FY BTech CSF Semester VI

Attack, Reporting and Documentation
Course Code: CSF4042B

Class Continuous Assessment (CCA)
(Active Learning)

PRESENTING TO:

Prof. Milind Bade

PRESENTED BY:

PA04_Nishad Wanjari_1032210680
PA09_Parth Zarekar_1032210846
PA15_Krishnaraj Thadesar_1032210888
PA23_Yashvardhan Tekawade_1032211025
PA29_Gaurav Mukherjee_1032211389

SONY PICTURES ENTERTAINMENT 2014 DATA BREACH

Contents

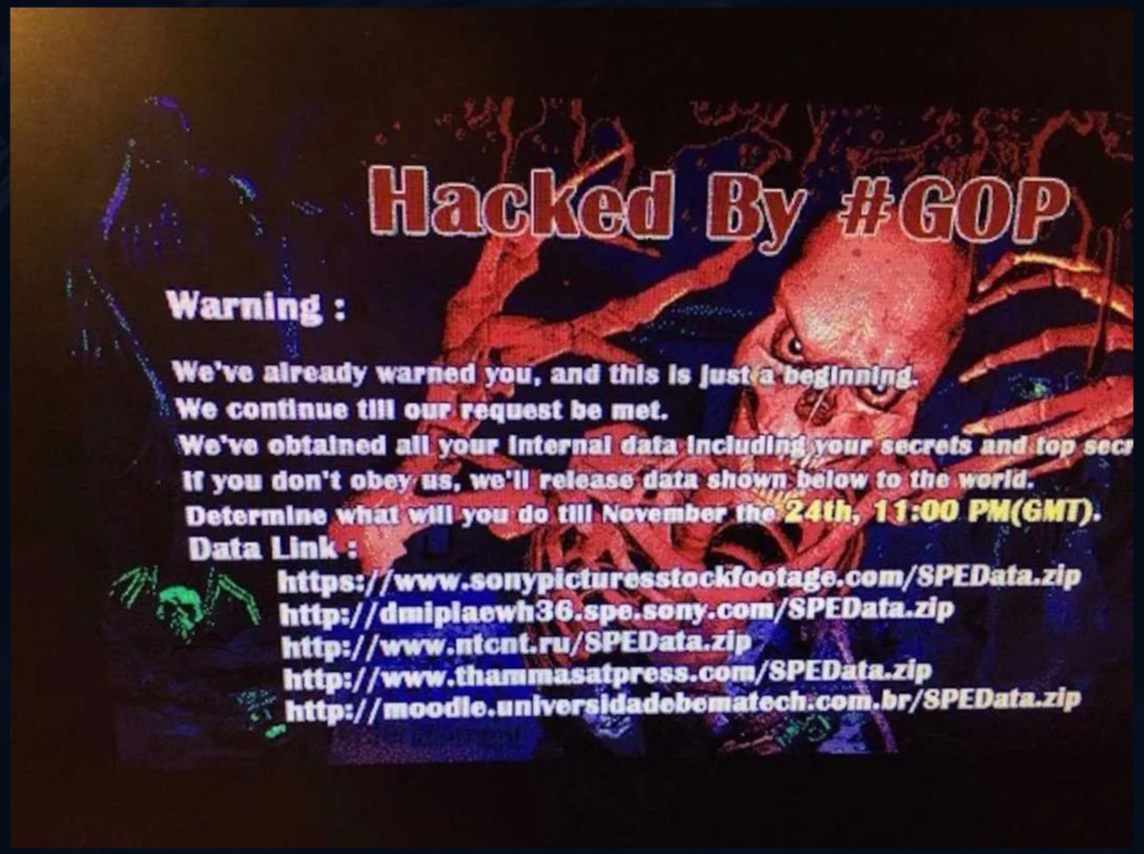
BACKGROUND

KRISHNARAJ

WHO WAS BEHIND THE ATTACK ?

- The attack was attributed to the Lazarus Group, a North Korean state-sponsored hacking group.

- The FBI and cybersecurity experts traced the attack to North Korea, based on malware similarities, IP addresses, and attack patterns.



MOTIVATION BEHIND THE ATTACK

The attack was politically motivated, primarily due to Sony's release of "The Interview", a comedy film depicting the assassination of Kim Jong-un.

IMPACT ON SONY PICTURES ENTERTAINMENT

- Financial Damage: Estimated losses of $35 million in IT infrastructure and recovery costs.
- Operational Disruption: Complete shutdown of Sony's IT systems, forcing employees to use pen and paper for weeks.
- Data Theft (100+ TB of sensitive files leaked):
  Unreleased movies leaked online.
- Confidential employee data, including Social Security Numbers & salaries.
- Internal emails exposed private conversations between executives.
- Reputation Damage:
- Leaked emails caused major controversies, leading to executive resignations.
- Sony's relationships with actors, directors, and studios were affected.
- Threats of Violence:
- Hackers threatened attacks on theaters screening "The Interview".

Many cinema chains refused to show the movie, forcing Sony to cancel its theatrical release.

Loss Type	Cost
Investigation + Remediation	$35 Million
Legal	$8 – 15 Million
Lost revenue (*The Interview*)	$30 Million
Additional film assets write-offs	$82 – 95 Million
Other (Reputational, etc.)	Unknown
Total	**$155 – 175 Million**

From: ODell, Steven
Sent: 17 July 2014 16:52
To: Braddel, Mark; Bruer, Rory; Clark, Nigel; Lear, Sharri; Eipper, Amy; Piersch, Dan; Scott, Leticia; Roy, Ananya
Cc: Harrison, Elizabeth
Subject: RE: **THE INTERVIEW** - TMR REVIEW

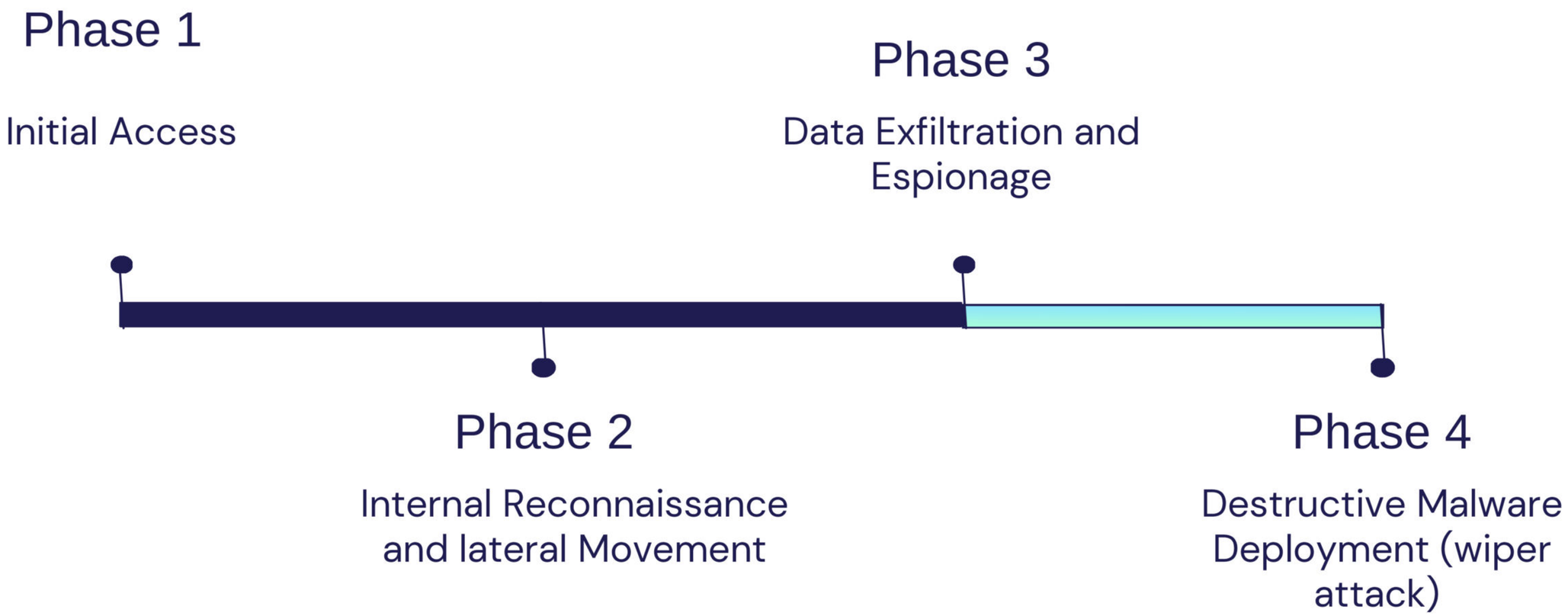
Mark,

Just to confirm, Jeff has given us **the** directive to go ahead and chase a release on all markets where we are confident we will be profitable. For markets which are expected/forecasted to be marginal/breakeven with little chance for upside we will lean towards **the** conservative side and not release.

With this in mind, can you please reconfirm if this changes

ATTACK KILL CHAIN

PA09. PARTH ZAREKAR


Phase 1
Initial Access
Phase 3
Data Exfiltration and Espionage
Phase 2
Internal Reconnaissance and lateral Movement
Phase 4
Destructive Malware Deployment (wiper attack)

PHASE 1: INTIAL ACCESS

- Hackers sent targeted phishing emails to Sony employees.
- Emails contained malicious attachments or links to fake login pages.
- Employees unknowingly entered credentials or executed malware, providing attackers with initial access.

PHASE 2: INTERNAL RECONNAISSANCE AND LATERAL MOVEMENT

Escalated Privileges Using Weak Passwords & Credential Dumping

- Sony's password management was weak—some stored passwords were unencrypted.
- Attackers used brute-force techniques, **Mimikatz** (credential-dumping tool), and pass-the-hash attacks to gain admin access.

Exploited Unpatched Vulnerabilities

- Sony had outdated software and unpatched security flaws.
- Attackers leveraged zero-day exploits and privilege escalation vulnerabilities to gain deeper access.

Lateral Movement Due to Poor Network Segmentation

- Sony's internal network was not properly segmented, allowing attackers to easily navigate across departments.
- Attackers moved from employee workstations to critical IT infrastructure, including file servers and email systems.

Persistence via Backdoor Installation

- Attackers installed custom Remote Access Trojans (RATs) to maintain access.
- Keyloggers and network sniffers were deployed to capture credentials.

PHASE 3: DATA EXFILTRATION

Massive Data Theft (100+ TB of Sensitive Information)

- Attackers exfiltrated movies, emails, HR records, financial data, and unreleased scripts.
- Data was sent to remote servers via encrypted connections to avoid detection.

Use of Encrypted Channels & Stealth Techniques

- Data was compressed, fragmented, and disguised as normal traffic.
- Attackers used Secure Shell (SSH) tunnels and HTTPS traffic to evade firewalls.
- Sony’s lack of anomaly detection allowed exfiltration to go unnoticed.

Leaks on Dark Web & Public Websites

- Stolen information was leaked via file-sharing platforms, dark web forums, and social media.
- This exposed Sony’s internal disputes, salaries, and film contracts, causing reputational damage.

PHASE 4: DESTRUCTIVE MALWARE DEPLOYMENT

Deployment of Destover Malware (Wiper)

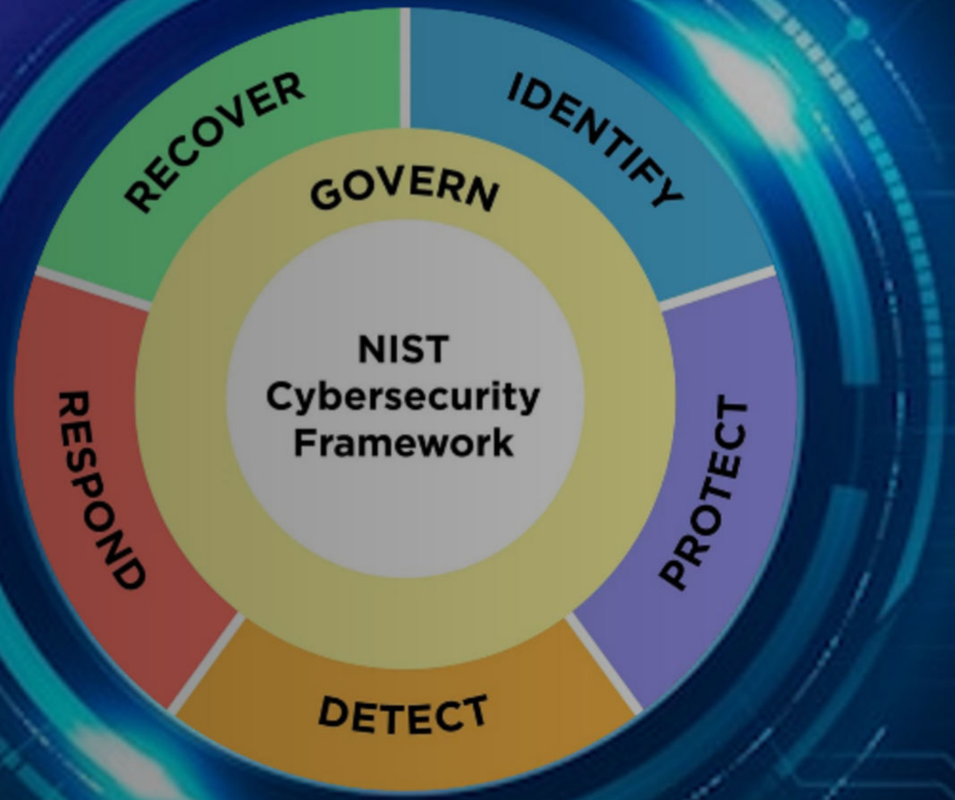
- Attackers deployed Destover, a wiper malware designed to erase system data.
- The malware was programmed to overwrite master boot records (MBRs), making recovery impossible.
- Thousands of computers were rendered inoperable, forcing Sony to shut down.

Use of Backdoor Trojans for Persistent Access

- Trojans were injected into critical Sony servers to allow continued access.
- Attackers could re-infect Sony’s network even if the malware was removed.

Sony had to disconnect its network and rebuild systems from scratch.

- Employees were forced to use pen and paper for weeks, causing severe operational disruptions.



NIST FUNCTION 1 - IDENTIFY

NISHAD

NIST FUNCTION 1 - IDENTIFY

Asset Management

Maintain an inventory of systems, data, and network assets.
Example:

- Implement automated asset discovery tools to track all devices connected to the network.
- Categorize assets based on sensitivity (e.g., confidential files, intellectual property).

Why?

- Sony lacked visibility into its IT infrastructure, making it easier for attackers to move laterally.
- Knowing where critical data resides could have helped apply better security controls.

Risk Management Strategy

Establish a risk management framework to assess cybersecurity threats.
Example:

- Conduct regular risk assessments to identify weak points in the system.
- Implement third-party risk management to vet vendors with network access.

Why?

- Attackers exploited weak third-party security measures to access Sony's network.
- Risk assessments could have flagged vulnerabilities in remote access systems.

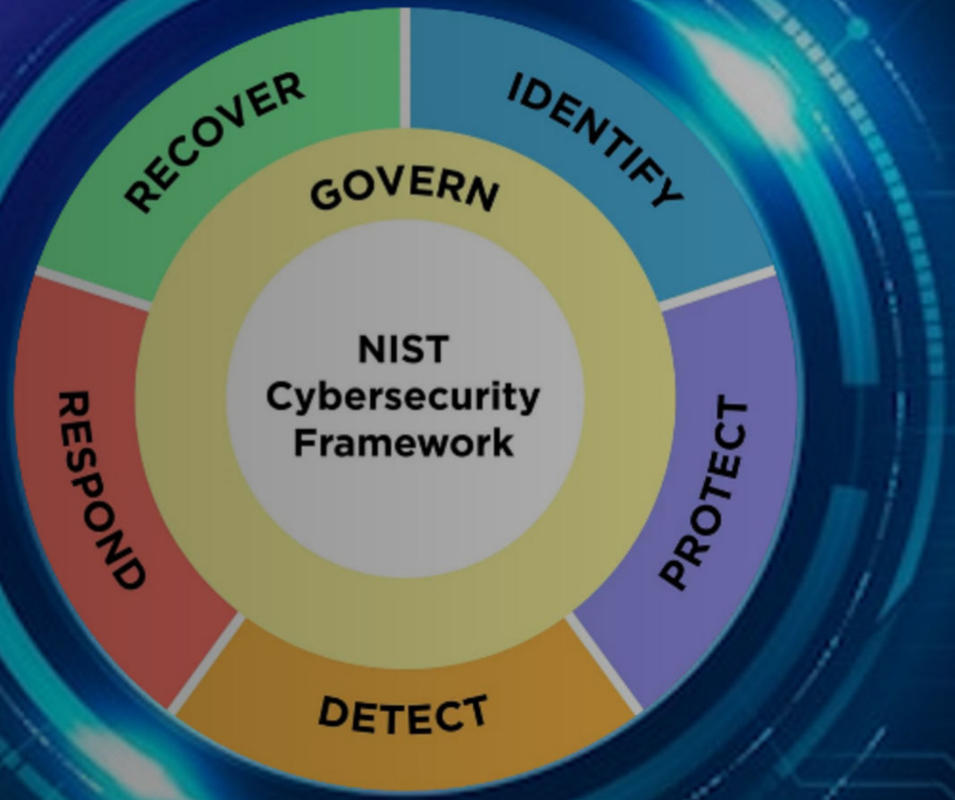
Supply Chain Risk Management

Manage risks related to third-party vendors and external access points.
Example:

- Require vendors to comply with cybersecurity best practices (e.g., MFA, encryption).
- Monitor third-party access logs for suspicious activity.

Why?

- The breach may have originated from a compromised vendor with network access.
- Stronger third-party security policies could have prevented unauthorized entry.



NIST FUNCTION 2 - PROTECT

GAURAV
MUKHERJEE

NIST FUNCTION 2 - PROTECT

Access Control

Ensure only authorized users can access critical systems and data.
Example:

- Implement Multi-Factor Authentication (MFA) to prevent unauthorized logins.
- Enforce least privilege access so employees only access what they need.

Why?

- Hackers used stolen credentials to access Sony's network.
- MFA could have blocked unauthorized access, even with compromised passwords.

Data Security

Protect sensitive data from unauthorized access or theft.
Example:

- Encrypt sensitive files and databases to prevent readable data leaks.
- Deploy Data Loss Prevention (DLP) tools to detect unauthorized data transfers.

Why?

- Sony's unencrypted confidential data was easily stolen and leaked.
- Encryption would have made the stolen files useless to attackers.

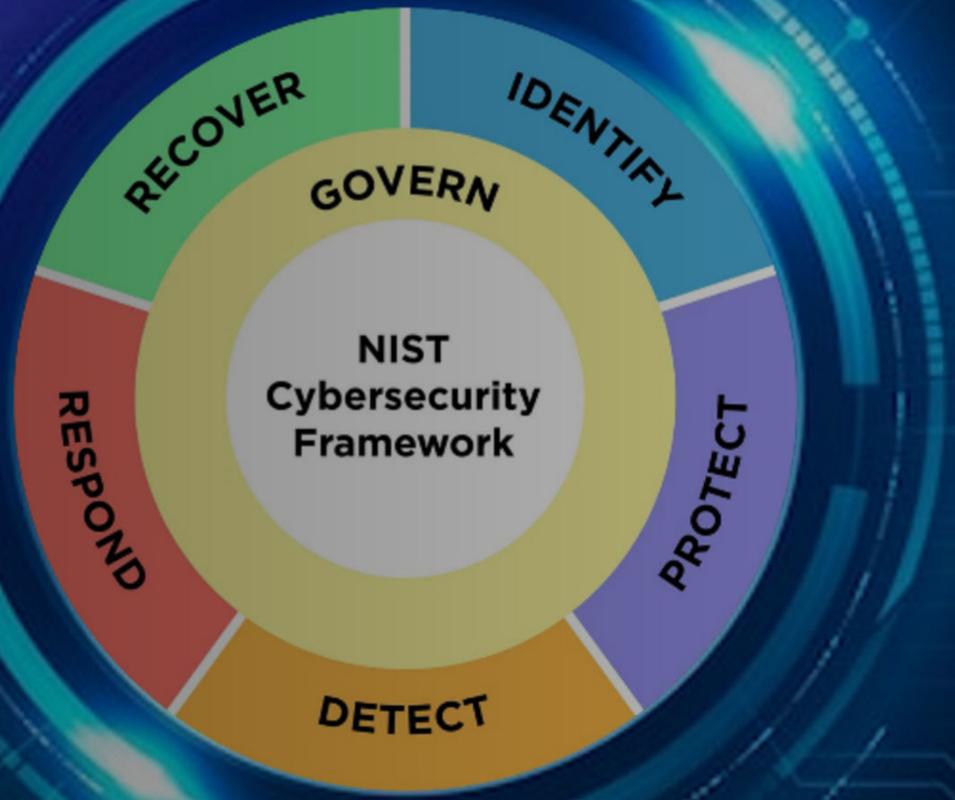
Network Security

Implement safeguards to prevent unauthorized movement within the network.
Example:

- Use network segmentation to isolate critical assets from general systems.
- Deploy Intrusion Prevention Systems (IPS) to detect and block suspicious activity.

Why?

- Attackers moved laterally across Sony's network, accessing multiple systems.
- Segmentation would have contained the attack, limiting damage.



NIST FUNCTION 3 - DETECT

YASH

NIST FUNCTION 3 - DETECT

Anomalous Activity Detection

Detect and analyze unusual system behavior to identify potential threats.
Example:

- Implement User and Entity Behavior Analytics (UEBA) to detect abnormal login patterns.
- Use AI-driven anomaly detection to flag suspicious data access or file movements.

Why?

- Sony lacked behavioral monitoring, allowing attackers to operate undetected for months.
- Early detection of irregular access patterns could have signaled an intrusion attempt.

Continuous Security Monitoring

Implement systems to monitor and respond to real-time threats.
Example:

- Deploy a Security Information and Event Management (SIEM) system for live event correlation.
- Use Intrusion Detection Systems (IDS) to monitor network traffic for malicious activity.

Why?

- Sony had no centralized threat monitoring, making it easy for attackers to escalate their access.
- Real-time threat alerts could have helped IT teams respond before major damage occurred.

Threat Intelligence & Logging

Collect and analyze security logs to detect malicious activities.
Example:

- Enable automated log correlation to identify attack patterns.
- Integrate threat intelligence feeds to detect known attacker signatures.

Why?

- Sony's lack of log analysis allowed attackers to operate undetected.
- Early correlation of attack patterns could have led to quicker incident response.

CONCLUSION

Recommendations:

- Short-Term Actions:
  - Enforce Multi-Factor Authentication (MFA) to prevent credential-based attacks.
  - Implement SIEM for real-time threat monitoring.
  - Restrict third-party access and enforce vendor security audits.
- Long-Term Actions:
  - Adopt a Zero Trust Security Model to prevent unauthorized lateral movement.
  - Conduct regular cybersecurity training for employees to prevent phishing.
  - Implement AI-driven threat detection to identify anomalies in network behavior.

THANK YOU