CAPSTONE PROJECT

07/10/2025

VIP EVENTS

CYBERSECURITY PROPOSAL

FILIPE MARQUES

MICROSOFT CYBERSECURITY ANALYST PROFESSIONAL CERTIFCATE

Microsoft

coursera

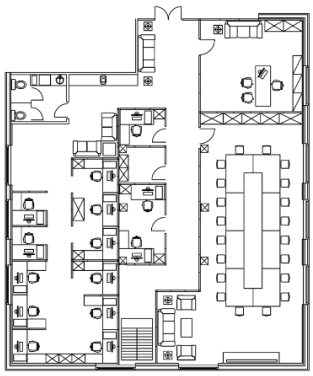
VIP EVENTS CYBERSECURITY PROPOSAL

EXECUTIVE SUMMARY

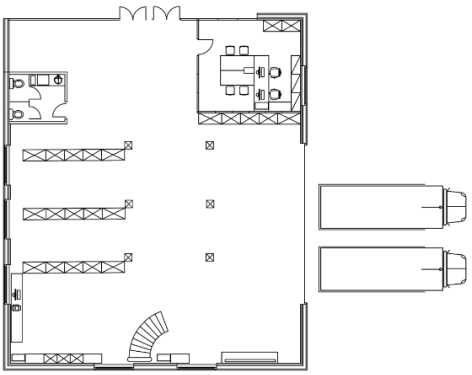
This proposal outlines a comprehensive cybersecurity solution for VIP Events' new facility and infrastructure, centred on the **Zero Trust Model** and **Defense in Depth (DiD)** principles. The primary goal is to establish precise, role-based access control for the expanding workforce of 21 permanent staff and numerous transient workers, managing access across 53 devices.

The architecture is built on **Azure Active Directory (AAD)**, providing centralized identity management, group-based access control, and seamless integration with the mission-critical **VIP Foods App**. The network implements deep segmentation using floor-specific subnets (Ground, First, Second Floor) and dedicated subnets for Production, Management, and Guest/Transient Workers to prevent lateral movement. Key controls include mandatory **Multi-Factor Authentication (MFA)** for all users, strict **Conditional Access (CA)** policies tailored to specific job roles, and a robust physical security layer (Layer 0) integrating ID-based access with AAD and CCTV monitoring. This document details the steps necessary to secure VIP Events, ensuring both high security compliance and business efficiency.

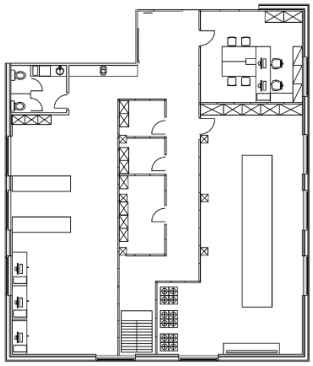
PHYSICAL INFRASTRUCTURE



Second Floor



Ground Floor



First Floor

DETAILED PROPOSAL OUTLINE

1. **Stage 1: Company Requirements and Network Design**

This foundational stage defines the scope and architecture, guided by Defense in Depth principles. The wired network will use dedicated subnets (VLANs) to isolate operational zones, including Corporate Administration, Kitchen Operations, and Logistics Storage, alongside isolated Production and Management subnets.

The wireless design employs a segregated approach with VIP-EMPLOYEE-SECURE (AAD-authenticated for corporate devices) and VIP-GUEST-LIMITED (isolated access for transient staff and visitors). Physical security, or Layer 0 DiD, will be enforced using an AAD-integrated ID-based access control system at entry points, combined with comprehensive CCTV integration for continuous monitoring.

2. **Stage 2: Azure AD Set-up**

Zero Trust starts with identity. The AAD tenant will be configured to host all permanent and transient user accounts. User provisioning will ensure all personnel, including the 21 permanent staff, have accounts with correctly defined job roles and departments.

Multi-Factor Authentication (MFA) will be made mandatory for every user to enforce explicit verification. To apply the Principle of Least Privilege (PoLP), eight dedicated AAD Security Groups will be created, mapping directly to employee roles (e.g., CEO, Head Chef, Equipment Handler). These groups will be configured as Role-Assignable to streamline privilege delegation.

3. **Stage 3: Roles and Access**

This stage focuses on granting access strictly based on job function. The VIP Foods App will undergo Application Registration in AAD. Eight corresponding custom App Roles (e.g., CEORole, TempRole) will be defined within the application registration to enable granular, in-application access control.

The AAD Security Groups created in Stage 2 will then be mapped directly to these App Roles, ensuring users automatically inherit the minimum necessary permissions required to execute their job duties within the application, thus enforcing PoLP.

4. **Stage 4: AAD Connections and Testing**

This stage validates the seamless and secure integration of AAD with the VIP Foods App. Testing will confirm that the Azure login functionality and the Role-Based Access Control (RBAC) implementation work correctly for all users across various device types (desktop, mobile, tablet).

Specific validation tasks include verifying user account attributes, confirming MFA enforcement, and reviewing access audit logs to ensure no irregular activities or unauthorized access attempts occurred during integration.

5. **Stage 5: Policy Implementation and Governance**

This final stage implements governance rules driven by the Zero Trust model using Azure's security features. Conditional Access (CA) Policies will be deployed to enforce context-aware controls, such as requiring device compliance and phishing-resistant authentication for the CEO and Managers and implementing Just-in-Time (JIT), time-restricted access for Transient Staff (TempRole).

Furthermore, Azure Policies will be assigned to enforce configuration standards, such as mandating HTTPS-only access for the VIP Foods App endpoints, ensuring continuous security and compliance.

STAGE 1: COMPANY REQUIREMENTS AND NETWORK DESIGN

VIP Events' Cybersecurity Requirements

VIP Events is moving to a new three-floor facility and expanding its workforce to 21 permanent staff plus transient personnel. The company will utilize 7 fixed devices and 46 mobile devices, necessitating a secure IT system. This proposal provides a solution that protects systems and data from unauthorized access by governing access based on job roles, ensuring a balance between security and business efficiency. The architecture is built on the **Zero Trust Model** and **Defense in Depth (DiD)** principles.

Building Structure and Network Design

Network segmentation is implemented through dedicated VLANs/Subnets across the building structure, following DiD principles to isolate critical systems and reduce attack risk. Role-based subnet restrictions are used for enhanced security.

Wired Network Segmentation

Subnet Name	Dedicated Floor/Area	Purpose
VLAN-30_CORP_ADMIN	Second Floor (Office, Management)	Handles sensitive administrative and financial data for the CEO, Catering Manager, and Office Workers.
VLAN-20_KITCHEN	First Floor (Food Prep)	Isolates operational kitchen management systems and shared Chef tablets.
VLAN-10_STORAGE	Ground Floor (Loading Dock, Storage)	Isolates logistics and inventory systems used by Equipment Handlers and the Equipment Manager.
VLAN-90_PRODUCTION/MGMT	Across all floors (Backbone)	Dedicated network for servers, printers, and core network management equipment (routers, firewalls).

Wireless Network Segmentation

SSID/Segment	Purpose	Authentication
VIP-EMPLOYEE-SECURE	Corporate-Owned Devices	Requires authentication integrated with **Azure AD (AAD)**.
VIP-GUEST-LIMITED	Transient Staff and Visitors	Fully isolated from the internal network; provides basic internet access only.

Access Control and Security Policies

Access control for all subnets and wireless segments will be enforced via the on-premises firewall and integrated with Azure AD Conditional Access (CA) policies.

Required Policy Creation

The implementation phase will include:

1. **Mandatory MFA Policy:** Requires Multi-Factor Authentication for all users accessing the network and applications.
2. **Device Compliance Policy:** Requires corporate devices to meet security standards before granting access (e.g., to VLAN-30_CORP_ADMIN).
3. **Just-in-Time (JIT) Access Policy:** Enforces time and location-based restrictions for **Transient Staff** (**TempRole**).
4. **High-Risk User Policy:** Applies elevated security and session limits for the CEO and all Manager roles.
5. **Firewall Access Matrix:** Strict policy enforcement to limit traffic between all subnets.

User Roles and Access Requirements

Azure Active Directory (AAD) will be the central identity system. User accounts will be created based on job roles, and group-based access control will be implemented by assigning roles directly within groups. This structure ensures users only have access aligned with their specific entitlements (**PoLP**).

Eight dedicated **AAD Security Groups** will be created, directly corresponding to the application roles in the VIP Foods App: **CEOGroup**, **HeadChefGroup**, **ChefsGroup**, **CateringManagerGroup**, **EquipManagerGroup**, **EquipHandlersGroup**, **OfficeWorkersGroup**, and **Worker-External** (for transient staff).

Physical Security Guidelines (Layer 0 Defense)

To secure Layer 0 of the DiD approach, VIP Events will implement:

- **ID-Based Access Control:** A robust system to regulate entry and exit, integrated with **Azure AD** to centralize authentication for physical and digital access.
- **Door and Main Entrance Integration:** Stringent access protocols will be implemented at critical entry points.
- **CCTV Surveillance:** Comprehensive coverage of entry points, storage, and the server room, integrated with the access control system for real-time monitoring.
- **Device Security:** Fixed devices will be physically secured, and **Mobile Device Management (MDM)** will be required for all corporate tablets and laptops.

STAGE 2: AZURE AD SET-UP

Azure AD Tenant Configuration

An Azure AD tenant will be created (or an existing one reconfigured) for VIP Events. This tenant will serve as the organization's central identity store, laying the groundwork for integration with the internal infrastructure and external applications like the VIP Foods App.

User Account Configuration and MFA

User accounts will be created for all 21 permanent employees and a template for transient staff. Accounts must be configured with user attributes (Job Role, Department) to facilitate RBAC.

Security Enhancement: Mandatory Multi-Factor Authentication (MFA) To enforce the Zero Trust principle of "Verify Explicitly," MFA must be enabled for all user accounts. This requires a dedicated policy (Stage 5) to mandate MFA enrolment and usage for all sign-in attempts.

Employee Group	Account Count	Department	MFA Status
CEO (Owner)	1	Executive	Mandatory
Head Chef	1	Kitchen	Mandatory
Chefs	10	Kitchen	Mandatory
Catering Manager	1	Operations	Mandatory
Office Workers	3	Administration	Mandatory
Equipment Manager	1	Operations	Mandatory
Equipment Handlers	4	Operations	Mandatory
Transient Staff	Varies	Temporary	Mandatory

Group-Based Access Control Implementation

To enforce the Principle of Least Privilege (PoLP), users are categorized into distinct security groups based on their roles. These groups are designated as **role-assignable** to streamline the application of permissions.

Security Group Name	VIP Foods App Role Equivalent	Role Assignment Status
CEOGroup	CEORole	Role-Assignable
HeadChefGroup	HeadChefRole	Role-Assignable
ChefsGroup	ChefsRole	Role-Assignable
CateringManagerGroup	CateringManagerRole	Role-Assignable
EquipManagerGroup	EquipManagerRole	Role-Assignable
EquipHandlersGroup	EquipHandlersRole	Role-Assignable
OfficeWorkersGroup	OfficeWorkersRole	Role-Assignable
Worker-External	TempRole	Role-Assignable

All provisioned user accounts will be immediately integrated into their corresponding security groups.

STAGE 3: ROLES AND ACCESS

VIP Foods Application Integration

The first step is to register the VIP Foods App within the Azure AD tenant. This **App Registration** provides the necessary Client ID and Tenant ID for the application to interact with Azure AD for authentication and authorization (SSO). A **Client Secret** will also be generated and secured to allow the application to securely access the necessary APIs.

Custom Application Roles Definition

Eight custom application roles are defined within the App Registration to align with the workforce structure and ensure granular access control. These roles will be utilized by the application developers to assign specific permissions to application features.

Application Role Name	Role Purpose
CEORole	Unrestricted access to all functionalities for strategic oversight.
HeadChefRole	Elevated access to overall kitchen management functionalities.
ChefsRole	Access to food preparation and kitchen management functionalities.
CateringManagerRole	Access to planning and managing catering events and logistics.
EquipManagerRole	Advanced oversight of equipment functionalities, maintenance, and tracking.
EquipHandlersRole	Access to essential equipment management and basic tracking.
OfficeWorkersRole	Access to office-related activities and data management functionalities.
TempRole	Limited, time-bound access for transient workers, automatically disabled after a pre-defined period (JIT access).

Assigning Permissions to Azure Roles

The details of the defined application roles (including their unique IDs/values) must be provided to the application development team. They will be responsible for implementing the internal Role-Based Access Control (RBAC) within the VIP Foods App, ensuring that each role is mapped to the correct application controllers and corresponding feature permissions.

Mapping User Groups to Azure Roles

The final step is to assign the **role-assignable AAD Security Groups** (created in Stage 2) directly to their corresponding **Application Roles**. This establishes the final link in the access chain, ensuring that users automatically inherit the necessary permissions simply by being members of their departmental group.

AAD Security Group	Assigned Application Role	Access Principle Enforced
CEOGroup	CEORole	Unrestricted Access
HeadChefGroup	HeadChefRole	Least Privilege

ChefsGroup	ChefsRole	Least Privilege
CateringManagerGroup	CateringManagerRole	Least Privilege
EquipManagerGroup	EquipManagerRole	Least Privilege
EquipHandlersGroup	EquipHandlersRole	Least Privilege
OfficeWorkersGroup	OfficeWorkersRole	Least Privilege
Worker-External	TempRole	Just-in-Time Access

STAGE 4: AAD CONNECTIONS

Testing and Verification Procedures

Client App and Authentication Integration

- **Test:** Log into the VIP Foods App using designated test user accounts.
- **Verify:** Ensure that the **Azure AD Authentication** prompts appear, and **Single Sign-On (SSO)** works correctly.
- **Test RBAC:** Log in with different role-specific test users to ensure they only see the application features applicable to their assigned role.

User Account Validation

- **Test:** Review the AAD portal's User Overview.
- **Verify:** Confirm that all 21 user accounts were successfully created and that critical attributes (Job Title, Department) are accurate as per the workforce list.

Application Role Assignment Verification

- **Test:** Navigate to the VIP Foods Enterprise Application in AAD and review the assigned users and groups.
- **Verify:** Confirm that the eight **role-assignable AAD Security Groups** are correctly mapped to their corresponding **Application Roles (e.g., ChefsGroup assigned to ChefsRole)**.

MFA Verification

- **Test:** Attempt to sign in to a corporate resource with an enabled test account that has not yet enrolled in MFA.
- **Verify:** Ensure the sign-in attempt is blocked or forced into the MFA registration process, validating the effectiveness of the MFA policy (precursor to Stage 5).

Logging and Monitoring Check

- **Test:** Review the AAD **Audit Logs** and **Sign-in Logs** in the Monitoring section.
- **Verify:** Confirm that test sign-ins and successful role assignments are recorded. Scrutinize logs to ensure no irregular activities (e.g., failed sign-ins from unexpected locations) occurred during testing.

Documentation Review

- **Test:** Compare the final configuration of the AAD portal settings against the details documented in Stages 2 and 3 of this proposal.
- **Verify:** Ensure full alignment. Promptly update all documentation to reflect any minor discrepancies identified during testing.

STAGE 5: POLICY IMPLEMENTATION

User Authentication Policy

A **Conditional Access (CA) Policy** will be created and enforced to mandate Multi-Factor Authentication (MFA) across all user groups, fulfilling the **Zero Trust** principle of "Verify Explicitly."

Conditional Access Policy Specifications

- **Policy Scope:** Target all users except emergency access accounts.
- **Target Resource:** All cloud apps, specifically the **VIP Foods App**.
- **Controls:** Require MFA for sign-in.
- **Risk Mitigation:** Additional CA policies will be created for high-risk users (CEO, Managers) requiring stricter session controls or device compliance.
- **Transient Staff Policy:** A specific policy will limit **TempRole** access to the VIP Foods App based on location and time (Just-in-Time Access), automatically disabling sessions outside defined work hours.

Network Configuration Policy for Web Applications

To ensure secure data transmission and access to the VIP Foods App, an **Azure Policy** will be utilized to enforce critical network security configurations.

- **HTTPS Requirement:** Implement the built-in Azure Policy "App Service app slots should only be accessible over HTTPS." This ensures all traffic to the VIP Foods App is encrypted in transit.
- **Application Gateways/Firewalls:** Policies will ensure the web application is protected by a Web Application Firewall (WAF) to filter malicious web traffic, adding another layer to the **Defense in Depth** strategy.

Testing in a Non-Production Environment

Policy implementation carries the risk of inadvertently blocking legitimate access or causing service disruptions.

- **Recommendation:** All new Conditional Access and Azure Policies must be implemented in a **"Report-only" mode** or tested thoroughly in a dedicated non-production (staging) environment first.
- **Verification Goal:** Verify that no legitimate users (e.g., the CEO or Office Workers) are blocked and confirm the Transient Staff policy correctly limits access based on time/location.

CONCLUSION

This proposal outlines a structured and comprehensive cybersecurity solution for VIP Events based on **Azure Active Directory (AAD)**. By integrating principles of **Defense in Depth (DiD)** and the **Zero Trust Model**, the plan ensures robust network segmentation, role-based access control, and continuous verification for all users and devices. The proposed framework, including mandatory **MFA** and specialized **Conditional Access Policies**, safeguards sensitive client and operational data, aligning VIP Events with best practices for secure and efficient business growth.