SIEM Alert Rules Documentation

The following rules are configured to generate alerts in the Security Information and Event Management (SIEM) system based on specific event conditions. Each rule has a defined severity level, which indicates the potential impact or priority of the alert.

1. Multiple Failed Logins

- **Description**: Detects multiple failed login attempts within a short timeframe across the Application or Security channels.
- **Conditions**:
  - Event ID: `4625` (Failed login attempt)
  - Frequency: 5 failed attempts within 5 minutes
  - Channels: `Application`, `Security`
- **Severity**: High

2. After-hours Login

- **Description**: Detects successful login attempts that occur outside of standard business hours (6:00 PM to 6:00 AM).
- **Conditions**:
  - Event ID: `4624` (Successful login)
  - Time Range: Between `18:00` and `06:00`
- **Severity**: Medium

3. Account Lockout

- **Description**: Detects when a user account is locked due to repeated failed login attempts.
- **Conditions**:
  - Event IDs: `4740`, `4767` (Account lockout events)
  - Channel: `Security`
- **Severity**: High

4. New User Account Created

- **Description**: Detects when a new user account is created in the system.
- **Conditions**:
  - Event ID: `4720` (New user account creation)
  - Channel: `Security`
- **Severity**: Medium

5. Scheduled Task Modified

- **Description**: Detects when a scheduled task is created, modified, enabled, or disabled on the system.

- **Conditions**:
  - Event IDs: `4698`, `4699`, `4700`, `4702` (Scheduled task changes)
  - Channel: `Security`
- **Severity**: Medium

6. PowerShell Execution

- **Description**: Detects when PowerShell commands are executed on the system.
- **Conditions**:
  - Event IDs: `4103`, `4104` (PowerShell activity)
  - Channel: `Windows PowerShell`
- **Severity**: Low

7. Explicit Credential Usage

- **Description**: Detects when a user logs on using explicit credentials while already logged into the system.
- **Conditions**:
  - Event ID: `4648` (Explicit credential logon)
  - Channel: `Security`
- **Severity**: High

8. Malware Detection

- **Description**: Detects malware-related events from Windows Defender.
- **Conditions**:
  - Event IDs: `1005`, `1006`, `1007`, `1008` (Windows Defender alerts)
  - Channel: `Microsoft-Windows-Windows Defender/Operational`
- **Severity**: Critical

9. Sensitive Group Modified

- **Description**: Detects when a sensitive group, such as Administrators or Domain Admins, is modified.
- **Conditions**:
  - Event IDs: `4728`, `4729`, `4732`, `4756` (Group membership changes)
  - Channel: `Security`
  - Target User Groups: `Administrators`, `Domain Admins`, `Enterprise Admins`
- **Severity**: High

10. Remote Desktop Connection

- **Description**: Detects when a remote desktop connection is established.
- **Conditions**:
  - Event ID: `4624` (Successful login)

  - Channel: `Security`
  - Logon Type: `10` (Remote interactive logon)
- **Severity**: Medium

11. System Boot

- **Description**: Logs when the system starts.
- **Conditions**:
  - Event ID: `6005` (System boot)
  - Channel: `System`
- **Severity**: Informational

12. System Shutdown

- **Description**: Logs when the system shuts down.
- **Conditions**:
  - Event ID: `6006` (System shutdown)
  - Channel: `System`
- **Severity**: Informational

13. Service Started

- **Description**: Detects when a system service is started.
- **Conditions**:
  - Event ID: `7001` (Service start)
  - Channel: `System`
- **Severity**: Informational

14. Service Stopped

- **Description**: Detects when a system service is stopped.
- **Conditions**:
  - Event ID: `7009` (Service stop)
  - Channel: `System`
- **Severity**: Informational

Summary

These alert rules are designed to monitor critical system activities and potential security incidents, helping security teams to respond to various threats such as failed login attempts, account lockouts, malware detection, and system modifications. Severity levels ranging from informational to critical guide the prioritization of incident responses based on the potential impact of the events.