EDR Internals From a Defenders Perspective

FalconForce
Olaf Hartong

Defensive Specialist @ FalconForce

Detection Engineer and Security Researcher

- Built and/or led Security Operations Centers
- Threat hunting, IR and Compromise assessments

Former documentary photographer
Father of 2 boys
“I like warm hugs”

@olafhartong
github.com/olafhartong
olaf@falconforce.nl
olafhartong.nl / falconforce.nl
What you can expect from this talk

- Microsoft Defender for Endpoint (MDE) capabilities
- What kind of telemetry can you work with
- Where does it get its telemetry from
- Analyzing its configuration
- Wrap up
Capability outline

What can it do for you?
Microsoft Defender for Endpoint

All-in-one solution for protecting Windows, Mac and Linux Endpoints

- Anti-Virus
- Attack Surface Reduction (ASR)
- Exploit Guard
- Application Control (WDAC)
- EDR Telemetry
- Incident Response
- Software Inventory / Vulnerability Management
- Network Sensor
- DLP

Some parts are also available natively on Windows. Defender for Endpoint integrates these parts into a combined product and allows for centralized logging and management.
Anti-Virus Engine

Leverages existing Microsoft Defender Anti-Virus product.
  • AV events are logged to M365 Defender Portal.

Signature-based detection (behavior + file characteristics).

Cloud-based detections where samples are uploaded to cloud for analysis and can be executed in a sandbox.

Great research on the signature database by Camille Mougey
(https://github.com/commial/experiments/tree/master/windows-defender/VDM)
Anti-Virus Engine

Exclusions

- Frequently used by attackers to allow their payload to pass, **monitor the registry changes**.

- Process exclusions apply to the children of the listed process. The listed process will **still** be scanned. Unless this file is added to the file exclusion list.

- These exclusions apply **ONLY** for the AV component, features like EDR and ASR still apply.
Anti-Virus Engine

Check what it flags on with DefenderCheck

Sometimes needs several changes to the source to not get detected anymore.

https://github.com/matterpreter/defendercheck
Attack Surface Reduction (ASR) rules

- ~16 rules to reduce the attack surface of Windows.
- Rules can be enabled and disabled via Reg keys / Group Policy.
- Can be configured to Block or only Audit.
- Events are logged in M365 Advanced Hunting tables.

https://blog.palantir.com/microsoft-defender-attack-surface-reduction-recommendations-a5c7d41c3cf8
Attack Surface Reduction (ASR) rules

The rules (currently) primarily look for file / path names or commandlines, not signer information or other unique attributes. This allows an attacker to bypass them.

```lang
if l_0_4:find(l_0_5 .. "\microsoft\word\", 1, true) ~= nil then
  return mp.CLEAN
end
if l_0_4:find(l_0_5 .. "\microsoft\internet explorer\quick launch", 1, true) ~= nil then
  return mp.CLEAN
end
if l_0_4:find(l_0_5 .. "\roaming\microsoft\", 1, true) ~= nil then
  return mp.CLEAN
end
```
Windows Defender Application Control (WDAC)

Used to control which drivers and applications are allowed to run, does not require license! Successor to AppLocker, available in Windows 10 and up and Server 2016+

Policies can be layered and built to allow on deny based on:

- The codesigning certificate(s)
- Attributes in the PE header
- Reputation in the Microsoft's Intelligent Security Graph
- The path from which the app or file is launched
- The parent process
- The launching identity

Excellent blogs on this by Matt Graeber [https://mattifestation.medium.com](https://mattifestation.medium.com)
EDR Telemetry

Relies on a separate Windows Service, exclusive to MDE called ‘Sense’ running via MsSense.exe.

Collects relevant data from running system, for example:

- File Events (File Creation, Deletion).
- Network Connections.
- Suspicious API usage such as Reading memory from another process.

All events are logged and stored in ‘Advanced Hunting’ tables where they can be queried, and custom detection rules can be created to detect unwanted behavior.
EDR Telemetry

Which events are logged is controlled and configured by Microsoft.

- For example: list of registry keys that are monitored is fixed and cannot be extended.
- Focus on events that change the system.

Some events are (heavily) sampled to avoid excessive logging taking place, most notably:

- Network connections.
- File writes.
- Less events are logged from trusted processes (Microsoft-signed).
- Some events such as reading memory from a remote process are limited to LSASS process.

Main data source is Event Tracing for Windows (ETW).

- Over 65 different providers queried.
- This includes ‘private’ ETW logs, such as Threat Intelligence.
Data Storage

Pay per device / user.

• Includes the storage of generated events.
• Detailed information available for 30 days.
• Timeline/condensed data available for 180 days.

Longer retention possible by copying data to other solutions such as Azure Dataspaces or Azure Sentinel.

• Should be approximately 15-20MB per device per day.
What kind of data can I build detections on hunt with?
Data schema

ActionType
- AntivirusScanCompleted
- ShellLinkCreateFileEvent
- AsrOfficeMacroWin32ApiCallsAudited
- ProcessPrimaryTokenModified
- AntivirusReport
- LdapSearch

- DriverLoad
- PnpDeviceConnected
- ReadProcessMemoryApiCall
- NtAllocateVirtualMemoryApiCall
- PowerShellCommand
- FirewallInboundConnectionBlocked
- NtMapViewOfSectionRemoteApiCall
- NtAllocateVirtualMemoryRemoteApiCall
- CreateRemoteThreadApiCall
- ExploitGuardWin32SystemCallBlocked
- GetClipboardData
- GetAsyncKeyStateApiCall
- FirewallOutboundConnectionBlocked
- ScreenshotTaken
- BrowserLaunchedToOpenUrl
- ScheduledTaskCreated
- AsrOfficeProcessInjectionAudited
- DeviceBootAttestationInfo
- AsrExecutableOfficeContentAudited
- ScheduledTaskDeleted
- ExploitGuardNonMicrosoftSignedAudited
- ProcessCreatedUsingWmiQuery
- ExploitGuardNonMicrosoftSignedBlocked
- ExploitGuardAcgEnforced
- ExploitGuardNetworkProtectionAudited
- FirewallInboundConnectionToAppBlocked
- AsrUntrustedExecutableAudited
- UsbDriveMount
- WriteProcessMemoryApiCall
- AsrOfficeChildProcessAudited
- UsbDriveUnmount
- ExploitGuardChildProcessAudited
- ControlledFolderAccessViolationAudited
- UserAccountCreated
- AntivirusScanCancelled
- ControlledFolderAccessViolationBlocked
- AND MUCH, MUCH MORE
Snatch them from the portal

az login --use-device-code -t [TENANTNAME]

az account get-access-token --resource https://securitycenter.microsoft.com/mtp

Snatch them from the portal

az login --use-device-code -t [TENANTNAME]

az account get-access-token --resource https://securitycenter.microsoft.com/mtp

MDE default alert coverage

Slide removed TLP: Amber
### MDE telemetry potential mapping to MITRE ATT&CK

<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution</th>
<th>Persistence</th>
<th>Privilege Escalation</th>
<th>Defense Evasion</th>
<th>Credential Access</th>
<th>Discovery</th>
<th>Lateral Movement</th>
<th>Collection</th>
<th>Command and Control</th>
<th>Exfiltration</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drive-by Compromise</td>
<td>Exploit Public-Facing Application</td>
<td>External Remote Services</td>
<td>Hardware Additions</td>
<td>Phishing</td>
<td>Replication Through Removable Media</td>
<td>Supply Chain Compromise</td>
<td>Trusted Relationship</td>
<td>Valid Accounts</td>
<td>System Services</td>
<td>User Execution</td>
<td>Windows Management Instrumentation</td>
</tr>
<tr>
<td>Command and Scripting Interface</td>
<td>Exploitation for Client Execution</td>
<td>Malicious Process Communication</td>
<td>Native API</td>
<td>Scheduled TaskJob</td>
<td>Shared Modules</td>
<td>Comromise Client Software Binary</td>
<td>Create Account</td>
<td>Create or Modify System Process</td>
<td>Event Triggered Execution</td>
<td>Windows Management Instrumentation</td>
<td></td>
</tr>
<tr>
<td>Pre-OS Boot</td>
<td>Boot or Login Autostart Execution</td>
<td>Boot or Login Initialization</td>
<td>Scripted Scripts</td>
<td>Browser Extensions</td>
<td>Domain Policy</td>
<td>Domain Policy Configuration</td>
<td>Domain Policy Modification</td>
<td>Escape to Host</td>
<td>Event Triggered Execution</td>
<td>Exploitation for Privilege Escalation</td>
<td></td>
</tr>
<tr>
<td>Office Application Startup</td>
<td>Exploit for Privilege Escalation</td>
<td>Exploit</td>
<td>Staged Execution</td>
<td>Exploit for Defense Evasion</td>
<td>Exploit</td>
<td>Exploit</td>
<td>Exploit</td>
<td>Exploit</td>
<td>Exploit</td>
<td>Exploit</td>
<td></td>
</tr>
</tbody>
</table>
MDE telemetry potential mapping to MITRE ATT&CK

<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution</th>
<th>Persistence</th>
<th>Privilege Escalation</th>
<th>Defense Evasion</th>
<th>Credential Access</th>
<th>Discovery</th>
<th>Lateral Movement</th>
<th>Collection</th>
<th>Command and Control</th>
<th>Exfiltration</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exploit Public-Facing Application</td>
<td>Exploitation for Client Execution</td>
<td>BITS Jobs</td>
<td>Exploit of Remote Services</td>
<td>BITS Jobs</td>
<td>Password Discovery</td>
<td>Internal Spearphishing</td>
<td>Communication Through Removable Media</td>
<td>Data Transfer Size Limits</td>
<td>Automated Exfiltration</td>
<td>Data Encrypted for Impact</td>
<td></td>
</tr>
<tr>
<td>Hardware Additions</td>
<td>Multi-Process Communication</td>
<td>Native API</td>
<td>Obfuscated/Decoded Files or Information</td>
<td>Cloud Service Dashboard</td>
<td>Remote Service Session</td>
<td>Data Obfuscation</td>
<td>Exfiltration Over Other Network Medium</td>
<td>Exfiltration Over Other Network Medium</td>
<td>Exfiltration Over Other Network Medium</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phishing</td>
<td>Malicious Code Execution</td>
<td>Native API</td>
<td>Obfuscated/Decoded Files or Information</td>
<td>Cloud Service Dashboard</td>
<td>Remote Service Session</td>
<td>Data Obfuscation</td>
<td>Exfiltration Over Other Network Medium</td>
<td>Exfiltration Over Other Network Medium</td>
<td>Exfiltration Over Other Network Medium</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Replication Technology Compromised</td>
<td>Supply Chain Compromise</td>
<td>Native API</td>
<td>Obfuscated/Decoded Files or Information</td>
<td>Cloud Service Dashboard</td>
<td>Remote Service Session</td>
<td>Data Obfuscation</td>
<td>Exfiltration Over Other Network Medium</td>
<td>Exfiltration Over Other Network Medium</td>
<td>Exfiltration Over Other Network Medium</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trusted Relationship Compromised</td>
<td>Trusted Relationship Compromised</td>
<td>Native API</td>
<td>Obfuscated/Decoded Files or Information</td>
<td>Cloud Service Dashboard</td>
<td>Remote Service Session</td>
<td>Data Obfuscation</td>
<td>Exfiltration Over Other Network Medium</td>
<td>Exfiltration Over Other Network Medium</td>
<td>Exfiltration Over Other Network Medium</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Valid Accounts</td>
<td>Valid Accounts</td>
<td>Native API</td>
<td>Obfuscated/Decoded Files or Information</td>
<td>Cloud Service Dashboard</td>
<td>Remote Service Session</td>
<td>Data Obfuscation</td>
<td>Exfiltration Over Other Network Medium</td>
<td>Exfiltration Over Other Network Medium</td>
<td>Exfiltration Over Other Network Medium</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Process Injection** (8/8)

- Score: 80
- Aggregate Score (average): 92.22
- Process Injection (T1055)
- Process file modification: Modify Registry
- module load: Obfuscated files or process access: OS api execution: Pre-OS Boot

**Steal or Forge Kerberos Tickets** (0/4)

- Steal Web Session Cookie
- Two-Factor Authentication
- DeviceFileEvents_FileModified
- DeviceFileEvents_FileRenamed
- DeviceEvents_OpenProcessApiCall
- DeviceEvents_CreateRemoteThreadApiCall
- System Network Configuration

**Process Discovery** (2/3)

- Query Registry
- Process Discovery
- Software Discovery
- System Information Discovery
- System Information Discovery
- System Location Discovery
- System Network Configuration

**Exfiltration** (8 techniques)

- Automated Exfiltration
- Data Transfer Size Limits
- Exfiltration Over Alternate Protocol
- Exfiltration Over G2 Channel
- Exfiltration Over Other Network Medium
- Exfiltration Over Other Network Medium
- Exfiltration Over Other Network Medium
- Exfiltration Over Other Network Medium

**Impact** (13 techniques)

- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation
- Defacement
- Disk Wipe
- Endpoint Denial of Service
- Firmware Corruption
- Network Denial of Service
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot
Data potential for 299 techniques
Visualizing relationships
Where does it get its telemetry?

This is important to understand bypass and tampering opportunities as well as possible blind spots.
Kernel Callbacks

The kernel's callback mechanism provides a general way for drivers to request and provide notification when certain conditions are satisfied.
Kernel Callbacks

* Process
  * Callback [type 3] - Handle 0xFFFFFB20FABC50910 (@ 0xFFFFFB20FABC50930)
    PreOperation : 0xFFFFFB80310D19A60 [mssecfilt.sys + 0x19a60]
  * Callback [type 3] - Handle 0xFFFFFB20FAE0300E0 (@ 0xFFFFFB20FAE030100)
    PreOperation : 0xFFFFFB80314803D90 [WdFilter.sys + 0x43d90]
  * Callback [type 1] - Handle 0xFFFFFB20FAE42290 (@ 0xFFFFFB20FAE42280)
    PreOperation : 0xFFFFFB80312305080 [SysmonDrv.sys + 0x5080]
    PostOperation : 0xFFFFFB803123092C0 [SysmonDrv.sys + 0x92c0]

Open
  - 0xFFFFFB803CEB5830 [ntoskrnl.exe + 0x6b5830]

Close
  - 0xFFFFFB803CEE48B0 [ntoskrnl.exe + 0x6e48b0]

Delete
  - 0xFFFFFB803CE1A210 [ntoskrnl.exe + 0x61a210]

Security
  - 0xFFFFFB803CE691A0 [ntoskrnl.exe + 0x6691a0]
Event Tracing for Windows

Event Tracing for Windows (ETW) provides a mechanism to trace and log events that are raised by user-mode applications and kernel-mode drivers.

ETW is implemented in the Windows operating system and provides a fast, reliable, and versatile set of event tracing features. Its architecture consists of three layers:

- Event providers
- Event consumers
- Event tracing sessions

Great reference material by Matt Graeber:
https://blog.palantir.com/tampering-with-windows-event-tracing-background-offense-and-defense-4be7ac62ac63
MsSense.exe ETW Providers

MsSense is one of the core components of MDE that routes the telemetry which it gathers in its own set of providers.

Curious about the traces it utilizes I had a look at the trace logging metadata with a script created by Matt Graeber.

```
PS C:\Users\olafhartong\Downloads> $Result = Get-TraceLoggingMetadata -Path 'C:\Program Files\Windows Defender Advanced Threat Protection\MsSense.exe'
PS C:\Users\olafhartong\Downloads> $Result.Providers

<table>
<thead>
<tr>
<th>ProviderGUID</th>
<th>ProviderName</th>
<th>ProviderGroupGUID</th>
</tr>
</thead>
<tbody>
<tr>
<td>65a1b6fc-4c24-59c9-e3f3-ad11ac518b41</td>
<td>Microsoft.Windows.Sense.Client</td>
<td>5ecb8bac-b930-47f5-a8a4-e8253529eddb7</td>
</tr>
<tr>
<td>c68a18cc-7e07-400f-ae3b-d521c5db96f</td>
<td>Microsoft.Windows.Sense.GeneratedETW</td>
<td>d0b1a44b-5ab3-4ff2-bb52-c2bb98be8f3</td>
</tr>
<tr>
<td>1dc74222-9e76-5499-e1b5-8dbb4982ff77</td>
<td>Microsoft.Windows.Sense.SensorHub</td>
<td>c5a3a379-e5b9-43da-9175-589af2ce2cc7</td>
</tr>
<tr>
<td>cb2ff72d-d4e4-585d-33f9-f3a395c40be7</td>
<td>Microsoft.Windows.Sense.CyberEvents</td>
<td>51dae91-c3c5-5807-b064-c2561c16d78e</td>
</tr>
<tr>
<td>b3861234-4273-58c5-545b-8b3611343471</td>
<td>Microsoft.Windows.Sense.CyberEvents</td>
<td>4f56731a-89cf-4782-b3e9-dce8c0076ba</td>
</tr>
<tr>
<td>458bba94-53ce-54e6-d150-9636aceaf886</td>
<td>Microsoft.Windows.Sense.SenseIR</td>
<td>f68c769c-cc2a-502e-ae3-115c2eda66f7</td>
</tr>
<tr>
<td>458bba94-53ce-54e6-d150-9636aceaf886</td>
<td>Microsoft.Windows.Sense.CollectionEtw</td>
<td>d0b1a44b-5ab3-4ff2-bb52-c2bb98be8f3</td>
</tr>
</tbody>
</table>
```

https://gist.github.com/mattifestation/edbac1614694886c8ef4583149f53658
MsSense.exe ETW data

The traced events are stored into a SQLite database in a protected folder on the file system. The table name used is AsimovEvents.

Asimov was the code name in 2014 for the Unified Telemetry Client, which is now deprecated and is replaced by the DiagTrack agent.

On regular intervals the contents of the database gets uploaded and the data gets flushed.
Tracing these providers

Curious to see what these providers contained I fired up Sealighter to trace these file to a file.

Sealighter is highly configurable and can subscribe to multiple providers at once, user and kernel traces.

Outputs to Stdout, JSON file, or Windows Event Log

https://github.com/pathToFile/Sealighter

Primarily built for research, if you want to use custom ETW events for monitoring SilkETW is probably more suited.

```plaintext
:c:\tools\service\sealighter.exe config.json
Session Name: MDK-traces
Outputs: file
User Provider: {65ab6ef-c424-59c9-ae3f-ad11ac510bf41} Trace Name: Microsoft.Windows.Sense.Client Keywords: All No event filters
User Provider: {c0841be-c7e8-f80f-ae3b-d521c5dbd96f} Trace Name: Microsoft.Windows.Sense.GeneratedETW Keywords: All No event filters
User Provider: {1de472c2-0c76-5486-5b58-8dd8482f77} Trace Name: Microsoft.Windows.Sense.SensorHub Keywords: All No event filters
User Provider: {c2ff72d-d4e4-585d-33f9-f3a39c49be7} Trace Name: Microsoft.Windows.Sense.CyberEvents Keywords: All No event filters
User Provider: {b3611234-4273-545b-8b3611343471} Trace Name: Microsoft.Windows.Sense.CyberEvents Keywords: All No event filters
User Provider: {31459be-26a1-cf39-e3f3-ad11ac510bf41} Trace Name: Microsoft.Windows.Sense.Ndr Keywords: All No event filters
User Provider: {60160f9-31e-5cf2-2d59-6ed005ad02b} Trace Name: Microsoft.Windows.Sense.Ndr Keywords: All No event filters
User Provider: {588ba94-53ce-54e6-6b90-9636abea6b86} Trace Name: Microsoft.Windows.Sense.SensorTR Keywords: All No event filters
User Provider: {8ff433a-b5a8-4800-a81d-b5888a96d04} Trace Name: Microsoft.Windows.Sense.SensorTrm Keywords: All No event filters
User Provider: {a8c769c-cc2b-582e-ae32-115c2eda66f7} Trace Name: Microsoft.Windows.Sense.CollectionEtw Keywords: All No event filters
User Provider: {2f68bde7-7ec8-518d-559e-b1679239484c} Trace Name: Microsoft.Windows.Defender Keywords: All No event filters
User Provider: {02cdbe67-b2af-57a0-969b-efb0adc0b915} Trace Name: Microsoft.Windows.Sec.Driver Keywords: All No event filters
Starting User Trace...
```
ContextInfo

Severity = Informational
Host Name = ConsoleHost
Host Version = 5.1.19041.1645
Host ID = 3e0fa74-3894-4a14-bf02-f4adbe38b6c6
Host Application = powershell.exe
Engine Version = 5.1.19041.1645
Runspace ID = 5c294dd3-8d69-4078-93e3-2c88fbd70d22
Pipeline ID = 16
Command Name = Get-Command
Command Type = Cmdlet
Script Name =
Command Path =
Sequence Number = 57
User = 0XFF-PC-OLAF\olafhartong
Connected User =
Shell ID = Microsoft.PowerShell

Payload!!!Command Get-Command is Started.

Cmdlet start

olafhartong
What is the binary jibberish?

The data is serialized with Bond.

Bond is a cross-platform framework for working with schematized data. It supports cross-language de/serialization and powerful generic mechanisms for efficiently manipulating data. Bond is broadly used at Microsoft in most of their services.

So far I have not found the schema's for these streams.

Next question is where is that data coming from, it clearly looks like PowerShell event logging.

https://github.com/microsoft/bond
Where is the data coming from?

No direct subscription for anything other than the EventLog service

So is MDE also making use of the regular EventLogs??

https://github.com/jthuraisamy/TelemetrySourceer
**DiagTrack**

MDE piggybacks of the Diagtrack service to get most of the ETW event telemetry. This service uses the DiagTrack-Listener subscription. MDE is not subscribing to all these providers itself.

By default, only Local Administrators, Performance Log Users, and services running as LocalSystem, LocalService, NetworkService can control trace sessions and consume event data.

Since MDE uses the MsSense service, which runs as System this is fine.

Looking into this service I learnt this service is not protected. When you stop the DiagTrack service, there is no telemetry sent to the cloud anymore.

```
C:\Users\falconforce>sc qprotection diagtrack
[SC] QueryServiceConfig2 SUCCESS
SERVICE diagtrack PROTECTION LEVEL: NONE.
```
MDE Configuration

Like any product MDE also requires a configuration to know what to log.

This configuration is maintained by Microsoft and is downloaded from the internet on a regular basis.

It is stored on the box, in a non-clear text format. Additionally it is signed and not easily tampered with.

The exact details are up to you to find out ;) (sorry, not sorry)
Configuration item examples

- Telemetry sources (ETW providers, Registry Keys etc.)
- Exclusions and Filters (for example; extensions, process names, certificate signatures)
- Capping (global and per event distinct field combination)
- Dynamic data collection
- Agent configuration
- Quotas (volumetric per time period)
Configuration stats

- ~70k lines of JSON
- ~65 ETW Providers utilized
- ~500 registry paths monitored
- ~60 data collection commands that fire frequently
- Different settings for high latency environments
- Elevated child process recording quotas for scripting tools and browsers
Configuration - ETW Providers (a selection)

Generic ETW CreateFile Pattern
Microsoft-Windows-ThreatIntelligence
Microsoft-Windows-DNS-Client
Microsoft.Web.Platform
Microsoft-Windows-Win32k
Microsoft-Antimalware-Scan-Interface
Microsoft-Antimalware-UacScan
Microsoft-Windows-TCPIP
Microsoft-Windows-WMI-Activity
Powershell cmdlets
Microsoft-Windows-AppLocker
Microsoft-Windows-CodeIntegrity
Microsoft.Windows.OLE.Clipboard
Microsoft-Windows-RemoteDesktopServices-RdpCoreTS
Microsoft-Windows-RPC
Microsoft-Windows-SEC
SecureETW

< Very interesting provider, only for AV/EDRs
< We've just seen these events
< What would this be?
SecureETW

Listed in the configuration with the following ProviderGuid: {54849625-5478-4994-A5BA-3E3B0328C30D}

Also known as Microsoft-Windows-Security-Auditing
What does that config look like?

```json
{
  "capping": {
    "globalCapping": {
      "capping": 1000
    },
    "localCapping": {
      "id": "LogonLocalCapping",
      "expirationPeriodInHours": 1,
      "fields": {
        "fieldName": "TargetUserName"
      },
      "filters": {
        "expressionType": "Operator",
        "operator": "Not",
        "expressions": [
          < some SID filters
        ]
      }
    }
  },
  "properties": {
    "source": "SubjectUserSid",
    "type": "SID"
  }},
  "source": "SubjectDomainName",
  "type": "UNICODESTRING",
  "scrubType": "Domain",
  "scrubMethod": "Simple",
  "scrubProfile": 514
},
  "source": "SubjectLogonId",
  "type": "HEXINT64",
  "Transformer": "ExtractUser",
  "targetFieldNames": ["TargetAccountEntity"],
  "transformerValues": {
    "SID"
  },
  "source": "TargetUserSid",
  "type": "UNICODESTRING",
  "scrubType": "User",
  "scrubMethod": "Simple",
  "scrubProfile": 514
},
  "source": "TargetDomainName",
  "type": "UNICODESTRING",
  "scrubType": "Domain",
  "scrubMethod": "Simple",
  "scrubProfile": 516
```

< and much more>
So, which other EventIDs is it looking for

Currently, the following Events are traced from the Security log:

<table>
<thead>
<tr>
<th>eventID name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5858</td>
<td>Persistent cryptographic key operation.</td>
</tr>
<tr>
<td>5859</td>
<td>Persistent cryptographic key export.</td>
</tr>
<tr>
<td>4676</td>
<td>Taking Ownership on file from TrustedInstaller</td>
</tr>
<tr>
<td>4678</td>
<td>Taking Ownership on KEK Key</td>
</tr>
<tr>
<td>4664</td>
<td>HardLink Create Audit Event</td>
</tr>
<tr>
<td>4907</td>
<td>Sense tampering through object sacl change</td>
</tr>
<tr>
<td>4907</td>
<td>A service was installed</td>
</tr>
<tr>
<td>4624</td>
<td>Logon event</td>
</tr>
<tr>
<td>4625</td>
<td>An account failed to log on</td>
</tr>
<tr>
<td>4698</td>
<td>A scheduled task was created</td>
</tr>
<tr>
<td>4699</td>
<td>A scheduled task was deleted</td>
</tr>
<tr>
<td>4702</td>
<td>A scheduled task was updated</td>
</tr>
<tr>
<td>4728</td>
<td>A user account was created</td>
</tr>
<tr>
<td>4661</td>
<td>Plug and Play event</td>
</tr>
<tr>
<td>5824</td>
<td>Firewall service started</td>
</tr>
<tr>
<td>5825</td>
<td>Firewall service stopped</td>
</tr>
<tr>
<td>5831</td>
<td>Firewall app blocked from listening</td>
</tr>
<tr>
<td>5157</td>
<td>Firewall has blocked a connection outbound</td>
</tr>
<tr>
<td>7567</td>
<td>Credman - Read Credentials</td>
</tr>
<tr>
<td>5300</td>
<td>Vault Credential - Find Credential</td>
</tr>
<tr>
<td>5302</td>
<td>Vault Credential - Get Unique Credential</td>
</tr>
<tr>
<td>4648</td>
<td>Logon using explicit credentials</td>
</tr>
<tr>
<td>4719</td>
<td>System Audit Policy was changed</td>
</tr>
<tr>
<td>4724</td>
<td>An Attempt was made to reset an account password</td>
</tr>
<tr>
<td>4726</td>
<td>A user account was deleted</td>
</tr>
<tr>
<td>4732</td>
<td>A member was added to a security-enabled local group</td>
</tr>
<tr>
<td>4734</td>
<td>A local group account was deleted</td>
</tr>
<tr>
<td>4738</td>
<td>A user account was changed</td>
</tr>
<tr>
<td>4732</td>
<td>A member was added to a security-enabled local group</td>
</tr>
<tr>
<td>4724</td>
<td>Forbidden installation (MSP Audit)</td>
</tr>
<tr>
<td>4798</td>
<td>User’s local group membership was enumerated</td>
</tr>
<tr>
<td>4799</td>
<td>Security-enabled local group membership was enumerated</td>
</tr>
<tr>
<td>eventId</td>
<td>MDE-Name</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>5058</td>
<td>Persistent cryptographic key operation.</td>
</tr>
<tr>
<td>5059</td>
<td>Persistent cryptographic key export.</td>
</tr>
<tr>
<td>4670</td>
<td>Taking Ownership on File from TrustedInstaller</td>
</tr>
<tr>
<td>4670</td>
<td>Taking Ownership on MDE Key</td>
</tr>
<tr>
<td>4664</td>
<td>Hardlink Create Audit Event</td>
</tr>
<tr>
<td>4907</td>
<td>Sense tampering through object sacl change</td>
</tr>
<tr>
<td>4977</td>
<td>A service was installed</td>
</tr>
<tr>
<td>4624</td>
<td>logon event</td>
</tr>
<tr>
<td>4625</td>
<td>An account failed to log on</td>
</tr>
<tr>
<td>4698</td>
<td>A scheduled task was created</td>
</tr>
<tr>
<td>4699</td>
<td>A scheduled task was deleted</td>
</tr>
<tr>
<td>4702</td>
<td>A scheduled task was updated</td>
</tr>
<tr>
<td>4720</td>
<td>A user account was created</td>
</tr>
<tr>
<td>4718</td>
<td>Plug and Play event</td>
</tr>
<tr>
<td>5024</td>
<td>firewall service started</td>
</tr>
<tr>
<td>5025</td>
<td>Firewall service stopped</td>
</tr>
<tr>
<td>5031</td>
<td>Firewall app blocked from listening</td>
</tr>
<tr>
<td>5157</td>
<td>Firewall has blocked a connection outbound</td>
</tr>
<tr>
<td>5157</td>
<td>Firewall has blocked a connection inbound</td>
</tr>
<tr>
<td>5376</td>
<td>Credman - Credentials Backup</td>
</tr>
<tr>
<td>5379</td>
<td>Credman - Read Credentials</td>
</tr>
<tr>
<td>5380</td>
<td>Vault Credential - Find Credential</td>
</tr>
<tr>
<td>5381</td>
<td>Vault Credential - Enumerate Credentials</td>
</tr>
<tr>
<td>5382</td>
<td>Vault Credential - Get Unique Credential</td>
</tr>
<tr>
<td>4648</td>
<td>Logon using explicit credentials</td>
</tr>
<tr>
<td>4719</td>
<td>System Audit Policy was changed</td>
</tr>
<tr>
<td>4724</td>
<td>An Attempt was made to reset an account password</td>
</tr>
<tr>
<td>4726</td>
<td>A user account was deleted</td>
</tr>
<tr>
<td>4732</td>
<td>A member was added to a security-enabled local group</td>
</tr>
<tr>
<td>4731</td>
<td>Local group created</td>
</tr>
<tr>
<td>4732</td>
<td>A member was added to a security-enabled local group</td>
</tr>
<tr>
<td>4733</td>
<td>Local group removed</td>
</tr>
<tr>
<td>4734</td>
<td>Local group deleted</td>
</tr>
<tr>
<td>4738</td>
<td>A user account was changed</td>
</tr>
<tr>
<td>4732</td>
<td>A member was added to a security-enabled local group</td>
</tr>
<tr>
<td>6423</td>
<td>Forbidden installation (PNP Audit)</td>
</tr>
<tr>
<td>4798</td>
<td>User's local group membership was enumerated</td>
</tr>
<tr>
<td>4799</td>
<td>security-enabled local group membership was enumerated</td>
</tr>
</tbody>
</table>
Microsoft Audit Policy settings

Audit policy settings determine whether the operating system generates audit events when certain tasks are performed.

These settings can be configured on 4 levels:

- No Auditing (0)
- Success (1)
- Failure (2)
- Success and Failure (3)

https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/basic-security-audit-policies
Are all these events available on all machines?

<table>
<thead>
<tr>
<th>eventId</th>
<th>MDE-Name</th>
<th>AuditCategory</th>
<th>AuditSubCategory</th>
<th>Required setting</th>
<th>Win10 default</th>
<th>Default OK?</th>
</tr>
</thead>
<tbody>
<tr>
<td>5058</td>
<td>Persistent cryptographic key operation</td>
<td>Other System Events</td>
<td>Other System Events</td>
<td>3</td>
<td>3</td>
<td>TRUE</td>
</tr>
<tr>
<td>5059</td>
<td>Persistent cryptographic key export</td>
<td>Default</td>
<td>Default</td>
<td>1</td>
<td>0</td>
<td>FALSE</td>
</tr>
<tr>
<td>4670</td>
<td>Taking Ownership on File from TrustedInstaller</td>
<td>Other System Events</td>
<td>Other System Events</td>
<td>1</td>
<td>0</td>
<td>FALSE</td>
</tr>
<tr>
<td>4670</td>
<td>Taking Ownership on MDE Key</td>
<td>Authorization Policy Change</td>
<td>Authorization Policy Change</td>
<td>1</td>
<td>0</td>
<td>FALSE</td>
</tr>
<tr>
<td>4664</td>
<td>Hardlink Create Audit Event</td>
<td>File System</td>
<td>File System</td>
<td>1</td>
<td>0</td>
<td>FALSE</td>
</tr>
<tr>
<td>4992</td>
<td>Same tampering through object and change</td>
<td>Audit Policy Changes</td>
<td>Audit Policy Changes</td>
<td>1</td>
<td>1</td>
<td>TRUE</td>
</tr>
<tr>
<td>4697</td>
<td>A service was installed</td>
<td>Security System Extension</td>
<td>Security System Extension</td>
<td>1</td>
<td>0</td>
<td>FALSE</td>
</tr>
<tr>
<td>4697</td>
<td>A service was installed</td>
<td>Security System Extension</td>
<td>Security System Extension</td>
<td>1</td>
<td>0</td>
<td>FALSE</td>
</tr>
<tr>
<td>4698</td>
<td>A scheduled task was created</td>
<td>Other Object Access Events</td>
<td>Other Object Access Events</td>
<td>1</td>
<td>0</td>
<td>FALSE</td>
</tr>
<tr>
<td>4699</td>
<td>A scheduled task was deleted</td>
<td>Other Object Access Events</td>
<td>Other Object Access Events</td>
<td>1</td>
<td>0</td>
<td>FALSE</td>
</tr>
<tr>
<td>4702</td>
<td>A scheduled task was updated</td>
<td>Other Object Access Events</td>
<td>Other Object Access Events</td>
<td>1</td>
<td>0</td>
<td>FALSE</td>
</tr>
<tr>
<td>4720</td>
<td>A user account was created</td>
<td>User Account Management</td>
<td>User Account Management</td>
<td>1</td>
<td>1</td>
<td>TRUE</td>
</tr>
<tr>
<td>6416</td>
<td>Plug and Play event</td>
<td>Plug and Play Events</td>
<td>Plug and Play Events</td>
<td>1</td>
<td>0</td>
<td>FALSE</td>
</tr>
<tr>
<td>6416</td>
<td>Plug and Play event</td>
<td>Plug and Play Events</td>
<td>Plug and Play Events</td>
<td>1</td>
<td>0</td>
<td>FALSE</td>
</tr>
<tr>
<td>5062</td>
<td>Firewall event</td>
<td>Filtering Platform Connection</td>
<td>Filtering Platform Connection</td>
<td>1</td>
<td>3</td>
<td>FALSE</td>
</tr>
<tr>
<td>5031</td>
<td>Firewall app blocked from listening</td>
<td>Other System Events</td>
<td>Other System Events</td>
<td>1</td>
<td>0</td>
<td>FALSE</td>
</tr>
<tr>
<td>5157</td>
<td>Firewall has blocked a connection outbound</td>
<td>Filtering Platform Connection</td>
<td>Filtering Platform Connection</td>
<td>2</td>
<td>0</td>
<td>FALSE</td>
</tr>
<tr>
<td>5157</td>
<td>Firewall has blocked a connection inbound</td>
<td>Filtering Platform Connection</td>
<td>Filtering Platform Connection</td>
<td>2</td>
<td>0</td>
<td>FALSE</td>
</tr>
<tr>
<td>5379</td>
<td>Credman - Read Credentials</td>
<td>User Account Management</td>
<td>User Account Management</td>
<td>3</td>
<td>1</td>
<td>TRUE</td>
</tr>
<tr>
<td>5380</td>
<td>Vault Credential - Find Credential</td>
<td>Other Logon/Logoff Events</td>
<td>Other Logon/Logoff Events</td>
<td>2</td>
<td>0</td>
<td>FALSE</td>
</tr>
<tr>
<td>5381</td>
<td>Vault Credential - Enumerate Credentials</td>
<td>Other Logon/Logoff Events</td>
<td>Other Logon/Logoff Events</td>
<td>2</td>
<td>0</td>
<td>FALSE</td>
</tr>
<tr>
<td>5382</td>
<td>Vault Credential - Get Unique Credential</td>
<td>Other Logon/Logoff Events</td>
<td>Other Logon/Logoff Events</td>
<td>2</td>
<td>0</td>
<td>FALSE</td>
</tr>
<tr>
<td>4719</td>
<td>System Audit Policy was changed</td>
<td>Security Group Management</td>
<td>Security Group Management</td>
<td>1</td>
<td>1</td>
<td>TRUE</td>
</tr>
<tr>
<td>4724</td>
<td>An Attempt was made to reset an account password</td>
<td>User Account Management</td>
<td>User Account Management</td>
<td>3</td>
<td>1</td>
<td>FALSE</td>
</tr>
<tr>
<td>4725</td>
<td>A user account was deleted</td>
<td>User Account Management</td>
<td>User Account Management</td>
<td>1</td>
<td>1</td>
<td>TRUE</td>
</tr>
<tr>
<td>4732</td>
<td>A member was added to a security-enabled local group</td>
<td>Security Group Management</td>
<td>Security Group Management</td>
<td>1</td>
<td>1</td>
<td>TRUE</td>
</tr>
<tr>
<td>4732</td>
<td>A member was added to a security-enabled local group</td>
<td>Security Group Management</td>
<td>Security Group Management</td>
<td>1</td>
<td>1</td>
<td>TRUE</td>
</tr>
<tr>
<td>4731</td>
<td>Local group created</td>
<td>Security Group Management</td>
<td>Security Group Management</td>
<td>1</td>
<td>1</td>
<td>TRUE</td>
</tr>
<tr>
<td>4731</td>
<td>Local group created</td>
<td>Security Group Management</td>
<td>Security Group Management</td>
<td>1</td>
<td>1</td>
<td>TRUE</td>
</tr>
<tr>
<td>4734</td>
<td>Local group deleted</td>
<td>Security Group Management</td>
<td>Security Group Management</td>
<td>1</td>
<td>1</td>
<td>TRUE</td>
</tr>
<tr>
<td>4734</td>
<td>Local group deleted</td>
<td>Security Group Management</td>
<td>Security Group Management</td>
<td>1</td>
<td>1</td>
<td>TRUE</td>
</tr>
<tr>
<td>4798</td>
<td>A user account was changed</td>
<td>User Account Management</td>
<td>User Account Management</td>
<td>1</td>
<td>1</td>
<td>TRUE</td>
</tr>
<tr>
<td>4798</td>
<td>A user account was changed</td>
<td>User Account Management</td>
<td>User Account Management</td>
<td>1</td>
<td>1</td>
<td>TRUE</td>
</tr>
<tr>
<td>6423</td>
<td>Forbidden installation (PNP Audit)</td>
<td>Plug and Play Events</td>
<td>Plug and Play Events</td>
<td>1</td>
<td>0</td>
<td>FALSE</td>
</tr>
<tr>
<td>5378</td>
<td>A user’s local group membership was enumerated</td>
<td>User Account Management</td>
<td>User Account Management</td>
<td>1</td>
<td>1</td>
<td>TRUE</td>
</tr>
</tbody>
</table>
So, we seem to be having some blind spots.

Fortunately, the MDE team tries to help you a bit here.

They’ll enable some of the settings when you install the agent.

<table>
<thead>
<tr>
<th>eventId</th>
<th>MDE-Name</th>
<th>AuditCategory</th>
<th>AuditSubCategory</th>
<th>Required Setting</th>
<th>Win10 Default</th>
<th>Win10 + Defender</th>
<th>DefaultOk?</th>
<th>PostDefenderInstall</th>
</tr>
</thead>
<tbody>
<tr>
<td>4670</td>
<td>Taking Ownership on File from TrustedInstaller</td>
<td>Policy Change</td>
<td>Authorization Policy Change</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>4670</td>
<td>Taking Ownership on MDE Key</td>
<td>Policy Change</td>
<td>Authorization Policy Change</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>4664</td>
<td>Harlink Create Audit Event</td>
<td>Object Access</td>
<td>File System</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>FALSE</td>
<td>TRUE</td>
</tr>
<tr>
<td>4698</td>
<td>A service was installed</td>
<td>System</td>
<td>Security System Extension</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>FALSE</td>
<td>TRUE</td>
</tr>
<tr>
<td>4699</td>
<td>A scheduled task was created</td>
<td>Object Access</td>
<td>Other Object Access Events</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>FALSE</td>
<td>TRUE</td>
</tr>
<tr>
<td>4702</td>
<td>A scheduled task was deleted</td>
<td>Object Access</td>
<td>Other Object Access Events</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>FALSE</td>
<td>TRUE</td>
</tr>
<tr>
<td>6416</td>
<td>Plug and Play event</td>
<td>Detailed Tracking</td>
<td>Plug and Play Events</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>FALSE</td>
<td>TRUE</td>
</tr>
<tr>
<td>5031</td>
<td>Firewall app blocked from listening</td>
<td>Object Access</td>
<td>Filtering Platform Connection</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>5157</td>
<td>Firewall has blocked a connection outbound</td>
<td>Object Access</td>
<td>Filtering Platform Connection</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>5379</td>
<td>Credman - Read Credentials</td>
<td>Logon/Logoff</td>
<td>Other Logon/Logoff Events</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>5380</td>
<td>Vault Credential - Find Credential</td>
<td>Logon/Logoff</td>
<td>Other Logon/Logoff Events</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>5381</td>
<td>Vault Credential - Enumerate Credentials</td>
<td>Logon/Logoff</td>
<td>Other Logon/Logoff Events</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>5382</td>
<td>Vault Credential - Get Unique Credential</td>
<td>Logon/Logoff</td>
<td>Other Logon/Logoff Events</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>4724</td>
<td>An Attempt was made to reset an account password</td>
<td>Account Management</td>
<td>User Account Management</td>
<td>3</td>
<td>1</td>
<td>3</td>
<td>FALSE</td>
<td>TRUE</td>
</tr>
<tr>
<td>6423</td>
<td>Forbidden installation (PNP Audit)</td>
<td>Detailed Tracking</td>
<td>Plug and Play Events</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>FALSE</td>
<td>TRUE</td>
</tr>
</tbody>
</table>
So, we seem to be having some possible blind spots

However, the categories that are producing a larger volume of telemetry are untouched to not interfere with the log ingestion volume on your SIEM.

These settings are not documented in the MDE documentation and might be overwritten by Group Policy settings.

Make sure to check your GPOs and enable the events you care about. Otherwise there will be no telemetry AND no alerts on these events.
**PowerShell script to check your environment**

I’ve created an ugly script to check all your GPOs are set properly.

Obviously some are layered so make sure to check that too.

The script relies on the Remote Server Administration Tools (RSAT).

It’s available on my GitHub:

https://github.com/olafhartong/MDE-AuditCheck

```powershell
PS C:\Users\olafhartong.HATCH\Desktop> \MDE-AuditCheck.ps1
This script checks the Group Policies for Audit settings
Next it makes sure all categories that can impact MDE functionality are set properly
There is a total of 18 GPOs.
The following GPOs contain Audit settings:
Audit Settings: Workstations Enhanced Auditing Policy
Audit Settings: Default Domain Controllers Policy
Audit Settings: Servers Enhanced Auditing Policy
Audit Settings: Terrible Idea
Out of those, the following GPOs have potential blind spots due to lacking audit settings
GPO: Workstations Enhanced Auditing Policy
Authorization Policy Change - Not Set
GPO: Default Domain Controllers Policy
Audit Logon - Not Set
Authorization Policy Change - Not Set
Audit Security Group Management - Not Set
Audit User Account Management - Not Set
Audit PnP Activity - Not Set
Audit Other Logon/Logoff Events - Not Set
Audit FileSystem - Not Set
Audit Filtering Platform Connection - Not Set
Audit Other Object Access Events - Not Set
Audit Audit Policy Change - Not Set
Audit Other System Events - Not Set
Audit Security System Extension - Not Set
GPO: Servers Enhanced Auditing Policy
Authorization Policy Change - Not Set
GPO: Terrible Idea
Audit Logon - Expected setting is 3, current setting is: 0
Authorization Policy Change - Not Set
Audit Security Group Management - Expected setting is 1 or 3, current setting is: 0
Audit User Account Management - Expected setting is 1 or 3, current setting is: 0
Audit PnP Activity - Expected setting is 1 or 3, current setting is: 0
Audit Other Logon/Logoff Events - Expected setting is 2 or 3, current setting is: 0
Audit FileSystem - Expected setting is 1 or 3, current setting is: 0
Audit Filtering Platform Connection - Expected setting is 2 or 3, current setting is: 0
Audit Other Object Access Events - Expected setting is 1 or 3, current setting is: 0
Audit Audit Policy Change - Not Set
Audit Other System Events - Expected setting is 1 or 3, current setting is: 0
Audit Security System Extension - Expected setting is 1 or 3, current setting is: 0
```
Wrapping up

- Know your tools, understand their strengths and weaknesses
- Understand what your tools are detecting and HOW they are detecting it
- Continuously reassess this to see what is new or improved
- Augment the weak or blind spots with additional tools
Thank you! Questions ?

olaf@falconforce.nl
https://falconforce.nl
@olafhartong
@falconforce-team
https://linkedin.com/in/olafhartong
Wait, there is more...

Bonus content....
Sysmon vs MDE
Pros and cons per solution

**Sysmon**

+ Full control over the config and the data you’ll get
+ Best applied to augment MDE or in full parallel
+ Rich and unsampled telemetry
- You must maintain it yourself (config, ingestion and detections)
- Only detection, no response

**MDE**

+ Fully maintained by Microsoft (config and ingestion)
+ Detection and Response capability, custom detections possible in addition
+ Rich set of telemetry, way more than Sysmon
- The configuration is non-configurable
- Telemetry is sampled for most events

[Link to medium article](https://medium.com/falconforce/sysmon-vs-microsoft-defender-for-endpoint-mde-internals-0x01-1e5663b10347)
<table>
<thead>
<tr>
<th>Sysmon ID</th>
<th>Sysmon Event Name</th>
<th>MDE Table</th>
<th>ActionType</th>
<th>Notes on MDE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Process Creation</td>
<td>DeviceProcessEvents</td>
<td>ProcessCreated</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Process Changed a file creation time</td>
<td>n/a</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Network Connection</td>
<td>DeviceNetworkEvents</td>
<td>ConnectionFound, ConnectionSuccess, ConnectionFailed, InboundConnectionAccepted, ListeningConnectionCreated, ConnectionAttempt, ConnectionAcknowledged, ConnectionRequest</td>
<td>Heavily sampled, only 1st seen event</td>
</tr>
<tr>
<td>4</td>
<td>Sysmon Service State Change</td>
<td>n/a</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Process Terminated</td>
<td>n/a</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Driver Loaded</td>
<td>DeviceEvents</td>
<td>DriverLoad</td>
<td>No signer information only hashes</td>
</tr>
<tr>
<td>7</td>
<td>Image Loaded</td>
<td>DeviceImageLoadEvents</td>
<td>ImageLoaded</td>
<td>Heavily sampled</td>
</tr>
<tr>
<td>8</td>
<td>Create Remote Thread</td>
<td>DeviceEvents</td>
<td>CreateRemoteThreadApiCall</td>
<td>Missing info compared to Sysmon: NewThreadId, StartAddress, StartModule, StartFunction</td>
</tr>
<tr>
<td>9</td>
<td>Raw File Access Read</td>
<td>n/a</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Process Access</td>
<td>DeviceEvents</td>
<td>ReadProcessMemoryApiCall, WriteToLsassProcessMemory, OpenProcessApiCall</td>
<td>ONLY logged for the lsass.exe process. It does provide TotalBytesCopied on ReadProcessMemoryApiCall. On OpenProcessApiCall is supplies the DesiredAccess in decimal values</td>
</tr>
<tr>
<td>11</td>
<td>File Create</td>
<td>DeviceFileEvents</td>
<td>FileCreated</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Registry Create and Delete</td>
<td>DeviceRegistryEvents</td>
<td>RegistryKeyCreated, RegistryKeyDeleted, RegistryValueDeleted</td>
<td>Filters are applied</td>
</tr>
<tr>
<td>13</td>
<td>Registry Value Set</td>
<td>DeviceRegistryEvents</td>
<td>RegistryValueSet</td>
<td>Filters are applied</td>
</tr>
<tr>
<td>14</td>
<td>Registry Key and Value Rename</td>
<td>n/a</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>File Create Stream Hash</td>
<td>n/a</td>
<td>n/a</td>
<td>Seems to be there in MDE but often unpopulated</td>
</tr>
<tr>
<td>16</td>
<td>Sysmon Config Change</td>
<td>n/a</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Pipe Event Created</td>
<td>DeviceEvents</td>
<td>NamedPipeEvent</td>
<td>Only first seen event, connect or create</td>
</tr>
<tr>
<td>18</td>
<td>Pipe Event Connected</td>
<td>n/a</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>WMI Event Filter activity</td>
<td>n/a</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>WMI EventConsumer activity</td>
<td>DeviceEvents</td>
<td>ProcessCreatedUsingWmiQuery</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>WMI EventConsumerToFilter activity</td>
<td>DeviceEvents</td>
<td>WmiBindEventFilterToConsumer</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>DNS Query</td>
<td>DeviceEvents</td>
<td>DnsQueryResponse</td>
<td>Response to successful queries</td>
</tr>
<tr>
<td>23</td>
<td>File Delete</td>
<td>DeviceFileEvents</td>
<td>FileDeleted</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>Clipboard Change</td>
<td>n/a</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>Process Tampering</td>
<td>n/a</td>
<td>n/a</td>
<td>No exposed telemetry, it does have alerts for it</td>
</tr>
<tr>
<td>26</td>
<td>File DeleteDetected</td>
<td>DeviceFileEvents</td>
<td>FileDeleted</td>
<td>No file retention option</td>
</tr>
</tbody>
</table>
Sysmon vs MDE – features / telemetry

**Sysmon - Unique**
- Clipboard events saving
- Deleted files saving
- Preserve deleted PE files
- Preserve files for configured processes
- Preserve files with configured extensions
- Preserve files for configured SIDs

**MDE - Unique**
- DeviceFileEvents
- DeviceFileEvents
- DeviceLogonEvents
- DeviceLogonEvents
- DeviceLogonEvents
- DeviceFileCertificateInfo
- DeviceInfo
- DeviceNetworkInfo

---

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Description</th>
<th>Sysmon</th>
<th>MDE</th>
</tr>
</thead>
<tbody>
<tr>
<td>AntivirusDetection</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AntivirusDetectionActionType</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AntivirusReport</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AntivirusScanCancelled</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AntivirusScanCompleted</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AntivirusScanFailed</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AppControlCodeIntegritySigningInformation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AppControlScriptBlocked</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AsrAdobeReaderChildProcessBlocked</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AsrExecutableEmailContentBlocked</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AsrExecutableOfficeContentAudited</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AsrExecutableOfficeContentBlocked</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AsrLsassCredentialTheftAudited</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AsrLsassCredentialTheftBlocked</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AsrObfuscatedScriptAudited</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AsrOfficeChildProcessAudited</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AsrOfficeChildProcessBlocked</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AsrOfficeCommAppChildProcessAudited</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AsrOfficeCommAppChildProcessBlocked</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AsrOfficeMacroWin32ApiCallAudited</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AsrOfficeMacroWin32ApiCallBlocked</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AsrOfficeProcessInjectionAudited</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AsrOfficeProcessInjectionBlocked</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AsrPsexecWin32ChildProcessAudited</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AsrPsexecWin32ChildProcessBlocked</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AsrRansomwareBlocked</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AsrTrustedExecutableAudited</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AsrTrustedUsbProcessAudited</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AsrTrustedUsbProcessBlocked</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AuditPolicyModification</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BluetoothPolicyTriggered</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BrowserLaunchedToOpenUrl</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ControlFlowGuardViolation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ControlledFolderAccessViolationAudited</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ControlledFolderAccessViolationBlocked</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CreateRemoteThreadApiCall</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

CredentialsBackup
DeviceBootAttestationInfo
DriverLoad
ExploitGuardAcgAudited
ExploitGuardAcgEnforced
ExploitGuardChildProcessAudited
ExploitGuardChildProcessBlocked
ExploitGuardEafViolationBlocked
ExploitGuardLowIntegrityImageAudited
ExploitGuardLowIntegrityImageBlocked
ExploitGuardNetworkProtectionAudited
ExploitGuardNonMicrosoftSignedAudited
ExploitGuardNonMicrosoftSignedBlocked
ExploitGuardSharedBinaryAudited
ExploitGuardSharedBinaryBlocked
ExploitGuardWin32SystemCallAudited
ExploitGuardWin32SystemCallBlocked
FirewallInboundConnectionAudited
FirewallInboundConnectionToAppBlocked
FirewallOutboundConnectionAudited
FirewallOutboundConnectionBlocked
GetAsyncKeyStateApiCall
GetClipboardData
GetLdapSearch
MemoryRemoteProtect
NamedPipeEvent
NtAllocateVirtualMemoryApiCall
NtAllocateVirtualMemoryRemoteApiCall
NtMapViewOfSectionRemoteApiCall
NtProtectVirtualMemoryApiCall
OpenProcessApiCall
OtherAlertRelatedActivity
PowerShellAllowed
PowerShellBlocked
PowerShellConnected
ProcessCreatedUsingWmiQuery
ProcessPrimaryTokenModified
QueueUserApicRemoteApiCall
ReadProcessMemoryApiCall
RemoteDesktopConnection
RemoteWmiOperation
SafeDocFileScan
ScheduledTaskCreated
ScheduledTaskDeleted
ScheduledTaskUpdated
ScreenShotTaken
ScriptContent
SecurityGroupCreated
SecurityGroupDeleted
SecurityLogCleared
SensitiveFileRead
ServiceInstalled
ShellLinkCreateFileEvent
SmartScreenAppWarning
SmartScreenExploitWarning
SmartScreenUrlWarning
SmartScreenUseroverride
TrustedWifiConnection
UntrustedWifiConnection
UsbDriveDriveLetterChanged
UsbDriveMounted
UsbDriveUnmounted
UserAccountAddedToLocalGroup
UserAccountDeleted
UserAccountModified
UserAccountRemovedFromLocalGroup
WmiBindEventFilterToConsumer
WriteToLsassProcessMemory

---

.... 181 in total
## MDE telemetry potential mapping to MITRE ATT&CK

<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution</th>
<th>Persistence</th>
<th>Privilege Escalation</th>
<th>Defense Evasion</th>
<th>Credential Access</th>
<th>Discovery</th>
<th>Lateral Movement</th>
<th>Collection</th>
<th>Command and Control</th>
<th>Exfiltration</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>9 techniques</td>
<td>10 techniques</td>
<td>18 techniques</td>
<td>13 techniques</td>
<td>32 techniques</td>
<td>15 techniques</td>
<td>25 techniques</td>
<td>9 techniques</td>
<td>15 techniques</td>
<td>16 techniques</td>
<td>8 techniques</td>
<td>13 techniques</td>
</tr>
</tbody>
</table>

- **Drive-by Compromise**
- **Exploit Public-Facing Application**
- **External Remote Services**
- **Hardware Additions**
- **Phishing**
- **Replication Through Removable Media**
- **Supply Chain Compromise**
- **Trusted Relationship**
- **Valid Accounts**

---

**Command and Scripting Interpreter**

- **Account Manipulation**
- **BITS Jobs**
- **Boot or Logon Automation Script**
- **Native API**
- **Scheduled Task/Job**
- **Comprehensive Client Software Binary**
- **Software Deployment Tools**
- **System Services**
- **User Execution**
- **Windows Management Instrumentation**

**Abuse Elevation Control Mechanism**

- **Access Token Manipulation**
- **BITS Jobs**
- **Deobfuscate/Decode File or Information**
- **Direct Volume Access**
- **Domain Policy Modification**
- **Execution Environments**
- **File and Directory Permissions Modification**
- **Hide Artifacts**
- **Hijack Execution Flow**
- **Impersonation**
- **Indirect Command Execution**

**Brute Force**

- **Credentials from Password Stores**
- **Exploitation of Remote Services**
- **Internal Spearphishing**
- **Lateral Tool Transfer**
- **File and Directory Permissions Hijacking**
- **Remote Services**
- **Replication Through Removable Media**
- **Remote Service Discovery**
- **Remote Service Execution**

**Domain Trust Discovery**

- **File and Directory Discovery**
- **Network Service Scanning**
- **Network Share Discovery**
- **Process Discovery**
- **Domain Name System (DNS)**
- **DNS Poisoning**
- **DNS Query**
- **DNS Update**
- **DNS Update Query**
- **DNS Update Query Response**

**Application Layer Protocol**

- **Data Transfer Size Limit**
- **Data Encryption**
- **Data Manipulation**
- **Defacement**
- **Disk Wipe**
- **Endpoint Denial of Service**
- **Firmware Corruption**
- **Init System Recovery**
- **Network Denial of Service**
- **Resource Hijacking**
- **Service Stop**
- **System Shutdown/Reboot**
Sysmon telemetry potential mapping to MITRE ATT&CK

<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution</th>
<th>Persistence</th>
<th>Privilege Escalation</th>
<th>Defense Evasion</th>
<th>Credential Access</th>
<th>Discovery</th>
<th>Lateral Movement</th>
<th>Collection</th>
<th>Command and Control</th>
<th>Exfiltration</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Remote Services</td>
<td>Hardware Additions</td>
<td>Native API</td>
<td>Manipulation</td>
<td>Attack Mechanism</td>
<td>Access Token</td>
<td>Exploitation of Credential Access</td>
<td>Cloud Service</td>
<td>Data Transfer &amp; Encryption</td>
<td>Automated Exfiltration</td>
<td>Data Encryption</td>
<td>Data Transfer &amp; Encryption</td>
</tr>
<tr>
<td>Replication Through Removable Media</td>
<td>Supply Chain Compromise</td>
<td>Trusted Relationship</td>
<td>External Remote Services</td>
<td>Exploitation</td>
<td>Exploitation</td>
<td>Exploitation</td>
<td>Exploitation</td>
<td>Exploitation</td>
<td>Exploitation</td>
<td>Exploitation</td>
<td>Exploitation</td>
</tr>
<tr>
<td>System Compromise</td>
<td>Client Software Binary</td>
<td>System Services</td>
<td>System Services</td>
<td>System Services</td>
<td>System Services</td>
<td>System Services</td>
<td>System Services</td>
<td>System Services</td>
<td>System Services</td>
<td>System Services</td>
<td>System Services</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Account Discovery</td>
<td>Access Token Discovery</td>
<td>OS Credential Dumping</td>
<td>Password Policy Discovery</td>
<td>Taint Staged</td>
<td>Email Capture</td>
<td>Man-in-the-Middle</td>
<td>Ingress Transfer</td>
<td>Exfiltration Over Web Service</td>
<td>Exfiltration Over Physical Medium</td>
<td>Exfiltration Over Physical Medium</td>
<td>Exfiltration Over Physical Medium</td>
</tr>
<tr>
<td>Application Discovery</td>
<td>Exploitation of Remote Services</td>
<td>Network Discovery</td>
<td>Network Discovery</td>
<td>Network Discovery</td>
<td>Network Discovery</td>
<td>Network Discovery</td>
<td>Network Discovery</td>
<td>Network Discovery</td>
<td>Network Discovery</td>
<td>Network Discovery</td>
<td>Network Discovery</td>
</tr>
<tr>
<td>Clipboard Data</td>
<td>Data from Information Repositories</td>
<td>Data from Local System</td>
<td>Data from Local System</td>
<td>Data from Local System</td>
<td>Data from Local System</td>
<td>Data from Local System</td>
<td>Data from Local System</td>
<td>Data from Local System</td>
<td>Data from Local System</td>
<td>Data from Local System</td>
<td>Data from Local System</td>
</tr>
<tr>
<td>Data Obfuscation</td>
<td>Dynamic Resolution</td>
<td>Data Obfuscation</td>
<td>Dynamic Resolution</td>
<td>Data Obfuscation</td>
<td>Dynamic Resolution</td>
<td>Data Obfuscation</td>
<td>Dynamic Resolution</td>
<td>Data Obfuscation</td>
<td>Dynamic Resolution</td>
<td>Data Obfuscation</td>
<td>Dynamic Resolution</td>
</tr>
<tr>
<td>Data Encoding</td>
<td>Data Encoding</td>
<td>Data Encoding</td>
<td>Data Encoding</td>
<td>Data Encoding</td>
<td>Data Encoding</td>
<td>Data Encoding</td>
<td>Data Encoding</td>
<td>Data Encoding</td>
<td>Data Encoding</td>
<td>Data Encoding</td>
<td>Data Encoding</td>
</tr>
<tr>
<td>Data Transfer Size Limits</td>
<td>Data Transfer Size Limits</td>
<td>Data Transfer Size Limits</td>
<td>Data Transfer Size Limits</td>
<td>Data Transfer Size Limits</td>
<td>Data Transfer Size Limits</td>
<td>Data Transfer Size Limits</td>
<td>Data Transfer Size Limits</td>
<td>Data Transfer Size Limits</td>
<td>Data Transfer Size Limits</td>
<td>Data Transfer Size Limits</td>
<td>Data Transfer Size Limits</td>
</tr>
<tr>
<td>Data Transfer &amp; Encryption</td>
<td>Data Transfer &amp; Encryption</td>
<td>Data Transfer &amp; Encryption</td>
<td>Data Transfer &amp; Encryption</td>
<td>Data Transfer &amp; Encryption</td>
<td>Data Transfer &amp; Encryption</td>
<td>Data Transfer &amp; Encryption</td>
<td>Data Transfer &amp; Encryption</td>
<td>Data Transfer &amp; Encryption</td>
<td>Data Transfer &amp; Encryption</td>
<td>Data Transfer &amp; Encryption</td>
<td>Data Transfer &amp; Encryption</td>
</tr>
<tr>
<td>Data Encryption</td>
<td>Data Encryption</td>
<td>Data Encryption</td>
<td>Data Encryption</td>
<td>Data Encryption</td>
<td>Data Encryption</td>
<td>Data Encryption</td>
<td>Data Encryption</td>
<td>Data Encryption</td>
<td>Data Encryption</td>
<td>Data Encryption</td>
<td>Data Encryption</td>
</tr>
<tr>
<td>Exfiltration Over Network Medium</td>
<td>Exfiltration Over Network Medium</td>
<td>Exfiltration Over Network Medium</td>
<td>Exfiltration Over Network Medium</td>
<td>Exfiltration Over Network Medium</td>
<td>Exfiltration Over Network Medium</td>
<td>Exfiltration Over Network Medium</td>
<td>Exfiltration Over Network Medium</td>
<td>Exfiltration Over Network Medium</td>
<td>Exfiltration Over Network Medium</td>
<td>Exfiltration Over Network Medium</td>
<td>Exfiltration Over Network Medium</td>
</tr>
<tr>
<td>Inhibit System Recovery</td>
<td>Network Denial of Service</td>
<td>Network Denial of Service</td>
<td>Network Denial of Service</td>
<td>Network Denial of Service</td>
<td>Network Denial of Service</td>
<td>Network Denial of Service</td>
<td>Network Denial of Service</td>
<td>Network Denial of Service</td>
<td>Network Denial of Service</td>
<td>Network Denial of Service</td>
<td>Network Denial of Service</td>
</tr>
<tr>
<td>Resource Hijacking</td>
<td>Service Stop</td>
<td>Service Stop</td>
<td>Service Stop</td>
<td>Service Stop</td>
<td>Service Stop</td>
<td>Service Stop</td>
<td>Service Stop</td>
<td>Service Stop</td>
<td>Service Stop</td>
<td>Service Stop</td>
<td>Service Stop</td>
</tr>
</tbody>
</table>