

Windows auditing baseline

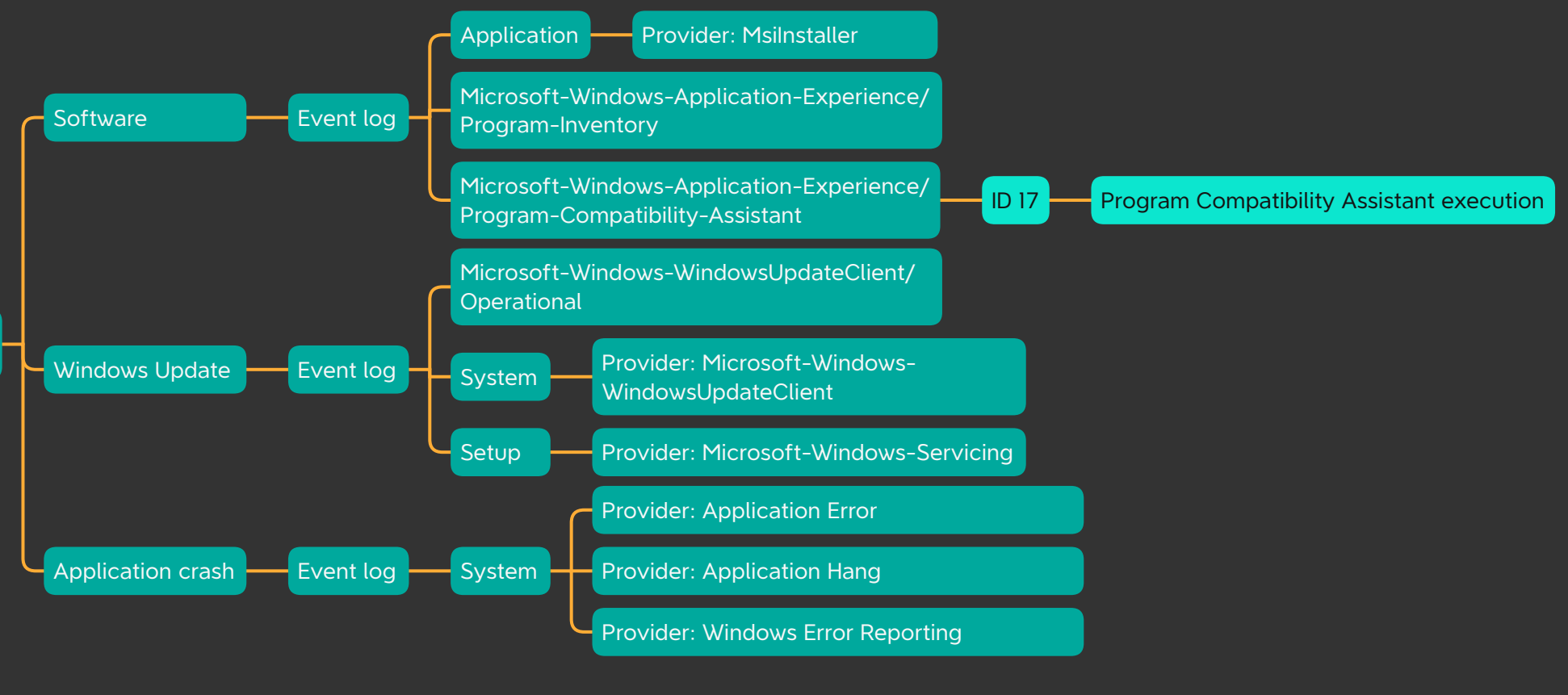
Classic event log

- System
- Security
- Application

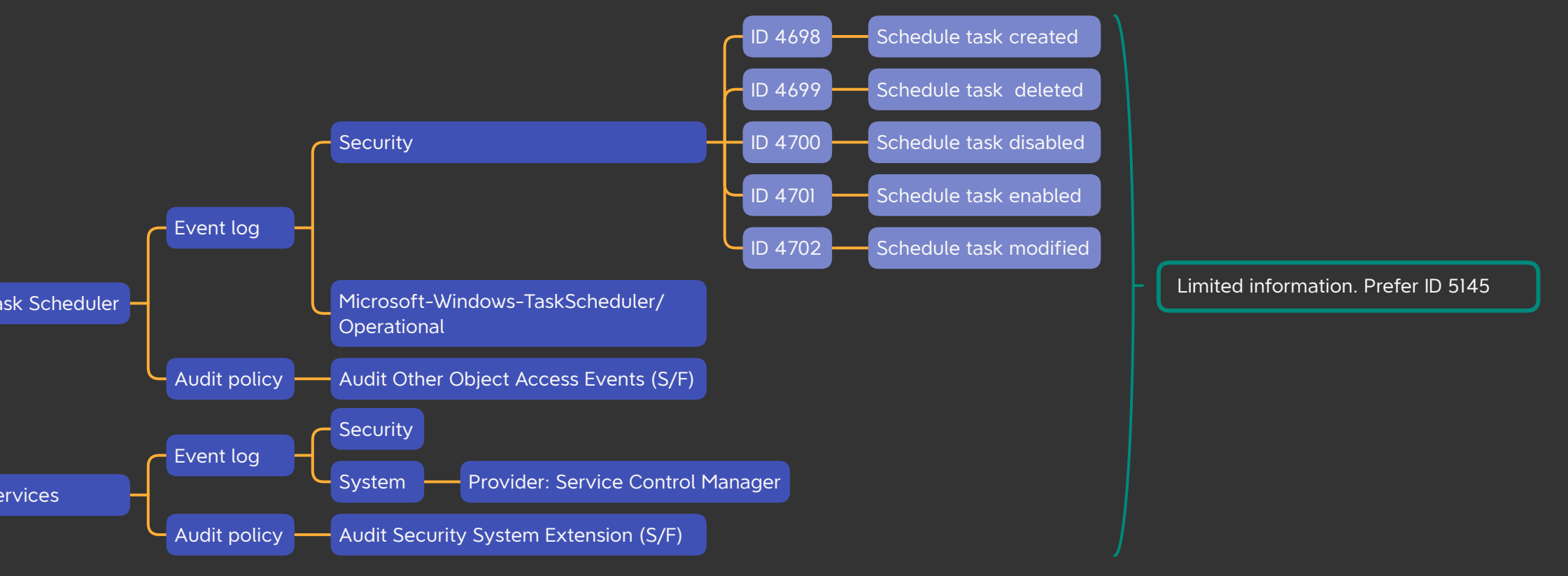
Microsoft-Windows-Sysmon/Operational Event log

**SYSMON**

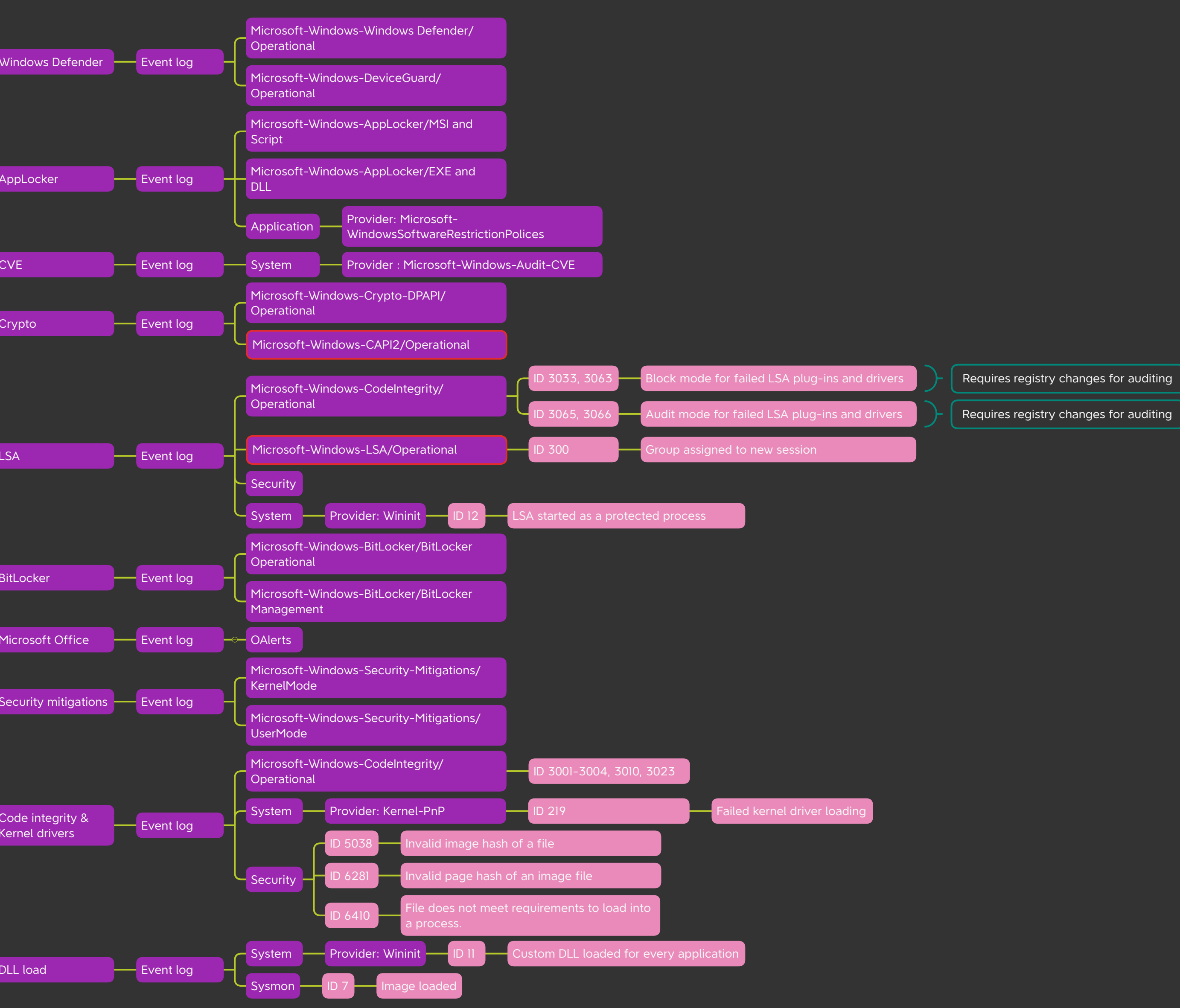
Software & Updates



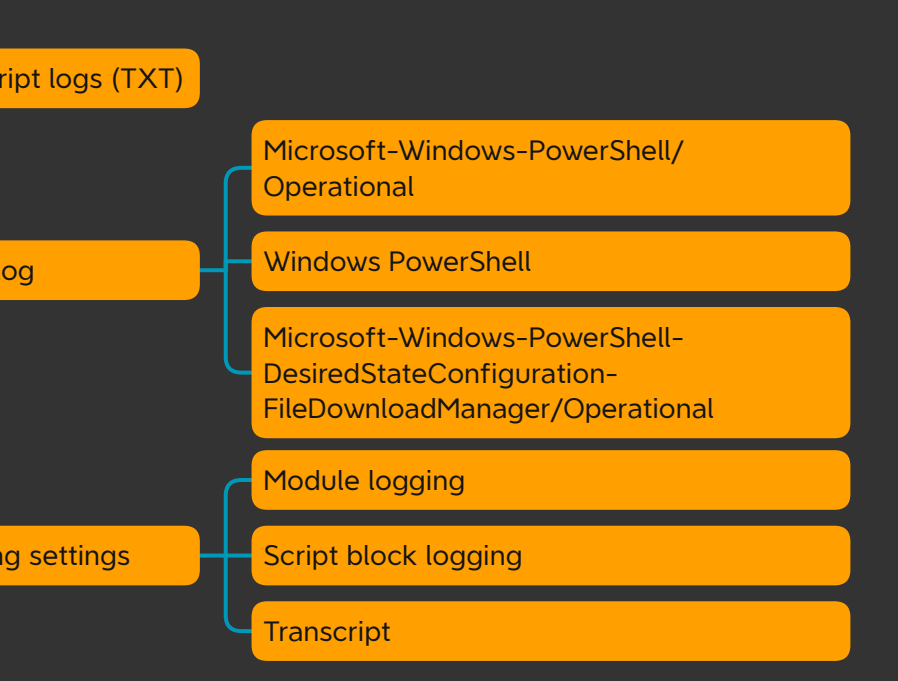
Task & Service



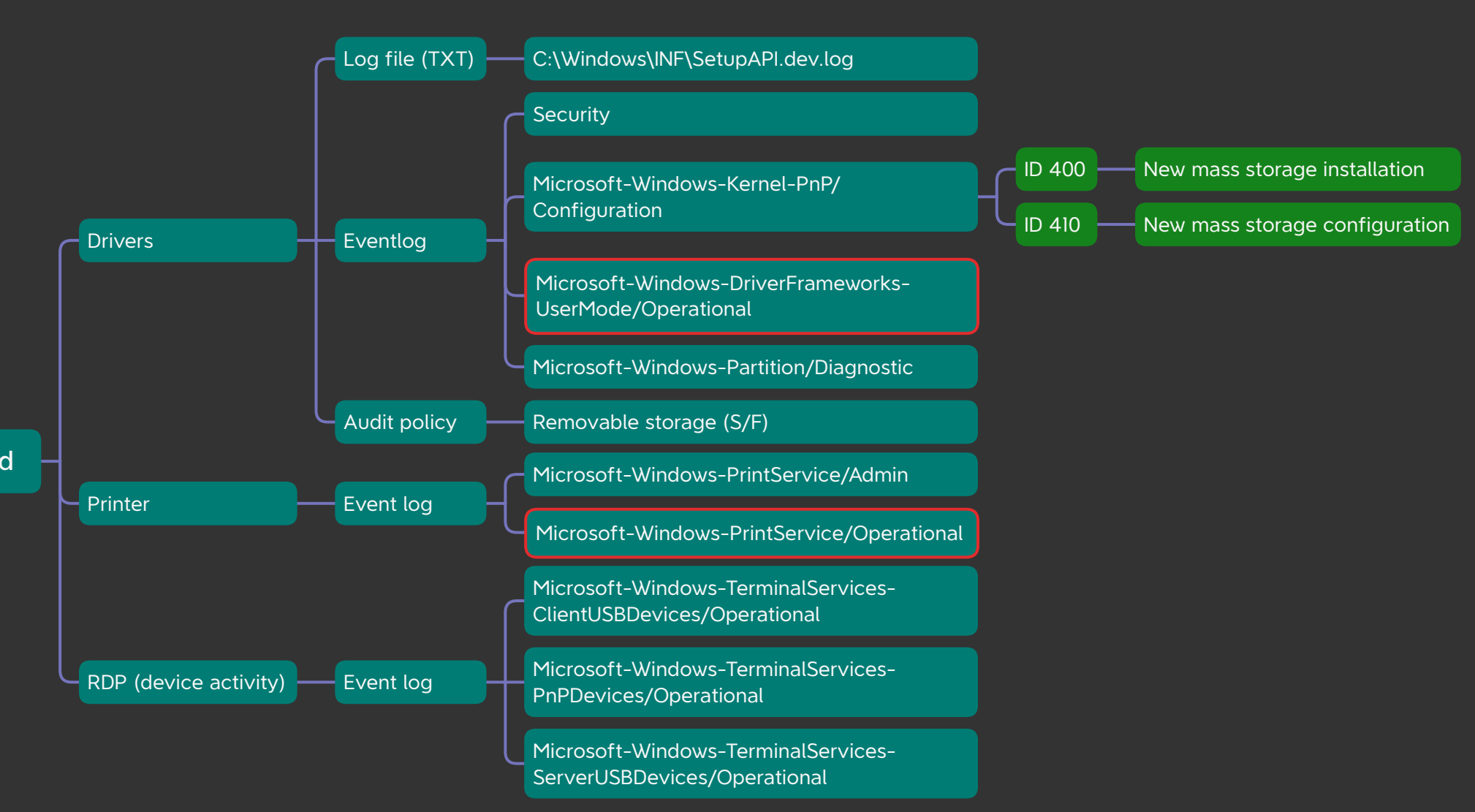
Security related



PowerShell



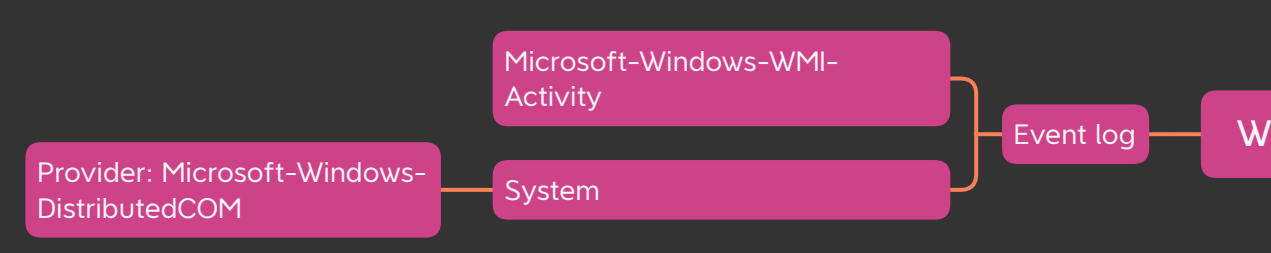
External device related



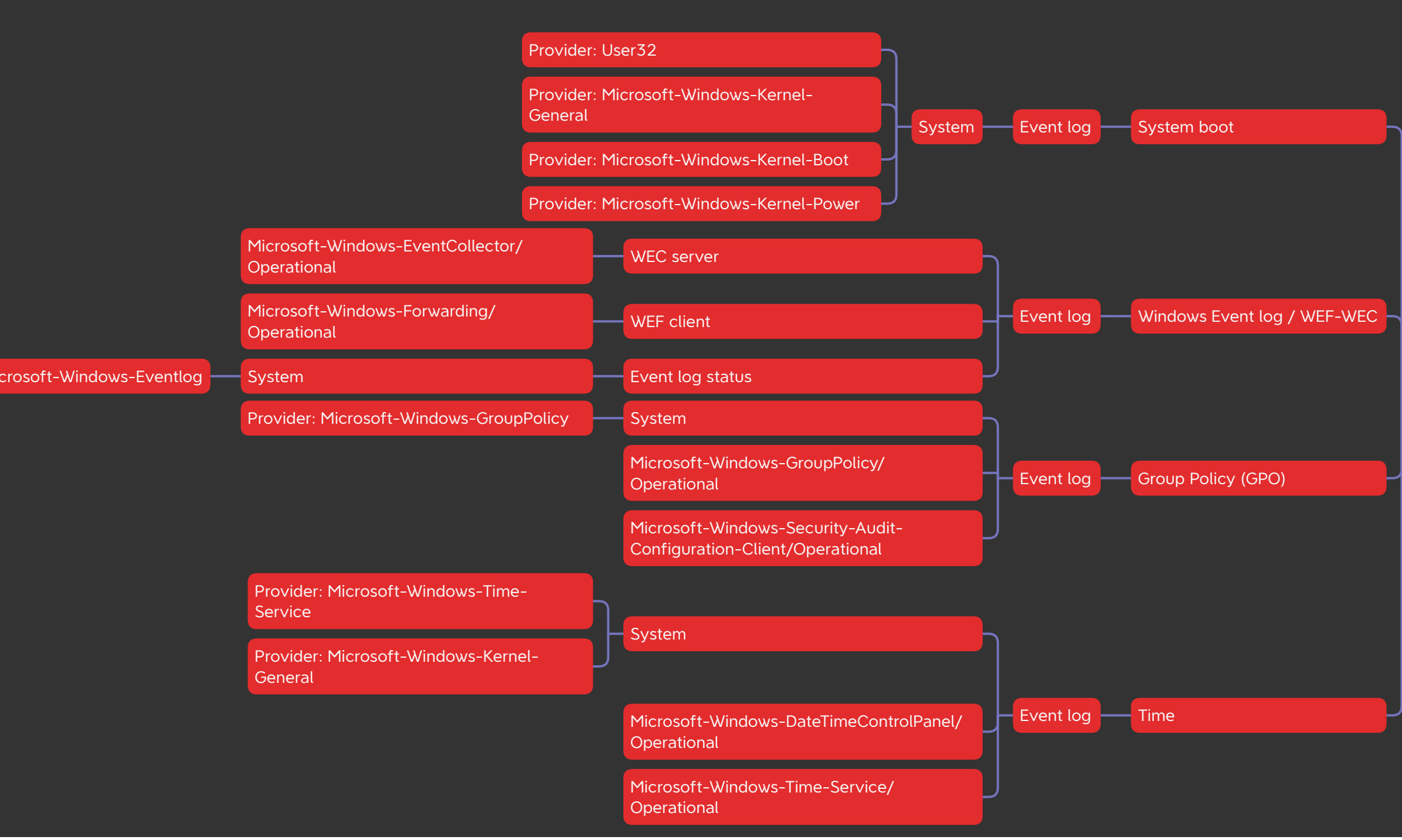
Network related



WMI / DCOM



System



Author: mdecrevoisier  
Version: 2022.04.15  
Status: stable

Disabled event log

Noisy subcategory