Detection Strategy for Dynamic Resolution through DNS Calculation, Detection Strategy DET0262

Archived: 2026-04-05 16:19:41 UTC

AN0728

Monitor DNS query results where subsequent connections use derived or unusual port numbers not explicitly resolved, especially when tied to suspicious processes. Correlate Sysmon DNS logs (Event ID 22) with process creation and socket activity.

Log Sources

Mutable Elements

Field	Description
PortDeviationThreshold	Deviation from common service ports (e.g., >1024 when DNS resolved service expects 80/443)
TimeWindow	Correlation window between DNS response and network connection (e.g., 5 minutes)

AN0729

Inspect resolver and audit logs for processes initiating outbound connections to ports calculated from DNS response IPs. Abnormal ephemeral port usage shortly after DNS queries can indicate DNS calculation behavior.

Log Sources

Mutable Elements

Field	Description
EphemeralPortRange	Configured ephemeral port ranges per environment to reduce false positives
ResolverWhitelist	Exclude trusted resolvers or internal services from analysis

AN0730

Use unified logs to detect unusual DNS responses correlated with subsequent connections to calculated or non-standard ports. Monitor non-browser apps making repeated outbound connections that deviate from expected patterns.

Log Sources

Mutable Elements

Field	Description
ProcessAllowlist	Expected processes allowed to open non-standard ports (e.g., developer tools)
ConnectionVolumeThreshold	Volume of unusual connections needed before flagging as suspicious

AN0731

Analyze ESXi syslogs for management agents or VMs making outbound connections to dynamically calculated ports derived from DNS responses. Cross-check with VM traffic baselines to identify anomalies.

Log Sources

Mutable Elements

Field	Description
ManagementPlaneIPs	Known trusted ESXi management plane IPs to exclude from alerts
DomainReputationFeed	Integrate external feeds for reputation context on DNS-derived domains

---