GROUP ASSIGNMENT

NAME (TP NUMBER)	**:**	Androjuniko (TP081988) Tung Jean San (TP082276) Koo Wai Kit (TP081761)
INTAKE CODE	**:**	APUMF2406CYS
MODULE TITLE	**:**	Security Operations Centre and Incident Response (072024-JUL)
MODULE LECTURER	**:**	Dr. Julia Binti Juremi
PROJECT TITLE	**:**	Assignment 1 Section B (Proposal)
DATE ASSIGNED	**:**	16 July 2024
DATE COMPLETED	**:**	9 September 2024

Table of Contents

List of Tables

1.0 Introduction

In today’s rapidly evolving digital landscape, organisations face an increasing volume of cyberattacks, ranging from ransomware to distributed denial-of-service (DDoS) attacks. These threats are becoming more sophisticated and can severely impact business operations, customer trust, and overall financial performance. As a result, it has become imperative for organisations to enhance their cybersecurity capabilities to detect, respond, and mitigate potential risks swiftly.

A Security Operations Center (SOC) serves as a centralised function that addresses this need by enabling continuous monitoring, analysis, and response to security incidents (Scapicchio et al., 2024). By having a well-structured SOC, an organisation can proactively manage cybersecurity threats, improving its incident handling capabilities and reducing the time it takes to detect and respond to cyberattacks. Beyond securing assets, an SOC contributes to an organisation’s overall business objectives by supporting a more resilient and adaptive security posture.

For this proposal, we have chosen Grab Holdings Ltd., a leading Southeast Asian technology company that offers ride-hailing, food delivery, and digital payment services, as the organisation under study. Given its expansive user base and diverse operations across multiple countries, Grab is highly exposed to a wide range of cyber threats, making the establishment of a SOC crucial for its continued success.

This proposal outlines the specific needs and requirements for establishing an SOC within Grab and provides a detailed plan for implementing a highly effective SOC that addresses the company’s unique security challenges.

2.0 Security Operations Center (SOC) Overview

In this section, we provide an overview of the Security Operations Center (SOC), exploring its definition and purpose, key functions, team roles, and the critical role it plays in protecting modern businesses and ensuring continuity. This section aims to provide a basic understanding and background a SOC. Further technical information regarding SOC’s implementation will be discussed under Section 5.0.

2.1 Definition and Purpose

According to Microsoft (n.d.), a SOC is a centralised team tasked with strengthening an organisation's cybersecurity defenses through threat prevention, detection, and response. The SOC team, which can be either in-house or outsourced, continuously monitors various systems such as identities, endpoints, servers, databases, and network applications to detect cyberattacks in real time. When not hosted on-site, a SOC is frequently included in outsourced managed security services (MSS) provided by a managed security service provider (MSSP) (Scapicchio et al., 2024).

Additionally, SOCs perform proactive security tasks by leveraging the latest threat intelligence to stay informed about emerging threats and vulnerabilities (Microsoft, n.d.). Most SOCs operate 24/7, and larger organisations may utilise a global security operations center (GSOC) to coordinate efforts across multiple regions and manage global security risks effectively.

2.2 Key Functions

The activities and responsibilities of SOC can be organised into three main categories: preparation, planning, and prevention; monitoring, detection, and response; and recovery, refinement, and compliance (Scapicchio et al., 2024). According to Trellix (n.d.), a SOC provides ten core functionalities, and Table 1.0 below provides a summary of its key functions and descriptions.

Table 1: SOC Key Functions (Trellix, n.d.)

Key Function	**Description**
Resource Management	SOC oversees the security of various devices and applications, ensuring visibility across the network to prevent blind spots. This involves understanding and managing all cybersecurity tools and workflows.
Preparation and Preventative Maintenance	SOC engages in proactive measures to prevent security breaches by staying updated on emerging threats, maintaining systems, updating firewall policies, and applying patches.

Continuous Monitoring	SOC tools continuously scan the network for abnormalities and suspicious activities, using advanced technologies to differentiate between normal operations and potential threats.
Alert Management	SOC evaluates alerts from monitoring tools, filtering out false positives, and prioritising genuine threats to address the most critical issues promptly.
Threat Response	Upon confirming an incident, the SOC acts to contain and mitigate threats, minimising impact on business operations by isolating affected systems and eliminating harmful processes.
Recovery and Remediation	After an incident, the SOC works to restore systems and recover data, employing measures like reconfiguring systems or using backups to return operations to normal.
Log Management	SOC collects and reviews logs of all network activity to establish a baseline for normal behaviours, detect threats, and support forensic investigations.
Root Cause Analysis	Following an incident, the SOC investigates to determine the cause and prevent future occurrences, using log data and other information to trace the problem.
Security Improvement	SOC continuously refines its practices to counter evolving cyber threats, implementing improvements based on security roadmaps and practical exercises.
Compliance Management	SOC ensures adherence to regulatory requirements and industry standards, performing regular audits to protect sensitive data and avoid legal issues.

These functions enable the SOC to effectively safeguard an organisation’s digital assets, ensuring a proactive and responsive approach to cybersecurity.

2.3 Benefits

According to Scapicchio et al. (2024), SOC offers significant benefits to organisations. First of all, it enhances asset protection by proactively monitoring and addressing threats, which helps safeguard critical systems and sensitive data. In addition, SOC not only manages security incidents, but it also oversees the deployment and maintenance of cybersecurity tools, helping to improve the organisation's overall security posture.

Scapicchio et al. (2024) further explains that having a SOC can help to ensure business continuity by minimising the impact of security incidents, thus maintaining productivity and customer satisfaction. They also aid in regulatory compliance by implementing effective security measures and keeping detailed records. Financially, SOC provides cost savings by preventing costly data breaches. In the case of outsourced SOCs, it will reduce the need for in-house security staff. Furthermore, it can build customer trust through a demonstrated commitment to cybersecurity. SOC also improves risk management and incident response, allowing for quicker threat detection and resolution, ultimately reducing downtime and mitigating potential damage.

For Grab Holdings Ltd., implementing a SOC could greatly enhance its ability to protect its extensive digital infrastructure and customer data. The SOC would play a crucial role in ensuring business continuity by managing and mitigating the impact of security incidents, which is essential for maintaining operational efficiency and customer trust. Additionally, the SOC's proactive threat detection and regulatory compliance efforts would align with Grab's commitment to security and privacy, ultimately supporting its strategic goals and protecting its reputation in the competitive tech landscape (Grab, n.d.).

3.0 Organisation Overview

Grab Holdings Ltd., also known as Grab, is one of Southeast Asia's largest multi-functional app that offers a variety of daily services. This includes ride-hailing, food and parcels delivery, digital payments, financial services, and many more. Founded in 2012 as a taxi-booking app in Malaysia (Siddharth, 2014), Grab has expanded its reach across Southeast Asia and is currently operating in eight countries: Singapore, Malaysia, Indonesia, Thailand, Vietnam, the Philippines, Cambodia, and Myanmar. With Singapore being its headquarter, Grab's mission is to drive Southeast Asia forward by leveraging technology to solve everyday challenges, empower communities, and enhance economic inclusion in the region.

3.1 Business Model and Services

Grab's business model is centred around its functional platform, which incorporates services to address the daily needs of consumers, drivers, and merchants. This model not only improves user convenience by having diverse services on one platform but also promotes customer loyalty through a seamless user experience. Main services include:

- **Mobility Services**: Started as a ride-hailing service and has now transformed into various transportation modes, including private cars, motorbikes, taxis, and carpooling options.
- **Deliveries**: With GrabFood, GrabMart, and GrabExpress, the company offers food delivery, grocery shopping, and courier services. They are tailored to the increasing demand for contactless delivery options.
- **Financial Services**: Grab Financial Group, a subsidiary of Grab, provides digital payment solutions via GrabPay, which also includes lending, insurance, and investment products. They have huge markets and in demand in Southeast Asia, where many consumers remain unbanked or underbanked.

3.2 Market Position and Impact

Grab has transformed into an essential part of daily life for many customers in Southeast Asia, with app downloads of over 214 million, as well as millions of partners which is comprised of drivers, merchants, and small businesses. Grab’s approach has placed itself as one of the biggest players in the region, which earned itself the title of one of the most innovative companies in Asia-Pacific (Marwan, 2023), competing with others such as Gojek and Foodpanda.

Grab’s operations have a major impact on the socio-economic background of Southeast Asia, which is possible through the creation of income opportunities for drivers and small businesses. The company's dedication corporate social responsibility is noticeable through various actions taken with the goal of supporting local communities, fostering sustainability, and expanding financial inclusion.

3.3 Cyber Security Challenges

As an online platform processing a huge amount of sensitive data, including personal information, purchase details, and transaction records, Grab can be seen as a prime target by threat actors. Threats such as ransomware, phishing, and data breaches, pose significant issue to its operations and prominence. Given the important nature of Grab's services, any disruption could cause considerable financial damages, legal actions, and the loss of customer loyalty.

To address these cybersecurity issues, a thorough Security Operations Centre (SOC) is required for Grab. An SOC will allow for constant monitoring, threat detection, responsive incident response, and synchronised approach to defence against cyber threats (Scapicchio et al., 2024). By implementing an SOC into its operations, Grab can enhance its security posture, comply with regulatory requirements, and protect the integrity of its digital landscape.

4.0 Needs and Requirements for a SOC in Grab Holdings Ltd.

Grab Holdings Ltd. has revolutionised the way people get their access to transportation, delivery, and financial services. Operating in a digital landscape that develops rapidly, Grab's offerings depend on a system technological environment that handle a large quantity of sensitive user data, financial transactions, and logistical operations. This causes Grab to be exposed to a variety of cyber threats that could cause a considerable disruption to its business operations, compromise confidential data, and damage its reputation.

To address these challenges and ensure the security and resilience of its technological infrastructure, a comprehensive solution to cybersecurity that includes a properly designed Security Operations Centre (SOC) is essential for Grab. A SOC is a team with the assigned responsibility of monitoring, detecting, analysing, and responding to cybersecurity incidents in real time. It serves as the centre of an organisation's security posture, providing continual surveillance and robust defence against cyber threats.

The establishment of a SOC within Grab is not only a defensive measure. It is a strategic requirement that goes along with the company's dedication to user protection, complying with data protection regulations, and maintaining consumers' trust towards the brand (Grab, n.d.). A well-built SOC will foster growth in Grab's capacity to anticipate, prevent, and mitigate, thereby keeping the level of potential damages low and ensuring services are delivered smoothly.

4.1 Organisation’s Threat Landscape

Since Grab operates in a highly interconnected digital landscape, it is prone to a broad range of cybersecurity threats. As a sizable organisation in Southeast Asia's digital economy, Grab deals with plenty of sensitive data that needs to be secured, which are attractive targets for cybercriminals who are continuously looking for window of opportunities to exploit those data for financial gains or other malicious intents. Not only that, but Grab also has to contend with risks that may come from within its own, such as insiders and accidental damages by employees. With all that being said, it is essential for Grab to identify the threat landscape, where it is comprised of a general scope of the currently recognised cyberattacks and future cyber threats (Chipeta, 2023). In this case, Grab’s threat landscape can be divided into three main categories, which are threat actors, attack vectors, and vulnerabilities.

4.1.1 Threat Actors

a. Cybercriminals

Cybercriminals are defined as perpetrators of cybercrimes with many reasons, some of which include to generate profit, damaging or disabling computers or online services, and to obtain illicit information (Brush, n.d.). They pose a notable threat to Grab due to the fact that it holds a considerable amount of data that can be lucrative for anyone with malicious intent.

Given Grab’s wide-reaching digital landscape across Southeast Asia, cybercriminals often carry out phishing schemes, ransomware attacks, and data breaches. Those attacks not only harm customer trust but also risk potential tremendous financial loss and legal penalties for Grab. With the rise of digital payments and ever-increasing reliance on digital transactions, Grab must guard against complex cybercriminal approaches designed to exploit vulnerabilities in its systems.

b. Insiders

An insider, or insider threat in this context, is anyone who has been granted a certain degree of authorised access in an organisation and misuses it for similar reasons as cybercriminals, all of which affects the confidentiality, integrity, and the availability of the organisation (YourShortlist, 2024). Although not always identical to cybercriminals, an insider can be related to them as an initial procedure to extend the reach to the desired information.

Insider threats represent a huge risk for Grab, since employees, contractors, or other parties with direct relationship to Grab that have authorised access to systems and database, they may intentionally or unintentionally put the organisation's security to a compromise. In Grab's context, insiders could misuse their access to leak data of customers', modify records, or disrupt operations. For instance, cybercriminals may take advantage of an insider as a beginning attack vector to pass through external defences, providing unauthorised access to sensitive information. Since Grab employs vast workforce and complex service environment, it must implement strict access controls, monitoring, and facilitate employee awareness programs to diminish the risks posed by insiders.

c. Hacktivists

Hacktivists are people who resort to hacking to voice their dissatisfaction motivated by an event or a particular social agenda, such as a political unrest (Putman, n.d.). While hacktivism begins when there is an elevated sense of social or political awareness, it generally does not carry malicious intent. For instance, a group of hacktivists may steal money or data. But those are being used to uphold social justice or to bring about policy changes, such as redistributing the stolen money to those in need. This distinction of objective ultimately sets them apart from cybercriminals.

Despite not having the tendency to pursue financial gain, hacktivists can cause significant interference to Grab's services by launching attacks such as Distributed Denial of Service (DDoS) or website defacement to make a statement. For example, Grab's operations might be targeted when there is a regional socio-political movement, where Grab is being perceived by the hacktivists as representing larger corporate or governmental interests that they oppose. Such attacks can risk public trust and obstruct Grab's ability to serve its customers, especially in a region as socially and politically diverse as Southeast Asia.

4.1.2 Attack Vectors

a. Phishing

Phishing is a branch within the cyberattack methods that makes use of fake emails, text messages, phone calls, or websites to scam people into sensitive data being shared without them knowing (Kosinski, 2024). It is also a form of social engineering, which takes advantage of human error, one of which is the lack of technological expertise, fake stories, and pressure tactics (IBM, n.d.). This meticulous approach results in victims being manipulated into cause unintentional damage.

Normally, a threat actor pretends to be the person in whom the victim has a trust. This can be a co-worker, boss, or anyone that the victim thinks is harmless. The attacker then asks for a request while also sending a set of instruction through an attachment or a malicious link, where the victim ends up falling into the perpetrator's trap. In its relevance to Grab's case, attackers can use phishing to exploit human errors to gain illegal access to information stored within Grab. Sophisticated phishing attempt can be launched against Grab's employees or customers, tricking and leading them into exposing sensitive credentials or downloading malicious software.

b. Ransomware

Ransomware is one type of malicious software that causes a victim's data or device entirely to be held hostage (Kosinski, 2024). This is followed by a threat to keep the information or device locked, or to a certain extent, deleted, unless the demanded ransom, which involves exorbitant rates, has been paid by the victim in exchange for the encryption key to regain access.

With that in mind, when Grab is being infected by a ransomware, it can cause severe financial losses due to the hefty amount of ransom being demanded. Additionally, secondary damages to its operations where service delivery or customer data changes are needed can also take place as a result of the encryption, which may also cost Grab financially. While data backup is an option, it is just a part of a larger solution, which is to employ a SOC for prevention, detection, and mitigation measures.

c. Distributed Denial of Service (DDoS)

A distributed denial-of-service attack (DDoS) happens when a series of machines are working in tandem to launch an attack against a specific target (CISA, 2021). DDoS attacks usually leverage botnets, which typically refers to hijacked IoT devices or devices that are purposedly rented out for such a use case, to launch wide-reaching attacks. The more devices that are being used, the more powerful the attack is, rendering the victim's system overwhelmed with requests, or worse, crashes, therefore unable to provide services of information access, or other network resources to legitimate users.

For an enterprise which operations rely heavily on providing services such as Grab, DDoS is one of the main focuses of cyberattack prevention within the attack vector field. A DDoS attack will not only cause unwanted disruptions, but also erode public trust in such a massive and well-established organisation in one of the most economically important part of the world.

4.1.3 Vulnerabilities

Vulnerabilities can be described as a weakness in a system that can be taken advantage of by threat actors to perform cyberattacks (NCSC, 2024). Vulnerabilities can be divided into several types, which include:

a. Flaws

Flaws refer to unintended functionalities or a defect in implementation. This can result from a lack of proper design or mistakes from implementation, and they can remain undetected due to lack of supervision. Understanding flaws is important since they are the points entry through which attackers can launch their attacks and therefore must be addressed to mitigate any risks. Flaws can take many forms, such as:

- **Buffer overflow**: Happens when more data is being written than the space specifically allocated for a program. This can be used to overwrite adjacent memory and execute malicious codes. Grab's services that involve processing real-time data such as payments, can be vulnerable if the validation of input is inadequate.
- **Open ports**: As Grab relies on cloud infrastructure, when network ports are left open because of errors in configuration, it can result in internal services to be revealed to the public and susceptible to scanning.
- **Misconfigured firewalls**: Firewalls that are not properly configured may lead to failure in restricting access, causing critical points within Grab's system to be exposed and heightens the potential of data breach.

- **Design flaws**: Not using secure encryption due to the result of a poor design approach will leave Grab users' data exposed to interception, inherently making the architecture of a system weak and easy to intercept.

b. Zero-day vulnerability

Zero-day vulnerabilities are security vulnerabilities that are discovered only recently, making them dangerous as there is no patch for the related issue, and increases the likelihood of the attack to succeed. They are typically used in higher-level attacks by attackers with considerable amount of resources, making them more advanced in nature. Furthermore, even though a zero-day attack is made publicly known, other threat actors may take advantage of it and create a reusable attack for other targets. This, in turn, further worsens the attack surface as a result of the lack of solution in the form of security patches.

As a high-profile target, Grab is prone to zero-day attacks, where it can be leveraged against common security measures and obtain access to private data or to cause disruption in services. If a zero-day vulnerability is discovered, it will provide a time window for attackers before a patch is made available. To make things worse, this risk is even larger when considering the size of Grab and the vast data that it stores. As attackers actively finds their way to launch attacks, Grab has to be proactive in hunting for threats and be able to respond in a swift manner to immediate threats.

c. User error

User error happens when a thoroughly designed computer or system is not used according to the intended design. This can potentially happen because of a lack of understanding or experience in using the relevant tool. For instance, a system administrator may unknowingly leave default account login credentials unchanged, making it vulnerable for attackers to access, or installing a software that they perceive to be harmless and therefore safe to use. Such common of a mishap can be problematic and as a security measure, Grab would need to consider constant investment in security training for its staffs, enforce comprehensive internal regulations regarding access controls, and apply security tools that can discover user errors and respond to them before they become a more serious security issue.

4.2 Security Goals

As a leading super-app in one of the most rapidly advancing regions in Asia, Grab handles an extensive amount of sensitive data, including personal information, transaction records, and users' location data. Protecting this data is of utmost importance to maintaining customer loyalty and ensuring the safety and quality of its services. Grab's cybersecurity goals are directed by the awareness to safeguard its digital ecosystem against continuously evolving cyber threats, and they are founded upon several primary principles and strategies.

4.2.1 Protecting User Data and Privacy

Grab places a strong emphasis on user data protection and privacy as a core part of its cybersecurity strategy. Given the nature of its business, Grab collects users' information to be processed further, and ensuring the confidentiality and integrity of this data is essential. Grab's approach includes advanced data encryption, strict access controls, and regular audits for compliance check with data protection laws such as the Personal Data Protection Act (PDPA) in Singapore and similar frameworks in other markets.

According to Grab's 2023 annual report from the U.S. Securities and Exchange Commission Form 20-F, Grab is committed to its risk management and strategy through the adoption of Enterprise Risk Management (ERM) (Grab Holdings Limited, 2024). This is also coupled with having a dedicated Cyber security leader for a cyber security team with the task of establishing relevant policies and frameworks, determine roles and responsibilities for the implementation of said policies and frameworks, facilitating and supervising the application of proper cyber security risk management strategies, among many others, to ensure strong cyber security posture. Grab also perform annual evaluations of the policies and frameworks to align themselves with relevant laws in the areas that they operate in. To further improve transparency, Grab also work together with third-party assessment providers and internal IT security compliance analysis, which are subject to internal and external audits.

Grab has been proactively upgrading its data protection measures in response to past incidents. One of such is the failure of Grab to safeguard both passengers' and drivers' personal details due to a software update vulnerability, which was the fourth time of the same incident to happen over the span of 2018 to 2020, resulting in multiple data breaches and fines from regulatory bodies (Wong, 2020). These incidents underscored the importance of establishing more stringent security policy and regularly monitoring for flaws and vulnerabilities that could attract attackers.

4.2.2 Ensuring Availability of Service and Resilience

Availability of service and resilience are pillars of Grab's operations, considering its heavy role in providing services like transportation, delivery, and digital payments. The objective of Grab's cybersecurity strategy aims to protect its infrastructure from disruptions caused by cyberattacks such as DDoS attacks, ransomware, and other types of malicious activities that could damage Grab's ability to provide services. In an effort to make the realisation of the objective possible, Grab has implemented several measures to fortify its cyber security defences and deploy detection tools to identify threats.

According to Grab's head of information security, Suchit Mishra, one step that they have taken was to apply detective controls in areas with the highest risk of being targeted by attacks, such as products, applications, services, and infrastructure (Tan, 2018). The strategy, which was referred to as "offence informing defence", was chosen since it was less intrusive and more affordable as the company placed a priority in threat detection. The detection stage was then followed by the process of building dashboards to provide insights from the collected data for better overview of the overall security position and to aid in future planning process. Furthermore, in support of maintaining resilience, Grab also provided a bug bounty programme with a reward of up to $10,000. This serves as an incentive for the broader cybersecurity community to contribute to the organisation's cyber security stance and to keep the business informed of their vulnerabilities and emerging threats.

4.2.3 Fostering a Culture of Security Awareness

Grab realises that its security posture does not only depend on the facility that technology offers, but also on the behaviour and awareness of its workforce, partners, and users. To promote a security awareness culture, Grab has set up training programs and other initiatives with educating its workforce about the importance of cybersecurity best practices as their aim (Grab, n.d.). This includes mandatory cyber security training, data privacy protection classes, as well as annual refreshers.

The culture of security awareness is further enhanced with implementing security-by-design principles and the data protection framework in its product development processes.

This ensures that fundamental security concerns are incorporated into every part of the products and services from the earliest stages of design, greatly reducing the risk of vulnerabilities being introduced into the organisation.

4.2.4 Building Trust and Transparency

Establishing trust with its users and stakeholders is a critical objective for Grab, and this also stretches to its approach to cybersecurity. Grab is committed to being transparent about its security practices and how it keeps user data safe, including allowing users to be a part of the privacy protection scheme (Grab, n.d.). For instance, Grab believes that users should have the privilege to control who can access their information. This, accompanied by security frameworks employed by Grab such as security email alerts or the ban of modified devices, consolidates the role of users even more in the security landscape, which serves as a base for building mutual trust.

The collection and use of customers' data is disclosed in greater detail in Grab's privacy notice, where explicitly defined use cases of the obtained information are communicated. This includes maintaining GrabDefence (a digital security service from Grab), identifying patterns on fraudulent activities, regulatory and internal audit compliance cases, and responding to law enforcement requests or court orders. With regards to data retention, customer information will be kept for purposes only related to Grab, such as to provide GrabDefence service, and any other requirements that is legal in nature. Once they are satisfied, the data are considered irrelevant, and steps will be taken to either delete or anonymise them.

4.3 SOC's Role in Achieving the Security Goals

Based on the overview of SOC's key functionalities in section 2, there are four main areas that are relevant to Grab's effort to realise its goals, which are continuous monitoring, alert management, threat response, security improvement, and compliance management. Each of the functionalities are related to the previously discussed goals in the following way:

4.3.1 Protect User Data and Privacy

A dedicated team of SOC plays a vital role in keeping user data and privacy safe by performing continuous monitoring of Grab's networks, systems, and applications for any indications of unauthorised access or data breaches. By using security tools such as Security Information and Event Management (SIEM), Intrusion Detection Systems (IPS), or Intrusion Prevention Systems (IDS/IPS), the SOC can detect potential threats and respond promptly to lower risks or prevent them from happening altogether. This proactive approach ensures that any attempt to compromise user data is detected and addressed in a quick manner, thereby upholding the confidentiality and integrity of the users' data.

In terms of regulatory compliance, the SOC is pivotal in ensuring compliance with data protection laws, some of which including GPDR (Global Data Protection Regulation) and PCI DSS (Payment Card Industry Data Security Standard) (Scapicchio et al., 2024). When applied to Grab, it would have to comply with the Personal Data Protection Act (PDPA) in Singapore and other relevant regulations across the regions where Grab operates. By maintaining an accurate log of security incidents and conducting regular audits, the SOC provides Grab the ability to meet the necessary regulatory requirements and demonstrate its responsibility to data privacy and protection.

4.3.2 Ensuring Availability of Service and Resilience

Maintaining service availability and resilience by SOC is integral to the company's operations. The SOC continuously scans for threats that could cause issues to Grab's services, such as DDoS attacks, ransomware, and other kinds of cyber threats. By applying high-level threat detection methods and leveraging machine learning and artificial intelligence technology, the SOC can swiftly identify anomalous behaviour, which is indicative of an attack, allowing for a rapid response and maintaining smooth service delivery.

The SOC's real-time monitoring allows Grab to come up with defensive measures before an attack can cause considerable damages. For example, when a DDoS attack is detected, the SOC can quickly resort to blocking suspicious IP addresses, ensuring that essential services remain intact. This proactive defence procedure helps maintaining the resilience of Grab's services, leading it to provide continual service to its customers in the face of growing cyber threats.

4.3.3 Fostering Culture of Security Awareness

Since SOC aggregates data and communicates it to the organisation, it provides actionable intelligence and an understanding for further development of cybersecurity training and awareness initiatives. By analysing security incidents and identifying attack patterns, the SOC can contribute to highlighting existing threats and vulnerabilities that employees should be informed of. This information is then used to develop more specific training programs that prepares employees for recognising and countering possible cyber attacks.

Furthermore, the SOC helps enforce the security-by-design idea by working closely with developers to pinpoint and address security issues during the product development stage. By consolidating security considerations early in the design process, the SOC ensures that Grab's products and services are built from the ground up with strong security, reducing the risk of introducing vulnerabilities.

4.3.4 Building Trust and Transparency

The SOC can help in demonstrating the commitment in building trust and transparency with Grab's users and stakeholders. Since monitoring and reporting processes are involved, the SOC offers clarity into Grab's security posture and displays the company's adherence to user data privacy and protection. This transparency helps in building users' level of confidence that their data is safe, and Grab is taking all necessary measures to proper maintenance.

In addition, the SOC's role in dealing with security incidents follows Grab's commitment to operational transparency. In the event of a data breach, the SOC is responsible for coordinating the necessary actions, communicating with relevant parties, and providing comprehensive reporting on the incident and preventive measures. This degree of transparency not only promotes trust but also reinforces Grab's reputation as a company that places the security of its users' information as a priority.

4.4 Budget and Resource Allocation

To manage cyber security effectively, it requires a carefully planned allocation of financial and human resources to address the ever-evolving threat landscape. Grab must invest in both technology and personnel in order to protect its wide range of data assets and allow for operational continuity. However, having an accurate understanding of the needs of the organisation and its objectives is the first step before ensuring that the budgeting and resource allocation are done effectively (Consultia, 2024). Section 4.4.1 below discusses some of the essential steps to establish a foundation before employing a SOC according to the same source.

4.4.1 Foundational Steps to Employ SOC

i. Understand the objectives

Prioritising consumers' rights to data protection and privacy is one of the primary objectives of Grab as it handles a wide array of information, along with complying with legal standards such as the Personal Data Protection Act (PDPA) in Singapore and other laws concerning data protection in other countries where Grab operates. The objectives also extend beyond just data protection, which covers the wider financial impact on Grab, as cyber attacks can cause tremendous financial losses through legal fees, reputation damage, and loss of customers' trust. Therefore, achieving the said goals can be done through actions such as employing advanced encryption methods and strict access controls, as well as regular compliance check with legal standards.

ii. Identify key assets

Although there are many areas that need protection, Grab has to identify several assets that are heavily tied to maintaining its operation, such as:

- **Customer and partners data**: Basic users' information, payment history, and location data.
- **Core business systems**: Infrastructure that provides Grab's online functions such as ride-hailing, delivery, and digital payments.
- **Intellectual property**: This includes business strategies and software that offers a competitive advantage for Grab.

iii. Establish identifiable policies and procedures

After critical assets have been identified, policies and procedures must be established, which dictate how the assets are being allocated with the necessary resources. They include, but are not limited to:

- **Incident response plan**: This highlights the steps needed to be taken when an incident occurs.
- **Standard operating procedures**: They define the day-to-day SOC activities such as alert management, threat detection, log recording, and others.
- **Continuous monitoring, documentation, and improvements**: Utilising monitoring tools and conducting detailed documentation are necessary for review to make improvements to the SOC possible.

iv. Adopt a stage-oriented approach

Instead of employing the SOC within a single phase, spreading the process into several stages can be advantageous and potentially save costs on unnecessary adjustments.

- **Phase 1: Initial Setup**. This begins with fundamental components of a SOC such as a Security Information and Event Management (SIEM) tool and monitoring features.
- **Phase 2: Expansion**. More advanced features can be slowly added according to the identified needs as the SOC performs its duties, such as the integration with threat intelligence platforms, forensic tools, and automated response features.
- **Phase 3: Optimisation**. This phase focuses on refinements to the use of tools, as they can change due to development of attack vectors, which leads to shifting requirements.

Once the foundational steps have been understood, the organisation can then move on to budgeting process. The following underscores the important considerations for budget allocation as well as balancing the cost and effectiveness in Grab’s cyber security strategy, with the focus placed on the importance of prioritising investments that align with its security goals.

4.4.2 Strategic Allocation of Budget

Grab's cybersecurity budget must be in accordance with the broader business objectives and risk management concerns. Because of the complexity of the digital landscape, resource allocation must be strategic in nature, addressing current threats while also taking long-term resilience into consideration. Key areas of budget allocation are:

- **Technology Investments**: Major part of the budget specifically allocated for Grab's cybersecurity are dedicated to obtaining and maintaining security tools and technologies. This includes real-time monitoring systems such as SIEM, threat detection and response such as Intrusion Detection System (IDS) and Intrusion Prevention System (IPS), as well as data protection such as encryption protocols and access control. Investments in cloud security solutions are equally important as Grab continues to utilise cloud platforms to grow its services.
- **Staffing and Training**: Ample budget allocation for cyber security staffing is required for Grab's SOC to function according to the given purpose. This includes not only hiring cyber security professionals but also investing in regular training classes to keep the workforce informed on the latest developments (Warner, 2022). A workforce that is well-knowledgeable can adapt very well to competitive cybersecurity challenges.

4.4.3 SOC Cost Breakdown

According to Netsurion (n.d.), there are three levels of SOC cost breakdown:

- **Basic**: Provides the detection tools with limited investigation and no treat hunting capabilities that costs $1.5 million per year, including $300,000 for technology and $1.2 million for labour.
- **Intermediate**: This level has upgraded detection tool which includes SIEM and User and Entity Behaviour Analysis (UEBA), which costs $2.5 million annually, comprises of $400,000 for technology and $2.1 million for labour.
- **Advanced**: The advanced level offers automation, where AI is leveraged to manage vast amount of data and remove false positives to free up resources, as well as having threat hunting capabilities, which costs $5 million yearly, consists of $1.1 million for technology and $3.9 million for labour.

All in all, considering the size and the financial position of Grab, it would be best to opt for the advanced level of SOC as it does not compromise Grab's objectives, rather than having the other two options that do not align well with the company's commitment to cyber security.

4.4.4 Balancing Cost and Security Effectiveness

It is a responsibility of Grab to find the balance between the costs associated with cyber security investments and their associated effectiveness. Otherwise, this will introduce an alert fatigue, where there is an excess of technology in a SOC that overwhelms the operators due to the massive amount of security threats (Warner, 2022). This requires an approach to budget allocation based on risk evaluation, where resources are prioritised depending on the impact and likelihood of threats. There are two considerations that are available for Grab:

- **Leveraging Cost-Effective Solutions**: To maximise the impact of its cybersecurity spending, Grab explores cost-effective solutions such as cloud-based security services, open-source tools, and partnerships with external security firms. Managed Security Service Providers (MSSPs) can also be a good option since it offers thorough security coverage like other security tools would, but with lower initial costs (Consultia, 2024). Engaging through services such as bug bounty programs is also a cost-effective way of detecting and addressing vulnerabilities.
- **Continuous Evaluation and Adjustment**: Because of the continuously changing nature of cyber security threats, Grab's resource allocation strategy must include facilitating continuous post-incident assessment and adjustment. Regular reviews of budget effectiveness and the evolving threat landscape through key performance indicators (KPIs), feedback loops, and performance reviews, allow for adjustable resource reallocation to address risks and adopt new technologies (Consultia, 2024).

5.0 SOC Implementation Plan

To ensure the successful establishment of a SOC at Grab, a comprehensive implementation plan is essential. This plan outlines the critical steps required to build, deploy, and operate an effective SOC that aligns with Grab's security goals and business objectives. By covering both technical and strategic aspects, the SOC will enable Grab to monitor, detect, and respond to cybersecurity threats in real time, enhancing its security posture and supporting secure, resilient growth.

The subsections below outline the step-by-step process for implementing the SOC at Grab, starting with the development of a clear strategy, followed by designing the solution, developing processes and training, preparing the environment, and deploying relevant use cases. Ongoing efforts will focus on maintaining and enhancing the solution to ensure its long-term effectiveness. The implementation steps are based on the guidelines provided by SecureOps (2022) and Belmore (2024).

5.1 Develop Strategy

For Grab, the first step in implementing a SOC is to align the SOC's objectives with its overall business strategy (SecureOps, 2022). This involves identifying the critical systems and data that are essential to sustaining Grab's operations, such as its ride-hailing platform, payment systems, and customer data. By focusing the SOC on these key assets, Grab can ensure that the security measures put in place are aligned with its operational goals, reducing the risk of overlooking critical threats.

In addition, collaboration with key stakeholders, which includes the C-suite, IT, and executive management, is essential to ensure that the SOC strategy is aligned with Grab's overall business objectives (Belmore, 2024). By involving these stakeholders early, the strategy can be tailored to meet Grab's specific security and operational requirements, creating a solid foundation for the successful implementation of the SOC.

Another important step is to assess the company's unique security needs and identify any existing gaps (Belmore, 2024). This involves evaluating the current security infrastructure, considering factors such as budget constraints, available resources, and compliance with industry regulations. By gaining a clear understanding of the security challenges facing Grab, the SOC can be designed to effectively address these gaps and bolster protection for critical systems.

Additionally, an assessment of Grab's current SOC capabilities is necessary. This evaluation will help determine the readiness of its people, processes, and technology (SecureOps, 2022). Since Grab may be building its SOC from the ground up, it is recommended to initially focus on core functions such as monitoring, detection, response, and recovery. More advanced features like vulnerability management can be added as the SOC matures.

5.2 Design Solution

Designing the SOC solution for Grab requires starting with a focus on business-critical use cases, ensuring that the initial implementation addresses key operational needs while remaining scalable for future growth (SecureOps, 2022). By keeping the initial scope manageable, Grab can implement the SOC faster and achieve measurable results early on. According to SecureOps (2022), to design an effective SOC solution, the following steps can followed:

i. **Define Functional Requirements** – The first step is to outline the functional needs of the SOC, starting with identifying the sources of log and event data to be monitored, such as network traffic, user activity, application logs, and cloud services. Grab must also determine the sources of threat intelligence to inform proactive security measures. Additionally, defining performance requirements such as acceptable response times to security incidents, is essential to ensure the SOC meets the organisation’s operational needs.

ii. **Choose the SOC Model** – Next, Grab needs to select a SOC model that aligns with its operational and security objectives. This involves determining the level of coverage required (such as 24/7 monitoring) and whether certain roles, like incident responders and security analysts, will be handled internally or outsourced. By choosing the right balance between in-house and external resources, Grab can ensure both cost-efficiency and effectiveness in managing security threats.

iii. **Design the Technical Architecture** – The technical architecture of Grab's SOC should integrate seamlessly with the company's existing systems, including core applications, cloud platforms, and payment services. The SOC’s SIEM platform must be configured to aggregate and analyze data from these systems, providing a unified view of the security landscape. Additionally, workflows for event handling and incident response should be designed to fit within Grab's operational processes, ensuring a smooth transition from detection to resolution. Lastly, automation should be embedded where possible to improve detection accuracy and reduce response times, helping mitigate threats early in the attack lifecycle.

By following these steps, Grab's SOC solution will be tailored to meet current business needs while being flexible enough to scale as the company grows and faces evolving security challenges.

5.3 Develop Processes, Procedures, and Training

For SOC implementation, developing well-defined processes, procedures, and training programs is essential for effective operation (Belmore, 2024). This involves defining specific roles and responsibilities for SOC team members, setting up detailed protocols for handling incidents, and creating comprehensive documentation practices.

Effective processes will streamline how the SOC responds to threats and manages day-to-day operations (Belmore, 2024). This means having well-documented procedures for incident response and regular updates to reflect new challenges and best practices. For Grab's SOC, establishing well-defined processes and procedures is crucial for effective incident management and overall cybersecurity operations. According to Global CIO (2022), the four key processes to build a SOC are as follows:

i. **Event Classification and Triage** – The first step involves quickly classifying and triaging incoming security events. SOC analysts need to sift through a large volume of log data to identify significant indicators of compromise. This process helps in filtering out noise and focusing on critical events that require further investigation. For Grab, this means setting up a system where Tier 1 analysts can efficiently prioritise high-severity events and escalate them to more experienced analysts if needed.

ii. **Prioritisation and Analysis** – Once events are classified, prioritisation and analysis are essential. SOC analysts must assess which threats pose the most risk to Grab's business operations. This involves determining the impact of an event based on the criticality of affected assets. Analysts should focus on potential intrusions and actions that could harm Grab's operations, such as unauthorised network communications or malware infections.

iii. **Remediation and Recovery** – Prompt remediation is key to limiting damage from security incidents. Grab's SOC should have clear procedures for addressing and recovering from attacks, which may include re-imaging systems, applying patches, and adjusting access controls. Clear communication with management is vital, and

SOC analysts should coordinate with other IT teams as needed to execute remediation steps effectively.

iv. **Assessment and Audit** – Regular assessments and audits help identify and address vulnerabilities before they can be exploited. Grab's SOC should conduct periodic vulnerability scans and reviews of their security practices. This process includes generating compliance reports and evaluating SOC performance to ensure continuous improvement and adherence to security policies.

Furthermore, ensuring that SOC staff are up-to-date with the latest cybersecurity skills and knowledge helps them stay ahead of emerging threats and enhances the overall effectiveness of the SOC (Belmore, 2024). For Grab's SOC, developing comprehensive training programs is crucial for optimizing the effectiveness of the SOC team and ensuring robust cybersecurity practices throughout the organization (Knerler et al., 2022). The training programs can be categorised as below:

i. **Internal Training and Education** – Focuses on enhancing the skills of SOC analysts by providing targeted training in SOC operations. This training should cover key areas such as incident response, threat analysis, and the use of SOC tools and technologies. By continuously developing their proficiency, SOC analysts will be better equipped to handle evolving security challenges.

ii. **External Training and Education** – Aims to improve the cybersecurity awareness of Grab's wider team. This involves delivering educational programs to employees on various cybersecurity topics, ensuring they understand their role in maintaining a secure environment and can recognize potential threats.

iii. **Exercises** – Essential for testing and improving SOC readiness. Conducting scenario-based simulations, such as mock critical incidents, helps the SOC team practice their response strategies and refine their procedures. These exercises are valuable for identifying gaps and ensuring that the team can handle real-world situations effectively.

5.4 Prepare Environment

It is essential to prepare a suitable environment before deploying the SOC at Grab to ensure the environment is secure, scalable and ready for operations (SecureOps, 2022). Some key elements in the environment preparation phase includes:

i. **Device Security** – Each device used by Grab's SOC team members such as a workstation, laptop or mobile device must be fully secured (SecureOps, 2022). This can be achieved by installing antivirus software, encryption and endpoint protection. This step ensures that the security team is working in a secure environment.

ii. **Access Management and Authentication** – It is crucial to manage the access controls to SOC tools and data (Belmore, 2024; SecureOps, 2022). Enforcing the principle of least privilege as well as implementing multi-factor authentication (MFA) and role-based access controls (RBAC) can ensure that only authorised individuals can access to sensitive systems and data, preventing insider threats or privilege escalation techniques by threat actors.

iii. **Network Segmentation** – According to Belmore (2024), segmenting networks into smaller, isolated sections can help to contain potential breaches. This ensures that attackers cannot easily move laterally across other segments even after compromising one part of the network. Additionally, network segmentation also makes it easier for analysts to monitor and control traffic within the SOC.

iv. **Infrastructure Requirements** – Adequate infrastructure is vital to support SOC operations at Grab (Belmore, 2024). SOCs require sufficient bandwidth to handle the large volumes of data generated by monitoring, logging and alerting systems. Additionally, sufficient storage capacity is also needed for retaining logs and other security-related data which is essential for digital investigations as well as compliance rules. Implementing redundancy with failover mechanisms is also important to ensure the SOC operations can continue even during hardware failure or network issues.

v. **Scalability** – The SOC infrastructure must also be scalable to accommodate future growth in terms of data, tools and human resources (Belmore, 2024). In the continuous advancement of technology in the cybersecurity landscape, it is important to leverage these new technologies to keep up with new emerging threats. In addition to that, SOC operations may expand in size as the Grab's business continue to grow. Hence, Grab's SOC environment must be designed with scalability in mind to ensure it can grow and enhance without the need for any design overhaul.

Preparing a suitable environment for Grab's SOC is a foundational step that ensures all components are secure, properly segmented and equipped with adequate resources to support the SOC operations. This preparation step helps to mitigate potential risks and ensure the SOC at Grab is ready to handle its responsibilities of detecting, responding and mitigating cyber threats effectively.

5.5 Implement Solution

The next phase involves implementing the initial SOC deployment at Grab by setting up its key infrastructure (SecureOps, 2022). There are several key components in the initial implementation plan which includes:

i. **Log Management Infrastructure** – A robust log management structure involves deploying a SIEM system that collects and processes logs from the organisation's data sources, such as firewalls, IDS/IPS systems, and endpoint devices (Belmore, 2024). A SIEM provides centralised log management and real-time analysis of security incidents, enabling effective anomaly detection and incident response. As the foundation of an effective SOC, the SIEM system must be well-suited to the organisation's infrastructure and properly configured to ensure it is able to collect and correlate relevant events and detect threats effectively with minimal false positives (Knerler et al., 2022).

ii. **Integrate the Essential Set of Key Data Sources** – After Grab's SOC is operational, it is essential to integrate the essential collection of key data sources (SecureOps, 2022). These data sources often include network traffic logs from firewalls and IDS/IPS systems, endpoint detection logs from antivirus tools, threat intelligence including those from internal and external feeds, as well as authentication logs from Active Directory, VPNs and SSO systems. By focusing on these critical sources, the SOC at Grab can start to identify potential threat patterns across multiple points within their system infrastructure.

iii. **Enable Security Analytics and Automation Features** – To maximise the efficiency of threat detection and response, the SOC should enable security analytics and automation capabilities within their SIEM (SecureOps, 2022). Security analytics can help to provide more in-depth insights into anomalies by correlating data across different sources, applying machine learning models and generating actionable intelligence (Knerler et al., 2022). Analytics is commonly paired with automation tools such as the Security Orchestration, Automation, and Response (SOAR) system, which helps to automate incident response workflows. By automating tasks such as alert prioritisation, incident analysis and incident response actions, response time can be reduced and SOC analysts are free to focus on more critical tasks.

iv. **Integrate Threat Intelligence Feeds** – Finally, the SOC can integrate threat intelligence feeds to enhance detection accuracy (SecureOps, 2022). Cyber threat intelligence (CTI) can include useful information such as malicious IP addresses, suspicious DNS, signatures of specific malware families, as well as adversary tactics, techniques and procedures (TTPs) from the MITRE ATT&CK framework (Knerler et al., 2022). These information helps to enhance the SOC by shifting focus from individual incidents to adversary behaviour. By integrating CTI, SOCs can refine their detection tools, better prioritise resources and anticipate threats. Hence, CTI enables SOCs to shift from a reactive to proactive defence, enhancing their ability to predict and prevent sophisticated attacks and reduce costs over time.

5.6 Deploy End-to-End Use Cases

Deploying end-to-end use cases involves integrating and operationalising the SOC solutions that have been previously set up (SecureOps, 2022). This phase is crucial to turn the theoretical capabilities of the SOC at Grab into practical, actionable measures that address specific threats. After deploying the fundamental components of the SOC, the team can start implementing specific use cases across various tiers, which are the analytics, security automation and orchestration tiers.

i. **Analytics Tier** – The next step of implementation involves defining use cases aimed at detecting potential threats such as compromised credentials and spear phishing (SecureOps, 2022). These use cases leverage analytics tools such as SIEM systems to identify suspicious indicators. For instance, behavioural analytics can be used to detect compromised credentials through anomalies like unusual login patterns and access from unusual locations at odd hours. Spear phishing emails can also be identified through phishing-specific signatures, reputation-based checks and URL analysis.

ii. **Security Automation Tier** – Automating responses to common threats help reduce manual effort needed to address these threats. In addition, automation also ensure threats are handled quickly and consistently, reducing response times. Belmore (2024) recommends SOCs to start their automation use case with the phishing triage due to the high volume and low complexity of phishing email attacks. Additionally, Endpoint Detection and Response (EDR) triage is another automation use case which can help Grab's SOC teams to research alerts and execute endpoint actions more efficiently.

iii. **Orchestration Tier** – Security orchestration involves integrating various security tools and workflows to create an efficient incident response process (SecureOps, 2022). This focuses on coordinating the actions of different security tools such as SIEMs, threat intelligence platforms and EDR solutions. An example of use case in this tier is the SIEM triage, which involves integrating SIEM alerts with orchestration platforms to centralise information, reduce false positives, and streamline the response to high-priority alerts (Belmore, 2024). Another use case in the orchestration tier is the incident response, where SOC playbooks can be utilised to automate predefined responses to incidents such as malware detection and unauthorised access, ensuring a timely containment of threats.

5.7 Maintain and Enhance Solution

Lastly, it is critical to maintain and enhance the Grab's SOC to ensure it remains effective over time against new threats and technologies (SecureOps, 2022). This ensures the SOC stays adaptive and responsive to both internal organisational changes and the external cybersecurity landscape. According to Belmore (2024), these include:

i. Ongoing Maintenance

- **Configuration Updates** – This involves fine-tuning detection rules in the SIEM or updating the logic in automation workflows, which is essential for improving detection accuracy and minimising false positives.
- **Patch Management** – It is crucial to keep both hardware and software components of an SOC up to date to address any potential vulnerabilities that can be exploited by malicious threat actors.
- **Vulnerability Management Program** – A proactive vulnerability management program can help identify and mitigate potential weaknesses in the SOC before they can be exploited by threat actors. This can include regular vulnerability scans and penetration testing.

ii. Performance Assessments

- **Regular Reviews** – SOC performance should be continuously evaluated to identify any vulnerabilities or inefficiencies. For instance, reviews can include the SOC's ability to handle high volume of alerts, the effectivity of automated responses, and the accuracy of detection mechanisms.
- **Address Performance Gaps** – After reviewing the SOC's performance, any gaps in speed, accuracy or coverage should be promptly addressed. This can involve adjusting alert thresholds, refining playbooks or reallocating resources.

iii. Monitor Emerging Threats and Trends

- **Adapting to New Threats** – As cyber threats are evolving constantly, the SOC must be able to adapt by incorporating new strategies and tools. Continuous threat monitoring is crucial to anticipate and defend against new emerging risks.
- **Leveraging New Technologies** – To keep up with the advancement of cybersecurity technology, organisations can look into technologies such as artificial intelligence, machine learning and cloud-based SOC services. This can enhance the SOC's capabilities and efficiency by helping to streamline workflows, improve threat detection and reduce analyst fatigue.

iv. Training and Skill Development

- **Regular training** – it is vital to ensure that the SOC team are updated with the latest tools, technologies and threats. The training should focus on new technologies including automation, artificial intelligence and threat intelligence analysis. Investing in training will help the SOC maintain a high level of expertise and readiness.

v. Compliance and Governance

- **Regulatory Compliance** – As regulations evolve, it is important to ensure that the SOC remains compliant with the industry standard such as the Personal Data Protection Act 2010 (PDPA), Financial Services Act 2013, and the Anti-Money Laundering and Counter Financing of Terrorism (AML/CTF), International Organisation for Standardisation (ISO) as well as other local and international regulations (Grab, 2016; Lee, n.d.).

- **Security Audits** – Regular security audits can help to maintain compliance and ensure that the SOC follows industry best practices. Security audits also provide an opportunity to assess the effectiveness of the organisation's security posture and make any necessary changes or adjustments.

Hence, it is important to continuously maintain and enhance the SOC at Grab to ensure that it stays ahead of cyber threats, adapt to technological advancements and maintain compliance with regulations. Through prioritising regular maintenance and continuous improvements, Grab can remain resilient in the ever-evolving cybersecurity landscape.

6.0 Conclusion

In conclusion, the implementation of an SOC at Grab is critical to strengthen the company's security posture and resilience, ensuring the safety and privacy of its customer base and maintaining business operations regardless of any security incidents. Given the evolving cyber threats in the digital landscape, the establishment of an SOC will allow the company to effectively detect, respond and mitigate any potential cyber threats. By integrating advanced analytics and monitoring tools, threat intelligence as well as automation features, Grab's SOC will enhance its ability to protect sensitive data, reduce downtime caused by security incidents and ensure compliance with regional and global cybersecurity and data protection regulations. In addition to that, the SOC implementation by Grab will play a pivotal part in fostering a culture of cybersecurity awareness within the company, ensuring that both employees and users are aligned with the best practices of data protection. The strategic investment in the resources of Grab's SOC and continuous training will further enhance the organisation's adaptability to new and emerging threats.

Ultimately, the successful implementation of the SOC by Grab will both safeguard the company's digital infrastructure and reinforce their customer trust, supporting the company's long-term business goals and reputation in increasingly competitive digital market.

7.0 References

Belmore, M. (2024, March 19). *How to build a modern security operations center (SOC)*. Swimlane. Retrieved from https://swimlane.com/blog/building-modern-soc-2/

Brush, K. (n.d.). *Cybercrime*. TechTarget. Retrieved from https://www.techtarget.com/searchsecurity/definition/cybercrime

Chipeta, C. (2023, November 14). *What is the Cyber threat Landscape*. UpGuard. Retrieved from https://www.upguard.com/blog/cyber-threat-landscape

Consultia. (2024, July 2). *How to build a security operations center on a budget*. Retrieved from https://www.consultia.co/how-to-build-a-security-operations-center-on-a-budget/

Cybersecurity and Infrastructure Security Agency. (n.d.). *Defining insider threats*. CISA. Retrieved from https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats

Cybersecurity and Infrastructure Security Agency. (2021, February 1). *Understanding denial of service attacks*. CISA. Retrieved from https://www.cisa.gov/news-events/news/understanding-denial-service-attacks

Deorwine Infotech. (2022, April 26). *Key features of Grab that secured $200M funding*. Retrieved from https://deorwine.com/blog/key-features-of-grab-that-secured-200m-funding/

Global CIO. (n.d.). *How to build a Security Operations Center (on a budget)*. Retrieved from https://globalcio.com/upload/main/ac6/g4d87a6d2geaqgu9fv91sysvb75uuldc/How-to-built-SOC.pdf

Grab. (2016). *Grab awarded ride-hailing industry's first ISO certification.* Retrieved from https://www.grab.com/sg/press/social-impact-safety/grab-awarded-ride-hailing-industrys-first-iso-certification/

Grab. (n.d.). *Grab. The everyday everything app*. Retrieved from https://www.grab.com/sg/

Grab. (n.d.). *Our guiding principles*. Retrieved from https://www.grab.com/my/about/our-principles/

Grab. (n.d.). *Trust and safety*. Retrieved from https://www.grab.com/sg/about/trust-and-safety/

Grab Holdings Limited. (2024). *Grab annual report 2023*. Grab. Retrieved from https://investors.grab.com/static-files/89efbb6b-531f-4fef-a953-2d7e8c19c93f

IBM. (n.d.). *What is social engineering?* IBM. Retrieved from https://www.ibm.com/topics/social-engineering

Knerler, K. , Parker, I., Zimmerman, C. (2022). *11 strategies of a world-class cybersecurity operations center.* The MITRE Corporation.

Kosinski, M. (2024, May 17). *Phishing*. IBM. Retrieved from https://www.ibm.com/topics/phishing

Kosinski, M. (2024, June 4). *What is ransomware?* IBM. Retrieved from https://www.ibm.com/topics/phishing

Lee. S. (n.d.). *E-wallet laws and regulations in Malaysia: Here's what you need to know.* Retrieved from https://ewhallet.com/blog/post/e-wallet-laws-and-regulations-in-malaysia

Marwan, S. (2023, March 2). *Most innovative companies in Asia-Pacific 2023*. Fast Company. Retrieved from https://www.fastcompany.com/90846729/most-innovative-companies-asia-pacific-2023

Microsoft. (n.d.). *What is a security operations center (SOC)?* Retrieved from https://www.microsoft.com/en-us/security/business/security-101/what-is-a-security-operations-center-soc

National Cyber Security Centre. (2024, February 12). *Understanding vulnerabilities*. NCSC. Retrieved from https://www.ncsc.gov.uk/collection/vulnerability-management/understanding-vulnerabilities

Netsurion. (n.d.). *The true cost of setting up and operating a security operations center*. Retrieved from https://www.netsurion.com/articles/true-cost-of-setting-up-and-operating-security-operations-center

Philip, S. (2014, June 10). *Harvard inspires man to ditch family riches for taxis*. Bloomberg. Retrieved from https://web.archive.org/web/20180101220915/https://www.smu.edu.sg/sites/default/files/smu/news_room/smu_in_the_news/2014/sources/june11/Bloomberg_20140610_1.pdf

Putman, P. (n.d.). *Hacktivist*. U.S. Cybersecurity Magazine. Retrieved from https://www.uscybersecurity.net/hacktivist/

SecureOps. (2022, September 9). *7 steps to building a security operations center*. Retrieved from https://secureops.com/blog/building-a-soc/

Scapicchio, M., Downie, A., Finio, M. (2024, March 15). *What is a SOC?* IBM. Retrieved from https://www.ibm.com/topics/security-operations-center

Tan, A. (2018, May 24). *Grab outlines its approach to cyber security*. Computer Weekly. Retrieved from https://www.computerweekly.com/news/252441824/Grab-outlines-its-approach-to-cyber-security

Trellix. (n.d.). *What is a security operations center?*. Retrieved from https://www.trellix.com/security-awareness/operations/what-is-soc/

Wong, L. (2020, September 18). *Grab fined $10,000 for fourth data privacy breach in two years*. The Straits Times. Retrieved from https://www.straitstimes.com/tech/grab-fined-10000-for-fourth-data-privacy-breach-in-two-years

Workat Tech. (n.d.). *Grab overview (about, mission, vision, values, principles)*. Retrieved from https://workat.tech/company/grab

YourShortlist. (2024, July 17). *The importance of the CIA triad to cybersecurity*. YourShortlist. Retrieved from https://yourshortlist.com/the-importance-of-the-cia-triad-to-cybersecurity/