The evaluator has to make sure that all eventualities are covered, the prototype is functional, the user gave his consent for recording the session, and that a suitable method for recording is set into place. The evaluator has to ensure that the user is aware of the purpose of the investigation and with the tasks that have to be completed. Another mandatory action that has to be performed by the evaluator is ensuring the user that the system is tested and anything that might happen will bring useful insights regarding the way in which the system has to be improved. During the investigation, notes should be taken, both regarding the actions performed on the dashboard and the feelings that they experience (frustration, surprise, anticipation). In the end of the testing session, the user should be encouraged to ask for clarification if there is any need and he or she should be thanked for the effort.

- Analysing the results – the findings of the usability testing sessions should be listed so that they can be examined, and possible causes and solutions should be crafted.

An illustration of the process that will be followed for the development of this thesis is presented below in Figure 9.

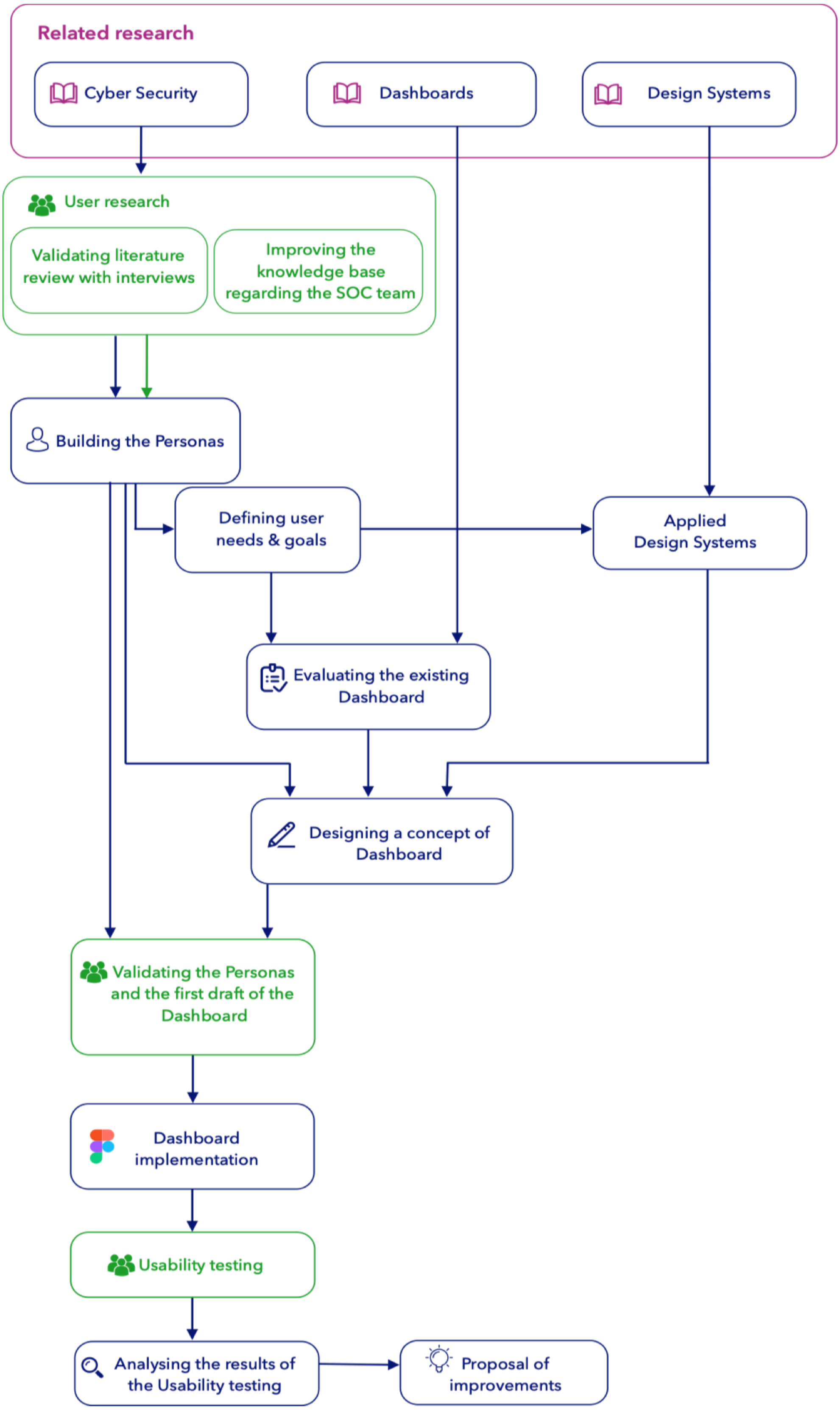

Related research
Cyber Security
Dashboards
Design Systems
User research
Validating literature review with interviews
Improving the knowledge base regarding the SOC team
Building the Personas
Defining user needs & goals
Applied Design Systems
Evaluating the existing Dashboard
Designing a concept of Dashboard
Validating the Personas and the first draft of the Dashboard
Dashboard implementation
Usability testing
Analysing the results of the Usability testing
Proposal of improvements

Figure 9: Process scheme

4. Results and Analysis

4.1 Modelling Users: Personas

In the direction of building the dashboard, the next step is to use the user-centred design method “Persona” which constructs fictional characters that represent different user types that potentially will use the product. The most important attributes of the users that are deeply related to the product are aggregated and represented by the persona. By using this technique, we can develop a broad understanding of the goals of our users in a specific context. Without this model construction, we would face the challenge of reviewing “unstructured, raw data, without the benefit of any organising principle.”(Cooper, Reinmann and Cronin, 2007) As the design is targeting the users, it is important that it is based on a deep understanding and visualization of the salient aspects of the relationship with others, the social and physical environment in which they are placed and the expectation that they have from the product.

Considering that the personas offer a representation of the diverse motivations, behaviours, skills, mindsets, workflows, environment, and the current failures of the products that they are using, the appropriate step forward in the development of the dashboard is building the personas. As the persona has to be built following a standard process, the framework that was chosen was one developed by Alan Cooper which created the persona in 1999(Cooper, Reinmann and Cronin, 2007).This process is preceded by a research phase during which the data is gathered. The data can be collected through direct means such as engaging real users through interviews, surveys or ethnographic research and indirect means such as prior experience and a literature review. In the current case, the data consists of interviews with 6 Security experts with different roles and from different SOC team from different locations. The semi-structured interviews were performed using a questionnaire (see 7.1 Appendix 1: Interview with SOC experts) that was prepared in advance and helped the researcher to maintain a structure but also giving the researcher the flexibility to ask for clarifications or different questions based on the answers coming from the participants. Before conducting the interviews, several decisions had to be clarified.

- Decide whom to interview. According to Spradley (1979), the respondent should be “a person with a history of the situation, who is currently in the situation, and who will allow adequate time to interview them”(Griffee, 2005). In the interviews performed for this thesis, the interviewees were selected from different SOC teams as they possess the knowledge and opinion on how this team operates, the tools that they use, and they can express their needs and challenges. As it is a subject that is very technical and is a discussion among experts, in order to obtain relevant answers that can be translated into persona descriptions the respondents should have studies and experience on the topic that is reviewed.

- Decide on a number of participants. In the given case, the access to the professionals is limited and as a consequence, the number of respondents was limited. In the beginning, 9 experts were contacted. Out of the 9 experts, at first all confirmed, but changes occurred and 2 of them cancelled and withdrew from the study. One of the interviews that was performed was irrelevant, the answers that were gathered did not followed the structure and answers that were received were unrelated to the study. The other 6 interviews that were performed were significant and added value to the research that was performed previously.

- Select a place for the interview. In the context of these 7 sessions, the respondents were distributed across different countries such as Sweden, India, Romania, Netherlands, New Zealand, and Finland. The interviews that were performed in Finland, the interviews were performed in person, in a meeting room, but for the interviews that were performed with experts that were located outside of Finland, the interview was performed via Skype calls.

- Decide on the question that will be part of the interview. The questions were divided into 6 sections, in which the following topics were debated:
    - General information about the person that is participating in the interview, such as their background – education, working experience, current working place, walk through a typical working day, their responsibilities, the process that is followed, etc. The passions regarding the job that they practice, and their personal hobbies were covered in another section.
    - Description of the environment in which they are performing their activities. In this category the schedule of the team, the facilities and the whole set-up of the team were covered.
    - Team structure and characteristics.
    - Tools and the dashboards of the tools that are being used in the team.

- Consider how the data will be collected. Because of the complexity of the answers, the best method to collect the data was to record the conversation and the screen (in case they were sharing their screen during the call). Before the interview, permission to record was asked from the participants.

The data obtained through the direct means of engaging the real-world users was enriched by the analysis of job postings, organisational charts, and SOC guidelines. The need for additional information to complement the interviews came from the limited number of interviews that comes from the problems of user’s access in this field, from the limitation of resources dedicated and for the confidentiality of the information.

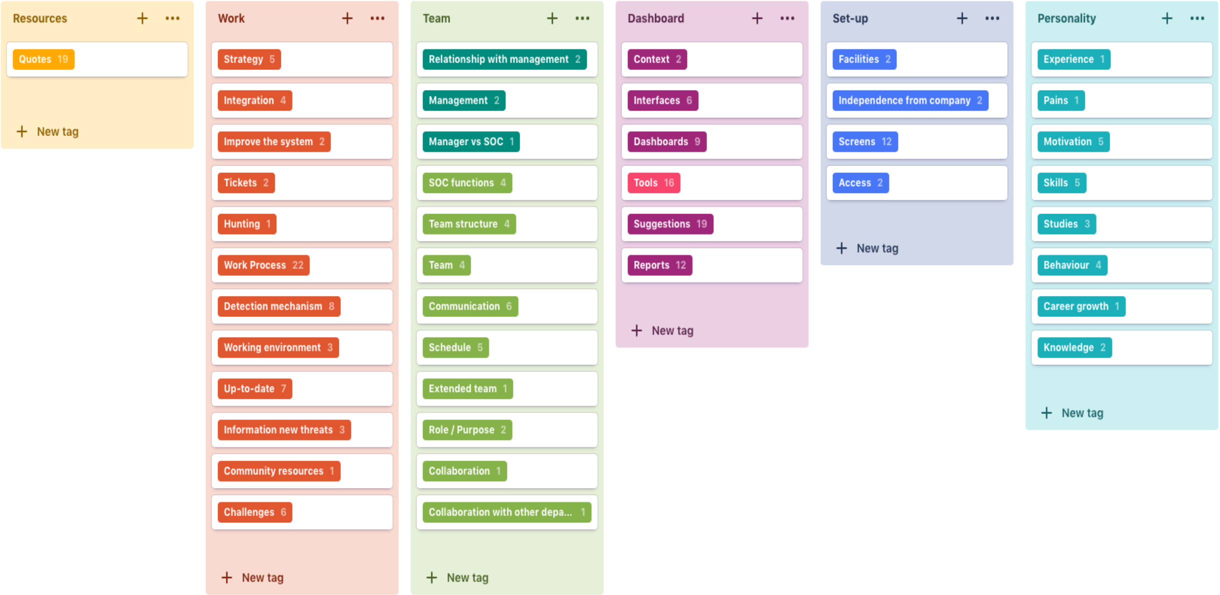
The process that has been followed to build the personas has seven steps, each one of which will be applied to the given data and context.

1. Identify Behavioural Variables

The first step consists of a cursory organization of the data and of refining the information. To process the data, the qualitative coding – a fundamental method in qualitative research – was used. “Coding is the process of analysing qualitative text data by taking them apart to see what they yield before putting the data back together in a meaningful way”(Lewis, 2015). Coding is a method of indexing or mapping data by tagging sections of text with salient short word structures which offers an overview of the various data and enables the researcher to gather answers and connections to the research questions. This technique retrieves the relevant data for further analysis.

The qualitative coding technique was applied to the transcript of the interviews. In the first level of coding the tags used were descriptive, with low inference and that summarise partitions of text. In the second level of coding, the tags were analysed and grouped together by the main idea that they are covering. As it is presented in the figure below, five main categories were created, focusing on different aspects. One independent category is the one that contains the resources used in the thesis, the notable quotes that were identified in the interviews. The next four main categories are correlated with each other, covering aspects such as the Work of SOC team, the Team and the Personality of the team members, the Set-up in which the team is working and the Dashboard of the tools that they are using.

For the coding of the interviews, a computer assisted software "Dovetail" was used. It offers a better management of the files and tags, fast access to the paragraphs belonging to a tag and statistics regarding the tags. To keep everything organised, for tags corresponding to the same group the same colour was assigned. For the groups that had tags which had two categories within the same topic, such as team or dashboard, two similar colours were used within the group.



Resources

Quotes 19

Work

Strategy 5
Integration 4
Improve the system 2
Tickets 2
Hunting 1
Work Process 22
Detection mechanism 8
Working environment 3
Up-to-date 7
Information new threats 3
Community resources 1
Challenges 6

Team

Relationship with management 2
Management 2
Manager vs SOC 1
SOC functions 4
Team structure 4
Team 4
Communication 6
Schedule 5
Extended team 1
Role / Purpose 2
Collaboration 1
Collaboration with other depa... 1

Dashboard

Context 2
Interfaces 6
Dashboards 9
Tools 16
Suggestions 19
Reports 12

Set-up

Facilities 2
Independence from company 2
Screens 12
Access 2

Personality

Experience 1
Pains 1
Motivation 5
Skills 5
Studies 3
Behaviour 4
Career growth 1
Knowledge 2

Figure 10: Qualitative coding categories

Analysing the categories and the labels that belong to each category, we can see that the Work and Team categories have an increased number of sub-categories.

The subcategory Work is the one with the highest number of appearances, the participants explaining the whole process, from the beginning, the identification of an event to the end, when it is solved and the knowledge that was gained is implemented into the system, improving the detection mechanism, not only the parts that were their responsibilities. Some other subcategories that have been identified in the Work category are Detection Mechanism, a subcategory in which the participants were talking about the detection system that they have set up, which is related to the subcategory "Improve", the system that gathers information about the way in which the detection mechanism can be improved based on the "lessons learned". Other three subcategories that are tight together, are "Up-to-date, Information new threats and Community resources", which refers to the way in which the participants learn about new threats or how to solve certain incidents that might occur.

In the "Team" category we can see that the subcategories have been divided into two sections. The division can be recognised also in the colours that were used for the labelling, the first three categories covering the management and the relationship with the management topic. The other subcategories cover the Team structure, SOC Functions, Communication and Collaboration among the team.

The Dashboard category covers the Tools that are in the process, and other attributes and functionalities of those tools, such as Interface, Context, and even the Dashboards of those tools. As the interviews had covered the topic of Dashboards, the participants made some suggestions about what they would be interested to see in a dashboard, suggestions that can be found in the subcategory Suggestions.

The Set-up category covers the environment in which the team is working such as the number of screens, the facilities and the access.

The Personality category covers aspects such as the study of the team members, the skills that they possess, their motivations and their behaviours.

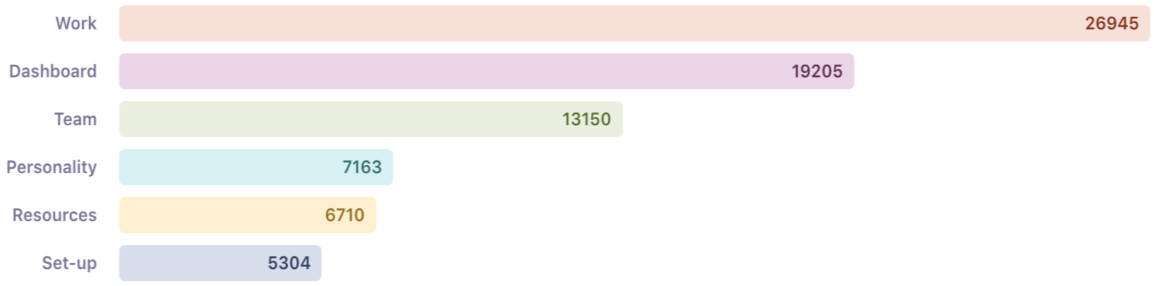


Figure 11: Tagged text volume

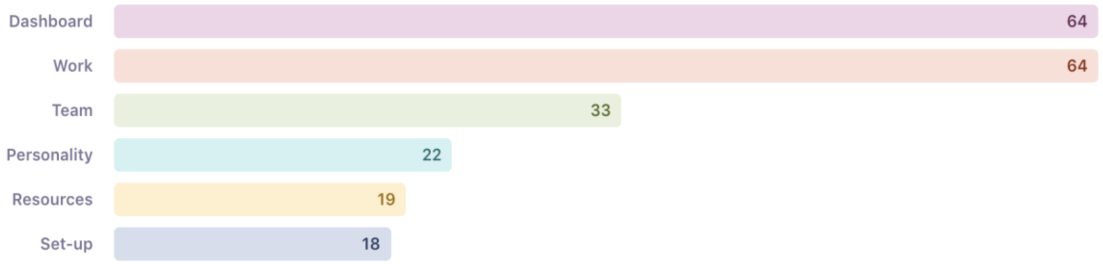


Figure 12 : Highlights by tag

We can see from the bar charts above that both in the case of the volume of the text and in the number of tags, the Dashboard, Work, and Team were the three most discussed topics in the interviews. That is also visible in the number of subcategories that were grouped in these categories.

From the volume of text that was tagged in the category "Work", we can observe that the participants enjoyed the discussion and the questions regarding their job, and they were passionate about the profession in which they were practicing. The category “Dashboard” has the same number of tags as the category “Work”, which is due to the fact that the focus of the interview was on the needs and current situation of the dashboards that are used by the team.

2. Map interview subjects to behavioural variables

From the results of the qualitative coding we identified some behavioural, skills, and environment variables. In this step we will map the participants answers to this attribute.

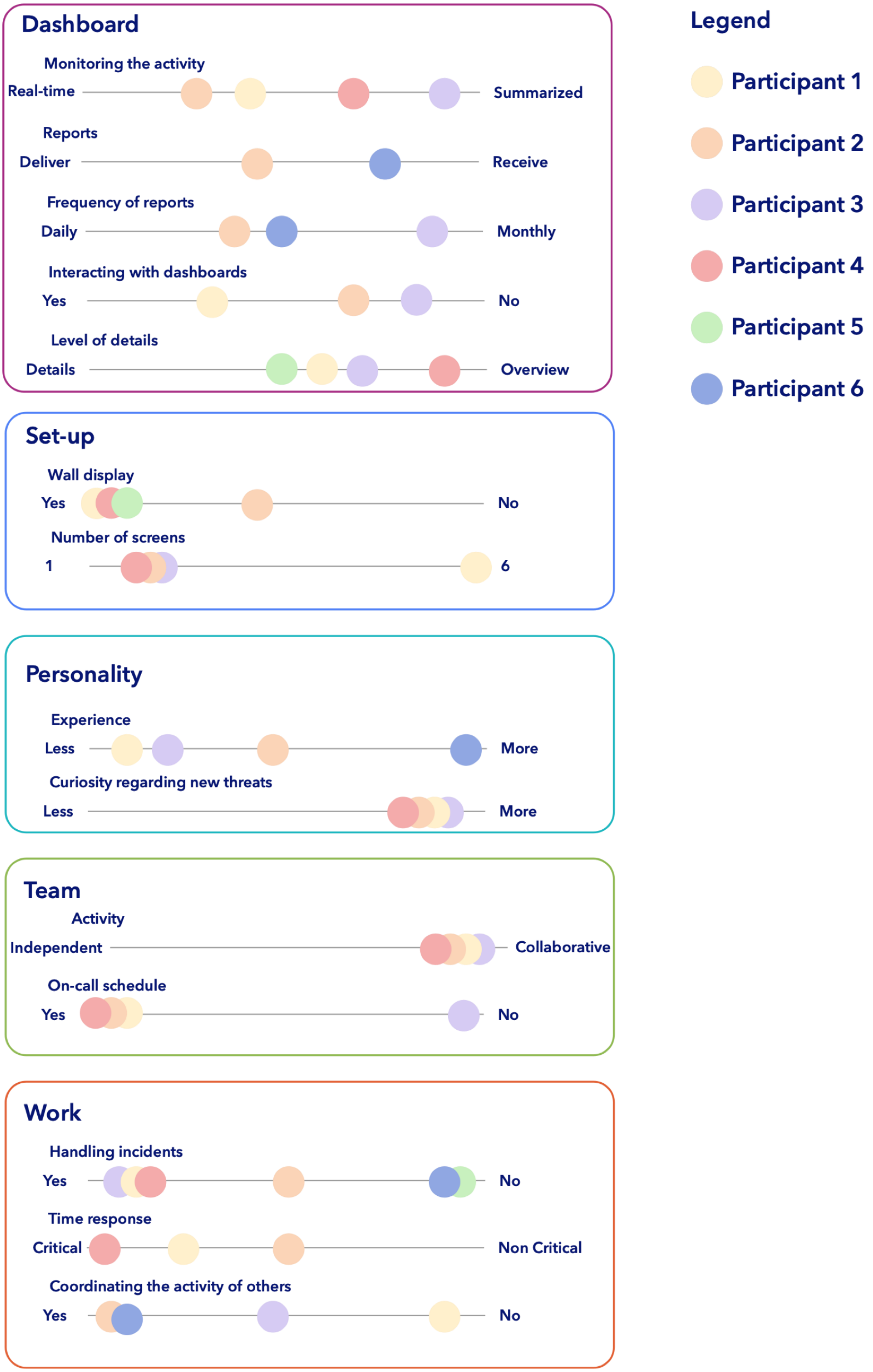


Figure 13:Mapping interview subjects to behavioural variables

The attributes were divided based on the categories defined in the coding process. This step was a difficult step to implement as the participants answered by explaining the whole process, describing not only their responsibilities but also the context in which they are operating. This led to extra details about the other responsibilities that their colleagues are performing in the team. Also, as the interview was semi-structured, the answers differed, and some topics were not covered by some participants.

The five categories that were established in the coding process can be identified in the figure above, and the behaviour variables are grouped into the same categories. The behaviour variables were chosen by the classification that has been previously performed on the dashboard and the attributes that have been defined, attributes that were also mentioned in the interviews by at least two participants.

The dashboard section covers five points regarding the way in which people interact with the dashboard of the products that they are using, the level of detail in which the information is presented and the reports that they have to create. In monitoring the activity variable, we cannot identify any trends or clusters, as the answers are scattered. From the answer of one of the participants we can understand that for him, the concept of dashboard implies real-time data:

"*You could call it dashboard but there is not like 'real time dashboard'. For those pieces of information is more like people extract the data and they make visualisations out of that. For example, from the SOC team, they report on all the use cases that are created, that they are working on, that exist. They report on a weekly basis the statistics of those. And that goes on a weekly report. So that is a very well-structured way of reporting." (Participant 2)*

The type of reports and their frequency is covered also in the dashboard section. For the first point we have only two answers, from two participants that said that they receive reports, but they also have to create reports, so this particular behavioural variable is inconclusive. Regarding the frequency of the reports, there are reports that are performed when an incident happens, weekly, as some of the participants reported: "*When there is no incident, the major piece of the report is the on-call information that is aggregated, weekly report by whoever is on-call, but of course you can go on the logs or on the ticketing system."(Person 2),* monthly or quarterly. In regards to the interactivity, one participant stated that:" The *dashboards that are located on the TVs and they are not interactive. The content on the screen is updated according to the time that has been set: 15 s to 15 min." (Participant 4)*

The Set-up category covers two aspects of the devices that the team are using, which are the wall displays that display real-time information that is monitored by the entire team and the number of personal displays that a team member possesses. The set-up of the team is designed based on the needs of the unit and on the resources that were allocated to the department. In the teams that have L1 and L2 analysts that perform the monitoring and event handling, they usually have the screens on the wall for better awareness and for improved communication among the team as one of the participants revealed in the interview: "*In a SOC or NOC there are screens out there all the time, maybe on 3 different screens: the Threats, the Status, the Compliance. Then click and show me what is under it, guide to the next level to let people to troubleshoot." (Participant 5)* Regarding the number of external personal screens, the majority of the team members, the common number is two, as it presented by the cluster of answers. There is one outlier which revealed that each team member owns 6 monitors, but he also stated that it is quite unique: "*If you are a security analyst that has 6 monitors, that is quite a luxury*". *(Participant 1)*

The personality category covers the working experience and the curiosity that they have regarding new threats. From the answers provided, we can see that the participants of the interviews cover all the range, from juniors that have less experience in the field to managers with 18 years of experience. We can identify a connection between the working experience and the curiosity regarding the new threats; the analysts are more curious and they have a higher determination to keep up-to-date, while managers have other priorities. We can also indicate that the same participants who stated that they have a high curiosity and determination to keep up to date with the new threats are the same people that said that they are handling incidents in their daily work (P1, P2, P3, P4).

The team category covers the activity and schedule. The schedule differs based on the size of the team and their demographics. From the answers provided during the interviews we identified some trends that are conventional in the field:

- the night shift has less personnel than the day shift as several participants stated:

  "*Yes, they were offering 24/7 coverage. During night times there were less people, and during the office hours there were more people. During the day there would be 8-9 and during the night there would be 2-3." (Participant 1)*

- the team that offers 24/7 coverage is spread across several countries. Two participants presented their strategy and demographics:

  "*We have an on-call schedule, which means that somebody is always on call. And of course, as we are both in Sweden, India and the US and UK there is always people online, somebody that is looking at all the alerts that are coming in, so we can communicate to each other, and we have chat channels in order to do that."(Participant 2)*

  "*Typically, what happens is that a few members of the team are located in Asia, some in Europe, some in the US so they can cover with their 24/7. Usually, for this shift, people are not working 8h but 12. At the moment, there is a team that operates in Romania, and they have a 24/7 NOC that operates in India*." (*Participant 3*)

The activity topic covers the way in which the team members work. Some tasks are independent, especially for the senior analysts, but the communication in general is very active among senior and junior analysts, as one of the participants presented: "*So, we communicate with them all the time. Sometimes there is like silent periods or sometimes there are ongoing chats that are going every minute regarding how you should approach that, how are you thinking to do that, what would be the next step." (Participant 2)*

The work category covers the incident handling, the time response and the coordination of other team members. From the literature review that was covered in the cybersecurity chapter we know that only analysts handle incidents, a fact that was confirmed in this step. This is the only variable from the analysis that was covered by all the participants.

For the time response criticality, we cannot identify any pattern from the responses, as the topic was covered only by three participants, but we know that the first level of analysts has the most critical time response, up to 15 minutes per event. Regarding the coordination of the team, people with more experience coordinate juniors, while the managers coordinate the whole team.

3. Identify Significant Behaviour Patterns

After the mapping of the participant's answers to the identified attributes, the significant behaviour patterns should be identified. This pattern could be determined by analysing the clusters of subjects that appear across numerous "ranges of variables". According to Alan Cooper, a behaviour pattern constitutes of a set of subjects who cluster in more than six different variables. The validity of the pattern is validated by the causative behaviour between the clustered behaviours.

By analysing the transcripts of the interviews and based on the previous literature review that is presented in the Cybersecurity chapter, we can see that three different behavioural patterns emerge. These three types are the junior analyst, corresponding to level 1 analyst, the person that is particularly involved with the incidents and his main responsibility is to monitor the "situational awareness and automation systems for security events", the senior analyst that investigates all the escalated tickets and improves and optimizes the security monitoring tools, and the manager whose responsibilities are to communicate with the stakeholders and, as one of the participants said, to "make sure that the people follow the procedure."

4. Synthesize Characteristics and Relevant Goals

The fourth step in the process is synthesizing the details from the gathered data for each one of the identified patterns. The main differences that we can identify from the interviews and research are the following:

- The **age** and **experience** are the main aspects that differentiate the three profiles. The junior analysts are young people that just finished their studies, and they want to gain experience by working in this field. The senior analysts are also young, but they have gathered more experience and they can now train and mentor the junior analysts. The managers are people that worked as analysts previously and they progressed their careers to the manager level.

- The **activities** that they perform is the essential aspect that differentiates the three categories. The junior analysts handle incident and they are monitoring the events, the senior analysts investigate the escalated tickets and improve the optimization of the security monitoring tools and the managers allocate resources for the team, discuss with the upper management and coordinate the team. A consequence of the difference in activity is the **set of tools** that is used by the personas.

- The **schedule** that they follow differs among teams and among job roles. Some analysts are required to offer 24/7 coverage, while others offer only 8/5 monitoring. Managers have regular 8/5 schedules as their responsibilities are not urgent.

- The **criticality** of the tasks and **time response** differs between the analyst levels and also between analysts and managers. The lower level – junior analyst (L1 level) has the fastest time response, as it was also presented in the literature review of the SOC team.

- The **skill set** between analysts and managers are complementary. In most of the cases, the managers started with analyst positions and they were promoted to managerial positions. A key skill for managers is communication skills. The difference between junior and senior analysts is that the senior analyst possesses the basic skills of the junior plus the ability to handle stressful situations, the curiosity to find the root cause of the incidents, and the ability to perform penetration testing and to understand visualization tools.

- The **set-up** differs among the teams and positions within the team mainly due to tasks and resources. The analysts require more screens as they have to continuously monitor the network.

- The **personality** and **motivations** vary among the team members, but a defining motivation of the analysts are the challenges that come with new threats.

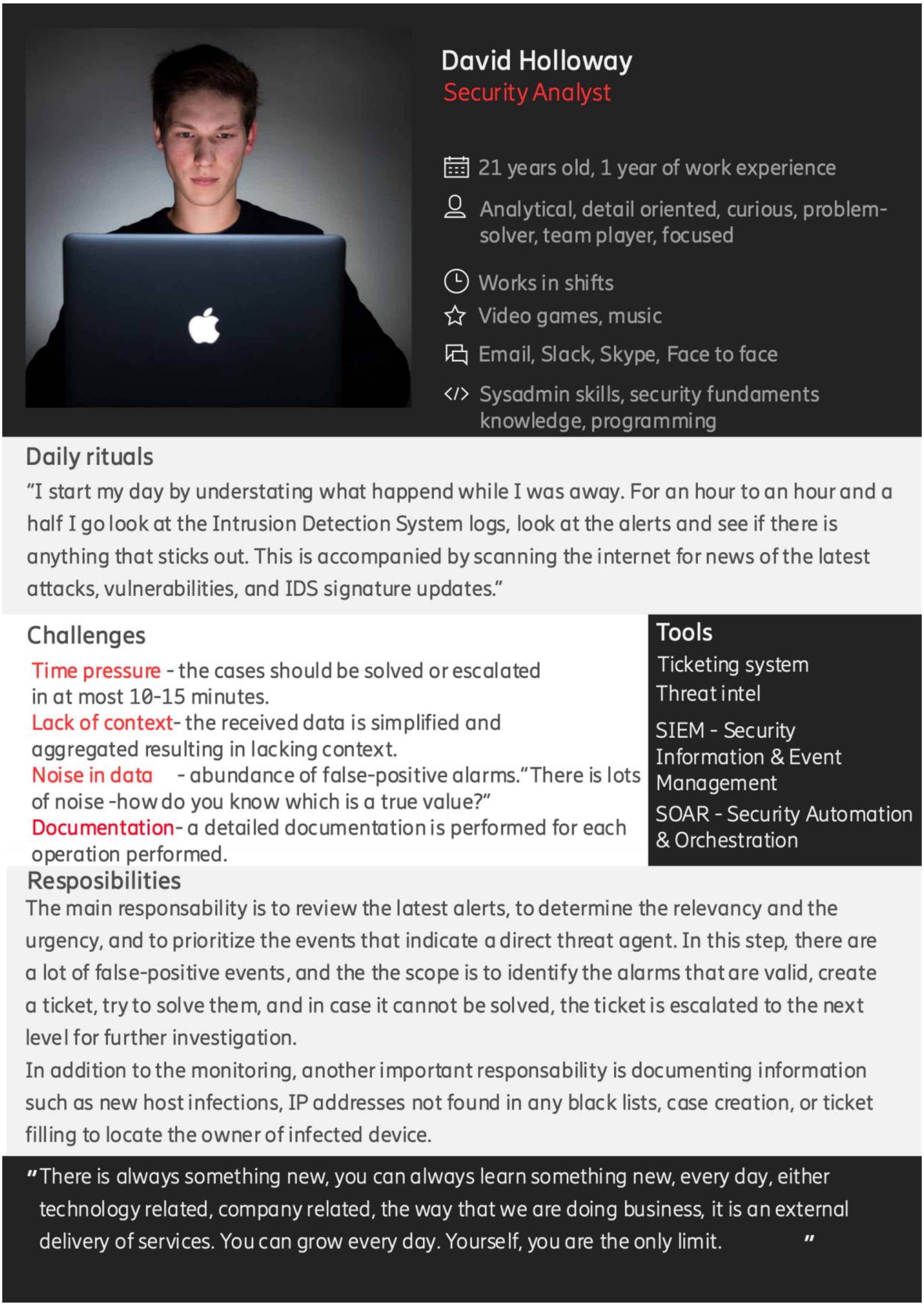
- The **goals** of the three personas are complementary. The analyst's final goals are to maintain the security and integrity of the network, while the manager's final goal is to procure the resources for the team and to operate correctly.

5. Check for completeness and redundancy

In the fifth step, the three personas are analysed and, in order to fulfil the requirements of the process, the personas have to be meaningfully distinct, to represent the diversification of behaviours. In the concrete case that we analyse, the three personas are designed on three fundamentally different types of behaviour, so there is no redundancy. The three personas differentiate from each other by their tasks, by their experience and age, by their responsibilities, challenges that they face, and their goals.

6. Expand description of attributes and behaviours

In the sixth step, the persona is built. The differences and characteristics that were presented previously take the form of personas in a third person narrative that conveys its attitude, needs and problems.



David Holloway

Security Analyst

- 21 years old, 1 year of work experience
- Analytical, detail oriented, curious, problem-solver, team player, focused
- Works in shifts
- Video games, music
- Email, Slack, Skype, Face to face
- </> Sysadmin skills, security fundaments knowledge, programming

Daily rituals

"I start my day by understating what happend while I was away. For an hour to an hour and a half I go look at the Intrusion Detection System logs, look at the alerts and see if there is anything that sticks out. This is accompanied by scanning the internet for news of the latest attacks, vulnerabilities, and IDS signature updates."

Challenges

Time pressure - the cases should be solved or escalated in at most 10-15 minutes.
Lack of context- the received data is simplified and aggregated resulting in lacking context.
Noise in data - abundance of false-positive alarms."There is lots of noise -how do you know which is a true value?"
Documentation- a detailed documentation is performed for each operation performed.

Tools

Ticketing system
Threat intel
SIEM - Security Information & Event Management
SOAR - Security Automation & Orchestration

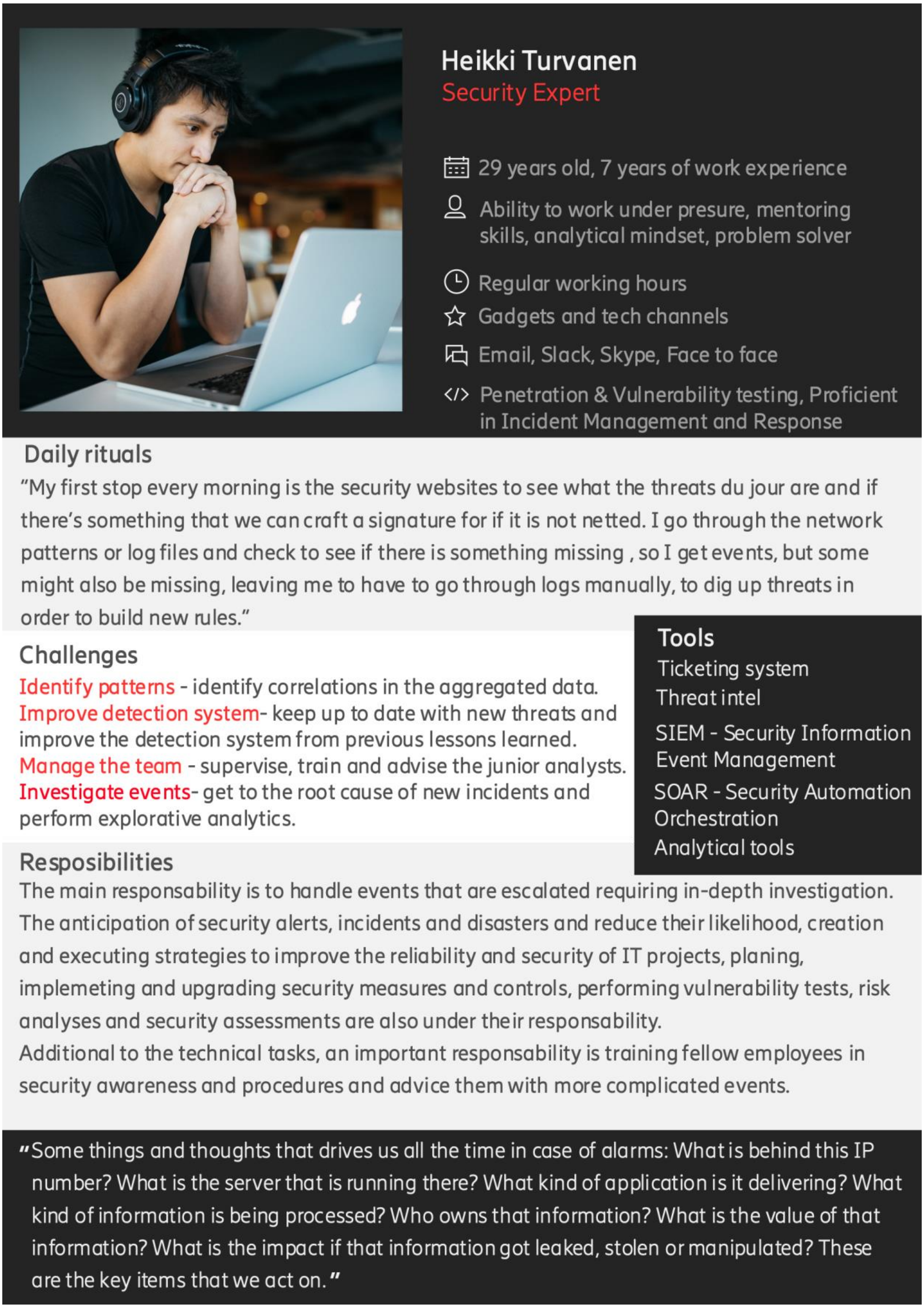
Resposibilities

The main responsability is to review the latest alerts, to determine the relevancy and the urgency, and to prioritize the events that indicate a direct threat agent. In this step, there are a lot of false-positive events, and the the scope is to identify the alarms that are valid, create a ticket, try to solve them, and in case it cannot be solved, the ticket is escalated to the next level for further investigation.

In addition to the monitoring, another important responsability is documenting information such as new host infections, IP addresses not found in any black lists, case creation, or ticket filling to locate the owner of infected device.

"There is always something new, you can always learn something new, every day, either technology related, company related, the way that we are doing business, it is an external delivery of services. You can grow every day. Yourself, you are the only limit. "

Figure 14: Persona Security Analyst



Heikki Turvanen

Security Expert

📅 29 years old, 7 years of work experience

👤 Ability to work under presure, mentoring skills, analytical mindset, problem solver

🕒 Regular working hours

☆ Gadgets and tech channels

Email, Slack, Skype, Face to face

</> Penetration & Vulnerability testing, Proficient in Incident Management and Response

Daily rituals

"My first stop every morning is the security websites to see what the threats du jour are and if there's something that we can craft a signature for if it is not netted. I go through the network patterns or log files and check to see if there is something missing , so I get events, but some might also be missing, leaving me to have to go through logs manually, to dig up threats in order to build new rules."

Challenges

Identify patterns - identify correlations in the aggregated data.
Improve detection system- keep up to date with new threats and improve the detection system from previous lessons learned.
Manage the team - supervise, train and advise the junior analysts.
Investigate events- get to the root cause of new incidents and perform explorative analytics.

Tools

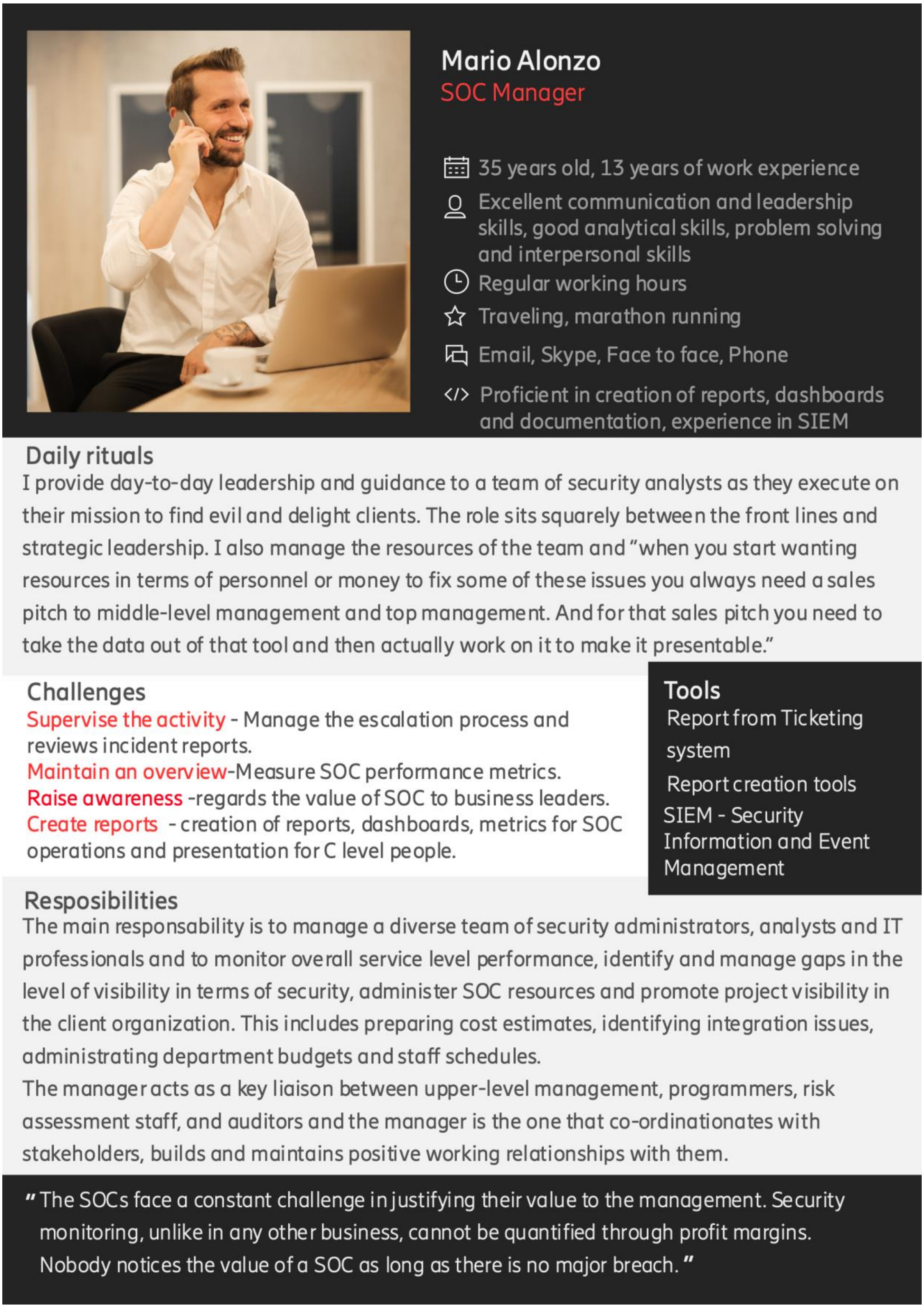
Ticketing system
Threat intel
SIEM - Security Information Event Management
SOAR - Security Automation Orchestration
Analytical tools

Resposibilities

The main responsability is to handle events that are escalated requiring in-depth investigation. The anticipation of security alerts, incidents and disasters and reduce their likelihood, creation and executing strategies to improve the reliability and security of IT projects, planing, implemeting and upgrading security measures and controls, performing vulnerability tests, risk analyses and security assessments are also under their responsability.
Additional to the technical tasks, an important responsability is training fellow employees in security awareness and procedures and advice them with more complicated events.

"Some things and thoughts that drives us all the time in case of alarms: What is behind this IP number? What is the server that is running there? What kind of application is it delivering? What kind of information is being processed? Who owns that information? What is the value of that information? What is the impact if that information got leaked, stolen or manipulated? These are the key items that we act on."

Figure 15:Persona Security Expert



Mario Alonzo

SOC Manager

- 35 years old, 13 years of work experience
- Excellent communication and leadership skills, good analytical skills, problem solving and interpersonal skills
- Regular working hours
- Traveling, marathon running
- Email, Skype, Face to face, Phone
- Proficient in creation of reports, dashboards and documentation, experience in SIEM

Daily rituals

I provide day-to-day leadership and guidance to a team of security analysts as they execute on their mission to find evil and delight clients. The role sits squarely between the front lines and strategic leadership. I also manage the resources of the team and "when you start wanting resources in terms of personnel or money to fix some of these issues you always need a sales pitch to middle-level management and top management. And for that sales pitch you need to take the data out of that tool and then actually work on it to make it presentable."

Challenges

Supervise the activity - Manage the escalation process and reviews incident reports.
Maintain an overview-Measure SOC performance metrics.
Raise awareness -regards the value of SOC to business leaders.
Create reports - creation of reports, dashboards, metrics for SOC operations and presentation for C level people.

Tools

Report from Ticketing system
Report creation tools
SIEM - Security Information and Event Management

Resposibilities

The main responsability is to manage a diverse team of security administrators, analysts and IT professionals and to monitor overall service level performance, identify and manage gaps in the level of visibility in terms of security, administer SOC resources and promote project visibility in the client organization. This includes preparing cost estimates, identifying integration issues, administrating department budgets and staff schedules.

The manager acts as a key liaison between upper-level management, programmers, risk assessment staff, and auditors and the manager is the one that co-ordinationates with stakeholders, builds and maintains positive working relationships with them.

" The SOCs face a constant challenge in justifying their value to the management. Security monitoring, unlike in any other business, cannot be quantified through profit margins. Nobody notices the value of a SOC as long as there is no major breach. "

Figure 16:Persona SOC Manager

The challenges of the personas are named in the personas poster that are displayed above, and now they will be illustrated and detailed below.

For the junior analyst, the challenges are the following:

- Time Pressure

  As presented in the literature review presented in the Cybersecurity chapter, the level one analyst has a limited time to solve incidents, otherwise they have to escalate them to the higher level. Person 5 presented this issue in the following quote:

  "Time is a critical resource for security analysts, who must determine whether to escalate an alert or write it off as a false positive in under 20 minutes. Due to the around-the-clock nature of incident response, security teams should invest in machine learning tools that can filter out the noise and present reliable analysis with speed and scale."

- Lack of Context

  One pertinent example was presented by the participant 6 and it is quoted below:

  "Compliance is 92%. What is that missing 8 %? The context is missing here. "It is like a home alarm system in your house. If the alarm company reported that 92% of your alarm system is compliant, you would panic, because that means that 8 % of your either doors or windows are not shut and that is not good enough. ... and it depends is it a second-floor window, is it a third-floor window that you know somebody needs a really long ladder to get it to you don't need to worry. Or is it your front door. So, the context is missing here."

- Noise in Data

  The participant 3 explained his opinion regarding the noise in the data and it is presented in the quote below:

  "So, the more noise you reduce, the less noise you see, the better it is for you to look at the next problem, to see the real problems. And that is what security is about. You pump loads of data into your tool and then you are going to have lots and lots of alarms and from those alarms you need to find out which are real, and which are false, based on your solution design. Eventually, you need to spend time to work through all the different alerts to water them down, to have only the real ones to investigate."

- Documentation

  The documentation process is mostly detailed in the handbook and in the speciality literature, but it was also mentioned in the interviews by participant 1 and 2.

  "They look at one alert, they make a ticket out of it, and then they work on it. If they cannot solve it on the L1 level, they escalate to L2. If they cannot solve it, they escalate to L3. That is kind of the flow, so all of the things that go into that, they are extremely well defined and documented: what is expected, what they should do and where." (Participant 2)

“Administration is a big part of the job. All the record keeping, creating folders for the incidents, emails, documenting things.” (Participant 1)

For the senior analysts, the challenges are the following:

- Identify Patterns and Investigate Events
  The problems that are faced by analysts are that they are confronted with considerable amounts of data that they further process and filter. The problem with this operation is that if the analyst does not have a clear idea of what is relevant, important events can be ignored. “Suspicious activity usually manifests itself in certain patterns, combinations of particular kinds of log lines that are hard to distinguish from the surrounding log lines.”(Stange *et al.*, 2014)

- Improve Detection System
  This challenge is constant as the threat’s scene is changing regularly. Participant 1 explains in the quote below how valuable knowledge gained from computer security incidents can be useful to prevent future incidents by enhancing the security features of functions within defences.

  “Of course, there are lessons learned in that cycle as well that come up all the time. Between those incidents that we are running, we sharpen our weapons, we make sure that the lessons learned, that what we have gone through earlier are implemented: the things that were missing, lacking, or not working properly.

  That involves things such as onboarding new load sources that we thought we have had, that are missing or that are wrong and we cannot use them efficiently , in could be like brand new load sources that we have to onboard , it could be like a way of working or it could be like a process that needs to come into place - how do we do it in the best way; it could be data enrichment that we need to do.”(Participant 2)

- Manage the Team and Provide Training
  The senior analyst should provide proper education and on-going training so that the skills and knowledge of the team members can evolve with the changing threat landscape.

  ” The purpose of that is to grow people, to organically grow our organisation so that we can take on more people, and we will promote more people from India to work with us.” (Participant 2)

  “We need to constantly evaluate our capabilities to assess our technical relevance and performance against evolving internal and external threats.” (Participant 4)

  “So whenever there is an alert, there is a ticket created, the L2 or the team works on that all the time and we have opened chat channels and we communicate in real time all the time about things that they have done, about things that we are curious about , so we are kind of overseeing them in the ticketing system, looking at the logs of what they are doing , we are sampling that and we are asking them

questions about it to make sure that we are doing some kind of quality check all the time and in order to see how they are thinking." (Participant 2)

For the managers, the challenges are the following:

- Supervise the Activity and Maintain an Overview
  The managers are responsible for the completion of the projects and commitments which reflects in the technical work, staff supervision, budgets and resources. The manager is responsible also for the schedule of the team members and for the productivity of the analysts.

- Raise Awareness
  The manager's tasks include the advertising of the SOC in order to raise awareness within the organisation and to obtain funds for the team.

  "Everything starts with the business of security within the business. We assure the client that we know their business, their core operating processes, their all-hazards risk and their alignment of value with their organization. A considerable amount of time is spent to understand the business, the existing challenges and risks and by constructing a strategy for risk mitigation. [...]

  One of the most significant challenges that are faced by the SOC team is the manner in which we are perceived by the community. Our aim is to make the security presence like electricity – omnipresent; everybody is aware of its presence. If they need help, we are here."

- Create Reports
  The managers can create insightful metrics and performance measures by using analytics. They facilitate managers to make more informed decisions "when balancing the trade-offs between costs and risks"(EY, 2014) and they serve as "compelling communication vehicle for financial and operational concerns".(EY, 2014)

7. Designate Persona Types

The last step in the process is designating the persona types. As the design requires a target on which to focus, this step prioritizes the personas and determines which is the primary design target. There are six types of personas according to Alan Cooper (Cooper, Reinmann and Cronin, 2007) : Primary, Secondary, Supplemental, Customer, Served and Negative. The three personas defined previously can be categorised as follows: The junior analyst is a primary persona and represents the primary target for the design of the interface. The senior analyst is a secondary persona as it would be satisfied with the interface designed for the primary persona – the junior analyst – but it would have some additional needs that could be accommodated in the same interface. The manager is also defined as a primary persona which means that it would have a dedicated interface for his role and needs. Between the two primary personas we can identify a callosal difference in role, task and personality as they have distinct goals. As their activities, responsibilities and interests do not overlap, they have completely different needs from the tool. In the comparison of the junior analyst with the senior analyst we can recognize some common tasks and responsibilities which leads to common needs for the dashboard. Between these two personas, the decision to establish the junior analyst as the primary persona was reached considering the lack of experience in the field of the junior and the fact that careful consideration should be taken in order to design the dashboard to prevent any mistakes and to make the completion of tasks straightforward. According to the design principle, each interface should focus on a single primary persona which means that in the design of the dashboard, there should be two interfaces, one designed for the manager persona and one designed for the analyst personas.

Another aspect that should be considered in the design of the interfaces is the goals of the personas in regard to the product. The goals are the drivers behind the behaviour patterns that we have identified. In the design process, the user goals can serve as "lenses through which the designer must consider the functions of a product"(Cooper, Reinmann and Cronin, 2007). The goals of the personas in rapport with a product can be categorised into three categories that correspond to Norman's three levels of cognitive processing from Emotional Design. (Norman, 2009) These types of user goals are the following:

- Experience goals
- End goals
- Life goals

The following section describes the categories in detail, and it classifies the goals of the defined personas in these categories.

The experience goals correspond to the visceral level of cognitive processing and covers the "most immediate level of processing"(Cooper, Reinmann and Cronin, 2007) which covers the way a product is perceived before significant interaction occurs. In the case of our personas, all of them have the same experience goal: they want to have a tool that is easy to use, with a modern interface and a pleasant visual appearance.

The end goals correspond to the behavioural level of cognitive processing and cover the simple, everyday behaviour. The focus on usability, interaction design and information architecture is placed on the behavioural level. The foundation of a product's tasks and behaviour are the end goals of the personas. In order to satisfy the persona end goals, in the concrete case of the three personas that have been built, two different interfaces have to be built. The tasks that the managers have to fulfil, their daily activities and the way they interact with the product are different than the tasks, activities and interactions of the analysts.

The life goals represent the personal aspirations of the users. Determining this particular goal for our personas requires more research so we will not focus on the reflective cognitive level of cognitive processing.

4.2 Evaluating the Existing Dashboard

According to the previous section, two main things have to be considered when developing the requirements for the dashboard:

- The prioritization of personas. According to the prioritization, two different interfaces, one for the manager persona and one that would integrate the needs of both analyst personas should be developed.

- The goals of the personas in regard to the product. The goals are categorised by the two cognitive levels, visceral and behavioural. The experience goals which correspond to the visceral level of cognitive processing are the same for the three personas and they will be covered by implementing the dashboard according to the design system provided. The end goals which correspond to the behavioural level are different between the two interfaces and they will be defined according to the categories presented in the Dashboard classification in the previous chapter. In this section, the focus is centred on the end goals, and the experience goals will be presented in a different section.

Taking into account the personas and the literature review that has been performed, the dashboard for the manager persona should follow the structure described below:

Table 5: Manager Dashboard attributes definition

Category	Dimensions	Description
Purpose	Strategic	The dashboard concentrates on high-level measures of performance of the team, including forecasts to light the path into the future.
Point of view	Exploratory	The dashboard should enable the manager with the possibility of interpreting and analysing the results.
Interactivity	Interactive display	The dashboard displays statistics that can be narrowed with filters and slicers or by selecting certain items within the views in order to gain an understanding of what has occurred, providing an insight on how the process has improved and which are the points that need extra efforts for improvements.
Time horizon	Historical	Provides an overview of the activity that happened in the past over a certain period of time.
Span of data	Departmental	The data that is presented in the dashboard should present the information collected at the department level.

Data acquisition	Automated	The data should be collected from the activity that is performed by the team but in the case of managers, there should be a possibility to add additional data manually.
Control	Role based personalization	The dashboard has been personalised according to the needs that have been identified in the research phase.
Triggers	Pull scenario	The dashboard will be consulted when in need of certain reports, specific information is required or to supervise the performance of the team.

The dashboard structure for the analysts should follow the structure described below:

Table 6: Analyst Dashboard attributes definition

Category	Dimensions	Description
Purpose	Operational	Supports the monitoring of events and enables the user to perform immediate and dynamic actions. The content should enable the user to monitor operations and it should maintain awareness on the constantly changing events that need to be solved.
Point of view	Exploratory	The dashboard should enable the analyst with the possibility of interpreting and analysing the results.
Interactivity	Interactive display	The dashboard enables the analyst to perform easy and fast actions on the dashboard such as selecting certain items within the views and accessing data in a lower or higher level of a hierarchically-structured database.
Time horizon	Real Time	The content of the dashboard regarding the events is automatically updated with the most current data available.
	Historical	For further analysis and trend identification the dashboard provides an overview of the previous events.
Span of data	Enterprise-wide	The data is collected at the enterprise level and the dashboard offers an overview of the whole network that the department is responsible for.
Data acquisition	Automated	The tool should acquire the data in an automatic way as also some of the analysts that took part in the interview mentioned:

		“*That is another thing that you must be able to do. You must be able to take application logs which might be in different formats such as json and then be able to pull them into the incident tool to read them.*”
Control	Role based personalization	The dashboard has been personalised according to the needs that have been identified in the research phase.
Triggers	Pull scenario	The analyst is in control of when to consult the dashboard. Due to the high number of alerts, the push scenario that would send notifications to the user when an alert occurs would be overwhelming and it would distract the users from the activity that they are performing.

The current version of the dashboard will be compared to the requirements or design characteristics that have been presented above. The first thing that has to be mentioned is that in the current version of the dashboard there is no personalization of the interface according to role, which is a major difference that is set in the new version. The comparison will be performed against the two designs that have been proposed, in order to get a better understanding of the changes that have to be made and also of the elements that have to be shifted from the old version to the new one.

Table 7: Comparison between current dashboard attributes and the new defined analyst and manager Dashboards

Category	Current interface	Manager interface	Analyst interface
Purpose	Operational	Strategic	Operational
Time horizon	Real Time & Historical	Historical	Real Time & Historical
Interactivity	Interactive display	Interactive display	Interactive display
Point of view	Exploratory	Exploratory	Exploratory
Span of data	Enterprise-wide	Departmental	Enterprise-wide
Data acquisition	Automated	Automated	Automated
Control	One-size-fits all	Role-based personalization	Role-based personalization
Triggers	Pull scenario	Pull scenario	Pull scenario

4.3 Applied Design System

The design system that will be applied on the dashboard is an open design system that belongs to a multinational networking and telecommunications company, available only within the organizations and applied on the products that are developed under their brand. The goal of the design system, especially for the company's digital services is "to provide an iconic user experience to customers and end users" (Ericsson, 2018b) The brand identity is "firmly rooted in product design principles" and the design system was awarded with two Red Dot Awards for brand and interface design in 2018.

The foundation of the design is based on a strategy. The strategy covers the purpose, the business strategy, the brand, and it introduces the brand promise. As presented in the literature review performed on design systems, the foundation for a well-functioning system is a set of solid principles. In this case, they are gathered under the title "experience principles" and are the following:

- Focus and act now – decide and act fast, proving efficiency
- Get closer – engage in the customer needs and create value for them
- Lead the way – help customers to move safely and quickly towards new opportunities
- Plug and play – solutions that are user friendly and effortless to install, deploy and maintain

Under the "Strategy" category is also the tone of voice principles that cover the words that are chosen, the personality that is presented to the user and that is the spirit behind it all. These principles that sit behind the visual identity are the following three:

- Compelling and frank – "telling it straight is what captures people's attention and interest."(Ericsson, 2018b)
- Constructively and challenging – keep moving forward and constantly challenge the status quo.
- Considerate but commercial – indicate that the business focus and dedication is on delivering efficiency, unique digital experiences and new revenue streams.

The next category, "Identity", are covers the visual identity and brand consistency. The digital-first brand identity is committed to simplicity, trust, and enhanced productivity. The visual identity covers components such as logo, typography, colour, iconography, the grid, photography, video, printed material, email templates, and charts and data visualization.

The last category is the "Product design" and it is focused on the digital products, covering subcategories such as UX design, UX principles, design system foundation, and concept flows. For the UX strategy, the goals are to create "experiences that are valuable, aesthetically pleasing, emotionally satisfying, and easy to learn, to use, to install, to maintain and to upgrade"(Ericsson, 2018b) and to deliver intuitive and tailored experiences. The main goals of the user experience in this particular case are:

- Usefulness – the product solves a meaningful problem and fulfils the needs of the target audience.

- Usability – the product is efficient, enjoyable and easy to learn and use.

- Branding – every designed product complies with the defined brand guidelines and utilizes the predefined assets.

The UX principles that have to be taken into consideration when developing the design of a digital product are the following:

- Focused on simplicity – remove unnecessary details and decorations which might distract the user.

- Visual hierarchy – follow the 3 layers structure – system, application and content – in order to create an architecture of the information throughout the application.

- Actionable first – in the industry for which the products are developed, decisions have to be made in a short time span and decisive actions to be taken within seconds. For this particular reason, the actions should be accompanied by their contexts and they should be placed conveniently and on the most immediate layer.

- Responsiveness – the elements on the interface should scale, stack, and change according to the screen size.

- Progressive disclosure – data with massive volumes of information should be turned into insights.

- Iconic data visualization – deliver valuable information.

- Motion as a UX enhancer – the motion is used to present changes in the system and to display the results of the actions performed by the user.

- Contextual UI contrast – two different themes have been defined – dark theme and light theme- and the decision regarding which one to use in the product should be based on user research.

The principles are transposed to patterns, meaning that they should focus on value over aesthetics, keeping a minimalist interface that would not overwhelm and distract the user.

The perceptual design has been designed with these principles in mind and they cover things such as the visual hierarchy, the theme and colours – both for the light and dark theme, the grid system and the repository of iconography.

The functional patterns, the tangible building blocks of the interface, have the purpose of encouraging a certain user behaviour and to simplify the work of designers and developers. For the designers, the assets are available both in Sketch and Adobe Illustrator while for the developers, the code is modularized into two different repositories, Vanilla JS repository and Angular repository. Each component follows the basis pattern:

- Usage guidelines
- Implementation guidelines
- Example of interaction
- Download option
- Code snippets covering HTML, LESS, and JavaScript

The repository consists of components such as buttons, cards, checkboxes, radio buttons, switches, dropdowns, text fields, progress bars, tables, tabs, navigation, dialogs, data visualization widgets, and many other components.

The design system presented will be used in the development of the dashboard that covers the requirements defined in the chapters "4.1 Modelling users: Personas" and "4.2 Evaluating the Existing Dashboard". The design system is responsible of covering visceral cognitive level.

The needs that are common among the three personas on the visceral level are simplicity, functionality, ease of use, and modern look. These needs are covered and common to the approach of the design system as it is rooted in digital performance and functionality. The focus is on functionality and performance while not neglecting the aesthetics.

The design principles put the emphasis on the needs of the user, keeping the interface minimalistic, decluttering not only the graphical user interface but also the physical experiences which leads to solutions that are easy to use, functional and focus on the essential information.

The perceptual and functional patterns contribute to achieving these goals. The typeface used by the design system, Hilda, has been designed and optimized specifically to bring clarity and legibility to messages and interactions. The icons are focused, designed for screen performance targeted to the technology portfolio of the product. The colours that were chosen to have the power to transform and elevate the user experience. The colour palette consists of grayscale shades and accent colours which are intended to help guide the user towards key messages and interactions. Two themes were available to choose from, light and dark theme. The light theme was designed for specific cases in which high luminosity and readability are crucial, pages that consists of great amounts of text or forms and wizards. The dark theme carries a "tech oriented and future proof brand message, while catering to our users' health, improving productivity and ability to assimilate data."(Ericsson, 2018) The dark theme is designed for dashboards that are used for long periods of time as it reduces the eye strain and it is appropriate for dark-room environment – such as the ones used by the SOC teams. The dark theme elicits a tech-oriented ambience and the accent colours increase the importance and the awareness on the new events, incidents, warnings, and notifications.

4.4 Dashboard Implementation

This chapter covers the decisions and the process that was followed in order to develop the two dashboards, designed for the analyst persona and for the manager persona. The first thing that was considered in the design, is the structure which was covered in the chapter “4.2 Evaluating the Existing Dashboard” and the content. Another major decision that was made from the start is that the two pages will not have overlapping information and that both personas will have access to the two different dashboards.

The main differentiating characteristic is the purpose: strategic vs operational. Starting with the Strategic dashboard, which was designed to accommodate the needs of the analysts, the fundamental ground from which it has been refined is that it will display the pressing matters, the most crucial tasks that need to be operated on. The operational dashboard has been constructed to offer an overview of the recent activity of the team and their tasks, to present at a glance the results in relation to the minimum baseline and to raise the awareness of any danger. On the grounds of that, the labels of the two dashboards are “System status” – corresponding to the manager dashboard and “Activity review” for the analyst.

Starting from the challenges, responsibilities, and daily rituals that characterise the user types, the wireframes and low fidelity prototypes have been developed. The issues that we aim to solve with the current design in the case of the analyst profile are:

- Lack of context
- Identify patterns
- Investigate events
- Time pressure
- Noise in the data

The challenges that were faced at this stage is identifying the functions that correspond to the needs. Studying also the capabilities of the developed product we realised that these challenges can be covered as follows:

- “Investigate events and review the latest alerts” is a task specific to the analysts. That is why, a full section has been dedicated to the Real time events. For an easier prioritization and identification of urgency and validity of events, the feature of sorting by the severity of the event, by the risk percentage indicating a direct threat and by the number of affected devices. The implementation of these features aims to reduce the time pressure that is experienced by the analysts. Another feature that was integrated into the design is the ability to identify from the dashboard if any events were assigned directly to you, a feature that would benefit more the experienced analysts, who receive escalated events for further analysis.

- The issue of noise in the data is more problematic. The real time events section intends by prioritization to ignore the events that have less significance.

- “Identify patterns challenge” is covered by the event history section which presents the number of incoming events on a timescale and by the graphic that clarifies and shows the distribution and flows of events by their categories.

- The section “Top lowest compliance results” which presents the lowest results of the compliance checks for assets, policy and policy set presents the issues that are in the worst condition and that should be improved in the first place. The section “Assets requiring attention” presents the assets that need configuration, updates or additional set-up. The “Policy updates” section presents a list of policies that need updates, a list which can be sorted based on the number of updates that are pending, by the type of update-minor, critical, urgent- and by the number of devices that are affected.

The issues that we aim to solve with the current design in the case of the manager profile are:

- Supervise the activity
- Maintain an overview
- Create reports

The main challenge that was faced at this stage is identifying the functions that correspond to the needs. Studying also the capabilities of the developed product we realised that these challenges can be covered as follows:

- The issue of supervising the activity of the team is covered by two sections: “Average ticket” and “Tickets by status”.
  The average ticket performs a mean of the time taken for solving each ticket, from the time it has been assigned to the time it has been fixed.
  The section “Tickets by status” presents the total number of tickets that have been created followed by an explanation, where the total number is divided by category. Five categories have been defined and they are Resolved – counting the tickets that have been solved and closed, Open – tickets that have been assigned and are currently being worked on, Dismissed – tickets that referred to false alarms, Escalated – tickets that could not be solved by the level 1 analysts and have been escalated to a higher level so that more experienced analysts will investigate the events and Unassigned – tickets that have been created but have not been assigned to an analyst.

- The problem of maintaining an overview of the state of the system is covered in the next other sections of the dashboard: “Active events by severity”, “Policy set checks”, “Pending updates”, “Compliance checks” and “Compliance history”. The main idea behind these sections is that the manager can make sure that the system is working within the set boundaries, that the baseline conditions that are defined in the system level of agreement are met and that there is no imminent danger.

  “Active events by severity” section classifies the events that has to be operated on by their severity, and the categories that have been defined are: Critical, Major, Minor, Warning, and Informational. The categories were presented in the application sorted by severity, from high to low.

  “Policy set checks” section presents all the policy sets with their last compliance score, ranging from 0% to 100%.

  “Pending updates” presents the number of policy sets updates available.

“Compliance check” offers the possibility to set a range between 0 to 100 % for the compliance score and it will display as a percentage and also as the accurate number, the policy sets, policies and assets that have the result of their compliance score in the given interval.

“Compliance history” displays the trend of the compliance score over a given period of time and the score of the last compliance score.

- For the problem of creating reports, the function “Download report” was created, allowing the user to customise according to their needs what to be added into the final report.

For both of the dashboards, the option of selecting a timeframe is available. The options that are available are last 12 hours, last 24 hours, the last 3 days, last 7 days and last 14 days.

The options of charts were used to display large amounts of information in a condensed manner, to enable a clear identification of trends and issues. For the chart presenting the events history, showing the incoming number of incoming events in the form of a line graph. If the number of events exceeds the set accepted number, the line will be coloured in red to draw the attention of the user. In order to display the types of events, the same type of line graph has been used but the user can select the specific types of events that he wants to be displayed by enabling or disabling them from a checkbox.

For “Policy set check” section a horizontal bar chart was used, showing the compliance status, accompanied by the percentage that it represents. In the case of “Active events by severity”, the same bar chart was used, in this case representing the number of events that belong to a category and that are active.

A pie chart was chosen to display the created tickets and the slices, accompanied by the legend, present the status of the tickets.

In the analyst dashboard entitled “System status”, multiple table views have been utilised. For the information that is displayed multiple filters can be applied to sort the relevancy of the results. The tables present a small selection of data, offering the possibility to get a detailed look on a different view by clicking the icon in the right part of the tile, an action that would redirect to a different portion of the application.

The fist iteration of the design consisted of a paper prototype that integrated all of the previously specified aspects. The paper prototype was chosen as it was a fast method to present the idea in a tangible form. The low-fidelity prototypes that were constructed in this step and the personas were validated with an open discussion with two SOC experts from the organisation and it covered aspects such as terminology and workflow logic. The suggestions that were presented by the experts were considered for the high-fidelity design of the Dashboard.

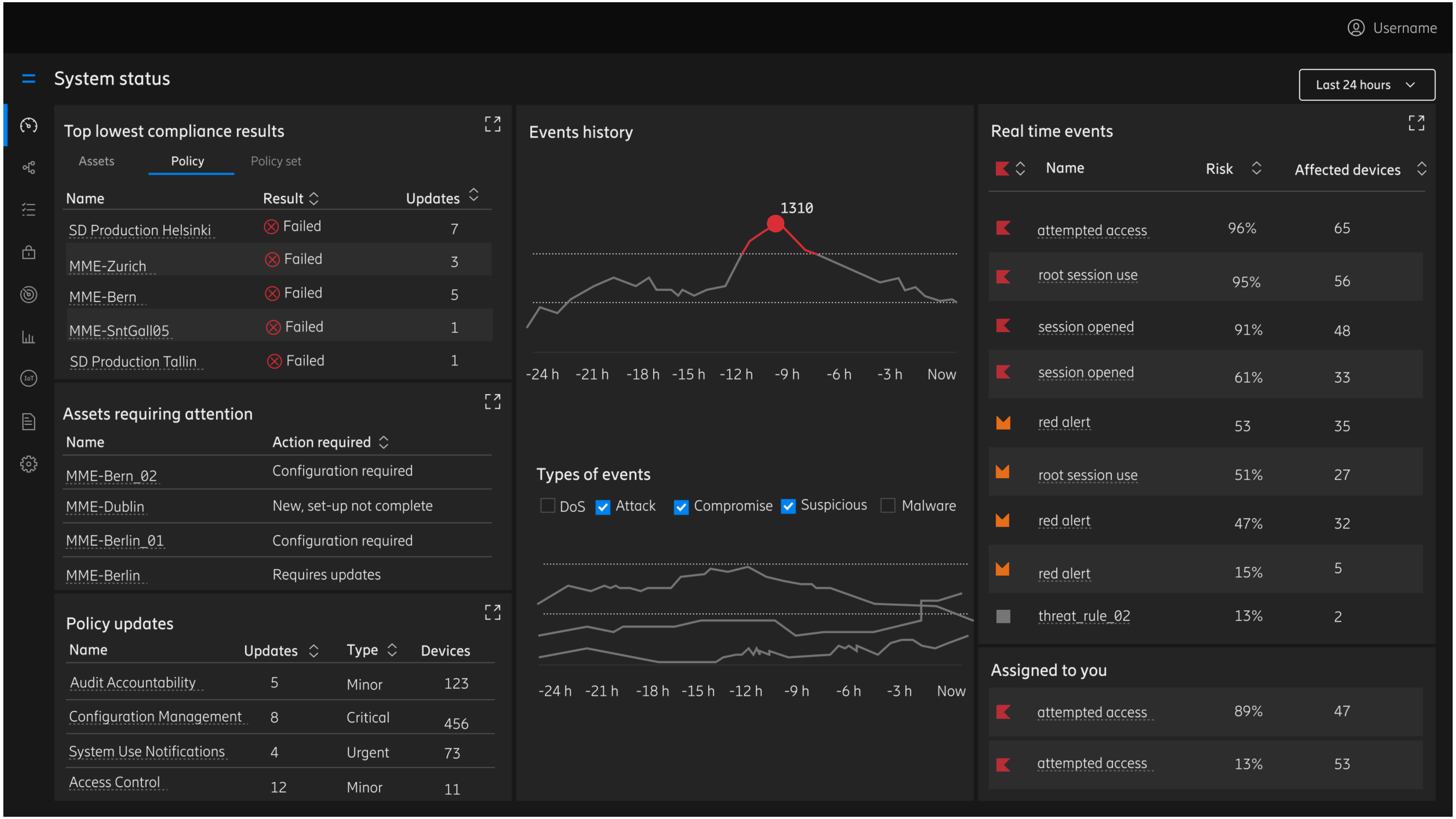
The high-fidelity design was constructed according to the design system guidelines. The dark theme was chosen as it has been intentionally designed for dashboards that are used for long periods of time as it reduces the eye strain and it is appropriate for dark-room environment. The dark theme also elicits a tech-oriented ambiance. The colours that were used are part of a palette of grayscale shades, and as an accent, for the metrics or elements that were exceeding a certain baseline, the accent colours were used to raise their awareness and importance. The content was divided into three columns based on the information that was displayed and on the functionality.

The high-fidelity prototypes were implemented using Figma, a cloud-based tool for collaborative design. Some of the advantages that were considered while deciding on the most appropriate tool are the availability – as a browser-based product it is available on any platform and it does not require installation; collaboration – multiple team members can work simultaneously on the same file; version control feature; specific view for developers and built-in comments feature. The main convenience of this cloud-based tool is the sharing feature, an URL address can be created to a page or a project and the file which is updated automatically can act as a single-source-of-truth for designers, product owners and developers.

In order to use the components and styles provided by the design system, the Symbol pages that contain all of these elements had to be imported in the tool and they were automatically converted into a Team Library. The Team Library is a master document that provides all of the styles – colour, typography- font and sizes of text, colour palette, layers, assets and components – UI elements that can be further reused across the developed designs. The collection of components consists of reusable simple components such as buttons, checkboxes, radio buttons, switches, dropdowns, text, number and date fields, progress bar, pills, tabs and tooltips but also more complex components such as tables, wizards, navigation and data visualization elements.

Having the complete library of components provided by the design system reduces friction and speeds up the design process as the team can utilize the existing components as building blocks. By reusing the elements, the consistency can be maintained throughout the product.

Figma offers the possibility to create interactive flows that simulate the interaction that a user can perform in the interface level. The tool provides an interaction feature that enables the designer to create products that feel real and respond in predictive ways to the user's input which can be utilised in user testing. For the developed prototype, the interactions that were used are On Hover – for the tooltips displaying values for the compliance history and for the type of events graph, highlighting and displaying the type for each line; On click – for interaction such as navigation amount the dashboards, change of time interval, selection of a policy set, download of report and "After delay" which causes transitions to occur automatically after a specified amount of time and was used to mimic the appearance of notification message for successful download of the report.



Username

System status

Last 24 hours

Top lowest compliance results

Assets | **Policy** | Policy set

Name	Result	Updates
SD Production Helsinki	⊗ Failed	7
MME-Zurich	⊗ Failed	3
MME-Bern	⊗ Failed	5
MME-SntGall05	⊗ Failed	1
SD Production Tallin	⊗ Failed	1

Assets requiring attention

Name	Action required
MME-Bern_02	Configuration required
MME-Dublin	New, set-up not complete
MME-Berlin_01	Configuration required
MME-Berlin	Requires updates

Policy updates

Name	Updates	Type	Devices
Audit Accountability	5	Minor	123
Configuration Management	8	Critical	456
System Use Notifications	4	Urgent	73
Access Control	12	Minor	11

Events history

Types of events

☐ DoS ☑ Attack ☑ Compromise ☑ Suspicious ☐ Malware

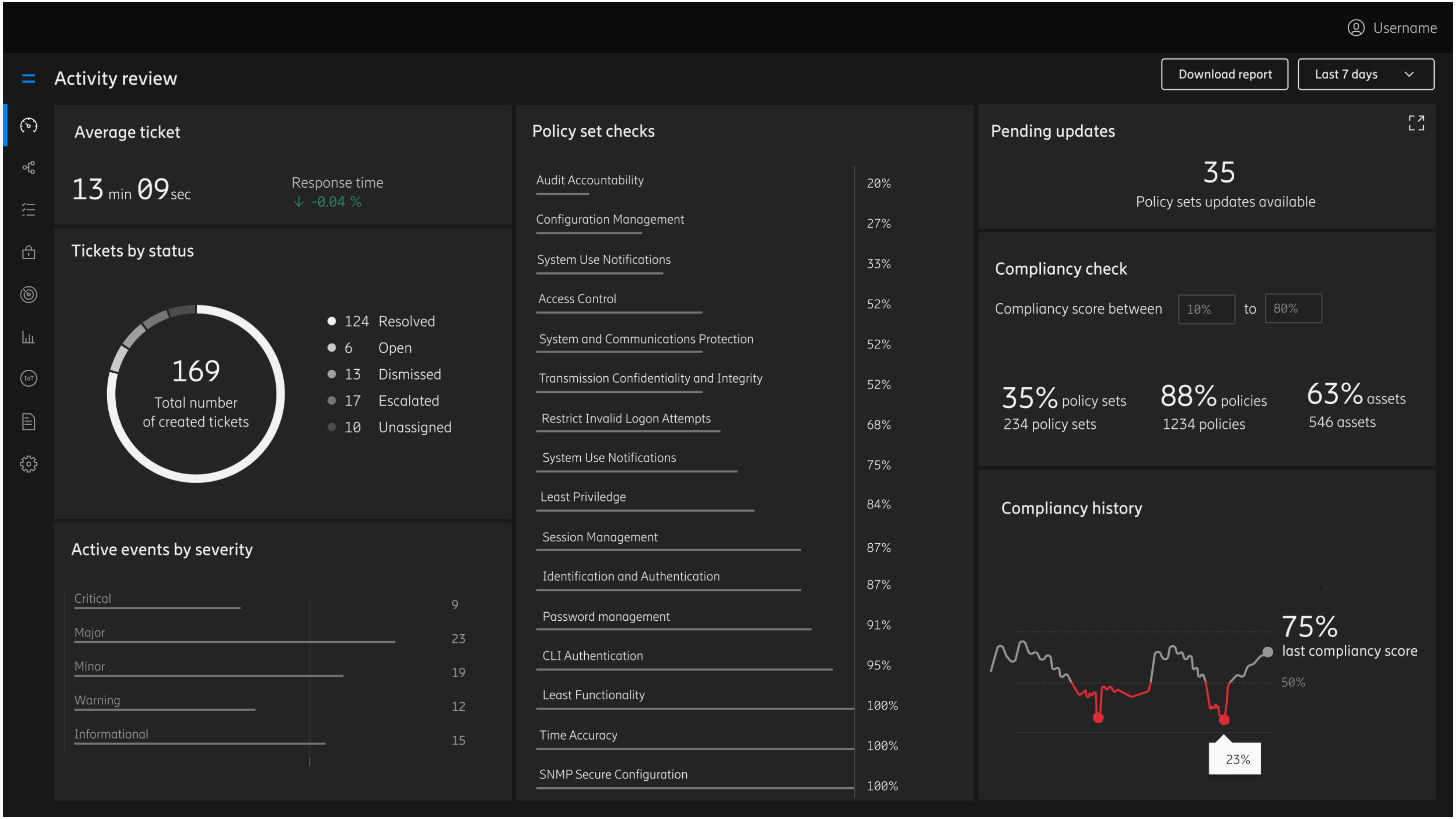
Real time events

	Name	Risk	Affected devices
🟥	attempted access	96%	65
🟥	root session use	95%	56
🟥	session opened	91%	48
🟥	session opened	61%	33
🟧	red alert	53	35
🟧	root session use	51%	27
🟧	red alert	47%	32
🟧	red alert	15%	5
⬜	threat_rule_02	13%	2

Assigned to you

	Name	Risk	Affected devices
🟥	attempted access	89%	47
🟥	attempted access	13%	53

Figure 17: Dashboard System status



Average ticket

13 min 09 sec

Response time ↓ -0.04 %

Tickets by status

169 Total number of created tickets

● 124	Resolved
● 6	Open
● 13	Dismissed
● 17	Escalated
● 10	Unassigned

Active events by severity

Critical	9
Major	23
Minor	19
Warning	12
Informational	15

Policy set checks

Audit Accountability	20%
Configuration Management	27%
System Use Notifications	33%
Access Control	52%
System and Communications Protection	52%
Transmission Confidentiality and Integrity	52%
Restrict Invalid Logon Attempts	68%
System Use Notifications	75%
Least Priviledge	84%
Session Management	87%
Identification and Authentication	87%
Password management	91%
CLI Authentication	95%
Least Functionality	100%
Time Accuracy	100%
SNMP Secure Configuration	100%

Pending updates

35 Policy sets updates available

Compliancy check

Compliancy score between 10% to 80%

35% policy sets 234 policy sets

88% policies 1234 policies

63% assets 546 assets

Compliancy history

Figure 18: Dashboard Activity review

4.5 Usability Test Planning

One of the major questions that arises now that the prototypes corresponding to the two dashboards are completed is if the product is suitable for the purpose for which it has been designed. The dashboards have been built after the phase of user research in which the tasks and the environment in which the task will be performed have been studied. The results of this phase materialized in the requirements for the system. The usability test endeavours to validate the relevance of the solution and to prove that the system is fit for the purpose for which it was designed.

This evaluation with users in which direct feedback for the design will be collected aims to ensure that the concept that has been produced meets the user requirements and it is usable. The purpose of the early evaluation is to guarantee that the usability faults are gathered at an early stage leading to a lower cost of change.

The structure that was followed for planning the usability test is the one described in the book "Usability engineering" (Faulkner, 2000) and the steps that were pursued are:

- Identify the target group
  Security experts, preferably occupying a position in a security operation centre. The target group can be divided in two main categories – managers and analysts, corresponding to the two primary personas that have been identified.

- Recruit users
  The users were recruited within the organization as the availability of these experts is limited and also, a major constraint is that the field of security implies extra care regarding the confidentiality of the work, so obtaining permission to test with users outside of the organisation is problematic. Extra care was taken to ensure that the appropriate user type with the necessary skills were recruited. The initial plan is to test with 9 users, 4 managers and 5 analysts. The optimal number of users that is needed for the usability test is 3 per persona, as Bruce Tognazinni recommends, but more sessions have been reserved in the event of cancelation. Future deviations due to cancelation will be reported.

- Establish the duration of the test, the tasks, and the questions
  The session is planned to take 60 minutes and it consists of 3 parts. The first part intends to test the application and the user is asked to perform some given tasks. The second part consists of a set of questions regarding the system that was experienced followed by a SUS questionnaire. The tasks and the questions that will be covered in the test are the following:

  Question: Can you describe the state of the system after the weekend?
  Expected output: The expected result is an open description of the dashboard, a first impression of the content that is present in the two dashboards.

  Question: What would be the first thing that you would check?
  Expected output: The question does not have a desired result, expecting a personal opinion over the importance and the urgency of the actions that have to be performed on the dashboard.

Question: Do you see any major changes that happened during the time that you were away? Which are the days with the peak number of incoming events? What are those numbers?

Expected output: This is one of the tasks that will be measured in order to determine the effectiveness. The desired solution is that the user will check from the analyst dashboard the event's history over the last 7 days and will report the numbers 2675 and 1310. The view from which they should identify these values is the following:

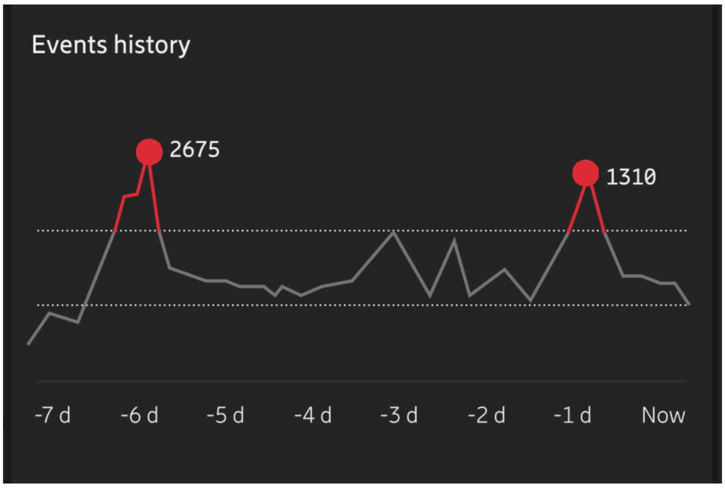


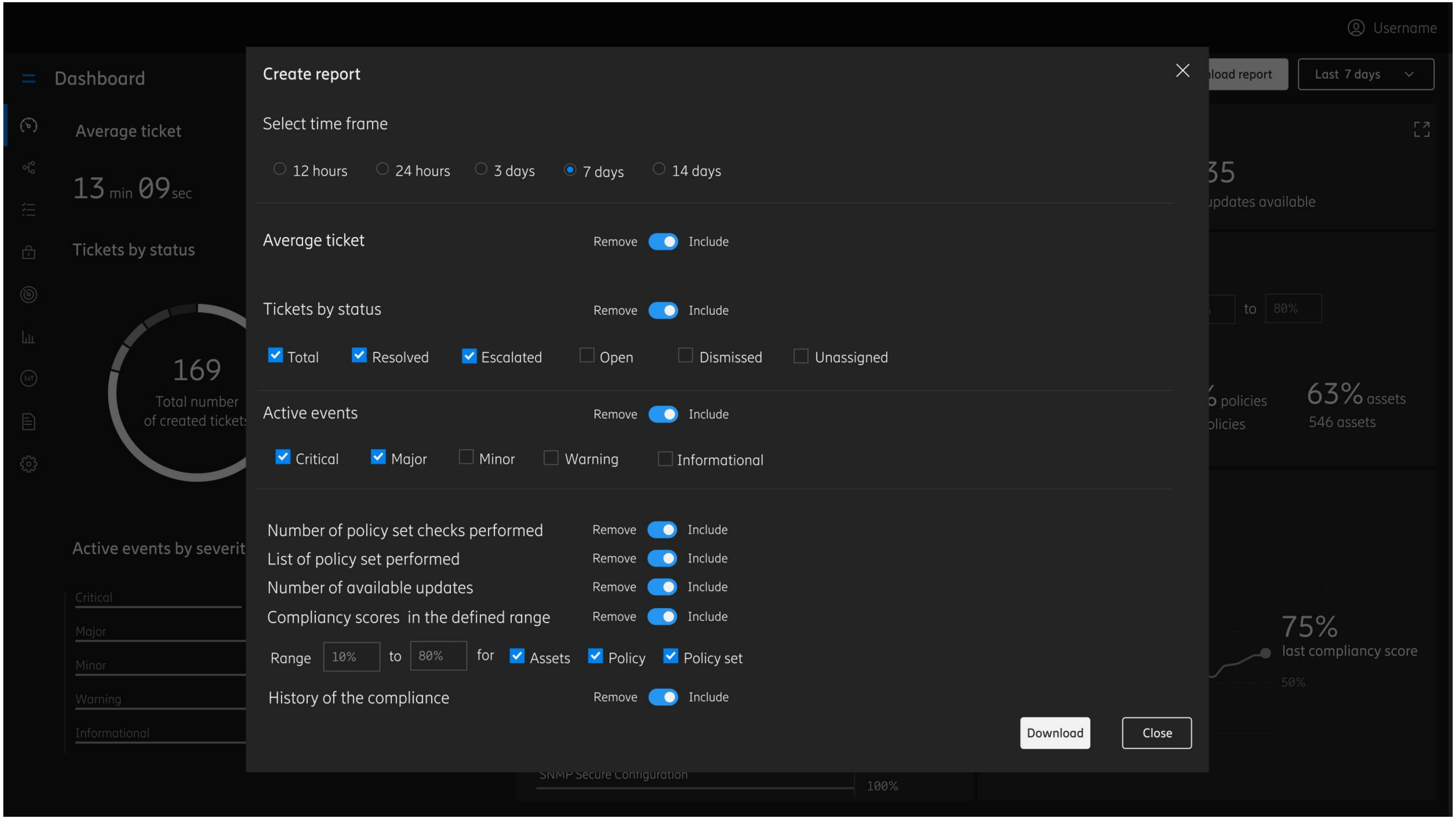
Figure 19: Graphical representation of incoming events

Question: Identify the lowest compliance score of a policy set and get more details about that.

Expected out: There are multiple ways to reach to the desired page, both from the manager dashboard, entitled “Activity review” in the interface and from the analyst page entitled “System status”.

Question: Create a summary of the activity of the team from the last week. What would you include?

Expected output: The task will be measured in order to determine the effectiveness of the dashboard. The action that has to be performed by the user is to download a report of the activity over the last 7 days. There are two options for selecting the timeframe of 7 days, one from the dropdown on the dashboard and one from the radio buttons from the interface presented beneath. The task is considered complete if the user is able to reach the screen presented below and a discussion regarding what would be selected from these options will start.



Create report

Select time frame

○ 12 hours ○ 24 hours ○ 3 days ● 7 days ○ 14 days

Average ticket — Remove ● Include

Tickets by status — Remove ● Include

☑ Total ☑ Resolved ☑ Escalated □ Open □ Dismissed □ Unassigned

Active events — Remove ● Include

☑ Critical ☑ Major □ Minor □ Warning □ Informational

Number of policy set checks performed — Remove ● Include

List of policy set performed — Remove ● Include

Number of available updates — Remove ● Include

Compliancy scores in the defined range — Remove ● Include

Range 10% to 80% for ☑ Assets ☑ Policy ☑ Policy set

History of the compliance — Remove ● Include

Download Close

Figure 20: Create report

Question: Which one of the two presented dashboards do you think you would use more for your work?
Expected output: This question has the purpose of validating the personas and the expected response is that the analysts will choose the dashboard designed for their persona and the managers will also choose the dashboard designed for their persona.

The next set of questions has the goal of gathering opinions and problems identified by the users. The questions that are going to be asked in this session are the following:

- Which one of the two presented dashboards do you think you would use more for your work?
- What are the main problems and difficulties you have found while using this prototype?
- Which functions have you liked most of the prototype? Why?
- Can you describe your overall experience with this prototype?
- How did you like the user interface design?
- How would you evaluate the set of functions being offered in the prototype?
- What would you improve in this prototype? If you had one free wish, what or which function would you like to have for such a system?

A SUS questionnaire will be answered in the last part of the session.

One major decision that was made in the usability test planning is that, for a better coverage, both personas – analyst and managers – will have access to both dashboards, and the tasks that are performed will not differ between these two roles. The expected are that the users will appreciate and will find more useful the dashboard that was designed for their line of work and their needs, and this assumption has to be proved in the testing session.

- Perform the evaluation
  The sessions will be help face to face and one user, one moderator and one notetaker will be present. The moderator will present the scope of the test, will introduce the user to the system and will ask for permission to record. Both the screen and the audio will be recorded in order to have all the information available for analysis. Once that the user is comfortable, the moderator can start to present the questions and tasks according to the plan made ahead.

  During the evaluation the users are asked to think aloud, expressing all their concerns, expectations, thoughts, and feelings while they carry out the activity within the system. In this way, the evaluator can obtain valuable insights on how the users operate the system and what their strategy is for carrying out the tasks.

  Through the investigation, the notetaker has to observe and document all the physical actions of the users, to note all the results -successes and errors of the tasks and to check for any feelings regarding the use of the application – curiosity, excitement, surprise, boredom, etc.

- Report the findings
  The results that have been obtained from the usability testing sessions will be reported in the next chapter.

4.6 Results of the Usability Test

4.6.1 Tasks Performed on the Prototype

The final number of interviews that were performed is six. All of the interviews took place over the course of one week and four of them took place face to face in a meeting room within the organisation and the other, were performed via the communication platform Microsoft Teams. For the remote sessions, the notetaker, the moderator, and the user participated in the call. Access to the screen was allowed via the screen-sharing functionality combined with allowing remote access for the participant. One issue that was observed by the moderator during the first session is that the users are not aware of the fact that they can switch to the two dashboards from the menu, so a decision was made to help the users and present to them how to change the views. This decision will not influence the results as the navigation technique is not the official one that is used in the application.

You are coming to work Monday morning and get straight into work.

1. Can you describe the state/status of the system after the weekend?
   All of the users stayed on the Activity review view and tried to determine the state of the system from that dashboard.

   A first thing that captivated the participant and which was the first thing that was noticed by most of them is the “Compliance history” tile. They see a drop in the graph that is accentuated in red and they automatically recognise that something bad happened. One important lesson learned from this observation is that the urgent or critical issues and the aspects that should be considered by the user at first glance should be in accent colours in order to be identified at first glance. The majority of the users claimed that they would like to see a timeframe at the bottom of the graph so that they would be able to identify the exact moment when the drop happened.

   In order to see the system status after the weekend, three participants decided to have a broader view over what has happened over the weekend by selecting a longer time span than the default of 24 hours – only the option of 7 days was only implemented but some of them would have liked to see what has happened during the last 3 days when they were out of the office.

   The “Average ticket” section was not clear for a lot of the participants who either expressed their confusion or just ignored it completely. One participant considered it a useful feature that should illustrate what is the solving time of the critical events.

   “Ticket by status” functionality was appreciated by all of the participant and the first things that they were curious about were the open, escalated, and unassigned tickets. They said that it would be a good improvement if these sections would be accentuated by colour so that they would identify them easier. The users expected that by clicking either on the pie chart or on the list on a category that a list of a more detailed view would appear where they would be able to identify which are the tickets that belong to that category, for example, which are the tickets that are still open.

"I would prefer colours for open or unassigned so that I know what are the things that I need to concentrate on. I would like if they could be highlighted somehow." (Participant 4)

The "Active events" by severity section was clear and the participants appreciated how the list was organised by severity, from the critical ones to the ones that have a lower severity and are warnings of informational events. Some of the participants expressed their wish to have the critical and major active events highlighted by using an accent colour.

"I would have liked if the critical events would have been presented in a different colour because I can imagine that if we have 9 critical events that is pretty bad." (Participant 3)

Policy set checks
The participants who were familiar with the concept of "Policy set" understood what the related scores are, but one observation regarding the design is that the participants identified the visuals as a list, not as a horizontal bar chart.

An important lesson that was learned from this interview is that there are some policy sets that are more important for a system than the others. That is why one of the participants mentioned that a customisation of the list would be a good improvement.

"I typically would like to keep an eye on some policy sets, for example Access control or Password management, so if I could put them into my preferred order that would be great" (Participant 4)

"Pending updated" was not commented by the participants. They said that it is an interesting feature to have and they correlated it to the release of a new catalogue of policies.

Compliance check section was confusing for the majority of the participants. They tried to add the percentages at first, but no relevant result was obtained. Some of them realised after further analysis that next to the percentages there are the explanations of the results in text and that they can change the range of the scores for the compliance score.

All of the participants started to examine the dashboard to get the state of the system and they were expecting to see something highlighted or coloured in case the system was in a critical state. They reported that their conclusion is that the system is in a good state. One opinion of a participant regarding the content of the first dashboard is: *"If I am the boss, it is too detailed; If I am the middle manager it is good; If I am the analyst, I need more details"* (Participant 3)

2. What would be the first thing that you would check?
For the second task the approach differs from one participant to another, but all of them stated that they would proceed with the most critical issues that present a high risk. The following quote describes the attitude of all of the participants:

"If I start working on something Monday morning that would be the negative side of numbers. I see what is not ok and I focus on that." (Participant 2)

Participant 1 said that his approach would be to start with the critical events, to see what they include and try to solve them, followed by investigating and trying to improve the low scores of the policy set checks. Participants 2 and 5 described a similar approach to this problem. Participant 3 stated that he would investigate the critical events, but the second action that will be performed is understating why there was a compliancy score drop during the weekend. Participant 4 had a different approach by starting with the tickets that are opened and unassigned, followed by further examination of the results of the policy set checks. Participant 6 said that the first thing that he would do is try to solve the events with the highest risk, but he would like to have what nodes or assets are affected by these events mapped to the events themselves.

3. Do you see any major changes that happened during the time that you were away? Which are the days with the peak number of incoming events? What are those numbers?

The participants were not able to identify this in the first dashboard and they were confused. The mediator explained to them how they can go to the second dashboard from the menu.

All of the participants were able to successfully complete the task, identifying the peak number of incoming events, as can be seen in the table below.

Table 8:Distribution of results for task number 3 by participant

Participant	P1	P2	P3	P4	P5	P6
Completed	Success	Success	Success	Success	Success	Success

An interesting finding regarding the way in which the users interacted with the event history and their expectations is that they expect not only to relate to the chart Types of events, which breaks down the number of events by category. They expect also to be able to find out at any given point on the chart what the corresponding number of events. Another wish that was expressed by the participants is that if they select the dot (with the value of 1310 in this case) that the Real time events would update according to the selected section.

"If I click at a certain point in the first chart, I would expect that it would be highlighted or reflected also in the type of events chart. If there was a peak, were all of the registered events the same type or what is the relevance?" (Participant 5)

4. Identify the lowest compliance score of a policy set and get more details about that.

As it can be concluded from the table below five out of six participants managed to identify the lowest compliance score. They had different opinions and suggestions regarding the page that presents the policy set details but as it is not relevant to the dashboard design, the analysis of that part will not be performed in this master thesis.

Table 9: Distribution of results for task number 4 by participant

Participant	P1	P2	P3	P4	P5	P6
Completed	Success	Success	Success	Success	Success	Fail

5. Create a summary of the activity of the team from the last week. What would you include?

Five out of six participants managed to create a summary of the team activity. Participant five, who did not complete the task, did not understand the requirement and he described what he would add from the dashboard in the report, without actually going through the download process. About the naming of the button, “download report”, one participant said that it was confusing, and he was not sure about clicking it: *“Create report would work better, it would be less confusing”* (Participant 1)

Table 10: Distribution of results for task number 5 by participant

Participant	P1	P2	P3	P4	P5	P6
Completed	Success	Success	Success	Success	Fail	Success

The common information that was added by the five participants are the tickets by status, the activity by status and the compliance histogram. During the discussion they raised the problem of the length of the report and the intended target group. They would prefer the report to contain all the details, in which case they would include everything, even in more details than the current option, but in case there is a short report, in that case that would add only the relevant information. They also said that the compliancy score in the defined range is a very relevant information that can be presented in a report. The content of the report depends also on the people that will read the report and the content for the upper management would be different that the one that would be presented to the team. When they were asked in which format they would prefer to have the report, the most common answer was pdf.

Some interesting suggestions that were made by one participant are that the selection of dates should be allowed from a calendar and that there should be a personal configuration of the setting applied for the report.

“I would like to have a calendar from which to select the dates because it might be also that I would like to make the report for the other week, for two or three weeks back, or for a longer period of time” (Participant 4)

“I think that this is a good way of creating the report just by pick and choose what to add. If I could even store my settings, that this is kind of a weekly report for my team, this is my weekly report for my manager, then I could just apply the settings.” (Person 4)

Another pertinent suggestion that was made by one of the participants is including the average solving time of events by category, as the critical events should be solved faster than the ones with a lower risk:

" I would like to also see some more statistics for each category of the events because if it is a critical event than it should be solved faster, if it is a major than it doesn't have to be solved that fast and if it is a warning, it doesn't matter how much it took to solve that one. If it is a critical event that has been resolved, then what was the average time? That is what is typically measured for the customer." (Participant 3)

The results of the task 3, 4, 5 show a good effectiveness result with one task that was completed by all of the participants, and the other two tasks that had a success rate of 83,3%, with only one participant that was not able to complete the task. Because of the small number of tests, only six, the results are not so reliable and even if the result is favourable, further testing should be performed to determine the effectiveness of the dashboard.

4.6.2 General Impressions of Participants

1. Which one of the two presented dashboards do you think you would use more for your work?

   The answers provided by the participants can be divided into two separate categories and they are describing either an approach or a preferred dashboard according to the role. Some of the participants stated that they would start with the "Activity review" screen for a better overview and that they would move next to the "System status" dashboard, which offers them more in-detail information. They declared that more time would be spent on the second dashboard as it provides more information that would offer a clear image of the context and of the steps that have to be performed next. Participant 5 even affirmed that *"I am a technical guy who likes details"*

   The other participants explained that in their vision and from their experience, the preference depends upon the role that the person performs. They stated that the managers would prefer the "Activity review" and the analysts would prefer the System status dashboard. This answer validates our hypothesis and proves that the persona method was appropriate to use. Participant four answered to this question:

   "Depends on the role. If I am in the SOC, on a daily basis I will use the System status more as my daily tool, really seeing what has happened but as a manager, or if I want just a quick overview, then I would use the Activity review dashboard. Exactly when I come to work, as a landing page I would like to see the Activity review page. I think that we need dashboards as they have a different level of details."

2. What are the main problems and difficulties you have found while using this prototype?

One problem that was identified by a high number of participants is that the compliance graph was missing a timeframe which would make it easier for them to identify the exact time when the drop and the fix happened. Another issue that was confusing for the users was that the results of the compliance check that had scores in a certain boundary. This feature has to be studied further to understand what the true value of it is and if the problems were in the way the information was displayed or at the core of the functionality.

Another issue that was identified by the participants in the System Status page is the lack of interactivity on the graph and that clear relationship was not defined. They would expect that if something is selected in the event history graph, that would be reflected also in the other tiles and the information would be updated accordingly. Also, in the same chart, they would like at each given point in time to be able to find out the number of incoming events.

3. What or which functions have you liked most of the prototype? Why?

   Participants really appreciated that the urgency of the issues were colour-coded in the interface so that they could identify quickly what was the first thing that they should start working on. They have also liked the ease of creating reports by only selecting what to include from the dashboard. The functionalities that were offered were appreciated but the most appreciated elements were the ones presented in a graphical format, such as a pie chart showing the status of the tickets and the graphs displaying the compliancy history, events history and types of events.

   "I like these elements that resemble a traffic light and that from the first sight I can identify if is good or bad. I like also that we have some graphs and I think it has to be a mix of different elements, not just lists, tables or graphs. If everything's the same, it gets boring and if I have only similar things, like lists, then I get so tired that I do not even see the changes anymore" (Participant 4)

   "I like that the urgency is colour coded. That makes it easy to see what is wrong and also, that you can sort the events by risk, by severity and by the number of affected devices. Also, from the "Activity review" page it is really good that you can see the total number of tickets, but I think that the details are more important for this." (Participant 3)

4. Can you describe your overall experience with this prototype?

   Overall, all participants described their experience as good. Some participants mentioned that they liked the division of elements into different blocks as it makes it feel well organised and clear. Some participants stressed the good integration of many useful functions and some mentioned that it is clear that a lot of thinking and work has been put into the design. However, some of the participants would like to customise the system, to make it more familiar and useful.

5. How did you like the user interface design?

   The users praised the design and found it simple and good looking. They liked the new implemented design in the dark theme and the only improvement that was requested by them was to accentuate more with the accent colours the urgent issues of the critical events. They found that the division by tiles helped them to identify easily and quicly what they were interested in. One of the participants even appreciated that the relevant metrics were in a bigger format so that they can be observed faster: *"I like in general the percentages in bigger figures I can spot some items really because of big numbers."* (Participant 4)

6. How would you evaluate the set of functions being offered in the prototype?

   The set of functions that were offered in the prototype were very well received by the participants. They evaluated the functionalities according to their daily work and to their experience. The opinions are quite diverse. Some functionalities such as the average ticket were not understood by all of the participants but some of them said that that functionality is very useful to have. A full answer of one participant: *"It is at the border of being too much. The UI is well structured by blocks which gives it a sense of clarity and the views do not feel too overcrowded by information. If we would add even one more feature, then I think it would be too much."* (Participant 4)

7. What would you improve in this prototype?

   The thing that was mentioned numerously by the participants as an improvements that they would like to see is customization of the dashboard, regarding the positioning of the elements, the content that is displayed, and the personal settings. Another wish that was expressed by the majority of the participant is a clear relationship between the elements on the "System status" page. They asked for a clear identification of the events that cause the peaks of incoming events in the other sections, such as the list of real time events.

8. If you had one wish free, what or which function would you like to have for such a system?

   None of the users had any suggestions for additional separate feature that should be integrated into the design, only on how the existing features should be improved.

4.6.3 SUS results

Achieved SUS. score: **75,83** (standard deviation: 15,48)
The above average SUS score of 75,83 indicates a high feeling of satisfaction, above 68 which is considered the average score for the SUS survey. The standard deviation of 15,48 is high, a result of the very different ratings among the participants, ranging from 57,5 to 87,5 as it can be seen in the table below:

Table 11: Distribution of SUS results by participant

ID	P1	P2	P3	P4	P5	P6
SCORE	77,5	65	57,5	82,5	87,5	85

The distribution of the answers of the participants are displayed in the following table:

Table 12: Distribution of SUS answers by question

	Strongly disagree	**Disagree**	**Neutral**	**Agree**	**Strongly agree**
	1	**2**	**3**	**4**	**5**
1	0	0	0	5	1
2	2	3	0	1	0
3	0	1	1	2	2
4	3	2	0	1	0
5	0	0	2	4	0
6	0	5	1	0	0
7	0	0	1	3	2
8	3	3	0	0	0
9	0	0	2	2	2
10	1	4	1	0	0
	Strongly disagree	**Disagree**	**Neutral**	**Agree**	**Strongly agree**

Analysing the distribution of the answers from the table, it can be observed that for the majority of the questions there is no strong commitment to the statement but more of an agreement. Some of the statements that incline to a clear and uniform opinion of all of the participants are statement 1 and 8.

The first statement, “I think that I would like to use this website frequently”(Brooke, 1996) got a positive answer from all of the participants, with four answers of agree and one of strongly agree. From the start of the discussion that took place during the test, the users considered the dashboard as being a point of reference for the state of the system.

The eight statement “I found this website very cumbersome/awkward to use.”(Brooke, 1996) got all of the answers disagree or strongly disagree, result that might be also due to the fact that all of the participants are technical persons that have years of experience in working and developing different systems. One valid comment that was made a participant is that clicking on the prototype developed in Figma was confusing and not very intuitive.

The number of participants is low for obtaining a significant result and for identifying a trend in the answers. The questionnaire helps us to understand if there is an additional problem that was not identified in the previous parts of the testing session. Some outliers that have been identified are in the answers to the second question, “I found the system unnecessarily complex”(Brooke, 1996) where one of the participants rated this statement with agree. The same issue can be identified also in the answers of the fourth statement, “I think that I would need the support of a technical person to be able to use this system”(Brooke, 1996) where one of the participants agreed with the statement while all the others disagreed or strongly disagreed with it.

4.6.4 Proposal of improvement

The following table presents improvements that should be considered for the next iteration of the design:

Table 13: Proposal of future improvements presented by topic

Topic	Improvement
User Interface	Include time frame to the compliance history graph.
	Highlight with accent colours the tickets that are opened, escalated and unassigned.
	Use accent colour to display critical events that are still active.
User Control	Offer the possibility to customize the list of the of Policy checks by relevance to the user.
	Offer customization options for the information that the tiles display and also for the position of the tiles on the interface.
Navigation	The navigation between the two dashboards should be improved.
Functionality	More details on the tickets by status. Offer the possibility to identify which are the tickets that are in each category.
	The average ticket time should be visible for each severity category. A general average of all of the severity categories is not relevant.
	Ability to dig deeper in the active events by severity. The user should be able to click on each category and get a different view where to see a list of those events and what is their status.
	The user should be able to see at any given point in time, what is the number of incoming events by clicking on the graph.
Additional Functionalities	The relationship between the events history and the types of events, real time events and the other tiles should be visible. The users requested that they would be able to identify which are the events that happened at a given point in time by selecting on the histogram.
Research	Identify what is the standard relationship between the tickets and the events. Determine if a ticket is created manually by someone and it refers to several events or each event is automatically transformed into a ticket.
	Investigate more and evaluate the need of displaying the section Assets requiring attention on the dashboard.

In general, we can argue to have achieved good results with the first iteration of the design. From the positive feedback that we got for the usefulness of the system; we are confident to say that this would be the right way to proceed further. The next step consists of implementing the improvements that were presented above and then validating the improved design. For the next validation session, an appropriate method for validating should be decided on. One lesson learned from this usability test is that, because of the different backgrounds and daily activities of the participants, they considered different features as important and they could evaluate the utility only of the functionalities that they had encountered in the past. A proposed approach would be to have all the participants present so that their vast and diverse knowledge could be utilised.

5. Discussion

The abstract nature of cybersecurity combined with the socio-technical interferences the immense impact and constant changes of ways of fighting cybercrime make this topic extremely complex to grasp. (de Bruijn and Janssen, 2017).

From the testing sessions that have been performed on the designs it has been validated the theory presented in the paper "Visual Filter: Graphical Exploration of Network Security Log Files" (Stange *et al.*, 2014). The theory states that SOC experts need an interface that offers both explorative browsing as well as focused search that can be used in the situations in which the security experts have to discover the root of the problem and to develop strategies to achieve their goals.

As presented in the study "I know my network" (Goodall, Lutters and Komlodi, 2004) the interviews and studies performed on the subject should be accompanied by naturalistic observations to capture the behaviour and the tacit knowledge of their daily activity.

5.1 Limitations Encountered in the Design Process

Cybersecurity is a very complex topic and as presented in the literature review, the topic of Security Operation Centres and the way in which they operate has been thoroughly studied before starting with the design. The theoretical information that was gained was validated with a round of interviews with experts that are currently working in this area. The interviews took place via a telecommunication application, which limited the interaction between the two parties, and it made it impossible for the interviewer to capture the non-verbal communication including body language.

Due to this approach, the time spent by the designer with the targeted user was limited and not all of the topics could be clarified. One constraint that was experienced due to the method that was used to gather information about the users is that the users could not be observed in their natural environment. The understanding of the user's workplace was constructed from the answers given by the participants in the interviews. The setting of the teams differs considerably, based on the funding that they obtained, on the importance and on the magnitude of the team. Particularly for analysts, it is important that the designer has a clear understanding of the environment and how the workspace improves the activity of the team. One distinct element that was discussed in the interviews was the number of screens that each member of the team possesses, the display off additional screens located on the wall and what information is displayed on them. Another topic that was covered was the tasks performed by the individuals and by the team. The limitations of the interviews are that the designer does not have the opportunity to see how the user is performing the daily tasks, what prioritisation is assigned to the task, and how the collaboration is within the team members.

Concluding from these limitations and dilemmas encountered, the interviews should have been accompanied by an observation session. During these sessions, the researchers would spend time with the team and would observe their behaviour, their interactions, and the activities that they perform. There are different methods that can be used for the observation, such as contextual inquiry, naturalistic observation, shadowing or participant observation, but the appropriate method has to be chosen after careful consideration of all of the advantages and disadvantages. The usage of observation, as involvement on one-on-one level implies more resources – money and time – invested in the user research.

5.2 Promising Future Development Directions

The first improvement that has to be implemented in the second iteration are the changes that have been analysed and presented in the previous chapter "Proposal of improvement". The changes that have been proposed at the user interface level can be implemented without a considerable effort and without any additional investigation on the topic. The Navigation issue that has been identified will be solved by integrating the current navigation design that is found through the rest of the product. The next improvements that will be mentioned require performing additional research in order to determine the best approach that would satisfy the needs of the users and can be technically implemented. Regarding the degree of user control, additional studies have to be performed in order to determine what level of customization is required from the user interface. During the interviews, the participants expressed their wishes to customize certain functions within the application with certain personalised settings and preferences or to have the possibility to change the layout of the tiles according to their particular needs. The benefits that would be gained from each type of customisation have to be analysed and more literature research must be conducted on how other cases of dashboard customisation has been completed. The other functionalities that have been requested refer to the ability of investigating deeper and obtaining advanced details. For this issue, the functionalities and the corresponding screens have been designed but they were not linked in the prototype, while others have to be thought and developed from scratch.

The most problematic issue that requires further research is the identification of the relationship between the tickets and the events. Starting with investigating the way in which the tickets are created and the way in which the events are categorised as relevant items that would require attention, the study should also consider how this features and relationship would be integrated in the context of the existing application.

Following the implementation phase of the second iteration of the prototype, a validation should be performed. For the validation process on the improved prototype, a different approach should be taken. Because of the complexity of the system and of the area that the product tries to cover, some of the options that should be taken into consideration should involve all of the participants being present and evaluating the product at the same time. Facilitated workshops or focus groups would be some viable options as they involve cross functional team members and the problem is tackled from different perspectives. For the future iterations and validation, the implication of the final client should be also taken into account as it might bring to light different issues that have not been identified with the tests performed in the organisation.

6. Conclusion

In this work the applicability of a design system in the in the development of a cybersecurity dashboard was studied. By applying user-centred design methods the needs, goals and behaviour patterns of the user can be identified and the requirements for the dashboard can be constructed. A first iteration of the deliverable was achieved, and the user's feedback was favourable regarding the manner in which the information was divided by role in terms of the functionalities were implemented and the visual design was presented.

6.1 Answers to the research questions

Two main research questions have been posed in this master's thesis:

- What is the role of a dashboard for cybersecurity professionals?

  The first thing that had to be established from the literature review phase was the concept of a dashboard. Four fundamentals that had to be considered in the dashboard were defined and they claim that the dashboard should have clear and explicit goals, should integrate in the context of the application or system that it is a part of, that it should accommodate the appropriate visualization elements, and that the content should not exceed a single screen. Apart from the fundamentals, eight categories have been defined that help in the phase of structuring the dashboard. This category includes the purpose behind the dashboard, the time horizon of the activity that is presented to the viewer, the degree of interactivity and control, the point of view in which the data is presented, the method in which the data is acquired and span of data, and the triggers that initiate the interaction with the dashboard.

  The second issue that was identified by performing a literature review and empirical research is the particular needs of cybersecurity experts in regard to a dashboard. The requirements have been defined based on user research that incorporated interviews with Security Operation Centre experts in which the theoretical information was validated, and behaviour patterns and goals have been identified. As this is a technical field, the behaviour patterns and the goals associated mapped to the professional roles that are in such a team. The step that followed the interviews was the modelling phase in which the personas have been defined.(Cooper, Reinmann and Cronin, 2007) By using the persona method and performing the user research, the designers were able to deepen their understanding of the domain, of the behaviour, goals, motivation and workflow patterns that are followed by the team. Having a suite of personas helped the team to make sure that the user needs are appropriately addresses and to articulate the degree of flexibility needed for each functionality identified as needed. (Mccolgin, Gregory and Elsevier, 2008) By performing the designation of the persona types, two primary design targets have been identified: analyst and manager. The two user types have different responsibilities, motivations, and end goals, that is why the dashboards have different purposes: operational for the manager, presenting an overview of the system and of the activity of the team that he is coordinating and strategic for the analyst, presenting the most urgent issues that require immediate intervention. The outcomes of the usability testing session that was performed on the prototypes developed are that the defined personas are relevant and illustrate the real needs of the team members and that both of the two dashboards are necessary. Every team member should have access to the two dashboards as they offer different perspectives over the activity.

- How does the Design System approach support cybersecurity dashboard development?

  The development of the dashboard studies also the ability to apply the design system on the requirements defined. The particular design system of the case company was analysed, and the goal was to determine the suitability of the principles on a cybersecurity product and the diversity of the elements implemented. By performing research on the design system documentation, the most appropriate theme for the dashboard was the dark theme, as the perceptual design has been created for technical people, for dashboards that are used for long periods of time as it reduces the eye strain and enables a better ability of assimilating data. The accent colours were used to increase the importance and the urgency of certain events and actions.

  By using the elements that the design system provided and having all of the requirements defined, the creation of the final design of the prototype was straightforward. Although not all of the visual encodings needed in the dashboard were present, the freedom that is offered to the design team to create new elements following the rules predefined gave us the opportunity to construct new components and still maintain the consistency of the product. The final design accomplished by adopting the design system was genuinely appreciated by the participant in the usability test and the tangible and aesthetic features had a salient impact on the user experience.

7. Appendices

7.1 Appendix 1: Interview with SOC experts

About the person

1. Please give us a little background on you and your job. (education, since when do you work at your current place, why)
2. Please walk me through your typical working day.
3. What kind of tasks are you responsible for? (tasks, time, size, interfaces) (Daily scan/ Compliance check/ Troubleshooting)
4. What is the process that you are following? (How it escalades from SOC Level 1 to SOC Level 3)
5. What is the area of responsibility for monitoring? (Global / Local)
6. How do you keep yourself "up-to-date" with the new vulnerabilities? (Eg. Start the day by examining a collection of blogs & websites to find new vulnerabilities
7. Are there any particular elements which you have to keep an eye on during the day?

About the environment

8. What kind of alerting tools or websites do you use?
9. How often do you check them?
10. How critical is the information on those?
11. What is your next step after that?
12. For what kinds of tasks do you use dashboards?
13. What would be the most important things that you would like to see on a dashboard?
14. In what context (when you open your computer / on the / the state of the system)?

About the job

15. What is the best thing about your job? What do you like best?
16. What do you like least with your job? What is the most stressful part?
17. What skills are required to do your job?
18. How did you get into security? (school/ self-taught/ games)
19. What do you like about this field the most?

About the tools

20. What tools/applications are you using to complete your tasks?
21. What do you like, and what do you dislike about those tools?
22. Approximately how much time does it take to complete such a task?
23. What does completion mean in this case? What do you do with the information once you got it?

7.2 Appendix 2: Usability Test Dashboard

Hey. My name is Andra Cimpan and I am going to be walking you through this session today. My colleague Virag will help us by taking the notes.

Before we begin, I have some information for you, and I'm going to read it to make sure that I cover everything.

INTRO

You probably already know why we asked you to come here but let me go over it again briefly. During the last months we have been working on creating a new concept of dashboard that would suit the needs of our users and we would like to do a first usability test in order to validate the prototypes.

DURATION

The session will take about 60 minutes and I'll break it into 3 parts. In the first part we will take a look at the application where I'll ask you to perform some given tasks on the prototype. In the second part I will ask you some general questions regarding the system that you experienced followed by the last part, in which I will ask you to fill in a survey.

TESTING THE APP, NOT YOU

The first thing I want to make clear right away is that we're testing the applications, not you. You can't do anything wrong here. Also, the current system is just a prototype and not all the functionalities have been implemented.

THINK OUT LOUD

As you use prototypes, I'm going to ask you as much as possible to try to think out loud: to say what you're looking at, what you're trying to do, and what you're thinking. This will be a big help to us. Also, please don't worry that you're going to hurt our feelings. We're doing this to improve the applications, so we need to hear your honest reactions.

QUESTIONS

If you have any questions as we go along, just ask them. I may not be able to answer them right away, since we're interested in how people do when they don't have someone sitting next to them to help. But if you still have any questions when we're done, I'll try to answer them then. And if you need to take a break at any point, just let me know.

PERMISSION TO RECORD

With your permission, I'm going to record what happens on the screen and our conversation. The recording will only be used to help us figure out how to improve the app, and it won't be seen by anyone except the people working on this project. And it helps me, because I don't have to take as many notes.

QUESTIONS?

Do you have any questions so far? OK. Before we look at the site, I'd like to ask you just a few quick questions.

TASKS

1. You are coming to work Monday morning and get straight into work.
   Can you describe the state/status of the system after the weekend?

2. What would be the first thing that you would check?

3. Do you see any major changes that happened during the time that you were away? Which are the days with the peak number of incoming events? What are those numbers?

4. Identify the lowest compliance score of a policy set and get more details about that.

5. Create a summary of the activity of the team from the last week. What would you include?

QUESTIONS

1. Which one of the two presented dashboards do you think you would use more for your work?

2. What are the main problems and difficulties you have found while using this prototype?

3. What or which functions have you liked most of the prototype? Why?

4. Can you describe your overall experience with this prototype?

5. How did you like the user interface design?

6. How would you evaluate the set of functions being offered in the prototype?

7. What would you improve in this prototype?

8. If you had one wish free, what or which function would you like to have for such a system?

6. Bibliography

Abomhara, M. and Køien, G. (2015) *Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks, Journal of Cyber Security*. doi: 10.13052/jcsm2245-1439.414.

Adobe XD (2019) *Adobe XD User Guide*. Available at: https://helpx.adobe.com/xd/help/design-systems.html%0D%0A%0D%0A.
Alla-Kholmatova (2017) *Design Systems*. Edited by S. Magazine. Smashing Media AG (October 15, 2017). Available at: https://www.amazon.com/Design-Systems-Smashing-eBooks-Kholmatova-ebook/dp/B076H49W1G.

Alper Sarikaya, Michael Correll, Lyn Bartram, Melanie Tory, and D. F. (2015) 'What do we talk about when we talk about dashboards?', *IEEE Transactions on Visualization and Computer Graphics*. Available at: https://research.tableau.com/sites/default/files/DashboardsConspiracy_final.pdf.

Atlassian (2019) *Atlassian Design Principles*. Available at: https://atlassian.design/guidelines/designPrinciples/design-principles.
Blackstratus (2019) *What is a Security Operations Center and Why Is It Important?* Available at: https://www.blackstratus.com/what-is-a-security-operations-center-and-why-is-it-important/ (Accessed: 25 February 2019).

Bohemia, E., Liedtka, J. and Rieple, A. (2012) *Leading Innovation Through design*. Available at: https://s3.amazonaws.com/academia.edu.documents/40692530/Leading_Innovation_through_Design_Procee20151208-21966-ccwlds.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1536082216&Signature=NJX6R%2FQTiMjZVdosPkoSUSSoK90%3D&response-content-disposition=inlin.

Brooke, J. (1996) 'SUS - A quick and dirty usability scale', in *Usability Evaluation in Industry*.

de Bruijn, H. and Janssen, M. (2017) 'Building Cybersecurity Awareness: The need for evidence-based framing strategies', *Government Information Quarterly*. doi: 10.1016/j.giq.2017.02.007.

BSA The Software Alliance (2016) 'The $1 Trillion Economic Impact of Software', (September). Available at: www.bsa.org/softwareimpact.
Chauncey Wilson (2014) *Interview Techniques for UX Practitioners*. 1st editio. Morgan Kaufmann.

Chen, C., Hrdle, W. and Unwin, A. (2008) *Handbook of Data Visualization (Springer Handbooks of Computational Statistics), Handbook of Data Visualization*.
Christopher Alexander, Sara Ishikawa, M. S. (1977) *A Pattern Language: Towns, Buildings, Construction*. Oxford University Press.

Cooper, A., Reinmann, R. and Cronin, D. (2007) *About Face 3.0: The essentials of interaction design, Information Visualization*.

Dawson, J. and Thomson, R. (2018) 'The future cybersecurity workforce: Going beyond technical skills for successful cyber performance', *Frontiers in Psychology*, 9(JUN), pp. 1–12. doi: 10.3389/fpsyg.2018.00744.

Enanv, S. I. S. *et al.* (2010) 'International Standard', 2004.

Ericsson (2018a) 'Ericsson anual report', p. 208. Available at: www.ericsson.com.
Ericsson (2018b) *Ericsson Design System*. Available at: https://brandhouse.ericsson.net/en/home.

EY (2014) 'Security Operations Centers — helping you get ahead of cybercrime', (October), p. 20. Available at: http://www.ey.com/Publication/vwLUAssets/EY-security-operations-centers-helping-you-get-ahead-of-cybercrime/$FILE/EY-security-operations-centers-helping-you-get-ahead-of-cybercrime.pdf.

Faulkner, X. (2000) *Usability engineering*. Palgrave.
Few, S. (2006) *Information Dashboard Design, O'Reilly Press*. doi: 10.1017/S0021849904040334.

Fink, G. A. *et al.* (2009) 'Visualizing cyber security: Usable workspaces', in *6th International Workshop on Visualization for Cyber Security 2009, VizSec 2009 - Proceedings*. doi: 10.1109/VIZSEC.2009.5375542.

Goodall, J. R., Lutters, W. G. and Komlodi, A. (2004) 'I Know My Network: Collaboration and Expertise in Intrusion Detection', *ACM conference on Computer supported cooperative work*, pp. 342–345. doi: 10.1145/1031607.1031663.

Gray, D. *et al.* (2015) 'Improving Federal Cybersecurity Governance Through Data-Driven Decision Making and Execution', (September). Available at: http://www.sei.cmu.edu.

Griffee, D. (2005) *Research Tips: Interview Data Collection, Journal of Developmental Education*.
Hámornik, B. P. and Krasznay, C. (2018) 'A team-level perspective of human factors in cyber security: Security operations centers', *Advances in Intelligent Systems and Computing*, 593, pp. 224–236. doi: 10.1007/978-3-319-60585-2_21.

James Waldo , Herbert S . Lin, and L. I. . M. (2007) *Toward a Safer and More Secure Cyberspace*. Washington, D.C.: National Academies Press. doi: 10.17226/11925.
Lewis, S. (2015) 'Qualitative Inquiry and Research Design: Choosing Among Five Approaches', *Health Promotion Practice*. doi: 10.1177/1524839915580941.
Limcaco, J. (2019) *Design Systems Gallery*.

Maurya, A. (2012) 'Running Lean: Iterate from Plan A to a Plan That Works', *Science of Aging Knowledge Environment*. doi: 10.1126/sageke.2002.20.nw68.

McAfee and Intel Security (2016) ‘Creating and Maintaining a SOC’, *McAfee Labs*, pp. 1–16.

Mccolgin, D., Gregory, M. and Elsevier, B. V (2008) ‘VizSEC 2007’, (February). doi: 10.1007/978-3-540-78243-8.

Muniz, J., McIntyre, G. and AlFardan, N. (2015) ‘Security Operations Center: Building, Operating, and Maintaining your SOC’, 2, p. 448.

NASA (1976) ‘National Aeronautics and Space Administration Graphics Standards Manual Index Introduction 1 The NASA Logotype 2 Reproduction Art 3 Stationery 4 Forms 5 Publications’.

National Institute of Standards and Technology (2013) *NIST Cybersecurity Framework*. Available at: https://www.nist.gov/cyberframework/online-learning/components-framework.

Norman, D. A. (2009) ‘Emotional design’, *Ubiquity*. doi: 10.1145/985600.966013.
Pawar, M. V. and Anuradha, J. (2015) ‘Network security and types of attacks in network’, *Procedia Computer Science*. Elsevier Masson SAS, 48(C), pp. 503–506. doi: 10.1016/j.procs.2015.04.126.

Ponemon, I. (2017) ‘2017 Cost of Data Breach Study, Global Overview’, *IBM Security*.
Pyrhönen, E. (2019) *Hack the design system.* Idean Publishing. Available at: idean.com/learn.

Roca, S. F. and Cited, R. (2006) ‘Systems and methods for the detection and management of network assets’, 2(12). doi: 10.1038/incomms1464.

SANDOVAL, R. (2018) ‘Intelligent Security Operations: A Staffing Guide’. Available at: https://www.microfocus.com/media/white-paper/intelligent_security_operations_a_staffing_guide_wp.pdf.

Sauro, J. and Lewis, J. R. (2016) *Quantifying The User Experience. Practical Statistics for user research, Morgan Kaufmann*.

Stange, J.-E. *et al.* (2014) ‘Visual Filter: graphical exploration of network security log files’, *Proceedings of the 11th Workshop on Visualization for Cyber Security*, pp. 41–48. doi: 10.1145/2671491.2671503.

Tom D’Aquino (2018) ‘How to Build a Security Operations Center (On a Budget) | AlienVault’. Available at: https://www.alienvault.com/resource-center/ebook/how-to-build-a-security-operations-center.

UX Collective (2019). Available at: https://uxdesign.cc/.
Yigitbasioglu, O. and Velcu, O. (2010) ‘Dashboards in performance management: The foundations and research opportunities for their effective use’, in *Proceedings of the 5th International Conference Accounting and Management Information Systems: AMIS 2010*.