30+ Vital Windows Event IDs and Sysmon Event IDs

Every Cybersecurity Analyst Should Master

No	Event Source	Event ID	Description	Potential Security Implications
1	Windows Security	4624	Successful account logon	Tracking user activity, potential unauthorized access
2	Windows Security	4625	Failed account logon	Brute force attempts, password spraying
3	Windows Security	4720	A user account was created	Unauthorized account creation, persistence
4	Windows Security	4722	A user account was enabled	Potential reactivation of dormant accounts
5	Windows Security	4725	A user account was disabled	Account lockouts, potential security measures
6	Windows Security	4726	A user account was deleted	Unauthorized account removal
7	Windows Security	4672	Special privileges assigned to new logon	Privilege escalation, admin account usage
8	Windows Security	1102	The audit log was cleared	Potential cover-up of malicious activities
9	Windows Security	4688	A new process has been created	Malware execution, suspicious process creation
10	Windows Security	4634	An account was logged off	Session tracking
11	Windows Security	4647	User initiated logoff	Distinguishing user vs. system-initiated logoffs
12	Windows Security	4648	Logon attempted using explicit credentials	Potential lateral movement, credential theft
13	Windows Security	4719	System audit policy was changed	Attempts to modify auditing, evade detection
14	Windows Security	4663	An attempt was made to access an object	Unauthorized access to sensitive data

15	Windows Security	5140	A network share object was accessed	Monitoring file sharing activities
16	Windows System	7000	Service failed to start	System instability, misconfigurations
17	Windows System	7045	A service was installed in the system	Detection of unauthorized services
18	Windows System	6005	The Event Log service was started	System startup, timeline establishment
19	Windows System	6006	The Event Log service was stopped	System shutdown, timeline establishment
20	Windows System	1	The system time has changed	Potential log tampering
21	Windows Application	1000	Application error (crash)	Application instability, potential exploits
22	Windows Application	1002	Application hang	Performance issues, resource exhaustion
23	Windows Setup	19	Windows Update installation successful	System patching status
24	Windows Setup	20	Windows Update installation failure	Potential vulnerabilities due to failed updates
25	PowerShell	4103	PowerShell Pipeline Execution Details	Detection of malicious scripts
26	PowerShell	4104	PowerShell Script Block Logging	Analysis of PowerShell activities
27	Sysmon	1	Process creation	Malware execution, suspicious processes
28	Sysmon	3	Network connection	Command and control, data exfiltration
29	Windows Defender	1000	Malware Detection	Potential system compromise
30	Task Scheduler	106	Task registered or updated	Potential persistence mechanism
31	Remote Desktop	1149	User authentication succeeded via RDP	Monitoring remote access