CYBERSECURITY · SEC-05

Windows for Defenders

Use this when: you check a Windows PC or server for signs of compromise: logons, new accounts, odd tasks, connections and Defender status.

BreakFixLearn

Security+ · CySA+
Sheet v1.0 · Nov 2026

Scan to visit

Security log events to know

Event Viewer › Windows Logs › Security · red = investigate every time

4624	Logon succeeded	check logon type	4720	User account created	expected?
4625	Logon failed	many = guessing	4724	Password reset attempted	by whom?
4648	Logon with explicit credentials	runas, lateral	4732	Added to a local group	Administrators?
4672	Admin rights given to a logon	who is admin?	4740	Account locked out	find the source
4688	New process created	needs auditing on	4768	Kerberos TGT requested	on DCs
4697	Service install attempted	persistence	4719	Audit policy changed	high
4698	Scheduled task created	persistence	1102	Audit log cleared	high

Logon types

in 4624 / 4625

2	**Interactive**	At the keyboard
3	**Network**	File share, net use
4	**Batch**	Scheduled task
5	**Service**	Service started
7	**Unlock**	Screen unlocked
10	**RemoteInteractive**	RDP
11	**CachedInteractive**	No DC contacted

Hunt with PowerShell

Run as admin

```
# last 20 failed logons
Get-WinEvent -FilterHashtable @{LogName='Security';Id=4625}
  -MaxEvents 20
```

`Get-LocalGroupMember Administrators`	Who is admin?
`Get-ScheduledTask`	Tasks: odd names, paths
`Get-NetTCPConnection -State Established`	Live connections
`Get-Process | Select-Object Name, Id, Path`	Exe path

Defender and files

`Get-MpComputerStatus`	AV on? Updated?
`Update-MpSignature`	Update definitions
`Start-MpScan -ScanType QuickScan`	Quick scan
`Get-MpThreatDetection`	What it caught
`Get-FileHash .\file.exe`	SHA-256 to look up
`Get-AuthenticodeSignature .\file.exe`	Who signed it?

Turn on visibility first

`auditpol /get /category:*`	Audited?
`wevtutil epl Security C:\IR\sec.evtx`	Export

Script block logging (event 4104): Group Policy › Administrative Templates › Windows Components › Windows PowerShell › *Turn on PowerShell Script Block Logging*. Logs to `Microsoft-Windows-PowerShell/Operational`.

4688 needs *Audit Process Creation* on, plus the command-line policy to see arguments.

Triage order, then clean up safely

1. Who logged on? 4624, 4625
2. New users or admins? 4720, 4732
3. What persists? Tasks, services, Run keys
4. What talks out? Connections
5. Defender healthy?

Run keys: `Get-ItemProperty HKLM:\Software\Microsoft\Windows\CurrentVersion\Run` (and the same path under `HKCU:`).

DANGER Isolate the host. Do not wipe it. Escalate.

CAUTION Export logs before a reboot or reimage.

CAUTION Never turn off Defender to make an app work.

REMEMBER

- **4625** burst + one user = guessing
- Type **10** = RDP logon
- **1102** = someone cleared the log

Sources: Microsoft Learn (Events to Monitor, event 4624, PowerShell logging, Defender) · CompTIA CySA+

CC BY-NC 4.0 · SEC-05 v1.0