Network Connection Creation, Data Component DC0082

Archived: 2026-04-05 13:47:03 UTC

auditd:SYSCALL connect auditd:SYSCALL execve: Execs of chromium, google-chrome, firefox, libreoffice with http(s) in cmdline auditd:SYSCALL connect/sendto auditd:SYSCALL open or connect syscalls on /tmp/ssh-* or $SSH_AUTH_SOCK auditd:SYSCALL socket/connect with TLS context by unexpected process auditd:SYSCALL socket/bind: New bind() to a previously closed port shortly after the sequence. auditd:SYSCALL sendto/connect auditd:SYSCALL outbound connections auditd:SYSCALL socket/bind: Process binds to a new local port shortly after knock auditd:SYSCALL socket/connect calls showing SSH processes forwarding arbitrary ports auditd:SYSCALL openat,connect -k discovery AWS:VPCFlowLogs Outbound connection to 169.254.169.254 from EC2 workload AWS:VPCFlowLogs Large transfer volume (>20MB) from RDS IP range to external public IPs AWS:VPCFlowLogs High outbound traffic from new region resource AWS:VPCFlowLogs Outbound connections to port 22, 3389 AWS:VPCFlowLogs Traffic observed on mirror destination instance cni:netflow outbound connection to internal or external APIs ebpf:syscalls socket connect esxi:esxupdate /var/log/esxupdate.log or /var/log/vmksummary.log esxi:hostd System service interactions esxi:hostd Service initiated connections esxi:hostd Service-Based Network Connection esxi:vmkernel protocol egress esxi:vmkernel network activity esxi:vmkernel None esxi:vmkernel network session initiation with external HTTPS services linux:osquery family=AF_PACKET or protocol raw; process name not in allowlist. linux:syslog network linux:syslog postfix/smtpd linux:syslog New Wi-Fi connection established or repeated association failures linux:syslog None linux:Sysmon EventCode=3, 22 macos:endpointsecurity ES_EVENT_TYPE_NOTIFY_CONNECT macos:osquery process_events/socket_events macos:osquery execution of trusted tools interacting with external endpoints macos:osquery launchd or network_events macos:osquery process_events + launchd macos:osquery process_events, socket_events macos:osquery CONNECT: Long-lived connections from remote-control parents to external IPs/domains macos:osquery None macos:unifiedlog connection attempts macos:unifiedlog connection open macos:unifiedlog network connection events macos:unifiedlog First outbound connection from the same PID/user shortly after an inbound trigger. macos:unifiedlog network sessions initiated by remote desktop apps macos:unifiedlog Inbound connections to VNC/SSH ports macos:unifiedlog network macos:unifiedlog Outbound Traffic macos:unifiedlog None macos:unifiedlog networkd or socket macos:unifiedlog log stream network activity macos:unifiedlog Association and authentication events including failures and new SSIDs Network Traffic None networkdevice:Flow Traffic from mirrored interface to mirror target IP networkdevice:syslog Dynamic route changes NSM:Connections web domain alerts NSM:Connections New outbound connection from Safari/Chrome/Firefox/Word NSM:Connections Outbound connections from newly spawned child processes or from the browser to uncommon endpoints or on anomalous ports NSM:Firewall Outbound Connections NSM:Firewall proxy or TLS inspection logs NSM:Flow New TCP/443 or TCP/80 to domain not previously seen for the user/host NSM:Flow conn.log NSM:Flow Outbound connection to *.tunnels.api.visualstudio.com or *.devtunnels.ms NSM:Flow Connections to *.devtunnels.ms or tunnels.api.visualstudio.com NSM:Flow HTTPs connection to tunnels.api.visualstudio.com NSM:Flow Outbound or inbound TFTP file transfers of ROMMON or firmware binaries NSM:Flow connection: TCP connections to ports 139/445 to multiple hosts NSM:Flow connection: SMB connections to multiple internal hosts NSM:Flow Outbound HTTP/S initiated by newly installed interpreter process NSM:Flow outbound

connections to RMM services or to unusual destination ports NSM:Flow Multiple failed connections (conn_state=REJ/S0 or history has 'R') across distinct ports from the same src_ip followed by success to a specific port. NSM:Flow Sequence of REJ/S0 then SF success from same src_ip within TimeWindow. NSM:Flow Series of denied/closed flows to distinct ports then success to mgmt port from same src_ip within TimeWindow. NSM:Flow Outbound traffic spike through formerly blocked ports/subnets following config change NSM:Flow New egress to Internet by the same UID/host shortly after terminal exec NSM:Flow connection: Inbound connections to SSH or VPN ports NSM:Flow External access to container ports (2375, 6443) NSM:Flow remote access NSM:Flow Outbound Connections NSM:Flow connection attempts NSM:Flow High-volume or repeated SNMP GETBULK/GETNEXT queries from untrusted or external IPs NSM:Flow outbound connections from host during or immediately after image build NSM:Flow new outbound connection from browser/office lineage NSM:Flow new outbound connection from exploited lineage NSM:Flow Multiple failed connections to closed ports (history contains 'R' or conn_state in {REJ, S0}) followed by a successful handshake to a new port from same src within TimeWindowKnock NSM:Flow Closed-port hits followed by success from same src_ip NSM:Flow Port-knock pattern from one src to device unicast,broadcast,network addresses on same port within TimeWindowKnock NSM:Flow Unexpected inbound/outbound TFTP traffic for device image files NSM:Flow Unexpected or unauthorized inbound connections to SNMP, NETCONF, or RESTCONF services snmp:access GETBULK/GETNEXT requests for OIDs associated with configuration parameters WinEventLog:Microsoft-Windows-Bits-Client/Operational BITS job lifecycle events such as job create/modify/transfer/complete and URL/remote name fields WinEventLog:Microsoft-Windows-WLAN-AutoConfig EventCode=8001, 8002, 8003 WinEventLog:Security EventCode=5156, 5157 WinEventLog:Sysmon EventCode=3, 22 WinEventLog:System EventCode=8001
