Detection Strategy for Non-Standard Ports, Detection Strategy DET0227

Archived: 2026-04-05 12:55:50 UTC

AN0633

Processes initiating outbound connections on uncommon ports or using protocols inconsistent with the assigned port. Correlating process creation with subsequent network connections reveals anomalies such as svchost.exe or Office applications using high, atypical ports.

Log Sources

Mutable Elements

Field	Description
PortThresholds	Define what constitutes a 'non-standard port' based on organizational baselines (e.g., allow 443/80/22 but flag 8088/587/3389 changes).
ProcessAllowList	Processes normally allowed to use non-standard ports (e.g., custom apps).
TimeWindow	Correlate process creation and network activity within N seconds.

AN0634

Unusual daemons or user processes binding/listening on ports outside of standard ranges, or initiating client connections using mismatched protocol/port pairings.

Log Sources

Mutable Elements

Field	Description
AllowedServices	Exclude ports intentionally configured for enterprise apps.
PayloadEntropyThreshold	Define thresholds for anomalous payload entropy to catch tunneled traffic.

AN0635

Applications making outbound connections on non-standard ports or launchd services bound to ports inconsistent with system baselines.

Log Sources

Mutable Elements

Field	Description
BaselinePortProfiles	Define expected macOS service port usage (e.g., AirDrop, Bonjour).

AN0636

VM services or management daemons communicating on ports not defined by VMware defaults, such as vpxa or hostd processes initiating traffic over high-numbered or unexpected ports.

Log Sources

Mutable Elements

Field	Description
ESXiAllowedPorts	Default VMware service ports that should not be flagged.
