TALLINN UNIVERSITY OF TECHNOLOGY

School of Information Technologies

Reno Špitsmeister 201727IVSB

Implementing a SOAR Solution in a Security Operations Center on the Example of Cybers

Bachelor's thesis

Supervisor:	Risto Vaarandi
	PhD
Co-supervisor:	Aleksei Zjabkin
	BSc

Tallinn 2023

TALLINNA TEHNIKAÜLIKOOL

Infotehnoloogia teaduskond

Reno Špitsmeister 201727IVSB

SOAR-lahenduse rakendamine turvaseirekeskuses ettevõtte Cybers näitel

Bakalaureusetöö

Juhendaja:	Risto Vaarandi
	PhD
Kaasjuhendaja:	Aleksei Zjabkin
	BSc

Tallinn 2023

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Reno Špitsmeister

10.05.2023

Abstract

This thesis explores the implementation of Security Orchestration Automation and Response (SOAR) in a Security Operations Center (SOC) to address the challenges of cybersecurity faced by organizations. Despite the benefits of SOAR, many organizations struggle with its implementation. The thesis outlines the advantages of SOAR and identifies the criteria that a SOC should meet before implementing it. It also examines the reasons why organizations and service owners fail in implementing SOAR. A working SOAR implementation methodology is developed and tested in a real Managed Service Security Provider's (MSSP) SOC. The thesis aims to provide valuable insights to help organizations make better decisions when implementing SOAR to enhance the effectiveness and efficiency of their SOC. This thesis is written in English and is 52 pages long, including 4 chapters and 2 figures.

Annotatsioon

Käesolevas lõputöös uuritakse *Security Orchestration Automation and Response* (SOAR) süsteemi rakendamist turvaseirekeskuses (SOC), et lahendada organisatsioonide ees seisvaid küberturvalisuse probleeme. Vaatamata SOARi eelistele on paljud organisatsioonid selle rakendamisega hädas. Töös kirjeldatakse SOARi eeliseid ja määratakse kindlaks kriteeriumid, millele SOC peaks enne selle rakendamist vastama. Samuti uuritakse põhjusi, miks ettevõtted ja teenuseomanikud SOARi rakendamisel ebaõnnestuvad. Töötatakse välja toimiv SOARi rakendamise metoodika ja testitakse seda ühe reaalse *Managed Service Security Provider* (MSSP) SOCi puhul. Lõputöö eesmärk on anda väärtuslikke teadmisi, mis aitavad organisatsioonidel teha paremaid otsuseid SOARi rakendamisel, et suurendada oma SOCi tõhusust ja tulemuslikkust. Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 52 leheküljel, 4 peatükki ja 2 joonist.

List of abbreviations and terms

AI	Artificial Intelligence
API	Application Programming Interface
GUI	Graphical User Interface
IMS	Incident Management System
ISO	International Organization for Standardization
MITRE ATT&CK	MITRE Adversarial Tactics, Techniques, and Common Knowledge
ML	Machine Learning
MSSP	Managed Security Service Provider
POC	Proof of Concept
POV	Proof of Value
ROI	Return on Investment
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SOAR	Security Orchestration, Automation, and Response
SOC	Security Operations Center
SOCaaS	Security Operations Center as a Service
XDR	Extended Detection and Response

Table of contents

List of figures

1 Introduction

With the relevance of cybersecurity rising each day, new problems erupt which heed for solutions. The technological level of tools is rising while the complexity of usage is getting lower. This creates an attractive environment for lowly skilled threat actors entering the fray. Following online guides or documentation is more than enough to conduct successful attacks. Furthermore, the tools are automated and can cause effect in a brief time.

Most often the cybersecurity specialists on the defending side belong to a Security Operations Center (SOC). This is a team consisting of analysts, engineers and some other key people integrated together with backing technology and processes. SOCs are suffering under a lack of manpower, skills, and efficient solutions. As the need for cybersecurity professionals defending from threat actors is higher than ever, the blue team needs to equal the playing field. The problem is that maintaining a team of cybersecurity professionals is expensive and finding new people is hard. At the same time the attackers, like terrorists, usually do not require large funding and time is on their side.

Moreover, many security operations rely on old documentations, protocols, tools, and processes. Security teams are often dispersed and disorganized. They have a wide array of tools without a cohesive way of using them effectively. This is why the defenders need to integrate fresh solutions and processes into daily operations to equal the playing field.

There is a relatively new tool to combat these problems called Security Orchestration Automation and Response (SOAR). It provides vital orchestration to unify security tools and their actions. Despite the numerous benefits of SOAR in enhancing the efficiency and effectiveness of SOCs, its adoptions rates are low, and many organizations continue to struggle with implementing it and are thus fighting a losing battle.

The main goal of the thesis is to develop an implementation methodology for SOAR and describe the application of this methodology by successfully implementing a SOAR in an Estonian Managed Service Security Provider (MSSP) Cybers' SOC.

First, the advantages of SOAR will be outlined, and a criterion defined, which a SOC should have prior to implementation. Secondly, the thesis will look at the pitfalls and reasons why businesses and service owners fail at implementing SOAR in their SOCs. Based on the findings, a working SOAR implementation methodology will be developed and tested.

The thesis aims to be unique and valuable by assembling the necessary research into a single document to help other organizations make better decisions when it comes to SOAR tool implementation. To back up the theoretical basis the thesis presents, an implementation with post-analysis is made on a real MSSP's SOC.

2 Related works and background

2.1 SOC and SOAR

Cyber threats are more actual than ever. It is no longer the case if a breach will happen, but instead when it will happen. Defenders have been struggling to resist due to lacking resources, time and being understaffed. The percentage of professionals with good skills is low. [12]

SOC can be defined as a combination of the people, technology, and processes to assure cybersecurity proactively and reactively in an organization. The security personnel are conducting procedures and tasks by using a wide variety of security tools to improve and maintain cybersecurity posture. [1]

Preventing incidents is done by doing proactive work using threat intelligence and patching vulnerabilities. The main method of detecting is done via continuous monitoring – using solutions like Security Information Enterprise Management (SIEM) or Extended Detection and Response (XDR) to analyse logs collected from monitored devices in a central tool. The solutions are used to identify threats, create alerts, and tune the detection rules. If an incident has happened, SOC will respond to it and conduct remediation actions – starting with scoping the incident, isolating endpoints, and finishing with recovery and lessons learned. [2]

Organizations can have their own internal SOC team, or the service can be outsourced from a MSSP. Building and maintaining an internal SOC from scratch is an expensive and challenging task, requiring a large investment. Thus, many smaller organizations outsource the service.

Security tools often create a lot of alerts and investigating these alerts requires a lot of manual repetitive actions. This is a huge time sink which will consume much of the security operations time, even for a staffed and experienced SOC [12]. Investigating many alerts, you are racing against time to see if there is a real incident in one of the alerts.

There is a solution to combat these difficulties, SOAR. SOAR is something that can help with incident response, security automation, case management and orchestration of the tools at your disposal. SOAR is not a magic piece of software, but instead aligns people, process, and technology [12].

When looking at the underlying security orchestration and automation concept, we have several definitions for it. For example, Microsoft has said [5]: “Security Automation is the use of information technology in place of manual processes for cyber incident response and security event management” and “Security orchestration is the integration of security and information technology tools designed to streamline process and drive security automation”.

Forrester has defined security orchestration and automation as follows: “Technology products that provide automated, coordinated, and policy-based action of security processes across multiple technologies, making security operations faster, less error-prone, and more efficient” [4].

Coined by Gartner in 2015, SOAR initially stood for security operations, analytics, and reporting [8], the definition further changed throughout the years. Currently, 2022 Gartner market guide [6] defines SOAR as “solutions that combine incident response, orchestration and automation, and threat intelligence platform management capabilities in a single solution. SOAR tools can be used for many security operations tasks, including: - To document and implement processes. - To support security incident management. - To apply machine-based assistance to human security analysts and operators. To better operationalize the use of threat intelligence. Workflows can be orchestrated via integrations with other technologies, and automated to achieve desired outcomes.”

SOAR tool itself is a relative newcomer to the scene, but it is not a revolution in technology. In a way, it is scripting with a graphical user interface. Anything done in a SOAR can be done with scripts. SOAR tools simplify and bring the required skill level down when developing, orchestrating, and automating workflows. SOAR tool complements SIEM by providing the automated response to automated detection.

As the definitions said, SOAR seeks to combine different capabilities into a single platform, focusing on security incident response and overall automation of security operations. Effectively implementing SOAR, its individual components reduce the strain on security teams.

The large security stack that is constantly increasing is difficult to manage and use effectively. The specialists tend to spend a lot of time hopping between the security tools. Orchestration helps different components across a complex infrastructure to work together in a unified manner, thus freeing valuable time for the security team to do what is important. By having everything in a centralized platform, automating these tools to interact with each other is the next logical step. Automation eliminates the time-consuming manual actions. The human aspect in cybersecurity has always been the weakest link. The same is occasionally true for the cybersecurity defenders as well. Doing repetitive tasks amidst the overwhelming number of alerts, things will go unnoticed and wrong. By correctly implementing automation in a SOC, the error prone human element can be reduced. Response provides the ability to detect, investigate, respond, and remediate security incidents from start to end with minimal or no human interaction. [3]

In a non-automated SOC, the mean time to detect and investigate can vary greatly and depends on the capabilities of the human analyst. In other words, the performance of the human element is unpredictable and incomparable to machine’s processing power. For humans, it may be a struggle to meet the Service Level Agreements (SLA) on time, as the workload increases, or other actions require attention. This is a problem that SOAR does not have, the mean time to do the initial investigation is measurable in seconds, something humans are not able to compete against. It is already an important improvement if SOAR can help with the initial investigation and triage. This helps create a clearer view of the situation and brings the analyst’s attention to the more critical alerts.

The same is true for the next measurable times – act, respond, and resolve. Depending on the configured SOAR’s capabilities, the actions can be taken at incomparable speeds. This improves the overall security posture of your organization, ensuring faster reaction to potential threats. By using fast and automated workflows to deal with incidents, the maturity and reputation of the organization rises. This is especially important for service providers, by having good security posture, they can build trust and credibility in their clients.

2.2 SOAR workflows and automations

When looking at the types of workflows which can be developed and deployed with the help of SOAR, there are options for different use cases with varying levels of human interaction.

When looking at the human aspect in security workflows, there are three options [22]:

a. Manual workflows (a series of manual tasks)
b. Semi-Automated workflows (a hybrid of automated and manual subtasks)
c. Fully Automated workflows (completely automated)

When first deploying SOAR and finding out what works for the SOC, semi-automated workflows should be opted for. This ensures that the machine actions are supervised, and humans are still in control of the outcomes. This is also the way to go for empowering the SOC analysts, augmenting them with automated subtasks within a larger workflow. Fully automated workflows must be carefully considered before deploying high fidelity processes which can be automated with high confidence.

When talking specifically about SOAR dealing with security alerts, following automation are proposed [22]:

a. Defensive Automation (prevent the threat or risk)
b. Forensic Automation (retrieve additional evidence)
c. Offensive Automation (pro-active and reactive actions on assets)
d. Deception Automation (retrieve or adjust deception tools)

And three actions [22]:

a. Enrichment (investigations, collecting data, performing lookups)
b. Escalation (report to humans)
c. Mitigation (perform actions to resolve)

The enrichment part is the most time consuming for SOC analysts and something that is relatively easy to automate. By combining it with escalation, important SOC metrics, such as mean time to investigate and resolve, are tackled, and successfully lowered. Whether the mitigation aspect requires human confirmation to apply or is automated, the result is still more effective than fully manual intervention.

2.3 Statistics, predictions, market state

Cybersecurity Ventures claimed in 2023, that there are about 3.5 million cybersecurity positions unfilled globally [18]. Furthermore, the number of unfilled positions has grown by 350% in ten years and this trend is expected to continue in the coming years. The unemployment rate of experienced cybersecurity specialists has been zero since 2011. The field is rapidly expanding and the skill requirements constantly evolving. The employers are seeking highly qualified, yet scarce workers to fill important roles. SOAR is seeking to make a difference in the widening gap inside security teams. The technology has become sophisticated enough to start helping security experts to do cybersecurity.

According to Gartner in 2019, "by year-end 2022, 30% of organizations with a security team larger than five people will leverage SOAR tools in their security operations, up from less than 5% today" [13].

Gartner's 2022 market guide stated that mature and larger security teams and service providers make up the main consumer of SOAR. They use the tools for improving efficiency, productivity, and consistency in Security Operations. The main drivers for SOC adoption are staff shortage, alert overload, and complexity of cyber threats. Automation in the SOAR is the primary capability to resolve the problems. The main use cases Gartner brings out are SOC optimization, threat monitoring, investigation and response, and Threat Intelligence management. [7]

Gartner claims the SOAR is growing increasingly prevalent in the industry and the market is slowly expanding beyond the large mature organizations. The SOAR role for MSSPs is especially crucial because they can optimally respond to threats. Large SIEM vendors are also creating add-on SOAR solutions alongside their SIEMs for extra cost. [7]

A 2022 survey by Cynet [19] analysed responses from 200 small company CISOs. In this survey, 94% of the respondents reported having barriers to improve their security posture.

The common barriers which SOAR also aims to combat are the lack of skilled security personnel (40%), excessive manual work (37%) and lack of integration (orchestration) between security tools (16%). There were also the issues regarding managing policies across multiple point solutions and having multiple cloud providers, which are related to the orchestration aspect.

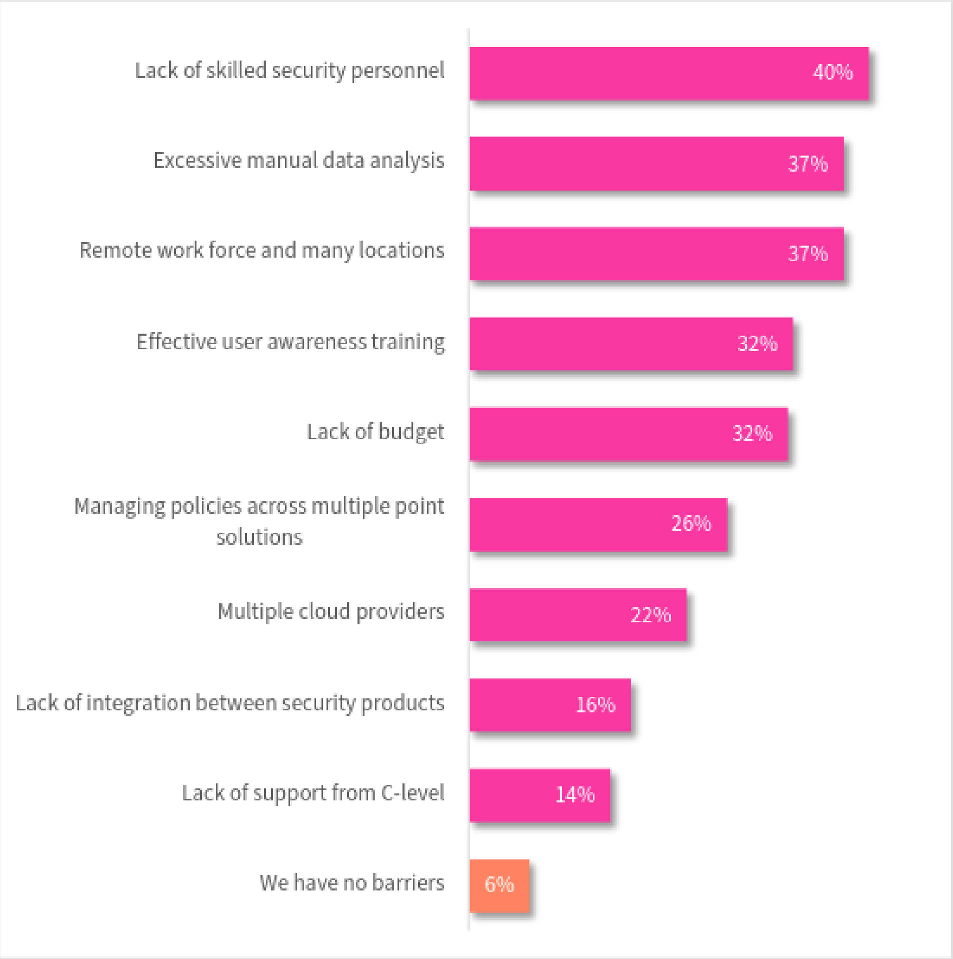

Figure 1. Top Barriers in Maintaining Security Posture. Cynet 200 CISO survey [19]

Comparable results can be observed from SANS 2022 SOC survey, where the top barriers were caused by high staffing requirements and lack of skilled staff, automation, orchestration. [25]

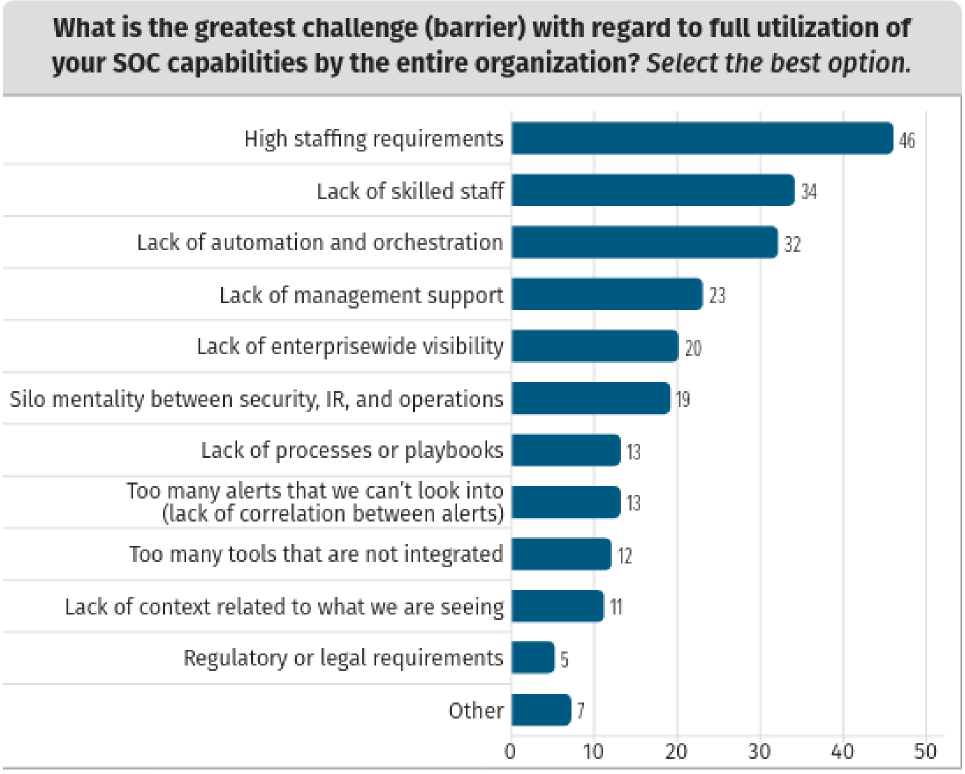

Figure 2. Challenges to Using SOC Capabilities (n = 235) [25]

This large quantity of unfilled positions rising in the future cannot be solved by finding cybersecurity specialists which do not really exist. A faster and more effective solution is needed to combat the deficit of manpower. SOAR is a way to relieve humans of time-consuming manual tasks through raising efficiency and doing automations. The security experts can instead focus on solving the advanced challenges and tasks, ultimately decreasing the amount of total security personnel an organization needs. Still, not to forget that SOAR still needs someone to actively manage the tool and ensure it is running as expected. The most important part about a SOAR is the configuration, this task should be done by a dedicated person or a team. Experts effectively controlling the SOAR should be able to do the work of many others.

According to market research [17] the SOAR market is expected to double from 2022 with a value of USD 1.1 billion to USD 2.3 billion in the next 5 years. The compound annual growth rate being 15.8%. One of the prevalent reasons is the large gap in unfilled cybersecurity positions, which are not possible to be filled due to the lack of experts. Automation is expected to help address this issue. Cynet's 200 CISO research [19] also found out, that currently 5% of responders are using SOAR, while 90% responders reported plans to buy a SOAR or expressed willingness to consider buying it. Just 5% did not have any plans for SOAR.

2.4 Testing and deploying SOAR tools

There was research conducted in US Navy SOC in 2022 [11], where the authors tested SOAR solutions in practice. According to authors, this topic has received almost no attention in prior academic research literature, and mostly the focus has been on SOCs without the SOAR solutions. The research [11] fills this gap and provides the first experimental framework to evaluate and compare SOAR solutions. The practical test involving 24 participants evaluated 6 SOAR solutions in a cyber range test environment. It was found that the main criterion for success is the correct SOAR configuration, which facilitates user success and work performance of the SOAR. It was found by senior participants that SOAR tools can indeed over-automate SOC processes. SOCs should opt for semi-automated workflows, as uncertainty in cybersecurity is inevitable. The workflows should prompt the user for confirmation to complete the investigation with the correlated and presented data. [11]

In 2022, a thesis by Lalos [14] looked at three different large vendor SOAR products to compare and investigate in a test environment. The thesis showed how these SOAR tools work, how they compare to one another and what are some of the practical ways you can utilize them. A conclusion the work made was that the tier 1 security analyst was not replaced by the SOAR, but instead made the analyst more efficient and effective by removing the burden of repetitive tasks. The SOAR empowered analyst remains to counter emerging threats. [14]

Doing a decent job at configuring the software is no doubt a challenging task for an expert. This brings us back to the irony of automation [15], as it is no different for a SOAR, “The more we depend on technology and push it to its limits, the more we need highly-skilled, well-trained, well-practised people to make systems resilient, acting as the last line of defence against the failures that will inevitably occur”.

Karu wrote in her thesis in 2021 about Cybers’ SOC [9]. More specifically analyst workflow was described, analysed, and a redesign was proposed. A SOAR solution called

TheHive (open-source free software at the time) was analysed and usage possibilities in Cybers were presented. The work focused on the analyst's point of view and finding opportunities to improve that. This is at the time of writing the only academic writing focusing on possible SOAR implementation and usage at an Estonian cybersecurity provider. [9]

Zamora has written and shown in his work [16] how to deploy TheHive SOAR as well. Several SOAR tool demo versions were compared and evaluated to find the most suitable one for the company to deploy. Two roads were also suggested, you either buy an expensive vendor’s proprietary SOAR or choose a cheaper (open source) SOAR option and accept the fact that you must have a dedicated person to develop and work with the SOAR. The author did note that TheHive does not market itself as a SOAR, but it does possess the components to act as such. However, to use it as a SOAR a lot of custom modifications are required. All the automations must be manually scripted and the interface to do that is not no-code. A reference to another tool called Shuffle is given as an alternative to develop automations in a no-code way. The work proposed a TheHive-based solution deployment with detailed descriptions on how it could be done. [16]

2.5 ML/AI in SOAR

To solve the main problems SOCs have, the idea of expanding Artificial Intelligence (AI) use in SOAR systems has been explored [10]. Using deep learning, threat detections are made and then discriminated whether a reported threat is a true or false positive. Such a model is already actively used in Network Intrusion Detection systems. Human assistance is still required since the tools need daily tuning and updates. The end goal is to use AI to tackle the areas where human intervention is needed the most. Overall, the reason for using AI in automated detections and responses is not to detect using known signatures, but to be able to react to threats unseen before. [10]

The conventional anti malware solutions relied on signature-based detections; this is something AI/Machine Learning (ML) has changed and revolutionized. AI/ML systems have proven to be able to deal with large data sets and identifying anomalous and suspicious patterns faster than any human can [13]. The idea of using them for detection phase has been implemented with success. [13]

Where the SIEM goals (identification and detection) end, the SOAR begins [13]. The machine handled incident response process is not an easy thing to accomplish, especially due to the constantly evolving complexity of threats. SOAR system is not meant to replace skilled security analysts, because deploying SOAR to get rid of human element would create more risks. The traditional human-in-the-loop (HITL) model of the man machine relationship is not sufficient to use in cyber security, because the tasks need to be carried out quickly in the dynamic cyber defence environments. Human-on-the-loop (HOTL) model has instead been suggested [13], which allows the machine to autonomously perform tasks while the analyst monitors and intervenes only if it is necessary. SOAR should be looked at as the force multiplier for the analyst, allowing them to work more efficiently due to the capabilities of ML/AI, thus providing value for the whole organization. [13]

SOAR should be applied to empower SOC to reduce mean time to detect, investigate, respond and act - the critical metrics for cyber threat detection, mitigation, and prevention efforts. This also creates a more appetizing return on investment for SOAR systems. The goal of using machine learning and AI by SOAR vendors is in early development, but to make it trustworthy and effective, a lot of work needs to be done. [13]

2.6 SOAR tools on the market

When looking for a SOAR in the market, there are quite a lot of product options, and the selection is growing fast.

According to Gartner’s Critical Capabilities for SIEM 2017 report [20], it was envisioned that SOAR should be a natively integrated part of SIEM. Thus, also being capable of handling and responding to detected incidents either by automated or assisted workflows. There are still several ways vendors have approached the SOAR concept. Some vendors do include native SOAR in a SIEM, such examples are LogRhythm, Exabeam and Microsoft Azure Sentinel.

On the other hand, Gartner [7] has pointed out that large SIEM vendors have created the most popular SOAR’s. To get the maximum value, they are meant to be bought and used alongside the same vendor SIEM platforms. Still, these SOARs are optional and are an additional large expense. Such tools are for example Splunk SOAR, IBM Security QRadar SOAR, Siemplify and Rapid7 InsightConnect. Another market leading commercial SOAR platform is Palo Alto Cortex XSOAR, aiming to orchestrate with all other security tools.

It is important to note that commercial products also offer community editions and free trials, which are not meant to be deployed in production, but rather a way to test their functionality. There are also open-source SOAR solutions, which aim to offer a standalone platform to integrate with any other SIEM or security tools. It is hard for open-source SOARs to compete with commercial counterparts due to limitations in advanced features, maintenance, scalability, and vendor support. SOAR implementation is a long and expensive process which depends on the vendor by a lot. Currently, in 2023 there is just one open-source SOAR solution able to compete with commercial solutions. It is called Shuffle and is inspired by the NSA’s WALKOFF. WALKOFF itself is a SOAR product by NSA, which was discontinued in 2019 due to lack of funding. Shuffle’s goal is not to offer the SIEM+SOAR experience but focus only on the orchestration and automation aspect as a separate tool.

2.7 Mapping research on the topic

In previous academic works, the failures and problems faced when implementing SOAR are not well described. The steps prior to technical deployment have been overlooked. There have been works where SOAR implementation has been proposed, but the vital aspects and questions related to a SOC maturity have been ignored or not well described, which is important to look at to understand whether SOAR is a viable problem solver in that case or not.

Most of the implementation works have focused on TheHive “SOAR,” which was free in the past, but is no more. Moreover, TheHive is a Security Incident Response Platform (SIRP) and while it does have some SOAR capabilities, it is not considered a full-fledged

SOAR solution. SOAR solutions typically offer more advanced automation and orchestration capabilities than TheHive does. Starting with a wide range of built-in integrations and having more advanced scripting and workflow automation capabilities. The line between SIRP and SOAR can be blurry, and it depends how each vendor differentiates between them. For some organizations, TheHive capabilities may be enough, while others require a more advanced and capable SOAR solution.

Therefore, the current thesis will investigate the aspects of SOC maturity one should evaluate before opting for implementing a SOAR. The issues that are happening during the SOAR implementation are looked at to better understand the obstacles organizations may face. Additionally, a real implementation of a SOAR solution will be conducted in a company specializing in offering SOC services to its clients.

3 Development of the SOAR implementation methodology

3.1 Maturity criteria

Before considering the implementation of a SOAR, several other key aspects need to be thought through and analysed. Even though SOAR is a tool, which is being adopted at a rapid pace, as of today, it is not by any means a tool that everyone needs. It is also important not to forget that SOAR systems need a great deal of personalized configuration. The default configuration SOARs come with is not enough to use these tools in production environment. Each infrastructure is unique, and SOAR needs to be well configured to successfully communicate and execute actions with all the security tools across the network. Organizations need to carefully evaluate and consider the readiness of their people, technology, and processes before deploying a SOAR system [23].

Every SOC is different, but having a framework makes assessing the situation and implementing tools easier [24]. It is important to understand your current security posture, because if this is unknown it is hard to know in which direction to improve or how SOAR could help to improve the existing capabilities. To measure the overall level of an organization's SOC maturity, for example the SOC-CMM [26] assessment can be taken. However, the SOAR technology is listed as a single capability in the assessment.

3.1.1 SOAR in a new or a mature SOC?

SOAR is usually adopted by mature SOCs with experienced SOC teams who have extensive knowledge on their SOC’s operational issues. They have the knowledge of their processes and can imagine how to improve them by utilizing SOAR. Their goal is to multiply their efficiency with SOAR. However, there have been organizations which successfully implemented SOAR from day zero of their SOC [21]. In the case of starting a SOC with SOAR, you will need to heavily depend upon the maturity of the SOAR tool itself. As commercial solutions do have many predefined workflows, using them can be feasible, since no custom processes are holding you back. The onboarding process by SOAR vendor can also help with, even by using external consultants to build the SOAR in SOC [29]. Implementing SOAR in a new SOC is an exceedingly challenging task, but also rewarding if successful. Although it is recommended to grow your SOC through maturity stages before deploying SOAR, it will take a lot of time and that is exactly what is tried to be bypassed when adopting a SOAR from day zero [21]. In this thesis, the focus will be on integrating SOAR with a mature SOC, which is a far more common SOAR deployment scenario.

3.1.2 Do you need to improve SIEM/XDR or deploy SOAR?

Sometimes SOAR may not even be the solution a SOC needs. There are problems that are better solved elsewhere. If for most of the time SOC is preoccupied with investigating and responding to meaningful SIEM/XDR alerts, then a SOAR deployment can be considered. However, if the SOC is overwhelmed with enormous amounts of low fidelity of data and alerts, then the problem should be looked at from another angle. In these cases, it is better to invest in overhauling the SIEM/XDR ecosystem to produce meaningful detections.

The maturity of the SIEM/XDR platform must not be overlooked. As SIEM has been the main security tool for creating alerts and investigating them, the current trend has also been towards using XDR in place of SIEM due to its ability to create higher fidelity security alert data. Nevertheless, they must be trustworthy to use SOAR to act upon the alerts with great confidence. The SOAR solution should be tightly integrated with the SIEM/XDR solution to successfully perform the investigations [22]. This means being able to pull additional related logs, effectively use the required fields in the logs and consider the severity of SIEM/XDR alerts when doing further actions and escalations. If a SOC has a lot of uncertainty and false positives created by countless amounts of unique rules, automating the cases one by one will be difficult, very time consuming and not feasible. In other words, to automate something, a clear manual process must be known [22].

3.1.3 People, process, and technology.

The people aspect is the source of most frustration in an SOC. This is due to lack of skill, personnel and because of human irrationality and the nature of being prone to errors. In the case of SOAR, the human element is of utmost criticality to get it implemented, managed, and operating. People need to possess the skills to successfully complete security investigations, evaluate risks and respond to incidents. When a SOC decides to deploy SOAR, it means the people need to be able to support and use SOAR to get value out of it. It is a sophisticated tool which requires a motivated team seeking to get the most out of it.

Automation is about automating processes. Gartner’s SOAR market guide has stated that the main obstacles of SOAR implementation are unclear or undefined incident management processes and procedures in a SOC [23]. The manual processes need to exist and be consistent when dealing with each unique use case. By having a clear process on how to investigate and respond to the alert, the automation of both the investigation and mitigation of the alert is achievable [22]. The processes, starting from mundane tasks to advanced investigations - must be known and clearly defined to be implemented as automatic workflows. Furthermore, workflow development in an ongoing process and the standard manual incident response methodologies should be employed, which also means the post incident lessons learned are of critical importance to be evaluated and workflows in SOAR updated. It is also beneficial if frameworks like MITRE ATT&CK are already integrated in manual workflows to be used in SOAR.

Technology is the aspect where SOAR intends to make a significant difference. The orchestration of scattered tools is one of the key benefits of SOAR. However, for SOAR to do that, the tools must be ready for that. This means proper configuration and integration capabilities of the tools is a prerequisite. For example, it is crucial to have strong integration between SIEM/XDR and SOAR to effectively detect and investigate alerts. Additionally, it is necessary to have a case management solution that can work in tandem with SOAR and support bidirectional collaboration between the SOAR system for the SOC analysts. To enable fluent work, the visibility coverage and data fed to the SOAR must be sufficient to rely on. In the end, the important criterion for this is a strong API compatibility in the existing technologies, since this is what SOAR utilizes.

3.1.4 Business compatibility

The SOAR is a relatively expensive security tool, which may be an issue when justifying its value to the management and having enough funds in the budget to implement it and not to forget, constantly maintain and develop it after initial implementation. Due to this, the budget of an SOC should be considered. This is especially true in small and medium organizations, where the SOC budget is typically not enough for a commercial SOAR. A business case could be created for SOAR implementation. This document is used to explain how the return value of a project overweighs its costs and why it should be done.

To determine whether a SOAR solution complements your business needs, the current and future operational problems need to be evaluated. Factors such as SOC size, security environment complexity and the number of alerts and other tasks your team has need to be accounted for. By knowing this, the level of automation and orchestration the organization needs are clearer.

A more specific and important metric relevant for this is ROI. It should include the cost savings from automating tasks (savings on labour costs) and the potential improvement in security posture. In cybersecurity there is a lot of unknown, and the rough statistics regarding historic incidents and impacts are not trustworthy to make predictions upon. The ROI should be evaluated to determine whether the investment could provide a return and how soon. A hidden cost saving is in the potential security breaches causing significant financial losses, which could be mitigated by the fast response by a SOAR. Finally, the benefits of enhanced security and improved SOC metrics are difficult to quantify in monetary terms, but they are crucial for ensuring security and business viability in the industry.

To conclude, here are the main points to assess and think about when considering the organization’s overall maturity:

- Consider assessing overall maturity of a SOC
- Readiness (skills and time) to maintain and develop SOAR workflows (People)
- Mature manual processes and procedures (Processes)
- Well configurable tools (over API) to be orchestrated and automated by SOAR (Technology)
- Mature SIEM/XDR with meaningful detections and appropriate visibility (Technology)
- Budget for SOAR implementation and later development

- Understanding if SOAR is able to assist with your SOC problems
- Beneficial return on investment (ROI)

3.2 Where do things go wrong?

SOAR implementation is not a very straightforward task and before actually getting to the tool deployment, several preparations and analyses must be done. SOAR implementation may have several obstacles that need to be overcome. There are many connections between the slow or failed SOAR implementations with the maturity criteria. A SOAR implementation can be a complex process that requires careful planning, effective integration, and skilled resources. Organizations need to be prepared to overcome common implementation challenges.

3.2.1 Common mistakes organizations do

Upon analysing the previously given maturity criteria and additional articles [27-30], the following common mistakes organizations do can be outlined:

[Mistake 1] Poor planning and execution

Before venturing into the SOAR implementation, a carefully crafted plan with clear objectives must be created. Without understanding what exactly the organization seeks to achieve by implementing SOAR, it will be difficult to follow through upon and issues such as securing the finances, selecting the right solution, or prioritizing tasks and resources will cause problems during implementation.

SOAR deployment errors start with the planning phase. Organizations tend to underestimate the complexity of the implementation process and the obstacles that they may face at SOAR implementation. Bad planning and execution can cause delays or even critical problems which are not worth overcoming. It is important to appoint a dedicated person responsible for the successful SOAR implementation and further operation.

[Mistake 2] Personnel lacking skills and motivation

The organization's security teams do not always possess the skills and competencies required for a smooth and on-time SOAR deployment. The personnel need to have security expertise and technical proficiency in areas such as scripting, automation, system administration and project management. They also need to have problem-solving skills to troubleshoot issues and optimize the SOAR for the organization's unique needs. Without these skills, delays and difficulties will be faced and finding these competencies outside the organization (consultants, new hires) will be an additional cost and time loss. During the selection of the SOAR tool, the skills of the employees need to be considered, since there are different tools with varying number of built-in capabilities and coding knowledge requirements. Choosing the right one for the skillset the organization has is vital.

Furthermore, the personnel must be motivated to accept and use this new technology. The importance and benefit of it must be made clear to the personnel, otherwise there may be resistance to the change. Resistance may cause delays, increased costs, and overall complicate achieving the desired goals during implementation and further use.

[Mistake 3] Lacking SOAR functionality and integration

Each SOAR tool is unique and careful consideration should be made to avoid unexpected missing functionalities. This may be due to the SOAR missing built-in integrations, workflows or even functionality required to do them by yourself. It may very well be the other way around – the existing tools failing to integrate with SOAR even though they were a goal of the implementation. Integrations can prove to be complex and lengthy tasks requiring custom work by the organization. Usually, the lacking functionality can be created on demand by the organization or vendor, important to understand that this needs time and budget.

[Mistake 4] Lack of stakeholder buy-in

It is important that the management is on board with SOAR implementation, and this is also a step where many attempts fail due to insufficient funding, limited resources, or lack of management support. SOAR is a comparatively expensive tool with significant impact, it requires overhauling processes and requires time and work from many people. Without the buy-in from the stakeholders, it will be difficult to follow through with the implementation.

[Mistake 5] Overinflation of expectations

Organizations tend to expect that buying as expensive software, they are getting a SOC in a box and no further investment is needed. Organizations should not expect to automate everything with SOAR, automation is not always the answer to operational problems. Not everything should be automated, some problems require to be solved at source. A balance between machine-driven and analyst-driven operations must be found for each SOC.

Buying and deploying SOAR are just the first steps in a larger process, no results can be expected immediately. Even after creating the workflows, one should not expect them to be developed once and forgotten. They require constant tuning and improvement. The threats and software keep on evolving and constant maintenance must be done on SOAR. Furthermore, the workflows should be constantly tested to ensure they remain up to date against constantly evolving threats. For a SOAR to fully meet an organization’s needs, there is no doubt a significant amount of work needs to be done by the organization itself.

It is important to understand what a SOAR can do and what not. The expectations and capabilities must be discussed and matched with the SOAR vendors.

3.2.2 What is Cybers and their attempted TheHive implementation

Cybers is a MSSP to a wide variety of clients in the Nordic-Baltic region. One of their most important offered services is 24/7 Security Operations Center as a Service (SOCaaS), which is one of the objectives this thesis aims to improve.

In 2021, there was a proposal to adopt TheHive into Cybers technology stack along with reworked SOC analyst procedure [9]. TheHive at that time was looked at as a SOAR platform capable of making the analyst work more effective by automation, case management and debatably response. Truth is, TheHive is today classified as a SIRP platform meant to fulfil similar, but not exactly SOAR goals (common misconception talking about TheHive). It can empower the SOC analysts to be more effective when it comes to investigation, minimizing some repetitive actions and collaboration, but the fact is that orchestration of security tools along with automated responses is something TheHive is not meant to do out of the box. This is also something Karu mentioned in her work [9], TheHive at that time was a young project and much of the automation functionality was envisioned, but not implemented. The main ready-made automation aspect TheHive succeeded in was automating threat intelligence for observables lookup. The SOAR concept described in the current thesis goes beyond what TheHive accomplished. SOAR is not limited to case management and threat intelligence automation but aims to orchestrate an organization's security tools with their infrastructure and processes for comprehensive security automation.

An alternative to TheHive SIRP is an Incident Management System (IMS) with scripts empowering it. The alternative IMS Cybers was already using was Jira service management, which is proprietary software with moderate cost per person each month. This was acceptable for smaller SOCs (especially with sharing accounts), but as personnel grew, the subscription cost would increase. The upside of TheHive was that it was free, and it did not matter how many people were working there. For an expanding SOC it was a reasonable option.

IMS however, was still what Cybers opted to go for instead of TheHive. This decision had several reasons, and it was further justified by later developments. Most notably, it was unexpected that TheHive would not offer a free viable solution to professional SOCs in the future, as it initially had gained popularity due to being an open-source contender. Spending resources to migrate onto TheHive would today either mean being locked there with large subscription fee or starting development of a yet another solution. TheHive5 license for an MSSP costs about 20,000 euros per year, and this would have cost roughly two times more than Jira licenses, with the actual deployment further increasing the costs.

As Cybers used Jira service management as their IMS and as the main analyst tool for managing incidents, collaborating, and reporting previously, it was already personalized to some extent and was fulfilling almost the same goals. It was decided to continue with using the IMS solution as the main analyst tool. TheHive implementation did not outweigh the current working solution since the migration and development for such an important technological solution would have been a considerable investment. Karu also focused [9] on the fact that adopting the solution would mean large demand for engineer development. Beyond development, learning a new tool will inevitably be costly for the analysts and administrators alike. There were other business priorities, and the ROI was not enough to proceed with it. Jira was instead developed with further capabilities throughout the years to offer the same functionality as TheHive offered.

To summarize the errors, the main reason for not fully implementing the tool was in unclear use case and lack of focus due to questionable ROI (Mistake 4 from previous section). TheHive did not possess the necessary capabilities to demonstrate its uniqueness and usefulness (Mistake 3). The difficult part for security teams is also to adopt new and unfamiliar tools if a solution is already doing almost the same thing (Mistake 2).

Likewise, the important learning steps here would be to carefully consider and evaluate what is exactly that your team needs and what is the best way to solve it. The use cases must be defined before starting to look for a SOAR tool. When organizations decide whether to adopt a new tool, the ROI needs to be evaluated. If there is low added value, but excessive cost when implementing the tool, then it may not be approved. The cost of just the licenses is one part of the investment needed, the other is the time personnel needs to invest for learning the tool to effectively use it.

3.3 Successful SOAR implementation methodology

For the proposed implementation methodology, the previously analysed pitfalls and maturity criteria will be considered. Additionally, the methodology will take inspiration from existing works on the topic [24, 31] and internal Cybers sources focusing on the industry best practices. The following implementation methodology will be suggested, that has been outlined below:

1. Determine if you really need a SOAR and whether it can help you. What are your expectations for SOAR?
2. Think about the maturity of the organization and SOC, can it manage a SOAR adoption?
3. Create a business case, present it to the management and secure buy-in from the stakeholders.
4. Analyze your SOC and find the use cases SOAR could help with. Set initial workflows that SOAR should first develop.

5. Find a SOAR tool suitable for your organization. Evaluate and test tools. Consult with the vendor of the tool and get a PoV/PoC if they offer one.
6. Onboarding SOAR to your SOC. Integrating your security ecosystem with SOAR - configure and customize. Implementing initial workflows. Train and educate personnel.
7. Deploy SOAR in production.

3.3.1 Do you need SOAR?

The first step should be to evaluate whether the organization really needs SOAR and whether SOAR can help with the organization's operational problems. What are the issues the organization’s security teams are facing and what are the expectations for SOAR, can SOAR even assist with addressing the problems? Here, the organization’s expectations should be compared with the abilities of SOAR systems to reduce the risk of over expectations. The following questions should be answered to determine whether the project should be continued with. The questions help to understand whether the organization is facing issues SOAR can tackle.

Does your security team get too many meaningful alerts to handle effectively and in a timely manner? The data potentially fed to SOAR needs to be of quality and consistency to be effectively and predictably processed.

Do you have repetitive processes, which could be automated? SOAR can be used to do tasks only if they can be automated.

Do you have security staffing problems, which could be fixed by automation and orchestration? The time-consuming simpler tasks can be shifted to the machine to release resources for more advanced tasks.

Are your processes inefficient or manual, causing delays or errors? By increasing consistency and machine actions in the processes, the time to complete tasks and human error are reduced.

Do you have security tools and systems that are not well-integrated or managed? The orchestration aspect helps to integrate tools into a more logical and efficient structure.

Are you looking to improve your SOC metrics such as mean time to respond, detect and investigate? The improvement of the security posture to deal with cybersecurity alerts.

Would SOAR have an acceptable ROI in your organization? The SOAR may very well be able to solve problems, but it does come at a hefty investment.

3.3.2 Does the organization meet maturity criteria?

In detail, the criteria and considerations are described in the Maturity Criteria chapter. Here is a good place to answer some questions to determine whether the organization is ready. Positive answers to the questions 1-6 are of critical importance to proceed and answers for questions 7-9 are good to have for greater success.

1. What are the exact objectives and goals the SOAR system would need to achieve?
2. Are the operational problems that your security team is facing known?
3. Does your SOC have the necessary skills and resources to implement and manage a SOAR platform, or are you ready to buy this service from external consultants?
4. Do you have the necessary stakeholder support, funding, and resources to conduct a SOAR implementation and keeping it operational?
5. Can your security tools integrate with SOAR over API?
6. Are your manual processes known and consistent, are they ready to be automated?
7. Are you ready to transform current processes and culture to fully reap the benefits of SOAR?
8. Is your SIEM/XDR system mature and producing meaningful alerts?
9. Have you assessed the overall maturity of the SOC?

3.3.3 Create a business case

It is important to create a business case that justifies the investment required and secures stakeholder buy-in [26]. This step is crucial for obtaining the necessary funding and resources to proceed with the implementation. The business case should clearly explain the value proposition of the SOAR system and its potential benefits to the organization. It should involve stakeholders throughout the project to ensure their support and buy-in. The financial maturity of the organization should also be considered in creating the business case, and the results of previous steps should be presented to support the case for SOAR adoption.

Creating a SOAR business case, the following aspects should be analysed and presented.

1. **Define the problem** the organization is facing, which SOAR solution can help to address.
2. **Establish goals and objectives** implementing a SOAR solution.
3. **Evaluate benefits** SOAR implementation gives, both short and long term.
4. **Estimate the cost** of implementing, customizing, and maintaining a SOAR solution.
5. **Project plan** to outline the steps and timeline for the SOAR implementation.
6. **Outline risks** and challenges associated with this project.
7. **ROI analysis** to compare the expected SOAR benefits with the costs.

3.3.4 SOC analysis and initial workflows

During this step, an analysis of your SOC needs to be done. This analysis helps you understand where the key issues and problem spots are which should be first dealt with. Data can be gathered from the ticketing or SIEM/XDR system statistics, talking to the analysts, and hearing out their ideas or even focusing on other goals you have set.

Complex automation should not be implemented in the beginning – the simplest use cases are the best place to start. Another peculiarity to focus on are the noisiest alerts, the ones that are happening the most. If there is a noisy and simple use case that can be automated, it will already be a big win for the SOC if that is done. If the excessive number of alerts are false positive, then, if possible, they should be tuned, as that is a cheaper and more effective solution.

Fully automated workflows are something that should be done after the initial implementation of a SOAR. Initially, the workflows should be semi-automated, requiring human confirmation or supervision during execution [11]. By doing this, the impact and risk of unexpected results is reduced, and the workflows can be complemented on the go.

Considering the latter, the initial workflows should be decided upon and followed through as the first ones to be developed and even tested in different SOAR solutions during the selection process. The possible workflows vary by a lot depending on the SOC and its daily tasks.

3.3.5 Choosing the SOAR

Choosing a SOAR to proceed with will be a longer procedure and a particularly important one. The options need to be carefully evaluated and the best choice made. It is also important to test the tools to get a better glimpse of what they have to offer and whether they suit the organization’s needs. For testing purposes vendors offer community or trial editions. In the case of Cloud based SOAR’s the testing is easier since no deployment or dedicated hardware is needed. Some vendors also offer free guided proof of concept or proof of value deployments to test out their tool; this option should be taken after most of the vendors have been filtered out, as it will need more time to test out.

Functionality and integration capabilities

The interface of the tool should be user-friendly and ensure that it will not be a bottleneck itself when developing workflows and overall using the tool. Being easy to learn also helps with reaching full productivity potential quickly. The SOAR platform functionality affects the analysts and engineers who will work with the tool. The platform must have the necessary capabilities to develop the organization planned use cases simply and successfully. Typically, with SOAR the no-code aspect simplifying workflow creation is significant since analysts will develop the use cases not developers.

It is important to check if the SOAR can integrate with the existing tools if the integrations are already developed and how much functionality they offer. Vendors tend to also offer prebuilt workflows, which could be done with the same security tools you are using, they may even be like the same process which your organization is using. However, if they do not have any prebuilt integrations or workflows for needed security tools, it is important to consider how difficult it is to create them internally or on request and deploy into SOAR. Usually, this is supported, but does require additional resources. These integrations should not be very hard to make if your organization has the skillset for it, rather a question would be will there be any obstacles from the vendor side.

Cloud or on-premises SOAR?

This is an especially important question to ask. Is your organization seeking a SOAR on cloud or on-premises? Not all vendors offer both solutions and if they do there might be differences between the two versions. The trend has been to prefer cloud, but there are organizations for whom cloud is out of the question. Furthermore, the choice is not as black and white as it seems. Sometimes, orchestrating security tools which are either on cloud or on-premises may prove to be difficult. There may be extensive security controls, which need to be reconfigured or some SOAR vendors require an additional piece of hardware to be bought and installed on premises to allow fluent orchestration and execution of workflows between on-premises and cloud security tools.

During selection, security and compliance may be one of the deciding factors. Cloud SOAR may cause compliance and security concerns due to less control. Opening cloud connections from otherwise isolated resources creates additional attack vectors. On the other hand, on-premises SOAR provides complete control over data, SOAR itself, compliance, and security. Furthermore, on-premises SOAR can operate in isolated conditions and without internet. A thorough security assessment is advised for both cases as SOAR plays a crucial role in managing a company's security ecosystem. Compromising the SOAR solution could have severe consequences for business operations.

An advantage cloud SOAR usually offers is scalability. The SOAR solution needs to support the possible fluctuations in workload. A SOAR being unable to do that may cause slow response times, inability to handle tasks due to increased workload and overall decreased productivity bringing down the same metrics SOAR intended to improve. A well-designed solution should be able to support more or reduced resources when needed. This is something hard to achieve with an on-premises physical solution. Typically, the vendor is responsible for maintaining the SOAR, making it easier for the organization, as no resources are needed to deal with the underlying SOAR system itself.

The cost of an on-premises SOAR is generally higher since it requires allocation of computing resources and constant input from the IT staff. Fluctuations can cause unexpected problems and costs as it will be much harder to scale. However, on-premises SOAR may excel in performance depending on the infrastructure. Since it is already located on-premises, the latency and response time are significantly reduced.

Will SOAR be used for incident response management?

Many commercial SOAR systems have made SOAR a central platform to also investigate alerts and manage incidents (case management). To pursue this feature or avoid it is completely up to the organization. If the SOC already has a working IMS able to integrate with the SOAR, then it will probably not be in their interest to migrate onto a SOAR to conduct the same activities there. This would need complete overhaul of processes. Even if SOAR would only be used to conduct investigations on this separate platform, it could be a deal breaker to some organizations. This is because SOCs have already invested considerable number of resources to develop these platforms, likewise the platforms are already fulfilling the same goals that SOAR case management aims to offer. Bringing another platform to analyst toolset to do some investigations or see results in is counterproductive. The organizations see SOAR as a separate component to communicate with existing tools and empower them, not replace them.

On the other hand, if the organization will start to use a SIEM+SOAR solution or is willing to migrate onto SOAR as the all-in-one platform, then it could be a reasonable option. There is demand and market for it, which is why some SOAR vendors offer this functionality and keep it as one of their focus points.

The costs of SOAR implementation.

The most important aspect interesting to all stakeholders is the cost of SOAR implementation and operation. There are two main possibilities when choosing a SOAR solution. It is either a large vendor’s expensive solution or an open-source solution. Both have their pros and cons. A good question to also ask here is whether you need fast time to market or low cost and slow adoption, since this helps immensely when deciding the right tool.

The cost of the SOAR platform license is usually the most significant. Some vendors are offering one-time payment solutions, while others have monthly or yearly subscriptions. The costs vary depending on the number of users, assets, and functionality. The market leader’s solutions are usually priced at more than 100 000 euros a year, making it unreachable for small to medium organizations. The SIRP solution TheHive is going for about 20 000 euros a year; they are offering a free community edition, but that is just not enough for professional SOCs. An alternative option could be an open-source SOAR solution.

The implementation and integration cost includes the initial installation, configuration, and integration. Sometimes the few initial workflows may also be packaged with this cost. It varies a lot depending on the vendor and bought services. Anyway, dedicating resources to SOAR development is something that cannot be avoided.

Training is necessary for the organization's SOC to be able to operate with this platform. The SOC needs to be trained in how to use the platform's features, develop workflows, and integrate the platform with other security tools. Vendor-provided training can help ensure that analysts have the knowledge and skills required to effectively use the platform. If the training is skipped and no in-house experience exists, then relying on external consultants will be much more expensive eventually.

Maintenance and support costs vary depending on where the solution is deployed, who is maintaining it and how much does the service cost. Depending on whether the SOAR is deployed on premises or in the cloud and who is responsible for maintaining it, the costs and processes may vary. The fact is that using any system resources is also an expense that needs to be considered. For proprietary SOAR systems on the cloud, the maintenance responsibility can be shifted to the vendor.

Vendor support

Commercial software is often chosen due to its professional support, which should help the software to be relevant and effective for the client. This gives them confidence that in case something happens they are guaranteed some kind of assistance from the vendor. With SOAR, timely technical support is important and oftentimes critical since a fully integrated SOAR keeps the SOC running. API modifications may cause a SOAR solution to cease functioning, therefore vendors include official API maintenance as part of their support package. When developing workflows and customizing the tool, getting assistance from the vendor should be provided in time and with excellent quality. On the other hand, open-source projects tend to have a helpful community behind them, and this is where you get help with your issues, but you have no guarantees nor SLAs to rely on. The help you can get may take time and delayed downtime is not an acceptable solution. However, there are upsides regarding this part for open-source software as well. Having access and seeing inside the software's source code means that you may be able to figure the issues out yourself, but this further requires that the person responsible for organization's SOAR needs to be skilled and dedicated to the SOAR.

As SOAR is a security tool constantly interacting with sensitive data, it is important that the tool itself is secure. Getting and applying quick patches to fix bugs and vulnerabilities is needed to ensure security and relevance of the SOAR.

3.3.6 Onboarding and post-onboarding

For the onboarding, a plan needs to be made and realized regarding the goals the organization wants to achieve, which security tools to integrate, how to deploy the SOAR and which workflows need to be first made. This process is assisted by the SOAR vendor to ensure everything goes smoothly. During this time, the SOAR will be configured and customized to the organization's needs and work will start to get the tool into production. SOCs initial SOAR deployment should opt for reactive and highly manual workflows. The initial workflows should be to automate the basic and repetitive manual tasks. Some of the use cases could be enrichment (observables or assets lookup), integrating the ticketing (case management) system with SOAR and simpler investigations, like for example some steps of phishing analysis.

It is also wise to start training personnel who will start developing and maintaining the workflows and/or SOAR in the future. After SOAR has been integrated with security tools in the organization's ecosystem, proper configurations made, initial workflows successfully developed and the personnel trained to work with SOAR, the deployment into production can be made and the implementation considered completed.

3.4 Sample Cybers implementation

Following the proposed implementation methodology, the author conducted a SOAR implementation in Cybers to test it in practice. Due to business confidentiality reasons, some information may be presented at a higher level of abstraction and not everything will be explicitly written out or explained.

3.4.1 Goals and objectives

Cybers is taking on new challenges meaning larger scale automations and orchestrations than before; the need for a dedicated SOAR became apparent some time ago. As SOAR is used to make it easier to develop, deploy and maintain automation workflows (scripts), a centralized automation and orchestration platform to complement existing technologies and processes is what Cybers sought.

The set goal for Cybers was to improve service efficiency by introducing advanced level of automation through entire incident response lifecycle. To make SOC service more affordable to small-medium-size customers by delegating repetitive tasks to a machine. At the same time, leverage the security benefits of machines – human error reduction, improved metrics and reducing analyst burnout.

Cybers expects the SOAR to be able to develop and execute automation playbooks, it does not need to have separate interface which analysts use daily. It must be able to integrate with existing security infrastructure and it is good if these integrations are already developed to some extent. As an MSSP, it is especially important that customer support is competent and responsive. As Cybers is a very small company compared to the usual SOAR adopters, the cost must be low and in budget.

3.4.2 Maturity of Cybers SOC

In case of Cybers, the company’s SOC was mature and ready for a SOAR implementation. The problems this tool needed to tackle were known. The in-house experience did exist regarding SOAR and could be utilized. The SOC was ready to invest resources into going through with the process and take additional training for the personnel to successfully develop and work with the tool. The stakeholders were onboard with the project and their support was secured. The security tools which Cybers used could be orchestrated and automated over API. The procedures and processes throughout the incident response lifecycle were known and at the same time the willingness of overhauling these procedures to fully reap the benefits of SOAR was adequate. The SIEM system Cybers is using did produce high fidelity alerts and did have enough data to be fed to SOAR, however for Cybers case, SIEM was not the critical starting point. The overall maturity of the SOC was well known and considered.

3.4.3 Business case and initial workflows

Business case

A business case was created and presented to the stakeholders. It is important to keep in mind that this varies a lot depending on whether the SOC is a service provider to external clients or for the internal clients. In case of Cybers, the case is built from the perspective of the MSSP. The business case had the following contents.

The problem the project intends to tackle is the high cost of a managed SOC service. Due to its high cost, it is not attractive and feasible to small and medium businesses, which make up most of the local market.

The goal is to make the SOC service more affordable to small and medium businesses. To do that, human resources consumption needs to be reduced by efficient orchestration and automation. The tool for that is SOAR. The SOAR's objectives are to optimize all stages of the client cycle: onboarding, providing semi-automated SOC service, billing and offboarding.

As an MSSP, it will provide several benefits. By reducing the number of human resources needed at each step, the SOC can provide the service to more customers on the market without needing to constantly hire more people. As the service becomes cheaper, a wider range of clients can be reached, and it makes the SOC service easier to sell.

The major cost related to the implementation of SOAR will be the development costs - human resources and external consultancy. The operational costs will be vendor costs related to the SOAR licenses, maintenance, support, and resources to keep the software running.

The project in the larger plan is defined by critical timelines and milestones for the minimal valuable product to be on track and ensure the success of the project.

The primary risks associated with this project are related to human competence. These risks can arise from multiple sources, such as the implementation team's abilities, inadequate service from vendors, or the proficiency of analysts and developers working with the tool after deployment. Unforeseen expenses could also cause problems due to resource constraints.

The ROI for the project was calculated by summing development and operational costs and compared to the sales forecast by month. As the exact workflows Cybers is aiming to build are not expected to be packaged with the SOAR's the development cost will remain high with all SOARs.

SOAR use cases, initial workflows

The quest for finding the initial workflows started with analysing the existing SOC processes to find gaps and inefficiencies that could be addressed through SOAR automation. The goal was to start with the repetitive, time-consuming workflows which are simple to develop, but yield value if automated. To identify the workflows, the SOC personnel were interviewed, and SIEM/IMS statistics analysed.

It was decided that there are three workflows which should be done as the initial ones. First being an email phishing analyser, which would be following the same manual workflow as analysts do. This is an important one, since phishing is the most common vector for attack and something that can be automated to investigate and respond to. Secondly the improved enrichment of observables in IMS is a highly requested feature, which is relatively easy to do and yields much value to the analysts. Thirdly, there is a need to synchronise XDR alerts with IMS, which is great to understand the orchestration aspect of the SOAR and is something different from the usual investigations and responses SOAR systems focus on.

The goal with initial workflows is that they do not need to be fully production ready, the fine tuning of these will happen on the fly. Additionally, during the development of these the tool capabilities can be better understood.

3.4.4 SOAR tool selection and testing

SOAR tool expectations

When selecting the SOAR for Cybers, there are essential features that the tool must have. As security analysts are the main users of this tool, it is particularly important that it is easy to use by offering good GUI support when building workflows. It should be a no-code tool, which does not need daily intervention from developers. The SOAR must be able to integrate with the important tools currently in Cybers ecosystem.

The SOAR must have cloud support and it was preferred if the software is hosted and managed by the vendor, thus requiring less resources from Cybers side to maintain it. Due to GDPR and ISO compliance, data must be secured accordingly, and the datacentre must be in the EU.

Due to Cybers being a MSSP, the multi tenancy support of the tool was a critical requirement. As SOAR will be a central component in Cybers' SOC services, it is necessary that the vendor is able reliably provide uptime of the service and in case of any problems with the platform or building workflows, a priority support channel be present. The vendor must also provide technical training for Cybers to be successful at using this tool.

As Cybers itself is a small company, the cost of the tool is a deciding factor, cheaper SOAR vendors are preferred. MSSP's tend to have a wide range of security tools from several vendors, it is important to take this into account and look for more vendor neutral SOAR systems. The Cybers SOC analysts also have many different tools they need to switch between; thus, the SOAR should be a separate platform which the analysts do not need to directly interact with during their daily work. An automation platform is needed, not an overlapping investigation platform.

Viable options

The viable options were also described in chapter 2.6, the top commercial vendors were set as the backup variants, since their high cost is not Cybers' first choice. TheHive was also considered not an option due to not really being capable of performing as a SOAR out of the box and no longer being open source. The other cheaper and open-source variants were investigated.

The first possible tool was something Cybers had already used to some extent – Microsoft Azure Sentinel SIEM, which also has SOAR functionality built in. However, this would only work in cases where the client would be using Microsoft products. Additionally, it does not make sense to orchestrate other security tools with this SIEM+SOAR solution, it simply lacks the capabilities and is not meant for that. Cybers will still intend to use it for some cases to empower the usage of Sentinel, but further than that it is not the SOAR Cybers is looking for.

A basically free option would be Cisco SecureX, to get it you need to have at least one Cisco service bought. This SOAR is very Cisco solutions centric and expects to be integrated in a Cisco environment. However, Cybers has a multitude of varying tools and being vendor locked is not an option. It does offer a cloud and on-premises version, but for the on-premises version another piece of specific hardware needs to be installed on site to function properly. By default, there are a few needed integrations, but majority of the work will need to be done any way on Cybers' side. It is also expected to be used as a central investigation tool, which is not ideal.

Next, Google owned Siemplify was evaluated in further depth. Partly because there was no public info on the tool or pricing information. It did offer a community edition to be tested out, unfortunately that version was very limited and did not offer enough for Cybers. The full version is costly and comparable to other top vendors. Other than that, the tool was overall easy to use and offered many ready use cases, integrations, and dashboards. The tool is a mature SOAR but was deemed too expensive.

Currently, the only actively maintained open-source SOAR system on the market is Shuffle (shuffler.io). Shuffle is also the SOAR Cybers opted to go with. This tool offers both free and paid versions on the cloud and on premises. The paid versions come with priority support from the vendor along with other benefits and functionalities. The cloud version itself offers a free version, which could be utilized in specialized use cases in SOCs, since it has a certain number of free executions per month. The tool can be deployed anywhere and just the cost of keeping it running is important. Unlike other

SOAR vendors, it is purely focusing on the automation aspect and analysts do not need to directly interact with the tool. The only reason to access the tool is to configure it or modify the created workflows. Critical features such as multi tenancy and running it simultaneously on cloud and on premises are very much possible. Shuffle has easy to use UI and user-friendly workflow building options, it is powerful and customizable. The problem with this tool is that it is only three years old and the company developing it is very small. This will also mean that Cybers side development cost will be bigger, but at the same time saving financially from not purchasing an expensive SOAR will outweigh the cost. With Shuffle, the paid Cloud MSSP version was chosen to get priority support and other features. For comparison, now of this writing, Shuffle cloud version pricing starts from 180 dollars a month for 100000 app executions in the cloud. The cost is significantly lower compared to TheHive, approximately one-tenth, and much less than other competing commercial SOAR options.

Another open-source tool shortly considered was n8n, which is a general workflow automation tool. It was simple, flexible, and very versatile. However, it is oriented towards general workflow automation, not for security. This meant it did not have any integrations with required security tools, ultimately making it a SOAR without the security and response.

3.4.5 Onboarding of Shuffle SOAR

After briefly testing out Shuffle SOAR on a server in Cybers infrastructure and seeing it being up to the challenge, the vendor was contacted to start the official onboarding procedures. During this time Shuffle offered to help build 3 initial workflows as a proof of value concept, which was a good proposition for a SOAR at this price range. The same workflows which were established and outlined after the SOC analysis were chosen to be first developed and tested out. The vendor offering proof of value was a great way to see whether this SOAR is suitable, and its abilities put to the test. During this phase, upon facing serious obstacles, the SOAR system could still be changed without many negative consequences.

As Shuffle is used in the cloud, the first bottlenecks faced were due to properly getting the authentication and thus fluent integration of security tools working. Shuffle being a relatively new tool meant that not everything was ready to be integrated. Shuffle features and integrations are developed as needed and mostly on-demand basis, the product is tailored to user needs to prevent unnecessary development of features which will not be used. The vendor is more than willing to develop requested features, but inevitably it means delays in the clients applying the tool.

Another unnecessary delay was due to not enough resources being dedicated to the SOAR onboarding. Dependence on vendor to develop the workflows was complicated since the vendor is not familiar with the SOC's processes and procedures. Choosing a bit too difficult workflows to be initially developed caused them to delay the onboarding process due to needing many tweaks and testing from Cybers side. Inefficient cooperation caused some delays and misunderstandings on how something should work. Same thing went with some tool integrations, which had to wait on getting approvals and necessary reconfigurations from Cybers side. Overall, it must be noted that it is essential to have good cooperation with the vendor during the implementation to minimize delays and problems. The organization which is implementing the tool must be ready to react fast to problems and be willing to dedicate time and resources by other teams alike to ensure smooth progress.

Due to large need of Cybers to build further workflows after the onboarding, Shuffle offered training course was opted for during the later stage of the onboarding period. This is to ensure the security staff assigned to SOAR can develop and maintain workflows independently. The onboarding phase ended with finishing the vendor offered proof of value, signing the contract, and deploying the initial workflows into production. With the deployment of the created workflows, the implementation of the SOAR was considered completed. The next steps are to further utilize the SOAR in production processes through continuous maintenance and building of new workflows.

4 Summary

The maturity criteria were investigated, to better grasp the readiness of a SOC for a SOAR implementation. The thesis studied the common mistakes of a SOAR implementation and put them into perspective with a real case where mistakes were made. By analysing the maturity criteria, examples of what not to do and limited existing works, a SOAR implementation methodology was developed. The proposed methodology was tested in practice on a MSSP Cybers SOC.

The Cybers SOC SOAR implementation was an overall success. Cybers SOC had a clear goal with objectives to start with SOAR adoption. Due to being a mature SOC with stakeholder support for the project, it qualified for the maturity criteria. Out of the SOAR options, an open-source SOAR system by Shuffle was opted for to complete the set goals. As Shuffle was a considerably cheaper and less mature tool than the counterparts, small delays related to the vendor were an acceptable risk. Most obstacles were faced during the onboarding stage, which caused delays in the tool adoption. The delays were caused by first developing too complex workflows, overconfidence in vendor's abilities, inefficient cooperation with the vendor and lack of free Cybers human resources during the onboarding stage. Despite the minor setbacks, the proposed methodology still yielded positive results.

The present thesis constitutes a valuable resource for organizations seeking to enhance their knowledge of SOAR and its potential benefits for their operations. By providing a comprehensive overview of the concept, the thesis serves to inform decision-makers about the suitability of SOAR for their organization and their readiness for its implementation. In addition, the thesis offers a tested methodology, validated through its application to a real-world case study, that may serve as a guide for organizations seeking to embark on a SOAR implementation journey.

The topic of SOAR remains relatively unexplored, presenting a promising area for future research. Deeper investigation of the onboarding stage optimization and later utilization of SOAR tools could yield valuable insights into their impact on SOC effectiveness.

References

[1] C. Crowley and J. Pescatore, "Common and Best Practices for Security Operations Centers: Results of the 2019 SOC Survey," SANS Institute, Bethesda, MD, USA, Tech. Rep., 2019.

[2] "What Is a Security Operations Center (SOC)?," Microsoft, [Online]. Available: https://www.microsoft.com/en-us/security/business/security-101/what-is-a-security-operations-center-soc. [Accessed: April 03, 2023].

[3] "What Is SOAR?," Fortinet, [Online]. Available: https://www.fortinet.com/resources/cyberglossary/what-is-soar. [Accessed: April 03, 2023].

[4] J. Blankership, S. Balaouras, B. Barringham and R. Birrell, "Breakout Vendors: Security Automation and Orchestration (SAO)," Forrester, April 18, 2017.

[5] J. Trull, "Top 5 Best Practices to Automate Security Operations," Microsoft Secure, Enterprise Cybersecurity Group, Online Blog, August 3, 2017. [Online]. Available: https://cloudblogs.microsoft.com/microsoftsecure/2017/08/03/top-5-best-practices-to-automate-security-operations/. [Accessed: April 03, 2023].

[6] "Security Orchestration, Automation, and Response Solutions," Gartner, [Online]. Available: https://www.gartner.com/reviews/market/security-orchestration-automation-and-response-solutions. [Accessed: April 03, 2023].

[7] "SOAR Market Guide 2022: What Does the Gartner Research Say?" Sumo Logic, [Online]. Available: https://www.sumologic.com/blog/soar-market-guide-2022-what-does-the-gartner-research-say/. [Accessed: April 03, 2023].

[8] S. Shea, "SOAR (security orchestration, automation and response)," TechTarget, [Online]. Available: https://www.techtarget.com/searchsecurity/definition/SOAR. [Accessed: April 03, 2023].

[9] K. Karu, "Implementing an Effective Security Operations Center as a Service (SOCaaS) by the Usage of Open Source SOAR System The Hive, Case of CYBERS," TalTech 2021.

[10] R. Vast, S. Sawant, A. Thorbole and V. Badgujar, "Artificial intelligence based security orchestration, automation and response system," in 2021 6th International Conference for Convergence in Technology (I2CT), April 2021, pp. 1-5, doi: 10.1109/I2CT51068.2021.9418109.

[11] R. A. Bridges, et al., "Testing SOAR tools in use," Computers & Security, vol. 129, pp. 103201, 2023. doi: 10.1016/j.cose.2023.103201.

[12] R. Brewer, "Could SOAR save skills-short SOCs?," Computer Fraud & Security, vol. 2019, no. 10. doi: 10.1016/S1361-3723(19)30106-X

[13] J. Kinyua and L. Awuah, "AI/ML in Security Orchestration, Automation and Response: Future Research Directions," Intelligent Automation & Soft Computing, vol. 28, no. 2, 2021. doi: 10.32604/iasc.2021.016240.

[14] D. Lalos, "Analysis on Security Orchestration Automation and Response (SOAR) platforms for Security Operation Centers," (master's thesis, Πανεπιστήμιο Πειραιώς), 2022.

[15] G. D. Baxter, J. Rooksby, Y. Wang, and A. Khajeh-Hosseini, "The ironies of automation: still going strong at 30?," European Conference on Cognitive Ergonomics, 2012.

[16] A. I. Zamora, "Deployment of a SOAR open-source tool called the Hive" (bachelor's thesis, Universitat Politècnica de Catalunya), 2022.

[17] "Security Orchestration Automation and Response (SOAR) Market by Component, Application, Service, Organization Size, Deployment Mode, Vertical and Region - Global Forecast to 2027," MarketsandMarkets, July 2022. [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/security-orchestration-automation-response-market-176584778.html

[18] S. Morgan, "Top 10 Cybersecurity Predictions and Statistics For 2023," Cybersecurity Ventures, December 10, 2022. [Online]. Available: https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025/

[19] "2022 CISO Survey of Small Security Teams," Cynet, July 2022. [Online]. Available: https://go.cynet.com/2022_ciso_survey. [Accessed: April 03, 2023].

[20] "Incident Response and Automation," Exabeam Explainers. [Online]. Available: https://www.exabeam.com/explainers/siem/incident-1response-and-automation/. [Accessed: April 03, 2023].

[21] A. Chuvakin, "SOAR-native SOC, Can This Work?," Gartner Blog Network, July 13, 2018. [Online]. Available: https://blogs.gartner.com/anton-chuvakin/2018/07/13/soar-native-soc-can-this-work/. [Accessed: April 03, 2023].

[22] J. Visser, "Why a mature SIEM environment is critical for SOAR implementation" Correlated Security, May 3, 2020. [Online]. Available: https://correlatedsecurity.com/soar-critical-success-factors/. [Accessed: April 03, 2023].

[23] C. Saran, "Considerations when deciding on a new SIEM or SOAR tool," ComputerWeekly.com, August 23, 2021. [Online]. Available: https://www.computerweekly.com/feature/Considerations-when-deciding-on-a-new-SIEM-or-SOAR-tool. [Accessed: April 03, 2023].

[24] "The SOAR Adoption Maturity Model," Splunk Inc. [Online]. Available: https://www.splunk.com/en_us/form/the-soar-adoption-maturity-model.html. [Accessed: April 03, 2023].

[25] C. Crowley, B. Filkins, "SANS 2022 SOC Survey," SANS Institute, May 16, 2022. [Online]. Available: https://www.sans.org/white-papers/sans-2022-soc-survey/. [Accessed: April 03, 2023].

[26] J. Bridges, "How to Write a Business Case," ProjectManager.com, July 5, 2022. [Online]. Available: https://www.projectmanager.com/blog/how-to-write-a-business-case. [Accessed: April 03, 2023].

[27] W. Banerd, "Pitfalls and Best Practices of SOAR Implementation," D3 Security, January 3, 2019. [Online]. Available: https://d3security.com/blog/pitfalls-and-best-practices-of-soar-implementation/. [Accessed: April 03, 2023].

[28] "SOAR Implementation: Challenges and Countermeasures," SIRP. [Online]. Available: https://www.sirp.io/blog/soar-implementation-challenges-and-countermeasures/. [Accessed: April 03, 2023].

[29] "What are the Pros and Cons of SOAR?," Trustwave, September 1, 2020. [Online]. Available: https://www.trustwave.com/en-us/resources/blogs/trustwave-blog/what-are-the-pros-and-cons-of-soar/. [Accessed: April 03, 2023].

[30] A. Froehlich, J. Groopman, "Top benefits of SOAR tools, plus potential pitfalls to consider," TechTarget. [Online]. Available: https://www.techtarget.com/searchsecurity/feature/Top-benefits-of-SOAR-tools-plus-potential-pitfalls-to-consider. [Accessed: April 03, 2023].

[31] D. Murdoch, "2020 SANS Automation and Integration Survey," SANS Institute, May 18, 2020. [Online]. Available: https://www.sans.org/white-papers/39575/. [Accessed: April 03, 2023].

Appendix 1 – Non-exclusive licence

I Reno Špitsmeister

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis “Implementing a SOAR Solution in a Security Operations Center on the Example of Cybers”, supervised by Risto Vaarandi and Aleksei Zjabkin
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

10.05.2023