Padlock Trend

EventCode=6416 Device\_Name=\*Padlock\* | timechart count by Device\_Name span=1d

\*\* Look for any events that are related to Packlocks and Plug and Play Devices and display as daily trend\*\*

USB Trend

EventCode=6416 Device\_Name=\*USB\* | timechart count by Device\_Name span=1d

\*\*Look for any events that are related to USB and Plug and Play Devices and display as daily trend\*\*

Powershell used by Users

EventCode=4688 \*PowerShell\* Account\_Name!=\*$\* Account\_Name!=\*svc\* | table \_time, Account\_Name, Process\_Command\_Line, ComputerName

\*\*Display PowerShell usage, lookout for any flags that looks like –ExecutionPolicy Unrestricted or any –ExecutionPolicy as it is an attempt to elevate privileges\*\*

RDP User Logon Off Hours (Successful)

Sourcetype=\*WinEventLog:Security\* EventCode=4624 (((date\_hour>17 OR date\_hour < 6) AND (date\_wday!=\*sat\* OR date\_wday!=\*sun\*)) OR (date\_wday=\*sat\* OR date\_wday=\*sun\*)) (Account\_Name!=\*$\* AND Account\_Name!=\*svc\* Account\_Name!=”” Account\_Name!=\*ANONYMOUS\*) (Logon\_Type=8) | stats count by Account\_Name | table Account\_Name

\*\* Off Peak hours RDP logons \*\*

Unsuccessful Logon (4625)

EventCode=4625 sourcetype=\*WinEventLog:Security\* (Account\_Name!=\*$\* OR Account\_Name!=\*svc\*) | stats count by Account\_Name | sort – count

\*\* all non-service non-computer unsuccessful logons \*\*

Plug and Play (6416)

EventCode=6416 (Device\_Name!=\*HID\* AND Device\_Name!=\*Microsoft\*) | table \_time, Device\_Name, ComputerName, Account\_Name | stats count by Device\_Name | sort – count

\*\* All non-HID and non-Microsoft Plug and Play devices \*\*

Logoff Off Hours

Sourcetype=\*WinEventLog:Security\* EventCode=4647 (((date\_hour>17 OR date\_hour<6) AND (date\_wday!=\*sat\* OR date\_wday!=\*sun\*)) OR (date\_wday=\*sat\* OR date\_wday=\*sun\*)) (Account\_Name!=\*$\* AND Account\_Name!=\*svc\* Account\_Name!=”” Account\_Name!=\*ANONYMOUS\*) | stats count by Account\_Name | table Account\_Name

\*\* Logoff Off Hours (outside of standard business hours) that are user initiated \*\*

**Prior Dashboard Panels**

Audit Log Cleared (1102)

Sourcetype=\*WinEventLog:Security\* EventCode=1102 | rex field=Message ”Account\_Name:(?<AccountName>.\*)” | table EventCode,\_time,ComputerName,AccountName

Security Log Full (1104)

EventCode=1104 sourcetype=\*WinEventLog:Security\*

Event Logging Service Encountered (1108)

Sourcetype=\*WinEventLog:Security\*

EventCode=1108 | table EventCode, \_time, ComputerName, User

System Time Changes (4616)

Sourcetype=\*WinEventLog:Security\* EventCode=4616 (NOT \*svchost.exe\*) | table EventCode, \_time, ComputerName, Account\_Name

Permission on an object were changed (4670)

Sourcetype=\*WinEventLog:Security\* EventCode=4670 (NOT \*svchost.exe\* NOT \*Search had exer.exe\* NOT \*services.exe\*) | table EventCode,\_time,ComputerName,Account\_Name,Process\_Name