

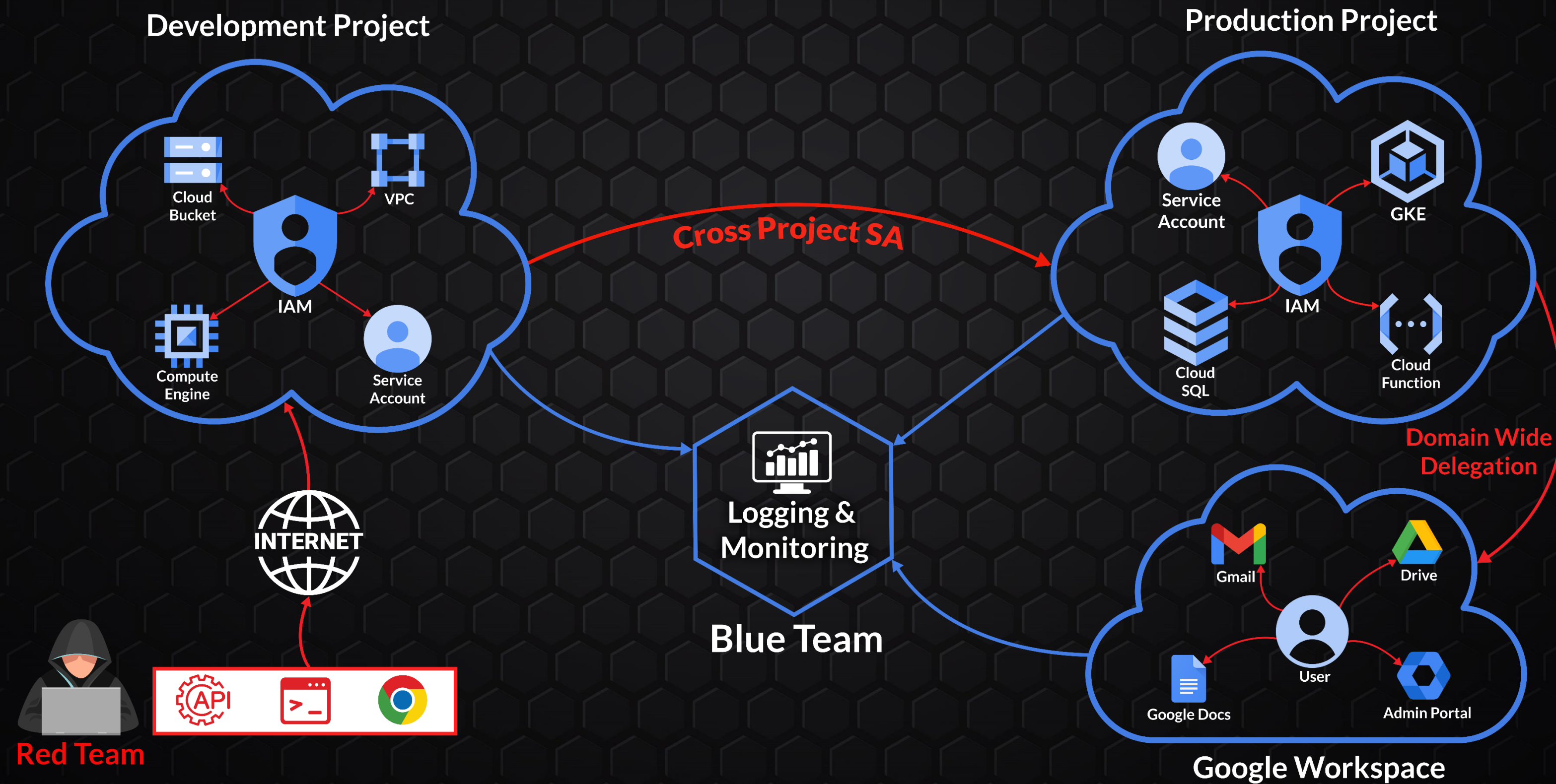


Certified Google Cloud Red Team Specialist [CGRTS]



@CyberWarFare Labs

Certified Google Cloud Red Team Specialist Architecture



Module 1: Google Cloud Red Team Fundamentals

- **Google Cloud Platform**
 - **Hierarchy**
 - **Service Account**
 - **Identity & Access Management**
- **Google Workspace**
 - **Management**
 - **Productive Apps**
- **Google Cloud Authentication**
 - **GUI, CLI & API**

- **Motive / Objective in Red Team Ops in Google Cloud**
- **Red Team Methodology**
 - **Cyber Kill Chain**
 - **Assume Breach Scenario**
 - **MITRE ATT&CK Matrix for Cloud**

Module 2 : **Red Team Operations in Google Cloud Environment**

- **Open Source Information Gathering (OSINT)**
 - **Passive [DNS based]**
 - **Active**
- **Gaining Initial Access**
 - **Stolen Credential [SVN, Dev System Compromise]**
 - **Exploiting Application [App running on VM, Serverless, Kubernetes]**
- **Internal Recon**
 - **Google Cloud Services**

▪ **Privilege Escalation**

- **Local [VM] Based [Windows, Linux]**
- **Cloud Based [IAM Misconfiguration, Service Account etc.]**

▪ **Maintaining Access**

- **Local [VM] Based [Users, OsLogin, SSH Key etc.]**
- **Cloud Based [Service Account, Cloud Function etc.]**

▪ **Hunting for Credentials**

- **Secret [Secret Manger etc.]**
- **Sensitive Data [Buckets, Databases etc.]**

- **Lateral Movement**

- **Pivot the Networks Boundary [VPC]**
- **Expand Access Control Plane to Data Plane [VMs]**
- **GCP to Workspaces Access [Domain Wide Delegation]**

- **Achieving the Objectives**

- **Data Exfiltration / Destruction / Encryption**

Google Cloud Red Team Specialist Training Materials

- **Lab:**
 - Demo Lab
 - Challenge Lab
 - Exam Lab
- **Study Material:**
 - Study Material PPT
 - Training / Course Slides
 - Challenge Lab Walkthrough PPT
- **Tools:**
 - Cloud Enum
 - Gcploit
 - GCP PrivESC Scanner



Thank You

Cyberwarfare.live

