Detection Strategy for Dynamic Resolution across OS Platforms, Detection Strategy DET0039

Archived: 2026-04-02 10:40:48 UTC

AN0109

Correlate high-frequency or anomalous DNS query activity with processes that do not normally generate network requests (e.g., Office apps, system utilities). Detect pseudo-random or high-entropy domain lookups indicative of domain generation algorithms (DGAs).

Log Sources

Mutable Elements

Field	Description
EntropyThreshold	Adjust based on environment to differentiate DGAs from legitimate CDNs
TimeWindow	Interval for correlating bursts of DNS queries from the same process

AN0110

Monitor /var/log/audit/audit.log and DNS resolver logs for repeated failed lookups or connections to high-entropy domain names. Correlate suspicious DNS queries with process lineage (e.g., Python, bash, or unusual system daemons).

Log Sources

Mutable Elements

Field	Description
DomainReputationFeed	Whitelist/blacklist tuned with external threat intel sources
ProcessWhitelist	Known safe daemons that frequently query domains

AN0111

Inspect unified logs for anomalous DNS resolutions triggered by non-network applications. Flag repeated connections to newly registered or algorithmically generated domains. Correlate with endpoint process telemetry.

Log Sources

Mutable Elements

Field	Description
NewDomainThreshold	Age of domain registration considered suspicious (e.g., < 30 days)
DNSQueryVolume	Number of queries per process per time window

AN0112

Monitor esxcli and syslog records for DNS resolver changes or repeated queries to unusual external domains by management agents. Detect unauthorized changes to VM or host network settings that redirect DNS lookups.

Log Sources

Mutable Elements

Field	Description
ResolverConfigPaths	Expected resolvers or DNS forwarders in ESXi configurations
ExternalDomainWhitelist	Set of trusted external domains expected for ESXi host activity

---