Faysal Aziz

Hybrid Multi-Cloud Red Team Specialist

Attack-path thinking for AWS, Azure, and Active Directory in real hybrid environments

FA-0240 · 5 day

DevOps, Cloud & Infrastructure

Introduction

This 3 to 5 day course is built from the structure of the CHMRTS, but with all the focus sharpened around AWS, Azure, and on-premises Active Directory. It also reflects today's threat reality, where identity abuse, public-facing application exploitation, password spraying, and cloud-to-on-prem pivot paths remain central concerns, and where ATT&CK continues to maintain dedicated cloud and identity-provider coverage for real-world adversary tradecraft.

This course is delivered by an instructor with over 30 years of industry experience and is designed around real industry-demanded content rather than academic abstraction. The result is a practical, operations-minded program that helps learners understand how hybrid attack paths are modeled, exercised, mapped, and reported in modern enterprise environments.

Learning outcomes

- Understand the structure and security characteristics of hybrid environments spanning AWS, Azure, and on-premises Active Directory.
- Identify major trust boundaries, identity dependencies, and attack surfaces across cloud and enterprise environments.
- Analyze how red team operations align to the MITRE ATT&CK Enterprise and Cloud matrices.
- Evaluate common categories of hybrid attack paths involving reconnaissance, initial access, privilege escalation, persistence, credential access, and lateral movement.
- Distinguish platform-specific risks in AWS, Azure, and Active Directory without treating them as isolated silos.
- Plan red team infrastructure, tooling strategy, and operational workflows for hybrid assessments.

- Map technical findings into realistic organizational impact narratives and reporting structures.
- Interpret cloud and identity-centric threat trends that make hybrid red team capability strategically relevant today.

Prerequisites

- Working knowledge of TCP/IP, DNS, authentication, and enterprise networking
- Basic familiarity with AWS and Azure administration concepts
- Foundational understanding of Active Directory, Windows security, and common identity services
- Prior exposure to penetration testing, red teaming, or adversary emulation concepts
- Comfort with command-line tooling (both Windows and Linux), scripting basics, and security assessment workflows
- Familiarity with security logging, IAM concepts, and role-based access control
- General understanding of MITRE ATT&CK terminology is helpful but not required

Training outline

1. Course foundations and hybrid threat context

1. What defines a hybrid multi-cloud environment
2. Why hybrid estates create compound attack surfaces
3. Control plane, identity plane, and workload plane relationships
4. Trust boundaries across AWS, Azure, and on-premises infrastructure
5. Business drivers behind hybrid architecture adoption
6. Security consequences of federation, synchronization, and delegated administration

   Current threat relevance

   1. Identity-led attack patterns
   2. Public-facing exposure in cloud-connected enterprises
   3. Password spraying and credential abuse in enterprise ecosystems
   4. ATT&CK cloud and identity-provider alignment for red team planning

2. Hybrid multi-cloud environment overview

On-premise architecture

1. Core enterprise infrastructure components
2. Domain services and identity dependencies
3. Administrative tiers and trust relationships

4. Connectivity models to cloud services

Multi-cloud architecture

1. Shared versus isolated operating models
2. Identity centralization versus platform-native identity
3. Management plane exposure and operational complexity

Hybrid multi-cloud architecture

1. Integration patterns between cloud and enterprise identity
2. Workload placement and connectivity assumptions
3. Cross-platform administration and support paths
4. Security implications of hybrid join, federation, and sync

On-premise versus multi-cloud versus hybrid comparison

1. Visibility differences
2. Attack surface differences
3. Detection and response considerations
4. Governance and operational maturity challenges

3. AWS environment introduction and enumeration

AWS cloud overview

1. Account structure and organizational models
2. Shared responsibility implications for red team assessments
3. Core services commonly in scope

Identity and Access Management

1. Users, groups, roles, and policies
2. Permission boundaries and effective access
3. Temporary credentials and role assumption concepts

Federation and identity integration

1. Enterprise identity integration patterns
2. External identity providers and trust assumptions
3. Session-based access and operational risk

Cross-account access

1. Trust relationships between accounts
2. Administrative delegation models
3. Role chaining and boundary considerations

AWS enumeration strategy

1. Manual enumeration themes

2. Automated asset and identity discovery themes
3. Access review and privilege mapping
4. Service exposure mapping
5. Cross-account relationship analysis

4. Azure environment introduction and enumeration

Azure cloud overview

1. Tenant, subscription, resource group, and management concepts
2. Separation of identity and resource management planes

Azure Active Directory and cloud identity

1. Tenant structure and administrative model
2. Users, groups, service principals, managed identities, and applications
3. Role design and privilege distribution

Azure Resource Manager

1. IaaS, PaaS, and SaaS control boundaries
2. Deployment hierarchy and governance constructs
3. Resource access versus directory access

Multi-tenant access

1. B2B and external collaboration concepts
2. Cross-tenant trust considerations
3. Delegated access models

Roles and RBAC

1. Directory roles
2. Azure RBAC
3. Privileged administration paths
4. Scope inheritance and access sprawl

Microsoft 365 and Office 365 security context

1. Collaboration surfaces and identity exposure
2. SaaS-to-directory risk relationships

Azure enumeration strategy

1. Manual identity and application review
2. Tenant and subscription visibility mapping
3. Role and access relationship analysis
4. Administrative surface discovery
5. Automated assessment themes for Azure environments

5. On-premises Active Directory introduction and enumeration

On-premise infrastructure overview

1. Domain topology
2. Administrative boundaries
3. Core services and dependency chains

Active Directory fundamentals

1. Forests, domains, trusts, and organizational units
2. Kerberos and directory-based authorization concepts
3. Identity lifecycle and administrative delegation

Cross-forest access

1. Trust design
2. Cross-forest privilege considerations
3. Enterprise sprawl and inherited risk

Authentication and authorization in Active Directory

1. Authentication flows
2. Privilege assignment
3. Service account exposure
4. Delegation models

On-premise to cloud connectivity

1. Sync and federation patterns
2. Hybrid identity dependencies
3. Enterprise application integration

AD enumeration strategy

1. Identity mapping
2. Trust mapping
3. Privileged group and delegation review
4. Infrastructure and endpoint visibility
5. Manual and automated enumeration themes

6. Reconnaissance and external profiling in hybrid environments

Targeted organization profiling

1. Business footprint mapping

2. Technology stack inference
3. Identity and brand surface analysis

Open-source information gathering across hybrid estates

1. Cloud footprint discovery themes
2. Internet-facing platform identification
3. Documentation and metadata leakage awareness

Unauthenticated service enumeration

1. Tenant and service discovery concepts
2. Exposure validation themes
3. External identity endpoint visibility

Password spray risk in enterprise identity ecosystems

1. Why spray attacks remain relevant
2. Hybrid identity exposure patterns
3. Defensive implications for red team simulation

Leaked credential exposure

1. Cloud and enterprise credential risk categories
2. Access validation workflow design
3. Escalation of business impact through trust relationships

7. Initial access in hybrid environments

Public-facing application compromise pathways

1. Cloud-hosted and enterprise-hosted exposure categories
2. Application-to-identity implications
3. Application-to-control-plane impact pathways

Access through leaked or mismanaged credentials

1. Cloud credential categories
2. Session and token risk
3. Enterprise credential crossover risk

On-premise spoofing and trust abuse concepts

1. Identity trust weaknesses
2. Environmental assumptions that enable access

Phishing and consent-based abuse in Azure-centric ecosystems

1. User consent risk
2. Enterprise application abuse themes
3. SaaS-integrated identity compromise paths

8. Privilege escalation across cloud and enterprise platforms

Misuse of serverless and automation components

1. Execution context as an escalation surface
2. Secrets exposure through automation
3. Privileged runtime abuse patterns

Azure automation misuse

1. Automation accounts and privileged workflows
2. Runbook and identity context considerations

Excess IAM permission exploitation

1. Over-privileged identities
2. Privilege graph analysis
3. Control plane escalation pathways

Active Directory privilege escalation concepts

1. Replication-related privilege concerns
2. Delegation abuse themes
3. Administrative trust collapse

9. Persistence in hybrid environments

Cross-account and delegated-access persistence in AWS

1. Long-term trust abuse concepts
2. Role and access persistence themes

Azure application and directory persistence

1. Enterprise applications as a persistence surface
2. Service principal abuse concepts
3. Tenant-level persistence considerations

Active Directory persistence concepts

1. Ticketing and trust durability risks
2. Backdoor placement categories
3. Administrative recovery implications

Persistence strategy comparison across AWS, Azure, and AD

1. Identity-based persistence
2. Configuration-based persistence
3. Trust-based persistence

10. Credential access in cloud and hybrid estates

AWS role and identity abuse themes

1. Temporary credential exposure
2. Metadata and runtime-derived identity risk
3. Chained access possibilities

Azure Key Vault and secret management risk

1. Secret concentration and privilege implications
2. Access policy and RBAC exposure
3. Automation-driven secret access concerns

Memory and secret extraction concepts in enterprise environments

1. Endpoint and server credential residue
2. Service account material exposure
3. Identity relay into cloud-connected systems

11. Lateral movement across hybrid trust boundaries

Breaking cloud and enterprise segmentation assumptions

1. Network boundary misconceptions
2. Identity-driven movement versus network-driven movement

Azure hybrid-joined device compromise concepts

1. Device identity as a pivot layer
2. Endpoint-to-directory trust implications

On-premise to cloud lateral movement

1. Seamless SSO and hybrid identity exposure
2. Federation-linked movement paths
3. Administrative workstation and sync-server significance

Cloud to on-premise lateral movement

1. Identity synchronization trust paths
2. Administrative credential crossover
3. Workload-to-directory adjacency

12. Red team operations overview for hybrid environments

AWS versus Azure versus Active Directory

1. Platform differences in visibility
2. Platform differences in privilege models

3. Platform differences in operational tradecraft

Red team infrastructure setup

1. Assessment infrastructure planning
2. Segregation, logging, and operational hygiene
3. Identity-safe and evidence-safe operating practices

Red team arsenal for hybrid environments

1. Cloud assessment tooling categories
2. Identity analysis tooling categories
3. Automation, scripting, and orchestration considerations
4. Evidence management and reporting support tools

13. MITRE ATT&CK alignment for enterprise and cloud operations

1. Unauthenticated enumeration
2. Initial access
3. Authenticated enumeration
4. Privilege escalation
5. Persistence
6. Credential access
7. Discovery
8. Lateral movement
9. Data exfiltration

Using ATT&CK to structure planning

1. Scoping
2. Coverage analysis
3. Exercise design
4. Reporting and executive mapping

14. Full-spectrum hybrid red team exercise design

Objective-driven operation planning

1. Cloud-to-on-premise compromise narrative
2. On-premise-to-cloud compromise narrative

2. Chaining identity, workload, and control plane findings
3. Attack path prioritization based on business impact

4. Detection engineering touchpoints for purple team value
5. Rules of engagement and safety boundaries
6. Evidence collection and deconfliction

    Reporting structure

    1. Technical findings
    2. Attack path storyline
    3. Business risk articulation
    4. Strategic remediation themes

15. Course wrap-up and applied outcomes

1. Hybrid attack path review
2. Cross-platform risk comparison
3. Common failure patterns in real environments
4. Translating red team observations into hardening priorities
5. Building an internal roadmap for hybrid adversary simulation maturity

---

© 2026 Faysal Aziz · Kuala Lumpur