445Cyber Co

Owner: David Nguyen
Reviewer: Mohammed Gebril
Contributors: Kamyar Berenjkar
Date Generated: Sun Dec 07 2025

Executive Summary

High level system description

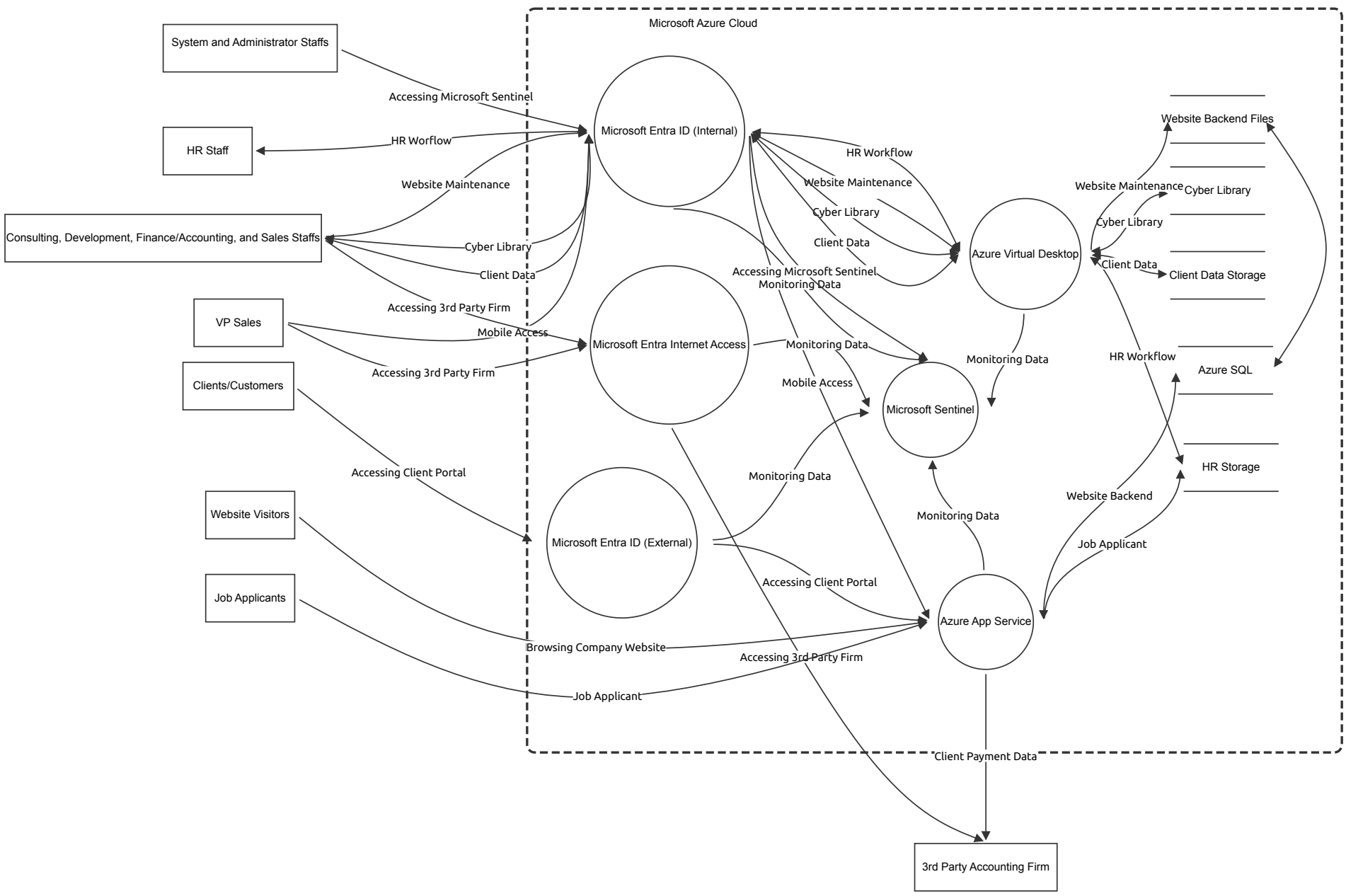
A cloud-based solution

Summary

Total Threats	7
Total Mitigated	0
Total Not Applicable	7
Total Open	0
Open / Critical Severity	0
Open / High Severity	0
Open / Medium Severity	0
Open / Low Severity	0

445Cyber Co Cloud Solution

A proposed cloud solution for 455Cyber Co



445Cyber Co Cloud Solution

System and Administrator Staffs (Actor)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

HR Staff (Actor)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Consulting, Development, Finance/Accounting, and Sales Staffs (Actor)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

VP Sales (Actor)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Clients/Customers (Actor)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
1	Compromised Credentials	Spoofing	High	N/A		Client credential could be compromised and allowed the attackers to spoof as the client	Enforce strict MFA and password policies like password complexity and rotation.

Job Applicants (Actor)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Website Visitors (Actor)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

3rd Party Accounting Firm (Actor)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Microsoft Entra ID (Internal) (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Accessing Microsoft Sentinel (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Website Maintenance (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Cyber Library (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Mobile Access (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

HR Worflow (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Client Data (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Website Maintenance (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

HR Workflow (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Cyber Library (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Client Data (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Mobile Access (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Website Backend (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Job Applicant (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

HR Workflow (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Client Data (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Cyber Library (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Website Maintenance (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

(Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Accessing Client Portal (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Accessing Client Portal (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Client Payment Data (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Monitoring Data (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Monitoring Data (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Monitoring Data (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Monitoring Data (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Accessing Microsoft Sentinel (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Accessing 3rd Party Firm (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Accessing 3rd Party Firm (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Accessing 3rd Party Firm (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Monitoring Data (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Job Applicant (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
5	Botnet Attack	Denial of service	High	N/A		An attacker could used botnet to overwhelmed the website with requests and causing disruption in site availability.	Implementing Azure Web Application Firewall with DDoS protection and enforce rate limit policy.

Browsing Company Website (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
6	Botnet Attack	Denial of service	High	N/A		An attacker could used botnet to overwhelmed the website with requests and causing disruption in site availability.	Implementing Azure Web Application Firewall with DDoS protection and enforce rate limit policy.

Azure Virtual Desktop (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Azure App Service (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
7	Malicious Macro File Upload	Elevation of privilege	Critical	N/A		Attacker can upload malicious macro disguised as resume that cause the HR staff to open and potential escalation of privilegde by stealing the HR staff credential.	Implementing Azure Web Application Firewall with content scanning with Microsoft Defender

Website Backend Files (Store)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Cyber Library (Store)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Client Data Storage (Store)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
8	Disgruntle Employee	Information disclosure	High	N/A		A disgruntle employee or insider threat could download sensitive client information to disclose it to public	Azure File Storage has a DLP feature to prevent data with high sensitive label from being exfiltrated without proper permission.

Azure SQL (Store)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
2	SQL Injection	Information disclosure	Critical	N/A		Attacker can inject malicious SQL query from the company website frontend to cause a disclosure of sensitive data.	Enable Microsoft Defender for SQL to provide advance SQL attack protection on the SQL database.
3	SQL Injection	Tampering	Critical	N/A		Attacker can inject malicious SQL qeries that cause a deletion of data	Enable Microsoft Defender for SQL to provide advance SQL attack protection on the SQL database.

HR Storage (Store)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Microsoft Entra ID (External) (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Microsoft Sentinel (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Microsoft Entra Internet Access (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations