Detection Strategy for Wi-Fi Networks, Detection Strategy DET0536

Archived: 2026-04-05 13:51:47 UTC

AN1476

Detects anomalous wireless connections such as unexpected SSID associations, failed or repeated authentication attempts, and connections outside of known geofenced networks. Defenders should monitor wireless connection logs and event codes for network discovery, authentication, and association events.

Log Sources

Mutable Elements

Field	Description
KnownSSIDList	Defines approved Wi-Fi SSIDs for the environment; deviations may indicate malicious connection attempts.
GeoLocationContext	Correlates expected physical location of systems with observed Wi-Fi connections to detect anomalies.

AN1477

Detects unauthorized wireless associations by monitoring wpa_supplicant logs, NetworkManager events, and system calls related to interface state changes. Anomalies include repeated association failures, new SSIDs outside baselined values, and rogue AP connections.

Log Sources

Mutable Elements

Field	Description
AllowedSSIDRegex	Regex-based whitelist of corporate SSIDs; anomalous matches indicate suspicious activity.
RetryThreshold	Number of failed association attempts allowed before triggering detection.

AN1478

Detects unauthorized Wi-Fi associations and SSID scanning activity using unified logs and airport command telemetry. Anomalies include rapid SSID switching, connections to unapproved SSIDs, or repeated authentication failures.

Log Sources

Mutable Elements

Field	Description
BaselineSSIDHistory	Historical record of corporate SSID associations per device; deviations may indicate rogue AP usage.

AN1479

Detects rogue or suspicious wireless access attempts by monitoring firewall, WIDS/WIPS, and controller logs. Focus is on firewall rule changes, rogue AP detection, and anomalous MAC addresses connecting to access points.

Log Sources

Mutable Elements

Field	Description
AuthorizedAPList	Defines known access points and MAC addresses; deviations highlight rogue or unauthorized devices.
