Bundesamt
für Sicherheit in der
Informationstechnik

The Anatomy of Windows Telemetry Pt. II

Maximilian Winkler, Dominik Phillips, Tillmann Osswald

Bundesamt
für Sicherheit in der
Informationstechnik

Agenda

Introduction
Preparation
Data Analysis
Final Remarks

ERNW
providing security.

Bundesamt
für Sicherheit in der
Informationstechnik

Introduction

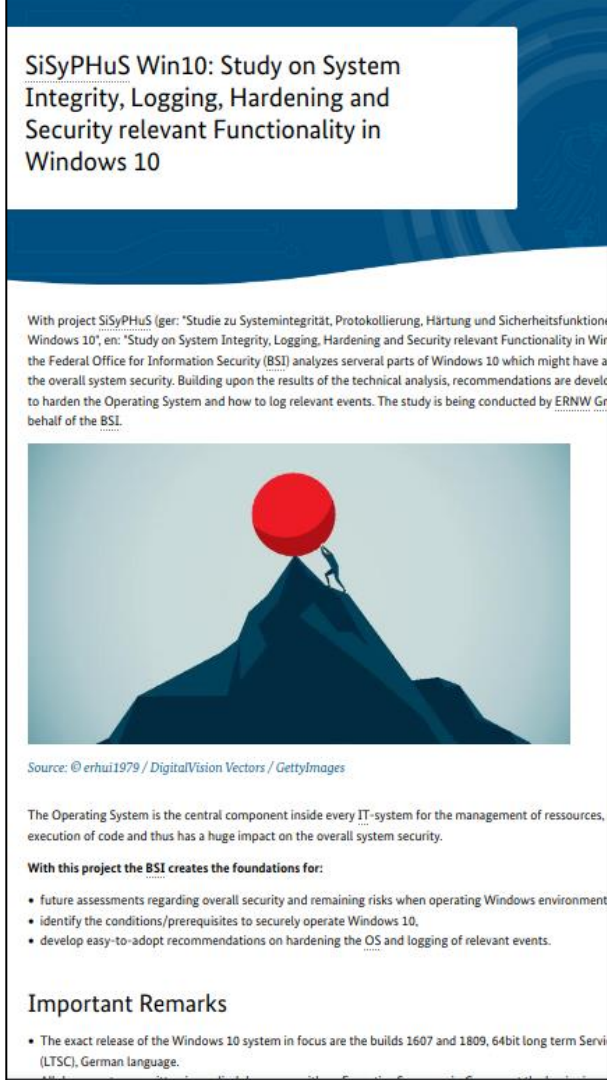
ERNW providing security.

Bundesamt für Sicherheit in der Informationstechnik

SiSyPHuS Win10

- Set up by the BSI in 2017
- Analysis done by ERNW – System Analysis Group
- 24+ work packages
- https://www.bsi.bund.de/EN/Service-Navi/Publikationen/Studien/SiSyPHuS_Win10/SiSyPHuS.html

- Several work packages focus on telemetry or underlying infrastructure
  - Telemetry Service
  - Delta Analysis – Evolution of the telemetry service in Windows 10, LTSC 2019
  - ETW Monitoring Methodology
  - Telemetry Monitoring Framework (SAM tool)
  - Telemetry Deactivation



SiSyPHuS Win10: Study on System Integrity, Logging, Hardening and Security relevant Functionality in Windows 10

With project SiSyPHuS (ger: "Studie zu Systemintegrität, Protokollierung, Härtung und Sicherheitsfunktione
Windows 10", en: "Study on System Integrity, Logging, Hardening and Security relevant Functionality in Wir
the Federal Office for Information Security (BSI) analyzes serveral parts of Windows 10 which might have a
the overall system security. Building upon the results of the technical analysis, recommendations are develo
to harden the Operating System and how to log relevant events. The study is being conducted by ERNW Gr
behalf of the BSI.

Source: © erhui1979 / DigitalVision Vectors / GettyImages

The Operating System is the central component inside every IT-system for the management of ressources,
execution of code and thus has a huge impact on the overall system security.

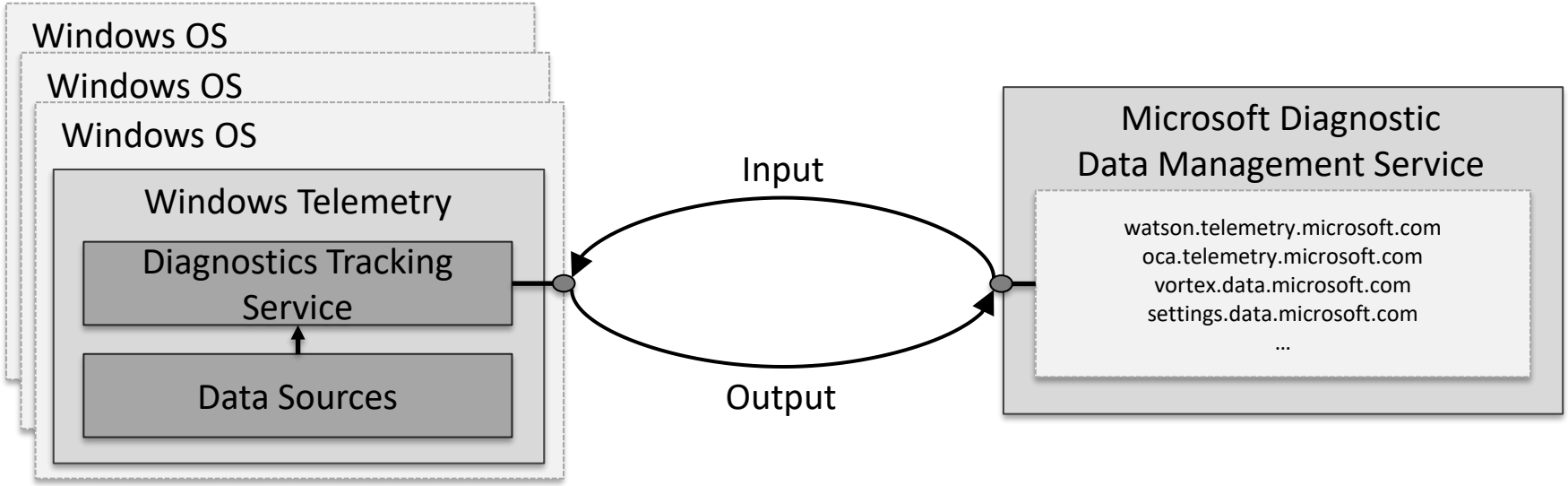
With this project the BSI creates the foundations for:

- future assessments regarding overall security and remaining risks when operating Windows environment
- identify the conditions/prerequisites to securely operate Windows 10,
- develop easy-to-adopt recommendations on hardening the OS and logging of relevant events.

Important Remarks

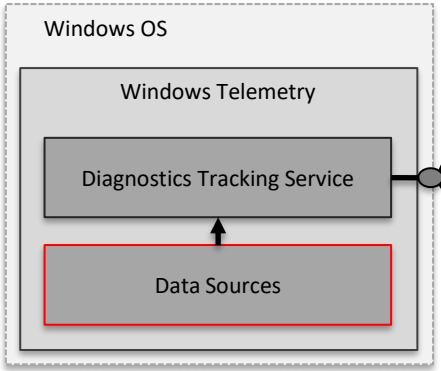
- The exact release of the Windows 10 system in focus are the builds 1607 and 1809, 64bit long term Servi
(LTSC), German language.

Windows Telemetry: Architecture



- Primary data source: *Event tracing for Windows* (ETW)
- Secondary data source: Executables and API functions

Windows Telemetry: Mission



- Network Interface
  - HTTP and compressed messages
  - TLS-secured network interface.
  - Certificate pinning.
    - Verifies the public key of the root certificate against a hash (hardcoded in crypt32.dll) of the "Microsoft Root Certificate Authority 2011" public key.
    - Can be disabled by adjusting the registry value at HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\DiagTrack\TestHooks\SkipMicrosoftRootCertCheck to 0x1.

- **How can we – with little effort – monitor telemetry data?**
  - Primary data source: *Event tracing for Windows* (ETW)

ERNW
providing security.

Bundesamt
für Sicherheit in der
Informationstechnik

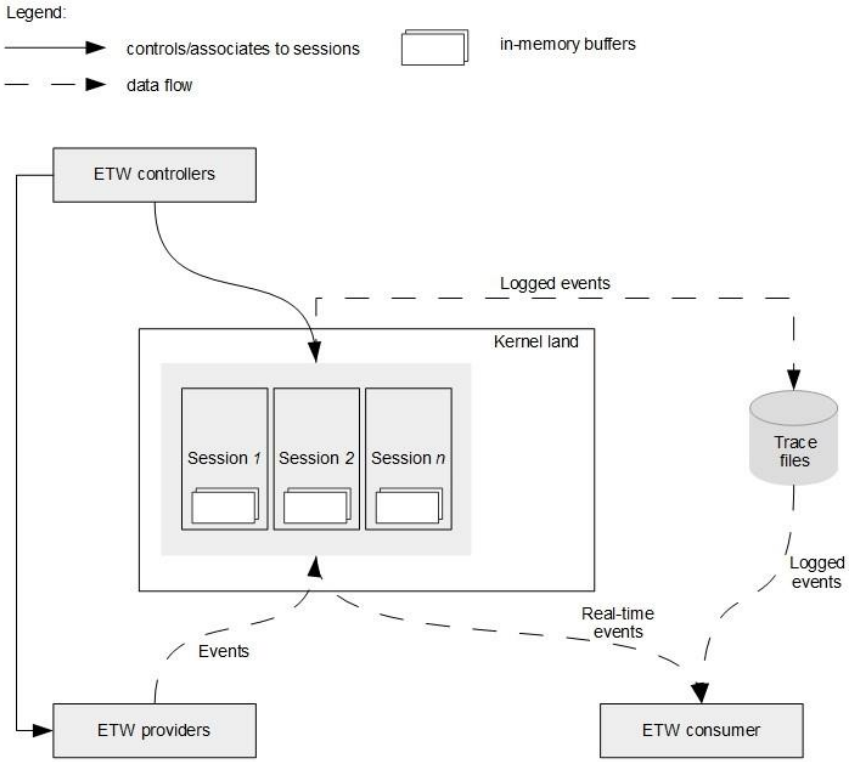
Preparation

Why not use what MS uses? -> ETW

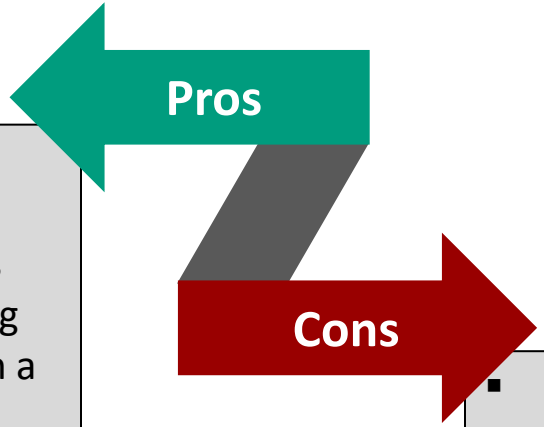
- Microsoft incorporates comprehensive ETW based tracing properties into their code.

- ETW is a tracing facility enabling tracing of both user-land and kernel-land activities.

- The core building blocks of ETW are:
  - Providers, Controllers, and Collectors



Pros and Cons



- Efficient and dependable data processing
- A well-defined architecture forms the foundation for data processing
- Data is collected and processed in a standardized format, ensuring consistency and compatibility

- Restrictions on the developer's tracing preferences
- Uncertainty regarding the potential data records that may emerge
- Significant effort required to assess the suitability of a measurement point for a specific scenario

ERNW providing security.

Bundesamt für Sicherheit in der Informationstechnik

Challenges

The advantages are essentially on the operation side. However, to fully utilize them, you need the right tools.

The main disadvantages lie in the identification and evaluation of the correct ETW providers:

- How do we even identify providers?
- How do we know what data a provider records?
- How do we ensure that the record reflects the desired activity?

Discover Providers (1)

In order to discover ETW providers there are numerus tools available.

- logman, xperf, wpr ….

Regardless of the tool in use they discover providers based on:

- Information stored on the system (install time)

or

- Information provided by ETW (runtime)

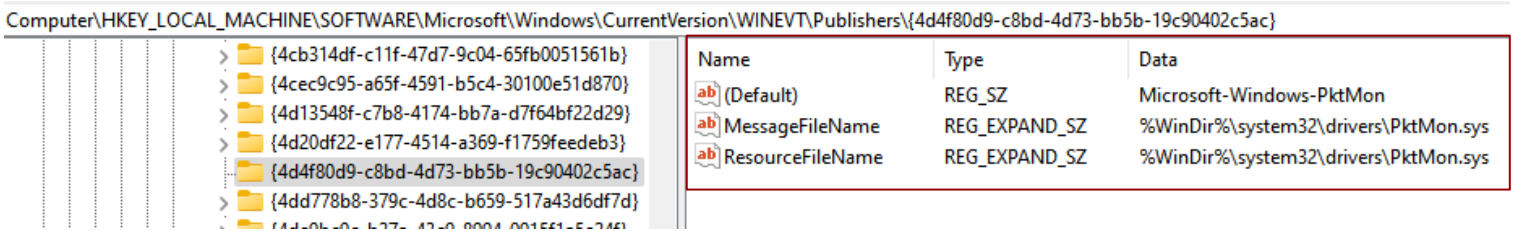
```
PS C:\Users\dphillips> xperf.exe -providers I R

Known User Mode Providers:
        0063715b-eeda-4007-9429-ad526f62696e             : Microsoft-Windows-Services
        0075e1ab-e1d1-5d1f-35f5-da36fb4f41b1             : Microsoft-Windows-Network-ExecutionContext
        00b7e1df-b469-4c69-9c41-53a6576e3dad             : Microsoft-Windows-Security-IdentityStore
        01090065-b467-4503-9b28-533766761087             : Microsoft-Windows-ParentalControls
        014de49f-ce63-4779-ba2b-d616f6963a87             : Microsoft-Windows-NetworkConnectivityStatus
        01578f96-c270-4602-ade0-578d9c29fc0c             : Microsoft-Windows-VAN
[...]

Registered User Mode Providers:
        38ed3633-5e3f-5989-bf25-f0b1b3318c9b
        087e0a2d-9ea8-40aa-aa54-fa5aef34bf3d
        dfba1e0c-6d07-4b8a-8175-3e320a16f3f8
        273c19b2-6643-5a58-6288-c336d3688b8d
        56c06166-2e2e-5f4d-7ff3-74f4b78c87d6
        Microsoft-Windows-Direct3DShaderCache
[...]
```

How do we know where the ETW provider is implemented?

Discover Providers (2)

Provider information stored on the system (install time)

- **HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Publishers**



ERNW providing security.

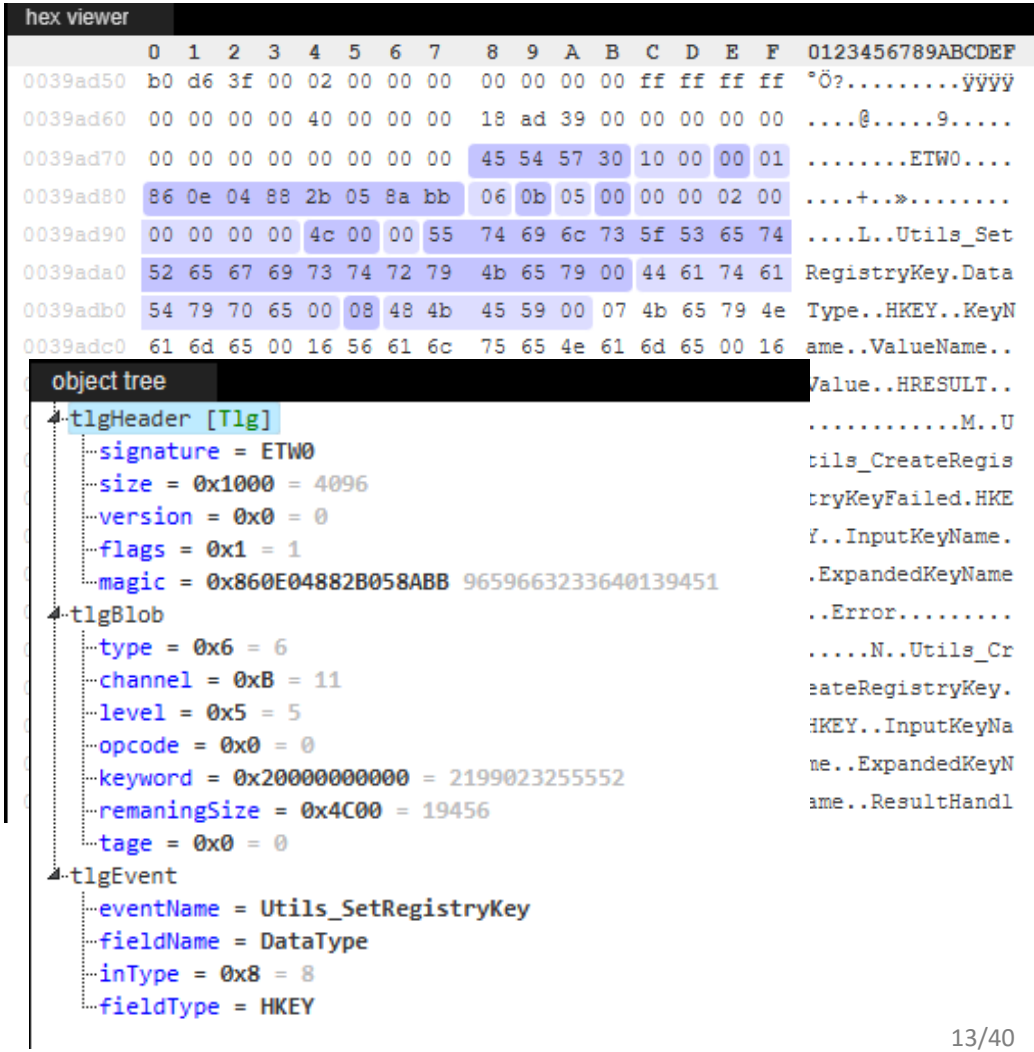
Bundesamt für Sicherheit in der Informationstechnik

Discover Providers (3)

- Search for ETW provider metadata artefacts.

- The advantage is that you are independent of installation or runtime information.
  - At this point we need provider-specific context information.

Tools:
- etw_discover.exe (developed during project)
- TLGMetadataParser.psm1 (Matt Graeber)



Discover Providers: Result (1)

The result at this point is ETW provider specific metadata.

Diagtrack.dll ETW provider statistics	
Number of providers types	2
Number of providers	11
Number of records	> 1000

Name	Type
Microsoft-Windows-UniversalTelemetryClient	wevt
Microsoft.Windows.DeviceDelete	tlg
Microsoft.Windows.DiagTrack	tlg
Microsoft.Windows.DiagTrack.XML	tlg
Microsoft.Windows.Sentinels	tlg
Microsoft.Windows.TelemetryViewer	tlg
Microsoft.Windows.Utc.ReentrancyTest	tlg
Microsoft.Windows.Utc.WatchdogProvider	tlg
Microsoft.Windows.WindowsErrorReporting	tlg
TelClientSyntheticAggregation	tlg
UtcTelemetryAssertDump	tlg

ERNW providing security.

Bundesamt für Sicherheit in der Informationstechnik

Discover Providers: Result (2)

At this stage, we have only metadata.

In order to achieve a more precise specification of the dataset - **concrete data** - we must either:

- conduct a brief test

  or

- perform static and dynamic analysis


```
{
    "Channel": 11,
    "Level": 5,
    "RecordName": "AsimovUploader_PersistEvent",
    "Version": 0,
    "Opcode": 0,
    "Keyword": "0x400001003",
    "Id": 0,
    "FieldList": [
        {
            "FieldName": "EventPayload",
            "TlgOut": "UTF8",
            "TlgIn": "ANSISTRING"
        },
        {
            "FieldName": "EventSizeBytes",
            "TlgOut": "UINT64",
            "TlgIn": "UINT64"
        },
        {
            "FieldName": "EventPersistence",
```

ERNW providing security.

Bundesamt für Sicherheit in der Informationstechnik

AsimovUploader_PersistEvent

```
"RecordName": "AsimovUploader_PersistEvent",
"FieldName": "EventPayload", "TlgOut": "UTF8"
"FieldName": "EventSizeBytes", "TlgOut": "UINT64"
```

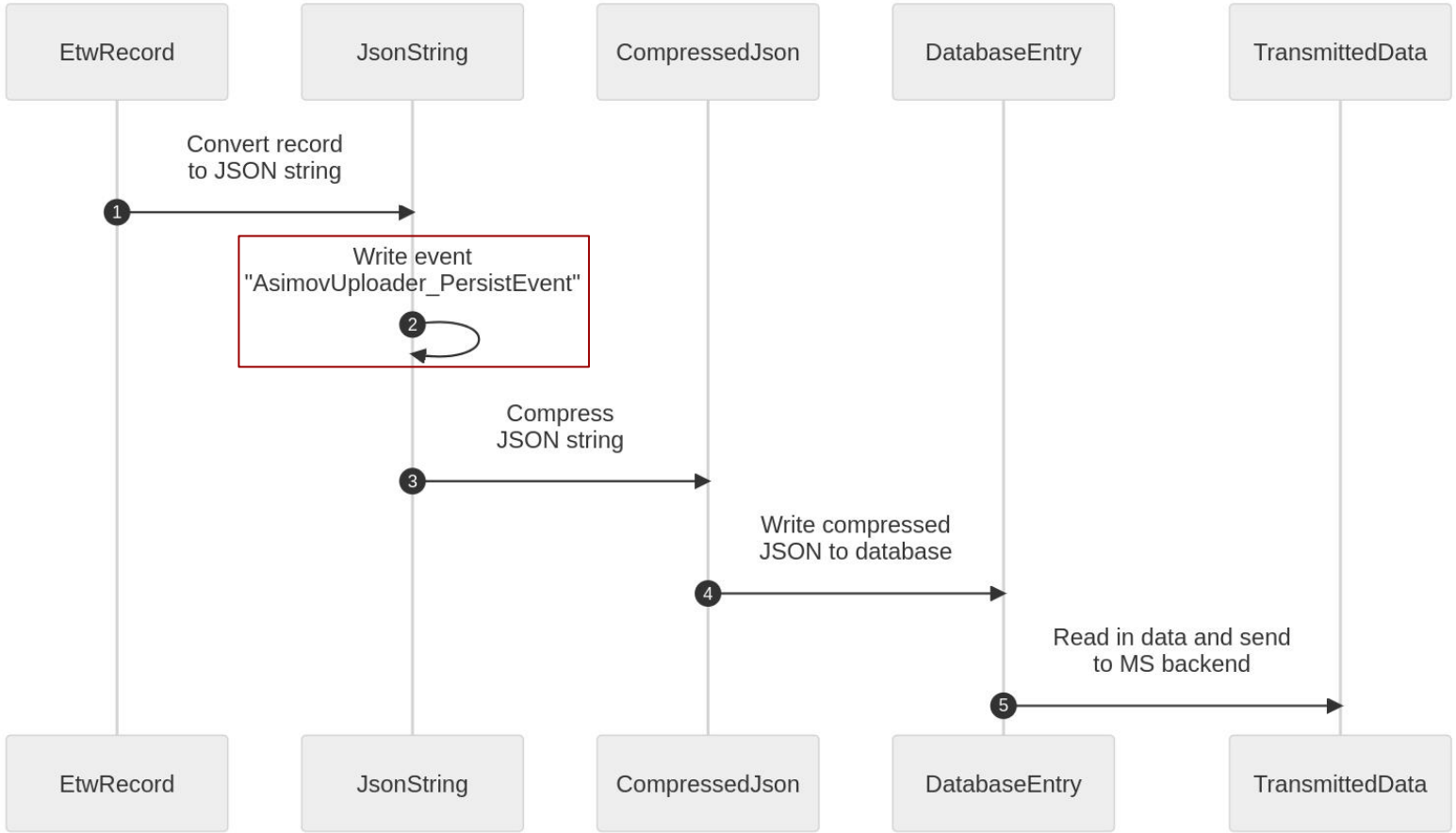

```
{"ver":"4.0","name":"SoftwareUpdateClientTelemetry.CheckForUpdates","time":"2023-06-
12T13:43:05.9244741Z","iKey":"o:0a89d516ae714e01ae89c96d185e9ae3","ext":{"utc":{"eventFlags":514,"p
gName":"WINCORE","flags":1040187908,"epoch":"3105055","seq":816},"metadata":{"f":{"EventInstanceID"
:8,"ServiceGuid":8,"QualityUpdatePause":2,"FeatureUpdatePause":2,"StatusCode":2,"ExtendedStatusCode
":2,"ActivityMatchingId":8,"SyncType":2,"IPVersion":2,"NumberOfApplicationsCategoryScanEvaluated":2
,"ScanDurationInSeconds":2,"ScanEnqueueTime":2,"NumberOfLoop":2,"NumberOfUpdatesEvaluated":2,"Numbe
rOfNewUpdatesFromServiceSync":2,"MetadataIntegrityMode":2,"NumberOfApplicableUpdates":2,"DeferralPo
licySources":2,"QualityUpdateDeferral":2,"FeatureUpdateDeferral":2,"DriverExclusionPolicy":2}},"msc
v":{"cV":"gbZAehkywUexPWbS4YZmYA.130.4.1.0.0.4.0"},"os":{"bootId":27,"name":"Windows","ver":"10.0.1
9045.2965.amd64fre.vb_release.191206-
```

Record Verification: Example

To ensure that the record reflects the desired activity, we need to perform static and dynamic analysis.

```
Microsoft::Diagnostics::EtwSession::StartConsumingForwarder()
{
  [...]
  status = EnableTraceEx2(traceHandle, &ProviderId, 1u, level,
MatchAnyKeyWord, 0, 0, &EnableParameters);
  [...]
  _tlgWriteTemplate<[...]>(
    tlgProviderHandle,
    eventSessionProviderBlob,
    [...]
    sessionName,
    &providerId,
    &isGroup,
    &keywordsBeforeIndividualEventRules,
    &finalKeywords,
    &level,
    &EnableParameters.EnableProperty,
    &status);
  [...]
}
```

Record Verification: AsimovUploader_PersistEvent



ERNW
providing security.

Bundesamt
für Sicherheit in der
Informationstechnik

Data Analysis

Data Analysis Setup

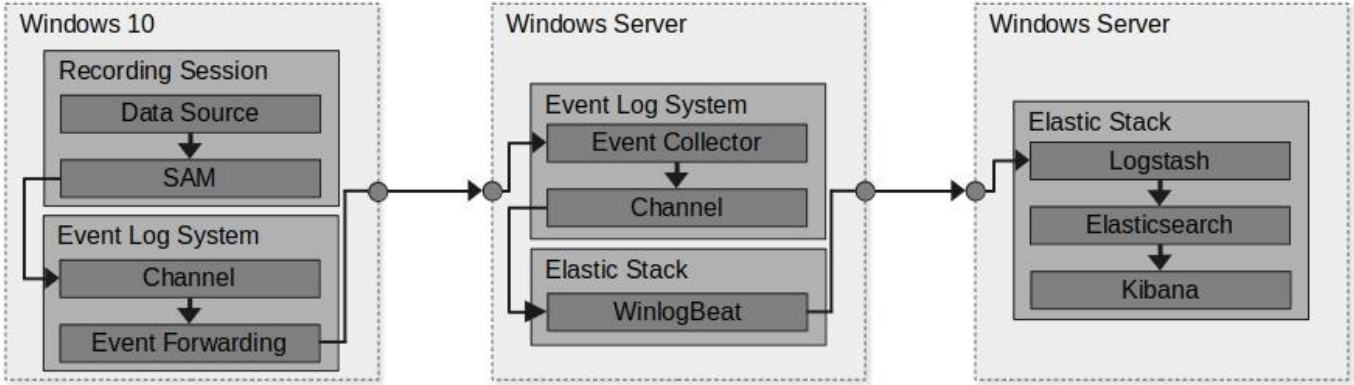
Considerable number of telemetry data:

- ~300k / week
- ~8k regarding transmitted telemetry
- With up to 800 records per minute for this record point

Data analysis requirements:

- Performance
- Search and filter
- Flexible data model
- Transferable to other research questions

Infrastructure



System Purpose	Windows system DiagTrack service SAM recording session.	Windows Server Windows Event Collector WinlogBeat components.	Windows Server Elastic Stack
Additional Configured and Installed Software	• Windows Event Forwarding • SAM (incl. corresponding recording profile)	• Windows Event Collector • WinlogBeat	• Logstash • Elasticsearch • Kibana

Telemetry Record: Header Section

```
{
    "ver": "4.0",
    "name": "Microsoft.Windows.Bluetooth.BthPort.LocalDriverInfo",
    "time": "2023-06-12T13:02:15.6087803Z",
    […]
    "ext": {
        […]
    },
    "data": {
        […]
    }
}
```

Telemetry Record: Extension Section

```
{
    ...
    "ext": {
        "os": { Windows Version, bootId },
        "device": { Device class (i.e., Desktop), and a Device GUID
},
        "app": { Application Information },
        "user": { A user GUID },
        ...
    },
    "data": { ... }
}
```

Telemetry Record: Data Section


```
{
    ...
    "ext": { ... },
    "data": {
        "DeviceExtensionSessionId": "01FCE708-9D2B-0000-0484-FF012B9DD901",
        "DriverDate": "2022-08-11T00:00:00.0000000Z",
        "DeviceInstallDate": "2023-05-12T05:20:48.8390000Z",
        "DriverVersion": "22.160.0.4",
        "DeviceInstanceId": "USB\\VID_8087&PID_0A2B\\5&12c8f4c0&0&2",
        "MatchingDeviceId": "USB\\VID_8087&PID_0A2B&REV_0010",
        "DriverDescription": "Intel(R) Wireless Bluetooth(R)",
        "DeviceManufacturer": "@oem4.inf,%company_name%;Intel Corporation",
        "DriverProvider": "Intel Corporation",
        "DriverInfPath": "oem4.inf",
        "DriverInfSection": "ibtusb",
        […]
    }
}
```

Telemetry Record: Types

Technical Data
- Recording of technical data

Activity Data
- Recording of activity a user performed on the system

Aggregated Data
- Aggregation and combination of records

Technical Data: Trace Route Information


```
{
    "data": {
        "experimentId": 0,
        "startTime": 1333104815625446l4,
        "networkType": "Ethernet",
        "destIP": "41.63.96.0",
        "hopInfoList": [
            { "IP": "185.144.92.0", "RTT"
            { "IP": "62.115.188.3", "RTT"
            […]
            { "IP": "62.115.58.203", "RTT"
            { "IP": "41.63.96.0", "RTT": 1
        ],
        "deviceProfile": 1114112
    }
}
```


IP range details

185.144.92.0/22

AS211417 · ERNW Enno Rey Netzwerke GmbH

IP address details

62.115.188.3

Frankfurt am Main, Hesse, Germany

Summary

ASN	AS1299 - Arelion Sweden AB
Hostname	pfalzkom-ic-353709.ip.twelve99-cust.net

Technical Data: Windows Defender


```
{
    "data": {
        "Count": 1,
        "SigSeq": 18144498279967,
        "SigName": "ALF:HeraklezEval:HackTool:Win32/Mimikatz.A!rfn",
        "Persist": false,
        "Cached": false,
        "FileSize": 1355680,
        "FileName": "mimikatz.exe",
        "ProductGuid": "77BDAF73-B396-481F-9042-AD358843EC24",
        "EngineVersion": "1.1.19000.8",
        […]
        "FeatureName": "Core",
        "FeatureScenario": "InternalSignatureMatch"
    }
}
```

Activity Data: Website Page Title


```
{
    "data": {
      "Timestamp": "2023-06-19T08:03:01.661Z",
      "app_version": "114.0.1823.43-64",
      "payload_id": 47244640259,
      "Channel": 4,
      "CorrelationGuid": "7da62b73-082f-4eb2-a370-135d0113e1dd",
      "EventInfo.Level": 2,
      "PageTitle": "SiSyPHuS AFUNKT - Search",
      "TabId": 830425073,
      "client_id": -7497793556371901000,
      "pop_sample": 100,
      "utc_flags": 140737488355328
    }
}
```

Activity Data: Website Navigation

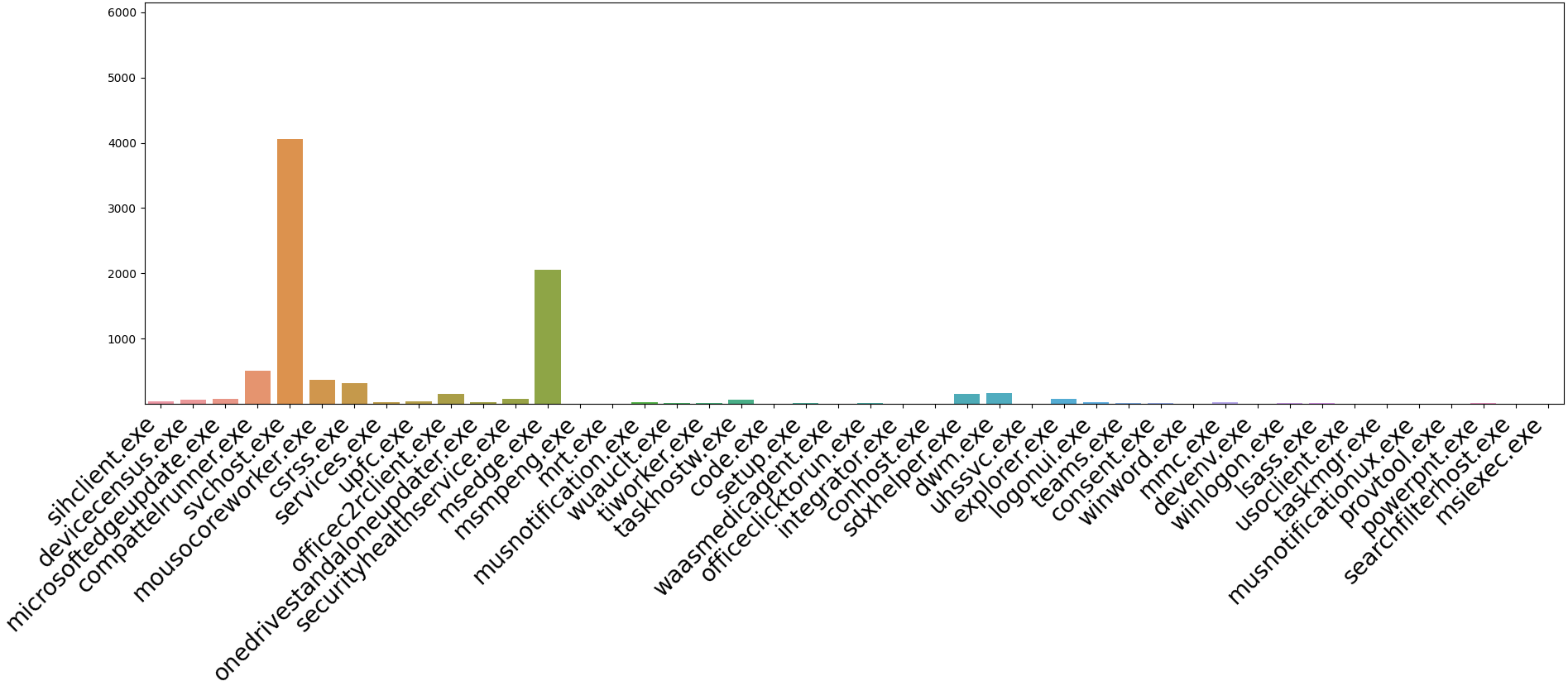

```
{
    "data": {
      "IsSameDocumentNavigation": 0,
      "client_id": -7497793556371901000,
      "navigationUrl": "https://www.bsi.bund.de/DE/Service-
Navi/Publikationen/Studien/SiSyPHuS_Win10/AFUNKT/SiSyPHuS_AFUNKT_node.html",
      "referUrl": "https://www.bing.com/",
      "HttpStatusCode": 200,
      "EventInfo.Level": 3,
      "TabId": 830425076,
      "referUrlRejectCode": 0,
      […]
}
```

Activity Data: Link Clicked

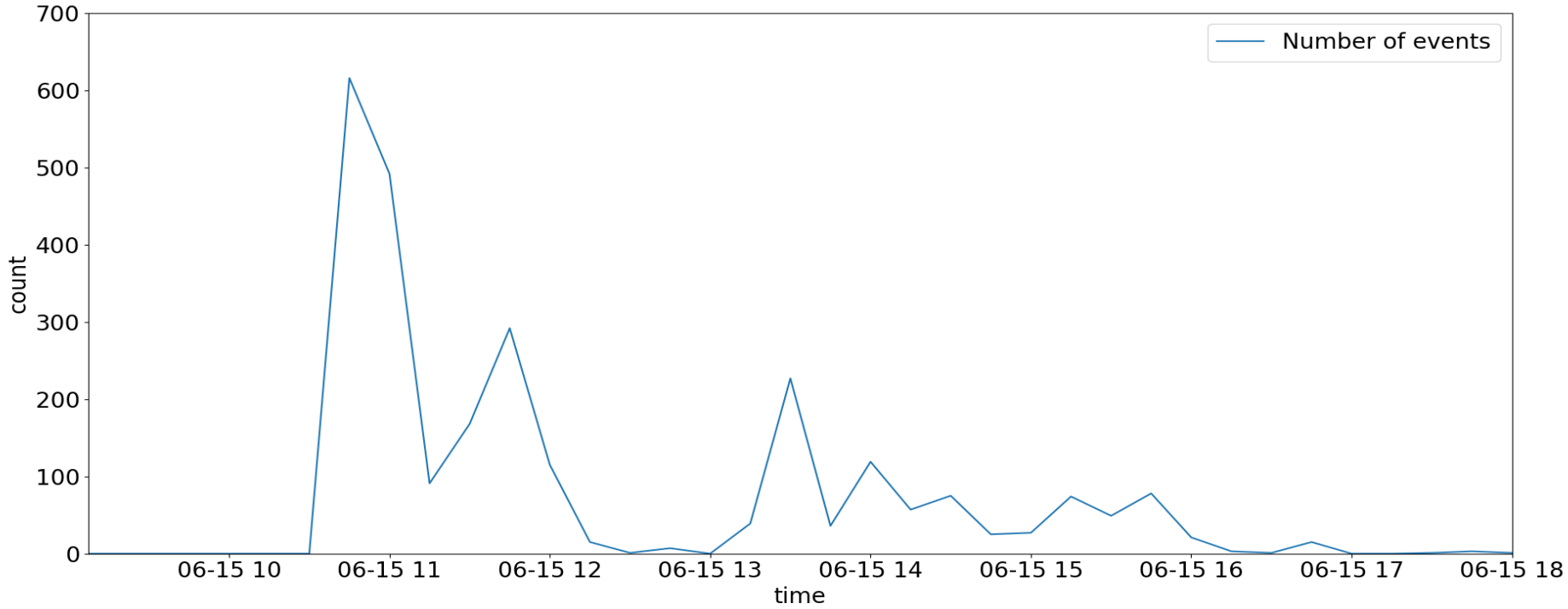

```
{
    "data": {
        "DOMElementPath": "A|1||c-link%20c-link--
download%20FTpdf;P|5[…]gsb%20lang-de%20fixed%20js-on;HTML|1||",
        "DOMAnchorHrefUrl":
"https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-
Sicherheit/SiSyPHus/AFUNKT.pdf?__blob=publicationFile&v=6",
    […]
    }
}
```

Activity Data: File Open


```
{
    "data": {
        "Channel": 4,
        "CorrelationGuid": "ebeb5485-4ab7-4ef2-b611-332a2c1f41eb",
        "LaunchSourceAppName": "explorer.exe",
        "RequestInitialUrl": "file:///C:/Users/ernw/Documents/AFUNKT.pdf",
        "Timestamp": "2023-06-19T08:13:15.838Z",
        […]
        "app_version": "114.0.1823.43-64",
        "client_id": -7497793556371901000,
        "utc_flags": 140737488355328
    }
}
```


6000
5000
4000
3000
2000
1000
sihclient.exe
devicecensus.exe
microsoftedgeupdate.exe
compattelrunner.exe
svchost.exe
mousocoreworker.exe
csrss.exe
services.exe
upfc.exe
officec2rclient.exe
onedrivestandaloneupdater.exe
securityhealthservice.exe
msedge.exe
msmpeng.exe
mrt.exe
musnotification.exe
wuauclt.exe
tiworker.exe
taskhostw.exe
code.exe
setup.exe
waasmedicagent.exe
officeclicktorun.exe
integrator.exe
conhost.exe
sdxhelper.exe
dwm.exe
uhssvc.exe
explorer.exe
logonui.exe
teams.exe
consent.exe
winword.exe
mmc.exe
devenv.exe
winlogon.exe
lsass.exe
usoclient.exe
taskmgr.exe
musnotificationux.exe
provtool.exe
powerpnt.exe
searchfilterhost.exe
msiexec.exe

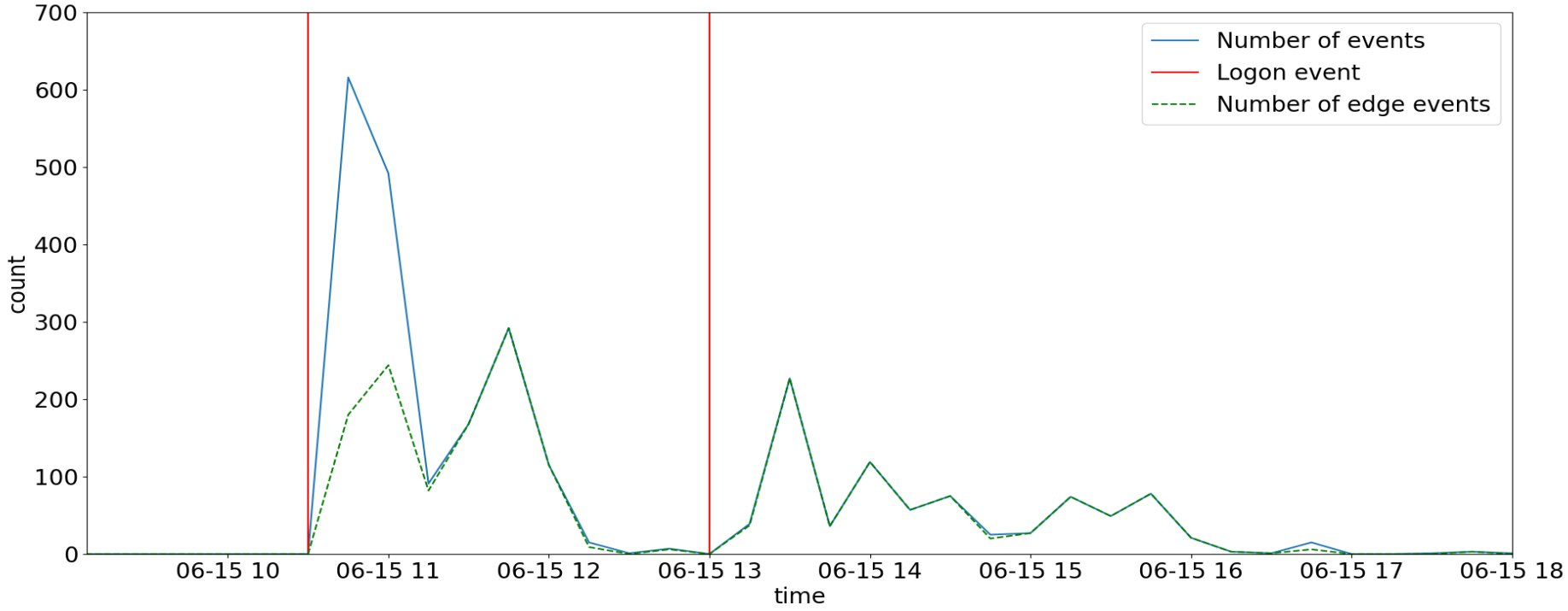
Correlation: Telemetry Records over Time



Correlation: User Login

```
{
  "name": "Microsoft.Windows.CredProvDataModel.SignedInCredProv",
  ...
  "ext": {
    "app": {
      "id": “...!logonui.exe“,
     […]
    }
  },
  "data": {
    "logonUiReason": 1,
    "credProvScenario": 0,
    "ntsStatus": -1073741715,
    "ntsSubstatus": 0,
    "credProviderGuid": "{60B78E88-EAD8-445C-9CFD-0B87F74EA6CD}",
    "userType": 1
  }
}
```

Correlation: User Activity Browsing



ERNW
providing security.

Bundesamt
für Sicherheit in der
Informationstechnik

Final Remarks

Informed Decision Making

In the end, it‘s about taking a decision.

A questionnaire-based approach could help:

1. Define some key questions
2. Answer the questions
3. Weight the answers
4. Take your decission – and justify

Telemetry Decision Bar

„telemetry is good“ **„telemetry is bad“**

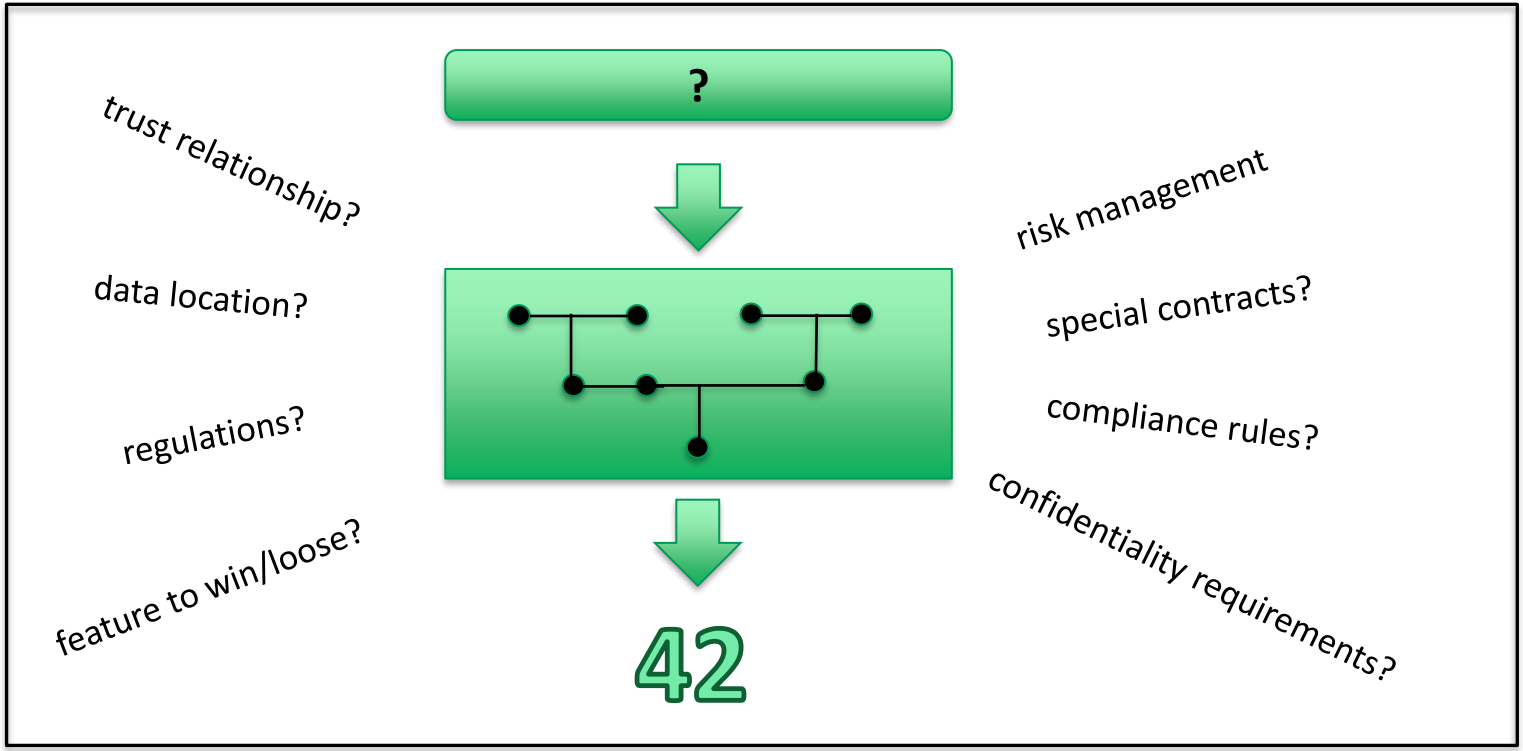
- It’s not black or white (or 0 or 1) in the end
- Sometimes telemetry could be required
- Usually there is at least some configuration possible, e.g. deactivate only browser events
- In these cases it might be helpful looking into the data
- There are cases when telemetry needs to be active, e.g. SAC

Why is Smart App Control turned off?

Smart App Control is only available on clean installs of Windows 11. Also, there are other reasons why Smart App Control could be turned off.

- You have optional diagnostic data in Windows turned off. If you want to turn Smart App Control on, you'll need to reset this PC, or reinstall Windows, and select **Send optional diagnostic data** during the setup process.

Questionnaire



ERNW providing security.

Bundesamt für Sicherheit in der Informationstechnik

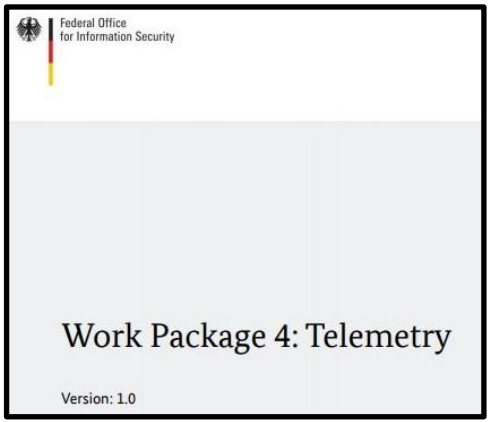
A Government Use Case Example

Trust relationship ?	→	US based vendor / under US regulation
Data location ?	→	Outside Germany
Regulations ?	→	GDPR, etc.
Features ?	→	N.A.
Special contracts ?	→	N.A.
Confidentiality requirements ?	→	Very strict
Compliance rules ?	→	E.g. restricted information handling directives

Thank you for your attention!
Questions?

Publications

https://tinyurl.com/WinTelWP4
https://tinyurl.com/WinTelAFUNKT
https://tinyurl.com/WinTelSAM



Contact

Dominik Phillips
dphillips@ernw.de
@0xdphillips__

Tillmann Osswald
tosswald@ernw.de
@_murks

Maximilian Winkler
bsi@bsi.bund.de