Detection Strategy for Rogue Domain Controller (DCShadow) Registration and Replication Abuse, Detection Strategy DET0276

Archived: 2026-04-02 12:09:48 UTC

AN0770

Detection of rogue Domain Controller registration and Active Directory replication abuse by correlating: (1) creation/modification of nTDSDSA and server objects in the Configuration partition, (2) unexpected usage of Directory Replication Service SPNs (GC/ or E3514235-4B06-11D1-AB04-00C04FC2DCD2), (3) replication RPC calls (DrsAddEntry, DrsReplicaAdd, GetNCChanges) originating from non-DC hosts, and (4) Kerberos authentication by non-DC machines using DRS-related SPNs. These events in combination, especially from hosts outside the Domain Controllers OU, may indicate DCShadow or rogue DC activity.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Window (seconds) between nTDSDSA object creation and subsequent replication traffic from same host (default 300s).
AllowedReplicationPartners	List of legitimate DCs authorized for replication to reduce false positives.
SuspiciousSPNs	SPNs indicating replication service usage (GC/, GUID E3514235-4B06-11D1-AB04-00C04FC2DCD2).
NonDCObjectCreationAlert	Trigger alerts only when AD object creation is by accounts not in Domain Admins or Enterprise Admins groups.