Detection Strategy for Exfiltration Over C2 Channel, Detection Strategy DET0348

Archived: 2026-04-05 16:34:47 UTC

AN0988

Identifies suspicious outbound traffic volume mismatches from processes that typically do not generate network activity, particularly over C2 protocols like HTTPS, DNS, or custom TCP/UDP ports, following file or data access.

Log Sources

Mutable Elements

Field	Description
DataVolumeThreshold	Set threshold for outbound transfer size exceeding typical C2 traffic (e.g., >1MB in <5min).
KnownBenignProcesses	List of approved processes that may exhibit high outbound traffic (e.g., updates).

AN0989

Monitors for processes reading sensitive files then immediately initiating unusual outbound connections or bulk transfer sessions over persistent sockets, particularly with encrypted or binary payloads.

Log Sources

Mutable Elements

Field	Description
OutboundEntropyScore	Threshold for high-entropy payloads indicative of encoded or encrypted exfil data.
ConnectionDuration	Defines length of time over which transfer size must be aggregated to trigger detection.

AN0990

Detects unauthorized applications or scripts accessing sensitive data followed by establishing encrypted outbound communication to rare external destinations or with abnormal byte ratios.

Log Sources

Mutable Elements

Field	Description
ParentProcessAncestry	Enables defenders to tune legitimate vs. suspicious lineage (e.g., launchd → curl is uncommon).
ProtocolList	Focus detection on unusual protocols (e.g., IRC, FTP, DNS over HTTPS).

AN0991

Detects VMs sending outbound traffic through non-standard services or to unknown destinations. Exfiltration over reverse shells tunneled via VMkernel or custom payloads routed via hostd/vpxa.

Log Sources

Mutable Elements

Field	Description
GuestOSAllowList	Limit detection to sensitive or externally-exposed VMs handling confidential data.
TransferSizeThresholdMB	Minimum outbound transfer size before flagging anomalous C2-based exfiltration.
ProtocolAllowList	Define expected protocols for outbound data (e.g., disallow FTP/SCP over high ports).
