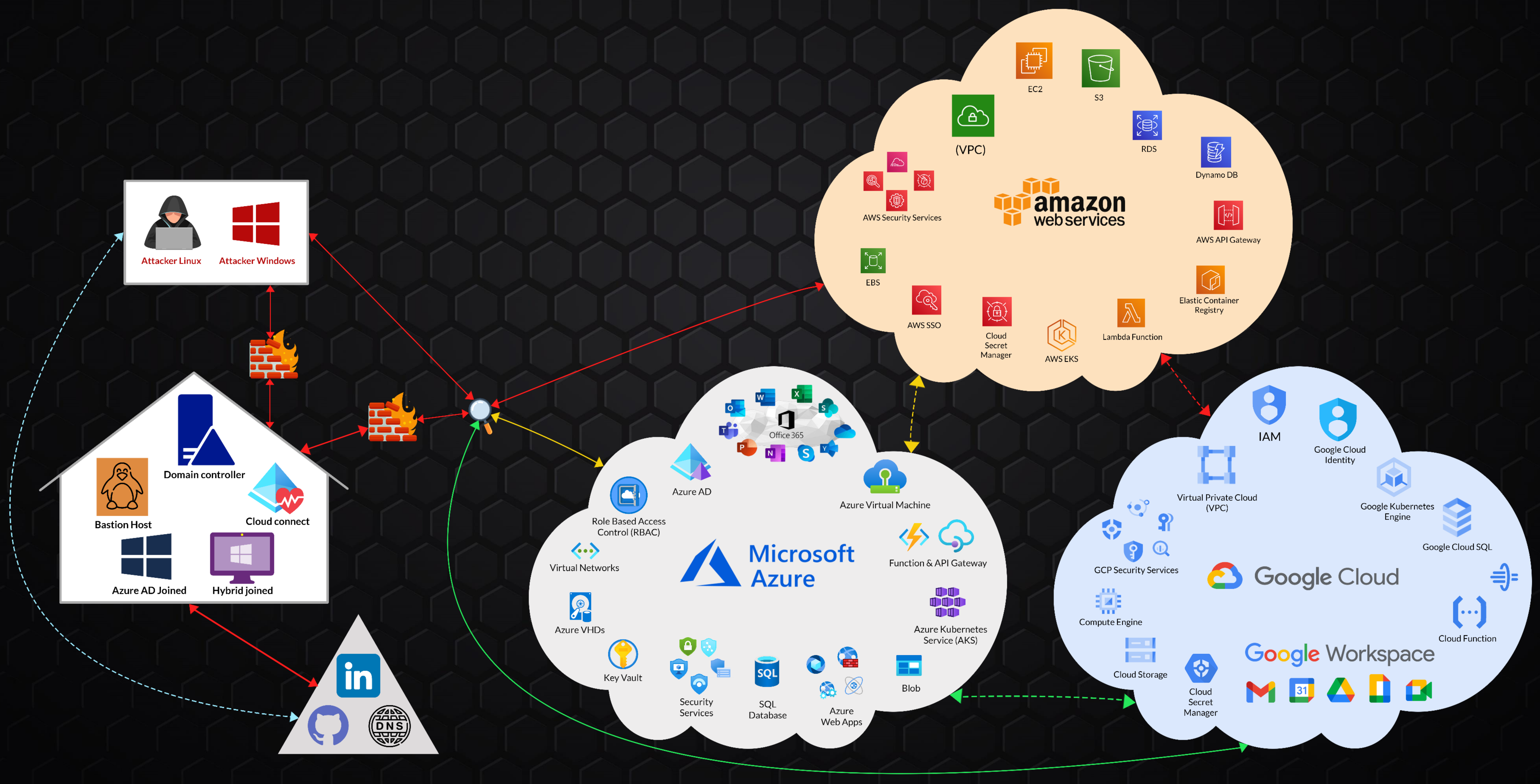
CWL

CyberWarFare Labs

Certified Hybrid Multi-cloud Red Team Specialist [CHMRTS]

@CyberWarFare Labs

Certified Hybrid Multi-cloud Red Team Specialist Architeture



CWL
CyberWarFare Labs

PART-1

Section 1 : Introduction & Enumeration Of Hybrid Multi Cloud Environment

CWL
CyberWarFare Labs

Module 1

Hybrid Multi Cloud Environment Overview

- On-Premise Architecture
- Multi Cloud Architecture
- Hybrid Multi Cloud Architecture
- On-Premise v/s Multi Cloud

Module 2

Introduction & Enumeration AWS Cloud Environment

- AWS Cloud Overview
- Identity & Access Management [IAM]
- AWS Federation Identity
- AWS Cross Account Access
- Automated and Manual Enumeration of AWS Environment

Module 3

Introduction & Enumeration Azure Cloud Environment

- Azure Active Directory [Idaas]
- Azure Resource Manager [IaaS, PaaS & SaaS]
- Azure Multi Tenant Access
- AAD Roles and Role Based Access Control
- Office 365 [0365]
- Automated and Manual Enumeration of Azure Environment

Module 4

Introduction & Enumeration Google Cloud Environment

- Cloud Identity [Idaas]
- Google Workspace [G-Suite]
- GCP Cross Project Access
- G-Suite Roles and Identity & Access Management
- Google Cloud Platform [IaaS, PaaS & SaaS]
- Automated and Manual Enumeration of GCP Environment

CWL
CyberWarFare Labs

Module 4

Introduction & Enumeration On-Premise [AD] Environment

- On-Premise Infrastructure Overview
- Active Directory Fundamentals
- AD Cross Forest Access
- Authentication & Authorization in Active Directory Environment
- On-Premise to Cloud Connectivity
- Automated and Manual Enumeration of AD Environment

PART-2

Section 2: Attacks In Hybrid Multi Cloud Environment

CWL
CyberWarFare Labs

Module 1

Reconnaissance [OSINT]

- Targeted Organization Profiling
- Multi Cloud Open Source Information Gathering
- Unauthenticated Service Enumeration
- Password Spray Attack
- Leaked AWS/ GCP/ Azure Cloud Credential

Module 2

Initial Access

- Exploiting Public Facing Application
- Gaining Access with Leaked Cloud Credential
- Spoofing Technique in On-Premise Environment
- Phishing [Consent Grant Attack] in Azure & GCP]

Module 3

Privilege Escalation

- Exploiting Serverless Function
- Misusing Azure Automation Account
- Exploiting Excess IAM Permission
- DCSync Attack

Module 4

Persistence

- AWS Cross Across Account Backdoor
- Abusing Azure Active Directory Applications Functionality
- Modifying GCP Service Account Configuration
- Golden Ticket Attack

Module 5

Credential Access

- Abusing AWS Role Identity
- Azure Key Vault Compromise
- Compromise Google Kubernetes Engine
- Memory Dumping

Module 6

Lateral Movement

- Breaking the Boundary of Virtual Private Network
- Azure Hybrid Joined Devices Compromise
- GCP Cross Project Compromise
- On-Premise to Cloud Lateral Movement by compromising Seamless SSO

PART-3

Section 3 : Red Team Ops In Hybrid Multi Cloud Environment

CWL
CyberWarFare Labs

Module 1

Red Team Ops Overview

- AWS v/s Azure v/s GCP v/s AD
- Red Team Infrastructure Setup
- Red Team Arsenal for Hybrid Multi Cloud Environment

Module 2

MITRE ATT&CK Enterprise & Cloud Matrix

- Unauthenticated Enumeration
- Initial Access
- Authenticated Enumeration
- Privilege Escalation
- Persistence
- Credential Access
- Discovery
- Lateral Movement
- Data Exfiltration

Module 3

Full Fledged Red Team Operations with Automated Tools & Scripts

- **Objective 1 :** Compromise Entire Organization from Cloud to On-Premise
- **Objective 2 : Compromise Entire Organization from On-Premise to Cloud**

CWL
CyberWarFare Labs

Thank You

Cyberwarfare.live