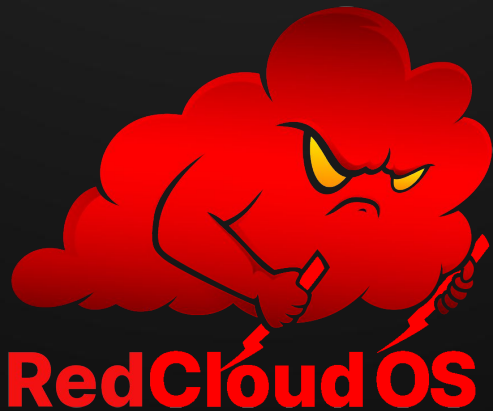




Attacking the cloud with RedCloud OS

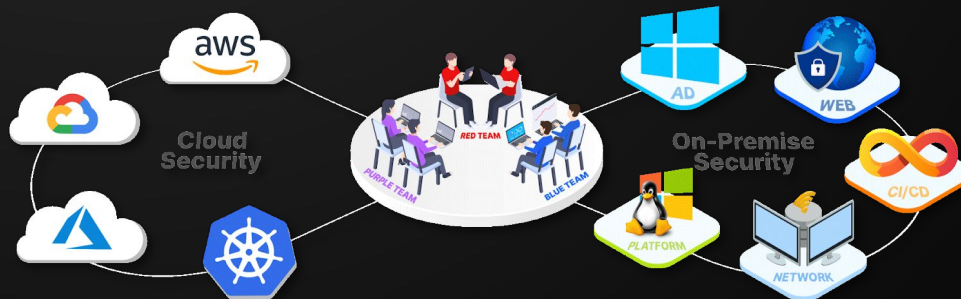


© All Rights Reserved CyberwarFare Labs

About CyberWarfare Labs :

CW Labs is a renowned Infosec company specializing in cybersecurity practical learning. They provide on-demand educational services. The company has 3 primary divisions :

- 1. Learning Management System (LMS) Platform**
- 2. CWL CyberSecurity Playground (CCSP) Platform**
- 3. Infinity Learning Platform**



INFINITE LEARNING EXPERIENCE

About Speaker :

Abhijeet Kumar **(Security Researcher)**

His research areas include Red Team Operations, Network Security, Cloud Infrastructure, and Linux Systems. Apart from this, he enjoys researching Adversarial TTPs and conducting experimenting in his homelab.

CLOUD 101

- ★ Compute resources which are globally distributed with high availability

CLOUD 101

- ★ Compute resources which are globally distributed with high availability
- ★ Ease of access & resource provisioning

CLOUD 101

- ★ Compute resources which are globally distributed with high availability
- ★ Ease of access & resource provisioning
- ★ Commonly used flavours include
 - Infrastructure as a Service (IaaS)
 - Platform as a Service (PaaS)
 - Software as a Service (SaaS)

CLOUD ACCESS 101

- ★ Ways to access cloud services:
 - Through web-based console through browser

CLOUD ACCESS 101

- ★ Ways to access cloud services:
 - Through web-based console through browser
 - With Command Line Interface (CLI)
 - E.g: AWS CLI, Azure CLI, Gcloud CLI

CLOUD ACCESS 101

★ Ways to access cloud services:

- Through web-based console through browser
- With Command Line Interface (CLI)
 - E.g: AWS CLI, Azure CLI, Gcloud CLI
- Programmatically through official Software Development Kits (SDKs) available in multiple languages
 - E.g: Boto3 (AWS), Azure SDK , Google Cloud SDK

CLOUD ACCESS 101

- ★ Credentials types used to access cloud services:
 - Username + Password (web-based console)

CLOUD ACCESS 101

- ★ Credentials types used to access cloud services:
 - Username + Password (web-based console)
 - Access Credentials:
 - Keys
 - Tokens
 - Service Accounts

CLOUD ACCESS 101

- ★ Credentials types used to access cloud services:
 - Username + Password (web-based console)
 - Access Credentials:
 - Keys
 - Tokens
 - Service Accounts
 - Federated Identities/Single Sign On (SSO)

REDCLOUD OS

- ★ Debian-based Cloud Adversary Simulation OS for Red Teams



REDCLOUD OS

- ★ Debian-based Cloud Adversary Simulation OS for Red Teams
- ★ Supports most of the Cloud Service Providers (CSPs)



REDCLOUD OS

- ★ Debian-based Cloud Adversary Simulation OS for Red Teams
- ★ Supports most of the Cloud Service Providers (CSPs)
- ★ Includes 50+ specialised tools for cloud security assessments



REDCLOUD OS

★ Available for x64 architecture



REDCLOUD OS

- ★ Available for x64 architecture
- ★ Future roadmap:
 - Support for Apple Silicon architecture
 - Automated tool updates via APT
 - Inclusion of more tools

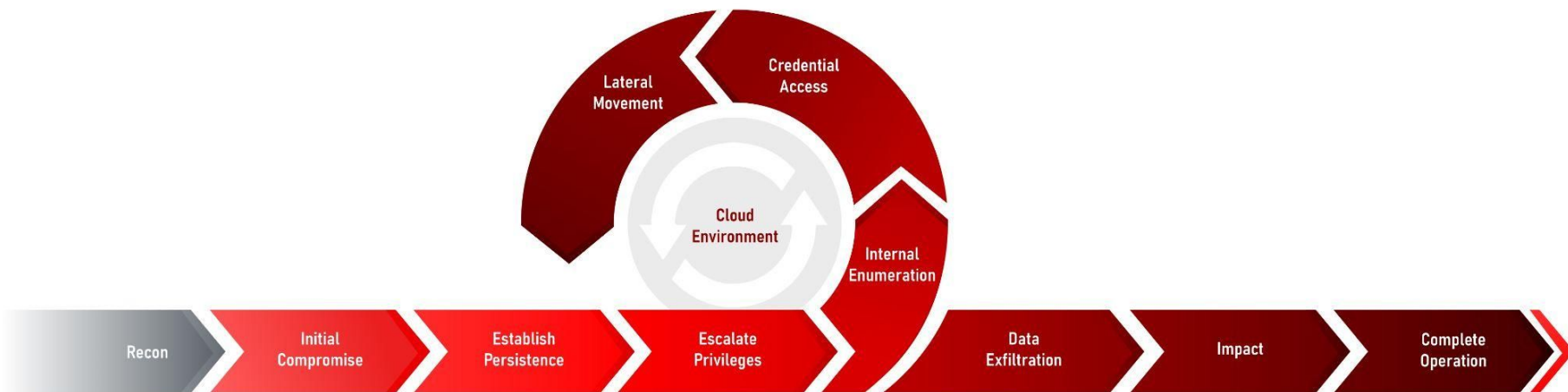


REDCLOUD OS

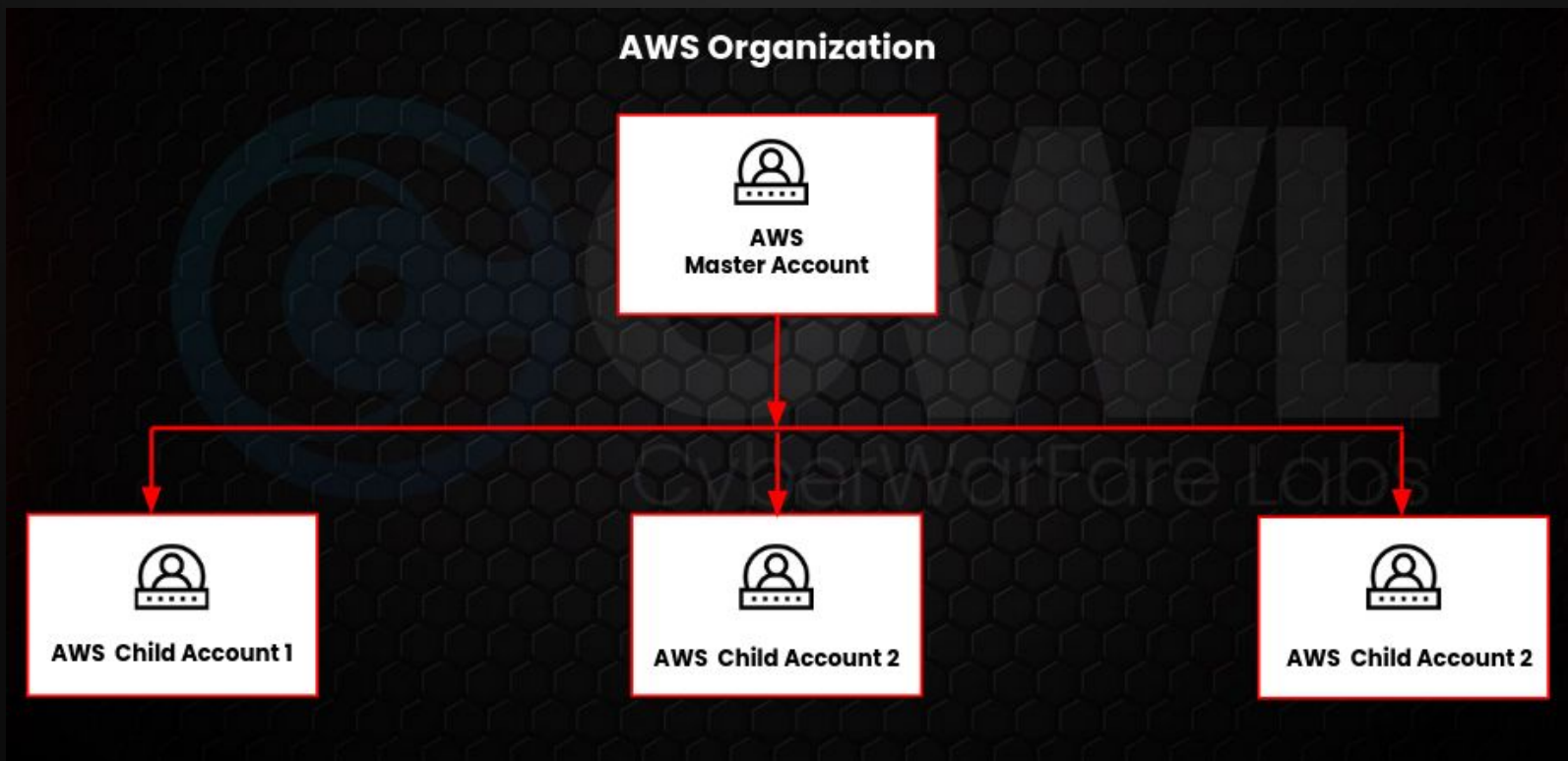
- ★ Available for x64 architecture
- ★ Future roadmap:
 - Support for Apple Silicon architecture
 - Automated tool updates via APT
 - Inclusion of more tools
- ★ Link: <https://linktr.ee/redcloudos>



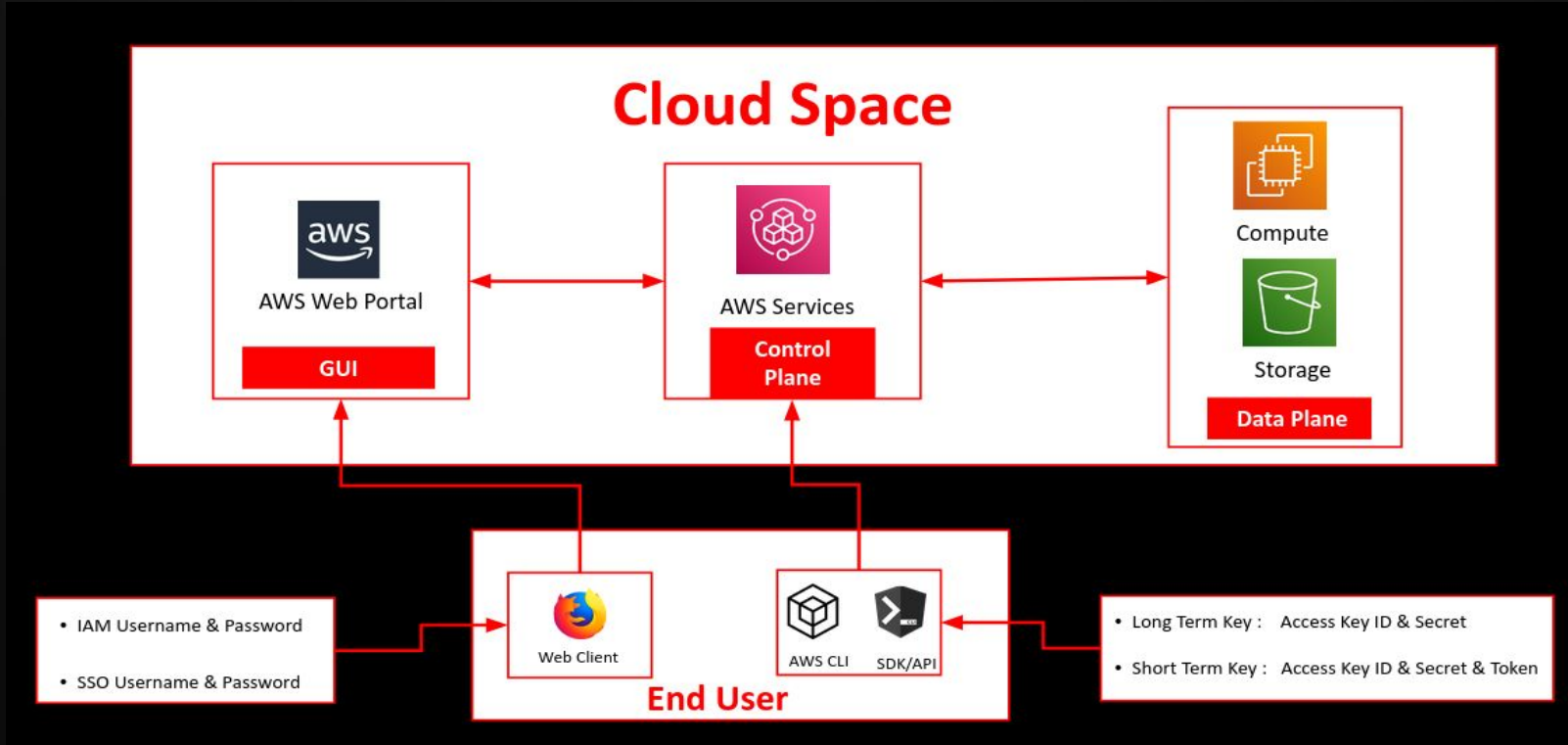
CLOUD ATTACK LIFECYCLE



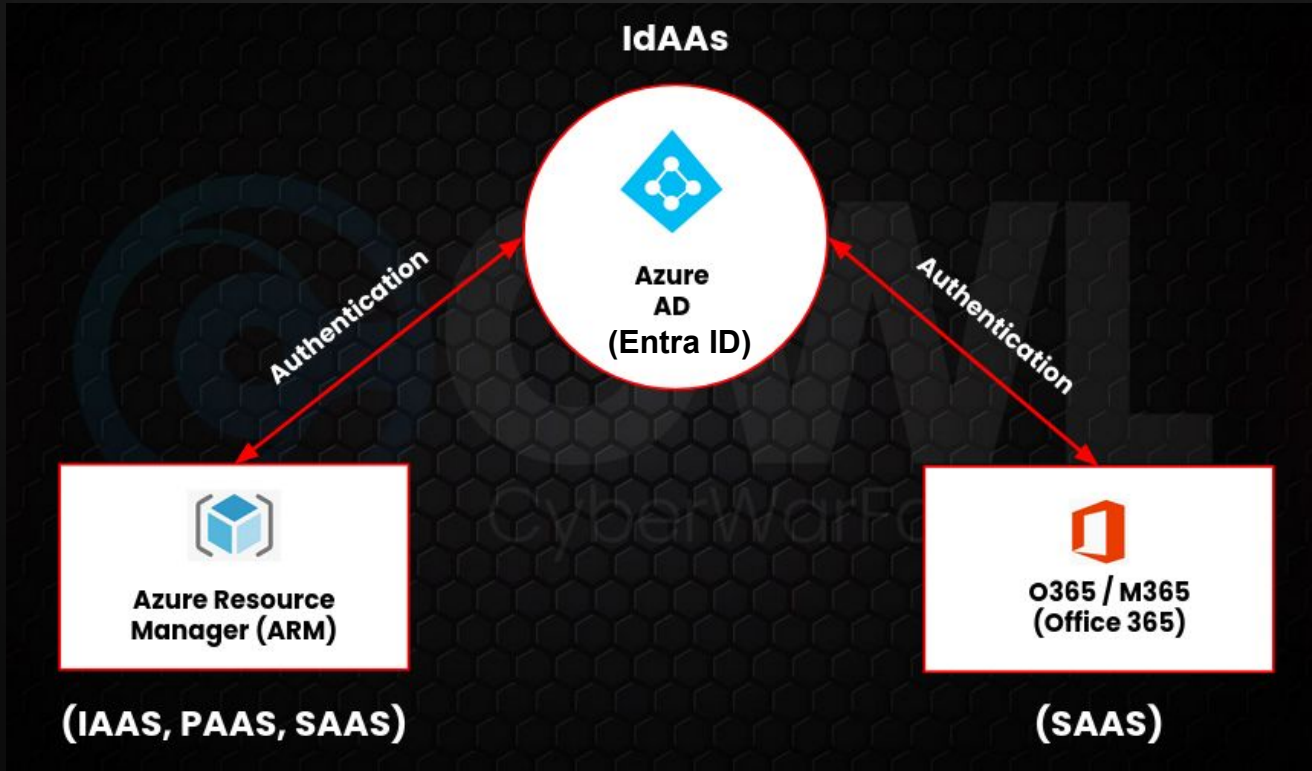
AWS MULTI ACCOUNTS HIERARCHY



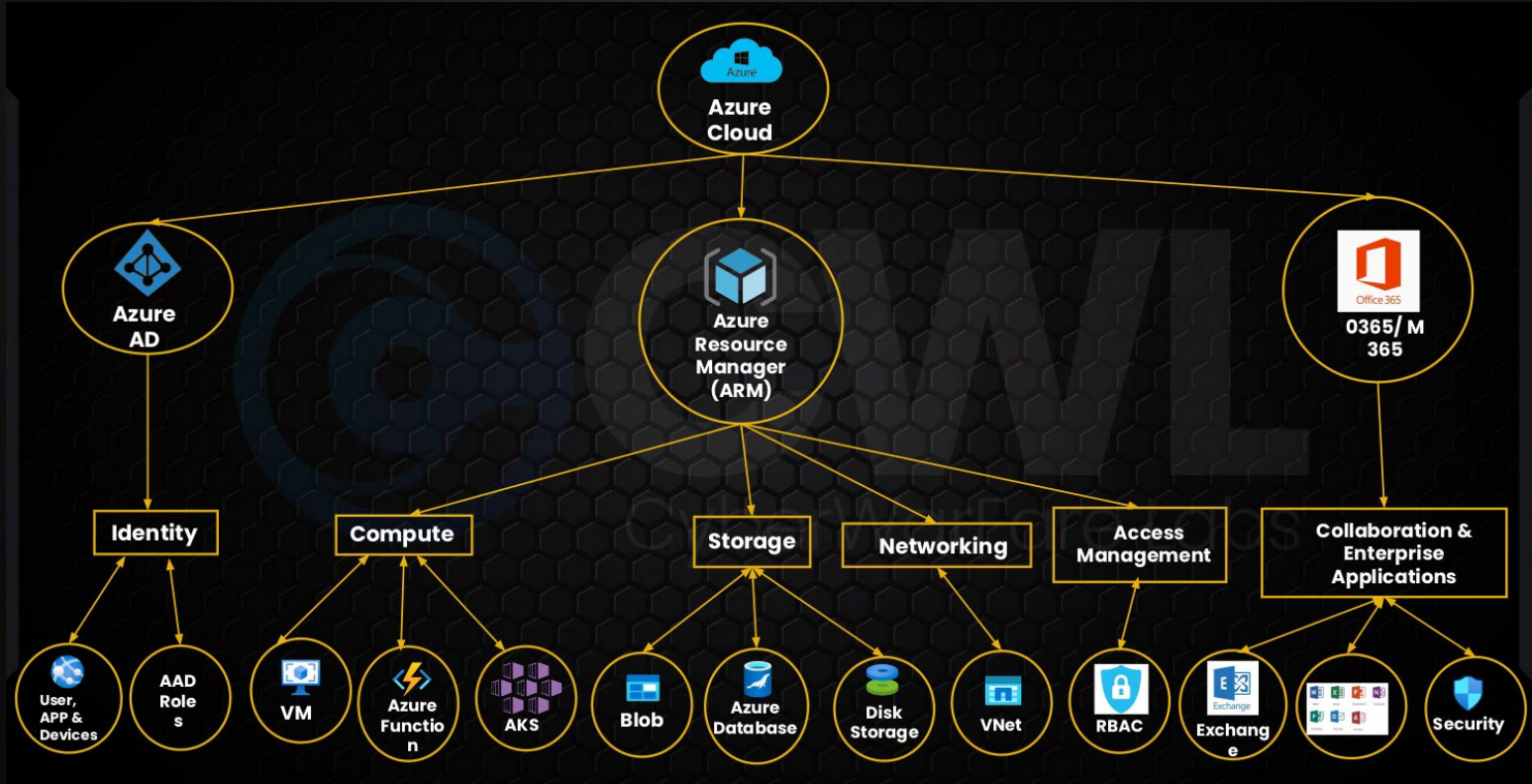
AWS ARCHITECTURE



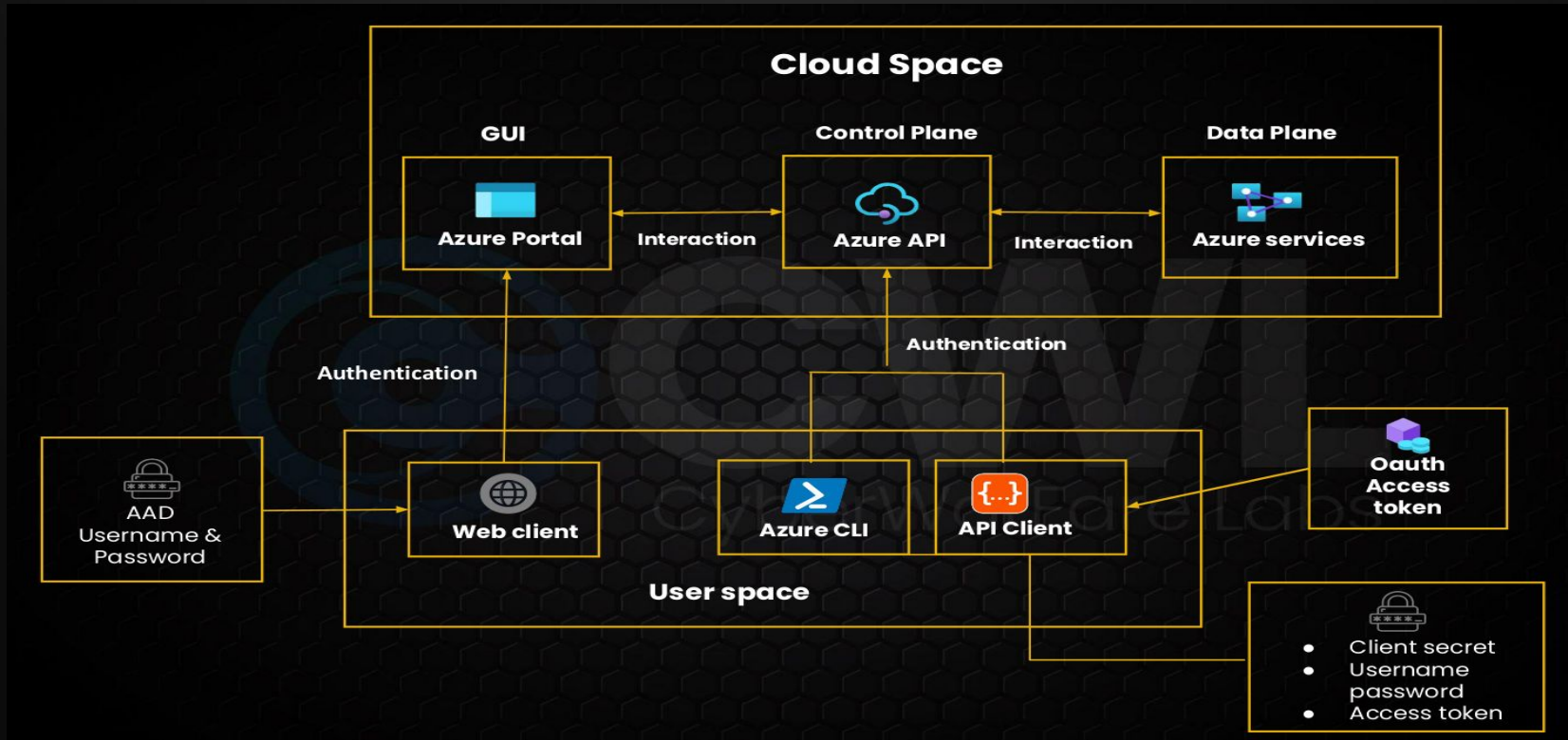
AZURE HIERARCHY



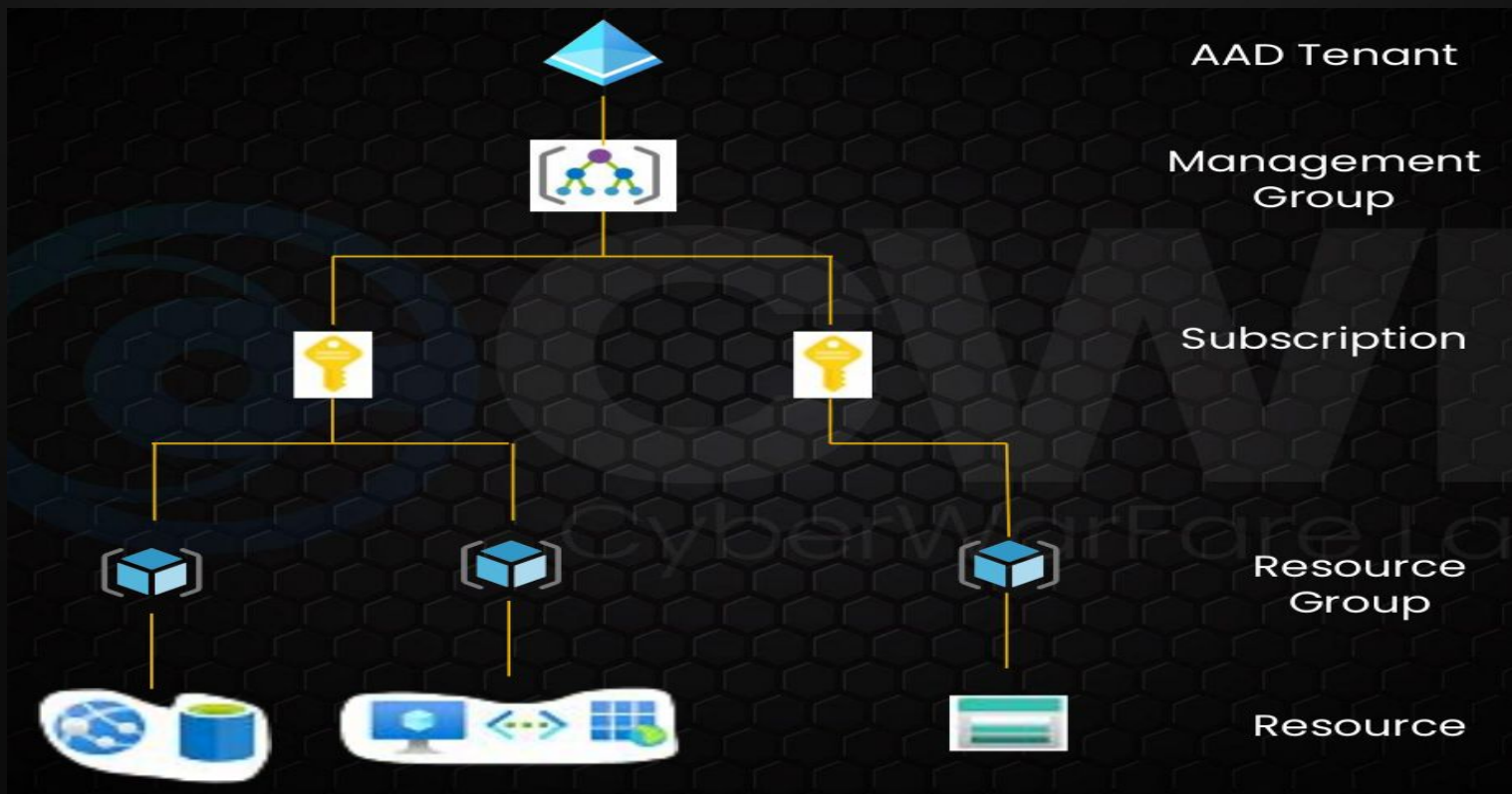
AZURE HIERARCHY



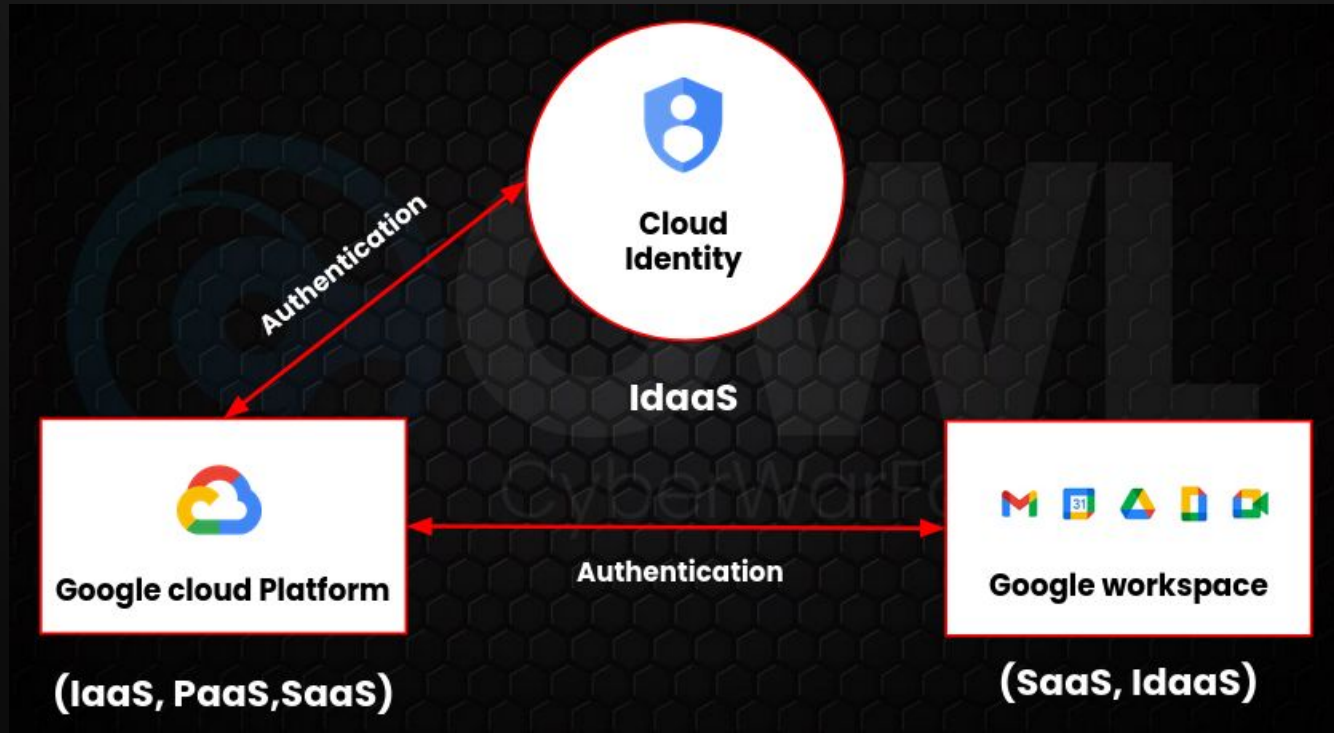
AZURE ARCHITECTURE



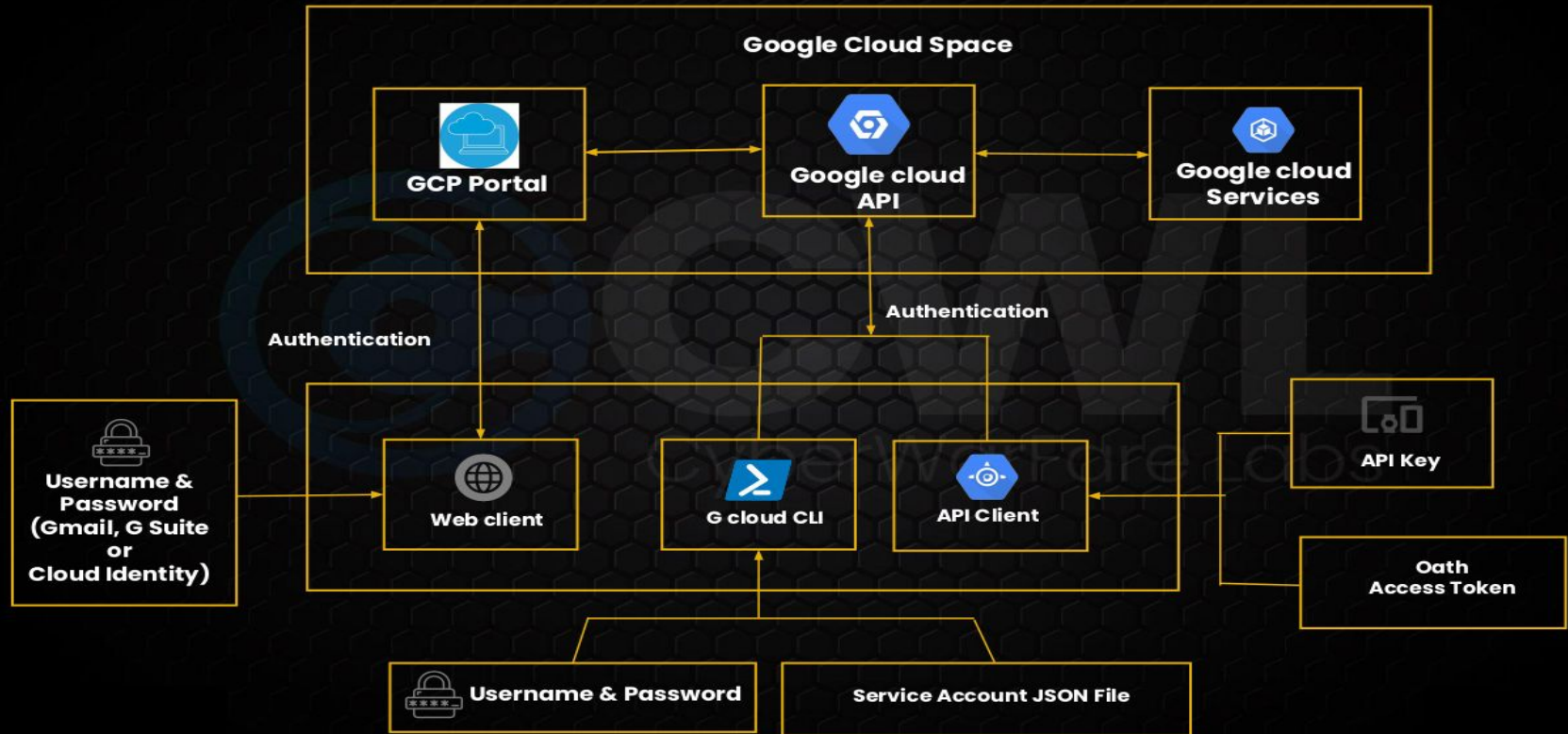
AZURE ARCHITECTURE



GCP HIERARCHY



GCP ARCHITECTURE



COMMON CLOUD MISCONFIGURATIONS

★ Misconfigurations include:

○ Compute:

- Public snapshots
- Open ports with 0.0.0.0/0 rules
- Backend instances in Public subnets
- Vulnerabilities leading to SSRF/RCE
- Overly permissive IAM roles attached

COMMON CLOUD MISCONFIGURATIONS

- Identity:
 - Usage of root account for resource provisioning
 - Lack of MFA
 - Usage of wildcard (*) in IAM policies
 - Assigning overly permissive roles & policies
 - Insufficient logging & monitoring

COMMON CLOUD MISCONFIGURATIONS

- Storage:
 - Anonymous access to storage objects
 - Overly permissive IAM policies
 - List actions by anyone
 - Principal set to wildcard (*)

DEMO TIME



GET

90%

OFF

Multi-Cloud Red Team Analyst
(MCRTA) Course

Use Coupon Code : **“ONCLOUD90”**

ENROLL NOW

Thank You

**For Professional Red Team / Blue Team / Purple Team,
Cloud Cyber Range labs / Courses / Trainings, please contact**

info@cyberwarfare.live

To know more about our offerings, please visit:

<https://cyberwarfare.live>