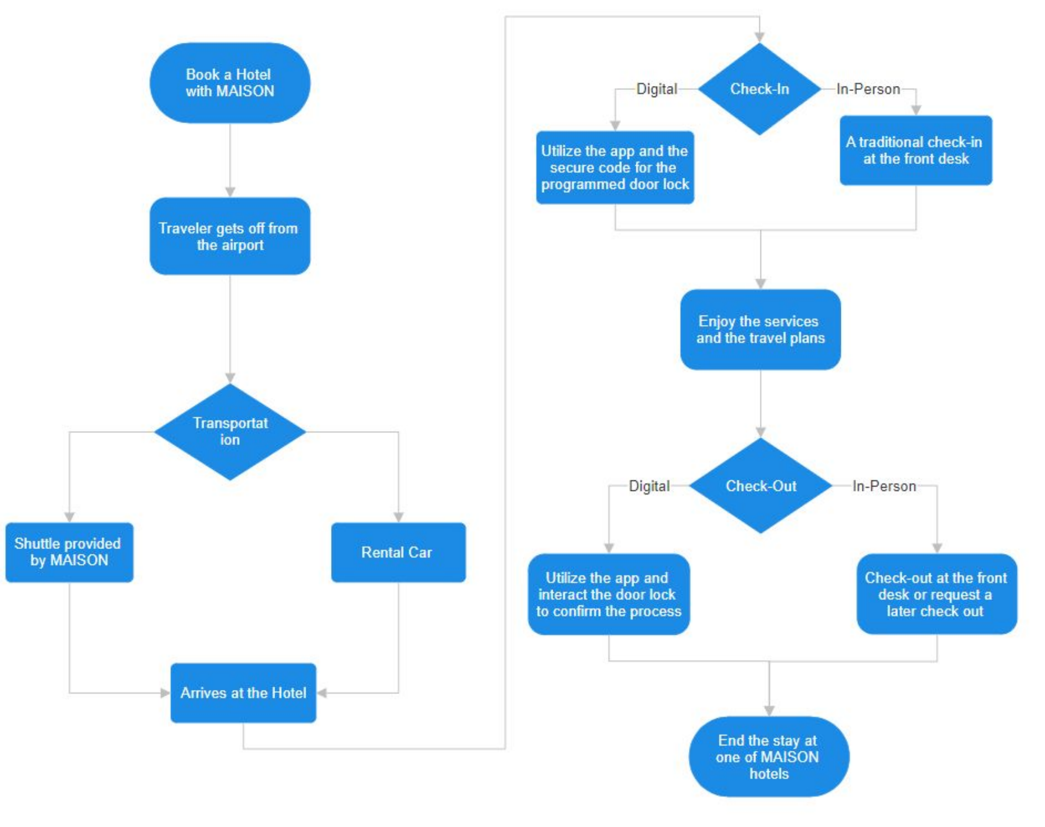
Digital Guest Experience: MAISON

Presented By: Eric Lee

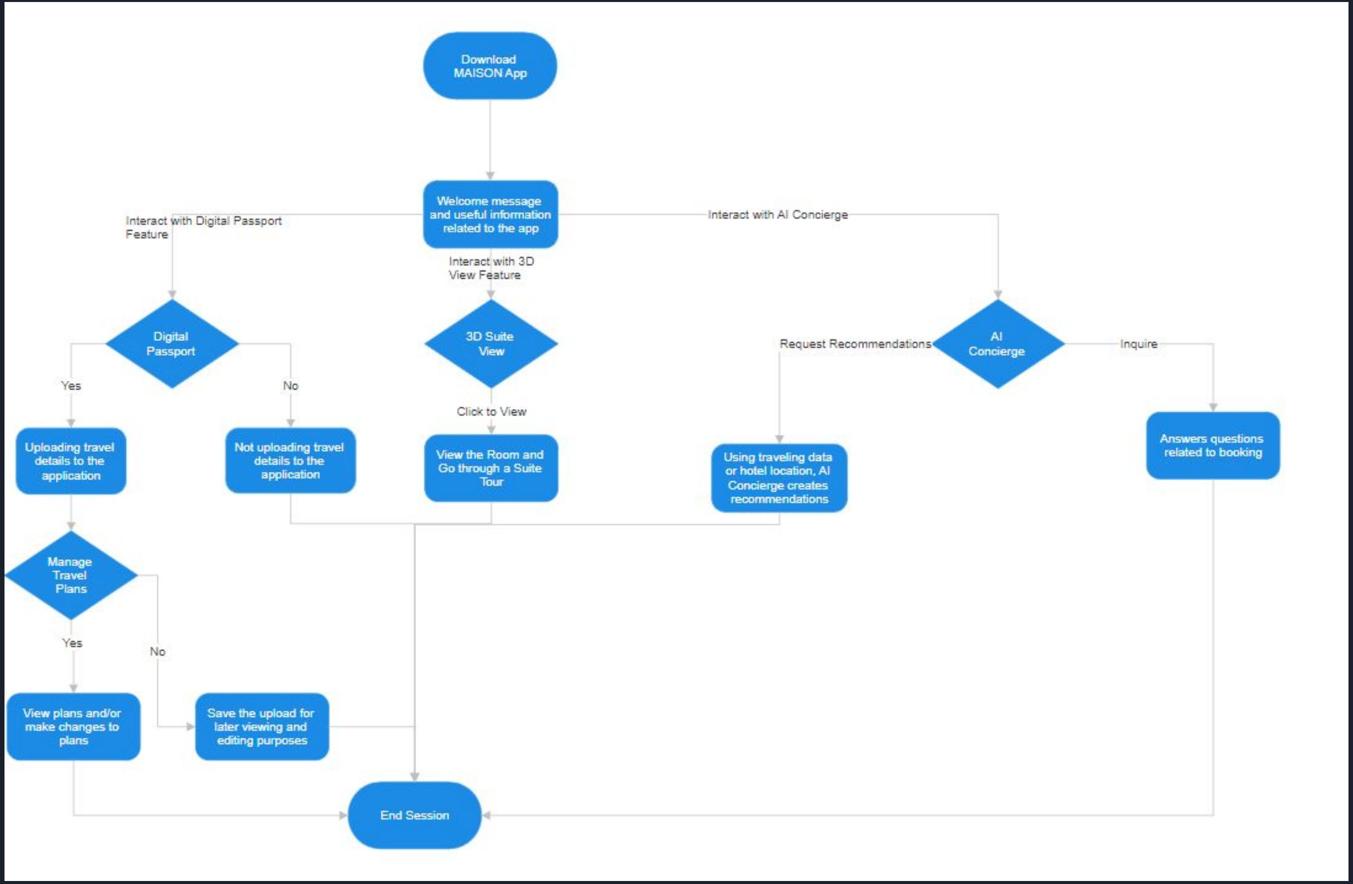
Introduction

- Digital-First Hotel Startup Company
- Key locations across the United States
- Mostly Remote
  - No Dedicated Headquarters
  - Only Staff Members at Physical Locations
  - 300 Corporate Employees Have Remote Access

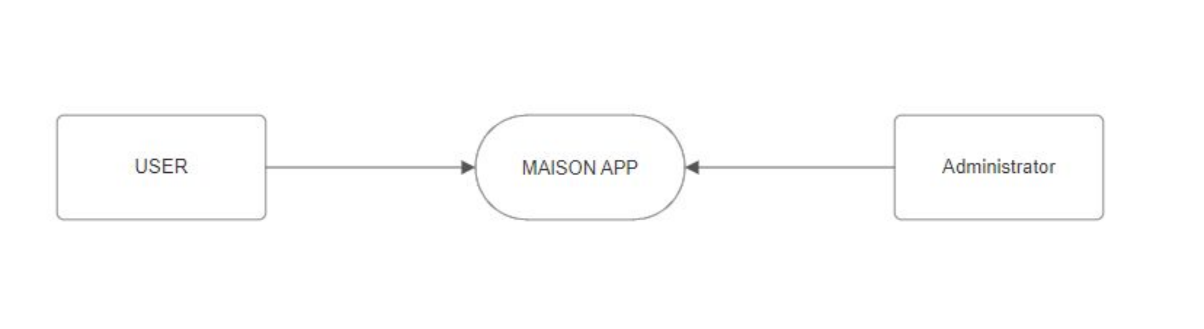
Flow Chart: User Hotel Interaction


Book a Hotel with MAISON
Traveler gets off from the airport
Transportat ion
Shuttle provided by MAISON
Rental Car
Arrives at the Hotel
Check-In
Digital
In-Person
Utilize the app and the secure code for the programmed door lock
A traditional check-in at the front desk
Enjoy the services and the travel plans
Check-Out
Digital
In-Person
Utilize the app and interact the door lock to confirm the process
Check-out at the front desk or request a later check out
End the stay at one of MAISON hotels

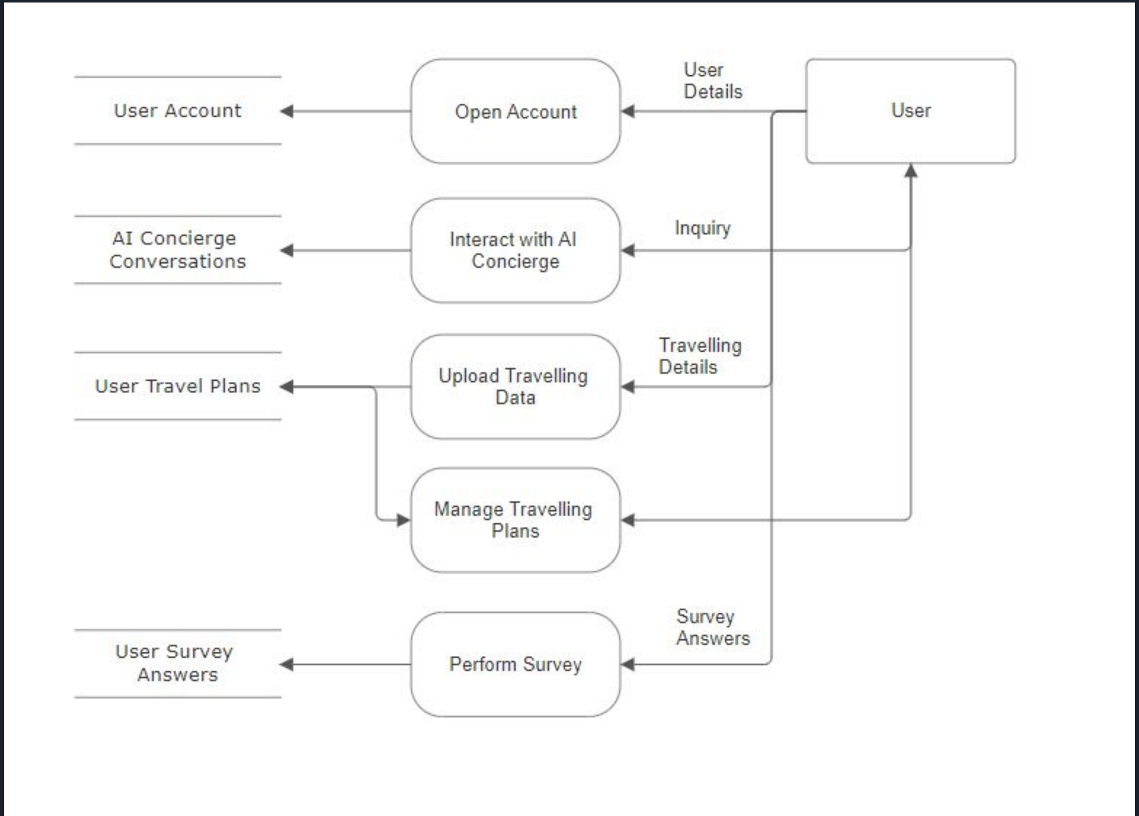
Flow Chart: User App Interaction


Download MAISON App
Welcome message and useful information related to the app
Interact with Digital Passport Feature
Interact with 3D View Feature
Interact with AI Concierge
Digital Passport
Yes
No
Uploading travel details to the application
Not uploading travel details to the application
Manage Travel Plans
Yes
No
View plans and/or make changes to plans
Save the upload for later viewing and editing purposes
3D Suite View
Click to View
View the Room and Go through a Suite Tour
AI Concierge
Request Recommendations
Inquire
Using traveling data or hotel location, AI Concierge creates recommendations
Answers questions related to booking
End Session

Data Flow Diagram: Level 0



Data Flow Diagram: Level 1



Asset List

- MAISON Application
    - AI Concierge
    - Digital Passport
    - 3D Suite View
- Hotel Locations
- Cloud Infrastructure
- Custom Built CRM Software
- Customer Data

Risk Register

Risks	Severity	Likelihood	Risk Level
DDoS	Intolerable	Possible	Critical
SQL Injection	Intolerable	Possible	Critical
Man-in-the-Middle	Intolerable	Possible	Critical
Phishing Attack	Undesirable	Probable	High
AI Manipulation	Undesirable	Probable	High
Third-Party Risk	Undesirable	Possible	Medium

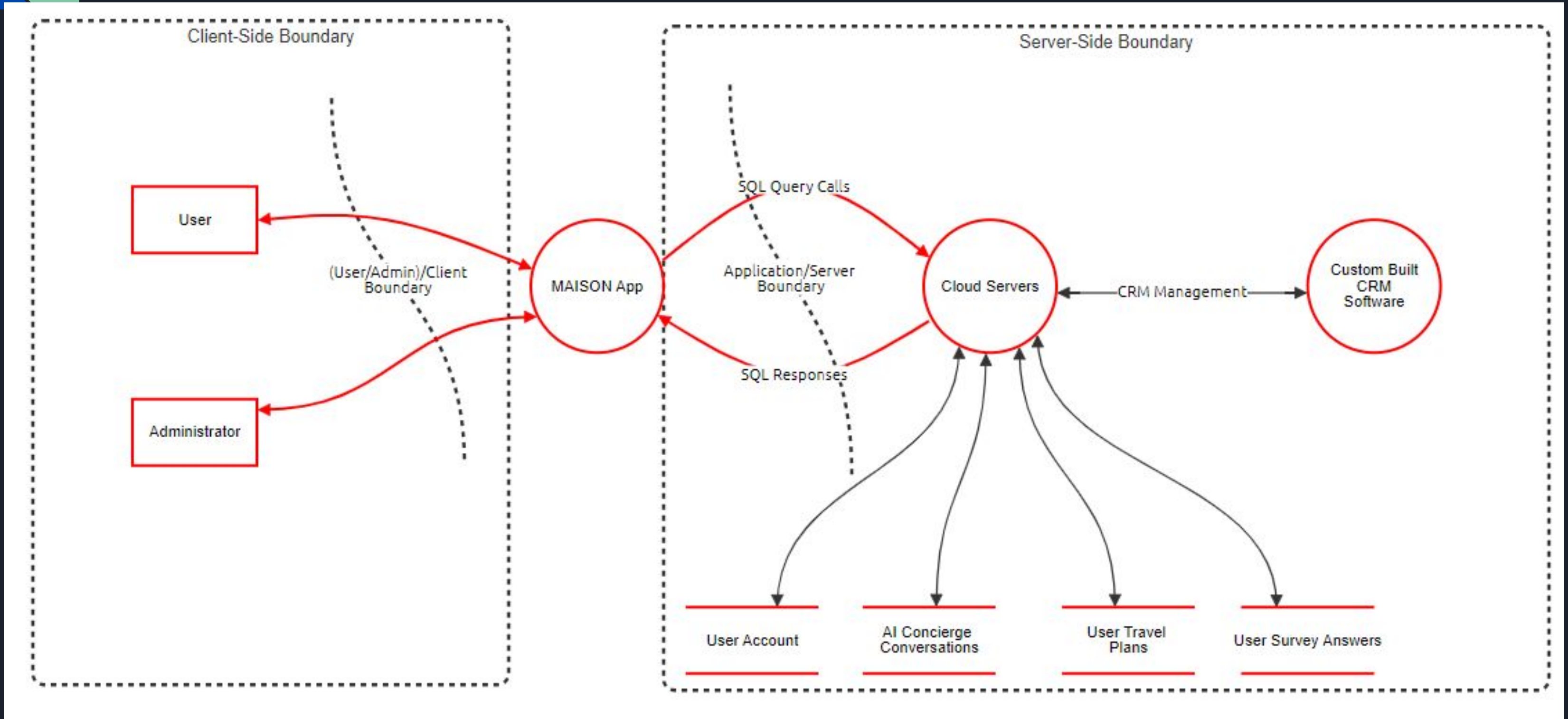
Mitigation Recommendations

- DDoS
  - Monitoring Systems
  - Load Balancer
- SQL Injection
  - User Input Validation
- MITM
  - Data Encryption
- Phishing Attack
  - Cybersecurity Awareness Training
- AI Manipulation
  - Content Filters
  - Rejection Sampling
- Third-Party Risk
  - Due Diligence with new partners

STRIDE Threat Model Summary

Name	Value
Total Threats	25
Total Mitigated	0
Not Mitigated	25
Open / High Priority	15
Open / Medium Priority	9
Open / Low Priority	1
Open / Unknown Priority	0

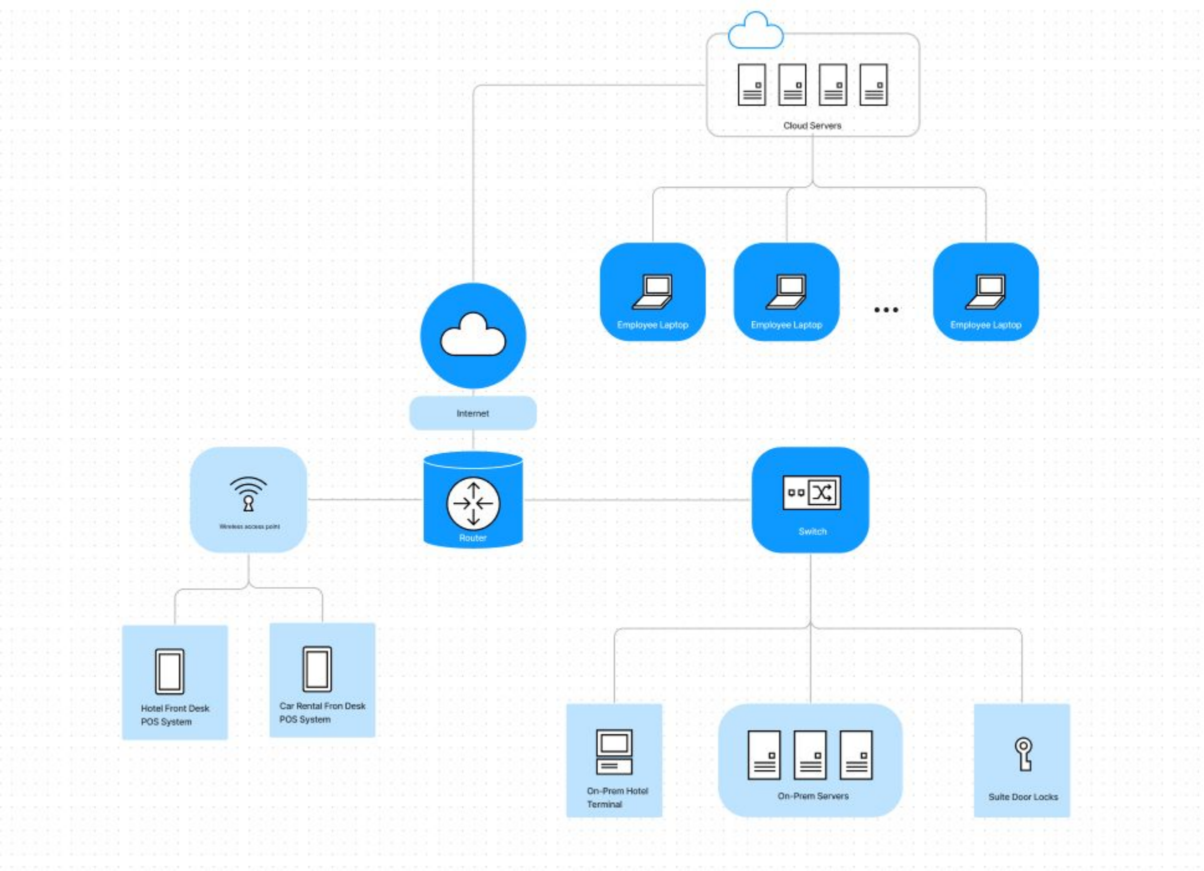
STRIDE Threat Model



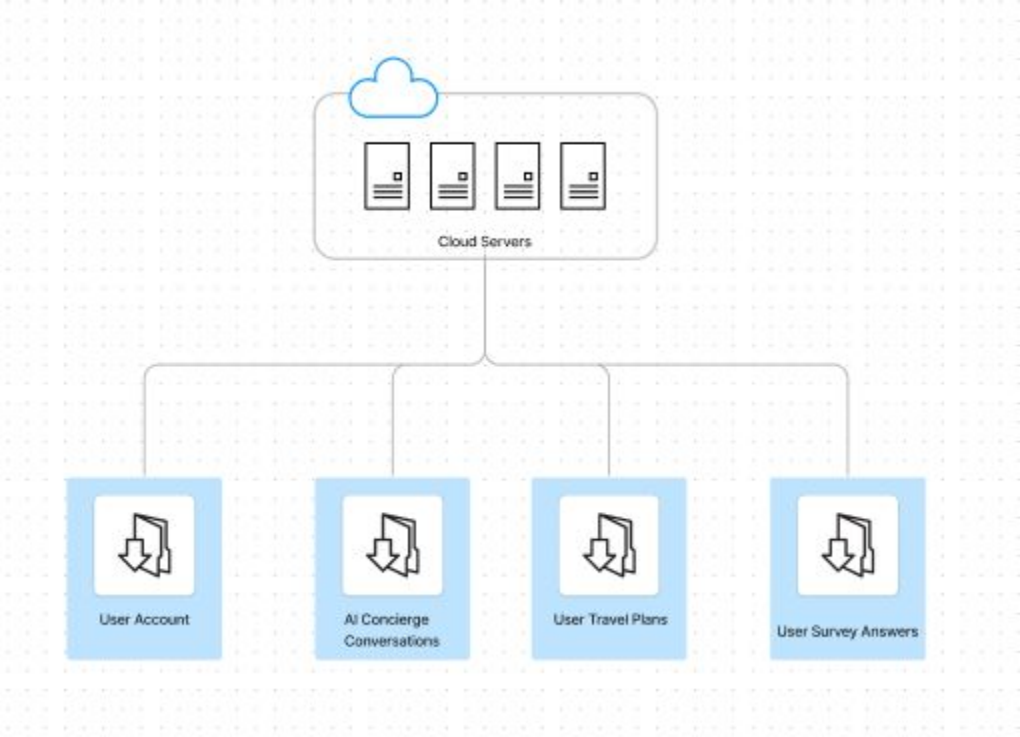
Key Recommendations

- Implementation of Role Based Access Control (RBAC)
    - Along with the implementation of Least Privilege
- Utilization of Data Encryption
- Implement DDoS Protection Tools
    - Rate Limit
    - Load Balancer
    - IP Block List
- Perform Continuous System Monitoring to Detect any Suspicious Activities

Current Data & Network Architecture



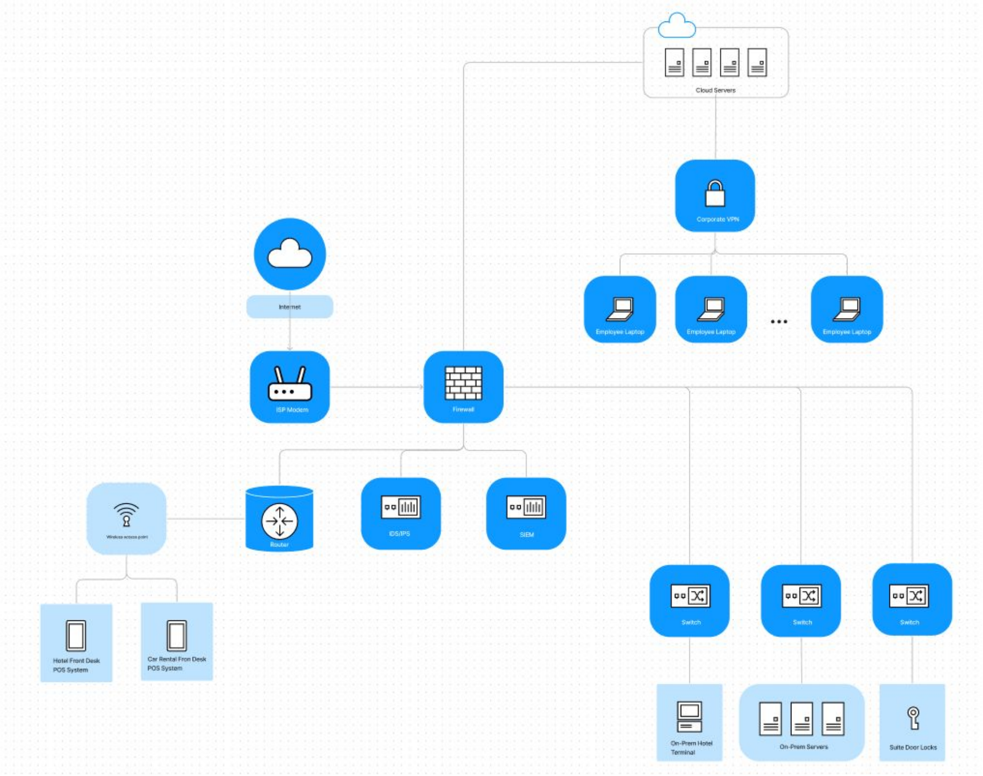
Data Stored on Cloud Servers



Security Concerns

- No Monitoring Systems Present
  - IDS
  - IPS
  - EDR
  - SIEM
- No Firewall Present
- Lack of Segregation in the Network Structure
- No Utilization of Encrypted Networks for the Employees

Revised Data & Network Architecture

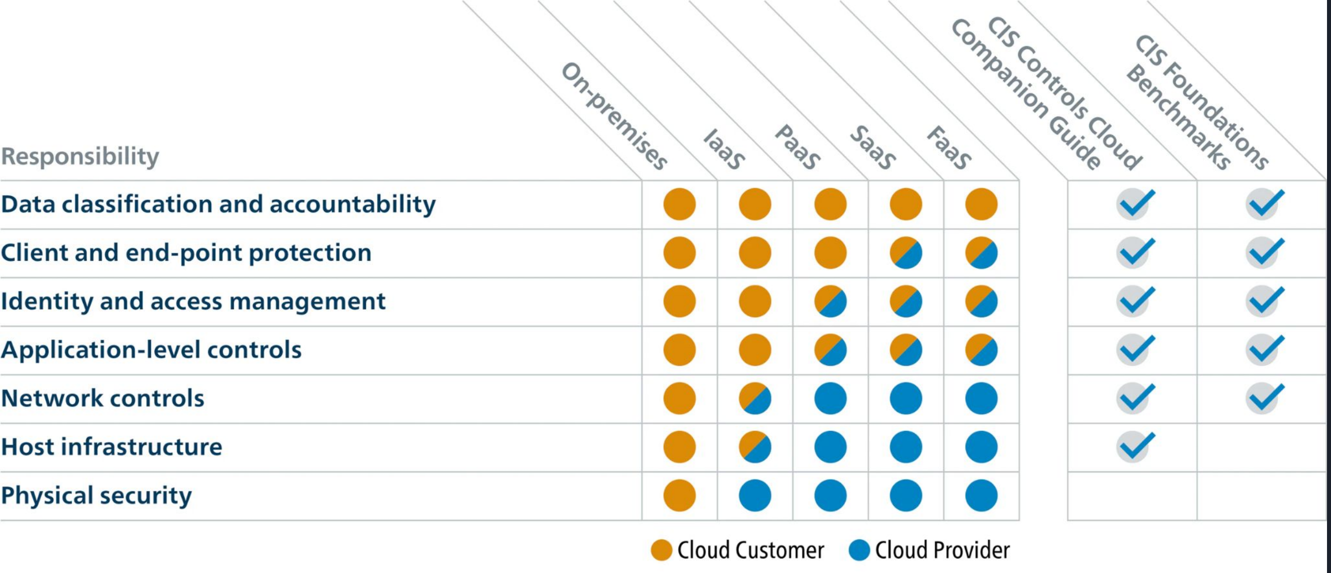


- Key Changes
  - Firewall
  - More Segregation in the Network
  - Monitoring Systems
  - Corporate VPN

Third-Party Risk Register

Third-Party Risks	Severity	Likelihood	Risk Level
Operational	Intolerable	Possible	Critical
Strategic	Intolerable	Improbable	High
Reputational	Tolerable	Possible	Medium
Compliance	Undesirable	Possible	Medium
Financial	Undesirable	Possible	Medium

Shared Responsibility Model



Responsibility	On-premises	IaaS	PaaS	SaaS	FaaS	CIS Controls Cloud Companion Guide	CIS Foundations Benchmarks
Data classification and accountability	🟠	🟠	🟠	🟠	🟠	✓	✓
Client and end-point protection	🟠	🟠	🟠	🟠🔵	🟠🔵	✓	✓
Identity and access management	🟠	🟠	🟠🔵	🟠🔵	🟠🔵	✓	✓
Application-level controls	🟠	🟠	🟠🔵	🟠🔵	🟠🔵	✓	✓
Network controls	🟠	🟠🔵	🔵	🔵	🔵	✓	✓
Host infrastructure	🟠	🟠🔵	🔵	🔵	🔵	✓	
Physical security	🟠	🔵	🔵	🔵	🔵		

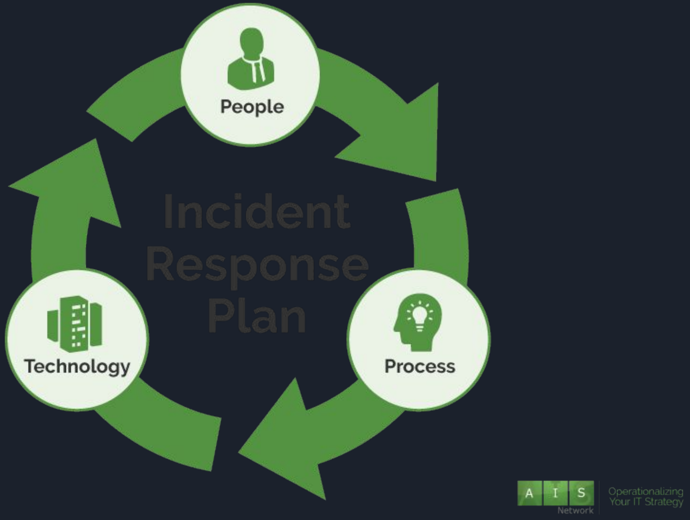
🟠 Cloud Customer 🔵 Cloud Provider

- Allocates different set of responsibilities to the customer and the service provider.

Third-Party Risk Management Strategies

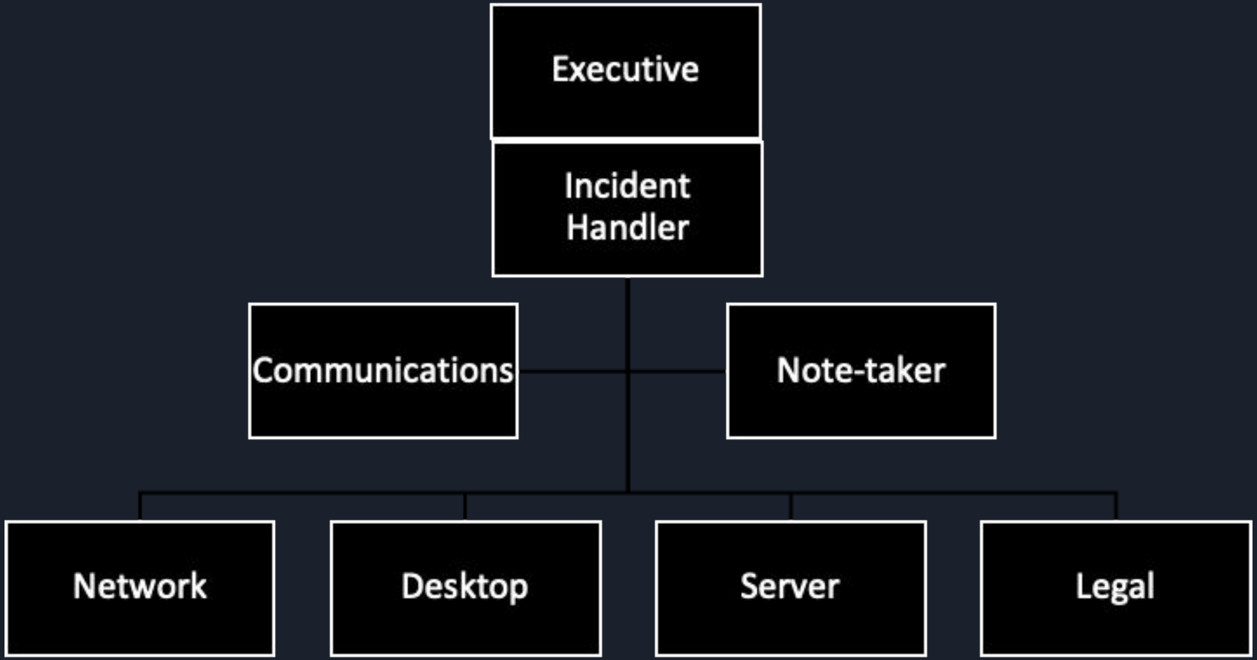
- Conduct a Third-Party Risk Assessment
- Conduct Application Dependency Mapping
- Develop a Third-Party Incident Response Plan
- Perform Continuous System Monitoring

Incident Response Plan

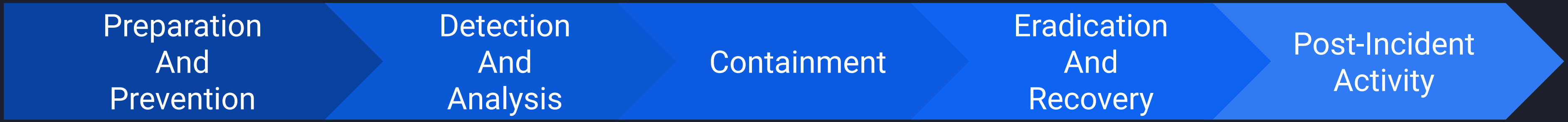


- Prepare the organization’s ability to handle cybersecurity incidents effectively and efficiently.
- Applies to the network structure, application, and other key resources.
- Defines clear roles and responsibilities.

Key Roles and Responsibilities



NIST Incident Response Framework



Preparation And Prevention

Detection And Analysis

Containment

Eradication And Recovery

Post-Incident Activity

The phases focuses on building a strong foundation for the organization’s ability to perform during incident handling process.

The phases focuses on identification and classification of the cybersecurity incident.

Utilizes precursor and indicators to confirm the incident.

The phases focuses on stopping the incident to minimize the damage.

The phases focuses on removing traces of attacker’s malicious actions and restoring the affected devices or areas back to its normal operational state.

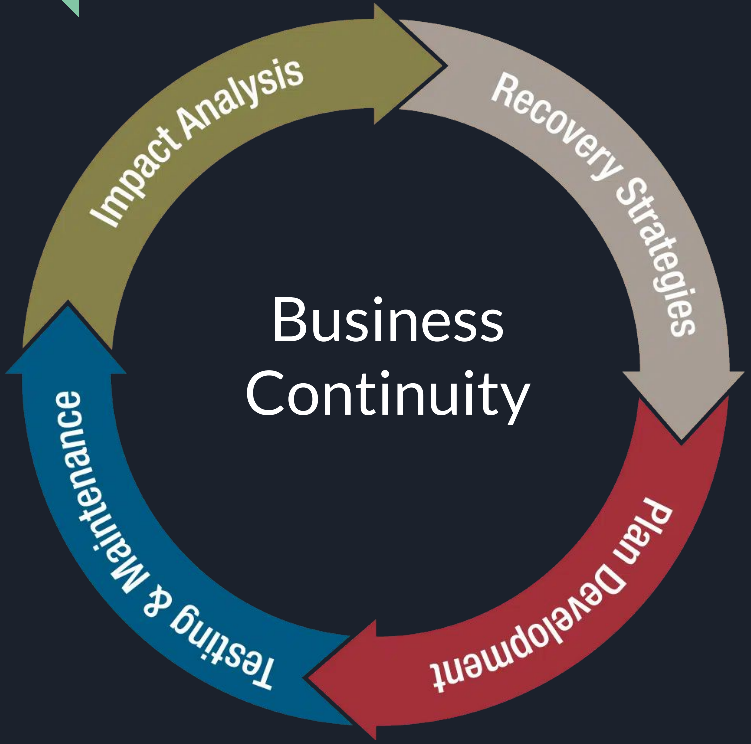
The phases focuses on learning and improving as an organization.

Post-Mortem Meetings with the stakeholders to improve overall security and processes.

Specific Incident Handling

- Planning for particular scenarios that can occur.
  - Sensitive Data Breach
  - Distributed Denial of Service (DDoS) Attacks
  - Ransomware
- Providing clear and precise procedures for the CSIRT to follow.

Business Continuity Plan



- Purpose
  - Provide Clear Guidelines for the Organization during a Disaster.
- Scope
  - The 2 core processes
    - User Hotel Interaction
    - User App Interaction

Risk Registers of Risk Scenarios

Risk Scenarios	Severity	Likelihood	Risk Level
Unavailability of Services Due to Cybersecurity Attacks	Intolerable	Possible	Critical
Sensitive Data Leak Due to Cybersecurity Attacks	Intolerable	Possible	Critical

Business Impact Assessment (BIA)

- Consider the negative impact on the business' daily operations.
- Consider the acceptable Mean Time to Recover (MTTR).
- Evaluate the Impact on Customer Relationship and Retention.
- Evaluate Reputational Damage for the Organization.

- Calculate the Potential Financial Damage.
- Evaluate the Financial Involvement Required to Resolve the Issue.
- Evaluate the Impact of Compromised Account Credentials.

Strategies to Maintain Critical Operations

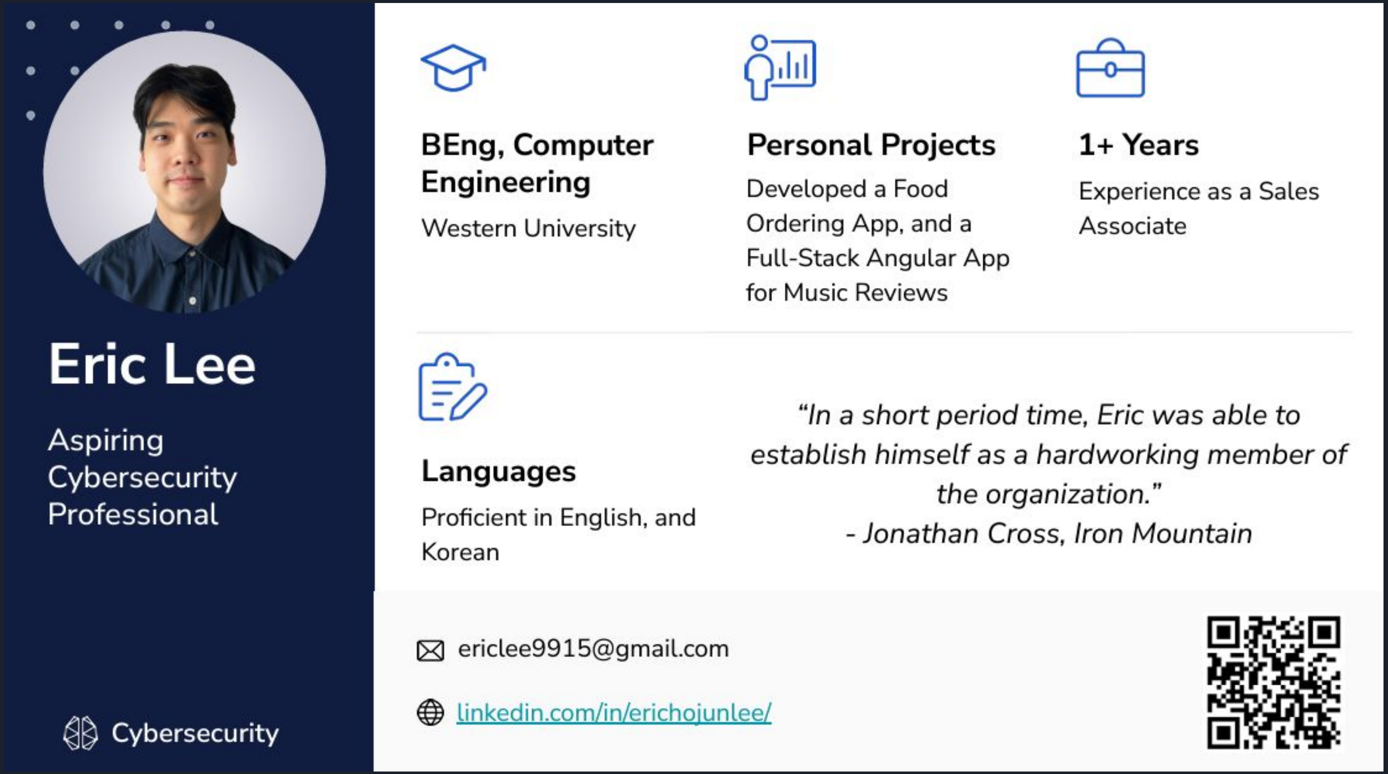
- Transfer the workload to the on-prem staff members during the incident handling process.
- Utilize Backup Cloud Infrastructures to maintain business operations.
- Consider deploying a version of the application with less features.

- Contain the incident and restore the affected areas.
- Utilize Backup Servers and Resources during the investigation.

Requirements - Recommendations

Risk Scenarios	Recommended Actions
Unavailability of Services Due to Cybersecurity Attacks	● Implement Monitoring Tools and Security Controls ● Implement Backup Resources and Infrastructure
Sensitive Data Leaks Due to Cybersecurity Attacks	● Data Encryption ● Implement Monitoring Tools ● Implement RBAC with Least Privilege ● Implement User Input Validation

Thank You For Watching!



Eric Lee

Aspiring Cybersecurity Professional

Cybersecurity

BEng, Computer Engineering

Western University

Personal Projects

Developed a Food Ordering App, and a Full-Stack Angular App for Music Reviews

1+ Years

Experience as a Sales Associate

Languages

Proficient in English, and Korean

"In a short period time, Eric was able to establish himself as a hardworking member of the organization."
- Jonathan Cross, Iron Mountain

✉ ericlee9915@gmail.com

🌐 linkedin.com/in/erichojunlee/