Detection Strategy for Endpoint DoS via Service Exhaustion Flood, Detection Strategy DET0173

Archived: 2026-04-05 16:57:34 UTC

AN0489

High-frequency, repetitive service requests (e.g., HTTP, TLS renegotiation) originating from a single or small set of source IPs targeting endpoint web services or application ports, leading to exhaustion of CPU or memory on targeted Windows services.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Defines burst threshold (e.g., 1 min, 5 min) for connection spikes
TargetServicePort	Specific ports/services likely to be abused (e.g., 80, 443, 8080)
CPUThreshold	Level of sustained CPU usage considered anomalous for a given service

AN0490

Excessive inbound HTTP or TLS connections to services such as Apache or Nginx, causing worker thread exhaustion or segmentation faults.

Log Sources

Mutable Elements

Field	Description
ErrorCodeWindow	Tunable count of specific HTTP error codes in timeframe
ConnectionRateThreshold	Defines number of connections per second considered anomalous

AN0491

Flood of incoming TLS or HTTP(S) connections to macOS-hosted services (e.g., MAMP, Apache), causing high CPU usage and system unresponsiveness.

Log Sources

Data Component	Name	Channel
Host Status (DC0018)	macos:unifiedlog	Web service process (e.g., httpd) entering crash loop or consuming excessive CPU
Network Traffic Content (DC0085)	macos:unifiedlog	Rapid incoming TLS handshakes or HTTP requests in quick succession

Mutable Elements

Field	Description
TLSHandshakeRate	Number of renegotiations per minute considered suspicious
ServiceCrashFrequency	Threshold of crashes before alerting on instability

AN0492

Automated or scripted HTTP/TLS flooding from one VM or cloud instance against another service, exploiting compute-based billing or exhaustion of service infrastructure.

Log Sources

Mutable Elements

Field	Description
VPCFlowBurstRate	Threshold for traffic burst on target service port
EC2CPUThreshold	Compute saturation level for alerting (e.g., >90% for 3 minutes)
