red canary

Tidying up your Nest

Validating ATT&CK Technique Coverage
Using EDR Telemetry

Presenters

Adam Ostrich

Senior Detection Validation Engineer

Jesse Brown

Senior Detection Validation Engineer

@jessecbrown

Detection Validation Team

- Understand how things should work
- Make sure things work like they should
- Make things work better

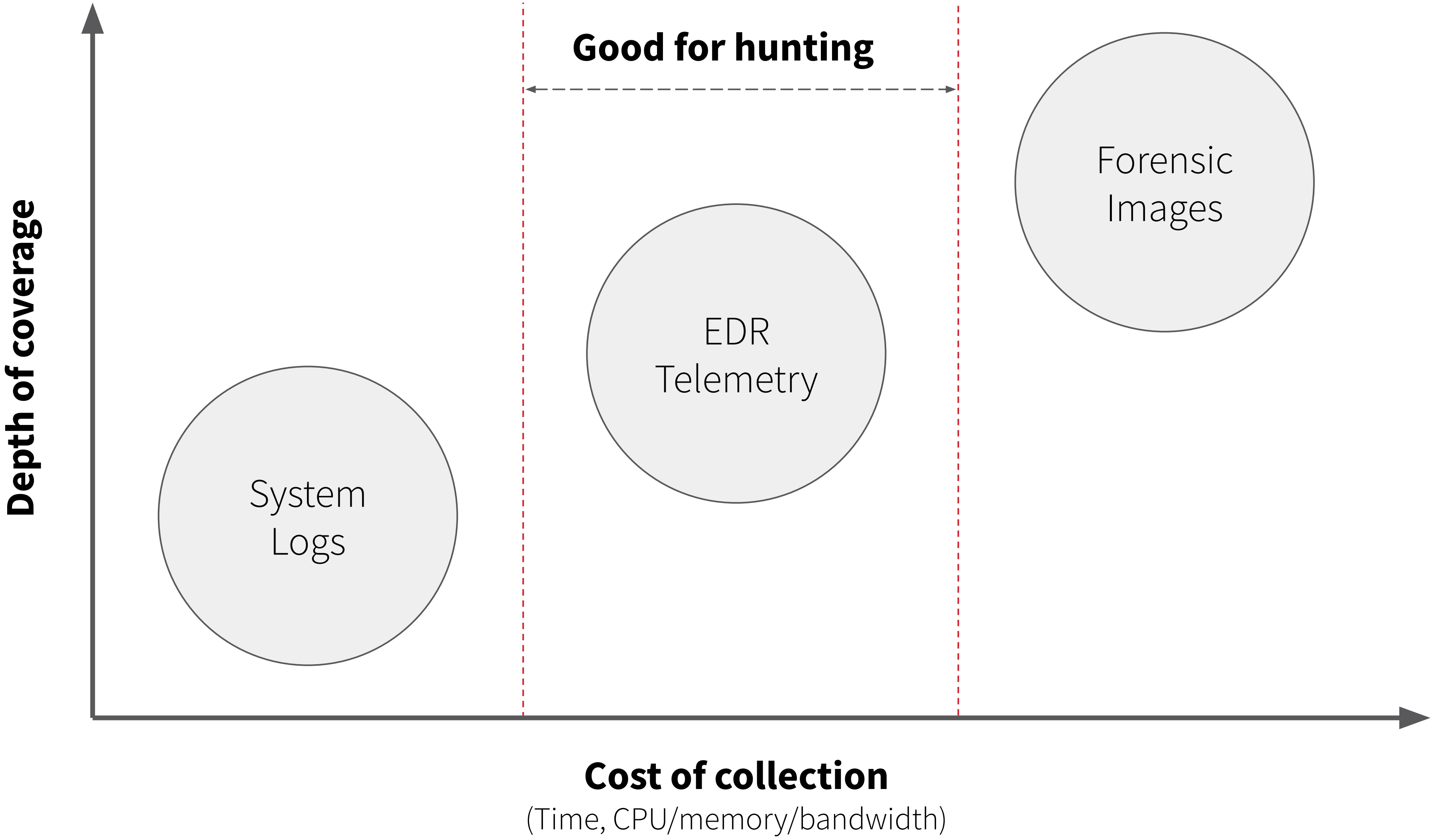
Outline

- What is EDR telemetry?
- How Red Canary works
- Validation of ATT&CK techniques
- Automated validation workflow
- Lessons learned

Outline

- **What is EDR telemetry?**
- How Red Canary works
- Validation of ATT&CK techniques
- Automated validation workflow
- Lessons learned

What is EDR Telemetry?



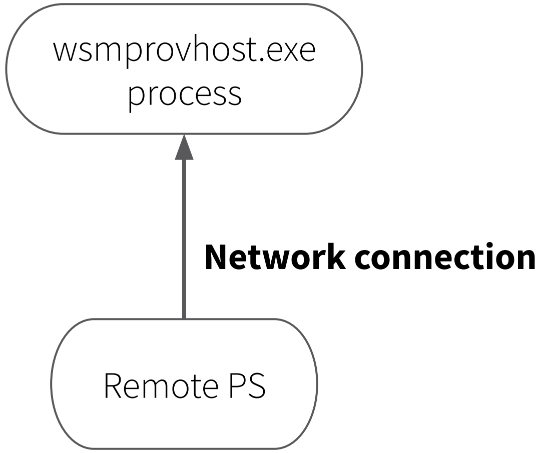
Telemetry Types

```
PS > Invoke-Expression -Command "procdump -ma lsass.exe lsass.dmp"
```

Remote PS

Telemetry Types

```
PS > Invoke-Expression -Command "procdump -ma lsass.exe lsass.dmp"
```



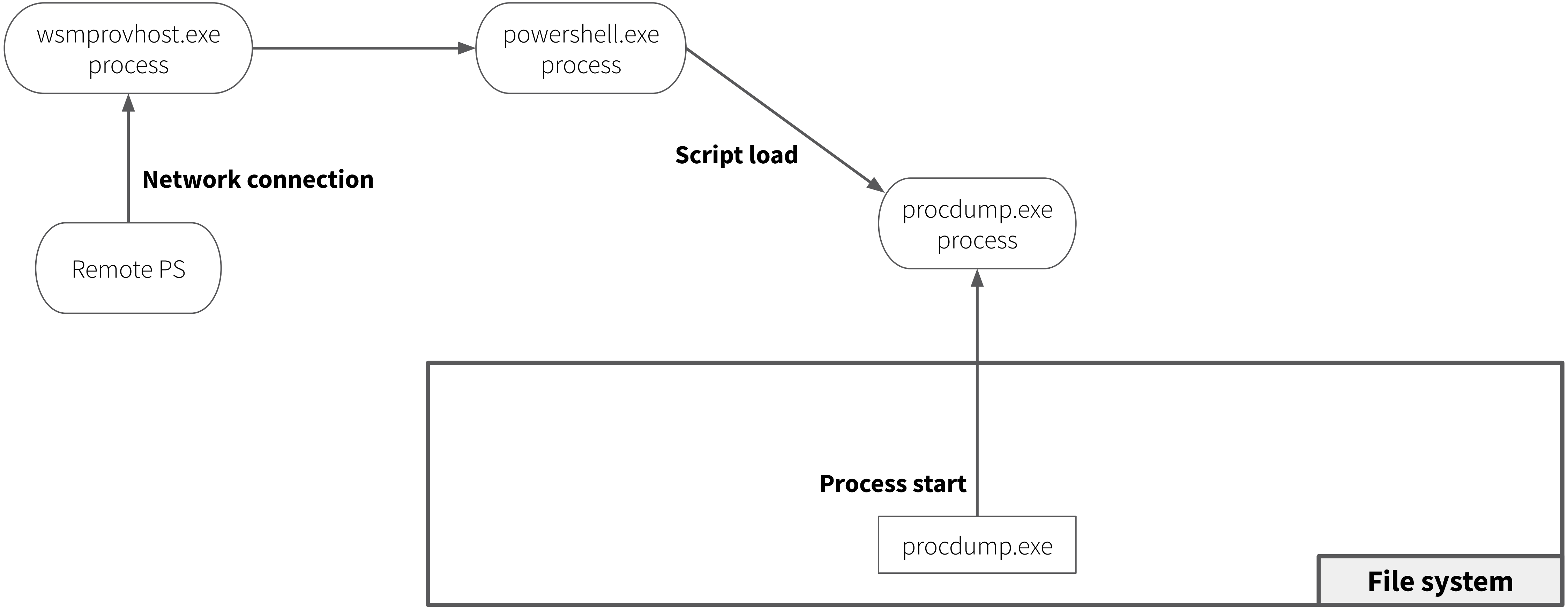
wsmprovhost.exe process

Network connection

Remote PS

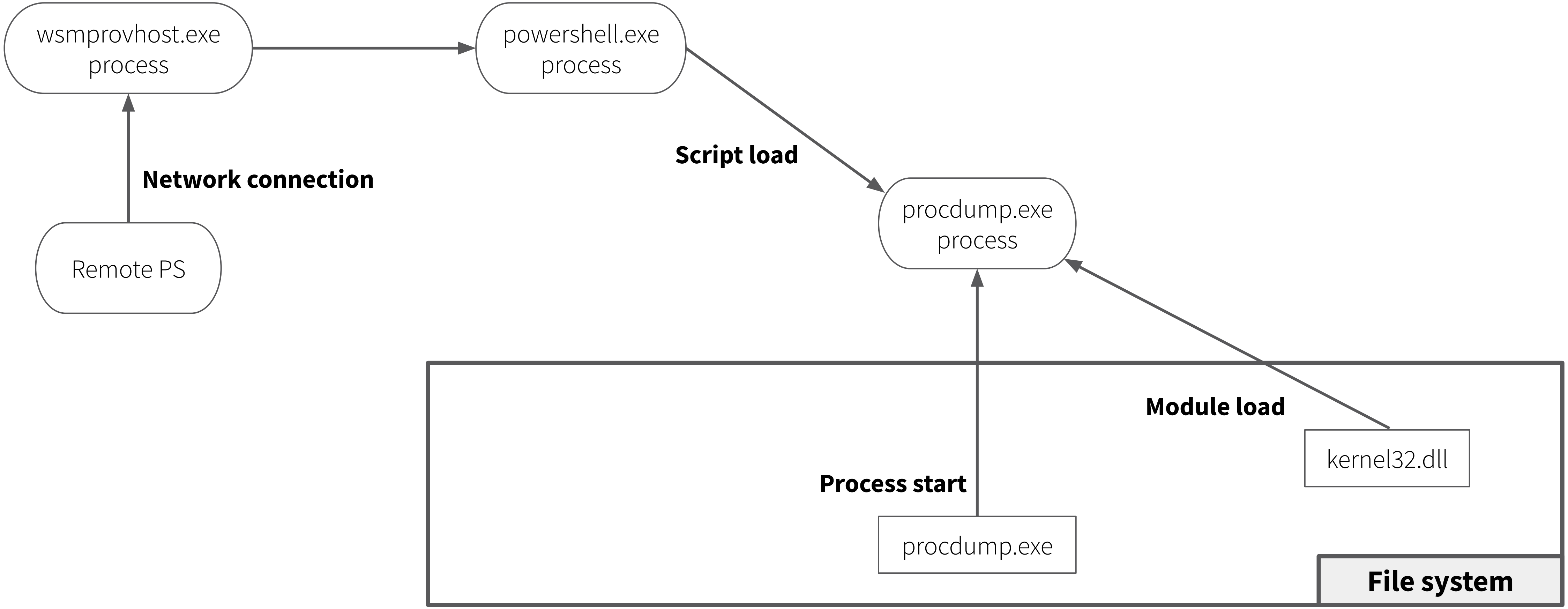
Telemetry Types

```
PS > Invoke-Expression -Command "procdump -ma lsass.exe lsass.dmp"
```



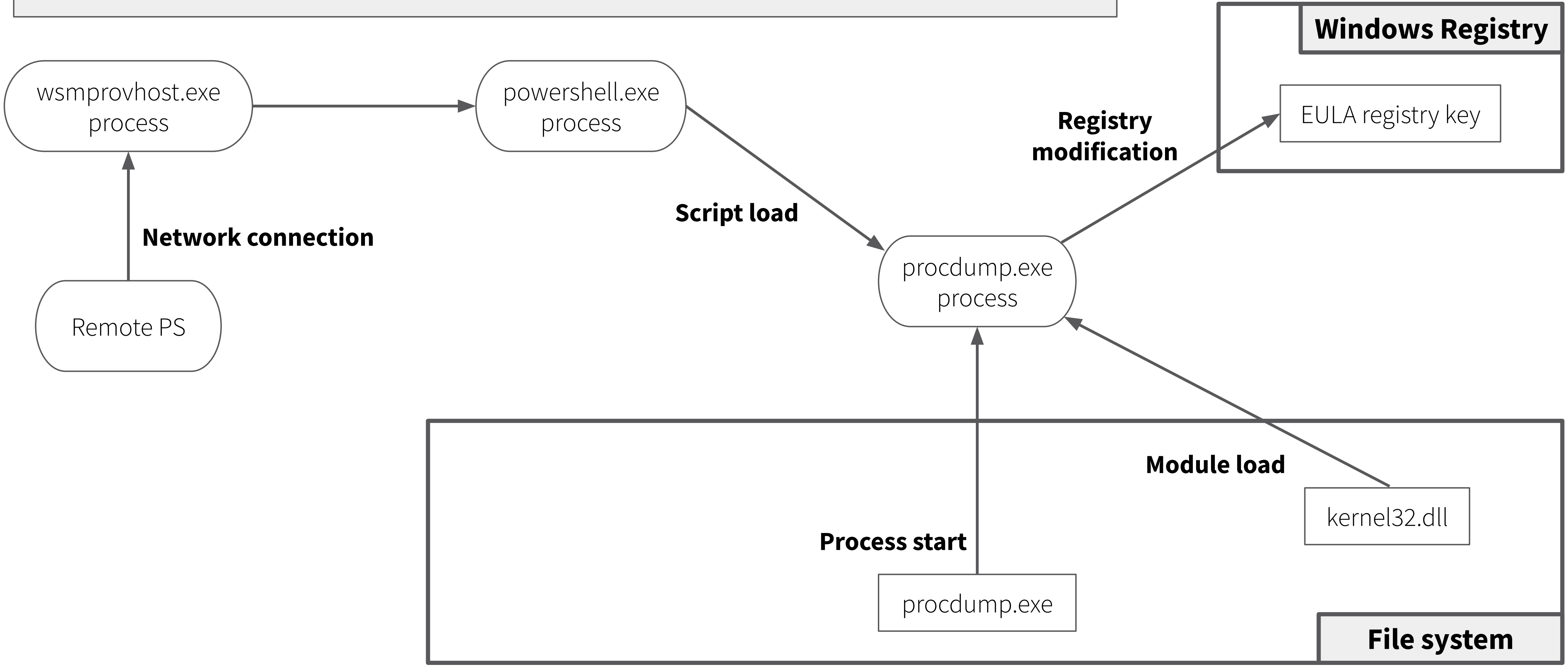
Telemetry Types

```
PS > Invoke-Expression -Command "procdump -ma lsass.exe lsass.dmp"
```



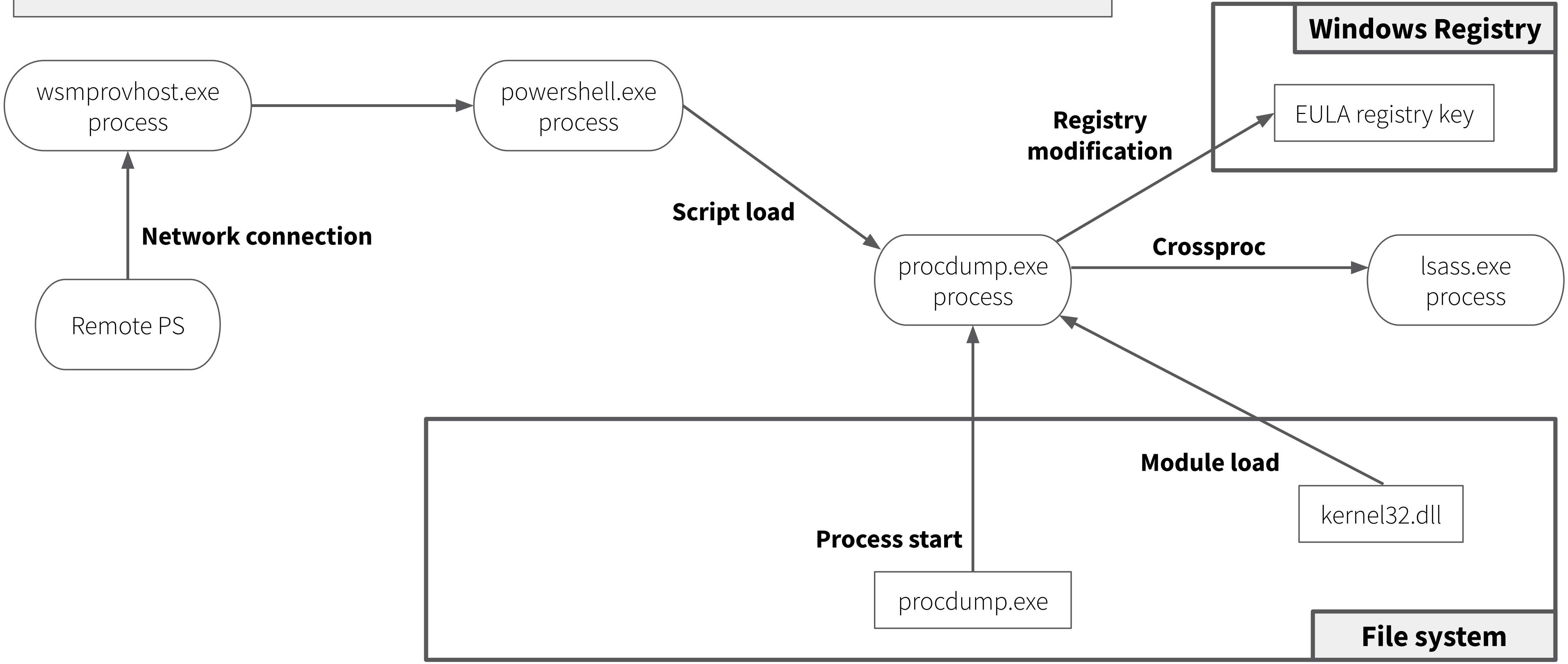
Telemetry Types

```
PS > Invoke-Expression -Command "procdump -ma lsass.exe lsass.dmp"
```



Telemetry Types

```
PS > Invoke-Expression -Command "procdump -ma lsass.exe lsass.dmp"
```



wsmprovhost.exe process

powershell.exe process

Network connection

Remote PS

Script load

Registry modification

Windows Registry

EULA registry key

procdump.exe process

Crossproc

lsass.exe process

Module load

kernel32.dll

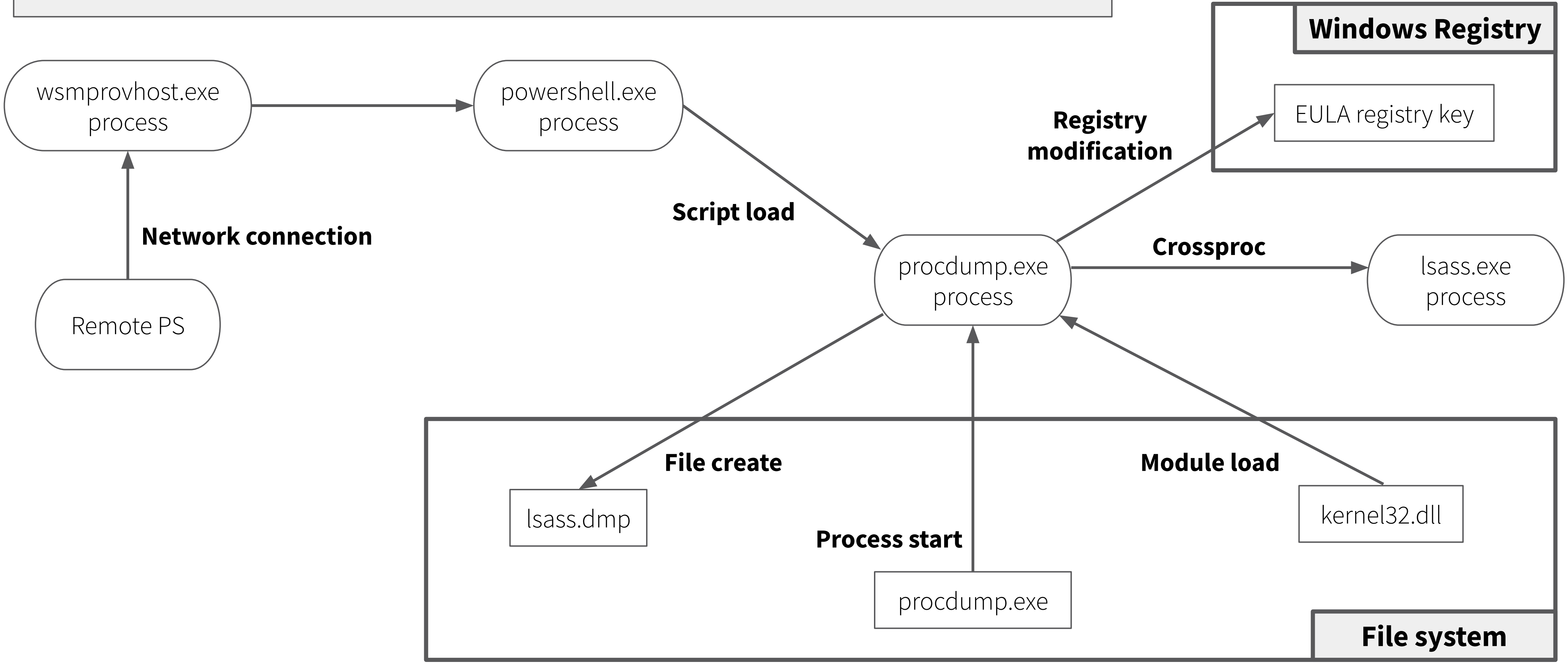
Process start

procdump.exe

File system

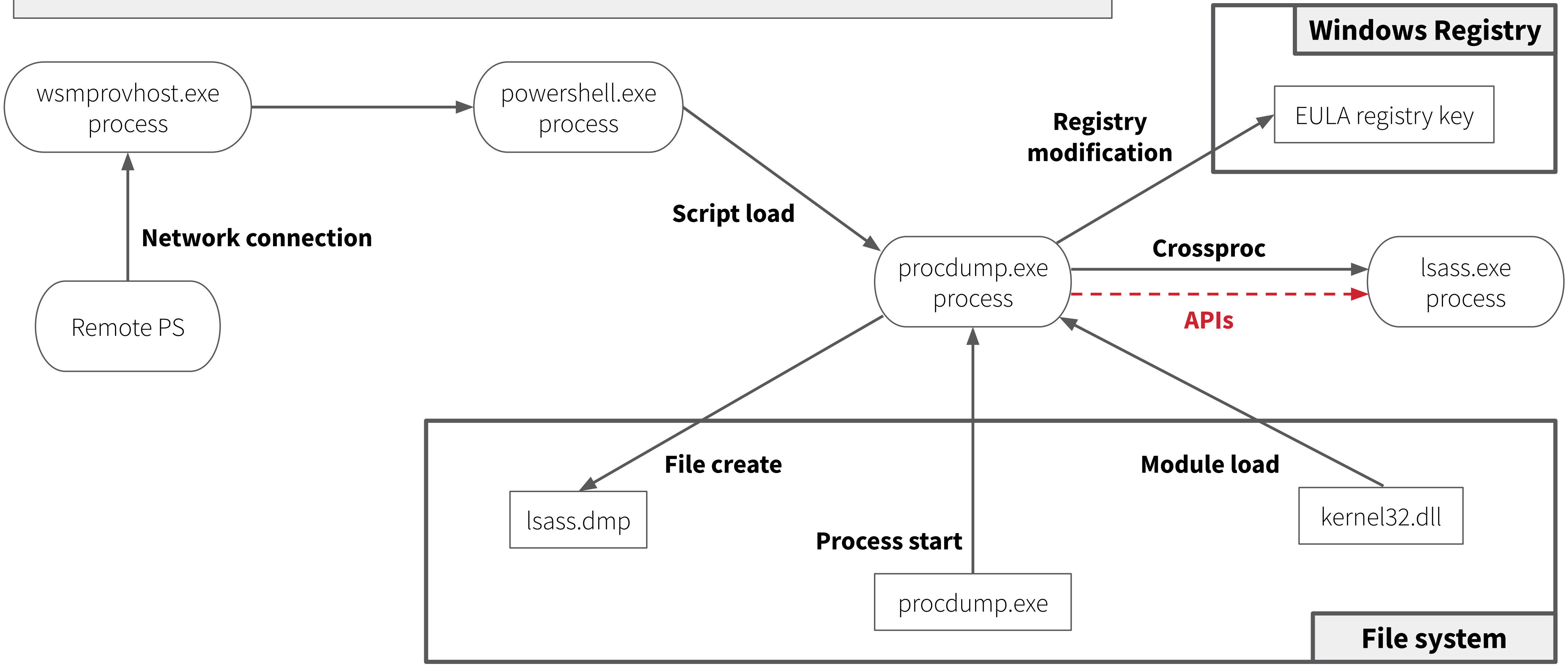
Telemetry Types

PS > Invoke-Expression -Command "procdump -ma lsass.exe lsass.dmp"



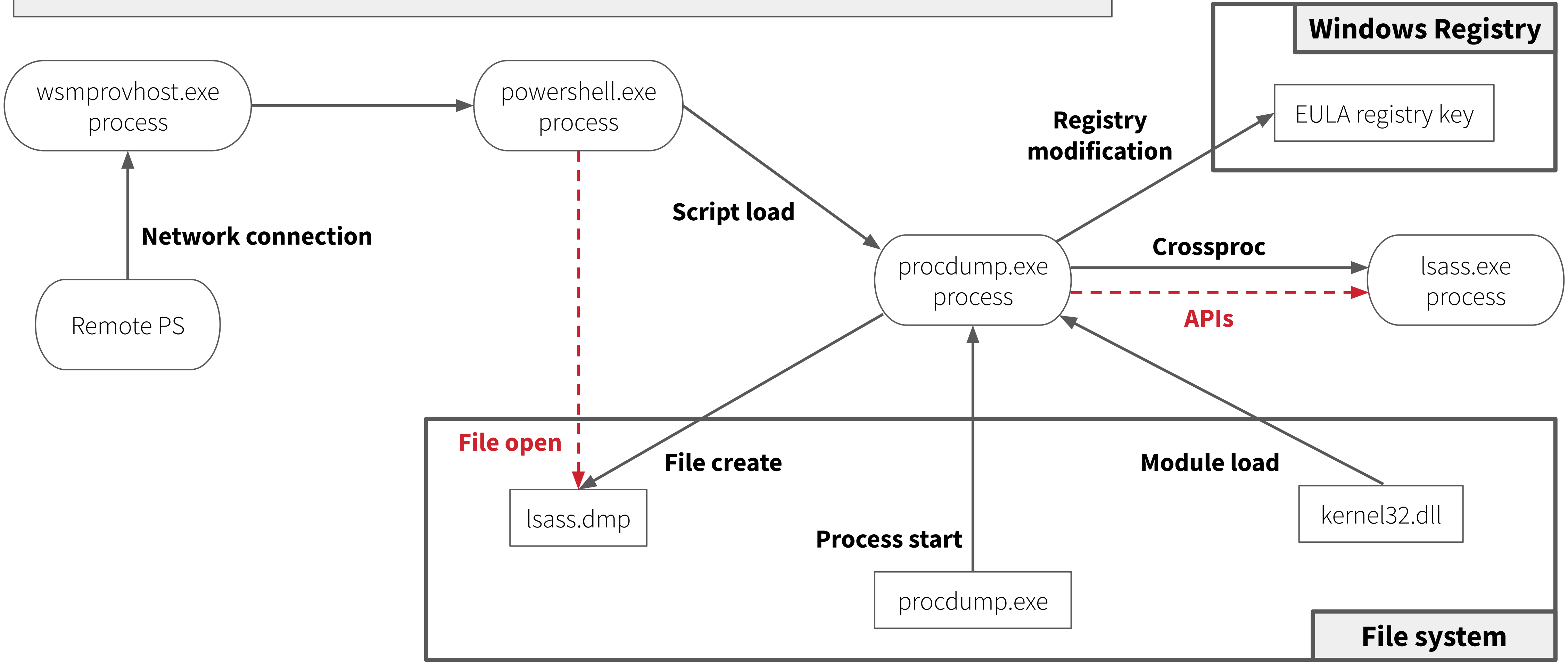
Telemetry Types

```
PS > Invoke-Expression -Command "procdump -ma lsass.exe lsass.dmp"
```



Telemetry Types

PS > Invoke-Expression -Command "procdump -ma lsass.exe lsass.dmp"



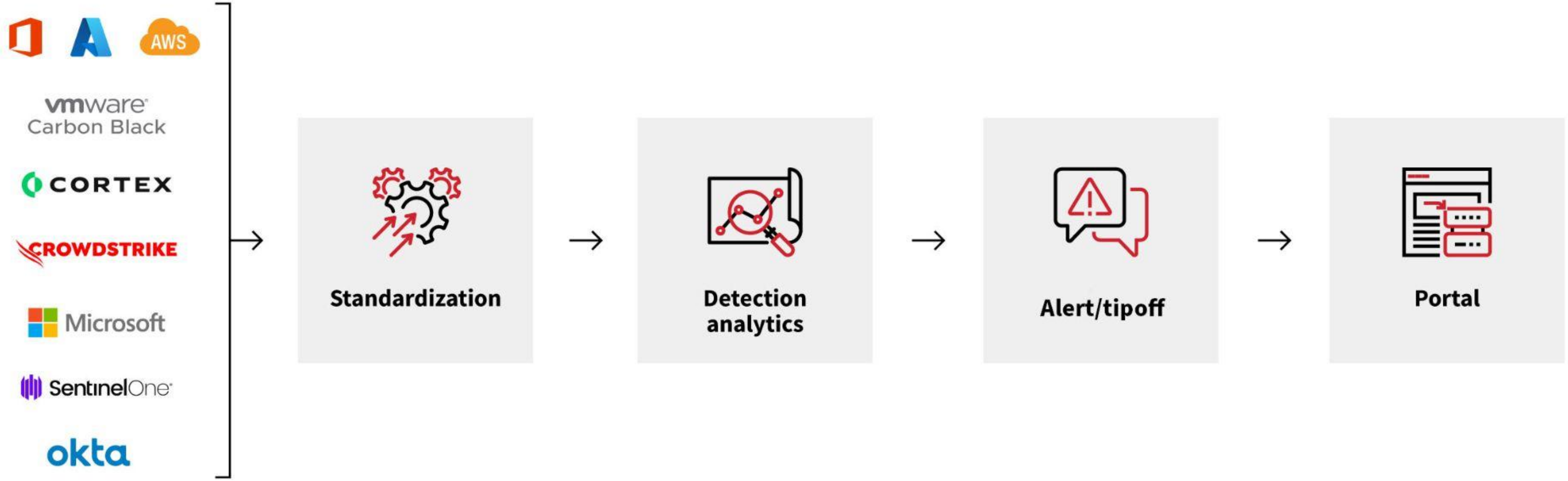
It’s JSON!

```
{
  "event_type": "process_start",
  "process_command_line": "procdump -ma lsass.exe lsass.dmp",
  "process_md5": "f2091c44d89789f689d98bc244358878",
  "process_name": "procdump.exe",
  "process_path": "C:\Sysinternals\procdump.exe",
  "process_pid": 1528,
}
```

Outline

- What is EDR telemetry?
- **How Red Canary works**
- Validation of ATT&CK techniques
- Automated validation workflow
- Lessons learned

How Red Canary works (and maybe you too?)



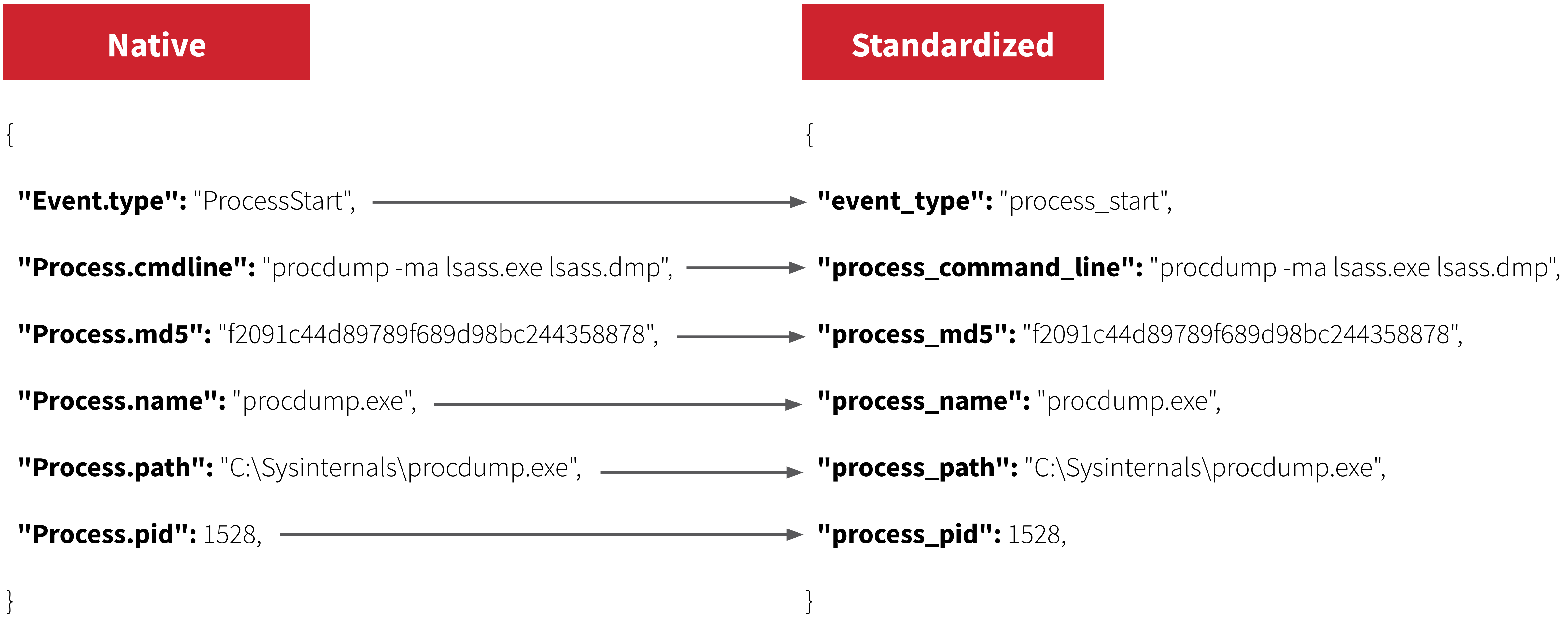
Standardization

Detection analytics

Alert/tipoff

Portal

Standardization



Native

```
{
  "Event.type": "ProcessStart",
  "Process.cmdline": "procdump -ma lsass.exe lsass.dmp",
  "Process.md5": "f2091c44d89789f689d98bc244358878",
  "Process.name": "procdump.exe",
  "Process.path": "C:\Sysinternals\procdump.exe",
  "Process.pid": 1528,
}
```

Standardized

```
{
  "event_type": "process_start",
  "process_command_line": "procdump -ma lsass.exe lsass.dmp",
  "process_md5": "f2091c44d89789f689d98bc244358878",
  "process_name": "procdump.exe",
  "process_path": "C:\Sysinternals\procdump.exe",
  "process_pid": 1528,
}
```

Outline

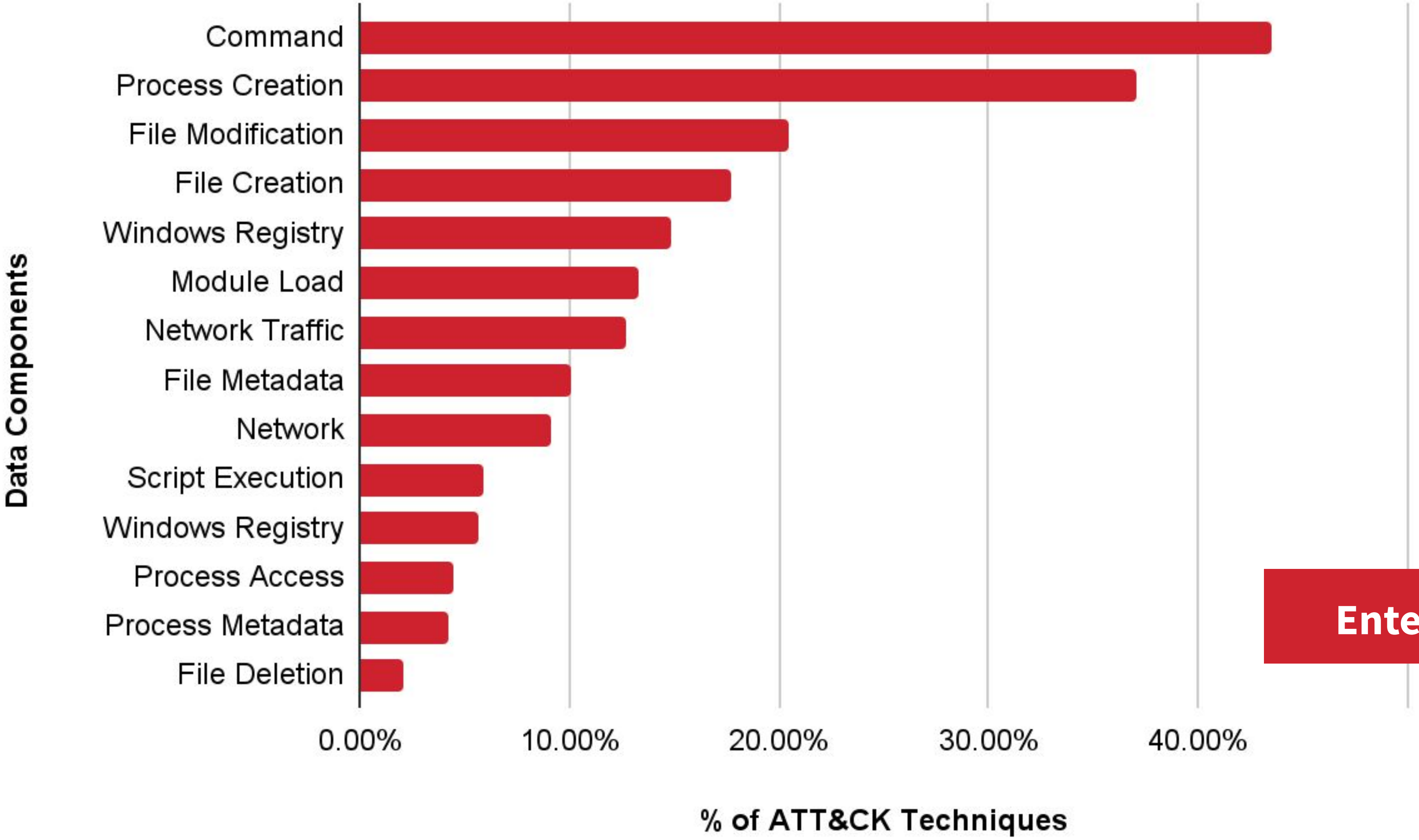
- What is EDR telemetry?
- How Red Canary works
- **Validation of ATT&CK techniques**
- Automated validation workflow
- Lessons learned

Validate coverage across ATT&CK techniques

- **Break techniques down to data components**

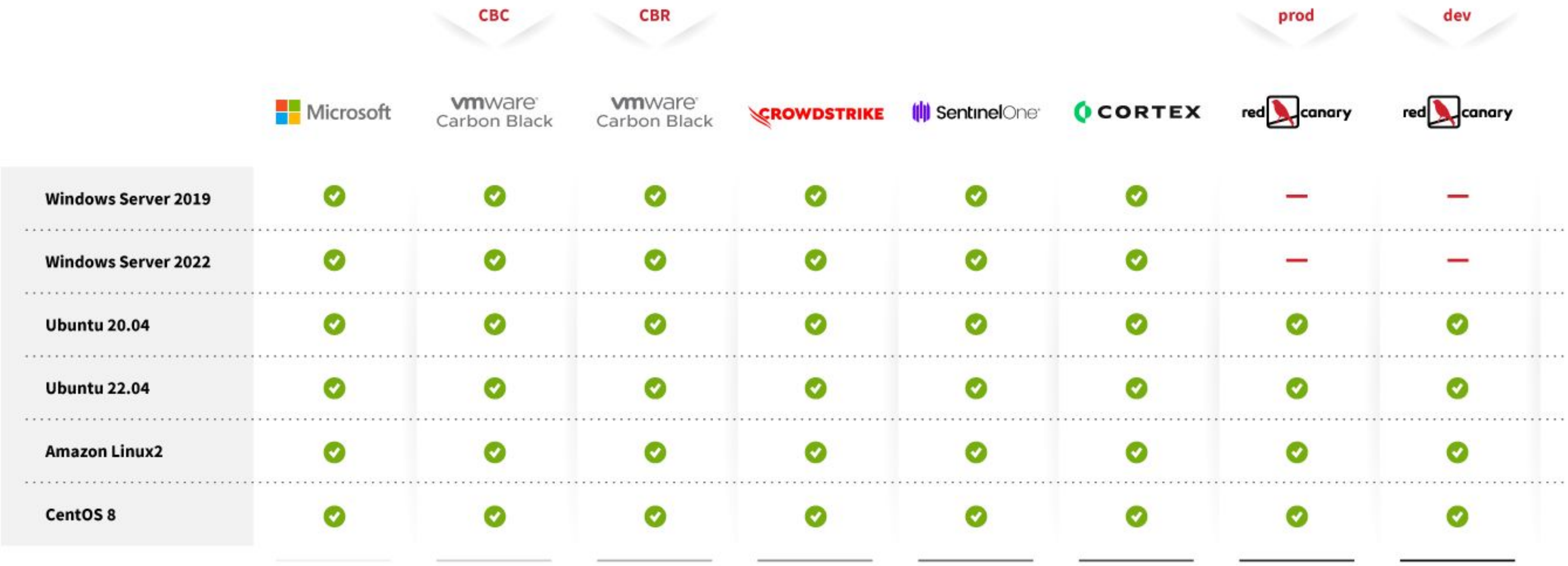
OS Credential Dumping: LSASS Memory (T1003.001)	
Data component	**Detects**
Process creation	procdump -ma lsass.exe lsass.dmp
Command execution	Invoke-Mimikatz
Process access	API calls to OpenProcess/MiniDumpWriteDump
Process access	Crossproc (e.g. open process handle)
File modification	File lsass.dmp written to disk

ATT&CK Technique Coverage by Data Component



Enterprise Techniques

So many combinations.. Oh my!



		CBC	CBR				prod	dev
	Microsoft	vmware Carbon Black	vmware Carbon Black	CROWDSTRIKE	SentinelOne	CORTEX	red canary	red canary
Windows Server 2019	✓	✓	✓	✓	✓	✓	—	—
Windows Server 2022	✓	✓	✓	✓	✓	✓	—	—
Ubuntu 20.04	✓	✓	✓	✓	✓	✓	✓	✓
Ubuntu 22.04	✓	✓	✓	✓	✓	✓	✓	✓
Amazon Linux2	✓	✓	✓	✓	✓	✓	✓	✓
CentOS 8	✓	✓	✓	✓	✓	✓	✓	✓

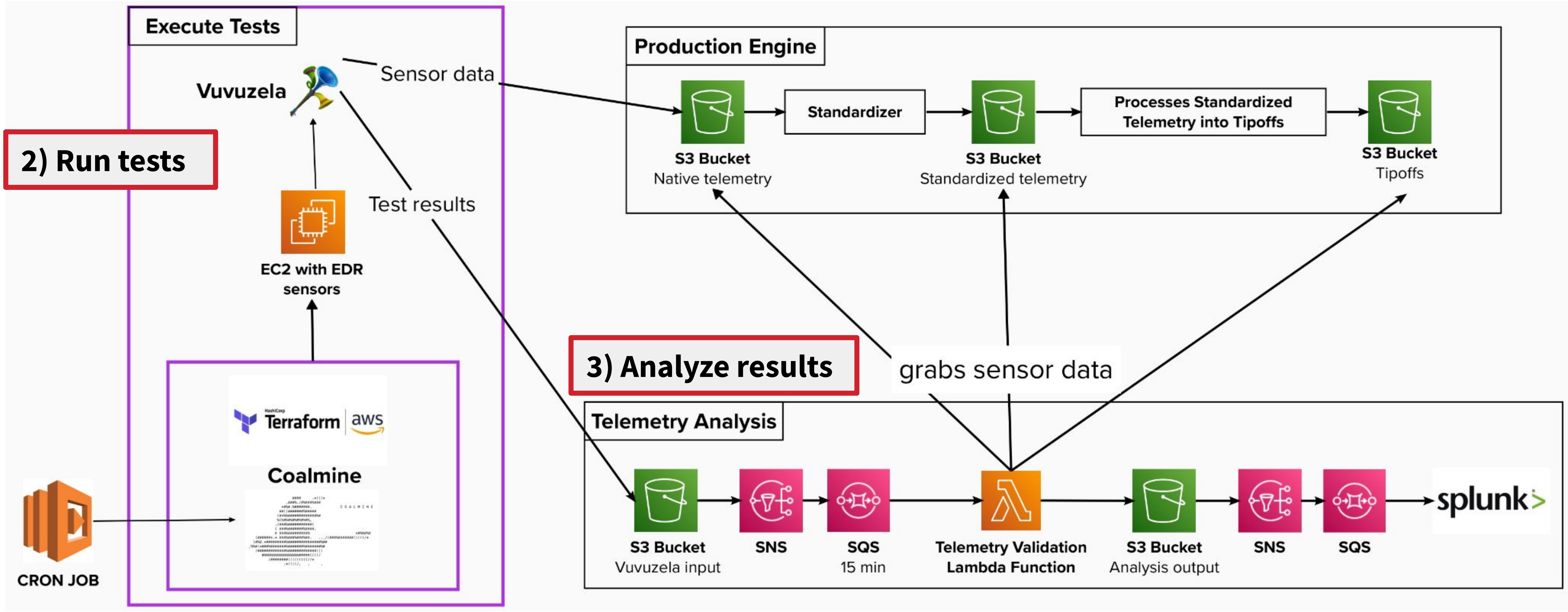
End-to-end functional testing!

- Run functional test
- Report expected results
- Compare expected results to actual results
- Analyze/detect changes in results

Outline

- What is EDR telemetry?
- How Red Canary works
- Validation of ATT&CK techniques
- **Automated validation workflow**
- Lessons learned

Scaling Validation with Automation

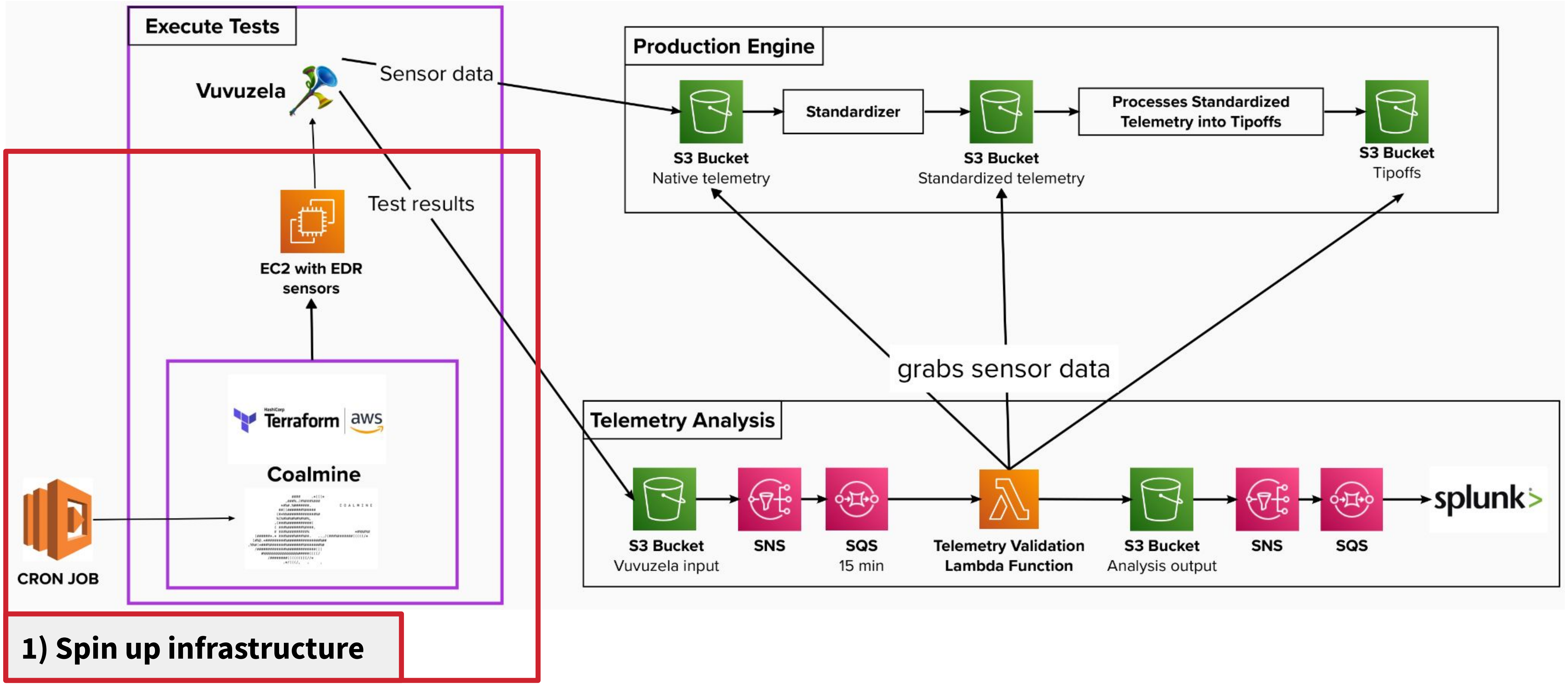


2) Run tests

3) Analyze results

1) Spin up infrastructure

Architecture



1) Spin up infrastructure

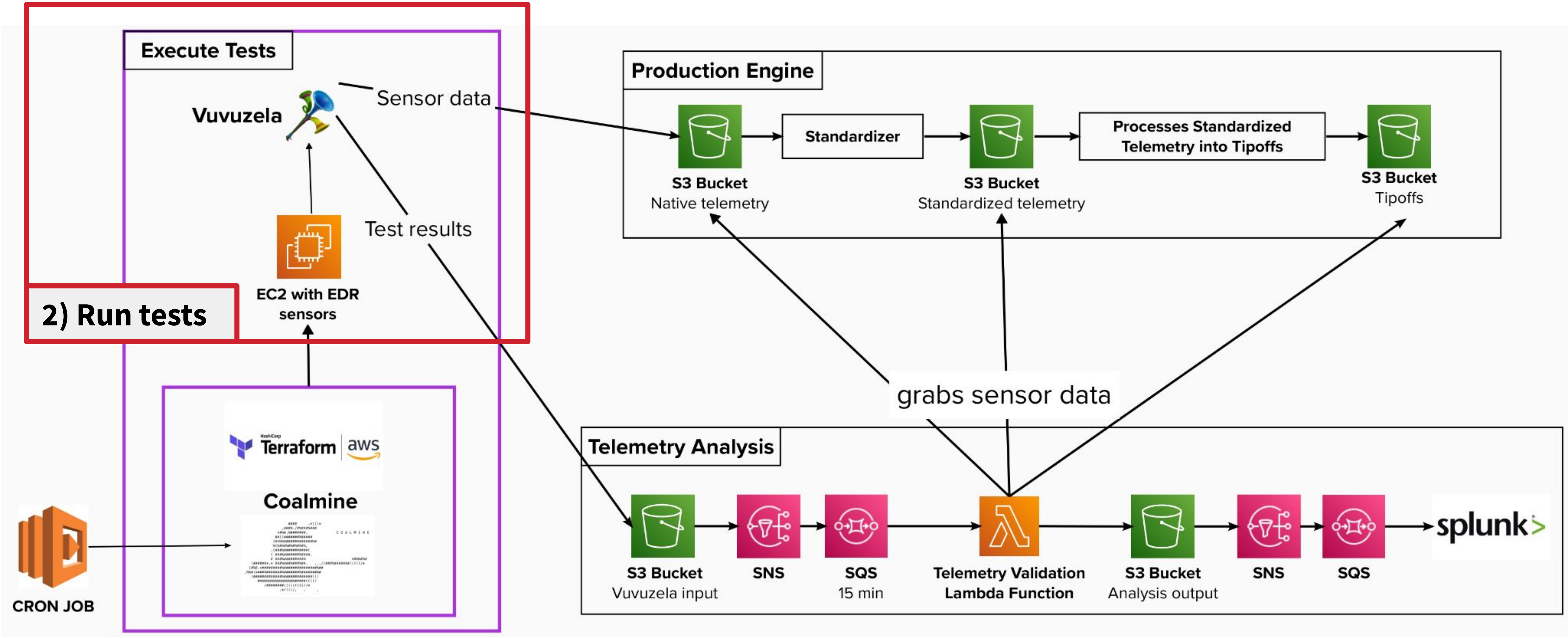
Coalmine

- **Spin up infrastructure**
  - Terraform and ansible
  - Creates/configures EC2 instances
- **Run tests**
  - Atomic Red Team

    https://github.com/redcanaryco/ansible-atomic-red-team
  - Atomic Test Harnesses

    https://atomicredteam.io/atomic-test-harnesses
  - Vuvuzela

Architecture



2) Run tests

Execute Tests

Vuvuzela

Sensor data

Test results

EC2 with EDR sensors

Terraform | aws

Coalmine

CRON JOB

Production Engine

S3 Bucket
Native telemetry

Standardizer

S3 Bucket
Standardized telemetry

Processes Standardized Telemetry into Tipoffs

S3 Bucket
Tipoffs

grabs sensor data

Telemetry Analysis

S3 Bucket
Vuvuzela input

SNS

SQS
15 min

Telemetry Validation Lambda Function

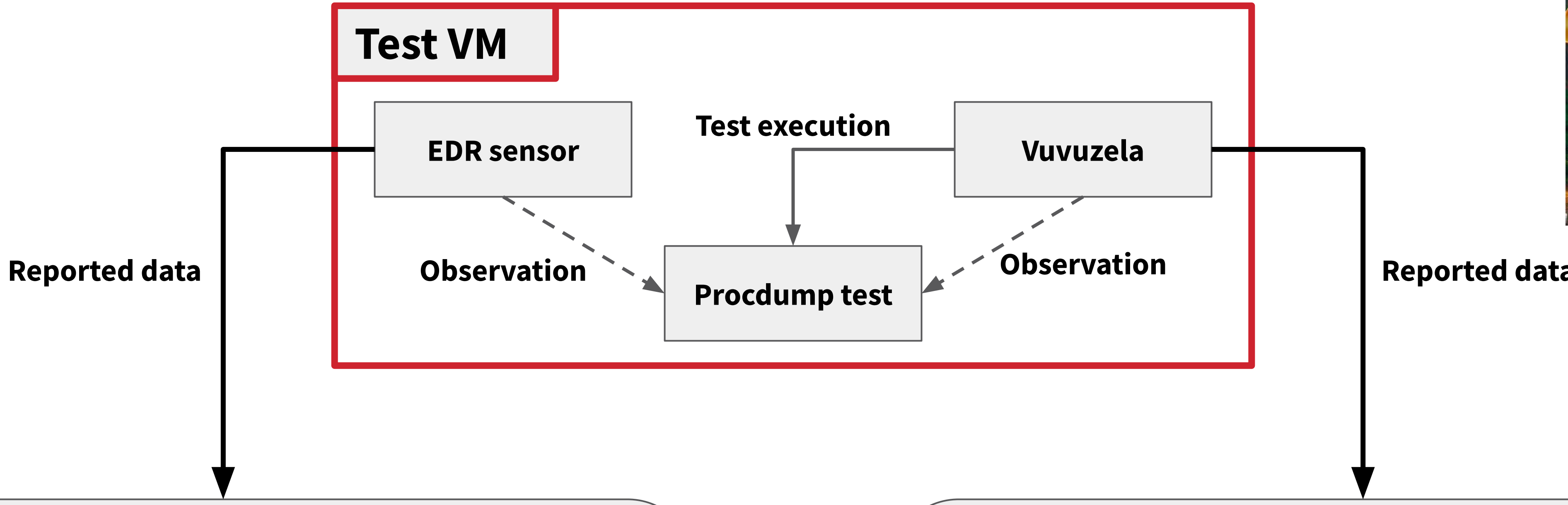
S3 Bucket
Analysis output

SNS

SQS

splunk>

Vuvuzela: Black box testing



Test VM

EDR sensor

Test execution

Vuvuzela

Observation

Procdump test

Observation

Reported data

Reported data

EDR sensor data

"event_type": "process_start"
"process_command_line": "procdump -ma lsass.exe lsass.dmp"
"process_md5": "f2091c44d89789f689d98bc244358878"
"process_name": "procdump.exe"
"process_path": "\Device\HarddiskVolume1\Sysinternals\procdump.exe"
"process_pid": 1529

Mismatch

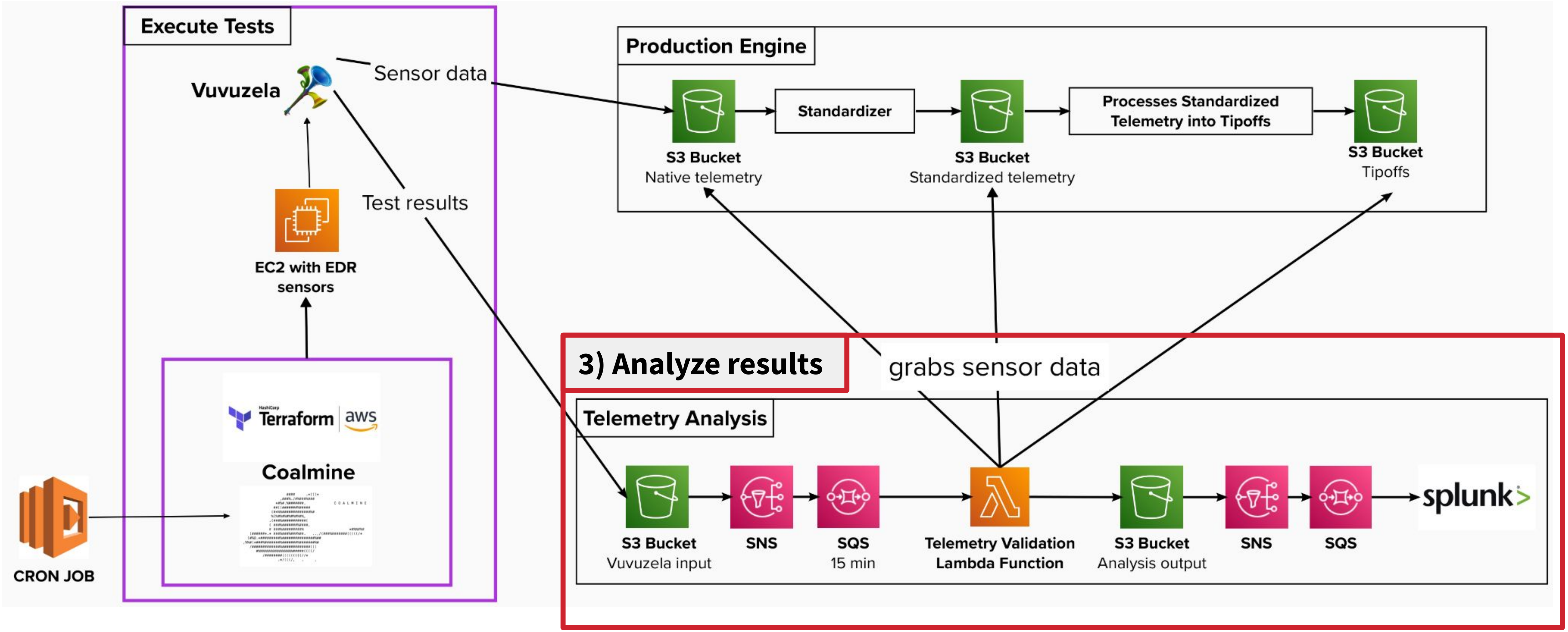
Vuvuzela (OS) data

"event_type": "process_start"
"process_command_line": "procdump -ma lsass.exe lsass.dmp"
"process_md5": "f2091c44d89789f689d98bc244358878"
"process_name": "procdump.exe"
"process_path": "C:\Sysinternals\procdump.exe"
"process_pid": 1528

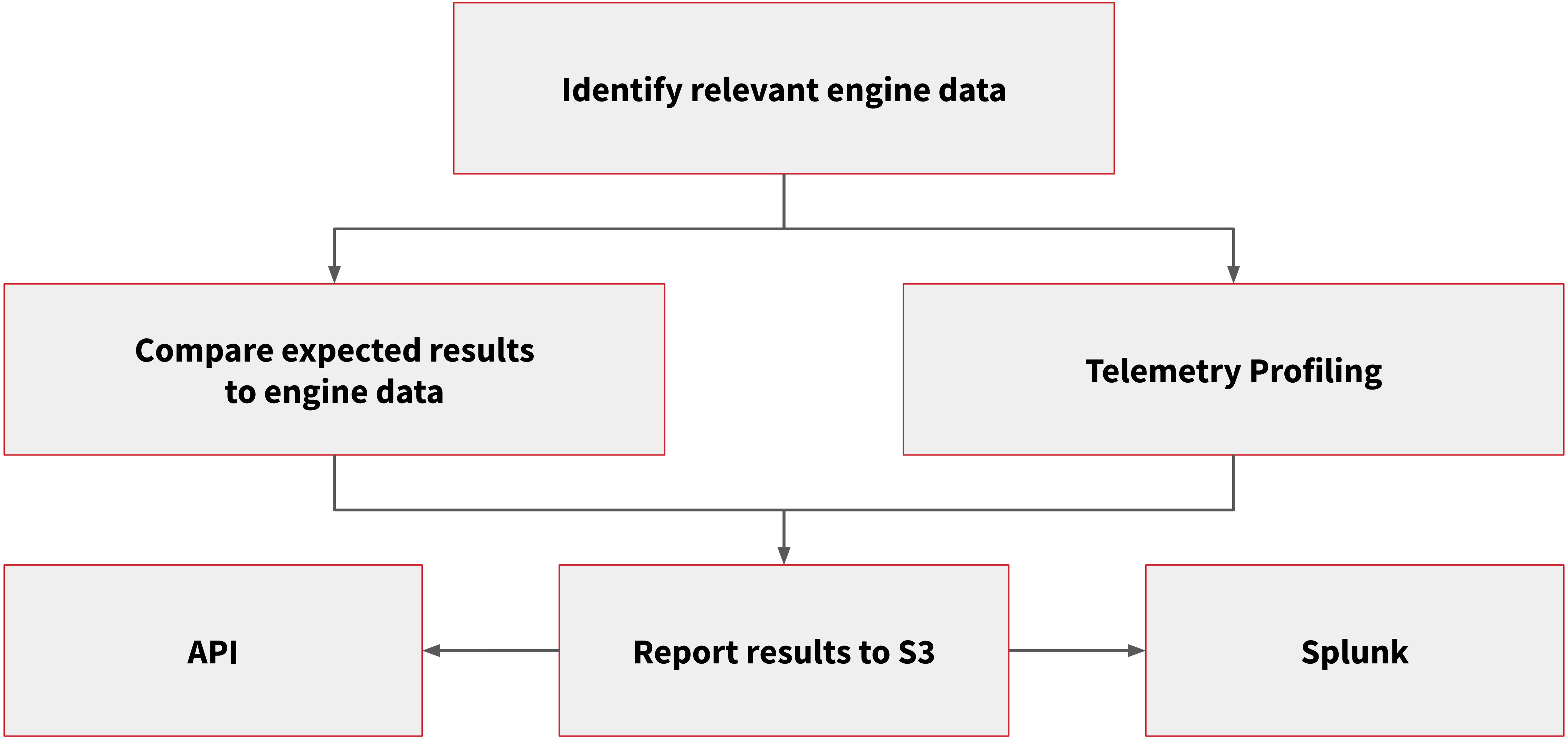
Expected Results Report

- Test sensor/endpoint to identify sensor data
- Expected detection analytics
- Expected standardized telemetry

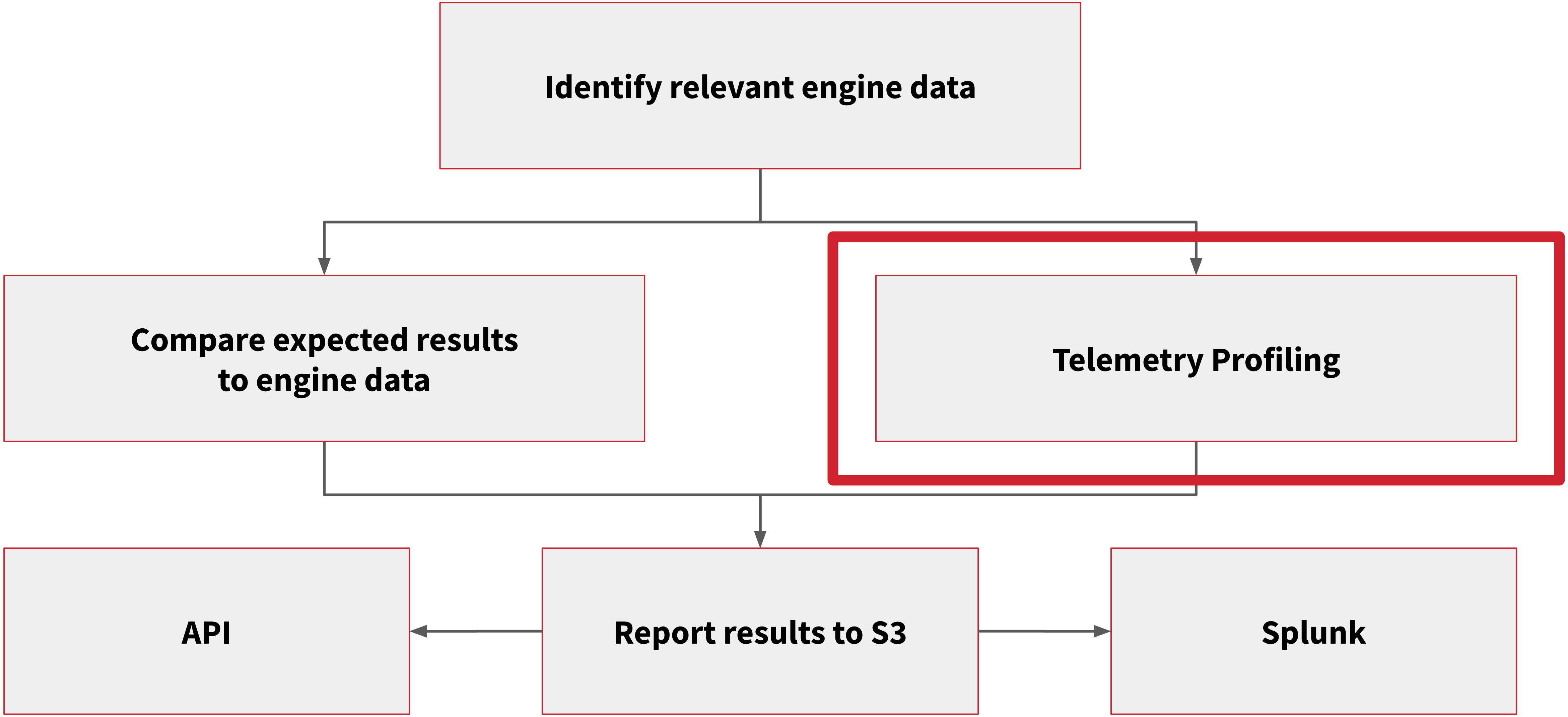
Architecture



Telemetry Validation Lambda Function

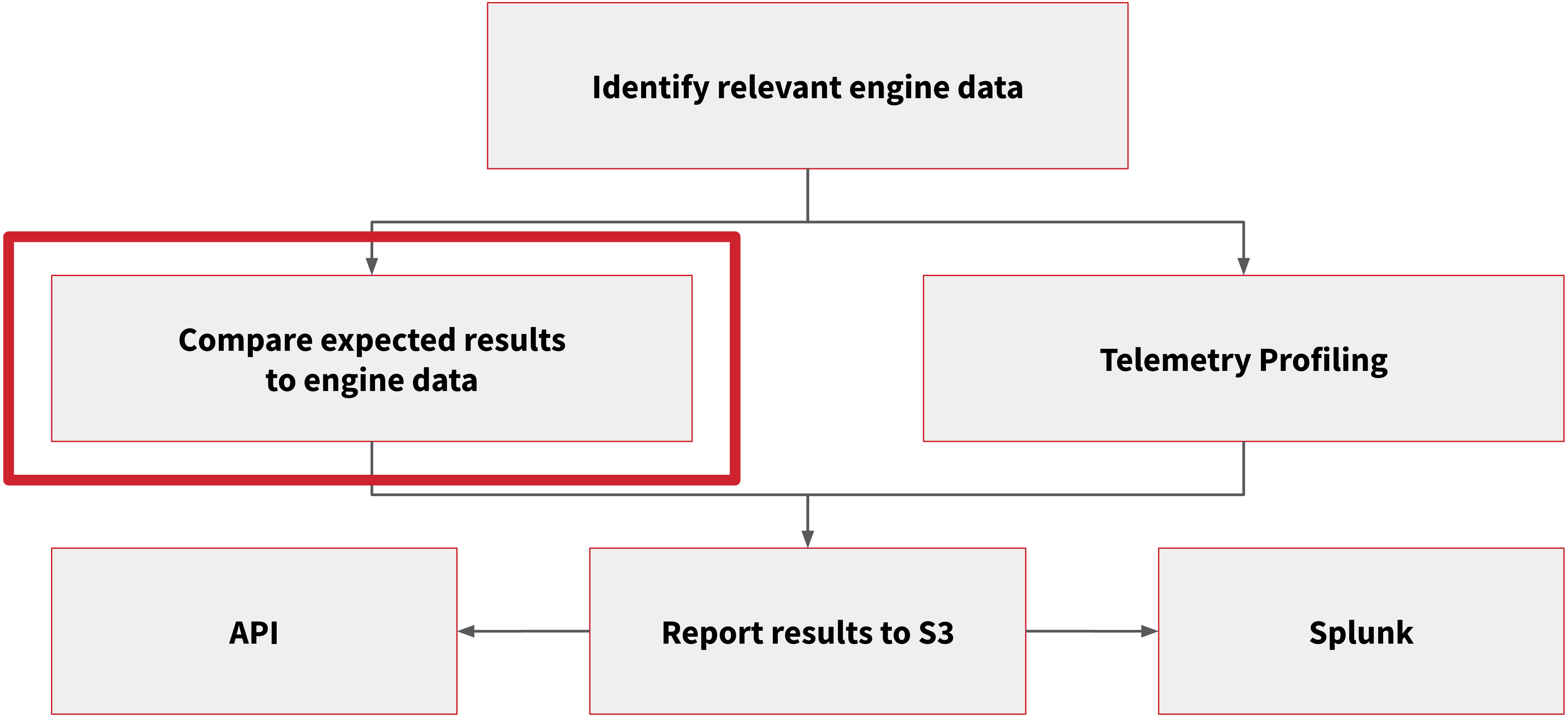

Identify relevant engine data
Compare expected results to engine data
Telemetry Profiling
API
Report results to S3
Splunk

Telemetry Validation Lambda Function

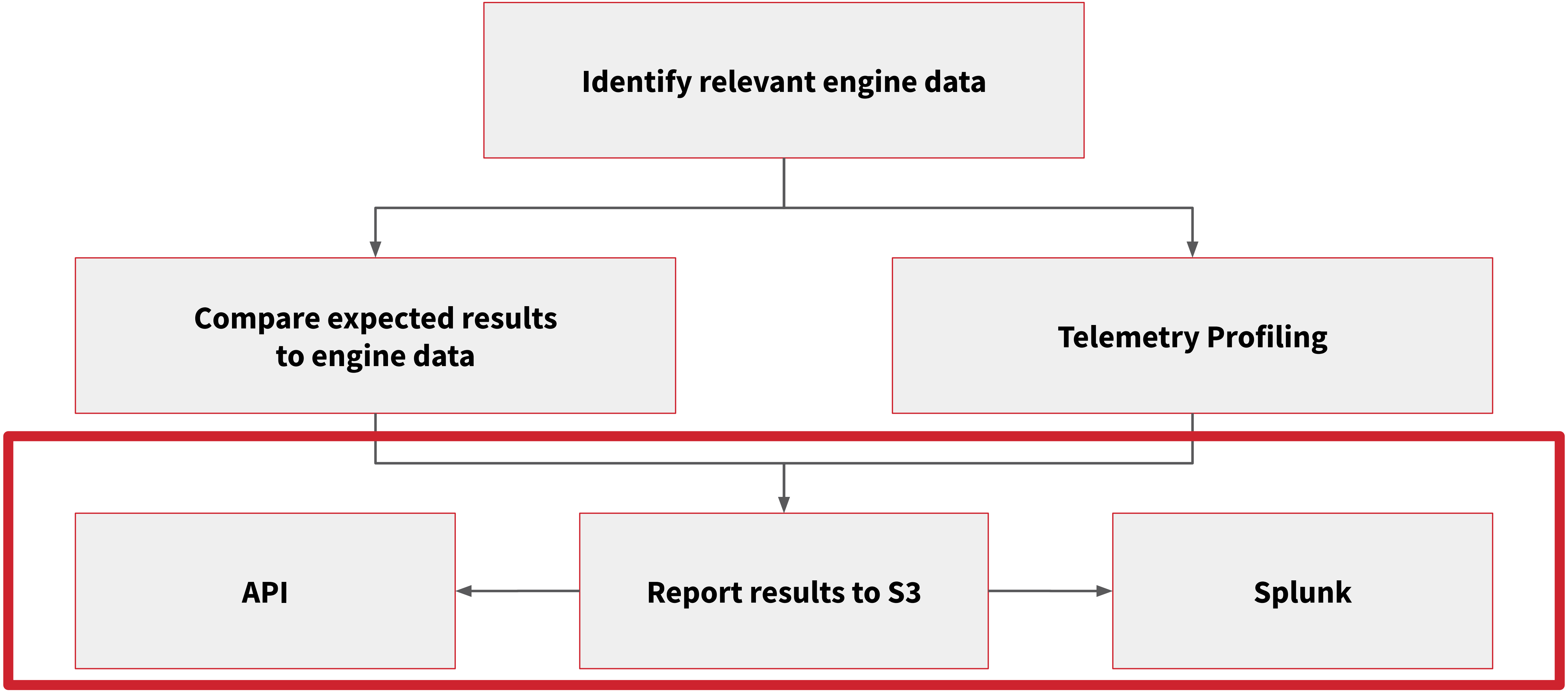


Identify relevant engine data
Compare expected results to engine data
Telemetry Profiling
API
Report results to S3
Splunk

Telemetry Validation Lambda Function


Identify relevant engine data
Compare expected results to engine data
Telemetry Profiling
API
Report results to S3
Splunk

Telemetry Validation Lambda Function


Identify relevant engine data
Compare expected results to engine data
Telemetry Profiling
API
Report results to S3
Splunk

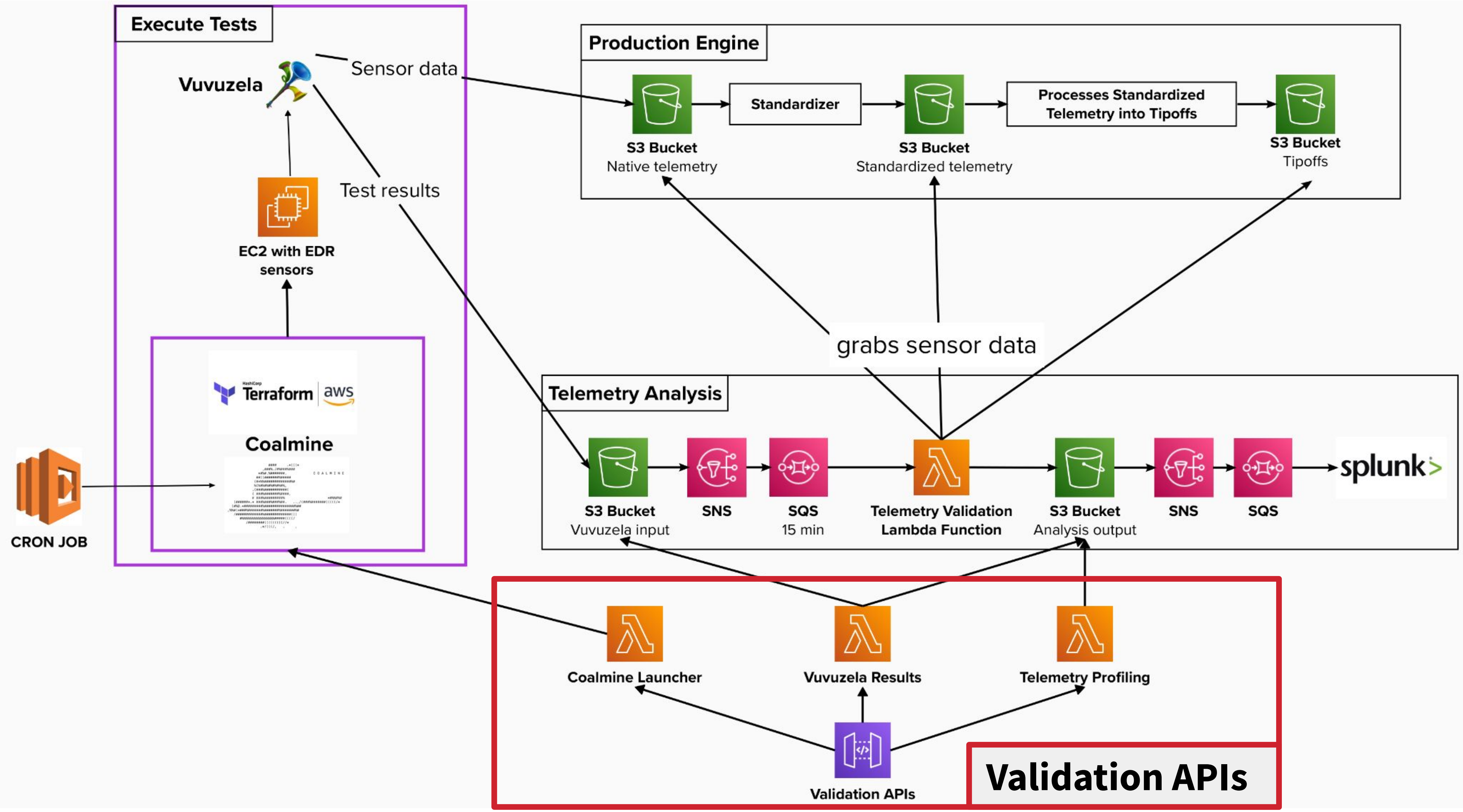
Splunk dashboard example

Valid	Field name	Expected	Found
	process_command_line	procdump -ma lsass.exe lsass.dmp	procdump -ma lsass.exe lsass.dmp
	process_md5	f2091c44d89789f689d98bc244358878	f2091c44d89789f689d98bc244358878
	process_name	procdump.exe	procdump.exe

Skipped	Field name	Expected	Found
	process_sha1	db1ef4ce56820c93a3b7f1fdf36d3fffc7d1ec96	
	process_sha256	e4ea34a7c2b51982a6c42c6367119f34bec9aeb9a609378365400355 83a5b3bc	

Invalid	Field name	Expected	Found
	process_path	C:\Sysinternals\procdump.exe	\Device\HarddiskVolume1\Sysinternals\procdump.exe
	process_pid	1528	1529

Validation APIs



Outline

- What is EDR telemetry?
- How Red Canary works
- Validation of ATT&CK techniques
- Automated validation workflow
- **Lessons learned**

Telemetry quirks

- **Signal/noise ratio different for each sensor**
  - Lower quality telemetry (i.e. filemods & regmods) can be highly filtered
  - Filemod filtering by process, directory, and file type

- **File telemetry has inconsistent meaning/terminology**
  - What is a filemod?
  - Creation vs. modification

Challenges of using EDR telemetry

- **Level of detail is limited**
  - Limited insight into certain types of behaviors like API calls
  - Can’t use static binary signatures outside of a hash
  - Certain telemetry types are limited because they’re noisy
- **Example: Credential theft**
  - Dumping lsass -> good telemetry
  - Application credential theft (e.g. browsers) -> limited/no telemetry
  - EDR sensors are good at generating alerts for this activity

Benefits of using EDR telemetry

- **Offloading detections from endpoints**
  - Avoids limitations of analytics on endpoints
  - Highly scalable
  - Adversary can’t see alerts
- **Versatile representation of behavior**
  - Captures context
  - Useful for correlation

Key takeaways

- **EDR telemetry balances signal/noise**
- **Validating ATT&CK techniques using data components scales well**
- **End-to-end functional testing**
    - Provides a clear signal when there's a problem
    - Captures nuances of techniques
- **Automation allows us to scale validation**
- **Con: EDR telemetry provides a limited level of detail**
- **Pro: EDR telemetry offloads detections from endpoints and provides context around an alert**

Questions?

Team blog series: The Validated Canary

Our validation philosophy
https://redcanary.com/blog/detection-validation/

Unearthing changes in our detection engine with Coalmine
https://redcanary.com/blog/coalmine/