

# SEC559: Cloud and Hybrid Identity Security™

5 Day Program | 30 CPEs | Laptop Required

## You Will Be Able To

- Detect OAuth consent abuse, token theft, and service principal compromise
- Analyze Entra ID sign-in, audit, and Graph activity logs for identity anomalies
- Map hybrid attack paths across Active Directory and Entra ID using BloodHound
- Detect hybrid identity attacks including sync abuse, federation manipulation, and Kerberos escalation
- Uncover governance and lifecycle weaknesses that enable long-term attacker persistence
- Execute safe remediation by revoking sessions, rotating credentials, and restoring trust

## Business Takeaways

- Reduce risk from identity attacks that bypass traditional perimeter defences
- Detect attackers using legitimate credentials, tokens, and trusted access
- Prevent tenant-wide compromise with structured IR workflows
- Improve visibility across cloud and hybrid identity control planes
- Strengthen Zero Trust, identity governance, and compliance programs

## Prerequisites

- Familiarity with Microsoft Active Directory: users, groups, domain trusts
- Basic understanding of cloud identity: Entra ID, OAuth 2.0, or SAML
- Windows environment experience with basic PowerShell familiarity
- Familiarity with common attack types—credential theft and privilege escalation
- Intermediate security experience—no cloud certification required



## Guard the Cockpit—Secure Your Identity Control Plane

SEC559 is the only SANS course dedicated entirely to cloud and hybrid identity security. Attackers aren't kicking down doors — they're slipping through misconfigured applications, leaked secrets, rogue certificates, and quietly abused OAuth flows. SEC559 gives practitioners the attacker knowledge and hands-on experience to detect and respond to identity-based attacks before trusted access becomes full compromise.

Identity is now the primary attack vector. Common challenges include:

- OAuth token abuse and consent phishing that bypass standard detection
- Service principal compromise and CI/CD credential leakage
- Hybrid attack paths from on-premises Active Directory to full cloud tenant compromise
- Federation abuse — rogue SAML certificates granting persistent backdoor access
- Privilege sprawl, orphaned access, and ungoverned identity lifecycle

## Hands-On Identity Attack Detection and Response Training

SEC559 is built around 20 hands-on exercises using real Entra ID and Active Directory telemetry that mirror how modern identity attacks actually unfold. Students work through a connected, real-world breach scenario across all five days—covering human, workload, and agent identities, learning how attackers misuse OAuth consent, tokens, service principals, synchronization, and cross-tenant trust to stay hidden without triggering standard alerts.

Each lab helps students spot subtle signs of identity abuse that blend in as legitimate activity. By the end of the course students will have practiced mapping identity attack paths across cloud and hybrid environments, detecting governance failures that enable persistence, and executing safe remediation, revoking sessions, rotating credentials, securing sync infrastructure, and restoring trust without disrupting business operations.

**“Over the years, I've seen identity incidents where defenders did everything right — but attackers still kept access. Tokens, application identities, federation trust. This course teaches defenders how to investigate when identity authority is under threat.”**

—Maxim Deweerdt, Course Author

# Section Descriptions

## SECTION 1: Identity as the Control Plane

Section 1 establishes the identity foundations students need before engaging with attacker techniques. Students explore the modern cloud identity threat landscape and learn how Microsoft Entra ID, Active Directory, and hybrid architectures function as interconnected control planes that attackers target. The day covers all identity types—users, devices, workloads, and agent identities—and examines how applications, service principals, and managed identities interact with Graph API permissions to create an attack surface that most defenders have never fully mapped.

**TOPICS:** Modern Cloud Identity Threat Landscape; Identity Types and Trust Boundaries in Entra ID; Applications, Service Principals, and Managed Identities; Graph API Permissions and Attack Surface Mapping; Identity Telemetry Foundations

## SECTION 2: Authentication, Tokens and Session Security

Section 2 focuses on how authentication and token issuance define access in modern environments. Students analyze how tokens, sessions, and authentication methods work in Microsoft Entra ID, and how attackers abuse them to gain persistent, often invisible access. The day covers token relationships across access tokens, refresh tokens, and primary refresh tokens, and how these are exploited through token replay, device code abuse, and session hijacking. Students also explore how authentication strength and Conditional Access policies influence token issuance, and how to detect and contain token-based attacks.

**TOPICS:** Authentication Flows and Identity Providers; Authentication Strength: Passwordless, FIDO2, and Device Binding; Token Model: Access, Refresh, PRT, and Token Chaining; Token Abuse: Replay, Persistence, Device Code, and Session Hijacking; Conditional Access, Session Control, and Token Protection

## SECTION 3: Hybrid Identity and Active Directory Security

Section 3 expands identity security into hybrid environments where Active Directory and Microsoft Entra ID form a combined control plane. Students analyze how synchronization, trust, and Kerberos enable cross-plane attacks and privilege escalation. The day covers how identity synchronization introduces attack primitives including object matching abuse, attribute manipulation, and connector account compromise—and how attackers move from on-premises AD to full cloud tenant compromise. Students use AzureHound and BloodHound to map hybrid attack paths and understand how to secure the hybrid identity control plane.

**TOPICS:** Hybrid Identity Architecture and Trust Boundaries; Identity Synchronization Models and Object Matching; Sync Infrastructure and Connector Identity Risks; Hybrid Privilege Escalation and Cross-Plane Attack Paths; Kerberos, Federation, and Modern Hybrid Authentication Models; Hybrid Attack Path Analysis with AzureHound and BloodHound

## SECTION 4: Identity Governance, External Trust and Lifecycle Security

Section 4 covers identity governance—the layer most organizations under-invest in until after an incident. Students learn how attackers exploit privilege sprawl, orphaned access, and cross-tenant trust relationships that accumulate over time. The day covers Privileged Identity Management, just-in-time access, access reviews, break-glass account security, external identity abuse, and delegated administration risks—giving defenders the skills to govern identity lifecycle as a security control, not just an operational one.

**TOPICS:** Privileged Identity Management and JIT Access; Break-Glass Account Security; Access Reviews and Lifecycle Management; Orphaned Access and Privilege Sprawl; External Identity and B2B Guest Abuse; Cross-Tenant Trust and Delegated Administration Risks; Identity Governance and NIS2/DORA Alignment

## SECTION 5: Hybrid Identity Threat Detection, Prevention and Response

The final section brings everything together into a full detection, prevention, and response capability. Students use telemetry from Microsoft Entra ID and Active Directory to investigate attacks, contain compromised identities, and restore trust.

**TOPICS:** Identity Telemetry: Sign-in Logs, Audit Logs, Graph Activity Logs; Building Identity Detection Use Cases; Full Kill Chain Detection Across Cloud and Hybrid; Structured IR: Revoke, Rotate, Contain, Validate; AI and Automation in Identity Detection and Response

## Who Should Attend

- IAM engineers and architects
- Cloud security engineers
- SOC analysts and incident responders
- Microsoft 365 and Entra ID administrators with security responsibility
- Cybersecurity consultants focused on Microsoft or hybrid identity
- IT administrators moving into security or identity-focused roles