CSEC5615 Assignment 2 Group Report

CSEC5615 Cloud Security S1,2024

Group member:

Ziyuan Jing 480153157
Yuanchen Shi 540451168
Weiran Wang 540421677
Xijiu Wang 500437485
Ilce Andrea Aquino 530594664
Fengquan Jiang 540784103

Table of Content

Introduction

This report sets out to thoroughly examine key aspects of application and container security, policies for managing vulnerabilities, regulatory requirements, and procedures for responding to incidents. Crafted to enhance cyber defence capabilities and reduce the likelihood of data breaches and malicious attacks, the recommendations in this report are customised to suit the particular requirements of a mid-sized financial institution serving a varied international clientele.

1 . Application Security

Migrating applications to the cloud presents significant advantages, including enhanced scalability, availability, and cost reduction for the organization (What Is Application Migration? | Microsoft Azure, n.d.). However, to ensure a successful migration, it is essential to consider several factors and adopt the best strategies. Security must be meticulously integrated throughout every phase, from the planning and design stages of cloud migration assets to deployment and maintenance (ISO/IEC 27041-1:2011), particularly in sectors such as the financial industry.

In terms of software assets, ensuring secure applications is critical for any organization to uphold the principles of confidentiality, integrity, and availability, as these applications manage, process, and generate data relevant for the business. Additionally, compliance with regulations regarding the handling and use of sensitive information is crucial due to the inherent risks associated with such data and the specific nature of the organization's operation.

Furthermore, applications are susceptible to deliberate or inadvertent actions that may result in the loss and alteration of critical business data, potentially damaging the organization's reputation. Notably, recent years have witnessed a heightened prevalence of cyberattacks, particularly targeting the financial sector. For instance, in Australia, the Finance sector ranked second in reporting the highest number of data breaches in 2023 (OAIC, 2024). Nevertheless, amidst escalating security concerns linked to cloud migration, prioritizing security measures at each stage of the migration process and adhering to established best practices are essential. Through meticulous planning, businesses can ensure a secure transition to the cloud (Cloud Migration Security, n.d.)

Analyzing our client's scenario, the company operates a set of in-house critical applications for managing financial and customer transactions, supported by a well-established development team. The client's IT Department, comprising 75 IT specialists, is responsible for developing and maintaining custom applications used within the institution, supporting business operability. Ensuring the security of these applications is vital to protect against vulnerabilities and unauthorized access to critical financial data.

Given the critical nature of these applications, the cloud model proposed to the client (IaaS) where the cloud customer is responsible for its application, the Cloud architecture environment (Cloud On-premise architecture), and ensuring security and integrity of these applications during the Cloud-Secure Software Development Life Cycle (SDLC), we propose the following strategies and recommendation adapted to our client’s operation in

compliance with finance sector regulation and best practices (Guidelines for Software Development | Cyber.gov.au, 2023):

First, we are aboard to adopt comprehensive application security testing methodologies to identify vulnerabilities. This includes non-functional security test using Dynamic Application Security Testing (DAST) to assess the security of running applications, Static Application Security Testing (SAST) to analyze source code for potential vulnerabilities, and Software Composition Analysis (SCA) to evaluate third-party and open-source components used by the company's software assets in order to detect known security issues.

Secondly, we recommend three secure coding practices to minimize the risk of application-level attacks: ensuring input validation and sanitization to prevent attacks like SQL injection or cross-site scripting, implementing robust authentication and authorization mechanisms to control access, and adhering to secure error handling and logging practices to prevent sensitive information exposure and ensure comprehensive monitoring.

Moreover, we further describe encryption industry-standards methods for data at rest and in transit to maintain data confidentiality and integrity of the sensitive information such as customer financial transactions, employees PII, business sensitive data, etc. that the company handles and store (CHAPTER 3: Secure Design - Alice and Bob Learn Application Security [Book], n.d.).

Finally, we highlight three key considerations when migrating applications to the cloud. These include addressing integration challenges with existing systems to ensure seamless functionality, managing third-party dependencies to avoid introducing vulnerabilities.

1.a. Application security testing methodologies recommendations

a. Static Application Security Testing (SAST)

This testing method involves analyzing the source application code before compilation, providing a detailed view to identify potential vulnerabilities and code flaws early in the development process (Li, 2020). Additionally, its ability to promptly address and resolve issues makes it ideal for integration into the software development lifecycle (SDLC) (Li, 2020). This allows programmers to detect, identify, and fix problematic code lines that could cause application anomalies, secrecy disclosure and other security risks, ultimately saving time, effort, and resources that might otherwise be spent on addressing security incidents (The Top 10 Static Application Security Testing (SAST) Tools, 2023).

In our client's context, which develop custom application with crucial operation like online banking for its clients, dealing with sensitive information, Static Application Security Testing (SAST) is an important technique for identifying critical code issues that could be exploited by malicious actors to gain access to these sensitive data within the client's organization. For example, a common vulnerability like SQL injection exploits a weakness in the input data from a web application client to the database by injecting a modified SQL query (OWASP, 2024), thereby compromising the confidentiality of sensitive information such as the client's bank account details. By employing SAST during the design phase, IT developers can prevent

security vulnerabilities from reaching production, ensuring the safety of the user's financial information and integrity in each transaction made in any of its financial applications.

In SAST testing, tools play a critical role in the overall security program. They can simplify and speed up the security process by assisting security teams in their tasks (WSTG - Stable | OWASP Foundation, n.d.). To select the appropriate SAST tool, consideration must be given to the integration with the development platform and the programming languages used by the IT development team in the organization. Since this information is not specified, we list two of the most used tools recommended by The Open Web Application Security Project (OWASP, 2021):

- SonarQube:

SonarQube is an open-source platform for continuous inspection of code quality, focusing on detecting bugs, vulnerabilities, and code smells across multiple programming languages. It offers integration with popular CI/CD tools, enabling automated code analysis throughout the development pipeline. SonarQube provides detailed reports and visualizations of code quality metrics, helping teams identify and prioritize improvements. SonarQube also addresses technical debt and enhances security by highlighting vulnerabilities based on recognized standards (SAST Testing, Code Security & Analysis Tools | SonarQube, n.d.).

- Checkmarx SAST:

Is an SAST solution that is engineered to detect and resolve software vulnerabilities in the early stages of the development process. Through sophisticated static analysis methodologies, it scrutinizes source code and binaries to uncover security weaknesses and ensure compliance across diverse programming languages. Checkmarx SAST boasts extensive coverage of proprietary, open-source, and third-party components, equipping developers with actionable insights to promptly rectify security lapses. With seamless integration into popular CI/CD pipelines and development environments (Checkmarx, 2024).

b. Dynamic Application Security Testing (DAST)

This type of test, well-known as black box test or web application test, consists of detecting security vulnerabilities by emulating external attacks on an application in real-time. This involves examining the application and APIs as they are running from an external perspective, probing its exposed interfaces for potential vulnerabilities (Mohan, n.d.).

Incorporating DAST throughout the software development life cycle allows teams to detect vulnerabilities before their applications reach production. DAST serves as a fundamental element of software security and should complement other practices like SAST, to ensure a thorough security evaluation of the applications.

DAST test is recommended to ensure security for critical finance operation, helping the IT development team in our client to identify vulnerabilities on its financial custom application in runtime mode using a test environment. To illustrate this concept, due to DAST test applied to a digital wallet for a financial organization in India, it was detected 5 vulnerabilities, included one in a Payment process that exposed a Json payload used during the payment transaction that could lead attacks like MITM to modify the payload or extract

sensitive information (“Security Assessment for Digital Wallet Payment Partner Applications Using the OWASP Method: A Case Study in Indonesia,” 2024).

To finalize DAST section, two of the list most used tools recommended by The Open Web Application Security Project (OWASP, 2021):

- Burp Suite:
  Is a dynamic application security testing (DAST) component designed to assess web application security by simulating real-world attacks while the application is running. It offers dynamic analysis capabilities, automatically scanning for a wide range of vulnerabilities such as SQL injection, Cross-Site Scripting (XSS), and authentication issues. It allows for customizable testing, enabling users to focus on specific parts of the application and configure scan policies according to their needs. The tool generates detailed reports summarizing the findings of the security scans, making it a valuable asset for security professionals and penetration testers seeking to identify and remediate vulnerabilities in web applications (*Introducing DAST Scanning in the Cloud, with Burp Suite Enterprise Edition*, 2024).

- OWASP ZAP:

  It assesses web application security by intercepting and analyzing HTTP/HTTPS traffic, identifying vulnerabilities like SQL injection and Cross-Site Scripting (XSS). ZAP offers automated scanning and interactive testing capabilities, along with detailed reporting and seamless integration with existing development workflows, providing a comprehensive solution for improving web application security making ideal for our financial client security testing’s need (*OWASP ZAP – Getting Started*, n.d.)

  c. Software Composition Analysis (SCA)

  Software Composition Analysis (SCA) is a set of techniques for identifying vulnerabilities in an application’s third-party dependencies, particularly in open-source libraries and, when combined with SAST, helps uncover static application code vulnerabilities (Mohan, n.d.-b).

  SCA tools offer significant value by providing feedback during development and integrating in the Continuous Integration process for every commit. These tools primarily examine open-source dependencies rather than the custom code, automatically identifying components and versions used, and cross-referencing them against known vulnerabilities. Additionally, the tools manage open-source licenses to avoid unfavorable licensing issues (Dotson, n.d.).

  It is highly recommended for the IT development team to include at least two SCA tools in its SDLC to analyze its software’s dependency such as third-party libraries, external APIs that interact with the in-house application to ensure those dependencies do not present a risk. An example on how it works a scan tool is presented by Mohan (n.d.-c) where it was used OWASP Dependency-Check on a Web Project example, and the tool reported a vulnerability on an external jquery library that could lead to a Cross-site scripting attack.

1.b Security coding practices at application-level proposed

Implementing secure coding practices such as **input validation and sanitization**, **strong authentication and authorization**, and proper **error handling and logging** can significantly reduce the risk of application-level attacks. These practices help ensure that applications are robust, secure, and capable of defending against common threats

a. **Input Validation and Sanitization**: is a process to analyze that entries input is secure and it will not threaten the application or its data.

   Implementing strict input validation and sanitization will protect your systems from manipulation and enhance the overall security of the financial application.

   Input validation and sanitization are crucial for securing APIs, application, queries, etc and preventing various attacks, such as SQL injection (SQLi). Always must be validated and sanitized data sent to client's APIs to ensure that user inputs do not contain malicious scripts. For instance, when users submit comments through an online feedback form, the system should check these entries to ensure they don't contain harmful scripts that could compromise the the banking website

b. **Strong authentication and authorization:** A strong policy must be placed to guarantee that only authorized users, entities are accessing the financial resources and data and give only essential access to perform their corresponding task (Zero Trust). Enhancing authentication and authorization mechanisms is crucial to minimize the risks of repudiation, information disclosure, and elevation of privilege. Implement strong, multi factor authentication (MFA) for all users and use role-based access control (RBAC) to ensure users have appropriate permissions. Log all access attempts and actions to provide an audit trail, aiding in repudiation protection. Regularly review and update access controls and permissions to maintain robust security (Shrivastava & Srivastav, n.d.).

c. **Error handling and logging:** Ensuring proper error handling is essential for creating high-quality software systems and enhances the resilience of our systems against attacks. Logging serves multiple purposes, not only aiding in debugging but also assisting in the investigation of security incidents and events (Error Handling and Logging Checklist, n.d.).

   For error handling, we recommend to avoid exposure of sensitive information when an error displays such as username, account number, email address to avoid potential data phishing. Security-related errors (login fails, access control failures.

   For log handling, server-side input validation failures) should issue a system alert. Systems log does not have to contain sensitive data, it must be registered any login attempts. All logs must register a timestamp, event id and the entity/module which triggered the event, the outcome and any individual who was involved in it.

Integrating STRIDE into Secure Coding Practices

Threat modeling is a structured approach for application design in order to identify, analise and address the security risk associated with the software and take countermeasures and corresponding mitigation.

We encourage the IT department to adopt a tread modeling and specifically we recommend STRIDE, a Microsoft threat modeling tool which categorizes and approaches different types of threats and simplifies the overall security conversations (Microsoft, 2022).

1.c Encryption

Encryption is a mathematical two-ways process to make the information not readable, ensuring that only authorized people can disclose the encrypted data using a key.
Encryption safeguards the security of routine digital transactions, including online banking and shopping.
To assure confidentiality, this technique is used on data transmission and at rest.
Regarding our financial client, encryption is a priority to be in compliance with local regulators such as the Australian Privacy Act (Federal Register of Legislation, 2022) This encompasses the use of encryption as a means to secure personal financial data. Also Payment Card Industry Data Security Standard (PCI DSS), financial institutions handling payment card information, compliance with PCI DSS is mandatory. This standard explicitly requires the encryption of cardholder data during transmission and storage to protect against data breaches.

a. Data encryption at rest: as we aboard in previous Section (Network security), we highly recommend the use of the latest TLS protocol. TLS offers three security measures in one solution. It involves a server generating a key pair (a public and private key) and obtaining a certificate authority's signature for the public key (Dotson, n.d.-b). Also the use of key Management such as Azure key Vault is highly recommended to the IT financial team to manage public, private keys.

In case of payment transaction or credit card processes we highly recommend mutual TLS, where client certificate validation is necessary (ensuring mutual authentication), services without client authentication might be suitable for public-facing applications but are inadequate for the transaction that requires extreme confidentiality. Mutual authentication is essential for security protocols adhering to the zero trust model (Rais et al., n.d.-b).

b. Data encryption in transit: Applying encryption to data at rest (storage data) in for example, the online banking system, can significantly enhance security by adding an extra layer of protection against unauthorized access. Implementing full disk encryption is crucial, as it offers more comprehensive protection compared to file-based encryption. By

using full disk encryption, all data stored on the disk is encrypted, minimizing the risk of data breaches. When choosing cryptographic solutions, must be considered the sensitivity of the data to ensure the appropriate level of assurance, the recommended one is symmetric AES-256 at least (Australian Signals Directorate, 2023)

1.d. Key considerations for cloud applications migration

a. Integration Challenges

One of the challenges that the organisation may face is the way its on premises applications will migrate to the cloud and how. Evaluation must be held to ensure a smooth migration without compromising Confidentiality Availability and Integrity of the organisation's information. Many custom-built applications will move to the cloud without modification, others will require reengineering of some kind, and some will need to be scrapped and rebuilt from scratch. To determine the appropriate steps for each application factors such as cost-effective rebuilding, awareness about the new technology for programming, architecture of the current application, level of critical operation, integration with Azure environment cloud and more (5. Refactoring, Redesigning, and Rebuilding Applications - Migrating Applications to the Cloud [Book], n.d.)

b. Third-party dependencies

Modern applications heavily rely on third-party dependencies, comprising 20–40 percent of the codebase (Janca, n.d.). These dependencies inherently introduce risks, as the application inherits the vulnerabilities present in the utilized code (Janca, n.d.). To mitigate these risks, it's recommended to use two different scanning tools(as we previously recommended on SCA tools). Regular scanning of code repositories, ideally daily or weekly, and before each production release is crucial to catch new vulnerabilities and updates in third-party components (Janca, n.d.-b). Integration of scanning into the CI/CD pipeline helps prevent the inadvertent inclusion of harmful code (Janca, n.d.-b). The IT financial development team must be aware of the risks associated with new technologies and the use of third party dependencies and propose alternative solutions . This proactive approach, though challenging, is more likely to yield positive outcomes by addressing risks and offering constructive alternatives(Janca, n.d.-b).

c . Migration complexity:

It could represent a challenge to migrate the entire on premises infrastructure to Azure Cloud due to its complexity. Cloud offers new resources that if not appropriate configure may lead to cost or security risk. Addressing these migration complexities requires careful planning, stakeholder collaboration, and expertise in cloud technologies and migration strategies. Engaging with experienced cloud migration consultants or service providers can help financial institutions navigate these challenges and ensure a successful transition to the cloud.

2. Container Security

A. Container isolation mechanisms to prevent unauthorized access and data leakage.

Container isolation refers to the practice of limiting interactions and communications between different containers within a containerized environment, such as Docker or Kubernetes (Irvine et al., 2017). Containerization, on the other hand, is a virtualization technique that allows computer applications along with the dependancies to consistently operate across various environments. Commonly, the containers usually consist of the application or app, runtime components and any libraries which nowadays facilitates scalability. Below are three key mechanisms discussed that are instrumental in preventing unauthorized access and data leakage.

1. Namespaces

Namespaces are a feature of the Linux Kernel that partitions kernel resources such that one set of processes sees one set of resources, while another set of processes sees a different set of resources. There are various types of namespaces each serving a different need and purpose;

PID Namespace: This namespace encapsulates the process IDs and thus makes processes in one container inaccessible to other processes in different containers, not to mention processes in the host system. This avoids conflicts with the process ID and boosts the process security isolation through distinct process address spaces.

NET Namespace: Network namespaces mean that each container is provided with its own network identities, including network interfaces as well as IP addresses, routing table as well as a firewall. This isolation helps in establishing virtual networks within the host system thus making virtual networking a reality. Usually, in Kubernetes namespaces give developers a way of isolating API resources and other clusters. For example, through definition of network policies, developers can control communication across namespaces which generally act as virtual firewalls. All these help to ensure stringent security meaures, prevent unauthorized access and also maintain flexibility within the microservice architecture.

IPC Namespace: IPC namespaces include inter-process communication resources, and system IPC objects/POSIX message queues, and do not allow these resources to be seen in other containers.

MNT Namespace: The mount namespaces enable each container to have a user-directed path for the file systems hierarchy; making the file system mounts in one namespace to unseen in others.

UTS Namespace: As the name suggests, it enumerates system identifiers like hostname and domain names for containers enabling them to have unique hostnames and domains.

USER Namespace: It is a mechanism for the isolation of the user and the group IDs; hence, every container is free to map the user IDs in the container to different IDs on the host, which further helps in matters concerning security and permission on the containers.

2. Control Groups (cgroups)

The *control groups*, abbreviated as *cgroups* in this guide, are a Linux kernel feature that allows you to allocate resources — such as CPU time, system memory, network bandwidth, or combinations of these resources — among hierarchically ordered groups of processes running on a system (Casalicchio & Iannucci, 2020).

Consequently, usage of cgroups includes restriction of resources and allocations per container. For instance, the amount of CPU or memory required to be allocated for use by a certain container can be set to a limit below which a container can by no means go, this would help to avoid the occurrence of DoS conditions. Resource accounting makes it possible to check the utilization of the resources appropriately by containers, which is beneficial in monitoring their performances and security measures taken against improper utilization of those resources.

The advantages derived from the use of cgroups remain impressive. It guarantees the non-starvation of resources for certain containers, avoids excessive utilization by others, and isolates them from each other effectively. This isolation is very relevant for multi-tenant environments, which use the same physical elements for one or more containers (Adhikari & Baidya, 2024). Also, control groups make containers more secure as resource limits slash the capability of DoS attacks from unsafe or compromised containers.

3. Seccomp (Secure Computing Mode)

As its name implies, Seccomp allows the Linux Kernel to place intense constraints on which system calls a container is allowed to execute, minimizing the capabilities that a compromised/malicious container can exploit, thus constituting an ideal choice for containers (Irvine et al., 2017). Seccomp can be implemented by writing and applying seccomp profiles: Initially, the default-deny policy is insisted upon and then fully specifies lists of system calls that are needed for a container. This substantially reduces the likelihood of having security flaws because the containers are simply able to run a predetermined number of operations. In our case, the second has several remarkable advantages: it removes many of the ways for an attacker to use kernel vulnerabilities and gives fine-grained control over the actions happening within the containerized space, thus greatly improving the security of the containers (Shahriar et al., 2020). Additionally, secure computing mode always restrict system calls which usually arise from the containerized applications. For example, it logs all system calls (audit.json), block some system calls (violation.json) or issue customized restrictions depending on the use cases and usually stored in the (violation.json) file.

B. Importance of image scanning for identifying vulnerabilities and malware

Image scanning is an effective strategy to scan container images to check for specific kinds of risks before releasing these images to the open public. The principle applies constantly in containerized environments to ensure their safety and sustainability (Zhang, 2021). During the image scanning process, it is possible to identify fields or libraries that may contain outdated or insecure code and address them before a threat becomes more severe.

Key Tools for Image Scanning

- Clair

- Trivy
- Aqua Security

C. Container runtime security measures to ensure secure operations

Securing the runtime environment of containers is highly important when it comes to the safe use of these technologies in production. Below are three essential runtime security measures discussed;

i. Runtime Monitoring and Logging
Real-time monitoring and logging alerts as well as tracking events that may be found suspicious or indicative of a security breach. Intrusion detection activities may include monitoring of system calls, network connections, file system access, and modification among other activities that may show suspiciousness. Documenting these activities is important as it creates a timeline that can be used in any investigations or resolution of incidents. Monitoring and logging are useful for the timely identification of threats and, therefore, are effective in preventing much of the possible harm.

ii. Implementing Least Privilege Policies
Programs and processes should be allowed to operate in as restrictive a security profile as possible, and least privilege policies confine containers to only those privileges required by their role in the system to avoid allowing a process with potential vulnerabilities to take control of the system. Any container should and can run as non-root users, and another security layer, such as AppArmor or SELinux, should limit capabilities. Another defense mechanism is that of operating with the least amount of rights/privileges possible to cut down on the damage that could potentially be caused if a hacker were to infiltrate the system (Raza et al., 2020).

iii. Automated Security Policy Enforcement
Implementing PSPs and OPA are semblances of automated security policy enforcement where policies are automatically implemented across the system. Automation also minimizes human aspects of security by reducing the chance of error occurrence and ensuring that all the implementations made are within the acceptable standards set according to the company's guidelines.

Machine learning and Deep learning are the essential methods that can help in detecting anomalies hence improve cybersecurity regarding data. These models can help in observation, leraning and predicting behavior solely depending on data and hence predict attacks effectively. The anomaly dtecetion from pattern recognition and behaviour analysis is not only a current technique but one that future architectural features depend on for security measures.

D. Recommendation of container orchestration tools and best practices

Container Orchestration is a critical element for the efficient and effective administration of containerization models. Below, I discuss two before-mentioned container orchestration tools which I recommend, Kubernetes and Docker Swarm, and describe key approaches to container management.

1. Kubernetes

Kubernetes is an open-source container orchestration tool that helps the organization manage and run containers at scale. It offers a great deal of flexibility, security, reliability, and operational excellence along with features like service discovery, load balancing, auto-progressive deployment, and rollback as well as inherent self-health-check functionality. Kubernetes' robust security measures inclusive of RBAC, policies, and secrets lend to its favor in enterprise adoption.

2. Docker Swarm

Docker Swarm is an open-source clustering and orchestration tool from Docker, which is used to manage multiple Docker hosts. Another MLEM is Docker-friendly, which makes it straightforward to use (Yücel et al., 2018). There are several features of Docker Swarm, including load balancing, service discovery, scaling of services, as well as multi-host networking and scheduling. It also has features such as multi-host networking, as well as secrets management. Docker Swarm is not as powerful as Kubernetes but since it is from Docker, it can be used easily and practically in simpler operations and environments.

Best Practices

- Security Configurations
- Resource Limits
- Regular Updates
- Monitoring and Logging

Kubernetes and Docker Swarm are strong contenders, each offering their own merits. Security guidelines, resource control, frequent updates, and effective monitoring reduce risks and maintain optimized grounds for containerized Applications. These practices bring the necessity of the orchestration of Operating System improvements in the reliability and security of containers, which have become the basis of the modern IT industry.

3. Vulnerability Management Policy:

A. Vulnerability management policy

Purpose

The purpose of this Vulnerability Management Policy is to establish the rules for the monitoring, review, evaluation, application and verification of system updates to mitigate vulnerabilities in the IT environment and the risks associated with them.

Audience

This Vulnerability Management Policy applies to the IT resources management team and any other individuals who are involved in the management of IT resources.

Policy

Vulnerability Scanning

1/ Vulnerability scans of all IT properties must be conducted periodically of after any changes made to the system.

2/ Failed vulnerability scan results of critical or highly sensitive properties must be remediated and re-scanned until all the scans complete successfully on critical or highly sensitive properties.

3/ Any evidence of a compromised or exploited IT resources found during vulnerability scanning must be reported to the IT team.

4/ Compromised or exploited properties must be isolated from other parts of the system by the IT team.

Logging and Alerting

1/ Documented standard configurations for IT properties must include log settings to record any activities that may cause harm or are relevant to information system security.

2/ Activity logs must be conducted according to the standard Logging Standard and sent to a central log management solution.

3/ A review of log files must be conducted periodically by the IT team and a third-party organization.

4/ All compromised or exploited properties identified during the log reviews must be documented, review and isolated.

5/ File integrity monitoring or change detection mechanisms must be applied to logs and critical files.

6/ Strict access privilege and tampering detection must be applied to log files.

7/ The time information used in the whole system must be retrieved from a single reference time source on a regular basis to make the timestamps in logs stay consistent.

8/ All log files must be maintained for at least one year.

Vulnerability Identification and Assessment

1/ All the reported compromised or exploited properties reported to the IT team must be documented and traced. The IT team or a third-party organization must conduct IT forensics on the affected properties to produce a complete report. The report should contain at least these aspects: affected properties, identified vulnerability, mitigation procedures and configuration standards update recommendations.

2/ All the vulnerability identified in the report must be documented and traced among all properties. Whole through scans and tests must be conducted on all propertied.

3/ The potential impact of identified vulnerabilities and affected properties must be evaluated by the IT team and third-party organization.

4/ Mitigation measures including configuration standard update, vulnerability scan & test standards update and patch procedures must be implemented by the IT team or a third-party organization.

Penetration Testing

1/ Penetration testing of all IT properties including internal network, external network and hosted applications must be conducted at least once a year or after any significant changes to the system.

2/ Any vulnerabilities found during the penetration test must be documented and traced. The vulnerabilities must be put into vulnerability identification and assessment procedures.

Patch Management

1/ All IT properties must be scanned on a regular basis to identify mis-installed or missing updates.

2/ All mis-installed or missing updates must be evaluated according to the attack surface they expose to. They must be implemented within a time period.

3/ All updates and configuration changes applied to the system must be tested in the development environment and review environment before pushed to product environment.

4/ All update deployment must be verified within a reasonable time period.

B. Prioritize and categorize of vulnerabilities

Using the CVE Details and EPSS scores, we can identify, prioritize and categorize three most-risky vulnerabilities for the organization as follows:

1/ CVE-2021-44228 (Log4Shell):

-Severity: Critical (CVSS score: 10.0)

-Impact: Expose code execution vulnerability to malicious attackers on servers running vulnerable version of log4j. This can lead to complete system compromise.

-EPSS Score: Very High, indicating widespread exploitation.

-Category: System Vulnerability

2/ CVE-2021-34527 (PrintNightmare):

-Severity: Critical (CVSS score: 9.8)

-Impact: Expose code execution vulnerability to malicious attackers. This can lead to complete system compromise.

-EPSS Score: High, indicating a high likelihood of exploitation.

-Category: Critical Infrastructure

3/ CVE-2022-22965 (Spring4Shell):

-Severity: High (CVSS score: 9.8)

-Impact: This vulnerability allows malicious attackers to execute arbitrary code on the server.

-EPSS Score: Medium to High, suggesting significant exploitation potential.

-Category: Application Vulnerability

C. Remediation and patch management

Discovery of Vulnerabilities

1/ Vulnerability Detection: All the properties including hardware and software must be scanned regularly using automated tools. All security activities in the system must be monitored.

2/ Assessment: Evaluate the severity of identified vulnerabilities with CVSS scores and EPSS ratings

Prioritization of Vulnerabilities

1/ Risk Assessment: Vulnerabilities should be prioritized based on their severity, potential impact and affected properties range. Critical vulnerabilities should be addressed immediately due to their high severity and possibility of exploitation.

2/ Asset Inventory: The IT team should maintain an updated inventory of all properties and determine the criticality of each property to prioritize patching efforts.

Planning and Testing

1/ Patch Availability: Check the availability of patches from vendors or open-source communities for identified vulnerabilities. If the patches are not available now, other measures including halt affected properties or isolate affected properties should be considered and discussed.

2/ Testing: All the patches should be tested in an all-controlled environment before been applied to product environments to ensure that they will not cause negative impact on systems or applications.

3/ Validation: All the patches applied to the system should be verified after deployment to ensure that they do mitigate vulnerabilities.

Deployment

1/ Patch Deployment: The patches should be deployed in a phased manner and start from the most critical parts. Verified automated patch management tools can be used for efficient deployment.

2/ Backup and Rollback: Backup & Rollback procedures should be implemented and maintained before the deployment of patches. If there are any issues during the deployment of patches, rollback plans should be taken up to conduct the recovery of systems.

Monitoring and Verification

1/ Post-Deployment Monitoring: The patched properties should be monitored for any unusual/unsafe activities or performance issues after the deployment of patches. Verification should be conducted by the IT team to ensure that the patches are deployed successfully and the vulnerabilities are mitigated.

2/ Continuous Monitoring: The IT team should continuously monitor for new vulnerabilities and ensure that the patch management process is ongoing.

D. Monitoring and reporting mechanisms

SIEM system

The functions of SIEM systems vary, but typically provide the following core functions:

Log management: The SIEM system collects a large amount of data in one location, organizes the data, and then determines whether it reflects signs of threat, attack, or destruction.

Event correlation: The system will then sort the data, determine relationships and patterns, and quickly detect and respond to potential threats.

Event monitoring and response: SIEM technology monitors security events in organizational networks and provides alerts and audits for all activities related to events.

The working mode of SIEM:

Firstly, The SIEM system monitors the event logs of hardware or software devices and generates an event every time the device observes a change. Therefore, The SIEM system will access device log files from storage or use event stream protocols to monitor network data. Once the event data is obtained, The SIEM system will organize and aggregate data during the log flow process. Although this process varies between SIEM systems, the first step is usually to filter out noise, such as excluding reports of devices operating under expected parameters. Index various event logs to classify data and enable search and event connectivity. Then analyze the collected event data to identify patterns and establish relationships, in order to identify vulnerabilities and suspicious events. Associate analyzed data with security threats based on rules typically manually provided by administrators. Each step in this process (sorting, indexing, and analysis) helps to achieve relevance, which is the core security feature of SIEM. For example, if the SIEM system discovers 1000 login failures due to password errors, it can associate the activity with some type of security threat and create an alert, which can then be handled by human experts or automated systems.

Due to the sensitivity of the collected data, The SIEM system has traditionally been locally hosted. However, the cost of maintaining these local systems is high as they require the use of specialized software and supervision by security personnel.

To avoid this complexity, many companies have to look for other solutions. Like most systems in today's hybrid cloud world, SIEM can be provided as locally installed software, cloud-based self-service processes, or through hosted services provided by cloud providers or hosted security service providers (SIEM as a service). Many SIEM solutions can also be

divided into a hybrid model, where some data (which may be more sensitive) resides locally, while others are stored in the cloud.

For reports, it is necessary to establish a regular reporting mechanism, and staff need to regularly summarize monitoring reports. The report content should include identified vulnerabilities, vulnerability fixes, and future trend analysis, and send them to stakeholders

E. Vulnerability scanning and assessment tools

Nessus

Based on the popular Nessus vulnerability scanning tool, Tenable provides integrated enterprise level vulnerability detection that can evaluate 47000 unique IT vulnerabilities, IoT , OT, Operating systems and applications. It provides integrated functionality for vulnerability scanning of networks, websites, and applications (webapps), and is backed by proprietary research to discover zero day vulnerabilities and provide support for their proprietary threat intelligence sources.

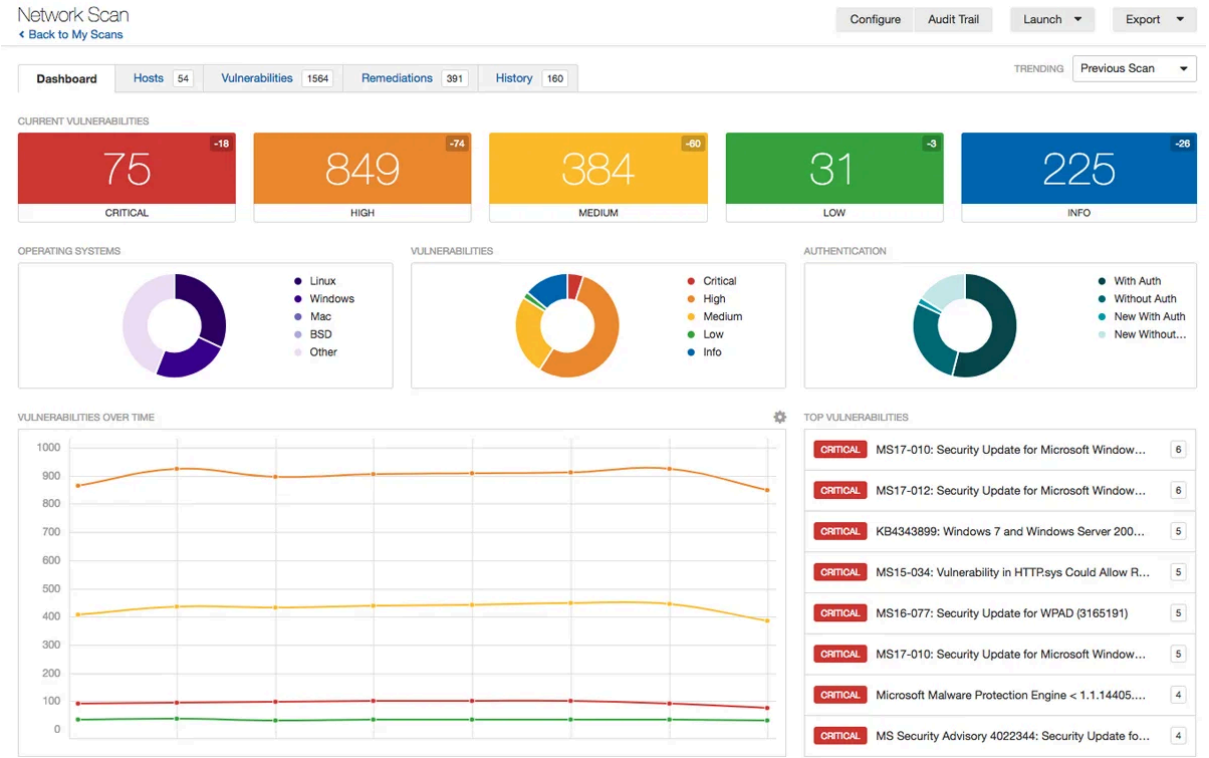
Nessus can pre configure templates for quick startup, trigger automatic comprehensive scanning after adding all new vulnerabilities, continuously scan for vulnerabilities and compliance configurations, provide multi tenant options and customizable templates for IT service providers, and include automatic alerts for security events and event management (SIEM) tools

Advantages:

One tool can scan IT infrastructure as well as websites and applications

The dashboard and powerful filtering functions allow for deep exploration and discovery

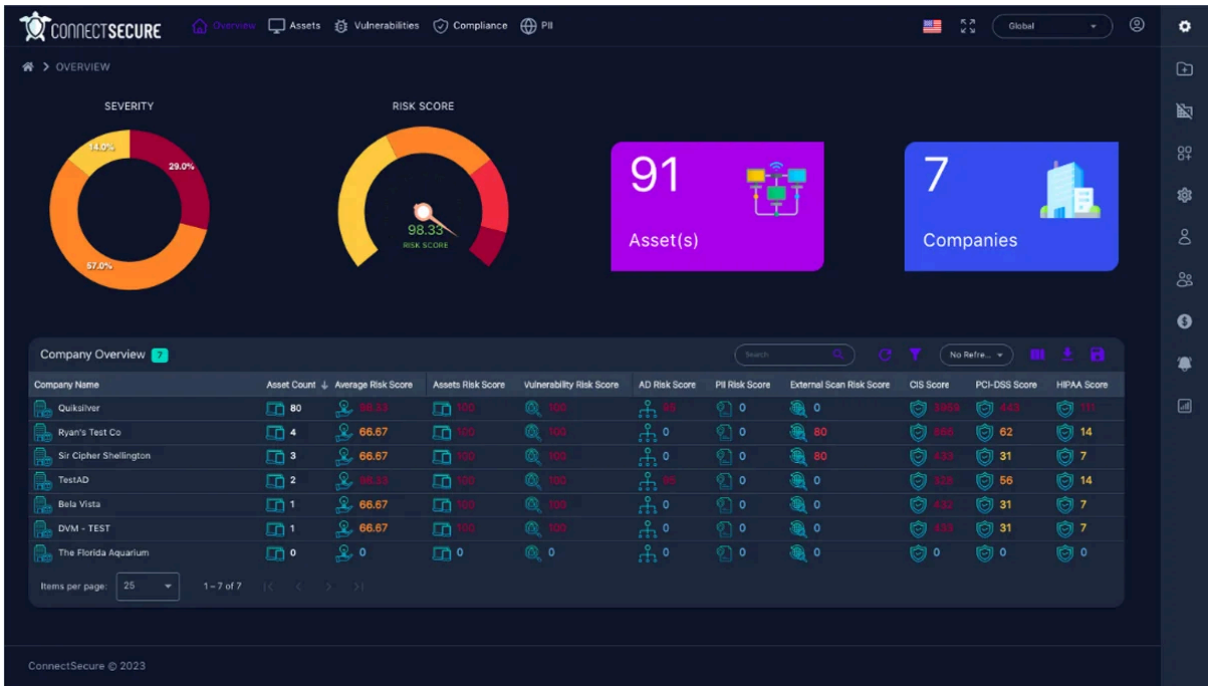
Threat intelligence developed internally can provide early warning of zero day vulnerabilities



Kime, C. (2021)

ConnectSecure

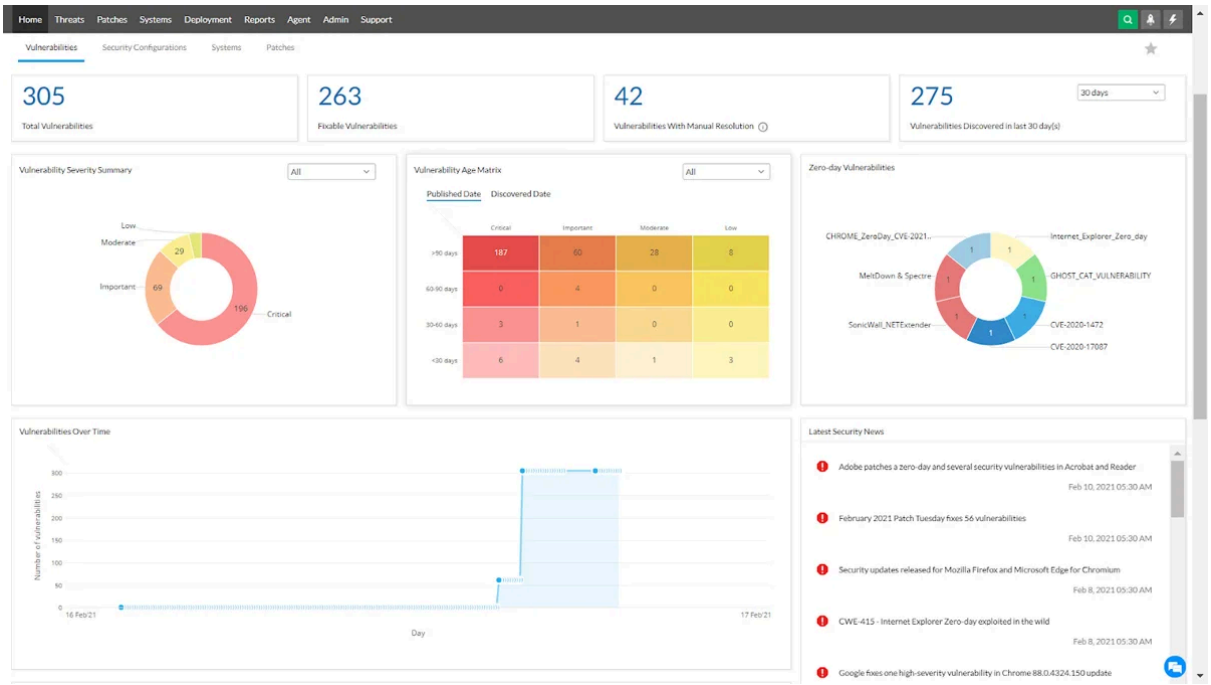
Connect Secure is a vulnerability scanner for hosted IT service providers (MSPs) and hosted IT security service providers (MSSPs), which can scan endpoints, servers, network devices, printers, and mobile devices for vulnerabilities and compliance issues.
Connect Secure has priority multi customer reporting, role-based custom reporting, and multi tenant functionality with white highlighted options. It can visualize client dashboards to provide customers with easy to understand, customizable, and non-technical automated reports, and is compatible with popular ticketing systems such as Connect Wise SyncroMSP and other communication tools (email Powerful integration options for Slack and Microsoft Teams. Its powerful asset and threat management options are used for asset discovery, patch deployment, compliance management, and prioritization of threats and vulnerabilities.
Advantages:
Provide excellent coverage for expected devices in most simple IT environments (endpoints, servers, and basic network devices)
Customizable report support for provider or customer brand reports
Basic ticket generation or vulnerability management options, such as applying patches or prioritizing vulnerabilities



Kime, C. (2021)

Vulnerability Manager Plus
Operating system and third-party software scanning can detect expired software, peer-to-peer software, and unpatched vulnerabilities. The pipe cleaner can detect vulnerabilities by scanning default credentials, firewall configuration errors, open sharing, and user permission issues, and perform basic web server vulnerability scans on unused web pages, improperly configured HTTP headers/options, expired certificates, and more.
Advantages of Vulnerability Manager Plus:

Integrate vulnerability assessment, compliance, patch management, and system security configuration into one tool
Entry level friendly product, easy to set up, cost-effective, and able to meet common IT needs
Open port detection for all IT assets



Kime, C. (2021)

F. Cloud infrastructure guidelines

Access control and identity management

Authenticate users, computers, or software components by verifying their claimed identities. Multiple authentication (MFA) can be added to individual users for additional security, or single sign on (SSO) can be added to allow users to authenticate their identity using a portal instead of many different resources. Authorization ensures that users are granted the exact level and type of access to the tools they have access to. Users can also be divided into groups or roles to grant the same permissions to a large number of users. Using MFA to reduce security risks and improve security response.

Data encryption

Use AWS for data encryption and TLS protocol to ensure that information is not intercepted during transmission. Using encryption algorithms to ensure
The key needs to be replaced or updated regularly, and automated tools can be used to assist, such as the AWS platform.

Configuration management and vulnerability patching

Use code tools to manage the configuration of cloud resources. Code can be traced and audited through version control. Set up an automated management process to ensure that the system can update security patches in real-time. Security configurations need to be checked periodically to identify and fix vulnerabilities.

4. Regulations and Compliances

This section describes how to manage personal information data, financial data, and cloud computing cybersecurity control frameworks using the General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS), CSA Cloud Control Matrix (CSA CCM), and ISO 27017, the security regulations and standards for protecting data.

A. General Data Protection Regulation (GDPR)

Requirement:

processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

Content:
This requirement means that personal data must be collected and used in accordance with the requirements of the GDPR (lawful basis)(ICO), it must be ensured that nothing will be done with the data that would contravene any other law, it must be used in a way that is fair and does not cause undue harm to the individuals concerned, it must be processed in an accidental or misleading way and it must be publicly communicated from the outset as to how it will be used.

Impact:
Policies on the processing of personal data need to be transparent to ensure easy access to personal data information.
The processing of personal data must comply with legal requirements, which means that every organization needs to have a detailed personal data privacy policy that clearly and publicly states how personal data will be collected, used and processed.
Organizations need to review and update their personal data privacy policies on a regular basis to ensure that the organization's collection, processing and use of personal data meets the latest legal requirements and business needs.

Requirement:

adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

Content:
The processing of personal data must be adequate, relevant and limited to the extent necessary for the purposes of the processing. Personal data may only be processed if the purpose of the processing cannot reasonably be achieved by other means.

Impact :
Organizations should tailor their business needs to ensure that only the minimum amount of data required for a specific purpose is collected and processed.
The data collection system should be designed based on the minimum number of data entry fields.
Regularly review the data update process to update the data collection system and remove outdated/unnecessary data.
Delete data regularly to ensure that only data required for the business is retained.

Requirement :

> processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Content:
This is the only principle of the GDPR that explicitly deals with security.It is about integrity and confidentiality. it specifies how the organization handles personal data and how it prevents leakage.

Impact :
Organizations need to adopt strong data security policies such as encryption, access control, auditing of logs, updating data security systems to protect personal data from unauthorized access/use and disclosure of personal data.
Advanced encryption techniques are required to ensure the security of personal data during transmission and storage.
Multi-factor authentication, the principle of least privilege and strict access control policies are implemented to prevent unauthorized access.
Intrusion detection and disaster recovery need to be deployed in the system to detect and update system availability in a timely manner to prevent potential security threats (GDPR,2021).

B. Payment Card Industry Data Security Standard (PCI DSS)

First point: Build and Maintain a Secure Network and Systems. (PCI version4 ,2022)
Install and Maintain Network Security Controls

1.1 Define and understand processes and mechanisms for installing and maintaining network security controls
Content:
All security policies and operating procedures need to be: documented, kept up-to-date, in use, and known to all affected parties.
Implementation measures:
Ensure that these policies and procedures are properly documented, maintained and disseminated.
When updating policies and procedures, consideration should be given to updating them as soon as possible after a change occurs, rather than on a regular basis.
Use a responsibility assignment matrix that includes responsible, accountable, consulted and informed persons.
Impact:
If roles and responsibilities are not precisely assigned, staff may be unclear about their day-to-day responsibilities, resulting in key activities not being carried out.

Entities need to make staff accept and understand their assigned roles and responsibilities.

1.2 Configure and maintain network security controls

Content:

The configuration criteria for NSC rule sets are: defined，implemented，maintained。

Implementation measures:

These standards specify the requirements for acceptable protocols, the ports allowed to connect to the NSC, and the configuration of the NSC.

Examples of NSCs covered by these configuration standards are not limited to firewalls, but also routers configured with access control lists and cloud virtual networks.

To avoid security issues associated with processing changes, all changes should be approved prior to implementation and validated after implementation. Once approved and validated, the network documentation should be updated to incorporate the changes to prevent inconsistencies between the network documentation and the actual configuration.

Impact:

Implementing these configuration standards allows for proper configuration and management of the NSC so that it can properly perform its security functions.

An up-to-date, ready-to-use data flow diagram can show how account data flows across the network and between individual systems and devices, helping organizations understand and track the scope of their environment.

1.3 Restrict network access to the cardholder data environment

Content:

Restrictions on inbound traffic to CDE: Inbound traffic is restricted to essential traffic only, all other traffic is explicitly denied.

Restriction on outbound traffic for CDE: Inbound essential traffic only, all other traffic is explicitly denied.

Implementation measures:

All inbound and outbound CDE traffic, regardless of origin, should be evaluated for compliance with authorization rules.

Implement rules for rejecting all non-required inbound and outbound traffic, either through explicit reject all or implicit rejection.

Ensure that this traffic is authorized traffic by restricting source ip addresses/destination addresses and ports, and by blocking content.

Impact:

It prevents malicious people from accessing the physical network through unauthorized IP addresses or using services, protocols and ports in an unauthorized manner.

Sophisticated rules for inbound and outbound traffic help prevent vulnerabilities that allow unexpected and potentially harmful traffic.

Malicious individuals and compromised system components within the physical network can be prevented from communicating with untrusted external hosts.

1.4 Controls network connections between trusted and untrusted networks:

Content:

NSCs are implemented between trusted and untrusted networks to prevent potential security threats.

Implementation measures:

An entity implements a DMZ to manage connections between untrusted networks and organizational services. An entity's DMZ is also considered a CDE if it processes or transmits service data.

System components that store cardholder data cannot be directly accessed by untrusted networks.

Anti-spoofing is taken to detect and block spoofing of source IP addresses into the protected network.

Inbound traffic from untrusted networks to trusted networks is limited to: authorized, stateful responses to communications initiated by system components in the trusted network and denial of all traffic.

Disclosure of internal IP addresses and routing information is limited to authorized parties.

IMPACT:

Implementing NSCs on every connection to and from the trusted network allows entities to monitor and control access, minimizing unauthorized access to the internal network.

Reduce the risk of exposing system components to untrusted networks.

Filters packets entering the trusted network.

Use NSCs to ensure that system components storing cardholder data can only be accessed directly from a trusted network to avoid unauthorized network traffic reaching system components.

Disclosure of internal, private and local IP addresses can be effectively restricted to prevent hackers from obtaining IP address information and using it to access the network.

1.5 Mitigate the risk of computing devices capable of connecting to untrusted networks and CDEs

Content:

Risks posed by computing devices capable of connecting to untrusted networks and cardholder data environments (CDEs) should be mitigated.

Implementation measure:

Use security controls such as host-based controls (e.g., personal firewall software or endpoint protection solutions), network-based security controls (firewalls, network-based heuristic checks, and malware emulation), or hardware to protect devices from Internet-based attacks.

It is up to the entity to determine the specific security control settings and they need to be consistent with its cybersecurity policies and procedures.

Any disabling or changing of security controls is performed by authorized personnel.

Since administrators have special privileges to disable security controls, an alert mechanism should be set up and followed up when security controls are disabled.

Impact:

Reduce security threats from computing device connectivity through effective risk mitigation.

Improve network security and protect cardholder data from potential security threats.

Second point: Protect Account Data

Protect Stored Account Data

2.1 Defined and understand the processes and mechanisms to protect stored account data

Content:

All security policies and operating procedures in Protect Account Data are: documented, kept up to date, in use, and known to all affected parties.

Record, assign and understand roles and blame in activities.

Implementation measure:

Update policies and procedures and update these documents as changes occur, rather than periodically.

Roles and responsibilities are documented in policies and procedures so that employees understand and accept their backup assigned roles and responsibilities.

Impact:

The security policy defines the entity's security objectives and principles, and the operating procedures define and describe how activities are to be performed and the controls, methods, and processes to be followed in order for the objectives to achieve the desired results in a consistent manner.

If roles and responsibilities are not correctly assigned, staff may not be aware of their day-to-day responsibilities, and critical activities may not be carried out, with dramatic implications for security.

2.2 Minimize storage of account data

Content:

Minimize the storage of account data by implementing data retention and disposal policies, procedures and processes.

Implementation measure:

When determining where to store account data, all processes and accessible personnel should be considered, as data may have moved from its original location.

Determine appropriate retention requirements to fulfill any legal or regulatory obligations of the entity's industry or the type of data retained.

Implement automated processes to ensure that data is automatically and securely deleted within specified retention periods.

If you do not need it, do not store it.

Impact:

Identifying and securely eliminating stored data that has exceeded its established retention period prevents unnecessary retention of data that is no longer needed.

Helps ensure that account data is not retained beyond what is required for business, legal or regulatory purposes.

2.3 Sensitive Authentication Data (SAD) may not be stored after authorization

Content:

Ensure that all received sensitive authentication data is unrecoverable after authorization is complete.

Check recorded policies, procedures and system configurations to ensure that data is not retained after authorization.

Observe the secure data deletion process to ensure that data is securely deleted after authorization is completed.

Implementation measure:

If the card validation code is stored on a paper medium before the authorization is completed, the validation code shall be erased or overwritten in such a way that it cannot be read after the authorization is completed.

Ensure that PINs and PIN blocks are not retained after the authorization process is complete.

Entities should consider encrypting the SAD with a different encryption key than the encrypting PAN.

To ensure that no content is left behind after the authorization process is completed, sources of data to be reviewed include, but are not limited to: Input transaction data, logs, history files, trace files, database schema, contents of database storage and existing dump files.

Impact:

Reduce the risk of potential data breaches by avoiding the storage of sensitive authentication data.

Ensure data is unrecoverable after authorization is complete, enhancing data security.

2.4 Limit access to full PAN display and ability to copy cardholder data

Content:

Masking when displaying the PAN so that only those with legitimate business needs can see the content.

When using remote access technology, all personnel should be prevented from copying/relocating the PAN except authorized personnel.

Implementation measure:

If only the last four digits of data are required to perform an operation, the PAN should be masked and only the last four digits should be displayed.

If a feature needs to see the BIN (Bank Identification Number) for routing, the masking of the BIN digits should be removed for that feature only.

Copying and transferring of PAN can only be done on storage devices that are permitted and authorized by the individual.

Impact:

Ensuring that the full PAN is only displayed to those with a legitimate business need minimizes the risk of unauthorized personnel gaining access to PAN data.

Ensuring that only those who are explicitly authorized and have a legitimate business need to replicate the PAN can minimize the risk of unauthorized personnel gaining access to PAN data.

2.5 Secure the Primary Account Number (PAN) for storage

Content:

Wherever the PAN is stored, it should be secured. It can be secured in any one of the following ways:

One-way hash using strong encryption based on the entire PAN.

Truncation (can't use hashing to replace truncated segments of a PAN).

If there are hashed and truncated versions of the same PAN, or different truncated formats of the same PAN in the environment, additional controls are required so that the original PAN cannot be reconstructed between versions.

Index Tokens。

Strong encryption with associated key management processes and procedures.

Implementation measure:

Protect the stored PAN using strong encryption methods such as AES-256.

Regularly review and update encryption policies and techniques to ensure that they comply with the latest security standards.

Impact:

Remove Plaintext Storage PAN is a defense-in-depth control designed to protect data in the event that an unauthorized individual exploits a vulnerability or misconfiguration of an entity's primary access control to access stored data.

A secondary independent control system (which manages access to and use of encryption and decryption keys) prevents the confidentiality of the storage PAN from being compromised by failing the primary access controls.

2.6 Secure encryption keys used to protect stored account data

Content:

The following measures are taken to protect the encryption key of the stored account data from leakage and misuse:

Allow only a minimum number of custodians to access the keys.

The strength of the encryption key is at least the same as the encryption key for the data it protects.

The key encryption key is stored separately from the data encryption key.

Store keys securely in as few locations and forms as possible.

Implementation measure:

Develop and implement cryptographic key management policies and processes covering key generation, distribution, storage, rotation and destruction.

Use Hardware Security Module (HSM) to store encryption keys and ensure their security.

Impact:

Encryption keys must be strictly protected to ensure that only those who have been granted access are able to decrypt the data, avoiding unauthorized decryption that could lead to data leakage.

Secure storage of encryption keys prevents unauthorized or unwanted access than avoiding leakage of stored account data.

Limiting the number of people who can access the plaintext encryption key component reduces the risk of stored account data being retrieved or displayed by unauthorized parties.

Storing any encryption keys in a minimal number of locations helps organizations track and monitor all key locations and minimizes the likelihood of key exposure to unauthorized parties.

2.7 Define and implement key management processes and procedures when using encryption to protect stored account data

Content:

Implement key management policies and procedures, including generating, securely distributing, and securely storing encryption keys used to protect stored account data.

Implement a key management policy that replaces or destroys keys used to protect stored account data in the following situations: The key to meet a specified encryption period. The integrity of the key is already at risk (employee with knowledge of the plaintext key/key components leaves the company). And the key has been compromised.

Key management policies include the use of split knowledge and dual control.

Implementation measure:

Develop policies and procedures for strong encryption key generation.

Ensure secure distribution and storage of encryption keys.

Periodically review key management processes to ensure they are in line with industry best practices.

Impact:

The use of strong encryption keys greatly increases the level of security of encrypted account data.

When the encryption period of an encryption key ends, the encryption key must be replaced to minimize the risk of someone obtaining the encryption key and using it to decrypt data.

Split knowledge and dual control for keys is intended to eliminate the possibility of a single person having the entire key, and to avoid the risk of a single person being able to access the database without authorization, which could result in a data breach.

Third point: Maintain a Vulnerability Management Program

3.1 Define and understand the processes and mechanisms to protect all systems and networks from malware

Content:

All security policies and operating procedures in Protect Account Data are: documented, kept up to date, in use, and known to all affected parties.

Record, assign and understand roles and blame in activities.

Implementation measure:

Update policies and procedures and update these documents as changes occur, rather than periodically.

Roles and responsibilities are documented in policies and procedures so that employees understand and accept their backup assigned roles and responsibilities.

Impact:

Ensure consistency and effectiveness of malware protection through clear processes and mechanisms.

Increase employee awareness of malware protection and reduce the risk of malware infection.

3.2 Preventing, detecting and dealing with malware

Content:

Deploy anti-malware solutions on all system components.

Anti-malware solution: detects all known types of malware. Remove, block or include all known types of malware.

Perform periodic assessments of any system components that are not at risk for malware. Identify and assess evolving malware threats to system components. Confirm whether system components require anti-malware protection.

Users can not disable (or change) anti-malware mechanisms and anti-virus software mechanisms unless specifically documented and authorized by management at each level.

Implementation measure:

Install anti-virus and anti-malware software on all systems and ensure that they are automatically updated.

Scan systems regularly to detect and remove malware.

Develop and implement malware protection policies to ensure all system components are compliant.

Impact:

With regular updates to your anti-malware solution, you can effectively avoid the dangers of new situations where malware attacks your system, paralyzes your network and destroys your data.

Protect against all types and forms of malware to prevent unauthorized access.

3.3 Maintain and monitor anti-malware mechanisms and processes

Content:

Anti-malware solutions are kept up-to-date with automatic updates.

Anti-malware solutions perform regular scans or proactive scans for ongoing behavioral analysis of systems or processes.

For removable electronic media, performs automated scanning and ongoing behavioral analysis of systems or processes when media is inserted, connected, or logically mounted.

Enable and retain audit logs for anti-malware solutions.

Users may not disable or change anti-malware mechanisms unless specifically documented and authorized by management on a case-by-case basis, subject to time limits.

Implementation measure:

Regularly check the operational status of anti-malware mechanisms to ensure they remain active and effective.

Timely updating of anti-malware software and mechanisms to ensure that they are capable of responding to emerging malware threats.

Monitor system logs and alarms to detect and handle malware infections in a timely manner.

Impact:

Ensure system security by continuously monitoring and maintaining anti-malware mechanisms.

Improve the system's ability to defend against malware attacks and protect cardholder data.

3.4 Anti-phishing mechanisms protect users from phishing attacks

Content:

Processes and automated mechanisms are in place to detect and protect personnel against phishing attacks.

Implementation measure:

Deploy anti-phishing software and email filters to detect and block phishing emails.

Conduct employee training to increase their alertness and response to phishing attacks.

Establish a phishing attack reporting mechanism to encourage employees to report suspicious emails in a timely manner.

Impact:

Technical controls can limit the number of times staff can assess the authenticity of communications and also limit the impact of individual responses to phishing.

Reduce the risk of users being exposed to phishing attacks through anti-phishing mechanisms.

Increase employee awareness of phishing attacks and protect the overall security of the organization.

C. ISO 27017 and Cloud Security Alliance (CSA) Cloud Control Matrix

First point: ISO 27017 - Cloud Security Controls (ISO Edition1,2015)

Content:

ISO/IEC 27017 is a security standard for cloud service providers and subscribers to create more secure cloud environments and reduce the risk of security issues. ISO/IEC 27017, used in conjunction with the ISO/IEC 27001 family of standards, provides enhanced controls for both cloud service providers and cloud service customers. Unlike many other technology-related standards, ISO/IEC 27017 clarifies the roles and responsibilities of both parties to help ensure that cloud services are as secure and reliable as any other data contained in a certified information management system.

Control measure:

ISO/IEC 27017 builds on the 37 controls of ISO/IEC 27002 and adds seven new cloud controls to address: the responsible relationship between the cloud provider and the cloud subscriber, removal/return of assets upon contract termination, securing and segregating the subscriber's virtual environments, virtual machine provisioning, management operations and procedures related to cloud environments, monitoring of in-cloud activities by the cloud subscriber and virtual and cloud networks environment orchestration.

Implementation measure:

Ensure that virtual machines are set up in compliance with legal requirements and security standards to prevent unauthorized access that could lead to data leakage.

Implement a data segregation policy to ensure that each user's personal data is handled and stored separately to prevent data leakage.

Use multi-factor authentication and authorization to protect the cloud environment from attacks.

Impact:

With the above strategies, both the cloud service provider and the customer can be secured in the cloud environment while ensuring the confidentiality, integrity and availability of the customer's personal data.

Second point: Cloud Security Alliance (CSA) Cloud Control Matrix (CCM) (CSA,2024)

Content:

The CSA Cloud Control Matrix (CCM) is a cybersecurity framework designed to provide a structured, standardized set of security controls for cloud computing environments. Thus helping organizations to assess the security status of their cloud infrastructure and services.

Control measure:

The CCM consists of 197 control objectives organized into 17 domains covering all key aspects of cloud technology. It can be used as a tool to systematically assess cloud implementations and provide guidance on which security controls should be implemented by which participants in the cloud supply chain(CSA).

Implementation measure:

Enhancing Cloud Security: CCM Makes the Entire Cloud Supply Chain More Secure, and the cloud service providers use CCM to identify and mitigate security breaches and continuously monitor their compliance status.

Cloud services customers use CCM to assess and monitor the quality of their vendors' security practices to build more secure cloud and hybrid cloud architectures.

Simplified Compliance:CCM simplifies implementation and compliance programs by providing a comprehensive framework for protecting cloud architectures.

Impact:

Migrating IT assets from local data centers to the cloud reduces enterprise risk because companies no longer maintain servers and other network infrastructure

Every organization in the cloud supply chain can use CCM to enhance their security controls, assess vendor compliance, and assure customers that their security systems follow cloud computing industry best practices.

Third point: ISO 27018 - The protection of personal data(Wiki,2024)

Content:

ISO 27018 is a security standard in the ISO 27000 family of standards. It was created in 2014 as an addendum to ISO/IEC 27001, the first international specification of practice for cloud privacy. It helps cloud service providers that handle personally identifiable information (PII) assess risks and implement controls to protect PII. The aim is for cloud service providers whose infrastructure is certified to this standard to inform their existing and potential customers that their data is protected and will not be used for any purpose without their explicit consent.

Control measure:

Expanded Security Controls: Encrypt PII on transmission, storage and removable media.

Delete PII: Deletes PII after the data is no longer needed for a specified period of time.

Purpose of Processing: Process PII only for the purposes specified in the cloud service agreement.

Cooperative Processing: Cooperate with the PII subject's right to inspect and correct their PII.

Implementation measure:

The use of strict adherence to legal and regulatory requirements based on the region in which each organization is located ensures that ISO 27018 complies with those legal and regulatory requirements.

Organizations need to conduct a comprehensive risk assessment to identify potential risks associated with PII processing. They should also develop appropriate countermeasures to control the risks through the guidelines of ISO 27018.

Implement necessary technical controls such as encryption, access control and data loss prevention (DLP) systems.

Train employees on ISO 27018.

Implement a periodic review program to regularly assess the effectiveness of data protection measures.

Develop and implement a sound incident response and management system.

Impact:

The use of ISO 27018 effectively ensures an organization's ability to protect personally identifiable information (PII) while avoiding the risks associated with unauthorized access and data breaches.

The use of ISO 27018 improves an organization's compliance and competitiveness in the marketplace.

With detailed risk assessments and controls, organizations can better identify the risks posed by PII handling, thereby reducing data breaches and security incidents.

5. Incident Response Policy

5.1. Logs and Platforms

Privileged User Access Logs

Privileged user access logs record the activities of users with elevated permissions in an IT environment (Microsoft, 2024). These logs capture details such as who accessed privileged accounts, the timing and duration of access, the actions performed, and the systems involved. They are essential for monitoring, auditing, and securing privileged access to sensitive data and systems.

Platform: Microsoft Entra Privileged Identity Management (PIM)
PIM, a service within Microsoft Entra ID, allows users to manage and monitor access to critical organizational resources, including Microsoft Entra ID and Azure (barclayn, 2023b). Given the sensitivity of data managed by financial institutions, it is crucial to monitor privileged user access to prevent unauthorized access and potential data breaches.

Benefits to the client:

1. **Access monitoring and alerting**
   PIM delivers an extensive log of all privileged access activities, detailing who requested access, which resources were accessed, and the duration of each access (Australian Government, 2023). It also includes support for alerts and notifications concerning unusual or unauthorized access attempts. With real-time monitoring and alerting, clients' security teams can swiftly identify and respond to potential security incidents involving privileged accounts, ensuring rapid containment and mitigation of threats.

2. **Increased audit compliance**
   PIM logs can be integrated with Azure Sentinel for analysis (mzorich, 2021). These logs include detailed records of privileged access, which is critical for compliance audits. Financial institutions must adhere to strict regulatory requirements. Detailed logs and reports help demonstrate compliance with regulations such as GDPR (Intersoft Consulting, 2018), avoiding potential fines and reputational damage.

3. **Role-Based Access Control (RBAC)**
   PIM supports RBAC-based implementations to ensure that users can only access the resources required for their role (barclayn, 2023a). This least privilege principle reduces the risk of accidental or malicious access to critical systems and data, thereby protecting the confidentiality and integrity of client organisations' sensitive financial information.

Network Traffic Logs

A network traffic log is a type of log that keeps a record of packets sent over a network. For example, a log contains detailed data such as source and destination IP addresses, port numbers and the amount of data transmitted.

Platform: Azure Network Watcher

Azure Network Monitor is a tool for monitoring, diagnosing, and gaining a comprehensive understanding of network traffic in Azure (halkazwini, 2023). For organisations dealing with sensitive financial data, the ability to monitor network traffic helps detect and respond to potential cyber threats.

Benefits to the client:

1. **Real-Time Monitoring and Alerts**
   Azure Network Monitor can be set up as a means of proactively monitoring network traffic and issuing alerts based on rules set up in advance (halkazwini, 2023). This real-time monitoring capability allows security teams within customer organisations to deal with potential security threats, such as DDoS attacks or unauthorised access attempts, in a timely manner, thereby reducing potential losses.

2. **Easy forensics**
   Because network traffic logs provide important data for forensic analysis, they are critical in the security incident handling chain. Network traffic logs help reconstruct events and assess the impact of a breach. This data helps the customer organisation's security response team to conduct a full investigation to identify the root cause of the incident so that corrective action can be taken to avoid similar incidents in the future (Morales, 2023). Moreover, these logs serve as crucial evidence that can play an important role in future proceedings or legal actions.

3. **Network Performance Monitoring**
   Network traffic logs serve multiple purposes including monitoring network performance. By analyzing these logs, one can identify issues like latency, packet loss, and throughput bottlenecks. Maintaining optimal network performance is useful for financial services to ensure availability, efficiency and operational effectiveness. If performance falls short of customer expectations, cloud service configurations can be upgraded based on log analysis to meet these needs.

Application Logs

Application logs are records created by a software application while it's running. These logs include details about the application's actions, events, any errors encountered and metrics related to its performance (OWASP, 2024b).

Platform: Azure Monitor

Azure Monitor is a powerful monitoring tool that can be used to collect, analyse and process monitoring data from the cloud (rboucher, 2024). Using Azure Monitor can help IT departments within customer organisations ensure optimal performance and availability of their applications and services.

Benefits to the client:

1. **Security Event Detection**
   The incident response team can analyse application logs to identify potential security events, such as unusual user behaviour or system exceptions. This type of proactive monitoring helps client organisations reduce security risks and protect sensitive financial data simultaneously.

2. **Errors Detection**
   The incident response team in the client organisation can detect errors, exceptions and warnings during application execution by analysing application logs. This could help the incident response team identify and resolve errors and configuration issues on time, ensuring data accuracy and system reliability.

3. **Monitoring Application Performance**
   Financial institutions' trading systems can use analysing application logs to gain insight into the functionality and efficiency of running applications. This monitoring is critical for client organisations to maintain business continuity and provide a seamless user experience.

Together, these platforms can form a robust incident detection and response framework that improves an organisation's ability to protect the confidentiality, integrity and availability of critical financial and customer data. In addition, they enable comprehensive monitoring and detailed logging of relevant activities, helping client organisations to comply with financial regulations.

5.2. Incident Response Team's Roles and Responsibilities

1. **Incident Manager**
   Responsibilities (Atlassian, 2022)**:**
   - Ensure compliance with regulatory requirements and relevant incident response strategies.
   - Serve as the main contact for incident reporting and communication.
   - Manage and supervise all phases of incident response, starting from detection through resolution.

   Incident Reporting Channel: Reporting directly to the Chief Information Security Officer (CISO) and senior executive management.

   Benefits to the Client: An Incident Response Manager plays a crucial role in ensuring centralized coordination and leadership during security incidents (Atlassian, 2022). This position streamlines communication and decision-making processes, leading to swift and effective resolution of incidents and minimizing their potential impact and downtime.

2. **Tech Lead**
   Responsibilities (Atlassian, 2022)**:**

- Offer technical expertise and guidance throughout incident response endeavours. Analyzing the technical dimensions of security incidents, evaluate their potential impact, and suggest technical solutions or mitigation strategies.
- Collaborate with Incident Managers, Security Analysts, and System Administrators to ensure a cohesive approach to detecting, analyzing, containing, and resolving incidents.
- Investigate security incidents comprehensively, involving log analysis, forensic examination, root cause identification, and assessing the damage's scope.

Incident Reporting Channel: The Technical Supervisor directly reports to the Incident Manager.

Benefits to the Client:

- The Technical lead has extensive technical expertise and experience in effectively analyzing, managing, and resolving security incidents (Nearsure, 2023). This proficiency is crucial for addressing the intricate technical aspects of complex incidents.
- The Technical lead oversees technical efforts and guides the team, ensuring an efficient and coordinated response to incidents (Jones, 2020). This leads to reduced response times and minimizes the impact of security incidents on the organization's operations.
- Precise documentation of technical discoveries and steps taken by the technical lead guarantees adherence to regulatory standards and streamlines post-incident analyses (Jones, 2020). This aids regulatory compliance efforts and fortifies the organization's incident response proficiency.

3. **Communications manager**

Responsibilities (Atlassian, 2022)**:**

- The Communications Manager is responsible for all communication channels concerning security incidents. It involves managing internal communications from the Incident Response team and external communications with the client organisation’s stakeholders, customers, regulators, and the media.
- Ensure that security incidents are promptly communicated to relevant parties, such as senior management, IT teams, and external partners when necessary.
- Handle media communication and public relations during security incidents, ensuring accurate information is shared while maintaining confidentiality and reducing reputational risks for the client organization.

Incident Reporting Channel: The Communications Manager reports directly to the Incident Manager and collaborates closely with the Executive Team, Legal Counsel, IT team, and external communications partners.

Benefits to the Client:

- Notifying stakeholders promptly about security incidents can speed up response and containment efforts. This proactive strategy reduces the impact of incidents on operations and customer trust (Yadav, 2023).

- During a significant security incident or crisis, the communications manager takes on an important role in crisis management (Yadav, 2023). They provide direction for communication strategies, handle public perceptions, and work to minimize potential impacts.
- The communications manager can ensure that all communications related to security incidents are clear, consistent and in line with the organisation's messaging strategy (Yadav, 2023). This also benefits the client organisation by maintaining transparency and promoting trust with stakeholders.

Clear roles and responsibilities help the incident response team structure an efficient incident response capability. The goal is to maintain data confidentiality, integrity, availability and compliance throughout the cloud migration process.

5.3. Incident Response Procedures

5.3.1 Containment

Containment limits the damage caused by a security incident and prevents it from spreading further (AWS, 2024). The containment process includes immediate and short-term strategies.

Immediate containment

Immediate containment is the process of isolating the systems in a customer's organisation that has been affected by a security incident and preventing it from spreading further. The immediate containment process first requires the security response team to identify the affected systems, applications and network segments. Then, the security response team should immediately the affected systems will be disconnected from the network while the compromised user accounts will be disabled to prevent further unauthorised access (Andress, 2016). In addition, the security response team needs to implement firewall rules to block malicious IP addresses, domains, and protocols. The compromised web server must also be disconnected from the network to prevent data leakage.

The immediate benefits of immediate containment for client organisations are providing a rapid response, preventing the incident from spreading and reducing the risk of further intrusions. This approach limits damage and preserves evidence for future analysis.

Short-term containment

The goal of short-term containment is to stabilise the environment with minimal disruption to operations by implementing temporary measures. Security response teams can limit access to sensitive data and critical systems, such as using multi-factor authentication (MFA) to achieve the objective. In addition, applying emergency patches can be used to address known vulnerabilities exploited by attackers. Enhanced logging and monitoring of affected systems and network segments is also critical. Also real-time correlation and analysis of security events using Security Information and Event Management (SIEM) systems can further improve monitoring (Andress, 2016).

Short-term containment has the advantage of maintaining a stable environment whilst the client organisation develops a long-term solution. This approach ensures that critical operations continue with minimal disruption.

By implementing the containment procedures mentioned above, financial institutions can ensure an effective response to security incidents and minimise their impact, improving overall security and compliance during the transition to the cloud.

5.3.2 Investigation

The investigation is another crucial phase in the incident response process, aimed at comprehending the nature, scope, and root causes of the incident. This stage involves gathering, analyzing, and interpreting data to understand the incident's impact (Bluevoyant, 2023).

Preparation

The security response team must establish a clear outline of the information required from the investigation, including identifying how the attack occurred, assessing the scope of the breach, and determining the root cause (Nur, 2023). It's crucial to have team members with specialized knowledge, such as security analysts and IT experts. All potential evidence should remain untouched to preserve its integrity, and forensic tools should be utilized to generate exact replicas of affected systems.

The aim of this is to provide the team with specific goals, ensuring that the investigation remains targeted and effective. Preserving evidence is crucial for upholding its integrity, which is vital for precise analysis and possible legal proceedings.

Data Collection

The data comes from a variety of logs including network traffic, application activity, privileged user access, system and file operations, and network analysis (Rodrigues, 2022). Each type of log has a different purpose, such as identifying anomalous traffic patterns in firewall logs; and detecting unauthorised access through database logs.

Security response teams collect data from multiple sources in order to get a full picture of an incident. By analysing logs, the team helps to identify unauthorised behaviour and potential signs of intrusion.

Data Analysis

Security response teams can use a variety of techniques to analyse data during an incident, such as creating a timeline to understand the sequence of the attacker's actions; performing root cause analysis to determine how the attacker gained access and exploited vulnerabilities, etc. (Nur, 2023). Data analysis helps to assess the impact of a security incident, which includes compromised data and affected systems, as well as the potential disruption to business operations. In addition, it identifies threat actors and their methods, motives, and goals.

This approach enables client organisations to gain a deeper understanding of the origins of security incidents and their possible consequences. It helps to develop effective remediation and prevention strategies.

Reporting

The incident response team should prepare a comprehensive report as soon as possible after the incident happens. The data analysis report should include the findings, incident causes and effects, actions implemented, and recommendations for future prevention strategies. The incident response team also needs to share these findings with relevant stakeholders such as senior management, the IT team and regulators (Nur, 2023). The client organisation should organise a post-incident review meeting with all relevant parties to report the findings, actions taken and insights gained as well.

In conclusion, taking the mentioned measures would ensure transparency and accountability for safety incidents. And enhance the trust of the client organisation with the stakeholders and regulators. Analysing incidents after they have occurred and documenting lessons learned can help the client refine and improve their incident response procedures.

5.3.3 Remediation

Remediation is the process of restoring an affected system to a secure and trustworthy state by resolving vulnerabilities, addressing the root cause of the incident, and restoring the system affected by the security incident. As well as implementing preventative measures to avoid similar incidents in the future (Thompson, 2018).

Elimination

The impact of security incidents on the client organisation can be reduced by removing the root cause of the security incident. The incident response teams can do this through patch management, malware removal and configuration change measures.

Patch management measures refer to updating all relevant systems and software applications with security patches to address known vulnerabilities that could be exploited by attackers as early as possible (Intel, 2024). This measure also includes the use of antivirus and anti-malware tools to scan and remove any malware and potential backdoors from the affected systems. Additionally, the incident response team can change the system configuration to minimise vulnerabilities and enhance security settings (Ande, 2024).

Recovery

Recovering online resources and services affected by a security incident is also part of the incident response team's job. It includes data recovery, system validation, and recovery services.

Data recovery refers to retrieving data from an uncorrupted backup and repairing or replacing any corrupted or encrypted data (Hannan & Burton, 2023). The security team should keep the backups updated and securely stored regularly to avoid data loss. Additionally, the incident response team can conduct extensive testing and validation of the recovered system to confirm proper and secure operation (Brunell, 2023). Furthermore, the

affected services should be restored in a controlled manner and continuously monitored for any recurring issues.

Protective measure

Preventive measures are taken to minimise the likelihood of similar security incidents recurring and to enhance overall security.

For example, client organisations improve system security by implementing access controls, adhering to the principle of least privilege and using multi-factor authentication (MFA) (OWASP, 2024a). It is also important to provide cybersecurity awareness training to employees on topics such as phishing attacks, social engineering tactics, and best security practices (Zhang et al., 2021). Refine and update response plans based on incident lessons learned, and adopt automation and coordination tools for more effective incident detection, response, and resolution.

Most importantly, financial institutions can strengthen their security posture during the transition to the cloud and ongoing operations by developing comprehensive remediation procedures. These measures ensure rapid resolution of security incidents and enable a seamless return to normal operations, ultimately enhancing overall security.

5.4. Communication and Reporting Requirements

5.4.1 During Security Incidents

When a security incident occurs, the first staff member to notice an exception must notify the Incident Response Team (IRT) immediately. The IRT leader will then be responsible for assessing the situation, initiating an incident response plan, and notifying all relevant team members (Voigt, 2018). Additionally, the IRT leader must inform senior management of the situation provide an initial assessment and outline the potential impact.

During a security incident, the IRT should provide regular status updates on the development of the incident to all relevant departments in the client organisation. To ensure that sensitive information is protected, these updates must be communicated through secure channels such as encrypted emails (Voigt, 2018). In addition, the IRT should document all communications and actions taken during the incident for accountability and future reference.

Following a security incident, IRT is required to notify relevant regulators (e.g. financial regulators) and provide detailed information about the incident and the response actions being taken. The IRT must also transparently communicate with customers and partners if the incident affects the financial institution's customer data or services (Voigt, 2018). Communication includes but is not limited to providing information about the incident and possible impacts, as well as information about mitigation measures being implemented.

Client organisations can benefit from these practices because immediate notification and regular updates allow IRT to quickly respond to incidents, thereby mitigating losses.

Meanwhile, transparent communication with customers and regulators helps to maintain trust and ensure compliance with legal obligations. Documenting communications and actions ensures accountability and provides a valuable record for post-incident analysis.

5.4.2 After Security Incidents

Following a security incident, IRTs must write a complete incident report that details when the issue happened, what measures were taken, the underlying cause, the effect, and the remedial processes (Cichonski et al., 2012). Senior management receives an executive summary of the incident report, which highlights significant findings and suggestions. A complete report is sent to the regulator when needed to verify that reporting responsibilities are satisfied.

Holding post-accident review sessions is also needed. A debriefing session is arranged for all IRT members and important stakeholders to examine the event, the efficacy of the response, and the lessons learned. Lessons learned are documented, and incident response plans, policies, and procedures are revised depending on the information gathered (Cichonski et al., 2012).

Both during and after the occurrence, post-incident communication with impacted consumers is required to explain the incident and the steps taken to prevent future problems. If the incident has a substantial impact on the public, issue a public statement or news release to assuage worries and demonstrate the organization's dedication to safety.

If client organizations implement the recommended measures promptly, they can reduce the negative effects of security incidents. Thorough documentation creates a detailed account of events and responses, aiding internal reviews and regulatory adherence. Based on this, post-incident analyses and learning sessions enhance incident response strategies. Additionally, transparent communication with customers post-incident sustains their trust in the organization's dedication to security.

Contribution Table

Sections	Contributors
Application Security	Ilce Andrea Aquino
Container Security	Fengquan Jiang
Vulnerability Management Policy	Xijiu Wang, Yuanchen Shi
Regulations and Compliances	Weiran Wang
Incident Response Policy	Ziyuan Jing

References

Adhikari, S., & Baidya, S. (2024). Cyber Security in Containerization Platforms: A Comparative Study of Security Challenges, Measures and Best Practices. *arXiv preprint arXiv:2404.18082*.

Ande, C. (2024, May 1). *Understanding Vulnerabilities and Configuration issues*. Www.linkedin.com. https://www.linkedin.com/pulse/understanding-vulnerabilities-configuration-issues-chandrashekar-ande-6sa3c/

Andress, J. (2016). *Incident Response Process - an overview | ScienceDirect Topics*. Sciencedirect.com. https://www.sciencedirect.com/topics/computer-science/incident-response-process

Art. 5 GDPR – Principles relating to processing of personal data - General Data Protection Regulation (GDPR). (2021, October 22). General Data Protection Regulation (GDPR). https://gdpr-info.eu/art-5-gdpr/

Atlassian. (2022). *Understanding incident response roles and responsibilities*. Atlassian. https://www.atlassian.com/incident-management/incident-response/roles-responsibilities

Australian Government. (2023). *Essential Eight Assessment Process Guide | Cyber.gov.au*. Cyber.gov.au. https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-assessment-process-guide

Australian Signals Directorate. (2023). Guidelines for Cryptography | Cyber.gov.au. Cyber.gov.au. https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-cryptography

AWS. (2024). *Containment - AWS Security Incident Response Guide*. Docs.aws.amazon.com. https://docs.aws.amazon.com/whitepapers/latest/aws-security-incident-response-guide/containment.html

barclayn. (2023a, October 23). *Plan a Privileged Identity Management deployment - Microsoft Entra ID Governance*. Learn.microsoft.com. https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-deployment-plan

barclayn. (2023b, October 27). *What is Privileged Identity Management?* Learn.microsoft.com. https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-configure

Bluevoyant. (2023). *What is Incident Response? Process, Frameworks, and Tools*. BlueVoyant. https://www.bluevoyant.com/knowledge-center/what-is-incident-response-process-frameworks-and-tools

Brunell, R. (2023, August 23). *Cybersecurity Validation: Ensuring Safety in a Digital World*. Www.linkedin.com. https://www.linkedin.com/pulse/cybersecurity-validation-ensuring-safety-digital-world-ray-brunell/

Casalicchio, E., & Iannucci, S. (2020). The state-of-the-art in container technologies: Application, orchestration and security. *Concurrency and Computation: Practice and Experience*, *32*(17), e5668. *CHAPTER 3: Secure Design - Alice and Bob Learn Application Security [Book]*. (n.d.). Www.oreilly.com. Retrieved May 20, 2024, from https://learning.oreilly.com/library/view/alice-and-bob/9781119687351/c03.xhtml#c03-head-0002

Checkmarx. (2024, May 6). *SAST Scan: Source code vulnerability scanner - Checkmarx.com*. Checkmarx.com. https://checkmarx.com/cxsast-source-code-scanning/

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide. *Computer Security Incident Handling Guide*, *2*(2). https://doi.org/10.6028/nist.sp.800-61r2

Cloud Migration Security. (n.d.). Sysdig. https://sysdig.com/learn-cloud-native/cloud-security/cloud-migration-security/

CSA. (n.d.). CSA. https://cloudsecurityalliance.org/research/cloud-controls-matrix

CVE Details. (n.d.). *EPSS score history*. CVE Details. Retrieved May 25, 2024, from https://www.cvedetails.com/epss/epss-score-history.html?delta=110

CVE Details. (n.d.). *The ultimate security vulnerability datasource*. CVE Details. Retrieved May 25, 2024, from https://www.cvedetails.com/

Dotson, C. (n.d.-b). Practical Cloud Security. O'Reilly Online Learning. https://learning.oreilly.com/library/view/practical-cloud-security/9781098148164/ch06.html#id121

Error Handling and Logging Checklist. (n.d.). IANS. https://www.iansresearch.com/resources/all-blogs/post/security-blog/2023/08/17/error-handling-and-logging-checklist

Federal Register of Legislation. (2022, November 14). Privacy Act 1988. Www.legislation.gov.au; scheme=AGLSTERMS.AglsAgent; corporateName=Office Parliamentary Counsel; address=Locked Bag 30 Kingston ACT 2604; contact=+61 2 6120 1400. https://www.legislation.gov.au/C2004A03712/2022-11-14/text

FRSecure. (n.d.). *Vulnerability management policy template*. FRSecure. Retrieved May 25, 2024, from https://frsecure.com/vulnerability-management-policy-template/

Guidelines for Software Development | Cyber.gov.au. (2023). Cyber.gov.au. https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-software-development

halkazwini. (2023, September 15). *Azure Network Watcher overview*. Learn.microsoft.com. https://learn.microsoft.com/en-us/azure/network-watcher/network-watcher-overview

Hannan, E., & Burton, A. (2023). *What is data recovery? - Definition from WhatIs.com*. SearchDisasterRecovery. https://www.techtarget.com/searchdisasterrecovery/definition/data-recovery

ICO. (n.d.). *Principle (a): Lawfulness, fairness and transparency*. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/lawfulness-fairness-and-transparency/

intel. (2024). *What Is Patch Management? Benefits and Best Practices*. Intel. https://www.intel.com/content/www/us/en/business/enterprise-computers/resources/patch-management.html

Intersoft Consulting. (2018). *General data protection regulation (GDPR)*. General Data Protection Regulation (GDPR). https://gdpr-info.eu/

Introducing DAST scanning in the Cloud, with Burp Suite Enterprise Edition. (2024, April 18). PortSwigger Blog. https://portswigger.net/blog/introducing-dast-scanning-in-the-cloud-with-burp-suite-enterprise-edition

Irvine, C. E., Thompson, M. F., & Khosalim, J. (2017). Labtainers: a framework for parameterized cybersecurity labs using containers.

ISO/IEC 27017:2015. (n.d.). ISO. https://www.iso.org/standard/43757.html

ISO/IEC 27017 Security controls for cloud services. (n.d.). BSI Australia. https://www.bsigroup.com/en-AU/ISOIEC-27017-Security-controls-for-cloud-services-/

Iso.org. (2024). https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27034:-1:ed-1:v1:en

Janca, T. (n.d.). *Alice and Bob learn application security*. O'Reilly Online Learning. https://learning.oreilly.com/library/view/alice-and-bob/9781119687351/c01.xhtml#head-2-27

Jones, A. (2020, May 1). *What does a Tech Lead do?* Www.linkedin.com. https://www.linkedin.com/pulse/what-does-tech-lead-do-andrew-jones/

Kime, C. (2021). 13 Best Vulnerability Scanner Tools of 2021 | eSecurity Planet. [online] eSecurityPlanet. Available at: https://www.esecurityplanet.com/networks/vulnerability-scanning-tools/.

Li, J. (2020). Vulnerabilities Mapping based on OWASP-SANS: A Survey for Static Application Security Testing (SAST). *Annals of Emerging Technologies in Computing*, *4*(3), 1–8. https://doi.org/10.33166/aetic.2020.03.001

Microsoft. (2022, August 25). Threats - Microsoft Threat Modeling Tool - Azure. Learn.microsoft.com. https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats

Microsoft. (2024). *What is Privileged Access Management (PAM) | Microsoft Security*. Www.microsoft.com. https://www.microsoft.com/en-au/security/business/security-101/what-is-privileged-access-management-pam

Mohan, G. (n.d.). *Full stack testing*. O'Reilly Online Learning. https://learning.oreilly.com/library/view/full-stack-testing/9781098108120/ch07.html

Morales, C. (2023, December 19). *What is Network Forensic and why it is important*. Ip2location. https://medium.com/ip2location/what-is-network-forensic-and-why-it-is-important-3e2c0a8328a8

mzorich. (2021, July 26). *Enforce PIM compliance with Azure Sentinel and Playbooks*. Microsoft Sentinel 101.

https://learnsentinel.blog/2021/07/26/enforce-pim-compliance-with-azure-sentinel-and-playbooks/

Nearsure. (2023, November 24). *What's in a Tech Lead's Skills Kit?* Www.linkedin.com. https://www.linkedin.com/pulse/whats-tech-leads-skills-kit-nearsure-jr5of/

Nur, S. (2023, September 4). *Incident Response Framework's Second Phase: Understanding Identification & Scoping*. Medium. https://snynr.medium.com/incident-response-frameworks-second-phase-understanding-identification-scoping-22cc91ea98ce

OAIC. (2024, February 22). *Notifiable Data Breaches Report: July to December 2023*. OAIC. https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-report-july-to-december-2023

OWASP. (2024a). *Access Control for Software Security | OWASP Foundation*. Owasp.org. https://owasp.org/www-community/Access_Control

OWASP. (2024b). *Logging - OWASP Cheat Sheet Series*. Cheatsheetseries.owasp.org. https://cheatsheetseries.owasp.org/cheatsheets/Logging_Cheat_Sheet.html

OWASP ZAP – Getting Started. (n.d.). Www.zaproxy.org. https://www.zaproxy.org/getting-started/

PCI Security Standards Council, LLC. (2022). Payment Card Industry Data Security Standard: Requirements and testing Procedures. In *Payment Card Industry Data Security Standard: Requirements and Testing Procedures*.

PurpleSec. (n.d.). *Vulnerability remediation*. PurpleSec. Retrieved May 25, 2024, from [https://purplesec.us/learn/vulnerability-remediation)

Rais, R., Morillo, C., Gilman, E., & Barth, D. (n.d.-b). Zero Trust Networks, 2nd Edition. O'Reilly Online Learning. https://learning.oreilly.com/library/view/zero-trust-networks/9781492096580/ch08.html#mutually_authenticated_tls_left_parenth

Raza, A., Hasib, M., & Alvi, S. (2020). Towards the use of containerization technology to educate the cybersecurity engineers of tomorrow. EDULEARN20 Proceedings

rboucher. (2024, May 2). *Azure Monitor overview - Azure Monitor*. Learn.microsoft.com. https://learn.microsoft.com/en-us/azure/azure-monitor/overview

Refactoring, Redesigning, and Rebuilding Applications - Migrating Applications to the Cloud [Book]. (n.d.). Www.oreilly.com. Retrieved May 26, 2024, from https://learning.oreilly.com/library/view/migrating-applications-to/9781098102807/ch05.html

Rodrigues, J. (2022, October 3). *7 Phases of Incident Response*. TitanFile. https://www.titanfile.com/blog/phases-of-incident-response/

SAST Testing, Code Security & Analysis Tools | SonarQube. (n.d.). Www.sonarsource.com. Retrieved May 25, 2024, from https://www.sonarsource.com/solutions/security/?_gl=1

Security Assessment for Digital Wallet Payment Partner Applications using the OWASP Method: A Case Study in Indonesia. (2024). *Journal of System and Management Sciences*, *14*(3). https://doi.org/10.33168/jsms.2024.0319

Shahriar, H., Qian, K., & Zhang, H. (2020). Learning Environment Containerization of Machine Leaning for Cybersecurity. 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC),

The Top 10 Static Application Security Testing (SAST) Tools. (2023, October 2). Expert Insights. https://expertinsights.com/insights/the-top-static-application-security-testing-sast-tools/

Thompson, E. C. (2018). *Cybersecurity Incident Response : how to contain, eradicate, and recover from incidents*. New York Apress.

Voigt, L. (2018, September 29). *6 Incident Response Steps to Take After a Security Event*. Exabeam. https://www.exabeam.com/incident-response/steps/

What is Application Migration? | Microsoft Azure. (n.d.). Azure.microsoft.com. Retrieved May 20, 2024, from https://azure.microsoft.com/en-ca/resources/cloud-computing-dictionary/what-is-application-migration

Wikipedia contributors. (2024d, April 23). *ISO/IEC 27018*. Wikipedia. https://en.wikipedia.org/wiki/ISO/IEC_27018

WSTG - Stable | OWASP Foundation. (n.d.). https://owasp.org/www-project-web-security-testing-guide/stable/2-Introduction/README#Testing-Techniques-Explained

www.ibm.com. (2024). What is Security Information and Event Management (SIEM)?| IBM| IBM. [online] Available at: https://www.ibm.com/cn-zh/topics/siem.

Yadav, D. (2023, January 24). *The Importance of Communication in Major Incident Management*. Www.linkedin.com. https://www.linkedin.com/pulse/importance-communication-major-incident-management-deepak-yadav/

Yücel, Ç., Koltuksuz, A., Ödemiş, M., Kademi, A. M. a., & Özbilgin, G. (2018). A programmable threat intelligence framework for containerized clouds. International Conference on Cyber Warfare and Security

Zhang, H. (2021). Learning Environment Containerization of Machine Learning for Cybersecurity.

Zhang, Z. (Justin), He, W., Li, W., & Abdous, M. (2021). Cybersecurity awareness training programs: a cost–benefit analysis framework. *Industrial Management & Data Systems*, *121*(3). https://doi.org/10.1108/imds-08-2020-0462

Zurro, P. (n.d.). Top 13 Vulnerability Scanners for Cybersecurity Professionals | Core Security Blog. [online] www.coresecurity.com. Available at: https://www.coresecurity.com/blog/top-14-vulnerability-scanners-cybersecurity-professionals.