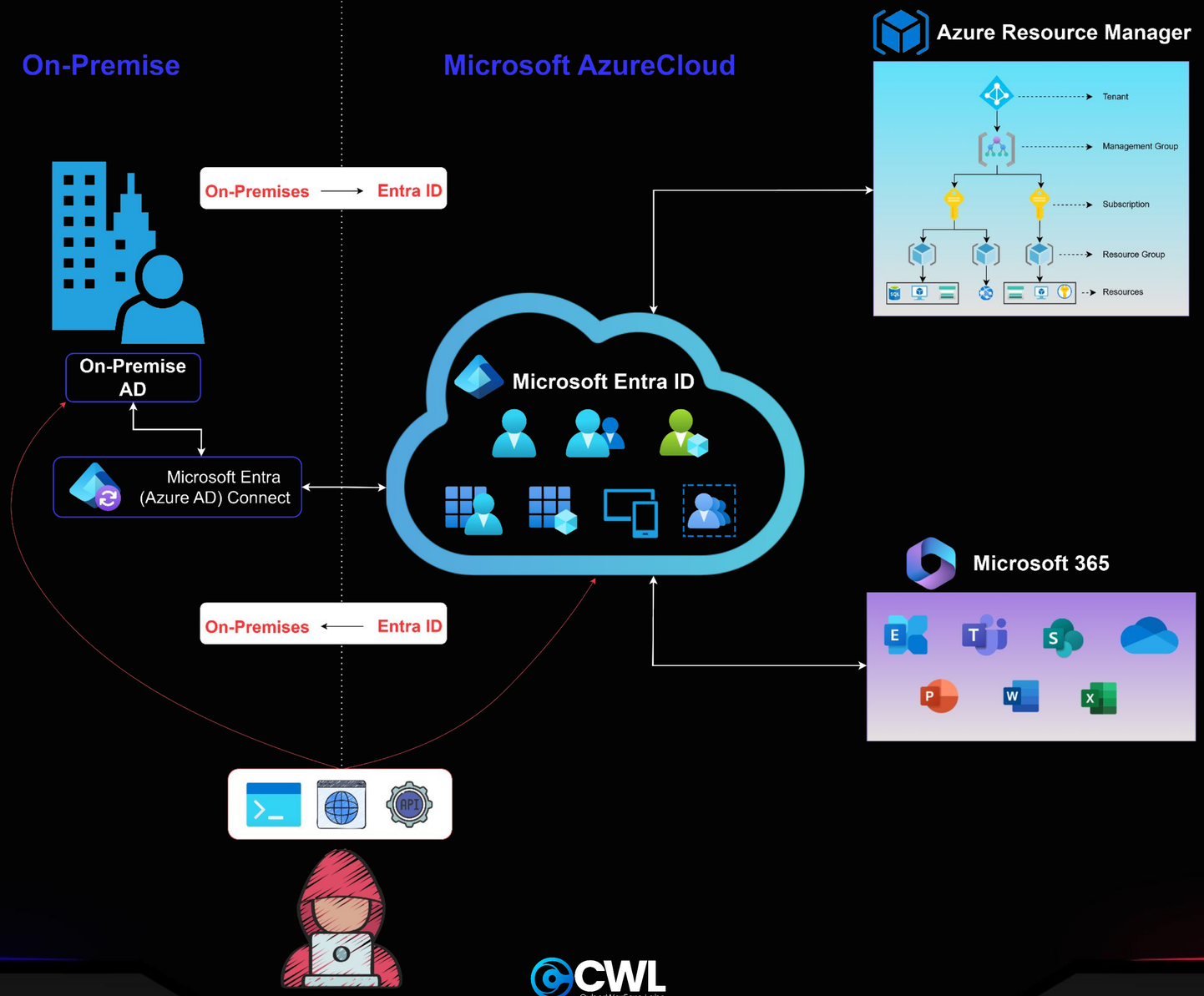
CWL
CyberWarFare Labs

Azure Red Team Specialist (Az-RTS)

Azure Red Team Specialist (Az-RTS) Architecture



CWL
CyberWarFare Labs

Module-1:
Introduction to Azure

- Overview of Azure cloud computing platform, including core services, cloud concepts, and benefits such as scalability, availability, and cost efficiency.

I. Introduction to Azure

- What is Azure?
- Azure Architecture for Red Teaming
- Control Plane V/S Data Plane
- Authentication Flow for Microsoft Graph API
- Cyber Kill Chain in Azure
- Red Team Objectives in Azure
- Attack lifecycle inside Azure
- Azure Threat Research Matrix
- MITRE ATT&CK for Cloud

Module-2:
Microsoft Entra ID (AAD)

- Explains how Azure resources are deployed, managed, and organized using ARM, including resource groups, templates, and access control.

2.1: Fundamentals of Entra ID

- What is Entra ID?
- Identity Types in Entra ID
- Administrative Units (AUs)
- Roles & Administrators
- Identity Governance - PIM
- Conditional Access Policies
- Entra ID Connect

2.2: Red Team Ops in Entra ID

- Anatomy of Attack
- Attack Overview
- Attack Demonstration

CWL
CyberWarFare Labs

Module-3:
Azure Resource Manager (ARM)

- Explains how Azure resources are deployed, managed, and organized using ARM, including resource groups, templates, and access control.

3.1: Fundamentals of Azure Resource Manager (ARM)

- What is ARM?
- Role based access control
- Managed Identities
- Resource Providers
  - Services
- Automation Account

3.2: Red Team Ops in Azure Resource Manager (ARM)

- Anatomy of Attack
- Attack Overview
- Attack Demonstration

CWL
CyberWarFare Labs

Module-4:
Microsoft 365 (M365)

- Overview of Microsoft 365 cloud productivity services such as email, collaboration, and document management using tools like Teams, Outlook, and OneDrive.

4.1: Fundamentals of Microsoft 365 (M365)

- What is M365?
- Services
- Authentication
- Admin Roles

4.2: Red Team Ops in Azure Resource Manager (ARM)

- Anatomy of Attack
- Attack Overview
- Attack Demonstration

CWL
CyberWarFare Labs

Module-5:
Lateral Movement

- Introduction to the concept of lateral movement in cybersecurity, where attackers move within a network to gain access to additional systems and sensitive resources.

5.1: On-premises to Entra ID

- Anatomy of Attack
- Attack Overview
- Attack Demonstration

5.2: Entra ID to On-premises

- Anatomy of Attack
- Attack Overview
- Attack Demonstration

CWL
CyberWarFare Labs

Thank You

Cyberwarfare.live