UNIVERSITETET I AGDER

IS-304 spring 2023

Title: Security Monitoring of the Google Cloud Platform and Workspace.

Subject code:	IS-304
Subject name:	Bacheloroppgave i Informasjonssystemer
Subject manager:	Hallgeir Nilsen
Supervisor:	Peter Andre Busch
Client:	Netsecurity

Students:

Surname:	**First name:**
Berg	David
Eriksen	Alexandra
Sharo	Dlir
D. Omar	Dana
H. Fjermeros	Marius

I/we confirm that we do not quote or otherwise use other people's work without this being stated, and that all references are stated in the bibliography list.	Yes **X**	No
Can the answer be used for teaching purposes?	Yes **X**	No
We confirm that everyone in the group has contributed to the answer.	Yes **X**	No

Preface

This report was written as part of the bachelor project completed in the spring semester of 2023. It serves dual purposes: as a report for UIA, detailing the project's implementation, and as a report for Netsecurity, documenting findings obtained through experimentation. The members of Group 14 have gained an impressive amount of knowledge this semester, covering various subjects such as technology, cyber security, and teamwork. Importantly, we have also discovered a great deal about our growth and development as a group. Despite varying levels of experience in cybersecurity among us, we successfully came together to overcome challenges, leveraging our diverse perspectives and skills to quickly adapt and seize opportunities. Together, we developed a plan in collaboration with the enterprise to achieve the best outcome. Our collective experience this semester has been invaluable, further strengthening our unity and performance as a team.

First and foremost, we would like to thank our supervisor, Peter Andre Busch, from UIA, and our project owner, Espen Abildgaard, from Netsecurity, who showed great interest in our group. Both have been actively engaged throughout the semester, providing valuable feedback, inspiration, and motivation. We would also like to express our appreciation for their availability to hold meetings when we encountered difficulties, discuss problems, and offer suggestions. We are grateful for your prompt responses and active participation in our sprint reviews and group management meetings.

University of Agder, Kristiansand. May 16, 2023

Marius Fjermeros
H. Fjermeros, Marius

Dana D. Omar
D. Omar, Dana

Dlir Sharo
Sharo, Dlir

Alexandra Eriksen
Eriksen, Alexandra

Berg, David

Summary

This report has been written and designed by all five group members from group 14 in the spring of 2023. The assignment was completed and designed by the group, together with the product owner. The goal of the report is to research and make recommendations for Netsecurity’s security monitoring of the Google Cloud Platform - both for themselves and their customers.

We collaborated with Netsecurity to research and enhance their security monitoring of the Google Cloud Platform (GCP). We evaluated Google Workspace's security features and the role of Managed Security Service Providers (MSSPs), like Netsecurity, in improving cybersecurity. Our findings reveal the benefits of integrating advanced automation tools like Security Orchestration, Automation, and Response (SOAR) and MSSPs, which boost security infrastructure and offer cost-effective solutions. We also addressed challenges faced by businesses adopting GCP and explored how cybersecurity measures can be optimized for data protection.

Throughout the project, we navigated security rules and performed functional tests to establish customized security rules for Google Workspace. We encountered challenges during testing and explained how we overcame them. Concurrently, we explained the process of GCP integration in XSOAR, involving data mapping and playbook configuration to automate tasks.

Adopting the Scrum methodology, our team was divided into the roles of Scrum Master, Product Owner, and Developer. This facilitated efficient progress and allowed us to focus on key aspects of the project using the MoSCoW-method for prioritization. Our project management strategy was comprehensive, encompassing risk management, communication, and peer review protocols to ensure high-quality project execution. We utilized various digital tools to foster effective communication, cooperation, and task management.

The culmination of our efforts was a thorough research document for Netsecurity, proposing innovative solutions for GCP and Workspace security. The document extensively explored Identity Security by focusing on various authentication methods and access control. Additionally, the role of Threat Intelligence, comparisons of Google's SOAR tool with external services, and comprehensive measures for device enrollment and security. Key topics such as Google Cloud Session Control, alert center functionalities, phishing detection, and integrated threat intelligence were discussed, along with advanced mobile and computer security measures.

To conclude, our project delivered a deep dive into GCP's security features and recommended strategies for strengthening Netsecurity's security monitoring systems. The research outcomes align with our initial objective of enhancing GCP's security, thus contributing significantly to the field of cybersecurity.

Table of Contents:

List of Figures

List of tables

1.0 – Introduction

The purpose of our assignment was to assess whether the inclusion of a third-party actor, namely Netsecurity, would bring enhanced value to cybersecurity measures. While proving this proposition may be arduous - if not impossible - several factors strongly indicate an increased level of security. One such factor is Netsecurity's provision of continuous surveillance and prompt response to security threats.

Breakout time, which measures the duration an adversary takes to move laterally within a victim's environment, is a critical metric in security. In 2022, the average breakout time for interactive eCrime intrusion was a mere 84 minutes, marking a significant 14% decrease compared to 2021 (Crowdstrike, 2023, p.9). This highlights the paramount importance of continuous and constant surveillance. If surveillance is limited to regular work hours, there is a heightened risk of the company network already being compromised or acquired by the time employees return to the workplace the following day.

By responding within the breakout time window, defenders can minimize damages and costs (Crowdstrike, 2023, p. 9). Netsecurity employs full-time personnel specialized in dealing with security threats, ensuring a swift response time whenever qualified experts are available around the clock.

In parallel to our exploration of cyber security, it is essential to navigate the landscape of cloud computing solutions. Google Cloud Service stands out by offering a wide array of applications and storage options, mirroring its adoption trends in the European market, and reflecting the patterns observed in the United States (Businesswire, 2022). The 2022 ISG provider report for Europe emphasizes the increasing integration of Google Cloud Platform (GCP) in multi-cloud strategies, driven by its advanced data management and analytics capabilities (Businesswire, 2022). Despite initial caution from European companies, who tend to favor established providers like AWS and Azure, GCP sets itself apart by catering to advanced application requirements and demonstrating a commitment to sustainability (Businesswire, 2022). Understanding these distinctions becomes paramount for European organizations venturing into the realm of cloud computing.

While the vision of fully automated solutions that respond instantly to threats may materialize in the future, the present reality presents significant challenges in terms of the required skills, time, and resources (Benzoni, 2020). Nonetheless, automation, particularly in Security Orchestration, Automation, and Response (SOAR), is already alleviating the burdens faced by defenders by automating repetitive behaviors and recurring tasks (Benzoni, 2020). As we delve into the realms of cybersecurity and cloud computing, comprehending these nuances and possibilities becomes essential for organizations seeking to fortify their defenses and embrace innovative solutions.

1.1 - Our project

Netsecurity is a Norwegian-owned company focused on and specializing in IT security. They help businesses before, during, and after an attack. With more than 10 years of experience in the Norwegian market, they have a team consisting of strategic advisors, security consultants, product specialists, and ethical hackers. Their holistic security approach is built around their world-class SOC (Security Operation Center) services. They have developed a market-leading cybersecurity operation, by investing in breakthrough innovation and best-of-breed technology. This enables their customer's access to an agile security organization that embeds security into every aspect of their operations, aligning it with each customer's specific business needs. In building resilience from the core, their customers' businesses can operate and grow confidently even in today's rapidly evolving threat landscape (Netsecurity, 2023).

They are approved by NSM (Nasjonal Sikkerhetsmyndighet), which is a national approval scheme for suppliers that offer services for handling a cyber-attack. Their customers consist of large and small customers from both the private and public sectors (Netsecurity, 2023).

Netsecurity was established in 2009 and currently employs 110 individuals, with offices located in Kristiansand, Grimstad, Oslo, Stavanger, Bergen, and Stockholm (Netsecurity, 2023). Our bachelor project is a collaboration with Netsecurity's office located in Kristiansand, closely followed up by our supervisor and product owner, Espen Abildgaard.

Netsecurity has proposed an intriguing project focused on enhancing the security and monitoring capabilities of the Google Cloud Platform. This project has piqued the interest of the group due to the platform's increasing popularity among medium to small-sized companies and official institutions. With a rising demand for secure services, the project aims to conduct research on Google Workspace, identify potential security measures, perform tests to evaluate security warnings, and logs, and integrate these findings with Netsecurity's SOAR tool.

The SOAR tool, an essential component of this project, warrants its own dedicated section for detailed exploration. SOAR, which stands for Security Orchestration, Automation, and Response, empowers security experts with the ability to streamline and optimize security operations with great efficiency (Cyberpedia, n.d.). Netsecurity relies on a robust SOAR platform known as XSOAR, crafted by the esteemed Palo Alto Networks. This seamless integration equips Netsecurity's security analysts with the necessary firepower to handle security breaches concerning Google Cloud users promptly and effectively.

1.2 - Google Workspace

Google Workspace was first launched in 2006 as “Gmail for your domain” before later the same year being expanded into “Google apps for your domain”. In 2016 it was rebranded as “G Suite” before it once again was rebranded in 2020 as “Google Workspace” (Google Workspace, 2023). As of 2021, Google Workspace has more than 3 billion users worldwide (Maxson, 2022).

Google Workspace is a collection of all of Google's productivity apps in one place, including Gmail, Drive, Calendar, Docs, Sheets, Slides, Meet, etc. Within Google Workspace one handles users and controls access to applications, including who can access and which areas of the system`s infrastructure. The goal is to create a platform that is easy to create, collaborate and communicate whether you are sitting at the office, working from home, connecting with customers, or using your mobile device (Google Workspace, 2023).
Google offers a range of powerful tools under the Google Workspace suite, including Gmail, Google Drive, and Google Docs. While these tools are available at no cost for personal use, it's important to note that they don't include administrative rights. As a result, they are not suitable for use in organizations that require strict security controls and centralized management (Google Workspace, 2023)

To address these needs, Google Workspace offers an enterprise version with advanced security features and administrative rights. This version is designed specifically for organizations of all sizes and is available at different price points depending on the specific needs of the organization. Here, the organization can access advanced security controls and administration rights (Google Workspace, 2023).

2.0 - Research of Google Cloud Platform Security Features

In this section, we will provide a concise overview of the key aspects of the security features offered by the Google Cloud Platform. This will help you gain a better understanding of the focus and content of the report.

2.1 - Identity Security

Identity Security is arguably the most important feature in cybersecurity, as a breach may have serious consequences. This includes financial loss, reputational damage, and loss of privacy. Cybercrime continues to grow in sophistication, and providing suitable solutions for protecting sensitive information is critical. Based on the report from Verizon about data breach investigations, almost 85 % of the breaches involved human elements, and almost 61% involved the use of credentials (Verizon, 2021, p. 7).

Identity security can be defined as a comprehensive solution that protects all types of identities within the enterprise - human or machine, on-prem or hybrid, regular or privileged -- to detect and prevent identity-driven breaches, especially when adversaries manage to bypass endpoint security measures (Shastri, 2022).

In 2020, The Identity Defined Security Alliance (IDSA) published a study stating that 94% of organizations had experienced an identity-related breach at some point – 79% of those within the last two years (Smith, 2020). A large driving force in this development is the explosion of digital identities. Identity is not the only access point for threat actors to gain access but is often a weak point with less resistance (Bradley, 2023).

For these reasons, Identity Security management is more important than ever before to protect sensitive information and resources in cloud computing. This includes preventing unauthorized access, securing access, and enforcing authorization to protect this information. Google Workspace provides a range of features and tools to help organizations protect their sensitive information and resources in cloud computing. These features include strong authentication mechanisms, such as two-factor authentication and security keys, as well as granular access controls and auditing capabilities. By implementing these measures, organizations can better protect their data and minimize the risk of a breach (Google, Workspace, 2023).

2.2 - Threat Intelligence

Threat Intelligence (TI) involves collecting and analyzing information to understand and predict cybersecurity threats. It provides evidence-based knowledge about existing or emerging threats and their implications, helping inform decisions on how to respond. Various sources, such as malware and network traffic, contribute to this knowledge (McMillan, 2013).

Identifying malware involves using unique hash values that represent specific files or code. By comparing suspicious file hash values to a database of known malware hashes, researchers can quickly determine if the file is a threat. Behavioral analysis helps identify the type of threat, even if hash values change or the code is encrypted. TI allows for comparing attacks, understanding malware capabilities, and developing defense strategies. TI also enabled the registration of harmful IP addresses, websites, and email addresses in advance, preventing their access. (Google, 2023f)

Google Workspace incorporates Threat Intelligence by using technologies like Google Safe Browsing and machine learning algorithms to detect phishing and malware. The Threat Analysis Group (TAG) at Google focuses on analyzing and defending against targeted attacks. Integrating a Security Orchestration, Automation, and Response (SOAR) platform with Google Workspace automates and standardizes incident response, enhances collaboration, reduces response time, and improves overall security operations (Google, 2023f).

Google Workspace offers additional security features such as data loss prevention (DLP) to identify and block sensitive information from leaving an organization, and mobile device management (MDM) to enforce security policies on mobile devices. Administrators receive security reports and alerts, enabling them to identify and prevent potential security issues. İntegrating a SOAR platform streamlines incident response procedures and facilitates real-time collaboration and information exchange among security teams (Google, 2023f).

2.3 - SOAR

SOAR (Security Orchestration, Automation, and Response) is a cybersecurity technology that automates incident response, protects against threats, and enhances organizational security. It collects and integrates data from multiple sources, enabling faster and more informed decision-making. Soar’s three program functions are: *Orchestration* automates security incident workflows, *Response* reacts swiftly to minimize damage, and *Automation* organizes and prioritizes security alerts (Cyberpedia n.d.).

2.3.1 Detection Rules

One advantage of SOAR technology is that it eliminates the need to create new detection rules for each integrated system (Paloaltonetworks, n.d.). The predefined rules for detection can be easily applied to new systems, saving time and resources. With Netsecurity’s existing detection rules, our group can seamlessly integrate Google Cloud Service with the SOAR platform without the burden of developing and maintaining new rules. This allows us to focus on adapting and optimizing the existing rules to meet our organization’s specific need for Google Cloud.

2.3.2 Automation

Automation is a key feature of SOAR that effectively handles incidents. The extent of incident handling is determined by the type and characteristics of the automation used. Security automation reduces response time for repetitive incidents and false positives, allowing analysts to focus on strategic tasks. Automated playbooks provide predefined actions for known security scenarios (Paloaltonetworks n.d.). When outsourcing SOAR services, customers need not concern themselves with configuring these automations as it is managed by the service providers. In our case, since Netsecurity has already defined these automations, Google Workspace users are relieved from working on this matter.

2.3.3 Platform Limitations

SOAR overcomes platform limitations by creating adaptable automation processes that work across different companies’ setups. Once an automation process is created for a specific platform, it can be easily used by new customers without extensive modifications. This saves time, effort, and resources, ensuring consistent implementation across platforms. SOAR streamlines the automation process, reduces errors, and improves efficiency.

2.3.4 Competence

Successful utilization of tools like Palo Alto Networks XSOAR and Google Chronicle SOAR requires a deep understanding of IT security. Users must comprehend and respond to threats detected by the SOAR system effectively. This necessitates accurate comprehension of information from enrichment tools such as CVE details, Virus Total, and MITRE ATT&CK framework-based sources.

Proper interpretation of logs from various sources enhances defense against cyber threats. Additionally, users need a comprehensive understanding of their company's specific security requirements and potential threats. This entails identifying and prioritizing security incidents, customizing the SOAR platform, and developing effective playbooks for known scenarios. Therefore, users implementing SOAR should possess security engineering skills to build robust security architectures and create impactful playbooks. Meanwhile, analysts responsible for incident analysis and response should have security analyst skills. Ensuring the presence of these competencies enhances the effectiveness of SOAR implementation and strengthens overall organizational security.

2.3.5 Staffing

SOAR (Security Orchestration, Automation, and Response) tools optimize cybersecurity operations in response to the growing cybersecurity threats. They help combat attacks by reducing response time, even during weekends and holidays when cybercriminal activity tends to increase (CISA, 2022). In a survey of 1,200 cybersecurity professionals, it has been revealed that attacks carried out on weekends and holidays have more destructive impacts on organizations (Cybereason, 2022). These tools automatically detect and respond to threats using predefined playbooks created by security analysts. SOAR tools enhance the efficiency of cybersecurity teams, providing faster responses to attacks. However, human control is still necessary as some situations may require the approval or guidance of security analysts to execute playbooks. To maximize functionality and defend against cyberattacks, companies using SOAR systems should have dedicated personnel monitoring the system 24/7.

2.3.6 Threat Intelligence Integration

Threat intelligence is crucial for effective security operations, but the overwhelming number of alerts and indicators often poses challenges for security teams (Palo Alto Networks, 2021). The integration of Threat Intelligence with SOAR tools provides a comprehensive solution that combines aggregation, storing, sharing, and automation, enabling teams to manage Threat Intelligence effectively and enhance their defenses. To construct smart playbooks, actionable and real-time threat data is needed, which can be integrated into SOAR solutions. Leveraging Threat Intelligence in this manner improves the ability of security teams to detect and respond to threats, enhancing overall security posture.

2.3.7 Cost Effectiveness

Outsourcing Security Orchestration, Automation, and Response (SOAR) services offers cost-effective benefits for businesses. It eliminates the need to maintain an in-house Security Operations Center (SOC) and a dedicated team of security professionals, resulting in significant cost savings. One advantage is cost-sharing. Managed Security Service Providers (MSSPs) serve multiple clients, allowing them to distribute the cost of maintaining the SOC infrastructure and security experts. This makes outsourcing SOAR services more cost-effective than hiring an in-house team.

Outsourcing also provides access to the latest technology and a team of security experts at a lower cost. This enhances threat detection and response, reducing the risk and cost of security breaches. Furthermore, it offers flexibility and scalability, enabling businesses to adjust security services as needed without hiring or training new staff.

2.4 - Device Management

Device management is a critical aspect of modern business operations, especially with the increasing use of mobile devices and the growing complexity of enterprise networks. Device enrollment is a crucial component of device management, as it involves registering and configuring a device for use on a network, often managing and securing it (Microsoft, 2022).

Microsoft describes device enrollment as the process of installing specific software or agents on a device, which then communicates with a management server to receive configurations, policies, and software updates. This enables IT administrators to manage and secure devices at scale, ensuring that they are up-to-date and meet security standards. Google Workspace offers a cloud-based device management solution called Google Endpoint Manager, which allows administrators to manage and secure a wide range of devices from a single, centralized console. The solution is compatible with a range of devices and operating systems, including Android and iOS (Microsoft, 2022).

Google´s basic mobile security option provides essential tools for accessing work accounts on mobile phones and features like password customization, app management, and the ability to wipe corporate data from lost or departing devices. Password customization is a critical security feature that enhances the security of an organization's data. The administrator can mandate the use of a screen lock or password on managed mobile devices, and users receive prompt notifications if their password does not meet the set requirements. If password requirements are not met within the specified time frame, the user will be denied access until they comply with the requirements. Context-Aware Access can be set up to block non-compliant devices immediately to avoid the 24-hour delay. (Google, 2023a)

App management is another critical feature of Google´s basic mobile security option, allowing administrators to control which apps Android and iOS device users can find and install. This feature also allows the administrator to add private apps and third-party apps to the web and list them in the admin console (Google, 2023b).

The ability to wipe corporate data from a device is another key security feature included in Google's basic mobile security option. This feature is especially useful if a device is lost, or an employee leaves the organization. Depending on the platform, an administrator can wipe a user´s account, profile, or all data. The data is still accessible on another authorized device (Google, 2023c).

Google´s mobile security option also includes system-defined rules and a list of all devices that have accessed work accounts. This list includes information about the type of device, model, last time work data has been synchronized, and the name of the user. From this list, the administrator can block a device from syncing work data, wipe data from a lost device, and more. (Google, 2023d)

In conclusion, device management is a critical aspect of modern business operations, and device enrollment is a crucial component of this management process. Google's cloud-based device management solution, Google Endpoint Manager, offers a range of security features, including Google´s basic mobile security option. Which provides essential tools for accessing work accounts on mobile phones and includes features like password customization, app management, and the ability to wipe corporate data from lost or departing devices (Google, 2023e).

3.0 - Project Approach

In this section, we will discuss the most central decisions in the project regarding technologies, project management tools, and communication platforms. In each of the mentioned sections, further topics related to these will be covered.

3.1 - Product requirements from Netsecurity

Netsecurity aimed to comprehensively analyze the cybersecurity-related features within Google´s portfolio, identify the security challenges that Google can effectively address, and determine the potential for Netsecurity to leverage Google´s features in its own development efforts. Subsequently, our team collectively decided to produce a scholarly report that specifically outlines the available features in Google Workspace and Google Cloud, providing a comprehensive mapping of their relevance to the field of cybersecurity.

Defining quality can vary depending on the context and the specific criteria being considered. In general terms, quality can be described as the degree of excellence or superiority of a product, service, or process. It encompasses various attributes such as reliability, performance, functionality, usability, security, and adherence to standards or specifications. In the context of cybersecurity, quality can be defined as the effectiveness and reliability of measures implemented to protect systems, data, and networks from unauthorized access, malicious activities, and potential threats (Techqualitypedia, 2020).

It is important to note that defining quality in the context of cybersecurity may require a multidimensional approach, considering various factors such as technical capabilities, user requirements, organizational needs, and industry standards.

In addition to overall quality, there are two distinct dimensions to consider: internal and external qualities (Long, 2010). It is crucial for developers to strive for a balance between these two aspects, as neglecting one in favor of the other is not advisable (Long, 2010).

External quality refers to the extent to which a product meets the expectations and requirements set by the product owner. This encompasses various factors such as reliability, ease of use, adaptability, and more. Essentially, it represents the immediate and subjective experience of the end user. On the other hand, internal quality refers to the structure of the product, including characteristics like cohesion, low coupling, low duplicity, simplicity, and so on. These aspects are not directly experienced by the end user (Long, 2010).

3.1.1 Balancing Features, Time, and Costs

The project undertaken by Netsecurity focused on conducting a comprehensive analysis of the cybersecurity-related features within Google´s portfolio. A key deliverable within this project was the production of a scholarly report, which provided a comprehensive mapping of the available features in Google Workspace.

To accomplish this project, various resources were required. Firstly, access to Google Workspace and Google Cloud platforms was essential for conducting in-depth analysis and evaluation of the security features offered. Additionally, documentation and information related to Google´s security features and capabilities were crucial for a comprehensive assessment. Technical tools for testing and evaluating the security features were necessary to ensure accurate and reliable results. Lastly, collaboration and communication tools played a vital role in facilitating seamless teamwork and coordination among the group.

3.1.2 - MoSCoW.

During the work on the project, the group decided to use the MoSCoW-method to better prioritize the project tasks. The MoSCoW-method is a well-known project management method used to identify and prioritize tasks. The method makes it possible to prioritize the most important tasks in the project, while at the same time, less important tasks can be postponed. MoSCoW stands for “Must-have”, “Should-have”, “Could-have”, and “Won't-have” (Køster, 2022). We have visualized these in table 1.

The ”must-have” section is requirements that are critical for reaching the goal of the project. If even one must-have requirement is not included in the finished project, the project should be considered a failure. They can however be downgraded after agreement with the project owner (MoSCoW method, 2022). After a meeting with the product owner, we considered mapping out the features of GCP to be the most crucial part of the project. Simply, because the project would have to be considered a failure if we were not able to map out the features.

“Should-have” is requirements that are important, but not necessary for delivery. Even though they can be as important as “Must-have” requirements, they can often be delayed or satisfied in another way, making it possible to hold back the requirement to a later delivery date (MoSCoW method, 2022). We considered the implementation of SOAR, Playbooks, and detection rules to be important, but not critical for the project to be completed.

“Could-have” are desirable features, but not necessary. Often, they can improve the user experience or customer satisfaction. They are typically included if time permits (MoSCoW method, 2022). Automation around enrichment and filtering, as well as sketching playbooks were considered such features in our project. However, even though they would have been nice to include, there simply wasn’t enough time or experience for us to add those features to our project.

Lastly, the “Won’t-have” requirements are considered by the project owner to be the least critical or not appropriate at the time. Requirements that are included in “won't have” are either dropped or considered later (MoSCoW method, 2022). Initially, we had an idea that it would be a good feature for Netsecurity to have a comparison with their current supplier Microsoft Azure. However, we quickly discovered that the amount of work required to add this requirement to the project would consume way too much time considered the scope of our project. We therefore placed it under “wont have” after an agreement with the product owner.

Must have:	● Mapping the GCP
Should have:	● SOAR Implementation and integration (Workspace environment connected to SOAR). ● Integration playbook “Automation that receives and processes the alarm data we have received from the workspace - and processed data”. ● Detection Rules for GCP
Could have:	● Automation around enrichment and filtering *Sketch of playbook:* ● Fetch log data ● Categorize log data
Won`t have:	● Feature comparison (Compare to Azure)

Table 1: MoSCoW-analysis

3.2 - Methodology

Before we started working on our project, one of the key decisions we had to make was the choice of methodology to guide our work. After conducting extensive research and analysis, we narrowed down our options to two main contenders: an Agile methodology like Scrum or a more traditional approach like Waterfall.

Traditional software development methodologies are based on a sequential series of steps, like requirements definition, solution building, testing, and deployment (Leau et al., 2012, p. 162). Agile software development is based on the idea of incremental and iterative development, in which the phases within a development life cycle are revisited repeatedly. The development life cycle is divided into smaller parts called “increments" or “iterations". Agile methods emphasize teams, working software, customer collaboration, and responding to change; while the conventional methods stress on contracts, plans, processes, documents, and tools (Leau et al., 2012, p. 163).

One of the most popular traditional approaches is the Waterfall approach, which was established in 1970 by Winston W. Royce. It contains five phases of management, where each requires a deliverable from the previous phase to proceed. Waterfall is ideal for projects like software development, where the result is clearly established before starting and is best suited for projects that require a lot of predictability (Hoory & Bottorff, 2022).

A popular agile method is Scrum, which is a lightweight framework that helps people, teams, and organizations generate value through adaptive solutions for complex problems. Scrum employs an iterative, incremental approach to optimize predictability and to control risk, and engages groups of people who collectively have all the skills and expertise to do the work and share or acquire such skills as needed (Schwaber & Sutherland, 2020, p.3).

After discussing and researching the suggested methodologies, we decided to use Scrum to manage and organize our project. One of the main reasons was our familiarity with the framework from previous courses, and our projects' need for flexibility. The reason for this was the uncertainty regarding how extensive research on Google Workspace we were able to carry out, as well as the possibility of adding additional assignments to our project. We, therefore, considered Scrum to be an efficient way to meet the goals that were considered most valuable for Netsecurity, as well as to promote teamwork and acquire skills from each other. Daily scrum meetings were a useful tool for optimizing the predictability and routines for the project to ensure we were on track toward our end goal.

3.2.1 - Roles

The fundamental unit of Scrum is a small team of people - a Scrum Team. The Scrum Team consists of one Scrum Master, one Product Owner, and the Developers (Schwaber & Sutherland, 2020, p. 5). Each role has different responsibilities that are equally important for the development process. In this section, we will explain what each of these roles implies, as well as how we divided the roles within our group.

Scrum Master

The Group chose Dlir Sharo as the Scrum master to work on the project. We chose Dlir because he has worked with the scrum methodology in multiple previous courses and proved to have more experience with this than the rest of the group. He also expressed a strong interest in taking on this responsibility.

The Scrum Master is accountable for establishing Scrum as defined in the Scrum Guide. They do this by helping everyone understand Scrum theory and practice, both within the Scrum Team and the organization. He is also responsible for the team's effectiveness by enabling the team to improve its practices within the framework (Schwaber & Sutherland, 2020, p. 6).

The Scrum master was responsible for ensuring that all scrum events took place, while the rest of the group was responsible for conducting the events. Events included Daily Scrum, Sprint reviews, and Sprint Retrospectives (Schwaber & Sutherland, 2020, p. 6 - 7). However, since the Scrum Master was also working actively on backlog items, he also participated as a developer (Schwaber & Sutherland, 2020, p. 9). To summarize, the Scrum master's main goal was to ensure that he helped the Scrum Team focus on creating high-value increments that met the definition of done, causing the removal of impediments to the Scrum Team's progress; and ensured that all Scrum events took place and were positive, productive, and kept within the timebox (Schwaber & Sutherland, 2020, p. 6)

Product Owner

The Product Owner is accountable for maximizing the value of the product resulting from the work of the Scrum Team. He is also accountable for effective product backlog management. This includes developing and explicitly communicating the Product Goal, creating, and clearly communicating Product Backlog items, ordering Product Backlog items, and ensuring that the Product Backlog is transparent, visible, and understood (Schwaber & Sutherland, 2020, p. 5 - 6).

The product owner was responsible for creating a roadmap. A roadmap describes the way a product or a product portfolio is going to meet a set of business objectives and the work that is required to get there (Münch et al, 2019). The roadmap worked as our backlog. After each sprint review, the group held a sprint planning event. At this event, the developers together with the Scrum Master, planned and defined the product backlog into smaller precise items that could be finished within one sprint. We will explain further about the backlog in Chapter 3. An example of how this was organized is illustrated in Figure number 2.

Developers

Developers are the people in the Scrum Team that are committed to creating any aspect of a usable Increment each Sprint. The specific skills needed by the Developers are often broad and will vary with the domain of work. However, the Developers are always accountable for creating a plan for the Sprint (the Sprint Backlog), instilling quality by adhering to a Definition of Done, adapting their plan each day toward the Sprint Goal, and holding each other accountable as professionals (Schwaber & Sutherland, 2020, p. 5)

While Scrum methodology dictates that the Scrum Master is responsible for facilitating communication and collaboration between the development team and the product owner, it is not uncommon for teams to appoint another member to take on some of those responsibilities (Schwaber & Sutherland, 2020, p.6). In this case, David Berg was designated as responsible for contact between our group and Netsecurity. His responsibility involves promoting the group's challenges, arranging meetings with the company, and arranging joint meetings between the university and other general relations with the company's contact person Espen Abildgaard.

Since David Berg already had a network within the company and a good knowledge of cybersecurity, he took on the responsibilities of communicating with the product owner and having an overview of the cybersecurity competence to lead the technical part of the project. This freed up the Scrum Master to focus on other aspects of the project, such as facilitating Scrum events, removing any obstacles, and ensuring that the Scrum framework is being followed.

This project was done in collaboration with both Netsecurity and UiA, which resulted in several conversations between the two parties. Alexandra oversaw the communication with various people at UiA. The group considered it to be better to have one person communicating with the university and another person communicating with the company because they have different objectives and interests that need to be considered.
The university's primary concern is the academic progress of the students and the quality of their work, while the company's primary concern is the timely completion of the project and meeting business objectives. Having different people responsible for communicating with each entity ensured that both interests were considered and that potential conflicts were avoided. Additionally, it helped to maintain a clear and professional relationship with both the university and the company.

3.2.2 - Estimations

During project work, the group used time estimation and time logging. This allowed us to plan and arrange our work more effectively because it gave us a general idea of when the planned tasks were anticipated to be completed. The team decided to use Trello's built-in features for tracking and predicting time to make it easier. We were able to quickly arrange our work using Trello by making cards for each task and arranging them on a timetable. Trello allowed the team to easily modify the timetable and keep everyone informed about the tasks that needed to be completed. At the beginning of the project, we also had a separate Excel document where we manually listed our tasks, estimated times, and actual times spent. After the first sprint, we immediately concluded that this was time-consuming and that it would be preferable to track time more automatically in Trello.

3.3 - Quality Assurance

In our research project, we worked carefully to create a solid framework with well-defined rules and procedures, guaranteeing the best quality in project execution and the outcome report to Netsecurity. We determined that risk management, cooperation, communication, and peer review were crucial elements of our quality assurance strategy, fostering team members' shared understanding of the project's management. Work methods and technology, which were crucial to the project's implementation, have been covered in the earlier chapters. This section will explore and clarify the choices made to assure the quality of our project, focusing on the crucial aspects of quality assurance that have already been addressed.

3.3.1 - Risk management

Risk management was a crucial aspect to consider in our project. Risk management is a continual process that helps identify, analyze, and evaluate potential risks to people, assets, or the environment. This process helps reduce the harm that may result from identified risks by implementing measures to eliminate or reduce them (Rausand, 2011). Some projects may go smoothly while others may face challenges, causing the project to be terminated before reaching its goal. However, with proper risk analysis and management, it's possible to increase the chance of success and reduce the impact of the risks (Lavanya & Malarvizhi, 2008).

Our research project was dependent on the extensive work on a new topic from our group members, Espen Abildgaard's expertise, a working Google Workspace environment for testing crucial security functions, and finally the availability of documentation of the features in GCP. To ensure its successful completion, we reached a consensus on how to manage the project, created a roadmap, and assigned tasks to each group member. Initially, the group members had a positive outlook and believed that everything would go as planned. However, towards the end of the pre-sprint, we realized that there could be vulnerabilities in the project's progress that were necessary to analyze to reach our goal.

In the event of an unexpected risk, we needed to find a solution to keep the project moving forward. To determine the risks that our project could face, we discussed questions such as: What would we do if the problems grew and became extremely difficult to resolve? Would we be able to find immediate solutions to continue the project? Our discussions led us to conclude that the answer to these questions would help us define the risks involved in the project.

Risk Identification

We realized that accurately identifying possible risks was crucial to making effective risk management decisions. We determined that human resources were our most asset for completing the project and considered other assets and conditions. Thus, we tried to identify all possible risks. We divided the risks into internal and external categories and defined them with input from the group members. In total, we identified 10 risks that could threaten our project, and this number may increase as the project progresses.

Risk Analysis

Once the risks were defined, we could evaluate their severity and likelihood based on various factors, such as the potential impact or harm that the risk could cause, the likelihood or probability of the risk occurring, the ease or difficulty in identifying the risk before it occurs, and the level of susceptibility or exposure to the risk.

We decided to rate the risk severity from 1 (Negligible) to 5 (Catastrophic) and likelihood from 1 (Very Unlikely) to 5 (Very Likely) based on our group evaluation of these factors. The decision to adopt this point system for risk assessment was primarily driven by its simplicity and effectiveness in providing a clear, easily understandable categorization of risk. By assigning numerical values to the severity and likelihood of risks, we could quantify and prioritize them more objectively.

Based on the severity- and likelihood ratings assigned to each identified risk, the risks were categorized into low, medium, and high-risk categories. Risks with scores of 1-6 were considered low risk, 7-12 as medium risk, and 13-25 as high risk. The severity rating and likelihood rating were multiplied to determine the risk score, which is used to categorize the risks. This categorization helps to see the risk picture and prioritize risk management (United States Department of Defense, 2017, p. 23-30).

Risk Assessment

Following the risk analysis, we will discuss measures to prevent or, in the event of an occurrence, minimize the impact of the identified risks. Even though the probability of some risks may be low, their potential to result in catastrophic consequences cannot be ignored. As the project cannot tolerate these risks, actions must be taken to eliminate the possibility of their occurrence. While it may not be possible to fully prevent some risks, efforts will be made to reduce their impact should they occur. For instance, the company ceasing the use of resources for the project, although unlikely, would be catastrophic.

To mitigate this risk, maintaining open communication channels with the company and fostering good cooperation efforts will help prevent the cessation of resources for the project. Additionally, the risk of social loafing, where group members may contribute less effort towards a common goal, could occur within the group (Karau & Williams, 1993, p.681-706). Although it is challenging to fully prevent this risk, it can be minimized through the implementation of daily scrums and time estimation for each task. Other risk-management methods that will be utilized include proper planning, effective communication, continuous feedback, appropriate task distribution, assigning alternates for each team member, and involving supervisors in solving group problems.

As we look at the risk management table down below, we, the group have come up with some various risks that may possibly occur during the semester. The various risk factors are of course placed according to how risky they would be for the group and how big a problem would arise. As we can see, they are placed according to various elements such as which category they fit into, how serious the risk is, and how likely it is that the risk will occur (Likelihood). How big an impact the risk(s) will have on the group members. Not least whether they are internal or external risks. This means whether the group should use the measures only between the group or pass them on to for example our supervisor.
If one or more risks should occur, the group has created a prepared solution just in case, so that when the risk appears, the group is ready to stop the problem fast. We included both preventive and mitigating measures. And these depends on which ones the group will use, depending on how big the risks are and how much impact it has on the group, then the group candidates would implement those measures which would be the correct solution.

Risks	C	S	L	R.I.	Preventive measures	Mitigation measures
Problems between group member	I	4	2	8	Clearly defined roles and responsibilities	Open communication channels, involve supervisor in the solution
Long-term illness among the team member	I	4	2	8	Supporting a healthy work-life balance and stress management techniques	Assigning alternates for each team member
Lack of cooperation with the company	E	5	1	5	Scheduling regular meetings	Have a point person who can address any issues or conflicts between the team and the company
Group members do not have the necessary competencies to complete the project	I	5	2	10	Assigning tasks based on individual strengths and expertise	Reallocate tasks to other team members with the required competencies
Lack of cooperation with the university	E	5	1	5	Schedule regular meetings with university	Have a point person who can address any issues or conflicts between the team and the university
A person leaves the group.	I	3	2	6	Encouraging open communication and feedback	Increase workload
Social Loafing	I	4	3	12	Clear goals and expectations for each team member	Daily scrums and time estimation for each task
Miscalculation of time estimation for tasks	I	3	3	9	Breaking tasks into smaller, manageable components	Re-prioritize tasks based on project goals and deadlines
Misunderstanding parts of the given task	E	3	2	6	Encourage open communication with advisor at company	Review done work as necessary to ensure alignment with project goals
The company stops using resources for project	I	5	1	5	Open communication channels with company	Use own resource to complete viable product

Table 2: Risk-matrix

Abbreviation

C: Category,S: Severity, L: Likelihood, RI: RISK Impact, I: Internal, E: External

3.3.2 Peer Reviews and Feedback from Supervisors

After we finished investigating GCP´s security functions for our project, we wanted to make sure that the quality of our work was of the required standard. When we mention “our work” we mean to discuss, and plan who and how to solve tasks, then set time estimation for completing various tasks and in the end review it by the group. The review included 6 steps which are shown in Table 3 underneath. After approval, the work was added to the report. That's why we decided to do a peer review process. Peer review is a process where other experts in the same field evaluate an author's scientific work, research, or ideas. It helps writers to improve the quality of their work by finding any errors that need to be fixed (Kelly et al., 2014, p. 227-243). We executed this process in a two-step approach to achieve the highest possible quality.

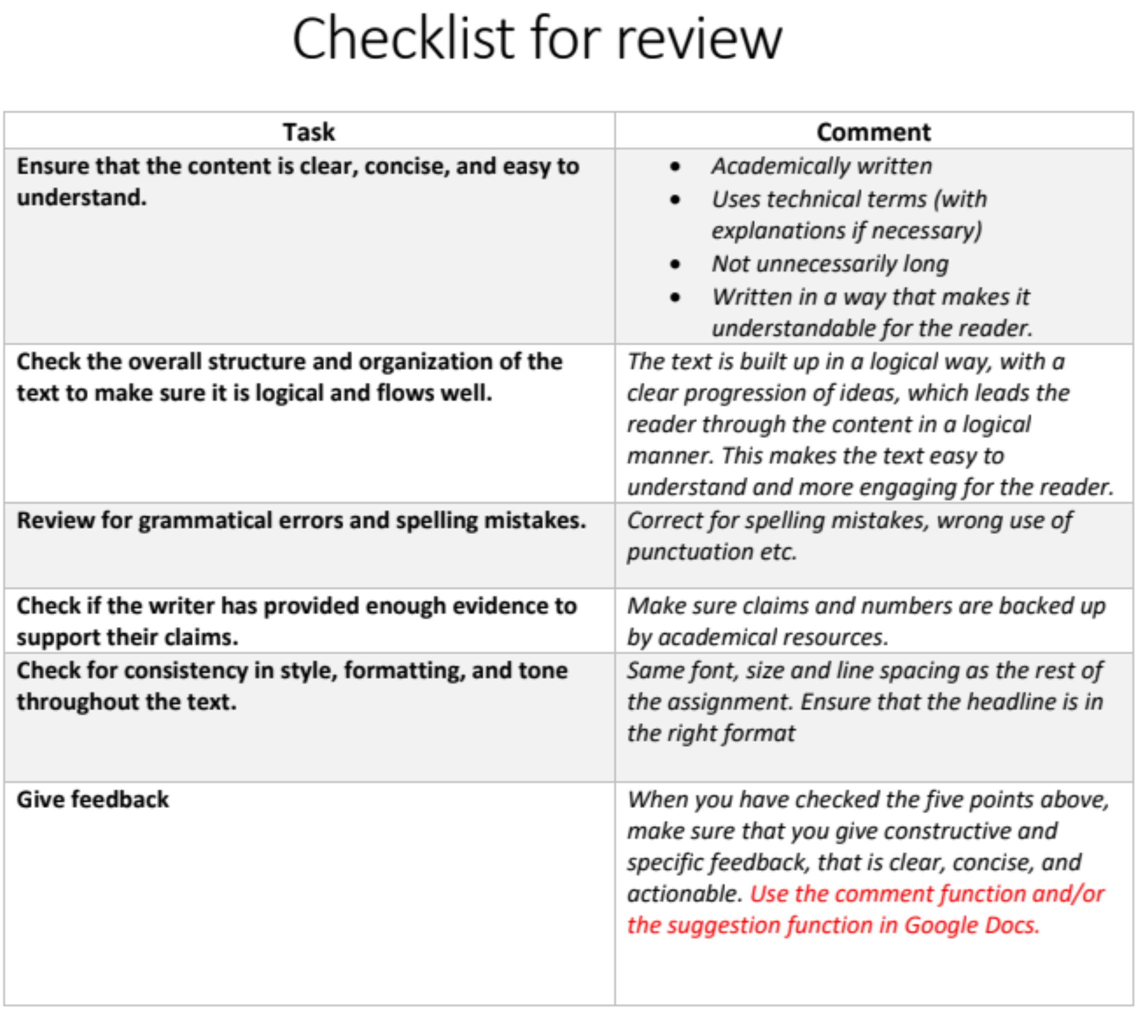
Step One: Creation and Utilization of a Checklist Document for Peer Review

Firstly, we created a checklist document for the peer review process (figure 1), a guideline that we all agreed to adhere to. Using this document, we critically evaluated the texts concerning our findings and project management, inserting suggestions for corrections in the form of comments.

Step Two: Consultation and Revision Based on Feedback

After making the necessary adjustments and corrections, we sought the expertise of our consultants. We asked them to evaluate our work from both technical and academic perspectives. They provided feedback on relevant parts of our work within the text. Based on their input, we revised some sections together in meetings to further enhance the quality of our project.

This peer review process was an essential component of our quality assurance approach, which also included risk management, communication and cooperation, and the use of appropriate tools and technologies. By following these well-defined rules and processes, we were able to ensure that our project implementation and the result report to Netsecurity were of the highest possible quality.



Checklist for review

Task	Comment
Ensure that the content is clear, concise, and easy to understand.	• *Academically written* • *Uses technical terms (with explanations if necessary)* • *Not unnecessarily long* • *Written in a way that makes it understandable for the reader.*
Check the overall structure and organization of the text to make sure it is logical and flows well.	*The text is built up in a logical way, with a clear progression of ideas, which leads the reader through the content in a logical manner. This makes the text easy to understand and more engaging for the reader.*
Review for grammatical errors and spelling mistakes.	*Correct for spelling mistakes, wrong use of punctuation etc.*
Check if the writer has provided enough evidence to support their claims.	*Make sure claims and numbers are backed up by academical resources.*
Check for consistency in style, formatting, and tone throughout the text.	*Same font, size and line spacing as the rest of the assignment. Ensure that the headline is in the right format*
Give feedback	*When you have checked the five points above, make sure that you give constructive and specific feedback, that is clear, concise, and actionable. Use the comment function and/or the suggestion function in Google Docs.*

Table 3: Checklist for review

3.3.3 - Communication and Cooperation

In this chapter, the group's progress and cooperation will be explained. It will also be explained why the group members agreed to use these selected solutions. It includes how the group members used and recorded working hours, which tools were used during meetings, task solving, and so on.

Management Tools

In this part, the five most important management tools that were used by the group to manage the project will be explained, including how these management tools played a vital part in the work process of this project. The most important tools we used were Discord, Trello, Google Docs, Office 365, and Microsoft Teams.

Discord

We agreed to use Discord as our main communication tool, especially written communication, as well as to track various goals such as the arrangement of meetings, document-sharing, and communication with our supervisors both from UiA and Netsecurity. The reason the group chose to use this application was primarily because of previous experience. We already had our own channel with an organization for different topics, which made it natural to carry on with Discord instead of using resources on establishing a new environment in another app.

Trello

Trello is a free online board, like a digital bulletin board. Trello has a straightforward card-and-list layout. To create lists, you must simply drag cards from one column to another. “To do”, “doing”, “ready for review” and “done”, for instance, are comparable to what we typed in our Trello board. A board like this is useful for group projects. This makes teamwork transparent and enables you to identify who is doing what. Additionally, we were able to use built-in features like time tracking, as described in time management.

Google Docs

Since everyone had experience with Google Docs, we decided to use it as our main tool for working on the report. It is also worth noting that Google Docs is a part of Google Workspace, which made it relevant for our project. We found it useful to be able to work on the same document simultaneously, as well as the built-in features for commenting and adding suggestions. Another advantage of this tool was how easy it was to share the document. This made it practical when we needed a review from the Netsecurity or our UiA-supervisor, who also took advantage of the opportunity to comment on our work. Additionally, it creates backups in the cloud, which decreases our risk of losing vital parts of our documents.

Microsoft Teams/Zoom

Sometimes, the group members couldn't meet in person, so they needed to meet online with supervisors. Both Microsoft Teams and Zoom are used for this purpose. The group members have agreed not to limit themselves to one program, and the meeting organizer will choose the one they prefer. Both programs have satisfactory video and voice quality and options.

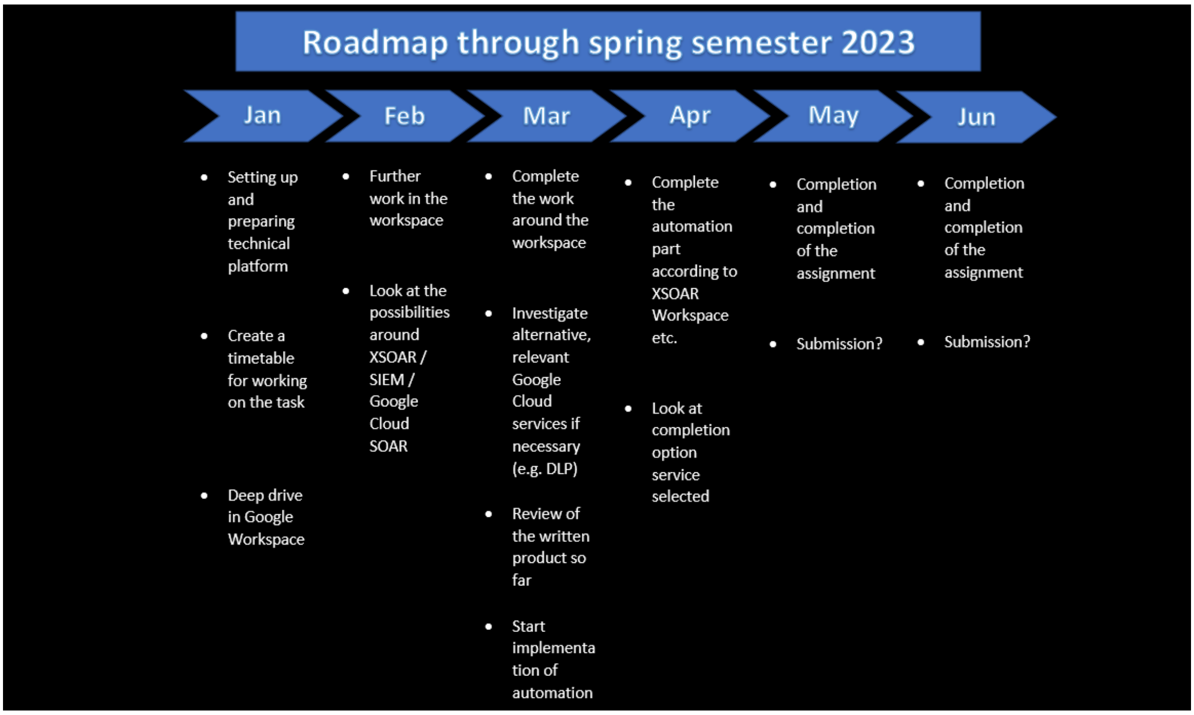
4.0 - Project Implementation

Project implementation is the process of putting a project plan into action to produce the deliverables for clients or stakeholders (Indeed Editorial Team, 2023). This involves coordinating resources and measuring performances to ensure the project remains within its expected scope and budget (Indeed Editorial Team, 2023).

4.1 - Project planning

As previously described, the group agreed to use the Scrum methodology while working on the project. At the start of the semester, we arranged a meeting to set up a plan for all the sprints with a specified duration and deadline date for the given tasks. After some discussion between group members, a total of 6 sprints were planned with a duration of around three weeks per sprint. We carefully organized the sprints to strike a balance between having enough time to complete the planned tasks within the designated period and ensuring that each sprint was not so long as to impede finding solutions to arising problems and implementing necessary changes. This approach allowed us to remain agile and adaptable while also maintaining productivity and progress toward our main goal.

Once we had finalized the semester plan within our group, we scheduled a meeting with Netsecurity to present and discuss our plan, ensuring that it aligned with their available resources. This collaborative approach allowed us to identify any potential roadblocks and make any necessary adjustments, enabling us to work together effectively towards our shared objectives. Through close collaboration with Netsecurity, we developed a comprehensive roadmap that enabled us to prioritize our tasks effectively. By identifying key milestones and outlining the necessary steps to achieve them, we gained a clear overview of our project's progress and ensured that our efforts remained aligned with our goals. This approach allowed us to work efficiently and proactively toward the successful completion of our project. This is illustrated in Figure 1.



Roadmap through spring semester 2023

Jan	Feb	Mar	Apr	May	Jun
• Setting up and preparing technical platform • Create a timetable for working on the task • Deep drive in Google Workspace	• Further work in the workspace • Look at the possibilities around XSOAR / SIEM / Google Cloud SOAR	• Complete the work around the workspace • Investigate alternative, relevant Google Cloud services if necessary (e.g. DLP) • Review of the written product so far • Start implementation of automation	• Complete the automation part according to XSOAR Workspace etc. • Look at completion option service selected	• Completion and completion of the assignment • Submission?	• Completion and completion of the assignment • Submission?

Figure 1: Roadmap

We initially planned for our project to include four sprints, in addition to a pre-sprint and final sprint, making it a total of six sprints. The group scheduled each sprint to last for approximately three weeks, finding this duration to be an appropriate balance between completing substantial work and allowing for adjustments before the next sprint. This ensured a seamless flow of progress, without a significant time gap that could impede the ability to make necessary changes. To ensure continuous improvement, we held a Sprint Review at the end of each sprint before starting the next one. The group's sprint planning was based on the roadmap as displayed in figure 1.

4.2 - Daily Scrum

Daily Scrum is a daily meeting of around 15 minutes, usually held at the same time and place every day. The purpose of the meeting is to inspect progress toward the sprint goal, and adapt the sprint backlog as necessary, adjusting the upcoming planned work (Schwaber & Sutherland, 2020, p. 9). Applying daily scrum to our project, helped the group track the progress of each group member, and to synchronize the tasks of the day. Each member was then able to answer the following three questions each day:

1. What did you do yesterday to help the team meet its sprint goal?
2. What will you do today to help the team meet its sprint goal?
3. Are there any obstacles preventing you from making progress toward the sprint goal?

By requiring each member to answer the three questions, we were able to ensure that we were on track towards the sprint goal, and able to handle problems at an early stage instead of the problems gathering up towards the end. As mentioned earlier, this is a valuable way of removing the danger of social loafing.

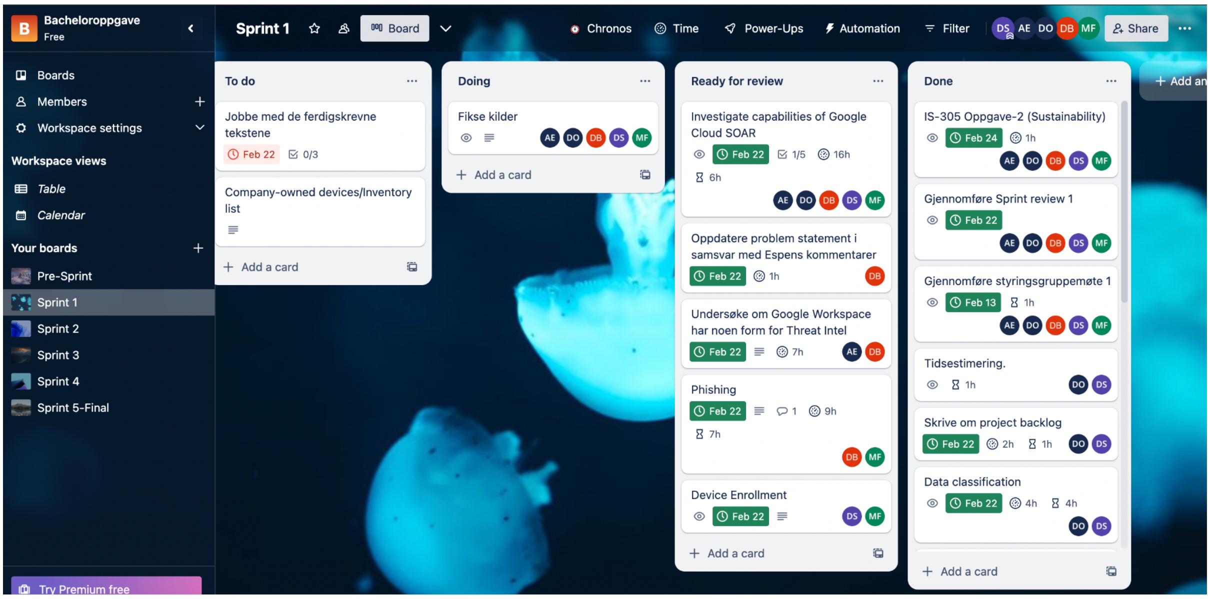
We had 1-2 days scheduled each week for group sessions at the university, and most of the daily scrum meetings were held through Discord voice channels. We considered this the most practical and effective way to fulfill the daily scrum requirements, especially considering many of the group members had a relatively long way to travel from their residence to the university.

4.3 Backlog

The Product Backlog is an emergent, ordered list of what is needed to improve the product. It is the single source of work undertaken by the Scrum Team (Schwaber & Sutherland, 2020, p. 10). As explained in Chapter 4.1, our product backlog was based on the roadmap created by the project owner. Since cybersecurity was a new subject for us, the product owner often influenced the development by helping us understand and to make trade-offs (Schwaber & Sutherland, 2020, p. 10). The backlog gave us an overview of what needed to be done, and who was responsible for each task. We used Trello to organize these tasks, as explained in Chapter 3.3.3. Figure 2 illustrates what a typical sprint backlog looked like in the middle of working on a sprint.

The Sprint Backlog is composed of the Sprint Goal (why), the set of Product Backlog items selected for the Sprint (what), as well as an actionable plan for delivering the Increment (how) (Schwaber & Sutherland, 2020, p. 11).

Most of the tasks for each sprint were planned before we started the sprint, however, some were also added as we found it necessary. We often asked our product owner for advice when we were unsure which backlog items to prioritize, as well as when we were unsure of the requirements for the relevant task.



To do

- Jobbe med de ferdigskrevne tekstene — Feb 22 — 0/3
- Company-owned devices/Inventory list
- Add a card

Doing

- Fikse kilder — AE DO DB DS MF
- Add a card

Ready for review

- Investigate capabilities of Google Cloud SOAR — Feb 22 — 1/5 — 16h — 6h — AE DO DB DS MF
- Oppdatere problem statement i samsvar med Espens kommentarer — Feb 22 — 1h — DB
- Undersøke om Google Workspace har noen form for Threat Intel — Feb 22 — 7h — AE DB
- Phishing — Feb 22 — 1 — 9h — 7h — DB MF
- Device Enrollment — Feb 22 — DS MF
- Add a card

Done

- IS-305 Oppgave-2 (Sustainability) — Feb 24 — 1h — AE DO DB DS MF
- Gjennomføre Sprint review 1 — Feb 22 — AE DO DB DS MF
- Gjennomføre styringsgruppemøte 1 — Feb 13 — 1h — AE DO DB DS MF
- Tidsestimering. — 1h — DO DS
- Skrive om project backlog — Feb 22 — 2h — 1h — DO DS
- Data classification — Feb 22 — 4h — 4h — DO DS
- Add a card

Figure 2: Screenshot from Backlog in Trello

As visualized in figure 2, there is a list of tasks displayed, and the group sat the deadline for when the various tasks were expected to be completed - with the status of the tasks “To do”, “Doing”, “Ready for Review”, and the final step “Done”. In addition to our backlog, the group members could at any time update the status on Trello to determine whether the task had been assigned.

4.4 - Sprint review

The goal of the Sprint Review is to present the work or tasks that were completed during the sprint between all team members, where the results of completed work and what was not completed are also discussed between the group members (Visual Paradigm, n.d.). At the end of each sprint, the group held a sprint review meeting to assess the sprint's outcome and plan for future adaptations. During the Sprint Review meeting, the group discussed which product backlog items have been completed through the previous Sprint and which product backlog items had not been done. Further, the group discussed what we thought about the results of the completed tasks. Finally, the group also discussed what needed to be improved for the next sprint, as well as creating a plan for the next Sprint. This approach allowed us to identify any issues and areas for improvement, as well as those that were successful, and should be continued in the next sprint.

4.5 - Sprint retrospective

Sprint retrospective is an important part of the Scrum methods. It is used appropriately to reflect on new sprints with a view to improving quality and processes (Schwaber & Sutherland, 2020, p.10). in addition, Sprint retrospective also focuses on what needs to be done to improve. Through the Sprint meetings, we carried out a Sprint retrospective where all the group members discussed what worked well and what problems or challenges arose, not least what should be improved further in the process or for the next sprints.
Although the product owner did not directly participate in the sprint retrospective, the notes created after the meeting were discussed with the product owner at the next meeting, and the product owner was able to give us feedback. Furthermore, we discussed issues related to the sprint retrospective and gathered feedback from the product owner during the project management meeting. This approach has been invaluable in enabling us to reflect effectively on our past work and plan our future actions in alignment with our project goals. Thanks to this collaborative approach, we have been able to improve our Scrum processes and make necessary adjustments.

4.6 – Sprints

In this chapter, the group will present a summary of each of the sprints that were carried out during the project. *Please note that the project report mentioned in these chapters refers to the report delivered as a part of our project with Netsecurity, while this report is referred to as the bachelor report.*

4.6.1 Pre-sprint - Getting to know Google Workspace and planning of the semester (January 11 - February 1)

During the initial phase of the project, we dedicated our efforts to getting acquainted with the features and security capabilities of Google Workspace. Our primary focus was on understanding its functionalities and ensuring a secure working environment. We formulated a semester plan, established efficient work routines, and fostered collaboration within Google Workspace. Collaborative meetings were conducted with our supervisor and Netsecurity to establish clear objectives for each sprint and determine task prioritization. Additionally, we organized regular weekly meetings and received guidance from Netsecurity to effectively set up our Google Workspace environment.

To gain a comprehensive grasp of Google Workspace´s security functions, we distributed specific research responsibilities among team members. Each member delved into a particular area, such as password management, rules, or SSO, and subsequently shared their findings with the team, enhancing our collective knowledge. The intention was to incorporate these insights into our final report as part of our project progression.

4.6.2 - Sprint 1 (February 2 - February 22)

During Sprint 1, our project made significant strides toward achieving its objectives. We continued our exploration of Google Workspace´s security features, specifically focusing on data classification, device enrollment, and anti-phishing measures. Additionally, we investigated whether Google Workspace offers any Threat Intelligence resources, such as a comprehensive database. Another area of emphasis was the investigation of Google Cloud SOAR functionalities.

Throughout Sprint 1, we conducted a thorough review of the tasks completed during the pre-sprint phase. This allowed us to assess our progress and identify areas for improvement. We also engaged in productive meetings with our supervisor and Netsecurity, receiving valuable feedback and guidance to enhance our work and keep us on track.

As we moved into Sprint 2, we scheduled further meetings with Netsecurity and our supervisor to continue receiving their guidance and support. Our plan involved diligently executing the planned tasks and incorporating the acquired knowledge into the project report. Moreover, we aimed to enhance the project report by implementing a new format for its chapters, ensuring a cohesive and organized presentation of our findings.

4.6.3 - Sprint 2 (February 23 - March 15)

During Sprint 2, our project group dedicated significant time to planning the future development of our project report. Our primary focus was on dividing the chapters and determining how we wanted to structure the project report. To incorporate these changes into the report, we had a meeting with our supervisor from UiA. Based on their guidance, we made the necessary adjustments and agreed to schedule another meeting during sprint 3 to evaluate any further modifications to our setup.

We investigated further on key topics such as SOAR, Identity Security, Device Management, and Threat Intelligence, gaining increased knowledge on each of these topics to further improve our project report.

Additionally, a substantial amount of time was invested in reorganizing our previous project work into new chapters. After receiving key points for assessment from the product owner, we utilized them as a guideline to construct the new chapters. Although not all the chapters were fully completed during sprint 2 due to illness within the group, most of the work was finished in time for the sprint review.

Fortunately, the missing parts were not viewed as a major issue since both our group and the product owner believed that we were well within the project’s designated timeframe. As we move into sprint 3, our focus will be on further enhancing the project report and exploring additional features of Google Workspace.

4.6.4 - Sprint 3 (March 16 - April 12)

During this sprint, our project group made significant strides toward achieving our project goals. We successfully completed several crucial tasks, with a particular focus on enhancing various chapters of the project report. Overall, the group members were satisfied with the outcome of these completed tasks, and the feedback received was generally positive, requiring only minor improvements. We conducted two important meetings during this sprint. The first meeting involved only our supervisor, who provided recommendations that were deemed beneficial for the group and would contribute to a stronger result. The second meeting involved both our supervisor and the product owner. In this meeting, we followed a well-prepared agenda and received substantial feedback that greatly helped improve the report.

However, due to a shortened time frame resulting from the Easter holiday, the group members were unable to review all the comments and suggestions provided for further improvements. Nevertheless, these outstanding tasks were incorporated into sprint 4 and were not expected to cause any significant delays, as per our group's plan. The group faced several challenges during this sprint. One of them was the need to condense and streamline the already written chapters, making them more concise.

4.6.5 - Sprint 4 (April 13 - May 3)

In Sprint 4, our project made significant progress in accomplishing the remaining tasks crucial for finalizing the bachelor's thesis report. This allowed us to shift our focus in the final sprint toward improving the existing content. A large part of the sprint was spent on reviewing each of the chapters to be able to add and investigate additional features that should be covered. We also started conducting tests of the rules created in the admin console.

Throughout the sprint, our group encountered challenges in conducting tests due to limited familiarity with the SOAR platform. We also investigated the triggering of verification challenges, due to a request from Netsecurity. We discovered that it was not possible to directly activate this function, however, it is possible using custom rules. Further information about this is covered in chapter 1.1 of the project report.

4.6.6 - Final sprint - Completion of the project (May 4 - May 16)

The final sprint marked the culmination of our project, as we made significant strides in completing the remaining crucial tasks for finalizing our bachelor's thesis report. Having successfully accomplished the necessary groundwork in the previous sprints, we shifted our attention in this final sprint towards enhancing the existing content and ensuring the report´s overall quality. One of our primary objectives for this sprint was to commence writing the reflection and conclusion chapter, which would provide a comprehensive overview of our findings and insights gained throughout the project. We aimed to summarize the key takeaways and reflect on the challenges, successes, and lessons learned during the research and implementation process.

With the completion of these tasks in the final sprint, we successfully concluded our project and prepared the bachelor´s thesis report for submission. Our collective efforts, coupled with the support and guidance we received, enabled us to overcome challenges, meet our objectives, and produce a comprehensive and well-structured report that showcased our research findings and the knowledge we gained throughout our project journey.

5.0 - Testing and Implementing Google Workspace in XSOAR

In this section, we will explore the process of testing and implementing customized security rules within the Google Workspace Admin Center. By carrying out functional testing, we ensure that the rules are effective and meet the organization's specific security needs. Challenges faced during the project, such as defining working rules and understanding the system, will be addressed. Furthermore, we will discuss XSOAR implementation, which involves connecting the alarm source, mapping data, and configuring playbooks to automate security tasks and responses tailored to the Google Cloud Platform environment.

5.1 - Testing Google Workspace Rules

In this chapter, we will discuss the various challenges and methods employed during the project to implement and test customized rules within the Google Workspace Admin Center. Our project required testing to ensure the functionality and effectiveness of the rules we defined on Google Workspace, which were tailored to address the specific security concerns that could be needed in the future. These tests focused on ensuring that the rules were properly configured when using Google Workspace as a standalone product, and on observing their effectiveness by monitoring alerts through the Alert Center.

5.1.1 Test Methodology

Functional testing is used to verify the functionality of the rules being implemented within the Google Workspace Admin Center (Mothiso, 2023). Functional testing ensures that the functions satisfy the specified requirements based on the client's needs. A requirement specification document (Attachment 2) is used as a guide for testing the application, and test data were crafted based on this document. Test cases are prepared, and the Google Workspace security rules are tested in a real environment to check whether the actual result aligns with the expected result. The importance of functional testing lies in describing the execution and behavior of the rules within the system (Softwaretestinghelp, 2022).

After deciding to conduct a functional test, we researched the process and the steps involved. We observed that the testing process typically consists of determining the product features (Lambdatest, n.d.), identifying the input data (Javatpoint, n.a.), determining the system output features, executing the test cases computing and comparing the actual and expected results (Motiso, 2023). As a result, we established a methodology that adheres to these testing processes, while being tailored to our specific testing subject. Our methodology for functional testing involved the following steps:

1. Identifying the requirements: We began to analyze what an organization can need if they wanted to use google workspace as a standalone product.

2. Defining the rules: Based on the identified requirements, we set up customized rules in the Google Workspace Admin Center to detect and respond to specific security concerns, for example, data protection.

3. Setting up the testing environment and determining the system output: We created a controlled testing environment to mimic different scenarios that would trigger the defined rules. In the testing environment, some of our admins behave as malicious users to mimic real-world situations. In these situations, the system should trigger security alert and warn the admin about the incidents.

4. Executing the tests: We carried out a series of tests to verify the customized rules work. Users did malicious behaviors that can trigger the rules. And we observe the system's response, such as issuing warnings or taking specified actions.

5. Analyzing the test results: After each test, we analyzed the results to determine whether the rule worked or not and fulfilled our expectations.

6. Documenting the findings: Throughout the testing process, we documented our findings, including the test scenarios, results, and any adjustments made to the rules. This documentation was crucial for reporting to Netsecurity.

By following this approach, we ensured that the customized rules were functional, effective, and met the organization's specific security needs.

5.1.2 Challenges

One of the most challenging aspects of the project was implementing and testing customized rules in the Google Workspace Admin Center. Google Workspace includes a set of predefined security rules designed to detect well-known security breaches. However, these rules tend to be general and fundamental, so organizations may need to define additional and specific rules to enhance their security, according to their needs. Therefore, in the report we will submit to Netsecurity, we first provided information about these rules. To have proof of concept, we have defined and tested for their effectiveness.

Since we lacked previous experience in this area, defining working rules posed a challenge for us. To ensure a rule works correctly, it is necessary to first determine which log to examine and then verify that the data found in that log meets specific conditions. The system issues a warning and acts if needed, when it obtains data that meets these conditions. Familiarizing ourselves with these log data, entering the correct conditions, and taking appropriate actions were the main problems we needed to solve.

At the beginning of the project, we tried to create rules and test them based on the information we obtained from Google's resources. For example, a rule was designed to block users who attempted to use leaked passwords on the internet. However, during our tests, we noticed that the rule did not trigger even when some users changed their passwords to leaked passwords. We also conducted different tests but could not obtain any results. Since we were still learning the system, we paused the tests to understand how it works.

Later, we discussed the issue with our consultant at Netsecurity and tried to find a solution. Although our consultant had experience with similar platforms, Google Workspace was a new and unknown area for them as well. During our joint meetings, we defined different rules and tested them, but we encountered similar issues; despite defining the rules correctly, we could not trigger them and receive security warnings. We searched the Google documentation regarding the issue, but we did not find any known issues related to it.

Eventually, we found that to define, edit rules, or see the alerts, even admins require extra permissions. The documentation mentions that the ability to create reporting rules vs. activity rules depends on your Google Workspace edition, your administrative privileges, and the data source. (Google Workspace Admin, n.d.) After the super admin granted extra permissions, our tests produced results, and we were able to see the alerts triggered by the rules.

According to the tests we conducted, if a user used certain predefined words in emails and Google Chat, a warning would be sent to the Google Workspace administrators according to data protection principles. The expected outcome occurred during our tests, and the rule was triggered, sending a warning to the system. Moreover, we later defined rules that would be triggered when a file was created in Google Drive and rules against phishing emails, and we tested them. In the end, we achieved positive results from our tests and reached a proof of concept.

At the very beginning of the project, we also had some issues with acquiring all the licenses necessary for taking advantage of the admin console. These were however resolved within the first sprint after valuable help from the project owner.

Another challenging aspect of the project was navigating through the extensive amount of documentation for the Google Cloud Platform. To fully be able to document the possibilities and power that are built into the platform, we had to spend extensive resources reading a vast amount of documentation. As the project progressed, we became more familiar with the documentation, and navigating between the different features became easier.

A helpful project owner, as well as an organized project, helped us overcome the challenges that arose, and even though there was some frustration at the time, we felt that each of the challenges lead to an improved product and valuable experience for each of the members.

5.2 - XSOAR implementation

We have discussed the integration phase with the product owner and based on that discussion we got valuable information on how to implement GCP to XSOAR and what are the important factors in that process. According to Netsecurity, to implement XSOAR, the first thing you need is an alarm source. This refers to the security tool or service that generates security alerts or incidents. In this case, the alarm source is GCP, but it could also be from other providers such as Azure or Cisco. To ensure that there are no security breaches, GCP offers several authentication measures that can be taken, such as 2-factor authentication, advanced multi-factor authentication, single sign-on, password management, Gmail authentication, and login challenges. The alarm source can then be connected to the SOAR platform, typically through APIs which makes it easy to exchange data between the platforms. (Swimlane, n.d.)

When the alarm source is connected with the SOAR platform through an API, the SOAR platform can start processing the data. The data coming from the alarm source is often in a format that the SOAR platform can understand. The incoming data must be processed in a way that the SOAR tool, XSOAR in our case, can use for further analysis and decision-making. This process is known as "data mapping" and that involves creating a link between two distinct data models' tables or attributes. (Shahbaz, 2015, p.1) This mapping process is important as it ensures continuous communication between GCP and the XSOAR platform. Playbooks in Cortex XSOAR automate key security tasks like investigations, handling incidents and responses, replacing manual effort, and standardizing security operations. (Cortex XSOAR, 2022) Playbooks also allow for the filtering and enrichment of alarm data. Filtering involves sorting out false positives and irrelevant data so that only legitimate security threats are dealt with.

Enrichment, on the other hand, involves gathering more data related to security threats to provide a more comprehensive view of the threat landscape. During integration, to ensure the effective operation of the playbooks, filters, and enrichments should be properly arranged and made specific according to GCP. It is possible by coding playbooks; the flexibility of playbooks means they can be customized to perform any kind of operation if it can be coded.

The cornerstone of effective automated responses in XSOAR is the careful definition and configuration of playbooks during the implementation phase. These playbooks are tailored to handle incoming alarms, trigger appropriate communication, and initiate technical responses according to the specifics of the Google Cloud Platform (GCP) environment.

Additionally, during implementation, it's essential to set up communication channels and protocols. This enables XSOAR to keep all stakeholders informed about the incident status. For more severe incidents, technical responses such as isolating infected systems, blocking malicious IP`s, or initiating a patch management process, should be predefined according to GCP specifics. This ensures streamlined and effective incident management.

Threat intelligence is a crucial aspect of XSOARs integration with GCP. By pulling data from various platforms, XSOAR enriches security alerts, offering crucial insights about threats. This intelligence, which includes details on malicious IPs, URLs, domains, files, malware behavior, and threat actors, equips security teams with vital information to enhance the speed and accuracy of their responses to alerts from GCP.

As a summary of the information presented in this part, please refer to the attached flowchart underneath (Figure 3). It gives a clear, visual representation of the XSOAR pipeline, starting from the alert source and leading up to the incident response. The flowchart illustrates the steps of XSOAR integration, the use of Cortex SOAR and XSOAR playbooks, alert data enrichment with log data, and the final stages of analyst analysis and incident response. This flowchart will serve as a useful reference for understanding the overall process and interaction between different stages.

In conclusion, using a SOAR platform like XSOAR with Google Cloud Platform can streamline security operations, making it more efficient and effective. From setting up the alarm source to automating responses using playbooks, every step can be customized to fit organizations’ unique needs.

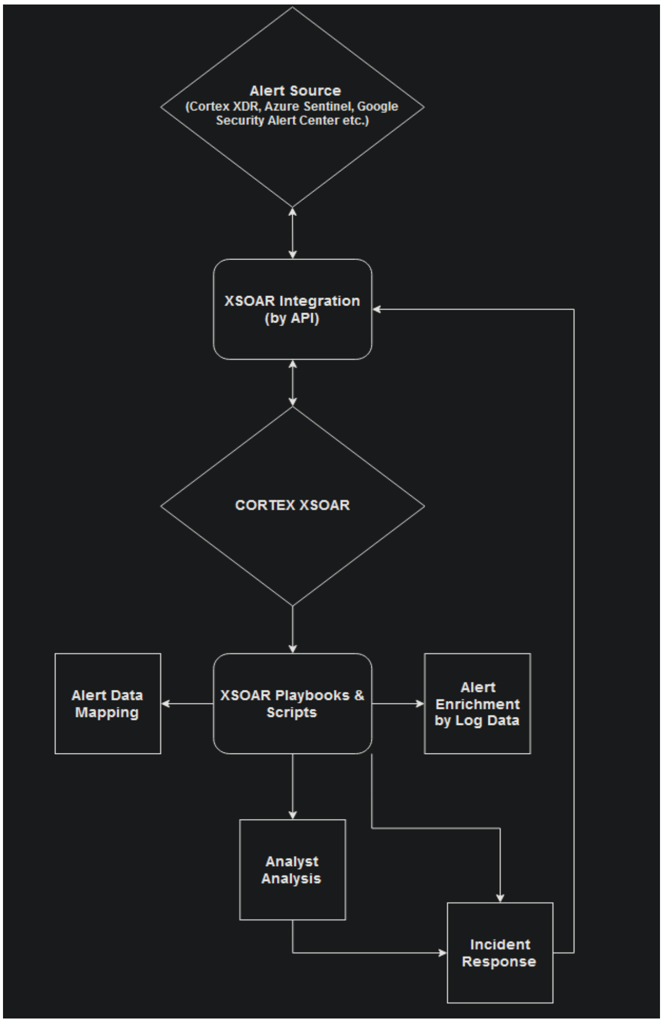

Alert Source
(Cortex XDR, Azure Sentinel, Google Security Alert Center etc.)
XSOAR Integration (by API)
CORTEX XSOAR
Alert Data Mapping
XSOAR Playbooks & Scripts
Alert Enrichment by Log Data
Analyst Analysis
Incident Response

Figure 3: XSOAR Flowchart

6.0 - Reflection

This bachelor project has contributed to new experiences and great learning outcomes. In this chapter, we will reflect on the experiences we had while working on the project, as well as what we have learned.

Before we decided to take on the project, the group was aware that there would be a steep learning curve due to limited experience with the Google Cloud Platform. We had to take charge of the organization of our project and put in a lot of effort into reading Google documentation and exploring the platform. Luckily, we also received a lot of help from Espen Abildgaard, who used his expertise to guide is through the extensive amount of documentation. We also thought it was an advantage that the group had worked together on previously, although with a different composition. We also found our previous experience with Scrum to be extremely helpful in the start of the project, as it made it easier to create a plan for the project without having to do extensive research on the topic. Despite these previous experiences, it was still challenging to put together a project of this size. By taking advantage of each other's skill sets, as well as adapting to changes throughout the project we are satisfied with how the project turned out.

We met Netsecurity through David Berg's previous relations with some of the colleagues, but it is also worth mentioning the Refresh IT arrangement which took place in late autumn 2022. This gave the group the possibility to check out other companies and their ideas for a bachelor project, which ultimately led to us deciding to go with the project Netsecurity already had presented to us. We also found the course *“Samskaping - kommunikasjon og prosjektarbeid”,* as well as *“Tjenestedesign og forretningsmodeller”* to be particlarly useful, especially when it came to project management. We have learned a lot about having to deal with expectations both from a client, as well as from school, who both have different sets of expectations and demands.

The learning curve has been steep, but ultimately the group is very satisfied with how the project turned out. We have learned a lot about cybersecurity, SOAR, and Google Cloud Platform, as well as gained increased experience in project management and the use of agile methodologies like Scrum.

6.1 - Further Development

When the project was planned, priorities were determined, and the scope of the project was narrowed down. Since the project was long-term and comprehensive, research was conducted in line with the priorities needed by the company. During our work, the foundation of the project was established, based on this, the project needs more development and needs to be continuously developed. In this section, we will discuss the future development of the project.

1. Expansion and Enhancement of XSOAR Playbooks: Continuing development, maintenance, and configuration of rules and playbooks.

As technology and the cyber threat landscape evolve, it is essential for Netsecurity to continuously develop and improve its security measures, including the use of XSOAR and Google Workspace Integration. The following points indicate some key aspects of the further development of the SOAR tool:

Continuous SOAR Integration Improvement: As Google Workspace evolves, maintaining up-to-date integration with the SOAR tool is vital. Regular updates provide security analysts with the latest features and threat intelligence.

SOAR Integration and Maintenance: As Google Workspace evolves, it's vital to maintain up-to-date integration with the SOAR tool. Regular updates give security analysts access to the latest features and threat intelligence. To ensure SOAR's effectiveness and reliability, performing regular maintenance is also important. Software updates, performance monitoring, and issue resolution help prevent system failures and security breaches.

Configuration of Rules and Playbooks: To improve detection and response, configure new rules and playbooks tailored to Google Workspace features. Currently, predefined rules and playbooks work well with other cloud platforms. Enhance threat detection and response by updating and refining criteria and creating new playbooks to address specific Google Workspace incidents.

Training and Education: As the SOAR tool evolves and new features are added, it is crucial to train security engineers and analysts on effectively using these features. Regular training and educational resources ensure the team stays up to date with the latest best practices and has a better understanding of managing security incidents.

2. Development of a GCP and/or Workspace Management Service:

Another important improvement should be developing a service focused on the maintenance and operation of a GCP and/or Workspace environment. This service could include the development of a system to create and push out new detection rules to customer environments, thereby enhancing their security posture. Using the available APIs (https://developers.google.com/admin-sdk), this service could also encompass managing user accounts and licenses, including rights management and the onboarding of new users. This would offer a comprehensive solution for businesses seeking to manage their cloud environments more efficiently.

3. Provision of a GCP / Workspace Service for Compatible Customers:

Finally, there should be an exploration of opportunities to develop and deliver a service for GCP/Workspace. The company should aim to create and configure a new GCP / Workspace environment from scratch for compatible customers. This service would be akin to those provided for Microsoft Azure and would parallel the work done by Microsoft consultants.

The goal should be to provide an end-to-end solution for customers seeking a comprehensive solution for a Google Cloud environment. This service could greatly assist the customer by streamlining their business's cloud processes and enhancing the security of their cloud computing ventures.

These points were initially outside the scope of our project, but our aim is to sketch out a roadmap for further development for the company. These further development suggestions not only build upon the existing project but also allows for the exploration of new, beneficial possibilities. In conclusion, the goal of further development is to continuously develop the service's capabilities while also adding significant value for the users and the customers.

7.0 Conclusion

To conclude the report, we would like to mention first that during the bachelor project we, the group members, worked on a project description, where the purpose of the task was to write a report to UIA that describes the project`s implementation. In addition to a second report which is delivered to Netsecurity itself, there we have documented our findings that have been achieved through experimentation.

The goal of our task was to examine Google's cloud security monitoring platform and come up with recommendations for Netsecurity that they can implement in their system. Throughout the semester we have also evaluated several Google Workspace security functions and the role of "Managed security services providers". So that Netsecurity can improve cybersecurity. Throughout the project, we managed to navigate rule definition challenges and additionally performed functional tests to establish custom security rules for Google Workspace. At the same time, we have explained the process of Google Cloud Platform (GCP) integration in XSOAR, which involved data mapping and playbook configuration to automate tasks.

Again, during the semester, we chose to implement a controlled system between us that included the status of tasks and our roles to get a neater overview of the status. Therefore, we agreed to adopt the "Scrum methodology", where each group member was divided into roles that we felt were best suited. These roles were: "Scrum Master", "product owner" and "developers".
We are satisfied to implement such a system because this enabled efficient progress and allowed us to focus on key aspects of the project using the "MoSCoW-method" of prioritization. We would also like to mention that our project management strategy was comprehensive and included protocols for risk management, communication, and peer review to ensure high-quality project implementation.

All in all, we can safely say that throughout the semester we have finished the project, thanks to our choice of implementation method we managed to reach the goal.

8.0 - List of references

Benzoni, E. (2020, March 17). Automation in cybersecurity: Benefit or threat? Sumo logic. Retrieved: 02.03.2023 from: https://www.sumologic.com/blog/cyber-security-automation-benefit-or-threat/

Bradley, T. (2023, January 27). The keys to effective identity security for 2023. *Forbes.* Retrieved: 12.03.2023 from: https://www.forbes.com/sites/tonybradley/2023/01/27/the-keys-to-effective-identity-security-for-2023/?sh=3736117d1b73

Businesswire. (2022, July 22). *Google´s Cloud strengths attracting European firms.* Retrieved 15.04.2023 from: https://www.businesswire.com/news/home/20220722005068/en/Google%E2%80%99s-Cloud-Strengths-Attracting-European-Firms

CISA, (2022, February 10). *Ransomware Awareness for Holidays and Weekends.* Retrieved 13.03.2023 from https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-243a

Crowdstrike (2023). *Global Threat Report.* Retrieved 11.02.2023 from: https://www.crowdstrike.com/global-threat-report/

Levinson, M. (2022, November 16), *Holiday, Weekend Ransomware Attacks Continue to Hit Companies Hard*. Retrieved 13.03.2023 from: https://www.cybereason.com/blog/holiday-weekend-ransomware-attacks-continue-to-hit-companies-hard

Cyberpedia (n.d.) *What is SOAR?* Retrieved 10.04.2023 from: https://www.paloaltonetworks.com/cyberpedia/what-is-soar

Google Workspace. (2023). *Pricing*. Retrieved 15.05.2023 from: https://workspace.google.com/pricing.html

Google Workspace. (2023, March 08). In Wikipedia. Retrieved: 22.01.2023 from: https://en.wikipedia.org/wiki/Google_Workspace

Google Workspace Admin Help (n.d.) Retrieved 26.04.2023 from: https://support.google.com/a/answer/11341109#zippy=%2Cprivileges-needed-for-creating-and-viewing-activity-rules%2Cgoogle-workspace-editions-with-access-to-activity-rules

Google Workspace Admin Help (2023a). *Setup basic mobile device management.* Retrieved 12.03.2023 from: https://support.google.com/a/answer/7400753?hl=en

Google Workspace Admin Help (2023b) *Manage mobile apps for your organization*. Retrieved 23.03.2023 from: https://support.google.com/a/answer/6328701?hl=en

Google Workspace Admin Help (2023c) *Wipe corporate data from a device*. Retrieved 14.04.2023 from: https://tinyurl.com/3jv3dw22

Google Workspace Admin Help (2023d) *View mobile devices that access work data.* Retrieved 16.04.2023 from: https://tinyurl.com/mwufmwz7

Google Workspace Admin Help (2023e) *Turn endpoint verification on or off*. Retrieved 02.05.2023 from: https://tinyurl.com/39dhdex3

Google Workspace Admin Help (2023f) *Advanced Protection Program.* Retrieved 13.02.2023 from: https://tinyurl.com/4k7bn9wh

Hoory, L. & Bottorff, C. (2022, March 25). What Is Waterfall Methodology? Here's How It Can Help Your Project Management Strategy. *Forbes. https://www.forbes.com/advisor/business/what-is-waterfall-methodology/*

Indeed Editorial Team (2023, March 11). *The 6 Steps of Project Implementation (With Tips).* Indeed. https://tinyurl.com/3m9y5xux

Javatpoint (n.d.) *Functional Testing.* Javatpoint. Retrieved 11.05.2023 from https://www.javatpoint.com/functional-testing

Karau, Steven J.; Williams, Kipling D. (1993). "Social loafing: A meta-analytic review and theoretical integration". Journal of Personality and Social Psychology. 65 (4): 681–706. https://doi.org/10.1037%2F0022-3514.65.4.681

Kelly, J., Sadeghieh, T., & Adeli, K. (2014). *Peer Review in Scientific Publications: Benefits, Critiques, & A Survival Guide. EJIFCC*, *25*(3), 227–243.

Køster, C. (2022, March 3). Slik gjør du enklere prioriteringer ved bruk av MoSCoW-metoden. *Smidigbloggen.* https://www.smidigbloggen.no/slik-gjor-du-enklere-prioriteringer-ved-bruk-av-moscow-metoden

Lambdatest (n.d.) *Functional Testing Tutorial: Comprehensive Guide With Best Practices*. Lambdatest. Retrieved 11.05.2023 from: https://www.lambdatest.com/learning-hub/functional-testing

Lavanya, N., & Malarvizhi, T. (2008, Marc 3). *Risk analysis and management: a vital key to effective project management*. Project Management Institute. https://www.pmi.org/learning/library/risk-analysis-project-management-7070

Leau, Y., Loo, W., Tham, W. & Tan, S. (2012). *Software Development Life Cycle AGILE vs Traditional Approaches. IPCSIT* (37), 162 - 163. http://ku-fpg.githuSoftware Development Life Cycle AGILE vs Traditional Approachesb.io/files/agile-traditional.pdf

Long, M. (2010, October 31). *Internal vs. External Software Quality*. Mike Long's Blog. https://meekrosoft.wordpress.com/2010/10/31/internal-and-external-software-quality/

Maxson, Charles. (2022, January 25). *Year in review: the Google Workspace Platform 2021.* Google Developers. Retrieved 21.03.2023 from https://developers.googleblog.com/2022/01/year-in-review-google-workspace.html

McMillan, Rob. (2013, May 16). *Definition: Threat Intelligence.* Gartner. https://www.gartner.com/en/documents/2487216

Microsoft. (2023, February 21). *What is device enrollment?* Microsoft. https://learn.microsoft.com/en-us/mem/intune/user-help/use-managed-devices-to-get-work-done

Microsoft. (n.d.). What is two-factor authentication? Microsoft. Retrieved 08.03.23 from https://www.microsoft.com/en-us/security/business/security-101/what-is-two-factor-authentication-2fa

MoSCoW method. (2022, December 20). In Wikipedia. https://en.wikipedia.org/wiki/MoSCoW_method

Münch, J., Trieflinger, S. & Lang, D. (2019). Product Roadmap – From Vision to Reality: A Systematic Literature Review. *IEEE. https://ieeexplore.ieee.org/document/8792654*

Netsecurity. (n.d.) *About us*. Netsecurity. Retrieved 02.05.2023 from: https://www.netsecurity.no/en/about-us

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T. & Koucheryavy, Y. (2018) Multi-Factor Authentication: A Survey. MDPI. https://www.mdpi.com/2410-387X/2/1/1

Palo Alto Networks (n.d.) *What Is SOAR?* Palo Alto Networks. Retrieved 10.03.2023 from https://tinyurl.com/2762zkn3

Palo Alto Networks. (2021, June 3). *Cortex XSOAR Threat Intelligence Management.* Palo Alto Networks. https://www.paloaltonetworks.com/resources/datasheets/cortex-xsoar-threat-intelligence-management

Palo Alto Networks, (2023). *Playbooks*. Palo Alto Networks. Retrieved 27.04.2023 from https://tinyurl.com/3mb6twvt
Rausand, M. (2011) Risk Assessment: Theory, Methods, and Applications. Wiley. Retrieved from: https://tinyurl.com/2kt734m6

Software Testing Help (n.d.) *Functional Testing Vs Non-Functional Testing.* Software Testing Help. Retrieved 11.05.2023 from: https://www.softwaretestinghelp.com/functional-testing-vs-non-functional-testing/

Schwaber, K., & Sutherland, J. (2020). *The Scrum Guide.* Scrumguides. Retrieved from https://scrumguides.org/docs/scrumguide/v2020/2020-Scrum-Guide-US.pdf#zoom=100

Shahbaz, Q. (2015). Data Mapping for Data Warehouse Design, Elsevier, p. 1,Retrieved 27.04.2023 from https://books.google.no/books?id=pRChCgAAQBAJ&pg=PA1&source=gbs_toc_r&cad=4#v=onepage&q&f=false

Shastri. V.(2022, 11 October) Identity Security. Crowdstrike, Cybersecurity 101 https://www.crowdstrike.com/cybersecurity-101/identity-security/

Shay, R., Komundari, S., Kelley, P., Leon, P., Mazurek, M., Bauer, L., Christin, N. & Cranor, L. (2010. July 14). Encountering stronger password requirements: user attitudes and behaviors. *SOUPS '10: Proceedings of the Sixth Symposium on Usable Privacy and Security.* 1-20. https://doi.org/10.1145/1837110.1837113

Smith, J. (2020, 14 May). *79% of Organizations Have Experienced an Identity-Related Security Breach in the Last Two Years According to New Identity Defined Security Alliance Study.* Globe Newswire. Retrieved from https://www.globenewswire.com/news-release/2020/05/14/2033444/0/en/79-of-Organizations-Have-Experienced-an-Identity-Related-Security-Breach-in-the-Last-Two-Years-According-to-New-Identity-Defined-Security-Alliance-Study.html

Swimlane (n.d). Security Orchestration, Automation, and Response (SOAR) Capabilities. Retrieved 26.04.2023 from https://swimlane.com/assets/uploads/documents/SOAR_Capabilities_e_book___Swimlane.pdf

Techqualitypedia,(10.March 2020) *What is quality?*. Retrieved 12.05.2023 from: https://techqualitypedia.com/quality/

United States Department of Defense, (2017, January). Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs. Retrieved 14.04.2023 from https://web.archive.org/web/20170704192215/https://www.acq.osd.mil/se/docs/2017-RIO.pdf#page=36

Mothiso, D (2023, 3 February) A Guide to Functional Testing (With Types and Steps). Retrieved 11.05.2023 from https://www.indeed.com/career-advice/career-development/functional-testing

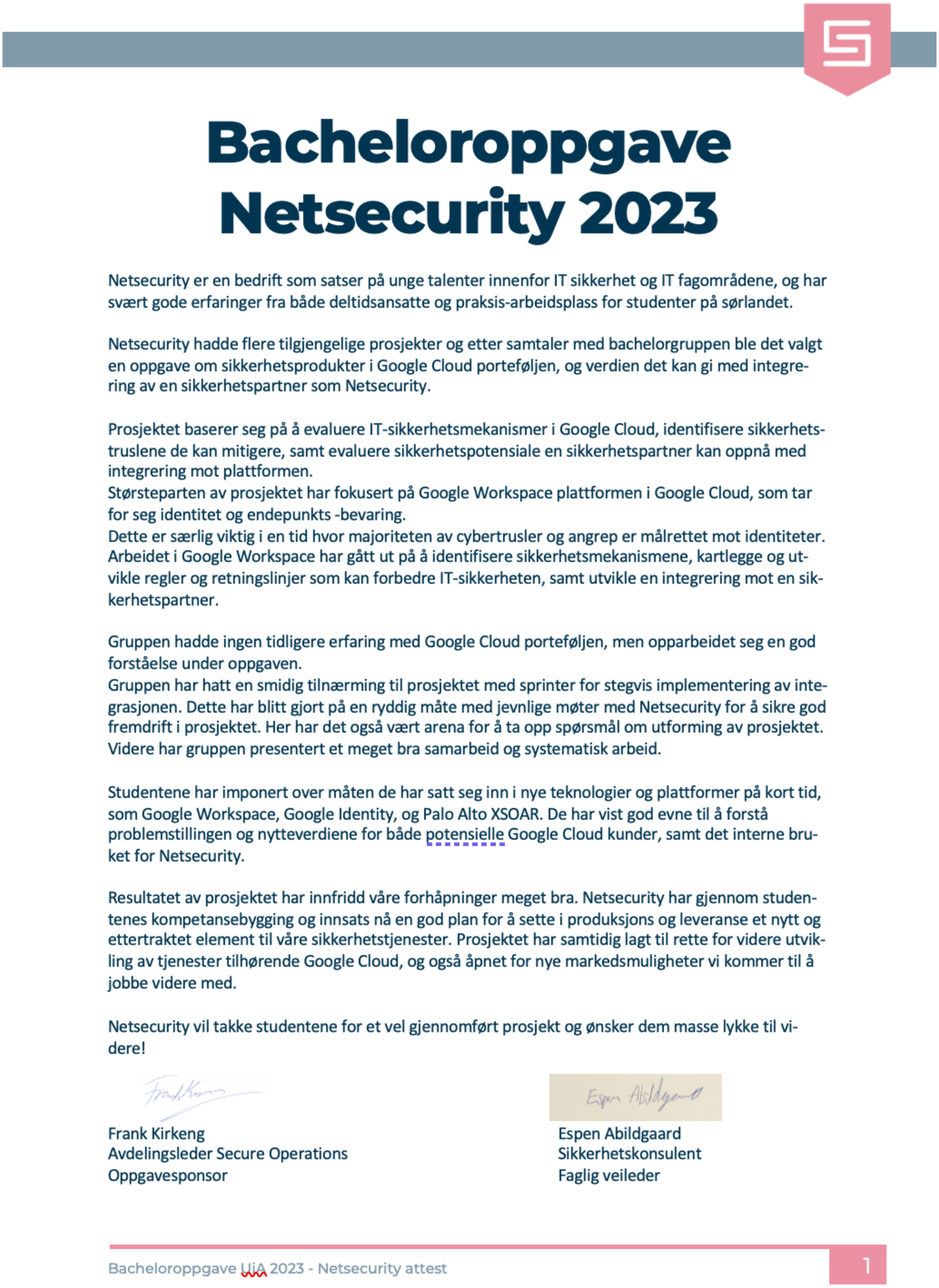
Verizon, DBIR, (2021) 2021 data breaches investigations report. Retrieved 26.04.23 from: https://www.verizon.com/business/resources/reports/2021-data-breach-investigations-report.pdf

Visual Paradigm, (n .d), What is sprint review. Retrieved 14.03.2023 from: *https://www.visual-paradigm.com/scrum/what-is-sprint-review/*

Attachments

Under this chapter, we, the group, have added some appendices, which are a requirement in addition to appendices which we thought were important to include. These include, among others: “Statement from the project owner”, “reflection of each individual group member`s own work”, “requirements specification document for test”, documents of our 5 sprint reviews addendum to a report that we have written, for Netsecurity itself.

Attachment 1 - Statement from the project owner



Bacheloroppgave Netsecurity 2023

Netsecurity er en bedrift som satser på unge talenter innenfor IT sikkerhet og IT fagområdene, og har svært gode erfaringer fra både deltidsansatte og praksis-arbeidsplass for studenter på sørlandet.

Netsecurity hadde flere tilgjengelige prosjekter og etter samtaler med bachelorgruppen ble det valgt en oppgave om sikkerhetsprodukter i Google Cloud porteføljen, og verdien det kan gi med integrering av en sikkerhetspartner som Netsecurity.

Prosjektet baserer seg på å evaluere IT-sikkerhetsmekanismer i Google Cloud, identifisere sikkerhetstruslene de kan mitigere, samt evaluere sikkerhetspotensiale en sikkerhetspartner kan oppnå med integrering mot plattformen.
Størsteparten av prosjektet har fokusert på Google Workspace plattformen i Google Cloud, som tar for seg identitet og endepunkts -bevaring.
Dette er særlig viktig i en tid hvor majoriteten av cybertrusler og angrep er målrettet mot identiteter.
Arbeidet i Google Workspace har gått ut på å identifisere sikkerhetsmekanismene, kartlegge og utvikle regler og retningslinjer som kan forbedre IT-sikkerheten, samt utvikle en integrering mot en sikkerhetspartner.

Gruppen hadde ingen tidligere erfaring med Google Cloud porteføljen, men opparbeidet seg en god forståelse under oppgaven.
Gruppen har hatt en smidig tilnærming til prosjektet med sprinter for stegvis implementering av integrasjonen. Dette har blitt gjort på en ryddig måte med jevnlige møter med Netsecurity for å sikre god fremdrift i prosjektet. Her har det også vært arena for å ta opp spørsmål om utforming av prosjektet.
Videre har gruppen presentert et meget bra samarbeid og systematisk arbeid.

Studentene har imponert over måten de har satt seg inn i nye teknologier og plattformer på kort tid, som Google Workspace, Google Identity, og Palo Alto XSOAR. De har vist god evne til å forstå problemstillingen og nytteverdiene for både potensielle Google Cloud kunder, samt det interne bruket for Netsecurity.

Resultatet av prosjektet har innfridd våre forhåpninger meget bra. Netsecurity har gjennom studentenes kompetansebygging og innsats nå en god plan for å sette i produksjons og leveranse et nytt og ettertraktet element til våre sikkerhetstjenester. Prosjektet har samtidig lagt til rette for videre utvikling av tjenester tilhørende Google Cloud, og også åpnet for nye markedsmuligheter vi kommer til å jobbe videre med.

Netsecurity vil takke studentene for et vel gjennomført prosjekt og ønsker dem masse lykke til videre!

	Espen Abildgaard
Frank Kirkeng Avdelingsleder Secure Operations Oppgavesponsor	Espen Abildgaard Sikkerhetskonsulent Faglig veileder

Bacheloroppgave UiA 2023 - Netsecurity attest 1

Attachment 2 - Reflection of own work

Marius H. Fjermeros

I have really enjoyed working on this project. Working with cyber security was a new experience for me, and I have learned a lot. Doing a deep dive into security measures that can be implemented in an organization has been very interesting, and I have also learned a lot about teamwork, and dealing with multiple parties with different expectations and demands. I believe what I have learned during this project will be very valuable for my future career, and I am very thankful for the cooperation both with my team members, the university, and Netsecurity.

Dlir Sharo

Through this project I have gained good experience and acquired valuable knowledge in Cyber Security and especially in Google Cloud Security Platforms and SOAR/XSOAR-platforms, which I can use further career, and have also gained more experience in project management and working within the team. Since my role in the project was Scrum Master. In addition, I have also been active to organizing meetings, and have actively participated in various meetings.
Have been active with writing, explaining both the UIA-report and the Netsecurity report. General this project was exciting. I have learned a lot during this project, and this will be very valuable for my further career and, I am very thankful for the cooperation with my exciting team members. And I'm also very thankful for the cooperation with the University and Netsecurity.

Dana D. Omar

Throughout the project I have done my best, contributed and learned very much of our task. Where I have written, explained and improved the various chapters both the report for UIA, but also the report for Netsecurity itself. Along the way, I and my group of colleagues have completed several different meetings. Like meeting with supervisor and client to get feedback and improvement on our report, not least sprint reviews and steering group meetings. Not least correcting comments that have appeared during the period, in addition to reading through, correcting and fixing the format of the report before final deliverable.

I would also like to mention that I have learned a lot about various aspects that we have implemented during the semester. What these are, what are they used for, why are these important in today's technology and digitalization, etc. These include, for example: “Google Cloud Workspace / Cloud security”, “SOAR”, “XSOAR” and beyond.

All in all, the work effort has been high, and I think the project has been exciting, as well as educational. Together with a fantastic group of colleagues, we have done what is needed to deliver the best possible result.

David
Throughout this project, I acquired valuable knowledge and experienced a wealth of new situations, particularly in the realms of project management and teamwork. These experiences posed numerous challenges, but each one offered an opportunity for growth and learning.

In the project's early stages, I contributed actively to planning and analyzing, drawing on my background in cybersecurity to clarify complex tasks for the group. I also assumed the responsibility of regular communication with the project owner, ensuring we met their expectations and requirements. I took it upon myself to conduct thorough research and examine past reports to improve the quality of our document. This research was crucial, especially since this was our team's first experience with a project of such magnitude. Deepening my knowledge of Google Cloud security systems and SOAR tools was particularly rewarding. This, combined with the communication and project management skills I honed, will undoubtedly be valuable in my future endeavors.

In retrospect, I think this project was challenging but also extremely rewarding. It allowed me to develop new skills and foster effective teamwork. We faced obstacles and encountered as opportunities for growth, and I am proud of the progress we made and the knowledge we gained. It was not just about completing a task, but also about personal and professional development. The relationships built and the experiences gained have made this journey truly valuable.

Alexandra Eriksen
Throughout this project, I have gained a wealth of new experiences and acquired valuable knowledge, particularly in the areas of project management and teamwork. These experiences have presented me with numerous challenges, from which I have learned and grown significantly. During the initial stages of the project, I actively contributed to the planning and analysis processes. I played a role in writing and structuring a substantial portion of the document ensuring its clarity and coherence. Additionally, I took on the responsibility of maintaining regular communication with the supervisor from UiA, ensuring that we stayed aligned with their expectations and requirements.
To ensure the quality of our bachelor document, I conducted thorough research and examined previous reports, seeking guidance on how to craft a comprehensive and professional document of this scale. Given that it was our team´s first experience with such a large-scale project, this research was crucial in guiding our approach and ensuring the document´s overall effectiveness. Overall, I view this project as a challenging yet highly valuable experience. It allowed me to develop new skills, such as project management, while also fostering effective teamwork. The obstacles I encountered throughout the process served as opportunities for growth, and I am proud of the progress I made and the knowledge I gained.

Attachment 3 - Requirement Specification Document for Test

Google Workspace Rules Testing

Version: 1.0

Date: 2023-01-15

Introduction

1.1 Purpose

The purpose of this software specification document is to provide a clear and comprehensive guide for testing the customized rules implemented within the Google Workspace Admin Center. This document will outline the requirements, functionality, and test scenarios necessary for the testing process.

1.2 Scope

This document covers the functional testing of customized rules in the Google Workspace Admin Center, focusing on the effectiveness of the customized rules.

System Overview

The Google Workspace Admin Center provides a set of predefined security rules to detect security breaches. To enhance security, organizations may need to define additional and specific rules according to their needs. The testing process ensures the correct implementation and functionality of these rules.

Requirements

3.1 Functional Requirements

The system must be able to detect and respond to events based on the defined rules.

The system must provide an alert mechanism (e.g., email notifications) when rules are triggered.

The system should allow administrators to define, edit, and manage rules.

Test Scenarios

4.1 Rule Configuration and Triggers

Test that the rule triggers when a user attempts to use a leaked password on the internet.

Test that the rule triggers when a user uses predefined words in emails or Google Chat.

Test that the rule triggers when a specific file is copied from Google Drive.

Test that the rule triggers when a file is created/uploaded in Google Drive.

Test that the rule triggers when a phishing email is detected.

4.2 Alert Mechanism

Test that the system sends an alert to the Google Workspace administrators when a rule is triggered.

Test that the alert contains relevant information about the event for the administrators to take appropriate action.

Test Cases

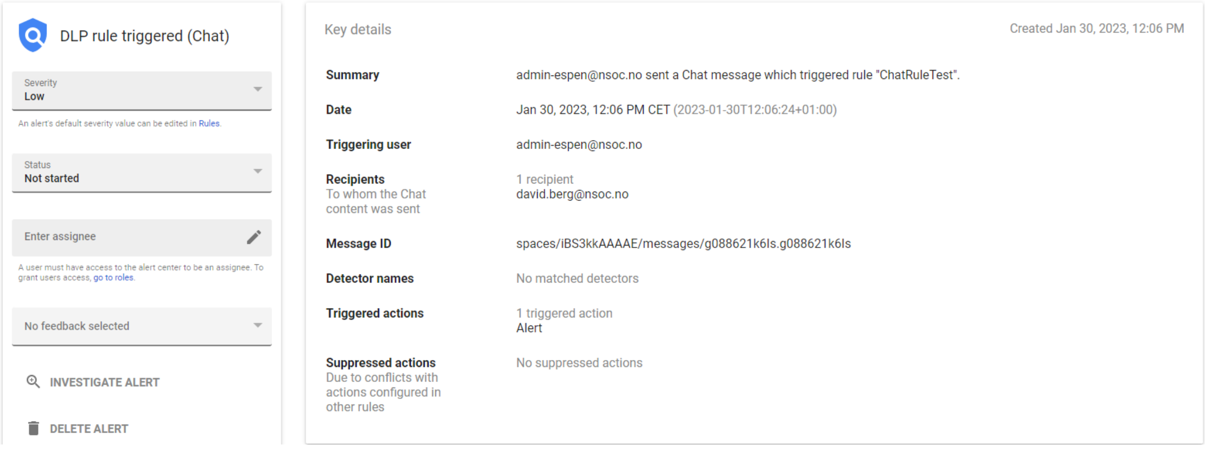
For each test scenario, prepare specific test cases that include:
Test case ID
Test case description
Preconditions
Test steps
Expected results
Actual results
Pass/Fail status
Remarks (if any)

This software requirement specification document serves as a guide for testing the customized rules within the Google Workspace Admin Center. It outlines the requirements and test scenarios necessary for ensuring the functionality and effectiveness of the rules in the system.

Tests

Test Case 1: Triggering a rule when a user attempts to use a leaked password
Test Case ID: TC-001
Test Case Description: Testing if the rule triggers when a user changes their password to a known leaked password.
Preconditions: Obtaining a leaked password from an open source.
Test Steps:
User changes their password to a known leaked password.
Expected Result: The system denies the password change and sends an alert to the admin.
Actual Result: The user can change their password to the known leaked password.
Pass/Fail Status: Fail
Remarks: After several tests, it is suspected that we are misconfiguring the rules. The test is paused until the problem is resolved.

Test Case 2: Triggering a rule when a user uses predefined words in emails or Google Chat
Test Case ID: TC-002
Test Case Description: Testing if the rule triggers when a user uses predefined words in emails or Google Chat.
Preconditions: Test users should have Google Chat and Mail access.
Test Steps:
Users use Google Chat and write a predefined magic word to trigger an alert.
Expected Result: An alert should be visible in the Alert Center, and the admin should be alerted.
Actual Result: The rule is triggered.
Pass/Fail Status: Pass



DLP rule triggered (Chat)

Severity
Low

An alert's default severity value can be edited in Rules.

Status
Not started

Enter assignee

A user must have access to the alert center to be an assignee. To grant users access, go to roles.

No feedback selected

INVESTIGATE ALERT

DELETE ALERT

Key details — Created Jan 30, 2023, 12:06 PM

Summary	admin-espen@nsoc.no sent a Chat message which triggered rule "ChatRuleTest".
Date	Jan 30, 2023, 12:06 PM CET (2023-01-30T12:06:24+01:00)
Triggering user	admin-espen@nsoc.no
Recipients To whom the Chat content was sent	1 recipient david.berg@nsoc.no
Message ID	spaces/iBS3kkAAAAE/messages/g088621k6Is.g088621k6Is
Detector names	No matched detectors
Triggered actions	1 triggered action Alert
Suppressed actions Due to conflicts with actions configured in other rules	No suppressed actions

Test Case 3: Triggering a rule when a specific file is copied from Google Drive

Test Case ID: TC-003

Test Case Description: Testing if the rule triggers when a user copies a specific document from Google Drive.

Preconditions: User should have Google Drive access.

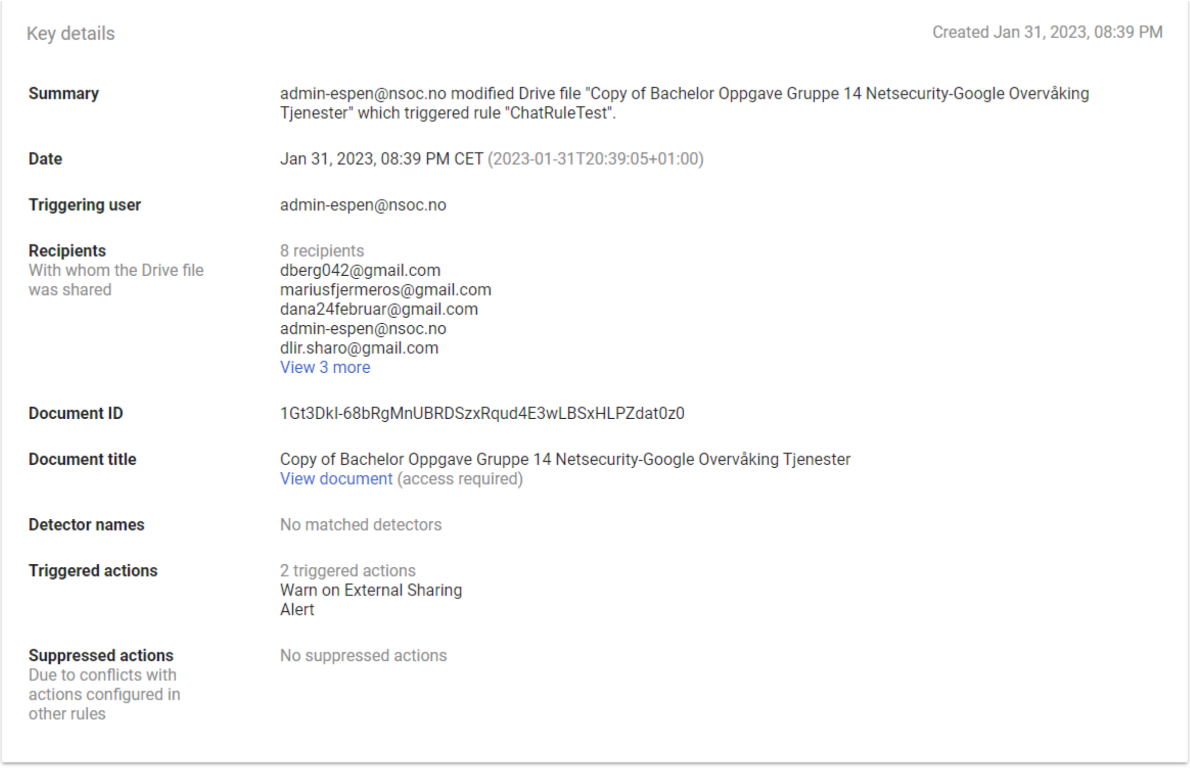
Test Steps:

The user attempts to copy a specific document from Google Drive.

Expected Result: A warning on external sharing is displayed, and an alert is sent to the admin.

Actual Result: The rule is triggered.

Pass/Fail Status: Pass



Key details — Created Jan 31, 2023, 08:39 PM

Summary	admin-espen@nsoc.no modified Drive file "Copy of Bachelor Oppgave Gruppe 14 Netsecurity-Google Overvåking Tjenester" which triggered rule "ChatRuleTest".
Date	Jan 31, 2023, 08:39 PM CET (2023-01-31T20:39:05+01:00)
Triggering user	admin-espen@nsoc.no
Recipients With whom the Drive file was shared	8 recipients dberg042@gmail.com mariusfjermeros@gmail.com dana24februar@gmail.com admin-espen@nsoc.no dlir.sharo@gmail.com View 3 more
Document ID	1Gt3DkI-68bRgMnUBRDSzxRqud4E3wLBSxHLPZdat0z0
Document title	Copy of Bachelor Oppgave Gruppe 14 Netsecurity-Google Overvåking Tjenester View document (access required)
Detector names	No matched detectors
Triggered actions	2 triggered actions Warn on External Sharing Alert
Suppressed actions Due to conflicts with actions configured in other rules	No suppressed actions

Test Case 4: Triggering a rule when a file is created/uploaded in Google Drive

Test Case ID: TC-004

Test Case Description: Testing if the rule triggers when a user uploads a file in Google Drive.

Preconditions: User should have Google Drive access.

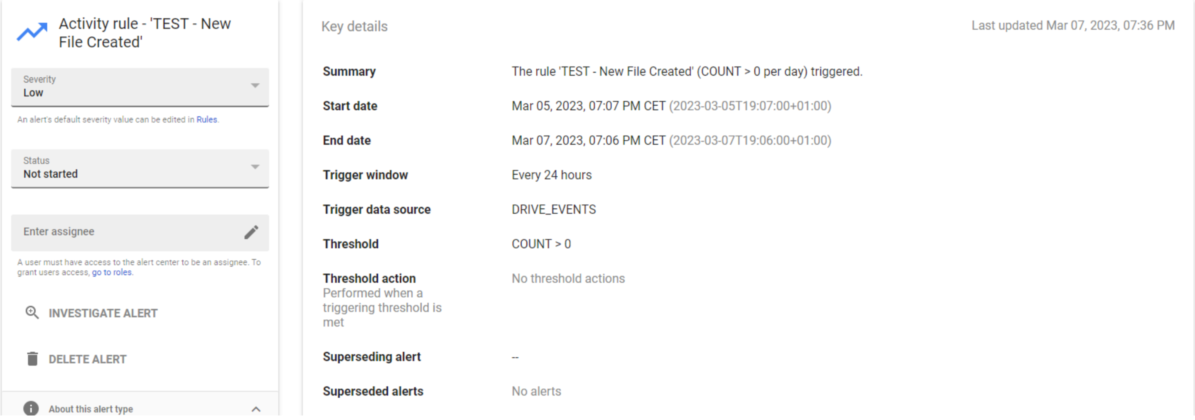
Test Steps:

The user attempts to upload a file in Google Drive.

Expected Result: An activity alert is sent to the Alert Center, and the admin is alerted.

Actual Result: The rule is triggered.

Pass/Fail Status: Pass



Activity rule - 'TEST - New File Created'

Severity: Low

An alert's default severity value can be edited in Rules.

Status: Not started

Enter assignee

A user must have access to the alert center to be an assignee. To grant users access, go to roles.

Key details — Last updated Mar 07, 2023, 07:36 PM

Summary	The rule 'TEST - New File Created' (COUNT > 0 per day) triggered.
Start date	Mar 05, 2023, 07:07 PM CET (2023-03-05T19:07:00+01:00)
End date	Mar 07, 2023, 07:06 PM CET (2023-03-07T19:06:00+01:00)
Trigger window	Every 24 hours
Trigger data source	DRIVE_EVENTS
Threshold	COUNT > 0
Threshold action Performed when a triggering threshold is met	No threshold actions
Superseding alert	--
Superseded alerts	No alerts

Test Case 5: Triggering a rule when a phishing email is detected

Test Case ID: TC-005

Test Case Description: Testing if the rule triggers when a user sends many emails in a short time.

Preconditions: User should have Gmail access.

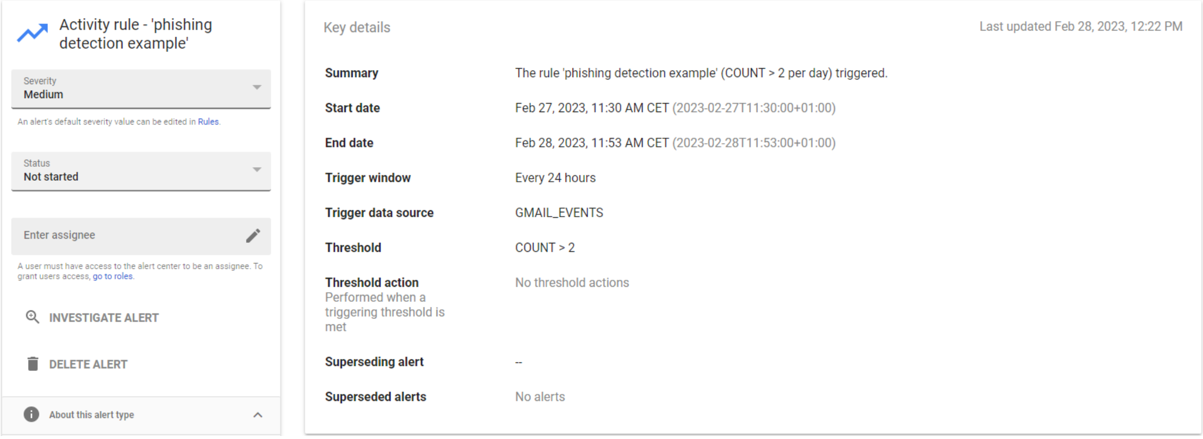
Test Steps:

The user attempts to send multiple emails in a short time.

Expected Result: An activity alert is sent to the Alert Center, and the admin is alerted.

Actual Result: The rule is triggered.

Pass/Fail Status: Pass



Activity rule - 'phishing detection example'

Severity: Medium

An alert's default severity value can be edited in Rules.

Status: Not started

Enter assignee

A user must have access to the alert center to be an assignee. To grant users access, go to roles.

Key details — Last updated Feb 28, 2023, 12:22 PM

Summary	The rule 'phishing detection example' (COUNT > 2 per day) triggered.
Start date	Feb 27, 2023, 11:30 AM CET (2023-02-27T11:30:00+01:00)
End date	Feb 28, 2023, 11:53 AM CET (2023-02-28T11:53:00+01:00)
Trigger window	Every 24 hours
Trigger data source	GMAIL_EVENTS
Threshold	COUNT > 2
Threshold action Performed when a triggering threshold is met	No threshold actions
Superseding alert	--
Superseded alerts	No alerts

Attachment 4 - Sprint Reviews

Sprint Review: Pre-Sprint

Dato: 01.02.2023
Deltakere: Marius, Dana, Dlir, Alexandra, David

Hva har blitt gjort?

- Alle oppgaver som ble satt opp ble gjort innenfor gitt tidsfrist. Flere av oppgavene kan utdypes ytterligere, og forbedres, men vi har fått utgangspunktet vi planla.

Hva har ikke blitt gjort?

- N/A

Hva har fungert bra?

- Økt kontakt med veiledere og bedrift
- Veileder er med i Discord
- God fordeling av oppgaver
- Bedre forståelse av hva Google Workspace/Cloud består av
- Alle har fullført sine oppgaver innenfor den gitte tidsfristen
- Gode til å oppdatere Trello kontinuerlig
- Startet tidlig og kom godt i gang

Hvilke utfordringer har vi hatt?

- Manglet noen tilganger i Google Workspace for å få tilgang til alle sikkerhetsfunksjoner
- Brukt litt tid på å finne ut av riktig bruk av Googles «Google Workspace Admin Help» som kilde

Hva kan forbedres?

- Mer konkrete planer for møtene med starttid og sluttid, slik at det er enklere for alle å planlegge dagen
- David ønsker hyppigere (fysiske) møter med bedrift, f.eks. hver
- Dele oppgaven med veileder for tips til forbedringer
- Huske å ta hyppigere bilder av f.eks. Trello Board ol. Som kan være greit å ha med i sluttrapporten
- Sette sammen de ulike tekstene om de forskjellige temaene til en mer helhetlig og sammenhengende tekst.

Sprint review: Sprint 1 (02.02 - 22.02)

Participants: Marius, Dlir, Dana, David, Alexandra
Date: 22.02.3023
Place: Universitetet i Agder, 50 137a

What has been done?

- Continued introduction, fixed problem statement according to Espen Abildgaard's suggestion.
- Searched and defined how Google prevent phishing attacks, and what technologies has Google in order to protect its users.
- Completed work with Data classification.
- Investigate whether Google Workspace have some Threat Intelligence like for example a data base.
- SOAR
  - Introduction about what SOAR is
  - Is Google Cloud SOAR at the same level as external SOAR services (which are not locked to an environment such as Google Cloud, Azure, etc.)
  - What kind of functionality does Google Cloud SOAR have, and what security challenges does it solve?
  - How complicated is it to use for an internal environment? Is this e.g. something that an IT administrator in a small company can handle, or is it so demanding that you have to have your own people / separate department to handle it
  - Threat Intelligence in SOAR, like which kind it have and how it works.
- Styringsgruppemøte 1
- Review of styringsgruppemøte 1
- Create a checklist for reviewing tasks
- Investigate Device Enrollment
- Update roadmap to english version
- Added some more general information about "Netsecurity"
- (Quality check) fixed format, spelling, line spacing of the written texts so far.
- Wrote about Project backlog and Time estimation.

What do you think about the results of the completed tasks during the previous sprint?

- Tasks are more difficult that previous sprint, especially Soar takes much time to examine. Google workspace has better documentation and we had a opportunity to test and use tha platform on the other hand Google soar documentation is more complicated, and these documentation actually created startup company Siemplify which has been bought by Google at 2022. And we have not opportunity to use platform.

What have not been done?

- Improvement of the existing texts, and adding them into the report.
- Write about company owned devices and inventory list.

Did we run into any problems? How were they solved?

- Use of source, we want to gather some source under same same category, we wil discuss it with our student supervisor on next meeting.

Sprint review: Sprint 2 (22.02 - 15.03)

Participants: Marius, Dlir, Dana, David, Alexandra
Date: 15.03.2023
Place: Universitetet i Agder, KRS 47-105

1- What has been done, about the product backlog items?

- Meeting with Netsecurity on 27 February
- Digital meeting with Peter.
- Status Meeting 2
- Working on chapters about SOAR, threat intelligence, identity security, device management, project implementation.
- Fixed chapters and headlines in the report.
- Written about sprint 1.
- Finished IS-305 assignment 2.
- Some of the reviews of tasks from sprint 1

2-What do you think about the results of the completed tasks?

We have made some progress into creating a better and more clean report. We have also created a better understanding of what the product owner expects from a finished product. We have taken steps into separating the report and the actual research. To summarize, we have made some valuable progress towards our end goal, and feel that most of the tasks have been completed in a sufficient way. Even though some of the task werent completed in time, we still feel like we are within schedule.

3-What product backlog items have not been done?

- Fix references
- Fix the table of contents
- Fix/review risk matrix
- Some of the reviews from sprint 1
- Create a chapter about sustainability
- Google Cloud Workspace

4-What challenges have we had?

- Building up the Chapters in the report was a challenge for the group.
- Tasks were to wide instead of splitting them into smaller task, which made it challenging to estimate how much time was needed to finish the given task.

5-What needs to be improved for the next sprint?

- The tasks need to be split into smaller tasks, with shorter deadlines for easier review of progress and potential changes that need to be made.

Sprint review: Sprint 3 (16.03 - 12.04)

Participants: Dlir, Marius, Dana, David, Alexandra
Date: 17.04.2023
Place: (Teams)

1-What has been done, about the product backlog items?

During this sprint, our team has successfully completed a number of tasks that have contributed to the progress of our project. In this sprint review, we will briefly summarize the work that has been done on each task:

- Improved several chapters
- Created a new risk analysis
- Improved the outlay of the report
- Added introductions to new chapters
- Investigated whether it was possible to decide when the "Verification Challenge" could be triggered.
- Reviewed tasks from sprint 2
- Finished assignment 3,4,5 in the IS-305 course
- We also had two meetings, one with the supervisor and one with the supervisor and product owner.
- Improved the list of references by shortening the URLs.

2-What do you think about the results of the completed tasks?

- After every task was completed, the group members became satisfied as they did their tasks. All five members were starting to feel more comfortable and understandable when answering various tasks.
- The feedback the group got is mostly ok, only that improvements are needed, so the teachers come up with recommendations that would be best for the group and to strengthen the final grade. As a result, the peer reviews greatly improved our work, making the results of our completed tasks better and helping our team understand the project more easily.

3-What product backlog items have not been done?

- We were not able to review all the comments added for further improvements. Some of the reason for that is the shortened period of time due to the easter break, however these tasks will be added to sprint 4, and should not lead to any further delays in accordance to our plan.

4-What challenges have we had?

- Some of the challenges were to shorten the chapters that we already have and make them better.
- Creating a new risk assessment was challenging, as it required careful analysis and comprehensive understanding of the project to identify potential issues.

5-What needs to be improved for the next sprint?

- Review and improve text, format and grammatic of the finished written texts
- Improve by estimating and tracking the time spent on tasks, which helps better understand the work pace and adjust deadlines or resource allocation accordingly.
- Add more about **XSOAR implementation**, **reflection**, **further development**, **conclusion** and consider the **MoSCoW methodology.**
- Strengthen and improve the whole report before final deliverable.

Sprint review: Sprint 4 (13.04 - 03.05)

Participants: Dlir, Marius, Dana, David, Alexandra
Date: 03.05.2023
Place: Universitetet i Agder, KRS 50 115d

1 - What product backlog items have been done?

- Illustrasjon av MoSCoW
- Lagt til introer i delkapitler som manglet
- Skrevet om hvordan 24/7 overvåkning gir økt sikkerhet
- Skrevet summary og preface
- Laget skisse av playbook
- Gjennomført tester
- Review av en del tekster som var skrevet i bacheloren
- Skrevet om “Further development of our product”
- Skrevet om “Further development of SOAR”
- Skrevet om “XSOAR implementation”
- Skrevet om Sprint 3
- Diverse korrektur

2 - What do you think about the results of the completed tasks?

- Gruppen føler at vi i Sprint 4 fikk ferdigstilt mange av oppgavene som manglet for å kunne fullføre rapporten, slik at den største delen av arbeidet i den siste sprinten kan dreie seg om å forbedre eksisterende innhold.

3 - What product backlog items have not been done?

- Det som ikke har blitt gjort i denne sprinten er å begynne å skrive på kapittel om refleksjon og konklusjon. Rette opp i kildene og se om alt står riktig i forhold til kildekompasset. En annen ting som heller ikke har blitt gjort er å laste ned oppgaven i Word og lage en innholdsfortegnelse. Ellers så har de fleste oppgavene blitt gjort, og vi går stadig gjennom bacheloren for å evt finne nye feil og lage nye oppgaver.
- Det var utfordrende å finne punkter for videreutvikling. Vi brukte en betydelig mengde tid på å identifisere og formulere slike punkter. Mens forbedringer i Xsoar var klare for oss, fant vi det vanskelig å finne andre punkter angående utvikling av tjenester og styring av GCP. For å klargjøre dette, måtte vi konsultere bedriften og gradvis generere ideer.

4 - What challenges have we had?

- Det var utfordrende å gjennomføre tester, siden gruppen ikke har veldig stor kjennskap til SOAR-plattformen, og å skrive om hvordan XSOAR implementeres ettersom det ikke er noen ren fasit på dette, og derfor er begrenset med kilder. Med god veiledning fra Espen føler vi imidlertid at vi fikk til et godt sluttresultat.
- En annen utfordring var å plassere nytt innhold i rapporten slik at det ble en logisk sammenheng med det tidligere innholdet.

5-What needs to be improved for the next sprint?

- Sjekke gjennom & rette kildelista ved behov
- Fokusere på ferdigstille rapporten og gjøre den klar til innlevering.
- Lese gjennom hele rapporten sjekke & rette opp i rettskriving, format osv.
- Flere gruppemedlemmer tar grundige gjennomganger av rapporten, kommenterer rom for forbedringer, påpeker feil osv.
- Legge inn innholdsfortegnelse & figurliste til sist (Word)

Sprint review: Final sprint (03.05 - 16.05)

Participants: Dlir, Marius, Dana, David, Alexandra
Date: 12.05.2023
Place: Universitetet i Agder, KRS 50 138

1 - What product backlog items have been completed during the last Sprint?

- Minor improvements
- Text Review
- Added conclusion, reflection and some attachments

2 - What product backlog items have not been done?

- Write what the test methodology is based on
- Explained how the product owner has been involved in scrum retrospective
- Update summary of report
-

3-What do you think about the results of the completed tasks?

- We are very satisfied with the improvements made to the report in the final sprint. In addition to adding more sections such as reflection and conclusion, several parts of the reports have been improved with more concise language and a better overall looking report.

4-What challenges have we had?

- It was challenging to make sure that all of the text were placed in what we considered the right part of the report, as well as to double check that all sources were correctly cited and that we had avoided stating the same things in multiple parts of the project.

5-What do you think of our project after it was completed?

- The group is satisfied with our report, and our collaboration with Netsecurity. We are satisfied with the results we have achieved, how we have worked together as a group and the learning outcome of taking on such a project.

Attachment 5 - Project report

Security monitoring of the Google Cloud Platform and Workspace

1.0 Identity Security

Identity Security is arguably the most important feature in cybersecurity, as a breach may have serious consequences. This includes financial loss, reputational damage, and loss of privacy. Cybercrime continues to grow in sophistication, and providing suitable solutions for protecting sensitive information is critical.

Identity security can be defined as a comprehensive solution that protects all types of identities within the enterprise—human or machine, on-prem or hybrid, regular or privileged—to detect and prevent identity-driven breaches, especially when adversaries manage to bypass endpoint security measures (Shastri, 2022)

In 2020 The Identity Defined Security Alliance (IDSA) published a study stating that 94% of organizations had experienced an identity-related breach at some point – 79% of those within the last two years (Smith, 2020). A large driving force in this development is the explosion of digital identities. Identity is not the only access point for threat actors to gain access but is often a weak point with less resistance (Bradley, 2023). According to a 2021 report from Verizon, 61% of data breaches involved the use of stolen credentials (Burbidge, 2021)

For this reason, identity security management is more important than ever before to protect sensitive information and resources in cloud computing. This includes preventing unauthorized access, securing access, and enforcing authorization to protect this information. Google Workspace provides a range of features and tools to help organizations protect their sensitive information and resources in cloud computing. These features include strong authentication mechanisms, such as two-factor authentication and security keys, as well as granular access controls and auditing capabilities. By implementing these measures, organizations can better protect their data and minimize the risk of a breach.

1.1 Authentication

Authentication is a term that refers to the process of proving that some fact or some document is genuine. In computer science, this term is typically associated with proving a user's identity. Usually, a user proves their identity by providing their credentials, that is, an agreed piece of information shared between the user and the system (Auth0, u.å.).

One of the most common authentication methods is password authentication. By providing the right credentials, typically a username and a password, the user is provided access to their account. This combination is notoriously known for being a weak security mechanism and is often being exploited by cybercriminals (Auth0, u.å). Creating a text-based password that is both strong and easy to remember is difficult. In general, they are short or based on dictionary words. This makes them vulnerable to dictionary attacks. Text-based passwords based on personal information or memorabilia are vulnerable to people close to the owner or attackers collecting information about the owner (Yildirim, 2019). Other types of attacks include brute force attacks, which try every possible combination of letters, numbers, and special characters, and hybrid attacks, which concatenate extra characters to dictionary words and try different combinations (Summers & Bosworth, 2004, s. 2).
To avoid security breaches through these types of attacks, multiple measures can be taken to gain an increased level of security. Some of these include:

1.1.1 Two-factor authentication (2FA)

Two-factor authentication (2FA) requires two forms of identification to gain access. Typically, this involves a username and password, combined with SMS verification, push notification, voice-based authentication, or hardware tokens (Microsoft, u.å). Hardware tokens are one of the oldest forms of 2FA, where users are given a key fob that produces codes within a given timeframe, for example, the small devices that produce codes for bank identification. These kinds of devices are often misplaced or lost, and more practical solutions have been developed. More commonly used today are SMS and push verification. SMS verification sends a message to a trusted phone, receiving a one-time verification code. Push verification removes the need for a code by simply sending a push notification to your device, which then can be either approved or denied (Microsoft, u.å).

2FA can be enforced in Google Workspace, which is recommended for your administrator account and users who work with the most important business information. Phone calls, SMS, authenticator, or security keys can be used as 2FA. If a user loses their 2FA, it can be turned off, or the admin can get backup codes for the user and send it to the user to allow them to sign in. (Google, 2023f)

Google has also implemented a security measure to protect its users' accounts from unauthorized access. In the event of suspicious login attempts, a login challenge will appear, requiring the user to verify their identity before granting access to the account. This can be done by providing a verification code sent to their recovery phone number or recovery email address, or by answering a challenge question that only the account owner would know. To ensure the security of their account, users need to update and maintain their recovery information with Google. If a user did not do that, administrators can add or edit the user’s recovery information.

Additionally, sensitive actions may trigger a "verify-it's-you challenge" which, if not passed, will block the action. If the authorized user is unable to verify their identity, the login or verify-it's-you challenge can be temporarily turned off for 10 minutes to allow the user to sign in.

While it is not possible to trigger a verify-it's-you challenge directly, as Google determines the appropriate security challenge based on multiple security and usability factors, organizations can still utilize context-aware access to create custom rules for granting or denying user access to applications. This approach allows administrators to set up policies based on a user's context, such as their location, device security status, and IP address, to enhance account security within Google Workspace. The detailed explanation of context-aware access and its implementation is provided further in this report. (Google, 2023ay)

1.1.2 - Advanced Multi-Factor Authentication (MFA)

Since it is about identity security, the group would like to include a type of solution that fits in this chapter. According to (Witts, 2023), this type of solution makes it possible for various companies to secure users' access to the network within the company itself. And not least cloud applications such as Office 365 and VPN`s
Another positive thing, is that from the central administration console, administrators may be able to create detailed reports with regard to account usage, where one can also know which of the users have gained access, and where in the network is in question.
Ensuring security both physically and digitally in terms of who is allowed to have access to the company's individual assets is very important so that unwanted users or people outside the company gain access to information. These can be, for example, digital certificates, mobile push authentication and PKI-based smart cards. (Witts, 2023). Thanks to Advanced MFA who does this job to secure corporate accounts and the company's system itself.
If desired, users can settle “Advanced MFA” for example in the cloud. This is so that it will be easy to set up, not least it will be versatile. Which means that this type of solution is strong enough for example for companies that are growing into an even larger organization. Those who have several office spaces in various places around. (Witts, 2023)

1.1.3 Password management

In Google Workspace’s admin console, the administrator can choose a password policy for their environment. Google requires passwords to be at least 8 characters by default, but this minimum requirement can be increased by the admin. The password management feature also includes an option to prevent users from reusing an old password, increasing the security if a password previously has been compromised. The downside of this security measure is the increased burden on the users. The users may find it difficult to remember multiple unique passwords and may turn to weaker and easily guessable passwords as a consequence. By enforcing strong passwords, Google uses a password strength-rating algorithm to ensure that a password has a high level of randomness (password entropy), is not a commonly used password (like “1234” or “password123”), is not easily guessable (simple words, phrases, or patterns where the password is the same as the username) and is not in a database of breached accounts (Google, 2023c). It is possible to choose the amount of time before a password expires. The admin can choose between a specific number of days or no expiration at all. By enforcing strong passwords, you can decrease the burden on the user by allowing a longer period between each password change, or perhaps even enforcing a password change at all. Password expiration is turned off by default, due to research showing little positive impact on security (Google, 2023c). Studies have shown that when a password change is forced, the new password is often algorithmically related to the old password, allowing many to be found in a few guesses. (Chiasson & Oorschot, 2015).

Admin has several rights over the users to increase security, such as resetting a user’s password and requiring the user to change the password at the next sign-on. If suspicious activity is discovered on an account, the admin can also force a password change.

Every organization faces a possible security risk if a user loses their device, or it gets stolen. To prevent unauthorized access, Google allows its admin to reset the user's sign-in cookies, effectively signing them out of their Google account and any Google Workspace applications on all devices and browsers. This ensures that access to the user's account is restricted even if the lost device falls into the wrong hand.

1.1.4 Single Sign-On (SSO)

When users need to use a web application or web-based desktop application, they usually need to authenticate with their username and password. Digitalization increases the need and usage of these kinds of services every day, therefore users need to memorize all their credentials to reach these applications and sign in every time (Pashalidis & Mitchell, 2003, s.249).

In addition to that some security and privacy issues can appear. It is not unusual to hear about service providers getting hacked and having their user credentials stolen. Therefore, the popularity and usage of SSO extend beyond the service provider and user. Clercq defines SSO as “the ability for a user to authenticate once to a single authentication authority and then access other protected resources without re authenticating” (Clercq, 2003, s 40-41). Google is one of the providers of SSO-services and also allows the user to use their application through another identity provider (idP).

When SSO is enabled, users can access Google apps directly through their third-party IdP without having to sign in again (with some exceptions). Google sometimes asks users to verify their identity as an extra security measure. In addition to that, two-step verification can be set up for users accessing Google services, but it is normally bypassed when SSO is turned on (Google, 2023f).

Workspace admins can set up SSO with Google as a service provider. SAML-based and OIDC-based SSO-protocols are supported by Google. OpenID Connect (OIDC) is a protocol that adds an identity layer on top of OAuth 2.0. It allows the users to verify their identity through an authorization server and get basic profile information in a REST-like manner (OpenID, November 2022).

Security Assertion Markup Language (SAML) is an XML-standard that allows for the exchange of user authentication and authorization data between web domains. Using the SAML-model, Google acts as the service provider and provides services such as Gmail, while partners act as identity providers and control usernames, passwords, and other information used to identify, authenticate, and authorize users for web applications that Google hosts. Admins should take into consideration that the SSO-solutions only apply to web applications. Passwords will still need to be provided and synced for desktop clients. The Google SSO-service uses SAML v2.0 specifications which is supported by many vendors (Google, 2023t).

Google suggests using security best practices when admins apply SSO for Google applications. For the third-party IdP configuration, maintain good password policies and enforce strong passwords, implement 2-Step Verification (2SV) on the IdP side, and recommend security keys where possible, especially those that are mobile-app based. For the Google Workspace configuration, disable user access to less secure apps, disable Post Office Protocol (POP) or Internet Message Access Protocol (IMAP) access, ensure that IMAP, POP, or SMTP clients support the OAuth 2.0 mechanism, and maintain strong passwords for Google Workspace accounts. For user devices, practice good cookie management, use Google mobile apps and update to the latest operating system version and security patches (Google, 2023u).

1.1.5 Login Challenges

A secure Login is very important once it involves protecting the user account or the user's personal information and is additionally important to forestall unauthorized access to their accounts. In addition, with a secure Login, it becomes tough for hackers to realize access to the user account, with a secured Login method also offers the user the chance for additional security by exploiting somewhat secure ways that ensure that it`s the correct person's Login. The great development of system networks and together with the development of personal computers or devices and their interconnection with each other, which made great need and great importance for data security. In addition to the major developments in network construction, a security breach in one system can lead to breaches in other systems and this can lead to major consequences (Dehand, 2002)

Login challenge in Google Workspace Security is a function that helps to provide an extra level of security to users who log in to a Google Workspace account. There are several logging challenge methods that Google offers, firstly when a user Logs In, Google requires the user must confirm their identity by completing a challenge, for example, it may be that users confirm their identity with a confirmation code that is sent via SMS to the user’s mobile phone or by answering security questions, this is because in order to ensure that there is only the correct user has access to the account. In addition, Google Workspace also has another Login challenge option which is by activating the employee -ID which is activated by the administrator, where the Users information is stored by Google workspace as an ID. This method is used by Google to be able to identify the users, the method requires the user to enter the employee – ID in order to complete the Login process (Google, 2023r).

Another method of Login challenge that Google offers is to activate SSO (Single Sign-on). The purpose of this is to give users a safe and easy way to log in, this also makes it easy to login to several services systems, SSO helps users with a good user experience since with these methods the user doesn’t need to log in several times to different service systems. And SSO also helps to reduce password prompts for users when they log in multiple times. By activating SSO, the company or organization can use idPS, which is known to third-party identity providers, this is to ensure a single Login process for users, this happens via SAML. With a configured SSO profile, the administrator can use (2SV) as it stands for 2-step verification (Google, 2023r). In general, Google SSO is a secure Login method for managing activities and Login. By using these methods, it is very difficult for hackers to gain access to the account. SSO will be discussed comprehensively in a separate section.

1.1.6 Gmail Authentication

It is possible to prevent spam, spoofing & phishing with Gmail authentication. Gmail administrators should set up email authentication in order to prevent the organization’s email from being marked as spam. This helps to prevent spammers from impersonating the organization's domain or name in spoofing and phishing emails, which can harm the organization's internet reputation over time. Gmail authentication has 4 steps these steps are;

1 - Admin should set up SPF which is a standard email authentication method. Thus admins can ensure mail delivery and prevent spoofing.

2 - Admin should set up DKIM which is DomainKeys Identified Mail.Thus admins can increase security for outgoing email and prevent mail from being marked as spam.

3 - Admin should set up DMARC which is Domain-based Message Authentication, Reporting, and Conformance. Thus DMARC instructs email receivers on how to handle the organization’s emails that don’t pass either SPF or DKIM. It also generates reports to help organizations identify potential email attacks and vulnerabilities.

4 - Admin optionally turn on Brand Indicators for Message Identification. Thus email receivers from your organization can see your logo in the inbox avatar section. (Google, 2023al)

Advanced security settings

By default, Gmail warns and moves suspicious emails to the spam folder. Google offers advanced security settings that can be tailored to different needs. Google's advanced setting covers attachments, links and external images, spoofing and authentication. Advanced security protects against suspicious attachments and scripts. It identifies links behind short URLs and linked images and scans for malicious content, and warns for links to untrusted domains. Furthermore it addresses spoofing and authentication, with protection against domain name and employee name spoofing, unauthenticated emails, and emails pretending to be from your domain. Unauthenticated emails display a question mark. (Google, 2023am)

1.2 Authorization and Access control

Authorization is the process of giving someone the ability to access a resource (Auth0, u.å).

1.2.1 API Controls

API Controls relate to security measures put in place to cover application programming interfaces (APIs) from unauthorized access, misuse, or abuse. APIs are interfaces that allow different software systems to communicate with each other and exchange data. As such they are an essential part of ultramodern software development and a crucial factor in digital transformation. Still, because APIs deliver access to sensitive functionality and data, it's very important for them to be protected so they can prevent unauthorized access and data leakage. (Kovacic, 2022).

It is important to mention that API controls also can include a variety of security measures like authorization, authentication, and access controls. The level of authorization determines whether a system or a user has the appropriate permissions to access a specific API. This is usually done by validating the user's role or group membership with a predefined set of access controls (Onelogin, i.d.).

API controls additionally consist of encryption, which is the system of remodeling facts right into a layout that is unreadable to unauthorized users. It is usually accomplished with the aid of using protocols consisting of HTTPS,SSL or TLS to encrypt the facts in transit between the API and the client. Other controls that may be applied consist of rate-proscribing, which is the system of proscribing the range of requests that may be made to an API inside a given time period, and IP whitelisting, which is the system of permitting get right of entry to the API best from particular IP addresses. (Kovacic,2022)

It's essential to say that the safety of an API is a shared duty among the API company and the API customer. The API company ought to make certain that the API is designed and carried out with protection in mind, and ensure that suitable controls are in place. The API customer ought to additionally take suitable measures to stabilize their stop of communication.

To summarize, API controls are a vital component of API security, and they are designed to guard API's from unauthorized users gaining access to abuse and misuse. A range of various safety features may be applied to offer a layered defense, which includes authorization, authentication, right of entry to controls, encryption, rate-limiting, and IP whitelisting

1.2.2 Context-Aware Access

Context-Aware Access gives the admin control over which apps a user can access based on their context, such as whether their device complies with the IT policy. Using Context-Aware Access, the admin can create granular access control policies for apps that access Workspace data based on attributes, such as user identity, location, device security status, and IP address (Google, 2023e).

This can be used by for example only allowing access through equipment issued by the company or restricting access to apps from outside the corporate network. These can also be combined with each other. One example is only allowing access from company-issued devices, on the company network which is encrypted (Google, 2023e).

A successful deployment means securing Workspace data based on the risk level of the user while ensuring that legitimate users are not blocked (Google, 2023e). To ensure this, it is recommended that these changes are made in a phased rollout, meaning that the changes are first applied to a small group or unit of the organization. This will reduce the risk of having many blocked users. It can also be a good idea to try it out on just a few apps at a time, that are frequently but not heavily used. By tracking what happens on these apps, you can later expand to more heavily used apps (Google, 2023e).

1.2.3 Data Classification

Data classification is a process for organizing data based on the organization's purpose and content. It also includes assigning categories to the data, making it easier to manage the data, and to protect and make it available to users who are authorized. This also makes it easier to save and retrieve data for use in the future.

Data classification is mostly used to identify sensitive data, such as personal information. This is to ensure that the data is processed securely. The purpose of the data classification system in terms of use for organizations, is that it helps to analyze and organize and track individual data. Additionally, the data classification system also helps organizations with data availability. This function ensures the security of the organization's information, and makes it easier to choose which data is shared with the specified users. Classification system is solid in terms of protecting sensitive data such as personal information, as well as helping organizations to control users permission by focusing on security policy requirements (Kranz & Fitzgibbons, 2022).

The data classification process helps to improve the organization's data and makes it easier to analyze. It also offers a great security strategy to take care of sensitive information. This function makes a regulatory obligation easier for the organization because it reduces costs by implementing a security level for all types of information (De Groot, 2022).

In Google workspace an organization can classify the information by using the tools that Google Workspace offers. In addition, the Google Workspace tools helps the organization adapt information or data within the workspace. It also improves organization and collaboration, as well as offering classification technologies to protect the organization's data. This happens by sorting the data based on the security level.

Some information or data may be external, for example the organization's private information or public data. Within Google Workspace, there are functions for data classification that offer security solutions that help users secure and share data information in a correct and safe manner within the workplace or organization, this happens through software as a service (SaaS) (Titus, n.d.).

1.2.4 Data Protection

The process of protecting vital information against corruption, compromise, or loss is known as data protection. As the amount of data created and saved continues to expand at unprecedented rates, the need for data protection grows. There is also minimal tolerance for downtime, which might make access to critical information impossible (Paul Crocetti, 2021)

The main principles of data protection are to protect and make data available in all circumstances. Data protection refers to both operational data backup and business continuity/disaster recovery (BCDR). Data security techniques are advancing in two directions: data availability and data management. (Paul Crocetti, 2021)

Protection rules and detectors

When it comes to preventing data leaks, Google Workspace provides numerous alternatives for data protection. Rules can be used to protect your content and prevent data leaks to unauthorized users. There is an option to manage the pre-existing rules, as well as to create your own rules. The rules under data protection, as mentioned earlier/ later in the text under rules, can be defined by domain administrators, and Google notifies when a specific behavior connected to the usage of chat, drive files, and chrome activity is activated. (Google, 2023h)

The administrator can establish their own rules by writing a name and a description, but they should consider choosing a descriptive name to make it easier to recognize the rules. Rules must also be assigned to an organization unit, and the data to be protected must be entered into an app. Some files may be unable to be checked for data protection standards due to size or other factors. In that situation, it is critical to include criteria that define the data you want the rule to look for. (Google, 2023j)

When an event matches the conditions for this rule, an action must be determined so that the rule can take it. Block external sharing, for example, means that whenever an event like this occurs, you have the option to warn on external sharing or disable download, print, and copy for commenters and viewers. Does something like that happen, the event can be reported in the security dashboard and alert center. It also allows you to select the severity level of the incident, which might be low, medium, or high. When a reported event is transmitted to the alert center, further in-depth facts allow you to act on issues and facilitate collaborative resolution with other administrators in your domain. (Google, 2023i)

Data protection in Google Workspace includes detectors, which can be used within a rule to identify sensitive content. Detectors can be added or exported in the same way as rules. When adding a detector, you can use regular expressions or a word list. Additionally, when using Google RE2 syntax, you must include the detector´s name and description (Google, 2023j).

Manual / Automatic controls

As mentioned earlier in the text, Google Workspace has controls. Under data protection, you can have automated restrictions based on data type and human controls based on organizational units or groups (Google, 2023v).

The automated safeguards, automatically prevent external sharing of sensitive files on Drive based on the data type. The rules must be configured to prevent external sharing, warn end users, or disable file downloading and copying. Detectors can check your organization´s drive files for content and select particular content categories to restrict sharing (Google, 2023v).

If you wish to manually configure Drive for external sharing by an organizational unit or group, then you should choose the organizational units or groups where you wish to limit external sharing and disable it (Google, 2023v).

Optical character recognition

In the data protection settings, you may enable optical character recognition (OCR), which is now only accessible for Google Chat. If you utilize OCR, scan text in photographs that users provide to comply with chat data protection laws. Turning this on may result in minor delays for messages that contain visuals. There is also a report that may be utilized when rules and detectors are present. (Google, 2023q)

The drive DLP data protection

The drive DLP data protection insights report provides the sensitive data categories in your organization, as well as the Drive files that include sensitive data. The report is available quarterly and may show you the total proportion of files with sensitive material that are shared externally. As well as the top data categories that are shared, it also displays the amount of disk files containing sensitive material, in addition to files containing sensitive content that is shared externally. Moreover, for each data category, the percentage of files with sensitive material that are shared outside (Google, 2023q).

Advanced protection program

Google´s robust security helps to safeguard your personal information. The advanced security program protects users with high visibility and sensitive data from targeted online attacks. To defend against today's diverse threats, new safeguards are automatically added. (Google, 2023w)

Every day, Gmail stops more than 100 million phishing attempts. (Kumaran, 2019) However, even the savviest users might be duped by sophisticated phishing techniques into providing their sign-in information to hackers. When using advanced protection, you must sign into your Google account using a security key to confirm your identity. Without your username and password, unauthorized users cannot sign in. That means the advanced data protection prevents phishing attacks on your account. (Google, 2023v)

Chrome´s Safe Browsing shields 4 billion devices from dangerous websites, while advanced protection does even more thorough checks before each download. (Google,2023aq) It alerts you to potentially hazardous files and may even stop you from downloading them. Installations of apps are only permitted from trusted stores, such as the Google Play Store and the App Store run by the company that produces your device. (Google, 2023w)

When you join up for new apps or services, your Google account information, such as your contacts, location or drive is frequently requested. Over 1 billion passwords are checked daily for breaches by Google Accounts, which have built-in security measures. (Google,2023aq). However, some intruders are capable of passing to a trustworthy third party in order to access information. Only Google apps and approved third-party apps can access your Google Account data with advanced protection enabled, and only with your consent. (Google, 2023)

Google's Advanced Protection program for high-risk users with malware protection.
Google has developed the Advanced Protection program to provide a higher level of security for individuals who are vulnerable to targeted attacks like for example politicians, journalists etc. The program offers various security features, such as restricted data access, preventing fraudulent account access, and using physical security keys. (Perez, 2020)

In 2020, Google added additional malware defenses, including turning on Google Play Protect by default for program members. While the verification process for account access may be more rigorous, the increased security measures provide a cost-free way to enhance the security of users' accounts and devices. Although the Advanced Protection program offers significant security benefits, it does come with increased restrictions and verification processes. For instance, users must use a physical security key to access their accounts, which may be less convenient than traditional passwords or two-factor authentication methods. Nonetheless, these measures help to protect against targeted attacks that could compromise sensitive information. (Perez, 2020)

Google has been gradually introducing new features to the Advanced Protection program, including protections for Chrome that target users at higher risk. This demonstrates Google´s commitment to safeguarding user accounts and enhancing overall cybersecurity, which is in line with the technology industry´s trend of prioritizing user privacy and protection against online threats (Perez, 2020).

1.2.5 Google Session Control

Google Session Control is a function within Google Workspace. This function is located in the security section, and enables the administrator to set limits for the duration of the user's session. The administrator can then decide when the user should have access to the service, after a certain period of time the user will be automatically logged out. The organization can then have full control over what the users should have access to at a certain period of time.

Certain industries and organizations are subject to laws and regulations that mandate timeouts for increased security. Google Session Control includes a feature that enables these organizations to comply with such requirements. In addition, the tool offers the ability to set limits on access to sensitive resources, such as external locations where automatic logout occurs. This feature enhances the security of the organization and ensures compliance with regulations. Furthermore, Google Session Control includes Business Plus and Enterprise plans that provide cost-effective solutions for enhancing organizational security and meeting regulatory requirements. The tool is user-friendly and easy to set up and manage, making it an ideal solution for organizations seeking to adapt to their unique needs (Google, 2023m).

1.2.6 Google Cloud Session Control

Google Cloud Session Control is a powerful feature of Google Cloud Identity that enables organizations to control and manage user sessions in the cloud. With this feature, administrators can set policies for session duration, idle timeout, and maximum number of concurrent sessions. These policies help organizations maintain control over user access to cloud resources and ensure that sessions are secure and in compliance with organizational policies. Google Cloud Session Control is an easy-to-use tool that enables administrators to set policies that meet the unique needs of their organization, providing enhanced security and greater control over cloud resources (Google, 2023d).

This feature is designed to improve security by limiting the amount of time a user can spend in an active session and blocking access to accounts that have been compromised. Moreover, it enables businesses to keep track of current sessions and end them as appropriate. Besides that, it enables the creation of policies that force users to log out automatically after a certain amount of inactivity or when a certain number of concurrent sessions is achieved (Google, 2023d). It is especially useful in situations where you want to limit the amount of time a user has access to sensitive data such as financial accounts, medical records, and credit card information.

Google suggests a reauthentication frequency of 16 hours, but the feature is fully customizable to suit your specific needs. You can choose to require re-authentication at any interval between one and 24 hours, depending on your security requirements. Additionally, you have the ability to exempt trusted apps from this requirement. These apps can be easily identified and marked on the "Apps Access Control" page, found under API Controls. This feature is particularly useful if you have apps that may not handle the re-authentication scenario gracefully, potentially resulting in confusing application crashes or stack traces. By exempting trusted apps from the re-authentication requirement, you can ensure that your apps remain functional and secure, while maintaining the overall security of your system.(Google, 2023d)

Google Cloud Session Control can be used in conjunction with other security features such as multi-factor authentication, passwordless authentication, and security keys to increase the security of user accounts in the cloud (Google, 2023d)

1.2.7 Less Secure Apps

In the security overview, Google offers an option for managing user access to less secure apps. As a best practice, Google recommends disabling access to these apps as they do not adhere to modern security standards, such as OAuth (Open Authorization) (Google, 2023b). OAuth is an open standard for token-based authentication and authorization on the internet, allowing users to grant limited access to their resources from one site to another site without sharing their credentials. This enables third-party applications to access a user's resources, such as their data on a social media platform, without the user sharing their login information.

By disabling access to less secure apps, the risk of unauthorized access to sensitive information is greatly reduced (OAuth, 2023). Examples of apps that don’t meet modern security standards are native mail, contacts, and calendar sync applications on older versions of iOS and OSX, and some computer mail clients, such as older versions of Microsoft Outlook (Google, 2023b).

1.2.8 Alert Center

When working through Google Workspace, and trying to create a platform, it is important to include an alert center. Because we know that the alert center will contain details that help a user activate measures so that it can solve problems that eventually arise.

According to (Google,2023a) an admin can use the notification center to help them to get easier overview over alerts about potential issues in a domain address, and there man can take action such as end-users or updating existing policies and settings to be able to fix issues and be able to protect the company from attackers and security threats. (Google, 2023a)

We mean it is important to mention Alert center API (Application Programming Interface) as well. It enables a user to manage alerts moving a domain. Associate alert cloud be a warning of a possible security issue that Google has detected. (Google 2023ac) Alerts embody the subsequent information like (Google 2023ac):

- Supply that the alert originated from
- Name of the alert
- Time this alert happened
- Specific knowledge related to this alert

Because we also can use it in the notification center to control notification about several different issues that may affect a domain address. While a domain address admin can both view and manage notification manually through the Google Admin console. (Google, 2023a) Another thing is that the alert center API allows applications which are built to retrieve notification data and notification feedback. Not least the API can possibly create new alert comments for existing alerts. According to the source mentioned several times in the text, there is a good example to understand more how this works.

The example is that a monitoring application could possibly use the Alert Center API to recover the latest alerts for a domain, prioritize them, and inform the people who are members of an organization. When the members answer to the alert, the app itself could attach comments to the alert based on the findings. (Google, 2023a)

Functions

We can start by saying that, for example, an organization can quickly notify members of any emergency situation (Drake, 2022) that will arise. The good thing here is that the members of the organization discuss and come up with different ideas to fix a problem or emergency. The more people, the easier it will be to come up with a quick and effective solution, not least in terms of time, it is an advantage not to lose too much valuable time.

One can easily update details for currently operating alerts (Drake, 2022). In other words, this is a great advantage when you want to know more about the warning that has appeared. For example, you can get details about what has gone wrong, what the alert is about, and how big it is, not least where in the system the alert has been notified.

1.2.9 Rules

In order to detect, defend, block, or respond to cyber attacks, IT-Security tools like firewalls, intrusion detection tools, security orchestration automation, and response tools need some rules or playbooks. Simply we can define rules, if x happens, do automatically y. Google admin console is no exception to that. Google cloud administrators can set up rules in the Google Admin console to be notified of specific activity within their domain, such as suspicious sign-in attempts or compromised mobile devices, or to automate actions in response to activity. Admins can also create custom alerts based on an organization's log event data. Different types of rules, such as activity, reporting, data protection, system defined, and trust rules, can be viewed and configured from the Rules page (Google, 2023g).

Reporting Rules

Reporting rules are custom rules that allow administrators to set up alerts based on log event data. That can be found on the audit and investigation page. To configure a reporting rule, administrators set up conditions and specify actions to be taken when those conditions are met. For example, admins can set a reporting rule to alert them when a user makes a drive file visible on the web, and receive email notifications or alerts in the Alert Center when the rule is triggered.(Google Workspace Admin Help Rules, 2023h)

Activity Rules

The security investigation tool allows administrators to set up alerts and automate actions to quickly and efficiently prevent, detect, and remediate security issues. This is done by creating activity rules which consist of setting up conditions and specifying actions to take when those conditions are met. For example, admins can set up a rule to send email notifications to certain admins if drive documents are shared outside the company. Activity rules are more advanced rules when compared with reporting rules.(Google, 2023i)

Data Protection Rules

Data protection rules can be set by the domain administrators and google notifies when a specific activity is triggered that is related to the use of drive files, chat, and chrome activity. (Google, 2023j)

System-defined Rules

Admins can set up admin email alerts based on default rules supplied by Google to be notified of specific activity within their domain such as suspicious sign-in attempts, compromised mobile devices, or changes in settings by other administrators. Admins can view and edit these rules on the Rules page and specify actions to be performed when certain conditions are met. System-defined rules can’t be created, these can be viewed or edited, for example, admins can change the severity level, turn them on or off, etc. (Google, 2023k).

Trust rules for Drive sharing

Trust rules allow admins to create specific policies to control access to Google Drive files. Admins can define these policies for individual users, groups, organizational units, and domains. Trust rules allow admins to specify who can share files with internal or external users, who can receive files from internal or external users, and who can be invited and add items to shared drives. These rules provide opportunities in setting collaboration boundaries, which can help to achieve best practices for securing sensitive information and maintaining compliance.(Google, 2023l)

1.3 Phishing

Before describing Phishing, social engineering should be understood. Social engineering methods are used by a malicious user to manipulate the target user to do something. According to Ross Anderson, social engineering involves psychological manipulation to extract confidential information or actions from individuals. It is a form of confidence trick used for information gathering, fraud, or system access (Anderson, 2008, p. 17). Phishing is a type of social engineering where attackers trick individuals into revealing sensitive information (Jansson, 2011, p 584-593). Phishing is a malicious attempt to steal sensitive information through fake emails, messages or websites that appear to be from a trustworthy source. These fake sources may ask for personal or financial information, urge you to click links, or download software. In addition, it may also impersonate well-known organizations or people you know, and appear identical to messages from trusted sources (Gmail Help, 2023a)

Google offers some protection against phishing, and also gives suggestions to users on how to identify phishing attacks. If a user receives a suspicious e-mail, in most cases Google warns about malicious content and tricky websites by using advanced security. In addition to that it is advised not to click links, download files or enter sensitive information in emails, webpages from unknown or suspicious providers. Google provides its users with extra security measures against phishing and other cyber attacks regardless of the Google cloud and Gmail. The Safe Browsing feature in Google Chrome alerts users of malicious software, phishing attacks, and dangerous websites. Additionally, the Password Alert feature in Chrome will warn users if they accidentally enter their Google account password on an another website. Thus, it helps to prevent users enter their information into an unauthorized site or a malicious site that mimics Google (Gmail Help,2023a).

1.3.1 Activity Rules

In order to detect, defend, block, or respond to cyber attacks, IT-Security tools like firewalls, intrusion detection tools, security orchestration automation, and response tools need some rules or playbooks. We can define simple rules that automatically trigger an action when a specific event occurs. For instance, if X happens, then Y will be executed automatically. Google admin console is no exception to that. Google cloud administrators can set up rules in the Google Admin console to be notified of specific activity within their domain, such as suspicious sign-in attempts or compromised mobile devices, or to automate actions in response to activity. Admins can also create custom alerts based on an organization's log event data. Different types of rules, such as activity, reporting, data protection, system defined, and trust rules, can be viewed and configured from the “rules” page (Google, 2023i).

Reporting Rules

Reporting rules are custom rules that allow administrators to set up alerts based on log event data. That can be found on the audit and investigation page. To configure a reporting rule, administrators set up conditions and specify actions to be taken when those conditions are met. For example, admins can set a reporting rule to alert them when a user makes a drive file visible on the web, and receive email notifications or alerts in the Alert Center when the rule is triggered (Google Workspace Admin Help Rules, 2023h).

Activity Rules

The security investigation tool allows administrators to set up alerts and automate actions to quickly and efficiently prevent, detect, and remediate security issues. This is done by creating activity rules which consist of setting up conditions and specifying actions to take when those conditions are met. For example, admins can set up a rule to send email notifications to certain admins if Drive documents are shared outside the company. Activity rules are more advanced rules compared to reporting rules (Google, 2023i).

Data Protection Rules

Data protection rules can be set by the domain administrators, and Google notifies when a specific activity is triggered that is related to the use of drive files, chat, and chrome activity (Google, 2023j).

System-defined Rules

Admins can set up admin email alerts based on default rules supplied by Google to be notified of specific activity within their domain, such as suspicious sign-in attempts, compromised mobile devices, or changes in settings by other administrators. Admins can view and edit these rules on the “rules” page and specify actions to be performed when certain conditions are met. System-defined rules can’t be created, these can be viewed or edited, for example, admins can change the severity level, turn them on or off, etc. (Google, 2023k).

Trust rules for Drive sharing

Trust rules allow admins to create specific policies to control access to Google Drive files. Admins can define these policies for individual users, groups, organizational units, and domains. Trust rules allow admins to specify who can share files with internal or external users, who can receive files from internal or external users, and who can be invited and add items to shared drives. These rules provide opportunities in setting collaboration boundaries, which can help to achieve best practices for securing sensitive information and maintaining compliance. (Google, 2023l)

2.0 Threat Intelligence

Threat intelligence (TI) is the process of collecting and analyzing information to understand and predict cybersecurity threats and risks to computer systems. According to Gartner analyst Rob McMillan, TI is evidence-based knowledge that includes context, mechanisms, indicators, implications, and actionable advice about existing or emerging menaces or hazards to assets that can be used to inform decisions regarding the subject's response to that menace or hazard. This knowledge can come from various sources, such as malware, network traffic, user activity, and others (McMillan, 2013).

One way to identify malware is by using a hash value, which is a unique identifier that represents a particular file or code. By comparing the hash value of a suspicious file to a database of known hash values for malware, security researchers can quickly determine whether the file is a threat or not. Another key task in threat intelligence is identifying the type of threat. Attackers may change hash values and encrypt code to make it difficult to detect, but behavioral analysis can be used to examine the actions of the malware. For example, an attacker might use a specific type of malware or a particular script to carry out an attack. In order to protect against this threat, security researchers need to know exactly what kind of software it is and how it works. TI allows us to compare attacks with each other, understand the type and capabilities of the malware, and develop defense strategies against them. Additionally, the hash value of newly identified malware can be recorded in databases, which enables faster blocking of the same attack in the future.Furthermore, TI allows harmful IP addresses, websites, and email addresses to be registered in the system in advance, so that SOAR and other security software will not grant access to these addresses.

Therefore, TI is an important part of understanding and protecting against cybersecurity threats, involving the collection, analysis, and derivation of conclusions from data about threats and risks to computer systems.

Google Workspace is a suite of productivity and collaboration tools that does not have a built-in threat intelligence database. However, Google uses various technologies, such as Google Safe Browsing and machine learning algorithms, to provide advanced phishing and malware detection and protect its users against cyber threats. Google also has a dedicated team, the Threat Analysis Group (TAG), responsible for analyzing and defending against targeted and sophisticated attacks on Google and its users (Google, 2023aq).

To enhance incident response procedures, integrating a Security Orchestration, Automation, and Response (SOAR) platform with Google Workspace can automate and standardize incident response processes, saving time and effort and improving overall security posture. Google Workspace's collaboration features, such as real-time document sharing and editing, can improve organizational collaboration during security events when used in combination with SOAR. Overall, integrating Google Workspace with SOAR can improve cooperation and communication among security teams, reduce the time it takes to detect and respond to security issues, and enhance security operations (Google,2023am).

Google Workspace is a suite of productivity and collaboration tools that does not have a built-in threat intelligence database. However, Google uses various technologies, such as Google Safe Browsing and machine learning algorithms, to provide advanced phishing and malware detection and protect its users against cyber threats. Google also has a dedicated team, the Threat Analysis Group (TAG), responsible for analyzing and defending against targeted and sophisticated attacks on Google and its users (Google, 2023av)

To enhance incident response procedures, integrating a Security Orchestration, Automation, and Response (SOAR) platform with Google Workspace can automate and standardize incident response processes, saving time and effort and improving overall security posture. Google Workspace's collaboration features, such as real-time document sharing and editing, can improve organizational collaboration during security events when used in combination with SOAR (Google, 2023am).

Overall, integrating Google Workspace with SOAR can improve cooperation and communication among security teams, reduce the time it takes to detect and respond to security issues, and enhance security operations (Google, 2023an).

As mentioned earlier, Google Workspace does not have a built-in database for threat intelligence, but it uses a variety of tools and technologies to provide threat intelligence and protect its users. In addition to the technologies already mentioned, Google Workspace also offers other security features such as data loss prevention (DLP), which helps prevent data leakage by identifying and blocking sensitive information from being sent outside of an organization. (Google, 2023an)
Google Workspace also offers mobile device management (MDM) to help protect mobile devices that access organizational data. This feature allows administrators to enforce security policies on mobile devices, such as requiring passwords or encrypting data, and remotely wiping devices that are lost or stolen.(Google, 2023ap)

Furthermore, Google Workspace provides security reports and alerts to administrators, which can help them identify potential security issues and take action to prevent them. These reports can provide information on user activity, such as logins and file access, and allow administrators to set up alerts for suspicious activity. In addition to the security features provided by Google Workspace, businesses can also integrate a security orchestration, automation, and response (SOAR) platform with Google Workspace to automate and streamline incident response procedures. This can save time and effort needed to respond to security occurrences and enhance the overall security posture of an organization (Google, 2023ap)

Integrating Google Workspace with a SOAR platform can also improve collaboration and communication amongst security teams during security events.

For instance, the SOAR platform can automatically generate an incident ticket and alert the security team using Google Workspace when a security problem is discovered. This enables them to work together and exchange information in real-time, improving incident response times Google, 2023ap).

In summary, while Google Workspace does not have a built-in database for threat intelligence, it offers a variety of tools and technologies to protect its users against cyber threats. Businesses can also integrate Google Workspace with a SOAR platform to automate incident response procedures and improve collaboration and communication amongst security teams.(Google, 2023ap)

3.0 Google SOAR

SOAR is a Technology in cybersecurity, it stands for "Security Orchestration, Automation, and Response". This is to improve the response to security incidents, SOAR helps to improve the security level of the organization. SOAR technology has a good role to help organizations to streamline the workflow for security incidents, for example, SOAR tools can automate processes such as incident response and protect the organization with threats. Not least SOAR technology also gives organizations more insight into security problems to improve security incidents. In addition, SOAR technology has functions that are for collecting and integrating data from different sources, it can be for example security tools, and system logs. This is something that can help organizations make better decisions faster (Cyberpedia n.d.).

SOAR Technology has three program functions. First, Orchestration: it is about automating the workflow of security incidents and security operations, and it also organizes activities between different security tools. Its benefit is to help the organization save time by detecting threat events. The second program function is known for Response: in terms of threats and incidents, the response is about reacting in a fast and efficient way, it also helps to minimize damage, for example blocking attacks and alerting the security team. The third function is Automation: it refers to technologies, which help to organize and periodize security alarms. (Cyberpedia n.d.)

3.1 - Siemplify

Siemplify is a security platform known for security operations, and stands for (Security Operations Platform), the Siemplify platform helps organizations with the ability to automate and orchestrate security events using various security technologies. With Siemplify, the SOAR platform also integrates with security orchestration, response, and automation with something known for (end the End) security incident management. In addition, Siemplify also provides a good overview of a security incident, which helps organizations to make quick and effective decisions regarding the handling of threats. And the Siemplify platform was designed to improve the efficiency of security, and it also reduces the response time of security teams (Softprom u. å).

3.2 Google Cloud SOAR: A Comparison with External Services

Google Cloud SOAR offers functionalities and features that are on par with external SOAR services But it is important to know that each SOAR service has its own unique functionality and characteristics (Kirtley, 2022). The choice between using an external SOAR service or Google Cloud SOAR will depend on the users specific needs, and you may want to thoroughly evaluate both options before making a decision.

It is also worth noting that choosing a SOAR service will not only contain about functionality and features, but according to (IBM, n.d.) it is also about availability, cost, support and integration with other systems. If a user already uses the Google Cloud platform or have an existing infrastructure on Google Cloud, it may be more appropriate to use Google Cloud SOAR. On the other hand, it may be more beneficial to use an external SOAR service that is not locked to a specific cloud platform, if you need more flexibility in terms of infrastructure. (Google, 2023ao).

It is also important to evaluate which security features are offered by the SOAR service, as security is a critical factor for all businesses. We must also consider the type of customer support available and whether it suits our needs. Another important factor is integration with other systems a user already use, for example SIEM or ticketing systems, which according to (Trost, n.d.) it allows several teams to describe, organize not least archive investigations and incidents. But in the end, we should also consider the cost of the SOAR service and compare it to other options on the market.

3.3 Google SOAR: Key Features & Solutions

3.3.1 Case Management

To better understand issues that need to be handled, the Siemplify Alert Grouping mechanism groups alerts into cases. The goal is to highlight the importance of additional context to a security alert and avoid situations where the security analyst investigates the same security alert without the context, which may lead to a loss of precious time, or the incident being handled in the wrong way (Siemplify, 2023a).

This mechanism enables you to create grouping rules. You can then decide which alerts should be grouped. Incoming alerts are matched against a rule in the following order:

1. Alert Type
2. Product
3. Data Source

There's also a fallback rule which ensures that alerts are always grouped in cases. If an alert matches a rule, and no existing case can be grouped into, it will be added to a new case (Siemplify, 2023). Creating rules makes it easier to sort out which incidents should be prioritized, especially for larger corporations with a large volume of incidents.

Cases are generated by alerts from the SIEM platform. Further alerts linked to the same entities may be grouped into an existing case based on a flexible configuration. In addition, Analysts can create manual cases and simulated cases and ingest specific data (Siemplify, 2023).

Another useful function is the feature that allows you to manage tasks from the cases screen. This enables you to create and manage case-specific and general tasks and assign them to a SOC role or team member (Siemplify, 2023). This allows for more control and easier distribution between different roles/members. Since responding to a security threat is often a team effort, it allows for more effective collaboration. It also provides the organization with a centralized system for managing security threats. All incident-related data, such as log files, alerts, and other relevant information can be stored for easier tracking.

3.3.2 Playbooks

A Playbook can best be described as a workflow of actions that are executed following a certain trigger. Playbooks are particularly useful because they can be predefined in advance to respond to various alerts coming from your SIEM and carry out automatic actions – thereby freeing up the analyst's time and efforts (Siemplify 2023).

A playbook is composed of two parts: triggers and actions as defined by the SOC Manager or higher-tier analysts for handling security alerts. Playbooks automatically gather information on alerts from internal and external sources, request essential information from users associated with the alerts, and take appropriate actions to proceed with the alerts (Siemplify, 2023).

This is done by creating workflows based on Security Operations Center (SOC), Network Operating Center (NOC) and Incident Response use cases to standardize and automate security tasks. Playbooks get triggered by alerts – logical conditions which tell the playbook when to run. (Siemplify 2023). Playbooks can then be used to create "families" of alerts (alert type). This can for instance be a user who failed the login multiple times. This alert is a specific alert in the" multiple failed login" family. Your playbook can then simplify this problem by automating any "multiple failed login" alerts, regardless of which user is responsible (Siemplify, 2020, p. 3)

3.3.3 Investigation

By creating playbooks, most of the job needed to perform investigations is already done, since much of the information needed is already gathered by Siemplify. This enables the analyst to respond more quickly to threats (Siemplify, 2023).

3.3.4 Integrated Threat Intelligence

Google Workspace does not have a built-in database for threat intelligence. It is also a suite of business productivity and collaboration tools, including Gmail, Google Drive, etc., however, it does not have specific tools for managing threat intelligence data.

Anyways Google Workspace uses a variety of tools and technologies to provide threat intelligence and protect its users against cyber threats. Some of these tools and technologies include:

1. Google Safe Browsing: This technology helps protect users against malicious websites that host malware or phishing scams.
2. Advanced Phishing and Malware Detection: Google Workspace uses machine learning algorithms and other technologies to detect and block phishing emails and malicious attachments.
3. Google Threat Analysis Group (TAG): This group tracks and responds to advanced cyber threats.

4. Google Play Protect: This technology scans Android apps in Google Play Store and on user devices to detect and prevent the installation of harmful apps.
5. Two-Factor Authentication (2FA): Google Workspace supports 2FA, which provides an extra layer of security by requiring users to enter a unique code in addition to their password.

These are just a few examples of the many security features and technologies that Google Workspace uses to provide threat intelligence and protect its users.
With the purpose of automating and streamlining incident response procedures, SOAR solutions often interact with several security tools and systems. You may automate and standardize your incident response processes by integrating a SOAR platform with Google Workspace, which will save the time and effort needed to respond to security occurrences and enhance your overall security posture.

The Google threat analysis group (TAG) is a team within Google that is responsible for analyzing and defending against targeted and sophisticated attacks on Google and its users. The team aims to discover security risks that affect Google's corporate infrastructure, staff, and clients, as well as to respond to them. It also transmits information about these dangers to clients and the larger security community. The group detects, analyzes, and reacts to threats in real-time using a mix of technology, knowledge, and teamwork. This includes keeping an eye out for questionable conduct, examining assault strategies, and dealing with current threats. To coordinate reactions and guarantee that a proper course of action is taken, the team also closely collaborates with other Google departments, such as the Google Security Team and the Google Law Team. (Google, 2022aq)

To assist shield its customers from online risks, Google Workspace offers sophisticated phishing and malware detection. These tools are intended to recognize and stop attacks like phishing emails and malicious malware that breach user accounts and steal private data.

3.4. Phishing Detection

Google Workspace detects and blocks phishing emails that may be disguised as authentic emails from reliable sources. It does this using machine learning algorithms and other cutting-edge technology. The program checks emails for phishing indicators and detects and flags communications that are most likely malicious. (Google, 2023an)

3.4.1 Malware Detection

Google Workspace includes strong malware detection features that aid in guarding against malicious software that might corrupt user devices and steal confidential data. The program checks links and attachments in emails for known malware before blocking any emails that include it. To help users from unintentionally exposing themselves to malware, the system can also limit access to potentially hazardous websites.

Overall, Google Workspace's sophisticated phishing and malware detection tools assist in shielding customers from risks online and guaranteeing the security of their data. These technologies enable users to lessen their vulnerability to malware infestations and phishing scams (Google, 2023an).

3.4.2 Collaboration

A company's security posture and incident response capabilities can be improved by combining Google Workspace with SOAR, which are two separate types of software technologies.

As mentioned earlier Gmail, Google Drive, Google Documents, etc, are all part of Google Workspace, a collection of productivity and collaboration applications. These technologies make it possible for teams to collaborate effectively by storing, producing, editing, and sharing documents, spreadsheets, presentations, and other data in real time. (Sandy Writtenhouse, 2022)

Adversely, SOAR is a platform for security orchestration and automation that enables businesses to automate and simplify their security processes, such as vulnerability management, threat detection, and incident response. The time it takes to identify and respond to security problems may be decreased with the use of SOAR technologies, which can also support security personnel. (Sharon Shea, Techtarget, 2021)

Google Workspace and SOAR can enhance organizational collaboration during security events when used in combination. For instance, the SOAR platform may instantly generate an incident ticket and alert the security team using Google Workspace when a security problem is discovered, enabling them to work together and exchange information in real time. The SOAR platform automates regular processes and assists in prioritizing and escalating security events as needed. The security team may then utilize Google Workspace capabilities to document their findings and coordinate their response efforts. (Google, 2021ap)

In general, integrating Google Workspace with SOAR may assist businesses in enhancing cooperation and communication amongst security teams, reducing the time it takes to detect and respond to security issues, and improving security operations.(Google, 2021ap)

3.5 A review of the complexity of Google SOAR

The investigation of whether the Google Chronicle SOAR application is user-friendly was a key issue that needed to be addressed. IT managers, especially those of small companies, had to determine whether they could handle the application, set up a dedicated unit for it, or outsource it through a third-party provider. However, there is no clear answer to this question, so we tried to answer it by examining the features that managers using Google SOAR should have, as well as by reviewing product training videos.

To begin with, we need to define the user types, their tasks, and the basic skills they should possess. There are two user types: security engineers and security analysts. Security engineers should create playbooks to prevent cyber attacks or mitigate their effects, taking into account the security procedures of the organization. Playbooks enable the software to work efficiently and effectively by automating workflows. Security analysts, on the other hand, are responsible for examining the alerts generated by SOAR, enriching the information about emerging threats, and intervening manually when necessary or investigating the causes and consequences of the incident. According to Siemplify, the application is user-friendly and has a playbook builder that can be easily used by anyone on the security team. Security engineers can define effective playbooks using predefined actions without requiring coding skills.(Playbook Lifecycle Management, 2020a, p.1)

To create playbooks, security engineers need to know which alert types they need to automate, which requires a comprehensive understanding of potential attacks and the ability to create a risk map.(Playbook Lifecycle Management, 2020b, p.4) In addition, they need to understand the connectors, i.e., the mechanisms of the products that generate the alerts, such as Siem, firewall, or casb. (*Using Triggers in Playbooks*,2023). Collaboration and documentation skills are essential when creating playbooks, and security engineers should learn from security analysts' experience with potential threats and their expectations of playbooks. Documentation of playbooks is essential to create a corporate memory and a better understanding of workflows. (Playbook Lifecycle Management, 2020c, p.6) Different actions need to be categorized into logical groups, such as enrichment, investigation, decision/escalation, response/remediation, and manage/logging, and each step has integrations for each category. Some of these can be added from the marketplace menu in SOAR, while others must be added manually using APIs. Security engineers may need to create custom connectors using the Siemplify IDE, which requires knowledge of Python and object-oriented programming. (*Creating a Custom Connector, 2023*)

Playbooks produce two types of results: simple text results and JSON results, which require the ability to write expressions to extract desired data. (Playbook Lifecycle Management, 2020d, p.17) Engineers can use the Expression builder to simplify and use a list of functions provided by Siemplify. It is possible to change the content and style of the data displayed in Playbooks with simple HTML editing using the HTML widget (Using the HTML Widget, 2023, siemplify https://siemplify.elevio.help/en/articles/562-using-the-html-widget)

As for security analysts, they will use the case view the most. They can view the cases created as a result of the alerts, access the details of that case, see the triggered playbook, examine it, and access the raw data generated at each step. In some cases, analysts may need to take action, such as responding to the event. To do this, they need to analyze the nature of the attack, such as who was activated, when and what happened. If Mitre and Virus Total are added to enrich the data in the Playbook, it can help to understand the threat and identify the necessary precautions to take. (Working with Cases, 2023)

In conclusion, security engineers should be chosen from professionals who have experience in this field to prevent threats and create the security architecture. Since this field requires expertise, IT managers of small and medium-sized companies should evaluate whether they have the skills listed above. Security analysis requires less technical skill, and if effective playbooks are created, security analysts will have less responsibility. However, the evaluation should be left to the IT managers of the companies. It is recommended that the security engineering task be performed by third-party providers or professionals in this field, based on the observations obtained throughout this study. On the other hand, the task of security analysts should involve classifying cases according to their severity. Low and medium-level cases can be evaluated by the IT managers of the companies, while the investigation and intervention of high-grade threats should be left to the experts. Companies can manage security operations by outsourcing these specialists or by establishing a dedicated unit for this purpose.

4.0 Device Enrollment

Device enrollment refers to the process of registering and configuring a device for use on a network, often to manage and secure it. The process typically involves installing a specific software or agent on the device, which then communicates with a management server to receive configurations, policies, and software updates. This allows IT administrators to manage and secure devices at scale, ensuring they are up-to-date and meet security standards. (Microsoft, 2022)

Google Workspace offers a cloud-based device management solution called Google Endpoint Manager. It allows administrators to manage and secure a wide range of devices from a single, centralized console.

4.1 Mobile security

Google has a wide range of compatibility and covers the most common devices and operating systems, such as android and iOS. Beneath is an overview of the minimum software requirements for each of the different security solutions Google offers for mobile security management.

For mobile:

Feature	Available for	Requirements
Basic mobile management	· Android 2.2 Froyo and later · Apple iOS 8 and later · iPadOS 13.1 and later	· Latest version of Google Play services app · Apple ID and Safari enabled
Advanced mobile management	· Android 6.0 Marshmallow and later · iOS 12.0 and later · iPadOS 13.1 and later	· Supports work profiles and company-owned (fully managed) device mode. · Apple ID and Safari enabled
App management	· Android 5.0 Lollipop and later · Android 2.2 to 4.4.4 KitKat devices without a work profile · iOS 12.0 and later · iPad OS 13.1 and later	· Work profile
Work profiles	· Android 5.0 and later	
Company-owned devices	· Android 6.0 Marshmallow and later · iOS 12.0 and later · Devices running Chrome OS	

(Google, 2023x)

The only significant difference is between the basic and the advanced mobile management features, where the basic is compatible with older versions of Android and iPhone and the advanced solution requires software that is relatively up to date.

4.1.1 Basic mobile security

This option provides the fundamental tools you need to let the employees in your organization access their work accounts through their mobile phones (Google, 2023y). This setting is turned on by default and provides core security like hijacking protection.

Google Endpoint Management provides an option to customize password requirements for managed mobile devices (Google, 2023y). The administrator can enhance the security of the organization's data by, for instance, mandating the use of a screen lock or password on managed mobile devices. The users will receive prompt notification if their password does not meet the set requirements, and they must change it within 24 hours to continue accessing their work data. In case the password requirements are not fulfilled within the specified time frame, the user will be denied access until they comply with the requirements. If you want to avoid the 24-hour delay, Context-Aware Access can be set up to block non-compliant devices immediately (Google, 2023y).

Another option is to manage mobile apps for your organization. This function allows the admin to control which apps android and iOS device users can find and install, by adding them to a web and list in the admin console. These include both third-party apps and private apps (Google, 2023z).

A third security function is an ability of an administrator to wipe corporate data from a device. This security feature is useful if a device goes missing or an employee leaves the organization. Depending on the platform, you can wipe a user’s account, profile, or all data. The data is still accessible on another authorized device (Google, 2023aa).

The basic mobile security management also includes system-defined rules and a list of all devices that have been used to access users' work accounts. This list includes information about the type of device, model, last time work data has been synchronized, and the name of the user. From this list, the administrator can block a device from syncing work data, wipe data from a lost device, and more (Google, 2023ab).

To prevent a device from syncing data, you can block the device. To require the user to sign in again, you can delete the device (Google, 2023ai).

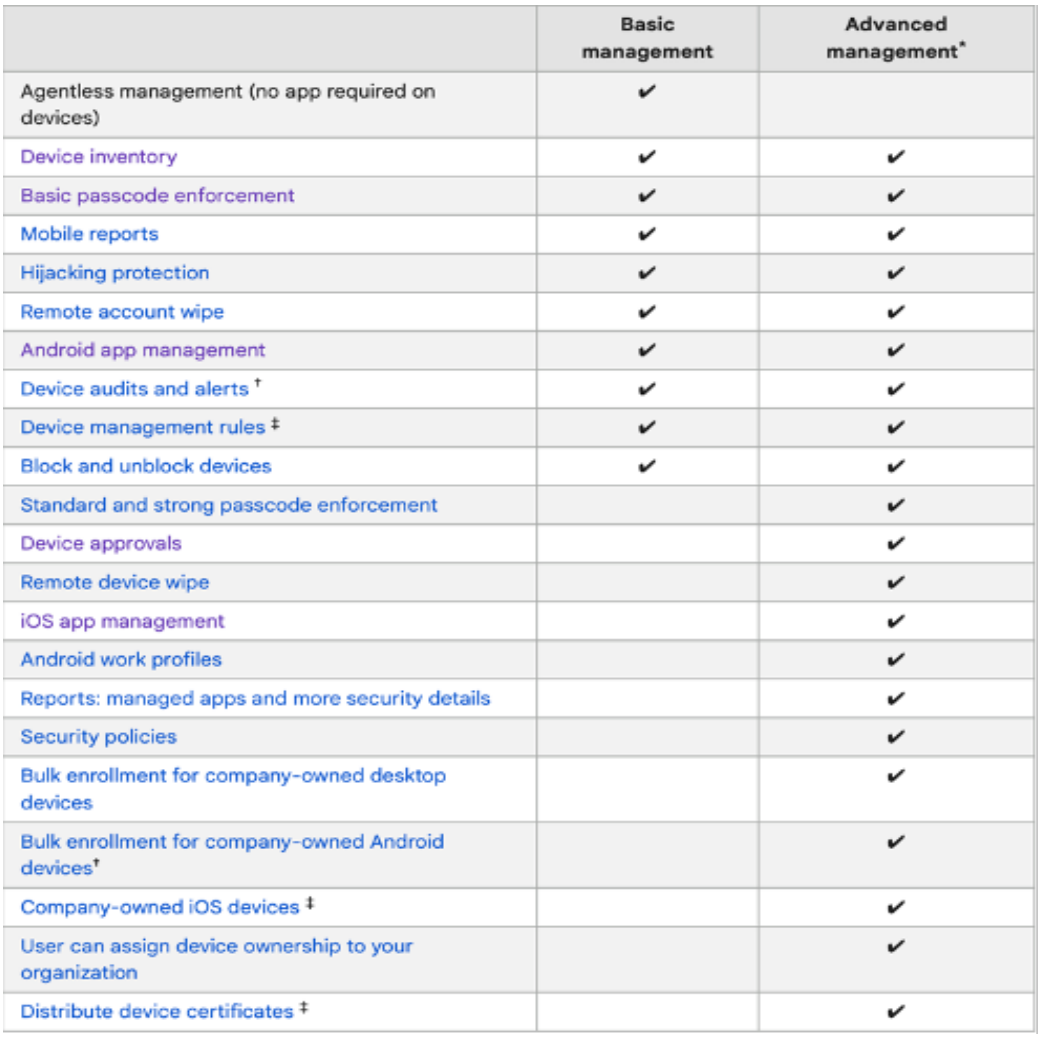
4.1.2 Advanced mobile security and app management

The advanced mobile security and app management offers the same options as the basic management option in addition to multiple other functions for more control over the organization. One of the differences is the option to require admin approval for device access. When a work account is added to a user's device, they will receive a message stating that an admin needs to review and approve the device. Exceptions can be made for company-owned devices that are registered by serial numbers. The same applies if the device has been added to the list of company-owned devices (which you can read more about later).

The advanced options also offer the possibility to wipe a device, not just an account. Unless the device is an Android device with a work profile, it removes all data and apps – Both work-related and personal (Google, 2023aa). This can be a great way to reduce the risk for both the organization and the user, as all data is erased and contributes to minimizing the risk of unauthorized access and theft. By also removing accumulated junk, it will improve the performance of the device for the next user, for example, if it is a company-owned device that is being overtaken by a new employee. It will also make it easier to reuse. It should, however, be compared to some downsides, like the possibility of losing data or personal information that may not be recoverable. It is also time-consuming to wipe a device and may be inconvenient for the users.

The advanced option also offers the possibility to approve, block or delete a device. Devices are approved by default unless you require admin approval. When admin approval is activated, devices are blocked by default and added to a list of devices pending approval. To deny syncing, the process is the same as for the basic management option. However, the advanced option allows you to set up management device rules to automatically approve or block devices, which decreases the administrator's workload (2023ai).

Beneath is an overview of the differences between the basic and the advanced option



	Basic management	Advanced management*
Agentless management (no app required on devices)	✔	
Device inventory	✔	✔
Basic passcode enforcement	✔	✔
Mobile reports	✔	✔
Hijacking protection	✔	✔
Remote account wipe	✔	✔
Android app management	✔	✔
Device audits and alerts †	✔	✔
Device management rules ‡	✔	✔
Block and unblock devices	✔	✔
Standard and strong passcode enforcement		✔
Device approvals		✔
Remote device wipe		✔
iOS app management		✔
Android work profiles		✔
Reports: managed apps and more security details		✔
Security policies		✔
Bulk enrollment for company-owned desktop devices		✔
Bulk enrollment for company-owned Android devices†		✔
Company-owned iOS devices ‡		✔
User can assign device ownership to your organization		✔
Distribute device certificates ‡		✔

(Google, 2023ad)

4.2 Computer security

Just like the mobile management features, Google supports most of the commonly used operating systems such as Windows, Mac, Linux, and Chrome. However, there are some significant differences depending on which endpoint management options your organization requires or prefers. The following part will cover the main differences between the various options.

Feature	Available for
Fundamental management	Microsoft Windows, Apple Mac, Linux, Chrome OS, smart home devices
Endpoint verification	Chrome OS, Chrome browser
Google Drive for desktop	Microsoft Windows, Apple Mac
Enhanced desktop security for Windows	Microsoft Windows 10 (company-owned)
Company-owned devices	Devices running Chrome OS, Mac, Windows, Linux

(Google, 2023x)

4.2.1 Fundamental management

All desktop devices that log into Google Workspace will get this package by default, with no setup required and no additional costs. This option allows you to control which laptops, desktops, and other endpoints can access your organization's data – and get details about those endpoints. In addition, you can see when a user signs into their managed account and get some details about the device. A useful security function is the ability to remotely sign out a user from a managed Google account. If you don’t recognize a device, a user is being suspended or removed, a device is lost or stolen or you’re changing a password, it can be a useful function against possible threats (Google, 2023ae). To deny devices syncing data, the process is similar to the basic mobile management option. (Google, 2023ai).

4.2.2 Endpoint verification

The endpoint verification option is only available with a Chrome Browser extension on user's devices (Google, 2023ag). However, Google Chrome is supported on most operating systems, and therefore shouldn't be a big issue (Google, 2023af). Unlike the fundamental option, this is not applied automatically. In this case, the administrator can turn endpoint verification on or off. Endpoint verification allows the administrator to get details about devices running Chrome OS or Chrome browser that access your organization's data. This gives access to information about the operating system, device, and users for personal devices and devices owned by your organization. Useful for controlling who has access to your data. This can be combined with Context-Aware Access (CAA), which enables the administrator to control access based on device location, security status, or other attributes. For example, you can require device approval (Similar to the advanced option for mobile management) and then create a CAA policy that blocks the device if the status is "pending" or "blocked" (Google, 2023ah).

You can also acquire a list of users who do not have endpoint verification enabled and send an email asking them to install it (Google, 2023ah).

To control which devices users can control access work data from, the administrator can approve, block, or delete a device in the admin console. Unless you require admin approval, users are approved by default. When approval is pending or blocked, you need to set up CAA levels to block status and deny users to sync data (Google, 2023ai).

4.2.3 Google Drive for desktop

Google Drive for desktop is only available for Microsoft Windows and Apple Mac. Google Drive is useful for enabling users to get started with cloud-based files and collaboration. As an administrator, you can control how users get Google Drive for desktop on their computers (Self installment or software deployment tools) and what features are available for them. This includes the option of only making it available to company-owned devices. The device will be blocked if the serial number doesn't match, or the device is not added to the inventory list. An important security measure to remember is that Drive for desktop does not prevent data theft, as it is still possible to copy data to other non-secured areas, like another hard drive (Google, 2023aj). The ability to approve, block, or delete a device is similar to the endpoint verification option, except for the extra security measure of restricting Drive to company-owned devices (Google, 2023ai)

4.2.4 Enhanced desktop security for Windows

This option offers the most security options, but it is only available for company-owned Microsoft Windows 10. By applying the Windows device management, the Windows setting you set in the admin console are applied to all Windows 10 devices in your organization (Google, 2023ak). This feature can be used in a standalone mode, but the best security is provided when it is combined with Google Credential Provider for Windows (GCPW). You can configure GCPW so a user's Google Account syncs with their Active Directory or local Windows profiles. GCPW also provides the user with additional security benefits, such as anti-hijacking, 2SV, and login challenges (Google, 2023ai).

GCPW can also be combined with SSO, which enables users to access Google Workspace and SSO apps in Chrome without having to re-enter credentials. GCPW and Windows device management together also automatically enroll Windows devices when the user signs in through GCPW – but only one user per device.

This option is a good way to secure your organization against data theft with the possibility of disabling USB drives, blocking specific apps, and configuring BitLocker to encrypt your data (Google, 2023ak).

References

Anderson, Ross J. (2008). Security engineering: a guide to building dependable distributed systems (2 ed.). Indianapolis, IN: Wiley. p. 1040. Chapter 2, page 17 https://books.google.com/books?id=ILaY4jBWXfcC

Auth0 (n.d.). *What is authentication?* Retrieved 07.03.23 from https://auth0.com/intro-to-iam/what-is-authentication

Bradley, T. (2023, 27.januar). The keys to effective identity security for 2023. *Forbes.* https://www.forbes.com/sites/tonybradley/2023/01/27/the-keys-to-effective-identity-security-for-2023/?sh=3736117d1b73

Chiasson, S. & Oorschot (2015). Quantifying the security advantage of password expiration policies. Designs Codes and Cryptography. 77(2-3). https://link.springer.com/article/10.1007/s10623-015-0071-9

Clercq, J.D. (2002). Single Sign-On Architectures, 40-41, https://link.springer.com/chapter/10.1007/3-540-45831-X_4

Cyberpedia (n.d.) What is SOAR- Retrieved 01.03.2023 from: https://www.paloaltonetworks.com/cyberpedia/what-is-soar

Dehand, Khosrow (2002, April), A Simple way of improving the Login security, Retrieved from: https://www.sciencedirect.com/science/article/pii/0167404889900539#aep-abstract-id3

Digital trends, Sandy Writtenhouse.(July, 2022) What is Google Workspace? Retrieved 22.02.2023 from: https://www.digitaltrends.com/computing/what-is-google-workspace/

Drake,B.(2022). Alert Center Overview. Founded: 17.01.2023. From: https://www.civicengagecentral.civicplus.help/hc/en-us/articles/115004729134--Alert-Center-Overview

De Groot J (December 2022), what is data classification. Retrieved from: https://digitalguardian.com/blog/what-data-classification-data-classification-definition

Google (2023):

a. *About the alert center.* Retrieved from : https://tinyurl.com/6abftmy4

b. *Control access to less secure apps*. Retrieved from: https://tinyurl.com/5xza2rzx

c. *Enforce and monitor password requirements for users*. Retrieved from: https://tinyurl.com/ydw9f2wt

d. *Set session length for Google Cloud Services*. Retrieved from: https://tinyurl.com/33uyrmzt

e. *Protect your business with Context-Aware Access.* Retrieved from: https://tinyurl.com/4unczpb

f. *Protect your business with 2-Step Verification.* Retrieved from: https://tinyurl.com/rb3b8jzm

g. *Create and manage rules from the Rules page.* Retrieved from: https://tinyurl.com/4r35ksz7

h. *Create and manage reporting rules.* Retrieved from: https://tinyurl.com/2w37j4m5

i. *Create and manage activity rules.* Retrieved from: https://tinyurl.com/bd4k7rej

j. *Create data protection rules.* Retrieved from: https://tinyurl.com/528a9kzr

k. *View and edit system-defined rules.* Retrieved from: https://tinyurl.com/24wvfh9j

l. *Create and manage trust rules for Drive sharing*. Retrieved from: https://tinyurl.com/a6y66ha4

m. *Set session length for Google Services.* Retrieved from: https://tinyurl.com/yks4d25j

n. *Create DLP for Drive rules and custom detectors.* Retrieved 16.01.23 from: https://tinyurl.com/yy3vnysa

o. *Manage external sharing for your organization.* Retrieved 16.01.23 from: https://tinyurl.com/3drpev7s

p. How to use predefined content detectors. Retrieved 16.01.23 from: https://tinyurl.com/2upctvfr

q. View the Drive DLP Data protection insights report. Retrieved 16.01.23 from: https://tinyurl.com/52ytve4y

r. *Login challenges.* Retrieved from: https://tinyurl.com/ms29t9c9

s. *About SSO.* Retrieved from: https://tinyurl.com/3zcrwy9r

t. *SAML-based SSO: technical overview.* Retrieved from: https://tinyurl.com/bddpsjud

u. *Best practices for third-party IdP SAML apps configurations.* Retrieved from: https://tinyurl.com/mzcy7u64

v. *About advanced data protection.* Retrieved 23.01.23 from: https://tinyurl.com/4k7bn9wh

w. *Device requirements for Google endpoint management.* Retrieved from: https://tinyurl.com/bdf9hx6j

x. *Set up basic mobile device management.* Retrieved from: https://tinyurl.com/42phfd7c

y. *Manage mobile apps for your organization.* Retrieved from: https://tinyurl.com/42phfd7c

z. *Wipe corporate data from a device.* Retrieved from: https://tinyurl.com/3jv3dw22

aa. *View mobile devices that access work data.* Retrieved from: https://tinyurl.com/mwufmwz7

ab. *Overview, Google Workspace Admin Help*. Retrieved 06.02.2023 from:https://tinyurl.com/46a52dfy

ac*. Compare mobile management features.* Retrieved from: https://tinyurl.com/ybucrjv6
ad. *Sign a user out of a managed Google Account.* Retrieved from: https://tinyurl.com/2buyxfvd
ae. *Chrome browser system requirements.* Retrieved from: https://tinyurl.com/9cfbv8fs
af. *Overview: Manage user´s computers & smart home devices.* Retrieved from: https://tinyurl.com/yc7aa66z
ag. *Turn endpoint verification on or off*. Retrieved from: https://tinyurl.com/39dhdex3
ah. *Approve, block, unblock, or delete a managed device.* Retrieved from: https://tinyurl.com/ys4dznxm
ai. *Use drive for desktop with Google Endpoint management.* Retrieved from: https://tinyurl.com/4nfzdwkm
aj. *Enable Windows device management.* Retrieved from: https://tinyurl.com/4m9dr6ja
ak. Overview: Enhanced desktop security for Windows. Retrieved from: https://tinyurl.com/vrf2whfa
al. Prevent spam, spoofing & phishing with Gmail authentication. Retrieved from: https://tinyurl.com/bn3ky28h
am. Advanced phishing and malware protection. Retrieved from: https://tinyurl.com/yaemzmrw
an. Chronicle SOAR Technical Support Services Guidelines. Retrieved 14.02.2023 from: https://tinyurl.com/8uxsc3f6
ao. 5 ways a SOAR solution improves SOC analyst onboarding. Retrieved 22.02.2023 from: https://tinyurl.com/y7abstym
ap. Google´s efforts to identify and counter spyware. Retrieved 22.02.2023 from: https://tinyurl.com/k2hp574p
aq. *Advanced Protection Program.* Retrieved from: https://tinyurl.com/4k7bn9wh
av. Protect Google Workspace accounts with security challenges. Retrieved 26.03.2023 from https://tinyurl.com/3u76patj
https://support.google.com/a/answer/6002699?hl=en#zippy=%2Cexamples-of-sensitive-actions%2Cwhen-does-a-user-see-a-security-challenge%2Cas-an-administrator-can-i-choose-which-type-of-login-challenge-to-show-my-users%2Csensitive-action-blocked
ay. Assign Context-Aware access levels to the Admin console. Retrieved 26.03.2023 from https://tinyurl.com/bddwxwkk https://support.google.com/a/answer/11068433
Gmail Help (2023a) *Avoid and report phishing emails.* Gmail Help. Retrieved from: https://tinyurl.com/2fwnpwbz
Jansson, K.; von Solms, R. (2011-11-09). "Phishing for phishing awareness". Behaviour & Information Technology. 32 (6): 584–593. doi:10.1080/0144929X.2011.632650
IBM. (n.d). Integrations. Retrieved 14.02.2023 from: https://www.ibm.com/products/qradar-soar/integrations
Kumaran, Neil (2019, February) Spam does not bring us joy—ridding Gmail of 100 million more spam messages with TensorFlow Retrieved from: https://workspace.google.com/blog/product-announcements/ridding-gmail-of-100-million-more-spam-messages-with-tensorflow

Kirtley, E. (2022). What is SOAR vs SIEM: Security Solutions Explained. Visited: 14.02.2023. Retrieved from: https://swimlane.com/blog/siem-soar

Kovacic, D. (2022). *API Security: The Complete Guide to Threats, Methods & Tools*. Visited: 19.01.2023. Retrieved from: https://brightsec.com/blog/api-security/

Kranz G &, Fitzgibbons L (July 2022) data classification, Retrieved: 05.02.2023. from: https://www.techtarget.com/searchdatamanagement/definition/data-classification

Microsoft. (2022, 07.november). *What is device enrollment?* Learn. Retrieved from: https://learn.microsoft.com/en-us/mem/intune/user-help/use-managed-devices-to-get-work-done

Microsoft. (n.d.). What is two-factor authentication? Retrieved 08.03.23 from https://www.microsoft.com/en-us/security/business/security-101/what-is-two-factor-authentication-2fa

OAuth. (2023, 5.januar). I Wikipedia. https://en.wikipedia.org/wiki/OAuth

Onelogin (i.d.). Authentication vs. Authorization. Visited: 19.01.2023 From: https://www.onelogin.com/learn/authentication-vs-authorization

OpenID (2022,November) What is OpenID Connect?, Retrieved from: https://openid.net/connect/

Pashalidis A. & Mitchell C. J. (2003) A Taxonomy of Single Sign-On Systems, 249 https://link.springer.com/chapter/10.1007/3-540-45067-X_22

Perez, Sara (18.March 2020) Techcrunch, *Googles advanced protection program for high risk users now includes malware protection.* Visited: 23.01.2023 Retrieved from: https://techcrunch.com/2020/03/18/googles-advanced-protection-program-for-high-risk-users-now-includes-malware-protection/

Playbook Lifecyle Management (2020a) Playbook Lifecyle Management, p. 1.
Visited: 21.02.2023 Retrieved from https://cdn.elev.io/file/uploads/raEXHEUeZuVTHs6dRYCY6y2voCpa34wo3QprCO0wQX4/81jDpI5Mb06o-0gjVrwAwU0Yw-jNp2YRDEFHDVUHd6U/PlaybookTheoryof--9Y.pdf

Playbooks. Retrieved 21.02.2023 from https://www.manula.com/manuals/siemplify/user-guide/5.6.x/en/topic/playbooks?q=investigate

Playbook Lifecyle Management (2020b) Know Your Allerts, p. 4.
Visited: 21.02.2023 Retrieved from https://cdn.elev.io/file/uploads/raEXHEUeZuVTHs6dRYCY6y2voCpa34wo3QprCO0wQX4/81jDpI5Mb06o-0gjVrwAwU0Yw-jNp2YRDEFHDVUHd6U/PlaybookTheoryof--9Y.pdf

Playbook Lifecyle Management (2020c) Analyze existing manual flow, p. 6.
Visited: 21.02.2023 Retrieved from https://cdn.elev.io/file/uploads/raEXHEUeZuVTHs6dRYCY6y2voCpa34wo3QprCO0wQX4/81jDpI5Mb06o-0gjVrwAwU0Yw-jNp2YRDEFHDVUHd6U/PlaybookTheoryof--9Y.pdf

Siemplify. (2023). Siemplify Product Documentaton.
Alert Grouping Mechanism (Admin). Retrieved from https://documents.siemplify.co/en/articles/39-alert-grouping-mechanism-admin 17.02.2023.

Cases overview. Retrieved from https://documents.siemplify.co/en/articles/64-cases-overview 17.02.2023.
Create and Run a Playbook. Retrieved from https://siemplify.elevio.help/en/articles/183-create-and-run-a-playbook 20.02.2023.
Creating a Custom Connector, Retrived from https://documents.siemplify.co/en/articles/170-creating-a-custom-connector 20.02.2023
How does Siemplify work? Retrieved from https://www.manula.com/manuals/siemplify/user-guide/5.6.x/en/topic/?q=investigate 22.02.2023
Manage task from the Cases Screen. Retrieved from https://documents.siemplify.co/en/articles/500-manage-tasks-from-the-cases-screen 17.02.2023.
Using the HTML Widget, Rertrieved 20.03.2023 from https://siemplify.elevio.help/en/articles/562-using-the-html-widget
Using Triggers in Playbooks. Retrieved from https://documents.siemplify.co/en/articles/416-using%20-triggers-in-playbook
Working with Cases. Retrieved from https://documents.siemplify.co/en/categories/50-working-with-cases 21.02.2023

Siemplify. (2020). *Playbook Lifecycle Management: Theory behind building the perfect Playbook.* Retrieved from https://cdn.elev.io/file/uploads/raEXHEUeZuVTHs6dRYCY6y2voCpa34wo3QprCO0wQX4/81jDpI5Mb06o-0gjVrwAwU0Yw-jNp2YRDEFHDVUHd6U/PlaybookTheoryof--9Y.pdf

Shastri. V.(2022, 11 October) Identity Security. Crowdstrike, Cybersecurity 101 https://www.crowdstrike.com/cybersecurity-101/identity-security/

Smith, J. (2020, 14 May). *79% of Organizations Have Experienced an Identity-Related Security Breach in the Last Two Years According to New Identity Defined Security Alliance Study.* Globe Newswire. Retrieved from https://www.globenewswire.com/news-release/2020/05/14/2033444/0/en/79-of-Organizations-Have-Experienced-an-Identity-Related-Security-Breach-in-the-Last-Two-Years-According-to-New-Identity-Defined-Security-Alliance-Study.html

Softprom (n.d.) Siemplify SOAR platform, Retrieved 01.03.2023 from: https://softprom.com/vendor/siemplify/product/soar-platform

Summers, W., Bosworth, E. (2004). Password Policy: The Good, The Bad, and The Ugly. 1-6. Retrieved from: https://www.researchgate.net/publication/234799064_Password_policy_The_good_the_bad_and_the_ugly

Techtarget, Paul Crocetti.(February 2021) *Definition of data protection.* Retrieved 26.01.2023 from: https://www.techtarget.com/searchdatabackup/definition/data-protection

Techtarget, Sharon Shea.(March 2021) *Definition of SOAR.* Retrieved 22.02.2023 from: https://www.techtarget.com/searchsecurity/definition/SOAR

Titus (n.d.). Data classification for Google workspace. Retrieved from: https://www.titus.com/resources/datasheets/data-classification-for-g-suite

Trost, R. (n.d). TIP vs. SIEM vs. Ticketing System – part 1. Visited: 14.02.2023. Retrieved from: https://www.threatq.com/tip-vs-siem-vs-ticketing-system-part-1/

Trost, R. (n.d). TIP vs. SIEM vs. Ticketing System – part 2. Visited: 14.02.2023. Retrieved from: https://www.threatq.com/tip-vs-siem-vs-ticketing-system-part-2/

Witts, J. (2023. 08. March). *The Top 10 User Authentication And Access Management Solutions.* Visited: 17.03.2023. Retrieved from: https://expertinsights.com/insights/top-10-user-authentication-and-access-management-solutions/

Yildirim, M., Mackie, I. Encouraging users to improve password security and memorability. Int. J. Inf. Secur. 18, 741–759 (2019). https://doi.org/10.1007/s10207-019-00429-y

Zhang, Y., Monrose, F. & Reiter, M. (2010). The security of modern password expiration: an algorithmic framework and empirical analysis. *CCS '10: Proceedings of the 17th ACM conference on Computer and communications* security. 176-186. https://doi.org/10.1145/1866307.1866328