Critical Windows Security Event IDs

The most important Windows security event log IDs to monitor

Monitoring Windows 10 event logs is one of the best ways to detect malicious activity on your network. Which event IDs should you watch? These are the most important types of log events to look for and what they can tell you.

Category	**Event ID and description**	**Reasons to monitor (by no means exhaustive)**
Logon and logoff	**4624** (Successful logon)	• To detect abnormal and possibly unauthorized insider activity, like a logon from an inactive or restricted account, users logging on outside of normal working hours, concurrent logons to many resources, etc. • To get information on user behavior like user attendance, user working hours, etc.
	4625 (Failed logon)	• To detect possible brute-force, dictionary, and other password guess attacks, which are characterized by a sudden spike in failed logons. • To arrive at a benchmark for the account lockout threshold policy setting. Failure Reason: • %%2305-The specified user account has expired. • %%2309-The specified account's password has expired. • %%2310-Account currently disabled. • %%2311-Account logon time restriction violation. • %%2312-User not allowed to logon at this computer. • %%2313-Unknown username or bad password
Account management	**4728** (Member added to security-enabled global group)	• To ensure group membership for privileged users, who hold the "keys to the kingdom," is scrutinized regularly. This is especially true for security group membership additions.

	4732 (Member added to security-enabled local group)	• To detect privilege abuse by users who are responsible for unauthorized additions. • To detect accidental additions
	4756 (Member added to security-enabled universal group)	
Event log	**1102** (Log cleared) (Alternatively, the event log service can also be disabled which results in the logs not getting recorded. This is done by the system audit policy, in which case event 4719 gets recorded.)	• To spot users with malicious intent, such as those responsible for tampering with event logs.
Account management	**4740** (User account locked out)	• To detect possible brute-force, dictionary, and other password guess attacks, which are characterized by a sudden spike in failed logons. • To mitigate the impact of legitimate users getting locked out and being unable to carry out their work
Object access	**4663** (Attempt made to access object)	• To detect unauthorized attempts to access files and folders.
A new process has been created	**4688**	• Event 4688 documents each program that is executed, who the program ran as and the process that started this process. • When you start a program, you are creating a "process" that stays open until the program exits. This process is identified by the Process ID. You can correlate this event to other events by Process ID to determine what the program did while it ran and when it exited (event 4689).
Password Reset	**4724**	• Password reset attempt by administrator

	4723	- Password change attempt by user