Windows Event ID for Cyber Defense

A Windows Event ID is a unique numeric code assigned to a specific type of event recorded in the Windows Event Log. These IDs help identify and categorize actions or incidents such as user logons, failed login attempts, file access, or system changes.

In cyber defense, Event IDs are crucial for:

- Detecting unauthorized or suspicious activities
- Investigating security breaches
- Monitoring user behaviour and system health
- Creating automated alerts and incident responses using tools like SIEMs

1.Authentication & Logon Events

Event ID	Description	Explanation & Example
4624	Account successfully logged on	Indicates a successful logon. Useful to track who accessed the system. **Example**: A user logs into a workstation—Event 4624 will be logged with logon type (e.g., Type 2 for interactive).
4625	Account failed to log on	Unsuccessful logon attempt. Indicates brute-force attempts. **Example**: A user enters the wrong password 3 times—3 instances of Event 4625.
4634	Account was logged off	Indicates the user has logged off the system. **Example**: After finishing work, a user logs off at 6 PM—Event 4634 is recorded.
4647	User initiated logoff	Different from 4634, this confirms that the **user** initiated logoff. **Example**: Helps distinguish between system shutdown vs. user logoff.
4648	Logon with explicit credentials	Occurs when a user runs a program as another user (e.g., "RunAs"). **Example**: Admin opens cmd.exe using another account—Event 4648 logs both users.
4672	Special privileges assigned to new logon	Typically logs when a privileged (admin) account logs in. **Example**: Domain Admin logs into a server—Event 4672 is logged.

2. User & Account Management

Event ID	Description	Explanation & Example
4720	User account created	New user account was made. **Example**: Sysadmin creates a new intern account—Event 4720 is logged.
4722	User account enabled	Disabled account is re-enabled. **Example**: Reactivating an employee's account after leave.
4798	Local group membership enumerated	A process (or user) is checking local group memberships. **Example**: Pen-testing tool scans group members—logs Event 4798.
4799	Security-enabled group membership enumerated	Similar to 4798, but for **security-enabled** groups. **Example**: Queries against "Administrators" or "Domain Admins" groups.

3. Kerberos & Domain Controller Events

Event ID	Description	Explanation & Example
4768	**Kerberos TGT requested**	**Indicates a Kerberos logon request (TGT - Ticket Granting Ticket).** **Example: When a user logs into the domain, Kerberos provides TGT—Event 4768 is triggered.**
4769	Kerberos service ticket requested	After a TGT is granted, the user requests access to a service (like a file share). **Example**: Accessing a shared folder triggers 4769.
4771	Kerberos pre-authentication failed	Might indicate a wrong password or malicious attempts. **Example**: Attackers using brute-force against Kerberos—this event shows failed pre-auth attempts.
4776	DC validates credentials	Logged by the domain controller when validating a username/password. **Example**: Useful for auditing password attempts across domain.

4. Process and Task Tracking

Event ID	Description	Explanation & Example
4668	A new process was created	Logs process creation. Critical for detecting malware behavior. **Example**: A script runs PowerShell—this is logged as 4688.
4698	Scheduled task was created	Used for persistence by attackers. **Example**: Malicious task to run a script daily is created—Event 4698 logs it.

5. Network and Resource Access

Event ID	Description	Explanation & Example
5140	Network share object accessed	User accessed a shared folder/file. **Example**: Employee accesses \\server\documents—logs Event 5140.
5145	Network share checked for access	Access check (even if denied). **Example**: User tried to open a restricted folder—5145 logs both successful and denied attempts.

6. Audit & Log Management

Event ID	Description	Explanation & Example
1102	Audit log cleared	Someone cleared the security log—high alert! **Example**: If Event 1102 appears without prior alerts, it may be an attempt to cover tracks.