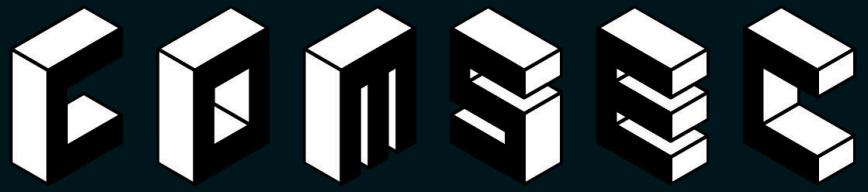
Efficient Pipelining for Windows Driver Vulnerability Research

Tobias Oberdörfer



Prof. Dr. Kaveh Razavi

InfoGuard
SWISS CYBER SECURITY

Luca Cappiello

Topic

Problem

Solution

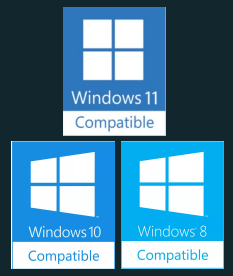
Results

Windows Kernel Driver Vulnerabilities

Privileged signed kernel drivers

Abusing | vulnerabilities

- Escalate Local Privilege
- Bypass Security Products
- Install Firmware Rootkits



Problem

Solution

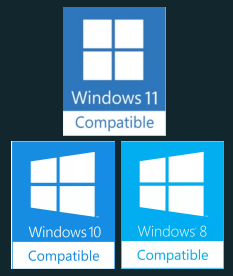
Results

Windows Kernel Driver Vulnerabilities

Privileged signed kernel drivers

Abusing | vulnerabilities

- Escalate Local Privilege
- Bypass Security Products
- Install Firmware Rootkits



Insufficient Auditing of Kernel Drivers

- Microsoft relying on third-parties

CROWDSTRIKE | BLOG

SCATTERED SPIDER Exploits Wi
Security Deficiencies with Bring-
Vulnerable-Driver Tactic in Attem
Bypass

January 10, 2023

DARKREADING

Kasseika Ransomware Linked to BlackMatter in BYOVD Attack

Elizabeth Montalbano, Contributing Writer
January 24, 2024

'Bring your own vulnera
becoming popular among threat actors

Solution

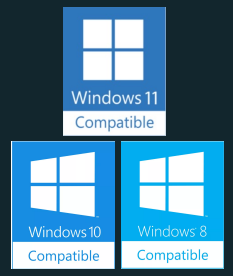
Results

Windows Kernel Driver Vulnerabilities

Privileged signed kernel drivers

Abusing | vulnerabilities

- Escalate Local Privilege
- Bypass Security Products
- Install Firmware Rootkits



Topic

Insufficient Auditing of Kernel Drivers

- Microsoft relying on third-parties
- No central repository
- Fast release cycle
- Missing ARM support

Problem

Solution

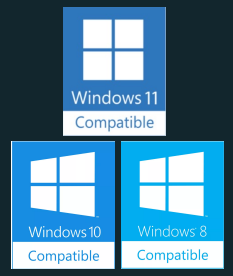
Results

Windows Kernel Driver Vulnerabilities

Privileged signed kernel drivers

Abusing | vulnerabilities

- Escalate Local Privilege
- Bypass Security Products
- Install Firmware Rootkits

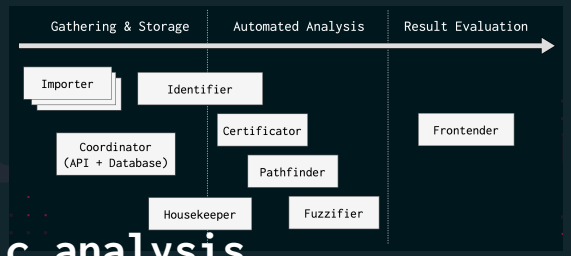


Insufficient Auditing of Kernel Drivers

- Microsoft relying on third-parties
- No central repository
- Fast release cycle
- Missing ARM support

Continuous Automated Driver Analysis

- Multi-source
- ARM support
- Automated
- Static & Dynamic analysis



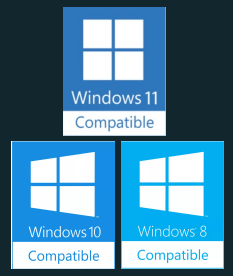
Results

Windows Kernel Driver Vulnerabilities

Privileged signed kernel drivers

Abusing | vulnerabilities

- Escalate Local Privilege
- Bypass Security Products
- Install Firmware Rootkits

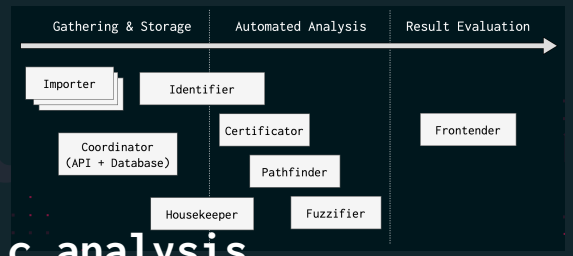


Insufficient Auditing of Kernel Drivers

- Microsoft relying on third-parties
- No central repository
- Fast release cycle
- Missing ARM support

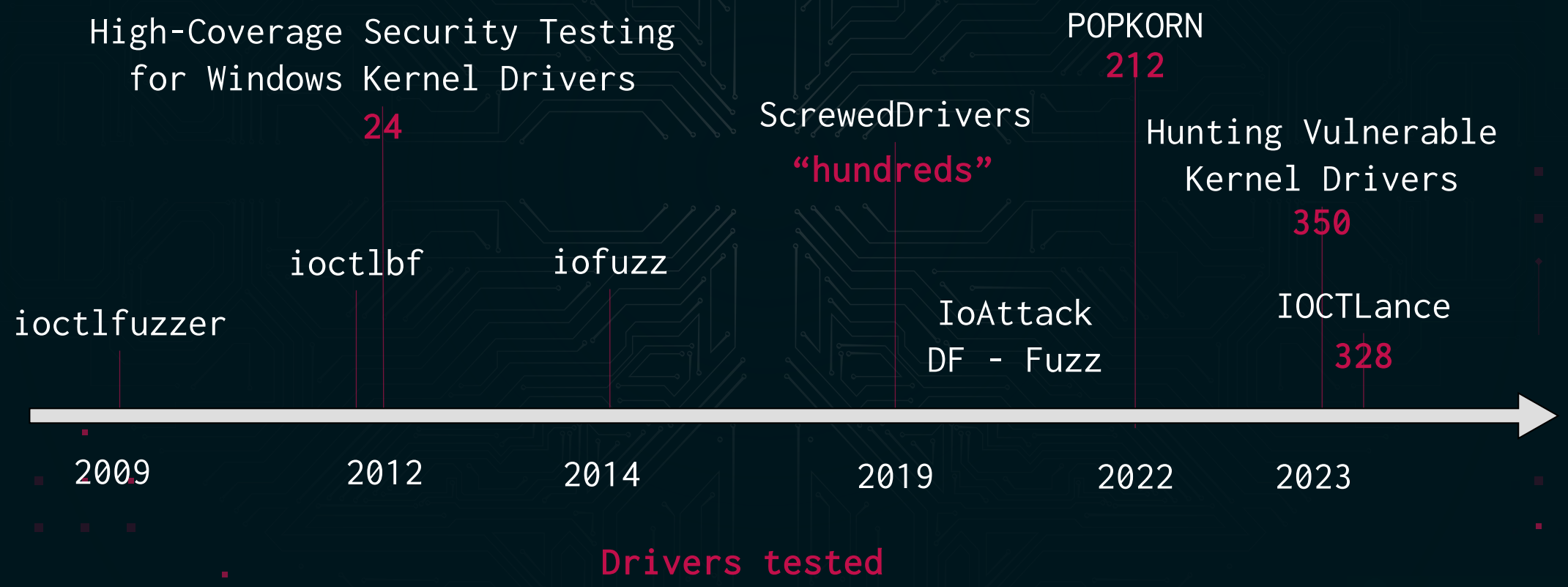
Continuous Automated Driver Analysis

- Multi-source
- ARM support
- Automated
- Static & Dynamic analysis



- Over 46’000 drivers gathered
  - ~27’000 automatically analysed
    - ~1’000 ARM drivers
- 10 new vulnerable drivers found

Timeline of existing work



Challenges for Automation

Gathering

- Non-existing central driver repository
- Continuous release of new drivers
- Varying distribution forms

Analysis

Architecture support

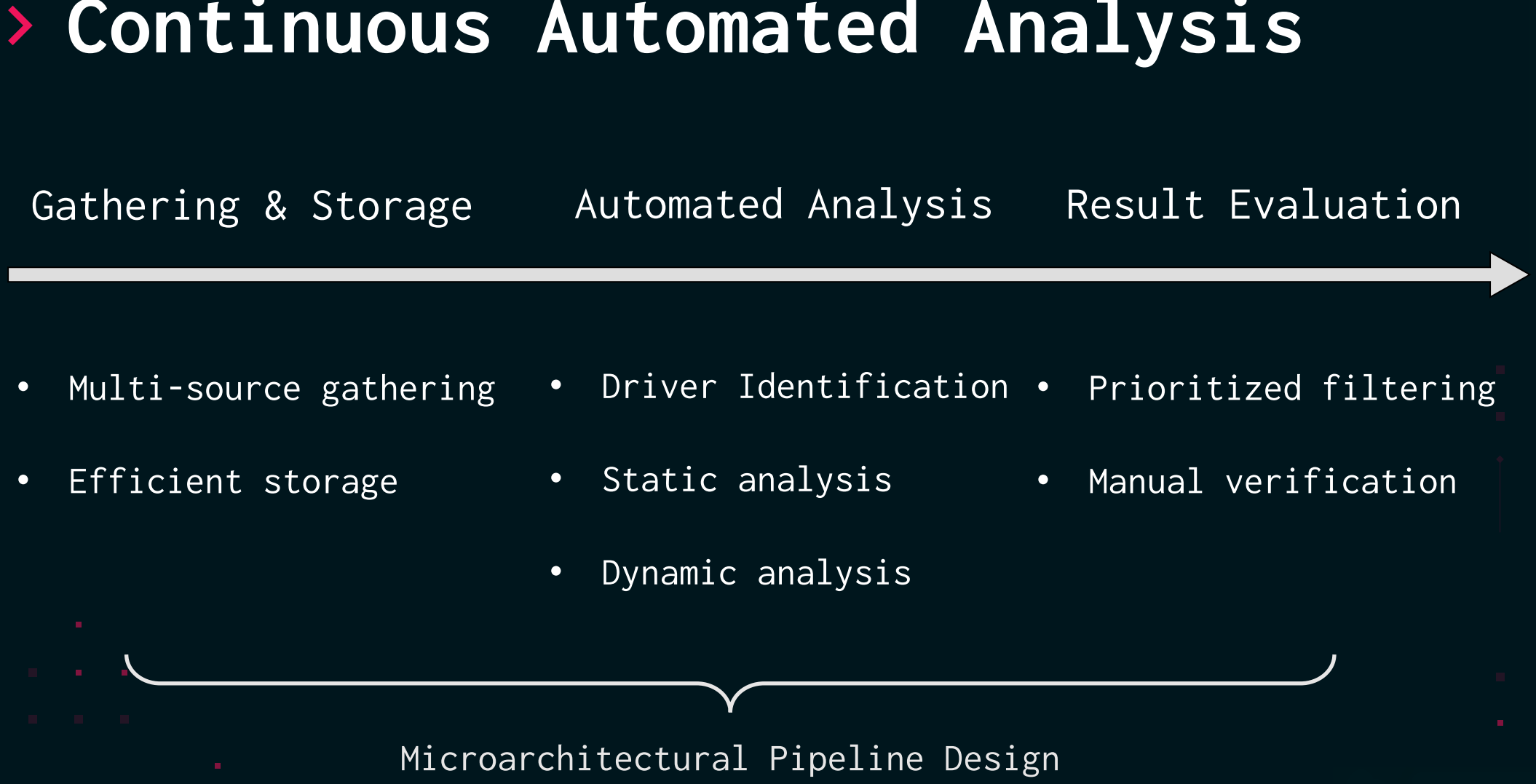
- Recent Windows ARM drivers

Automated Fuzzing

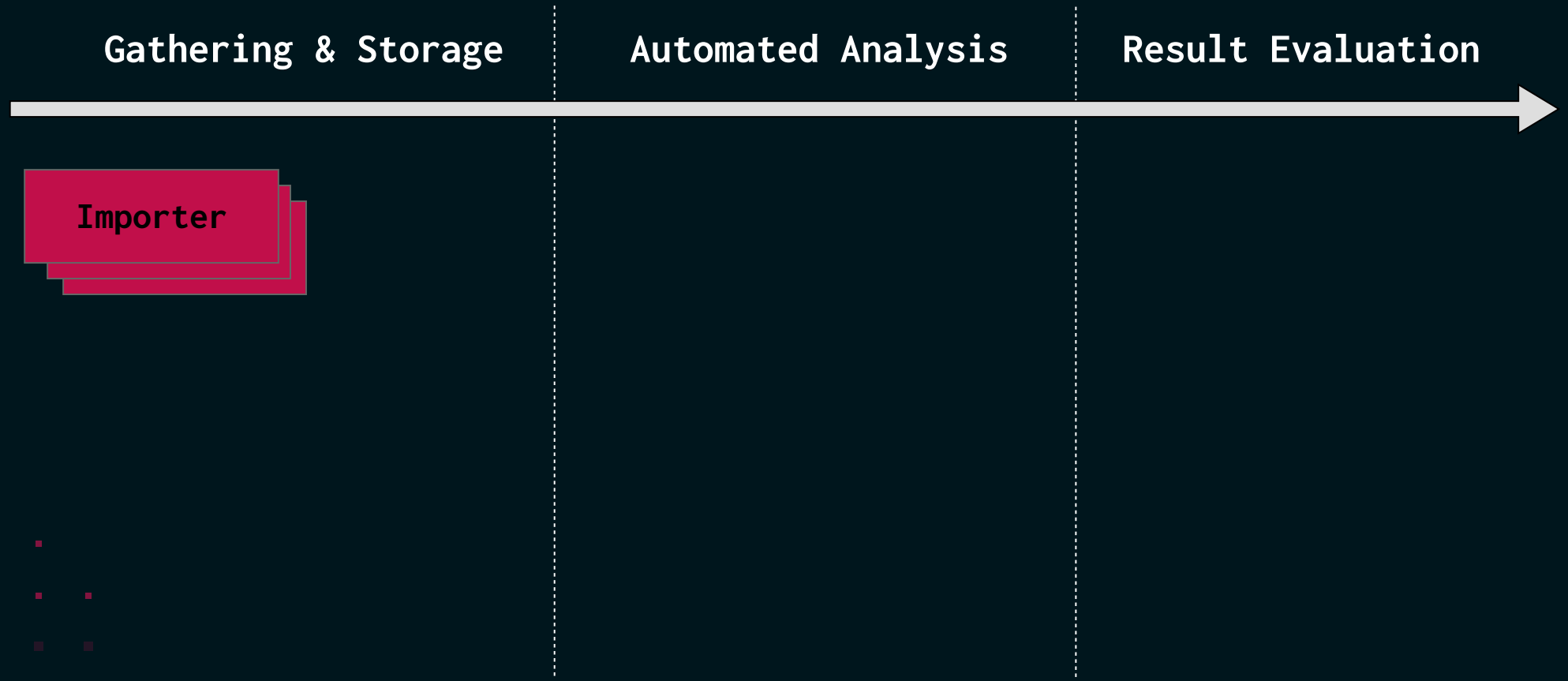
- Environment requirements
- Driver interaction complexity

Efficient Verification

Continuous Automated Analysis



File Importers



File Importers

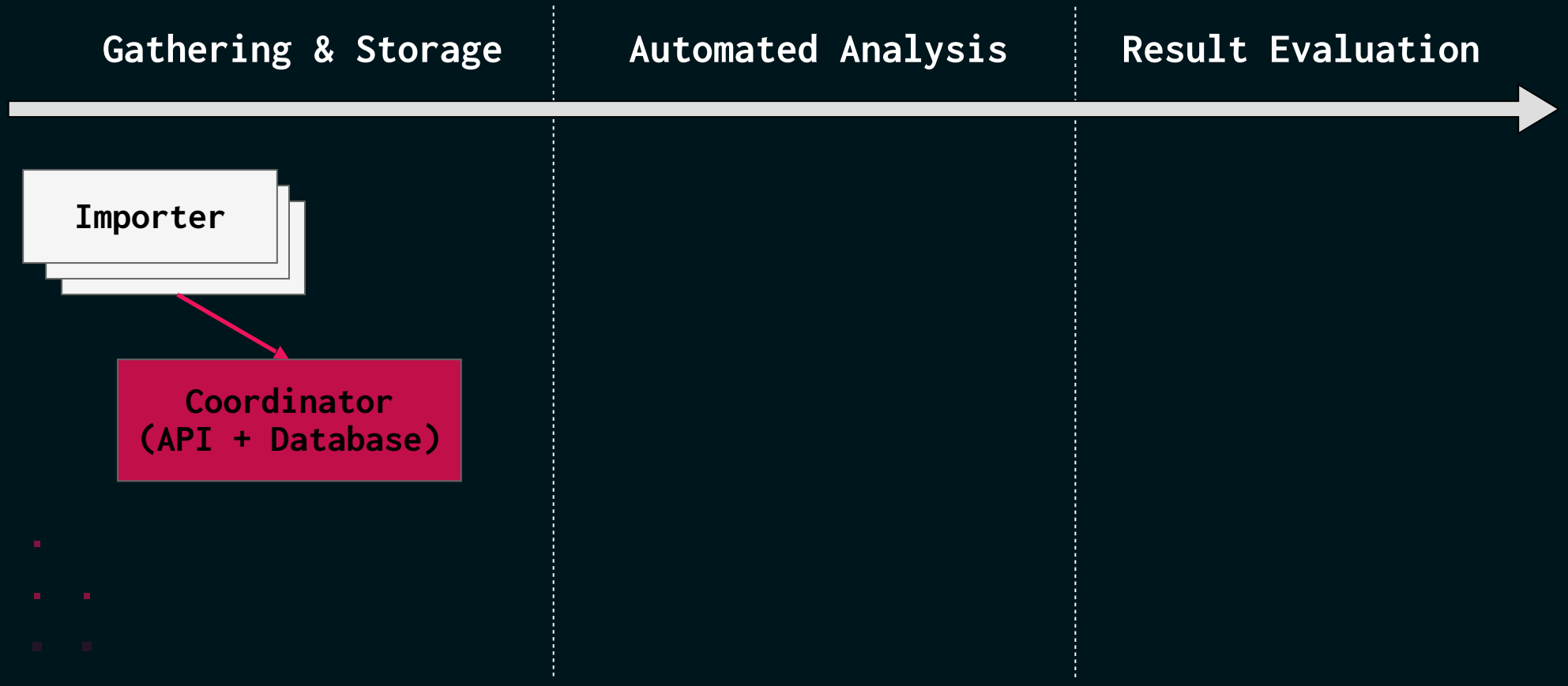
- Recursive Importer
  - Any files within a folder
- Cyber Defence Centre Importer
  - Microsoft XDR Queries in Client Networks
- Virus Total Importer
  - VT Intelligence Queries with filters

Partially Automated

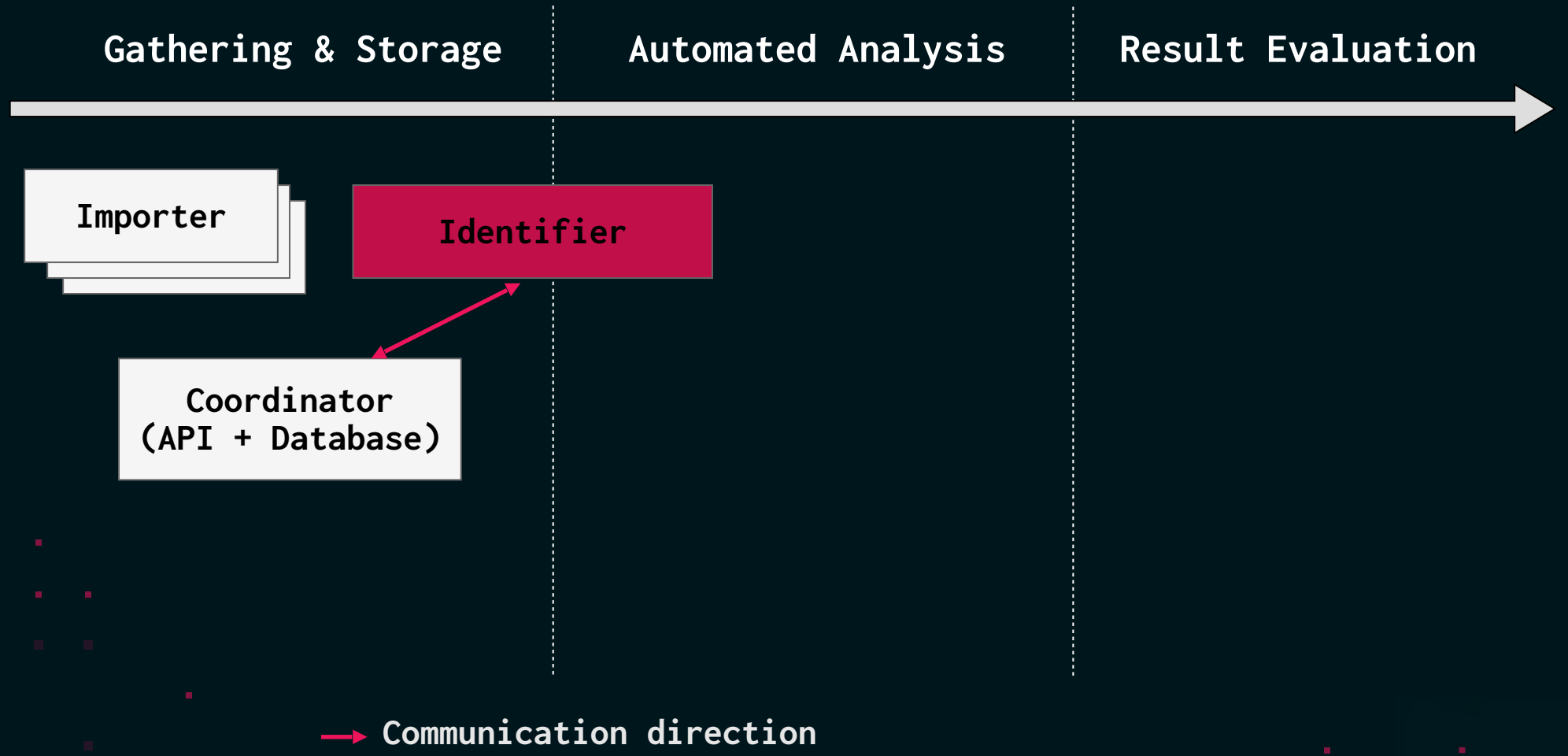
- Crawling Windows Update Catalog

Fully Automated

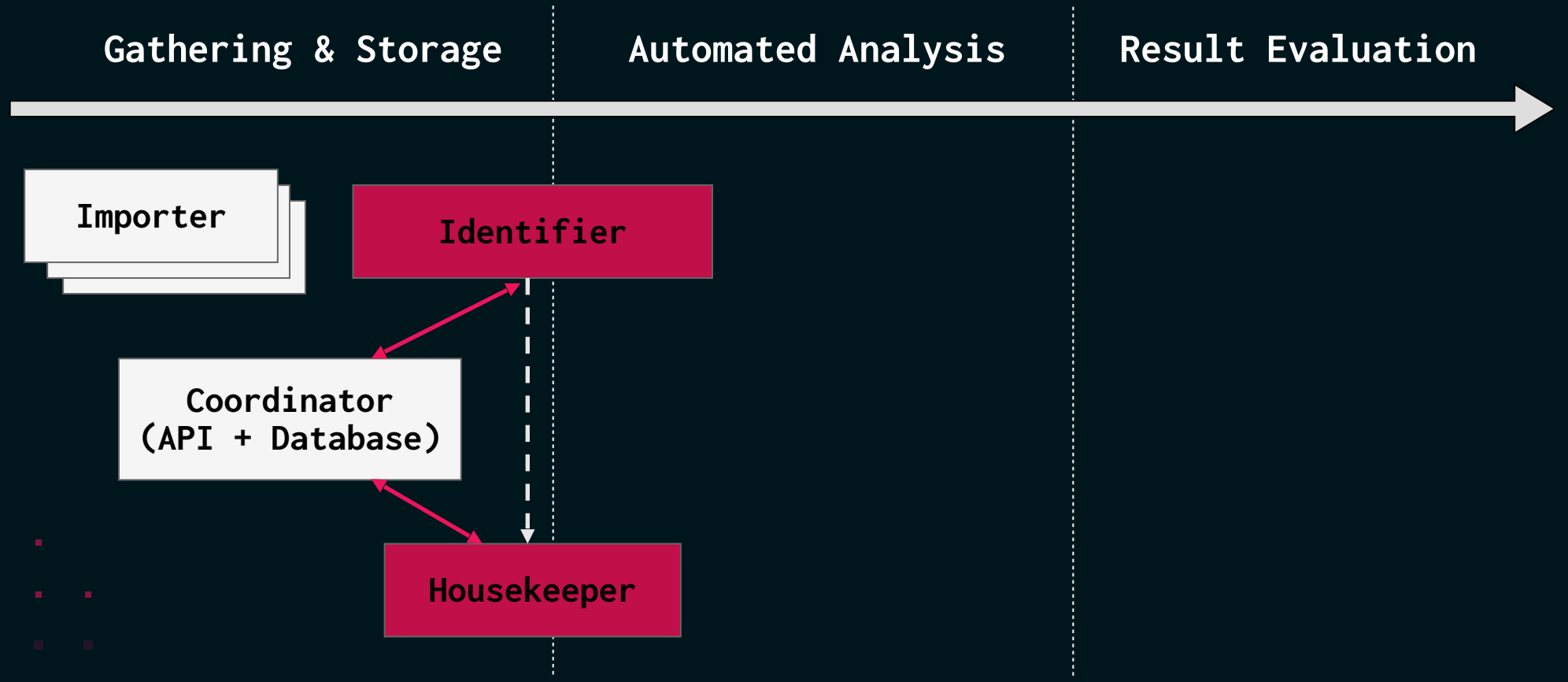
Coordinator



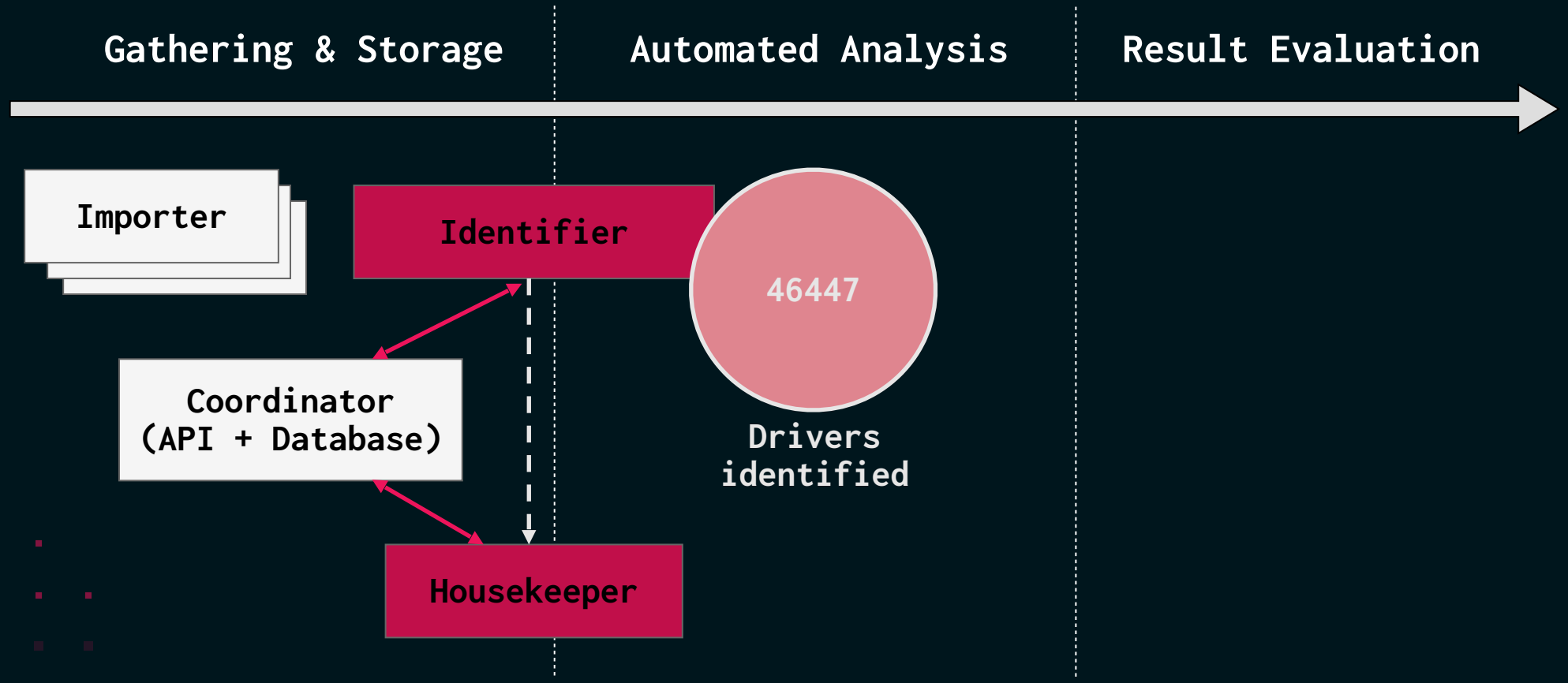
Identifier & Housekeeper



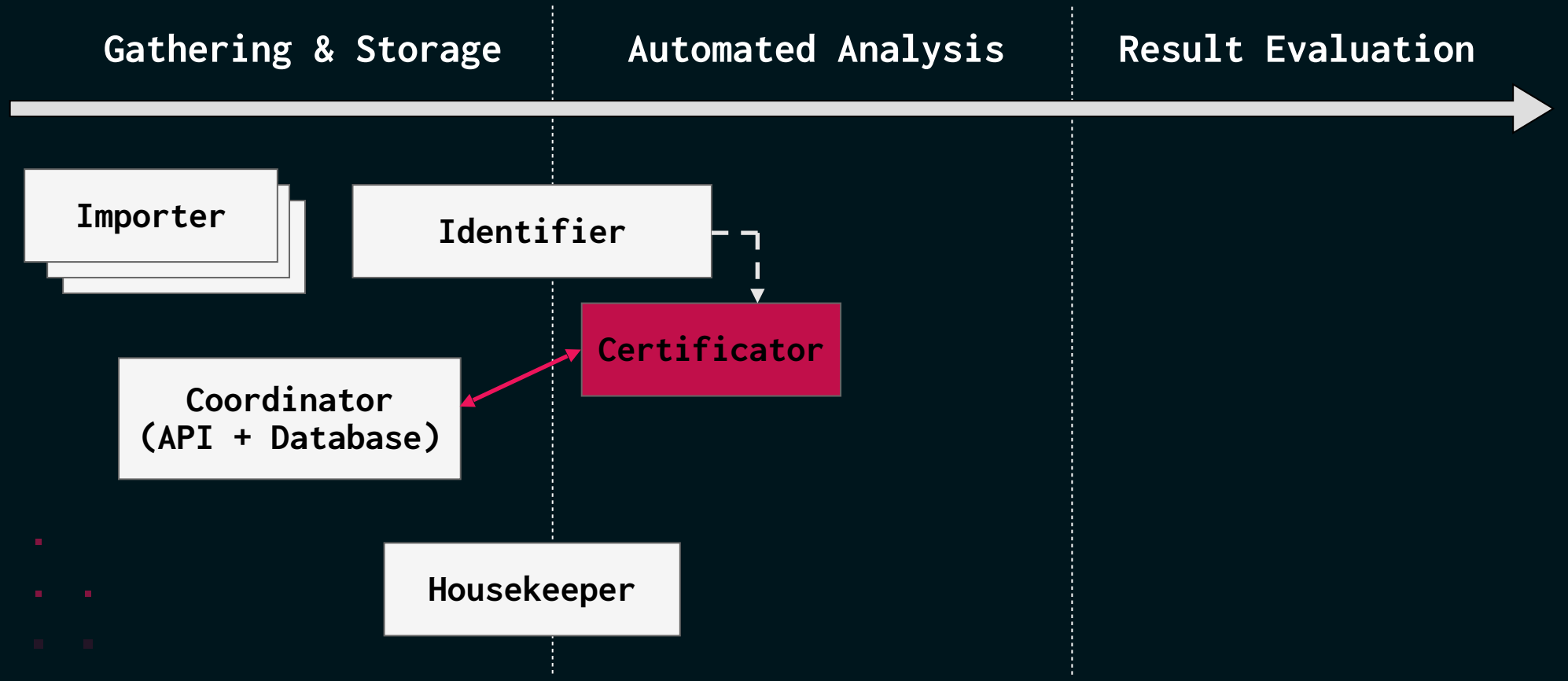
Identifier & Housekeeper



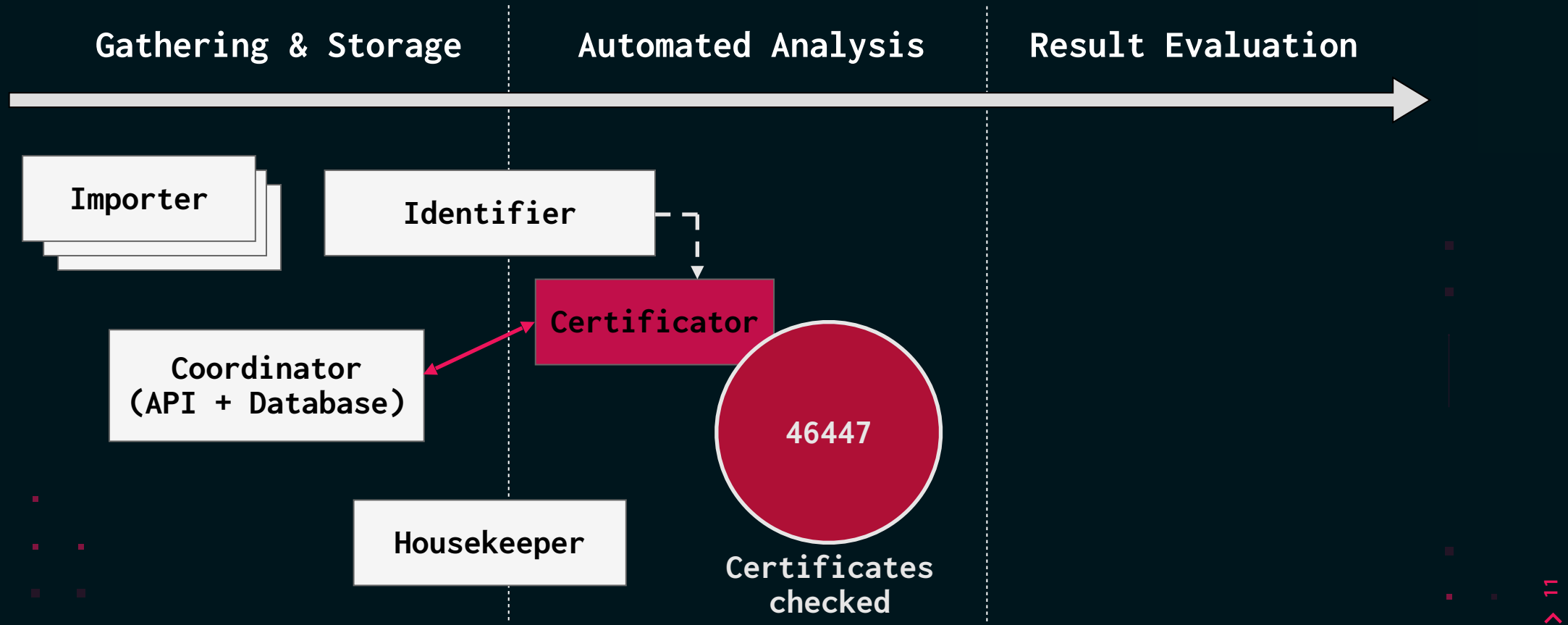
Identifier & Housekeeper



Certificator



Certificator



Pathfinder

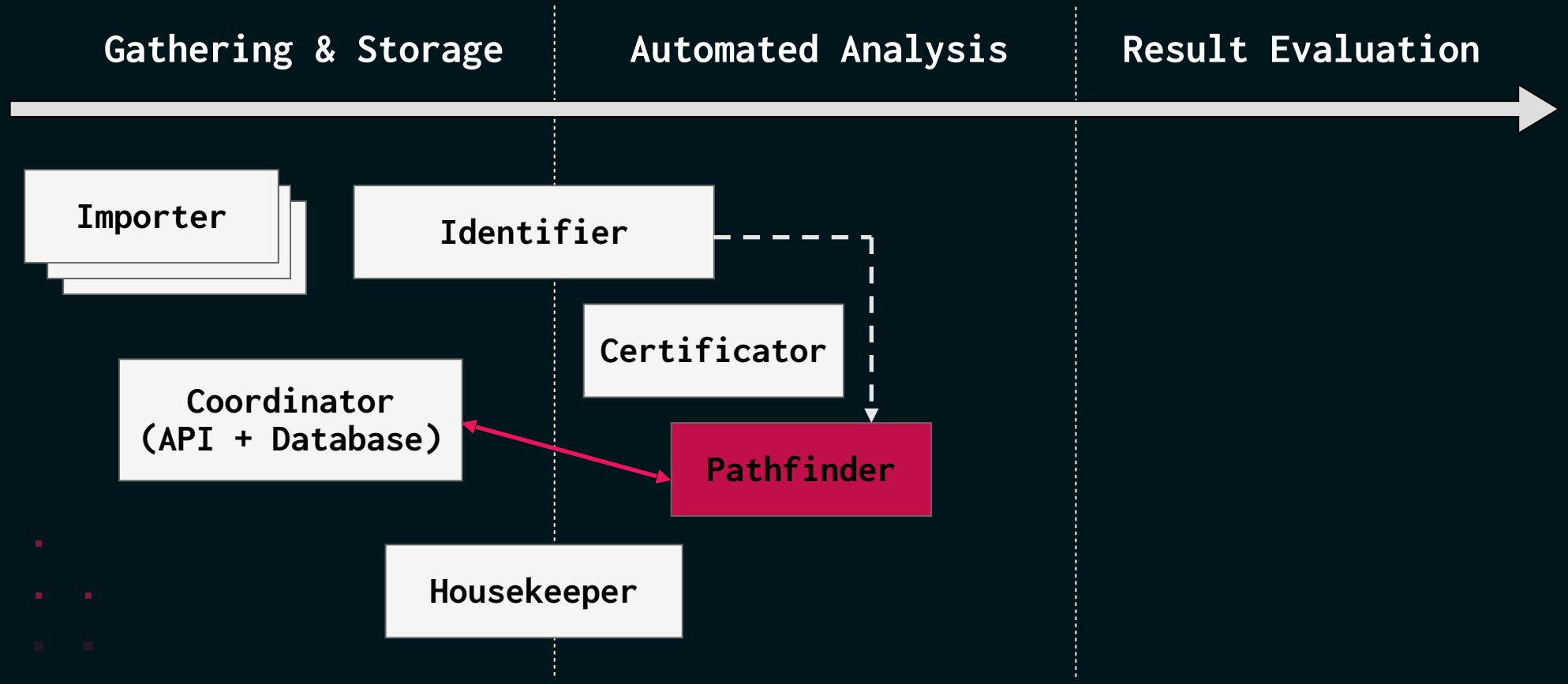
Paths to interesting kernel APIs

- Based on VMware TAU research
- Using Hex-Rays IDA Pro decompiler
- Modified for wider applicability

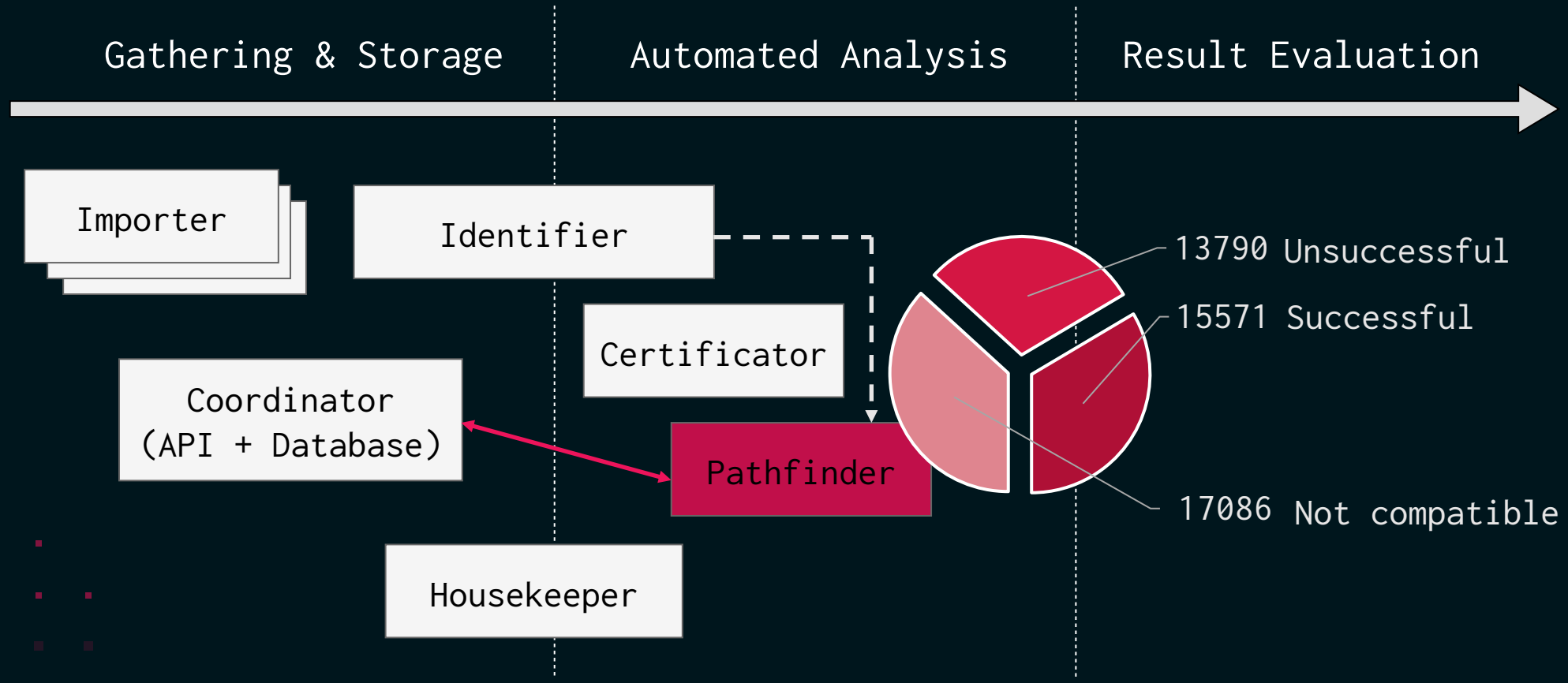
```
a1->DriverUnload = (PDRIVER_UNLOAD)sub_11580;
memset64(a1->MajorFunction, (unsigned __int64)fn_ioctl_handler_wdm_memset64, 0x1BuLL);
a1->MajorFunction[3] = (PDRIVER_DISPATCH)&sub_11958;
a1->MajorFunction[22] = (PDRIVER_DISPATCH)&sub_11A94;
a1->MajorFunction[27] = (PDRIVER_DISPATCH)sub_11AD8;
fn_11BD8(a1);
```

Addition for finding more handlers.

Pathfinder


Gathering & Storage
Automated Analysis
Result Evaluation
Importer
Identifier
Certificator
Coordinator
(API + Database)
Pathfinder
Housekeeper
Communication direction
Uses information of

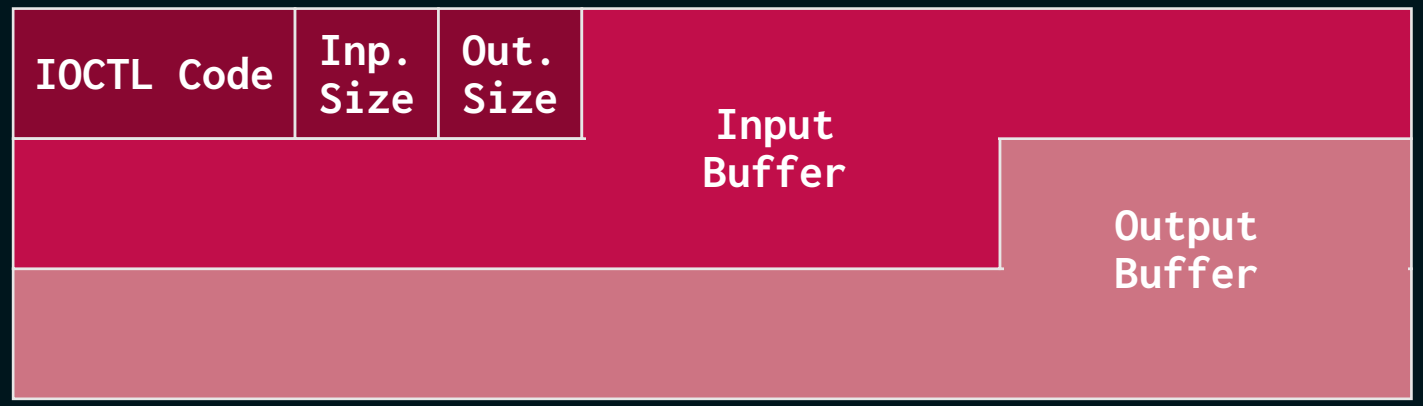
Pathfinder


Gathering & Storage
Automated Analysis
Result Evaluation
Importer
Identifier
Certificator
Coordinator
(API + Database)
Pathfinder
Housekeeper
13790 Unsuccessful
15571 Successful
17086 Not compatible
Communication direction
Uses information of

Fuzzifier

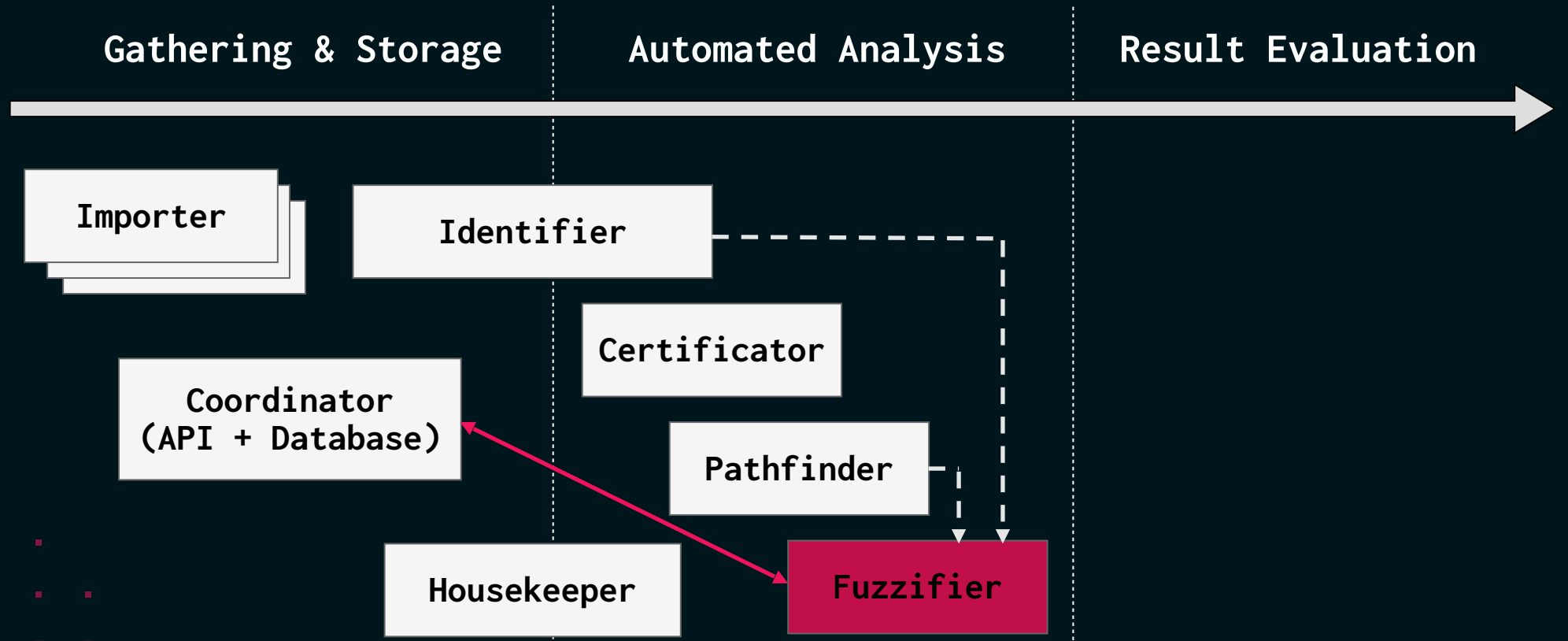
Fuzz testing AMD64 drivers

- Wrapper of Intel Labs kAFL/Nyx
- Modified Fuzzing Harness

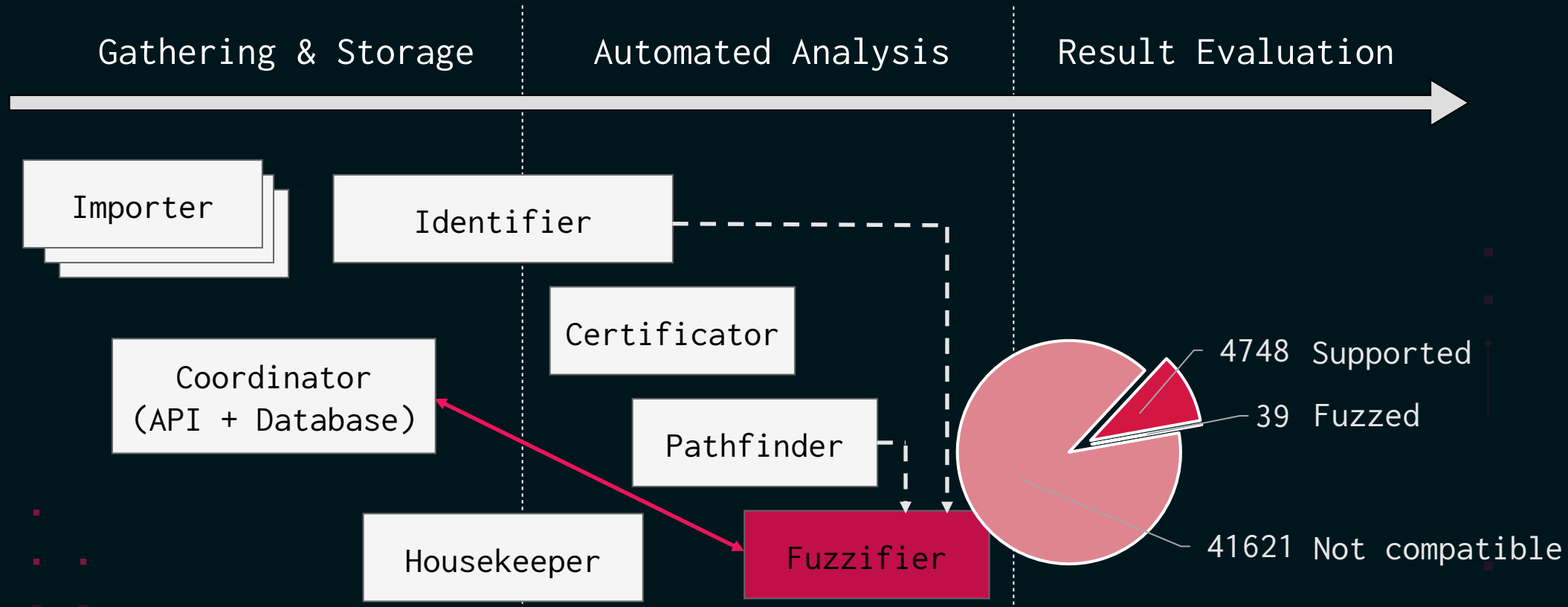


Fuzzing Payload with IOCTL Code

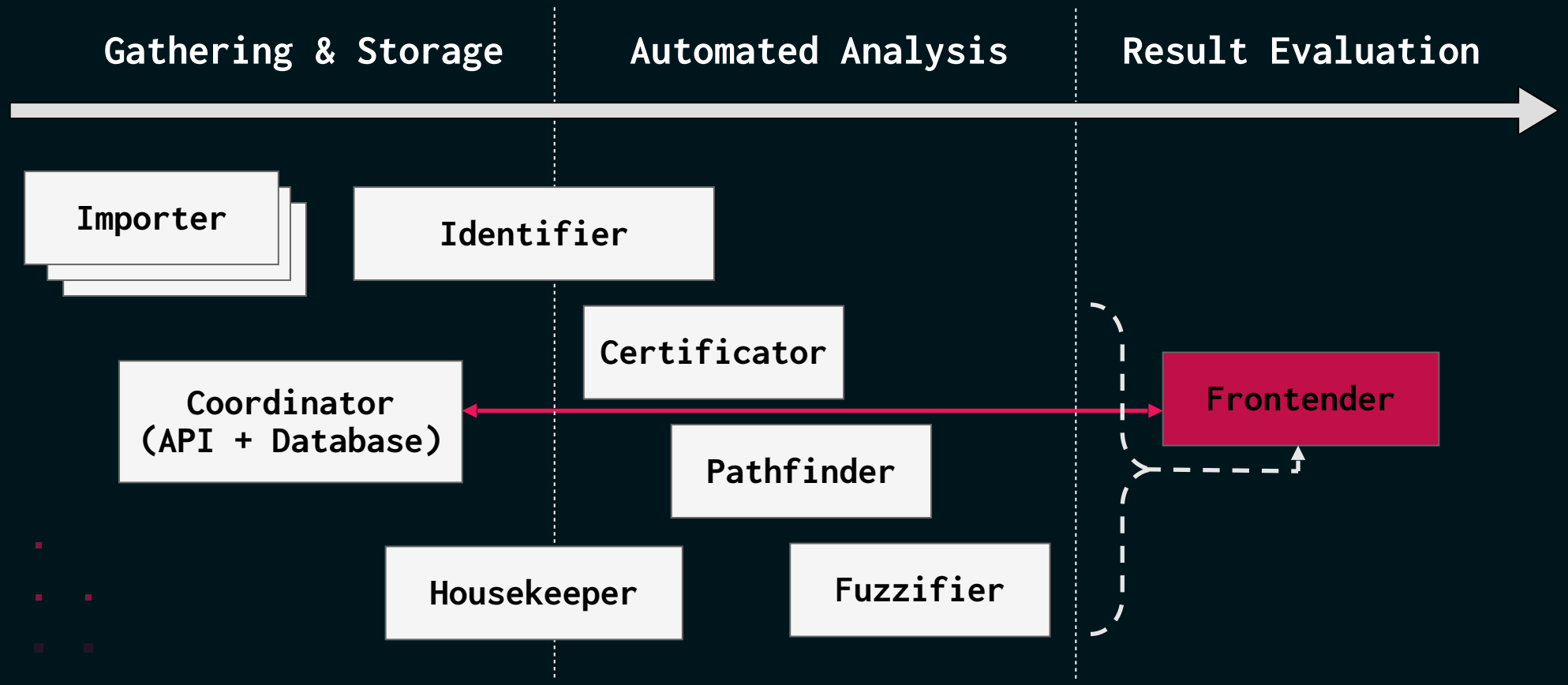
Fuzzifier


Gathering & Storage
Automated Analysis
Result Evaluation
Importer
Identifier
Certificator
Coordinator
(API + Database)
Pathfinder
Housekeeper
Fuzzifier
Communication direction
Uses information of

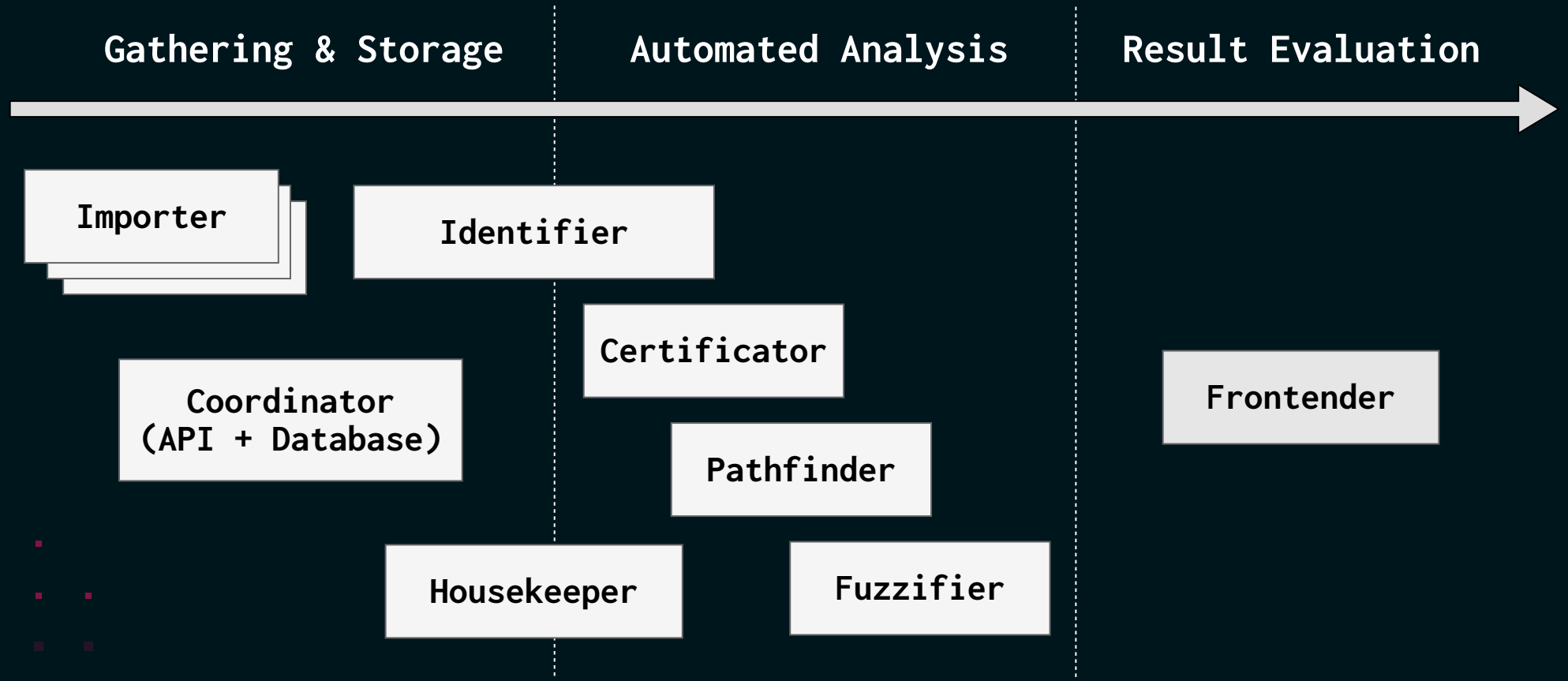
Fuzzifier


Gathering & Storage
Automated Analysis
Result Evaluation
Importer
Identifier
Certificator
Coordinator
(API + Database)
Pathfinder
Housekeeper
Fuzzifier
4748 Supported
39 Fuzzed
41621 Not compatible
Communication direction
Uses information of

Frontender

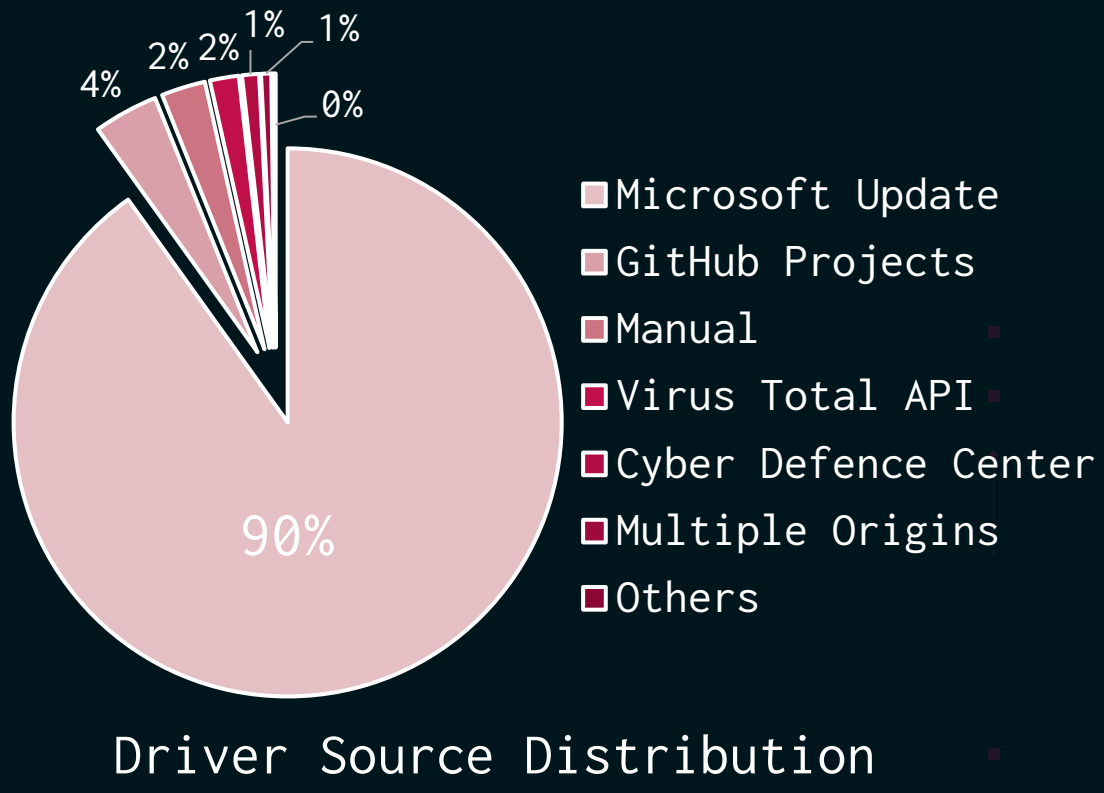

Gathering & Storage
Automated Analysis
Result Evaluation
Importer
Identifier
Certificator
Coordinator
(API + Database)
Frontender
Pathfinder
Housekeeper
Fuzzifier
Communication direction
Uses information of

Continuous Automated Analysis



Pipeline Gathering

- 1’155’155 total files
- 46’447 driver files
  - 1’012 are ARM drivers
  - 1’949 known vulnerable



Driver Source Distribution

Automated Analysis

Pathfinder improvements

- 94% of ARM drivers analysed
- 1’455 additional drivers through other modifications

Automated Analysis

Pathfinder improvements

- 94% of ARM drivers analysed
- 1’455 additional drivers through other modifications

Automated fuzzing

- 5’275 fuzzing configurations tried
- 10 drivers crashes found

New Vulnerable Drivers

Vendors	Signature Dates	Types of Vulnerabilities Found
Vendor 1	2014	rPM, wPM
Vendor 2	2022	rPM
Dynabook	2018	rPM
Tencent	2024	rMSR, wMSR, inB, outB
Dell	2017 2012 2014	rMSR, wMSR, inB, outB inB, outB, rPM rMSR, wMSR
Lenovo	2020	inB, outB, rMSR
NVidia	2015	inB, outB

rPM, wPM = Read/Write Physical Memory rMSR, wMSR = Arbitrary Read/Write MSR

inB, outB = Arbitrary I/O Port Read/Write

Coordinated Vuln. Disclosure

10.07.2024 initiated coordinated disclosure

Vendors	Response State
Vendor 1	No Response
Vendor 2	No Response
Dynabook	In Progress
Tencent	No Response
Dell	Rejected
Lenovo	Confirmed
NVidia	In Progress

Progress on disclosure

Rejected because outdated and not supported products.
Abuse still possible.

Example exploit - Token Exchange

Read / Write physical memory abuse

1. Search physical memory for:
   a. Privileged Process Token
   b. Own Process Token
2. Overwrite own Token

```
Found a valid EPROCESS struct at 000000031194CEB8:
000000: 77 69 6e 69 6e 69 74 2e 65 78 65 00 00 00 00     wininit.exe....
SYSTEM token at 000000031194CDC8 with:
000000: 79 39 0d 59 0b 97 ff ff                          y9.Y....
```

Privileged Token found

```
25  PhysicalAddress.QuadPart = *(unsigned int *)SystemBuffer_0;
26  physPageRef = (char *)MmMapIoSpace(PhysicalAddress, pyhsPageSize, MmNonCached);
27  v9 = 0;
28  switch ( *((_DWORD *)SystemBuffer_0 + 1) )
29  {
30    case 1:                                         // arbitray phys mem write
31      qmemcpy(physPageRef, (char *)SystemBuffer_0 + 12, *((unsigned int *)SystemBuffer_0 + 2));
```

Physical Memory Write Vulnerability

Cyber Defence Centre Findings

Cooperation with InfoGuard AG CDC

- Across three clients
- 33’000 endpoints checked

CDC Client	Total Drivers	Known Vulnerable	New Vulnerable
Client 1	250	7	2
Client 3	319	4	1
Client 2	108	1	2

Driver distribution across real business networks.

Current Pipeline Limitations

General

- Manual vulnerability verification necessary
- Niche drivers possibly not found

Tool-based

- Unsupported installers possibly contain more drivers
- Undetected certificate revocations
- Decompilation failures impact Pathfinder results
- Fuzzing specific:
  - Environment or device requirements
  - Lack of ARM64 kernel support

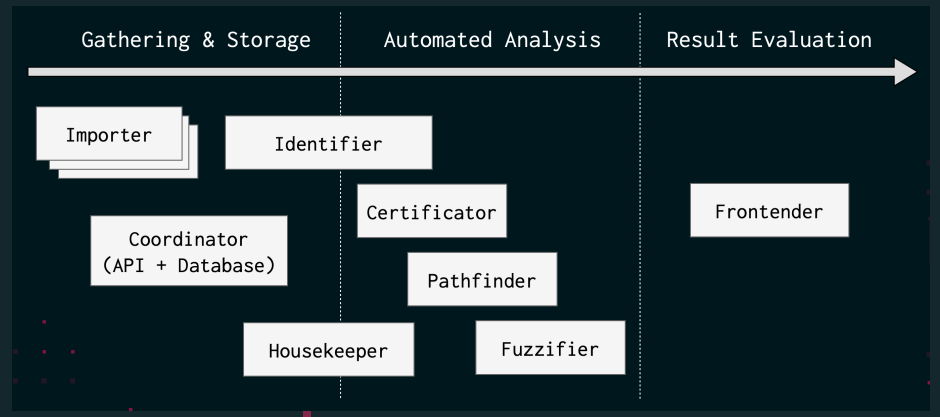
Windows Kernel Driver Vulnerabilities

- Escalate Local Privilege
- Bypass Security Products
- Install Firmware Rootkits

Insufficient Auditing of Kernel Drivers

- Microsoft relying on third-parties
- No central repository
- Fast release cycle
- Missing ARM support

Continuous Automated Driver Analysis



- Over 46’000 drivers gathered
  - ~27’000 automatically analysed
    - ~1’000 ARM drivers
- 10 **new** vulnerable drivers found