Top 25 Windows Event IDs for SOC Analyst

1. **4624** – Successful Logon
2. **4625** – Failed Logon
3. **4648** – Logon Attempt Using Explicit Credentials
4. **4672** – Special Privileges Assigned to New Logon
5. **4634** – Logoff
6. **4688** – A New Process Has Been Created
7. **4689** – A Process Has Ended
8. **5156** – Windows Filtering Platform Connection Allowed
9. **5158** – Windows Filtering Platform Connection Blocked
10. **1102** – Audit Log Cleared
11. **4720** – User Account Created
12. **4726** – User Account Deleted
13. **4732** – Member Added to Security-Enabled Local Group
14. **4738** – User Account Changed
15. **4740** – User Account Locked Out
16. **4756** – Member Added to Security-Enabled Global Group
17. **4768** – Kerberos TGT Requested
18. **4769** – Kerberos Service Ticket Requested
19. **4776** – Credentials Validation Attempted
20. **4798** – User's Local Group Membership Enumerated
21. **5140** – Network Share Accessed
22. **5152** – Connection Blocked by WFP
23. **5058** – KDC Service Stopped
24. **4703** – User Right Assigned
25. **Event ID 4743** – Computer Account Moved

1. Event ID 4624 – Successful Logon

- **What It Represents:** Logs a successful logon to a system.
- **Why It's Important:** Essential for identifying whether a legitimate user or unauthorized attacker has accessed a system.
- **How Analysts Use It:** Analysts track these events to verify if logins are coming from authorized users and if the login times, locations, or methods align with typical user behaviour.
- **Example Use Case:** An alert triggers when a user logs in from an unusual location (e.g., different country), which may indicate a compromised account.
- **Mitigation:** Implement multi-factor authentication (MFA), use VPN for remote access, and enforce strong password policies.
- **Detection:** Set alerts for logons from unusual IP addresses, geographic locations, or from accounts that rarely log in remotely.

---

2. Event ID 4625 – Failed Logon

- **What It Represents:** Captures failed logon attempts, often due to incorrect credentials.
- **Why It's Important:** Repeated failed logins can indicate brute-force or credential stuffing attacks.
- **How Analysts Use It:** Analysts monitor failed login attempts to identify abnormal login patterns, especially if coming from unfamiliar or blacklisted IP addresses.
- **Example Use Case:** Multiple failed logon attempts on a high-privilege account (admin, root) are detected, which may indicate an attacker trying to brute-force their way in.
- **Mitigation:** Set account lockout policies after a certain number of failed attempts and require MFA.
- **Detection:** Alert on multiple failed login attempts in a short period, especially for privileged accounts.

---

3. Event ID 4648 – Logon Attempt Using Explicit Credentials

- **What It Represents:** This event is logged when a process or service logs on using explicit credentials, such as credentials provided for a network resource.
- **Why It's Important:** Can indicate lateral movement or escalation where credentials are explicitly passed for system access.
- **How Analysts Use It:** Monitor these logons for unusual systems or accounts being accessed, especially during non-business hours.
- **Example Use Case:** An attacker compromises an account and uses explicit credentials to move laterally within the network.
- **Mitigation:** Use least privilege access controls and restrict explicit credentials use to essential services only.
- **Detection:** Set alerts for explicit credential usage for sensitive resources outside regular business activities.

---

4. Event ID 4672 – Special Privileges Assigned to New Logon

- **What It Represents:** Logged when a new logon is assigned special privileges, such as administrative rights.
- **Why It's Important:** Track when accounts gain privileged access to critical systems, which could indicate misuse or privilege escalation.
- **How Analysts Use It:** Watch for new or unexpected special privilege assignments that could indicate lateral movement or escalation.
- **Example Use Case:** A normal user account unexpectedly receives admin privileges, which could be a sign of credential theft or malicious behavior.
- **Mitigation:** Restrict privileged access to essential personnel and ensure user roles are reviewed regularly.
- **Detection:** Alert when special privileges are granted to non-administrative accounts or at odd times.

---

5. Event ID 4634 – Logoff

- **What It Represents:** Captures logoff events, indicating when a user has successfully logged off from a system.
- **Why It's Important:** Logoff events ensure that sessions are closed securely and help monitor when users unexpectedly remain logged on.
- **How Analysts Use It:** Analysts monitor logoff events to track if accounts remain logged on longer than expected or if unauthorized logoff activities occur.
- **Example Use Case:** A user is logged off unexpectedly during working hours, which could indicate a session hijack or abnormal termination.
- **Mitigation:** Set time-based logoff policies and employ session timeouts for inactivity.
- **Detection:** Set alerts for logoff events when accounts are active beyond normal session durations.

---

6. Event ID 4688 – A New Process Has Been Created

- **What It Represents:** Indicates that a new process has been created on the system.
- **Why It's Important:** The creation of processes can signal the start of potentially malicious activities like malware or unauthorized scripts.
- **How Analysts Use It:** Analysts track the creation of processes, especially those originating from unknown or untrusted locations.
- **Example Use Case:** A suspicious process is created by an unauthorized user, which is commonly associated with malware like ransomware.
- **Mitigation:** Use endpoint detection and response (EDR) tools to block unauthorized processes and maintain a known whitelist.
- **Detection:** Set alerts for process creation from unusual locations or unusual executables, such as those in temporary folders or unknown paths.

---

7. Event ID 4689 – A Process Has Ended

- **What It Represents:** Captures the termination of a process.
- **Why It's Important:** Terminated processes, particularly security-critical processes, could indicate that an attacker is attempting to hide traces of their activity.
- **How Analysts Use It:** Analysts track terminated processes to identify instances where important processes were forcefully stopped or crashed by malicious actors.
- **Example Use Case:** An attacker terminates antivirus software or system monitoring processes to avoid detection.
- **Mitigation:** Restrict access to critical system processes and maintain strong security configurations.
- **Detection:** Alert when key security processes are unexpectedly terminated or when multiple processes are ended in quick succession.

---

8. Event ID 5156 – Windows Filtering Platform Connection Allowed

- **What It Represents:** Logged when a connection is allowed by the Windows Filtering Platform (WFP), such as through a firewall or network filter.
- **Why It's Important:** This event helps in monitoring and confirming legitimate connections while allowing analysts to detect unauthorized or suspicious traffic.
- **How Analysts Use It:** SOC analysts use it to verify allowed traffic to critical systems, especially if coming from unexpected or unauthorized sources.
- **Example Use Case:** A legitimate user connects to a system, but if the connection is coming from a foreign IP or unfamiliar source, it raises suspicion.
- **Mitigation:** Regularly audit firewall configurations and restrict unnecessary services and ports.
- **Detection:** Alert on allowed connections to sensitive systems or services from unknown or external sources.

---

9. Event ID 5158 – Windows Filtering Platform Connection Blocked

- **What It Represents:** Captures when WFP blocks a connection, such as when a connection violates network filtering rules.
- **Why It's Important:** Blocking network connections is a key defense mechanism that stops potentially malicious traffic from reaching internal systems.
- **How Analysts Use It:** Analysts monitor blocked connections to detect possible malicious traffic attempts.
- **Example Use Case:** An attacker tries to connect to a C2 server (Command-and-Control) but is blocked by the firewall.
- **Mitigation:** Regularly review and update firewall rules to block known malicious IPs and traffic types.
- **Detection:** Set alerts when critical infrastructure is subject to connection attempts from known malicious IPs or unexpected sources.

---

10. Event ID 1102 – The Audit Log Was Cleared

- **What It Represents:** This event indicates that the security audit log has been cleared, which can be a red flag for malicious activity.
- **Why It's Important:** Attackers often clear logs to cover their tracks after executing an attack. This event is critical for detecting tampering or post-exploitation activity.
- **How Analysts Use It:** Analysts closely monitor for any attempts to clear logs as it suggests an attempt to cover up malicious behavior.
- **Example Use Case:** After a successful attack, an attacker clears the logs to erase any evidence of their actions.
- **Mitigation:** Limit access to security logs and configure logging to prevent clearing.
- **Detection:** Alert when log clearing occurs, especially by accounts that typically do not have log clearing privileges.

---

11. Event ID 4720 – A User Account Was Created

- **What It Represents:** Logs the creation of a new user account.
- **Why It's Important:** Creating a new user account without proper authorization may indicate an attacker is setting up a backdoor or persistent access.
- **How Analysts Use It:** Analysts monitor user account creation, particularly when it's outside normal business procedures.
- **Example Use Case:** An attacker creates a new admin account after compromising a system to maintain control over the environment.
- **Mitigation:** Regularly audit user account creations and implement strict controls on account management.
- **Detection:** Set alerts for unexpected user account creation or accounts with administrative privileges.

---

12. Event ID 4726 – A User Account Was Deleted

- **What It Represents:** This event captures the deletion of a user account.
- **Why It's Important:** The deletion of accounts can be used by attackers to erase traces of their presence or disable security controls.
- **How Analysts Use It:** Analysts monitor for any account deletions, especially for privileged accounts.
- **Example Use Case:** An attacker deletes a user account that was compromised to eliminate evidence of their presence.
- **Mitigation:** Limit the ability to delete accounts to authorized administrators only.
- **Detection:** Set alerts for any unexpected account deletions or deletions of high-privilege accounts.

---

13. Event ID 4732 – A Member Was Added to a Security-Enabled Local Group

- **What It Represents:** This event is logged when a user is added to a security-enabled local group.
- **Why It's Important:** Unapproved changes to group membership can signal an attacker escalating their privileges or gaining unauthorized access to resources.
- **How Analysts Use It:** Analysts track changes to group memberships to detect any unauthorized elevation of privileges.
- **Example Use Case:** An attacker adds themselves to a group with administrative privileges to increase control over the system.
- **Mitigation:** Regularly audit group memberships and restrict membership changes to trusted administrators.
- **Detection:** Set alerts for additions to sensitive or privileged groups.

---

14. Event ID 4738 – A User Account Was Changed

- **What It Represents:** This event indicates that an existing user account was modified, such as a password change or change in group membership.
- **Why It's Important:** Account changes, especially without proper authorization, can indicate misuse of privileged accounts or attacker activity.
- **How Analysts Use It:** Analysts use it to detect unauthorized changes to user accounts, particularly those with elevated privileges.
- **Example Use Case:** An attacker changes the password of a compromised account to prevent detection.
- **Mitigation:** Implement strong password policies and ensure that changes to critical accounts are logged and reviewed.
- **Detection:** Set alerts when sensitive account attributes are modified, particularly if done outside of normal working hours.

---

15. Event ID 4740 – A User Account Was Locked Out

- **What It Represents:** This event logs when a user account is locked due to exceeding the allowed number of failed login attempts.
- **Why It's Important:** Account lockouts often occur due to brute-force attempts or credential stuffing, indicating potential malicious behavior.
- **How Analysts Use It:** Analysts monitor these events to detect brute-force attacks and unusual account lockout patterns.
- **Example Use Case:** A brute-force attack locks out a user account after several failed login attempts.
- **Mitigation:** Enforce account lockout policies and use CAPTCHA or MFA to prevent automated attacks.
- **Detection:** Set alerts for multiple account lockouts, especially from the same source or on high-privilege accounts.

---

16. Event ID 4756 – A Member Was Added to a Security-Enabled Global Group

- **What It Represents:** This event logs when a member is added to a security-enabled global group.
- **Why It's Important:** Changes to global group memberships can impact access controls, and unauthorized additions can indicate malicious activity.
- **How Analysts Use It:** Analysts track this event to ensure that sensitive global groups are not modified by unauthorized users.
- **Example Use Case:** An attacker adds themselves to a group with broad permissions, which could allow access to sensitive data.
- **Mitigation:** Regularly review global group memberships and ensure only authorized personnel can make changes.
- **Detection:** Set alerts for changes to global groups, especially on sensitive groups like "Domain Admins."

---

17. Event ID 4768 – A Kerberos Authentication Ticket (TGT) Was Requested

- **What It Represents:** This event logs when a user requests a Ticket Granting Ticket (TGT) from the Kerberos Key Distribution Center (KDC).
- **Why It's Important:** TGT requests are a critical part of the authentication process and can be a target for attackers trying to hijack or impersonate users.
- **How Analysts Use It:** Analysts track TGT requests to detect anomalies like unusual ticket requests that may signal credential theft.
- **Example Use Case:** An attacker uses stolen credentials to request a TGT for a privileged account, attempting to impersonate the victim.
- **Mitigation:** Use strong passwords for Kerberos authentication and regularly monitor for unusual TGT request patterns.
- **Detection:** Set alerts for TGT requests that deviate from normal usage patterns (e.g., high number in a short period).

---

18. Event ID 4769 – A Service Ticket Was Requested

- **What It Represents:** Logs when a service ticket is requested from the KDC for accessing network services.
- **Why It's Important:** Service tickets can be abused in lateral movement attacks, such as the use of pass-the-ticket (PTT) techniques.
- **How Analysts Use It:** Analysts use this event to detect abnormal service ticket requests, such as those coming from unauthorized users or devices.
- **Example Use Case:** An attacker requests service tickets for systems they don't normally access, often as part of a lateral movement attack.
- **Mitigation:** Monitor for unusual service ticket requests and implement tighter control over service ticket issuance.

- **Detection:** Alert when service tickets are requested for systems not normally accessed by the user.

---

19. Event ID 4776 – The Computer Attempted to Validate the Credentials of an Account

- **What It Represents:** This event is logged when a computer attempts to validate credentials (e.g., a login).
- **Why It's Important:** These events are useful for detecting authentication failures related to unauthorized access attempts.
- **How Analysts Use It:** Analysts monitor this event for credential validation failures to identify attacks like brute force or NTLM relay.
- **Example Use Case:** An attacker repeatedly tries to authenticate using stolen credentials to gain access to critical systems.
- **Mitigation:** Enforce strong authentication controls and monitor login attempts for unusual activity.
- **Detection:** Set alerts on failed authentication attempts and correlate them with other events for indicators of compromise.

---

20. Event ID 4798 – A User's Local Group Membership Was Enumerated

- **What It Represents:** Logs when an attacker or admin enumerates the local group memberships for a specific user account.
- **Why It's Important:** Enumeration of group memberships can be part of an attacker's reconnaissance phase to find high-value targets.
- **How Analysts Use It:** Analysts watch for these events to detect any reconnaissance activity aimed at identifying privileged groups.
- **Example Use Case:** An attacker enumerates local groups to identify high-privilege accounts or systems.
- **Mitigation:** Limit access to group membership enumeration by implementing proper user permissions.
- **Detection:** Alert when group membership enumeration occurs, especially for users with privileged access.

---

21. Event ID 5140 – A Network Share Object Was Accessed

- **What It Represents:** This event logs when a network share or directory object is accessed over the network.
- **Why It's Important:** Monitoring network share access helps detect unauthorized access or suspicious file-sharing activities.
- **How Analysts Use It:** Analysts monitor this event to detect unauthorized access to critical file shares and data.

- **Example Use Case:** An attacker accesses sensitive files stored on a network share after compromising a user's account.
- **Mitigation:** Enforce access controls on file shares and require proper authentication for accessing sensitive data.
- **Detection:** Alert on access to sensitive shares or unusual access patterns that could indicate compromise.

---

22. Event ID 5152 – A Connection Was Blocked by the Windows Filtering Platform

- **What It Represents:** Logged when a connection is blocked by Windows Filtering Platform, such as when firewall rules or security filters prevent a connection.
- **Why It's Important:** Blocking unauthorized connections helps protect critical systems from external attacks or unauthorized access.
- **How Analysts Use It:** Analysts monitor blocked connections to detect and confirm malicious or suspicious traffic.
- **Example Use Case:** An attacker tries to access a system using a known malicious IP address but is blocked by the firewall.
- **Mitigation:** Regularly review and update firewall rules to block known malicious traffic.
- **Detection:** Set alerts when blocked connections are attempted, particularly from untrusted sources.

---

23. Event ID 5058 – Key Distribution Center Service Was Stopped

- **What It Represents:** This event logs when the Key Distribution Center (KDC) service stops functioning or is tampered with.
- **Why It's Important:** The KDC is crucial for Kerberos authentication, and stopping it can severely impact system access or facilitate attacks like Kerberos ticket manipulation.
- **How Analysts Use It:** Analysts watch for KDC service disruptions as they indicate system compromise or attack.
- **Example Use Case:** Attackers attempt to stop the KDC service to exploit vulnerabilities in Kerberos authentication.
- **Mitigation:** Ensure that the KDC service is protected and regularly monitored.
- **Detection:** Alert on the KDC service being stopped or restarted unexpectedly.

---

24. Event ID 4703 – A User Right Was Assigned

- **What It Represents:** Logged when a user right (e.g., backup operator) is assigned to an account.
- **Why It's Important:** Unwarranted changes in user rights can indicate privilege escalation attempts or abuse.

- **How Analysts Use It:** Analysts monitor these events to detect unexpected changes to user rights that might indicate exploitation.
- **Example Use Case:** An attacker escalates privileges by adding themselves to an account with elevated user rights, such as backup operator.
- **Mitigation:** Limit and audit the assignment of user rights to sensitive roles.
- **Detection:** Set alerts when user rights assignments are made to accounts outside of normal administrative operations.

---

25. Event ID 4743 – A Computer Account Was Moved

- **What It Represents:** This event is triggered when a computer account is moved to a new Organizational Unit (OU) within Active Directory.
- **Why It's Important:** Moving a computer account can indicate that attackers are attempting to hide the compromised system from view or manipulate its permissions.
- **How Analysts Use It:** Analysts monitor this event to detect unauthorized changes in computer account locations within AD.
- **Example Use Case:** An attacker moves a compromised system into a separate OU to avoid detection during auditing.
- **Mitigation:** Lock down permissions for moving computer accounts in Active Directory and perform regular audits.
- **Detection:** Set alerts for changes to computer account locations, particularly when they involve systems that should not have been moved.