Behavioral Detection of Internet Connection Discovery, Detection Strategy DET0357

Archived: 2026-04-05 16:32:05 UTC

AN1015

Execution of utilities (e.g., ping, tracert, Test-NetConnection) or scripted methods to test Internet connectivity by interacting with external IPs/domains.

Log Sources

Mutable Elements

Field	Description
DestinationIP	Tunable external IP ranges or domains used to verify Internet access (e.g., 8.8.8.8, example.com)
TimeWindow	Cluster rapid test connections with command execution in < 60 seconds
UserContext	Filter out known admin/script contexts to reduce false positives

AN1016

Execution of ping, traceroute, or curl/wget against public IPs/domains to verify Internet reachability.

Log Sources

Mutable Elements

Field	Description
DomainPatterns	Regex for common test domains like example.com, google.com
ProtocolType	Adjust focus to ICMP, HTTP, or mixed protocol testing

AN1017

Execution of ping, traceroute, or network utility tools to external destinations; may include `scutil` or system_profiler.

Log Sources

Mutable Elements

Field	Description
ExecutionFrequency	Rare use of ICMP utilities may be tuned based on user/host baselines
EnrichmentLevel	Tune data joins with parent process and user activity context

AN1018

Execution of `ping`, `vmkping`, or `curl` from shell or through automation jobs/scripts to verify Internet egress.

Log Sources

Mutable Elements

Field	Description
SSHSessionOrigin	Distinguish external SSH sessions from internal admin maintenance
TargetIP	Egress test destination may be filtered to known CDNs/test nodes

---