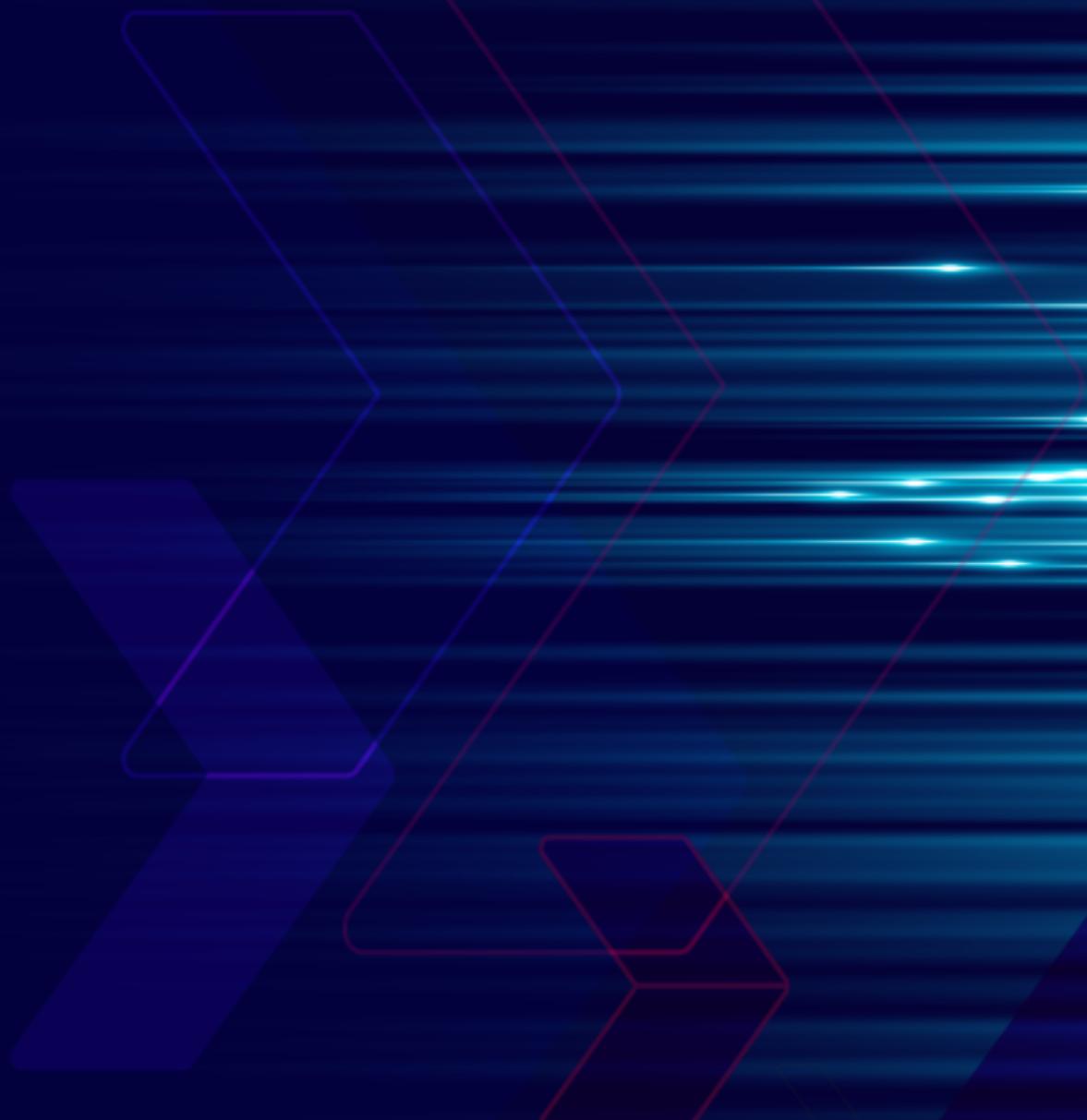


DQL Cheat Sheet

FOR ADRECON



Use Case	Example Query
Suspicious LDAP Scan on port 389	stream=sysmon-network where dstport="389" duration 1d groupby system,dstip,srcip,devsrcip,user limit 100 _checkif int_compare count_col1 >= 5 include
Suspicious Activity - Powershell Invoking CSC Executables	stream=sysmon-process where rlike(parentcommandline,"powershell.exe") and originalfilename="csc.exe" duration 1d groupby system,devsrcip,user limit 100
Suspicious Activity - Powershell Invoking CVTRES Executables	stream=sysmon-process where rlike(parentcommandline,"csc.exe") and originalfilename="CVTRES.EXE" duration 1d groupby system,devsrcip,user limit 100
Network Discovery via Powershell	stream=sysmon-dns where rlike(image,"powershell.exe") and querystatus="9003" and action="DNS_QUERY" duration 1d groupby system,devsrcip limit 100