Detection Strategy for Dynamic Resolution using Domain Generation Algorithms., Detection Strategy DET0419

Archived: 2026-04-05 14:26:51 UTC

AN1178

Correlate DNS queries that generate domains with high entropy or gibberish patterns, combined with short-lived connections from unusual processes. Monitor Sysmon DNS events and Windows Security logs for abnormal query rates and failed lookups.

Log Sources

Mutable Elements

Field	Description
EntropyThreshold	Set threshold for randomness in queried domain strings (e.g., >4.0)
QueryFailureRate	Failed resolution ratio above normal baseline (e.g., >30%)
TimeWindow	Duration for aggregating suspicious DNS queries (e.g., 5–10 min)

AN1179

Identify processes issuing repeated DNS queries to random-looking domains with abnormal entropy or word concatenations. Correlate resolver logs with high NXDOMAIN rates and auditd socket connections.

Log Sources

Mutable Elements

Field	Description
NXDOMAINThreshold	Ratio of failed queries triggering alert (e.g., >40%)
DomainAge	Flag queries to domains registered in last 7–30 days

AN1180

Monitor unified DNS logs for abnormal domain queries with low lexical similarity to known domains, repeated failed lookups, and random string structures. Cross-check with process logs to confirm unusual origins (non-browser apps).

Log Sources

Mutable Elements

Field	Description
ReputationFeedWhitelist	Exclude trusted CDN and cloud provider domains
LexicalScoreThreshold	Adjust score for word-based vs. letter-based DGAs

AN1181

Use ESXi syslogs to track abnormal DNS query patterns from management agents or VMs. Identify high-frequency, low-TTL, or unresolvable domains as suspicious. Correlate with unusual management plane process activity.

Log Sources

Mutable Elements

Field	Description
ResolverConfigPaths	Expected resolver settings for ESXi hosts
DomainWhitelist	Trusted external domains for hypervisor operations

---