Detect Adversary-in-the-Middle via Network and Configuration Anomalies, Detection Strategy DET0296

Archived: 2026-04-05 18:06:54 UTC

AN0823

Detects suspicious DNS/ARP poisoning attempts, unauthorized modifications to registry/network configuration, or abnormal TLS downgrade activity. Correlates changes in system configuration with subsequent unusual network flows or authentication events.

Log Sources

Mutable Elements

Field	Description
MonitoredRegistryPaths	Specific network stack and DNS registry keys that vary by enterprise configuration.
DowngradeCipherList	List of weak/legacy ciphers tuned per environment for TLS downgrade detection.
TimeWindow	Correlation period between config changes and abnormal network connections.

AN0824

Detects unauthorized edits to /etc/hosts, /etc/resolv.conf, or suspicious ARP broadcasts. Correlates file modifications with subsequent unexpected network sessions or service creation.

Log Sources

Mutable Elements

Field	Description
MonitoredFiles	List of system files shaping traffic flow (hosts, resolv.conf, PAM modules).
ARPThreshold	Rate/volume thresholds for ARP/DNS anomalies tuned per subnet.

AN0825

Detects unauthorized edits to system configuration profiles, unexpected certificate trust changes, or abnormal ARP/DNS patterns indicative of interception.

Log Sources

Mutable Elements

Field	Description
ProfileIdentifiers	Known good vs suspicious configuration profiles per enterprise baseline.
TLSVersionThreshold	Minimum TLS version accepted in network traffic inspection.

AN0826

Detects unauthorized firmware or configuration changes enabling adversary-in-the-middle positioning (e.g., route injection, DNS spoofing, SSL downgrade). Behavioral analytics focus on sudden changes to routing tables or image file integrity failures.

Log Sources

Mutable Elements

Field	Description
RoutingPolicyBaseline	Expected routing and BGP/OSPF paths for validation.
FirmwareChecksum	Baseline image checksum per device type used to detect tampering.
