UTM
UNIVERSITI TEKNOLOGI MALAYSIA

School of Professional and Continuing Education (SPACE)

DEPARTMENT OF COMPUTER SCIENCE & SERVICES

CENTRE FOR DIPLOMA STUDIES, SPACE

DDWD 3343

COMPUTER SECURITY

PROJECT REPORT

LECTURER NAME

MISS SITI FATIMAAH BTE MOHAMAD AYOP

SECTION 38

STUDENT NAME & MATRIC ID

DAYANG NUR NAZIHAH BINTI M ROSLAN
A22DW0255

NURALISYA AZWA BINTI ZAITOL ADHAR
A22DW0715

NUR FATIHAH BINTI MOHAMAD
A22DW1249

MUHAMMAD HAFIZ BIN MOHD HATTA
A22DW1967

Table of Contents

1.0 Introduction

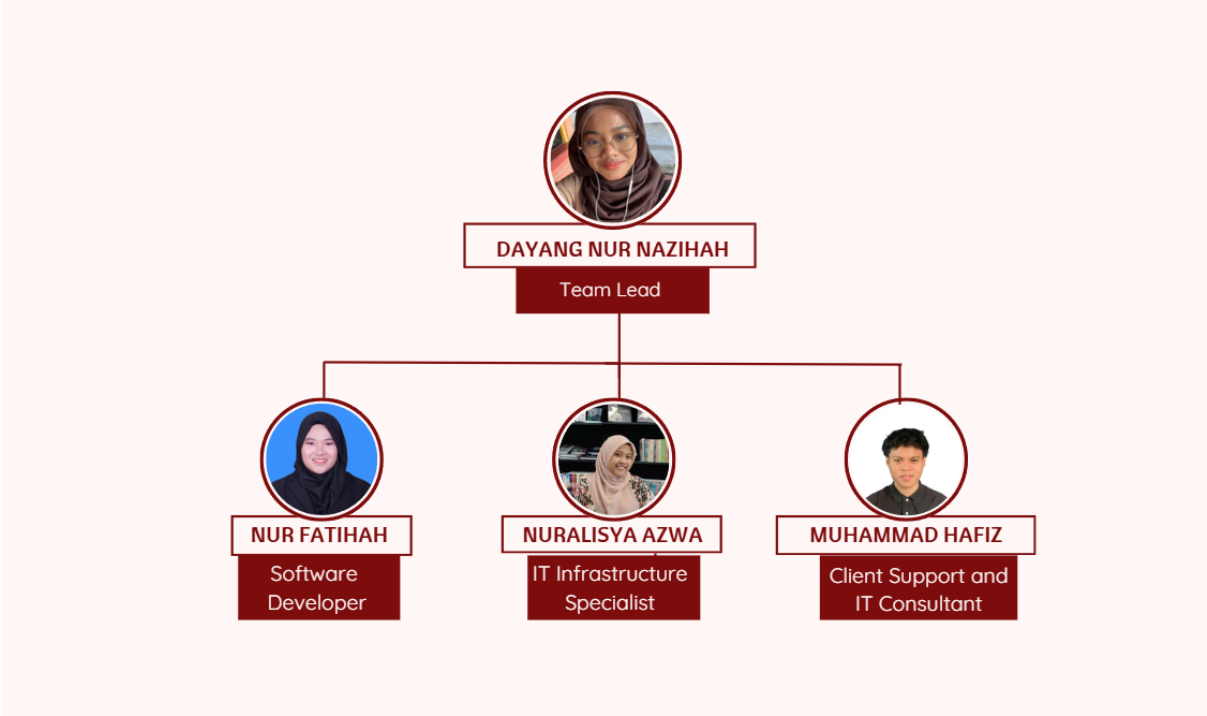
In today's business environment, technology is essential for enabling companies to improve productivity, maintain secure communication channels, and enhance operational efficiency. InnovateIT Solutions is an IT services provider focused on delivering comprehensive technology solutions tailored to meet the diverse needs of modern businesses. This report outlines InnovateIT's services, organizational structure, and network infrastructure capabilities, emphasizing its role in helping clients leverage technology for business growth and transformation.

1.1 Company Background

InnovateIT Solutions was founded in 2015 with a vision to empower businesses through high-quality IT solutions that adapt to the evolving technology landscape. Headquartered in Chicago, Illinois, InnovateIT has grown from a small startup into a trusted IT services provider for over 500 businesses across North America and Europe. The company's core mission is to simplify technology for businesses, allowing them to focus on their primary goals without being bogged down by IT complexities.

InnovateIT caters to a wide range of industries, including finance, healthcare, retail, and education. The company's offerings are structured to meet the demands of both small and medium-sized enterprises (SMEs) as well as large corporations. By delivering tailored solutions, InnovateIT aims to enhance clients' operational efficiency, reduce IT costs, and improve security and scalability. The company places a strong emphasis on innovation, incorporating the latest advancements in cloud computing, automation, and software development to deliver state-of-the-art services. InnovateIT is committed to a customer-centric approach, with 24/7 support and dedicated account managers for each client.

1.2 Company Organization



1. **Team Lead / Project Manager:**

This member oversees the company's projects, ensuring they are completed on time and meet client expectations. The Team Lead is responsible for coordinating tasks among team members, managing client communication, and overseeing the overall direction and strategy of InnovateIT Solutions. They play a crucial role in aligning the team's efforts with client needs and company goals.

2. **IT Infrastructure Specialist:**

The IT Infrastructure Specialist handles the network infrastructure setup, maintenance, and troubleshooting for client projects. They are responsible for configuring networks, installing hardware, and implementing essential security measures to ensure reliable and secure network performance. This specialist also assists clients with any infrastructure-related issues, providing support for smooth IT operations.

3. **Software Developer:**

The Software Developer is in charge of creating custom software solutions tailored to client requirements. They develop applications, manage software updates, and ensure the functionality and security of software systems. This role is vital for clients needing specialized tools or custom applications to enhance their operations.

4. **Client Support and IT Consultant:**

This team member serves as the primary point of contact for client support and consultations. They assist clients with technology adoption, provide guidance on best practices, and address any technical inquiries. They also work with clients to identify specific IT needs and recommend solutions that align with the client's business goals.

2.0 Company Specification

2.1 Company Feature Specification

CyberGuard's main product offerings include firewalls, intrusion detection systems (IDS), secure email solutions, and asset protection services.

2.1.1 Company Assset

InnovateIT Solutions' assets include its **proprietary software tools**, **cloud infrastructure**, **network management systems**, and skilled technical workforce. These assets allow the company to deliver a comprehensive range of IT services to its clients, including cloud management, software development, and managed IT support.

- **Software Tools:** Proprietary tools used to monitor client networks and perform automated maintenance tasks.
- **Cloud Infrastructure:** Servers and data centers used to host client applications and data.
- **Technical Workforce:** Highly trained IT professionals responsible for designing, implementing, and supporting technology solutions.

2.1.2 Asset Threat

The main threats to InnovateIT's assets include data loss, downtime, hardware failure, software bugs, and client system vulnerabilities. These threats could disrupt service delivery, impact client satisfaction, and lead to financial and reputational damage.

- **Data Loss**: Loss of critical client or company data due to accidental deletion, hardware failure, or mismanagement.
- **Downtime:** Unplanned outages due to equipment failure or external factors, impacting service availability.

- **Hardware Failure:** Malfunctions in servers or networking equipment that can disrupt client services.
- **Software Bugs:** Undiscovered flaws in proprietary software tools or third-party systems used in service delivery.
- **Client Vulnerabilities:** Security vulnerabilities in client systems that may affect their IT environment's stability.

2.1.3 Threat Agent

The primary threat agents include hardware malfunctions, software glitches, human error, and natural disasters. InnovateIT also faces potential issues from third-party software vendors whose systems are integrated into the company's services.

- **Hardware Malfunctions:** Issues like server overheating, power surges, and component wear that can disrupt services.
- **Software Glitches:** Errors or bugs in proprietary software or third-party tools that cause performance issues or outages.
- **Human Error:** Mistakes made by InnovateIT employees or client personnel, such as incorrect configurations or data mismanagement.
- **Natural Disasters:** Events like floods or power outages that can cause extended downtime for InnovateIT's systems and client data centers.
- **Third-Party Vendors**: Issues with vendor systems, including software or hardware, that may cause disruptions in InnovateIT's service offerings.

2.1.4 Control RIsk

InnovateIT implements a variety of risk controls to minimize the impact of these threats:

- **Data Redundancy:** Regular data backups and redundancy protocols ensure client data is preserved, even in the case of system failures.
- **Routine Maintenance and Updates:** Regularly scheduled maintenance and software updates to ensure systems are optimized and secure.
- **Disaster Recovery Plans:** A comprehensive disaster recovery plan that includes remote backups, data center failovers, and emergency response protocols.
- **Employee Training:** Continuous training on best practices, including system configuration, client data management, and software updates, to reduce human errors.

- **Vendor Management:** Regular audits and performance checks with third-party vendors to ensure their systems align with InnovateIT's service requirements.

2.1.5 Residual Uncontrol Risk

Despite these control measures, some residual risks remain, which cannot be fully mitigated:

- **Unexpected Server Failures:** Even with routine maintenance, unforeseen hardware issues may cause temporary downtime.
- **Data Corruption:** There is always a small risk of data corruption or loss, despite backup measures.
- **Third-Party Dependency Risks:** Issues with third-party vendors, such as delayed updates or unexpected service disruptions, may impact service delivery.
- **Natural Disaster Impact:** Although disaster recovery plans are in place, extreme events could disrupt services for extended periods.
- **Evolving Technology Risks:** As technology changes, there may be unknown risks or vulnerabilities that cannot be predicted with current control measures.

2.2 Intrusion Detection System (IDS)

InnovateIT offers Intrusion Detection Systems (IDS) that keep an eye on system and network activity in order to protect network integrity and stop unwanted access. These intrusion detection systems are set up to spot questionable activity and notify IT departments of any security breaches. Clients in sectors where data protection and regulatory compliance are crucial, like finance and healthcare, will find the IDS products especially beneficial.

2.2.1 NIDS

InnovateIT's NIDS solutions monitor all incoming and outgoing network traffic. By analyzing patterns and recognizing anomalies, the NIDS identifies potential security threats, such as abnormal access attempts or unexpected traffic patterns. The system immediately sends alerts to InnovateIT's support team, enabling a rapid response to prevent potential breaches.

2.2.2 HIDS

As an extra security measure for individual customer servers and workstations, InnovateIT provides HIDS. Unusual system behavior or unauthorized file alterations are examples of suspicious changes or unauthorized access at the host level that the HIDS is set up to identify. Because it offers better insight into certain host behaviors, this technology is crucial for clients who handle sensitive data.

2.2.3 System IDS

Combining NIDS and HIDS into a single, integrated platform, the System IDS offers a complete solution. A centralized security monitoring system that can be tailored to each client's specific security needs is made possible by InnovateIT's comprehensive IDS approach. The System IDS makes it possible to detect threats more precisely and react to any incidents more quickly by comparing data from the host and network systems.

2.3 Firewall

A firewall is a security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. Firewalls serve as the first line of defense, creating a barrier between secure internal networks and untrusted external networks like the internet. They help prevent unauthorized access, detect potential threats, and safeguard sensitive data, making them essential for maintaining network security and stability.

2.3.1 Packet firewall

A Packet Firewall (also known as a packet-filtering firewall) operates at the network layer, where it inspects individual packets of data based on specified rules such as source and destination IP addresses, ports, and protocols. It allows or blocks packets solely based on these criteria without inspecting the actual data content within each packet. While packet firewalls are efficient and easy to implement, they offer basic security and are often combined with other firewall types for added protection.

Advantages:

- Simple and fast, suitable for high-speed networks.
- Reduces unauthorized access by filtering based on specific rules.

Limitations:

- Doesn’t analyze data content within packets.
- Vulnerable to certain types of attacks, such as IP spoofing.

2.3.2 Hybrid Firewall

A Hybrid Firewall combines the functionalities of multiple firewall types, such as packet filtering, stateful inspection, and application-level filtering, to offer enhanced security and flexibility. Hybrid firewalls are capable of analyzing network packets at multiple levels (network, transport, and application), providing more robust protection against complex threats. They are often used in enterprise networks where high security and performance are both critical.

Advantages:

- Offers comprehensive security by integrating multiple firewall functions.
- Efficiently protects against a variety of sophisticated threats.

Limitations:

- More complex and resource-intensive than other firewall types.
- May require specialized configuration and monitoring.

2.3.3 Application Proxy

An Application Proxy (or proxy firewall) works at the application layer by acting as an intermediary between clients and servers. Instead of direct communication, all requests pass through the proxy, which inspects and filters the content based on security policies. Application proxies are highly effective for blocking malware, phishing attacks, and other threats that target specific applications, as they analyze data at a deeper level.

Advantages:

- High level of control over data requests and responses.
- Prevents direct exposure of internal networks to external traffic.

Limitations:

- Slower than packet firewalls due to deep content inspection.
- More suitable for specific applications and not high-speed network environments.

2.3.4 System Firewall

The System Firewall is a customizable firewall solution that combines packet filtering, stateful inspection, and application proxy capabilities. This firewall is configured to meet InnovateIT's specific needs and is adaptable to different types of network environments. By using the System Firewall, InnovateIT can effectively balance security with performance, enabling efficient traffic flow while providing deep inspection and control over data.

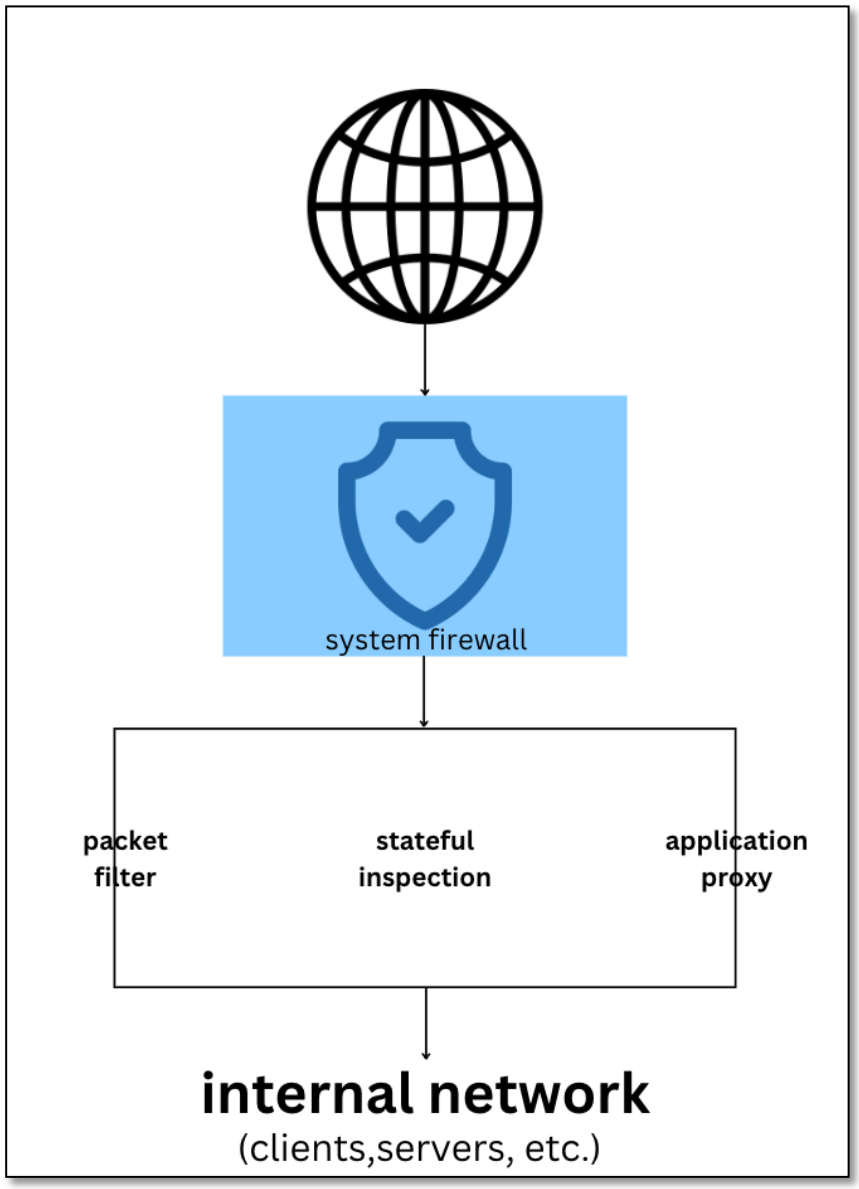


Figure 2.3.4 InnovateIT's System Firewall

The diagram illustrates the InnovateIT System Firewall setup, showcasing its key features for securing network operations. At the top, the Internet connects to the System Firewall, which acts as the first layer

of defense, filtering and inspecting incoming and outgoing traffic. The System Firewall incorporates three primary security mechanisms: Packet Filter, Stateful Inspection, and Application Proxy.

The Packet Filter examines individual data packets based on predefined rules, ensuring only authorized packets enter or leave the network. Stateful Inspection adds another layer of security by monitoring the state and context of active connections, blocking unauthorized attempts. The Application Proxy functions as an intermediary, analyzing and filtering application-level traffic to protect against malicious threats targeting specific software or systems.

All these components work together to safeguard the Internal Network, which consists of clients, servers, and other connected devices, ensuring a secure and efficient flow of data within the organization. This layered approach enhances the system's reliability and security, making it an integral part of InnovateIT's network infrastructure.

How System Firewall Improves InnovateIT's System Features:

- Enhanced Security: The System Firewall combines various filtering methods, providing multi-layered protection against unauthorized access and threats.
- Flexibility and Customization: InnovateIT can customize the firewall settings based on specific client needs and network configurations.
- Increased Performance: The firewall can be optimized to balance speed and security, allowing for smooth data flow while ensuring network safety.
- Centralized Control: With integrated capabilities, InnovateIT can manage and monitor the network from a single platform, making it easier to identify and respond to incidents.

2.4 Secured Email

In today's digital landscape, email remains one of the primary communication channels for businesses. Recognizing the importance of secure email communication, InnovateIT Solutions has implemented a robust mailing feature to protect client communications and ensure data confidentiality. The secure email system at InnovateIT uses encryption and secure protocols to safeguard emails from unauthorized access, interception, and potential breaches. This feature is essential, as clients rely on email not only for daily correspondence but also for transmitting sensitive data, such as financial information, project details, and other confidential business communications.

InnovateIT's mailing system is built with multiple layers of security, including protocol encryption, secure password policies, and regular monitoring for suspicious activity. This secure email infrastructure not only reinforces data protection but also supports regulatory compliance for clients in

industries where data privacy is paramount. The secured email system is integrated with firewalls and anti-spam filters to prevent common email-based threats, such as phishing and malware attacks, thereby maintaining the integrity of email exchanges within the company and with clients.

2.4.1 SMTP

InnovateIT Solutions' secured email system is built on the Simple Mail Transfer Protocol (SMTP), which is the foundation for sending and receiving emails across the network. SMTP facilitates the transfer of emails from the client's server to the recipient's email server in a smooth, efficient process. For InnovateIT, SMTP is configured with enhanced security settings, including Transport Layer Security (TLS) encryption, to ensure that data remains secure during transit.

TLS encryption protects emails from being intercepted by encrypting the data before it leaves the sender's server. Only the intended recipient's server can decrypt the email, significantly reducing the risk of unauthorized access during transmission. In addition, InnovateIT has implemented authentication mechanisms, such as SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail), to validate the origin of the emails sent. These authentication techniques prevent email spoofing, a common method used by attackers to impersonate legitimate contacts. By combining SMTP with these additional security layers, InnovateIT is able to provide a secure email infrastructure that minimizes the risk of interception or unauthorized access during email exchanges.

2.4.2 Secured Email Implementation

The secured email implementation within InnovateIT's system goes beyond basic protocol settings to ensure a comprehensive mechanism that addresses multiple aspects of email security. To achieve this, InnovateIT employs a multi-step mechanism that includes encryption, user authentication, and access control measures. First, emails are encrypted during transmission using TLS, as mentioned above, but they are also encrypted at rest within InnovateIT's servers. This ensures that even if an unauthorized user gains physical access to the server, the stored emails remain protected.

Furthermore, the system mandates multi-factor authentication (MFA) for accessing email accounts. This involves verifying users through multiple steps, such as a password and a one-time passcode sent to a verified device. MFA minimizes the chances of unauthorized access, even if a password is compromised. InnovateIT has also implemented role-based access control (RBAC) within the email system. This means that only authorized employees have access to sensitive email threads, based on their role and necessity within the company. For instance, certain client-related emails might only be

accessible to the project manager and client support team members, ensuring that sensitive data is only accessible to those who need it.

Additionally, the email system includes automated monitoring tools that flag suspicious activity, such as unusual login locations or mass email sending, which could indicate an account compromise. If any suspicious behavior is detected, InnovateIT's system automatically restricts access and prompts the user for further authentication. These layered security measures create a fortified environment for email exchanges, preventing unauthorized access, and ensuring secure client communications.

2.4.3 Mail Threat

Despite the robust security infrastructure, email systems remain a frequent target for cyber threats. InnovateIT Solutions is aware of the possible threats that could impact its email feature and has identified several key risks, along with measures to mitigate them effectively using firewalls and additional controls.

One major threat is phishing, where attackers attempt to deceive users into clicking malicious links or downloading infected attachments. InnovateIT addresses this through advanced anti-phishing filters, which detect and quarantine suspicious emails based on the sender's reputation and the email content. Additionally, the company conducts regular phishing awareness training for employees to help them identify and avoid potential phishing attempts. Another common threat is malware distribution via email attachments, which can infect the network and compromise data. InnovateIT's email system integrates with firewall solutions that actively scan incoming and outgoing emails for malware signatures. If a potentially malicious attachment is detected, it is automatically blocked, preventing the threat from reaching the recipient.

Another notable risk is business email compromise (BEC), where attackers impersonate high-ranking executives or trusted contacts to deceive employees into transferring sensitive information or funds. InnovateIT has implemented protocols to detect anomalies in communication patterns, which can indicate potential BEC attempts. Through these security measures, including rule-based filtering and anomaly detection within the firewall, InnovateIT is able to safeguard against BEC threats and protect the company's financial and data assets.

Finally, spam and unsolicited emails pose a risk as they clutter inboxes and occasionally contain malicious links. InnovateIT uses spam filters within its firewall, which analyze email metadata and keywords to prevent spam from reaching users' inboxes. This proactive approach to email security ensures that potential threats are identified and neutralized before they can harm the system or disrupt client communication.

3.0 Reflection

3.1 Reflection 1

Name: Dayang Nur Nazihah Binti M Roslan

The session really made me think about how important it is for all of us to take responsibility for cybersecurity. Simple things like using strong passwords, being careful with what we click on, and turning on two-factor authentication can make a huge difference in keeping us safe online. As students, we're always using digital platforms, and it's easy to forget how quickly threats can change. This session was a great reminder to stay updated and make smart choices online. By doing our part, we're not just protecting ourselves—we're helping create a safer digital space for everyone around us.

3.2 Reflection 2

Name: Nuralisya Azwa Binti Zaitol Adhar

The session underscored that cybersecurity is a shared responsibility, one where each of us plays a role in fostering a safer digital landscape. Small but essential practices such as approaching unfamiliar emails with caution, staying alert for potential scams, and regularly updating our software contribute significantly to our overall security. This talk was a valuable reminder of the increasing importance of cybersecurity, especially as students who are constantly engaging with digital platforms. Recognizing that threats are constantly evolving, it's essential for us to stay informed about the latest digital risks and make proactive adjustments to our habits and knowledge. By doing so, we not only protect ourselves but also contribute to a culture of digital safety that can benefit everyone around us.

3.3 Reflection 3

Name: Nur Fatihah Binti Mohamad

Attending the cybersecurity talk highlighted the importance of vigilance and proactive behavior in maintaining digital safety. I learned that cybersecurity isn't just the responsibility of IT specialists but is something we all play a part in. The talk emphasized simple yet impactful actions we can take to

safeguard our online presence, such as being cautious with unfamiliar emails, using strong passwords, and regularly updating software. These small habits can collectively make a big difference in minimizing risks. As students, we constantly interact with digital platforms, making us more exposed to cyber threats, which continue to evolve and grow more sophisticated. The session served as a reminder of the need to stay informed about new cyber risks and adopt preventive measures. By doing so, we contribute not only to our personal safety but also to a broader culture of cybersecurity. It was a powerful reminder that protecting ourselves online is a shared responsibility that ultimately helps build a more secure digital community for everyone.

3.4 Reflection 4

Name: Muhammad Hafiz Bin Mohd Hatta

Reflecting from talk about computer security highlights the critical importance of cybersecurity awareness, understanding the evolving threat, and implementing structured security policies and procedures. Proactive defense tactics are crucial since attackers are always changing. Security requires striking a balance between usability and strong protection, especially in settings with many users. A watchful, security-conscious culture combined with technical protections creates a multi-layered approach to effective security. Plans for incident reaction and recovery are essential since being ready can reduce the impact of an assault. Lastly, cybersecurity is a lifelong process that needs constant development and adjustment to prevent risks. This reflection emphasizes how important it is for people and organizations to work together to create a safe online environment.

4.0 Conclusion

For businesses aiming to improve and simplify their IT infrastructure, InnovateIT Solutions has shown to be a trustworthy partner. By offering a wide range of services, such as software development, cloud computing, network infrastructure, and managed IT support, InnovativeIT frees up companies to concentrate on expansion while managing and optimizing their technological surroundings.

Integrating Intrusion Detection Systems (IDS), which give customers real-time monitoring and warnings to identify anomalous or illegal activity on their networks, is a crucial part of InnovateIT's services. InnovateIT provides a tiered approach to security by putting in place Network IDS (NIDS) and Host IDS (HIDS), guaranteeing proactive detection and response. Customers greatly benefit from this, particularly in sectors where uptime and data integrity are essential.

InnovateIT's commitment to customization and flexibility allows it to cater to the specific needs of each client, from cloud migration and storage solutions to network management and troubleshooting. Its proactive monitoring and 24/7 support provide clients with peace of mind, knowing their IT infrastructure is both secure and continuously optimized.

Through its reliable IT services, IDS solutions, and a client-centered approach, InnovateIT Solutions helps businesses build resilient, scalable, and secure technology environments. By enabling organizations to harness the power of technology without the associated complexities, InnovateIT positions its clients for success in a rapidly evolving digital landscape.

5.0 References

- https://www.vigilantsoftware.co.uk/blog/risk-terminology-understanding-assets-threats-and-vulnerabilities
- https://www.twingate.com/blog/glossary/threat-agent
- https://www.geeksforgeeks.org/difference-between-hids-and-nids/
- https://www.spanning.com/blog/nids-hids-intrusion-detection-systems/