Network Traffic Flow, Data Component DC0078

Archived: 2026-04-05 15:28:42 UTC

auditd:SYSCALL socket/connect auditd:SYSCALL socket/connect syscalls auditd:SYSCALL connect or sendto system call with burst pattern auditd:SYSCALL ioctl: Changes to wireless network interfaces (up, down, reassociate) AWS:CloudTrail CreateTrafficMirrorSession or ModifyTrafficMirrorTarget AWS:VPCFlowLogs egress > 90th percentile or frequent connection reuse AWS:VPCFlowLogs VPC/NSG flow logs for pod/instance egress to Internet or metadata AWS:VPCFlowLogs Outbound data flows AWS:VPCFlowLogs Unusual volume of inbound packets from single source across short time interval AWS:VPCFlowLogs Outbound flow logs to known mining pools AWS:VPCFlowLogs source instance sends large volume of traffic in short window AWS:VPCFlowLogs Large outbound UDP traffic to multiple public reflector IPs container:cni Outbound network traffic to mining proxies containerd:runtime container-level outbound traffic events dns:query Outbound resolution to hidden service domains (e.g., `.onion`) esxi:hostd CLI network calls esxi:syslog esxcli network vswitch or DNS resolver configuration updates esxi:syslog DNS resolution events leading to outbound traffic on unexpected ports esxi:syslog /var/log/syslog.log esxi:syslog Frequent DNS queries with high entropy names or NXDOMAIN results esxi:syslog Frequent DNS resolution of same domain with rotating IPs esxi:vmkernel /var/log/vmkernel.log esxi:vmkernel HTTPS traffic to repository domains esxi:vmkernel None esxi:vmkernel egress log analysis esxi:vmkernel egress logs esxi:vmkernel network flows to external cloud services esxi:vmkernel port 22 access esxi:vobd Network Events esxi:vpxa connection attempts and data transmission logs esxi:vpxd ESXi service connections on unexpected ports esxi:vpxd TLS session established by ESXi service to unapproved endpoint esxi:vpxd None esxi:vpxd ESXi processes relaying traffic via SSH or unexpected ports iptables:LOG TCP connections iptables:LOG OUTBOUND linux:osquery socket_events linux:syslog Multiple IP addresses assigned to the same domain in rapid sequence m365:defender NetworkConnection: high out:in ratio, periodic beacons, protocol mismatch M365Defender:DeviceNetworkEvents NetworkConnection: bytes_sent >> bytes_received anomaly macos:osquery socket_events macos:osquery query: Historical list of associated SSIDs compared against baseline macos:unifiedlog Suspicious outbound traffic from browser binary to non-standard domains macos:unifiedlog HTTPS POST to known webhook URLs macos:unifiedlog com.apple.network macos:unifiedlog outbound TCP/UDP traffic over unexpected port macos:unifiedlog tcp/udp macos:unifiedlog Suspicious anomalies in transmitted data integrity during application network operations macos:unifiedlog HTTPS POST requests to pastebin.com or similar macos:unifiedlog Firewall/PF anchor load or rule change events. macos:unifiedlog sudden burst in outgoing packets from same PID macos:unifiedlog forwarded encrypted traffic macos:unifiedlog ARP table updates inconsistent with expected gateway or DHCP lease assignments macos:unifiedlog networkd or com.apple.network macos:unifiedlog log stream 'eventMessage contains "dns_request"' macos:unifiedlog Outbound UDP spikes to external reflector IPs macos:unifiedlog High entropy domain queries with multiple NXDOMAINs macos:unifiedlog Rapid domain-to-IP resolution changes for same domain macos:unifiedlog Firewall rule enable/disable or listen socket changes macos:unifiedlog Outbound connections from IDE processes to marketplace/tunnel domains NetFlow:Flow new outbound connections from exploited process tree Network Traffic None networkdevice:syslog flow records networkdevice:syslog Config/ACL changes, line vty transport input changes, telnet/ssh/http(s) enable, image/feature module changes. networkdevice:syslog Config change: CLI/NETCONF/SNMP – 'monitor session', 'mirror port'

networkdevice:syslog Config/ACL/line vty changes, service enable (telnet/ssh/http(s)), module reloads NIDS:Flow session stats with bytes_out > bytes_in NSM:Connections Internal connection logging NSM:Connections new connections from exploited lineage NSM:Connections Outbound Connection NSM:Connections Inbound on ports 5985/5986 NSM:firewall inbound connection to port 5900 NSM:Firewall Outbound connections to 139/445 to multiple destinations NSM:Firewall pf firewall logs NSM:Flow Unexpected flows between segmented networks or prohibited ports NSM:Flow First-time outbound connections to package registries or unknown hosts immediately after restore/build NSM:Flow First-time egress to new registries/CDNs post-install/build NSM:Flow First-time egress to non-approved registries after dependency install NSM:Flow Outbound connections to TCP 139,445 and HTTP/HTTPS to WebDAV endpoints from workstation subnets NSM:Flow large outbound data flows or long-duration connections NSM:Flow conn.log NSM:Flow connection metadata NSM:Flow LEASE_GRANTED NSM:Flow MAC not in allow-list acquiring IP (DHCP) NSM:Flow pf firewall logs NSM:Flow Inter-segment traffic NSM:Flow None NSM:Flow Long-lived or hijacked SSH sessions maintained with no active user activity NSM:Flow Abnormal browser traffic volume or destination NSM:Flow Outbound requests to domains not previously resolved or associated with phishing campaigns NSM:Flow Outbound traffic to domains/IPs not previously resolved, occurring shortly after attachment download or link click NSM:Flow NetFlow/Zeek conn.log NSM:Flow Flow records with entropy signatures resembling symmetric encryption NSM:Flow flow records NSM:Flow Source/destination IP translation inconsistent with intended policy NSM:Flow Sudden spike in incoming flows to web service ports from single/multiple IPs NSM:Flow port 5900 inbound NSM:Flow TCP port 5900 open NSM:Flow NetFlow/sFlow/PCAP NSM:Flow Outbound Network Flow NSM:Flow Device-to-Device Deployment Flows NSM:Flow Outbound traffic from suspicious new processes post-attachment execution NSM:Flow Outbound traffic to mining pools or proxies NSM:Flow Session records with TLS-like byte patterns NSM:Flow Unexpected route changes or duplicate gateway advertisements NSM:Flow Knock pattern: repeated REJ/S0 across ≥MinSequenceLen ports from same src_ip then SF success. NSM:Flow First-time egress to non-approved update hosts right after install/update NSM:Flow New outbound flows to non-approved vendor hosts post install NSM:Flow New/rare egress to non-approved update hosts after install NSM:Flow large outbound HTTPS uploads to repo domains NSM:Flow alert log NSM:Flow Outbound flow records NSM:Flow network_flow: bytes_out >> bytes_in, fixed packet sizes/intervals to non-approved CIDRs NSM:Flow session stats with bytes_out > bytes_in NSM:Flow High volumes of SYN/ACK packets with unacknowledged TCP handshakes NSM:Flow conn.log + ssl.log with Tor fingerprinting NSM:Flow Relayed session pathing (multi-hop) NSM:Flow Outbound TCP SYN or UDP to multiple ports/hosts NSM:Flow Gratuitous ARP replies with mismatched IP-MAC binding NSM:Flow Outbound UDP floods targeting common reflection services with spoofed IP headers NSM:Flow Connection Tracking NSM:Flow Flow Creation (NetFlow/sFlow) NSM:Flow conn.log, icmp.log NSM:Flow Abnormal SMB authentication attempts correlated with poisoned LLMNR/NBT-NS sessions NSM:Flow Gratuitous or duplicate DHCP OFFER packets from non-legitimate servers NSM:Flow uncommon ports NSM:Flow alternate ports NSM:Flow conn.log or flow data NSM:Flow High volume flows with incomplete TCP sessions or single-packet bursts NSM:Flow Knock pattern: multiple REJ/S0 to distinct closed ports then successful connection to service_port NSM:Flow First-time egress from host after new install to unknown update endpoints NSM:Flow First-time egress to unknown registries/mirrors immediately after install NSM:Flow New egress from app just installed to unknown update endpoints NSM:Flow Outbound connection to mining pool port (3333, 4444, 5555) NSM:Flow Outbound traffic to mining pool upon container launch NSM:Flow Flow records with RSA key exchange on unexpected port NSM:Flow Outbound connections from web server binaries (apache2, nginx, php-fpm) to unknown external IPs

NSM:Flow sustained outbound HTTPS sessions with high data volume NSM:Flow Connections from IDE hosts to marketplace/tunnel domains NSM:Flow large HTTPS outbound uploads NSM:Flow TCP port 22 traffic NSX:FlowLogs network_flow: bytes_out >> bytes_in to external PF:Logs outbound flows with bytes_out >> bytes_in PF:Logs high out:in ratio or fixed-size periodic flows PF:Logs External traffic to remote access services saas:api Webhook registrations or repeated POST activity snmp:config Configuration change traps or policy enforcement failures SNMP:DeviceLogs Unexpected NAT translation statistics or rule insertion events VPCFlowLogs:All High volume internal traffic with low entropy indicating looped or malicious DoS script vpxd.log API communication Windows Firewall Log SMB over high port wineventlog:dhcp DHCP Lease Granted WinEventLog:Microsoft-Windows-Windows Firewall With Advanced Security/Firewall EventCode=2004, 2005, 2006 WinEventLog:Security ARP cache modification attempts observed through event tracing or security baselines WLANLogs:Association Multiple APs advertising the same SSID but with different BSSID/MAC or encryption type

---