Detect Evil Twin Wi-Fi Access Points on Network Devices, Detection Strategy DET0379

Archived: 2026-04-05 14:41:53 UTC

AN1069

Detects rogue Wi-Fi access points broadcasting the same SSID as legitimate APs with stronger signal strength, unexpected MAC/BSSID values, or inconsistent encryption settings. Correlates authentication attempts, captive portal redirections, and anomalous traffic flows through unauthorized APs.

Log Sources

Mutable Elements

Field	Description
KnownSSIDs	Baseline of authorized SSIDs; deviations may indicate rogue AP.
AllowedBSSIDs	Whitelist of BSSID/MAC addresses mapped to corporate SSIDs.
SignalStrengthThreshold	Used to flag unusually strong signals from unexpected APs.
CaptivePortalDomains	Trusted login domains; unrecognized portals may be malicious.
