Direct Network Flood Detection across IaaS, Linux, Windows, and macOS, Detection Strategy DET0343

Archived: 2026-04-05 15:26:30 UTC

AN0969

High-volume packet generation by local processes (e.g., PowerShell, cmd, curl.exe) or network service processes resulting in excessive outbound traffic over short time window, correlated with abnormal resource usage or degraded host responsiveness.

Log Sources

Mutable Elements

Field	Description
PacketRateThreshold	Defines the burst threshold (e.g., 10,000 pps) above which activity should be flagged as anomalous.
TimeWindow	Duration over which to aggregate and analyze flow volume.

AN0970

Kernel or userland processes generating high-rate network traffic (ICMP, UDP, TCP SYN) beyond expected interface throughput or user behavior norms.

Log Sources

Mutable Elements

Field	Description
SyscallBurstCount	Threshold of repeated socket calls within a short interval indicating flood behavior.
UserContext	Restrict to non-admin user traffic unless elevated access is detected.

AN0971

Excessive outbound traffic via `ping`, `curl`, or custom scripts indicating flooding behavior, especially with no UI context or user interaction.

Log Sources

Mutable Elements

Field	Description
BurstTimeWindow	Tunable range (e.g., 15s, 30s) for detecting packet floods.

AN0972

VM or cloud instance generating anomalously high network egress targeting same destination IP or service, especially using stateless protocols.

Log Sources

Mutable Elements

Field	Description
InstanceTrafficThreshold	Alert when egress exceeds normal usage by X%.
ProtocolType	Prioritize alerts on stateless protocols such as UDP and ICMP.
