

ACTIVE DIRECTORY & KERBEROS.



Active Directory holds domain identities; Kerberos turns authentication into reusable tickets. **Protect the accounts, hosts, and keys behind that trust: a valid ticket is not proof of a safe session.**

- DOMAIN CONTROLLER PROTECTION
- SERVICE ACCOUNT HYGIENE
- TICKET ABUSE DETECTION
- PRIVILEGED ACCESS

01 THE MECHANISM



The Domain Authority

Domain controllers host AD Domain Services and the Kerberos Key Distribution Center (KDC). **Control of a domain controller can compromise the identities and systems that trust it.** Protect its administrators, backups, and management paths.



Tickets Replace Repeated Logons

After authentication, a client uses a ticket-granting ticket (TGT) to request service tickets. **The application still decides what access is allowed.** Ticket protection depends on the domain and service-account keys behind the exchange.



Trust Can Be Stolen or Forged

Kerberoasting targets service-account passwords; pass-the-ticket reuses stolen tickets. **A stolen KRBTGT key enables forged TGTs called Golden Tickets.** These are distinct attack paths, with different prerequisites and recovery actions.

02 THE FLOW

The Intended Authentication Flow EXPECTED

- 1 The client authenticates to the KDC on a domain controller and receives a **TGT for requesting service tickets**.
- 2 The client presents its TGT and requests a ticket for a service identified by a **Service Principal Name (SPN)**.
- 3 The client presents the service ticket; the service validates it and **applies its access permissions**. Single sign-on avoids repeated password prompts.

The Kerberoasting Attack Path ABUSED

- 1 An attacker with a valid domain identity requests a service ticket for an **SPN-bearing account**. The request can resemble ordinary activity.
- 2 The attacker tests password guesses against the ticket **offline**. Weak service-account passwords can be recovered without repeated logon failures.
- 3 A cracked password gives access as that service account. **Excessive privileges increase the damage**; obtaining a ticket alone does not grant domain administration.

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Domain & Admin Protection	Patch and restrict domain controllers. Use separate privileged accounts and secure administrative hosts; keep admin sessions off ordinary workstations.
Service Account Hygiene	Use gMSAs where supported; constrain which hosts may retrieve their passwords. Inventory SPNs, account owners, dependencies, and required privileges.
Kerberos Hardening	Require pre-authentication. Audit weak encryption and test AES compatibility before retiring RC4; keep passwords strong and delegation tightly scoped.
Detection & Recovery	Collect domain and endpoint telemetry, review identity alerts, and rehearse a forest-recovery plan with protected, tested backups.

04 DETECTION APPROACHES COMPARED

APPROACH	SUFFICIENT ALONE?	WHAT IT MISSES
Failed Logons Only	No	Offline password guessing and valid ticket reuse may produce no burst of failed logons.
RC4 Ticket Alerts	No	Useful exposure signal, but legitimate legacy activity exists and AES tickets can also be targeted.
Service Ticket Volume	No	Event 4769 exposes ticket requests; low-volume abuse can blend into normal service access.
Endpoint Alerts Only	No	Shows credential theft on covered hosts, but misses directory context and gaps in sensor coverage.
Correlated Identity + EDR	No	Best coverage combines ticket activity, host behavior, and account changes. Baselines and analyst review remain essential.

ACTIVE DIRECTORY & KERBEROS.

HARDEN · DETECT · RECOVER

05 PROGRAM OPERATIONS

Own the service-account inventory.

Record owners, SPNs, host access, privileges, and password handling. Prefer managed passwords; test application dependencies before rotations.

Baseline before alerting.

Collect DC ticket events and endpoint logons. Review unusual requester-to-service patterns, encryption changes, and privileged activity; a single signal is not a verdict.

Contain and scope ticket abuse.

Isolate affected hosts, preserve evidence, and identify exposed accounts and keys. A user password reset alone does not immediately revoke every issued ticket.

Plan domain recovery, not just resets.

For KRBTGT exposure, eradicate attacker access and coordinate two resets with replication and configured ticket lifetimes. Follow Microsoft's forest-recovery procedure.

06 CONTROL MAPPING

ATT&CK T1558.003

Kerberoasting: pair strong service-account secrets and least privilege with detection of unusual service-ticket requests.

ATT&CK T1550.003

Pass the Ticket: protect endpoint credentials and correlate unexpected ticket use with host and logon context.

ATT&CK T1558.001

Golden Ticket: protect KRBTGT and domain controllers; investigate forged-ticket indicators and prepare domain recovery.

MICROSOFT AD GUIDANCE

Operational baseline: reduce standing privileges, use secure admin hosts, harden domain controllers, and plan for compromise.

07 WHAT THIS DOES NOT SOLVE

Compromised Endpoints

Strong passwords do not prevent an attacker on a trusted host from abusing an already authenticated session.

Excessive Permissions

Kerberos authenticates identity; it does not repair overbroad groups, delegated rights, or application permissions.

Adjacent Identity Paths

AD certificate services, NTLM, and cloud identity require their own controls. Kerberos hardening does not cover every sign-in path.

Existing Persistence

Rotating secrets is not proof of eviction. Malicious accounts or directory changes may restore access after a reset.

08 MYTHS VS. REALITY

MYTH

"MFA makes stolen tickets harmless."

REALITY

MFA protects supported authentication steps. Ticket reuse can avoid a fresh interactive sign-in; endpoint and session defenses still matter.

MYTH

"AES eliminates Kerberoasting."

REALITY

AES raises the cost of guessing. Weak service-account passwords can still be cracked; use strong managed secrets as well.

MYTH

"Kerberoasting requires Domain Admin."

REALITY

A valid domain identity can request service tickets. The target account's password and privileges determine the impact.

MYTH

"Every unusual ticket proves compromise."

REALITY

Legitimate workloads and incomplete logs can look abnormal. Correlate identity, host, and service context before concluding an attack occurred.

MYTH

"One KRBTGT reset clears Golden Tickets."

REALITY

The previous key remains in password history. Two coordinated resets are required, with safe timing and removal of attacker persistence.

09 SPEAK THE PROGRAM — KEY TERMS

KDC

The Key Distribution Center runs on domain controllers and issues Kerberos authentication and service tickets.

TGT

A ticket-granting ticket lets a client ask the KDC for service tickets without resending its password for each request.

SERVICE TICKET & SPN

A service ticket targets a service identified by its Service Principal Name. The service enforces access.

KRBTGT

The domain account whose keys protect ticket-granting tickets. Key compromise enables Golden Ticket forgery.

GMSA

A group Managed Service Account lets Windows manage service-account passwords across authorized hosts.

EVENT 4769

A domain-controller audit event for a Kerberos service-ticket request. Useful for baselining, not proof of malicious activity.