Detection Strategy for Network Sniffing Across Platforms, Detection Strategy DET0314

Archived: 2026-04-05 15:30:38 UTC

AN0875

Detects suspicious execution of network monitoring tools (e.g., Wireshark, tshark, Microsoft Message Analyzer), driver loading indicative of promiscuous mode, or non-admin user privilege escalation to access NICs for capture.

Log Sources

Mutable Elements

Field	Description
ToolNames	Adjust list of known sniffing tools based on environment and known administrator usage.
TimeWindow	Tune time of day or frequency of capture sessions to reduce false positives from authorized use.

AN0876

Correlates interface mode changes to promiscuous with execution of sniffing tools like tcpdump, tshark, or custom pcap libraries. Detects abnormal NIC configurations and unauthorized sniffing from non-root sessions.

Log Sources

Mutable Elements

Field	Description
InterfaceList	Limit analysis to external interfaces (e.g., eth0, wlan0) and exclude virtual adapters.
PromiscuousSessionThreshold	Raise alerts if interface remains in PROMISC longer than threshold duration.

AN0877

Detects enabling of interface sniffing via packet capture tools or AppleScript triggering `tcpdump`. Leverages Unified Logs and process lineage to identify suspicious use of `pfctl`, `tcpdump`, or `libpcap` libraries.

Log Sources

Mutable Elements

Field	Description
AllowedTools	Whitelist Apple-native tools used by IT admins and mobile device management (MDM).
UserContext	Prioritize detections from non-admin or low-privilege users performing packet captures.

AN0878

Detects creation of traffic mirroring sessions (e.g., AWS VPC Traffic Mirroring, Azure vTAP) that redirect traffic from critical assets to other virtual instances, often followed by file creation or session establishment.

Log Sources

Mutable Elements

Field	Description
MirrorSourceList	Identify VMs or containers where mirror sessions are abnormal or unexpected.
TargetIAMRole	Monitor whether mirror target roles match administrative expectations.

AN0879

Detects execution of capture commands via CLI (`monitor capture` , `debug packet` , etc.) or unauthorized CLI access followed by logging configuration changes on Cisco/Juniper/Arista gear.

Log Sources

Mutable Elements

Field	Description
AdminSessionDuration	Tunable alerting threshold for interactive CLI sessions.
CaptureCommandList	Define set of known capture/debug commands per vendor to flag unexpected usage.
