Detection Strategy of Transmitted Data Manipulation, Detection Strategy DET0254

Archived: 2026-04-05 18:37:54 UTC

AN0702

Monitor for anomalies in transmitted data streams, including mismatched file integrity checks, API interception, or man-in-the-middle modifications. Detect unexpected use of APIs that handle network I/O where transmitted data integrity could be manipulated.

Log Sources

Mutable Elements

Field	Description
IntegrityBaseline	Hash baselines or digital signature references to validate transmitted data.
MonitoredPorts	List of ports/services where data integrity validation is enforced.

AN0703

Detect alterations of transmitted data via monitoring syscalls (`send` , `recv` , `write`) or middleware interception. Identify mismatched file hashes when compared at origin vs. destination. Watch for anomalous activity from processes interacting with secure transmission services (e.g., OpenSSL, scp).

Log Sources

Mutable Elements

Field	Description
WatchedProcesses	List of processes authorized to handle transmitted data (e.g., sshd, nginx).
HashCheckInterval	Frequency of out-of-band integrity verification checks.

AN0704

Monitor system APIs such as CFNetwork and SecureTransport for anomalies in transmitted data streams. Detect mismatches in file hashes or SSL/TLS downgrade attempts that enable manipulation of transmitted data.

Log Sources

Data Component	Name	Channel
Network Traffic Flow (DC0078)	macos:unifiedlog	Suspicious anomalies in transmitted data integrity during application network operations
OS API Execution (DC0021)	macos:osquery	CALCULATE: Integrity validation of transmitted data via hash checks

Mutable Elements

Field	Description
TLSValidationRules	Custom rules for enforcing HTTPS/TLS integrity checks to prevent downgrade manipulation.
AllowedApps	Whitelisted macOS apps permitted to transmit critical data.
