Defending Active Directory

SEC406

Detect a full Active Directory domain compromise from the telemetry it leaves, from recon and Kerberoasting through DCSync, AD CS abuse, and the Windows Server 2025 dMSA path, in the Windows Security log every domain already has. Source-first and SIEM-agnostic: write each detection as portable Sigma and render it into Windows, Sentinel KQL, and Splunk SPL.

Modules	20
Lessons	144
Phases	5
Free preview	Course Orientation (10 lessons)

The method

Active Directory attacks are visible if you know which event the technique cannot avoid writing. This course runs the same loop for every technique across the attack path.

1. See the attack as an artifact, not a description. Every technique is shown as the real trace it leaves or the documented command that produces it, because recognition is what a defender needs.

2. Reason from what the protocol requires. Kerberos, LDAP and certificate issuance each have to do certain things. Detections built on those survive the attacker changing tools.

3. Write it once, render it everywhere. Detections are authored in Sigma and shown in Windows event terms, Sentinel KQL and Splunk SPL, so they travel to whatever the estate runs.

4. Check it against the corpus. Every runnable detection in this course is verified against real data rather than asserted, including the ones that return nothing.

5. Follow the path to the seam. On-premises AD and Entra ID are one attack surface with a synchronization boundary in the middle, and the crossings are where investigations stop too early.

The capstone works the full Northgate compromise end to end.

What this course assumes

No minimum experience and no prerequisite course. Kerberos, delegation, AD CS and the replication model are explained where they first matter rather than assumed.

What makes it go faster: a domain you can break, virtual is fine, and any prior exposure to Windows event logs. Neither is required, and every detection is shown against data.

What this course does not cover: Active Directory administration, penetration testing as a profession, and cloud-only identity, which is its own course. This is defending the directory.

Full syllabus

Phase 1: Foundations

Course Orientation FREE PREVIEW

Defending Active Directory is attack-informed defense: you learn each attack against a modern domain from both sides, what the adversary does and what it leaves in the evidence, then how to detect and analyze it.

1. ADS0.1 What Is Active Directory
2. ADS0.2 Threats Against Active Directory
3. ADS0.3 The Active Directory Attack Surface
4. ADS0.4 The Most Common Paths to Active Directory Compromise
5. ADS0.5 Challenges to Maintaining a Secure Active Directory
6. ADS0.6 AD Architecture: Domains, Forests, Trusts, Controllers
7. ADS0.7 The Core Components of a Domain
8. ADS0.8 The Modern Context: Entra ID, AD CS, and ADFS
9. ADS0.9 Logical and Physical Structure
10. ADS0.10 Build Your Active Directory Lab

Threat Landscape and Adversary Perspectives

The threat landscape for Active Directory and the defensive doctrine that answers it.

1. ADS1.1 Why Active Directory Is a Prime Target
2. ADS1.2 The Active Directory Attack Lifecycle
3. ADS1.3 The Tools Attackers and Defenders Use
4. ADS1.4 Avenues to Compromise
5. ADS1.5 Attractive Accounts for Credential Theft
6. ADS1.6 Reducing the Active Directory Attack Surface
7. ADS1.7 Implementing Least-Privilege Administrative Models
8. ADS1.8 Implementing Secure Administrative Hosts
9. ADS1.9 Securing Domain Controllers Against Attack
10. ADS1.10 Monitoring Active Directory for Signs of Compromise
11. ADS1.11 Audit Policy Recommendations
12. ADS1.12 Planning for Compromise
13. ADS1.13 Maintaining a More Secure Environment
14. Check My Knowledge

Common Attacks and Techniques

A current, defender-led survey of how Active Directory is actually attacked: enumeration and recon, credential attacks, Kerberos roasting, ticket forgery and delegation abuse, privilege escalation and persistence, AD CS certificate abuse, the hybrid seam into Entra ID, and the network-side vectors.

1. ADS2.1 Enumeration and Recon
2. ADS2.2 Credential Attacks
3. ADS2.3 Kerberos Roasting
4. ADS2.4 Kerberos Ticket Forgery and Delegation
5. ADS2.5 Privilege Escalation and Persistence
6. ADS2.6 AD CS Abuse
7. ADS2.7 Hybrid and Identity Federation
8. ADS2.8 Other Vectors
9. Check My Knowledge

Recon, Enumeration, and Attack-Path Posture

Reconnaissance is the phase you cannot see in native logs, and the one that decides everything after it.

1. ADS3.1 The Reconnaissance Problem
2. ADS3.2 LDAP and SAMR Enumeration
3. ADS3.3 Attack-Path Mapping with BloodHound
4. ADS3.4 Posture: Tiering and ACL Hygiene
5. ADS3.5 Where Recon Becomes Visible: Defender for Identity
6. Check My Knowledge

Authentication and Access Management

The machinery Active Directory uses to prove identity and grant access is the single largest attack surface in the enterprise, and almost every AD intrusion is an abuse of it working as designed.

1. ADS4.1 The Authentication and Access Management Attack Surface
2. ADS4.2 Authentication Concerns
3. ADS4.3 Access and Privilege Concerns
4. ADS4.4 Reducing the Authentication and Access Attack Surface
5. ADS4.5 Authentication Protocols Deep Dive
6. ADS4.6 Credential Storage and Protection
7. ADS4.7 Major Authentication Attacks
8. ADS4.8 Access Control and Authorization
9. ADS4.9 Group Policy and Authentication Hardening
10. ADS4.10 Hybrid and Modern Authentication
11. ADS4.11 Detection and Monitoring
12. Check My Knowledge

Phase 2: The Attack Chain

Credential Theft and Replay

A stolen credential does not need to be cracked to be used.

1. ADS5.1 The Shape of Credential Theft and Replay
2. ADS5.2 Where Credentials Live and How They Are Lifted
3. ADS5.3 Pass-the-Hash: Replaying the NTLM Secret
4. ADS5.4 Pass-the-Ticket and Overpass-the-Hash
5. ADS5.5 BadSuccessor and dMSA Abuse
6. ADS5.6 Reconstructing Lateral Movement
7. ADS5.7 Detecting Credential Replay
8. ADS5.8 Capstone: Working the Northgate Intrusion
9. Check My Knowledge

Privilege Escalation

Most Active Directory privilege escalation is not an exploit, it is the abuse of delegation and directory write rights the domain already grants.

1. ADS6.1 The Shape of Privilege Escalation
2. ADS6.2 Unconstrained Delegation
3. ADS6.3 Constrained Delegation and Protocol Transition
4. ADS6.4 Resource-Based Constrained Delegation
5. ADS6.5 SPN-Write Abuse
6. ADS6.6 Reconstructing a Delegation Escalation
7. ADS6.7 Detecting Privilege Escalation
8. Check My Knowledge

Domain Dominance

Domain dominance is the point where an attacker stops escalating and starts owning the directory: replicate its secrets with DCSync, forge the tickets the domain trusts with the stolen krbtgt key, and write themselves persistence that survives the cleanup.

1. ADS7.1 The Shape of Domain Dominance
2. ADS7.2 DCSync
3. ADS7.3 Golden Tickets and the KRBTGT Key
4. ADS7.4 Silver and Diamond Tickets
5. ADS7.5 Privileged-Group Persistence
6. ADS7.6 Stealth Persistence: SIDHistory, AdminSDHolder, DCShadow
7. ADS7.7 Reconstructing a Domain Takeover
8. Check My Knowledge

AD CS and Coercion Vectors

Active Directory Certificate Services is a second set of keys to the domain, and coercion is the trick that forces a domain controller to authenticate where an attacker wants.

1. ADS8.1 The Shape of AD CS and Coercion
2. ADS8.2 ESC1: Enrollee-Supplies-Subject
3. ADS8.3 The Rest of the ESC Family
4. ADS8.4 Coercion: PetitPotam, the Printer Bug, and the Spooler
5. ADS8.5 NTLM Relay and the ESC8 Chain
6. ADS8.6 GPO Abuse
7. ADS8.7 Reconstructing the Certificate Path
8. Check My Knowledge

Phase 3: The Hybrid Seam

The Hybrid Seam

On-prem Active Directory and Entra ID are one trust boundary stitched together by synchronization, and the seam between them is how an attacker who owns the domain reaches the cloud.

1. ADS9.1 The Shape of the Hybrid Seam
2. ADS9.2 The Pivot: An On-Prem Identity in the Cloud
3. ADS9.3 The Entra Connect Bridge
4. ADS9.4 Seamless SSO, Federation, and Golden SAML
5. ADS9.5 Reconstructing the Crossing
6. Check My Knowledge

Phase 4: Respond and Recover

Respond and Recover

Detecting a domain compromise is half the job; this module is the other half.

1. ADS10.1 Responding to an AD Compromise
2. ADS10.2 Scoping the Compromise
3. ADS10.3 Containing Without Tipping the Attacker
4. ADS10.4 Eradication: Resetting the Keys
5. ADS10.5 Recovery: When Rebuild Is the Only Answer
6. ADS10.6 What a Patch Does Not Fix
7. Check My Knowledge

Phase 5: Capstone

Capstone: The Northgate Compromise

The course's two halves on one intrusion.

1. ADS11.1 The Brief
2. ADS11.2 Phase 1: Entry and Credential Access
3. ADS11.3 Phase 2: Escalation and Dominance
4. ADS11.4 Phase 3: Persistence, Coercion, and the Crossing
5. ADS11.5 The Reconstruction
6. ADS11.6 The Response
7. ADS11.7 Capstone Summary
8. Check My Knowledge

Phase 0: Course Resources

Cheatsheets

The question, the query, what a hit means, and what the check does not prove, one sheet per attack stage.

1. Recon and Attack-Path Posture
2. Authentication and Credential Storage
3. Credential Theft and Replay
4. Delegation Abuse
5. Domain Dominance and Persistence
6. AD CS and Coercion
7. The Hybrid Seam
8. Audit Policy and Visibility
9. Respond and Recover
10. The Attack Lifecycle
11. Operating Cadence and Thresholds
12. Event Reference and Detection Surfaces

Cookbooks

Ordered procedures for the Active Directory hardening that recurs, each with the breakage it causes named up front.

1. Building Tiering That Holds
2. Reducing NTLM Without an Outage
3. Cleaning Up Delegation
4. Fixing Certificate Templates
5. Turning On the Visibility
6. Reducing Standing Privilege
7. Responding to a Domain Compromise

Lab Setup

A domain built with the misconfigurations this course finds, where you can run the attacks and watch what they leave behind.

1. Building the Domain
2. Planting the Misconfigurations
3. Attacking It, and Reading What Appeared
4. Hardening It, and Breaking Things
5. Verify, and What the Lab Cannot Teach

Walkthroughs

Active Directory work reasoned end to end, including the cases where the finding was already there and the ones that end in doing nothing.

1. The DCSync That Was Not
2. The Hardening That Would Have Stopped Payroll
3. The Template That Had Been There Six Years
4. The Lateral Movement That Was a Patch Cycle
5. The One That Was Real
6. The Recovery That Did Not Recover

Playbooks

What to do when a detection fires or somebody asks: DCSync, ticket forgery, a coerced authentication, a delegation change, a locked-out estate.

1. A DCSync Alert Fires
2. A Delegation Attribute Changed
3. Roasting Activity Detected
4. An Account Is Moving Across the Estate
5. A Certificate Was Issued for Somebody Else
6. You Believe They Have the Domain
7. The Hardening Locked People Out

Playground

Every practice surface available for this course, what each one gives you, and where the gaps are.

References & Further Reading

Microsoft Active Directory and identity documentation, MITRE ATT&CK techniques, security frameworks and standards, threat-intelligence research, and hardening and recovery guidance used throughout the Defending Active Directory course.

1. ADS100.1 References & Further Reading

Course Completion

Course Completion

You've reached the end of Defending Active Directory.

1. Course Completion. Defending Active Directory

Generated 2026-09-01 from the published course. The current syllabus is always at ridgelinecyber.com/training/courses/active-directory-security/