

Authorized Identity Attack Path Validation Training Course

25 – 29 October 2027
Kuala Lumpur

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

Authorized Identity Attack Path Validation Training Course

Ref: 1719_229116 **Date:** 25 – 29 October 2027 **Location:** Kuala Lumpur **Fees:** 5200 Euro

Overview

Authorized Identity Attack Path Validation Training Course is a one-week course for authorized red team practitioners, penetration testers, identity security engineers, threat-emulation specialists, and defenders, who leave with an Identity Attack Path Validation Pack. Participants connect identity attack path validation, authorized adversary emulation, hybrid identity exposure, privilege relationship analysis, and a purple team debrief within controlled test environments. The course turns isolated identity findings into scoped evidence and remediation decisions. Agile Leaders Training Center presents authorized identity attack path validation.

Who Should Attend

- Functions responsible for authorized red team and penetration-test engagements
- Teams responsible for enterprise identity architecture and exposure management
- Functions responsible for threat emulation and control validation
- Teams responsible for identity detection engineering and incident readiness
- Functions responsible for remediation assurance across hybrid environments

The course assumes participants already perform authorized security testing or identity engineering and leaves out live third-party targets, malware development, destructive actions, real credential collection, and uncontrolled evasion.

Departments and Industries

The course supports departments and industries that validate identity exposure within governed security assessments.

- Cybersecurity testing and security engineering teams
- Identity and access management and directory-service functions
- Financial services and technology infrastructure operations
- Healthcare and energy security assurance teams
- Managed security and enterprise risk functions

Learning Objectives

By the end of this course, participants will be able to:

- Apply rules of engagement to identity-focused testing
- Build identity relationship and attack-path models
- Analyze credential, token, and permission exposure safely
- Compare directory, cloud, and hybrid identity paths
- Evaluate detection evidence against emulated behaviors
- Prioritize remediation and verify control changes

Course Agenda

Day 1: Authorization and Identity Threat Modeling

- NIST SP 800-115 Rules of Engagement and Scope Matrix
- Identity Test Boundary and Safeguard Checklist
- MITRE ATT&CK Identity Technique Mapping Board
- Critical Identity and Sensitive Asset Register
- Adversary Emulation Assumption and Stop-Condition Log

Day 2: Identity Relationship and Exposure Mapping

- Directory Account, Group, and Trust Relationship Graph
- Service Principal and Managed Identity Permission Map
- Credential and Token Exposure Evidence Matrix
- Kerberos and Authentication Protocol Scenario Model
- Hybrid Identity Pivot and Sensitive Asset Path Analysis

Day 3: Controlled Identity Adversary Emulation

- MITRE ATT&CK T1078 Valid Account Test Case
- MITRE ATT&CK T1558 Kerberos Abuse Simulation Plan
- MITRE ATT&CK T1098 Account Manipulation Control Scenario
- Lateral Movement and Privilege Escalation Evidence Chain
- Persistence and Command-Channel Boundary Control Sheet

Day 4: Detection, Evidence, and Remediation

- Identity Telemetry and Detection Coverage Matrix
- Alert Correlation and Emulation Timeline Record
- Finding Severity and Attack-Path Impact Method
- Remediation Ownership and Exposure Reduction Plan
- Retest Evidence and Control Validation Checklist

AGILE LEADERS
Training Center

Day 5: Identity Validation Practice

- Exercise: Define Identity Test Scope and Stop Conditions
- Exercise: Build a Hybrid Identity Attack-Path Graph
- Exercise: Evaluate Detection Evidence for Mapped Behaviors
- Exercise: Prioritize Remediation and Design a Safe Retest
- Capstone Exercise: Identity Attack Path Validation Pack

Practical Exercises

The course uses suggested activities in isolated lab scenarios based on finance, healthcare, technology, and energy environments.

- Suggested activity: convert written authorization into scope, safeguards, contacts, exclusions, and stop conditions.
- Suggested activity: map permissions and trust relationships from a fictional hybrid identity dataset.
- Suggested activity: compare emulated identity behaviors with expected telemetry and detection evidence.
- Suggested activity: turn a validated path into remediation owners, control changes, and retest criteria.

FAQs

Who suits identity attack path validation training, and what does it assume?

Identity attack path validation training suits authorized security testers and identity defenders and assumes experience with enterprise authentication, directory services, security assessments, and controlled lab practice.

How does identity attack path validation differ from general penetration testing?

Identity attack path validation concentrates on accounts, permissions, trust relationships, authentication, hybrid identity, detection evidence, and remediation; general penetration testing evaluates a broader range of network, system, and application exposure.

Why do identity attack paths use relationship graphs?

Relationship graphs show how permissions, memberships, roles, service identities, and trust links can combine into routes from an exposed identity to a sensitive asset.

How does purple team work improve identity attack path validation?

Purple team work connects controlled emulation with telemetry review, detection gaps, defensive decisions, remediation ownership, and evidence-based retesting.

AGILE LEADERS
Training Center

Conclusion

Participants take an Identity Attack Path Validation Pack back to work. It combines rules of engagement, identity graphs, mapped behaviors, safeguards, evidence records, detection coverage, remediation decisions, and retest criteria. The pack changes disconnected identity findings into a governed validation cycle that supports exposure reduction without uncontrolled offensive activity.