Application Exhaustion Flood Detection Across Platforms, Detection Strategy DET0415

Archived: 2026-04-05 14:01:12 UTC

AN1165

Repeated invocation of high-resource application endpoints or GUI components causing CPU and memory spikes, logged as elevated request volumes, prolonged handle locks, or frequent crash recoveries.

Log Sources

Mutable Elements

Field	Description
CPUThreshold	Define what percentage of CPU usage indicates abnormal behavior.
MemoryConsumptionWindow	Window (e.g., 5 mins) during which sustained memory usage may be abnormal.
AppCrashFrequency	Threshold for frequency of application faults within a specific interval.

AN1166

Automated scripts or repeated CLI/API requests that trigger application backends to consume high CPU or memory (e.g., Apache/PHP, MySQL, mail servers), resulting in syslog errors and excessive process spawning.

Log Sources

Mutable Elements

Field	Description
SyslogErrorRate	Defines number of critical errors in logs within time window.
PortRequestSpikeThreshold	Spike rate on monitored service port triggering alert.
ProcessSpawnRate	Rate of process creation that may overwhelm the system.

AN1167

Repetitive triggering of GUI or backend application workflows that cause increased CPU/memory usage, logged in unified logs as spin reports or crash dumps.

Log Sources

Mutable Elements

Field	Description
SpinReportCount	Threshold for number of system spin/crash reports in a defined window.
HeavyAppReopenRate	Frequency of user or script reopening GUI-heavy apps.

AN1168

Automated abuse of cloud-hosted applications (e.g., web apps, REST endpoints, internal APIs) causing compute exhaustion, high 5xx error rates, or frequent autoscaling triggers logged in app insights or cloudwatch.

Log Sources

Mutable Elements

Field	Description
HTTP5xxRateThreshold	Ratio of 5xx error codes over requests indicating resource exhaustion.
FunctionInvocationRate	Spike in lambda/API gateway executions indicating scripted behavior.
AutoscaleEventCount	Triggers linked to app DoS where legitimate scaling is mimicked.
