black hat®
BRIEFINGS

AUGUST 6-7, 2025
MANDALAY BAY / LAS VEGAS

I'm in your logs now, deceiving your analysts and blinding your EDR

OLAF HARTONG

Detection Engineer and Security Researcher

- Purple teaming, Threat hunting
- Security MVP

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

@olafhartong
github.com/olafhartong
olaf@falconforce.nl
olafhartong.nl / falconforce.nl

TODAY'S TOPICS

WHAT IS EVENT TRACING FOR WINDOWS

WHY SECURITY PRODUCTS USE ETW

CAN I SPOOF EVENTS?

CAN I FURTHER (AB)USE THIS ?

WHAT CAN YOU DO WITH/ABOUT THIS

WHAT IS EVENT TRACING FOR WINDOWS (ETW)

WHAT IS EVENT TRACING FOR WINDOWS [ETW]

Event Tracing for Windows (ETW) provides a mechanism to trace and log events that are raised by user-mode applications and kernel-mode drivers. It has been designed for performance monitoring and debugging.

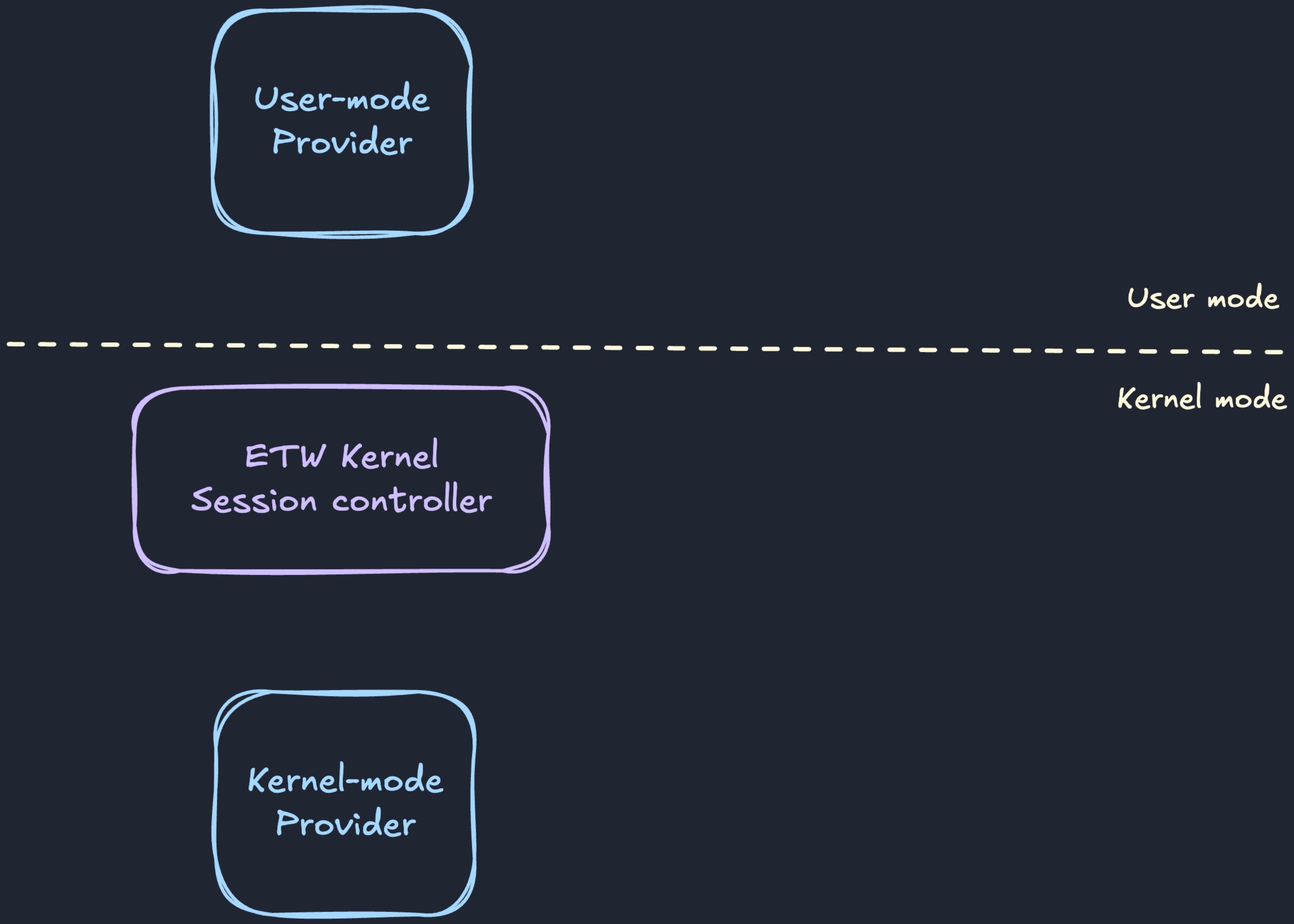
ETW is implemented in the Windows operating system and provides a fast, reliable, and versatile set of event tracing features. Its architecture consists of three primary components:

Event Providers

Trace sessions (logger sessions)

Event Consumers

The next slides provide a simplified overview of ETW, only focused on the components I've abused.



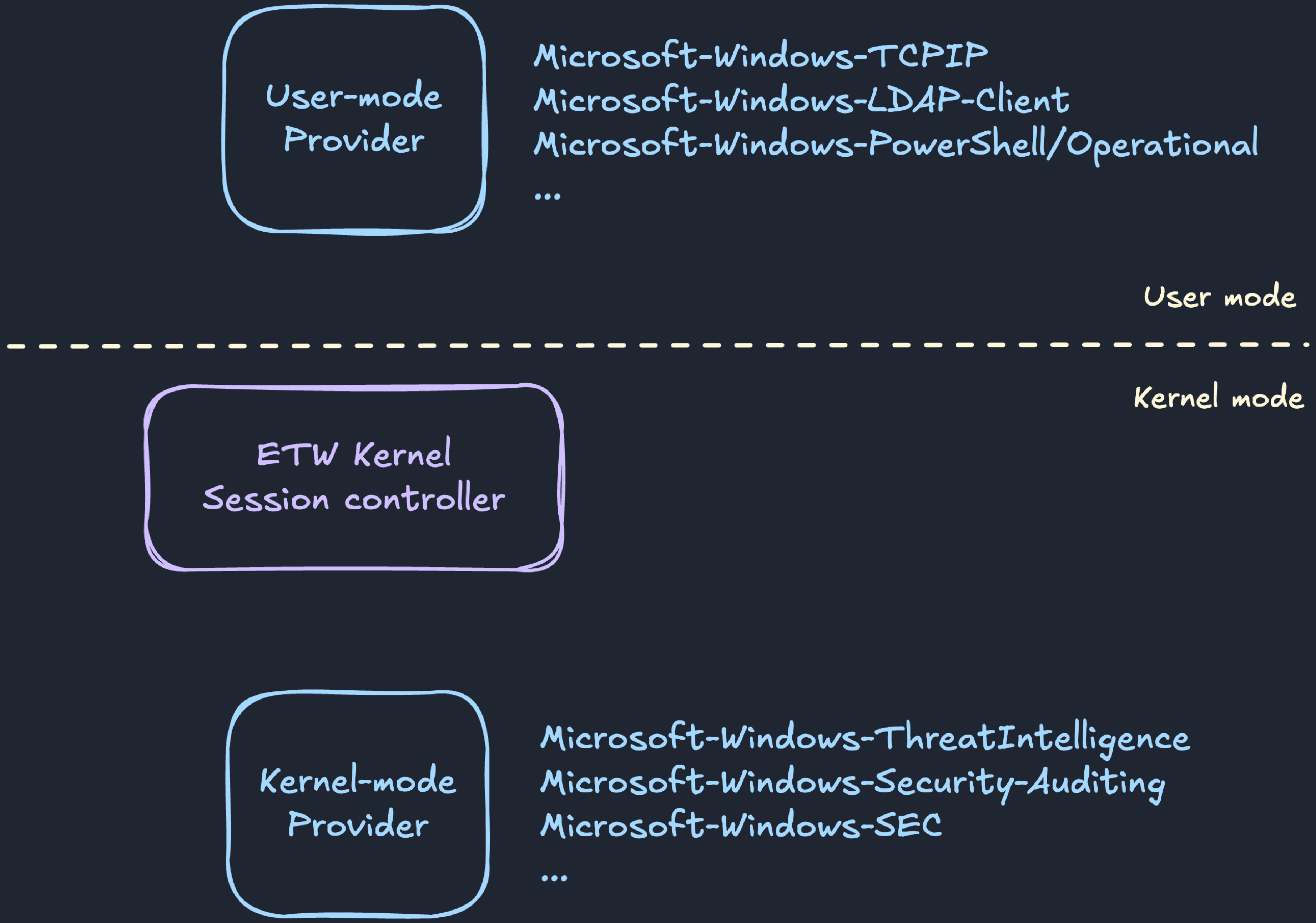
User-mode Provider

User mode

Kernel mode

ETW Kernel Session controller

Kernel-mode Provider



User-mode Provider

Microsoft-Windows-TCPIP
Microsoft-Windows-LDAP-Client
Microsoft-Windows-PowerShell/Operational
...

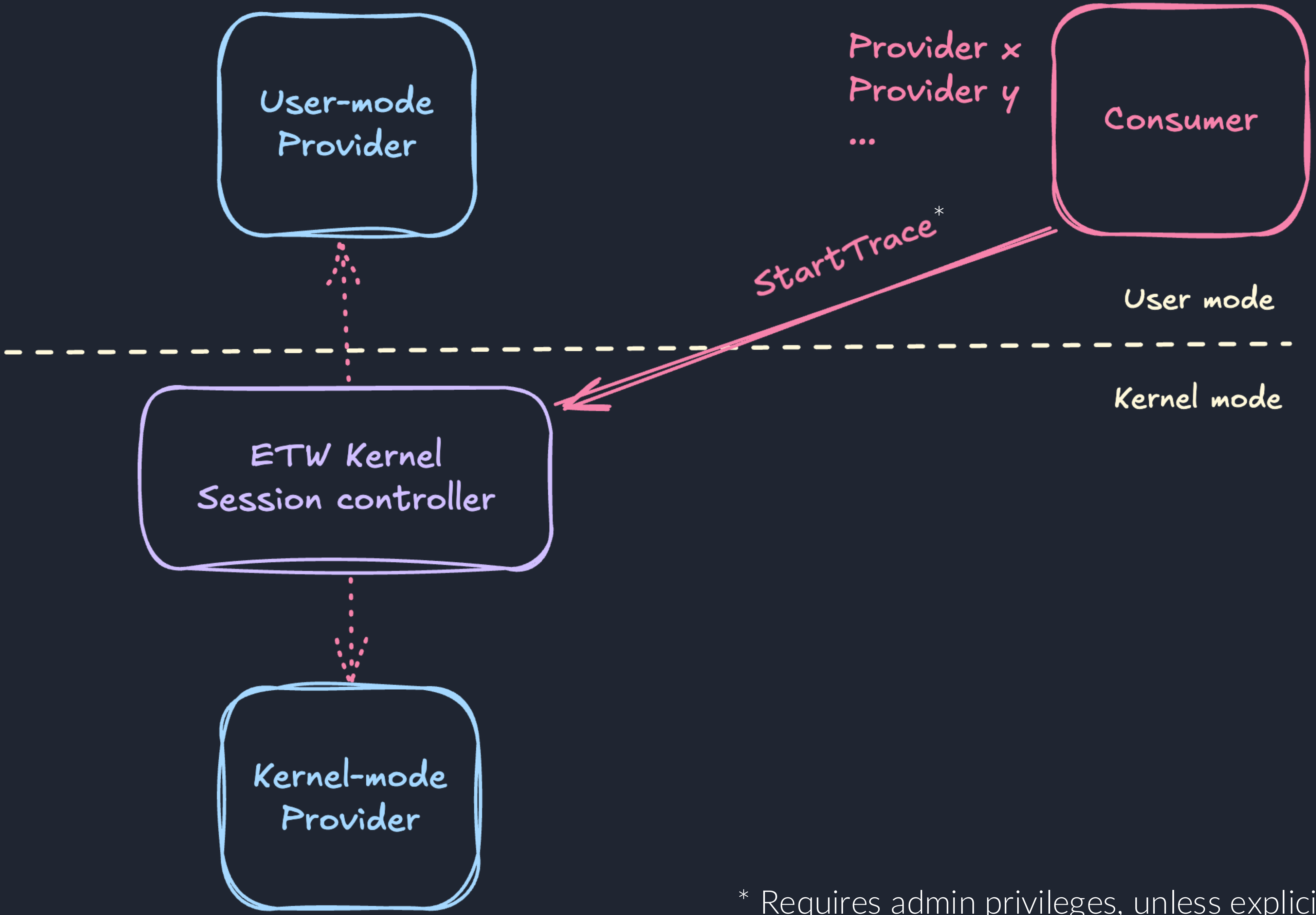
User mode

Kernel mode

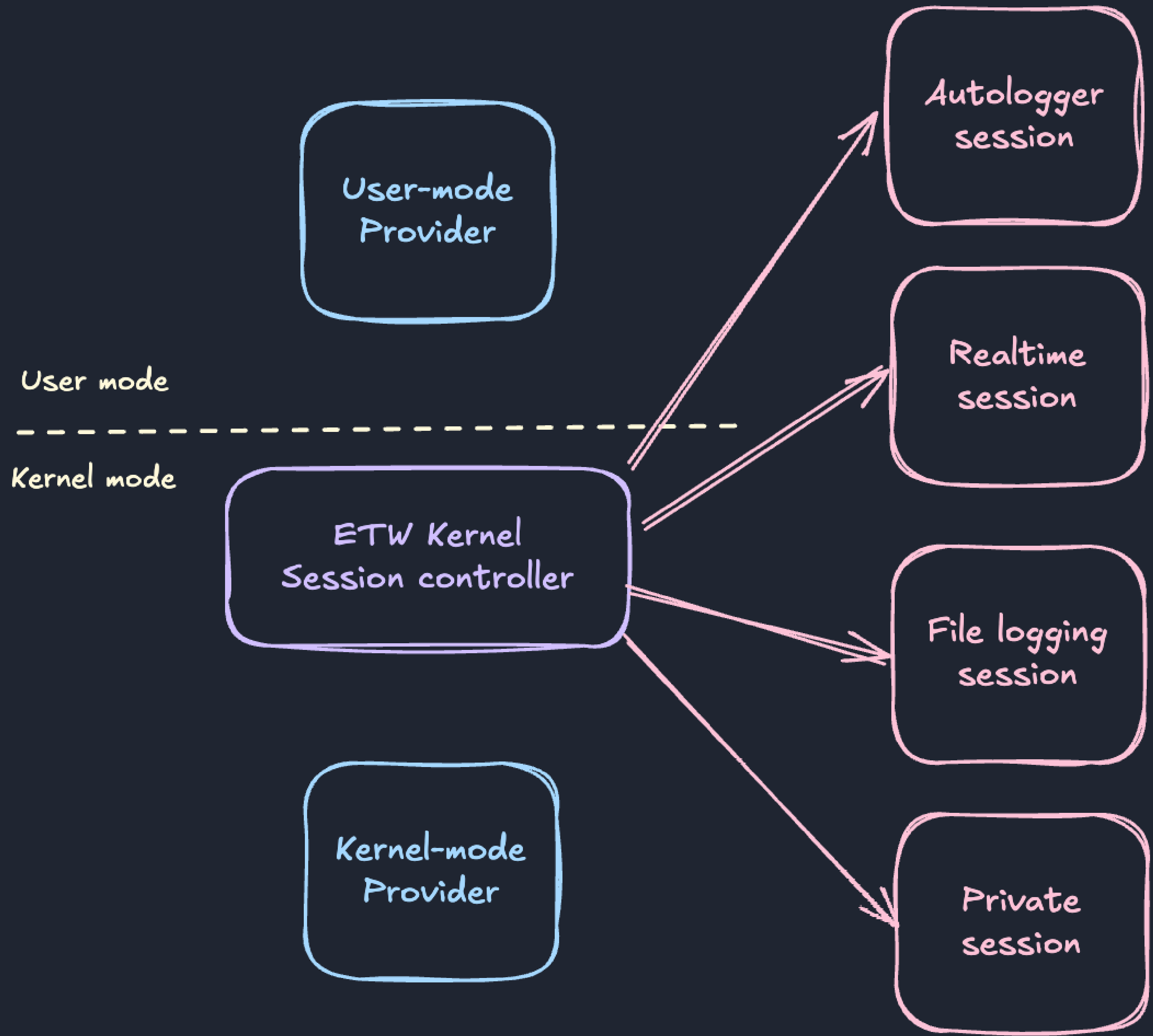
ETW Kernel Session controller

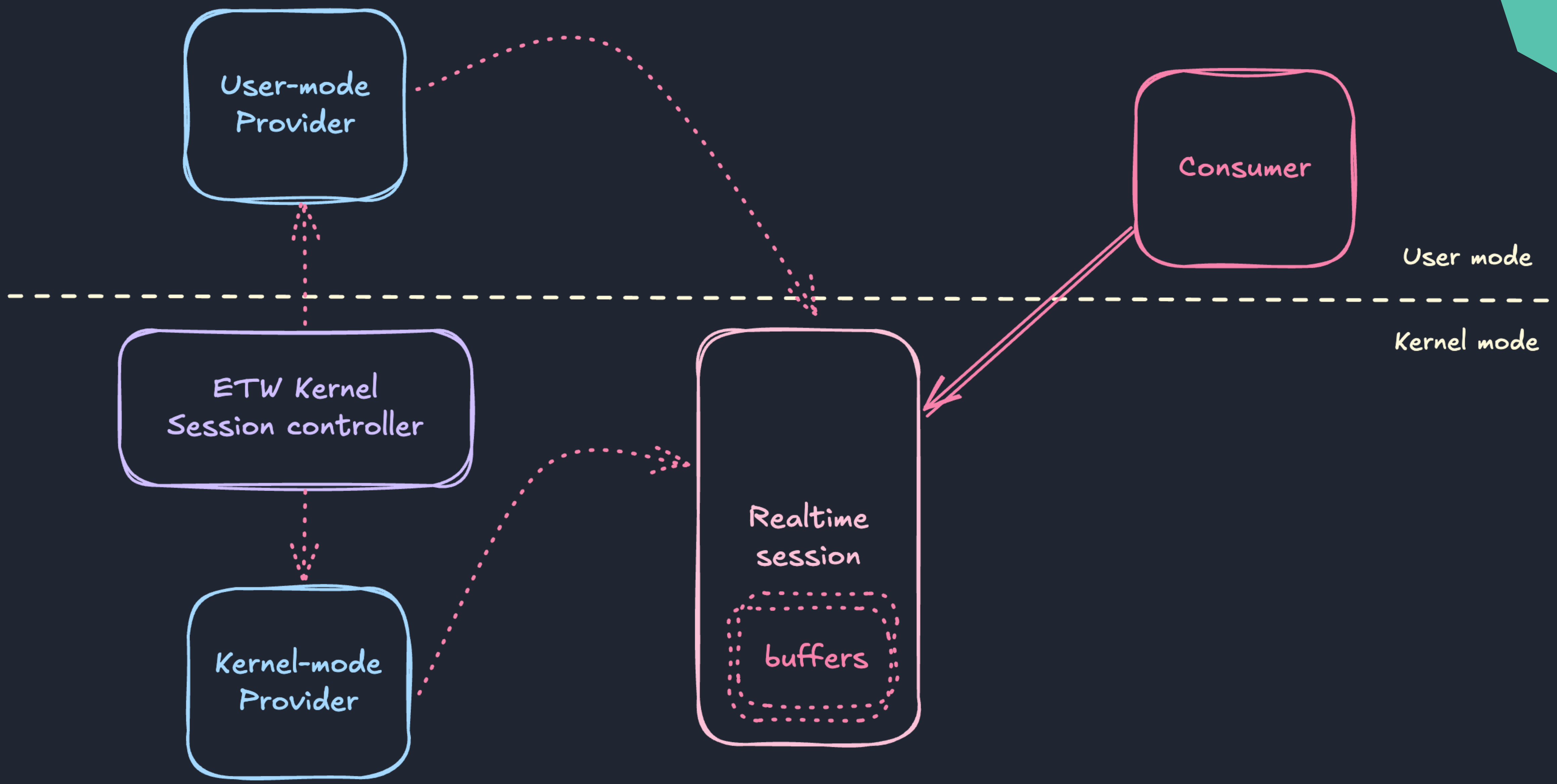
Kernel-mode Provider

Microsoft-Windows-ThreatIntelligence
Microsoft-Windows-Security-Auditing
Microsoft-Windows-SEC
...



* Requires admin privileges, unless explicitly permitted


User-mode Provider
User mode
Kernel mode
ETW Kernel Session controller
Kernel-mode Provider
Autologger session
Realtime session
File logging session
Private session



User-mode Provider

Consumer

User mode

Kernel mode

ETW Kernel Session controller

Realtime session

buffers

Kernel-mode Provider

* logical flow

COMMON ETW ATTACKS

- ✓ Patching the ntdll.dll EtwEventWrite function (often AMSI)
- ✓ Tamper with ETL files on disk or disable sessions in the registry
- ✓ Block specific events in one process by function hooking
- ✓ Disable tracing sessions (requires kernel level access)

https://attack.mitre.org/techniques/T1562/006/

WHY SECURITY PRODUCTS USE ETW

WHY DO SECURITY PRODUCTS USE ETW

Dynamic Control

Providers can be enabled/disabled
in a trace session at runtime

Coverage breath

Way more event types can
be collected

Less intrusive

No hooking or injection required to
all processes

Stability

Less code in the kernel is less
likely to crash

Filtering

ETW sessions can be
consumed filtered by level,
keywords, etc

Process Performance

Kernel events need to be filtered
after collection. ETW Sessions
are buffered, callbacks are not.

MDE RELIES HEAVILY ON ETW FOR EVENTS

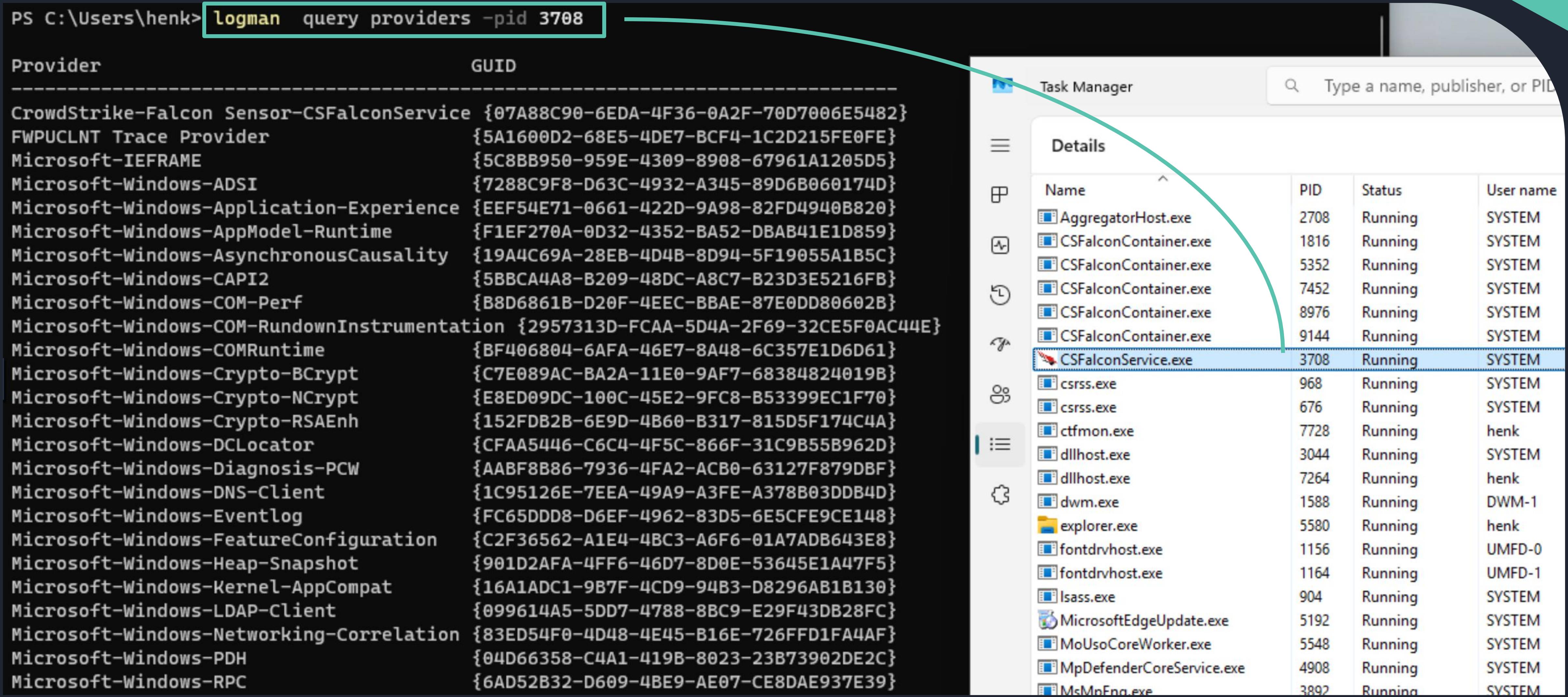
kernel callbacks

Process Start
Driver Load
Image (DLL) load
Network Connect
Named Pipe
Registry Events
Thread creation
Filesystem (via minifilter)
Object handle

ETW events

Anti Tampering
Anaheim-SmartScreen
Application Error
AttackSurfaceMonitor
Generic ETW CreateFile Pattern
Kernel Integrity
LsaSrv
Machine state
Microsoft-Antimalware-Engine
Microsoft-Antimalware-RTP
Microsoft-Antimalware-Scan-Interface
Microsoft-Antimalware-Service
Microsoft-Antimalware-UacScan
Microsoft-ThreatProtectionService
Microsoft-Windows-AppLocker
Microsoft-Windows-Audit-CVE
Microsoft-Windows-Bits-Client
Microsoft-Windows-Bluetooth-Policy
Microsoft-Windows-CAPI2
Microsoft-Windows-CodeIntegrity
Microsoft-Windows-Crypto-DPAPI-Events
Microsoft-Windows-DHCPV6-Client-Events
Microsoft-Windows-DNS-Client
Microsoft-Windows-DotNETRuntime
Microsoft-Windows-EDP-Audit-Regular
Microsoft-Windows-EDP-Audit-TCB
Microsoft-Windows-FilterManager
Microsoft-Windows-IE-SmartScreen
Microsoft-Windows-Kernel-Audit-API-Calls
Microsoft-Windows-Kernel-Network
Microsoft-Windows-Kernel-PnP-Events
Microsoft-Windows-Ldap-Client
Microsoft-Windows-LiveId
Microsoft-Windows-NTLM
Microsoft-Windows-PrintService
Microsoft-Windows-RemoteDesktopServices-RdpCoreTS
Microsoft-Windows-RPC
Microsoft-Windows-SEC
Microsoft-Windows-SEC-WFP
Microsoft-Windows-Security-Mitigations
Microsoft-Windows-Services
Microsoft-Windows-SmartScreen
Microsoft-Windows-TCPIP
Microsoft-Windows-TerminalServices-LocalSessionManager
Microsoft-Windows-ThreatIntelligence
Microsoft-Windows-VHDMP
Microsoft-Windows-WER-Diag
Microsoft-Windows-Win32k
Microsoft-Windows-Windows Defender
Microsoft-Windows-WMI-Activity
Microsoft.AAD.Runtime
Microsoft.Office.Security
Microsoft.Web.Platform
Microsoft.Windows.ComOleAut32
Microsoft.Windows.Console.Host
Microsoft.Windows.Defender
Microsoft.Windows.HVSI.ContainerService
Microsoft.Windows.HVSI.Manager
Microsoft.Windows.HyperV.Compute
Microsoft.Windows.NdrCollector
Microsoft.Windows.User32
Microsoft.Windows.WSL.DefenderPlugin
Microsoft.Windows.WebDefense.SenseLogging
Microsoft-Windows-Dhcp-Client
User32
Microsoft.Windows.NdrScanner
Microsoft.Windows.Oct.Enclave
Microsoft.Windows.OLE.Clipboard
Microsoft.Windows.Print.Winspool
Microsoft.Windows.Security.Wininit
Microsoft.Windows.Sense.AccountsLockoutProvider
Microsoft.Windows.Sense.AzureVmMetadata
Microsoft.Windows.Sense.BrowserExtensionCollection
Microsoft.Windows.Sense.CollectionEtw
Microsoft.Windows.Sense.ConnectivityChecker
Microsoft.Windows.Sense.GeneratedETW
Microsoft.Windows.Sense.LocalGroupsUsersCollection
Microsoft.Windows.Sense.PasswordPolicyProvider
Microsoft.Windows.Sense.PendingRebootUpdates
Microsoft.Windows.Sense.RegHeartBeat
Microsoft.Windows.Sense.ScheduledTasksCollection
Microsoft.Windows.Sense.SenseCm
Microsoft.Windows.Sense.SharesCollection
Microsoft.Windows.Sense.TimnaProductsFromRegistry
Microsoft.Windows.Sense.Tvm.Axon
Microsoft.Windows.Sense.Tvm.Collector
Microsoft.Windows.Sense.Tvm.NetworkScanner
Microsoft.Windows.Sense.TvmBaselineAssessorEtw
Microsoft.Windows.Sense.TvmCertificateCollectionEtw
Microsoft.Windows.Sense.TvmInfoGatheringCollectorEtw
Microsoft.Windows.Sense.ValidationEtw
Microsoft.Windows.Sense.WDCollection
Microsoft.Windows.SenseComponent.GeneratedETW
Microsoft.Windows.SenseNdr
Microsoft.Windows.ServiceControlManager
Open link
Powershell cmdlets
SGRM Report
SecureETW
microsoft-windows-grouppolicy

SO DOES CROWDSTRIKE



```
PS C:\Users\henk> logman  query providers -pid 3708

Provider                                 GUID
-------------------------------------------------------------------------------
CrowdStrike-Falcon Sensor-CSFalconService {07A88C90-6EDA-4F36-0A2F-70D7006E5482}
FWPUCLNT Trace Provider                  {5A1600D2-68E5-4DE7-BCF4-1C2D215FE0FE}
Microsoft-IEFRAME                        {5C8BB950-959E-4309-8908-67961A1205D5}
Microsoft-Windows-ADSI                   {7288C9F8-D63C-4932-A345-89D6B060174D}
Microsoft-Windows-Application-Experience {EEF54E71-0661-422D-9A98-82FD4940B820}
Microsoft-Windows-AppModel-Runtime       {F1EF270A-0D32-4352-BA52-DBAB41E1D859}
Microsoft-Windows-AsynchronousCausality  {19A4C69A-28EB-4D4B-8D94-5F19055A1B5C}
Microsoft-Windows-CAPI2                  {5BBCA4A8-B209-48DC-A8C7-B23D3E5216FB}
Microsoft-Windows-COM-Perf               {B8D6861B-D20F-4EEC-BBAE-87E0DD80602B}
Microsoft-Windows-COM-RundownInstrumentation {2957313D-FCAA-5D4A-2F69-32CE5F0AC44E}
Microsoft-Windows-COMRuntime             {BF406804-6AFA-46E7-8A48-6C357E1D6D61}
Microsoft-Windows-Crypto-BCrypt          {C7E089AC-BA2A-11E0-9AF7-68384824019B}
Microsoft-Windows-Crypto-NCrypt          {E8ED09DC-100C-45E2-9FC8-B53399EC1F70}
Microsoft-Windows-Crypto-RSAEnh          {152FDB2B-6E9D-4B60-B317-815D5F174C4A}
Microsoft-Windows-DCLocator              {CFAA5446-C6C4-4F5C-866F-31C9B55B962D}
Microsoft-Windows-Diagnosis-PCW          {AABF8B86-7936-4FA2-ACB0-63127F879DBF}
Microsoft-Windows-DNS-Client             {1C95126E-7EEA-49A9-A3FE-A378B03DDB4D}
Microsoft-Windows-Eventlog               {FC65DDD8-D6EF-4962-83D5-6E5CFE9CE148}
Microsoft-Windows-FeatureConfiguration   {C2F36562-A1E4-4BC3-A6F6-01A7ADB643E8}
Microsoft-Windows-Heap-Snapshot          {901D2AFA-4FF6-46D7-8D0E-53645E1A47F5}
Microsoft-Windows-Kernel-AppCompat       {16A1ADC1-9B7F-4CD9-94B3-D8296AB1B130}
Microsoft-Windows-LDAP-Client            {099614A5-5DD7-4788-8BC9-E29F43DB28FC}
Microsoft-Windows-Networking-Correlation {83ED54F0-4D48-4E45-B16E-726FFD1FA4AF}
Microsoft-Windows-PDH                    {04D66358-C4A1-419B-8023-23B73902DE2C}
Microsoft-Windows-RPC                    {6AD52B32-D609-4BE9-AE07-CE8DAE937E39}
```

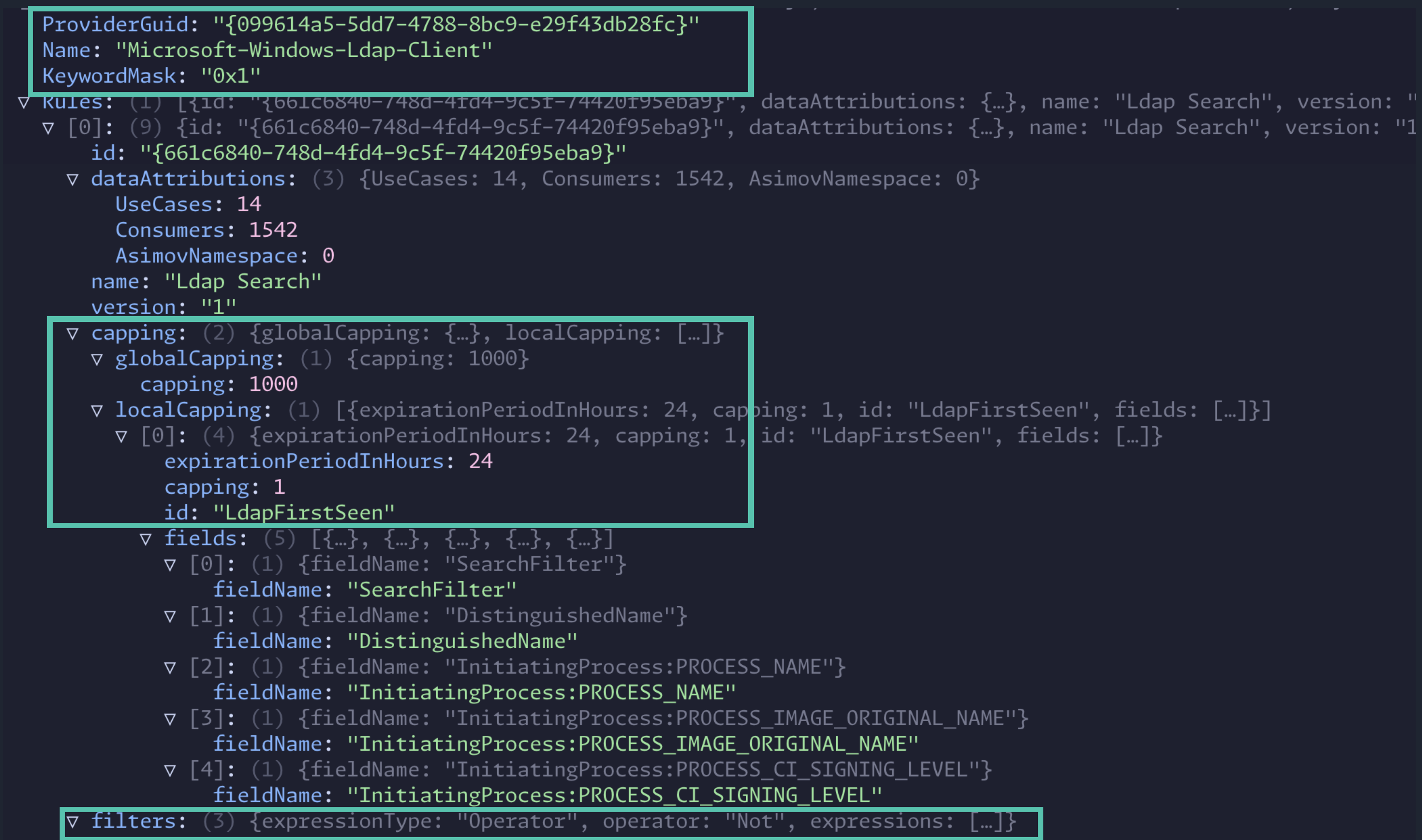
Details

Name	PID	Status	User name
AggregatorHost.exe	2708	Running	SYSTEM
CSFalconContainer.exe	1816	Running	SYSTEM
CSFalconContainer.exe	5352	Running	SYSTEM
CSFalconContainer.exe	7452	Running	SYSTEM
CSFalconContainer.exe	8976	Running	SYSTEM
CSFalconContainer.exe	9144	Running	SYSTEM
CSFalconService.exe	3708	Running	SYSTEM
csrss.exe	968	Running	SYSTEM
csrss.exe	676	Running	SYSTEM
ctfmon.exe	7728	Running	henk
dllhost.exe	3044	Running	SYSTEM
dllhost.exe	7264	Running	henk
dwm.exe	1588	Running	DWM-1
explorer.exe	5580	Running	henk
fontdrvhost.exe	1156	Running	UMFD-0
fontdrvhost.exe	1164	Running	UMFD-1
lsass.exe	904	Running	SYSTEM
MicrosoftEdgeUpdate.exe	5192	Running	SYSTEM
MoUsoCoreWorker.exe	5548	Running	SYSTEM
MpDefenderCoreService.exe	4908	Running	SYSTEM
MsMpEng.exe	3892	Running	SYSTEM

MDE CONFIGURATION – ETW PROVIDERS (A SELECTION)

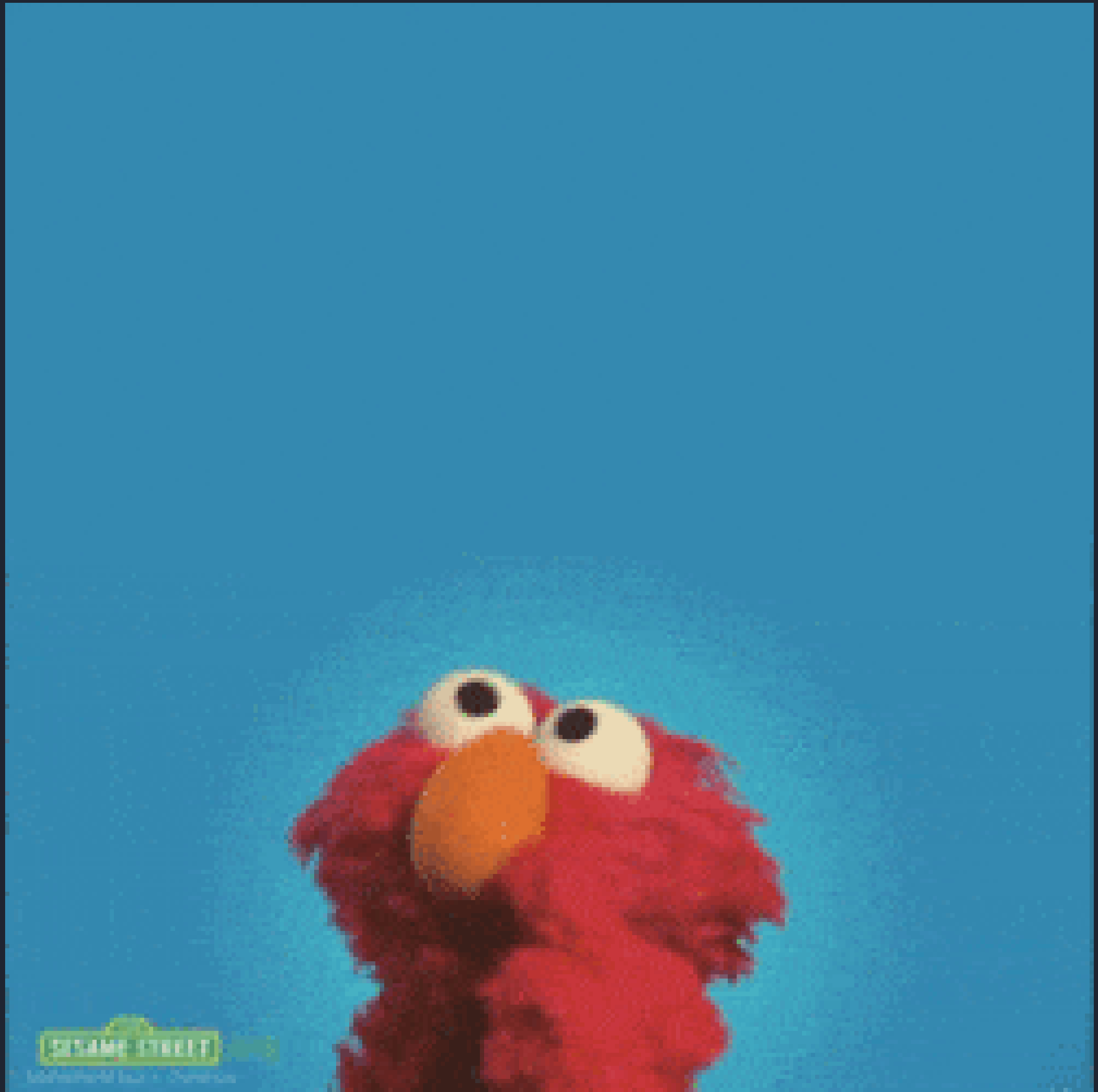
Generic ETW CreateFile Pattern
Microsoft-Windows-ThreatIntelligence
Microsoft-Windows-DNS-Client
Microsoft.Web.Platform
Microsoft-Windows-Win32k
Microsoft-Antimalware-Scan-Interface
Microsoft-Antaimalware-UacScan
Microsoft-Windows-TCPIP
Microsoft-Windows-WMI-Activity
Microsoft-Windows-LDAP-Client
Microsoft-Windows-AppLocker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

EXAMPLE CONFIG COMPONENT



```
ProviderGuid: "{099614a5-5dd7-4788-8bc9-e29f43db28fc}"
Name: "Microsoft-Windows-Ldap-Client"
KeywordMask: "0x1"
▽ Rules: (1) [{id: "{661c6840-748d-4fd4-9c5f-74420f95eba9}", dataAttributions: {…}, name: "Ldap Search", version: "
  ▽ [0]: (9) {id: "{661c6840-748d-4fd4-9c5f-74420f95eba9}", dataAttributions: {…}, name: "Ldap Search", version: "1
      id: "{661c6840-748d-4fd4-9c5f-74420f95eba9}"
    ▽ dataAttributions: (3) {UseCases: 14, Consumers: 1542, AsimovNamespace: 0}
        UseCases: 14
        Consumers: 1542
        AsimovNamespace: 0
      name: "Ldap Search"
      version: "1"
    ▽ capping: (2) {globalCapping: {…}, localCapping: […]}
      ▽ globalCapping: (1) {capping: 1000}
          capping: 1000
      ▽ localCapping: (1) [{expirationPeriodInHours: 24, capping: 1, id: "LdapFirstSeen", fields: […]}]
        ▽ [0]: (4) {expirationPeriodInHours: 24, capping: 1, id: "LdapFirstSeen", fields: […]}
            expirationPeriodInHours: 24
            capping: 1
            id: "LdapFirstSeen"
          ▽ fields: (5) [{…}, {…}, {…}, {…}, {…}]
            ▽ [0]: (1) {fieldName: "SearchFilter"}
                fieldName: "SearchFilter"
            ▽ [1]: (1) {fieldName: "DistinguishedName"}
                fieldName: "DistinguishedName"
            ▽ [2]: (1) {fieldName: "InitiatingProcess:PROCESS_NAME"}
                fieldName: "InitiatingProcess:PROCESS_NAME"
            ▽ [3]: (1) {fieldName: "InitiatingProcess:PROCESS_IMAGE_ORIGINAL_NAME"}
                fieldName: "InitiatingProcess:PROCESS_IMAGE_ORIGINAL_NAME"
            ▽ [4]: (1) {fieldName: "InitiatingProcess:PROCESS_CI_SIGNING_LEVEL"}
                fieldName: "InitiatingProcess:PROCESS_CI_SIGNING_LEVEL"
    ▽ filters: (3) {expressionType: "Operator", operator: "Not", expressions: […]}
```

WHICH MADE ME WONDER...



CAN I WRITE MY OWN

EVENT EVENT EVENT EVENT

EVENT EVENT EVENT EVENT

EVENT EVENT EVENT EVENT

EVENT EVENT EVENT EVENT

EVENT EVENT EVENT EVENT

EVENT EVENT EVENT EVENT

Can I write my own events?

- Make the EDR believe ‘things’ happened, for instance for impersonating attacks which are too risky or complicated to run.
- Use it offensively for creating distractions or spoofing events.
- Since most cloud based EDRs have caps on events, we potentially can create blind spots.

ETW USER-MODE PROVIDER REGISTRATION

□ ETW providers are registered by GUID, any process can register a provider with any GUID. Including one already registered by another process.

□ Each registration is process-specific: every registration gets a unique handle/registration for that process.

□ If you call `EventRegister` with the same provider GUID from two different processes, both will be registered and both can emit events.

UNDERSTANDING PROVIDERS

Manifest-based Providers

1. Introduced with Windows Vista and replace the classic providers
2. Use XML manifest files to define events, channels, and metadata
3. Typically stored in: `%SystemRoot%\System32\winevt\`

TraceLogging Providers

1. Introduced with Windows 10
2. Self-describing events (no separate manifest needed)
3. Good for dynamic scenarios where event structure isn't known at compile time

There are also MOF-based Providers, these are not so commonly used anymore

RELEVANT MANIFEST STRUCTURE 1/2

Provider Element

```
name="Microsoft-Windows-LDAP-Client"
guid="{099614a5-5dd7-4788-8bc9-e29f43db28fc}"
resourceFileName="Microsoft-Windows-LDAP-Client"
messageFileName="Microsoft-Windows-LDAP-Client"
symbol="MicrosoftWindowsLDAPClient"
source="Xml"
```

Event Elements

```
<event
  value="30"
  symbol="task_030"
  version="0"
  task="task_0"
  level="win:Always"
  keywords="search"
  template="task_030Args"
/>
```

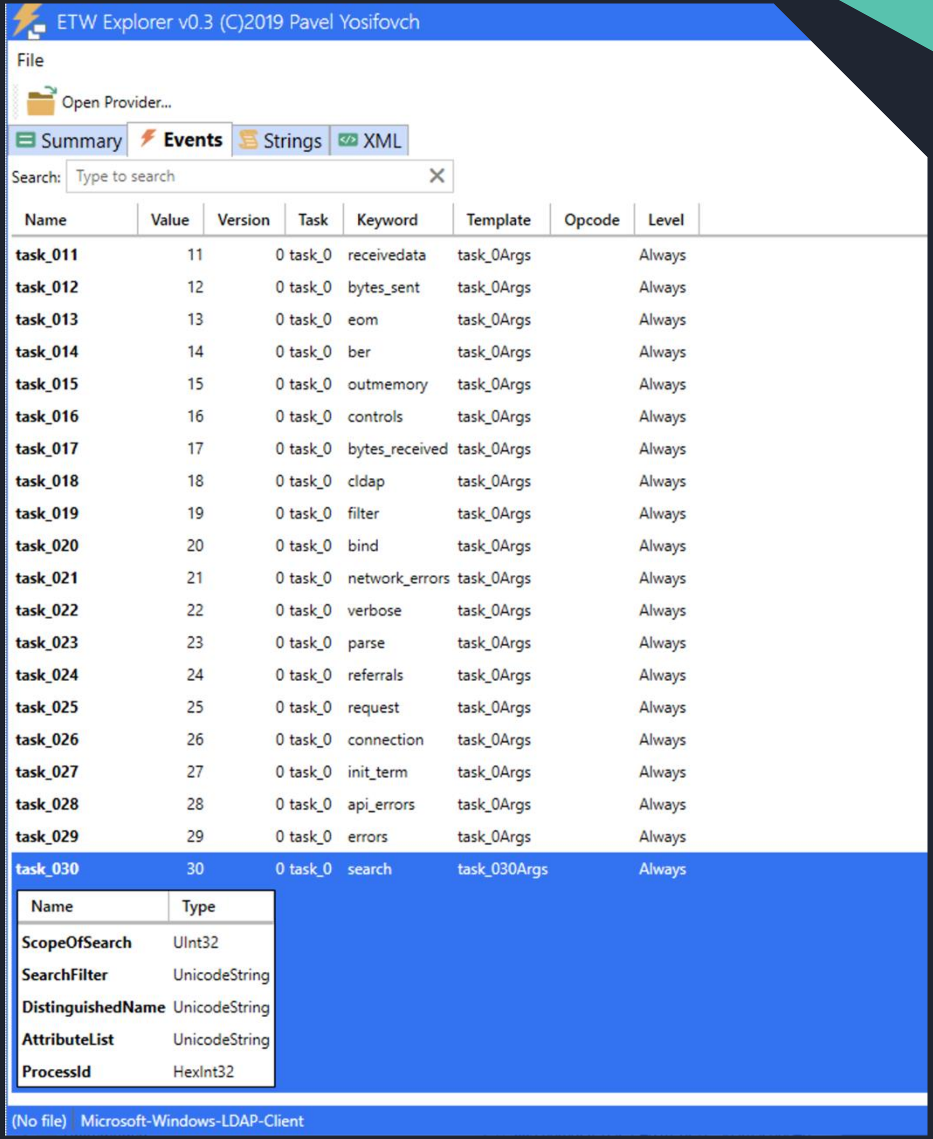
RELEVANT MANIFEST STRUCTURE 2/2

Template Elements

```
<template tid="task_030Args">
  <data name="ScopeOfSearch" inType="win:UInt32" />
  <data name="SearchFilter" inType="win:UnicodeString" />
  <data name="DistinguishedName" inType="win:UnicodeString" />
  <data name="AttributeList" inType="win:UnicodeString" />
  <data name="ProcessId" inType="win:HexInt32" />
</template>
```

RECOMMENDED TOOLS

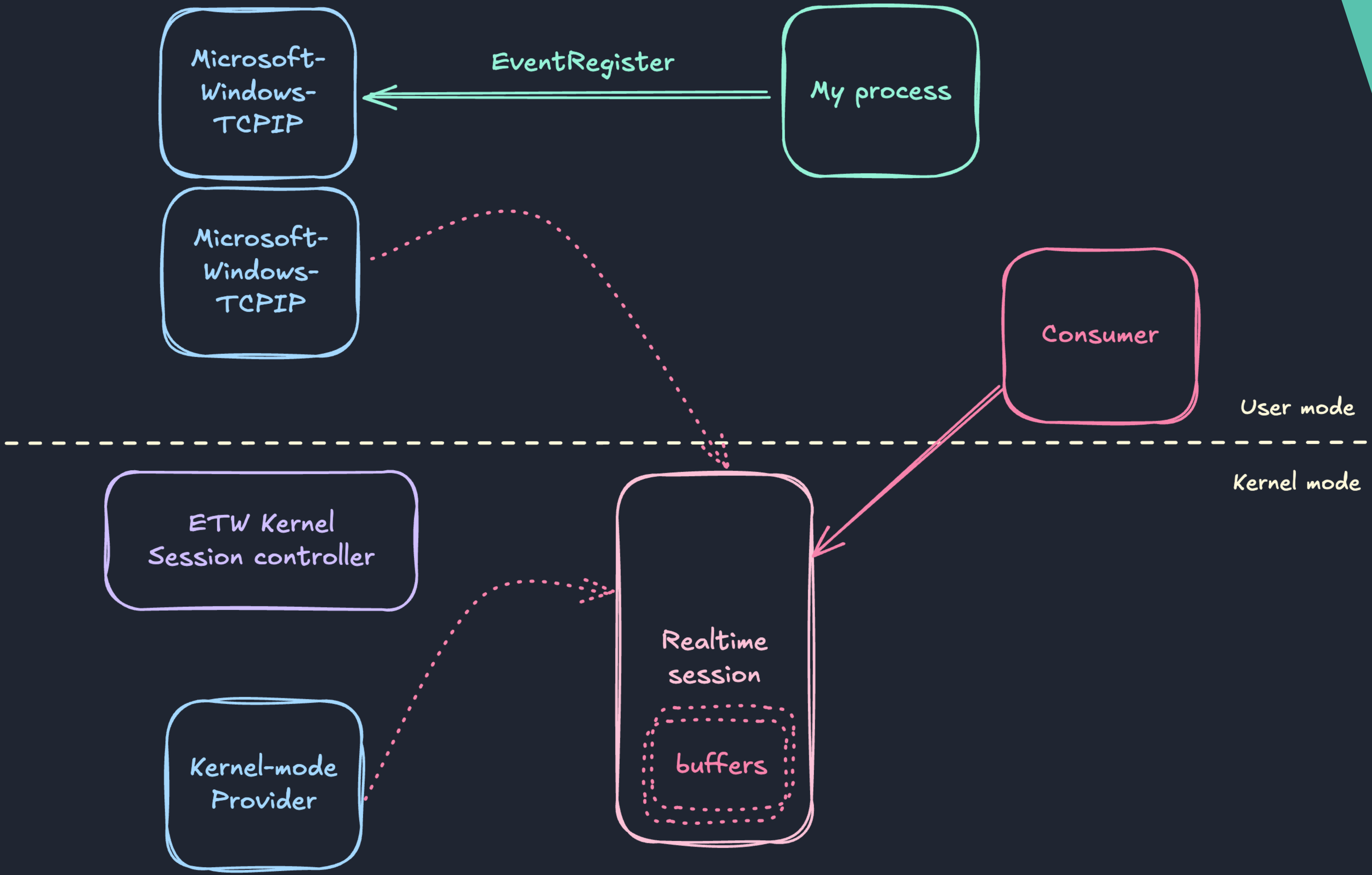
EtwExplorer	https://github.com/zodiacon/EtwExplorer
WEPExplorer	https://github.com/0xeb/WinTools
ETWInspector	https://github.com/jonny-jhnson/ETWInspector

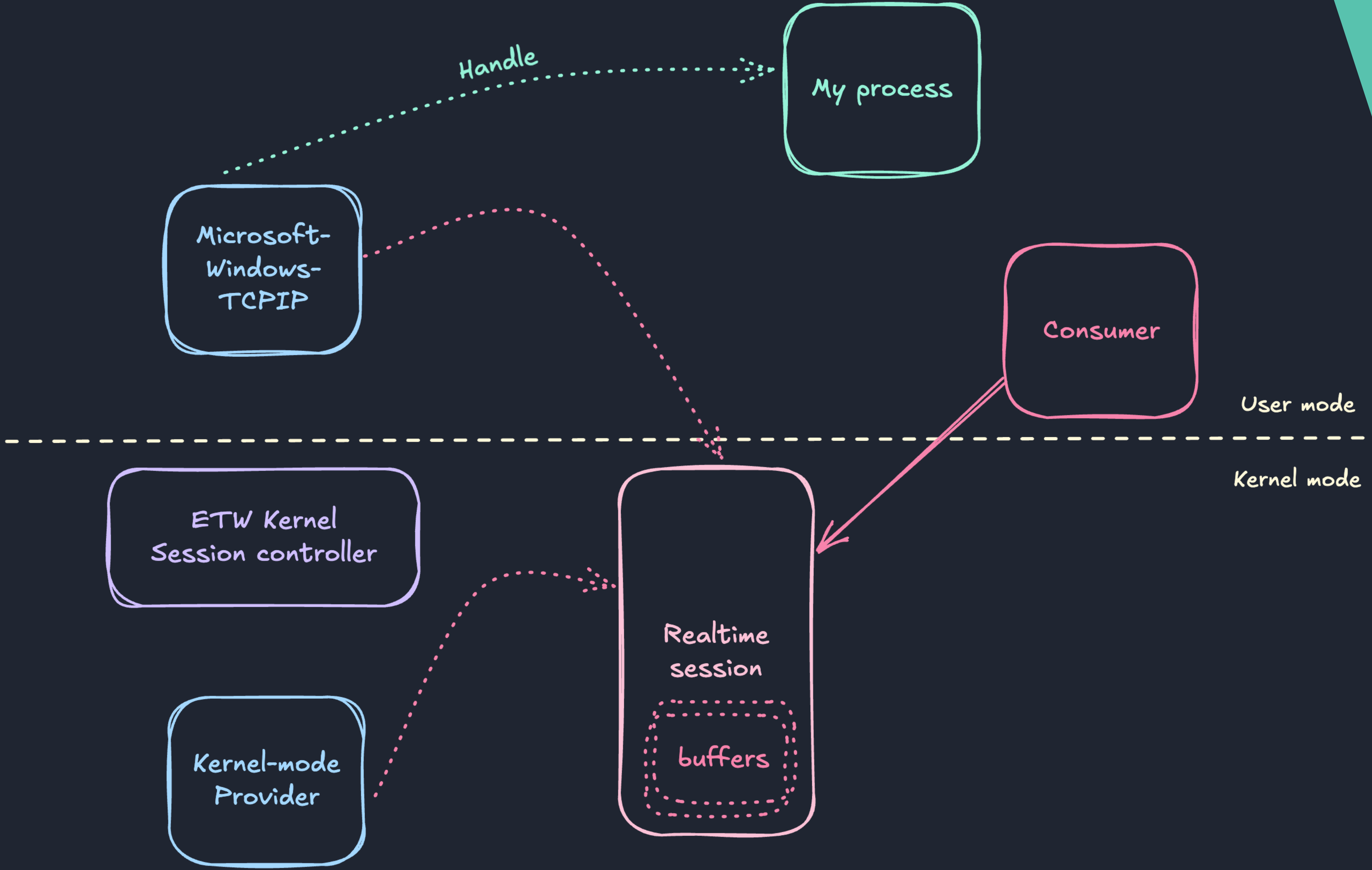


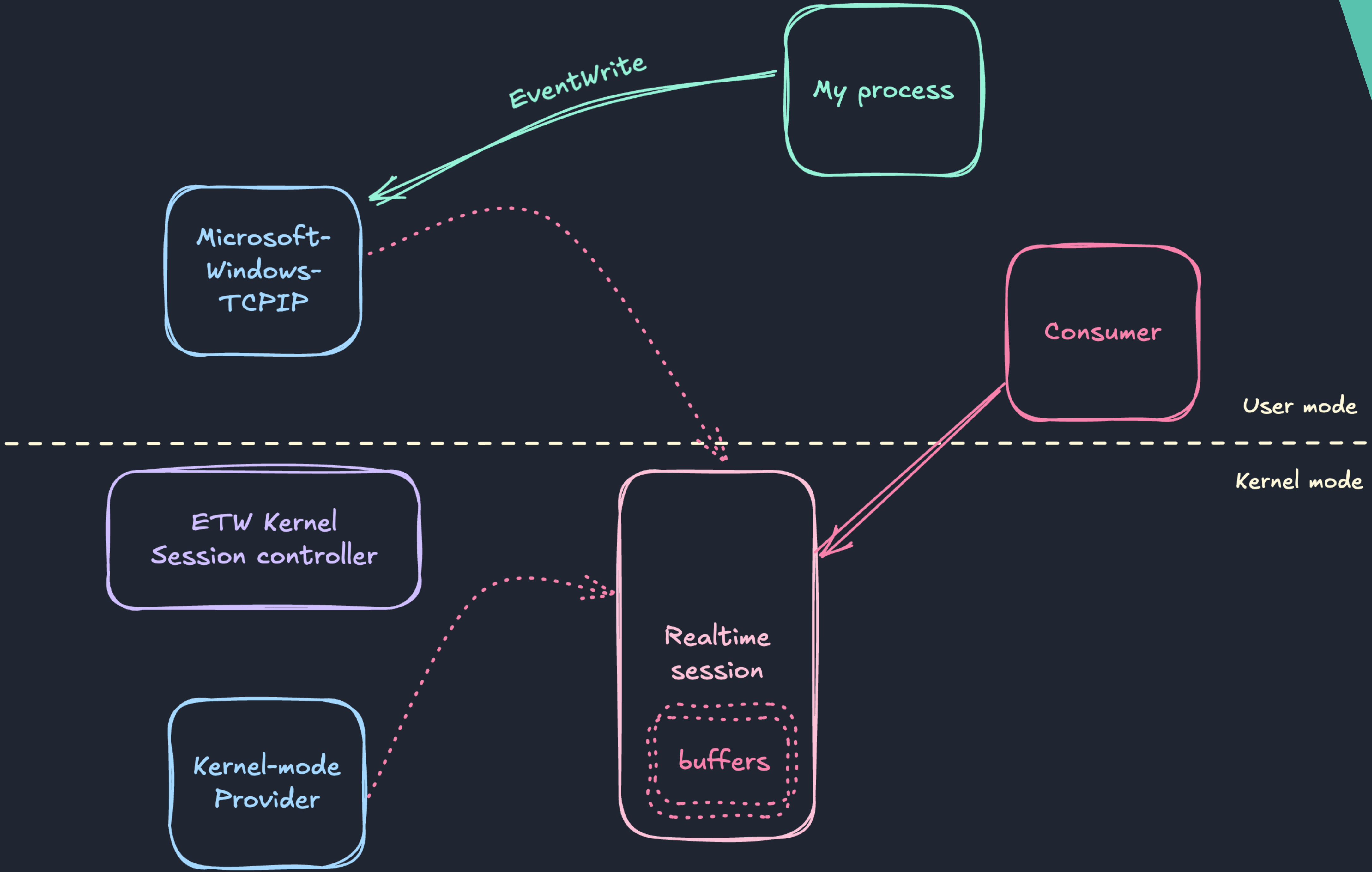
Name	Value	Version	Task	Keyword	Template	Opcode	Level
task_011	11	0	task_0	receivedata	task_0Args		Always
task_012	12	0	task_0	bytes_sent	task_0Args		Always
task_013	13	0	task_0	eom	task_0Args		Always
task_014	14	0	task_0	ber	task_0Args		Always
task_015	15	0	task_0	outmemory	task_0Args		Always
task_016	16	0	task_0	controls	task_0Args		Always
task_017	17	0	task_0	bytes_received	task_0Args		Always
task_018	18	0	task_0	cldap	task_0Args		Always
task_019	19	0	task_0	filter	task_0Args		Always
task_020	20	0	task_0	bind	task_0Args		Always
task_021	21	0	task_0	network_errors	task_0Args		Always
task_022	22	0	task_0	verbose	task_0Args		Always
task_023	23	0	task_0	parse	task_0Args		Always
task_024	24	0	task_0	referrals	task_0Args		Always
task_025	25	0	task_0	request	task_0Args		Always
task_026	26	0	task_0	connection	task_0Args		Always
task_027	27	0	task_0	init_term	task_0Args		Always
task_028	28	0	task_0	api_errors	task_0Args		Always
task_029	29	0	task_0	errors	task_0Args		Always
task_030	30	0	task_0	search	task_030Args		Always

Name	Type
ScopeOfSearch	UInt32
SearchFilter	UnicodeString
DistinguishedName	UnicodeString
AttributeList	UnicodeString
ProcessId	HexInt32

(No file) Microsoft-Windows-LDAP-Client


Microsoft-Windows-TCPIP
EventRegister
My process
Microsoft-Windows-TCPIP
Consumer
User mode
Kernel mode
ETW Kernel Session controller
Realtime session
buffers
Kernel-mode Provider


Handle
My process
Microsoft-Windows-TCPIP
Consumer
User mode
Kernel mode
ETW Kernel Session controller
Realtime session
buffers
Kernel-mode Provider


My process
EventWrite
Microsoft-Windows-TCPIP
Consumer
User mode
Kernel mode
ETW Kernel Session controller
Realtime session
buffers
Kernel-mode Provider

"INJECTING EVENTS"

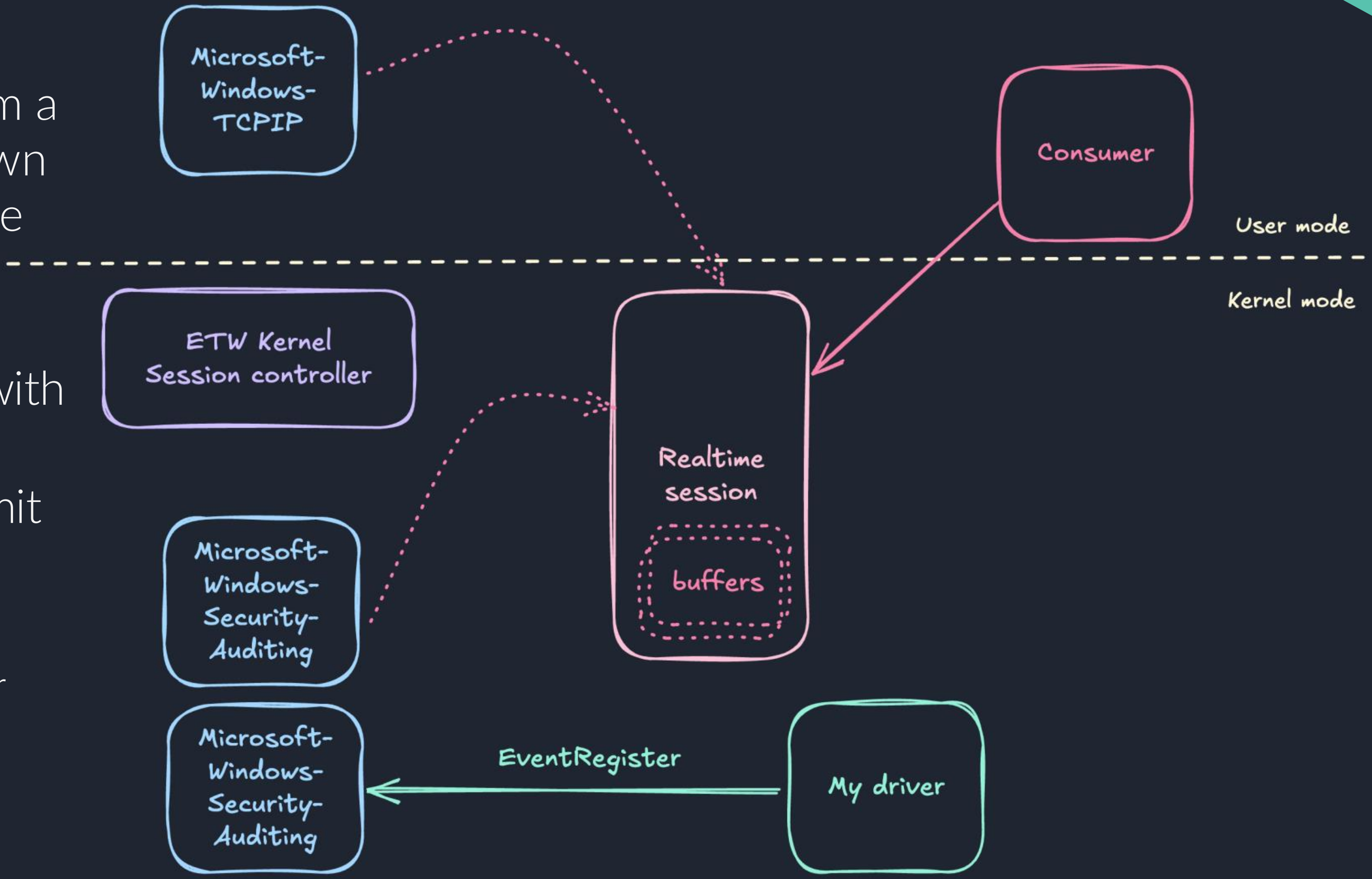
- You can emit events with the same provider GUID from a different process, and trace consumers will receive these events coming from that provider.
- ETW does not (in general) record which process emitted an event; most consumers just see the provider GUID, event ID, payload, and process ID (PID) info.
- You can't spoof the PID information in the events, this is handled by the kernel. ☹

KERNEL ETW PROVIDERS

The only way to emit events from a kernel provider is to load your own signed driver, then like user mode providers:

- Register a provider GUID with that driver.
- Use kernel ETW APIs to emit events.

I did not try to validate this via a driver (yet).


Microsoft-Windows-TCPIP
Consumer
User mode
Kernel mode
ETW Kernel Session controller
Realtime session
buffers
Microsoft-Windows-Security-Auditing
Microsoft-Windows-Security-Auditing
EventRegister
My driver

SECURITY SECURITY SECURITY SECURITY SECURITY
SECURITY SECURITY SECURITY SECURITY SECURITY
SECURITY SECURITY SECURITY SECURITY SECURITY
SECURITY SECURITY SECURITY SECURITY SECURITY
SECURITY SECURITY SECURITY SECURITY SECURITY
SECURITY SECURITY SECURITY SECURITY SECURITY
SECURITY SECURITY SECURITY SECURITY SECURITY
SECURITY SECURITY SECURITY SECURITY SECURITY
SECURITY SECURITY SECURITY SECURITY SECURITY
SECURITY SECURITY SECURITY SECURITY SECURITY
SECURITY SECURITY SECURITY SECURITY SECURITY
SECURITY SECURITY SECURITY SECURITY SECURITY
SECURITY SECURITY SECURITY SECURITY SECURITY
SECURITY SECURITY SECURITY SECURITY SECURITY
SECURITY SECURITY SECURITY SECURITY SECURITY

ETW SECURITY MODEL

Like almost any object in Windows, Providers can have permissions assigned to them. These are stored in the registry under the following key;

`HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\WMI\Security`

ETW inherits its security permission defaults from the original WMI security, with some additions.

If there is no specific configuration set for a provider, the default permissions set in the special GUID `{0811C1AF-7A07-4A06-82ED-869455CDF713}` will apply.

ASSIGNABLE PERMISSIONS

Permissions that can be assigned to a User or Group per provider are;

0x00000001	WMIGUID_QUERY
0x00000002	WMIGUID_SET
0x00000004	WMIGUID_NOTIFICATION
0x00000008	WMIGUID_READ_DESCRIPTION
0x00000010	WMIGUID_EXECUTE
0x00000020	TRACELOG_CREATE_REALTIME
0x00000040	TRACELOG_CREATE_ONDISK
0x00000080	TRACELOG_GUID_ENABLE
0x00000100	TRACELOG_ACCESS_KERNEL_LOGGER
0x00000200	TRACELOG_CREATE_INPROC
	TRACELOG_LOG_EVENT
0x00000400	TRACELOG_ACCESS_REALTIME
0x00000800	TRACELOG_REGISTER_GUIDS
0x00001000	TRACELOG_JOIN_GROUP
0x00121FFF	WMIGUID_ALL_ACCESS

THE DEFAULT PERMISSIONS

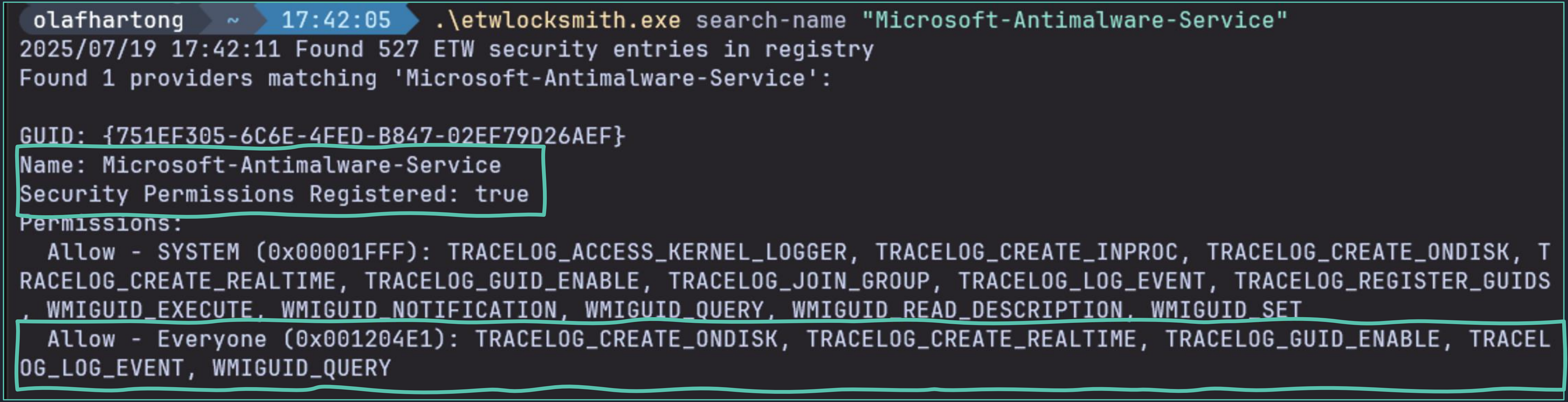
If no security policy is set, the default will be applied, which is:

User or Group	Access Rights
localhost\Everyone	TRACELOG_REGISTER_GUIDS TRACELOG_JOIN_GROUP
NT AUTHORITY\SYSTEM NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE BUILTIN\Administrators	WMIGUID_ALL_ACCESS WMIGUID_ALL_ACCESS without TRACELOG_JOIN_GROUP

BUILTIN\Performance Log Users	WMIGUID_QUERY;
	WMIGUID_NOTIFICATION;
	TRACELOG_CREATE_REALTIME;
	TRACELOG_CREATE_ONDISK;
	TRACELOG_GUID_ENABLE;
	TRACELOG_LOG_EVENT;
	TRACELOG_ACCESS_REALTIME;
	TRACELOG_REGISTER_GUIDS

BUILTIN\Performance Monitor Users	WMIGUID_NOTIFICATION
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	TRACELOG_REGISTER_GUIDS TRACELOG_JOIN_GROUP

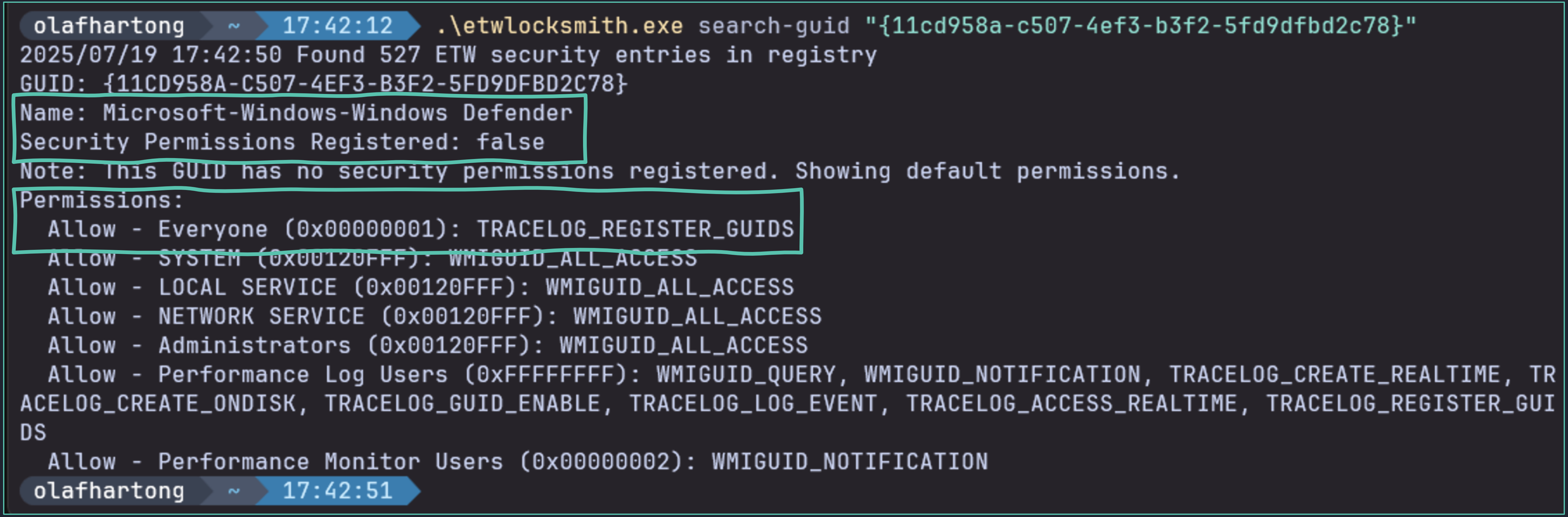
WHAT DOES THIS MEAN?



```
olafhartong  ~  17:42:05  .\etwlocksmith.exe search-name "Microsoft-Antimalware-Service"
2025/07/19 17:42:11 Found 527 ETW security entries in registry
Found 1 providers matching 'Microsoft-Antimalware-Service':

GUID: {751EF305-6C6E-4FED-B847-02EF79D26AEF}
Name: Microsoft-Antimalware-Service
Security Permissions Registered: true
Permissions:
  Allow - SYSTEM (0x00001FFF): TRACELOG_ACCESS_KERNEL_LOGGER, TRACELOG_CREATE_INPROC, TRACELOG_CREATE_ONDISK, T
RACELOG_CREATE_REALTIME, TRACELOG_GUID_ENABLE, TRACELOG_JOIN_GROUP, TRACELOG_LOG_EVENT, TRACELOG_REGISTER_GUIDS
, WMIGUID_EXECUTE, WMIGUID_NOTIFICATION, WMIGUID_QUERY, WMIGUID_READ_DESCRIPTION, WMIGUID_SET
  Allow - Everyone (0x001204E1): TRACELOG_CREATE_ONDISK, TRACELOG_CREATE_REALTIME, TRACELOG_GUID_ENABLE, TRACEL
OG_LOG_EVENT, WMIGUID_QUERY
```

https://github.com/olafhartong/ETWLocksmith

WHAT DOES THIS MEAN?



```
olafhartong ~ 17:42:12  .\etwlocksmith.exe search-guid "{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78}"
2025/07/19 17:42:50 Found 527 ETW security entries in registry
GUID: {11CD958A-C507-4EF3-B3F2-5FD9DFBD2C78}
Name: Microsoft-Windows-Windows Defender
Security Permissions Registered: false
Note: This GUID has no security permissions registered. Showing default permissions.
Permissions:
  Allow - Everyone (0x00000001): TRACELOG_REGISTER_GUIDS
  Allow - SYSTEM (0x00120FFF): WMIGUID_ALL_ACCESS
  Allow - LOCAL SERVICE (0x00120FFF): WMIGUID_ALL_ACCESS
  Allow - NETWORK SERVICE (0x00120FFF): WMIGUID_ALL_ACCESS
  Allow - Administrators (0x00120FFF): WMIGUID_ALL_ACCESS
  Allow - Performance Log Users (0xFFFFFFFF): WMIGUID_QUERY, WMIGUID_NOTIFICATION, TRACELOG_CREATE_REALTIME, TR
ACELOG_CREATE_ONDISK, TRACELOG_GUID_ENABLE, TRACELOG_LOG_EVENT, TRACELOG_ACCESS_REALTIME, TRACELOG_REGISTER_GUI
DS
  Allow - Performance Monitor Users (0x00000002): WMIGUID_NOTIFICATION
olafhartong ~ 17:42:51
```

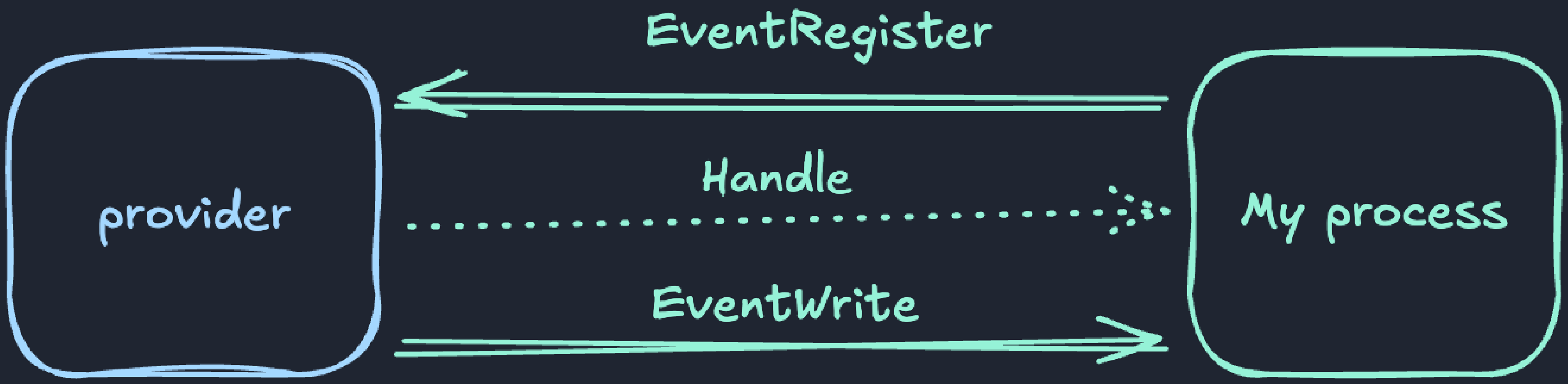
MICROSOFT.WINDOWS.SENSE.GENERATEDETW MICROSOFT-WINDOWS-CRYPTO-DPAPI-EVENTS MICROSOFT.WINDOWS.COMOLEAUT32
MICROSOFT-WINDOWS-TERMINALSERVICES-LOCALSESSIONMANAGER MICROSOFT-WINDOWS-SEC GENERIC ETW CREATEFILE PATTERN
MICROSOFT-WINDOWS-SEC-WFP MICROSOFT-WINDOWS-DOTNETRUNTIME LSASRV SECUREETW MICROSOFT-WINDOWS-TCPIP MICROSOFT-WINDOWS-VHDMP MICROSOFT.WINDOWS.WEBDEFENSE.SENSELOGGING MICROSOFT-THREATPROTECTIONSERVICE
MICROSOFT.WINDOWS.SENSE.CONNECTIVITYCHECKER MICROSOFT-WINDOWS-KERNEL-AUDIT-API-CALLS POWERSHELL CMDLETS MICROSOFT-WINDOWS-GROUPPOLICY MICROSOFT.WINDOWS.SENSE.REGHEARTBEAT ANAHEIM-SMARTSCREEN

ENUMERATING ALL PROVIDERS MDE USES

MICROSOFT.AAD.RUNTIME MICROSOFT.WINDOWS.SENSE.SENSECM MICROSOFT.WINDOWS.SENSENDR MICROSOFT.WINDOWS.NDRSCANNER
MICROSOFT-WINDOWS-DHCP-CLIENT MICROSOFT-WINDOWS-DHCPV6-CLIENT-EVENTS APPLICATION ERROR
MICROSOFT.WINDOWS.SENSE.VALIDATIONETW MICROSOFT.WINDOWS.SENSECOMPONENT.GENERATEDETW GENERIC ETW CREATEFILE PATTERN
MICROSOFT-WINDOWS-THREATINTELLIGENCE MICROSOFT.WINDOWS.SENSE.GENERATEDETW 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 MICROSOFT-WINDOWS-FILTERMANAGER ANTI TAMPERING ANAHEIM-SMARTSCREEN USER32 MICROSOFT.WINDOWS.USER32 APPLICATION ERROR MICROSOFT.WINDOWS.SENSECOMPONENT.GENERATEDETW

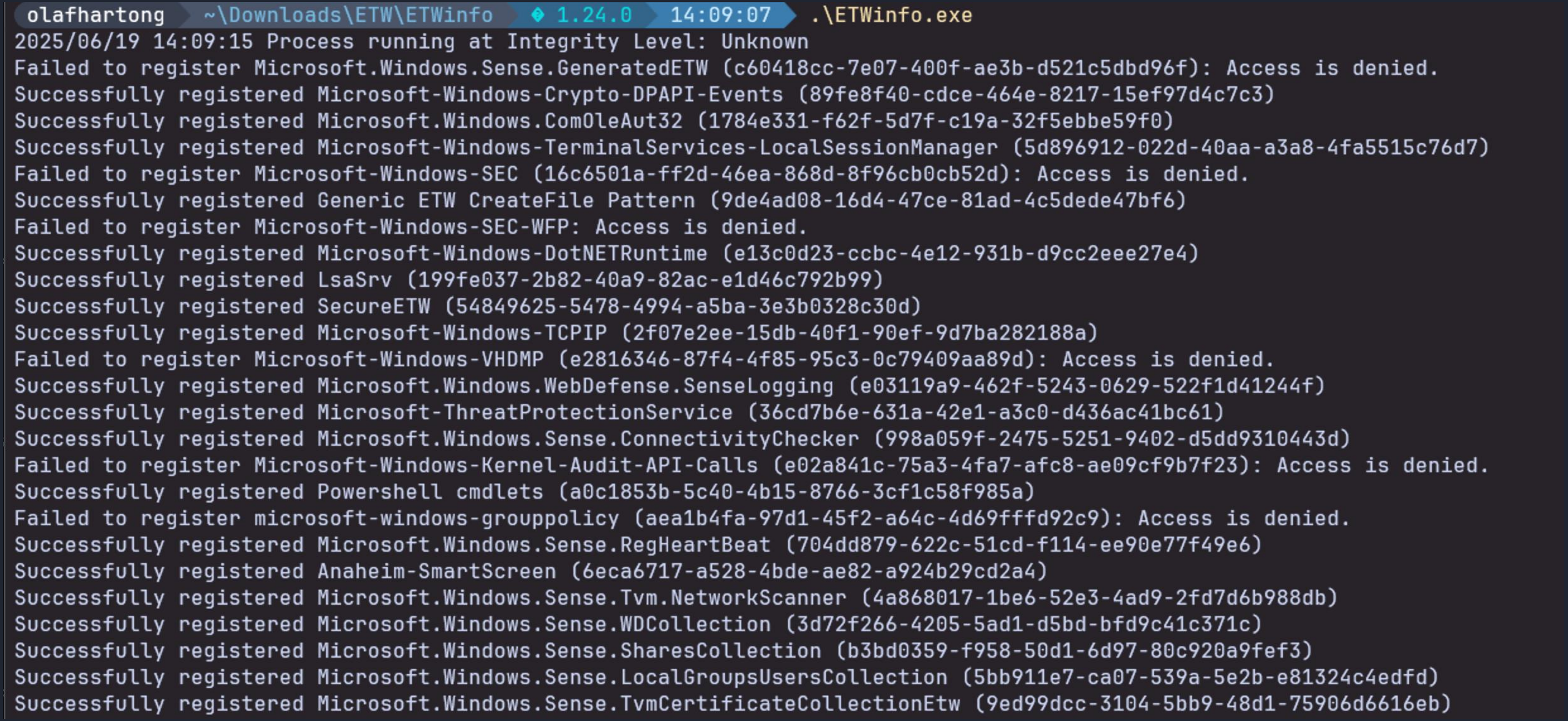
REGISTERING AND TRYING TO EMIT

```
For provider in providerlist {
```



```
}
```

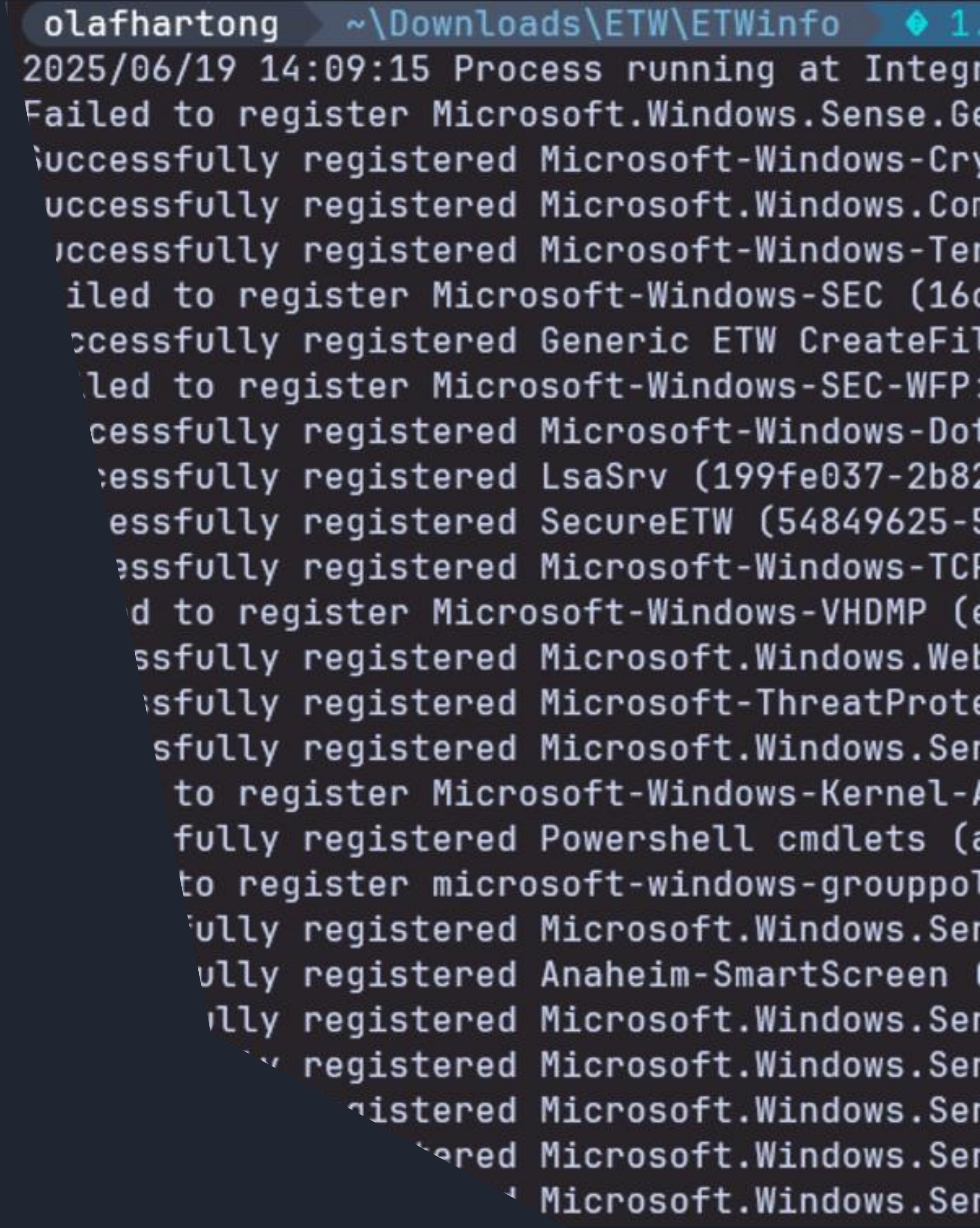
REGISTERING AND TRYING TO EMIT



```
olafhartong  ~\Downloads\ETW\ETWinfo  ◆ 1.24.0  14:09:07  .\ETWinfo.exe
2025/06/19 14:09:15 Process running at Integrity Level: Unknown
Failed to register Microsoft.Windows.Sense.GeneratedETW (c60418cc-7e07-400f-ae3b-d521c5dbd96f): Access is denied.
Successfully registered Microsoft-Windows-Crypto-DPAPI-Events (89fe8f40-cdce-464e-8217-15ef97d4c7c3)
Successfully registered Microsoft.Windows.ComOleAut32 (1784e331-f62f-5d7f-c19a-32f5ebbe59f0)
Successfully registered Microsoft-Windows-TerminalServices-LocalSessionManager (5d896912-022d-40aa-a3a8-4fa5515c76d7)
Failed to register Microsoft-Windows-SEC (16c6501a-ff2d-46ea-868d-8f96cb0cb52d): Access is denied.
Successfully registered Generic ETW CreateFile Pattern (9de4ad08-16d4-47ce-81ad-4c5dede47bf6)
Failed to register Microsoft-Windows-SEC-WFP: Access is denied.
Successfully registered Microsoft-Windows-DotNETRuntime (e13c0d23-ccbc-4e12-931b-d9cc2eee27e4)
Successfully registered LsaSrv (199fe037-2b82-40a9-82ac-e1d46c792b99)
Successfully registered SecureETW (54849625-5478-4994-a5ba-3e3b0328c30d)
Successfully registered Microsoft-Windows-TCPIP (2f07e2ee-15db-40f1-90ef-9d7ba282188a)
Failed to register Microsoft-Windows-VHDMP (e2816346-87f4-4f85-95c3-0c79409aa89d): Access is denied.
Successfully registered Microsoft.Windows.WebDefense.SenseLogging (e03119a9-462f-5243-0629-522f1d41244f)
Successfully registered Microsoft-ThreatProtectionService (36cd7b6e-631a-42e1-a3c0-d436ac41bc61)
Successfully registered Microsoft.Windows.Sense.ConnectivityChecker (998a059f-2475-5251-9402-d5dd9310443d)
Failed to register Microsoft-Windows-Kernel-Audit-API-Calls (e02a841c-75a3-4fa7-afc8-ae09cf9b7f23): Access is denied.
Successfully registered Powershell cmdlets (a0c1853b-5c40-4b15-8766-3cf1c58f985a)
Failed to register microsoft-windows-grouppolicy (aea1b4fa-97d1-45f2-a64c-4d69fffd92c9): Access is denied.
Successfully registered Microsoft.Windows.Sense.RegHeartBeat (704dd879-622c-51cd-f114-ee90e77f49e6)
Successfully registered Anaheim-SmartScreen (6eca6717-a528-4bde-ae82-a924b29cd2a4)
Successfully registered Microsoft.Windows.Sense.Tvm.NetworkScanner (4a868017-1be6-52e3-4ad9-2fd7d6b988db)
Successfully registered Microsoft.Windows.Sense.WDCollection (3d72f266-4205-5ad1-d5bd-bfd9c41c371c)
Successfully registered Microsoft.Windows.Sense.SharesCollection (b3bd0359-f958-50d1-6d97-80c920a9fef3)
Successfully registered Microsoft.Windows.Sense.LocalGroupsUsersCollection (5bb911e7-ca07-539a-5e2b-e81324c4edfd)
Successfully registered Microsoft.Windows.Sense.TvmCertificateCollectionEtw (9ed99dcc-3104-5bb9-48d1-75906d6616eb)
```

THIS RESULTED IN FALSE POSITIVES

- You can “register” a kernel-mode provider in user-mode.
- This will not be handled the same since user-mode and kernel-mode providers are isolated.
- User mode cannot spoof kernel events or GUIDs



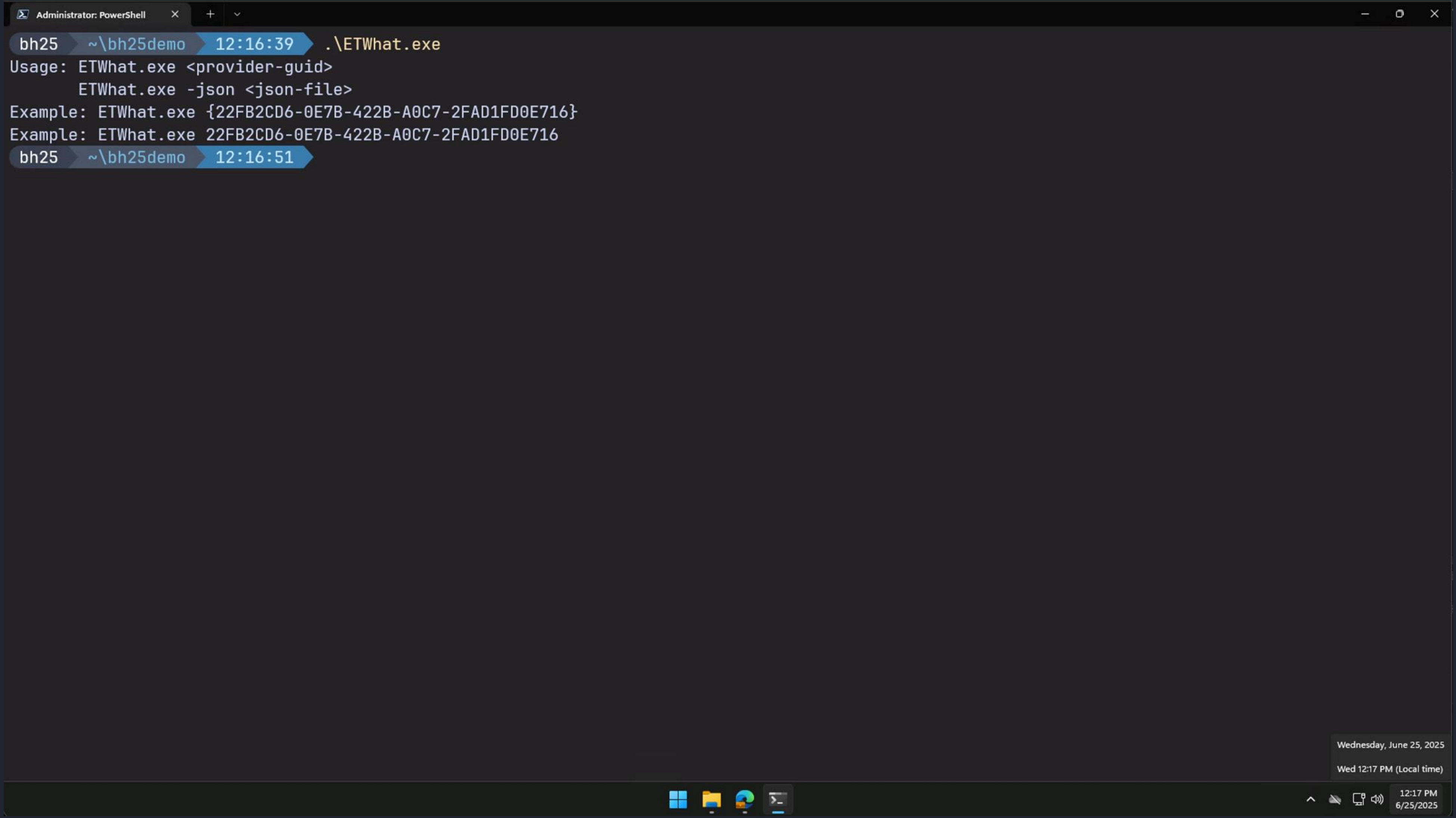
```
olafhartong  ~\Downloads\ETW\ETWinfo  1
2025/06/19 14:09:15 Process running at Integr
Failed to register Microsoft.Windows.Sense.Ge
Successfully registered Microsoft-Windows-Cry
uccessfully registered Microsoft.Windows.Con
uccessfully registered Microsoft-Windows-Ter
iled to register Microsoft-Windows-SEC (16c
ccessfully registered Generic ETW CreateFil
led to register Microsoft-Windows-SEC-WFP
cessfully registered Microsoft-Windows-Dot
essfully registered LsaSrv (199fe037-2b82
essfully registered SecureETW (54849625-5
essfully registered Microsoft-Windows-TCP
d to register Microsoft-Windows-VHDMP (e
ssfully registered Microsoft.Windows.Web
sfully registered Microsoft-ThreatProte
sfully registered Microsoft.Windows.Ser
 to register Microsoft-Windows-Kernel-A
fully registered Powershell cmdlets (a
to register microsoft-windows-grouppol
ully registered Microsoft.Windows.Ser
ully registered Anaheim-SmartScreen
lly registered Microsoft.Windows.Ser
 registered Microsoft.Windows.Ser
gistered Microsoft.Windows.Ser
ered Microsoft.Windows.Ser
 Microsoft.Windows.Ser
```

REFINED THE ENUMERATION

```
For provider in providerlist {
        Autologger config               HKLM\SYSTEM\CurrentControlSet\Control\WMI\Autologger\*
        Eventlog config                 HKLM\SYSTEM\CurrentControlSet\Services\EventLog\*
        User and kernel manifests       HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Publishers\*
        WMI registration                HKLM\SOFTWARE\Microsoft\WBEM\Providers\*
}
fmt.println (result)
```

https://github.com/olafhartong/ETWhat

REFINED THE ENUMERATION - ETWHAT



```
bh25  ~\bh25demo  12:16:39  .\ETWhat.exe
Usage: ETWhat.exe <provider-guid>
       ETWhat.exe -json <json-file>
Example: ETWhat.exe {22FB2CD6-0E7B-422B-A0C7-2FAD1FD0E716}
Example: ETWhat.exe 22FB2CD6-0E7B-422B-A0C7-2FAD1FD0E716
bh25  ~\bh25demo  12:16:51
```

POC ON LDAP-CLIENT ETW

- Wrote a basic POC in Go
- Tried building it with several available packages
- The options I found:

bi-zone/etw

Focused on consuming events

0xrawsec/golang-etw

Focused on consuming events

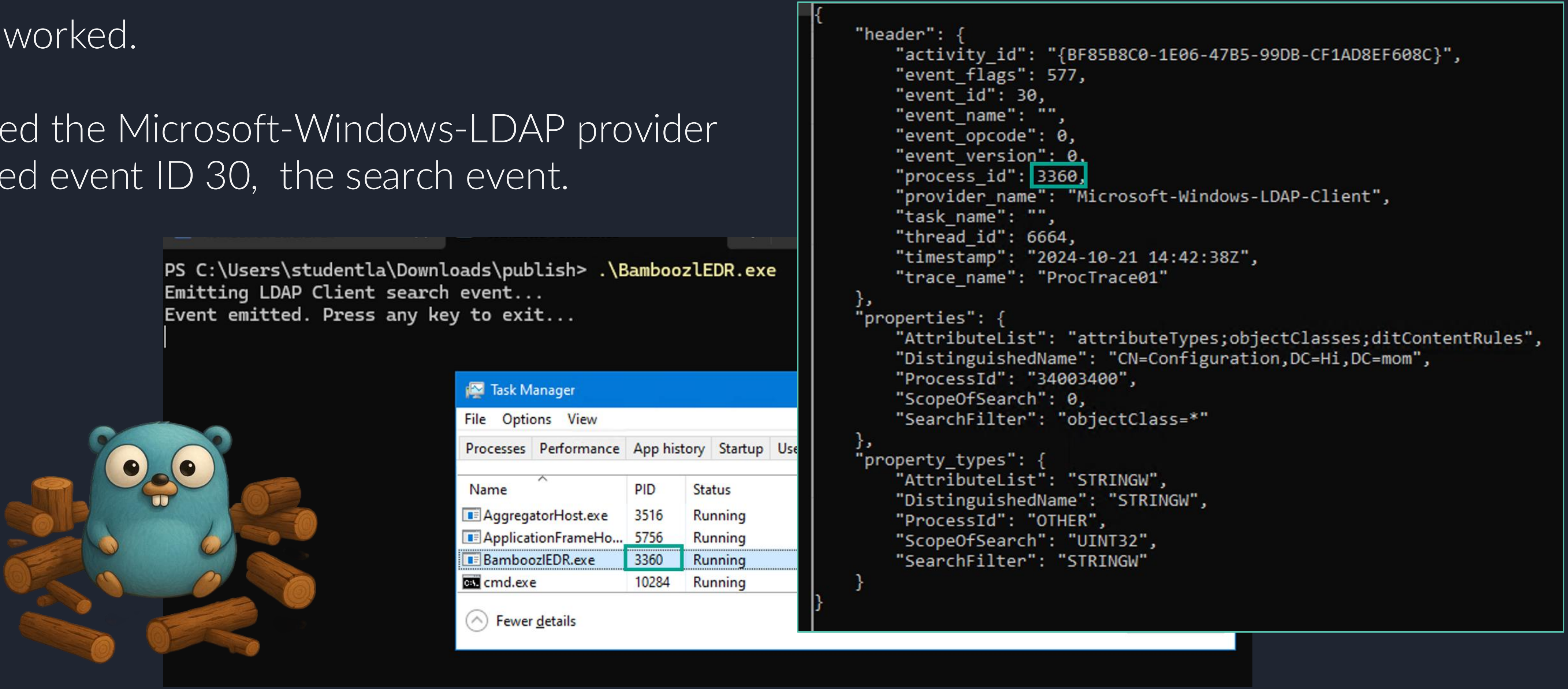
microsoft/go-winio/internal/etw

Focused on tracelogging (manifest-less) events
but can register providers and emit events

POC ON LDAP-CLIENT ETW

The POC worked.

It registered the Microsoft-Windows-LDAP provider and emitted event ID 30, the search event.



```
PS C:\Users\studentla\Downloads\publish> .\BamboozlEDR.exe
Emitting LDAP Client search event...
Event emitted. Press any key to exit...
```

Name	PID	Status
AggregatorHost.exe	3516	Running
ApplicationFrameHo...	5756	Running
BamboozlEDR.exe	3360	Running
cmd.exe	10284	Running

```
{
    "header": {
        "activity_id": "{BF85B8C0-1E06-47B5-99DB-CF1AD8EF608C}",
        "event_flags": 577,
        "event_id": 30,
        "event_name": "",
        "event_opcode": 0,
        "event_version": 0,
        "process_id": 3360,
        "provider_name": "Microsoft-Windows-LDAP-Client",
        "task_name": "",
        "thread_id": 6664,
        "timestamp": "2024-10-21 14:42:38Z",
        "trace_name": "ProcTrace01"
    },
    "properties": {
        "AttributeList": "attributeTypes;objectClasses;ditContentRules",
        "DistinguishedName": "CN=Configuration,DC=Hi,DC=mom",
        "ProcessId": "34003400",
        "ScopeOfSearch": 0,
        "SearchFilter": "objectClass=*"
    },
    "property_types": {
        "AttributeList": "STRINGW",
        "DistinguishedName": "STRINGW",
        "ProcessId": "OTHER",
        "ScopeOfSearch": "UINT32",
        "SearchFilter": "STRINGW"
    }
}
```

EVENTS SHOWED UP IN A TRACE BUT NOT MDE

AFTER A LONG TIME

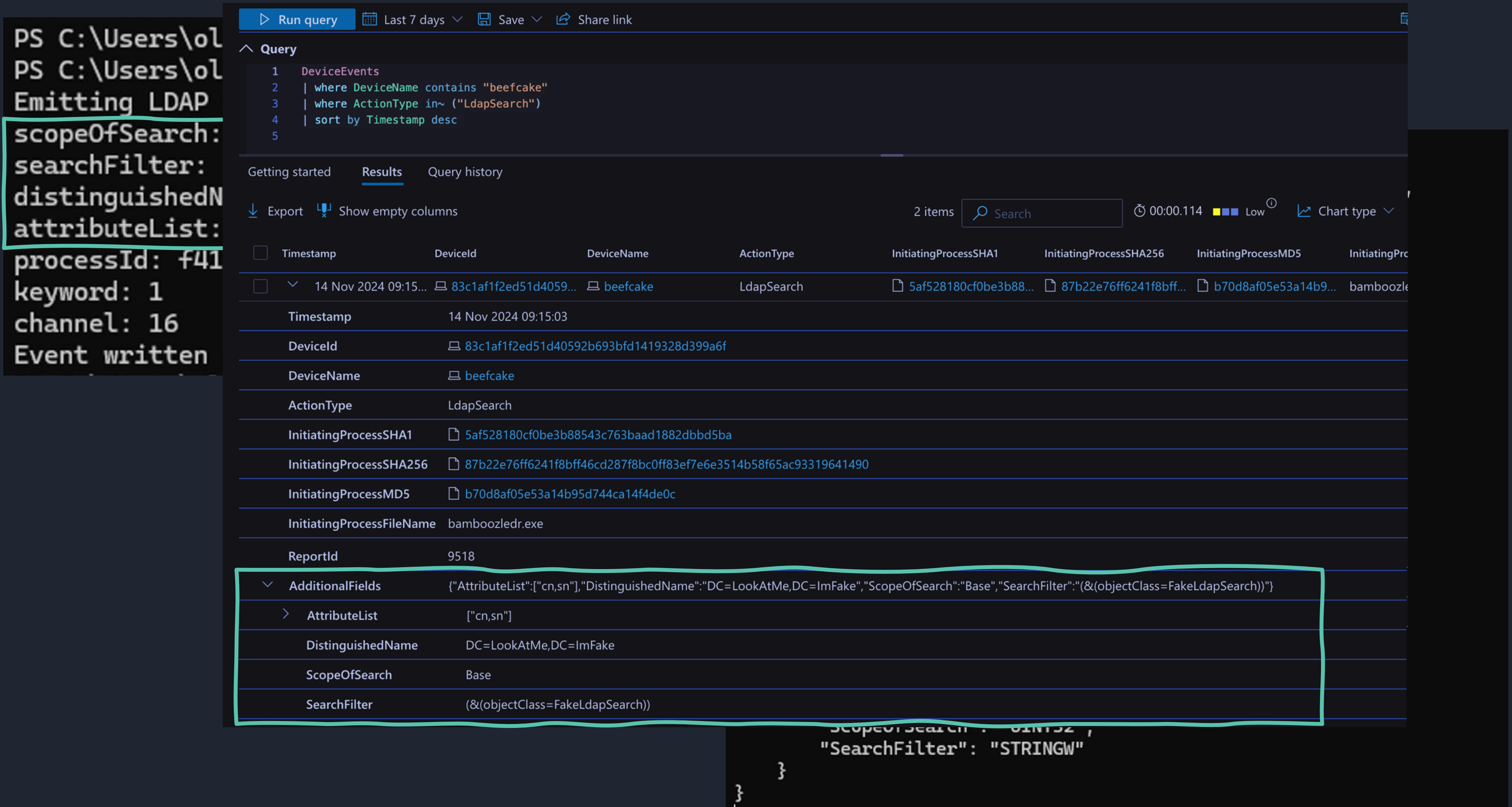
□ I started diffing real events vs my own, including the decoded values

□ Learnt the packages I tried didn’t provide control over the headers

□ Realized most Windows data should be written in little endian

□ Took a new approach, built a new implementation, based on Syscalls.

AND NOW IT DID SHOW UP IN MDE \o/



```
PS C:\Users\ol
PS C:\Users\ol
Emitting LDAP
scopeOfSearch:
searchFilter:
distinguishedN
attributeList:
processId: f41
keyword: 1
channel: 16
Event written
```

```
DeviceEvents
| where DeviceName contains "beefcake"
| where ActionType in~ ("LdapSearch")
| sort by Timestamp desc
```

Timestamp	DeviceId	DeviceName	ActionType	InitiatingProcessSHA1	InitiatingProcessSHA256	InitiatingProcessMD5	InitiatingPro
14 Nov 2024 09:15...	83c1af1f2ed51d4059...	beefcake	LdapSearch	5af528180cf0be3b88...	87b22e76ff6241f8bff...	b70d8af05e53a14b9...	bamboozle

Timestamp	14 Nov 2024 09:15:03
DeviceId	83c1af1f2ed51d40592b693bfd1419328d399a6f
DeviceName	beefcake
ActionType	LdapSearch
InitiatingProcessSHA1	5af528180cf0be3b88543c763baad1882dbbd5ba
InitiatingProcessSHA256	87b22e76ff6241f8bff46cd287f8bc0ff83ef7e6e3514b58f65ac93319641490
InitiatingProcessMD5	b70d8af05e53a14b95d744ca14f4de0c
InitiatingProcessFileName	bamboozledr.exe
ReportId	9518
AdditionalFields	{"AttributeList":["cn,sn"],"DistinguishedName":"DC=LookAtMe,DC=ImFake","ScopeOfSearch":"Base","SearchFilter":"(&(objectClass=FakeLdapSearch))"}
AttributeList	["cn,sn"]
DistinguishedName	DC=LookAtMe,DC=ImFake
ScopeOfSearch	Base
SearchFilter	(&(objectClass=FakeLdapSearch))

```
        "SearchFilter": "STRINGW"
    }
}
```

HOW CAN I ABUSE THIS ?

HOW CAN I ABUSE THIS ?

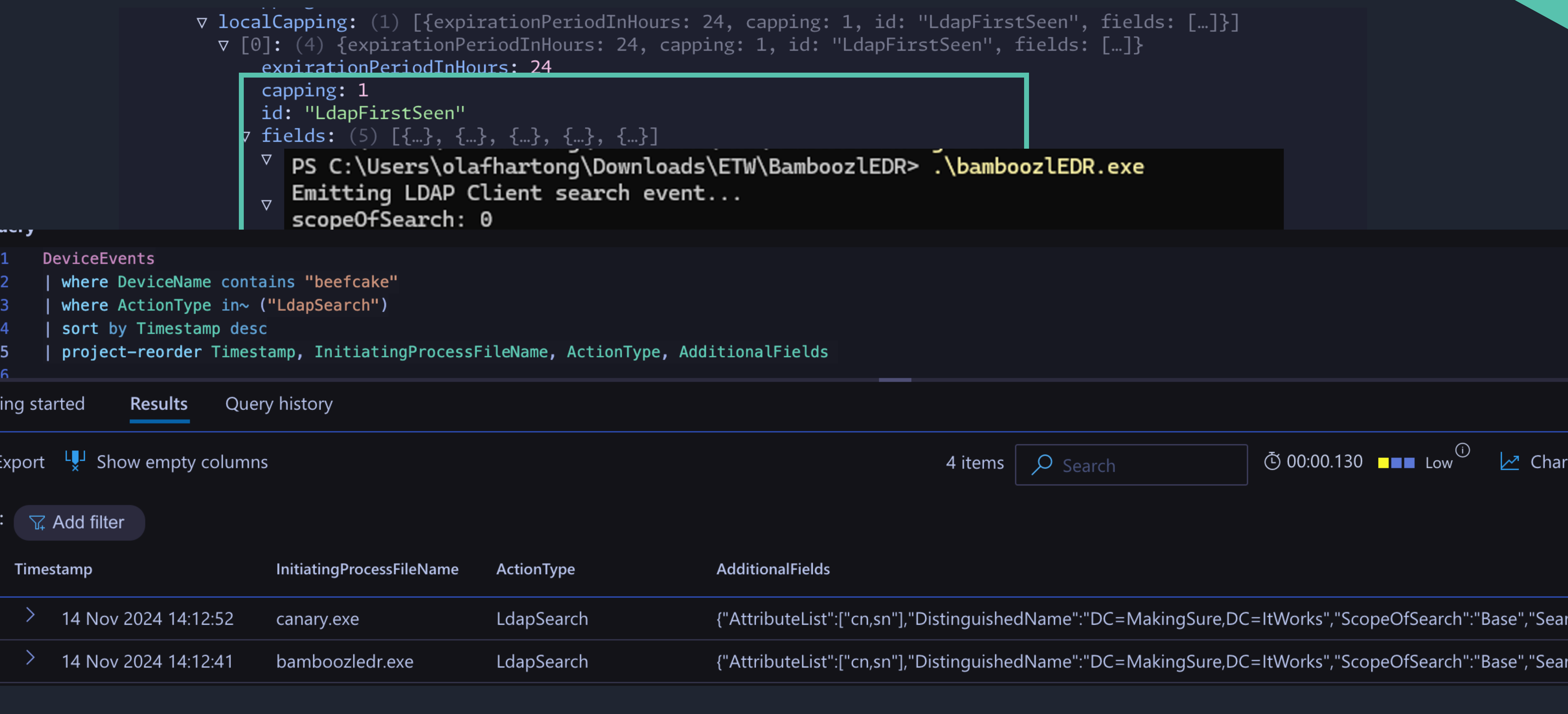
HOW CAN I ABUSE THIS ?

HOW CAN I ABUSE THIS ?

HOW CAN I ABUSE THIS ?

HOW CAN I ABUSE THIS ?

CHECKING THE LOCAL CAPPING CONFIG



```
▽ localCapping: (1) [{expirationPeriodInHours: 24, capping: 1, id: "LdapFirstSeen", fields: […]}]
  ▽ [0]: (4) {expirationPeriodInHours: 24, capping: 1, id: "LdapFirstSeen", fields: […]}
      expirationPeriodInHours: 24
      capping: 1
      id: "LdapFirstSeen"
    ▽ fields: (5) [{…}, {…}, {…}, {…}, {…}]
      ▽
      ▽
```

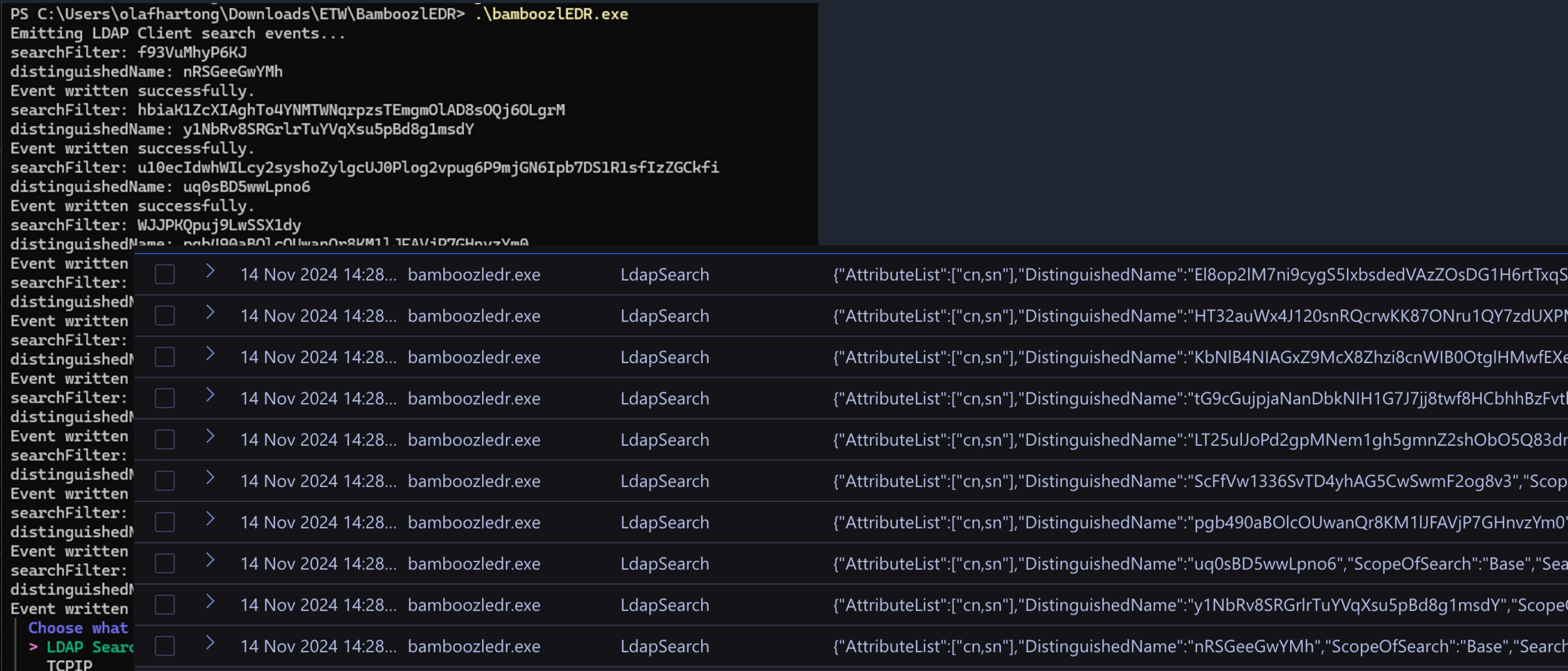
```
PS C:\Users\olafhartong\Downloads\ETW\BamboozlEDR> .\bamboozlEDR.exe
Emitting LDAP Client search event...
scopeOfSearch: 0
```

```
DeviceEvents
| where DeviceName contains "beefcake"
| where ActionType in~ ("LdapSearch")
| sort by Timestamp desc
| project-reorder Timestamp, InitiatingProcessFileName, ActionType, AdditionalFields
```

4 items ⏱ 00:00.130

Timestamp	InitiatingProcessFileName	ActionType	AdditionalFields
14 Nov 2024 14:12:52	canary.exe	LdapSearch	{"AttributeList":["cn,sn"],"DistinguishedName":"DC=MakingSure,DC=ItWorks","ScopeOfSearch":"Base","Sear
14 Nov 2024 14:12:41	bamboozledr.exe	LdapSearch	{"AttributeList":["cn,sn"],"DistinguishedName":"DC=MakingSure,DC=ItWorks","ScopeOfSearch":"Base","Sear

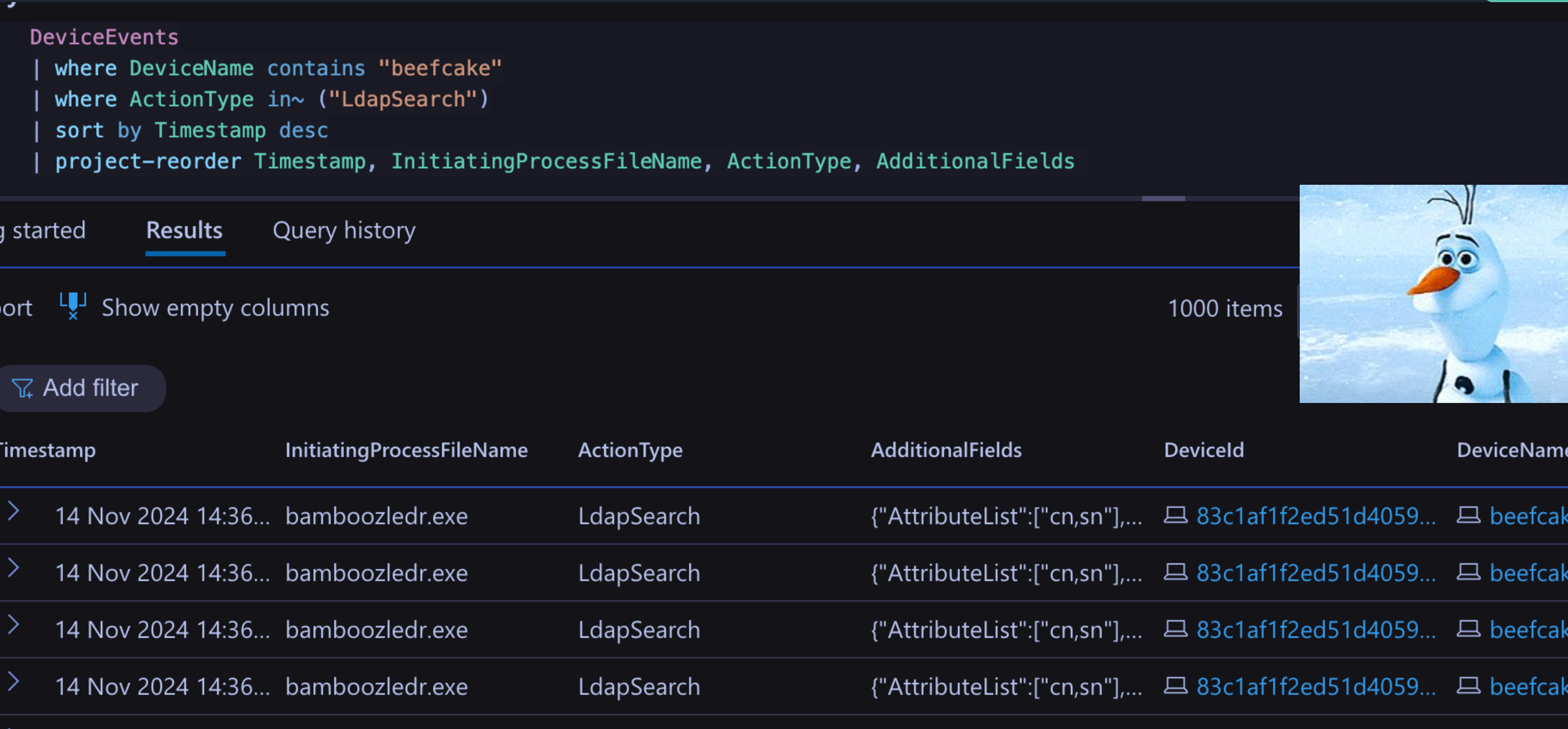
GENERATING 10 UNIQUE (GARBAGE) EVENTS



```
PS C:\Users\olafhartong\Downloads\ETW\BamboozlEDR> .\bamboozlEDR.exe
Emitting LDAP Client search events...
searchFilter: f93VuMhyP6KJ
distinguishedName: nRSGeeGwYMh
Event written successfully.
searchFilter: hbiaK1ZcXIAghTo4YNMTWNqrpzsTEmgmOlAD8sOQj6OLgrM
distinguishedName: y1NbRv8SRGrlrTuYVqXsu5pBd8g1msdY
Event written successfully.
searchFilter: u10ecIdwhWILcy2syshoZylgcUJ0Plog2vpug6P9mjGN6Ipb7DS1R1sfIzZGCkfi
distinguishedName: uq0sBD5wwLpno6
Event written successfully.
searchFilter: WJJPKQpuj9LwSSX1dy
distinguishedName: pgb490aBOlcOUwanQr8KM1lJFAVjP7GHnvzYm0
Event written
searchFilter:
distinguishedN
Event written
searchFilter:
distinguishedN
Event written
searchFilter:
distinguishedN
Event written
searchFilter:
distinguishedN
Event written
searchFilter:
distinguishedN
Event written
searchFilter:
distinguishedN
Event written
 Choose what
 > LDAP Searc
   TCPIP
```

☐	›	14 Nov 2024 14:28...	bamboozledr.exe	LdapSearch	{"AttributeList":["cn,sn"],"DistinguishedName":"El8op2lM7ni9cygS5IxbsdedVAzZOsDG1H6rtTxqS
☐	›	14 Nov 2024 14:28...	bamboozledr.exe	LdapSearch	{"AttributeList":["cn,sn"],"DistinguishedName":"HT32auWx4J120snRQcrwKK87ONru1QY7zdUXPN
☐	›	14 Nov 2024 14:28...	bamboozledr.exe	LdapSearch	{"AttributeList":["cn,sn"],"DistinguishedName":"KbNlB4NIAGxZ9McX8Zhzi8cnWIB0OtglHMwfEXe
☐	›	14 Nov 2024 14:28...	bamboozledr.exe	LdapSearch	{"AttributeList":["cn,sn"],"DistinguishedName":"tG9cGujpjaNanDbkNIH1G7J7jj8twf8HCbhhBzFvt
☐	›	14 Nov 2024 14:28...	bamboozledr.exe	LdapSearch	{"AttributeList":["cn,sn"],"DistinguishedName":"LT25ulJoPd2gpMNem1gh5gmnZ2shObO5Q83dr
☐	›	14 Nov 2024 14:28...	bamboozledr.exe	LdapSearch	{"AttributeList":["cn,sn"],"DistinguishedName":"ScFfVw1336SvTD4yhAG5CwSwmF2og8v3","Scop
☐	›	14 Nov 2024 14:28...	bamboozledr.exe	LdapSearch	{"AttributeList":["cn,sn"],"DistinguishedName":"pgb490aBOlcOUwanQr8KM1lJFAVjP7GHnvzYm0"
☐	›	14 Nov 2024 14:28...	bamboozledr.exe	LdapSearch	{"AttributeList":["cn,sn"],"DistinguishedName":"uq0sBD5wwLpno6","ScopeOfSearch":"Base","Sea
☐	›	14 Nov 2024 14:28...	bamboozledr.exe	LdapSearch	{"AttributeList":["cn,sn"],"DistinguishedName":"y1NbRv8SRGrlrTuYVqXsu5pBd8g1msdY","Scope
☐	›	14 Nov 2024 14:28...	bamboozledr.exe	LdapSearch	{"AttributeList":["cn,sn"],"DistinguishedName":"nRSGeeGwYMh","ScopeOfSearch":"Base","Search

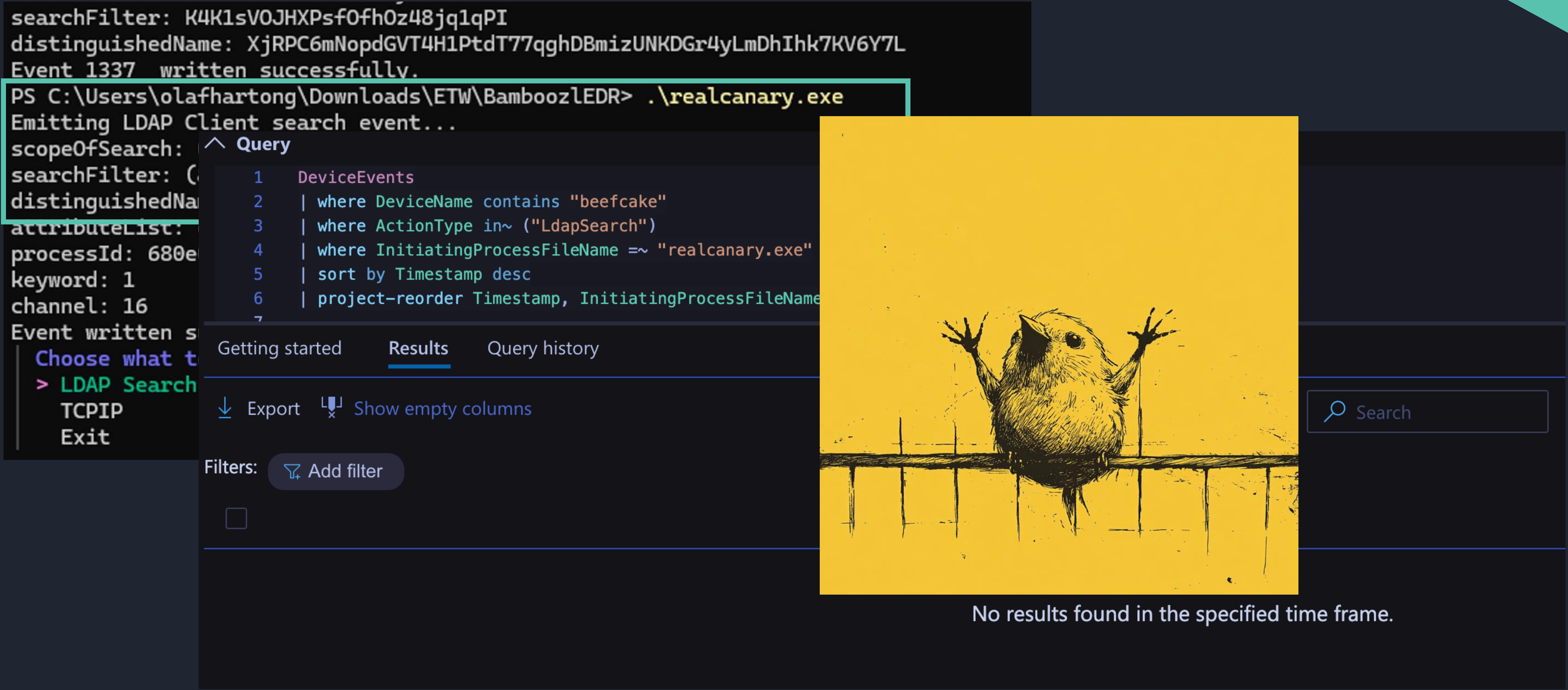
GENERATING > GLOBAL CAP



```
DeviceEvents
| where DeviceName contains "beefcake"
| where ActionType in~ ("LdapSearch")
| sort by Timestamp desc
| project-reorder Timestamp, InitiatingProcessFileName, ActionType, AdditionalFields
```

imestamp	InitiatingProcessFileName	ActionType	AdditionalFields	DeviceId	DeviceNam
14 Nov 2024 14:36...	bamboozledr.exe	LdapSearch	{"AttributeList":["cn,sn"],...	83c1af1f2ed51d4059...	beefcak
14 Nov 2024 14:36...	bamboozledr.exe	LdapSearch	{"AttributeList":["cn,sn"],...	83c1af1f2ed51d4059...	beefcak
14 Nov 2024 14:36...	bamboozledr.exe	LdapSearch	{"AttributeList":["cn,sn"],...	83c1af1f2ed51d4059...	beefcak
14 Nov 2024 14:36...	bamboozledr.exe	LdapSearch	{"AttributeList":["cn,sn"],...	83c1af1f2ed51d4059...	beefcak

NEXT, I SENT IN THE CANARY



```
searchFilter: K4K1sVOJHXPsfOfhOz48jq1qPI
distinguishedName: XjRPC6mNopdGVT4H1PtdT77qghDBmizUNKDGr4yLmDhIhk7KV6Y7L
Event 1337  written successfully.
PS C:\Users\olafhartong\Downloads\ETW\BamboozlEDR> .\realcanary.exe
Emitting LDAP Client search event...
scopeOfSearch:
searchFilter: (
distinguishedNa
attributeList:
processId: 680e
keyword: 1
channel: 16
Event written s
  Choose what t
  > LDAP Search
    TCPIP
    Exit
```

Query

```
DeviceEvents
| where DeviceName contains "beefcake"
| where ActionType in~ ("LdapSearch")
| where InitiatingProcessFileName =~ "realcanary.exe"
| sort by Timestamp desc
| project-reorder Timestamp, InitiatingProcessFileName
```

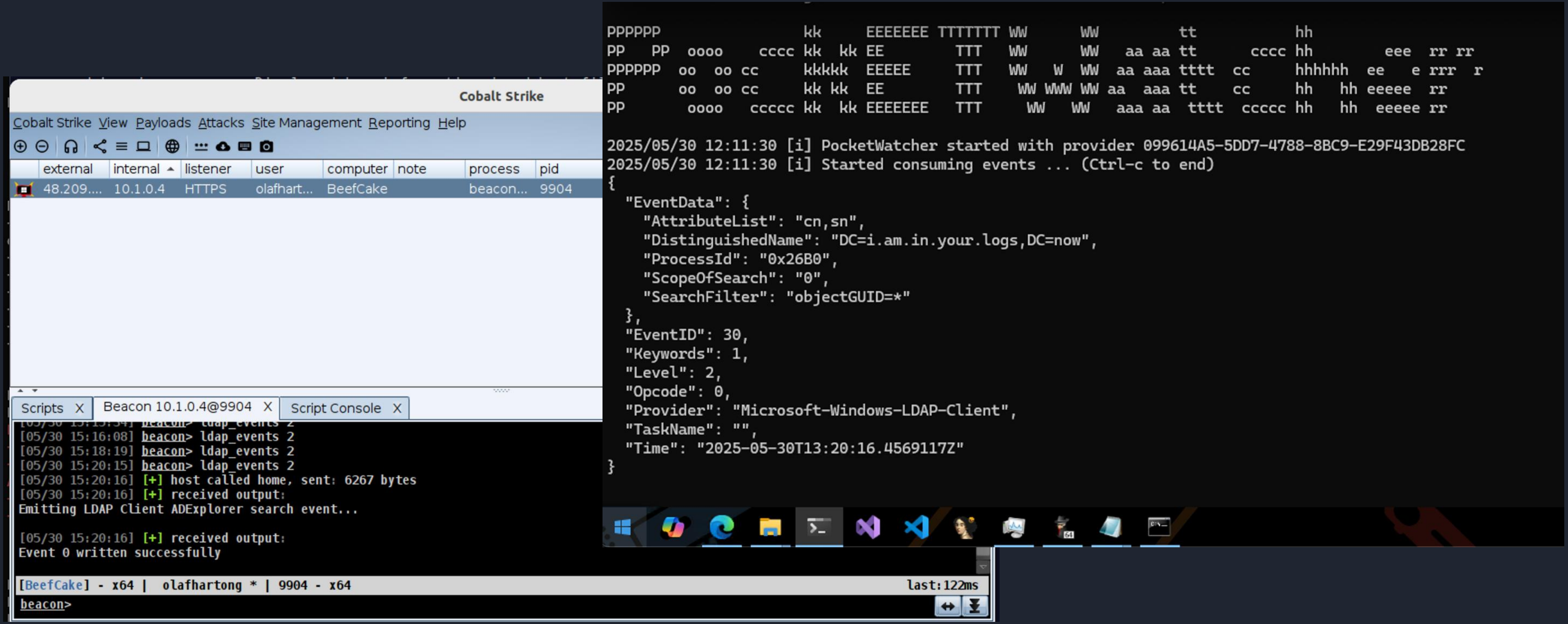
No results found in the specified time frame.

ABUSE POSSIBILITY

- □ Force MDE into global capping per event type
- □ Run our real attack, from any process on the box
- □ No telemetry, no detection…..

The EDR component relies on the same telemetry for its detection capability

BEACON OBJECT FILE (BOF)

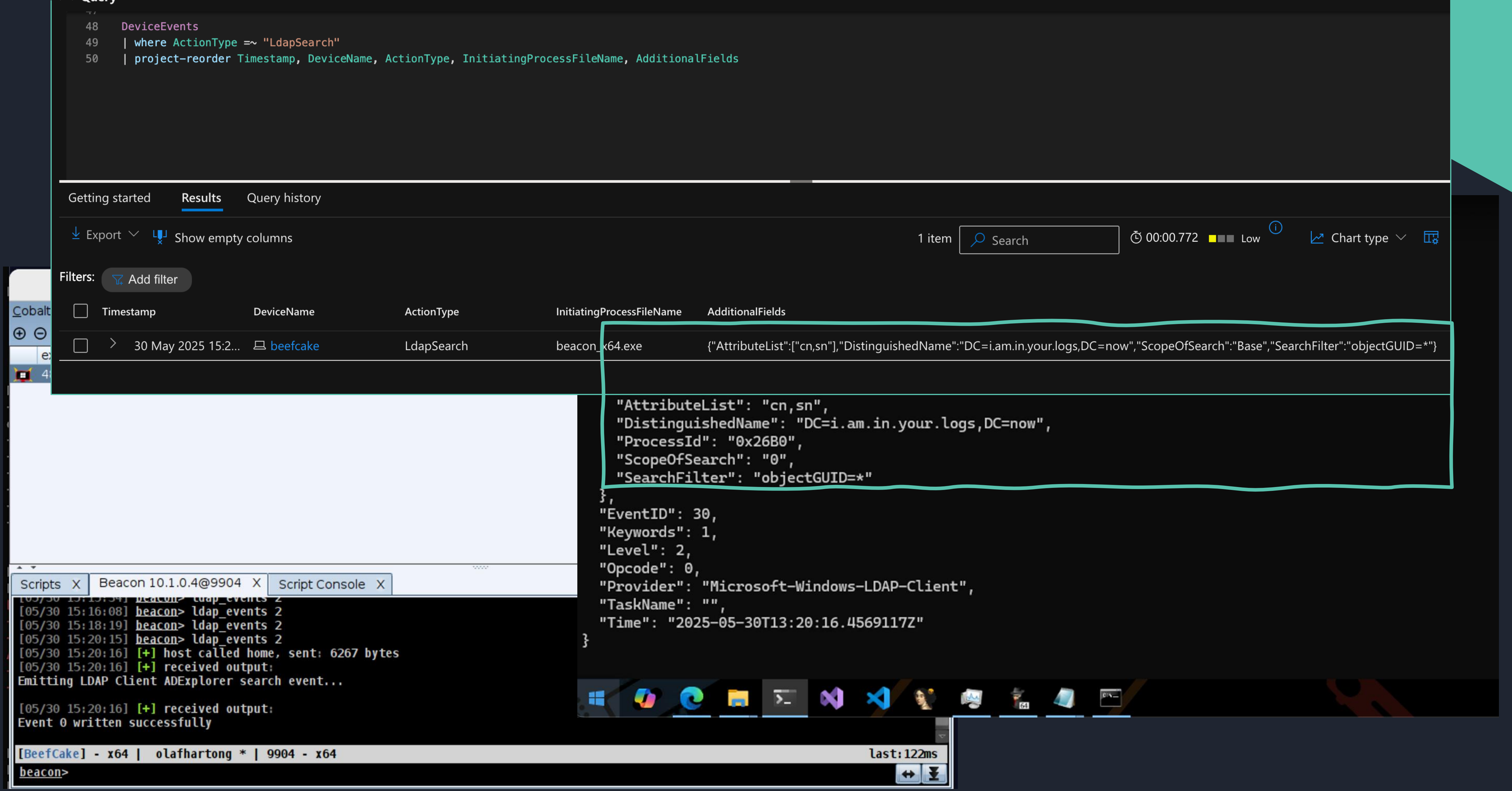


Cobalt Strike
Cobalt Strike View Payloads Attacks Site Management Reporting Help
Scripts X
Beacon 10.1.0.4@9904 X
Script Console X

external	internal	listener	user	computer	note	process	pid
48.209....	10.1.0.4	HTTPS	olafhart...	BeefCake		beacon...	9904

```
[05/30 15:16:08] beacon> ldap_events 2
[05/30 15:18:19] beacon> ldap_events 2
[05/30 15:20:15] beacon> ldap_events 2
[05/30 15:20:16] [+] host called home, sent: 6267 bytes
[05/30 15:20:16] [+] received output:
Emitting LDAP Client ADExplorer search event...

[05/30 15:20:16] [+] received output:
Event 0 written successfully

[BeefCake] - x64 |  olafhartong * | 9904 - x64                last:122ms
beacon>
```

```
PPPPPP               kk      EEEEEEE TTTTTTT WW       WW         tt           hh
PP   PP  oooo    cccc kk   kk EE        TTT   WW       WW   aa aa tt      cccc hh         eee  rr rr
PPPPPP  oo  oo cc     kkkkk  EEEEE     TTT   WW   W  WW  aa aaa tttt  cc     hhhhhh  ee   e rrr  r
PP      oo  oo cc     kk kk  EE        TTT    WW WWW WW aa   aaa tt    cc     hh   hh eeeee  rr
PP       oooo   ccccc kk   kk EEEEEEE   TTT     WW   WW   aaa aa  tttt  ccccc hh   hh  eeeee rr

2025/05/30 12:11:30 [i] PocketWatcher started with provider 099614A5-5DD7-4788-8BC9-E29F43DB28FC
2025/05/30 12:11:30 [i] Started consuming events ... (Ctrl-c to end)
{
  "EventData": {
    "AttributeList": "cn,sn",
    "DistinguishedName": "DC=i.am.in.your.logs,DC=now",
    "ProcessId": "0x26B0",
    "ScopeOfSearch": "0",
    "SearchFilter": "objectGUID=*"
  },
  "EventID": 30,
  "Keywords": 1,
  "Level": 2,
  "Opcode": 0,
  "Provider": "Microsoft-Windows-LDAP-Client",
  "TaskName": "",
  "Time": "2025-05-30T13:20:16.4569117Z"
}
```



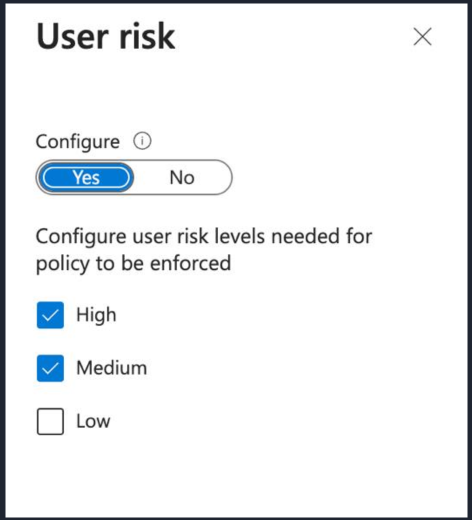
```
DeviceEvents
| where ActionType =~ "LdapSearch"
| project-reorder Timestamp, DeviceName, ActionType, InitiatingProcessFileName, AdditionalFields
```

Timestamp	DeviceName	ActionType	InitiatingProcessFileName	AdditionalFields
30 May 2025 15:2...	beefcake	LdapSearch	beacon_x64.exe	{"AttributeList":["cn,sn"],"DistinguishedName":"DC=i.am.in.your.logs,DC=now","ScopeOfSearch":"Base","SearchFilter":"objectGUID=*"}

```
    "AttributeList": "cn,sn",
    "DistinguishedName": "DC=i.am.in.your.logs,DC=now",
    "ProcessId": "0x26B0",
    "ScopeOfSearch": "0",
    "SearchFilter": "objectGUID=*"
  },
  "EventID": 30,
  "Keywords": 1,
  "Level": 2,
  "Opcode": 0,
  "Provider": "Microsoft-Windows-LDAP-Client",
  "TaskName": "",
  "Time": "2025-05-30T13:20:16.4569117Z"
}
```

```
[05/30 15:16:08] beacon> ldap_events 2
[05/30 15:18:19] beacon> ldap_events 2
[05/30 15:20:15] beacon> ldap_events 2
[05/30 15:20:16] [+] host called home, sent: 6267 bytes
[05/30 15:20:16] [+] received output:
Emitting LDAP Client ADExplorer search event...

[05/30 15:20:16] [+] received output:
Event 0 written successfully

[BeefCake] - x64 |  olafhartong * | 9904 - x64                    last:122ms
beacon>
```

BLOCKING ACCESS TO THE CLOUD



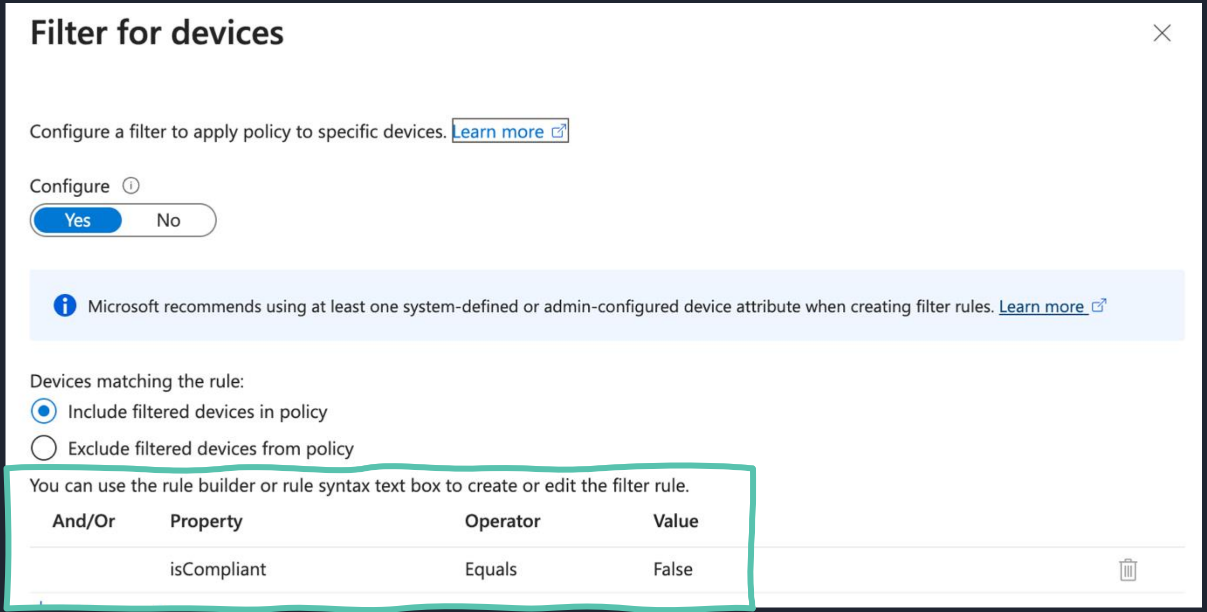
User risk

Configure

[✓ Yes] No

Configure user risk levels needed for policy to be enforced

- ☑ High
- ☑ Medium
- □ Low



Filter for devices

Configure a filter to apply policy to specific devices. Learn more

Configure

[✓ Yes] No

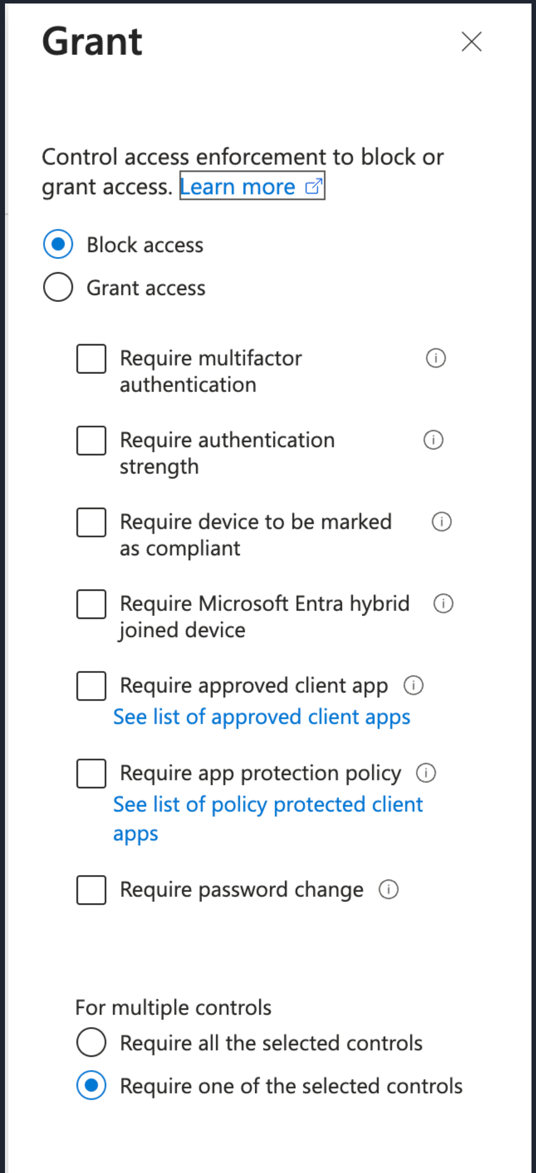
Microsoft recommends using at least one system-defined or admin-configured device attribute when creating filter rules. Learn more

Devices matching the rule:

- ● Include filtered devices in policy
- ○ Exclude filtered devices from policy

You can use the rule builder or rule syntax text box to create or edit the filter rule.

And/Or	Property	Operator	Value
	isCompliant	Equals	False



Grant

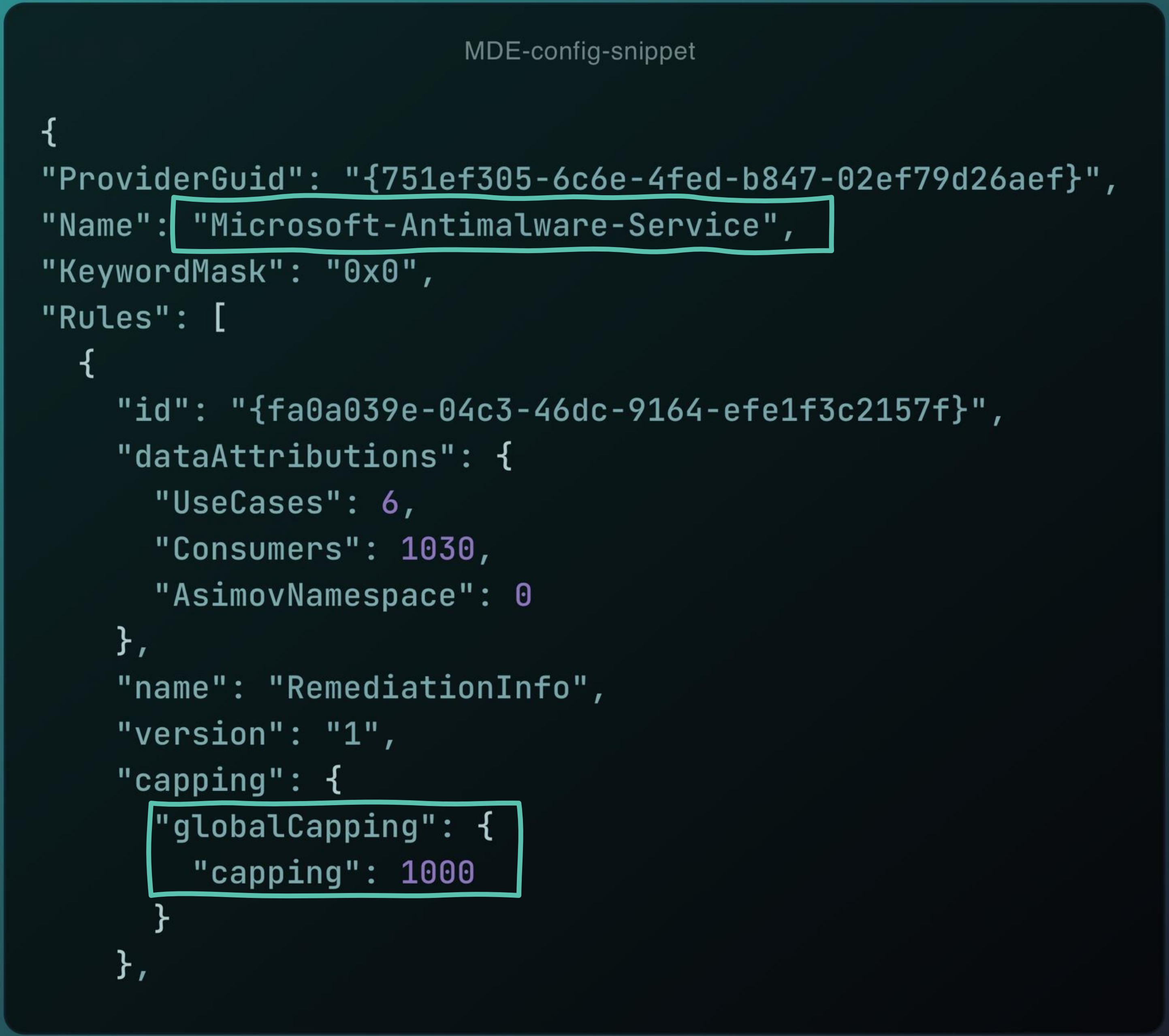
Control access enforcement to block or grant access. Learn more

- ● Block access
- ○ Grant access

- □ Require multifactor authentication
- □ Require authentication strength
- □ Require device to be marked as compliant
- □ Require Microsoft Entra hybrid joined device
- □ Require approved client app
  See list of approved client apps
- □ Require app protection policy
  See list of policy protected client apps
- □ Require password change

For multiple controls

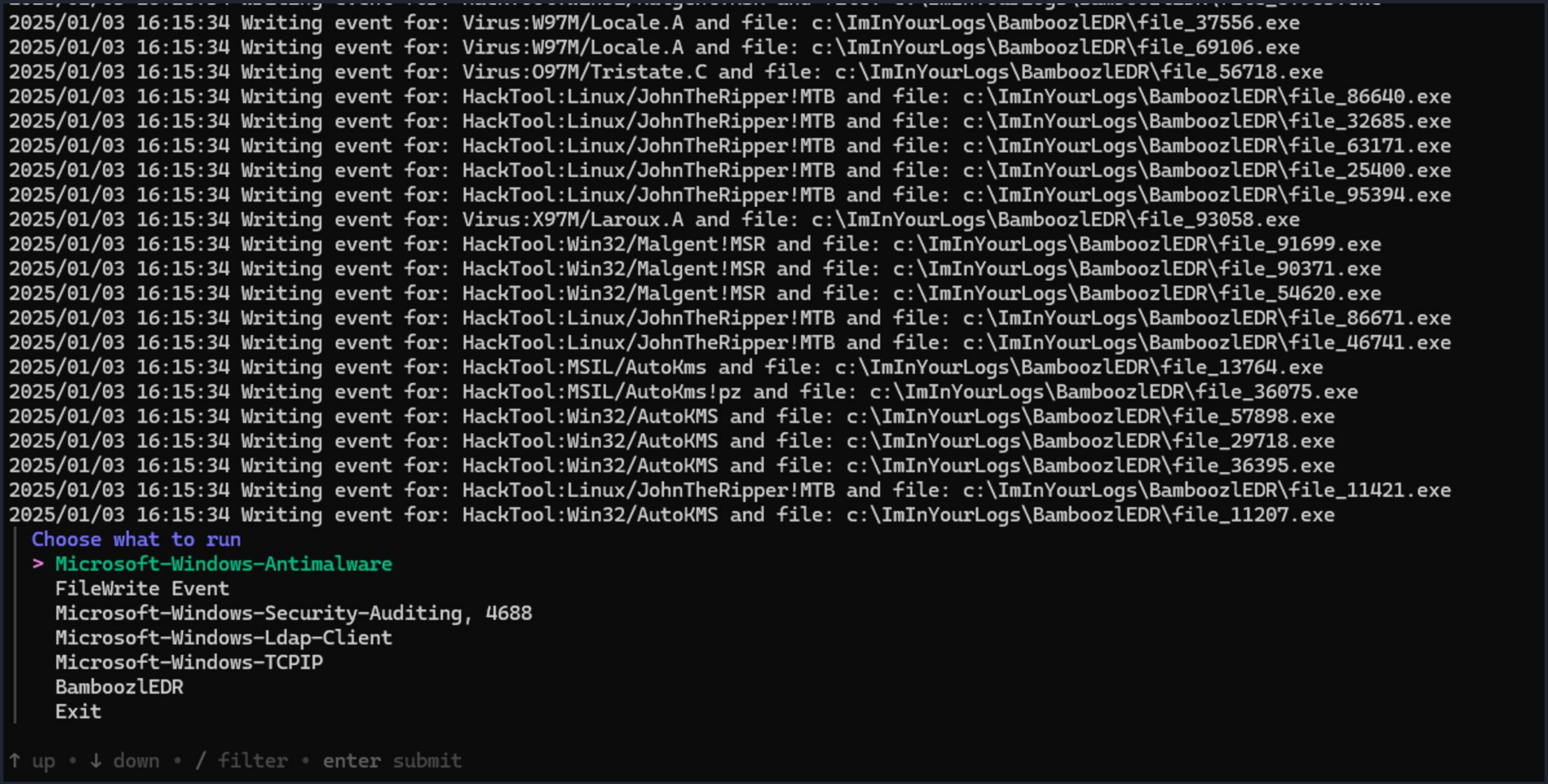
- ○ Require all the selected controls
- ● Require one of the selected controls



MDE-config-snippet

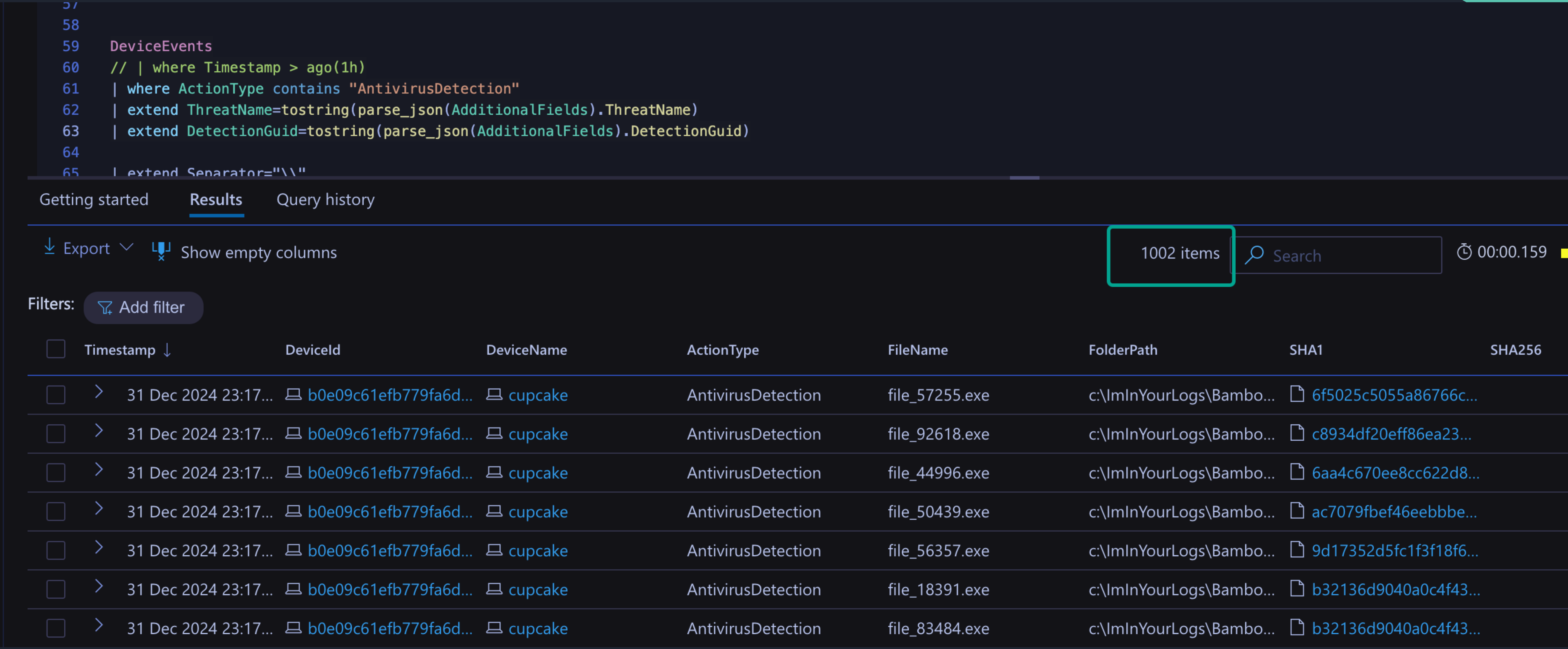
```
{
"ProviderGuid": "{751ef305-6c6e-4fed-b847-02ef79d26aef}",
"Name": "Microsoft-Antimalware-Service",
"KeywordMask": "0x0",
"Rules": [
  {
    "id": "{fa0a039e-04c3-46dc-9164-efe1f3c2157f}",
    "dataAttributions": {
      "UseCases": 6,
      "Consumers": 1030,
      "AsimovNamespace": 0
    },
    "name": "RemediationInfo",
    "version": "1",
    "capping": {
      "globalCapping": {
        "capping": 1000
      }
    },
```

EMITTED 1337 AV EVENTS



```
2025/01/03 16:15:34 Writing event for: Virus:W97M/Locale.A and file: c:\ImInYourLogs\BamboozlEDR\file_37556.exe
2025/01/03 16:15:34 Writing event for: Virus:W97M/Locale.A and file: c:\ImInYourLogs\BamboozlEDR\file_69106.exe
2025/01/03 16:15:34 Writing event for: Virus:O97M/Tristate.C and file: c:\ImInYourLogs\BamboozlEDR\file_56718.exe
2025/01/03 16:15:34 Writing event for: HackTool:Linux/JohnTheRipper!MTB and file: c:\ImInYourLogs\BamboozlEDR\file_86640.exe
2025/01/03 16:15:34 Writing event for: HackTool:Linux/JohnTheRipper!MTB and file: c:\ImInYourLogs\BamboozlEDR\file_32685.exe
2025/01/03 16:15:34 Writing event for: HackTool:Linux/JohnTheRipper!MTB and file: c:\ImInYourLogs\BamboozlEDR\file_63171.exe
2025/01/03 16:15:34 Writing event for: HackTool:Linux/JohnTheRipper!MTB and file: c:\ImInYourLogs\BamboozlEDR\file_25400.exe
2025/01/03 16:15:34 Writing event for: HackTool:Linux/JohnTheRipper!MTB and file: c:\ImInYourLogs\BamboozlEDR\file_95394.exe
2025/01/03 16:15:34 Writing event for: Virus:X97M/Laroux.A and file: c:\ImInYourLogs\BamboozlEDR\file_93058.exe
2025/01/03 16:15:34 Writing event for: HackTool:Win32/Malgent!MSR and file: c:\ImInYourLogs\BamboozlEDR\file_91699.exe
2025/01/03 16:15:34 Writing event for: HackTool:Win32/Malgent!MSR and file: c:\ImInYourLogs\BamboozlEDR\file_90371.exe
2025/01/03 16:15:34 Writing event for: HackTool:Win32/Malgent!MSR and file: c:\ImInYourLogs\BamboozlEDR\file_54620.exe
2025/01/03 16:15:34 Writing event for: HackTool:Linux/JohnTheRipper!MTB and file: c:\ImInYourLogs\BamboozlEDR\file_86671.exe
2025/01/03 16:15:34 Writing event for: HackTool:Linux/JohnTheRipper!MTB and file: c:\ImInYourLogs\BamboozlEDR\file_46741.exe
2025/01/03 16:15:34 Writing event for: HackTool:MSIL/AutoKms and file: c:\ImInYourLogs\BamboozlEDR\file_13764.exe
2025/01/03 16:15:34 Writing event for: HackTool:MSIL/AutoKms!pz and file: c:\ImInYourLogs\BamboozlEDR\file_36075.exe
2025/01/03 16:15:34 Writing event for: HackTool:Win32/AutoKMS and file: c:\ImInYourLogs\BamboozlEDR\file_57898.exe
2025/01/03 16:15:34 Writing event for: HackTool:Win32/AutoKMS and file: c:\ImInYourLogs\BamboozlEDR\file_29718.exe
2025/01/03 16:15:34 Writing event for: HackTool:Win32/AutoKMS and file: c:\ImInYourLogs\BamboozlEDR\file_36395.exe
2025/01/03 16:15:34 Writing event for: HackTool:Linux/JohnTheRipper!MTB and file: c:\ImInYourLogs\BamboozlEDR\file_11421.exe
2025/01/03 16:15:34 Writing event for: HackTool:Win32/AutoKMS and file: c:\ImInYourLogs\BamboozlEDR\file_11207.exe
 │ Choose what to run
 │ > Microsoft-Windows-Antimalware
 │   FileWrite Event
 │   Microsoft-Windows-Security-Auditing, 4688
 │   Microsoft-Windows-Ldap-Client
 │   Microsoft-Windows-TCPIP
 │   BamboozlEDR
 │   Exit

↑ up • ↓ down • / filter • enter submit
```

ONLY 1K ARE LOGGED



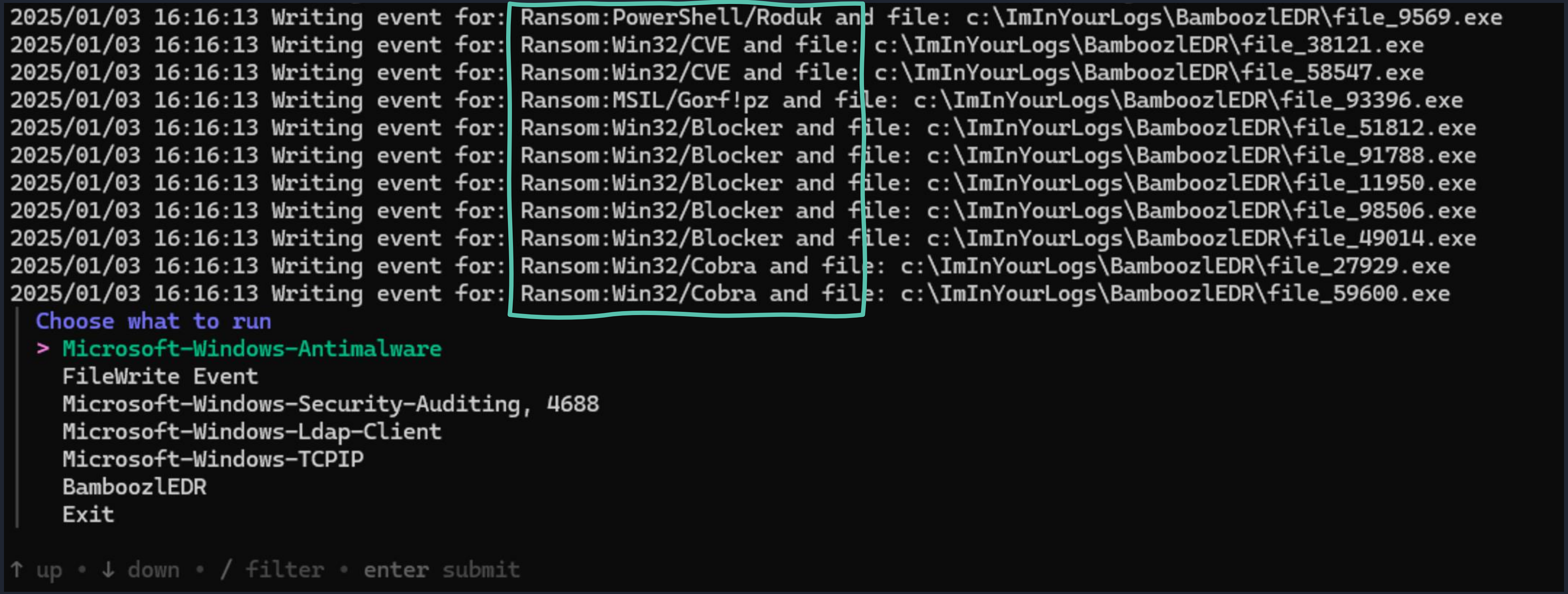
```
DeviceEvents
// | where Timestamp > ago(1h)
| where ActionType contains "AntivirusDetection"
| extend ThreatName=tostring(parse_json(AdditionalFields).ThreatName)
| extend DetectionGuid=tostring(parse_json(AdditionalFields).DetectionGuid)

| extend Separator="\\"
```

1002 items

00:00.159

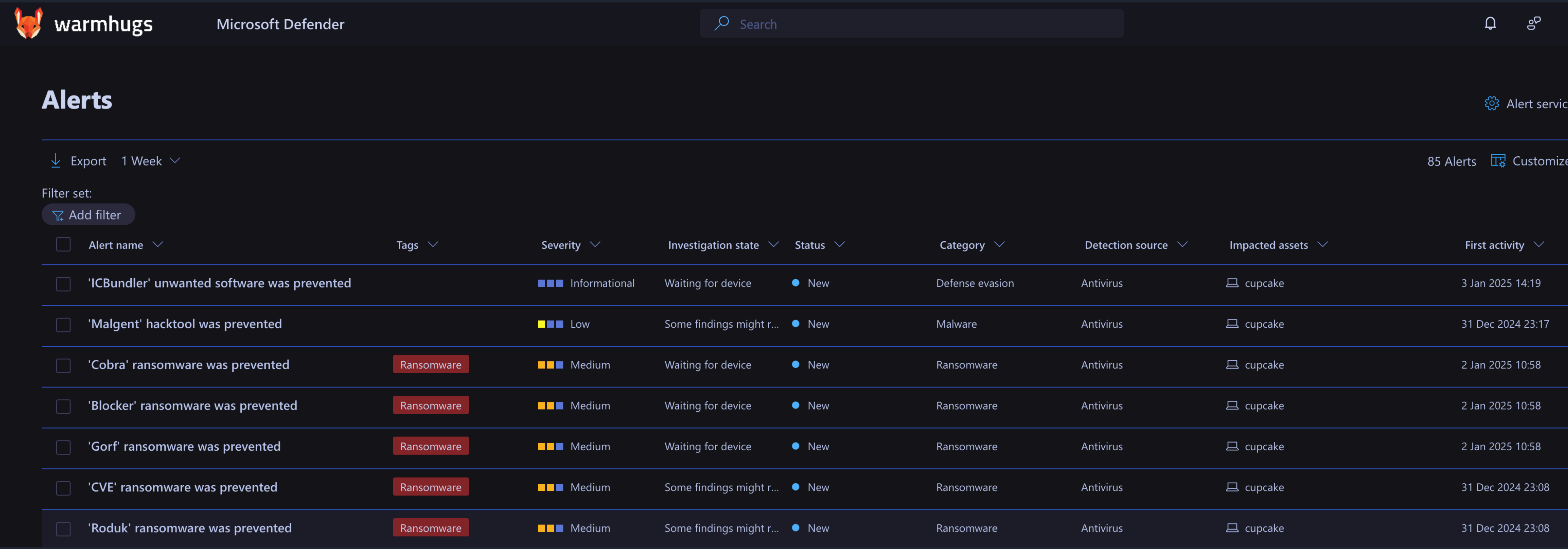
	Timestamp ↓	DeviceId	DeviceName	ActionType	FileName	FolderPath	SHA1	SHA256
□	31 Dec 2024 23:17...	b0e09c61efb779fa6d...	cupcake	AntivirusDetection	file_57255.exe	c:\ImInYourLogs\Bambo...	6f5025c5055a86766c...	
□	31 Dec 2024 23:17...	b0e09c61efb779fa6d...	cupcake	AntivirusDetection	file_92618.exe	c:\ImInYourLogs\Bambo...	c8934df20eff86ea23...	
□	31 Dec 2024 23:17...	b0e09c61efb779fa6d...	cupcake	AntivirusDetection	file_44996.exe	c:\ImInYourLogs\Bambo...	6aa4c670ee8cc622d8...	
□	31 Dec 2024 23:17...	b0e09c61efb779fa6d...	cupcake	AntivirusDetection	file_50439.exe	c:\ImInYourLogs\Bambo...	ac7079fbef46eebbbe...	
□	31 Dec 2024 23:17...	b0e09c61efb779fa6d...	cupcake	AntivirusDetection	file_56357.exe	c:\ImInYourLogs\Bambo...	9d17352d5fc1f3f18f6...	
□	31 Dec 2024 23:17...	b0e09c61efb779fa6d...	cupcake	AntivirusDetection	file_18391.exe	c:\ImInYourLogs\Bambo...	b32136d9040a0c4f43...	
□	31 Dec 2024 23:17...	b0e09c61efb779fa6d...	cupcake	AntivirusDetection	file_83484.exe	c:\ImInYourLogs\Bambo...	b32136d9040a0c4f43...	

NOW I'M A RANSOMWARE OPERATOR



```
2025/01/03 16:16:13 Writing event for: Ransom:PowerShell/Roduk and file: c:\ImInYourLogs\BamboozlEDR\file_9569.exe
2025/01/03 16:16:13 Writing event for: Ransom:Win32/CVE and file: c:\ImInYourLogs\BamboozlEDR\file_38121.exe
2025/01/03 16:16:13 Writing event for: Ransom:Win32/CVE and file: c:\ImInYourLogs\BamboozlEDR\file_58547.exe
2025/01/03 16:16:13 Writing event for: Ransom:MSIL/Gorf!pz and file: c:\ImInYourLogs\BamboozlEDR\file_93396.exe
2025/01/03 16:16:13 Writing event for: Ransom:Win32/Blocker and file: c:\ImInYourLogs\BamboozlEDR\file_51812.exe
2025/01/03 16:16:13 Writing event for: Ransom:Win32/Blocker and file: c:\ImInYourLogs\BamboozlEDR\file_91788.exe
2025/01/03 16:16:13 Writing event for: Ransom:Win32/Blocker and file: c:\ImInYourLogs\BamboozlEDR\file_11950.exe
2025/01/03 16:16:13 Writing event for: Ransom:Win32/Blocker and file: c:\ImInYourLogs\BamboozlEDR\file_98506.exe
2025/01/03 16:16:13 Writing event for: Ransom:Win32/Blocker and file: c:\ImInYourLogs\BamboozlEDR\file_49014.exe
2025/01/03 16:16:13 Writing event for: Ransom:Win32/Cobra and file: c:\ImInYourLogs\BamboozlEDR\file_27929.exe
2025/01/03 16:16:13 Writing event for: Ransom:Win32/Cobra and file: c:\ImInYourLogs\BamboozlEDR\file_59600.exe
 │ Choose what to run
 │ > Microsoft-Windows-Antimalware
 │   FileWrite Event
 │   Microsoft-Windows-Security-Auditing, 4688
 │   Microsoft-Windows-Ldap-Client
 │   Microsoft-Windows-TCPIP
 │   BamboozlEDR
 │   Exit

↑ up • ↓ down • / filter • enter submit
```

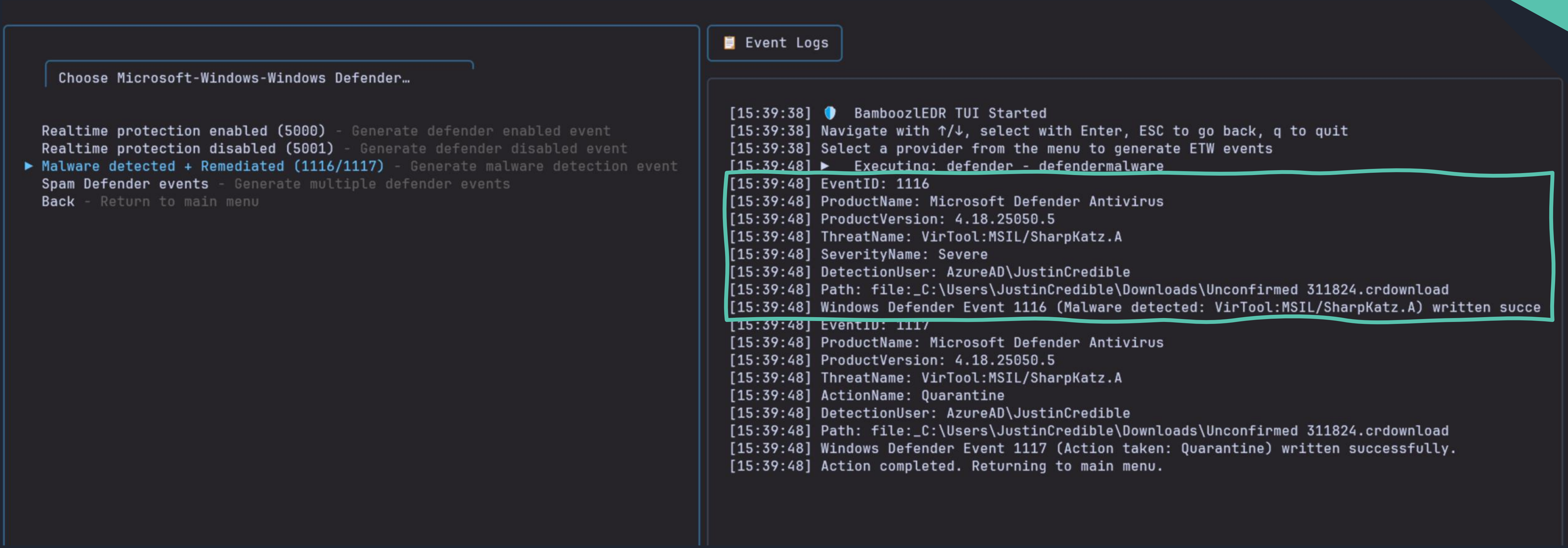
MANY ALERTS IN THE CLOUD



Alerts

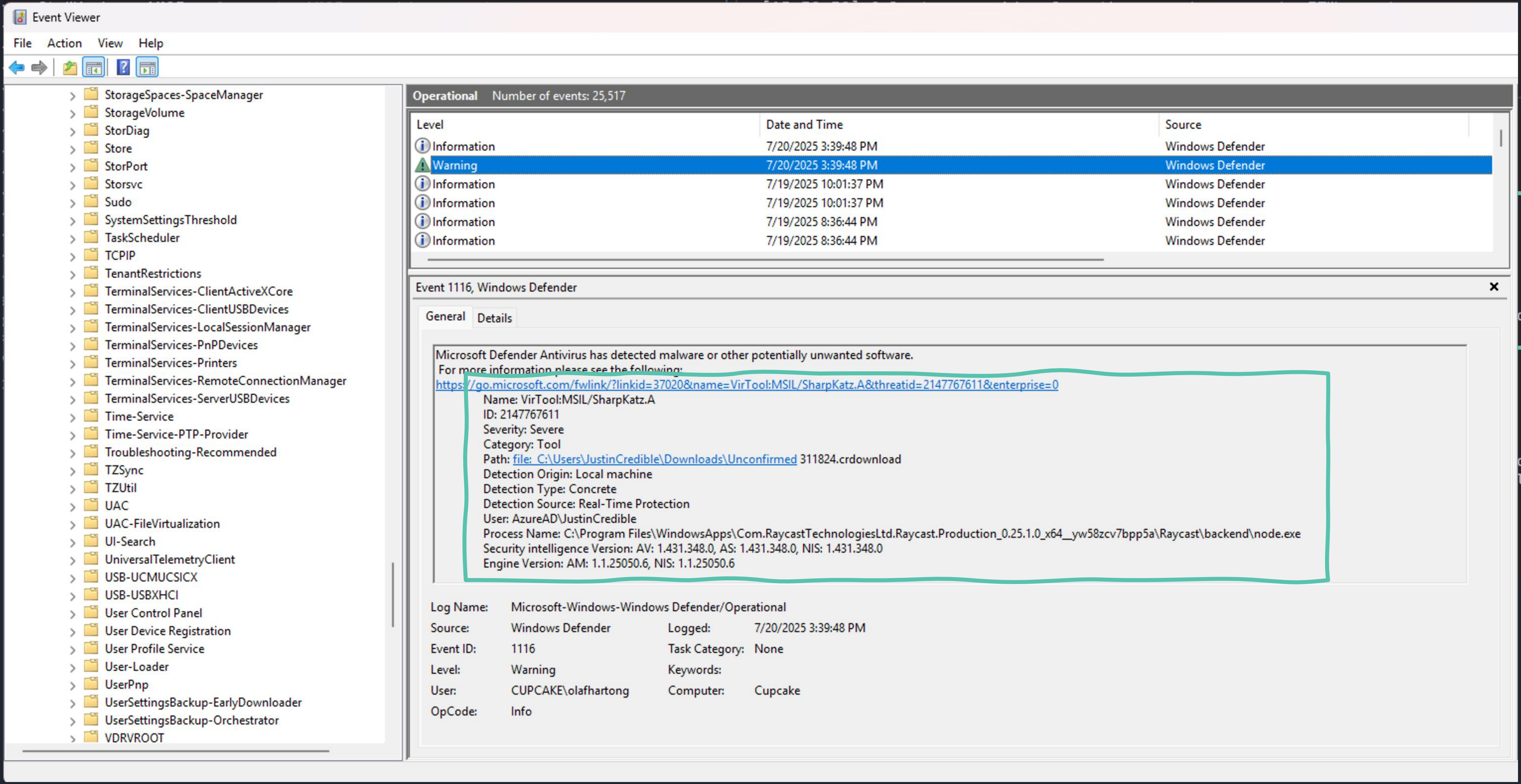
	Alert name	Tags	Severity	Investigation state	Status	Category	Detection source	Impacted assets	First activity
□	'ICBundler' unwanted software was prevented		Informational	Waiting for device	● New	Defense evasion	Antivirus	cupcake	3 Jan 2025 14:19
□	'Malgent' hacktool was prevented		Low	Some findings might r...	● New	Malware	Antivirus	cupcake	31 Dec 2024 23:17
□	'Cobra' ransomware was prevented	Ransomware	Medium	Waiting for device	● New	Ransomware	Antivirus	cupcake	2 Jan 2025 10:58
□	'Blocker' ransomware was prevented	Ransomware	Medium	Waiting for device	● New	Ransomware	Antivirus	cupcake	2 Jan 2025 10:58
□	'Gorf' ransomware was prevented	Ransomware	Medium	Waiting for device	● New	Ransomware	Antivirus	cupcake	2 Jan 2025 10:58
□	'CVE' ransomware was prevented	Ransomware	Medium	Some findings might r...	● New	Ransomware	Antivirus	cupcake	31 Dec 2024 23:08
□	'Roduk' ransomware was prevented	Ransomware	Medium	Some findings might r...	● New	Ransomware	Antivirus	cupcake	31 Dec 2024 23:08

AV ALERT EXAMPLE


Choose Microsoft-Windows-Windows Defender…
Realtime protection enabled (5000) - Generate defender enabled event
Realtime protection disabled (5001) - Generate defender disabled event
▶ Malware detected + Remediated (1116/1117) - Generate malware detection event
Spam Defender events - Generate multiple defender events
Back - Return to main menu
📋 Event Logs

```
[15:39:38] 🛡  BamboozlEDR TUI Started
[15:39:38] Navigate with ↑/↓, select with Enter, ESC to go back, q to quit
[15:39:38] Select a provider from the menu to generate ETW events
[15:39:48] ▶  Executing: defender - defendermalware
[15:39:48] EventID: 1116
[15:39:48] ProductName: Microsoft Defender Antivirus
[15:39:48] ProductVersion: 4.18.25050.5
[15:39:48] ThreatName: VirTool:MSIL/SharpKatz.A
[15:39:48] SeverityName: Severe
[15:39:48] DetectionUser: AzureAD\JustinCredible
[15:39:48] Path: file:_C:\Users\JustinCredible\Downloads\Unconfirmed 311824.crdownload
[15:39:48] Windows Defender Event 1116 (Malware detected: VirTool:MSIL/SharpKatz.A) written succe
[15:39:48] EventID: 1117
[15:39:48] ProductName: Microsoft Defender Antivirus
[15:39:48] ProductVersion: 4.18.25050.5
[15:39:48] ThreatName: VirTool:MSIL/SharpKatz.A
[15:39:48] ActionName: Quarantine
[15:39:48] DetectionUser: AzureAD\JustinCredible
[15:39:48] Path: file:_C:\Users\JustinCredible\Downloads\Unconfirmed 311824.crdownload
[15:39:48] Windows Defender Event 1117 (Action taken: Quarantine) written successfully.
[15:39:48] Action completed. Returning to main menu.
```

EVENT LOG EXAMPLE


Event Viewer
File
Action
View
Help
StorageSpaces-SpaceManager
StorageVolume
StorDiag
Store
StorPort
Storsvc
Sudo
SystemSettingsThreshold
TaskScheduler
TCPIP
TenantRestrictions
TerminalServices-ClientActiveXCore
TerminalServices-ClientUSBDevices
TerminalServices-LocalSessionManager
TerminalServices-PnPDevices
TerminalServices-Printers
TerminalServices-RemoteConnectionManager
TerminalServices-ServerUSBDevices
Time-Service
Time-Service-PTP-Provider
Troubleshooting-Recommended
TZSync
TZUtil
UAC
UAC-FileVirtualization
UI-Search
UniversalTelemetryClient
USB-UCMUCSICX
USB-USBXHCI
User Control Panel
User Device Registration
User Profile Service
User-Loader
UserPnp
UserSettingsBackup-EarlyDownloader
UserSettingsBackup-Orchestrator
VDRVROOT
General
Details

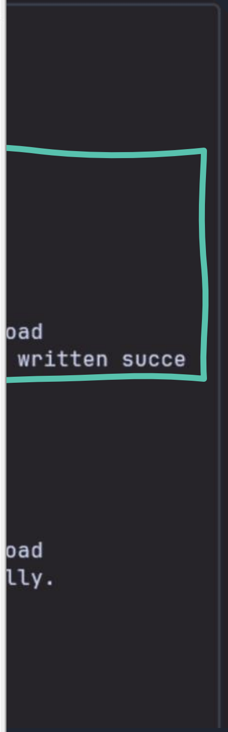
Operational Number of events: 25,517

Level	Date and Time	Source
Information	7/20/2025 3:39:48 PM	Windows Defender
Warning	7/20/2025 3:39:48 PM	Windows Defender
Information	7/19/2025 10:01:37 PM	Windows Defender
Information	7/19/2025 10:01:37 PM	Windows Defender
Information	7/19/2025 8:36:44 PM	Windows Defender
Information	7/19/2025 8:36:44 PM	Windows Defender

Event 1116, Windows Defender

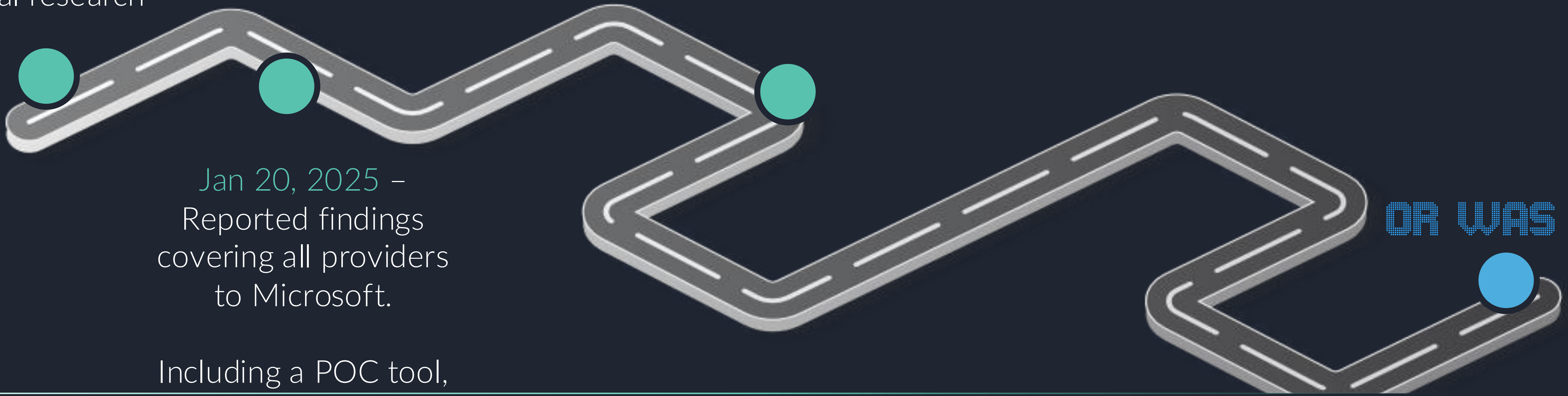
```
Microsoft Defender Antivirus has detected malware or other potentially unwanted software.
 For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=VirTool:MSIL/SharpKatz.A&threatid=2147767611&enterprise=0
	Name: VirTool:MSIL/SharpKatz.A
	ID: 2147767611
	Severity: Severe
	Category: Tool
	Path: file:_C:\Users\JustinCredible\Downloads\Unconfirmed 311824.crdownload
	Detection Origin: Local machine
	Detection Type: Concrete
	Detection Source: Real-Time Protection
	User: AzureAD\JustinCredible
	Process Name: C:\Program Files\WindowsApps\Com.RaycastTechnologiesLtd.Raycast.Production_0.25.1.0_x64__yw58zcv7bpp5a\Raycast\backend\node.exe
	Security intelligence Version: AV: 1.431.348.0, AS: 1.431.348.0, NIS: 1.431.348.0
	Engine Version: AM: 1.1.25050.6, NIS: 1.1.25050.6
```

Log Name:	Microsoft-Windows-Windows Defender/Operational		
Source:	Windows Defender	Logged:	7/20/2025 3:39:48 PM
Event ID:	1116	Task Category:	None
Level:	Warning	Keywords:	
User:	CUPCAKE\olafhartong	Computer:	Cupcake
OpCode:	Info		



DEAR MSRC

TIMELINE



Sept – Dec 2024
Initial research

Jan 20, 2025 –
Reported findings
covering all providers
to Microsoft.

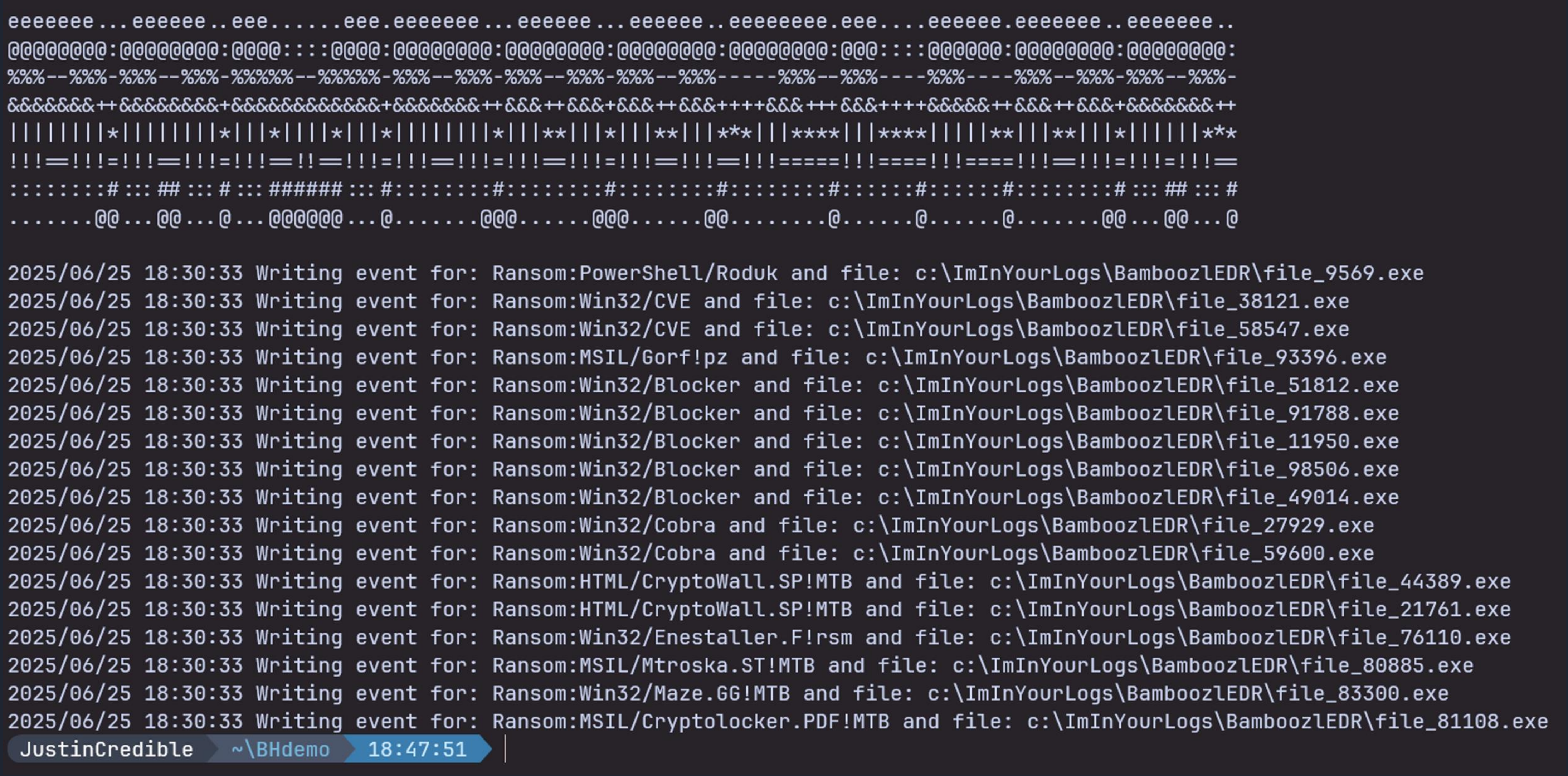
Including a POC tool,

Feb 4, 2025 - Assessed as a low severity, defense in depth item and does not meet MSRC’s bar for immediate servicing.

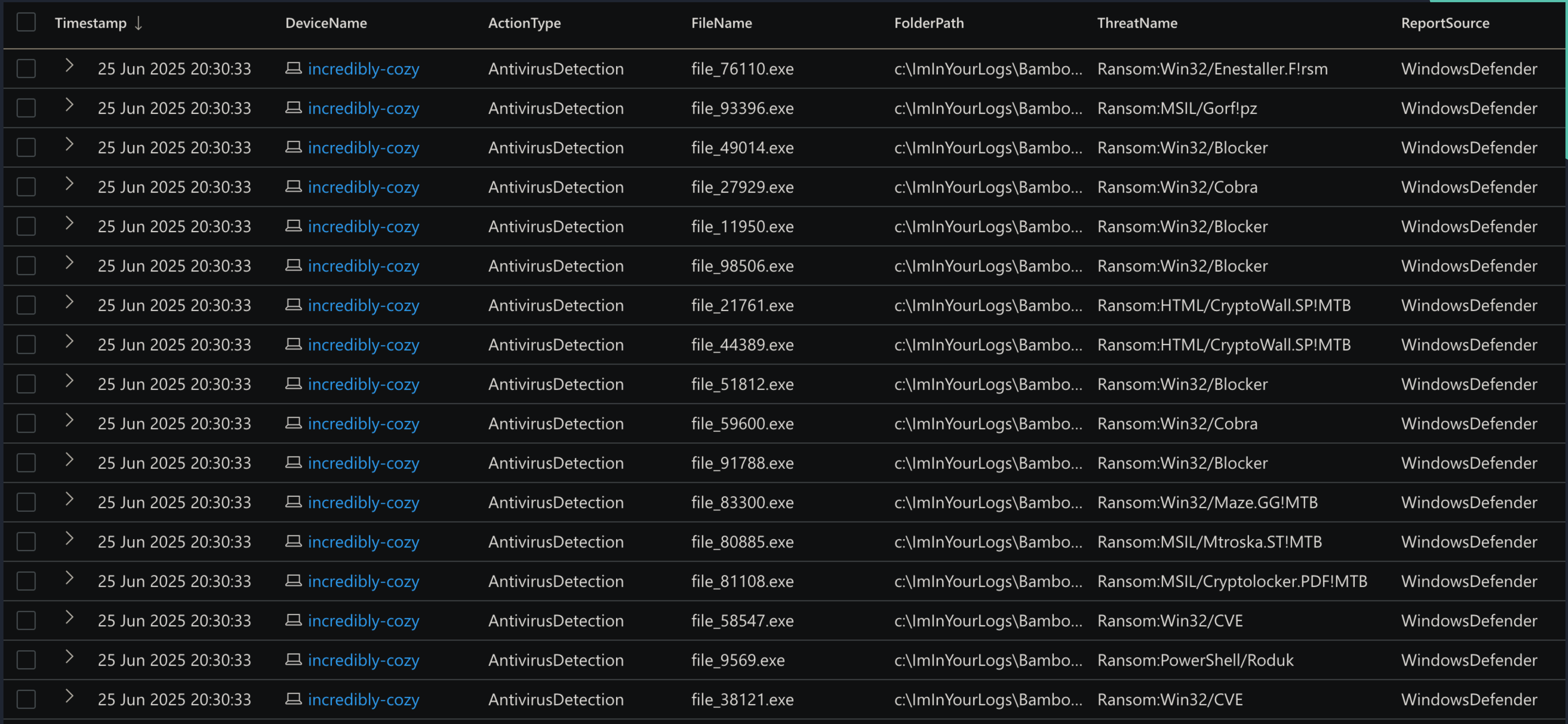
...CASE CLOSED...

OR WAS IT?

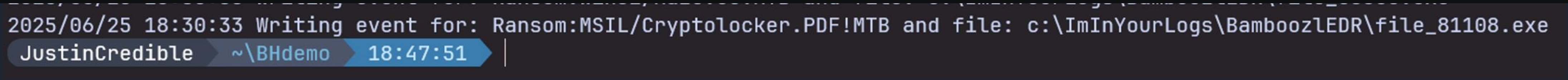
I STARTED RECORDING DEMOS



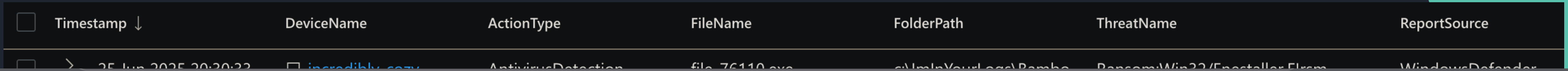
```
eeeeeee...eeeeee..eee......eee.eeeeeee...eeeeee...eeeeee..eeeeeeee.eee....eeeeee.eeeeeee..eeeeeee..
@@@@@@@@:@@@@@@@@:@@@@:::@@@@:@@@@@@@@:@@@@@@@@:@@@@@@@@:@@@@@@@@:@@@:::@@@@@@:@@@@@@@@:@@@@@@@@:
%%%--%%%-%%%--%%%-%%%%%--%%%%%-%%%--%%%-%%%--%%%-%%%--%%%-----%%%--%%%----%%%----%%%--%%%-%%%--%%%-
&&&&&&&++&&&&&&&&+&&&&&&&&&&&&+&&&&&&&++&&&++&&&+&&&++&&&++++&&&+++&&&++++&&&&&++&&&++&&&+&&&&&&&++
||||||||*||||||||*|||*||||*|||*||||||||*|||**|||*|||**|||***|||****|||****|||||**|||**|||*||||||***
!!!==!!!=!!!==!!!=!!!==!!==!!!=!!!==!!!=!!!==!!!=!!!==!!!==!!!=====!!!====!!!====!!!==!!!=!!!=!!!==
::::::::#:::##:::#:::######:::#::::::::#::::::::#::::::::#::::::::#::::::#::::::#::::::::#:::##:::#
.......@@...@@...@...@@@@@@...@.......@@@......@@@......@@........@......@......@.......@@...@@...@

2025/06/25 18:30:33 Writing event for: Ransom:PowerShell/Roduk and file: c:\ImInYourLogs\BamboozlEDR\file_9569.exe
2025/06/25 18:30:33 Writing event for: Ransom:Win32/CVE and file: c:\ImInYourLogs\BamboozlEDR\file_38121.exe
2025/06/25 18:30:33 Writing event for: Ransom:Win32/CVE and file: c:\ImInYourLogs\BamboozlEDR\file_58547.exe
2025/06/25 18:30:33 Writing event for: Ransom:MSIL/Gorf!pz and file: c:\ImInYourLogs\BamboozlEDR\file_93396.exe
2025/06/25 18:30:33 Writing event for: Ransom:Win32/Blocker and file: c:\ImInYourLogs\BamboozlEDR\file_51812.exe
2025/06/25 18:30:33 Writing event for: Ransom:Win32/Blocker and file: c:\ImInYourLogs\BamboozlEDR\file_91788.exe
2025/06/25 18:30:33 Writing event for: Ransom:Win32/Blocker and file: c:\ImInYourLogs\BamboozlEDR\file_11950.exe
2025/06/25 18:30:33 Writing event for: Ransom:Win32/Blocker and file: c:\ImInYourLogs\BamboozlEDR\file_98506.exe
2025/06/25 18:30:33 Writing event for: Ransom:Win32/Blocker and file: c:\ImInYourLogs\BamboozlEDR\file_49014.exe
2025/06/25 18:30:33 Writing event for: Ransom:Win32/Cobra and file: c:\ImInYourLogs\BamboozlEDR\file_27929.exe
2025/06/25 18:30:33 Writing event for: Ransom:Win32/Cobra and file: c:\ImInYourLogs\BamboozlEDR\file_59600.exe
2025/06/25 18:30:33 Writing event for: Ransom:HTML/CryptoWall.SP!MTB and file: c:\ImInYourLogs\BamboozlEDR\file_44389.exe
2025/06/25 18:30:33 Writing event for: Ransom:HTML/CryptoWall.SP!MTB and file: c:\ImInYourLogs\BamboozlEDR\file_21761.exe
2025/06/25 18:30:33 Writing event for: Ransom:Win32/Enestaller.F!rsm and file: c:\ImInYourLogs\BamboozlEDR\file_76110.exe
2025/06/25 18:30:33 Writing event for: Ransom:MSIL/Mtroska.ST!MTB and file: c:\ImInYourLogs\BamboozlEDR\file_80885.exe
2025/06/25 18:30:33 Writing event for: Ransom:Win32/Maze.GG!MTB and file: c:\ImInYourLogs\BamboozlEDR\file_83300.exe
2025/06/25 18:30:33 Writing event for: Ransom:MSIL/Cryptolocker.PDF!MTB and file: c:\ImInYourLogs\BamboozlEDR\file_81108.exe
 JustinCredible  ~\BHdemo  18:47:51 
```



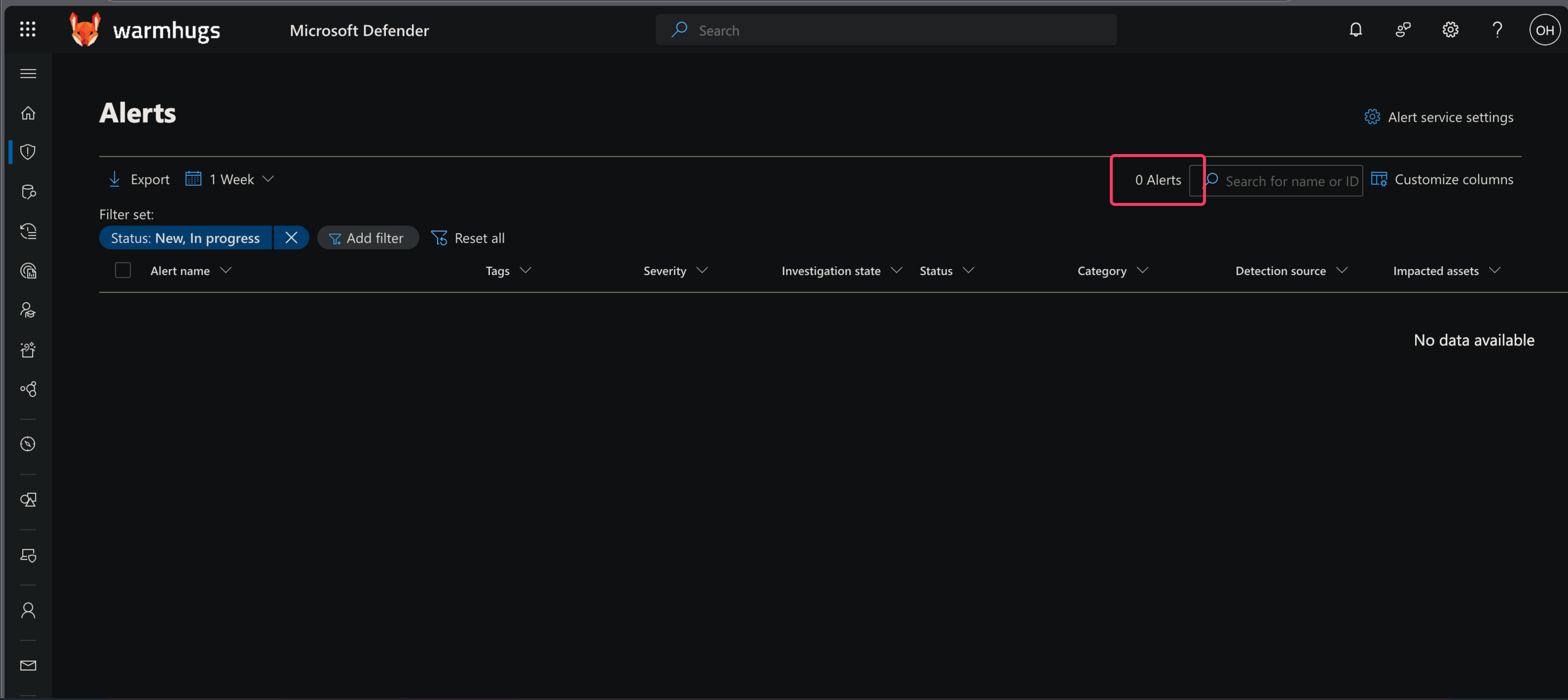
☐		Timestamp ↓	DeviceName	ActionType	FileName	FolderPath	ThreatName	ReportSource
☐	›	25 Jun 2025 20:30:33	incredibly-cozy	AntivirusDetection	file_76110.exe	c:\ImInYourLogs\Bambo...	Ransom:Win32/Enestaller.F!rsm	WindowsDefender
☐	›	25 Jun 2025 20:30:33	incredibly-cozy	AntivirusDetection	file_93396.exe	c:\ImInYourLogs\Bambo...	Ransom:MSIL/Gorf!pz	WindowsDefender
☐	›	25 Jun 2025 20:30:33	incredibly-cozy	AntivirusDetection	file_49014.exe	c:\ImInYourLogs\Bambo...	Ransom:Win32/Blocker	WindowsDefender
☐	›	25 Jun 2025 20:30:33	incredibly-cozy	AntivirusDetection	file_27929.exe	c:\ImInYourLogs\Bambo...	Ransom:Win32/Cobra	WindowsDefender
☐	›	25 Jun 2025 20:30:33	incredibly-cozy	AntivirusDetection	file_11950.exe	c:\ImInYourLogs\Bambo...	Ransom:Win32/Blocker	WindowsDefender
☐	›	25 Jun 2025 20:30:33	incredibly-cozy	AntivirusDetection	file_98506.exe	c:\ImInYourLogs\Bambo...	Ransom:Win32/Blocker	WindowsDefender
☐	›	25 Jun 2025 20:30:33	incredibly-cozy	AntivirusDetection	file_21761.exe	c:\ImInYourLogs\Bambo...	Ransom:HTML/CryptoWall.SP!MTB	WindowsDefender
☐	›	25 Jun 2025 20:30:33	incredibly-cozy	AntivirusDetection	file_44389.exe	c:\ImInYourLogs\Bambo...	Ransom:HTML/CryptoWall.SP!MTB	WindowsDefender
☐	›	25 Jun 2025 20:30:33	incredibly-cozy	AntivirusDetection	file_51812.exe	c:\ImInYourLogs\Bambo...	Ransom:Win32/Blocker	WindowsDefender
☐	›	25 Jun 2025 20:30:33	incredibly-cozy	AntivirusDetection	file_59600.exe	c:\ImInYourLogs\Bambo...	Ransom:Win32/Cobra	WindowsDefender
☐	›	25 Jun 2025 20:30:33	incredibly-cozy	AntivirusDetection	file_91788.exe	c:\ImInYourLogs\Bambo...	Ransom:Win32/Blocker	WindowsDefender
☐	›	25 Jun 2025 20:30:33	incredibly-cozy	AntivirusDetection	file_83300.exe	c:\ImInYourLogs\Bambo...	Ransom:Win32/Maze.GG!MTB	WindowsDefender
☐	›	25 Jun 2025 20:30:33	incredibly-cozy	AntivirusDetection	file_80885.exe	c:\ImInYourLogs\Bambo...	Ransom:MSIL/Mtroska.ST!MTB	WindowsDefender
☐	›	25 Jun 2025 20:30:33	incredibly-cozy	AntivirusDetection	file_81108.exe	c:\ImInYourLogs\Bambo...	Ransom:MSIL/Cryptolocker.PDF!MTB	WindowsDefender
☐	›	25 Jun 2025 20:30:33	incredibly-cozy	AntivirusDetection	file_58547.exe	c:\ImInYourLogs\Bambo...	Ransom:Win32/CVE	WindowsDefender
☐	›	25 Jun 2025 20:30:33	incredibly-cozy	AntivirusDetection	file_9569.exe	c:\ImInYourLogs\Bambo...	Ransom:PowerShell/Roduk	WindowsDefender
☐	›	25 Jun 2025 20:30:33	incredibly-cozy	AntivirusDetection	file_38121.exe	c:\ImInYourLogs\Bambo...	Ransom:Win32/CVE	WindowsDefender



```
2025/06/25 18:30:33 Writing event for: Ransom:MSIL/Cryptolocker.PDF!MTB and file: c:\ImInYourLogs\BamboozlEDR\file_81108.exe
JustinCredible  ~\BHdemo  18:47:51
```



☐	Timestamp ↓	DeviceName	ActionType	FileName	FolderPath	ThreatName	ReportSource
☐	25 Jun 2025 20:30:33	incredibly-cozy	AntivirusDetection	file-76110.exe	c:\ImInYourLogs\Rambo	Ransom:Win32/Encstaller.Elrsm	WindowsDefender



Alerts

0 Alerts

Filter set:

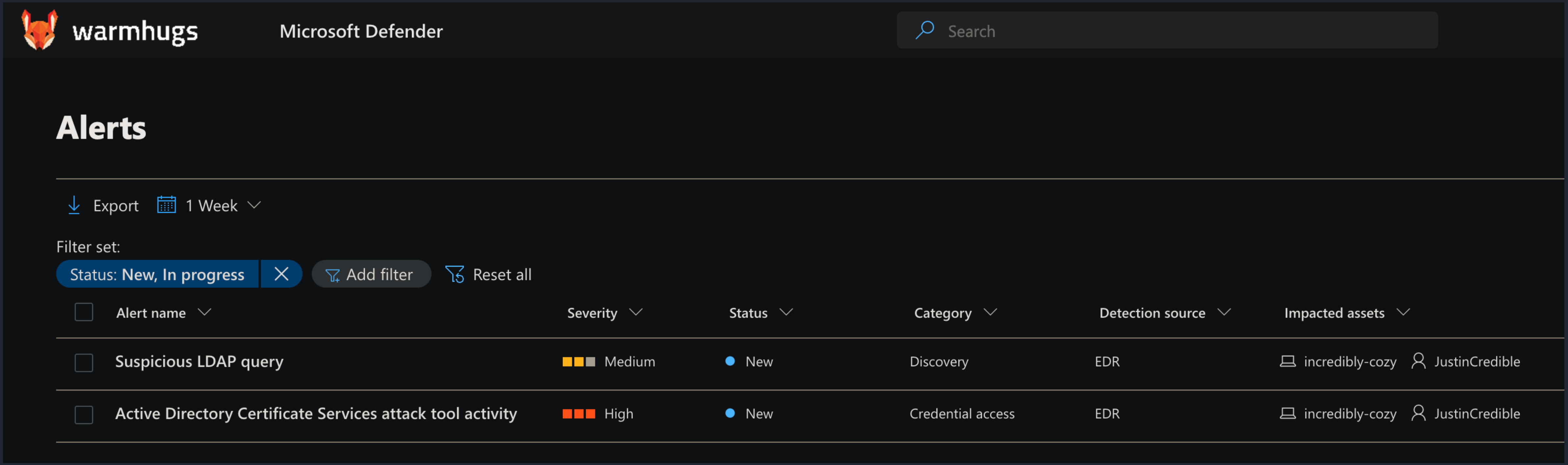
Status: New, In progress

☐	Alert name	Tags	Severity	Investigation state	Status	Category	Detection source	Impacted assets

No data available

SO, THEY FIXED IT AFTER ALL ?

NO, ONLY ANTIMALWARE ALERTS ARE FIXED



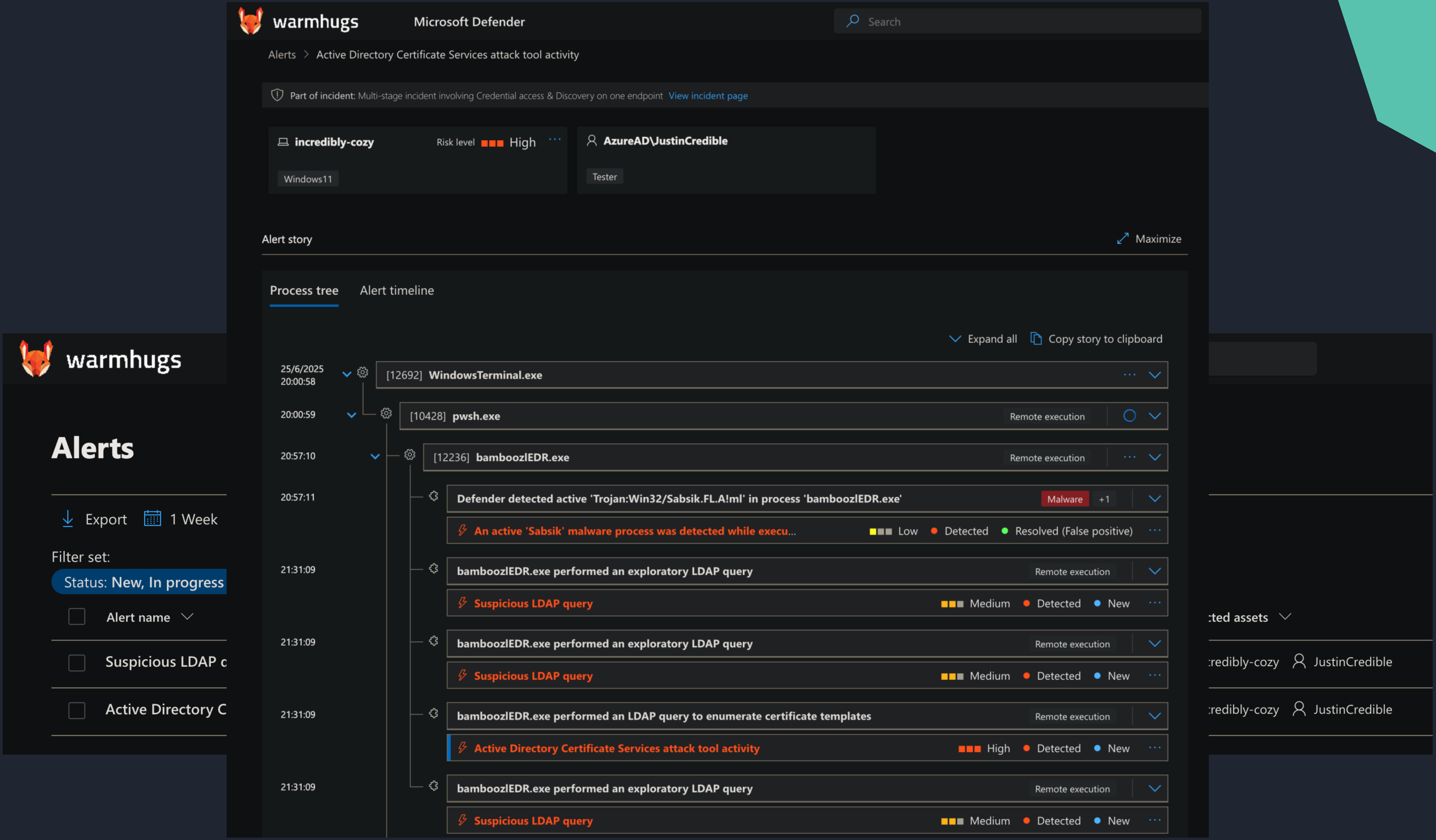
Alerts

Export 1 Week

Filter set:

Status: New, In progress ✕ Add filter Reset all

□	Alert name	Severity	Status	Category	Detection source	Impacted assets
□	Suspicious LDAP query	🟧🟧▨ Medium	● New	Discovery	EDR	incredibly-cozy JustinCredible
□	Active Directory Certificate Services attack tool activity	🟥🟥🟥 High	● New	Credential access	EDR	incredibly-cozy JustinCredible



warmhugs Microsoft Defender

Search

Alerts > Active Directory Certificate Services attack tool activity

Part of incident: Multi-stage incident involving Credential access & Discovery on one endpoint View incident page

incredibly-cozy Risk level High

Windows11

AzureAD\JustinCredible

Tester

Alert story

Maximize

Process tree Alert timeline

Expand all Copy story to clipboard

25/6/2025 20:00:58 [12692] WindowsTerminal.exe

20:00:59 [10428] pwsh.exe Remote execution

20:57:10 [12236] bamboozlEDR.exe Remote execution

20:57:11 Defender detected active 'Trojan:Win32/Sabsik.FL.A!ml' in process 'bamboozlEDR.exe' Malware +1

An active 'Sabsik' malware process was detected while execu... Low ● Detected ● Resolved (False positive)

21:31:09 bamboozlEDR.exe performed an exploratory LDAP query Remote execution

Suspicious LDAP query Medium ● Detected ● New

21:31:09 bamboozlEDR.exe performed an exploratory LDAP query Remote execution

Suspicious LDAP query Medium ● Detected ● New

21:31:09 bamboozlEDR.exe performed an LDAP query to enumerate certificate templates Remote execution

Active Directory Certificate Services attack tool activity High ● Detected ● New

21:31:09 bamboozlEDR.exe performed an exploratory LDAP query Remote execution

Suspicious LDAP query Medium ● Detected ● New

warmhugs

Alerts

Export 1 Week

Filter set:

Status: New, In progress

□ Alert name	:ted assets
□ Suspicious LDAP c	:redibly-cozy JustinCredible
□ Active Directory C	:redibly-cozy JustinCredible

THEN, I GOT AN EMAIL FROM MSRC

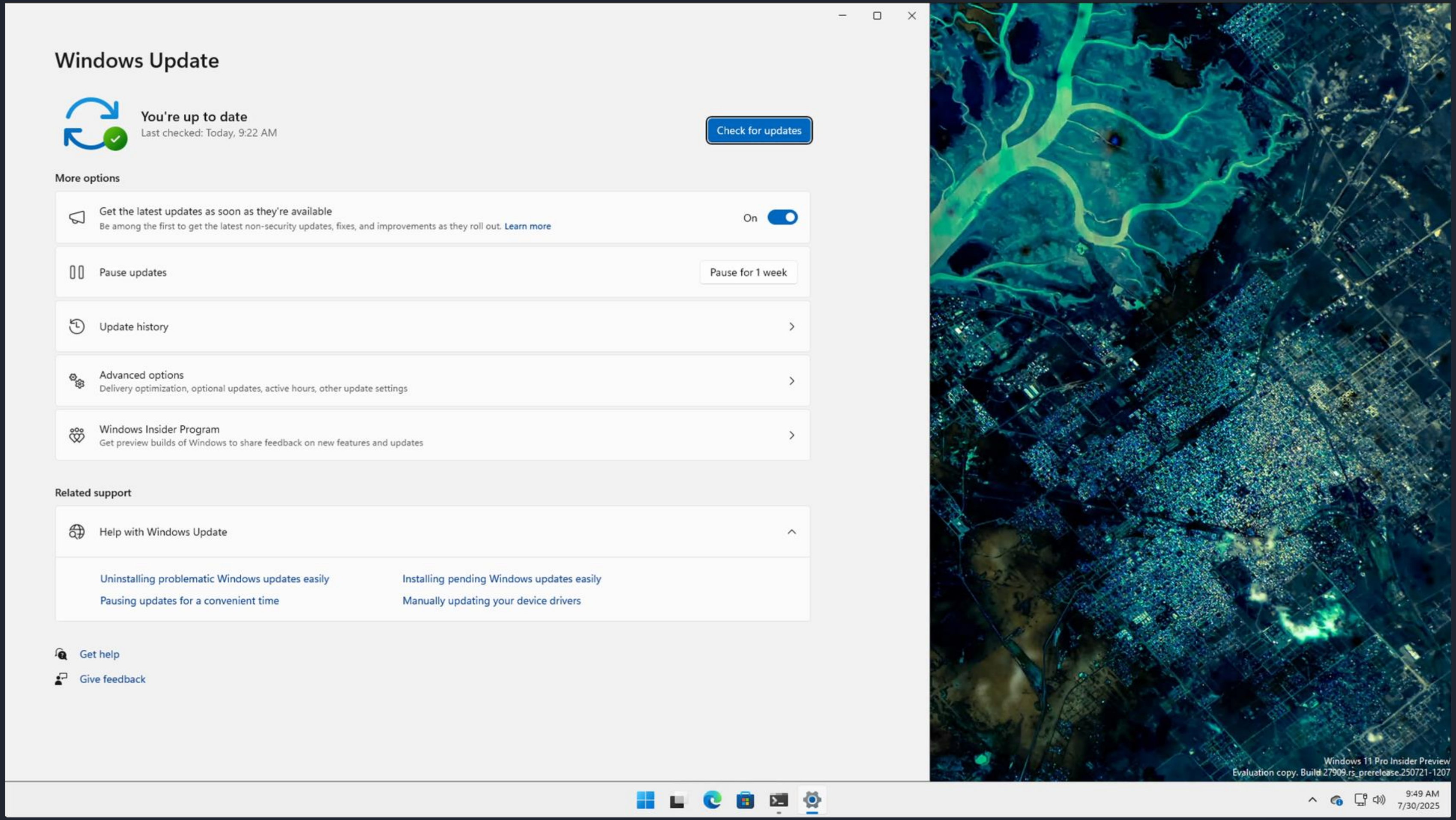
> “The revised fix began rolling out in July. It’s being deployed gradually through a ring-based approach and is expected to reach full deployment by August 7th”

The rest of the email gave me the impression they were addressing the ETW issue.
I requested details on what is fixed.. And what the scope of the solution is.

It took some back and forth emailing to get some more clarity, of which the TL;DR is:

> “The focus is on hardening the Defender product providers against non-privileged users.”

TESTED ON LATEST INSIDER BUILD



Windows Update

You're up to date
Last checked: Today, 9:22 AM

More options

Get the latest updates as soon as they're available
Be among the first to get the latest non-security updates, fixes, and improvements as they roll out. Learn more
On

Pause updates
Pause for 1 week

Update history

Advanced options
Delivery optimization, optional updates, active hours, other update settings

Windows Insider Program
Get preview builds of Windows to share feedback on new features and updates

Related support

Help with Windows Update

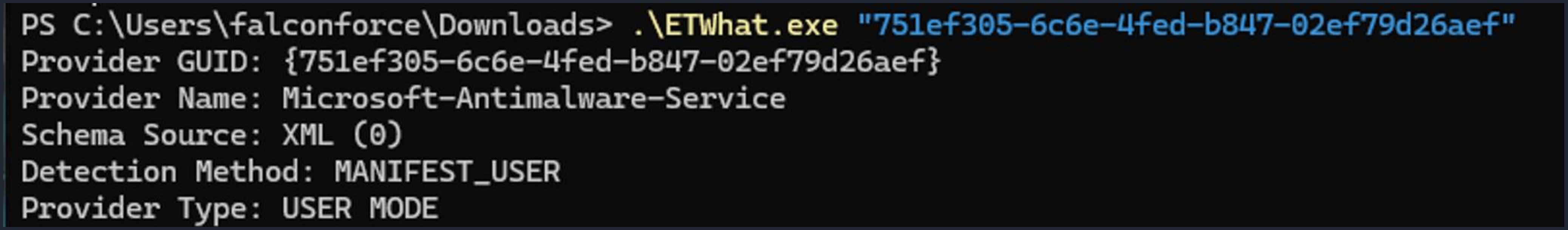
Uninstalling problematic Windows updates easily
Installing pending Windows updates easily
Pausing updates for a convenient time
Manually updating your device drivers

Get help
Give feedback

Windows 11 Pro Insider Preview
Evaluation copy. Build 27909.rs_prerelease.250721-1207

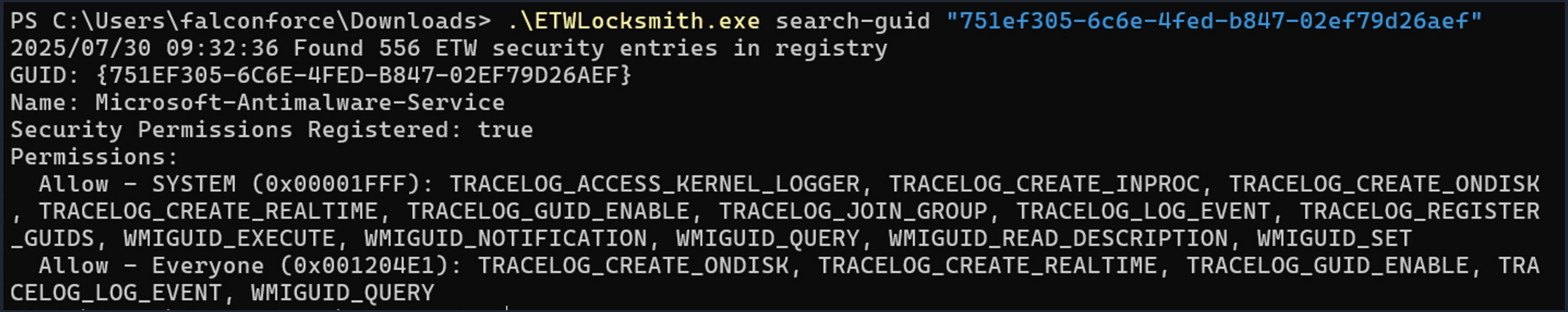
9:49 AM
7/30/2025

NOTHING VISIBLY CHANGED



```
PS C:\Users\falconforce\Downloads> .\ETWhat.exe "751ef305-6c6e-4fed-b847-02ef79d26aef"
Provider GUID: {751ef305-6c6e-4fed-b847-02ef79d26aef}
Provider Name: Microsoft-Antimalware-Service
Schema Source: XML (0)
Detection Method: MANIFEST_USER
Provider Type: USER MODE
```

Still the same permissions



```
PS C:\Users\falconforce\Downloads> .\ETWLocksmith.exe search-guid "751ef305-6c6e-4fed-b847-02ef79d26aef"
2025/07/30 09:32:36 Found 556 ETW security entries in registry
GUID: {751EF305-6C6E-4FED-B847-02EF79D26AEF}
Name: Microsoft-Antimalware-Service
Security Permissions Registered: true
Permissions:
  Allow - SYSTEM (0x00001FFF): TRACELOG_ACCESS_KERNEL_LOGGER, TRACELOG_CREATE_INPROC, TRACELOG_CREATE_ONDISK
, TRACELOG_CREATE_REALTIME, TRACELOG_GUID_ENABLE, TRACELOG_JOIN_GROUP, TRACELOG_LOG_EVENT, TRACELOG_REGISTER
_GUIDS, WMIGUID_EXECUTE, WMIGUID_NOTIFICATION, WMIGUID_QUERY, WMIGUID_READ_DESCRIPTION, WMIGUID_SET
  Allow - Everyone (0x001204E1): TRACELOG_CREATE_ONDISK, TRACELOG_CREATE_REALTIME, TRACELOG_GUID_ENABLE, TRA
CELOG_LOG_EVENT, WMIGUID_QUERY
```

THEY'VE GOT 99 PROBLEMS, AND FIXED 1

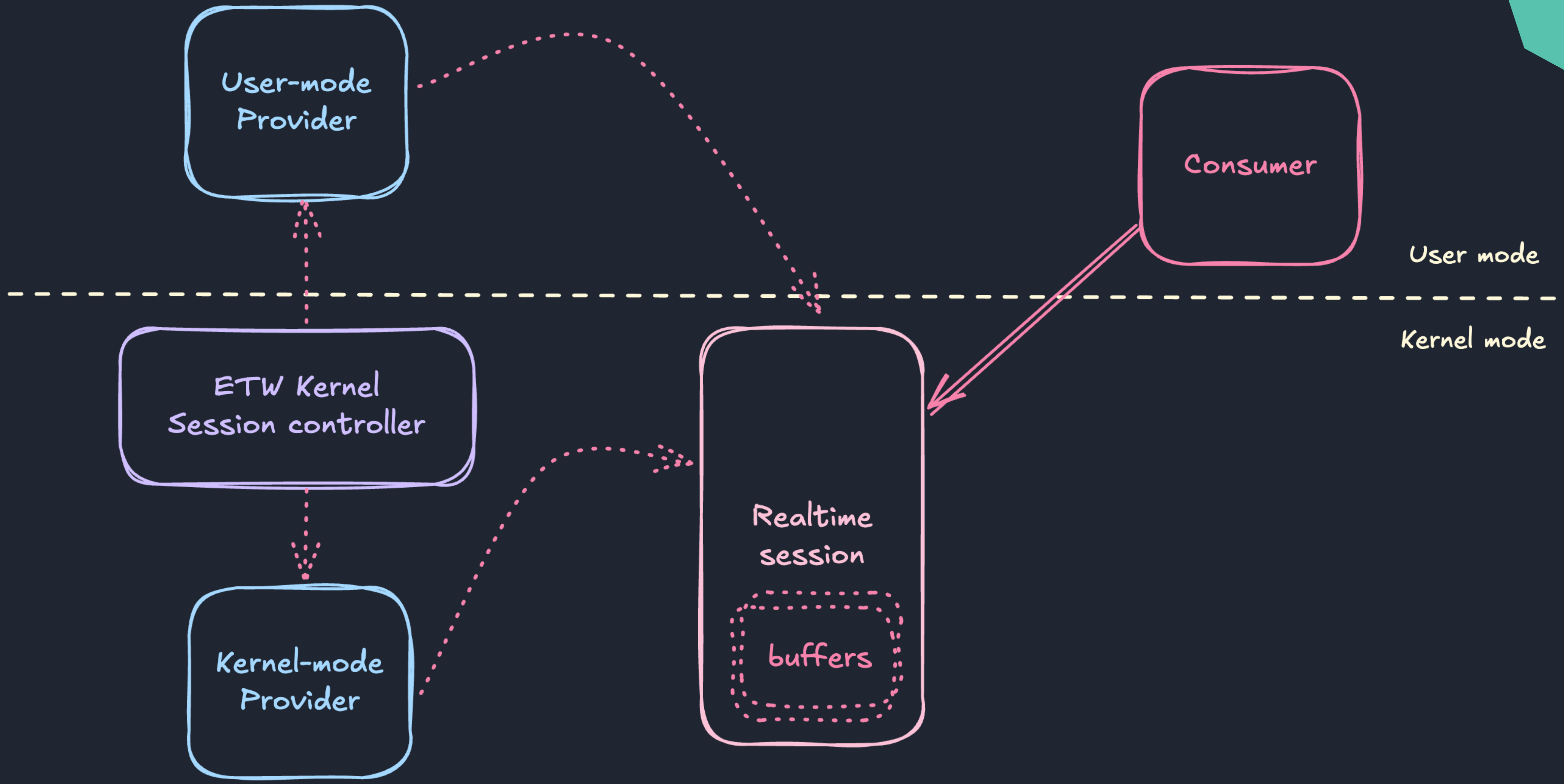
Tested Defender providers

Microsoft-Antimalware-Service	Protected, not sure how (yet)
Microsoft-Antimalware-RTP	Unprotected
Microsoft-Windows-AMSI	Unprotected
Microsoft-Windows-Windows Defender	Unprotected

All providers used by MDE for telemetry are out of scope for MSRC and remain to be available for (ab)use.

> “While we do encourage ETW provider owners to evaluate potential opportunities for hardening in future OS releases where feasible, the severity of addressing this scenario remains low.”

BUFF
ERS



User-mode Provider

Consumer

User mode

Kernel mode

ETW Kernel Session controller

Realtime session

buffers

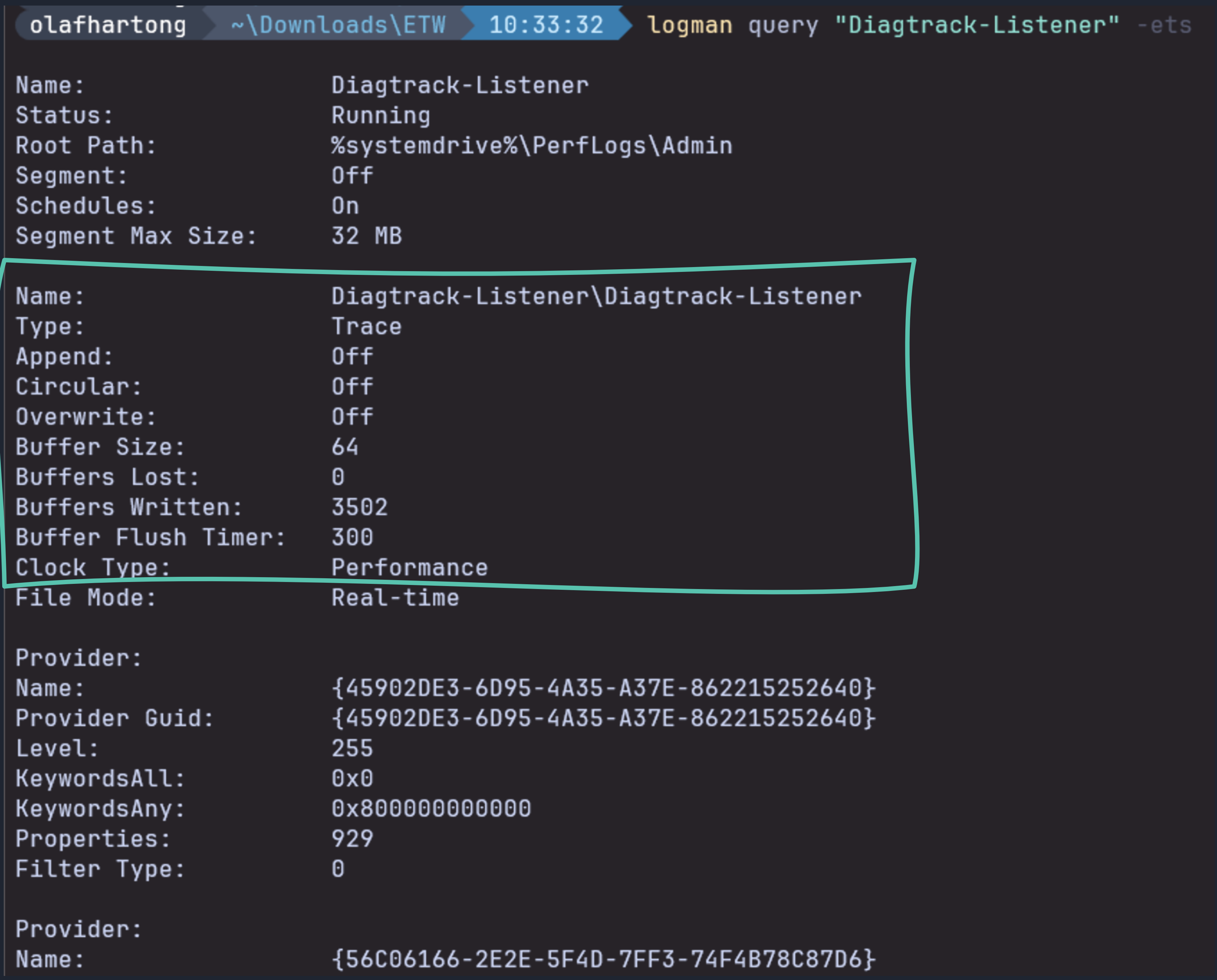
Kernel-mode Provider

BUFFER ARCHITECTURE

Shared Buffer Model:
ETW uses a pool of shared buffers for each tracing session, not per provider. Multiple providers can write to the same buffers within a session.

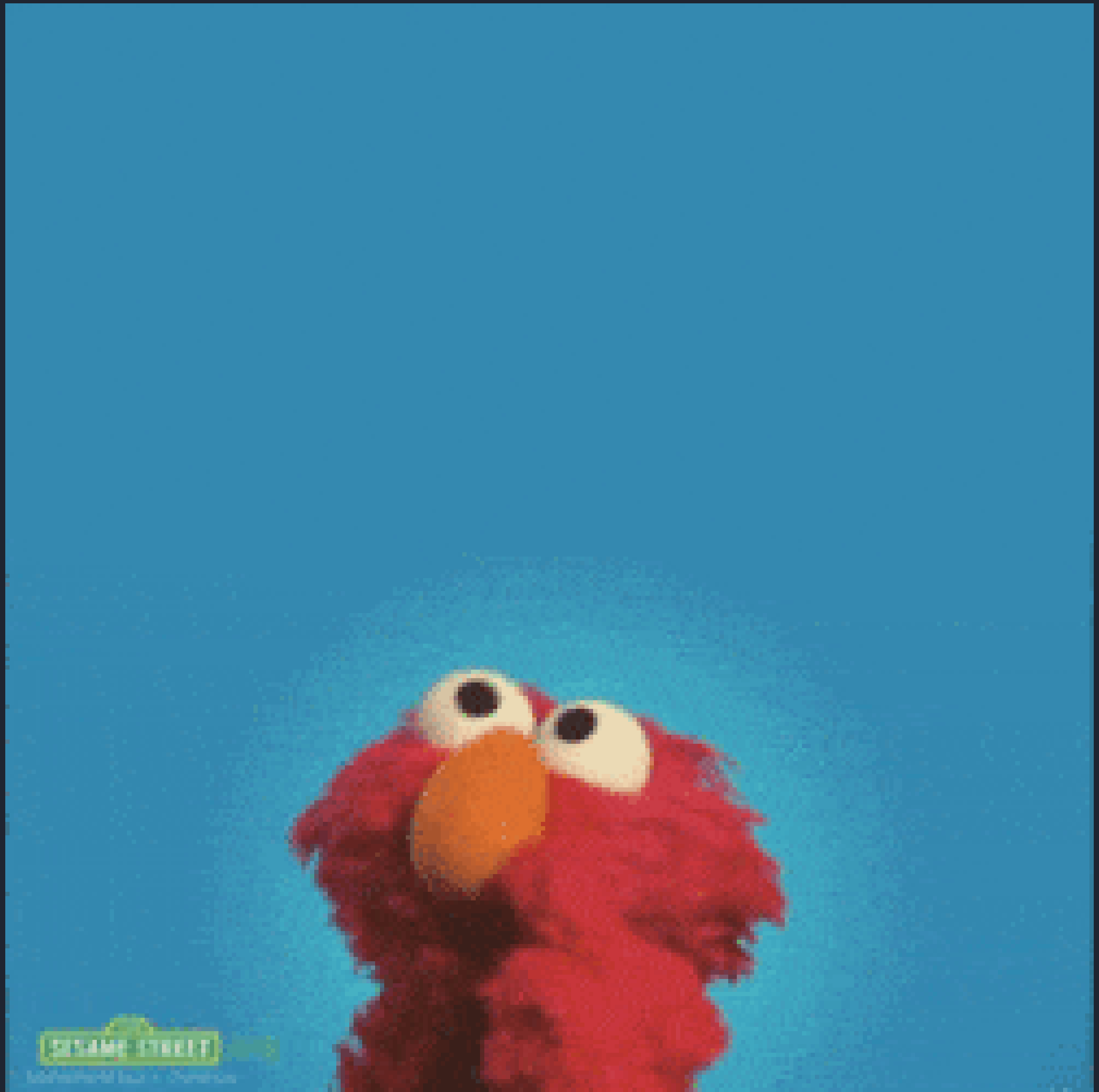
Buffer Pool

- Each ETW session maintains its own pool of buffers
- Buffer size is configurable (typically 64KB to 1MB)
- Number of buffers can be set when creating the session
- Buffers are allocated from non-paged pool memory

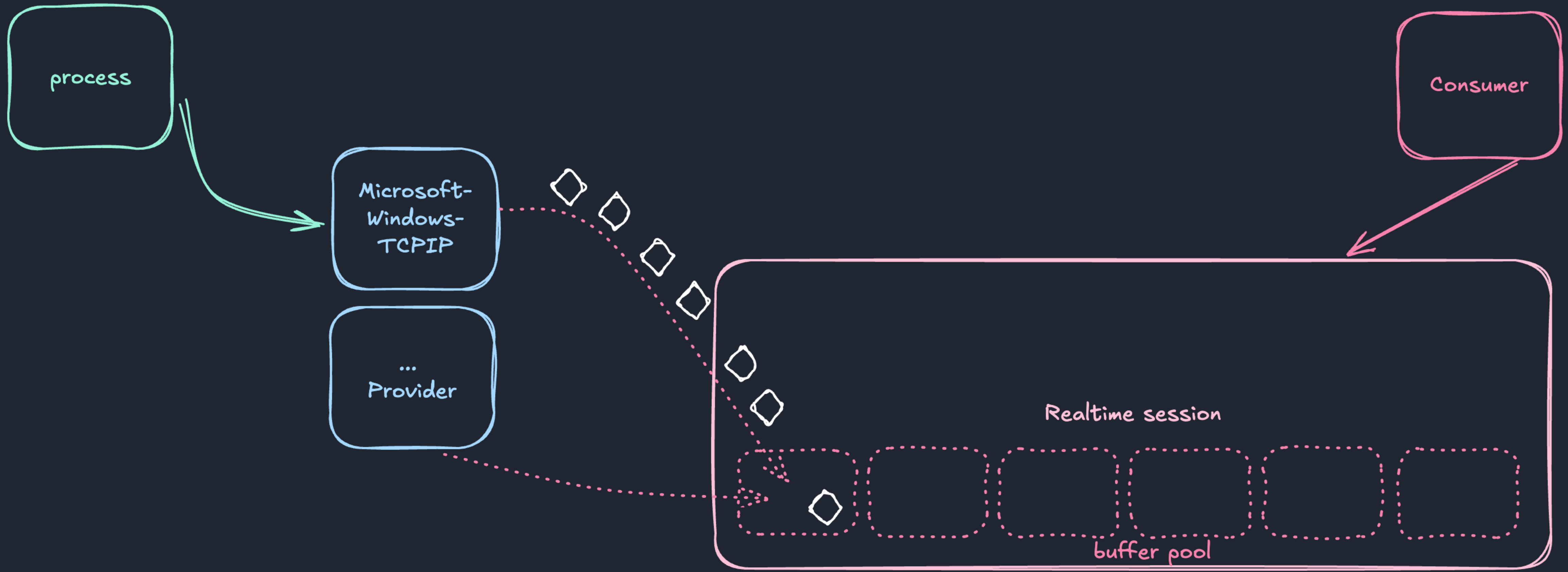


```
olafhartong  ~\Downloads\ETW  10:33:32  logman query "Diagtrack-Listener" -ets

Name:                   Diagtrack-Listener
Status:                 Running
Root Path:              %systemdrive%\PerfLogs\Admin
Segment:                Off
Schedules:              On
Segment Max Size:       32 MB

Name:                   Diagtrack-Listener\Diagtrack-Listener
Type:                   Trace
Append:                 Off
Circular:               Off
Overwrite:              Off
Buffer Size:            64
Buffers Lost:           0
Buffers Written:        3502
Buffer Flush Timer:     300
Clock Type:             Performance
File Mode:              Real-time

Provider:
Name:                   {45902DE3-6D95-4A35-A37E-862215252640}
Provider Guid:          {45902DE3-6D95-4A35-A37E-862215252640}
Level:                  255
KeywordsAll:            0x0
KeywordsAny:            0x800000000000
Properties:             929
Filter Type:            0

Provider:
Name:                   {56C06166-2E2E-5F4D-7FF3-74F4B78C87D6}
```

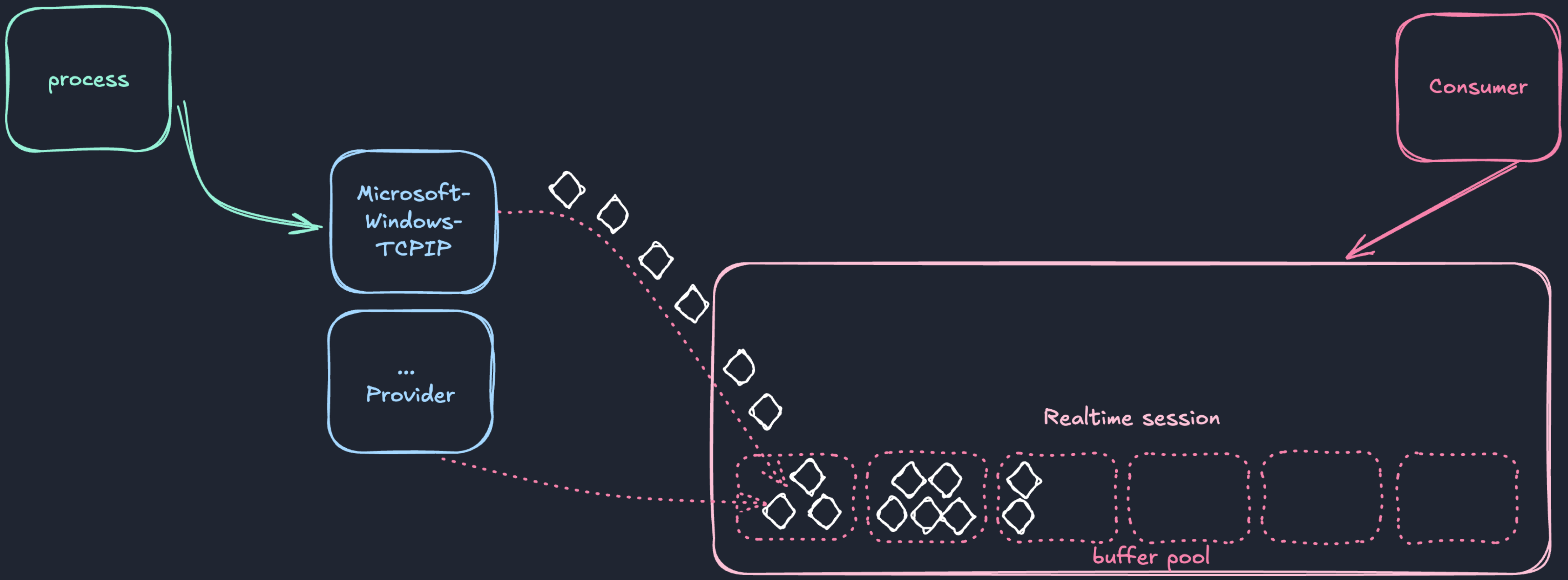
WHAT HAPPENS ON A BUFFER OVERFLOW



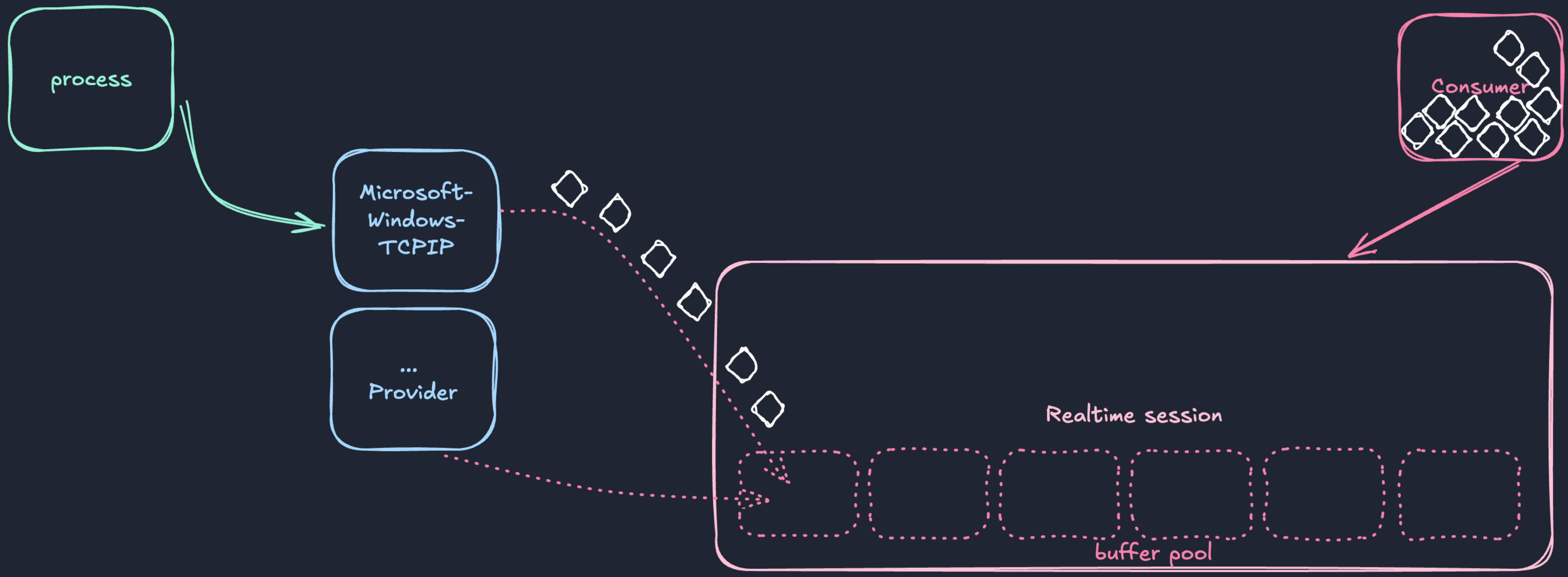
HOW DO THE BUFFERS WORK



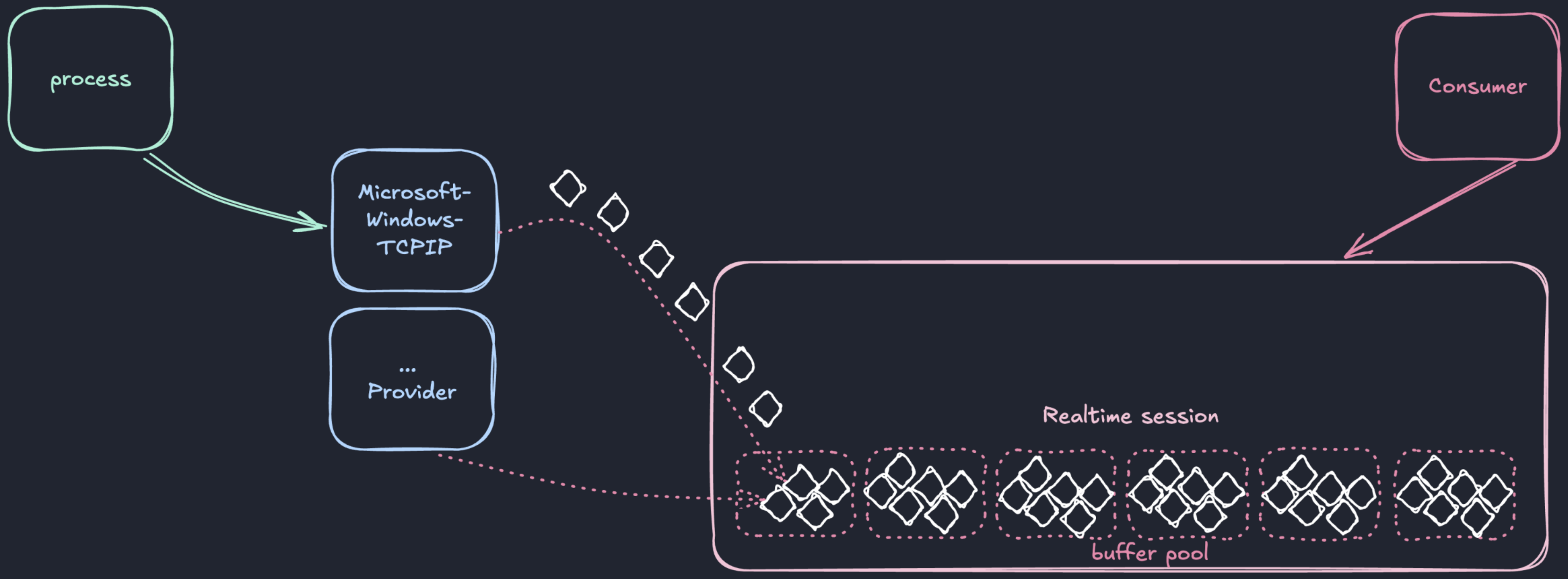
EVENTS ARE EMITTED AND FILL THE POOL



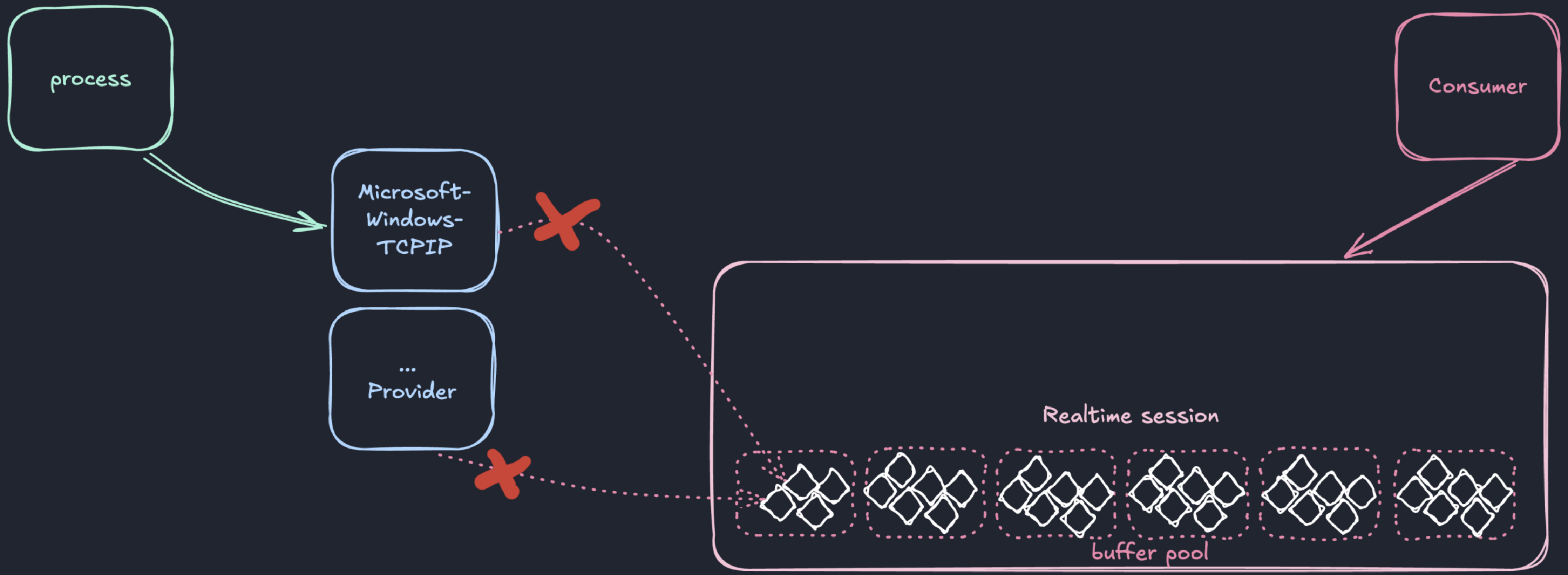
WHEN CONSUMED THE POOL FLUSHES



HOW BUFFER OVERFLOWS OCCUR

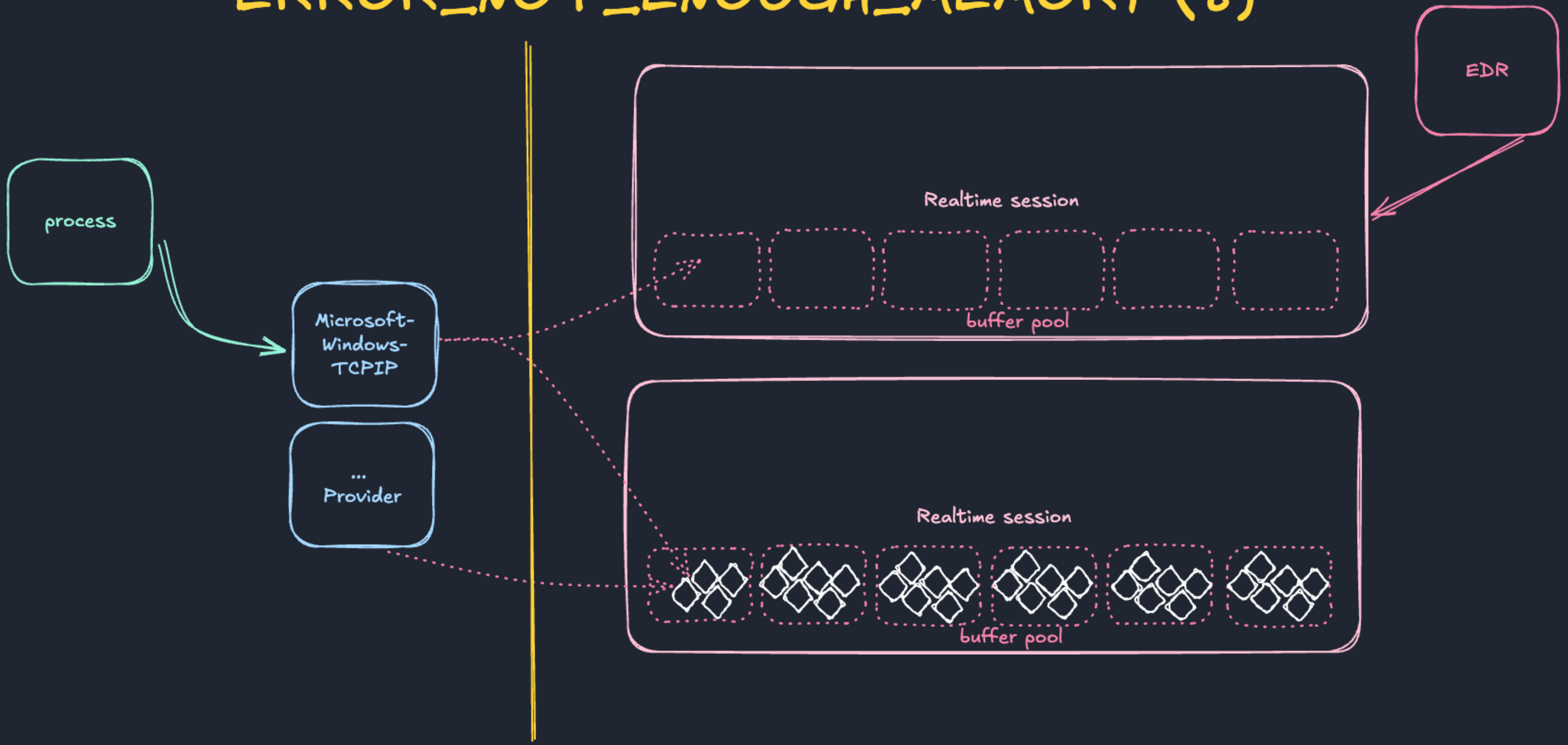


HOW BUFFER OVERFLOWS OCCUR



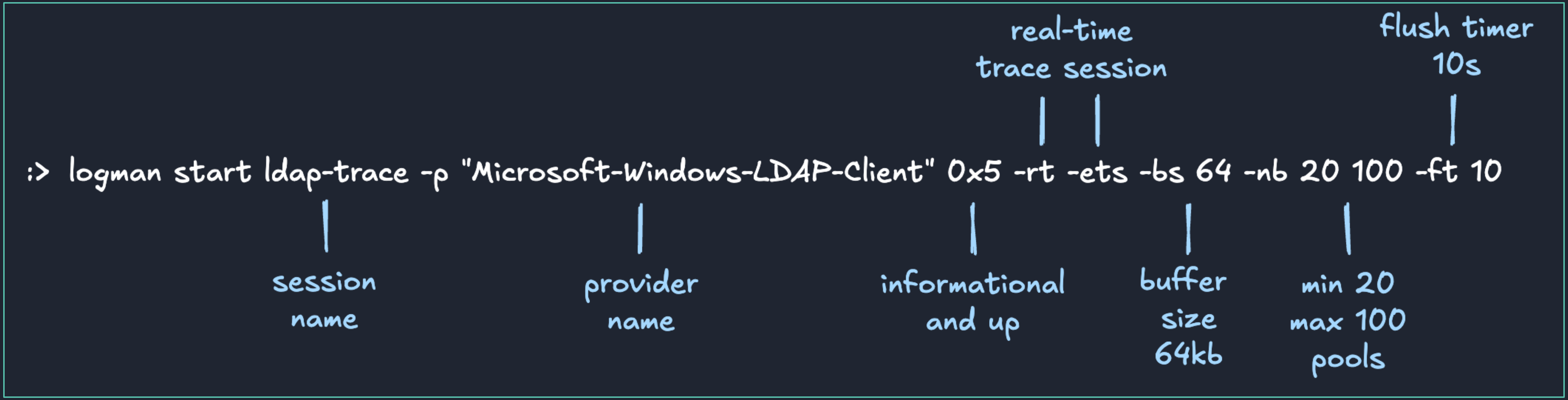
WHAT HAPPENS NOW

ERROR_NOT_ENOUGH_MEMORY (8)

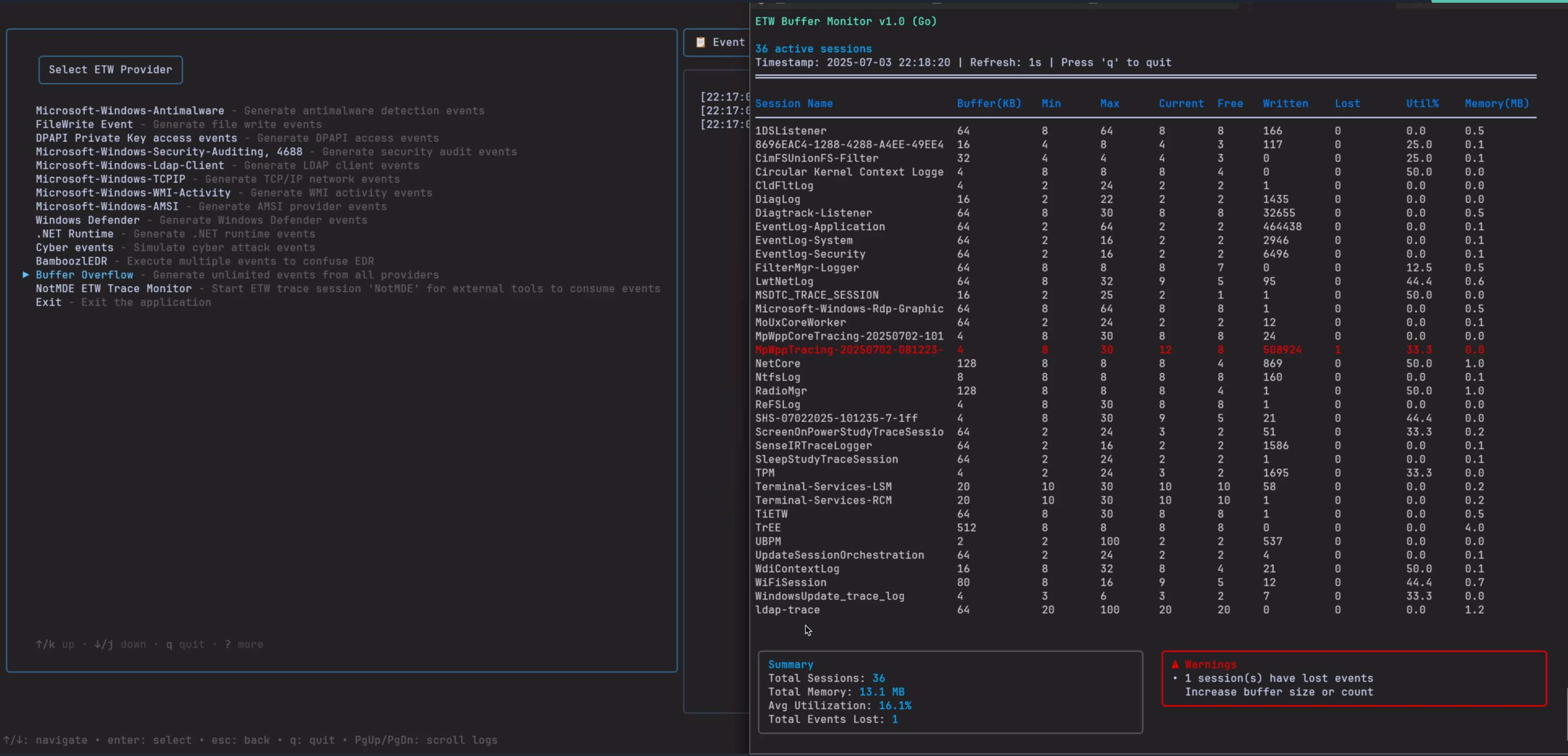


TESTING BUFFER OVERFLOW

- Wrote set of functions that emit as many ETW events to the providers as possible
- Started a real-time trace session for a provider with a common buffer size and generous pool
- Was a bit lazy and did not connect a consumer



```
:> logman start ldap-trace -p "Microsoft-Windows-LDAP-Client" 0x5 -rt -ets -bs 64 -nb 20 100 -ft 10
```



```
Select ETW Provider

  Microsoft-Windows-Antimalware - Generate antimalware detection events
  FileWrite Event - Generate file write events
  DPAPI Private Key access events - Generate DPAPI access events
  Microsoft-Windows-Security-Auditing, 4688 - Generate security audit events
  Microsoft-Windows-Ldap-Client - Generate LDAP client events
  Microsoft-Windows-TCPIP - Generate TCP/IP network events
  Microsoft-Windows-WMI-Activity - Generate WMI activity events
  Microsoft-Windows-AMSI - Generate AMSI provider events
  Windows Defender - Generate Windows Defender events
  .NET Runtime - Generate .NET runtime events
  Cyber events - Simulate cyber attack events
  BamboozlEDR - Execute multiple events to confuse EDR
▶ Buffer Overflow - Generate unlimited events from all providers
  NotMDE ETW Trace Monitor - Start ETW trace session 'NotMDE' for external tools to consume events
  Exit - Exit the application

  ↑/k up • ↓/j down • q quit • ? more

↑/↓: navigate • enter: select • esc: back • q: quit • PgUp/PgDn: scroll logs
```

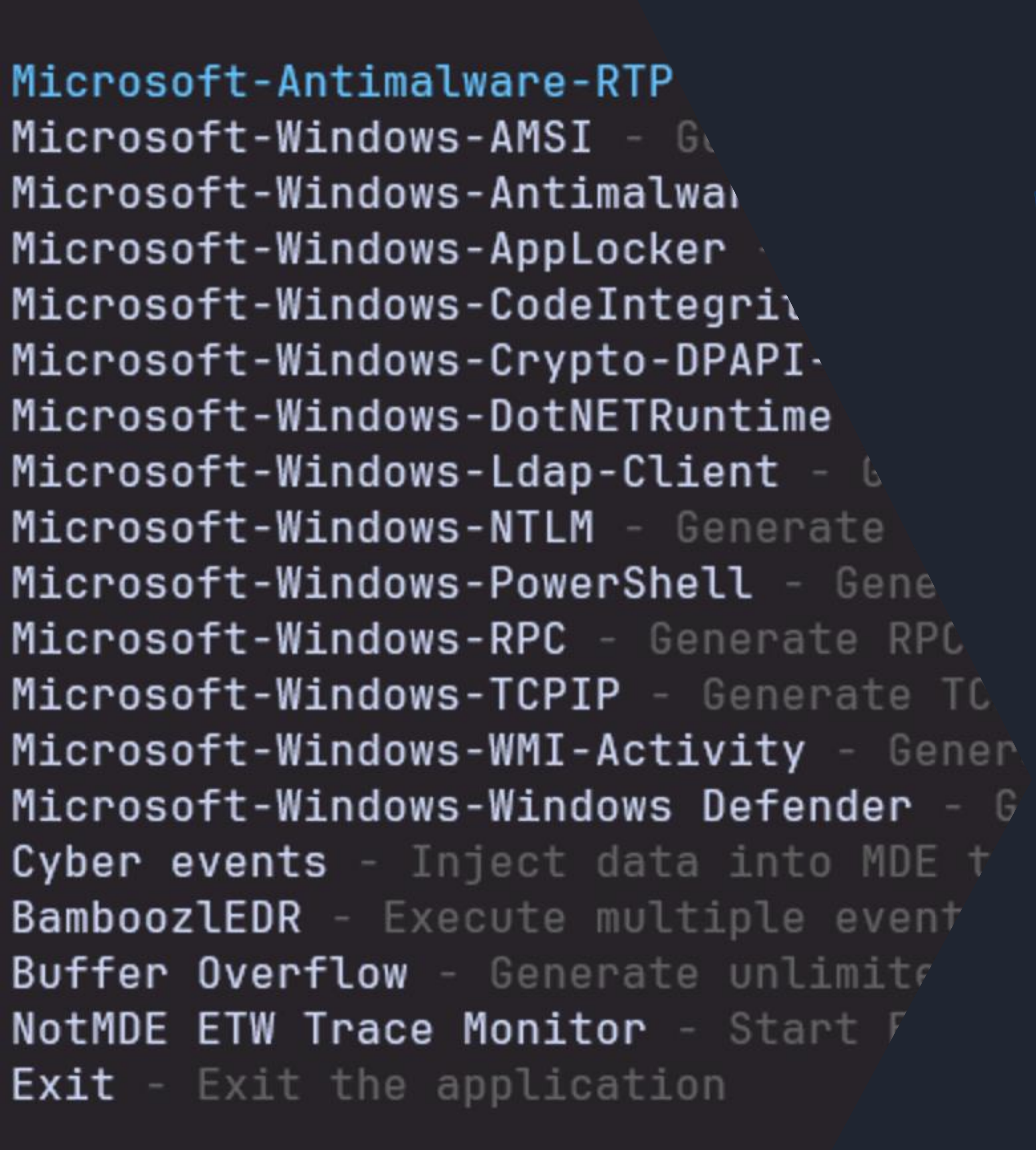
```
[22:17:0
[22:17:0
[22:17:0
```

```
ETW Buffer Monitor v1.0 (Go)

36 active sessions
Timestamp: 2025-07-03 22:18:20 | Refresh: 1s | Press 'q' to quit
═══════════════════════════════════════════════════════════════════════════════════════════════════════════

Session Name                   Buffer(KB)  Min   Max   Current  Free  Written  Lost   Util%  Memory(MB)
───────────────────────────────────────────────────────────────────────────────────────────────────────────
1DSListener                    64          8     64    8        8     166      0      0.0    0.5
8696EAC4-1288-4288-A4EE-49EE4  16          4     8     4        3     117      0      25.0   0.1
CimFSUnionFS-Filter            32          4     4     4        3     0        0      25.0   0.1
Circular Kernel Context Logge  4           8     8     8        4     0        0      50.0   0.0
CldFltLog                      4           2     24    2        2     1        0      0.0    0.0
DiagLog                        16          2     22    2        2     1435     0      0.0    0.0
Diagtrack-Listener             64          8     30    8        8     32655    0      0.0    0.5
EventLog-Application           64          2     64    2        2     464438   0      0.0    0.1
EventLog-System                64          2     16    2        2     2946     0      0.0    0.1
Eventlog-Security              64          2     16    2        2     6496     0      0.0    0.1
FilterMgr-Logger               64          8     8     8        7     0        0      12.5   0.5
LwtNetLog                      64          8     32    9        5     95       0      44.4   0.6
MSDTC_TRACE_SESSION            16          2     25    2        1     1        0      50.0   0.0
Microsoft-Windows-Rdp-Graphic  64          8     64    8        8     1        0      0.0    0.5
MoUxCoreWorker                 64          2     24    2        2     12       0      0.0    0.1
MpWppCoreTracing-20250702-101  4           8     30    8        8     24       0      0.0    0.0
MpWppTracing-20250702-081223-  4           8     30    12       8     508924   1      33.3   0.0
NetCore                        128         8     8     8        4     869      0      50.0   1.0
NtfsLog                        8           8     8     8        8     160      0      0.0    0.1
RadioMgr                       128         8     8     8        4     1        0      50.0   1.0
ReFSLog                        4           8     30    8        8     1        0      0.0    0.0
SHS-07022025-101235-7-1ff      4           8     30    9        5     21       0      44.4   0.0
ScreenOnPowerStudyTraceSessio  64          2     24    3        2     51       0      33.3   0.2
SenseIRTraceLogger             64          2     16    2        2     1586     0      0.0    0.1
SleepStudyTraceSession         64          2     24    2        2     1        0      0.0    0.1
TPM                            4           2     24    3        2     1695     0      33.3   0.0
Terminal-Services-LSM          20          10    30    10       10    58       0      0.0    0.2
Terminal-Services-RCM          20          10    30    10       10    1        0      0.0    0.2
TiETW                          64          8     30    8        8     1        0      0.0    0.5
TrEE                           512         8     8     8        8     0        0      0.0    4.0
UBPM                           2           2     100   2        2     537      0      0.0    0.0
UpdateSessionOrchestration     64          2     24    2        2     4        0      0.0    0.1
WdiContextLog                  16          8     32    8        4     21       0      50.0   0.1
WiFiSession                    80          8     16    9        5     12       0      44.4   0.7
WindowsUpdate_trace_log        4           3     6     3        2     7        0      33.3   0.0
ldap-trace                     64          20    100   20       20    0        0      0.0    1.2

┌ Summary                          ┐   ┌ ▲ Warnings                          ┐
│ Total Sessions: 36               │   │ • 1 session(s) have lost events     │
│ Total Memory: 13.1 MB            │   │   Increase buffer size or count     │
│ Avg Utilization: 16.1%           │   └─────────────────────────────────────┘
│ Total Events Lost: 1             │
└──────────────────────────────────┘
```

BamboozlEDR

Available after this talk

https://github.com/olafhartong/BamboozlEDR



```
Microsoft-Antimalware-RTP
Microsoft-Windows-AMSI - G
Microsoft-Windows-Antimalwa
Microsoft-Windows-AppLocker -
Microsoft-Windows-CodeIntegri
Microsoft-Windows-Crypto-DPAPI-
Microsoft-Windows-DotNETRuntime
Microsoft-Windows-Ldap-Client - G
Microsoft-Windows-NTLM - Generate
Microsoft-Windows-PowerShell - Gene
Microsoft-Windows-RPC - Generate RPC
Microsoft-Windows-TCPIP - Generate TC
Microsoft-Windows-WMI-Activity - Gener
Microsoft-Windows-Windows Defender - G
Cyber events - Inject data into MDE t
BamboozlEDR - Execute multiple event
Buffer Overflow - Generate unlimite
NotMDE ETW Trace Monitor - Start E
Exit - Exit the application
```

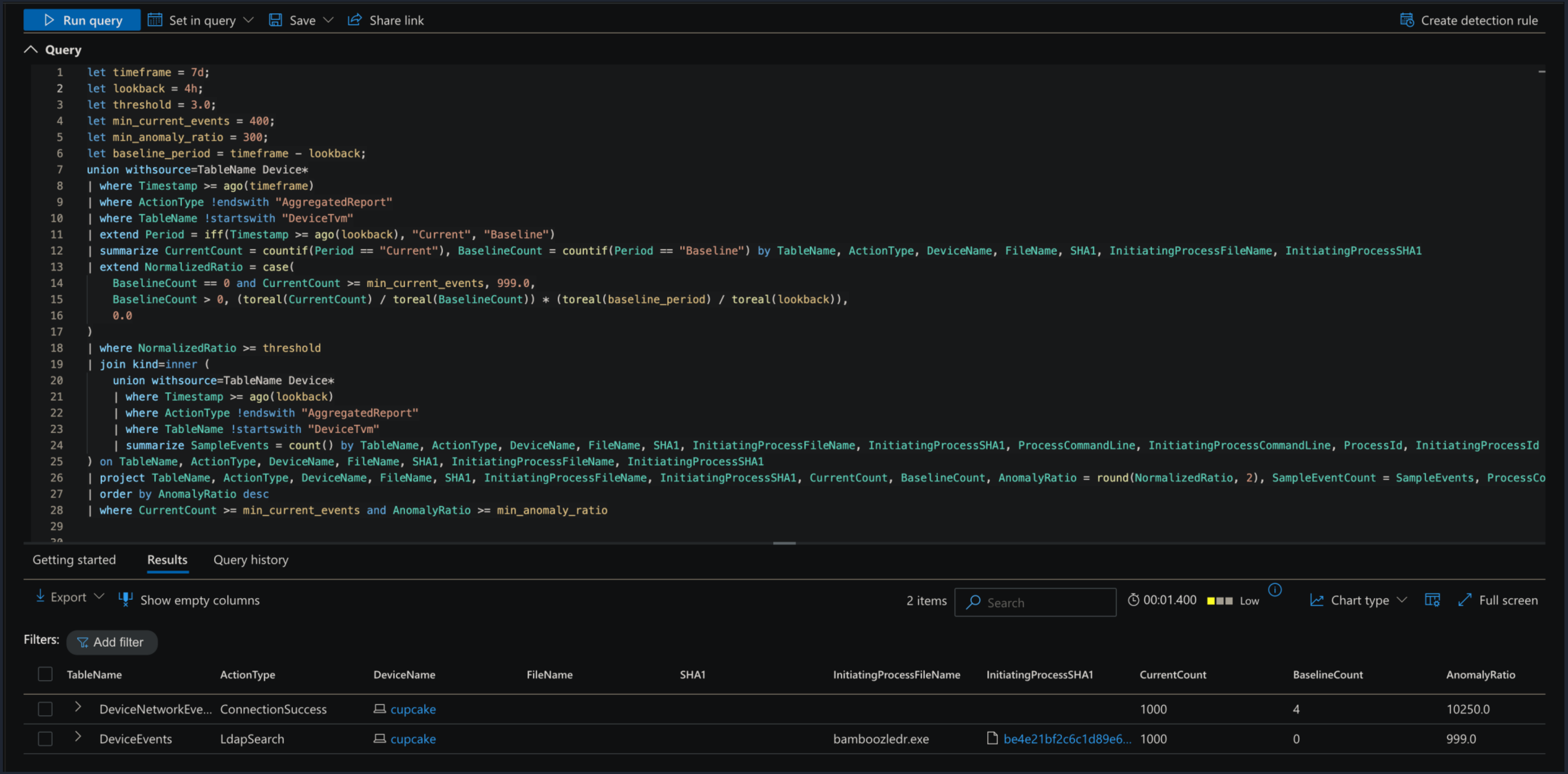
FEATURES

- □ Emit various events to many providers
- □ Hit the MDE capping for these providers
- □ Simulate telemetry for some attack tools
- □ Start a trace session, with all providers MDE uses, without a consumer
- □ Flood the trace session buffers

WHAT CAN A DEFENDER DO ABOUT THIS ?

- Build events to test custom detections which rely on the user-mode ETW providers
- Build detections on huge spikes followed by no events per provider source (complex)
- Try to change the default provider security ACLs (tricky)
- Pray Microsoft will properly fix this

"DETECTION"



```
let timeframe = 7d;
let lookback = 4h;
let threshold = 3.0;
let min_current_events = 400;
let min_anomaly_ratio = 300;
let baseline_period = timeframe - lookback;
union withsource=TableName Device*
| where Timestamp >= ago(timeframe)
| where ActionType !endswith "AggregatedReport"
| where TableName !startswith "DeviceTvm"
| extend Period = iff(Timestamp >= ago(lookback), "Current", "Baseline")
| summarize CurrentCount = countif(Period == "Current"), BaselineCount = countif(Period == "Baseline") by TableName, ActionType, DeviceName, FileName, SHA1, InitiatingProcessFileName, InitiatingProcessSHA1
| extend NormalizedRatio = case(
    BaselineCount == 0 and CurrentCount >= min_current_events, 999.0,
    BaselineCount > 0, (toreal(CurrentCount) / toreal(BaselineCount)) * (toreal(baseline_period) / toreal(lookback)),
    0.0
)
| where NormalizedRatio >= threshold
| join kind=inner (
    union withsource=TableName Device*
    | where Timestamp >= ago(lookback)
    | where ActionType !endswith "AggregatedReport"
    | where TableName !startswith "DeviceTvm"
    | summarize SampleEvents = count() by TableName, ActionType, DeviceName, FileName, SHA1, InitiatingProcessFileName, InitiatingProcessSHA1, ProcessCommandLine, InitiatingProcessCommandLine, ProcessId, InitiatingProcessId
) on TableName, ActionType, DeviceName, FileName, SHA1, InitiatingProcessFileName, InitiatingProcessSHA1
| project TableName, ActionType, DeviceName, FileName, SHA1, InitiatingProcessFileName, InitiatingProcessSHA1, CurrentCount, BaselineCount, AnomalyRatio = round(NormalizedRatio, 2), SampleEventCount = SampleEvents, ProcessCo
| order by AnomalyRatio desc
| where CurrentCount >= min_current_events and AnomalyRatio >= min_anomaly_ratio

```

2 items 00:01.400 Low

TableName	ActionType	DeviceName	FileName	SHA1	InitiatingProcessFileName	InitiatingProcessSHA1	CurrentCount	BaselineCount	AnomalyRatio
DeviceNetworkEve...	ConnectionSuccess	cupcake					1000	4	10250.0
DeviceEvents	LdapSearch	cupcake			bamboozledr.exe	be4e21bf2c6c1d89e6...	1000	0	999.0

WHAT CAN AN ATTACKER DO WITH THIS ?

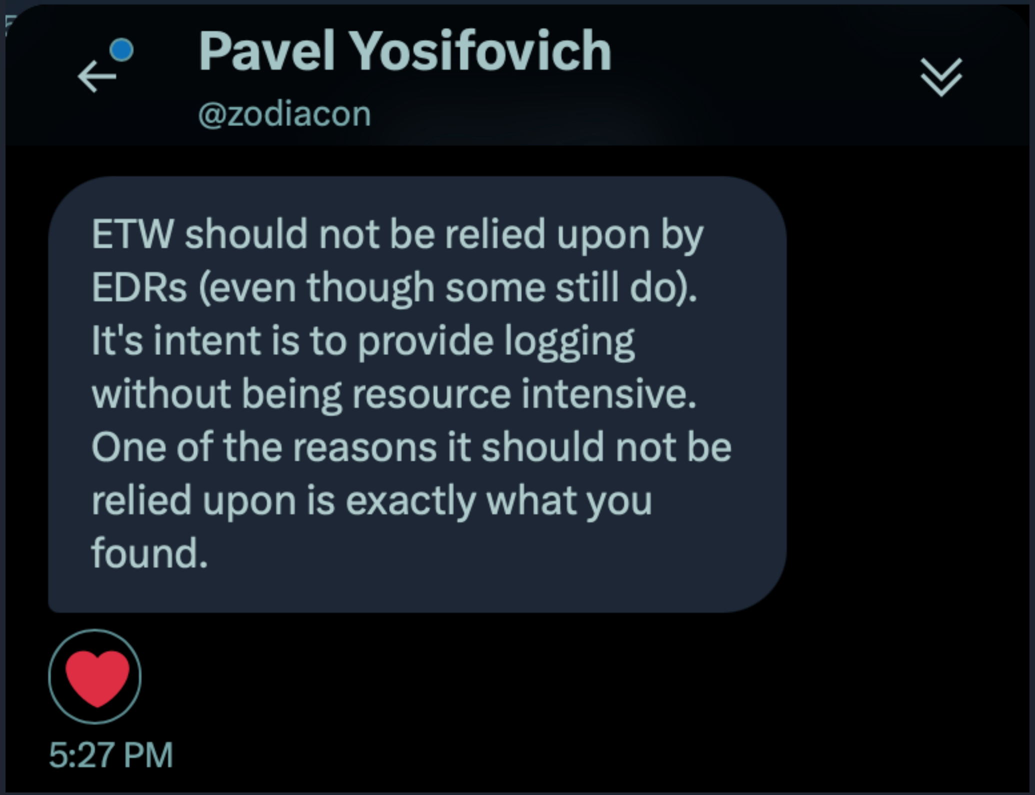
- □ Emit enough events to exceed the event cap, per provider which resets every 24h
- □ With admin permissions, subscribe to all providers the EDR uses, flood the session to make it blind until a reboot
- □ Emit fake events or alerts to set the defenders on a wild goose chase
- □ Get users or devices disconnected of the network when the right conditional access policies are in place
- □ Exhaust the amount of trace sessions or modify existing ones

LOG FICTION

Image by @KoosGoossens

SORRY

- You can't fully trust your logs anymore.
- Be mindful of the origin of your telemetry and if/how an attacker can tamper with this. Consider what the potential impact will be.
- These events are super valuable for detection and are often not easily collected in another way.
- It stands to reason EDR vendors make use of it. The current security model however does it make it untrustworthy.



Pavel Yosifovich

@zodiacon

ETW should not be relied upon by EDRs (even though some still do). It's intent is to provide logging without being resource intensive. One of the reasons it should not be relied upon is exactly what you found.

5:27 PM

BUT WAIT, THERE IS MORE

My next talk will cover parallel research where we were able to reverse engineer the MDE C2 communication protocols.

We've created PoltEDRgeist.

A tool to onboard (unlimited) fake devices into any MDE tenant with any details you want. This includes sending logs and spoofing computer and usernames, making it almost impossible to distinguish from the legitimate entities.

This method does not require any machine access to execute code on, so no complicated ETW events.

THIS RESEARCH HAS NOT BEEN POSSIBLE WITHOUT

@mattifestation / Matt Graeber- for his blogs on Trace Sessions and ETW tampering

@zodiacon /Pavel Yosifovich – for all his shared knowledge, tools and contributions to the Windows Internals books

@JonnyJohnson_ for listening to my failure stories and his ETW knowledge

@yardenshafir for helping me confirm some theories

@falconforceteam for their continued support

Geoff Chappell for his super useful windows internals website

ALL MY ETW TOOLS

PockETWatcher – Lightweight ETW consumer
https://github.com/olafhartong/PockETWatcher

ETWhat – Provider mode enumeration tool
https://github.com/olafhartong/ETWhat

ETWLocksmith – Provider security analyzer
https://github.com/olafhartong/ETWLocksmith

autologgerAnalyzer – Autologger details
https://github.com/olafhartong/autologgerAnalyzer

ETWtop – Session performance monitoring
https://github.com/olafhartong/ETWtop

BamboozlEDR – ETW event emitting and BOFs
https://github.com/olafhartong/BamboozlEDR

THANK YOU!

Together. Secure. Today.

olaf@falconforce.nl

https://falconforce.nl

@olafhartong
@falconforceteam

https://linkedin.com/in/olafhartong
https://linkedin.com/company/falconforce