```
EventID: 1
EventName: Process created
Logs:
  - UtcTime: "2024-03-31 16:15:00"
    ProcessGuid: "12345678-1234-5678-ABCD-1234567890EF"
    ProcessId: 1001          ──────→ Unique process identifier.
    Image: "C:\\Windows\\System32\\notepad.exe"  ──→ Identifies executed program.
    CommandLine: "C:\\Windows\\System32\\notepad.exe  ──→ Specifies executed command.
C:\\Users\\User1\\Document\\example.txt"
    ParentProcessGuid: "ABCD1234-5678-9012-EFGH-34567890ABCD"
    ParentProcessId: 2001
    ParentImage: "C:\\Windows\\System32\\explorer.exe"  ──→ Indicates parent program.
    ParentCommandLine: "C:\\Windows\\System32\\explorer.exe /desktop"
                                                    ↓
                                           Specifies parent command.
    Hashes:
      SHA256: "A1B2C3D4E5F6G7H8I9J0K1L2M3N4O5P6"
    Company: "Microsoft Corporation"
    Description: "Notepad"
    Product: "Microsoft® Windows® Operating System"
    OriginalFilename: "notepad.exe"
    IntegrityLevel: "Medium"
    LogonId: "0x123456789"
    TerminalSessionId: 1
    User: "User1"
    ParentUser: "User2"
    CurrentDirectory: "C:\\Users\\User1\\Document"
    ParentCurrentDirectory: "C:\\Users\\User2\\Desktop"
```

```
EventID: 11
EventName: File create
Logs:

   - UtcTime: "2024-03-31 16:20:00"
     ProcessGuid: "ABCDEFGH-1234-5678-9012-IJKLMNOPQRST"
     ProcessId: 3001
     Image: "C:\\Windows\\System32\\notepad.exe"        ⟶  Indicates source program.
     TargetFilename: "C:\\Users\\User1\\Documents\\new_document.txt"
                                                ↘  Specifies created file location.
```

EVENT ID 3: NETWORK CONNECTION

```
EventID: 3
EventName: Network Connection
Logs:

   - UtcTime: "2024-03-31 16:25:00"
     ProcessGuid: "JKLMNOP-9012-3456-7890-QRSTUVWXYZAB"
     ProcessId: 4001
     Image: "C:\\Windows\\System32\\chrome.exe"    ⟶ Identifies source program.
     DestinationIp: "192.168.1.100"    ⟶ Specifies target IP address.
     DestinationPort: 443
     Protocol: "TCP"
     Direction: "Outbound"
```

EVENT ID 13: REGISTRY EVENT (VALUE SET)

```
EventID: 13
EventName: Registry Event (Value Set)
Logs:
  - UtcTime: "2024-03-31 16:30:00"
    TargetObject: "HKLM\Software\Microsoft\Windows\CurrentVersion\Run\example"
    Details:
      ValueName: "ExampleValue"
      DataType: "REG_SZ"
      ValueData: "C:\example\example.exe"
```

Identifies affected registry key.

Specifies value name, data type, and value data.

EVENT ID 12: REGISTRY EVENT

```
EventID: 12
EventName: Registry Event (Object Create and Delete)
Logs:
  - UtcTime: "2024-03-31 16:35:00"
    TargetObject: "HKLM\Software\Microsoft\Windows\CurrentVersion\Run\example"
    Details:
      Operation: "Create"
```

Specifies whether the key was created or deleted.

Identifies affected registry key.

EVENT ID 6: DRIVER LOAD

```
EventID: 6
EventName: Driver Load
Logs:
  - UtcTime: "2024-03-31 16:40:00"
    ImageLoaded: "\Device\HarddiskVolume1\Windows\System32\drivers\example.sys"    → Identifies loaded driver.
    Hashes:
      SHA256: "A1B2C3D4E5F6G7H8I9J0K1L2M3N4O5P6"    → Verifies driver integrity.
    Description: "Example Driver"    → Provides information about driver purpose.
    Product: "Example Product"
    Company: "Example Company"
    OriginalFilename: "example.sys"
    Signed: "True"    → Validates driver authenticity.
    Signature: "Valid"    → Confirms driver signature validity.
```

EVENT ID 8: CREATE REMOTE THREAD

```
EventID: 8
EventName: Create Remote Thread
Logs:
  - UtcTime: "2024-03-31 16:45:00"
    SourceProcessGuid: "ABCDEFGH-1234-5678-9012-IJKLMNOPQRST"    → Identifies source process.
    SourceProcessId: 5001    → Unique process identifier.
    TargetProcessGuid: "JKLMNOPQ-5678-9012-3456-RSTUVWXYZABC"    → Identifies target process.
    TargetProcessId: 6001    → Unique process identifier.
    StartAddress: "0x0000000000000000"    → Specifies thread start address.
    StartModule: "kernel32.dll"
```

EVENT ID 10: PROCESS ACCESS

```
EventID: 10
EventName: Process Access
Logs:

 - UtcTime: "2024-03-31 16:50:00"
     SourceProcessGuid: "ABCDEFGH-1234-5678-9012-IJKLMNOPQRST"   → Identifies source process.
     SourceProcessId: 7001   →  Unique process identifier.
     TargetProcessGuid: "JKLMNOPQ-5678-9012-3456-RSTUVWXYZABC"   → Identifies target process.
     TargetProcessId: 8001   →  Unique process identifier.
     GrantedAccess: "Read, Write"   → Specifies granted access rights.
```

EVENT ID 7: IMAGE LOAD

```
EventID: 7
EventName: Image Load
Logs:

 - UtcTime: "2024-03-31 16:55:00"
     ProcessGuid: "ABCDEFGH-1234-5678-9012-IJKLMNOPQRST"
     ProcessId: 9001
     Image: "C:\\Windows\\System32\\kernel32.dll"   → Identifies loaded image.
     ImageLoaded: "C:\\Windows\\System32\\kernel32.dll"   → Specifies loaded image path.
     Hashes:
        SHA256: "A1B2C3D4E5F6G7H8I9J0K1L2M3N4O5P6"   → Verifies image integrity.
     Description: "Kernel32 Dynamic Link Library"   → Provides information about image.
     Product: "Microsoft® Windows® Operating System"
     Company: "Microsoft Corporation"   → Specifies image owner.
     OriginalFilename: "kernel32.dll"
```

EVENT ID 5: PROCESS TERMINATE

```
EventID: 5
EventName: Process Terminate
Logs:
   - UtcTime: "2024-03-31 17:00:00"
     ProcessGuid: "ABCDEFGH-1234-5678-9012-IJKLMNOPQRST"  → Identifies terminated process.
     ProcessId: 10001   → Unique process identifier.
     Image: "C:\\Windows\\System32\\notepad.exe"  → Indicates terminated program.
     ExitCode: 0   → Specifies process termination status.
```

EVENT ID 14: REGISTRY EVENT

```
EventID: 14
EventName: Registry Event (Key and Value Rename)
Logs:
   - UtcTime: "2024-03-31 17:05:00"
     TargetObject: "HKLM\Software\Microsoft\Windows\CurrentVersion\Run\example"
                                                           → Identifies affected registry object.
     Details:
        OldName: "OldValueName"   → Specifies old and new names.
        NewName: "NewValueName"
```

EVENT ID 2: FILE CREATION TIME CHANGE

```
EventID: 2
EventName: File Creation Time Change
Logs:
  - UtcTime: "2024-03-31 17:10:00"
    ProcessGuid: "ABCDEFGH-1234-5678-9012-IJKLMNOPQRST"  → Identifies creating process.
    ProcessId: 11001  → Unique process identifier.
    Image: "C:\\Windows\\System32\\cmd.exe"  → Indicates creating program.
    TargetFilename: "C:\\Users\\User1\\Documents\\example.txt"  → Specifies affected file location.
```

EVENT ID 9: RAW ACCESS READ

```
EventID: 9
EventName: Raw Access Read
Logs:
  - UtcTime: "2024-03-31 17:15:00"
    ProcessGuid: "ABCDEFGH-1234-5678-9012-IJKLMNOPQRST"  → Identifies reading process.
    ProcessId: 12001  → Unique process identifier.
    Image: "C:\\Windows\\System32\\notepad.exe"  → Indicates reading program.
    Device: "\\Device\\HarddiskVolume1\\example.txt"  → Specifies accessed device or file location.
```

EVENT ID 17: PIPE CREATED

EventID: 17

EventName: Pipe Created

Logs:

- UtcTime: "2024-03-31 17:20:00"

  PipeName: "\\.\pipe\example_pipe" → Identifies created pipe.

  Image: "C:\\Windows\\System32\\services.exe" → Indicates creating program.

EVENT ID 20: WMI EVENT CONSUMER

EventID: 20

EventName: WMI Event Consumer

Logs:

- UtcTime: "2024-03-31 17:25:00"

  Consumer: "example_consumer" → Identifies WMI event consumer.

  CommandLine: "C:\\Windows\\System32\\wbem\\wmiprvse.exe" → Specifies command line executed by the consumer.

EVENT ID 18: PIPE CONNECTED

```
EventID: 18
EventName: Pipe Connected
Logs:

  - UtcTime: "2024-03-31 17:30:00"
    PipeName: "\\.\pipe\example_pipe"  ──→ Identifies connected pipe.
    Image: "C:\\Windows\\System32\\svchost.exe" ──→ Indicates program connecting to the pipe.
```

EVENT ID 4: SYSMON CONFIGURATION CHANGE

```
EventID: 4
EventName: Sysmon Configuration Change
Logs:

  - UtcTime: "2024-03-31 17:35:00"
    Configuration: "EnableNetworkConnectionRule: true, EnableImageLoadRule: false"
```
Specifies the updated configuration settings.

EventID: 19

EventName: WMI Event Filter

Logs:

- UtcTime: "2024-03-31 17:40:00"

  Operation: "Created" ——→Indicates whether the filter was created,

  Consumer: "example_consumer" ——→Identifies the consumer associated with the filter.

  FilterName: "example_filter" ——→Specifies the name of the filter.

EVENT ID 21: WMI FILTER ACTIVITY

EventID: 21

EventName: WMI Filter Activity

Logs:

- UtcTime: "2024-03-31 17:45:00"

  Operation: "Evaluated" ——→Indicates whether the filter was evaluated, applied, or removed.

  Result: "True" ——→Specifies the result of the filter evaluation, such as "True" or "False".

```
EventID: 7
EventName: Image Load
Logs:
    - UtcTime: "2024-03-31 17:50:00"
      ProcessGuid: "ABCDEFGH-1234-5678-9012-IJKLMNOPQRST"  ──▶ Identifies the loading process.
      ProcessId: 13001  ──▶ Unique process identifier.
      Image: "C:\\Windows\\System32\\notepad.exe"  ──▶ Indicates the program or DLL loaded.
      ImageLoaded: "C:\\Windows\\System32\\notepad.exe"
      Hashes: "MD5: A1B2C3D4E5F6G7H8I9J10K11L12M13N14"
      Description: "Notepad"  ──▶ Unique process identifier.
      Product: "Microsoft Corporation"
      Company: "Microsoft Corporation"
      OriginalFilename: "notepad.exe"
```

EVENT ID 22: DNS QUERY

```
EventID: 22
EventName: DNS Query
Logs:
    - UtcTime: "2024-03-31 17:55:00"
      QueryName: "example.com"  ──▶ Identifies the domain being queried.
      QueryStatus: "NoError"  ──▶ Indicates whether the query was successful or encountered an error.
```

EVENT ID 23: FILE DELETE

```
EventID: 23
EventName: File Delete
Logs:
  - UtcTime: "2024-03-31 18:00:00"
    ProcessGuid: "ABCDEFGH-1234-5678-9012-IJKLMNOPQRST"
    ProcessId: 14001
    Image: "C:\\Windows\\System32\\cmd.exe"
    TargetFilename: "C:\\Users\\User\\Documents\\example.txt"
```

ProcessGuid → Identifies the process responsible for the deletion.

ProcessId → Unique process identifier.

Image → Indicates the program performing the deletion.

TargetFilename → Specifies the file that was deleted.

EVENT ID 15: FILE CREATE STREAM HASH

```
EventID: 15
EventName: File Create Stream Hash
Logs:
  - UtcTime: "2024-03-31 18:05:00"
    ProcessGuid: "ABCDEFGH-1234-5678-9012-IJKLMNOPQRST"
    ProcessId: 15001
    Image: "C:\\Windows\\System32\\notepad.exe"
    TargetFilename: "C:\\Users\\User\\Documents\\example.txt"
    StreamName: "stream1"
    Hash: "SHA256: 0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"
```

ProcessGuid → Identifies the process that created the file stream.

ProcessId → Unique process identifier.

Image → Indicates the program responsible for the action.

TargetFilename → Indicates the program responsible for the action.

EVENT ID 24: CLIPBOARD EVENT

```
EventID: 24
EventName: Clipboard Event
Logs:
  - UtcTime: "2024-03-31 18:10:00"
    ProcessGuid: "ABCDEFGH-1234-5678-9012-IJKLMNOPQRST"
    ProcessId: 16001
    Image: "C:\\Windows\\System32\\notepad.exe"
    ClipboardText: "example clipboard text"
```

Identifies the process involved in the clipboard event.

Unique process identifier.

Indicates the program responsible for the action.

Specifies the text copied to or from the clipboard.

EVENT ID 16: SYSMON CONFIGURATION STATE CHANGE

```
EventID: 16
EventName: Sysmon Configuration State Change
Logs:
  - UtcTime: "2024-03-31 18:15:00"
    ConfigurationState: "Enabled"
    Hash: "SHA256: 0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"
    ConfigurationFile: "C:\\Windows\\System32\\sysmon.xml"
```

Indicates whether Sysmon is enabled or disabled.

Ensures integrity of the configuration file.

Specifies the location of the configuration file.

EVENT ID 25: PROCESS TAMPERING

```
EventID: 25
EventName: Process Tampering
Logs:

  - UtcTime: "2024-03-31 18:20:00"
    ProcessGuid: "ABCDEFGH-1234-5678-9012-IJKLMNOPQRST"
    ProcessId: 17001
    Image: "C:\\Windows\\System32\\svchost.exe"
    TamperingType: "CodeInjection"
```

Identifies the process affected by tampering.

Unique process identifier.

Indicates the program affected by tampering.

Specifies the method of process tampering.

EVENT ID 26: FILE DELETE DETECTED

```
EventID: 26
EventName: File Delete Detected
Logs:

  - UtcTime: "2024-03-31 18:25:00"
    ProcessGuid: "ABCDEFGH-1234-5678-9012-IJKLMNOPQRST"
    ProcessId: 18001
    Image: "C:\\Windows\\System32\\cmd.exe"
    TargetFilename: "C:\\Users\\User\\Documents\\example.txt"
```

Identifies the process responsible for file deletion.

Unique process identifier.

Indicates the program responsible for the action.

Specifies the file that was deleted.

EVENT ID 255: SYSMON ERROR

```
EventID: 255
EventName: Sysmon Error
Logs:

  - UtcTime: "2024-03-31 18:30:00"
    ErrorCode: 1001          ──→ Identifies the type of error encountered.
    ErrorMessage: "Error: Unable to initialize driver."  ──→ Provides details about the error
                                                               encountered.
```

CONFIGURATION OPTIONS:

```
ConfigurationOptions:                     Determines where logs are stored, ensuring data
    ArchiveDirectory: "C:\\Sysmon\\Logs"  ──→ retention.
    CaptureClipboard: true        ──→ Monitors clipboard for potential data leaks.
    DriverName: "SysmonDrv"       ──→ Identifies the Sysmon driver for system integration.
    HashAlgorithms: "SHA256,SHA1,MD5"
    DnsLookup: true                   ──→ Specifies hash algorithms for file integrity verification.
    CheckRevocation: true     ──→ Logs DNS queries for network monitoring.
    FieldSizes:
      - NetworkProtocol: 50
      - ImageLoaded: 100
      - ParentCommandLine: 150
    FilterOptions: "IncludeRegistry"
```