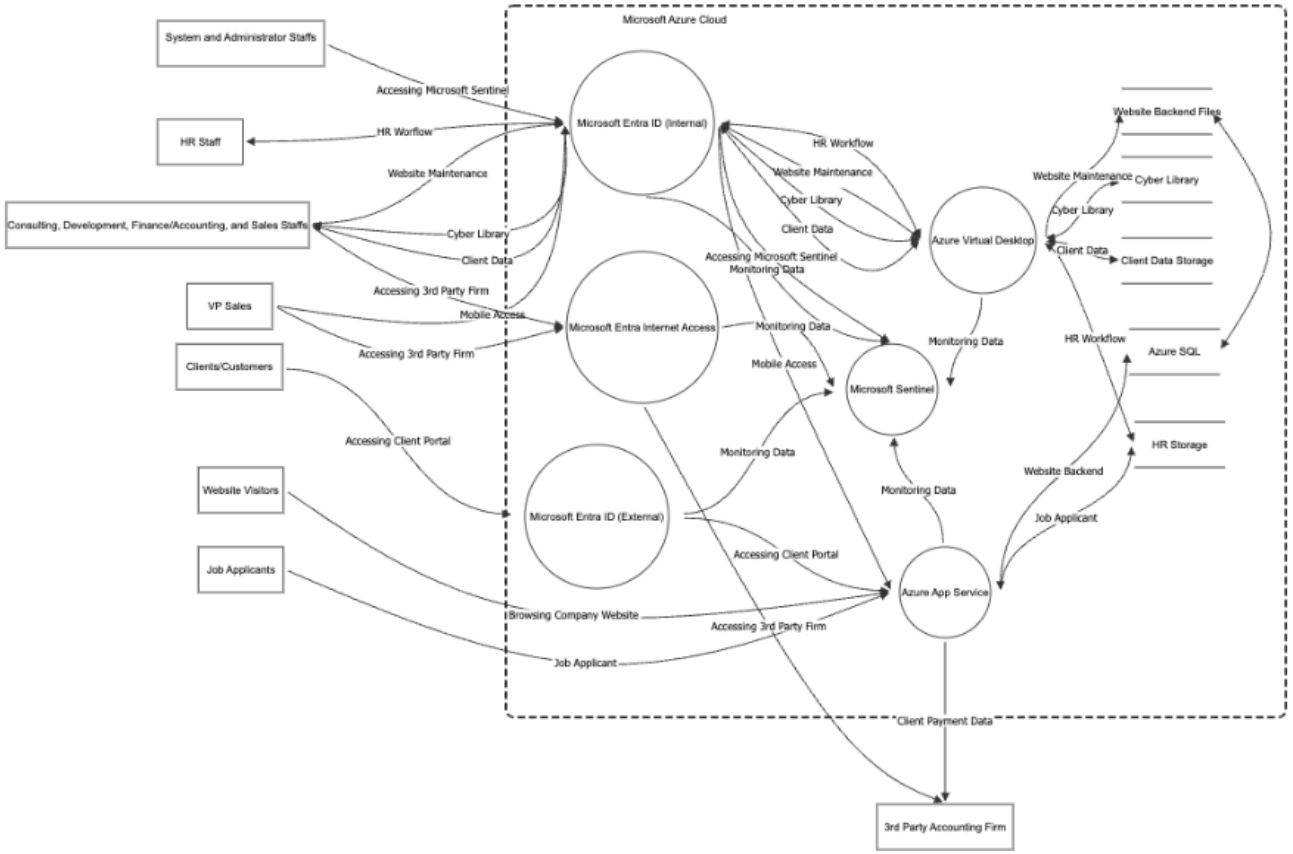
System Description

Microsoft Entra ID is being used as the major cloud service for 445CyberCo that meets the requirement of implementing Zero Trust Architecture, Identity and Access Management, and Active Directory service for proper authentication and RBAC authorization to ensure specific resources only be granted to specific user entities.

Dataflow Diagram - Level 0 DFD



Dataflows

Name	From	To	Data	Protocol	Port
Phishing Email (Spearphishing)	Potential Attacker	HR Staff	Malicious Email/Link		-1

Name	From	To	Data	Protocol	Port
Admin Login / Auth	System and Administrator Staffs	Microsoft Entra ID (Internal)	User Credentials	HTTPS	443
HR Workflow Auth	HR Staff	Microsoft Entra ID (Internal)	Auth Token (OIDC/SAML)	HTTPS	443
Website Maintenance, Cyber Library, client Data	Consulting, Dev, Finance, Sales Staffs	Microsoft Entra ID (Internal)	Auth Token (OIDC/SAML)	HTTPS	443
Accessing 3rd Party Firm	VP Sales	Microsoft Entra Internet access	Auth Token (OIDC/SAML)	HTTPS	443
Mobile Access	VP Sales	Microsoft Entra ID (Internal)	Auth Token (OIDC/SAML)	HTTPS	443
Accessing Client Portal	Clients/Customers	Microsoft Entra ID (External)	[]	HTTPS	443
Browsing Company Website	Website Visitors	Azure App Services	[]	HTTPS	443
Job Application Data	Job Applicants	Azure App Services	Employee/Client PII	HTTPS	443
Authenticated Access	Microsoft Entra ID (Internal)	Azure Virtual Desktop	Auth Token (OIDC/SAML)	Kerberos/TLS	-1
Identity Logs	Microsoft Entra ID (Internal)	Microsoft Sentinel	Syslog/Event Logs	HTTPS	-1
Network Logs	Microsoft Entra Internet access	Microsoft Sentinel	[]		-1
Mobile Access Tunnel	Microsoft Entra Internet access	Azure App Services	[]		-1
External Auth Logs	Microsoft Entra ID (External)	Microsoft Sentinel	[]		-1
Accessing Client Portal	Microsoft Entra ID (External)	Azure App Services	[]		-1
Accessing 3rd Party Firm	Microsoft Entra Internet access	3rd Party Accounting Firm	[]	HTTPS	443
Host Logs (Sysmon/WinEvent)	Azure Virtual Desktop	Microsoft Sentinel	[]		-1
Website Maintenance (SMB/NFS)	Azure Virtual Desktop	Website Backend files	[]	SMB	445
Read Cyber Library	Azure Virtual Desktop	Cyber Library	[]		-1
Read/Write Client Data	Azure Virtual Desktop	Client Data Storage	Employee/Client PII		-1
HR Workflow	Azure Virtual Desktop	HR Storage	Employee/Client PII		-1
Client Payment Transfer	Azure App Services	3rd Party Accounting Firm	Client Payment Info	API/HTTPS	443
App Logs	Azure App Services	Microsoft Sentinel	[]		-1
Backend Queries	Azure App Services	Azure SQL	[]	TDS/TCP	1433
Store Job Applicant	Azure App Services	HR Storage	Employee/Client PII		-1

Data Dictionary

Name	Description	Classification	Carried	Processed
User Credentials		RESTRICTED	Admin Login / Auth	Microsoft Entra ID (Internal) System and Administrator Staffs
Employee/Client PII		RESTRICTED	HR Workflow Job Application Data Read/Write Client Data Store Job Applicant	Azure App Services Azure Virtual Desktop Client Data Storage HR Storage Job Applicants

Name	Description	Classification	Carried	Processed
Client Payment Info		RESTRICTED	Client Payment Transfer	3rd Party Accounting Firm Azure App Services
Auth Token (OIDC/SAML)		RESTRICTED	Accessing 3rd Party Firm Authenticated Access HR Workflow Auth Mobile Access Website Maintenance, Cyber Library, client Data	Azure Virtual Desktop Consulting, Dev, Finance, Sales Staffs HR Staff Microsoft Entra ID (Internal) Microsoft Entra Internet access VP Sales
Malicious Email/Link		PUBLIC	Phishing Email (Spearphishing)	HR Staff Potential Attacker
Syslog/Event Logs		RESTRICTED	Identity Logs	Microsoft Entra ID (Internal) Microsoft Sentinel

Actors

Name	System and Administrator Staffs
Description	
Is Admin	False
Finding Count	0

Name	HR Staff
Description	
Is Admin	False
Finding Count	0

Name	Consulting, Dev, Finance, Sales Staffs
Description	
Is Admin	False
Finding Count	0

Name	VP Sales
Description	
Is Admin	False
Finding Count	0

Name	Clients/Customers
Description	
Is Admin	False

Name	Clients/Customers
Finding Count	0

Name	Website Visitors
Description	
Is Admin	False
Finding Count	0

Name	Job Applicants
Description	
Is Admin	False
Finding Count	0

Name	Potential Attacker
Description	
Is Admin	False
Finding Count	0

Boundaries

Name	Microsoft Azure Cloud with Microsoft Entra
Description	
In Scope	True
Immediate Parent	N/A, primary boundary
All Parents	
Classification	Classification.UNKNOWN
Finding Count	0

Assets

Name	Microsoft Entra ID (Internal)
Description	
In Scope	True
Type	Server
Finding Count	44

Threats

- 1 – INP03 – Server Side Include (SSI) Injection
- 2 – INP05 – Command Line Execution through SQL Injection
- 3 – AA01 – Authentication Abuse/ByPass
- 4 – DS01 – Excavation
- 5 – DE02 – Double Encoding
- 6 – AC01 – Privilege Abuse
- 7 – DO01 – Flooding
- 8 – HA01 – Path Traversal
- 9 – DO02 – Excessive Allocation
- 10 – INP08 – Format String Injection
- 11 – INP09 – LDAP Injection
- 12 – INP10 – Parameter Injection
- 13 – INP11 – Relative Path Traversal
- 14 – INP14 – Input Data Manipulation
- 15 – CR03 – Dictionary-based Password Attack
- 16 – DS03 – Footprinting
- 17 – AC06 – Using Malicious Files
- 18 – HA03 – Web Application Fingerprinting
- 19 – SC02 – XSS Targeting Non-Script Elements
- 20 – AC07 – Exploiting Incorrectly Configured Access Control Security Levels
- 21 – SC03 – Embedding Scripts within Scripts
- 22 – INP16 – PHP Remote File Inclusion
- 23 – AA02 – Principal Spoof
- 24 – DS04 – XSS Targeting Error Pages
- 25 – SC04 – XSS Using Alternate Syntax
- 26 – CR05 – Encryption Brute Forcing
- 27 – AC08 – Manipulate Registry Information
- 28 – SC05 – Removing Important Client Functionality
- 29 – INP17 – XSS Using MIME Type Mismatch
- 30 – AA03 – Exploitation of Trusted Credentials
- 31 – AC09 – Functionality Misuse
- 32 – INP18 – Fuzzing and observing application log data/errors for application mapping
- 33 – AA04 – Exploiting Trust in Client
- 34 – INP19 – XML External Entities Blowup
- 35 – AC11 – Session Credential Falsification through Manipulation
- 36 – INP21 – DTD Injection
- 37 – INP22 – XML Attribute Blowup
- 38 – INP28 – XSS Targeting URI Placeholders
- 39 – INP29 – XSS Using Doubled Characters
- 40 – INP34 – SOAP Array Overflow
- 41 – INP36 – HTTP Response Smuggling
- 42 – INP37 – HTTP Request Smuggling
- 43 – AC16 – Session Credential Falsification through Prediction
- 44 – AC17 – Session Hijacking - ServerSide

Name	**Microsoft Entra Internet access**
Description	
In Scope	True
Type	Server
Finding Count	44

Threats

- 45 – INP03 – Server Side Include (SSI) Injection
- 46 – INP05 – Command Line Execution through SQL Injection
- 47 – AA01 – Authentication Abuse/ByPass
- 48 – DS01 – Excavation
- 49 – DE02 – Double Encoding
- 50 – AC01 – Privilege Abuse
- 51 – DO01 – Flooding
- 52 – HA01 – Path Traversal
- 53 – DO02 – Excessive Allocation
- 54 – INP08 – Format String Injection
- 55 – INP09 – LDAP Injection
- 56 – INP10 – Parameter Injection
- 57 – INP11 – Relative Path Traversal
- 58 – INP14 – Input Data Manipulation
- 59 – CR03 – Dictionary-based Password Attack
- 60 – DS03 – Footprinting
- 61 – AC06 – Using Malicious Files
- 62 – HA03 – Web Application Fingerprinting
- 63 – SC02 – XSS Targeting Non-Script Elements
- 64 – AC07 – Exploiting Incorrectly Configured Access Control Security Levels
- 65 – SC03 – Embedding Scripts within Scripts
- 66 – INP16 – PHP Remote File Inclusion
- 67 – AA02 – Principal Spoof
- 68 – DS04 – XSS Targeting Error Pages
- 69 – SC04 – XSS Using Alternate Syntax
- 70 – CR05 – Encryption Brute Forcing
- 71 – AC08 – Manipulate Registry Information
- 72 – SC05 – Removing Important Client Functionality
- 73 – INP17 – XSS Using MIME Type Mismatch
- 74 – AA03 – Exploitation of Trusted Credentials
- 75 – AC09 – Functionality Misuse
- 76 – INP18 – Fuzzing and observing application log data/errors for application mapping
- 77 – AA04 – Exploiting Trust in Client
- 78 – INP19 – XML External Entities Blowup
- 79 – AC11 – Session Credential Falsification through Manipulation
- 80 – INP21 – DTD Injection
- 81 – INP22 – XML Attribute Blowup
- 82 – INP28 – XSS Targeting URI Placeholders
- 83 – INP29 – XSS Using Doubled Characters
- 84 – INP34 – SOAP Array Overflow
- 85 – INP36 – HTTP Response Smuggling
- 86 – INP37 – HTTP Request Smuggling
- 87 – AC16 – Session Credential Falsification through Prediction
- 88 – AC17 – Session Hijacking - ServerSide

Name	**Microsoft Entra ID (External)**
Description	
In Scope	True
Type	Server

Name	Microsoft Entra ID (External)
Finding Count	44

Threats

- ▶ 89 – INP03 – Server Side Include (SSI) Injection
- ▶ 90 – INP05 – Command Line Execution through SQL Injection
- ▶ 91 – AA01 – Authentication Abuse/ByPass
- ▶ 92 – DS01 – Excavation
- ▶ 93 – DE02 – Double Encoding
- ▶ 94 – AC01 – Privilege Abuse
- ▶ 95 – DO01 – Flooding
- ▶ 96 – HA01 – Path Traversal
- ▶ 97 – DO02 – Excessive Allocation
- ▶ 98 – INP08 – Format String Injection
- ▶ 99 – INP09 – LDAP Injection
- ▶ 100 – INP10 – Parameter Injection
- ▶ 101 – INP11 – Relative Path Traversal
- ▶ 102 – INP14 – Input Data Manipulation
- ▶ 103 – CR03 – Dictionary-based Password Attack
- ▶ 104 – DS03 – Footprinting
- ▶ 105 – AC06 – Using Malicious Files
- ▶ 106 – HA03 – Web Application Fingerprinting
- ▶ 107 – SC02 – XSS Targeting Non-Script Elements
- ▶ 108 – AC07 – Exploiting Incorrectly Configured Access Control Security Levels
- ▶ 109 – SC03 – Embedding Scripts within Scripts
- ▶ 110 – INP16 – PHP Remote File Inclusion
- ▶ 111 – AA02 – Principal Spoof
- ▶ 112 – DS04 – XSS Targeting Error Pages
- ▶ 113 – SC04 – XSS Using Alternate Syntax
- ▶ 114 – CR05 – Encryption Brute Forcing
- ▶ 115 – AC08 – Manipulate Registry Information
- ▶ 116 – SC05 – Removing Important Client Functionality
- ▶ 117 – INP17 – XSS Using MIME Type Mismatch
- ▶ 118 – AA03 – Exploitation of Trusted Credentials
- ▶ 119 – AC09 – Functionality Misuse
- ▶ 120 – INP18 – Fuzzing and observing application log data/errors for application mapping
- ▶ 121 – AA04 – Exploiting Trust in Client
- ▶ 122 – INP19 – XML External Entities Blowup
- ▶ 123 – AC11 – Session Credential Falsification through Manipulation
- ▶ 124 – INP21 – DTD Injection
- ▶ 125 – INP22 – XML Attribute Blowup
- ▶ 126 – INP28 – XSS Targeting URI Placeholders
- ▶ 127 – INP29 – XSS Using Doubled Characters
- ▶ 128 – INP34 – SOAP Array Overflow
- ▶ 129 – INP36 – HTTP Response Smuggling
- ▶ 130 – INP37 – HTTP Request Smuggling
- ▶ 131 – AC16 – Session Credential Falsification through Prediction
- ▶ 132 – AC17 – Session Hijacking - ServerSide

Name	Azure Virtual Desktop
Description	

Name	Azure Virtual Desktop
In Scope	True
Type	Server
Finding Count	44

Threats

- ▶ 133 – INP03 – Server Side Include (SSI) Injection
- ▶ 134 – INP05 – Command Line Execution through SQL Injection
- ▶ 135 – AA01 – Authentication Abuse/ByPass
- ▶ 136 – DS01 – Excavation
- ▶ 137 – DE02 – Double Encoding
- ▶ 138 – AC01 – Privilege Abuse
- ▶ 139 – DO01 – Flooding
- ▶ 140 – HA01 – Path Traversal
- ▶ 141 – DO02 – Excessive Allocation
- ▶ 142 – INP08 – Format String Injection
- ▶ 143 – INP09 – LDAP Injection
- ▶ 144 – INP10 – Parameter Injection
- ▶ 145 – INP11 – Relative Path Traversal
- ▶ 146 – INP14 – Input Data Manipulation
- ▶ 147 – CR03 – Dictionary-based Password Attack
- ▶ 148 – DS03 – Footprinting
- ▶ 149 – AC06 – Using Malicious Files
- ▶ 150 – HA03 – Web Application Fingerprinting
- ▶ 151 – SC02 – XSS Targeting Non-Script Elements
- ▶ 152 – AC07 – Exploiting Incorrectly Configured Access Control Security Levels
- ▶ 153 – SC03 – Embedding Scripts within Scripts
- ▶ 154 – INP16 – PHP Remote File Inclusion
- ▶ 155 – AA02 – Principal Spoof
- ▶ 156 – DS04 – XSS Targeting Error Pages
- ▶ 157 – SC04 – XSS Using Alternate Syntax
- ▶ 158 – CR05 – Encryption Brute Forcing
- ▶ 159 – AC08 – Manipulate Registry Information
- ▶ 160 – SC05 – Removing Important Client Functionality
- ▶ 161 – INP17 – XSS Using MIME Type Mismatch
- ▶ 162 – AA03 – Exploitation of Trusted Credentials
- ▶ 163 – AC09 – Functionality Misuse
- ▶ 164 – INP18 – Fuzzing and observing application log data/errors for application mapping
- ▶ 165 – AA04 – Exploiting Trust in Client
- ▶ 166 – INP19 – XML External Entities Blowup
- ▶ 167 – AC11 – Session Credential Falsification through Manipulation
- ▶ 168 – INP21 – DTD Injection
- ▶ 169 – INP22 – XML Attribute Blowup
- ▶ 170 – INP28 – XSS Targeting URI Placeholders
- ▶ 171 – INP29 – XSS Using Doubled Characters
- ▶ 172 – INP34 – SOAP Array Overflow
- ▶ 173 – INP36 – HTTP Response Smuggling
- ▶ 174 – INP37 – HTTP Request Smuggling
- ▶ 175 – AC16 – Session Credential Falsification through Prediction
- ▶ 176 – AC17 – Session Hijacking - ServerSide

Name	Microsoft Sentinel
Description	
In Scope	True
Type	Server
Finding Count	44

Threats

- ▶ 177 – INP03 – Server Side Include (SSI) Injection
- ▶ 178 – INP05 – Command Line Execution through SQL Injection
- ▶ 179 – AA01 – Authentication Abuse/ByPass
- ▶ 180 – DS01 – Excavation
- ▶ 181 – DE02 – Double Encoding
- ▶ 182 – AC01 – Privilege Abuse
- ▶ 183 – DO01 – Flooding
- ▶ 184 – HA01 – Path Traversal
- ▶ 185 – DO02 – Excessive Allocation
- ▶ 186 – INP08 – Format String Injection
- ▶ 187 – INP09 – LDAP Injection
- ▶ 188 – INP10 – Parameter Injection
- ▶ 189 – INP11 – Relative Path Traversal
- ▶ 190 – INP14 – Input Data Manipulation
- ▶ 191 – CR03 – Dictionary-based Password Attack
- ▶ 192 – DS03 – Footprinting
- ▶ 193 – AC06 – Using Malicious Files
- ▶ 194 – HA03 – Web Application Fingerprinting
- ▶ 195 – SC02 – XSS Targeting Non-Script Elements
- ▶ 196 – AC07 – Exploiting Incorrectly Configured Access Control Security Levels
- ▶ 197 – SC03 – Embedding Scripts within Scripts
- ▶ 198 – INP16 – PHP Remote File Inclusion
- ▶ 199 – AA02 – Principal Spoof
- ▶ 200 – DS04 – XSS Targeting Error Pages
- ▶ 201 – SC04 – XSS Using Alternate Syntax
- ▶ 202 – CR05 – Encryption Brute Forcing
- ▶ 203 – AC08 – Manipulate Registry Information
- ▶ 204 – SC05 – Removing Important Client Functionality
- ▶ 205 – INP17 – XSS Using MIME Type Mismatch
- ▶ 206 – AA03 – Exploitation of Trusted Credentials
- ▶ 207 – AC09 – Functionality Misuse
- ▶ 208 – INP18 – Fuzzing and observing application log data/errors for application mapping
- ▶ 209 – AA04 – Exploiting Trust in Client
- ▶ 210 – INP19 – XML External Entities Blowup
- ▶ 211 – AC11 – Session Credential Falsification through Manipulation
- ▶ 212 – INP21 – DTD Injection
- ▶ 213 – INP22 – XML Attribute Blowup
- ▶ 214 – INP28 – XSS Targeting URI Placeholders
- ▶ 215 – INP29 – XSS Using Doubled Characters
- ▶ 216 – INP34 – SOAP Array Overflow
- ▶ 217 – INP36 – HTTP Response Smuggling
- ▶ 218 – INP37 – HTTP Request Smuggling
- ▶ 219 – AC16 – Session Credential Falsification through Prediction

- 220 – AC17 – Session Hijacking - ServerSide

Name	Azure App Services
Description	
In Scope	True
Type	Server
Finding Count	44

Threats

- 221 – INP03 – Server Side Include (SSI) Injection
- 222 – INP05 – Command Line Execution through SQL Injection
- 223 – AA01 – Authentication Abuse/ByPass
- 224 – DS01 – Excavation
- 225 – DE02 – Double Encoding
- 226 – AC01 – Privilege Abuse
- 227 – DO01 – Flooding
- 228 – HA01 – Path Traversal
- 229 – DO02 – Excessive Allocation
- 230 – INP08 – Format String Injection
- 231 – INP09 – LDAP Injection
- 232 – INP10 – Parameter Injection
- 233 – INP11 – Relative Path Traversal
- 234 – INP14 – Input Data Manipulation
- 235 – CR03 – Dictionary-based Password Attack
- 236 – DS03 – Footprinting
- 237 – AC06 – Using Malicious Files
- 238 – HA03 – Web Application Fingerprinting
- 239 – SC02 – XSS Targeting Non-Script Elements
- 240 – AC07 – Exploiting Incorrectly Configured Access Control Security Levels
- 241 – SC03 – Embedding Scripts within Scripts
- 242 – INP16 – PHP Remote File Inclusion
- 243 – AA02 – Principal Spoof
- 244 – DS04 – XSS Targeting Error Pages
- 245 – SC04 – XSS Using Alternate Syntax
- 246 – CR05 – Encryption Brute Forcing
- 247 – AC08 – Manipulate Registry Information
- 248 – SC05 – Removing Important Client Functionality
- 249 – INP17 – XSS Using MIME Type Mismatch
- 250 – AA03 – Exploitation of Trusted Credentials
- 251 – AC09 – Functionality Misuse
- 252 – INP18 – Fuzzing and observing application log data/errors for application mapping
- 253 – AA04 – Exploiting Trust in Client
- 254 – INP19 – XML External Entities Blowup
- 255 – AC11 – Session Credential Falsification through Manipulation
- 256 – INP21 – DTD Injection
- 257 – INP22 – XML Attribute Blowup
- 258 – INP28 – XSS Targeting URI Placeholders
- 259 – INP29 – XSS Using Doubled Characters
- 260 – INP34 – SOAP Array Overflow
- 261 – INP36 – HTTP Response Smuggling
- 262 – INP37 – HTTP Request Smuggling

- 263 – AC16 – Session Credential Falsification through Prediction
- 264 – AC17 – Session Hijacking - ServerSide

Name	Website Backend files
Description	
In Scope	True
Type	Datastore
Finding Count	4

Threats
- 265 – AC01 – Privilege Abuse
- 266 – DO02 – Excessive Allocation
- 267 – CR05 – Encryption Brute Forcing
- 268 – DE04 – Audit Log Manipulation

Name	Cyber Library
Description	
In Scope	True
Type	Datastore
Finding Count	4

Threats
- 269 – AC01 – Privilege Abuse
- 270 – DO02 – Excessive Allocation
- 271 – CR05 – Encryption Brute Forcing
- 272 – DE04 – Audit Log Manipulation

Name	Client Data Storage
Description	
In Scope	True
Type	Datastore
Finding Count	4

Threats
- 273 – AC01 – Privilege Abuse
- 274 – DO02 – Excessive Allocation
- 275 – CR05 – Encryption Brute Forcing
- 276 – DE04 – Audit Log Manipulation

Name	Azure SQL
Description	
In Scope	True
Type	Datastore
Finding Count	4

Threats

- 277 – AC01 – Privilege Abuse
- 278 – DO02 – Excessive Allocation
- 279 – CR05 – Encryption Brute Forcing
- 280 – DE04 – Audit Log Manipulation

Name	HR Storage
Description	
In Scope	True
Type	Datastore
Finding Count	4

Threats

- 281 – AC01 – Privilege Abuse
- 282 – DO02 – Excessive Allocation
- 283 – CR05 – Encryption Brute Forcing
- 284 – DE04 – Audit Log Manipulation

Name	3rd Party Accounting Firm
Description	
In Scope	True
Type	ExternalEntity
Finding Count	0

Data Flows

Name	Phishing Email (Spearphishing)
Description	
Sink	Actor(HR Staff)
Source	Actor(Potential Attacker)
Is Response	False
In Scope	True
Finding Count	7

Threats

- 285 – DE01 – Interception
- 286 – AC05 – Content Spoofing
- 287 – DE03 – Sniffing Attacks
- 288 – CR06 – Communication Channel Manipulation
- 289 – CR08 – Client-Server Protocol Manipulation
- 290 – DS06 – Data Leak
- 291 – DR01 – Unprotected Sensitive Data

Name	Admin Login / Auth
Description	
Sink	Server(Microsoft Entra ID (Internal))
Source	Actor(System and Administrator Staffs)
Is Response	False
In Scope	True
Finding Count	7

Threats

- 292 – DE01 – Interception
- 293 – AC05 – Content Spoofing
- 294 – DE03 – Sniffing Attacks
- 295 – CR06 – Communication Channel Manipulation
- 296 – CR08 – Client-Server Protocol Manipulation
- 297 – DS06 – Data Leak
- 298 – DR01 – Unprotected Sensitive Data

Name	HR Workflow Auth
Description	
Sink	Server(Microsoft Entra ID (Internal))
Source	Actor(HR Staff)
Is Response	False
In Scope	True
Finding Count	7

Threats

- 299 – DE01 – Interception
- 300 – AC05 – Content Spoofing
- 301 – DE03 – Sniffing Attacks
- 302 – CR06 – Communication Channel Manipulation
- 303 – CR08 – Client-Server Protocol Manipulation
- 304 – DS06 – Data Leak
- 305 – DR01 – Unprotected Sensitive Data

Name	Website Maintenance, Cyber Library, client Data
Description	
Sink	Server(Microsoft Entra ID (Internal))
Source	Actor(Consulting, Dev, Finance, Sales Staffs)
Is Response	False
In Scope	True
Finding Count	7

Threats

- 306 – DE01 – Interception
- 307 – AC05 – Content Spoofing
- 308 – DE03 – Sniffing Attacks
- 309 – CR06 – Communication Channel Manipulation
- 310 – CR08 – Client-Server Protocol Manipulation
- 311 – DS06 – Data Leak
- 312 – DR01 – Unprotected Sensitive Data

Name	**Accessing 3rd Party Firm**
Description	
Sink	Server(Microsoft Entra Internet access)
Source	Actor(VP Sales)
Is Response	False
In Scope	True
Finding Count	7

Threats

- 313 – DE01 – Interception
- 314 – AC05 – Content Spoofing
- 315 – DE03 – Sniffing Attacks
- 316 – CR06 – Communication Channel Manipulation
- 317 – CR08 – Client-Server Protocol Manipulation
- 318 – DS06 – Data Leak
- 319 – DR01 – Unprotected Sensitive Data

Name	**Mobile Access**
Description	
Sink	Server(Microsoft Entra ID (Internal))
Source	Actor(VP Sales)
Is Response	False
In Scope	True
Finding Count	7

Threats

- 320 – DE01 – Interception
- 321 – AC05 – Content Spoofing
- 322 – DE03 – Sniffing Attacks
- 323 – CR06 – Communication Channel Manipulation
- 324 – CR08 – Client-Server Protocol Manipulation
- 325 – DS06 – Data Leak
- 326 – DR01 – Unprotected Sensitive Data

Name	**Accessing Client Portal**
Description	

Name	Accessing Client Portal
Sink	Server(Microsoft Entra ID (External))
Source	Actor(Clients/Customers)
Is Response	False
In Scope	True
Finding Count	5

Threats

- 327 – DE01 – Interception
- 328 – AC05 – Content Spoofing
- 329 – DE03 – Sniffing Attacks
- 330 – CR06 – Communication Channel Manipulation
- 331 – CR08 – Client-Server Protocol Manipulation

Name	Browsing Company Website
Description	
Sink	Server(Azure App Services)
Source	Actor(Website Visitors)
Is Response	False
In Scope	True
Finding Count	5

Threats

- 332 – DE01 – Interception
- 333 – AC05 – Content Spoofing
- 334 – DE03 – Sniffing Attacks
- 335 – CR06 – Communication Channel Manipulation
- 336 – CR08 – Client-Server Protocol Manipulation

Name	Job Application Data
Description	
Sink	Server(Azure App Services)
Source	Actor(Job Applicants)
Is Response	False
In Scope	True
Finding Count	7

Threats

- 337 – DE01 – Interception
- 338 – AC05 – Content Spoofing
- 339 – DE03 – Sniffing Attacks
- 340 – CR06 – Communication Channel Manipulation
- 341 – CR08 – Client-Server Protocol Manipulation

- ▶ 342 – DS06 – Data Leak
- ▶ 343 – DR01 – Unprotected Sensitive Data

Name	Authenticated Access
Description	
Sink	Server(Azure Virtual Desktop)
Source	Server(Microsoft Entra ID (Internal))
Is Response	False
In Scope	True
Finding Count	7

Threats

- ▶ 344 – DE01 – Interception
- ▶ 345 – AC05 – Content Spoofing
- ▶ 346 – DE03 – Sniffing Attacks
- ▶ 347 – CR06 – Communication Channel Manipulation
- ▶ 348 – CR08 – Client-Server Protocol Manipulation
- ▶ 349 – DS06 – Data Leak
- ▶ 350 – DR01 – Unprotected Sensitive Data

Name	Identity Logs
Description	
Sink	Server(Microsoft Sentinel)
Source	Server(Microsoft Entra ID (Internal))
Is Response	False
In Scope	True
Finding Count	7

Threats

- ▶ 351 – DE01 – Interception
- ▶ 352 – AC05 – Content Spoofing
- ▶ 353 – DE03 – Sniffing Attacks
- ▶ 354 – CR06 – Communication Channel Manipulation
- ▶ 355 – CR08 – Client-Server Protocol Manipulation
- ▶ 356 – DS06 – Data Leak
- ▶ 357 – DR01 – Unprotected Sensitive Data

Name	Network Logs
Description	
Sink	Server(Microsoft Sentinel)
Source	Server(Microsoft Entra Internet access)
Is Response	False
In Scope	True

Name	Network Logs
Finding Count	5

Threats

- 358 – DE01 – Interception
- 359 – AC05 – Content Spoofing
- 360 – DE03 – Sniffing Attacks
- 361 – CR06 – Communication Channel Manipulation
- 362 – CR08 – Client-Server Protocol Manipulation

Name	Mobile Access Tunnel
Description	
Sink	Server(Azure App Services)
Source	Server(Microsoft Entra Internet access)
Is Response	False
In Scope	True
Finding Count	5

Threats

- 363 – DE01 – Interception
- 364 – AC05 – Content Spoofing
- 365 – DE03 – Sniffing Attacks
- 366 – CR06 – Communication Channel Manipulation
- 367 – CR08 – Client-Server Protocol Manipulation

Name	External Auth Logs
Description	
Sink	Server(Microsoft Sentinel)
Source	Server(Microsoft Entra ID (External))
Is Response	False
In Scope	True
Finding Count	5

Threats

- 368 – DE01 – Interception
- 369 – AC05 – Content Spoofing
- 370 – DE03 – Sniffing Attacks
- 371 – CR06 – Communication Channel Manipulation
- 372 – CR08 – Client-Server Protocol Manipulation

Name	Accessing Client Portal
Description	
Sink	Server(Azure App Services)

Name	Accessing Client Portal
Source	Server(Microsoft Entra ID (External))
Is Response	False
In Scope	True
Finding Count	5

Threats

- 373 – DE01 – Interception
- 374 – AC05 – Content Spoofing
- 375 – DE03 – Sniffing Attacks
- 376 – CR06 – Communication Channel Manipulation
- 377 – CR08 – Client-Server Protocol Manipulation

Name	Accessing 3rd Party Firm
Description	
Sink	ExternalEntity(3rd Party Accounting Firm)
Source	Server(Microsoft Entra Internet access)
Is Response	False
In Scope	True
Finding Count	5

Threats

- 378 – DE01 – Interception
- 379 – AC05 – Content Spoofing
- 380 – DE03 – Sniffing Attacks
- 381 – CR06 – Communication Channel Manipulation
- 382 – CR08 – Client-Server Protocol Manipulation

Name	Host Logs (Sysmon/WinEvent)
Description	
Sink	Server(Microsoft Sentinel)
Source	Server(Azure Virtual Desktop)
Is Response	False
In Scope	True
Finding Count	5

Threats

- 383 – DE01 – Interception
- 384 – AC05 – Content Spoofing
- 385 – DE03 – Sniffing Attacks
- 386 – CR06 – Communication Channel Manipulation
- 387 – CR08 – Client-Server Protocol Manipulation

Name	Website Maintenance (SMB/NFS)
Description	
Sink	Datastore(Website Backend files)
Source	Server(Azure Virtual Desktop)
Is Response	False
In Scope	True
Finding Count	5

Threats

- ▶ 388 – DE01 – Interception
- ▶ 389 – AC05 – Content Spoofing
- ▶ 390 – DE03 – Sniffing Attacks
- ▶ 391 – CR06 – Communication Channel Manipulation
- ▶ 392 – CR08 – Client-Server Protocol Manipulation

Name	Read Cyber Library
Description	
Sink	Datastore(Cyber Library)
Source	Server(Azure Virtual Desktop)
Is Response	False
In Scope	True
Finding Count	5

Threats

- ▶ 393 – DE01 – Interception
- ▶ 394 – AC05 – Content Spoofing
- ▶ 395 – DE03 – Sniffing Attacks
- ▶ 396 – CR06 – Communication Channel Manipulation
- ▶ 397 – CR08 – Client-Server Protocol Manipulation

Name	Read/Write Client Data
Description	
Sink	Datastore(Client Data Storage)
Source	Server(Azure Virtual Desktop)
Is Response	False
In Scope	True
Finding Count	7

Threats

- ▶ 398 – DE01 – Interception
- ▶ 399 – AC05 – Content Spoofing
- ▶ 400 – DE03 – Sniffing Attacks

- ▶ 401 – CR06 – Communication Channel Manipulation
- ▶ 402 – CR08 – Client-Server Protocol Manipulation
- ▶ 403 – DS06 – Data Leak
- ▶ 404 – DR01 – Unprotected Sensitive Data

Name	HR Workflow
Description	
Sink	Datastore(HR Storage)
Source	Server(Azure Virtual Desktop)
Is Response	False
In Scope	True
Finding Count	7

Threats

- ▶ 405 – DE01 – Interception
- ▶ 406 – AC05 – Content Spoofing
- ▶ 407 – DE03 – Sniffing Attacks
- ▶ 408 – CR06 – Communication Channel Manipulation
- ▶ 409 – CR08 – Client-Server Protocol Manipulation
- ▶ 410 – DS06 – Data Leak
- ▶ 411 – DR01 – Unprotected Sensitive Data

Name	Client Payment Transfer
Description	
Sink	ExternalEntity(3rd Party Accounting Firm)
Source	Server(Azure App Services)
Is Response	False
In Scope	True
Finding Count	7

Threats

- ▶ 412 – DE01 – Interception
- ▶ 413 – AC05 – Content Spoofing
- ▶ 414 – DE03 – Sniffing Attacks
- ▶ 415 – CR06 – Communication Channel Manipulation
- ▶ 416 – CR08 – Client-Server Protocol Manipulation
- ▶ 417 – DS06 – Data Leak
- ▶ 418 – DR01 – Unprotected Sensitive Data

Name	App Logs
Description	
Sink	Server(Microsoft Sentinel)
Source	Server(Azure App Services)

Name	App Logs
Is Response	False
In Scope	True
Finding Count	5

Threats

- 419 – DE01 – Interception
- 420 – AC05 – Content Spoofing
- 421 – DE03 – Sniffing Attacks
- 422 – CR06 – Communication Channel Manipulation
- 423 – CR08 – Client-Server Protocol Manipulation

Name	Backend Queries
Description	
Sink	Datastore(Azure SQL)
Source	Server(Azure App Services)
Is Response	False
In Scope	True
Finding Count	5

Threats

- 424 – DE01 – Interception
- 425 – AC05 – Content Spoofing
- 426 – DE03 – Sniffing Attacks
- 427 – CR06 – Communication Channel Manipulation
- 428 – CR08 – Client-Server Protocol Manipulation

Name	Store Job Applicant
Description	
Sink	Datastore(HR Storage)
Source	Server(Azure App Services)
Is Response	False
In Scope	True
Finding Count	7

Threats

- 429 – DE01 – Interception
- 430 – AC05 – Content Spoofing
- 431 – DE03 – Sniffing Attacks
- 432 – CR06 – Communication Channel Manipulation
- 433 – CR08 – Client-Server Protocol Manipulation
- 434 – DS06 – Data Leak
- 435 – DR01 – Unprotected Sensitive Data