情報流出・持ち出し
index=windows_sysmon EventCode=11
"encrypt" OR
"exfil" OR
"upload" OR
"rclone" OR
"custom.exe"

・初期アクセス
index=*
| where like(Image,"%Downloads%") OR like(Image,"%Temp%") OR like(Image,"%AppData%")
| table _time Image CommandLine ParentImage Hashes ParentCommandLine

index=* EventCode=1
| where like(Image, "%Downloads%")
| sort _time
| table _time host Image CommandLine ParentImage Hashes User

Officeマクロ系（超危険）
.docm
.xlsm
.pptm
.dotm
.xlam

圧縮ファイル
.zip
.rar
.7z
.tar
.gz
.bz2
.iso
.img
.cab

実行ファイル系
.exe
.msi
.bat

.cmd
.com
.ps1
.psm1
.vbs
.vbe
.js
.jse
.wsf
.scr
.cpl
.hta

業務でよく使われる拡張子
.pdf
.doc
.docx
.xls
.xlsx
.ppt
.pptx
.txt
.csv
.jpg
.jpeg
.png
.gif

・転送
index= *EventCode=1 sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" (CommandLine="*urlcache*" OR CommandLine="*http*" OR CommandLine="*https*"*)
| table _time Image CommandLine Hashes User

・永続化
index=main sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational"
EventCode=1
Image="C:\Windows\Tasks*.exe"
| table _time ComputerName Image CommandLine ParentImage ParentCommandLine Hashes User

index=*
(

"sc " OR
"schtasks" OR
"reg add" OR
"reg.exe add" OR
"wmic" OR
"powershell -enc" OR
"powershell -encodedcommand" OR
"New-Service" OR
"Set-Service" OR
"Startup" OR
"RunOnce" OR
"Run\"
)

index= *CommandLine*=
(
*"*sc *" OR*
*"*schtasks*" OR*
*"*reg add*" OR*
*"*wmic*" OR*
*"*powershell*encoded*" OR
"*New-Service*" OR
"*Set-Service*"
)

・永続化として
index=* EventCode=4720

・AD　スクリプト、ツール
index=main source="WinEventLog:Microsoft-Windows-Sysmon/Operational"
EventCode=1
(
CommandLine="*--ntds*"
OR CommandLine="*SharpHound*"
OR CommandLine="*powerview*"
OR CommandLine="*lsadump*"
OR CommandLine="*dcsync*"
OR CommandLine="*ntds.dit*"
)
| table _time ComputerName User Image CommandLine Hashes ParentImage
ParentCommandLine
| sort _time

user作成
index=main EventCode=1 Image="*net.exe" CommandLine=" /add /domain*"

Reconnaissance（偵察）
index=*
(
"whoami" OR
"ipconfig" OR
"ifconfig" OR
"net user" OR
"net view" OR
"net group" OR
"nslookup" OR
"ping " OR
"tracert" OR
"arp -a"
)

Weaponization（武器化）
index=*
(
"msfvenom" OR
"mimikatz" OR
"cobalt" OR
"beacon" OR
"payload" OR
"shellcode"
)

Delivery（配送：メール・Web）
index=*
(
".html" OR
".zip" OR
".iso" OR
".img" OR
".lnk" OR
".docm" OR
".xlsm" OR
"attachment" OR
"download"
)

Exploitation（侵入・実行）

```
index=*
(
".exe" OR
".js" OR
".vbs" OR
".ps1" OR
"powershell -enc" OR
"powershell -encodedcommand" OR
"cmd.exe /c" OR
"wscript.exe" OR
"cscript.exe"
)
```

Installation（インストール）

```
index=*
(
"msiexec" OR
"install" OR
"setup.exe" OR
"regsvr32" OR
"rundll32" OR
"certutil -urlcache"
)
```

Command & Control（C2）

```
index=*
(
"http://" OR
"https://" OR
"dns" OR
"beacon" OR
"callback" OR
"reverse shell" OR
"nc " OR
"ncat" OR
"curl" OR
"wget"
)
```

Actions on Objectives（目的達成）

```
index=*
(
"vssadmin delete shadows" OR
"wevtutil cl" OR
"cipher /w" OR
"rar a" OR
"7z a" OR
"exfil" OR
"upload" OR
"ransom" OR
"encrypt"
)
```

Persistence（永続化）

```
index=*
(
"sc create" OR
"schtasks /create" OR
"reg add" OR
"wmic startup" OR
"New-Service" OR
"Set-Service" OR
"RunOnce" OR
"Startup"
)
```

Privilege Escalation（権限昇格）

```
index=*
(
"runas" OR
"token" OR
"getsystem" OR
"bypass" OR
"SeDebugPrivilege" OR
"uac" OR
"fodhelper" OR
"eventvwr"
)
```

Defense Evasion（防御回避）

```
index=*
(
"disable" OR
"defender" OR
"amsi" OR
"tamper" OR
"exclude" OR
"Set-MpPreference" OR
"Add-MpPreference"
)
```

外部からなにかきていないか

```
index=
sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational"
EventCode=1
(
CommandLine="http" OR
CommandLine="https" OR
CommandLine="urlcache*"
)
```

権限昇格・内部調査の兆候

OS・権限調査ツールの実行

```
index=*
(
"linpeas" OR
"winpeas" OR
"seatbelt" OR
"whoami /all" OR
"sudo -l"
)
| table _time host Image CommandLine User
| sort -_time
```

不審な場所に exe が出現していないか

システム直下だが通常と違う exe 実行

```
index=
(
Image="\Windows\Tasks\.exe" OR
Image="\Windows\Temp\.exe" OR
```

Image="\Users\Public*.exe"
)
| table _time host Image CommandLine User
| sort -_time

圧縮・アーカイブ操作の検知
index=*
(
"Compress-Archive" OR
"tar " OR
"zip " OR
"7z "
)

外に出ていないか（まだIP不明）
外部通信の“連続性”を見る
index=*
(
"http://" OR
"https://" OR
"curl " OR
"wget "
)
| stats count by dest_ip
| sort -count

Workstation_Name の意味
ログオン要求を発生させた端末のホスト名
（ログオン元の端末名）