



Aurora Agent

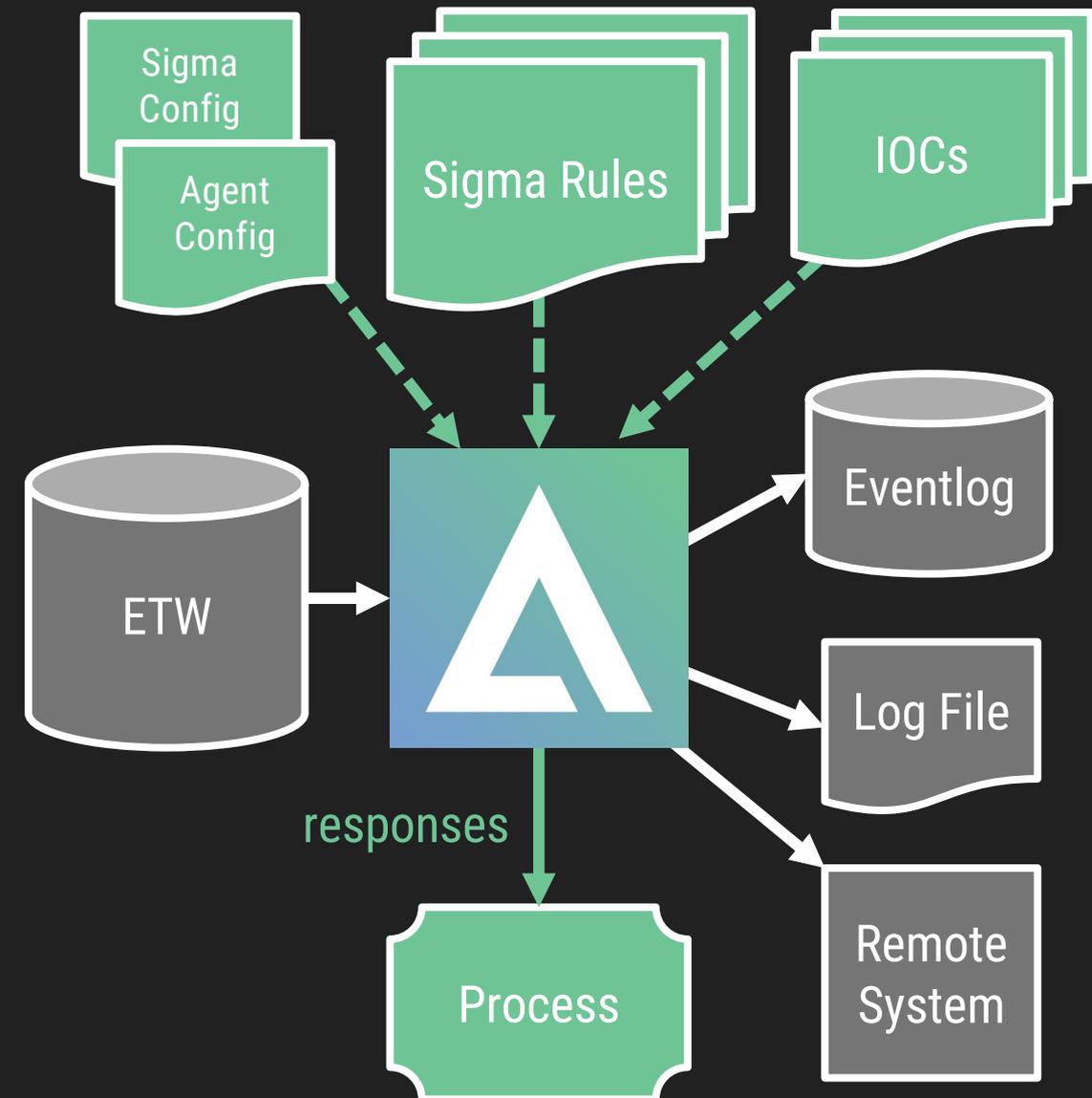
Your custom Sigma-based EDR

What is Aurora?

**A lightweight agent
that applies Sigma rules
on endpoints**

Aurora Agent

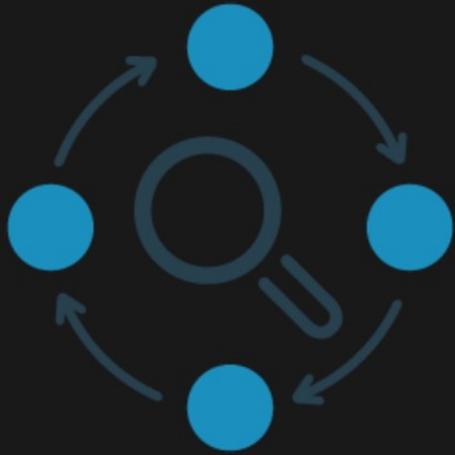
- Lightweight agent that applies Sigma rules on log data in real-time on endpoints
- Uses ETW (Event Tracing for Windows)
- Managed locally via config files or via ASGARD Management Center
- Extends the Sigma standard with 'response' actions
 - Kill, KillParent, Suspend, Dump
 - Custom actions
- Consider it your custom Sigma-based EDR
- Aurora Agent Lite
 - free, lacks comfort features and modules (e.g. Cobalt Strike beaconing detection)



Comparison Sysmon / Aurora

	Sysmon	Aurora
Event Source	Sysmon Kernel Driver	ETW (Event Tracing for Windows)
Sigma Rule Event Coverage	100%	95%
Relative Log Volume	High	Low
Sigma and IOC Matching	No	Yes
Response Actions	No	Yes
Resource Control (CPU Load, Output Throttling)	No	Yes
Output: Eventlog	Yes	Yes
Output: File	No	Yes
Output: TCP / UDP target	No	Yes
Risk: Blue Screen	Yes	No
Risk: High System Load	Yes	No
Risk: Incomplete Data due to Filters	Yes	No

Key Benefits 1/2



100% Transparency

You always know exactly why a rule triggered and can adjust that rule to your needs. Every rule has descriptions and references that explain the author's intentions. No machine learning magic that generates tons of false positives.



Highly Customizable

Create and add your own rules and decide if Aurora should block certain activity. Aurora supports simulated blocks, offers a variety of pre-defined and custom response actions. Let Aurora report into your SIEM or your MDR service provider.



Minimal Network Load and Storage Costs

As the matching happens on the endpoint, Aurora transmits only a fraction of the data that other EDRs generate and transmit to their backends. Usually you'll see less than 1% of the usual network load and storage used by log data collected from Aurora agents.

Key Benefits 2/2



Completely On-Premises

Your confidential data never leaves your network.



Limited Resource Usage

Aurora allows you to throttle its CPU usage and event output rate. These optional throttling options allow you to set priorities and put your system's stability first.

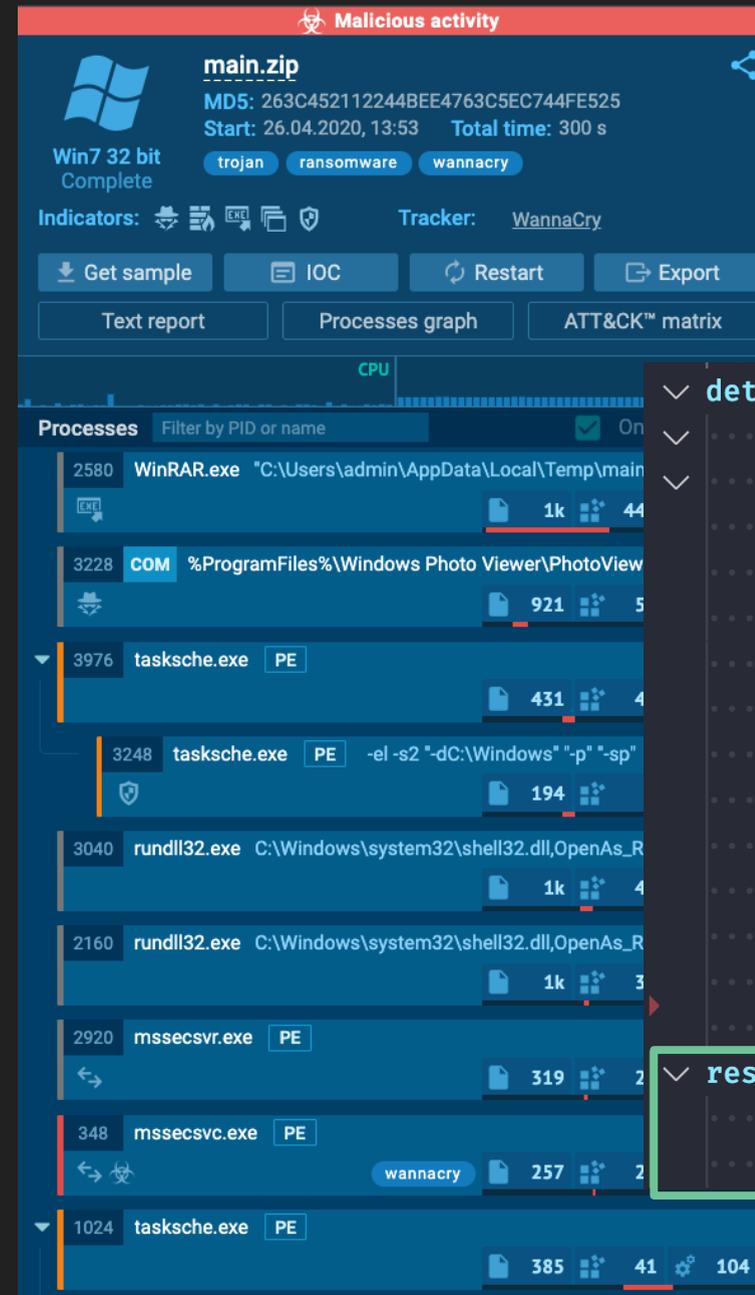


Free Version

Aurora Lite is a limited version of Aurora and free of charge. It's a great way to give it a whirl. All we ask for is a newsletter subscription.

Response Actions

- Use Sigma to detect a threat
- Add a response action
 - Predefined
 - Kill a process or parent process
 - Suspend a process
 - Dump process memory
 - Custom
 - A custom command line that can make use of environment variables and the event's values e.g. copy %Image% %%ProgramData%%\%ProcessId%.bin
- Contains threats in less than a second



Ransomware Example

Sigma Rule with Response

```

detection:
  selection1:
    - Image|endswith:
      - '\tasksche.exe'
      - '\mssecsvc.exe'
      - '\taskdl.exe'
      - '\taskhsvc.exe'
      - '\taskse.exe'
      - '\111.exe'
      - '\lhdfrgui.exe'
      - '\diskpart.exe'
      - '\linuxnew.exe'
      - '\wannacry.exe'
    - Image|contains: 'WanaDecryptor'
  condition: 1 of them

response:
  type: predefined
  action: kill
  
```

Response Action

Aurora – First Steps

Aurora Agent Package

Place the license file in the extracted folder

The downloaded archive

Utility that provides updates & other auxiliary functions

This x86 and x64 versions of the agent

The different configuration presets
(the one with the 'standard.yml' suffix is used by default)

Signature set that gets shipped with the agent

ETW log sources and field mappings

Manual and license acknowledgements

Your custom Sigma rules and other IOCs
(i.e. hash values, filename or C2 IOCs, named pipes etc.)

Name	Date modified	Type	Size
aurora-flo-2022.lic	2/16/2022 5:11 AM	LIC File	1 KB
aurora-agent-win-pack.zip	2/16/2022 5:01 AM	Compressed...	16,424 KB
aurora-agent-util.exe	2/18/2022 12:36 AM	Application	6,808 KB
aurora-agent-64.exe	2/18/2022 12:36 AM	Application	15,265 KB
aurora-agent.exe	2/18/2022 12:36 AM	Application	13,150 KB
agent-config-standard.yml	2/18/2022 12:36 AM	YML File	1 KB
agent-config-reduced.yml	2/18/2022 12:36 AM	YML File	1 KB
agent-config-minimal.yml	2/18/2022 12:36 AM	YML File	1 KB
agent-config-intense.yml	2/18/2022 12:36 AM	YML File	1 KB
signatures	2/18/2022 12:36 AM	File folder	
log-sources	2/18/2022 12:36 AM	File folder	
docs	2/18/2022 12:36 AM	File folder	
custom-signatures	2/18/2022 12:36 AM	File folder	

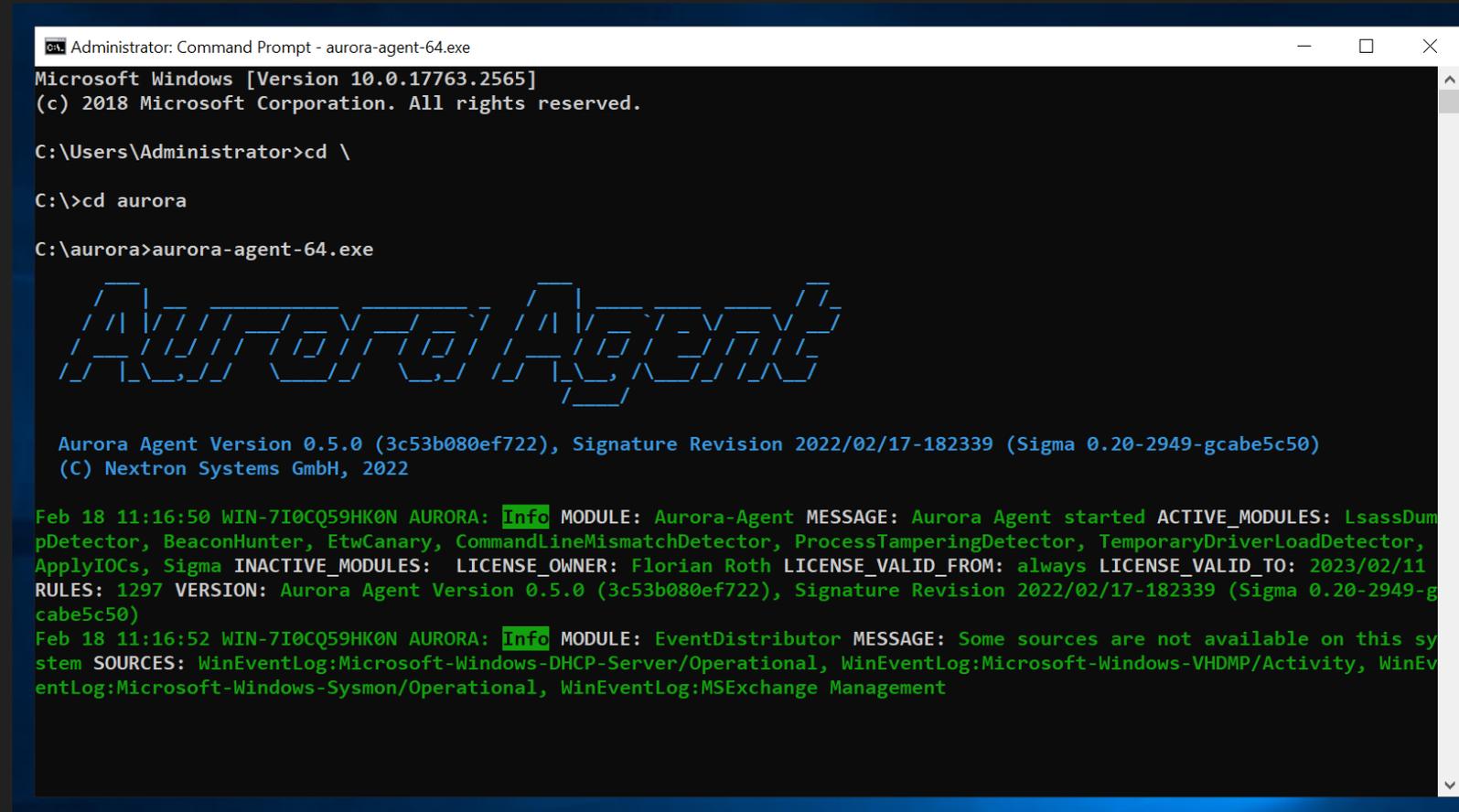
A First Run

Let's just run Aurora a first time to get a feeling for it

Steps:

- Start cmd.exe as Administrator
- Change to the extracted program folder
- Run: `aurora-agent-64.exe`

CTRL+C stops Aurora



```

Administrator: Command Prompt - aurora-agent-64.exe
Microsoft Windows [Version 10.0.17763.2565]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd \

C:\>cd aurora

C:\aurora>aurora-agent-64.exe

Aurora Agent

Aurora Agent Version 0.5.0 (3c53b080ef722), Signature Revision 2022/02/17-182339 (Sigma 0.20-2949-gcabe5c50)
(C) Nexttron Systems GmbH, 2022

Feb 18 11:16:50 WIN-7I0CQ59HK0N AURORA: Info MODULE: Aurora-Agent MESSAGE: Aurora Agent started ACTIVE_MODULES: LsassDumpDetector, BeaconHunter, EtwCanary, CommandLineMismatchDetector, ProcessTamperingDetector, TemporaryDriverLoadDetector, ApplyIOCs, Sigma INACTIVE_MODULES: LICENSE_OWNER: Florian Roth LICENSE_VALID_FROM: always LICENSE_VALID_TO: 2023/02/11 RULES: 1297 VERSION: Aurora Agent Version 0.5.0 (3c53b080ef722), Signature Revision 2022/02/17-182339 (Sigma 0.20-2949-gcabe5c50)
Feb 18 11:16:52 WIN-7I0CQ59HK0N AURORA: Info MODULE: EventDistributor MESSAGE: Some sources are not available on this system SOURCES: WinEventLog:Microsoft-Windows-DHCP-Server/Operational, WinEventLog:Microsoft-Windows-VHDMP/Activity, WinEventLog:Microsoft-Windows-Sysmon/Operational, WinEventLog:MSExchange Management
  
```

Usage Help

Let's see what the help has to offer

Steps:

- Run:
`aurora-agent-64.exe --help`

Don't worry. We won't need all options. Looking over the different command line flags will give you a first impression of the feature set and the many customizing options.

```
Administrator: Command Prompt
C:\aurora>aurora-agent-64.exe --help

Aurora Agent

Aurora Agent Version 0.6.0 (62b63beac8336), Signature Revision 2022/03/01-143433 (Sigma 0.20)
(C) Nexttron Systems GmbH, 2022

Usage of aurora-agent-64.exe:
  --activate-module strings      Activate the given deactivated modules (see --module-info for a list)
  --activate-responses           Execute responses that are specified in Sigma rules (e.g. --rule-id)
  --agent-name string            Set a different name for the service, the binary and other files
  -a, --auto-reload              Automatically reload the Sigma rules after changes
  -c, --config string            Use parameters from this YAML file
  --cpu-limit int                CPU usage (as percentage) that the Aurora Agent should not exceed
  --deactivate-all-consumers    Deactivate all consumers, except for those specified by --module-info
  --deactivate-module strings    Deactivate the given modules (see --module-info for a list)
  --debug                        Print debugging information
  --dump-folder string           Folder where process dumps should be stored (default "C:\aurora\dumps")
  --false-positive-filter string Path to a file containing false positive regexes (one per line)

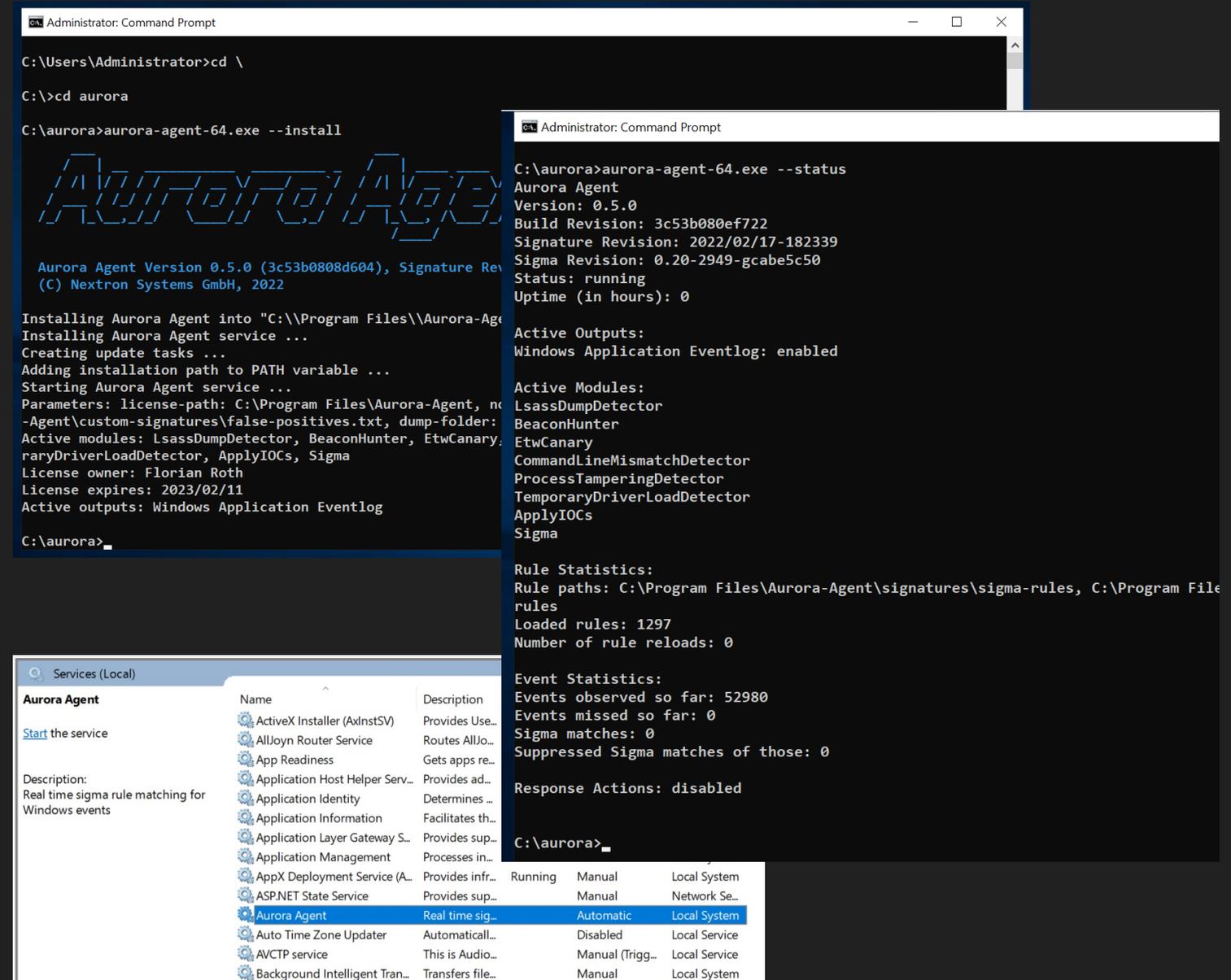
  --help                        Show help
  --install                     Install Aurora Agent as a service
  --ioc-path strings             Folders containing IOC files (default [C:\aurora\signature\ioc])
  --json                         Write output as JSON instead of plain text
  --license-path string          Path to the directory containing the Aurora Agent license
  --log-rotate uint              How many log rotations should be retained (default 7)
  --log-size string              Maximum file size for the log file. It will be rotated if it reaches this size
  -s, --log-source strings       Paths to the Sigma log sources that should be loaded (default ["%SystemRoot%\System32\log-sources-standard.yml", "C:\aurora\log-sources\etw-log-source-mappings.yml"])
  -l, --logfile string           Path to log file (default: no log file)
  --low-prio                     Run Aurora Agent with low process priority (can cause minor performance issues)
  --match-burst uint            Number of matches for a single rule that are allowed to be reported at once
  --match-throttling string      Minimum average time between matches. Sigma Rules with --match-throttling "medium" will report matches with a minimum average time of 5 seconds
  --minimum-level string         Report Sigma matches with rules of this level or higher (e.g. "medium")
  --module-info                 List all available modules and whether they are active
  --no-content-enrichment       Deactivate calculations that rely on disk access (e.g. --rule-id)
  --no-eventlog                  Don't log matches to the Windows event log
  --no-stdout                    Disable logging to the standard output
  --output-throttling string     Minimum average time between log messages (Warning: If set to 0, the output will be throttled)
  --pprof                       Start a server with debugging information on port 8080
```

Install Aurora as a Service

Let's install Aurora as a service

Steps:

- Start cmd.exe as Administrator
- Change to the extracted program folder
- Run: `aurora-agent-64.exe --install`
- Check the agents status with: `aurora-agent-64.exe --status`



The image displays two screenshots from a Windows Command Prompt running as Administrator.

The first screenshot shows the installation process:

```
C:\Users\Administrator>cd \
C:\>cd aurora
C:\aurora>aurora-agent-64.exe --install
```

The output shows the Aurora Agent logo and installation details:

```
Aurora Agent Version 0.5.0 (3c53b0808d604), Signature Rev (C) Nextron Systems GmbH, 2022
Installing Aurora Agent into "C:\Program Files\Aurora-Agent"
Installing Aurora Agent service ...
Creating update tasks ...
Adding installation path to PATH variable ...
Starting Aurora Agent service ...
Parameters: license-path: C:\Program Files\Aurora-Agent, no
-Agent\custom-signatures>false-positives.txt, dump-folder:
Active modules: LsassDumpDetector, BeaconHunter, EtwCanary,
raryDriverLoadDetector, ApplyIOCs, Sigma
License owner: Florian Roth
License expires: 2023/02/11
Active outputs: Windows Application Eventlog
C:\aurora>_
```

The second screenshot shows the status of the Aurora Agent service:

```
C:\aurora>aurora-agent-64.exe --status
Aurora Agent
Version: 0.5.0
Build Revision: 3c53b080ef722
Signature Revision: 2022/02/17-182339
Sigma Revision: 0.20-2949-gcabe5c50
Status: running
Uptime (in hours): 0

Active Outputs:
Windows Application Eventlog: enabled

Active Modules:
LsassDumpDetector
BeaconHunter
EtwCanary
CommandLineMismatchDetector
ProcessTamperingDetector
TemporaryDriverLoadDetector
ApplyIOCs
Sigma

Rule Statistics:
Rule paths: C:\Program Files\Aurora-Agent\signatures\sigma-rules, C:\Program File
rules
Loaded rules: 1297
Number of rule reloads: 0

Event Statistics:
Events observed so far: 52980
Events missed so far: 0
Sigma matches: 0
Suppressed Sigma matches of those: 0

Response Actions: disabled
C:\aurora>_
```

The third screenshot shows the Windows Services console with the Aurora Agent service installed and running:

Name	Description	Startup Type	Log On As
Aurora Agent	Real time sigma rule matching for Windows events	Automatic	Local System

Function Tests and Event Review

Okay, now we verify that Aurora works as expected with a simple function test

Steps:

- Start cmd.exe as Administrator
- Run: `whoami /priv`
- Open the EventViewer and go to "Application"
- Look for the source "Aurora Agent"
- Select the "Details" Tab
- Review the event information

The image displays two screenshots. The top screenshot is a Command Prompt window showing the output of the `whoami /priv` command, which lists various system privileges and their states (e.g., Disabled, Enabled). The bottom screenshot is the Windows Event Viewer, showing the 'Application' log. A specific event from 'Aurora Agent' is selected, and the 'Details' tab is active, showing the event's description: 'Sigma rule match found: Run Whoami Showing Privileges (see Details tab for more information)'. The event data includes the rule title 'Run Whoami Showing Privileges', the author 'Florian Roth', and a description of the rule's function: 'Detects a whoami.exe executed with the /priv command line flag instructing the tool to show all current user privileges. This is often used after a privilege escalation attempt.'

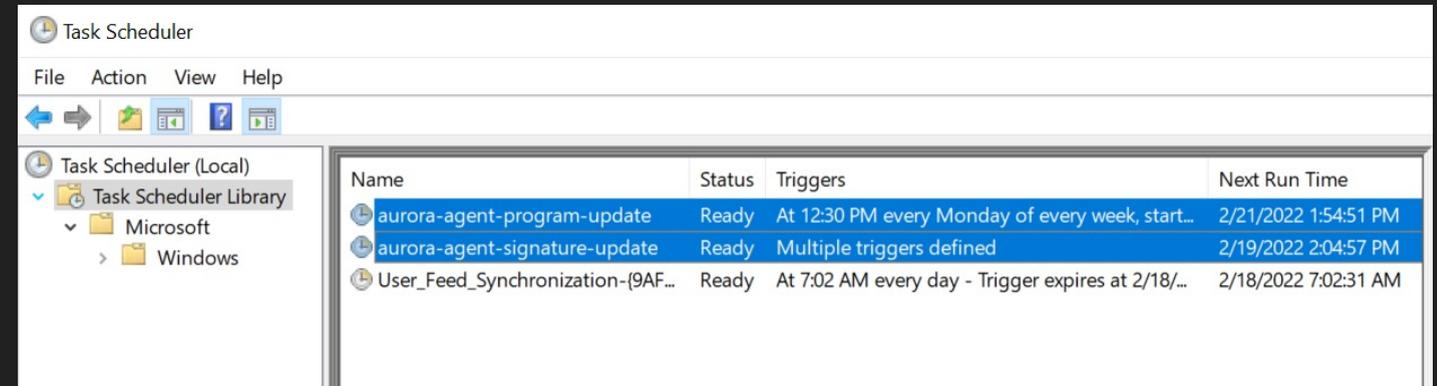
Update Aurora and Signatures

When you install Aurora as a service, two scheduled tasks are created to update the program (weekly) and the signatures (daily)

However, you can trigger an update manually using the “aurora-agent-util”

Steps:

- Start cmd.exe as Administrator
- Change directory to “C:\Program Files\Aurora-Agent” (service) or the extracted program folder, e.g. “C:\aurora” (standalone)
- Run `aurora-agent-util.exe upgrade`
- Get usage help for all functions of the utility with `aurora-agent-util.exe help`



Great!

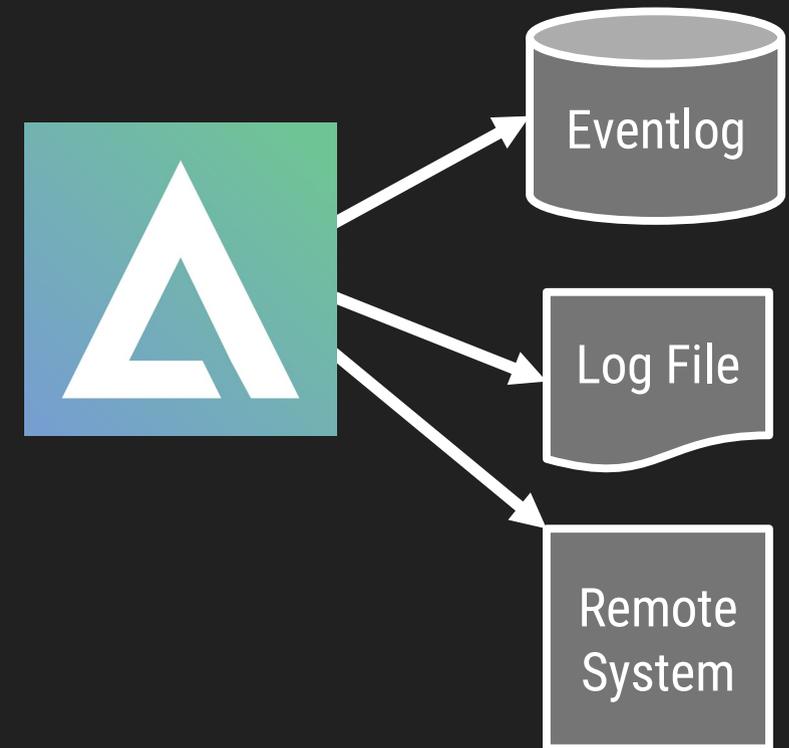
Aurora is up and running.

Now let's look at some customization options

Output Configuration

Aurora supports 3 different output channels

- The Windows Eventlog (Application)
deactivate with:
`--no-eventlog`
- A log file (automatically rotated)
`--log-file aurora-events.log`
- A remote system (UDP, TCP, plain or JSON)
`--udp-target oursyslog.internal`



More information:

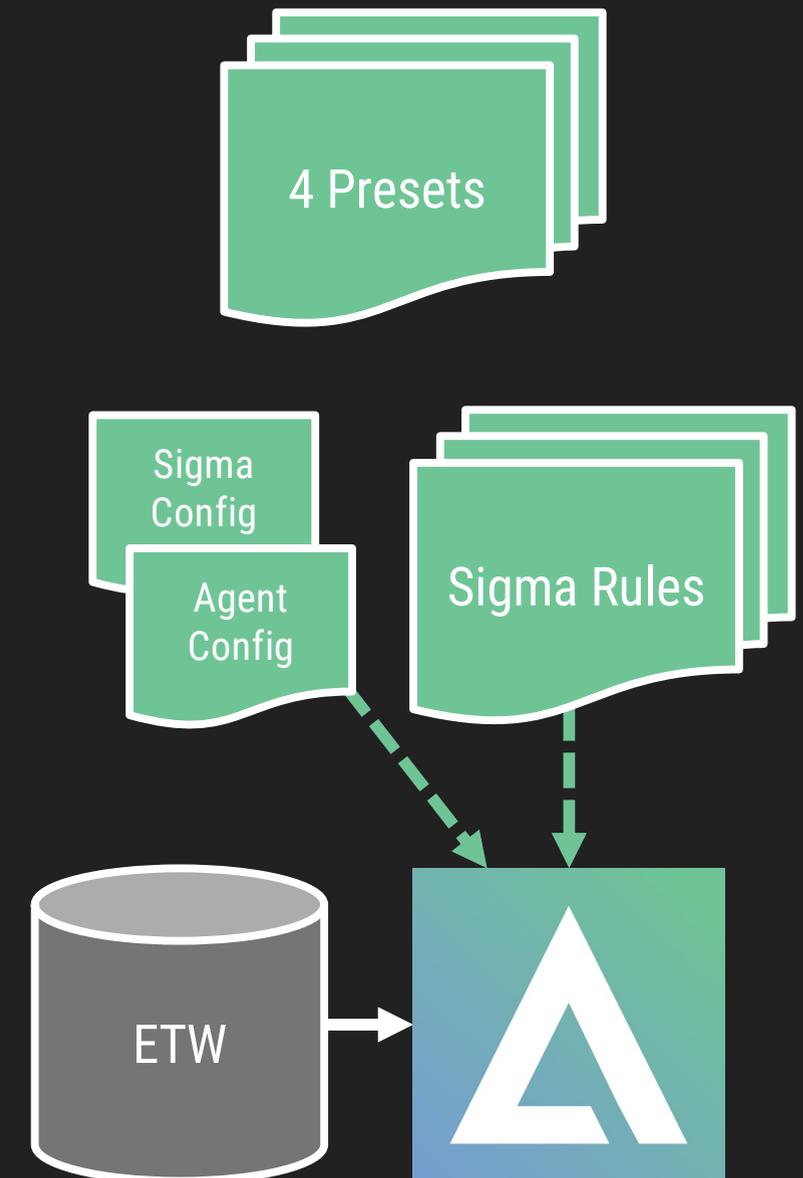
<https://aurora-agent-manual.nexttron-systems.com/en/latest/usage/configuration.html#output-options>

Configuration Presets

Aurora includes 4 configuration presets that select different ETW log sources and add/remove different log enrichment modules

- Standard
(implicitly used – doesn't have to be specified)
- Reduced `-c agent-config-reduced.yml`
TLDR; No process access events, CPU limit to 30%, minimum level "high"
- Minimal `-c agent-config-minimal.yml`
TLDR; no hash calculations, CPU limit 20%, no LSASS dump check, no Beacon Hunter, no Image load and Create Remote Thread events
- Intense `-c agent-config-intense.yml`
TLDR; every reasonable input activated, no limits

More information:
<https://aurora-agent-manual.nexttron-systems.com/en/latest/usage/configuration.html>

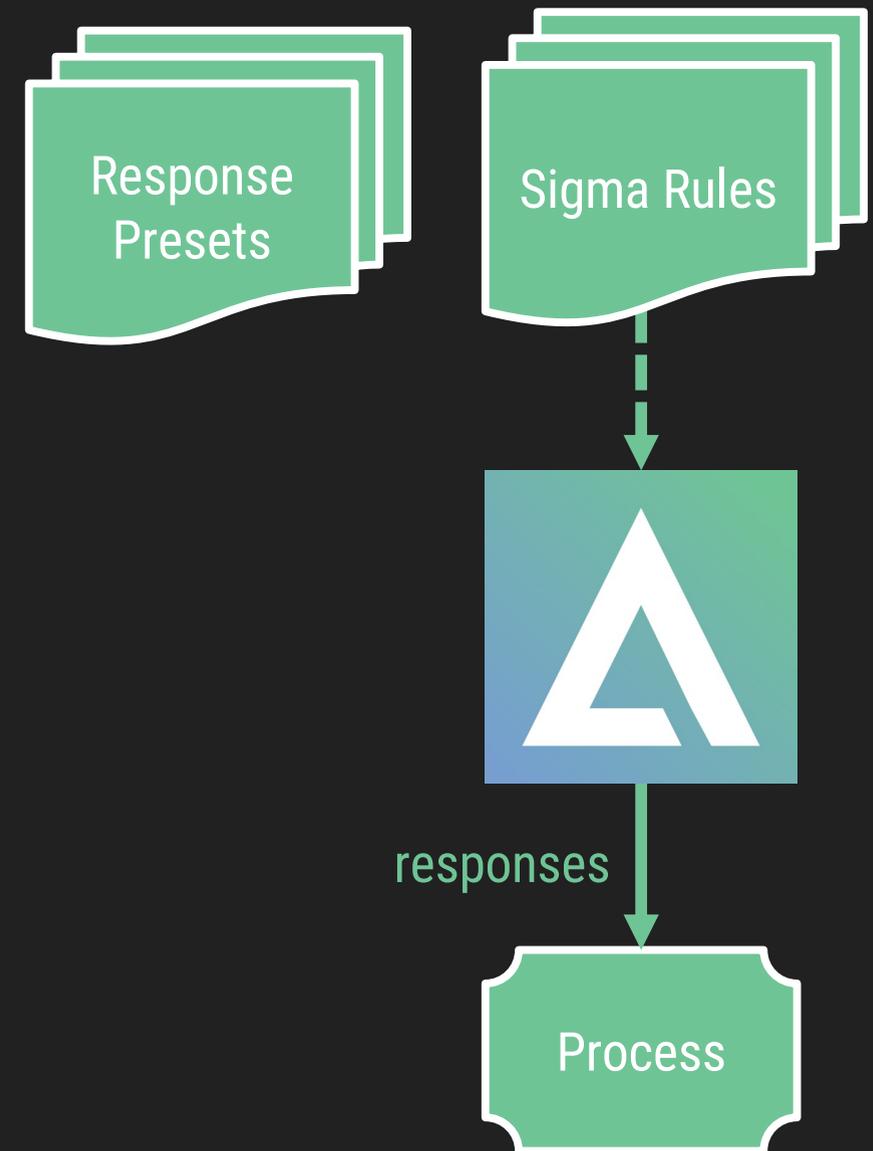


Response Presets

Aurora comes with several presets that help you select the recommended response for a given use case

```
--response-set ransomware.yml --activate-responses
```

This way you don't have to review all 1000+ rules and select the ones that you want to see blocked



```
ransomware.yml ●
1  description: Nextron Preset Responses for Ransomware (kill)
2  id: ee481a18-1f08-41f0-8418-1b0f90dee312
3  group: ransomware
4  response:
5    · type: predefined
6    · action: kill
7    · lowprivonly: true
8    · ancestors: all
9  rule-ids:
10  · -- '87df9ee1-5416-453a-8a08-e8d4a51e9ce1' · -- # Delete Volume Shadow Copies Via WMI With PowerShell
11  · -- 'ae9c6a7c-9521-42a6-915e-5aaa8689d529' · -- # CobaltStrike Load by Rundll32
12  · -- 'e17121b4-ef2a-4418-8a59-12fb1631fa9e' · -- # Delete Volume Shadow Copies via WMI with PowerShell
13  · -- 'c7a74c80-ba5a-486e-9974-ab9e682bc5e4' · -- # Created Files by Office Applications
14
```

More information:

<https://aurora-agent-manual.nextron-systems.com/en/latest/usage/responses.html>

The Cool Stuff

Features that make Aurora great

IOC Application

Example: Type Filenames

- The effectiveness of filename patterns is highly underrated
- Malware and attackers use repeating patterns, why shouldn't we?
- We apply these patterns in many different events: process creation, file creation, image loads, handle events, driver loads

```
# LSASS Dump Names
\\lsass[a-zA-Z_\-\.]{1,16}\.(dmp|zip|rar|7z);70

# Programs or scripts in C:\ProgramData folder (no sub folder)
:\\ProgramData\\[^\\]{1,40}\.(EXE|DLL|exe|dll|bat|BAT|vbs|VBS|ps1|jar)([^\._\\]|$);70

# Archive in suspicious folder
:\\ProgramData\\[\w]{1,6}\.(zip|7z|rar);$;40

# Typical Malware Location - AppData / Local / Roaming
(?:)\\AppData\\[^\\]{1,64}\.exe([^\._\\]|$);75
(?:)\\AppData\\[^\\]{1,64}\.(dll|bat|vbs|ps1|js|hta);80
(?:)\\AppData\\Local\\[^\\]{1,64}\.exe([^\._\\]|$);75
(?:)\\AppData\\Local\\[^\\]{1,64}\.(dll|bat|vbs|ps1|hta);80
(?:)\\AppData\\Roaming\\[^\\]{1,64}\.exe$;75
(?:)\\AppData\\Roaming\\[^\\]{1,64}\.(dll|bat|vbs|ps1|hta);80
```

We also apply: C2 FQDNs, IPs, Named Pipes, Handles, File Hashes

Unique New Fields

- Since Aurora generates only a few events, we said:

“Why not add new fields that are helpful in evaluating the event?”

e.g.

The field **ProcessTree** allows you to write rules like:

“If new process powershell.exe and w3wp.exe somewhere in the process tree.”

The field **FileAge** allows you to write rules like:

“If access to lsass.exe process memory and FileAge starts with 00d00h00m.”

```
GrandparentCommandLine: c:\windows\system32\inetsrv\w3wp.exe -ap "DefaultAppPool" -v
"v4.0" -l "webengine4.dll" -a \\.\pipe\iisipm8ff443c1-cfe8-4a0d-ac14-a9816f37bb80 -h
"C:\inetpub\temp\appools\DefaultAppPool\DefaultAppPool.config" -w "" -m 0 -t 20 -ta 0
GrandparentImage: C:\Windows\System32\inetsrv\w3wp.exe
GrandparentProcessId: 4728
```

```
ParentProcessId: 5296
ParentUser: IIS APPPOOL\DefaultAppPool
ProcessId: 4400
ProcessTree: C:\Windows\System32\wininit.exe|C:\Windows\System32
\services.exe|C:\Windows\System32\svchost.exe|C:\Windows\System32
\inetsrv\w3wp.exe|C:\Windows\System32\cmd.exe|C:\Windows\System32\whoami.exe
Product: Microsoft® Windows® Operating System
Provider_Guid: {3D6FA8D0-FE05-11D0-9DDA-00C04FD7BA7C}
Provider_Name: SystemTraceProvider-Process
```

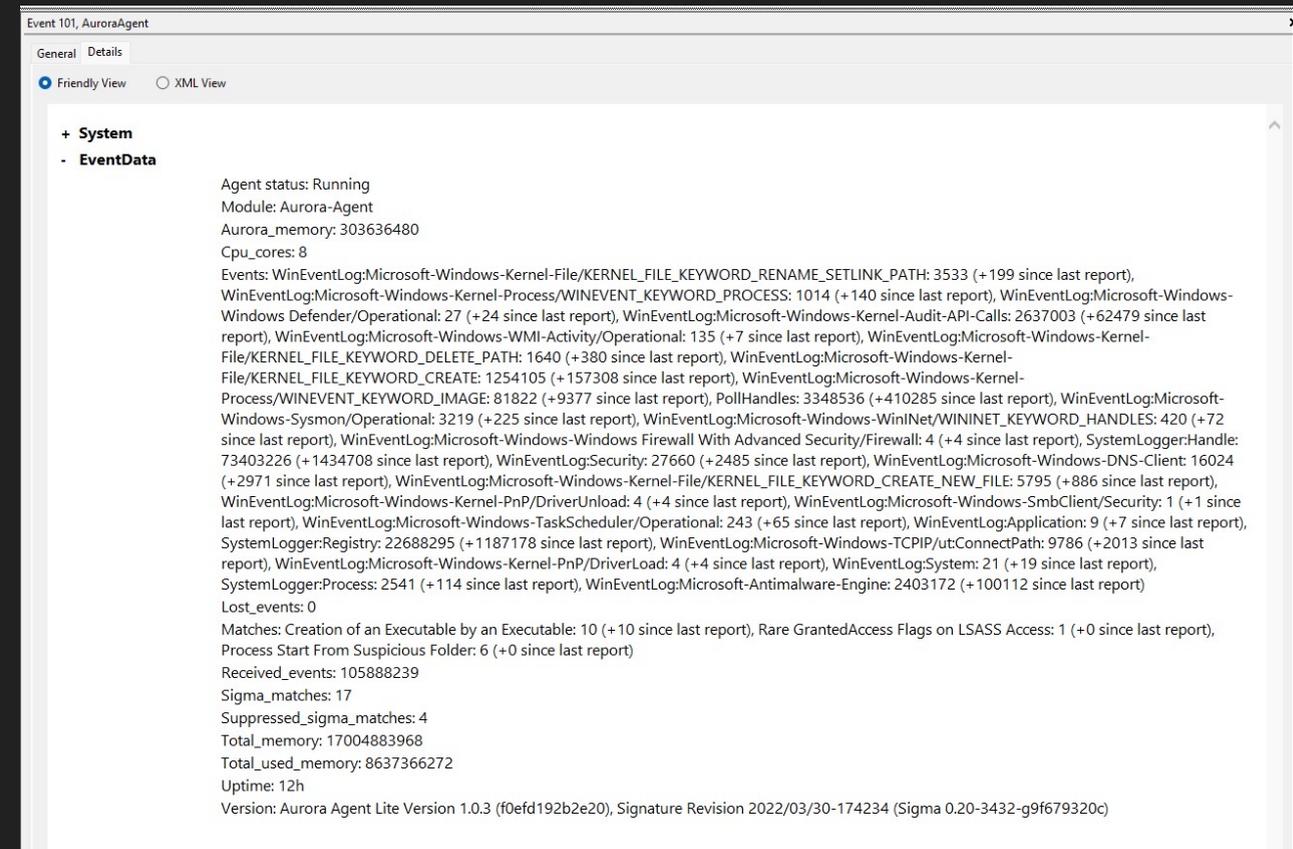
```
Field: ImageLoaded
FileAge: 00d00h14m12s
FileCreationDate: 2022-03-30T06:16:03
```

Statistics Reporting

- Reports event statistics at frequent intervals
- Allows you to monitor the agents for manipulations
 - Attacker disables / stops agent
 - Attacker disables ETW
 - Attacker tampers with ETW event channels
- The idea: you cannot completely rule out manipulations of the agents – but you can detect them!
- Get it as plain text or JSON with “diff” values to last report, e.g.

Microsoft-Windows-Kernel-Audit-API-Calls: 260000 (+4400 since last report)

*^ this is great for monitoring ;
diff is 0 = tampering with ETW*

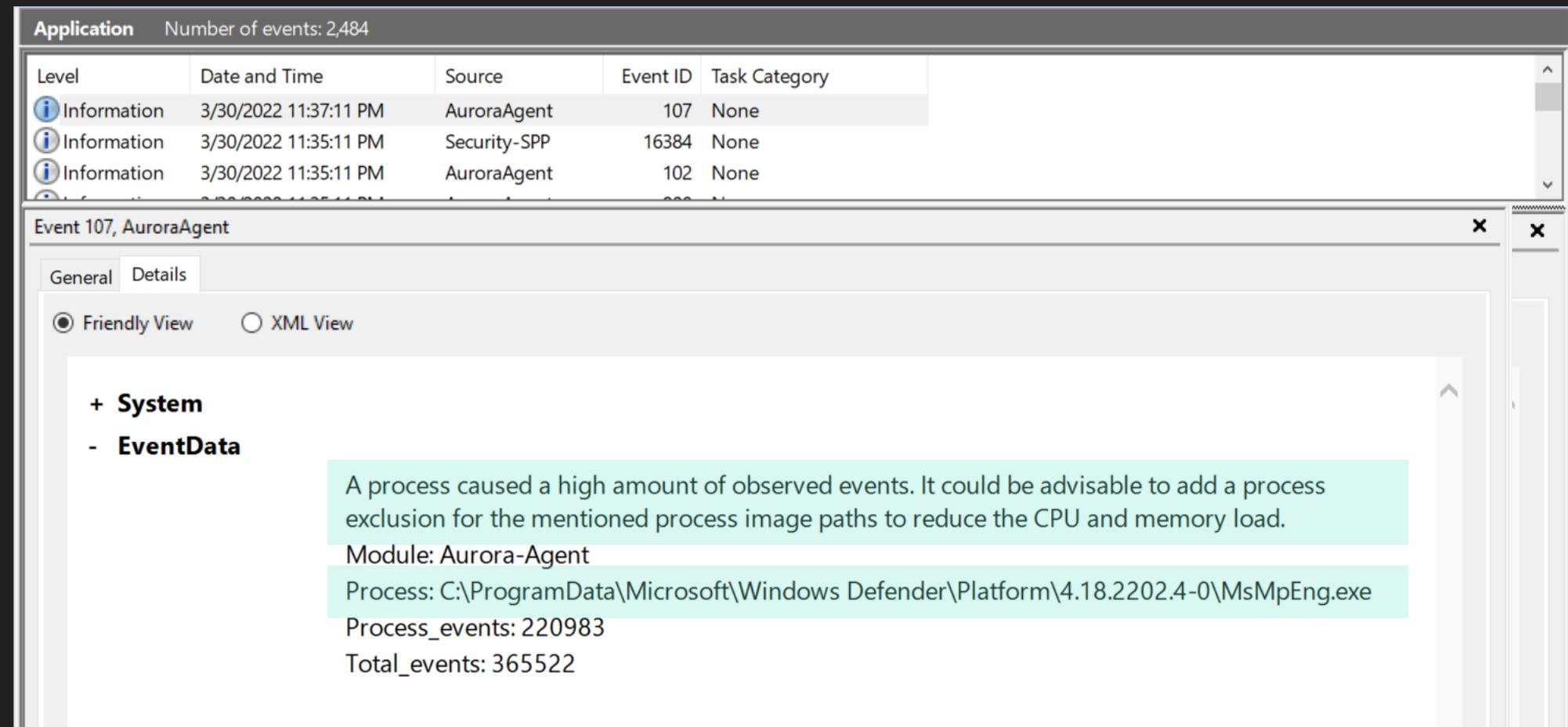


```
--report-stats
--report-stats-interval string
--report-stats-verbose
```

```
Log a message about the current agent status regularly
Interval between status messages when --report-stats is enabled (default "1h")
Include more details in --report-stats messages, such as received events per channel
```

Reports Extraordinary Event Producers

- Aurora highlights events producers that are responsible for over 50% of the observed events and recommends an exclusion



The screenshot displays the Aurora Agent interface. At the top, it shows 'Application' with 'Number of events: 2,484'. Below this is a table of event log entries:

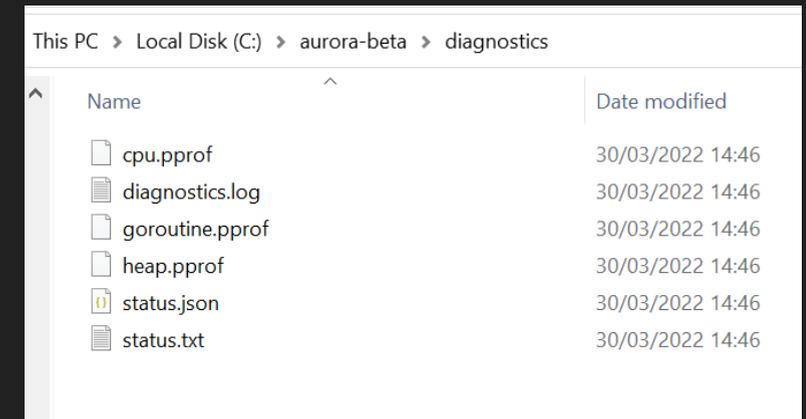
Level	Date and Time	Source	Event ID	Task Category
Information	3/30/2022 11:37:11 PM	AuroraAgent	107	None
Information	3/30/2022 11:35:11 PM	Security-SPP	16384	None
Information	3/30/2022 11:35:11 PM	AuroraAgent	102	None

Below the table, a detailed view for 'Event 107, AuroraAgent' is shown. It includes tabs for 'General' and 'Details', and radio buttons for 'Friendly View' (selected) and 'XML View'. The event details are organized into expandable sections:

- + System**
- EventData**
 - A process caused a high amount of observed events. It could be advisable to add a process exclusion for the mentioned process image paths to reduce the CPU and memory load.
 - Module: Aurora-Agent
 - Process: C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2202.4-0\MsMpEng.exe
 - Process_events: 220983
 - Total_events: 365522

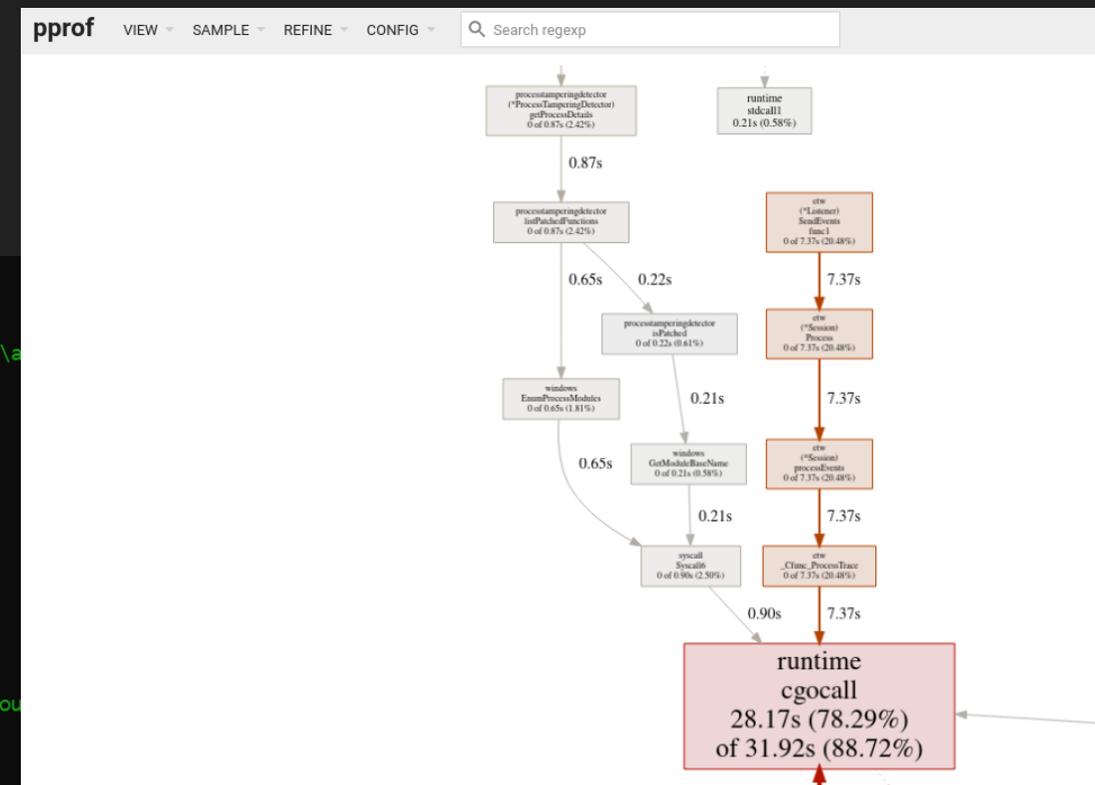
Diagnostics

- Generate a package with diagnostics data
- Can help you ...
 - find and exclude top event producers
 - Identify modules that cause higher CPU usage and disable them
 - debug agents that show abnormal behavior



```

C:\aurora-beta>aurora-agent-util.exe diagnostics
Mar 30 12:44:46 HYPERION AURORA: Info MODULE: Aurora-Agent MESSAGE: Creating diagnostics pack. This might take a while...
Mar 30 12:44:46 HYPERION AURORA: Info MODULE: Aurora-Agent MESSAGE: Searching for agent process
Mar 30 12:44:46 HYPERION AURORA: Info MODULE: Aurora-Agent MESSAGE: Found Aurora process EXECUTABLE: C:\Program Files\Aurora-Agent\aurora-agent.exe PID: 12272
Mar 30 12:44:46 HYPERION AURORA: Info MODULE: Aurora-Agent MESSAGE: Searching for Aurora service
Mar 30 12:44:46 HYPERION AURORA: Info MODULE: Aurora-Agent MESSAGE: Found Aurora service STATUS: 1
Mar 30 12:44:46 HYPERION AURORA: Info MODULE: Aurora-Agent MESSAGE: Searching for Aurora service startup log
Mar 30 12:44:46 HYPERION AURORA: Info MODULE: Aurora-Agent MESSAGE: Requesting agent status
Mar 30 12:44:46 HYPERION AURORA: Info MODULE: Aurora-Agent MESSAGE: Packed full agent status to ZIP FILE: status.json
Mar 30 12:44:46 HYPERION AURORA: Info MODULE: Aurora-Agent MESSAGE: Packed human readable agent status to ZIP FILE: status.txt
Mar 30 12:44:46 HYPERION AURORA: Info MODULE: Aurora-Agent MESSAGE: Requesting agent profile PROFILE: cpu
Mar 30 12:45:05 HYPERION AURORA: Info MODULE: Aurora-Agent MESSAGE: Packed agent profile to ZIP FILE: cpu.pprof PROFILE: cpu
Mar 30 12:45:05 HYPERION AURORA: Info MODULE: Aurora-Agent MESSAGE: Requesting agent profile PROFILE: heap
Mar 30 12:45:05 HYPERION AURORA: Info MODULE: Aurora-Agent MESSAGE: Packed agent profile to ZIP FILE: heap.pprof PROFILE: heap
Mar 30 12:45:05 HYPERION AURORA: Info MODULE: Aurora-Agent MESSAGE: Requesting agent profile PROFILE: goroutine
Mar 30 12:45:05 HYPERION AURORA: Info MODULE: Aurora-Agent MESSAGE: Packed agent profile to ZIP FILE: goroutine.pprof PROFILE: goroutine
Mar 30 12:45:05 HYPERION AURORA: Info MODULE: Aurora-Agent MESSAGE: Packed diagnostics log to ZIP FILE: diagnostics.log
Mar 30 12:45:05 HYPERION AURORA: Info MODULE: Aurora-Agent MESSAGE: Created diagnostics pack FILE: diagnostics.zip
    
```



Custom Service Name

- Choose a service name to hide Aurora's presence from simple attempts to detect it

```

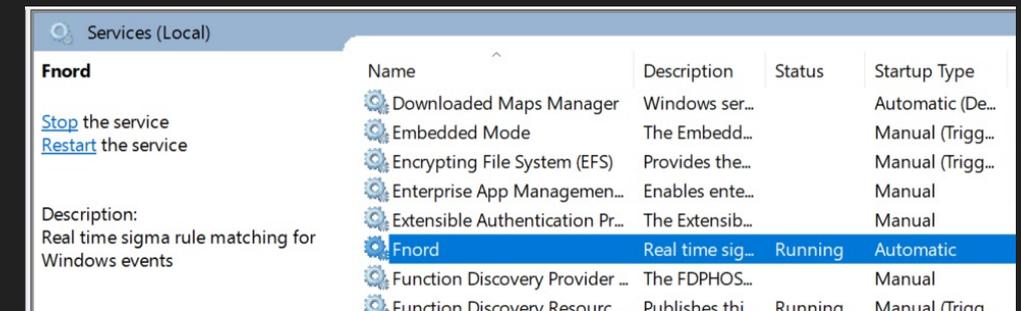
Administrator: Command Prompt
C:\aurora>aurora-agent-64.exe --install --agent-name Fnord

Aurora Agent

Aurora Agent Version 1.0.1 (c7fd171ab216b), Signature Revision 2022/03/29-135547 (Sigma 0.20-3418-g7cd65a73)
(C) Nexttron Systems GmbH, 2022

Installing Aurora Agent into "C:\\Program Files\\Fnord" ...
Installing Aurora Agent service ...
Creating update tasks ...
Adding installation path to PATH variable ...
Starting Aurora Agent service ...
Parameters: license-path: C:\Program Files\Fnord, agent-name: Fnord, no-stdout: true, false-positive-filter: C:\Program
Files\Fnord\config>false-positives.cfg, dump-folder: C:\Program Files\Fnord\process-dumps, process-excludes: C:\Program
Files\Fnord\config\process-excludes.cfg
Active modules: LsassDumpDetector, BeaconHunter, EtwCanary, CommandLineMismatchDetector, ProcessTamperingDetector, Tempo
raryDriverLoadDetector, ApplyIOCs, Rescontrol, Sigma, ETWSource, ETWKernelSource, EventlogSource, PollHandles
License owner: Florian Roth
License expires: 2023/02/11
Active outputs: Windows Application Eventlog

C:\aurora>
  
```



Process Name	Memory Usage
svchost.exe	1,592 K
svchost.exe	4,140 K
svchost.exe	8,560 K
SecurityHealthService.exe	3,856 K
svchost.exe	1,612 K
Fnord-64.exe	0.77 211,668 K
lsass.exe	7,288 K
fontdrvhost.exe	1,596 K
csrss.exe	< 0.01 2,556 K
winlogon.exe	3,376 K
fontdrvhost.exe	4,532 K
dwm.exe	< 0.01 103,408 K

Getting Started

Visit the contact form and mention “Aurora Agent”
<https://www.nexttron-systems.com/get-started/>

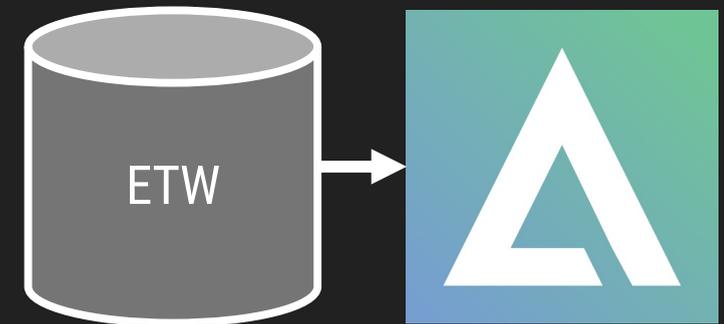


Extra Slides

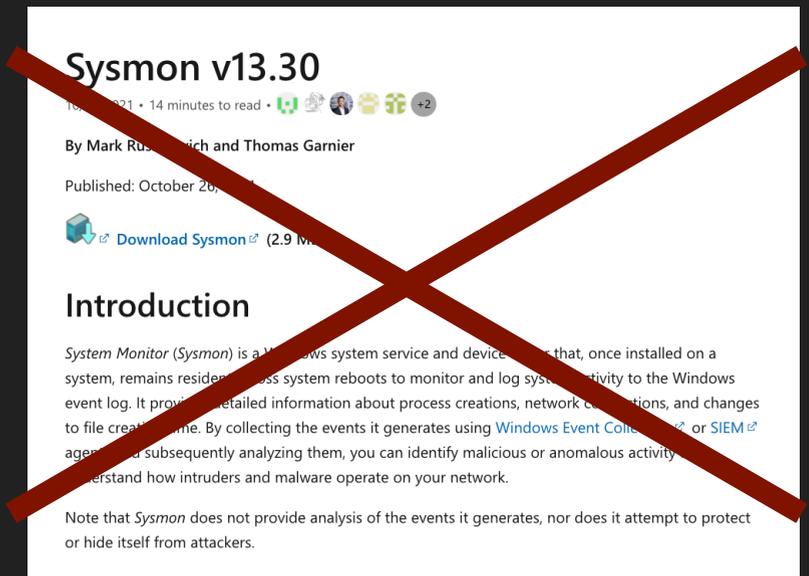
Used for discussions regarding some of the features

Independence and Stability

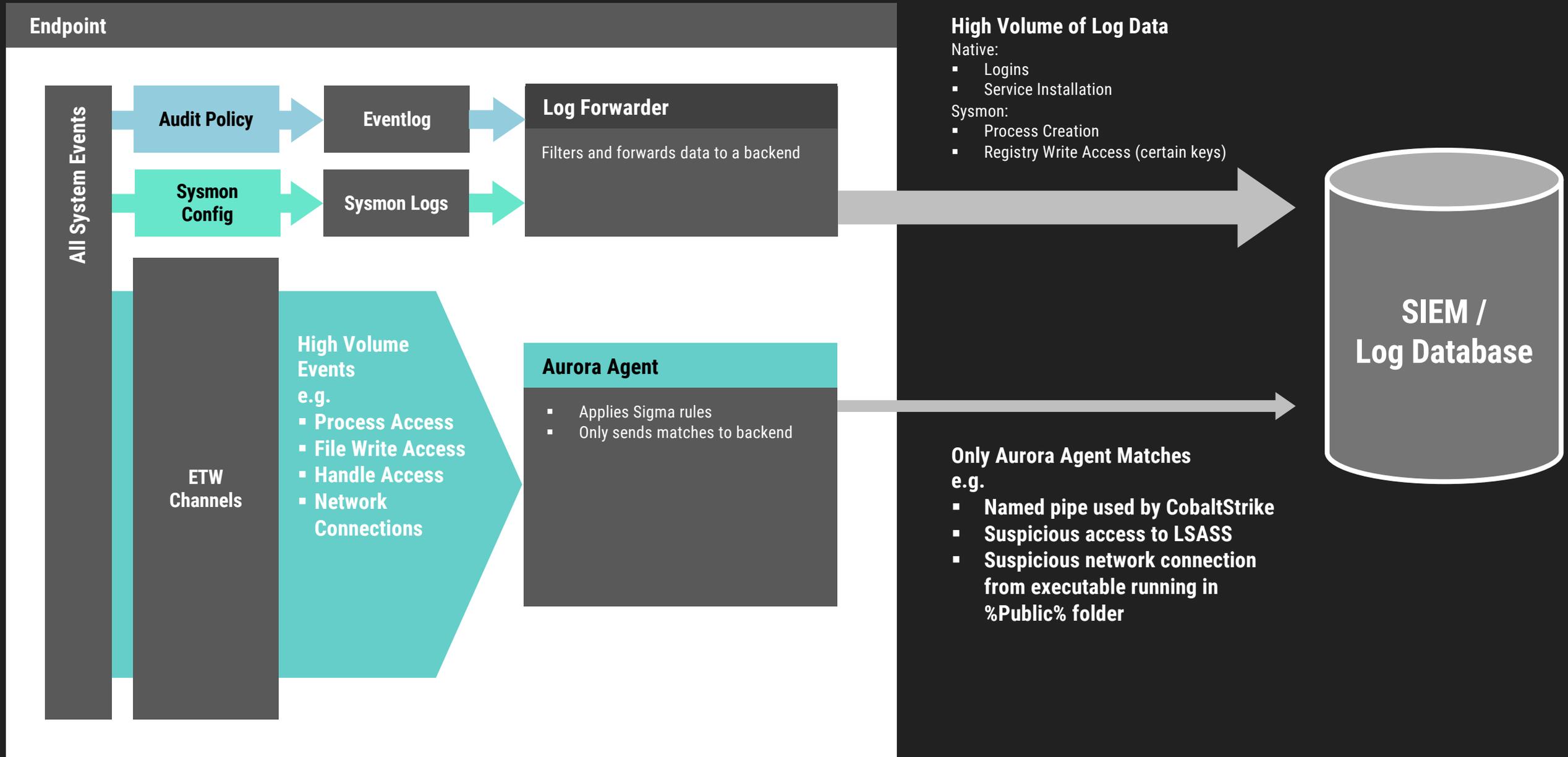
- No specific Windows audit policy required
- No Sysmon required
- We tap into ETW, recreate 90%* of the events used in Sysmon and apply Sigma rules to them
- No Kernel Driver used (no blue screens)
 - Disadvantage: we miss some events (NamedPipe events, in some corner cases the CommandLine of a process)



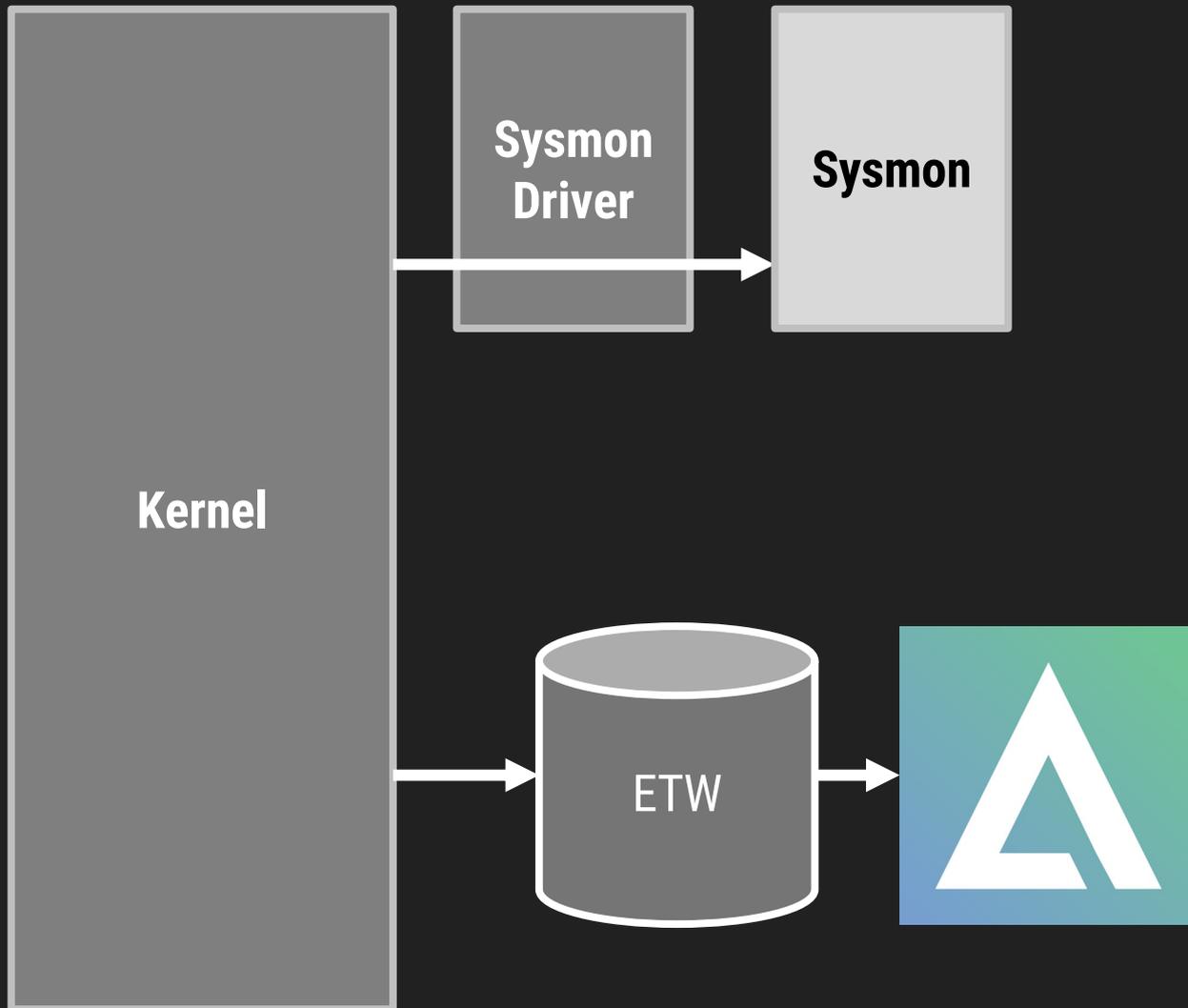
*some event types & fields may not be available in the first release version, but the most important ones



Reduced Log Volume



Recreation of Sysmon-like Events in Aurora



Event ID 1: Process Creation
 ProcessID
 Image
 ParentImage
 CommandLine
 Hash
 ...
 Event ID 2: A process changed a file creation time
 Event ID 3: Network connection
 Event ID 4: Sysmon service state change
 Event ID 5: Process Terminated
 Event ID 6: Driver loaded
 ImageLoaded
 Hashes
 Signature
 SignatureStatus

Event ID 1: Process Creation
 ProcessID
 Image
 ParentImage
 CommandLine
 Hash
 ...
 Event ID 2: A process changed a file creation time
 Event ID 3: Network connection
 Event ID 4: Sysmon service state change
 Event ID 5: Process Terminated
 Event ID 6: Driver loaded
 ImageLoaded
 Hashes
 Signature
 SignatureStatus

Percentage of
Event / Fields

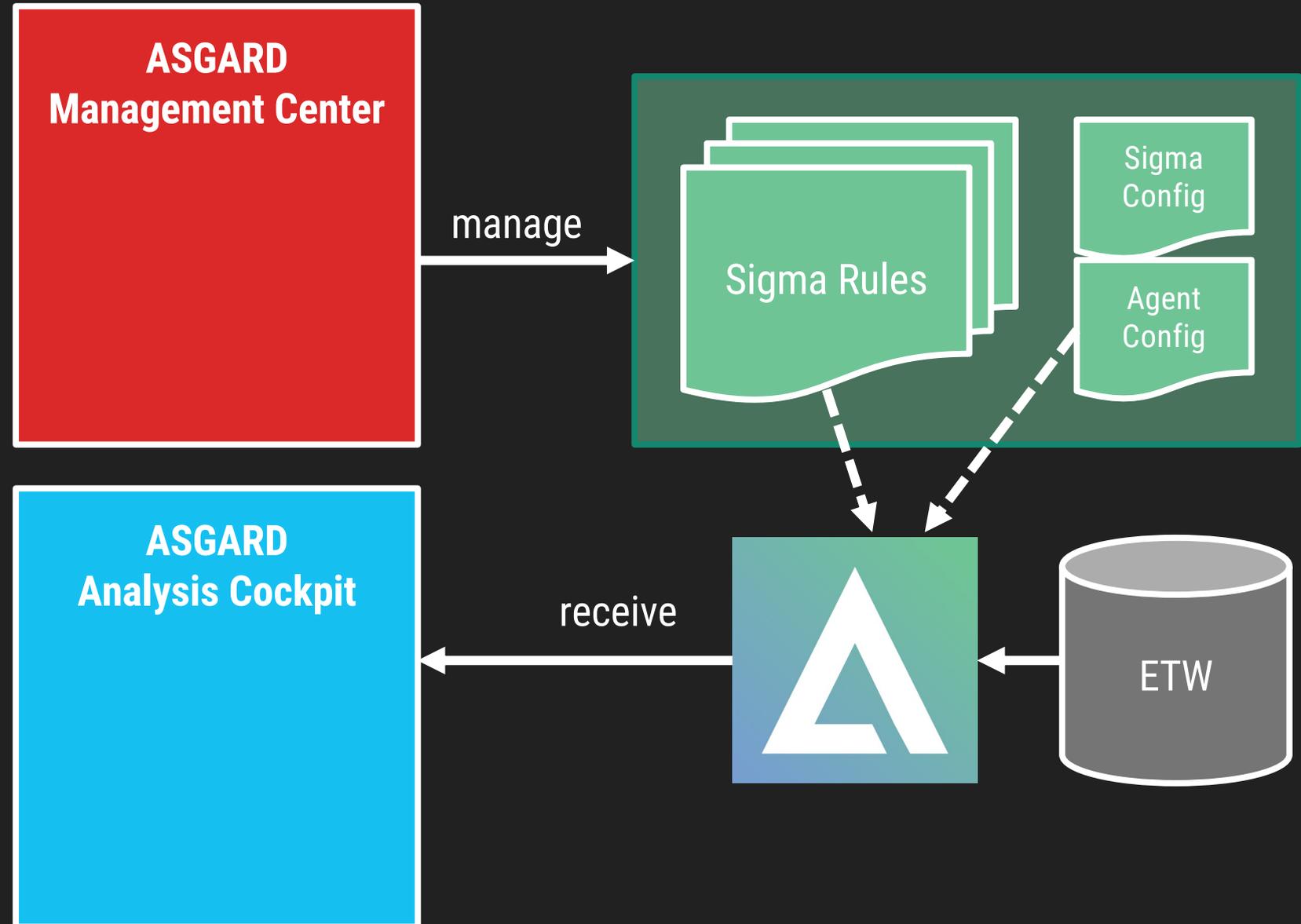
~70%

Percentage of
Event / Fields
used in Sigma Rules

~95%

ASGARD and Aurora Agent

- Deploy Aurora with the ASGARD Agent (no installation, Aurora runs as a sub process of our service controller)
- Manage Sigma rules and updates of these rules
- Deploy specific rule sets on groups of endpoints
- Manage the response actions



Management in ASGARD

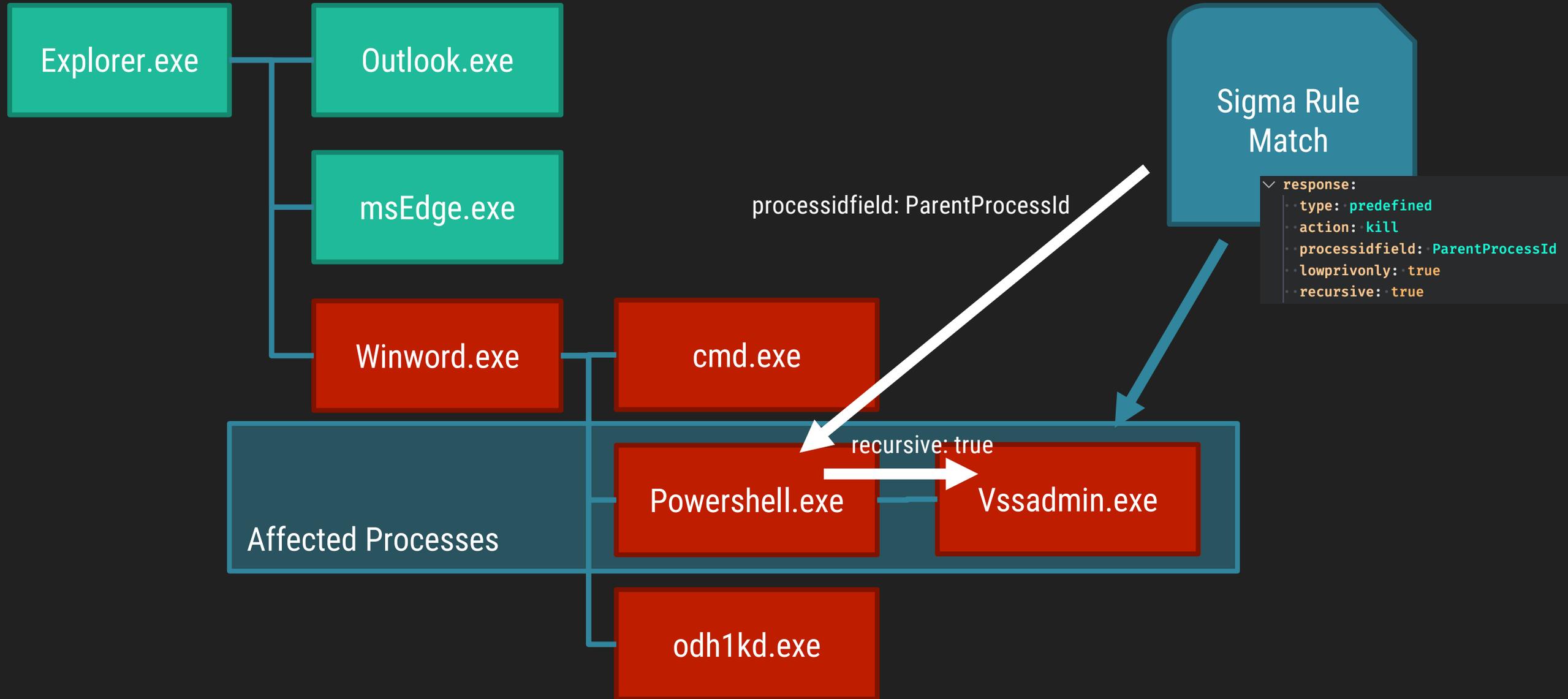
- Comfortable Sigma rule management
 - Enable / disable rules
 - Create rule sets for different asset groups
 - Manage updates of the rules
 - Identify changes in updated rules and decide to deploy them
 - Define response actions, put them in simulation mode or arm them

Title	Level	Description	Tags	Rulesets	Response Actions	Actions
Fsutil Drive Enumeration	low	Attackers may leverage fsutil to enumerated connected drives.	attack.peripheral_device_discovery attack.t1120			[Icons]
Shells Spawned by Web Servers in Process Tree	high	Web servers that spawn shell processes could be the result of a successfully placed web shell or an other attack	attack.persistence attack.t1505.003 attack.t1190	All high Sigma rules Nexttron Testing Setup		[Icons]
Hacktool KrbRelay Usage Indicators	high	Detects hacktool KrbRelay usage based on command line flags and program names		All high Sigma rules Nexttron Testing Setup	Process Kill	[Icons]
PowerShell Web Download and Execution	high	Detects suspicious ways to download files or content using PowerShell		All high Sigma rules Nexttron Testing Setup		[Icons]

1 Sigma rulesets contain uncompiled changes

ID	Name	Description	Rules and Response Actions	Default Response Mode	Last Push	Uncompiled Changes	Autom. add new rules	Actions
6	Ransomware	All rules related to ransomware	27 0 1	Simulation	2022-03-29 11:41:34	No		[Icons]
4	Nexttron Testing Setup	Testruleset with all medium, high, critical rules	1332 0 5	Simulation	2022-03-29 11:41:30	Yes	critical high medium	[Icons]
2	All high Sigma rules	Ruleset with all high Sigma rules. New high sigma rules will automatically be added to this ruleset	672 0 4	Simulation	2022-03-29 12:10:38	Yes	high	[Icons]

Action: Kill, Recursive



Action: Kill, Recursive, LowPrivOnly, Ancestors: All

