Threat Hunting Cheatsheet

Quick Wins

Monero Cryptomining

KQL: `process.name: "xmr-stak" OR process.name: "xmrig"`

Lucene: `process.name:(xmr-stak OR xmrig)`

Petya, Mischa, und GoldenEye

KQL: `file.name: "*petya*" OR file.name: "*mischa*" OR file.name: "*goldeneye*"`

Lucene: `file.name:(*petya* OR *mischa* OR *goldeneye*)`

Suspicious Logins (Windows)

KQL: `event.category: "authentication" AND event.outcome: "failure"`

Lucene: `event.category:authentication AND event.outcome:failure`

Local File Inclusion (Web Application Attacks)

KQL: `http.request.body.content: "/etc/passwd"`

Lucene: `http.request.body.content:/etc/passwd`

Command Injection (Web Application Attacks)

KQL: `http.request.body.content: ";"`

Lucene: `http.request.body.content:;`

Binary Attacks (Windows)

KQL: `file.extension: "exe" AND process.args: ("-nop", "-exec")`

Lucene: `file.extension:exe AND process.args:(-nop OR -exec)`

PowerShell Logging for Phishing Attacks

KQL: `process.name: "powershell.exe" AND process.args: "DownloadString"`

Lucene: `process.name:powershell.exe AND process.args:DownloadString`

Bypassing UAC (Windows Privilege Escalation)

KQL: `event.code: "4688" AND process.args: "sdbinst.exe"`

Lucene: `event.code:4688 AND process.args:sdbinst.exe`

Persisting via Windows Service (Windows Persistence)

KQL: `event.code: "7045" OR event.code: "4697"`

Lucene: `event.code:(7045 OR 4697)`

Command Injection (Linux Server Side Attacks)

KQL: `process.args: "&&" OR process.args: ";" OR process.args: "|"`

Lucene: `process.args:(&& OR ; OR |)`

SQL Injection (Linux Server Side Attacks)

KQL: `http.request.body.content: "UNION SELECT"`

Lucene: `http.request.body.content:UNION SELECT`

Known Vulnerabilities (Network Detections)

KQL: `network.protocol: "http" AND http.response.status_code: "404"`

Lucene: `network.protocol:http AND http.response.status_code:404`

Antivirus Overview (Antivirus Alerts and Evasion)

KQL: `event.category: "antivirus" AND event.outcome: "block"`

Lucene: `event.category:antivirus AND event.outcome:block`

Brute Force Anmeldeversuche

KQL: `event.category: "authentication" AND event.outcome: "failure" AND event.duration > 5`

Lucene: `event.category:authentication AND event.outcome:failure AND event.duration:>5`

Unbekannte oder seltene User-Agents

KQL: `NOT user_agent.name: ("Chrome", "Firefox", "Safari", "Edge")`

Lucene: `NOT user_agent.name:(Chrome OR Firefox OR Safari OR Edge)`

Zugriff von unbekannten geografischen Regionen

KQL: `NOT source.geo.country_iso_code: ("US", "DE", "FR", "GB")`

Lucene: `NOT source.geo.country_iso_code:(US OR DE OR FR OR GB)`

Dateiänderungen in kritischen Verzeichnissen (z.B. /etc/)

KQL: `file.path: "/etc/*" AND event.action: "modified"`

Lucene: `file.path:/etc/* AND event.action:modified`

Ausführung von seltenen Prozessen

KQL: `NOT process.name: ("sshd", "httpd", "mysqld")`

Lucene: `NOT process.name:(sshd OR httpd OR mysqld)`

Verdächtige PowerShell-Befehle

KQL: `process.name: "powershell.exe" AND process.args: ("EncodedCommand", "Bypass", "-NoP")`

Lucene: `process.name:powershell.exe AND process.args:(EncodedCommand OR Bypass OR -NoP)`

Zugriff auf kritische Dateien

KQL: `file.name: ("passwd", "shadow", "hosts") AND event.action: "read"`

Lucene: `file.name:(passwd OR shadow OR hosts) AND event.action:read`

Verdächtige Netzwerkverbindungen zu bekannten schlechten IP-Adressen

KQL: `destination.ip: ("9.9.9.9", "8.8.8.8")`

Lucene: `destination.ip:(9.9.9.9 OR 8.8.8.8)`

Verdächtige Outbound-Verbindungen auf hohen Ports

KQL: `destination.port > 1024 AND network.direction: "outbound"`

Lucene: `destination.port:>1024 AND network.direction:outbound`

Dateierstellung in temporären Verzeichnissen

KQL: `file.path: "/tmp/*" AND event.action: "created"`

Lucene: `file.path:/tmp/* AND event.action:created`

OilRig Angriffserkennung (APT)

KQL: `process.name: "powershell.exe" AND process.args: "Invoke-WebRequest"`

Lucene: `process.name:powershell.exe AND process.args:Invoke-WebRequest`

APT3 Angriffserkennung

KQL: `file.name: "*backdoor*" OR process.name: "mimikatz.exe"`

Lucene: `file.name:*backdoor* OR process.name:mimikatz.exe`

APT28 Angriffserkennung

KQL: `network.protocol: "http" AND http.request.body.content: "*malware*"`

Lucene: `network.protocol:http AND http.request.body.content:*malware*`

Suspicious PowerShell Core Remote Access

KQL: `process.name: "pwsh.exe" AND process.args: "-Command"`

Lucene: `process.name:pwsh.exe AND process.args:-Command`

Persisting via DLL-Sideloading/Hijacking

KQL: `file.extension: "dll" AND event.action: "created"`

Lucene: `file.extension:dll AND event.action:created`

Linux Suspicious Logins

KQL: `event.category: "authentication" AND event.outcome: "failure" AND host.os.name: "Linux"`

Lucene: `event.category:authentication AND event.outcome:failure AND host.os.name:Linux`

Linux Command Injection

KQL: `process.name: "bash" AND process.args: (";", "&&")` Lucene: `process.name:bash AND process.args:(; OR &&)`

Linux SQL Injection

KQL: `http.request.body.content: "UNION SELECT" AND host.os.name: "Linux"`

Lucene: `http.request.body.content:UNION SELECT AND host.os.name:Linux`

Linux Abusing System Programs

KQL: `process.name: ("sudo", "cron") AND user.name: "root"`

Lucene: `process.name:(sudo OR cron) AND user.name:root`

Network IDS Rule Crafting

KQL: `network.protocol: "http" AND http.response.status_code: "403"`

Lucene: `network.protocol:http AND http.response.status_code:403`

Antivirus Block Events

KQL: `event.category: "antivirus" AND event.outcome: "block"`

Lucene: `event.category:antivirus AND event.outcome:block`

Active Directory (AD) Angriffe

NTLM-Relay Angriff

KQL: `(event_id:4624 OR event_id:4625) AND authentication_package:"NTLM" AND (logon_type:3 OR logon_type:10)`

Lucene: `(event_id:4624 OR event_id:4625) AND authentication_package:"NTLM" AND (logon_type:3 OR logon_type:10)`

Token Impersonation Angriff

KQL:
`(event_id:4688 OR event_id:4624) AND (new_process_name:("*\\runas.exe" OR "*\\psexec.exe" OR "*\\at.exe" OR "*\\schtasks.exe" OR "*`

Lucene:
`(event_id:4688 OR event_id:4624) AND (new_process_name:("*\\runas.exe" OR "*\\psexec.exe" OR "*\\at.exe" OR "*\\schtasks.exe" OR "*`

Kerberos Diamon Ticket Angriff

KQL:
`(event_id:4769 OR event_id:4770) AND (service_name:"krbtgt" OR service_name:"krbtgt/") AND user_name != "ANONYMOUS LOGON"`

Lucene:
`(event_id:4769 OR event_id:4770) AND (service_name:"krbtgt" OR service_name:"krbtgt/") AND NOT user_name:"ANONYMOUS LOGON"`

Kerberos Golden Ticket Angriff

KQL: `event.code: "4769" AND ticket.options: "0x40810000"`

Lucene: `event.code:4769 AND ticket.options:0x40810000`

Kerberos Silver Ticket Angriff

KQL: `event.code: "4769" AND ticket.encryption: "0x17"`

Lucene: `event.code:4769 AND ticket.encryption:0x17`

Pass-the-Hash (PtH)

KQL: `event.code: "4624" AND logon.type: "9"`

Lucene: `event.code:4624 AND logon.type:9`

Pass-the-Ticket (PtT)

KQL: `event.code: "4624" AND logon.type: "3" AND ticket.encryption: "0x12"`

Lucene: `event.code:4624 AND logon.type:3 AND ticket.encryption:0x12`

DCSync Angriff

KQL: `event.code: "4662" AND object.name: "DS-Replication-Get-Changes"`

Lucene: `event.code:4662 AND object.name:DS-Replication-Get-Changes`

DCShadow Angriff

KQL:
`(event_id:4662 OR event_id:5141 OR event_id:5142 OR event_id:5143 OR event_id:5144 OR event_id:5137 OR event_id:4660) AND (object_t`

Lucene:
`(event_id:4662 OR event_id:5141 OR event_id:5142 OR event_id:5143 OR event_id:5144 OR event_id:5137 OR event_id:4660) AND (object_t`

Gruppenmitgliedschaftsänderungen

KQL: `event.code: "4728" OR event.code: "4729"`

Lucene: `event.code:(4728 OR 4729)`

SID History Injection

KQL: `event.code: "4769" AND ticket.sids: "*S-1-5-*"`

Lucene: `event.code:4769 AND ticket.sids:*S-1-5-*`

Kerberoasting

KQL: `event.code: "4769" AND ticket.service: "krbtgt"`

Lucene: `event.code:4769 AND ticket.service:krbtgt`

AS-REP Roasting

KQL:
`(event_id:4768 OR event_id:4771) AND (user_account_control:532480 OR user_account_control:532512) AND (service_name:"krbtgt" OR ser`

Lucene:
`(event_id:4768 OR event_id:4771) AND (user_account_control:532480 OR user_account_control:532512) AND (service_name:"krbtgt" OR ser`

Overpass-the-Hash (Pass-the-Key)

KQL: `event.code: "4624" AND logon.type: "3" AND authentication.package: "Kerberos"`

Lucene: `event.code:4624 AND logon.type:3 AND authentication.package:Kerberos`

ACL (Access Control List) Manipulation

KQL: `event.code: "5136" AND object.class: "groupPolicyContainer"`

Lucene: `event.code:5136 AND object.class:groupPolicyContainer`

AdminSDHolder Object Tampering

KQL: `event.code: "5136" AND object.name: "AdminSDHolder"`

Lucene: `event.code:5136 AND object.name:AdminSDHolder`

Skeleton Key Injection

KQL: `event.code: "4624" AND logon.type: "9" AND process.name: "mimikatz.exe"`

Lucene: `event.code:4624 AND logon.type:9 AND process.name:mimikatz.exe`

RID (Relative ID) Hijacking

KQL: `event.code: "4724" AND user.id: "500" OR user.id: "512" OR user.id: "514"`

Lucene: `event.code:4724 AND (user.id:500 OR user.id:512 OR user.id:514)`

NTDS.dit Extraction

KQL: `file.name: "ntds.dit" AND event.action: "read"`

Lucene: `file.name:ntds.dit AND event.action:read`

Group Policy Preference (GPP) Passwords

KQL: `file.path: "\\SYSVOL\\*\\Policies\\*" AND file.name: "*.xml"`

Lucene: `file.path:\\SYSVOL\\*\\Policies\\* AND file.name:*.xml`

SPN Scanning (Service Principal Name)

KQL: `network.protocol: "ldap" AND ldap.request: "searchRequest" AND ldap.filter: "servicePrincipalName=*"`

Lucene: `network.protocol:ldap AND ldap.request:searchRequest AND ldap.filter:servicePrincipalName=*`

Token Manipulation und Privilege Escalation

KQL: `event.code: "4672" AND NOT user.name: "Administrator"`

Lucene: `event.code:4672 AND NOT user.name:Administrator`

Suspicious Service Creation

KQL: `event.code: "7045" AND service.name: "*mimikatz*"`

Lucene: `event.code:7045 AND service.name:*mimikatz*`

Suspicious Scheduled Task Creation

KQL: `event.code: "4698" AND task.name: "*powershell*"`

Lucene: `event.code:4698 AND task.name:*powershell*`

Lateral Movement via WMI (Windows Management Instrumentation)

KQL: `network.protocol: "dcerpc" AND process.name: "wmiprvse.exe"`

Lucene: `network.protocol:dcerpc AND process.name:wmiprvse.exe`

Lateral Movement via Remote Desktop (RDP)

KQL: `event.code: "4624" AND logon.type: "10"`

Lucene: `event.code:4624 AND logon.type:10`

Suspicious Active Directory Replication

KQL: `event.code: "4662" AND object.name: "DS-Replication-Get-Changes-All"`

Lucene: `event.code:4662 AND object.name:DS-Replication-Get-Changes-All`

Suspicious Directory Service Access

KQL: `event.code: "4662" AND object.name: "user"`

Lucene: `event.code:4662 AND object.name:user`

Clear Text Passwords in Group Policy Preferences

KQL: `file.path: "\\SYSVOL\\*\\Policies\\*" AND file.name: "Groups.xml"`

Lucene: `file.path:\\SYSVOL\\*\\Policies\\* AND file.name:Groups.xml`

Suspicious DNS Queries (e.g., DGA patterns)

KQL: `event.category: "dns" AND dns.question.name: "*aaaabbbbcccc*"`

Lucene: `event.category:dns AND dns.question.name:*aaaabbbbcccc*`

Unusual Hours of Activity (e.g., nighttime logins)

KQL: `event.code: "4624" AND NOT @timestamp: ["08:00:00" TO "18:00:00"]`

Lucene: `event.code:4624 AND NOT @timestamp:["08:00:00" TO "18:00:00"]`

LDAP Angriffe

LDAP Anonymous Bind

KQL: `event.category: "authentication" AND user.name: "ANONYMOUS LOGON" AND network.protocol: "ldap"`

Lucene: `event.category:authentication AND user.name:"ANONYMOUS LOGON" AND network.protocol:ldap`

LDAP Brute Force

KQL: `event.category: "authentication" AND event.outcome: "failure" AND network.protocol: "ldap"`

Lucene: `event.category:authentication AND event.outcome:failure AND network.protocol:ldap`

LDAP Reconnaissance

KQL: `network.protocol: "ldap" AND (ldap.request: "searchRequest" OR ldap.request: "bindRequest")`

Lucene: `network.protocol:ldap AND (ldap.request:searchRequest OR ldap.request:bindRequest)`

LDAP Clear-Text Passwörter

KQL: `network.protocol: "ldap" AND ldap.attribute: "userPassword"`

Lucene: `network.protocol:ldap AND ldap.attribute:userPassword`

Windows Endpoint Angriffe

Suspicious Parent-Child Process Relationship (z.B. cmd.exe spawning powershell.exe)

KQL: `process.parent.name: "cmd.exe" AND process.name: "powershell.exe"`

Lucene: `process.parent.name:cmd.exe AND process.name:powershell.exe`

Suspicious File Extensions (z.B. ausführbare Dateien aus dem Temp-Verzeichnis)

KQL: `file.path: "C:\\Windows\\Temp\\*.exe"`

Lucene: `file.path:C:\\Windows\\Temp\\*.exe`

Mimikatz Execution Detection

KQL: `process.name: "mimikatz.exe"`

Lucene: `process.name:mimikatz.exe`

Rubeus Execution Detection

KQL: `process.name: "Rubeus.exe"`

Lucene: `process.name:Rubeus.exe`

Suspicious PowerShell Encoded Commands

KQL: `process.name: "powershell.exe" AND process.args: "-EncodedCommand"`

Lucene: `process.name:powershell.exe AND process.args:-EncodedCommand`

Remote Code Execution via WMIC

KQL: `process.name: "wmic.exe" AND process.args: "/NODE:"`

Lucene: `process.name:wmic.exe AND process.args:/NODE:`

Suspicious Use of net.exe (z.B. adding users)

KQL: `process.name: "net.exe" AND process.args: "user" AND process.args: "add"`

Lucene: `process.name:net.exe AND process.args:user AND process.args:add`

Suspicious Registry Modifications (z.B. Run Keys for Persistence)

KQL: `registry.path: "HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\*"`

Lucene: `registry.path:HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\*`

Suspicious Use of Bitsadmin (often used for downloading payloads)

KQL: `process.name: "bitsadmin.exe"`

Lucene: `process.name:bitsadmin.exe`

Suspicious Use of Certutil (often used for downloading payloads)

KQL: `process.name: "certutil.exe"`

Lucene: `process.name:certutil.exe`

Suspicious Network Connections to Uncommon Ports

KQL: `network.protocol: "tcp" AND NOT destination.port: (80, 443, 25, 53)`

Lucene: `network.protocol:tcp AND NOT destination.port:(80 OR 443 OR 25 OR 53)`

Suspicious Execution from Recycle Bin (often used to evade detection)

KQL: `file.path: "C:\\$Recycle.Bin\\*.exe"`

Lucene: `file.path:C:\\$Recycle.Bin\\*.exe`

Powershell Angriffe

Suspicious PowerShell Download Methods

KQL:
`process.name: "powershell.exe" AND (process.args: "DownloadFile" OR process.args: "Invoke-WebRequest" OR process.args: "Invoke-Rest`

Lucene:
`process.name:powershell.exe AND (process.args:DownloadFile OR process.args:Invoke-WebRequest OR process.args:Invoke-RestMethod)`

PowerShell Base64 Encoded Commands

KQL: `process.name: "powershell.exe" AND process.args: "-EncodedCommand"`

Lucene: `process.name:powershell.exe AND process.args:-EncodedCommand`

PowerShell Running with NoProfile Argument (often used to evade profile-based logging)

KQL: `process.name: "powershell.exe" AND process.args: "-NoProfile"`

Lucene: `process.name:powershell.exe AND process.args:-NoProfile`

PowerShell Direct Memory Access via Add-Type

KQL: `process.name: "powershell.exe" AND process.args: "Add-Type"`

Lucene: `process.name:powershell.exe AND process.args:Add-Type`

Suspicious Use of Get-Credential Cmdlet (possible credential harvesting)

KQL: `process.name: "powershell.exe" AND process.args: "Get-Credential"`

Lucene: `process.name:powershell.exe AND process.args:Get-Credential`

PowerShell Script Execution with Bypass Policy

KQL: `process.name: "powershell.exe" AND process.args: "-ExecutionPolicy Bypass"`

Lucene: `process.name:powershell.exe AND process.args:"-ExecutionPolicy Bypass"`

PowerShell Accessing Windows API

KQL: `process.name: "powershell.exe" AND process.args: "[DllImport"`

Lucene: `process.name:powershell.exe AND process.args:[DllImport`

PowerShell Reflective DLL Injection

KQL: `process.name: "powershell.exe" AND process.args: "System.Reflection.AssemblyName"`

Lucene: `process.name:powershell.exe AND process.args:System.Reflection.AssemblyName`

PowerShell Remote Command Execution

KQL: `process.name: "powershell.exe" AND process.args: "-Command" AND process.args: "New-PSSession"`

Lucene: `process.name:powershell.exe AND process.args:-Command AND process.args:New-PSSession`

Suspicious PowerShell User Agents (often used in web requests)

KQL: `user_agent.original: "Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell"`

Lucene: `user_agent.original:"Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell"`

CMD Angriffe

Suspicious net.exe Usage (z.B. User hinzufügen)

KQL: `process.name: "net.exe" AND process.args: "user" AND process.args: "add"`

Lucene: `process.name:net.exe AND process.args:user AND process.args:add`

Suspicious Execution of whoami (zum Abrufen des aktuellen Benutzers)

KQL: `process.name: "whoami.exe"`

Lucene: `process.name:whoami.exe`

Suspicious Execution of ipconfig (zum Abrufen von Netzwerkinformationen)

KQL: `process.name: "ipconfig.exe"`

Lucene: `process.name:ipconfig.exe`

Suspicious Execution of tasklist or taskkill

KQL: `process.name: "tasklist.exe" OR process.name: "taskkill.exe"`

Lucene: `process.name:tasklist.exe OR process.name:taskkill.exe`

Suspicious Use of netstat (zum Überprüfen von Netzwerkverbindungen)

KQL: `process.name: "netstat.exe"`

Lucene: `process.name:netstat.exe`

Suspicious Use of systeminfo (zum Abrufen von Systeminformationen)

KQL: `process.name: "systeminfo.exe"`

Lucene: `process.name:systeminfo.exe`

Suspicious Use of nslookup or ping (zum Auflösen von Domänen oder IP-Adressen)

KQL: `process.name: "nslookup.exe" OR process.name: "ping.exe"`

Lucene: `process.name:nslookup.exe OR process.name:ping.exe`

Suspicious Batch File Execution

KQL: `file.extension: "bat" AND event.action: "execution"`

Lucene: `file.extension:bat AND event.action:execution`

Suspicious Use of cacls or icacls (zum Ändern von Dateiberechtigungen)

KQL: `process.name: "cacls.exe" OR process.name: "icacls.exe"`

Lucene: `process.name:cacls.exe OR process.name:icacls.exe`

Suspicious Use of reg.exe (zum Ändern der Registrierung)

KQL: `process.name: "reg.exe" AND (process.args: "add" OR process.args: "delete")`

Lucene: `process.name:reg.exe AND (process.args:add OR process.args:delete)`

VBScript Angriffe

Suspicious Execution of VBScript Files

KQL: `file.extension: "vbs" AND event.action: "execution"`

Lucene: `file.extension:vbs AND event.action:execution`

Suspicious Use of WScript or CScript (Standard VBScript Interpreter)

KQL: `process.name: "wscript.exe" OR process.name: "cscript.exe"`

Lucene: `process.name:wscript.exe OR process.name:cscript.exe`

Suspicious Network Activity from VBScript

KQL: `process.name: "wscript.exe" OR process.name: "cscript.exe" AND network.protocol: "http"`

Lucene: `process.name:(wscript.exe OR cscript.exe) AND network.protocol:http`

VBScript Accessing Shell.Application (often used for command execution)

KQL: `file.extension: "vbs" AND file.content: "CreateObject(\"WScript.Shell\")"`

Lucene: `file.extension:vbs AND file.content:CreateObject("WScript.Shell")`

VBScript Accessing ADODB.Stream (often used for writing files)

KQL: `file.extension: "vbs" AND file.content: "CreateObject(\"ADODB.Stream\")"`

Lucene: `file.extension:vbs AND file.content:CreateObject("ADODB.Stream")`

VBScript with Base64 Encoded Content (possible obfuscation)

KQL: `file.extension: "vbs" AND file.content: "base64"`

Lucene: `file.extension:vbs AND file.content:base64`

Suspicious Use of GetObject (possible COM object abuse)

KQL: `file.extension: "vbs" AND file.content: "GetObject"`

Lucene: `file.extension:vbs AND file.content:GetObject`

VBScript Accessing MSXML2.ServerXMLHTTP (often used for HTTP requests)

KQL: `file.extension: "vbs" AND file.content: "CreateObject(\"MSXML2.ServerXMLHTTP\")"`

Lucene: `file.extension:vbs AND file.content:CreateObject("MSXML2.ServerXMLHTTP")`

VBScript Accessing Scripting.FileSystemObject (file operations)

KQL: `file.extension: "vbs" AND file.content: "CreateObject(\"Scripting.FileSystemObject\")"`

Lucene: `file.extension:vbs AND file.content:CreateObject("Scripting.FileSystemObject")`

VBScript with Suspicious Keywords (e.g., Execute, Eval)

KQL: `file.extension: "vbs" AND (file.content: "Execute(" OR file.content: "Eval(")`

Lucene: `file.extension:vbs AND (file.content:Execute( OR file.content:Eval()`

SYSMON Events

Prozesserstellung (Event ID 1)

KQL: `event.code: "1" AND process.name: "suspicious.exe"`

Lucene: `event.code:1 AND process.name:suspicious.exe`

Dateizeitänderung (Event ID 2)

KQL: `event.code: "2" AND file.name: "suspicious.dll"`

Lucene: `event.code:2 AND file.name:suspicious.dll`

Netzwerkverbindung erkannt (Event ID 3)

KQL: `event.code: "3" AND destination.ip: "8.8.8.8"`

Lucene: `event.code:3 AND destination.ip:8.8.8.8`

Sysmon-Service-Status (Event ID 4)

KQL: `event.code: "4" AND event.action: "stopped"`

Lucene: `event.code:4 AND event.action:stopped`

Prozess beendet (Event ID 5)

KQL: `event.code: "5" AND process.name: "malware.exe"`

Lucene: `event.code:5 AND process.name:malware.exe`

Treiber geladen (Event ID 6)

KQL: `event.code: "6" AND driver.name: "suspiciousdriver.sys"`

Lucene: `event.code:6 AND driver.name:suspiciousdriver.sys`

Bild geladen (Event ID 7)

KQL: `event.code: "7" AND file.name: "suspicious.dll"`

Lucene: `event.code:7 AND file.name:suspicious.dll`

RemoteThread erstellt (Event ID 8)

KQL: `event.code: "8" AND process.name: "exploit.exe"`

Lucene: `event.code:8 AND process.name:exploit.exe`

RawAccessRead (Event ID 9)

KQL: `event.code: "9" AND file.name: "ntds.dit"`

Lucene: `event.code:9 AND file.name:ntds.dit`

Prozesszugriff (Event ID 10)

KQL: `event.code: "10" AND source.process.name: "hacker_tool.exe"`

Lucene: `event.code:10 AND source.process.name:hacker_tool.exe`

Windows Crendetial Abuse Angriffe

Mimikatz Execution Detection

KQL: `process.name: "mimikatz.exe"`

Lucene: `process.name:mimikatz.exe`

Suspicious Use of Windows Credential Dumping Tools

KQL: `process.name: ("lsass.exe" OR "procdump.exe" OR "pwdump.exe")`

Lucene: `process.name:(lsass.exe OR procdump.exe OR pwdump.exe)`

Suspicious Access to SAM Registry Hive

KQL: `registry.path: "HKLM\\SAM\\SAM\\Domains\\Account\\Users\\*" AND event.action: "value_set"`

Lucene: `registry.path:HKLM\\SAM\\SAM\\Domains\\Account\\Users\\* AND event.action:value_set`

Suspicious Access to SECURITY Registry Hive

KQL: `registry.path: "HKLM\\SECURITY\\Policy\\Secrets\\*" AND event.action: "key_read"`

Lucene: `registry.path:HKLM\\SECURITY\\Policy\\Secrets\\* AND event.action:key_read`

Suspicious Use of Windows Credential UI (possible phishing)

KQL: `process.name: "CredentialUIBroker.exe"`

Lucene: `process.name:CredentialUIBroker.exe`

Suspicious Dumping of LSASS Memory

KQL: `process.name: "rundll32.exe" AND process.args: "comsvcs.dll, MiniDump"`

Lucene: `process.name:rundll32.exe AND process.args:comsvcs.dll, MiniDump`

Suspicious Use of Windows VaultCmd (reading stored credentials)

KQL: `process.name: "vaultcmd.exe" AND process.args: "/list"`

Lucene: `process.name:vaultcmd.exe AND process.args:/list`

Suspicious Use of Windows Key Export (possible private key extraction)

KQL: `process.name: "certutil.exe" AND process.args: "-exportpfx"`

Lucene: `process.name:certutil.exe AND process.args:-exportpfx`

Suspicious Use of Windows DPAPI (Data Protection API)

KQL: `process.name: "powershell.exe" AND process.args: "Unprotect-CmsMessage"`

Lucene: `process.name:powershell.exe AND process.args:Unprotect-CmsMessage`

Suspicious Access to Cached Credentials

KQL: `file.path: "C:\\Windows\\System32\\config\\systemprofile\\AppData\\Local\\Microsoft\\Credentials\\*"`

Lucene: `file.path:C:\\Windows\\System32\\config\\systemprofile\\AppData\\Local\\Microsoft\\Credentials\\*`

Windows Brute Force Login-Angriffe

Mehrere fehlgeschlagene Anmeldeversuche (Event ID 4625)

KQL: `event.code: "4625" AND logon.type: "3"`

Lucene: `event.code:4625 AND logon.type:3`

Mehrere erfolgreiche Anmeldeversuche in kurzer Zeit (Event ID 4624)

KQL: `event.code: "4624" AND logon.type: "3"`

Lucene: `event.code:4624 AND logon.type:3`

Mehrere RDP-Anmeldeversuche (Event ID 4624 und Logon Type 10)

KQL: `event.code: "4624" AND logon.type: "10"`

Lucene: `event.code:4624 AND logon.type:10`

Mehrere Anmeldeversuche über NTLM (Event ID 4624 und Logon Process "NtLmSsp")

KQL: `event.code: "4624" AND logon.process.name: "NtLmSsp"`

Lucene: `event.code:4624 AND logon.process.name:NtLmSsp`

Mehrere Anmeldeversuche von einer einzigen IP-Adresse

KQL: `event.code: "4625" AND source.ip: "192.168.1.10"`

Lucene: `event.code:4625 AND source.ip:192.168.1.10`

Mehrere Anmeldeversuche für einen einzigen Benutzernamen

KQL: `event.code: "4625" AND user.name: "admin"`

Lucene: `event.code:4625 AND user.name:admin`

Mehrere Anmeldeversuche mit unterschiedlichen Benutzernamen von derselben IP

KQL: `event.code: "4625" AND source.ip: "192.168.1.10"`

Lucene: `event.code:4625 AND source.ip:192.168.1.10`

Mehrere Anmeldeversuche über SMB (Event ID 4624 und Logon Type 3)

KQL: `event.code: "4624" AND logon.type: "3" AND network.protocol: "smb"`

Lucene: `event.code:4624 AND logon.type:3 AND network.protocol:smb`

Mehrere Anmeldeversuche in kurzer Zeit (z.B. innerhalb von 5 Minuten)

KQL: `event.code: "4625" AND date.range: "now-5m/m"`

Lucene: `event.code:4625 AND date:[now-5m TO now]`

Mehrere erfolgreiche und fehlgeschlagene Anmeldeversuche in kurzer Zeit

KQL: `(event.code: "4624" OR event.code: "4625") AND date.range: "now-10m/m"`

Lucene: `(event.code:4624 OR event.code:4625) AND date:[now-10m TO now]`

Windows Internet Information Services (IIS) Angriffe

SQL-Injection-Angriffsversuche in IIS-Logs

KQL: `source: "iis" AND url: "*' OR 1=1--*"`

Lucene: `source:iis AND url:*' OR 1=1--*`

Cross-Site-Scripting (XSS) Angriffsversuche in IIS-Logs

KQL: `source: "iis" AND (url: "<script>" OR url: "%3Cscript%3E")`

Lucene: `source:iis AND (url:<script> OR url:%3Cscript%3E)`

Verdächtige User-Agents (z.B. Scanning-Tools)

KQL: `source: "iis" AND user_agent: "sqlmap"`

Lucene: `source:iis AND user_agent:sqlmap`

Zugriffsversuche auf administrative Pfade

KQL: `source: "iis" AND url: "/admin*"`

Lucene: `source:iis AND url:/admin*`

Zugriffsversuche auf nicht vorhandene Ressourcen (Error 404)

KQL: `source: "iis" AND http.response.status_code: "404"`

Lucene: `source:iis AND http.response.status_code:404`

Verdächtige HTTP-Methoden (z.B. PUT, DELETE)

KQL: `source: "iis" AND http.request.method: ("PUT" OR "DELETE")`

Lucene: `source:iis AND http.request.method:(PUT OR DELETE)`

Zugriffsversuche auf bekannte IIS-Schwachstellen

KQL: `source: "iis" AND url: "/vulnpath*"`

Lucene: `source:iis AND url:/vulnpath*`

Verdächtige Anfrageraten (z.B. für DDoS oder Brute-Force)

KQL: `source: "iis" AND event.rate: ">100"`

Lucene: `source:iis AND event.rate:>100`

Zugriffsversuche von verdächtigen IP-Adressen

KQL: `source: "iis" AND source.ip: "10.0.0.1"`

Lucene: `source:iis AND source.ip:10.0.0.1`

Zugriffsversuche auf Backup- oder Temp-Dateien

KQL: `source: "iis" AND (url: "*.bak" OR url: "*.tmp")`

Lucene: `source:iis AND (url:*.bak OR url:*.tmp)`

Windows Binary Attacks

Ausführung von selten verwendeten ausführbaren Dateien

KQL: `process.extension: "exe" AND NOT process.name: ("winword.exe", "explorer.exe", "chrome.exe")`

Lucene: `process.extension:exe AND NOT process.name:(winword.exe OR explorer.exe OR chrome.exe)`

Ausführung von Binärdateien aus temporären Verzeichnissen

KQL: `process.path: "C:\\Windows\\Temp\\*.exe" OR process.path: "C:\\Users\\*\\AppData\\Local\\Temp\\*.exe"`

Lucene: `process.path:C:\\Windows\\Temp\\*.exe OR process.path:C:\\Users\\*\\AppData\\Local\\Temp\\*.exe`

Ausführung von Binärdateien mit verdächtigen Argumenten (z.B. mimikatz Befehle)

KQL: `process.args: "sekurlsa::logonpasswords" OR process.args: "privilege::debug"`

Lucene: `process.args:sekurlsa::logonpasswords OR process.args:privilege::debug`

Ausführung von Binärdateien mit doppelten Dateierweiterungen (z.B. notepad.exe.doc.exe)

KQL: `file.name: "*.exe.*.exe"`

Lucene: `file.name:*.exe.*.exe`

Ausführung von Binärdateien, die als Dokumente getarnt sind (z.B. document.pdf.exe)

KQL: `file.name: "*.pdf.exe" OR file.name: "*.docx.exe"`

Lucene: `file.name:*.pdf.exe OR file.name:*.docx.exe`

Ausführung von Binärdateien aus dem Download-Verzeichnis

KQL: `process.path: "C:\\Users\\*\\Downloads\\*.exe"`

Lucene: `process.path:C:\\Users\\*\\Downloads\\*.exe`

Ausführung von Binärdateien mit Base64-kodierten Argumenten (mögliche Verschleierung)

KQL: `process.args: "/base64" OR process.args: "-base64"`

Lucene: `process.args:/base64 OR process.args:-base64`

Ausführung von Binärdateien mit verdächtigen Netzwerkverbindungen

KQL: `process.name: "suspicious_binary.exe" AND network.connection: "*"`

Lucene: `process.name:suspicious_binary.exe AND network.connection:*`

Ausführung von Binärdateien, die kürzlich geändert wurden

KQL: `file.name: "*.exe" AND file.mtime: "now-1d/d"`

Lucene: `file.name:*.exe AND file.mtime:[now-1d TO now]`

Ausführung von Binärdateien mit bekannten Malware-Hashes

KQL: `file.hash.md5: "known_malware_hash"`

Lucene: `file.hash.md5:known_malware_hash`

Windows Defender Exploit Guard (WDEG)

Erkennung von Exploit-Schutzverletzungen

KQL: `event.provider: "Microsoft-Windows-Security-Mitigations" AND event.code: "1"`

Lucene: `event.provider:Microsoft-Windows-Security-Mitigations AND event.code:1`

Erkennung von ASR-Regelverletzungen (Attack Surface Reduction)

KQL: `event.provider: "Microsoft-Windows-Security-Mitigations" AND event.code: "1122"`

Lucene: `event.provider:Microsoft-Windows-Security-Mitigations AND event.code:1122`

Verdächtige Aktivitäten im Zusammenhang mit Controlled Folder Access

KQL: `event.provider: "Microsoft-Windows-Security-Mitigations" AND event.code: "1124"`

Lucene: `event.provider:Microsoft-Windows-Security-Mitigations AND event.code:1124`

Verdächtige Aktivitäten im Zusammenhang mit Network Protection

KQL: `event.provider: "Microsoft-Windows-Security-Mitigations" AND event.code: "1125"`

Lucene: `event.provider:Microsoft-Windows-Security-Mitigations AND event.code:1125`

Verdächtige Aktivitäten im Zusammenhang mit Exploit Protection

KQL: `event.provider: "Microsoft-Windows-Security-Mitigations" AND event.code: "500"`

Lucene: `event.provider:Microsoft-Windows-Security-Mitigations AND event.code:500`

Verdächtige Änderungen der WDEG-Konfiguration

KQL: `event.provider: "Microsoft-Windows-Security-Mitigations" AND event.code: "1127"`

Lucene: `event.provider:Microsoft-Windows-Security-Mitigations AND event.code:1127`

Verdächtige Aktivitäten im Zusammenhang mit Exploit Protection Policy

KQL: `event.provider: "Microsoft-Windows-Security-Mitigations" AND event.code: "1128"`

Lucene: `event.provider:Microsoft-Windows-Security-Mitigations AND event.code:1128`

Verdächtige Aktivitäten im Zusammenhang mit Exploit Protection Rule

KQL: `event.provider: "Microsoft-Windows-Security-Mitigations" AND event.code: "1129"`

Lucene: `event.provider:Microsoft-Windows-Security-Mitigations AND event.code:1129`

Verdächtige Aktivitäten im Zusammenhang mit Exploit Protection Setting

KQL: `event.provider: "Microsoft-Windows-Security-Mitigations" AND event.code: "1130"`

Lucene: `event.provider:Microsoft-Windows-Security-Mitigations AND event.code:1130`

Verdächtige Aktivitäten im Zusammenhang mit Exploit Protection Audit

KQL: `event.provider: "Microsoft-Windows-Security-Mitigations" AND event.code: "1131"`

Lucene: `event.provider:Microsoft-Windows-Security-Mitigations AND event.code:1131`

Microsoft Office Angriffe

Ausführung von Office-Anwendungen mit Makros

KQL: `process.name: ("winword.exe", "excel.exe", "powerpnt.exe") AND process.args: "/m*"`

Lucene: `process.name:(winword.exe OR excel.exe OR powerpnt.exe) AND process.args:/m*`

Erstellung von Prozessen durch Office-Anwendungen (möglicher Indikator für Makro-Ausführung)

KQL: `parent.process.name: ("winword.exe", "excel.exe", "powerpnt.exe")`

Lucene: `parent.process.name:(winword.exe OR excel.exe OR powerpnt.exe)`

Zugriff auf verdächtige Dateipfade durch Office-Anwendungen

KQL: `process.name: ("winword.exe", "excel.exe", "powerpnt.exe") AND file.path: "C:\\Windows\\Temp\\*"`

Lucene: `process.name:(winword.exe OR excel.exe OR powerpnt.exe) AND file.path:C:\\Windows\\Temp\\*`

Office-Anwendungen, die PowerShell ausführen

KQL: `parent.process.name: ("winword.exe", "excel.exe", "powerpnt.exe") AND process.name: "powershell.exe"`

Lucene: `parent.process.name:(winword.exe OR excel.exe OR powerpnt.exe) AND process.name:powershell.exe`

Office-Anwendungen, die CMD ausführen

KQL: `parent.process.name: ("winword.exe", "excel.exe", "powerpnt.exe") AND process.name: "cmd.exe"`

Lucene: `parent.process.name:(winword.exe OR excel.exe OR powerpnt.exe) AND process.name:cmd.exe`

Office-Anwendungen, die Netzwerkverbindungen herstellen

KQL: `process.name: ("winword.exe", "excel.exe", "powerpnt.exe") AND network.connection: "*"`

Lucene: `process.name:(winword.exe OR excel.exe OR powerpnt.exe) AND network.connection:*`

Verdächtige Makro-Dateierweiterungen

KQL: `file.extension: ("docm", "xlsm", "pptm")`

Lucene: `file.extension:(docm OR xlsm OR pptm)`

Office-Anwendungen, die CMD ausführen

KQL: `parent.process.name: ("winword.exe", "excel.exe", "powerpnt.exe") AND process.name: "cmd.exe"`

Lucene: `parent.process.name:(winword.exe OR excel.exe OR powerpnt.exe) AND process.name:cmd.exe`

Zugriff auf verdächtige Registry-Schlüssel durch Office-Anwendungen

KQL:
`process.name: ("winword.exe", "excel.exe", "powerpnt.exe") AND registry.path: "HKCU\\Software\\Microsoft\\Office\\*\\Security\\*"`

Lucene:
`process.name:(winword.exe OR excel.exe OR powerpnt.exe) AND registry.path:HKCU\\Software\\Microsoft\\Office\\*\\Security\\*`

Office-Anwendungen, die verdächtige DLLs laden

KQL: `process.name: ("winword.exe", "excel.exe", "powerpnt.exe") AND dll.name: "suspicious.dll"`

Lucene: `process.name:(winword.exe OR excel.exe OR powerpnt.exe) AND dll.name:suspicious.dll`

Office-Anwendungen, die Skript-Interpreter ausführen (z.B. wscript, cscript)

KQL: `parent.process.name: ("winword.exe", "excel.exe", "powerpnt.exe") AND process.name: ("wscript.exe", "cscript.exe")`

Lucene: `parent.process.name:(winword.exe OR excel.exe OR powerpnt.exe) AND process.name:(wscript.exe OR cscript.exe)`

Angriffe mittels Obfuscating/Deobfuscating Commands

PowerShell-Befehle mit Base64-Codierung

KQL: `process.name: "powershell.exe" AND process.args: "-encodedcommand*"`

Lucene: `process.name:powershell.exe AND process.args:-encodedcommand*`

PowerShell-Befehle mit langen Argumenten (mögliche Obfuskierung)

KQL: `process.name: "powershell.exe" AND LENGTH(process.args) > 200`

Lucene: `process.name:powershell.exe AND process.args:[200 TO *]`

CMD-Befehle mit ^-Zeichen (mögliche Obfuskierung)

KQL: `process.name: "cmd.exe" AND process.args: "*^*"`

Lucene: `process.name:cmd.exe AND process.args:*^*`

PowerShell-Befehle mit -replace-Operator (mögliche Deobfuskierung)

KQL: `process.name: "powershell.exe" AND process.args: "-replace*"`

Lucene: `process.name:powershell.exe AND process.args:-replace*`

PowerShell-Befehle mit [char]-Casting (mögliche Obfuskierung)

KQL: `process.name: "powershell.exe" AND process.args: "[char]*"`

Lucene: `process.name:powershell.exe AND process.args:[char]*`

PowerShell-Befehle mit IEX (Invoke-Expression)

KQL: `process.name: "powershell.exe" AND (process.args: "iex" OR process.args: "Invoke-Expression")`

Lucene: `process.name:powershell.exe AND (process.args:iex OR process.args:Invoke-Expression)`

PowerShell-Befehle mit ToString-Methode (mögliche Deobfuskierung)

KQL: `process.name: "powershell.exe" AND process.args: "ToString()*"`

Lucene: `process.name:powershell.exe AND process.args:ToString()*`

PowerShell-Befehle mit FromBase64String-Methode

KQL: `process.name: "powershell.exe" AND process.args: "FromBase64String"*`

Lucene: `process.name:powershell.exe AND process.args:FromBase64String*`

PowerShell-Befehle mit verdächtigen -split-Operationen

KQL: `process.name: "powershell.exe" AND process.args: "-split"*`

Lucene: `process.name:powershell.exe AND process.args:-split*`

PowerShell-Befehle mit -join-Operationen

KQL: `process.name: "powershell.exe" AND process.args: "-join"*`

Lucene: `process.name:powershell.exe AND process.args:-join*`

Windows Privilege Escalation

Unerwartete Prozesse, die mit hohen Berechtigungen laufen

KQL: `process.integrity_level: "system" AND NOT process.name: ("services.exe", "lsass.exe", "winlogon.exe")`

Lucene: `process.integrity_level:system AND NOT process.name:(services.exe OR lsass.exe OR winlogon.exe)`

Zugriff auf SAM-Datei (enthält lokale Benutzerkonten)

KQL: `file.path: "C:\\Windows\\System32\\config\\SAM" AND event.action: "read"`

Lucene: `file.path:C:\\Windows\\System32\\config\\SAM AND event.action:read`

Zugriff auf SECURITY-Datei (enthält Sicherheitsinformationen)

KQL: `file.path: "C:\\Windows\\System32\\config\\SECURITY" AND event.action: "read"`

Lucene: `file.path:C:\\Windows\\System32\\config\\SECURITY AND event.action:read`

Verwendung von whoami /priv (zeigt Privilegien des aktuellen Benutzers an)

KQL: `process.name: "whoami.exe" AND process.args: "/priv"`

Lucene: `process.name:whoami.exe AND process.args:/priv`

Ausführung von mimikatz oder ähnlichen Tools

KQL: `process.name: "mimikatz.exe"`

Lucene: `process.name:mimikatz.exe`

Zugriff auf den Speicher von lsass.exe (möglicher Credential Dumping-Versuch)

KQL: `process.name: "lsass.exe" AND event.action: "process_access"`

Lucene: `process.name:lsass.exe AND event.action:process_access`

Verwendung von Windows-Ereigniscode 4672 (Spezielle Berechtigungen zugewiesen)

KQL: `event.code: "4672"`

Lucene: `event.code:4672`

Verwendung von Windows-Ereigniscode 4688 (Ein neuer Prozess wurde erstellt) mit hohen Berechtigungen

KQL: `event.code: "4688" AND process.integrity_level: "system"`

Lucene: `event.code:4688 AND process.integrity_level:system`

Zugriff auf secretsdump.py (Tool zum Dumpen von Passwörtern)

KQL: `file.name: "secretsdump.py" AND event.action: "read"`

Lucene: `file.name:secretsdump.py AND event.action:read`

Ausführung von bypassuac (Tool zur Umgehung der Benutzerkontensteuerung)

KQL: `process.name: "bypassuac.exe"`

Lucene: `process.name:bypassuac.exe`

Windows Persistence

Erstellung/Aktualisierung von geplanten Aufgaben

KQL: `event.provider: "Microsoft-Windows-TaskScheduler" AND (event.action: "created" OR event.action: "updated")`

Lucene: `event.provider:Microsoft-Windows-TaskScheduler AND (event.action:created OR event.action:updated)`

Zugriff auf den Run-Registry-Schlüssel (zur automatischen Ausführung von Programmen beim Start)

KQL: `registry.path: "HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run*"`

Lucene: `registry.path:HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run*`

Zugriff auf den Startup-Ordner

KQL: `file.path: "C:\\Users\\*\\AppData\\Roaming\\Microsoft\\Windows\\Start Menu\\Programs\\Startup\\*"`

Lucene: `file.path:C:\\Users\\*\\AppData\\Roaming\\Microsoft\\Windows\\Start Menu\\Programs\\Startup\\*`

Erstellung von WMI-Event-Consumern (zur Ausführung von Befehlen bei bestimmten Ereignissen)

KQL: `event.provider: "Microsoft-Windows-WMI-Activity" AND event.action: "consumer created"`

Lucene: `event.provider:Microsoft-Windows-WMI-Activity AND event.action:consumer created`

Zugriff auf den LSA-Secrets-Registry-Schlüssel (zum Speichern von Anmeldeinformationen)

KQL: `registry.path: "HKLM\\Security\\Policy\\Secrets\\*"`

Lucene: `registry.path:HKLM\\Security\\Policy\\Secrets\\*`

Zugriff auf BITS-Jobs (Background Intelligent Transfer Service)

KQL: `event.provider: "Microsoft-Windows-Bits-Client" AND event.action: "job created"`

Lucene: `event.provider:Microsoft-Windows-Bits-Client AND event.action:job created`

Zugriff auf COM-Objekte zur Persistenz

KQL: `registry.path: "HKLM\\SOFTWARE\\Classes\\CLSID\\*" OR registry.path: "HKCU\\SOFTWARE\\Classes\\CLSID\\*"`

Lucene: `registry.path:HKLM\\SOFTWARE\\Classes\\CLSID\\* OR registry.path:HKCU\\SOFTWARE\\Classes\\CLSID\\*`

Zugriff auf AppInit_DLLs (zum Laden von DLLs bei Systemstart)

KQL: `registry.path: "HKLM\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Windows\\AppInit_DLLs"`

Lucene: `registry.path:HKLM\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Windows\\AppInit_DLLs`

Zugriff auf Image File Execution Options (IFEO) zur Umleitung von Prozessausführungen

KQL: `registry.path: "HKLM\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\*"`

Lucene: `registry.path:HKLM\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\*`

Zugriff auf den Service Control Manager (zur Erstellung/Änderung von Diensten)

KQL: `event.provider: "Service Control Manager" AND (event.action: "service created" OR event.action: "service modified")`

Lucene: `event.provider:"Service Control Manager" AND (event.action:service created OR event.action:service modified)`

SYSLOG und RSYSLOG Event Codes

Facility-Codes:

- kern (0): Kernel-Nachrichten
- user (1): Benutzernachrichten
- mail (2): Mail-System
- daemon (3): System-Daemons
- auth (4): Sicherheits-/Autorisierungsnachrichten
- syslog (5): Internes syslogd
- lpr (6): Drucknachrichten
- news (7): Nachrichten-Subsystem
- uucp (8): UUCP-Subsystem

Schweregrade:

- emerg (0): System ist unbenutzbar
- alert (1): Sofortige Maßnahme erforderlich
- crit (2): Kritische Bedingungen
- err (3): Fehlerbedingungen
- warning (4): Warnbedingungen
- notice (5): Normale, aber signifikante Bedingungen
- info (6): Informative Nachrichten
- debug (7): Debug-Level-Nachrichten

Kernel-kritische Nachrichten

KQL: `syslog.facility: "kern" AND syslog.severity: "crit"`

Lucene: `syslog.facility:kern AND syslog.severity:crit`

Authentifizierungsfehler

KQL: `syslog.facility: "auth" AND syslog.severity: "err"`

Lucene: `syslog.facility:auth AND syslog.severity:err`

System-Daemon-Warnungen

KQL: `syslog.facility: "daemon" AND syslog.severity: "warning"`

Lucene: `syslog.facility:daemon AND syslog.severity:warning`

Mail-System-Nachrichten mit hoher Priorität

KQL: `syslog.facility: "mail" AND (syslog.severity: "alert" OR syslog.severity: "emerg")`

Lucene: `syslog.facility:mail AND (syslog.severity:alert OR syslog.severity:emerg)`

Benutzerinformationsnachrichten

KQL: `syslog.facility: "user" AND syslog.severity: "info"`

Lucene: `syslog.facility:user AND syslog.severity:info`

Drucksystem-Fehler

KQL: `syslog.facility: "lpr" AND syslog.severity: "err"`

Lucene: `syslog.facility:lpr AND syslog.severity:err`

Nachrichtensystem-Debug-Nachrichten

KQL: `syslog.facility: "news" AND syslog.severity: "debug"`

Lucene: `syslog.facility:news AND syslog.severity:debug`

UUCP-Subsystem-Warnungen

KQL: `syslog.facility: "uucp" AND syslog.severity: "warning"`

Lucene: `syslog.facility:uucp AND syslog.severity:warning`

Linux Credential Abuse

Verwendung von sudo ohne Passwort

KQL: `process.name: "sudo" AND process.args: "-n"`

Lucene: `process.name:sudo AND process.args:-n`

Zugriff auf die /etc/shadow-Datei (enthält verschlüsselte Passwörter)

KQL: `file.path: "/etc/shadow" AND event.action: "read"`

Lucene: `file.path:/etc/shadow AND event.action:read`

Verwendung von su-Befehl (Benutzerwechsel)

KQL: `process.name: "su" AND process.args: "-"`

Lucene: `process.name:su AND process.args:-`

Ausführung von sshpass (Befehlszeilen-SSH-Authentifizierung)

KQL: `process.name: "sshpass"`

Lucene: `process.name:sshpass`

Zugriff auf SSH-Private-Keys

KQL: `file.path: "/home/*/.ssh/id_*" AND event.action: "read"`

Lucene: `file.path:/home/*/.ssh/id_* AND event.action:read`

Verwendung von export mit Passwort (mögliche Exposition von Anmeldeinformationen)

KQL: `process.name: "export" AND process.args: "*PASSWORD=*"`

Lucene: `process.name:export AND process.args:*PASSWORD=*`

Verwendung von passwd-Befehl (Passwortänderung)

KQL: `process.name: "passwd"`

Lucene: `process.name:passwd`

Zugriff auf .pgpass-Datei (PostgreSQL-Passwortdatei)

KQL: `file.path: "/home/*/.pgpass" AND event.action: "read"`

Lucene: `file.path:/home/*/.pgpass AND event.action:read`

Zugriff auf .my.cnf-Datei (MySQL-Konfigurationsdatei mit Anmeldeinformationen)

KQL: `file.path: "/home/*/.my.cnf" AND event.action: "read"`

Lucene: `file.path:/home/*/.my.cnf AND event.action:read`

Verwendung von gpg mit --passphrase-Option (mögliche Exposition von Passphrasen)

KQL: `process.name: "gpg" AND process.args: "--passphrase"`

Lucene: `process.name:gpg AND process.args:--passphrase`

Web Application Attacks

SQL-Injection-Angriffsversuche

KQL: `http.request_uri: "*' OR 1=1--*" OR http.request_body: "*' OR 1=1--*"`

Lucene: `http.request_uri:*' OR 1=1--* OR http.request_body:*' OR 1=1--*`

Cross-Site Scripting (XSS) Angriffsversuche

KQL: `http.request_uri: "*<script>*" OR http.request_body: "*<script>*"`

Lucene: `http.request_uri:*<script>* OR http.request_body:*<script>*`

Directory Traversal Angriffsversuche

KQL: `http.request_uri: "../*" OR http.request_body: "../*"`

Lucene: `http.request_uri:../* OR http.request_body:../*`

Remote File Inclusion (RFI) Angriffsversuche

KQL: `http.request_uri: "*http:*" OR http.request_body: "*http:*"`

Lucene: `http.request_uri:*http:* OR http.request_body:*http:*`

Web Shell Upload-Versuche

KQL: `http.request_uri: "*.php" AND http.request_body: "*base64_decode*"`

Lucene: `http.request_uri:*.php AND http.request_body:*base64_decode*`

Brute-Force-Anmeldeversuche

KQL: `http.status_code: "401" OR http.status_code: "403"`

Lucene: `http.status_code:401 OR http.status_code:403`

Command Injection Angriffsversuche

KQL: `http.request_uri: "*;cat /etc/passwd*" OR http.request_body: "*;cat /etc/passwd*"`

Lucene: `http.request_uri:*;cat /etc/passwd* OR http.request_body:*;cat /etc/passwd*`

HTTP Response Splitting Angriffsversuche

KQL: `http.request_headers: "*%0d%0a*"`

Lucene: `http.request_headers:*%0d%0a*`

XML External Entity (XXE) Angriffsversuche

KQL: `http.request_body: "*<!DOCTYPE*"`

Lucene: `http.request_body:<!DOCTYPE*`

Server-Side Request Forgery (SSRF) Angriffsversuche

KQL: `http.request_uri: "*localhost*" OR http.request_body: "*localhost*"`

Lucene: `http.request_uri:*localhost* OR http.request_body:*localhost*`

Linux Privilege Escalation

Verwendung von sudo ohne Passwort

KQL: `process.name: "sudo" AND process.args: "-n"`

Lucene: `process.name:sudo AND process.args:-n`

Zugriff auf die sudoers-Datei

KQL: `file.path: "/etc/sudoers" AND event.action: "read"`

Lucene: `file.path:/etc/sudoers AND event.action:read`

Verwendung des su-Befehls

KQL: `process.name: "su" AND process.args: "-"`

Lucene: `process.name:su AND process.args:-`

Zugriff auf sensitive Dateien mit cat

KQL: `process.name: "cat" AND (file.path: "/etc/shadow" OR file.path: "/etc/passwd")`

Lucene: `process.name:cat AND (file.path:/etc/shadow OR file.path:/etc/passwd)`

Verwendung von chmod oder chown auf sensitive Dateien

KQL: `process.name: ("chmod", "chown") AND file.path: "/etc/sudoers"`

Lucene: `process.name:(chmod OR chown) AND file.path:/etc/sudoers`

Verwendung von Kernel-Exploits

KQL: `process.args: "*dirtyc0w*" OR process.args: "*CVE-20*"`

Lucene: `process.args:*dirtyc0w* OR process.args:*CVE-20*`

Zugriff auf .bash_history (könnte Befehle zur Rechteerweiterung enthalten)

KQL: `file.path: "/home/*/.bash_history" AND event.action: "read"`

Lucene: `file.path:/home/*/.bash_history AND event.action:read`

Verwendung von pkexec (PolicyKit für Rechteerweiterung)

KQL: `process.name: "pkexec"`

Lucene: `process.name:pkexec`

Zugriff auf cron-Jobs

KQL: `file.path: "/etc/cron*" AND event.action: "write"`

Lucene: `file.path:/etc/cron* AND event.action:write`

Verwendung von setuid oder setgid Binaries

KQL: `file.setuid: true OR file.setgid: true`

Lucene: `file.setuid:true OR file.setgid:true`

Detecting Known Vulnerabilities

Heartbleed (CVE-2014-0160)

KQL: `network.data: "18 03 02 00 03 01 40 00"`

Lucene: `network.data:18 03 02 00 03 01 40 00`

EternalBlue (CVE-2017-0144)

KQL: `network.data: "ff534d4272"`

Lucene: `network.data:ff534d4272`

Shellshock (CVE-2014-6271)

KQL: `http.request_headers: "() {"`

Lucene: `http.request_headers:() {`

WannaCry Ransomware

KQL: `file.name: "WannaDecryptor.exe"`

Lucene: `file.name:WannaDecryptor.exe`

Apache Struts (CVE-2017-5638)

KQL: `http.request_headers: "%{(#_= 'multipart/form-data')}" OR http.request_body: "%{(#_= 'multipart/form-data')}"`

Lucene: `http.request_headers:%{(#_= 'multipart/form-data')} OR http.request_body:%{(#_= 'multipart/form-data')}`

Drupalgeddon (CVE-2018-7600)

KQL: `http.request_uri: "user/register?element_parents="`

Lucene: `http.request_uri:user/register?element_parents=`

Joomla RCE (CVE-2015-8562)

KQL: `http.request_headers: "JDatabaseDriverMysqli"`

Lucene: `http.request_headers:JDatabaseDriverMysqli`

Magento Shoplift (CVE-2015-1397)

KQL: `http.request_body: "install/design_config/db_schema"`

Lucene: `http.request_body:install/design_config/db_schema`

Ghost (CVE-2015-0235)

KQL: `network.data: "0xdeadbeef"`

Lucene: `network.data:0xdeadbeef`

MS17-010 SMB RCE

KQL: `network.protocol: "smb" AND network.data: "0500"`

Lucene: `network.protocol:smb AND network.data:0500`

Dezerialisierung in Java (CVE-2015-4852)

KQL: `network.data: "rO0ABXNy"`

Lucene: `network.data:rO0ABXNy`

Microsoft IIS Shortname (CVE-2017-7269)

KQL: `http.request_uri: "*.asp;*"`

Lucene: `http.request_uri:*.asp;*`

OpenSSL CCS Injection (CVE-2014-0224)

KQL: `network.data: "140300000101"`

Lucene: `network.data:140300000101`

WordPress REST API Vulnerability (CVE-2017-1001000)

KQL: `http.request_uri: "/wp-json/wp/v2/posts"`

Lucene: `http.request_uri:/wp-json/wp/v2/posts`

DROWN Attack (CVE-2016-0800)

KQL: `network.protocol: "ssl2"`

Lucene: `network.protocol:ssl2`

Apache Tomcat RCE via JSP Upload (CVE-2017-12617)

KQL: `http.request_uri: "*.jsp" AND http.method: "PUT"`

Lucene: `http.request_uri:*.jsp AND http.method:PUT`

Windows SMBv1 RCE (CVE-2017-0143)

KQL: `network.protocol: "smb" AND network.data: "1100"`

Lucene: `network.protocol:smb AND network.data:1100`

Oracle WebLogic WLS Security Component RCE (CVE-2019-2725)

KQL: `http.request_uri: "/_async/*" AND http.request_body: "<async-response>"`

Lucene: `http.request_uri:/_async/* AND http.request_body:<async-response>`

BlueKeep (CVE-2019-0708)

KQL: `network.protocol: "rdp" AND network.data: "0300000902f0802180"`

Lucene: `network.protocol:rdp AND network.data:0300000902f0802180`

SIGRed (CVE-2020-1350)

KQL: `dns.query: "*SIG*" AND dns.response_code: "SERVFAIL"`

Lucene: `dns.query:*SIG* AND dns.response_code:SERVFAIL`

Meltdown und Spectre (CVE-2017-5754, CVE-2017-5753, CVE-2017-5715)

KQL: `process.name: ("meltdown", "spectre")`

Lucene: `process.name:(meltdown OR spectre)`

Zerologon (CVE-2020-1472)

KQL: `network.protocol: "netlogon" AND event.action: "zero-credentials"`

Lucene: `network.protocol:netlogon AND event.action:zero-credentials`

Apache Log4j RCE (CVE-2021-44228)

KQL: `http.request_body: "${jndi:ldap://" OR http.request_headers: "${jndi:ldap://"`

Lucene: `http.request_body:${jndi:ldap://* OR http.request_headers:${jndi:ldap://*`

Microsoft Exchange Server RCE (CVE-2021-26855)

KQL: `http.request_uri: "/owa/auth/x.js"`

Lucene: `http.request_uri:/owa/auth/x.js`

SolarWinds Orion (CVE-2020-14005)

KQL: `file.path: "SolarWinds.Orion.Core.BusinessLayer.dll" AND file.hash: "b91ce2fa41029f6955bff20079468448"`

Lucene: `file.path:SolarWinds.Orion.Core.BusinessLayer.dll AND file.hash:b91ce2fa41029f6955bff20079468448`

Drupalgeddon2 (CVE-2018-7600)

KQL: `http.request_uri: "/user/register?_format=hal_json"`

Lucene: `http.request_uri:/user/register?_format=hal_json`

PrintNightmare (CVE-2021-34527)

KQL: `process.name: "spoolsv.exe" AND network.destination_port: 445`

Lucene: `process.name:spoolsv.exe AND network.destination_port:445`

Joomla RCE (CVE-2015-8562)

KQL: `http.request_headers: "User-Agent: Mozilla/5.0 ${@print(md5(acunetix_wvs_security_test))}"`

Lucene: `http.request_headers:User-Agent: Mozilla/5.0 ${@print(md5(acunetix_wvs_security_test))}`

Dirty COW (CVE-2016-5195)

KQL: `process.name: "dirtyc0w"`

Lucene: `process.name:dirtyc0w`

Mimikatz Detection

KQL: `process.name: "mimikatz.exe"`

Lucene: `process.name:mimikatz.exe`

Erkennen von Command-and-Control (C2) Infrastrukturen

Ungewöhnlicher User-Agent in HTTP-Anfragen

KQL: `http.user_agent: "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"`

Lucene: `http.user_agent:Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)`

Base64-kodierte Daten in HTTP-GET-Anfragen

KQL: `http.request_uri: "/?data=*" AND http.request_uri: "*base64*"`

Lucene: `http.request_uri:/?data=* AND http.request_uri:*base64*`

Ungewöhnlicher Outbound-Traffic auf hohen Ports

KQL: `network.destination_port: >65000`

Lucene: `network.destination_port:[65001 TO *]`

DNS-Anfragen zu Domains mit hoher Entropie

KQL: `dns.query: /[A-Za-z0-9]{30,}/`

Lucene: `dns.query:/[A-Za-z0-9]{30,}/`

Ungewöhnliche Verbindungshäufigkeit zu einer IP

KQL: `network.destination.ip: "x.x.x.x" AND event.rate: >100`

Lucene: `network.destination.ip:x.x.x.x AND event.rate:[101 TO *]`

Verdächtige Domains mit vielen Subdomains

KQL: `dns.query: "*.suspiciousdomain.com"`

Lucene: `dns.query:*.suspiciousdomain.com`

Ungewöhnliche Verbindung zu bekannten C2-Ports (z.B. 6667 für IRC)

KQL: `network.destination.port: 6667`

Lucene: `network.destination.port:6667`

Verdächtige User-Agent-Strings (z.B. leere oder Standard-Strings)

KQL: `http.user_agent: "-" OR http.user_agent: "Mozilla/5.0"`

Lucene: `http.user_agent:- OR http.user_agent:Mozilla/5.0`

Ungewöhnliche Zeiten für ausgehenden Datenverkehr

KQL: `event.timestamp: ["00:00:00" TO "03:00:00"] AND network.direction: "outbound"`

Lucene: `event.timestamp:[00:00:00 TO 03:00:00] AND network.direction:outbound`

Verdächtige Verbindungen zu Ländern, mit denen keine Geschäftsbeziehungen bestehen

KQL: `network.destination.geo.country: "North Korea"`

Lucene: `network.destination.geo.country:North Korea`

Malicious Network Communications

Ungewöhnlicher Datenverkehr auf Port 80 (HTTP)

KQL: `network.destination.port: 80 AND network.bytes: >1000000`

Lucene: `network.destination.port:80 AND network.bytes:[1000001 TO *]`

Verdächtige User-Agent-Strings (z.B. leere oder Standard-Strings)

KQL: `http.user_agent: "-" OR http.user_agent: "curl/*" OR http.user_agent: "wget/*"`

Lucene: `http.user_agent:- OR http.user_agent:curl/* OR http.user_agent:wget/*`

Ungewöhnlicher Datenverkehr auf Port 443 (HTTPS) ohne SSL/TLS

KQL: `network.destination.port: 443 AND network.protocol: NOT "tls"`

Lucene: `network.destination.port:443 AND NOT network.protocol:tls`

Verdächtige Domains mit vielen Subdomains

KQL: `dns.query: "*.*.*.com"`

Lucene: `dns.query:*.*.*.com`

Datenverkehr zu bekannten Tor Exit Nodes

KQL: `network.destination.ip: (list_of_tor_ips)`

Lucene: `network.destination.ip:(list_of_tor_ips)`

Ungewöhnliche Verbindung zu Ländern, mit denen keine Geschäftsbeziehungen bestehen

KQL: `network.destination.geo.country: "North Korea" OR network.destination.geo.country: "Iran"`

Lucene: `network.destination.geo.country:North Korea OR network.destination.geo.country:Iran`

Verdächtige ICMP-Datenverkehrsmuster (z.B. für Datenexfiltration)

KQL: `network.protocol: "icmp" AND network.bytes: >1000`

Lucene: `network.protocol:icmp AND network.bytes:[1001 TO *]`

Verdächtige DNS-Anfragen mit hoher Entropie (z.B. für DGA-Kommunikation)

KQL: `dns.query: /[A-Za-z0-9]{25,}/`

Lucene: `dns.query:/[A-Za-z0-9]{25,}/`

Ungewöhnliche Zeiten für ausgehenden Datenverkehr

KQL: `event.timestamp: ["00:00:00" TO "03:00:00"] AND network.direction: "outbound"`

Lucene: `event.timestamp:[00:00:00 TO 03:00:00] AND network.direction:outbound`

Verdächtige Datenmengen in ausgehendem Datenverkehr (mögliche Datenexfiltration)

KQL: `network.direction: "outbound" AND network.bytes: >5000000`

Lucene: `network.direction:outbound AND network.bytes:[5000001 TO *]`

Antivirus Alerts and Evasion

Verdächtige Dateinamen, die auf Malware hindeuten könnten

KQL: `file.name: ("*malware*", "*trojan*", "*ransomware*")`

Lucene: `file.name:*malware* OR file.name:*trojan* OR file.name:*ransomware*`

Antivirus-Alarme

KQL: `log.source: "antivirus" AND log.level: "alert"`

Lucene: `log.source:antivirus AND log.level:alert`

Mehrere Antivirus-Alarme von einem Endpunkt in kurzer Zeit

KQL: `log.source: "antivirus" AND event.rate: >5`

Lucene: `log.source:antivirus AND event.rate:[6 TO *]`

Dateien mit Doppel-Dateiendungen (häufig bei Malware)

KQL: `file.name: ("*.exe.pdf", "*.doc.exe", "*.pdf.exe")`

Lucene: `file.name:*.exe.pdf OR file.name:*.doc.exe OR file.name:*.pdf.exe`

Verdächtige PowerShell-Befehle (z.B. Base64-kodiert)

KQL: `process.name: "powershell.exe" AND process.args: "-encodedCommand"`

Lucene: `process.name:powershell.exe AND process.args:-encodedCommand`

Dateien aus dem Internet, die sofort ausgeführt werden

KQL: `file.origin: "internet" AND process.action: "execute"`

Lucene: `file.origin:internet AND process.action:execute`

Verdächtige Prozesse, die von einem temporären Ordner aus gestartet werden

KQL: `process.path: "C:\\Windows\\Temp\\*" OR process.path: "C:\\Users\\*\\AppData\\Local\\Temp\\*"`

Lucene: `process.path:C:\\Windows\\Temp\\* OR process.path:C:\\Users\\*\\AppData\\Local\\Temp\\*`

Verdächtige Registry-Änderungen (z.B. zur Persistenz)

KQL: `registry.path: ("*\\Run", "*\\RunOnce") AND registry.action: "set"`

Lucene: `registry.path:*\\Run OR registry.path:*\\RunOnce AND registry.action:set`

Verdächtige Netzwerkanfragen an bekannte Malware-Domains

KQL: `network.destination.domain: (list_of_malicious_domains)`

Lucene: `network.destination.domain:(list_of_malicious_domains)`

Dateien, die versuchen, den Antivirus-Prozess zu beenden

KQL: `process.name: "taskkill" AND process.args: "*antivirus*"`

Lucene: `process.name:taskkill AND process.args:*antivirus*`

Antimalware Scan Interface (AMSI) und AMSI Bypasses

AMSI Bypass über AmsiScanBuffer-Patch

KQL: `process.name: "powershell.exe" AND process.args: "*[AmsiScanBuffer]*"`

Lucene: `process.name:powershell.exe AND process.args:*[AmsiScanBuffer]*`

Verdächtige AMSI-Fehler

KQL: `log.source: "AMSI" AND log.level: "error"`

Lucene: `log.source:AMSI AND log.level:error`

AMSI Bypass über AmsiUtils-Patch

KQL: `process.name: "powershell.exe" AND process.args: "*AmsiUtils*"`

Lucene: `process.name:powershell.exe AND process.args:*AmsiUtils*`

Verdächtige AMSI-Initialisierungsversuche

KQL: `log.source: "AMSI" AND log.message: "Initialization failed"`

Lucene: `log.source:AMSI AND log.message:"Initialization failed"`

AMSI Bypass über Speicherinjektion

KQL: `process.name: "powershell.exe" AND process.args: "*[System.Runtime.InteropServices.Marshal]::Copy*"`

Lucene: `process.name:powershell.exe AND process.args:*[System.Runtime.InteropServices.Marshal]::Copy*`

Verdächtige AMSI-Endpunkte

KQL: `network.destination.domain: "*amsi.microsoft.com"`

Lucene: `network.destination.domain:*amsi.microsoft.com`

AMSI Bypass über COM-Objekte

KQL: `process.name: "powershell.exe" AND process.args: "*[ComObject].CreateObject*"`

Lucene: `process.name:powershell.exe AND process.args:*[ComObject].CreateObject*`

AMSI Bypass durch das Entladen von AMSI-DLLs

KQL: `process.name: "powershell.exe" AND process.args: "*amsi.dll*"`

Lucene: `process.name:powershell.exe AND process.args:*amsi.dll*`

AMSI Bypass über Reflection

KQL: `process.name: "powershell.exe" AND process.args: "*[Reflection.Assembly]::Load*"`

Lucene: `process.name:powershell.exe AND process.args:*[Reflection.Assembly]::Load*`

AMSI Bypass durch das Manipulieren von AMSI-Scan-Ergebnissen

KQL: `process.name: "powershell.exe" AND process.args: "*AmsiScanStringResult*"`

Lucene: `process.name:powershell.exe AND process.args:*AmsiScanStringResult*`

Network Evasion and Tunneling

Ungewöhnlicher Datenverkehr auf Port 53 (DNS)

KQL: `network.destination.port: 53 AND network.bytes: >5000`

Lucene: `network.destination.port:53 AND network.bytes:[5001 TO *]`

Verdächtige ICMP-Datenverkehrsmuster (z.B. für Datenexfiltration oder Tunneling)

KQL: `network.protocol: "icmp" AND network.bytes: >1000`

Lucene: `network.protocol:icmp AND network.bytes:[1001 TO *]`

Ungewöhnlicher Datenverkehr auf Port 80 (HTTP) oder 443 (HTTPS)

KQL: `network.destination.port: (80, 443) AND network.bytes: >1000000`

Lucene: `network.destination.port:(80 443) AND network.bytes:[1000001 TO *]`

Verdächtige SSL/TLS-Zertifikate (z.B. selbstsigniert oder abgelaufen)

KQL: `tls.certificate.issuer: "unknown" OR tls.certificate.status: "expired"`

Lucene: `tls.certificate.issuer:unknown OR tls.certificate.status:expired`

Ungewöhnliche Verbindung zu Ländern, mit denen keine Geschäftsbeziehungen bestehen

KQL: `network.destination.geo.country: "North Korea" OR network.destination.geo.country: "Iran"`

Lucene: `network.destination.geo.country:North Korea OR network.destination.geo.country:Iran`

Verdächtige Tor-Datenverkehr

KQL: `network.destination.port: 9050 OR network.destination.port: 9150`

Lucene: `network.destination.port:9050 OR network.destination.port:9150`

Verdächtige SSH-Tunneling-Aktivitäten

KQL: `network.protocol: "ssh" AND network.bytes: >500000`

Lucene: `network.protocol:ssh AND network.bytes:[500001 TO *]`

Verdächtige VPN-Verbindungen

KQL: `network.protocol: "vpn" AND network.bytes: >1000000`

Lucene: `network.protocol:vpn AND network.bytes:[1000001 TO *]`

Ungewöhnliche Zeiten für ausgehenden Datenverkehr (mögliche Umgehung)

KQL: `event.timestamp: ["00:00:00" TO "03:00:00"] AND network.direction: "outbound"`

Lucene: `event.timestamp:[00:00:00 TO 03:00:00] AND network.direction:outbound`

Verdächtige Datenmengen in ausgehendem Datenverkehr (mögliche Datenexfiltration)

KQL: `network.direction: "outbound" AND network.bytes: >5000000`

Lucene: `network.direction:outbound AND network.bytes:[5000001 TO *]`

Egress Busting (Ausgehende Datenverkehrskontrolle)

Ungewöhnlich hoher ausgehender Datenverkehr

KQL: `network.direction: "outbound" AND network.bytes: >10000000`

Lucene: `network.direction:outbound AND network.bytes:[10000001 TO *]`

Ungewöhnliche Ports für ausgehenden Datenverkehr

KQL: `network.direction: "outbound" AND NOT network.destination.port: (80, 443, 21, 22, 25)`

Lucene: `network.direction:outbound AND NOT network.destination.port:(80 443 21 22 25)`

Ungewöhnliche Zeiten für ausgehenden Datenverkehr

KQL: `event.timestamp: ["00:00:00" TO "03:00:00"] AND network.direction: "outbound"`

Lucene: `event.timestamp:[00:00:00 TO 03:00:00] AND network.direction:outbound`

Ausgehender Datenverkehr zu verdächtigen Ländern

KQL: `network.direction: "outbound" AND network.destination.geo.country: "North Korea"`

Lucene: `network.direction:outbound AND network.destination.geo.country:North Korea`

Ungewöhnliche User-Agent-Strings im ausgehenden Datenverkehr

KQL: `network.direction: "outbound" AND http.user_agent: "curl/*"`

Lucene: `network.direction:outbound AND http.user_agent:curl/*`

Ausgehender Datenverkehr mit verdächtigen MIME-Typen (z.B. Anwendung oder Oktett-Stream)

KQL: `network.direction: "outbound" AND http.content_type: ("application/*", "octet-stream")`

Lucene: `network.direction:outbound AND http.content_type:(application/* octet-stream)`

Ausgehender Datenverkehr mit verdächtigen Dateianhängen (z.B. .exe, .bat)

KQL: `network.direction: "outbound" AND file.extension: ("exe", "bat")`

Lucene: `network.direction:outbound AND file.extension:(exe bat)`

Ausgehender Datenverkehr zu nicht standardmäßigen IP-Adressen (z.B. private IP-Bereiche)

KQL: `network.direction: "outbound" AND network.destination.ip: ("10.0.0.0/8", "172.16.0.0/12", "192.168.0.0/16")`

Lucene: `network.direction:outbound AND network.destination.ip:(10.0.0.0/8 172.16.0.0/12 192.168.0.0/16)`

Ausgehender Datenverkehr mit verdächtigen Domains (z.B. neu registrierte oder Domains mit hoher Entropie)

KQL: `network.direction: "outbound" AND dns.query: /[A-Za-z0-9]{25,}/`

Lucene: `network.direction:outbound AND dns.query:/[A-Za-z0-9]{25,}/`

Ausgehender Datenverkehr mit verdächtigen SSL/TLS-Zertifikaten

KQL: `network.direction: "outbound" AND tls.certificate.status: "self-signed"`

Lucene: `network.direction:outbound AND tls.certificate.status:self-signed`

Port Forwarding and Tunneling

SSH-Port-Weiterleitung (Local Forwarding)

KQL: `process.name: "ssh" AND process.args: ("-L", "-D")`

Lucene: `process.name:ssh AND (process.args:-L OR process.args:-D)`

SSH-Port-Weiterleitung (Remote Forwarding)

KQL: `process.name: "ssh" AND process.args: "-R"`

Lucene: `process.name:ssh AND process.args:-R`

Verdächtige Aktivität auf Port 1080 (oft für SOCKS Proxy verwendet)

KQL: `network.destination.port: 1080`

Lucene: `network.destination.port:1080`

Verdächtige Aktivität auf Port 8080 (oft für HTTP-Tunnel verwendet)

KQL: `network.destination.port: 8080`

Lucene: `network.destination.port:8080`

Plink.exe-Aktivität (oft für SSH-Tunneling verwendet)

KQL: `process.name: "plink.exe"`

Lucene: `process.name:plink.exe`

Verdächtige Aktivität auf Port 22 (SSH) von nicht-Standard-IPs

KQL: `network.destination.port: 22 AND NOT network.source.ip: (list_of_trusted_ips)`

Lucene: `network.destination.port:22 AND NOT network.source.ip:(list_of_trusted_ips)`

Verdächtige Aktivität auf Port 3389 (RDP) mit hohem Datenvolumen (möglicher Tunnel)

KQL: `network.destination.port: 3389 AND network.bytes: >1000000`

Lucene: `network.destination.port:3389 AND network.bytes:[1000001 TO *]`

Verdächtige VPN-Verbindungen

KQL: `network.protocol: "vpn" AND network.bytes: >1000000`

Lucene: `network.protocol:vpn AND network.bytes:[1000001 TO *]`

Verdächtige Aktivität auf Port 1194 (OpenVPN)

KQL: `network.destination.port: 1194`

Lucene: `network.destination.port:1194`

Verdächtige Aktivität auf Port 443 mit nicht-HTTPS-Protokoll (möglicher SSL-Tunnel)

KQL: `network.destination.port: 443 AND NOT network.protocol: "tls"`

Lucene: `network.destination.port:443 AND NOT network.protocol:tls`

Abusing Lightweight Directory Access Protocol

Verdächtige LDAP-Anfragen mit hohem Volumen

KQL: `network.protocol: "ldap" AND network.bytes: >1000000`

Lucene: `network.protocol:ldap AND network.bytes:[1000001 TO *]`

LDAP-Anfragen von nicht standardmäßigen IP-Adressen

KQL: `network.protocol: "ldap" AND NOT network.source.ip: (list_of_trusted_ips)`

Lucene: `network.protocol:ldap AND NOT network.source.ip:(list_of_trusted_ips)`

Verdächtige LDAP-Bindungen (z.B. anonyme Bindungen)

KQL: `event.category: "ldap" AND event.action: "bind" AND user.name: "anonymous"`

Lucene: `event.category:ldap AND event.action:bind AND user.name:anonymous`

LDAP-Anfragen nach sensiblen Attributen (z.B. userPassword)

KQL: `event.category: "ldap" AND event.action: "search" AND ldap.search.filter: "*userPassword*"`

Lucene: `event.category:ldap AND event.action:search AND ldap.search.filter:*userPassword*`

Verdächtige LDAP-Modifikationen

KQL: `event.category: "ldap" AND event.action: "modify"`

Lucene: `event.category:ldap AND event.action:modify`

LDAP-Anfragen, die zu vielen Ergebnissen führen

KQL: `event.category: "ldap" AND event.action: "search" AND ldap.search.result_count: >1000`

Lucene: `event.category:ldap AND event.action:search AND ldap.search.result_count:[1001 TO *]`

Verdächtige LDAP-Verbindungen zu nicht standardmäßigen Ports

KQL: `network.protocol: "ldap" AND NOT network.destination.port: 389`

Lucene: `network.protocol:ldap AND NOT network.destination.port:389`

LDAP-Anfragen zu ungewöhnlichen Zeiten

KQL: `event.category: "ldap" AND event.timestamp: ["00:00:00" TO "03:00:00"]`

Lucene: `event.category:ldap AND event.timestamp:[00:00:00 TO 03:00:00]`

Verdächtige LDAP-Entfernungen oder Löschungen

KQL: `event.category: "ldap" AND event.action: "delete"`

Lucene: `event.category:ldap AND event.action:delete`

LDAP-Replikationsanfragen von nicht-DCs (Domain-Controllern)

KQL: `event.category: "ldap" AND event.action: "replicate" AND NOT network.source.ip: (list_of_domain_controllers)`

Lucene: `event.category:ldap AND event.action:replicate AND NOT network.source.ip:(list_of_domain_controllers)`

Enumeration von Active Directory mit PowerView, SharpHound und PowerShell

PowerView-Modulaktivität

KQL: `process.name: "powershell.exe" AND process.args: "*PowerView.ps1*"`

Lucene: `process.name:powershell.exe AND process.args:*PowerView.ps1*`

SharpHound-Modulaktivität

KQL: `process.name: "SharpHound.exe"`

Lucene: `process.name:SharpHound.exe`

PowerView Get-NetDomain-Anfrage

KQL: `process.name: "powershell.exe" AND process.args: "*Get-NetDomain*"`

Lucene: `process.name:powershell.exe AND process.args:*Get-NetDomain*`

PowerView Get-NetUser-Anfrage

KQL: `process.name: "powershell.exe" AND process.args: "*Get-NetUser*"`

Lucene: `process.name:powershell.exe AND process.args:*Get-NetUser*`

PowerView Get-NetGroup-Anfrage

KQL: `process.name: "powershell.exe" AND process.args: "*Get-NetGroup*"`

Lucene: `process.name:powershell.exe AND process.args:*Get-NetGroup*`

PowerView Get-DomainPolicy-Anfrage

KQL: `process.name: "powershell.exe" AND process.args: "*Get-DomainPolicy*"`

Lucene: `process.name:powershell.exe AND process.args:*Get-DomainPolicy*`

PowerView Get-NetComputer-Anfrage

KQL: `process.name: "powershell.exe" AND process.args: "*Get-NetComputer*"`

Lucene: `process.name:powershell.exe AND process.args:*Get-NetComputer*`

PowerView Invoke-ShareFinder-Anfrage

KQL: `process.name: "powershell.exe" AND process.args: "*Invoke-ShareFinder*"`

Lucene: `process.name:powershell.exe AND process.args:*Invoke-ShareFinder*`

PowerView Invoke-UserHunter-Anfrage

KQL: `process.name: "powershell.exe" AND process.args: "*Invoke-UserHunter*"`

Lucene: `process.name:powershell.exe AND process.args:*Invoke-UserHunter*`

PowerShell AD-Modulaktivität

KQL: `process.name: "powershell.exe" AND process.args: "*ActiveDirectory*"`

Lucene: `process.name:powershell.exe AND process.args:*ActiveDirectory*`

Windows Lateral Movement

Verdächtige Verwendung von PsExec

KQL: `process.name: "psexec.exe" OR process.args: "*\\\\* -accepteula*"`

Lucene: `process.name:psexec.exe OR process.args:*\\\\* -accepteula*`

Remoteausführung mit WMIC

KQL: `process.name: "wmic.exe" AND process.args: "/node:* process call create*"`

Lucene: `process.name:wmic.exe AND process.args:/node:* process call create*`

Verdächtige Verwendung von RDP (Remote Desktop Protocol)

KQL: `event.category: "authentication" AND network.protocol: "rdp" AND event.outcome: "success"`

Lucene: `event.category:authentication AND network.protocol:rdp AND event.outcome:success`

Zugriff auf ADMIN$ oder C$ Freigaben

KQL: `file.path: "\\\\*\\ADMIN$" OR file.path: "\\\\*\\C$"`

Lucene: `file.path:\\\\*\\ADMIN$ OR file.path:\\\\*\\C$`

Verdächtige Verwendung von Scheduled Tasks

KQL: `process.name: "schtasks.exe" AND process.args: "/create"`

Lucene: `process.name:schtasks.exe AND process.args:/create`

Remoteausführung mit PowerShell Remoting

KQL: `process.name: "powershell.exe" AND process.args: "-remoting"`

Lucene: `process.name:powershell.exe AND process.args:-remoting`

Verdächtige Verwendung von DCOM

KQL: `process.name: "dllhost.exe" AND process.parent.name: "svchost.exe"`

Lucene: `process.name:dllhost.exe AND process.parent.name:svchost.exe`

Verdächtige Verwendung von BITSAdmin

KQL: `process.name: "bitsadmin.exe"`

Lucene: `process.name:bitsadmin.exe`

Verdächtige Verwendung von Net Commands

KQL: `process.name: "net.exe" AND (process.args: "use" OR process.args: "view")`

Lucene: `process.name:net.exe AND (process.args:use OR process.args:view)`

Verdächtige Verwendung von Remote Service Creation

KQL: `event.category: "service" AND event.action: "service_created" AND network.direction: "outbound"`

Lucene: `event.category:service AND event.action:service_created AND network.direction:outbound`

Linux Lateral Movement

Verdächtige Verwendung von SSH für Remote-Befehlsausführung

KQL: `process.name: "ssh" AND process.args: "-oProxyCommand*"`

Lucene: `process.name:ssh AND process.args:-oProxyCommand*`

Verdächtige Verwendung von SCP für Dateiübertragungen

KQL: `process.name: "scp"`

Lucene: `process.name:scp`

Verdächtige Verwendung von RSYNC für Dateisynchronisation

KQL: `process.name: "rsync" AND process.args: "--rsh*"`

Lucene: `process.name:rsync AND process.args:--rsh*`

Verdächtige Verwendung von Netcat für Port-Weiterleitung

KQL: `process.name: "nc" AND (process.args: "-l" OR process.args: "-p")`

Lucene: `process.name:nc AND (process.args:-l OR process.args:-p)`

Verdächtige Verwendung von SFTP

KQL: `process.name: "sftp"`

Lucene: `process.name:sftp`

Verdächtige Verwendung von TELNET

KQL: `process.name: "telnet"`

Lucene: `process.name:telnet`

Verdächtige Cron-Job-Erstellungen

KQL: `process.name: "cron" AND process.args: "* * * * *"`

Lucene: `process.name:cron AND process.args:* * * * *`

Verdächtige Verwendung von SSH-Tunneling

KQL: `process.name: "ssh" AND (process.args: "-D" OR process.args: "-L" OR process.args: "-R")`

Lucene: `process.name:ssh AND (process.args:-D OR process.args:-L OR process.args:-R)`

Verdächtige Verwendung von SSH-Passwortauthentifizierung

KQL: `process.name: "ssh" AND process.args: "-oPasswordAuthentication=yes"`

Lucene: `process.name:ssh AND process.args:-oPasswordAuthentication=yes`

Verdächtige Verwendung von SSH-Key-Scanning (SSH-Keyscan)

KQL: `process.name: "ssh-keyscan"`

Lucene: `process.name:ssh-keyscan`

Missbrauch von Kerberos-Tickets

Verdächtige Verwendung von Kerberos Ticket Granting Ticket (TGT) Erneuerung

KQL: `event.category: "kerberos" AND event.action: "TGT_Renewed"`

Lucene: `event.category:kerberos AND event.action:TGT_Renewed`

Verdächtige Verwendung von Kerberos Golden Ticket

KQL: `event.category: "kerberos" AND event.action: "TGT_Requested" AND user.domain: "KRBTGT"`

Lucene: `event.category:kerberos AND event.action:TGT_Requested AND user.domain:KRBTGT`

Verdächtige Verwendung von Kerberos Silver Ticket

KQL: `event.category: "kerberos" AND event.action: "Service_Ticket_Requested" AND user.domain: "KRBTGT"`

Lucene: `event.category:kerberos AND event.action:Service_Ticket_Requested AND user.domain:KRBTGT`

Verdächtige Verwendung von Kerberoasting

KQL: `event.category: "kerberos" AND event.action: "Service_Ticket_Requested" AND user.name: "*$"`

Lucene: `event.category:kerberos AND event.action:Service_Ticket_Requested AND user.name:*$`

Verdächtige Verwendung von Pass-the-Ticket (PTT)

KQL: `event.category: "kerberos" AND event.action: "TGT_Presented" AND NOT network.source.ip: (list_of_trusted_ips)`

Lucene: `event.category:kerberos AND event.action:TGT_Presented AND NOT network.source.ip:(list_of_trusted_ips)`

Verdächtige Verwendung von Overpass-the-Hash (Pass-the-Key)

KQL: `event.category: "kerberos" AND event.action: "TGT_Requested" AND event.reason: "NTLM_Hash_Used"`

Lucene: `event.category:kerberos AND event.action:TGT_Requested AND event.reason:NTLM_Hash_Used`

Verdächtige Verwendung von DCSync

KQL: `event.category: "directory_service" AND event.action: "replication_request" AND user.name: "DC$"`

Lucene: `event.category:directory_service AND event.action:replication_request AND user.name:DC$`

Verdächtige Verwendung von Kerberos Pre-Authentication Fehlern

KQL: `event.category: "kerberos" AND event.action: "preauth_failed"`

Lucene: `event.category:kerberos AND event.action:preauth_failed`

Verdächtige Verwendung von Kerberos Delegationsmissbrauch

KQL: `event.category: "kerberos" AND event.action: "delegation_requested"`

Lucene: `event.category:kerberos AND event.action:delegation_requested`

Verdächtige Verwendung von Kerberos Cross-Realm-Tickets

KQL: `event.category: "kerberos" AND event.action: "cross_realm_ticket"`

Lucene: `event.category:kerberos AND event.action:cross_realm_ticket`

Active Directory Persistence

Verdächtige Verwendung von Gruppenrichtlinienobjekten (GPO)

KQL: `event.category: "directory_service" AND event.action: "gpo_created"`

Lucene: `event.category:directory_service AND event.action:gpo_created`

Verdächtige Verwendung von Verzeichnisdienständerungen

KQL: `event.category: "directory_service" AND event.action: "object_modified"`

Lucene: `event.category:directory_service AND event.action:object_modified`

Verdächtige Verwendung von Sicherheitsunterstützungsanbieter (SSP)

KQL: `process.name: "lsass.exe" AND dll.name: "custom_ssp.dll"`

Lucene: `process.name:lsass.exe AND dll.name:custom_ssp.dll`

Verdächtige Verwendung von Golden Ticket

KQL: `event.category: "kerberos" AND event.action: "TGT_Requested" AND user.domain: "KRBTGT"`

Lucene: `event.category:kerberos AND event.action:TGT_Requested AND user.domain:KRBTGT`

Verdächtige Verwendung von Silver Ticket

KQL: `event.category: "kerberos" AND event.action: "Service_Ticket_Requested" AND user.domain: "KRBTGT"`

Lucene: `event.category:kerberos AND event.action:Service_Ticket_Requested AND user.domain:KRBTGT`

Verdächtige Verwendung von DCSync

KQL: `event.category: "directory_service" AND event.action: "replication_request" AND user.name: "DC$"`

Lucene: `event.category:directory_service AND event.action:replication_request AND user.name:DC$`

Verdächtige Verwendung von SID-History-Injektion

KQL: `event.category: "directory_service" AND event.action: "sid_history_added"`

Lucene: `event.category:directory_service AND event.action:sid_history_added`

Verdächtige Verwendung von Kerberos Delegationsmissbrauch

KQL: `event.category: "kerberos" AND event.action: "delegation_requested"`

Lucene: `event.category:kerberos AND event.action:delegation_requested`

Verdächtige Verwendung von AdminSDHolder-Objektänderungen

KQL: `event.category: "directory_service" AND object.name: "AdminSDHolder" AND event.action: "object_modified"`

Lucene: `event.category:directory_service AND object.name:AdminSDHolder AND event.action:object_modified`

Verdächtige Verwendung von Verzeichnisdienst-Wiederherstellungsagenten

KQL: `event.category: "directory_service" AND event.action: "recovery_agent_set"`

Lucene: `event.category:directory_service AND event.action:recovery_agent_set`

Angriffe auf einen Linux Mailserver

Verdächtige Anmeldeversuche über SMTP

KQL: `event.category: "authentication" AND network.protocol: "smtp" AND event.outcome: "failure"`

Lucene: `event.category:authentication AND network.protocol:smtp AND event.outcome:failure`

Verdächtige Mail-Relay-Aktivitäten

KQL: `event.category: "mail" AND event.action: "relay_attempt" AND event.outcome: "success"`

Lucene: `event.category:mail AND event.action:relay_attempt AND event.outcome:success`

Verdächtige IMAP/POP3 Anmeldeversuche

KQL:

```
event.category: "authentication" AND (network.protocol: "imap" OR network.protocol: "pop3") AND event.outcome: "failure"
```

Lucene: `event.category:authentication AND (network.protocol:imap OR network.protocol:pop3) AND event.outcome:failure`

Verdächtige Mailserver-Konfigurationsänderungen

KQL: `event.category: "configuration" AND process.name: "postfix" AND event.action: "config_changed"`

Lucene: `event.category:configuration AND process.name:postfix AND event.action:config_changed`

Verdächtige E-Mail-Anhänge

KQL: `file.extension: ("exe" OR "dll" OR "js" OR "vbs") AND event.action: "email_attachment_received"`

Lucene: `file.extension:(exe OR dll OR js OR vbs) AND event.action:email_attachment_received`

Verdächtige E-Mail-Links

KQL: `event.category: "mail" AND event.action: "link_received" AND url.domain: "suspicious-domain.com"`

Lucene: `event.category:mail AND event.action:link_received AND url.domain:suspicious-domain.com`

Verdächtige Ausgehende E-Mails

KQL: `event.category: "mail" AND event.action: "email_sent" AND destination.ip: "external_ip"`

Lucene: `event.category:mail AND event.action:email_sent AND destination.ip:external_ip`

Verdächtige E-Mail-Volumen

KQL: `event.category: "mail" AND event.action: "email_received" AND source.ip: "suspicious_ip" AND count: >100`

Lucene: `event.category:mail AND event.action:email_received AND source.ip:suspicious_ip AND count:>100`

Verdächtige Verwendung von Mailserver-Tools

KQL: `process.name: ("mailq" OR "postqueue")`

Lucene: `process.name:(mailq OR postqueue)`

Verdächtige Mailserver-Prozessaktivitäten

KQL: `process.name: "postfix" AND process.args: ("master" OR "pickup" OR "qmgr")`

Lucene: `process.name:postfix AND process.args:(master OR pickup OR qmgr)`

Angriffe auf einen Windows Mailserver

Verdächtige Anmeldeversuche über SMTP

KQL: `event.category: "authentication" AND network.protocol: "smtp" AND event.outcome: "failure"`

Lucene: `event.category:authentication AND network.protocol:smtp AND event.outcome:failure`

Verdächtige Exchange-Verwaltungskonsole (EAC) Anmeldeversuche

KQL: `event.category: "authentication" AND url.path: "/ecp" AND event.outcome: "failure"`

Lucene: `event.category:authentication AND url.path:/ecp AND event.outcome:failure`

Verdächtige Outlook Web App (OWA) Anmeldeversuche

KQL: `event.category: "authentication" AND url.path: "/owa" AND event.outcome: "failure"`

Lucene: `event.category:authentication AND url.path:/owa AND event.outcome:failure`

Verdächtige Exchange-Webdienste (EWS) Anfragen

KQL: `event.category: "web" AND url.path: "/ews/exchange.asmx"`

Lucene: `event.category:web AND url.path:/ews/exchange.asmx`

Verdächtige E-Mail-Anhänge

KQL: `file.extension: ("exe" OR "dll" OR "js" OR "vbs") AND event.action: "email_attachment_received"`

Lucene: `file.extension:(exe OR dll OR js OR vbs) AND event.action:email_attachment_received`

Verdächtige E-Mail-Links

KQL: `event.category: "mail" AND event.action: "link_received" AND url.domain: "suspicious-domain.com"`

Lucene: `event.category:mail AND event.action:link_received AND url.domain:suspicious-domain.com`

Verdächtige Ausgehende E-Mails

KQL: `event.category: "mail" AND event.action: "email_sent" AND destination.ip: "external_ip"`

Lucene: `event.category:mail AND event.action:email_sent AND destination.ip:external_ip`

Verdächtige Exchange PowerShell-Aktivitäten

KQL: `process.name: "powershell.exe" AND process.args: "Exchange.ps1"`

Lucene: `process.name:powershell.exe AND process.args:Exchange.ps1`

Verdächtige Exchange-Verwaltungsshell-Aktivitäten

KQL: `process.name: "exshell.psc1"`

Lucene: `process.name:exshell.psc1`

Verdächtige Mailbox-Exportanfragen

KQL: `event.category: "mail" AND event.action: "mailbox_export"`

Lucene: `event.category:mail AND event.action:mailbox_export`

Angriffe auf Content-Management-Systeme (CMS) wie WordPress, Joomla, Drupal und Co.

Verdächtige WordPress-Admin-Anmeldeversuche

KQL: `event.category: "authentication" AND url.path: "/wp-login.php" AND event.outcome: "failure"`

Lucene: `event.category:authentication AND url.path:/wp-login.php AND event.outcome:failure`

Verdächtige Joomla-Admin-Anmeldeversuche

KQL: `event.category: "authentication" AND url.path: "/administrator/index.php" AND event.outcome: "failure"`

Lucene: `event.category:authentication AND url.path:/administrator/index.php AND event.outcome:failure`

Verdächtige Drupal-Admin-Anmeldeversuche

KQL: `event.category: "authentication" AND url.path: "/user/login" AND event.outcome: "failure"`

Lucene: `event.category:authentication AND url.path:/user/login AND event.outcome:failure`

Verdächtige WordPress-Plugin-Uploads

KQL: `event.category: "web" AND url.path: "/wp-admin/update.php" AND http.request.method: "POST"`

Lucene: `event.category:web AND url.path:/wp-admin/update.php AND http.request.method:POST`

Verdächtige Joomla-Extension-Uploads

KQL: `event.category: "web" AND url.path: "/administrator/index.php?option=com_installer" AND http.request.method: "POST"`

Lucene: `event.category:web AND url.path:/administrator/index.php?option=com_installer AND http.request.method:POST`

Verdächtige Drupal-Modul-Uploads

KQL: `event.category: "web" AND url.path: "/admin/modules/install" AND http.request.method: "POST"`

Lucene: `event.category:web AND url.path:/admin/modules/install AND http.request.method:POST`

Verdächtige WordPress-XML-RPC-Anfragen

KQL: `event.category: "web" AND url.path: "/xmlrpc.php"`

Lucene: `event.category:web AND url.path:/xmlrpc.php`

Verdächtige Joomla-Template-Änderungen

KQL: `event.category: "web" AND url.path: "/administrator/index.php?option=com_templates" AND http.request.method: "POST"`

Lucene: `event.category:web AND url.path:/administrator/index.php?option=com_templates AND http.request.method:POST`

Verdächtige Drupal-Theme-Änderungen

KQL: `event.category: "web" AND url.path: "/admin/appearance/settings" AND http.request.method: "POST"`

Lucene: `event.category:web AND url.path:/admin/appearance/settings AND http.request.method:POST`

Verdächtige CMS-Dateiuploads

KQL: `event.category: "web" AND http.request.method: "POST" AND file.extension: ("php" OR "js" OR "html")`

Lucene: `event.category:web AND http.request.method:POST AND file.extension:(php OR js OR html)`

macOS

Erkennung von erhöhten Berechtigungen (Privilege Escalation)

KQL: `event.category:"process" AND process_parent_name:"sudo" AND process_path:"/usr/bin/sudo"`

Lucene: `event.category:"process" AND process_parent_name:"sudo" AND process_path:"/usr/bin/sudo"`

Erkennung von verdeckten Prozessen (Persistence):

KQL:
`event.category:"process" AND (process_name:"launchctl" OR process_name:"launchd") AND process_command_line:"/Library/LaunchAgents"`

Lucene:
`event.category:"process" AND (process_name:"launchctl" OR process_name:"launchd") AND process_command_line:"/Library/LaunchAgents"`

Erkennung von ungewöhnlicher Netzwerkkommunikation (Command and Control)

KQL: `event.category:"network" AND network_direction:"outbound" AND (destination_port:8080 OR destination_port:8888)`

Lucene: `event.category:"network" AND network_direction:"outbound" AND (destination_port:8080 OR destination_port:8888)`

Erkennung von Malware-Dateien

KQL: `event.category:"file" AND (file_name:"malware.exe" OR file_name:"malicious.dylib")`

Lucene: `event.category:"file" AND (file_name:"malware.exe" OR file_name:"malicious.dylib")`

Erkennung von Anomalien bei Benutzeranmeldungen

KQL: `event.category:"authentication" AND event_action:"logon" AND NOT (user_name:"admin" OR user_name:"root")`

Lucene: `event.category:"authentication" AND event_action:"logon" AND NOT (user_name:"admin" OR user_name:"root")`

Erkennung von ungewöhnlicher Hostnamenänderung

KQL: `event.category:"system" AND event_action:"hostname_change"`

Lucene: `event.category:"system" AND event_action:"hostname_change"`

Erkennung von bösartigen LaunchAgents

KQL:

`event.category:"file" AND file_path:"/Library/LaunchAgents" AND (file_name:"malicious.plist" OR file_name:"evil.plist")`

Lucene:
`event.category:"file" AND file_path:"/Library/LaunchAgents" AND (file_name:"malicious.plist" OR file_name:"evil.plist")`

Erkennung von ungewöhnlichen System- und Kernelmoduleinträgen

KQL:
`event.category:"system" AND event_action:"kernel_module_loaded" AND (target_name:"malicious.kext" OR target_name:"suspicious.kext")`

Lucene:
`event.category:"system" AND event_action:"kernel_module_loaded" AND (target_name:"malicious.kext" OR target_name:"suspicious.kext")`

Erkennung von ungewöhnlichen Cron-Jobs:

KQL: `event.category:"process" AND (process_name:"crontab" OR process_name:"cron") AND process_command_line:"*"`

Lucene: `event.category:"process" AND (process_name:"crontab" OR process_name:"cron") AND process_command_line:"*"`

Erkennung von Änderungen in der Firewall-Konfiguration

KQL: `event.category:"firewall" AND (firewall_action:"added_rule" OR firewall_action:"removed_rule")`

Lucene: `event.category:"firewall" AND (firewall_action:"added_rule" OR firewall_action:"removed_rule")`

Typische Angreifer Tools

PowerView.ps1

KQL:
`event.category:"process" AND process_name:"powershell.exe" AND (process_command_line:"*PowerView.ps1" OR (process_command_line:"*po`

Lucene:
`event.category:"process" AND process_name:"powershell.exe" AND (process_command_line:"*PowerView.ps1" OR (process_command_line:"*po`

PowerUp.ps1

KQL:
`event.category:"process" AND process_name:"powershell.exe" AND (process_command_line:"*PowerUp.ps1" OR (process_command_line:"*powe`

Lucene:
`event.category:"process" AND process_name:"powershell.exe" AND (process_command_line:"*PowerUp.ps1" OR (process_command_line:"*powe`

PowerUpSQL.ps1

KQL:
`event.category:"process" AND process_name:"powershell.exe" AND (process_command_line:"*PowerUpSQL.ps1" OR (process_command_line:"*p`

Lucene:
`event.category:"process" AND process_name:"powershell.exe" AND (process_command_line:"*PowerUpSQL.ps1" OR (process_command_line:"*p`

WinPEASx64.exe

KQL: `event.category:"process" AND (process_name:"WinPEASx64.exe" OR file_name:"WinPEASx64.exe")`

Lucene: `event.category:"process" AND (process_name:"WinPEASx64.exe" OR file_name:"WinPEASx64.exe")`

Certify.exe

KQL: `event.category:"process" AND (process_name:"Certify.exe" OR file_name:"Certify.exe")`

Lucene: `event.category:"process" AND (process_name:"Certify.exe" OR file_name:"Certify.exe")`

SharpWMI.exe

KQL: `event.category:"process" AND (process_name:"SharpWMI.exe" OR file_name:"SharpWMI.exe")`

Lucene: `event.category:"process" AND (process_name:"SharpWMI.exe" OR file_name:"SharpWMI.exe")`

HFS.exe

KQL: `event.category:"process" AND (process_name:"HFS.exe" OR file_name:"HFS.exe")`

Lucene: `event.category:"process" AND (process_name:"HFS.exe" OR file_name:"HFS.exe")`

MS-RPRN.exe

KQL: `event.category:"process" AND (process_name:"MS-RPRN.exe" OR file_name:"MS-RPRN.exe")`

Lucene: `event.category:"process" AND (process_name:"MS-RPRN.exe" OR file_name:"MS-RPRN.exe")`

hfs.exe

KQL: `event.category:"process" AND (process_name:"hfs.exe" OR file_name:"hfs.exe")`

Lucene: `event.category:"process" AND (process_name:"hfs.exe" OR file_name:"hfs.exe")`

PetitPotam.exe

KQL: `event.category:"process" AND (process_name:"PetitPotam.exe" OR file_name:"PetitPotam.exe")`

Lucene: `event.category:"process" AND (process_name:"PetitPotam.exe" OR file_name:"PetitPotam.exe")`

powercat.ps1

KQL:
`event.category:"process" AND process_name:"powershell.exe" AND (process_command_line:"*powercat.ps1" OR (process_command_line:"*pow`

Lucene:
`event.category:"process" AND process_name:"powershell.exe" AND (process_command_line:"*powercat.ps1" OR (process_command_line:"*pow`

NetCease.ps1

KQL:
`event.category:"process" AND process_name:"powershell.exe" AND (process_command_line:"*NetCease.ps1" OR (process_command_line:"*pow`

Lucene:
`event.category:"process" AND process_name:"powershell.exe" AND (process_command_line:"*NetCease.ps1" OR (process_command_line:"*pow`

ADACLScan.ps1

KQL:
`event.category:"process" AND process_name:"powershell.exe" AND (process_command_line:"*ADACLScan.ps1" OR (process_command_line:"*pc`

Lucene:
`event.category:"process" AND process_name:"powershell.exe" AND (process_command_line:"*ADACLScan.ps1" OR (process_command_line:"*pc`

Mimikatz

KQL: `event.category:"process" AND (process_name:"mimikatz.exe" OR file_name:"mimikatz.exe")`

Lucene: `event.category:"process" AND (process_name:"mimikatz.exe" OR file_name:"mimikatz.exe")`

LaZagne.exe

KQL: `event.category:"process" AND (process_name:"LaZagne.exe" OR file_name:"LaZagne.exe")`

Lucene: `event.category:"process" AND (process_name:"LaZagne.exe" OR file_name:"LaZagne.exe"`

SafetyKatz und BetterSafetyKatz

KQL:
`event.category:"process" AND (process_name:"SafetyKatz.exe" OR process_name:"BetterSafetyKatz.exe" OR file_name:"SafetyKatz.exe" OR`

Lucene:
`event.category:"process" AND (process_name:"SafetyKatz.exe" OR process_name:"BetterSafetyKatz.exe" OR file_name:"SafetyKatz.exe" OR`

Erkennung von SharpKatz und pypykatz

KQL:
`event.category:"process" AND (process_name:"SharpKatz.exe" OR process_name:"pypykatz.exe" OR file_name:"SharpKatz.exe" OR file_name`

Lucene:

```
event.category:"process" AND (process_name:"SharpKatz.exe" OR process_name:"pypykatz.exe" OR file_name:"SharpKatz.exe" OR file_name
```

procdump und minidump

KQL:
```
event.category:"process" AND (process_name:"procdump.exe" OR process_name:"minidump.exe" OR file_name:"procdump.exe" OR file_name:"
```

Lucene:
```
event.category:"process" AND (process_name:"procdump.exe" OR process_name:"minidump.exe" OR file_name:"procdump.exe" OR file_name:"
```

Snaffler.exe, SharpHound, BloodHound, PurpleKnight, BeRoot

KQL:
```
(process_name:"Snaffler.exe" OR process_name:"SharpHound.exe" OR process_name:"BloodHound.exe" OR process_name:"PurpleKnight.exe" O
```

Lucene:
```
(process_name:"Snaffler.exe" OR process_name:"SharpHound.exe" OR process_name:"BloodHound.exe" OR process_name:"PurpleKnight.exe" O
```

Windows File Transfer

Verdächtige Dateiübertragung über SMB (Server Message Block)

KQL:
```
event.category:"network" AND network_direction:"outbound" AND (destination_port:445 OR destination_port:139) AND (file_name:"*.exe"
```

Lucene:
```
event.category:"network" AND network_direction:"outbound" AND (destination_port:445 OR destination_port:139) AND (file_name:"*.exe"
```

Verdächtige Dateiübertragung über FTP (File Transfer Protocol)

KQL:
```
event.category:"network" AND network_direction:"outbound" AND destination_port:21 AND (file_name:"*.exe" OR file_name:"*.dll" OR fi
```

Lucene:
```
event.category:"network" AND network_direction:"outbound" AND destination_port:21 AND (file_name:"*.exe" OR file_name:"*.dll" OR fi
```

Verdächtige Dateiübertragung über HTTP/HTTPS

KQL:
```
event.category:"network" AND (destination_port:80 OR destination_port:443) AND (file_name:"*.exe" OR file_name:"*.dll" OR file_name
```

Lucene:
```
event.category:"network" AND (destination_port:80 OR destination_port:443) AND (file_name:"*.exe" OR file_name:"*.dll" OR file_name
```

Verdächtige Dateiübertragung über PowerShell Remoting

KQL:
```
event.category:"process" AND process_name:"powershell.exe" AND (process_command_line:"*-EncodedCommand*" OR process_command_line:"*
```

Lucene:
```
event.category:"process" AND process_name:"powershell.exe" AND (process_command_line:"*-EncodedCommand*" OR process_command_line:"*
```

Verdächtige Dateiübertragung über Remote Desktop Protocol (RDP)

KQL:
```
event.category:"network" AND network_direction:"outbound" AND destination_port:3389 AND (file_name:"*.exe" OR file_name:"*.dll" OR
```

Lucene:
```
event.category:"network" AND network_direction:"outbound" AND destination_port:3389 AND (file_name:"*.exe" OR file_name:"*.dll" OR
```

Verdächtige Dateiübertragung über Windows Management Instrumentation (WMI)

KQL:
```
event.category:"process" AND process_name:"wmiprvse.exe" AND (process_command_line:"*CopyTo*" OR process_command_line:"*Create*" OR
```

Lucene:
```
event.category:"process" AND process_name:"wmiprvse.exe" AND (process_command_line:"*CopyTo*" OR process_command_line:"*Create*" OR
```

Verdächtige Dateiübertragung über SMB mittels Windows-Freigaben

KQL:
```
event.category:"network" AND network_direction:"outbound" AND (destination_port:445 OR destination_port:139) AND (file_name:"*.exe"
```

Lucene:
```
event.category:"network" AND network_direction:"outbound" AND (destination_port:445 OR destination_port:139) AND (file_name:"*.exe"
```

Verdächtige Dateiübertragung über HTTP/HTTPS mit einem POST-Request

KQL:
```
event.category:"network" AND (destination_port:80 OR destination_port:443) AND (http_request_method:"POST" OR http_request_method:"
```

Lucene:
```
event.category:"network" AND (destination_port:80 OR destination_port:443) AND (http_request_method:"POST" OR http_request_method:"
```

Verdächtige Dateiübertragung über TFTP (Trivial File Transfer Protocol)

KQL:
```
event.category:"network" AND network_direction:"outbound" AND destination_port:69 AND (file_name:"*.exe" OR file_name:"*.dll" OR fi
```

Lucene:
```
event.category:"network" AND network_direction:"outbound" AND destination_port:69 AND (file_name:"*.exe" OR file_name:"*.dll" OR fi
```

Linux File Transfer Angriffe

Verdächtige Dateiübertragung über SSH (Secure Shell)

KQL: `event.category:"network" AND destination_port:22 AND (file_name:"*.exe" OR file_name:"*.dll" OR file_name:"*.zip")`

Lucene: `event.category:"network" AND destination_port:22 AND (file_name:"*.exe" OR file_name:"*.dll" OR file_name:"*.zip")`

Verdächtige Dateiübertragung über FTP (File Transfer Protocol)

KQL: `event.category:"network" AND destination_port:21 AND (file_name:"*.exe" OR file_name:"*.dll" OR file_name:"*.zip")`

Lucene: `event.category:"network" AND destination_port:21 AND (file_name:"*.exe" OR file_name:"*.dll" OR file_name:"*.zip")`

Verdächtige Dateiübertragung über SCP (Secure Copy Protocol)

KQL:
```
event.category:"network" AND destination_port:22 AND (file_name:"*.exe" OR file_name:"*.dll" OR file_name:"*.zip") AND (event.actio
```

Lucene:
```
event.category:"network" AND destination_port:22 AND (file_name:"*.exe" OR file_name:"*.dll" OR file_name:"*.zip") AND (event.actio
```

Verdächtige Dateiübertragung über HTTP/HTTPS mit wget oder curl

KQL:
```
event.category:"process" AND (process_name:"wget" OR process_name:"curl") AND (process_command_line:"*.exe" OR process_command_line
```

Lucene:
```
event.category:"process" AND (process_name:"wget" OR process_name:"curl") AND (process_command_line:"*.exe" OR process_command_line
```

Verdächtige Dateiübertragung über SCP mit rsync

KQL:
```
event.category:"process" AND (process_name:"scp" OR process_name:"rsync") AND (process_command_line:"*-P*" OR process_command_line:
```

Lucene:
```
event.category:"process" AND (process_name:"scp" OR process_name:"rsync") AND (process_command_line:"*-P*" OR process_command_line:
```

Verdächtige Dateiübertragung über SFTP (Secure FTP)

KQL: `event.category:"network" AND destination_port:22 AND (file_name:"*.exe" OR file_name:"*.dll" OR file_name:"*.zip")`

Lucene: `event.category:"network" AND destination_port:22 AND (file_name:"*.exe" OR file_name:"*.dll" OR file_name:"*.zip")`

Verdächtige Dateiübertragung über SMB (Server Message Block) aus Linux heraus

KQL:
```
event.category:"network" AND network_direction:"outbound" AND (destination_port:445 OR destination_port:139) AND (file_name:"*.exe"
```

Lucene:

```
event.category:"network" AND network_direction:"outbound" AND (destination_port:445 OR destination_port:139) AND (file_name:"*.exe"
```

Verdächtige Dateiübertragung über FTP (File Transfer Protocol) aus Linux heraus

KQL:

```
event.category:"network" AND network_direction:"outbound" AND destination_port:21 AND (file_name:"*.exe" OR file_name:"*.dll" OR fi
```

Lucene:

```
event.category:"network" AND network_direction:"outbound" AND destination_port:21 AND (file_name:"*.exe" OR file_name:"*.dll" OR fi
```

Verdächtige Dateiübertragung über SCP (Secure Copy Protocol) aus Linux heraus

KQL:

```
event.category:"process" AND process_name:"scp" AND (process_command_line:"*-P*" OR process_command_line:"*-E*" OR process_command_
```

Lucene:

```
event.category:"process" AND process_name:"scp" AND (process_command_line:"*-P*" OR process_command_line:"*-E*" OR process_command_
```

Wichtige OSQuery Queries

Verdächtige Prozesse (z.B. für Mailserver, CMS, etc.)

```
SELECT * FROM processes WHERE name IN ('wp-login.php', 'xmlrpc.php', 'administrator/index.php', 'user/login');
```

Verdächtige Anmeldeversuche (z.B. für Mailserver)

```
SELECT * FROM last WHERE user NOT IN ('known_user1', 'known_user2') AND type = 'failed_login';
```

Verdächtige Dateiänderungen (z.B. für CMS-Plugins oder -Themes)

```
SELECT * FROM file_events WHERE target_path LIKE '/var/www/html/%' AND action = 'CREATED';
```

Verdächtige Netzwerkverbindungen (z.B. für C2-Infrastruktur)

```
SELECT * FROM process_open_sockets WHERE remote_address NOT IN ('known_good_ip1', 'known_good_ip2');
```

Verdächtige Autostart-Einträge (z.B. für Persistenz)

```
SELECT * FROM startup_items WHERE name NOT IN ('known_good_startup1', 'known_good_startup2');
```

Verdächtige Kernel-Module (z.B. für Rootkits)

```
SELECT * FROM kernel_modules WHERE name NOT IN ('known_good_module1', 'known_good_module2');
```

Verdächtige geplante Aufgaben (z.B. für Lateral Movement)

```
SELECT * FROM crontab WHERE command LIKE '%suspicious_command%';
```

Verdächtige Benutzer und Gruppen (z.B. für Privilege Escalation)

```
SELECT * FROM users WHERE uid < 1000 AND username NOT IN ('root', 'known_user');
```

Verdächtige Dateiberechtigungen (z.B. für Privilege Escalation)

```
SELECT * FROM file WHERE path LIKE '/etc/%' AND permissions != '0644';
```

Verdächtige Systemänderungen (z.B. für System Manipulation)

```
SELECT * FROM yara_events WHERE sig_group = 'malicious_activity';
```

Verdächtige SSH-Anmeldeversuche

```
SELECT * FROM last WHERE user NOT IN ('known_user1', 'known_user2') AND type = 'failed_ssh_login';
```

Verdächtige geladene Kernel-Erweiterungen (z.B. für macOS Rootkits)

```
SELECT * FROM kernel_extensions WHERE name NOT IN ('known_good_kext1', 'known_good_kext2');
```

Verdächtige Docker-Container

```
SELECT * FROM docker_containers WHERE state = 'running' AND image NOT IN ('known_good_image1', 'known_good_image2');
```

Verdächtige Browser-Erweiterungen

```
SELECT * FROM browser_extensions WHERE name NOT IN ('known_good_extension1', 'known_good_extension2');
```

Verdächtige geöffnete Ports

```
SELECT * FROM listening_ports WHERE port NOT IN (80, 443, 22) AND address != '127.0.0.1';
```

Verdächtige SUID- und SGID-Dateien

```
SELECT * FROM suid_bin WHERE path NOT IN ('/bin/su', '/usr/bin/sudo');
```

Verdächtige Windows-Dienste

`SELECT * FROM services WHERE start*type = 'AUTO*START' AND name NOT IN ('known*good*service1', 'known*good*service2');

Verdächtige Windows-Treiber

```
SELECT * FROM drivers WHERE name NOT IN ('known_good_driver1', 'known_good_driver2');
```

Verdächtige Windows-Registry-Änderungen

```
SELECT * FROM registry_events WHERE action = 'SET' AND path LIKE 'HKEY_LOCAL_MACHINE\SOFTWARE\%';
```

Verdächtige Windows-Ereignisprotokolle

```
SELECT * FROM windows_events WHERE event_id IN (4624, 4625) AND log_name = 'Security';
```

Verdächtige Datei-Hashes

```
SELECT * FROM hash WHERE path LIKE '/var/www/html/%' AND sha256 NOT IN ('known_good_hash1', 'known_good_hash2');
```

Verdächtige Windows-Aufgabenplaner-Aufgaben

```
SELECT * FROM scheduled_tasks WHERE enabled = 1 AND action NOT LIKE '%known_good_program%';
```

Verdächtige ACPI-Tabellen (potenzielle UEFI-Rootkits)

```
SELECT * FROM acpi_tables WHERE description NOT IN ('known_good_description1', 'known_good_description2');
```

Verdächtige Kernel-Integritätsprüfungen (Linux)

```
SELECT * FROM kernel_integrity WHERE attribute = 'IMA' AND status != 0;
```

Verdächtige Windows-Prefetch-Dateien (Programmausführung)

```
SELECT * FROM prefetch WHERE last_execution_time > NOW() - 86400 AND filename NOT IN ('known_good_program1.exe', 'known_good_progra
```

Verdächtige Hardware-Änderungen

```
SELECT * FROM hardware_events WHERE action = 'added';
```

Verdächtige Windows-Firewall-Regeln

```
SELECT * FROM windows_firewall_rules WHERE action = 'Allow' AND direction = 'Outbound' AND remote_ip != '0.0.0.0/0';
```

Verdächtige ELF-Header (potenzielle Linux-Malware)

```
SELECT * FROM elf_info WHERE entry = 'malicious_entry_point';
```

Verdächtige Windows-Datei-Streams (ADS)

```
SELECT * FROM ntfs_acl_permissions WHERE inherited = 0 AND type = 'Allow' AND principal = 'Everyone';
```

Verdächtige USB-Geräte

```
SELECT * FROM usb_devices WHERE vendor NOT IN ('known_good_vendor1', 'known_good_vendor2');
```

Verdächtige Netzwerkverbindungen (z.B. für C2-Aktivitäten)

```
SELECT * FROM process_open_sockets WHERE remote_address NOT IN ('known_good_ip1', 'known_good_ip2');
```

Verdächtige Prozesse, die von nicht autorisierten Benutzern gestartet wurden

```
SELECT * FROM processes WHERE username != 'known_good_user' AND start_time > NOW() - 3600;
```

Verdächtige Änderungen an sicherheitsrelevanten Dateien

```
SELECT * FROM file WHERE path IN ('/etc/passwd', '/etc/shadow') AND action = 'MODIFY';
```

Verdächtige DNS-Anfragen (z.B. für Domain Generation Algorithms - DGAs)

```
SELECT * FROM dns_resolvers WHERE query_domain LIKE '%.example.com';
```

Verdächtige Benutzeraktivitäten (z.B. für Benutzerüberwachung)

```
SELECT * FROM user_events WHERE event_type = 'login_failed' AND username NOT IN ('known_good_user1', 'known_good_user2');
```

Verdächtige Änderungen an Windows-Diensten

```
SELECT * FROM windows_services WHERE service_name NOT IN ('known_good_service1', 'known_good_service2') AND service_start_type != '
```

Verdächtige Zugriffsrechteänderungen in der Windows-Registry

```
SELECT * FROM windows_registry WHERE hive LIKE 'HKEY_LOCAL_MACHINE\Software\%' AND key_name LIKE '%malicious_key%' AND change_type
```

Verdächtige Änderungen an Windows-Dateien und Ordnern

```
SELECT * FROM windows_file_events WHERE path LIKE 'C:\Windows\%' AND change_type IN ('created', 'modified');
```

Verdächtige Prozesse mit ungewöhnlichen Elternprozessen

```
SELECT * FROM processes AS p1 WHERE p1.parent NOT IN (SELECT parent FROM processes WHERE name = 'known_good_process');
```

Verdächtige Inbound-Verbindungen auf unüblichen Ports

```
SELECT * FROM listening_ports WHERE remote_port NOT IN (80, 443, 22) AND address != '127.0.0.1';
```

Verdächtige Prozesse, die auf sensible Dateien zugreifen

```
SELECT DISTINCT p.pid, p.name, p.path, f.path AS accessed_file FROM processes AS p JOIN file_events AS f ON p.pid = f.pid WHERE f.a
```

Verdächtige Verbindungen zu bekannten Malware-IP-Adressen

```
SELECT DISTINCT p.pid, p.name, c.remote_address FROM process_open_sockets AS c JOIN processes AS p ON c.pid = p.pid WHERE c.remote_
```

Verdächtige Ausführung von Verschlüsselungstools (z.B. Ransomware)

```
SELECT * FROM processes WHERE name IN ('openssl', 'cryptsetup', 'TrueCrypt');
```

Verdächtige Registrierungseinträge für Autostart (Windows)

```
SELECT * FROM registry WHERE path LIKE 'HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run%' AND value_name NOT IN ('
```

Verdächtige Änderungen an kritischen Systemdateien

```
SELECT * FROM file WHERE path IN ('/bin/login', '/usr/bin/sudo') AND action = 'MODIFY';
```

Verdächtige PowerShell-Aktivitäten (Windows)

```
SELECT * FROM process_events WHERE name = 'powershell.exe' AND cmdline LIKE '%malicious_command%';
```

Verdächtige Linux-Verzeichnisberechtigungen

```
SELECT * FROM file WHERE path LIKE '/etc/%' AND permissions != '0644';
```

Verdächtige Windows-Ereignisanzeigen für fehlgeschlagene Anmeldeversuche

```
SELECT * FROM windows_events WHERE event_id = 4625 AND log_name = 'Security' AND event_type = 'failure';
```

Verdächtige DNS-Anfragen nach bekannten C2-Domains

```
SELECT * FROM dns_resolvers WHERE query_domain IN ('malicious-c2-domain1.com', 'malicious-c2-domain2.com');
```

Verdächtige Apache/Nginx-Webserver-Logs (z.B. SQL Injection)

```
SELECT * FROM file WHERE path LIKE '/var/log/apache/%' AND content LIKE '%SQL Injection%';
```

Verdächtige Registry-Änderungen (Windows)

```
SELECT * FROM registry WHERE action = 'modified' AND hive IN ('HKEY_LOCAL_MACHINE', 'HKEY_USERS') AND key_path LIKE '%Software\\Mic
```

Verdächtige Dienste mit offenen Netzwerkverbindungen

```
SELECT DISTINCT s.service_name, s.display_name, p.name AS process_name, c.local_address, c.local_port, c.remote_address, c.remote_p
```

Verdächtige Prozesse, die Dateien löschen

```
SELECT DISTINCT p.pid, p.name, f.path AS deleted_file FROM file_events AS f JOIN processes AS p ON f.pid = p.pid WHERE f.action = '
```

Verdächtige PowerShell-Aktivitäten mit obfusziertem Code

```
SELECT * FROM process_events WHERE name = 'powershell.exe' AND cmdline LIKE '%-enc%' OR cmdline LIKE '%-e%';
```

Verdächtige Windows-Ereignisanzeigen für erhöhte Privilegien

```
SELECT * FROM windows_events WHERE event_id IN (4688, 4648) AND log_name = 'Security' AND event_type = 'success';
```

Verdächtige Netzwerkaktivitäten außerhalb von Bürozeiten

```
SELECT DISTINCT c.pid, p.name, c.remote_address, c.remote_port FROM process_open_sockets AS c JOIN processes AS p ON c.pid = p.pid
```

Verdächtige Benutzeraktivitäten (z.B. Änderung von Benutzereinstellungen)

```
SELECT * FROM user_events WHERE event_type = 'user_modified_settings' AND username NOT IN ('known_good_user1', 'known_good_user2');
```

Verdächtige DNS-Anfragen nach ungewöhnlichen Subdomänen

```
SELECT * FROM dns_resolvers WHERE query_domain LIKE '%.malicious-domain.com';
```

Verdächtige Prozesse, die aus dem Temp-Verzeichnis starten

```
SELECT * FROM processes WHERE path LIKE '/tmp/%';
```

Verdächtige SUID-/SGID-Dateien

```
SELECT * FROM suid_bin WHERE path NOT LIKE '/usr/bin/sudo' AND path NOT LIKE '/bin/su';
```

Verdächtige Datei- oder Verzeichnisberechtigungsänderungen

```
SELECT * FROM file WHERE permissions != '0644' AND path NOT LIKE '/tmp/%';
```

Verdächtige Anwendungsaufrufe aus nicht vertrauenswürdigen Verzeichnissen

```
SELECT * FROM file WHERE path LIKE '/var/tmp/%' AND (ext = 'exe' OR ext = 'dll' OR ext = 'so');
```

Verdächtige Änderungen an der Windows-Firewall

```
SELECT * FROM windows_firewall_rules WHERE action = 'Allow' AND direction = 'Inbound' AND remote_ip != '0.0.0.0/0';
```

Verdächtige PowerShell-Aktivitäten mit Downloads aus dem Internet

```
SELECT * FROM process_events WHERE name = 'powershell.exe' AND cmdline LIKE '%Invoke-WebRequest%' OR cmdline LIKE '%Invoke-RestMeth
```

Verdächtige SMB/CIFS-Dateifreigaben und Zugriffe

```
SELECT * FROM smb_shares; SELECT * FROM smb_sessions WHERE share_name NOT IN ('IPC$', 'C$', 'ADMIN$');
```

Verdächtige Windows-Verwaltungsinstrumente (WMI, PSExec)

```
SELECT * FROM processes WHERE name IN ('wmiprvse.exe', 'psexesvc.exe', 'PsExec.exe');
```

Verdächtige Dateiänderungen in den Benutzerprofilen (Windows)

```
SELECT * FROM file WHERE path LIKE 'C:\\Users\\%\\AppData\\Roaming\\%' AND action = 'MODIFY';
```

Verdächtige Dateiübertragungen über FTP/SFTP

```
SELECT * FROM processes WHERE cmdline LIKE '%ftp%' OR cmdline LIKE '%sftp%';
```

Verdächtige Aktivitäten von Privilegierten Benutzern

```
SELECT * FROM users WHERE uid >= 1000 AND username IN ('admin', 'root') AND password_change_time > NOW() - 604800;
```

Verdächtige Apache/Nginx-Webserver-Logs (z.B. XSS-Angriffe)

```
SELECT * FROM file WHERE path LIKE '/var/log/apache/%' AND content LIKE '%<script>alert("XSS")</script>%';
```