Detection Strategy for SNMP (MIB Dump) on Network Devices, Detection Strategy DET0453

Archived: 2026-04-05 15:03:45 UTC

AN1249

Defenders may observe suspicious SNMP MIB enumeration through abnormal queries for large sets of OIDs, repeated SNMP GETBULK/GETNEXT requests, or queries originating from non-administrative IP addresses. Anomalous use of community strings, authentication failures, or enumeration activity outside maintenance windows may also indicate attempts to dump MIB contents. Correlation across syslog, NetFlow, and SNMP audit data can reveal chains of behavior such as repeated authentication failures followed by successful large-scale OID retrieval.

Log Sources

Mutable Elements

Field	Description
AuthorizedAdminIPs	Expected IP ranges allowed to query SNMP. Deviation indicates possible misuse.
NormalSNMPQueryRate	Baseline frequency and volume of SNMP queries; anomalies above threshold may indicate dumping.
CommunityStringPatterns	Expected community strings (e.g., hashed or custom values). Unrecognized strings may signal abuse.
TimeWindow	Time periods during which SNMP queries are authorized. Queries outside these hours may be malicious.
