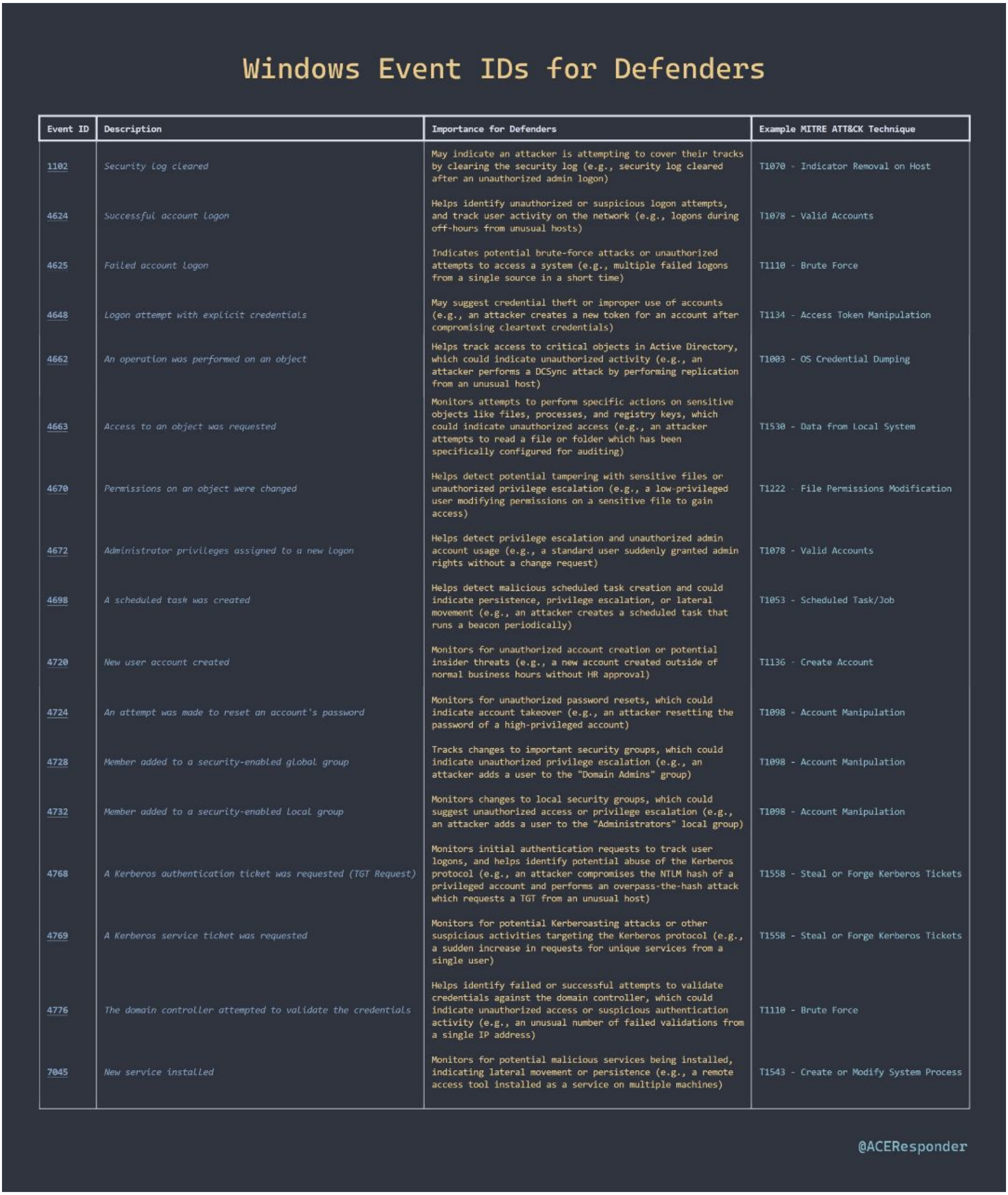

Windows Event IDs for Defenders

Event ID	Description	Importance for Defenders	Example MITRE ATT&CK Technique
1102	*Security log cleared*	May indicate an attacker is attempting to cover their tracks by clearing the security log (e.g., security log cleared after an unauthorized admin logon)	T1070 - Indicator Removal on Host
4624	*Successful account logon*	Helps identify unauthorized or suspicious logon attempts, and track user activity on the network (e.g., logons during off-hours from unusual hosts)	T1078 - Valid Accounts
4625	*Failed account logon*	Indicates potential brute-force attacks or unauthorized attempts to access a system (e.g., multiple failed logons from a single source in a short time)	T1110 - Brute Force
4648	*Logon attempt with explicit credentials*	May suggest credential theft or improper use of accounts (e.g., an attacker creates a new token for an account after compromising cleartext credentials)	T1134 - Access Token Manipulation
4662	*An operation was performed on an object*	Helps track access to critical objects in Active Directory, which could indicate unauthorized activity (e.g., an attacker performs a DCSync attack by performing replication from an unusual host)	T1003 - OS Credential Dumping
4663	*Access to an object was requested*	Monitors attempts to perform specific actions on sensitive objects like files, processes, and registry keys, which could indicate unauthorized access (e.g., an attacker attempts to read a file or folder which has been specifically configured for auditing)	T1530 - Data from Local System
4670	*Permissions on an object were changed*	Helps detect potential tampering with sensitive files or unauthorized privilege escalation (e.g., a low-privileged user modifying permissions on a sensitive file to gain access)	T1222 - File Permissions Modification
4672	*Administrator privileges assigned to a new logon*	Helps detect privilege escalation and unauthorized admin account usage (e.g., a standard user suddenly granted admin rights without a change request)	T1078 - Valid Accounts
4698	*A scheduled task was created*	Helps detect malicious scheduled task creation and could indicate persistence, privilege escalation, or lateral movement (e.g., an attacker creates a scheduled task that runs a beacon periodically)	T1053 - Scheduled Task/Job
4720	*New user account created*	Monitors for unauthorized account creation or potential insider threats (e.g., a new account created outside of normal business hours without HR approval)	T1136 - Create Account
4724	*An attempt was made to reset an account's password*	Monitors for unauthorized password resets, which could indicate account takeover (e.g., an attacker resetting the password of a high-privileged account)	T1098 - Account Manipulation
4728	*Member added to a security-enabled global group*	Tracks changes to important security groups, which could indicate unauthorized privilege escalation (e.g., an attacker adds a user to the "Domain Admins" group)	T1098 - Account Manipulation
4732	*Member added to a security-enabled local group*	Monitors changes to local security groups, which could suggest unauthorized access or privilege escalation (e.g., an attacker adds a user to the "Administrators" local group)	T1098 - Account Manipulation
4768	*A Kerberos authentication ticket was requested (TGT Request)*	Monitors initial authentication requests to track user logons, and helps identify potential abuse of the Kerberos protocol (e.g., an attacker compromises the NTLM hash of a privileged account and performs an overpass-the-hash attack which requests a TGT from an unusual host)	T1558 - Steal or Forge Kerberos Tickets
4769	*A Kerberos service ticket was requested*	Monitors for potential Kerberoasting attacks or other suspicious activities targeting the Kerberos protocol (e.g., a sudden increase in requests for unique services from a single user)	T1558 - Steal or Forge Kerberos Tickets
4776	*The domain controller attempted to validate the credentials*	Helps identify failed or successful attempts to validate credentials against the domain controller, which could indicate unauthorized access or suspicious authentication activity (e.g., an unusual number of failed validations from a single IP address)	T1110 - Brute Force
7045	*New service installed*	Monitors for potential malicious services being installed, indicating lateral movement or persistence (e.g., a remote access tool installed as a service on multiple machines)	T1543 - Create or Modify System Process

@ACEResponder