Detection Strategy for Encrypted Channel via Asymmetric Cryptography across OS Platforms, Detection Strategy DET0543

Archived: 2026-04-05 17:10:51 UTC

AN1496

Processes not typically associated with encryption loading asymmetric crypto libraries (e.g., rsaenh.dll, crypt32.dll) and subsequently initiating outbound TLS/SSL connections with abnormal certificate chains or handshakes. Defender correlates process creation, module load, and unusual encrypted sessions.

Log Sources

Mutable Elements

Field	Description
AllowedCryptoProcesses	Whitelist browsers, mail clients, or apps expected to use asymmetric crypto.
CertificateAuthorityList	Baseline CA list for validating abnormal certs.
HandshakeTimeout	Detection of incomplete or malformed handshakes.

AN1497

Processes (e.g., bash, python, custom binaries) dynamically linking libcrypto/libssl for RSA key exchange, then creating external connections with abnormal certificate validation or handshake anomalies. Defender observes syscall traces and outbound asymmetric key exchanges from non-SSL-native processes.

Log Sources

Mutable Elements

Field	Description
ExpectedCryptoLibs	Baseline libraries that normally handle asymmetric crypto.
TrafficAsymmetryRatio	Threshold for client-heavy data sending vs server.

AN1498

Applications or launchd services invoking RSA or public-key routines from the Security framework, followed by outbound SSL/TLS sessions with unrecognized certs or anomalous handshakes. Defender observes unified logs of

API calls and suspicious network entropy.

Log Sources

Mutable Elements

Field	Description
TrustedDoHEndpoints	Known legitimate DoH/SSL endpoints.
PayloadEntropyThreshold	Entropy scoring for outbound payloads.

AN1499

VMware services (hostd, vpxa) unexpectedly negotiating asymmetric crypto sessions to external endpoints outside vCenter or update servers. Defender sees encrypted handshakes in logs inconsistent with baseline ESXi communication patterns.

Log Sources

Mutable Elements

Field	Description
BaselineMgmtHosts	Expected external endpoints (vCenter, update repos).

AN1500

Encrypted sessions detected with asymmetric key exchange anomalies on non-standard ports or with invalid/malformed certs. Defender correlates NetFlow/IPFIX with IDS/IPS detecting RSA exchanges outside expected TLS flows.

Log Sources

Mutable Elements

Field	Description
PortProfiles	Define expected ports for asymmetric cryptography (e.g., 443, 993).
CertValidationPolicy	Thresholds for rejecting untrusted/self-signed certs.
