CWL
CyberWarFare Labs

Multi-Cloud **Threat Detection** Approaches

04-Apr-2025

cyberwarfare.live

About CyberWarFare Labs :

CW Labs is a Global Infosec company specializing in cybersecurity practical learning situated across UK, US & India. The company has 2 primary divisions :

1. Niche Cyber Range Labs
2. Continuous Learning : Infinity Platform

About Speaker

Harisuthan S

Senior Security Engineer

He Is a Blue Team Security researcher, bringing over 3+ years of experience in cyber defence. possesses a deep understanding of Blue Team methodologies including investigation and detection over cyber attacks.

Table of **Content**

Traditional vs Cloud Security

Traditional Security

Traditional Security refers to conventional methods used to protect IT systems, primarily in on-premises environments. It includes tools like firewalls, antivirus software, intrusion detection systems (IDS), and access controls. Traditional security focuses on perimeter defense,

SIEM

EDR/XDR

Network Monitoring

Firewall IDS/IPS

FIM

Traditional Security

Traditional Security refers to conventional methods used to protect IT systems, primarily in on-premises environments. It includes tools like firewalls, antivirus software, intrusion detection systems (IDS), and access controls. Traditional security focuses on perimeter defense,

- SIEM
- EDR/XDR
- Network Monitoring
- Firewall IDS/IPS
- FIM

Traditional Security

Traditional Security refers to conventional methods used to protect IT systems, primarily in on-premises environments. It includes tools like firewalls, antivirus software, intrusion detection systems (IDS), and access controls. Traditional security focuses on perimeter defense,

- SIEM
- EDR/XDR
- Network Monitoring
- Firewall IDS/IPS
- FIM

Traditional Security

Traditional Security refers to conventional methods used to protect IT systems, primarily in on-premises environments. It includes tools like firewalls, antivirus software, intrusion detection systems (IDS), and access controls. Traditional security focuses on perimeter defense,

- SIEM
- EDR/XDR
- Network Monitoring
- Firewall IDS/IPS
- FIM

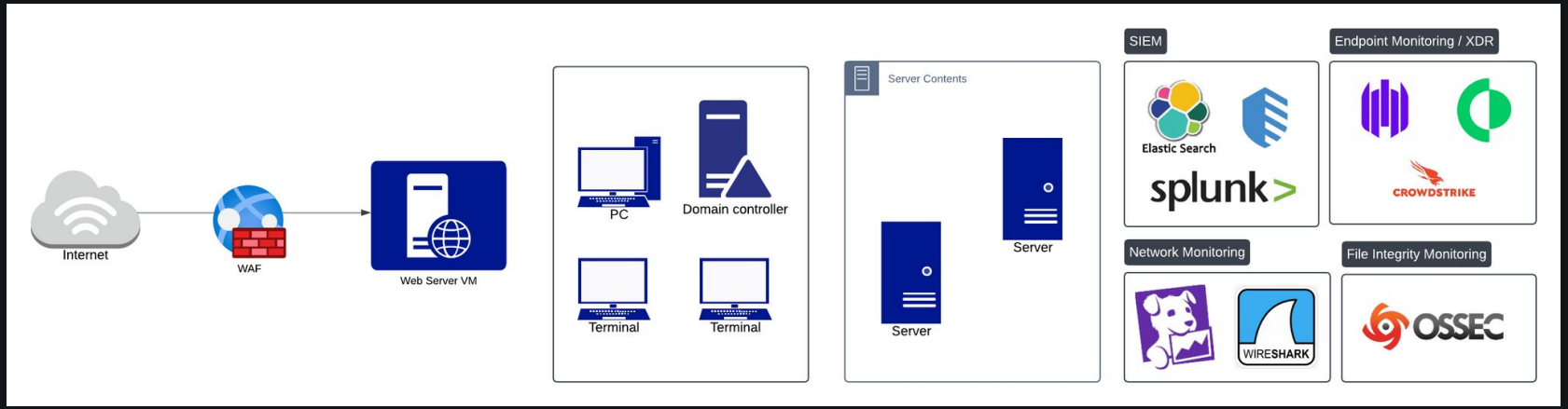
Traditional Security

Traditional Security refers to conventional methods used to protect IT systems, primarily in on-premises environments. It includes tools like firewalls, antivirus software, intrusion detection systems (IDS), and access controls. Traditional security focuses on perimeter defense,

- SIEM
- EDR/XDR
- Network Monitoring
- Firewall IDS/IPS
- FIM

Working of Traditional On-Premise Security

The illustrated architecture diagram will represent a functional implementation of traditional on-premises security



Cloud Security

Security implications in the cloud present unique challenges, as the architectural implementations and associated services differ significantly from traditional on-premises environments. Below are some commonly adopted steps used to achieve security in cloud environments:

Built-in Cloud Security Offerings

Access Management

Data Protection & Encryption

Logging & Monitoring

Challenges over Multi Cloud Security

Challenges over Multi Cloud Security

Inconsistent Security Controls

Complex Identity & Access Management

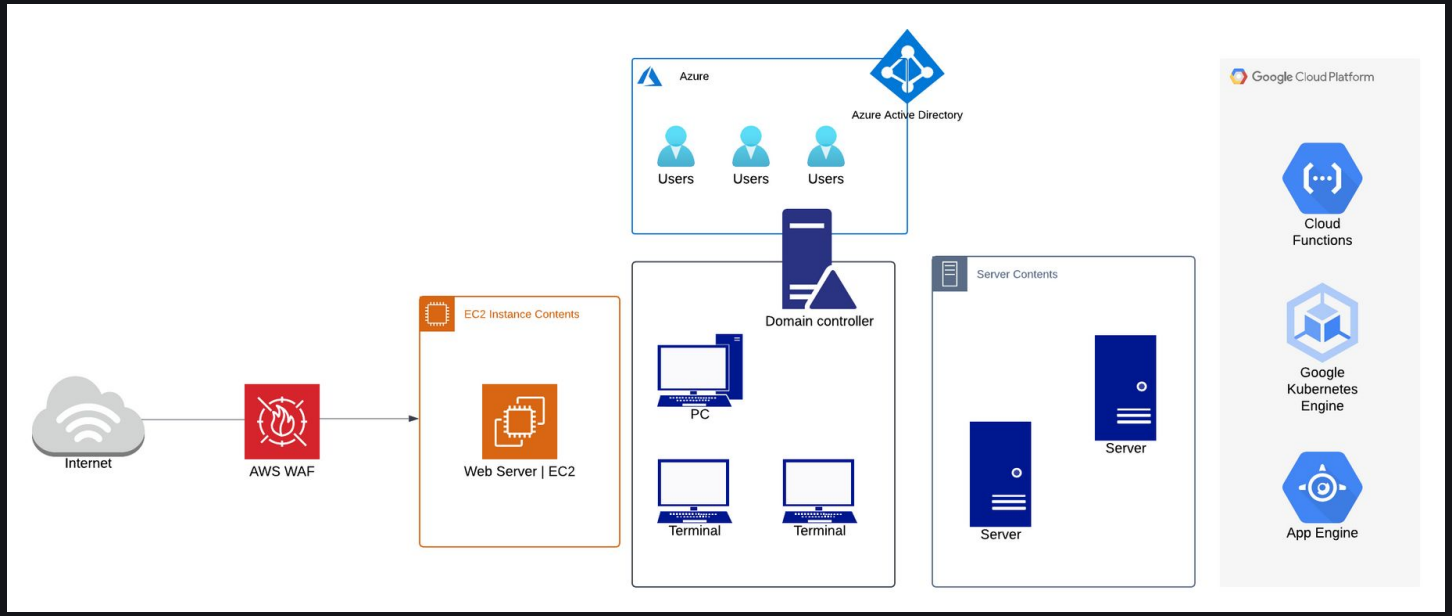
Limited Visibility & Monitoring

Configuration Drift & Misconfigurations

Limited Visibility & Monitoring

Compliance & Regulatory Challenges

Challenges over Multi Cloud Security



Importance of logging and monitoring

Importance of logging and monitoring

Logging and monitoring are critical components of a robust cybersecurity strategy. They involve the continuous collection, analysis, and review of system events and activities to ensure visibility, detect threats, and support incident response.

- Real-Time Threat Detection
- Incident Response & Investigation
- Operational Visibility
- Proactive Defense

Event-Based Security Insights

AWS CloudTrail Event Names

- ConsoleLogin
- CreateUser
- AttachRolePolicy
- DeleteUser
- AssumeRole
- PutBucketAcl
- GetObject

Azure CloudTrail Event Names

- Sign-in logs (AAD)
- AuditLogs
- RiskySignIns
- KeyVaultSecretRead
- SetSecurityPolicy
- AddServicePrincipalCredential
- UpdatePolicyAssignment

GCP CloudTrail Event Names

- iam.activity
- audit.logins
- vpc_flow_logs
- data_access
- service_usage
- compute.instances.setMetadata

CWL
CyberWarFare Labs

MULTI-CLOUD BLUE TEAM ANALYST (MCBTA)

cyberwarfare.live

- The MCBTA certification is structured around five key modules, including two cloud-specific labs focused on multi-cloud monitoring and investigation. It features over 15 investigative scenarios with detailed documentation of investigation steps and detection queries.

- Additionally, the certification explores the various built-in security services offered by multi-cloud providers and includes manual deployment steps for configuring monitoring services to achieve proactive monitoring across multi-cloud environments.

EXPLORING THE TRUE VALUE OF MCBTA

7+ HRS
HD RECORDED VIDEOS

20+ PDFS
250+ PAGES

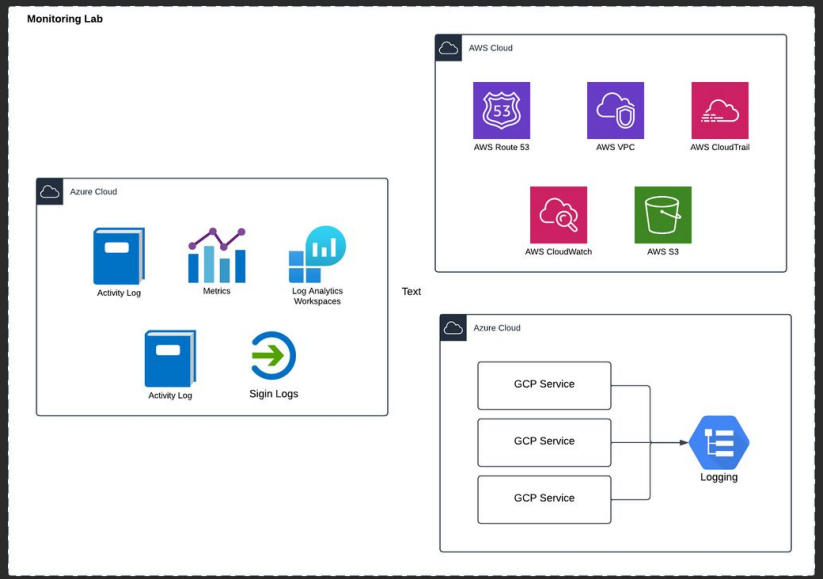
30+ GAMIFIED
FLAG-BASED CHALLENGES

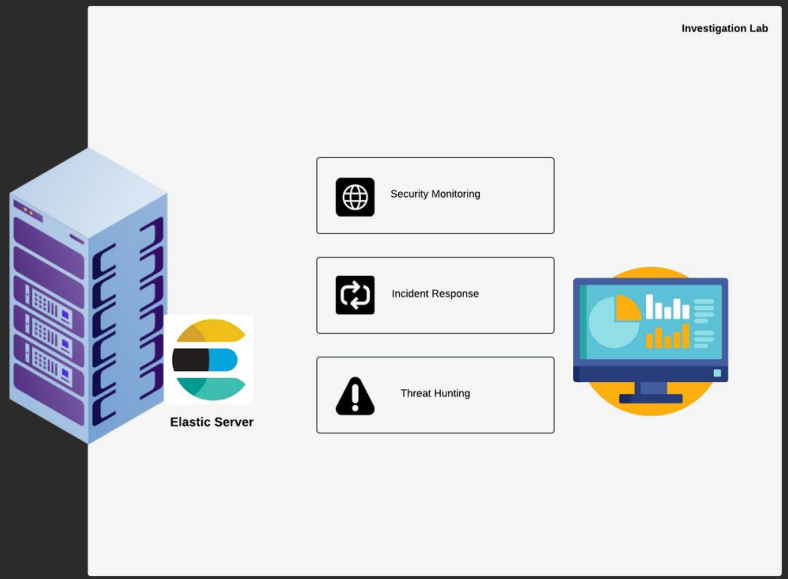
LOCAL LAB DEPLOYMENT
[MULTI CLOUD MONITORING & INVESTIGATIVE LABS]

AWS/AZURE/GCP
DEPLOYING MULTI CLOUD LOGGING AND MONITORING

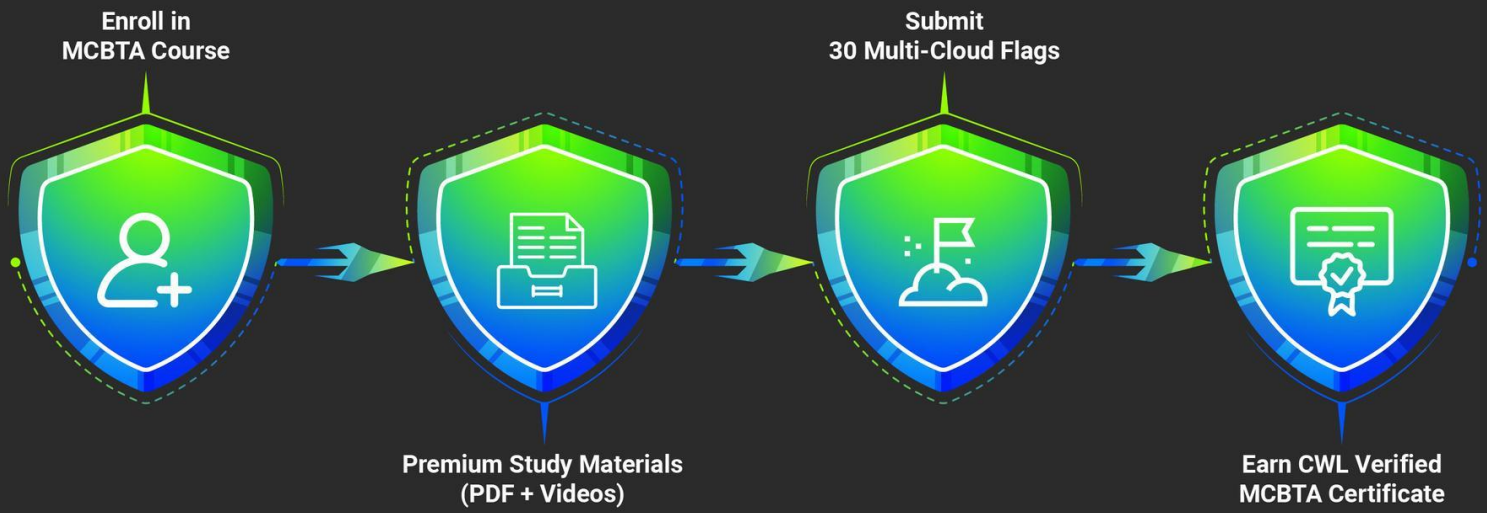
15+ MULTI-CLOUD INCIDENT
GUIDED INVESTIGATION LAB

LAB ARCHITECTURE | MCBTA





EXAMINATION PROCEDURE



Key Insights You'll Gain & Prove

- 15+ Threat Investigations Targeting Cloud Environments
- Unified Logging and Monitoring for Multi-Cloud Infrastructures
- Cloud-Specific Log Correlation and Analysis
- 30 Flag-Based Investigative Questions with a Gamified Approach
- Access to the CWL Cloud-Based Blue Team Network

Thank You

For Professional Red Team / Blue Team / Purple Team / Cloud Cyber Range labs / Trainings, please contact support@cyberwarfare.live

To know more about our offerings, please visit: https://cyberwarfare.live

www.cyberwarfare.live