Behavioral Detection Strategy for Network Service Discovery Across Platforms, Detection Strategy DET0376

Archived: 2026-04-05 17:29:44 UTC

AN1057

Detects processes performing network enumeration (e.g., port scans, service probing) by correlating process creation, socket connections, and sequential destination IP probing within a time window.

Log Sources

Mutable Elements

Field	Description
ScanRateThreshold	Defines the number of unique destination IPs or ports accessed within a time window that may indicate a scan.
KnownScannerExeList	List of binaries allowed to scan or used by IT (e.g., Nmap, Nessus).
TimeWindow	Temporal bounds for correlating sequential connections (e.g., 60 seconds).

AN1058

Detects use of network scanning utilities or scripts performing rapid connections to multiple services or hosts using auditd and netflow/pcap telemetry.

Log Sources

Mutable Elements

Field	Description
PortScanThreshold	Defines number of ports targeted per host within a short period.
ToolPatternRegex	Regex to match common scanner arguments (e.g., `nmap -sS`, `nc -zv`).
ExpectedScanSources	Trusted IPs or systems performing routine discovery.

AN1059

Detects Bonjour-based mDNS enumeration or use of system tools (e.g., dns-sd, nmap) to find active services via multicast probing or targeted scans.

Log Sources

Mutable Elements

Field	Description
MDNSServiceQueryPatterns	mDNS queries such as _ssh._tcp.local that may indicate service discovery.
UserContext	Adjust alerting based on whether discovery activity originates from a background daemon vs. interactive session.
ScanToolList	Expected tools that could trigger mDNS or TCP/UDP scans (e.g., dns-sd, nmap).

AN1060

Detects lateral discovery or container breakout attempts using netcat, curl, or custom binaries probing other services within the same namespace or VPC subnet.

Log Sources

Mutable Elements

Field	Description
ExecutablePath	Custom or renamed versions of tools may use different paths
TimeWindow	Aggregation interval for identifying anomalous traffic
NetworkDestinationCount	Tunable count of unique destinations to classify discovery

---