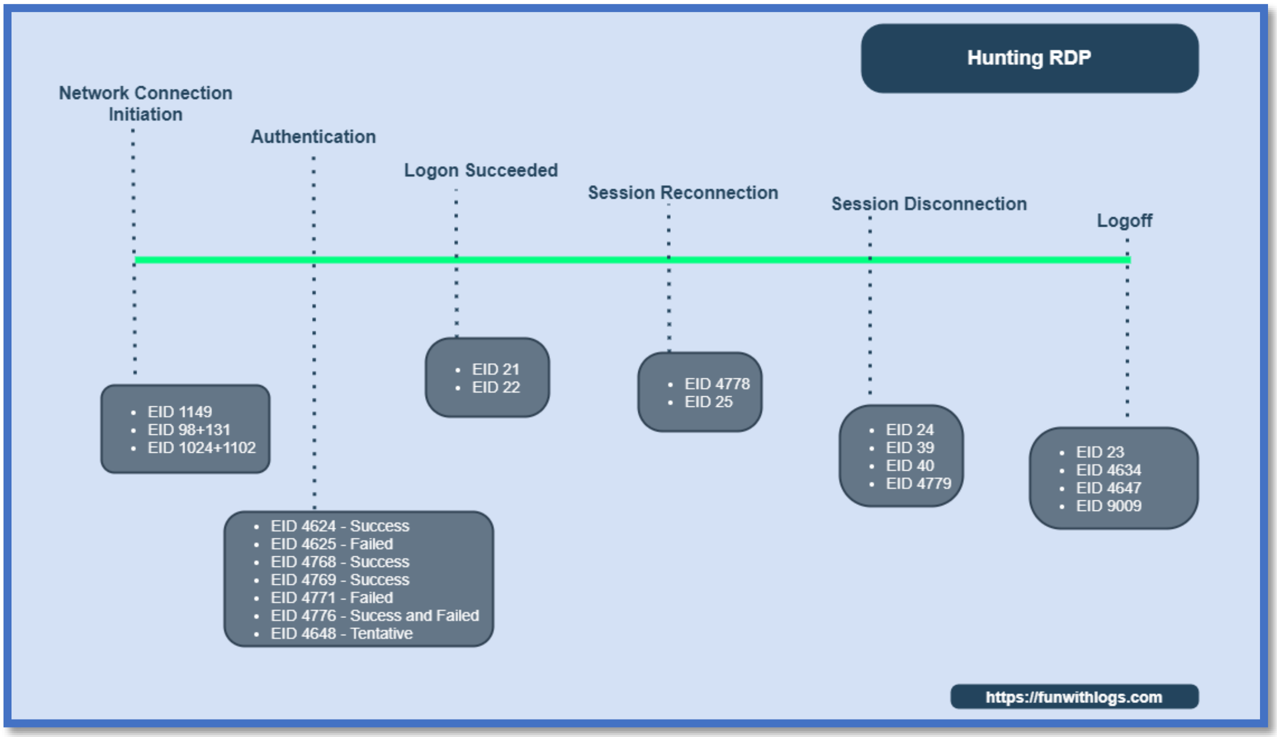
Cheat Sheet – Hunting RDP Activities



Evtx File	Event ID
Security.evtx	4624, 4625, 4634, 4647, 4771, 4776, 4768, 4769
Microsoft-Windows-TerminalServices-LocalSessionManager\Operational.evtx	21, 22, 23 24, 25
Microsoft-Windows-RemoteDesktopServices-RdpCoreTS%Operationnal.evtx	98, 131
Microsoft-Windows-TerminalServices-RDPClient/Operational.evtx	1024, 1102
Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational.evtx	1149
System.evtx	9009