Wazuh DQL Hunting Cheatsheet

Wazuh DQL Queries:

Detect Monero Cryptomining

```
data.win.system.process.name IN ["xmr-stak", "xmrig"]
```

Detect Petya, Mischa, and GoldenEye Ransomware Files

```
data.win.file.name LIKE "*petya*" OR data.win.file.name LIKE "*mischa*" OR data.win.file.name LIKE "*goldeneye*"`
```

Detect Authentication Failures

```
event.category = "authentication" AND event.outcome = "failure"
```

Detect Local File Inclusion in HTTP Request Body

```
data.http.request.body.content CONTAINS "/etc/passwd"
```

Detect Command Injection in HTTP Request Body

```
data.http.request.body.content CONTAINS ";"
```

Detect Binary Execution with Specific Arguments

```
data.win.file.extension = "exe" AND data.win.process.args IN ["-nop", "-exec"]
```

Detect PowerShell Downloads

```
data.win.process.name = "powershell.exe" AND data.win.process.args CONTAINS "DownloadString"
```

Detect Specific Windows Event Codes

```
event.code IN [4688, 4697, 7045]
```

Detect SQL Injection in HTTP Requests

```
data.http.request.body.content CONTAINS "UNION SELECT"
```

Detect HTTP 404 Status Codes

```
network.protocol = "http" AND data.http.response.status_code = "404"
```

Detect Antivirus Block Events

```
event.category = "antivirus" AND event.outcome = "block"
```

Detect Brute Force Attempts Based on Duration

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

Detect Unknown User Agents

```
NOT data.http.user_agent IN ["Chrome", "Firefox", "Safari", "Edge"]
```

Detect Access from Unusual Geolocations

```
NOT source.geo.country IN ["US", "DE", "FR", "GB"]
```

Detect Modifications in Critical Directories

```
data.win.file.path LIKE "/etc/*" AND event.action = "modified"
```

Detect Rare or Suspicious Processes

```
NOT data.win.process.name IN ["sshd", "httpd", "mysqld"]
```

Detect Kerberoasting

```
event.code = "4769" AND ticket.service = "krbtgt"
```

Detect Suspicious DLL Creations

```
data.win.file.extension = "dll" AND event.action = "created"
```

Detect Group Policy Changes

```
event.code = "5136" AND object.class = "groupPolicyContainer"
```

Detect Use of PowerShell Encoded Commands

```
data.win.process.name = "powershell.exe" AND data.win.process.args CONTAINS "-EncodedCommand"
```

File Access

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

IP Destination Match

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

Outbound Port Filtering

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

File Creation in Temp Directory

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

PowerShell Command Detection

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

Backdoor or Mimikatz Detection

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

Suspicious HTTP Content

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

PowerShell Core Command

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

DLL Creation Detection

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

Linux Authentication Failures

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

Bash Injection Attempts

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

SQL Injection in HTTP Requests

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

Root Activity Detection

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

HTTP Status Code Monitoring

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

Antivirus Alerts

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

Detection of Unauthorized AD Enumeration (e.g., BloodHound, ADRecon)

```
SELECT * FROM network_traffic WHERE destination.port IN (389, 445, 636, 3268, 3269) AND user_agent LIKE '%SharpHound%' OR process.n
```

Kerberoasting Attack Detection (Event ID 4769)

```
SELECT * FROM windows_events WHERE code = 4769 AND service.name LIKE '%krbtgt%';
```

Golden Ticket Activity Detection (Event ID 4672)

```
SELECT * FROM windows_events WHERE code = 4672 AND user.name = 'NT AUTHORITY\\SYSTEM';
```

Suspicious DCSync Activity (Event ID 4662)

```
SELECT * FROM windows_events WHERE code = 4662 AND object.access_mask = 'ControlAccess' AND object.name LIKE '%replication%';
```

Pass-the-Hash Detection

```
SELECT * FROM windows_events WHERE code = 4624 AND logon.type = 9;
```

NTLM Relay Attack Detection

```
SELECT * FROM network_traffic WHERE protocol = 'SMB' AND source.port = 445 AND destination.port = 445;
```

Malicious PowerShell Activity Related to AD

```
SELECT * FROM processes WHERE name = 'powershell.exe' AND args LIKE '%Get-Domain%' OR args LIKE '%Get-AD%';
```

Suspicious Group Membership Changes (Event ID 4728)

```
SELECT * FROM windows_events WHERE code = 4728 AND group.name = 'Domain Admins';
```

Unusual Service Account Activity (Event ID 4673)

```
SELECT * FROM windows_events WHERE code = 4673 AND user.account_type = 'service_account';
```

Enumeration of AD Objects with DSQuery

```
SELECT * FROM processes WHERE name = 'dsquery.exe' AND args LIKE '%domain%';
```

Certificate Authority Enumeration

```
SELECT * FROM network_traffic WHERE destination.port = 135 AND process.name = 'certutil.exe';
```

Abuse of Certificate Templates

```
SELECT * FROM windows_events WHERE code = 4886 AND object.name LIKE '%certificate%';
```

Certify Tool or Rubeus Enumeration Activity

```
SELECT * FROM processes WHERE name IN ('certify.exe', 'rubeus.exe') AND args LIKE '%/list%';
```

Certificate Request with Malicious SAN (Event ID 4888)

```
SELECT * FROM windows_events WHERE code = 4888 AND subject.alternative_name LIKE '%malicious%';
```

ADCS Exploitation Using ESC1 (Event ID 4887)

```
SELECT * FROM windows_events WHERE code = 4887 AND template.name LIKE '%VulnerableTemplate%';
```

Suspicious Certificate Renewal (Event ID 4890)

```
SELECT * FROM windows_events WHERE code = 4890 AND renewal_requester.name NOT LIKE '%authorized_user%';
```

Certificate Authority Configuration Changes (Event ID 4899)

```
SELECT * FROM windows_events WHERE code = 4899 AND object.name LIKE '%CA Configuration%';
```

Detection of Service Principal Name (SPN) Enumeration

```
SELECT * FROM windows_events WHERE code = 4769 AND service.class = 'SPN';
```

Failed Logins on AD Controllers (Event ID 4625)

```
SELECT * FROM windows_events WHERE code = 4625 AND source.hostname LIKE '%DC%';
```

Unusual Login Patterns on AD Controllers

```
SELECT * FROM windows_events WHERE code = 4624 AND logon.type IN (3, 10) AND source.hostname LIKE '%DC%';
```

DNS Recon Activity Against AD

```
SELECT * FROM dns_queries WHERE query LIKE '%_ldap._tcp.%';
```

Abuse of AD Replication (Event ID 4742)

```
SELECT * FROM windows_events WHERE code = 4742 AND object.name LIKE '%Replication Services%';
```