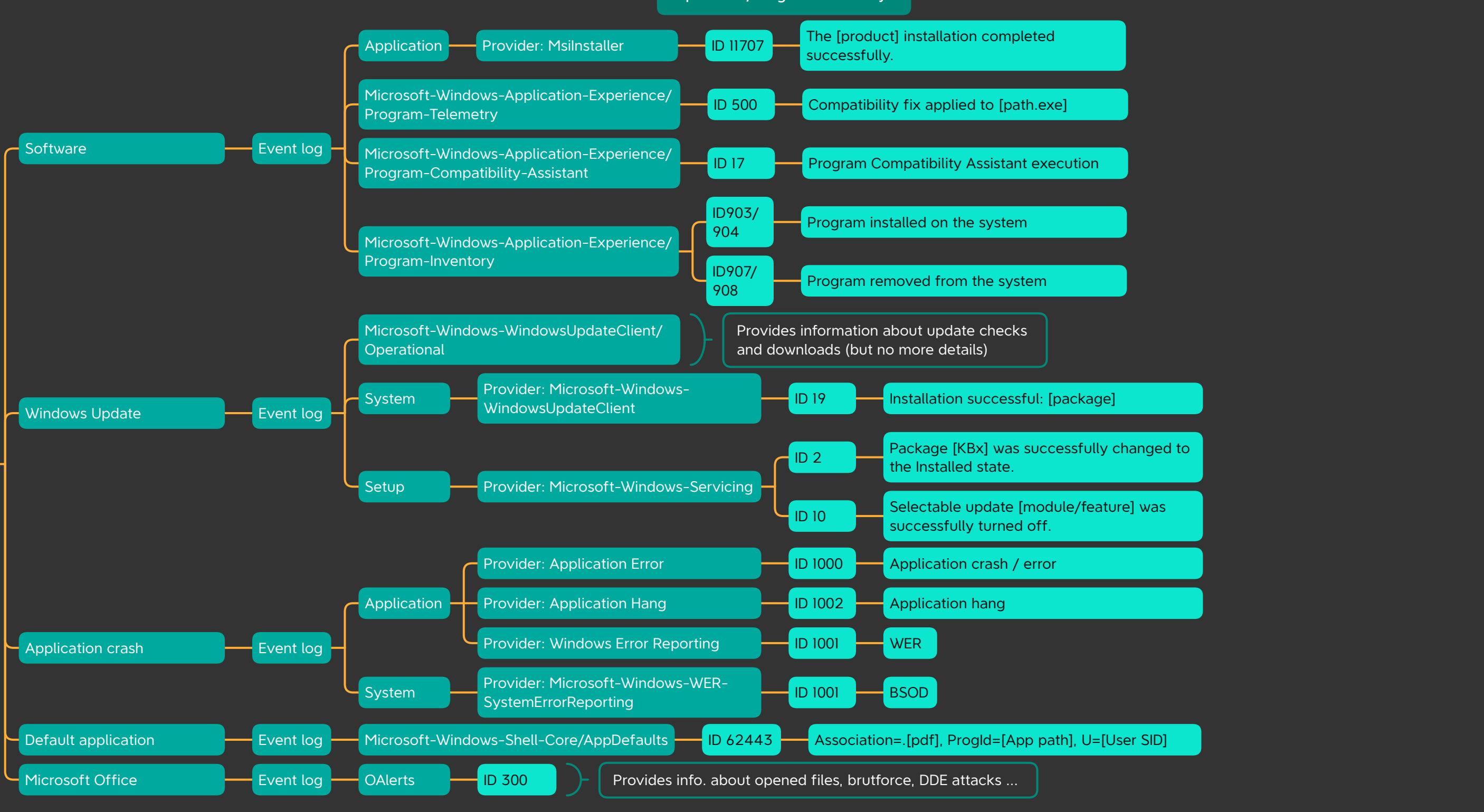


Windows event auditing reference

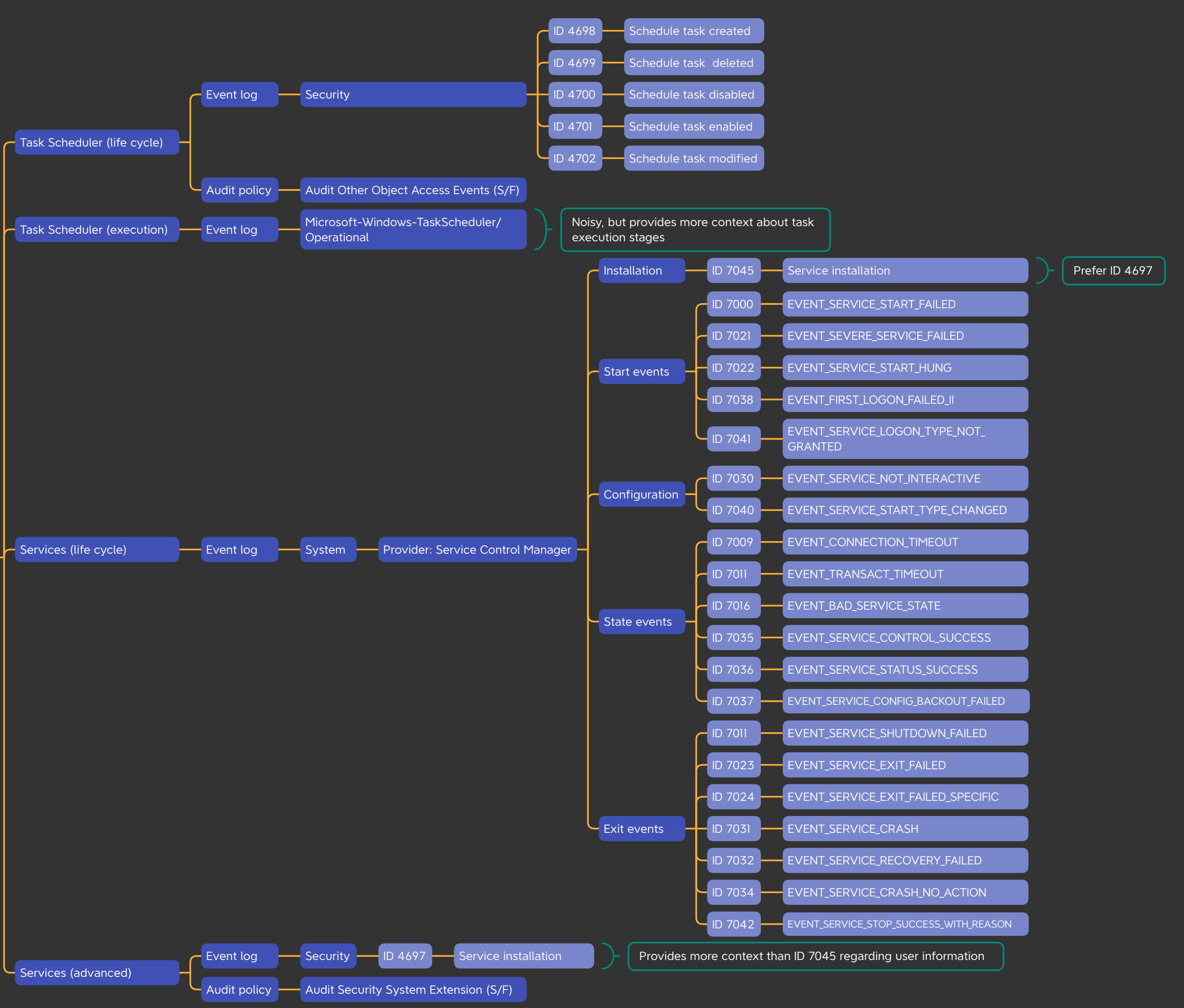
System  
Security  
Application

Classic event log

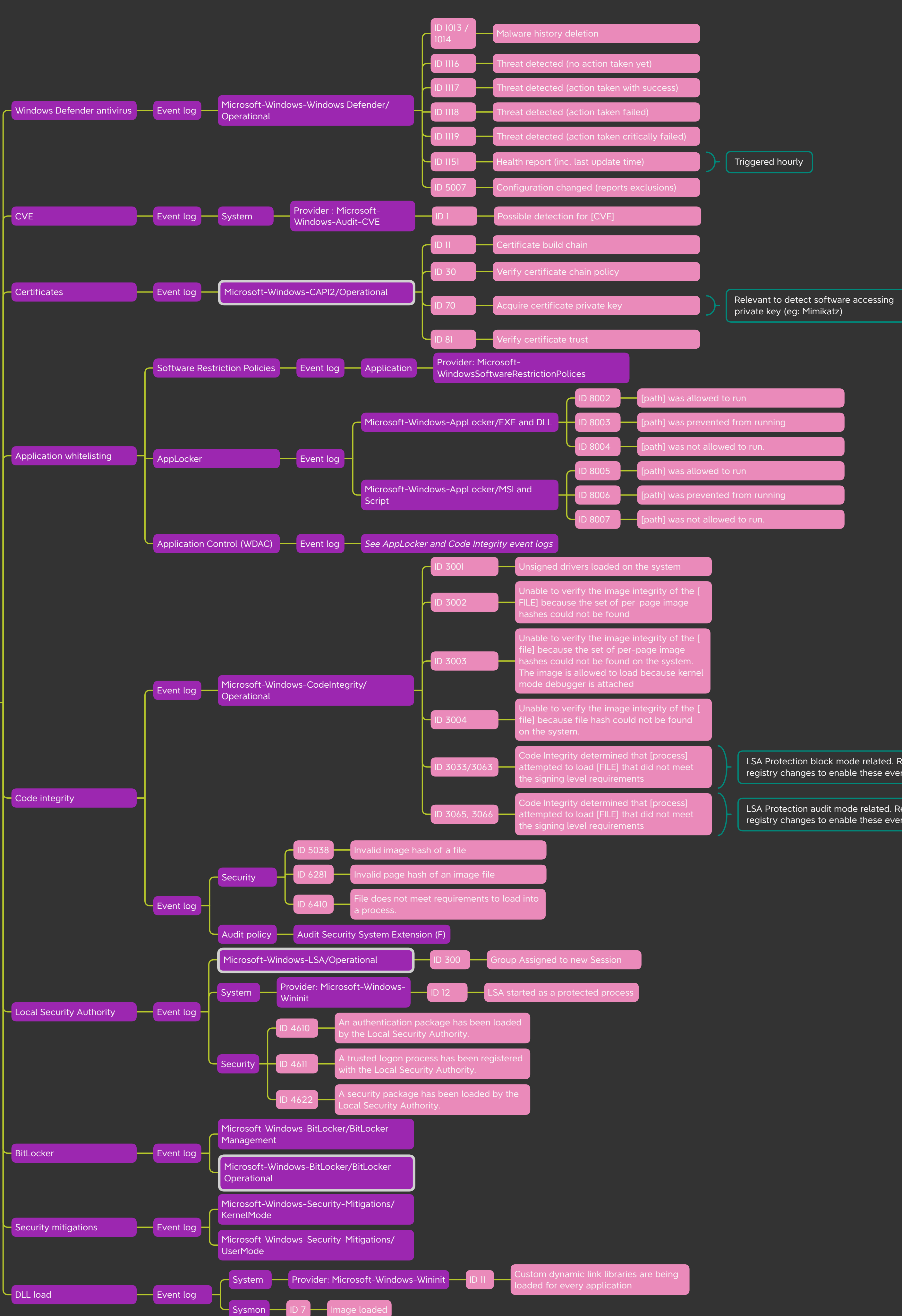
Application & Updates



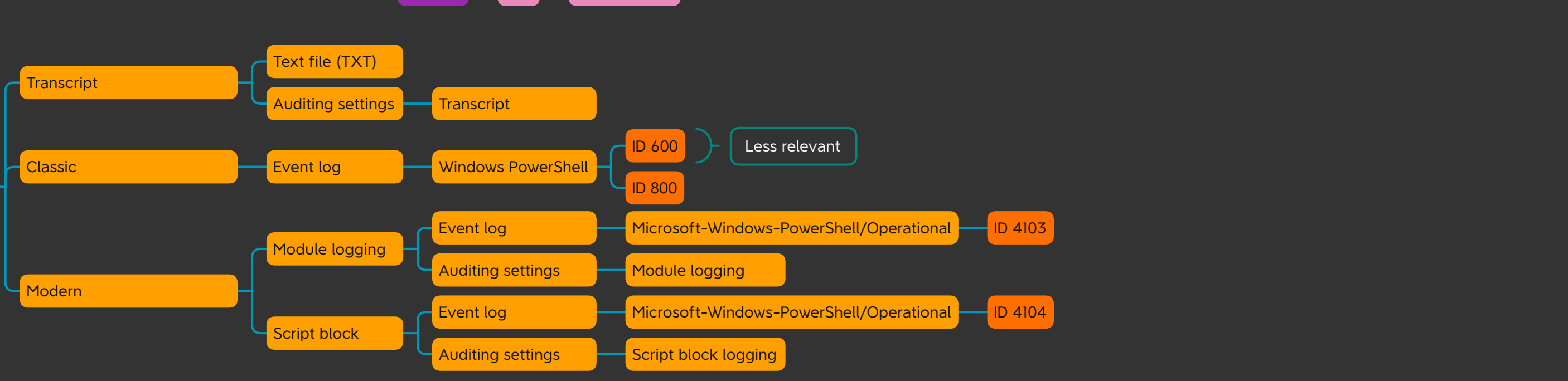
Task & Service



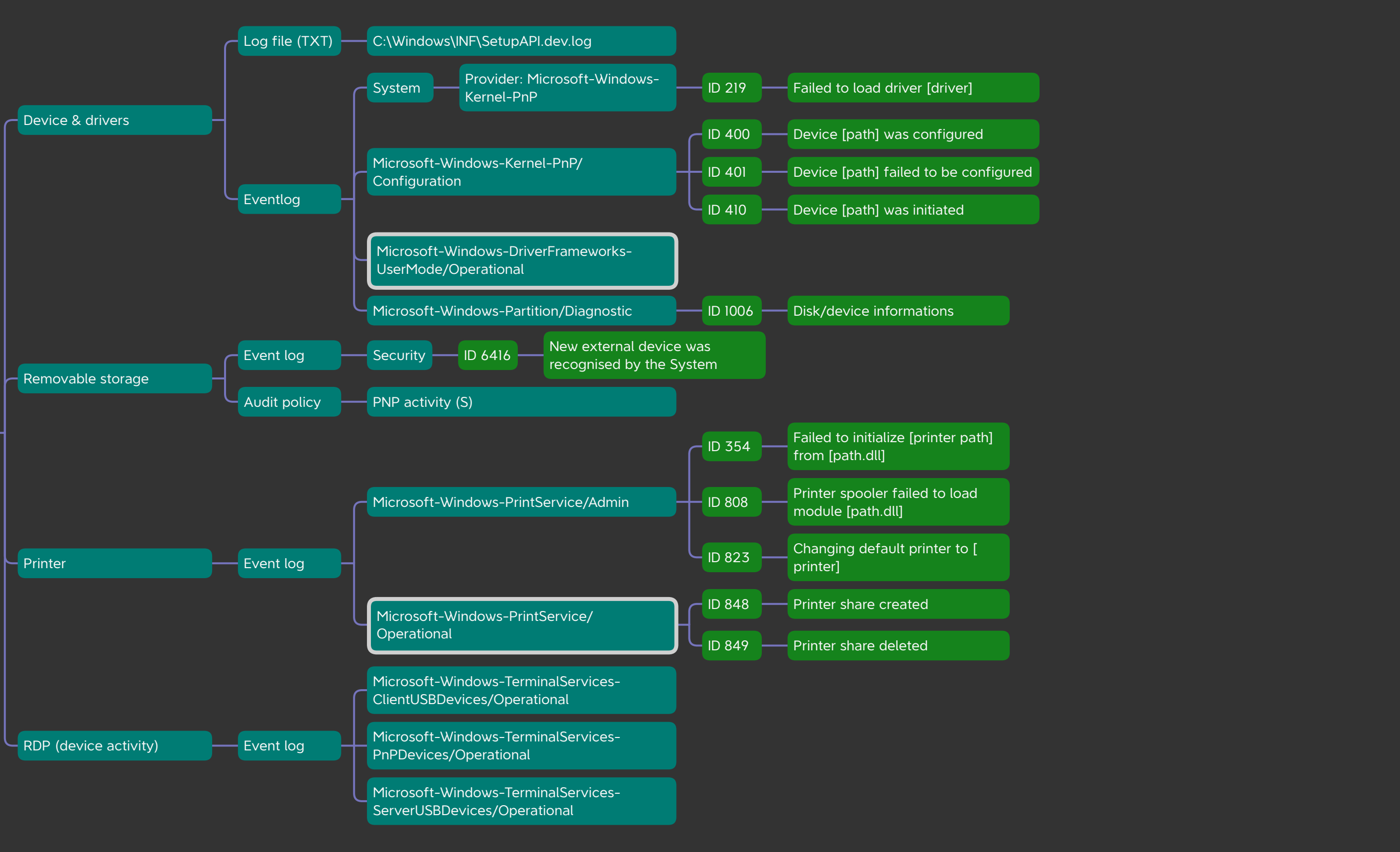
Security related



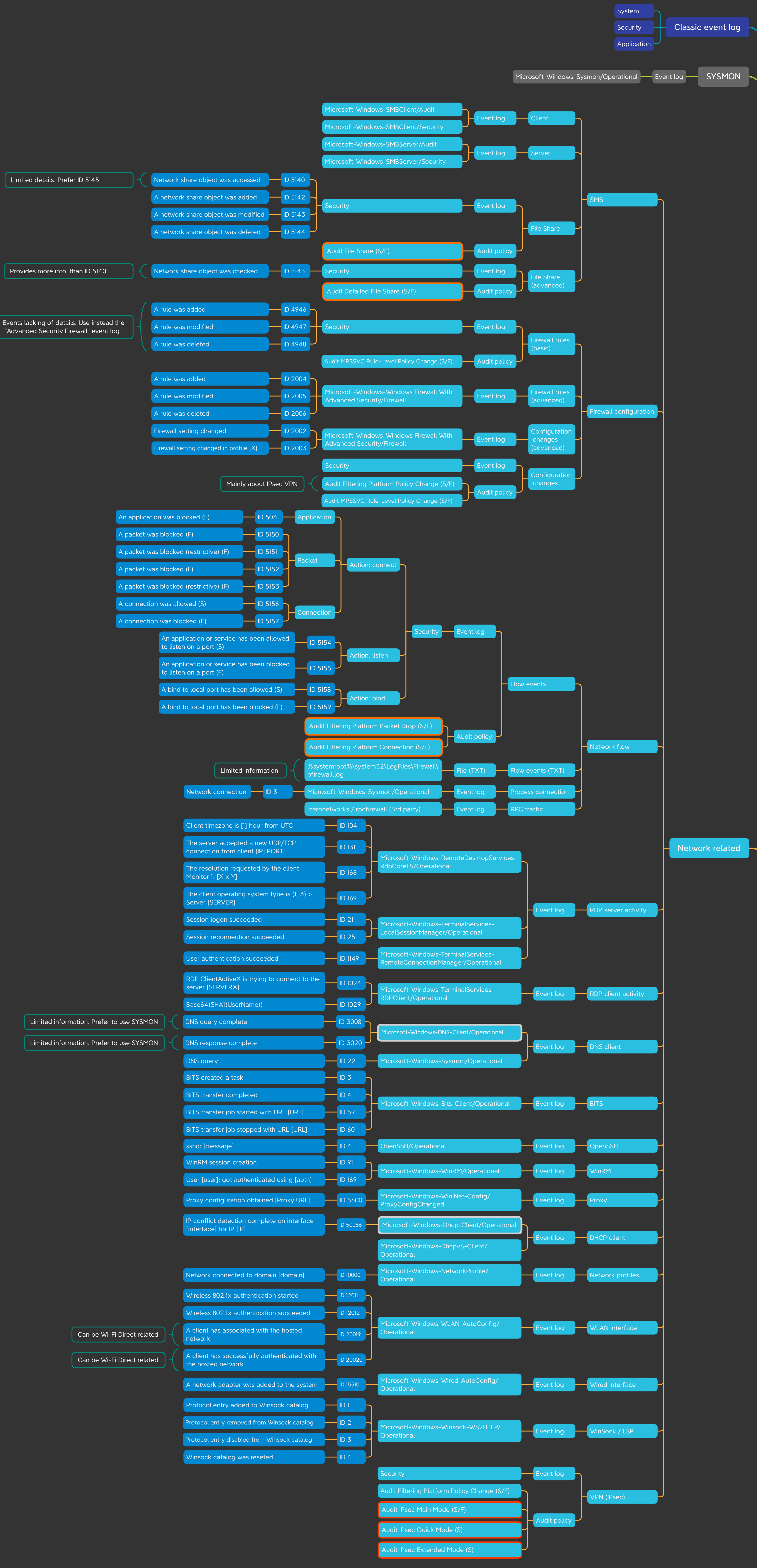
PowerShell



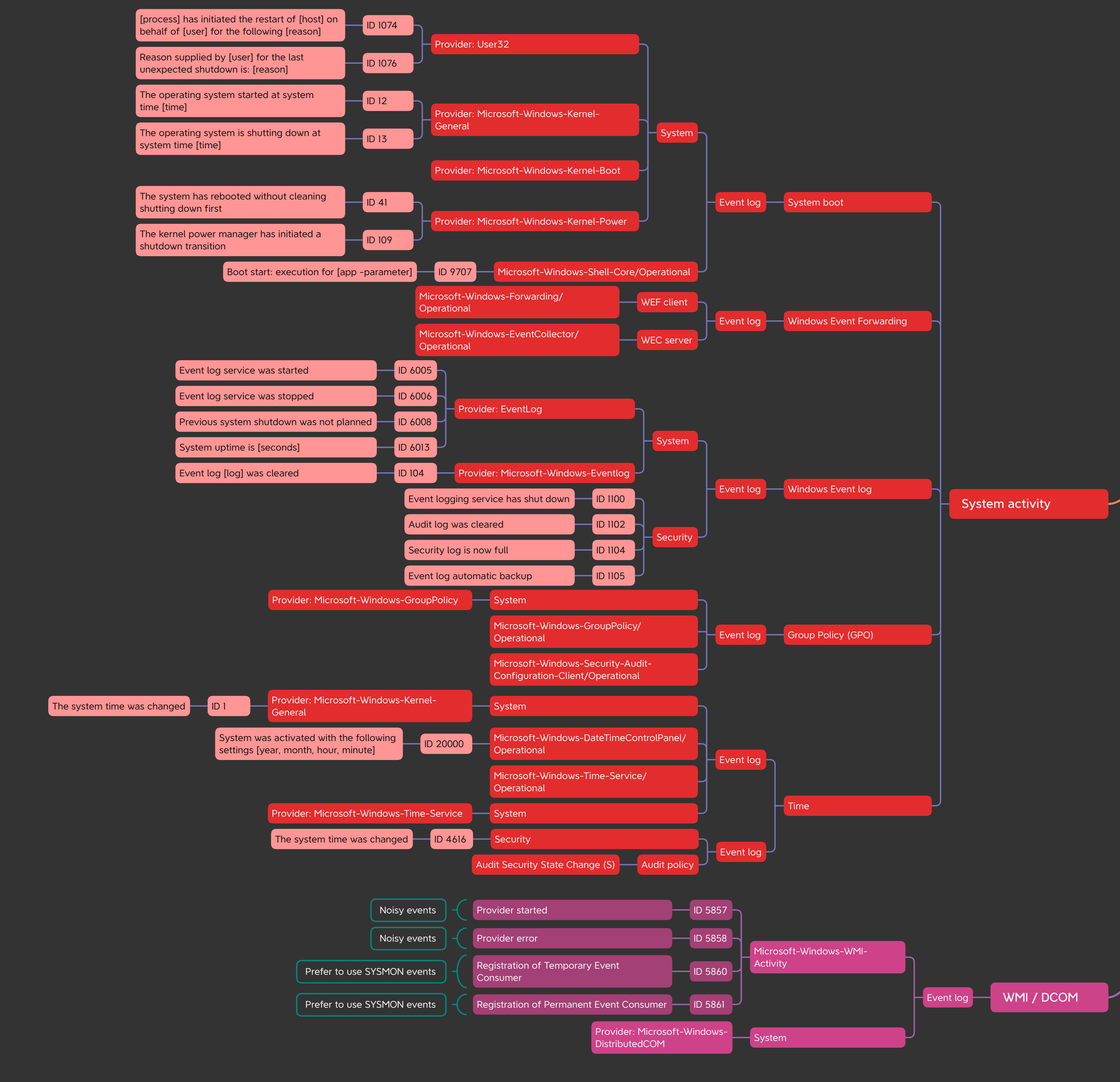
External device



Network related



System activity



Author: mdecrovoisier  
Version: 2022.05.05  
Status: stable

Noisy subcategory  
Disabled event log

SOURCES:  
- NSA guidance: <https://apps.nsa.gov/ia/chow/library/ia-guidance/security-configuration/applications/assets/public/upload/Spotting-the-Aversary-with-Windows-Event-Log-Monitoring.pdf>  
- Notable events: <https://github.com/TonyPhelps/SIEM/blob/master/Notable-Event-IDs.md#microsoft-windows-wmi-operational>  
- Event forwarding guidance: <https://github.com/haacyber/Event-Forwarding-Guidance/blob/master/Events/README.md>  
- WDAC/AppLocker/SRP: <https://4sysop.com/archives/application-whitelisting-software-restriction-policies-vs-applocker-vs-windows-defender-application-control/>