Detection of Wireless Sniffing, Detection Strategy DET0743

Archived: 2026-04-05 13:10:24 UTC

AN1876

Purely passive network sniffing cannot be detected effectively. In cases where the adversary interacts with the wireless network (e.g., joining a Wi-Fi network) detection may be possible. Monitor for new or irregular network traffic flows which may indicate potentially unwanted devices or sessions on wireless networks. In Wi-Fi networks monitor for changes such as rogue access points or low signal strength, indicating a device is further away from the access point then expected and changes in the physical layer signal.[1] [2] Network traffic content will provide important context, such as hardware (e.g., MAC) addresses, user accounts, and types of messages sent.

Log Sources
