



Aurora Agent

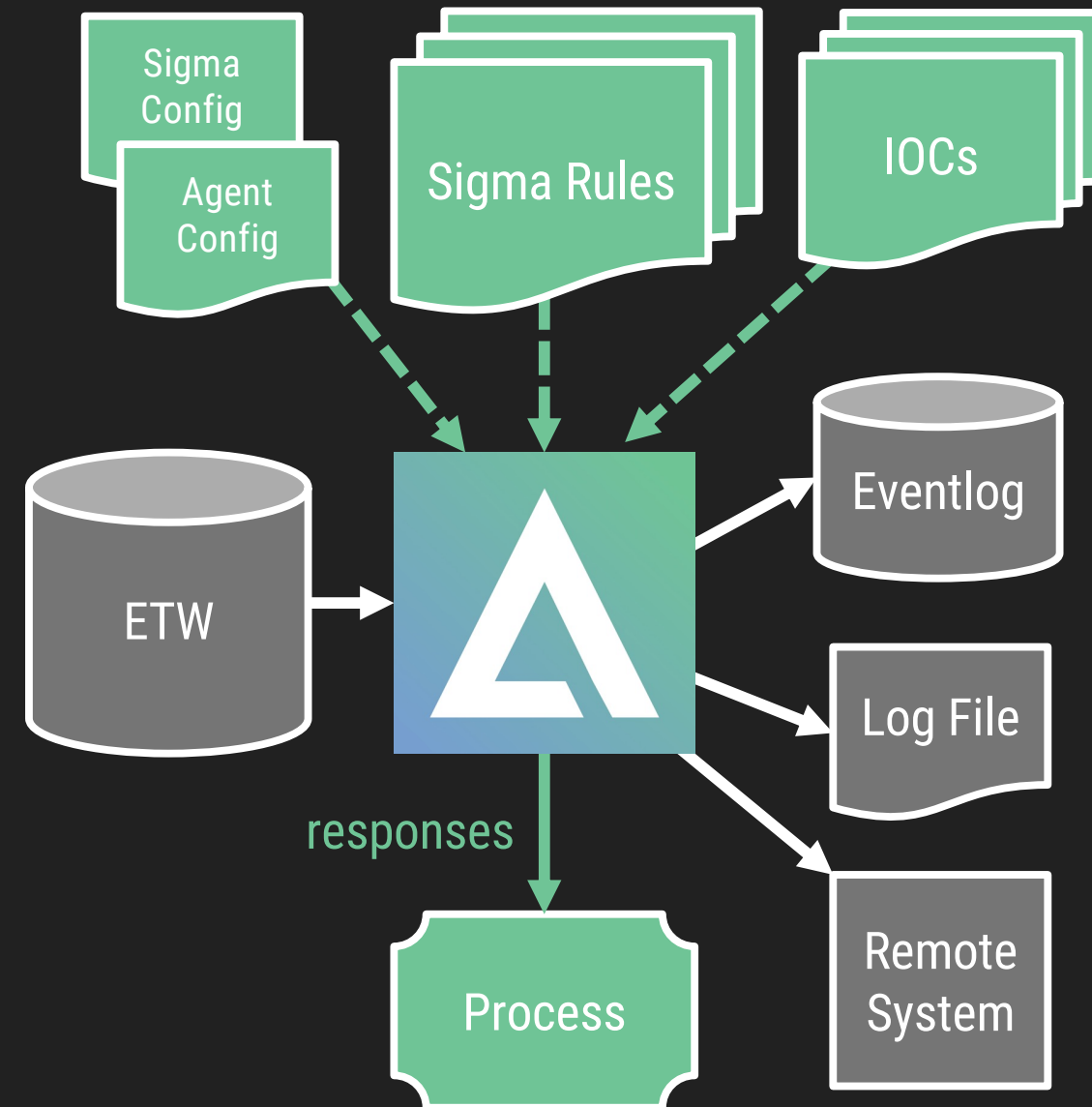
Your custom Sigma-based EDR

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

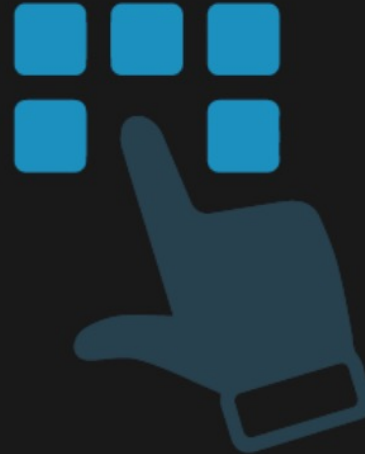
	Sysmon	Aurora
Event Source	Sysmon Kernel Driver	ETW (Event Tracing for Windows)
Sigma Rule Event Coverage	100%	95%
Relative Log Volume	High	Low
Sigma and IOC Matching	No	Yes
Response Actions	No	Yes
Resource Control (CPU Load, Output Throttling)	No	Yes
Output: Eventlog	Yes	Yes
Output: File	No	Yes
Output: 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

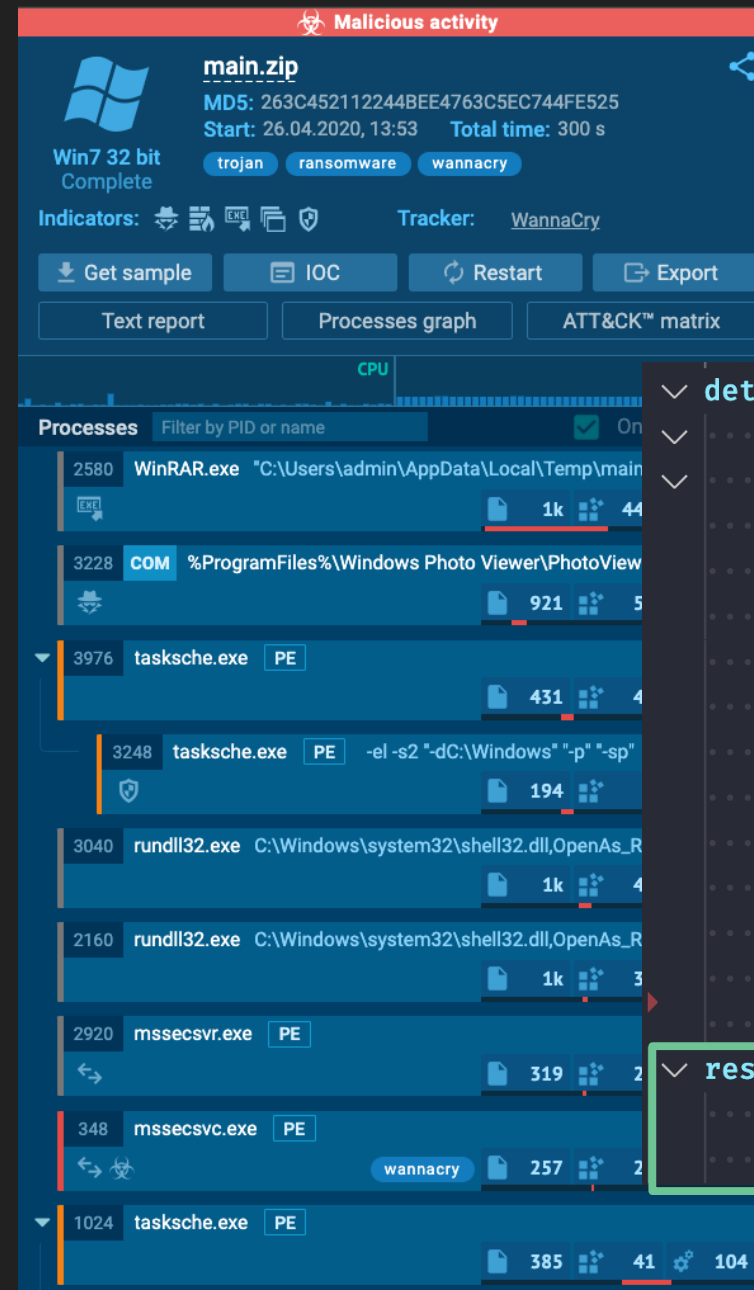
Aurora Lite is a limited version of Aurora and free of charge. It's a great way to give it a whirl. All we ask for is a newsletter subscription.

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'
      - '\mssecsvr.exe'
      - '\taskdl.exe'
      - '\taskhsvc.exe'
      - '\taskse.exe'
      - '\111.exe'
      - '\lhdfgrgui.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	

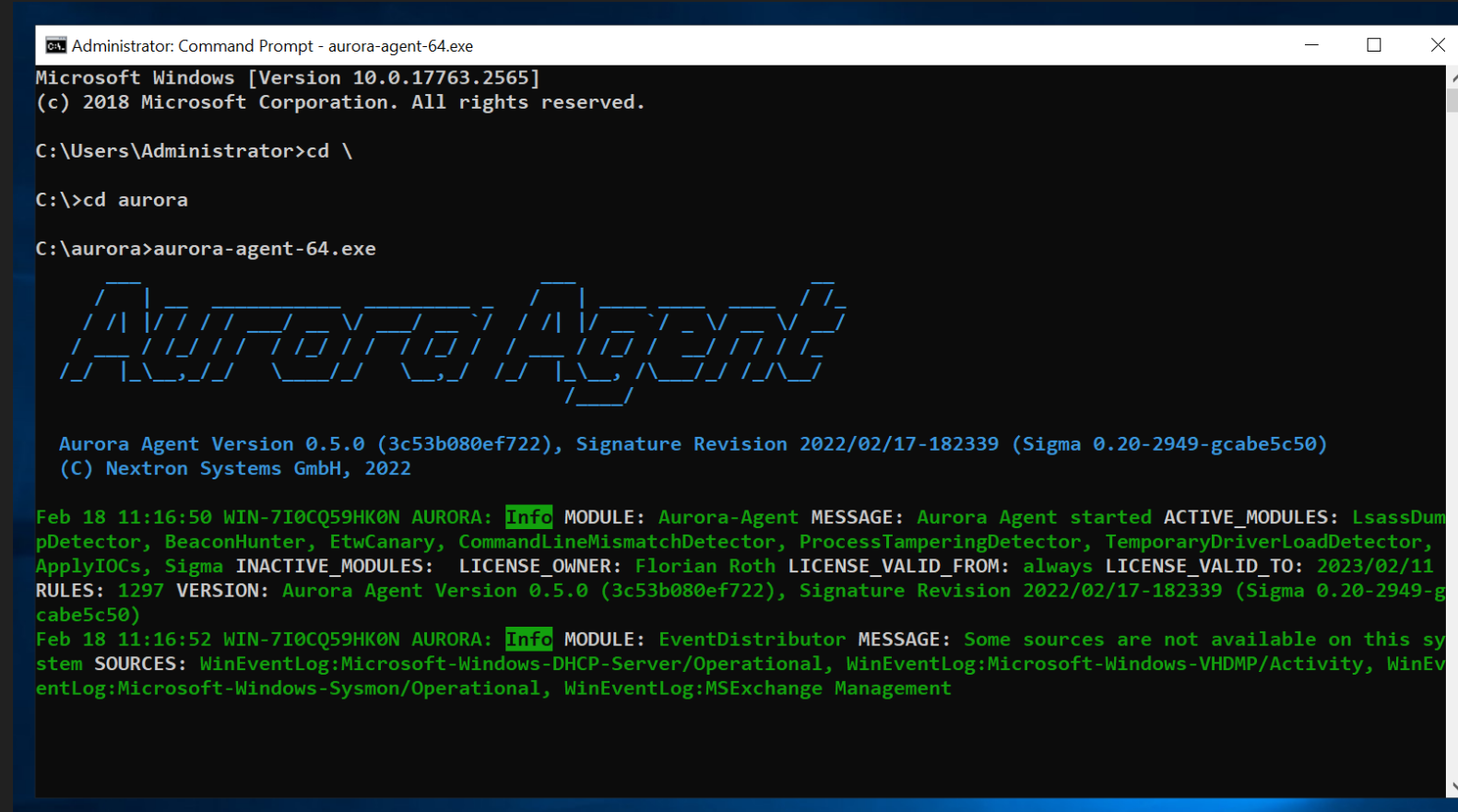
A First Run

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

Feb 18 11:16:50 WIN-7I0CQ59HK0N AURORA: Info MODULE: Aurora-Agent MESSAGE: Aurora Agent started ACTIVE_MODULES: LsassDum
pDetector, 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-g
cabe5c50)
Feb 18 11:16:52 WIN-7I0CQ59HK0N AURORA: Info MODULE: EventDistributor MESSAGE: Some sources are not available on this sy
stem SOURCES: WinEventLog:Microsoft-Windows-DHCP-Server/Operational, WinEventLog:Microsoft-Windows-VHDMP/Activity, WinEv
entLog:Microsoft-Windows-Sysmon/Operational, WinEventLog:MSExchange Management
```

Usage Help

Let's see what the help has to offer

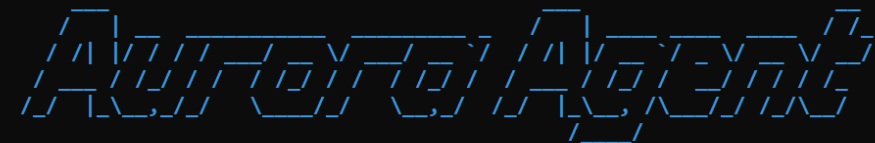
Steps:

- 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 Version 0.6.0 (62b63beac8336), Signature Revision 2022/03/01-143433 (Sigma 0.20.0)
(C) Nextron Systems GmbH, 2022

Usage of aurora-agent-64.exe:

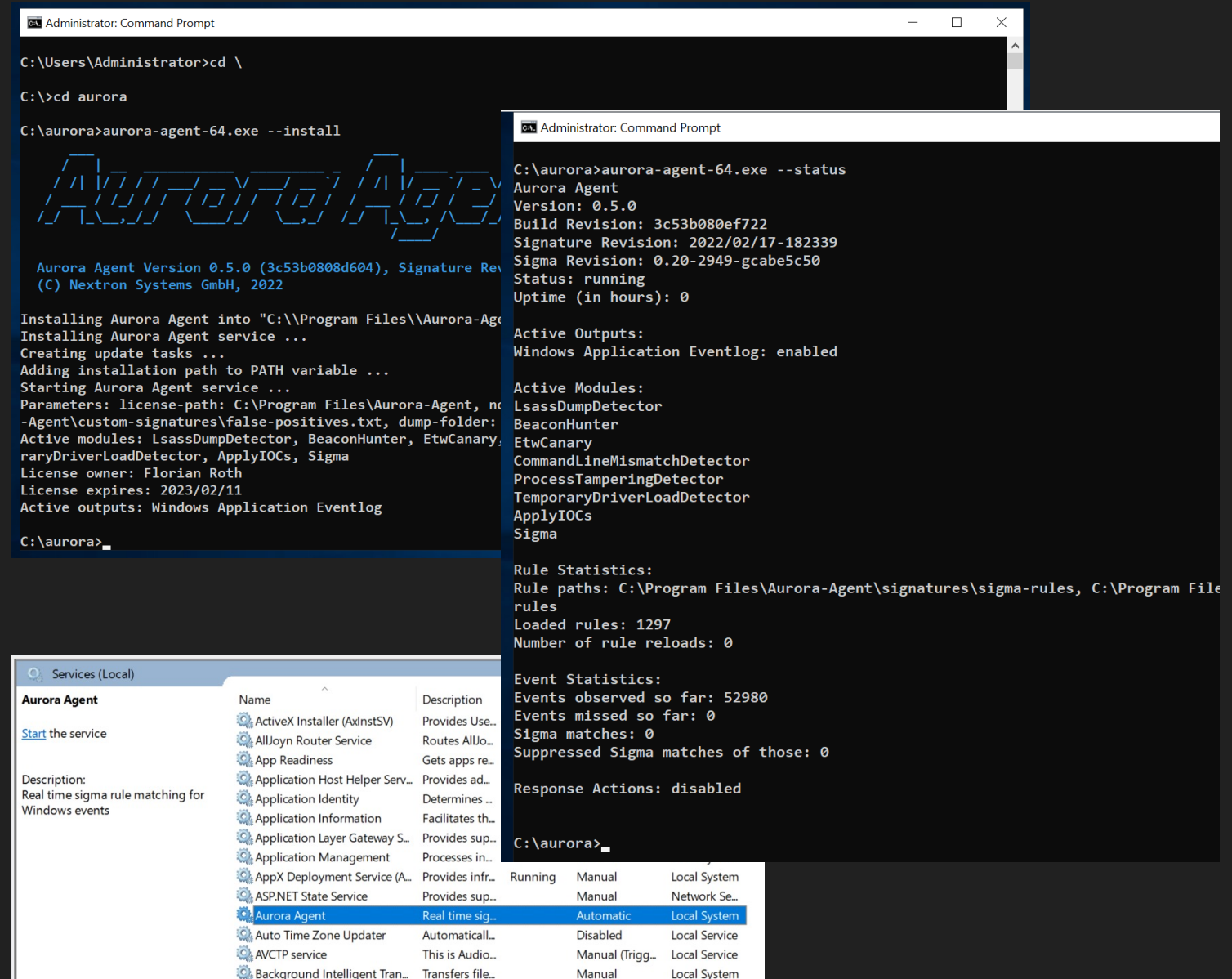
<code>--activate-module strings</code>	Activate the given deactivated modules (see <code>--module-info</code> for a list)
<code>--activate-responses</code>	Execute responses that are specified in Sigma rules (e.g. <code>run: command</code>)
<code>--agent-name string</code>	Set a different name for the service, the binary and other files
<code>-a, --auto-reload</code>	Automatically reload the Sigma rules after changes
<code>-c, --config string</code>	Use parameters from this YAML file
<code>--cpu-limit int</code>	CPU usage (as percentage) that the Aurora Agent should not exceed
<code>--deactivate-all-consumers</code>	Deactivate all consumers, except for those specified by <code>--activate-module</code>
<code>--deactivate-module strings</code>	Deactivate the given modules (see <code>--module-info</code> for a list)
<code>--debug</code>	Print debugging information
<code>--dump-folder string</code>	Folder where process dumps should be stored (default "C:\ProgramData\Nextron Systems\aurora-agent\debug")
<code>--false-positive-filter string</code>	Path to a file containing false positive regexes (one per line)
<code>--help</code>	Show help
<code>--install</code>	Install Aurora Agent as a service
<code>--ioc-path strings</code>	Folders containing IOC files (default [C:\aurora\signature\ioc])
<code>--json</code>	Write output as JSON instead of plain text
<code>--license-path string</code>	Path to the directory containing the Aurora Agent license
<code>--log-rotate uint</code>	How many log rotations should be retained (default 7)
<code>--log-size string</code>	Maximum file size for the log file. It will be rotated when it reaches this size
<code>-s, --log-source strings</code>	Paths to the Sigma log sources that should be loaded (default [C:\ProgramData\Nextron Systems\aurora-agent\log-sources-standard.yml, C:\aurora\log-sources\etw-log-source-mappings.yml])
<code>-l, --logfile string</code>	Path to log file (default: no log file)
<code>--low-prio</code>	Run Aurora Agent with low process priority (can cause missing matches)
<code>--match-burst uint</code>	Number of matches for a single rule that are allowed to be reported
<code>-t 5)</code>	
<code>--match-throttling string</code>	Minimum average time between matches. Sigma Rules with a higher level will be reported
<code>--minimum-level string</code>	Report Sigma matches with rules of this level or higher (default "medium")
<code>--module-info</code>	List all available modules and whether they are active
<code>--no-content-enrichment</code>	Deactivate calculations that rely on disk access (e.g. <code>rule: file</code>)
<code>--no-eventlog</code>	Don't log matches to the Windows event log
<code>--no-stdout</code>	Disable logging to the standard output
<code>--output-throttling string</code>	Minimum average time between log messages (Warning: If set to 0, the output will be throttled)
<code>--pprof</code>	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 and the Windows Services console.

Left Screenshot: Administrator: Command Prompt

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

The output shows the installation progress:

```
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>
```

Right Screenshot: Administrator: Command Prompt

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

The output shows the status of the Aurora Agent:

```
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>
```

Bottom Screenshot: Services (Local)

The Services console shows the 'Aurora Agent' service installed and running.

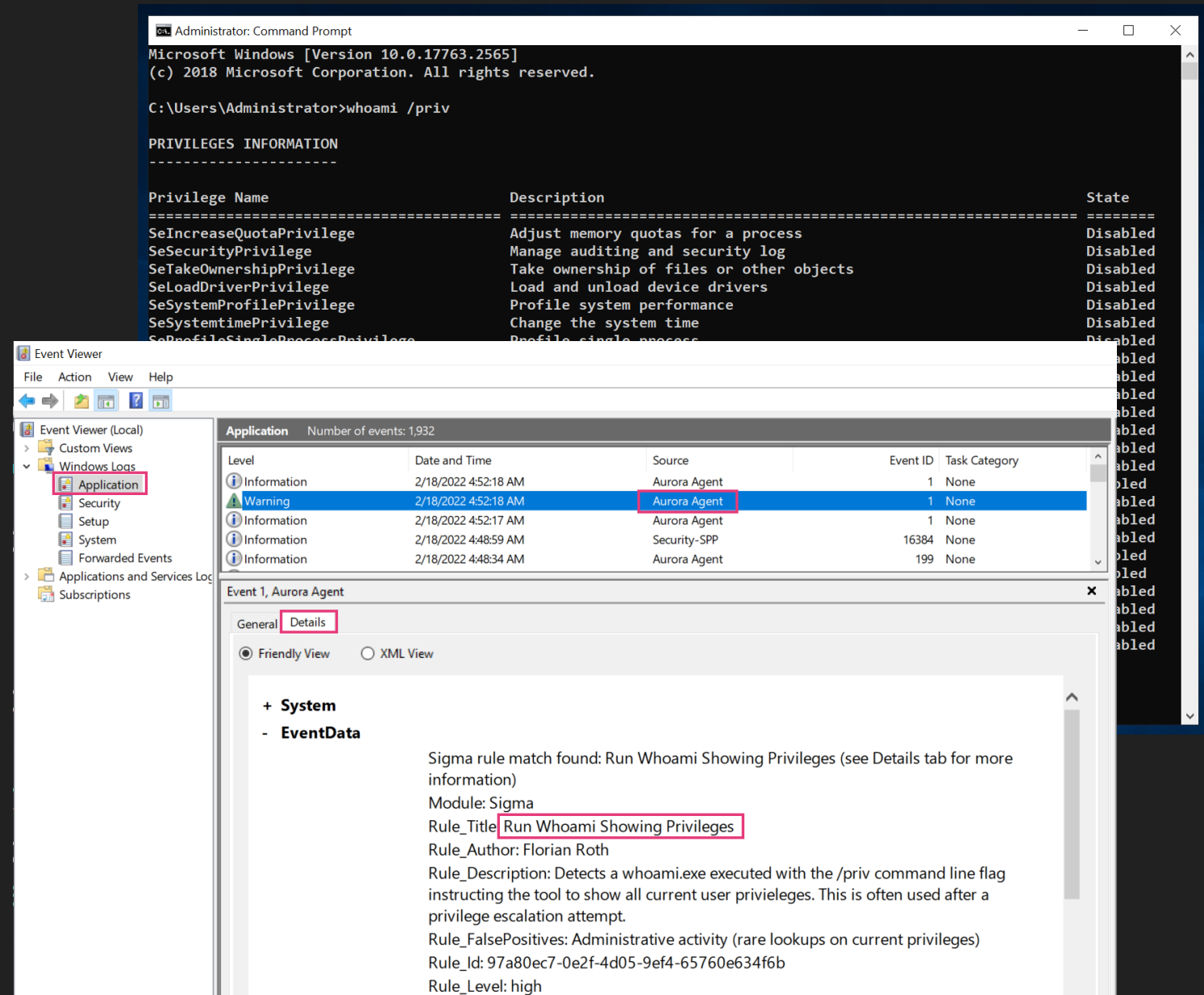
Name	Description	Status	Startup Type	Log On As
Aurora Agent	Real time sigma rule matching for Windows events	Running	Automatic	Local System

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 screenshot displays two windows. The top window is an Administrator Command Prompt showing the output of the `whoami /priv` command, which lists various system privileges and their states (e.g., SeIncreaseQuotaPrivilege, SeSecurityPrivilege, etc.). The bottom window is the Windows Event Viewer, showing the 'Application' log. A warning event from 'Aurora Agent' is selected, and the 'Details' tab is active, showing the event data: 'Sigma rule match found: Run Whoami Showing Privileges (see Details tab for more information)'. The event data includes the module 'Sigma', the rule title 'Run Whoami Showing Privileges', the rule author 'Florian Roth', and a detailed description of the rule's purpose and false positives.

Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.17763.2565]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>whoami /priv

PRIVILEGES INFORMATION
-----
Privilege Name      Description                                     State
-----
SeIncreaseQuotaPrivilege Adjust memory quotas for a process              Disabled
SeSecurityPrivilege   Manage auditing and security log                Disabled
SeTakeOwnershipPrivilege Take ownership of files or other objects        Disabled
SeLoadDriverPrivilege Load and unload device drivers                  Disabled
SeSystemProfilePrivilege Profile system performance                      Disabled
SeSystemtimePrivilege Change the system time                          Disabled
SeProfileSingleProcessPrivilege Profile single process                          Disabled
```

Event Viewer

Application Number of events: 1,932

Level	Date and Time	Source	Event ID	Task Category
Information	2/18/2022 4:52:18 AM	Aurora Agent	1	None
Warning	2/18/2022 4:52:18 AM	Aurora Agent	1	None
Information	2/18/2022 4:52:17 AM	Aurora Agent	1	None
Information	2/18/2022 4:48:59 AM	Security-SPP	16384	None
Information	2/18/2022 4:48:34 AM	Aurora Agent	199	None

Event 1, Aurora Agent

General Details

Friendly View XML View

+ System

- EventData

Sigma rule match found: Run Whoami Showing Privileges (see Details tab for more information)

Module: Sigma

Rule_Title: Run Whoami Showing Privileges

Rule_Author: Florian Roth

Rule_Description: 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.

Rule_FalsePositives: Administrative activity (rare lookups on current privileges)

Rule_Id: 97a80ec7-0e2f-4d05-9ef4-65760e634f6b

Rule_Level: high

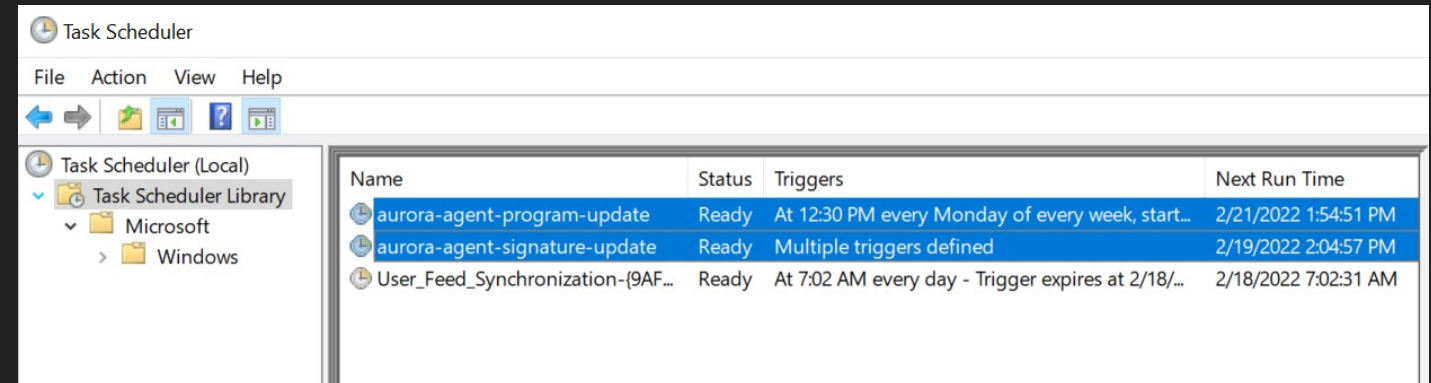
Update Aurora and Signatures

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!

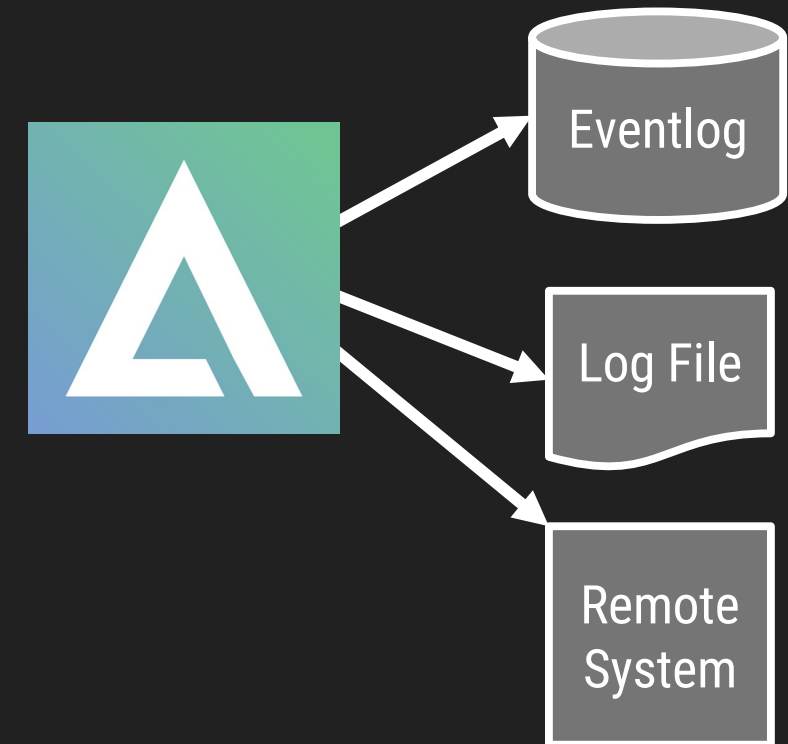
Aurora is up and running.

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>

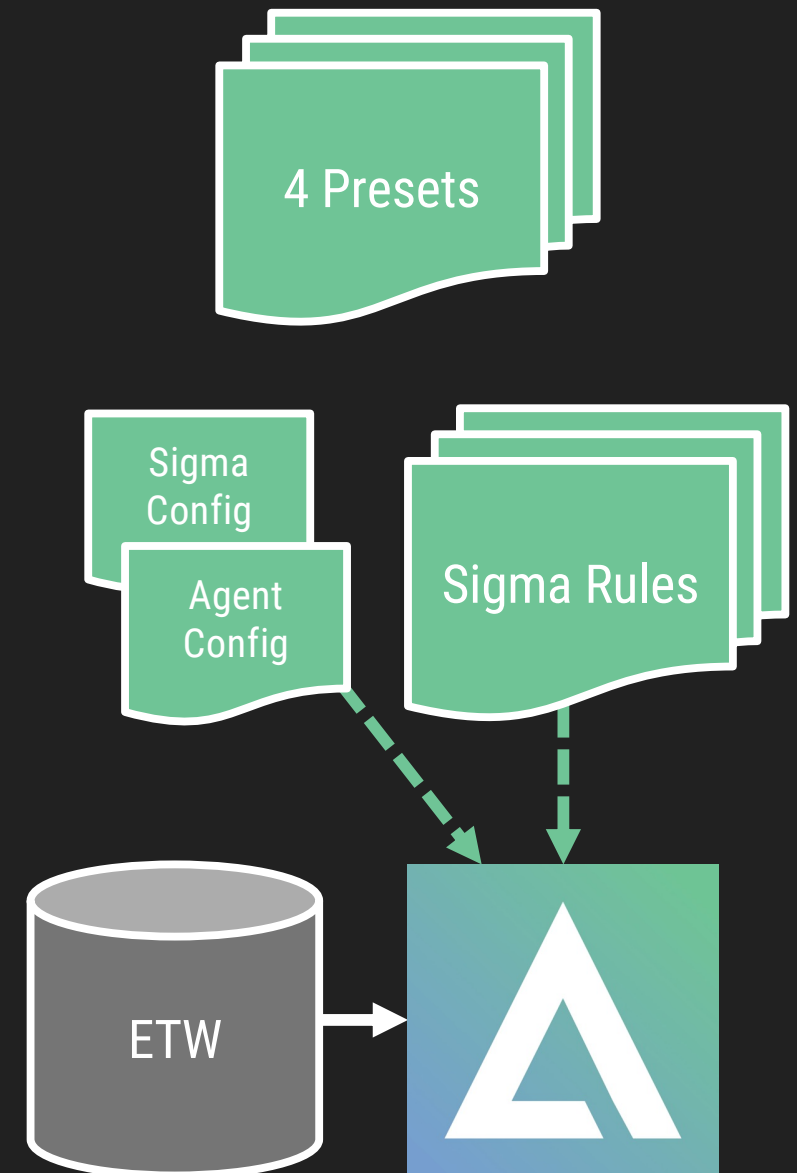
Configuration Presets

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.nextron-systems.com/en/latest/usage/configuration.html>

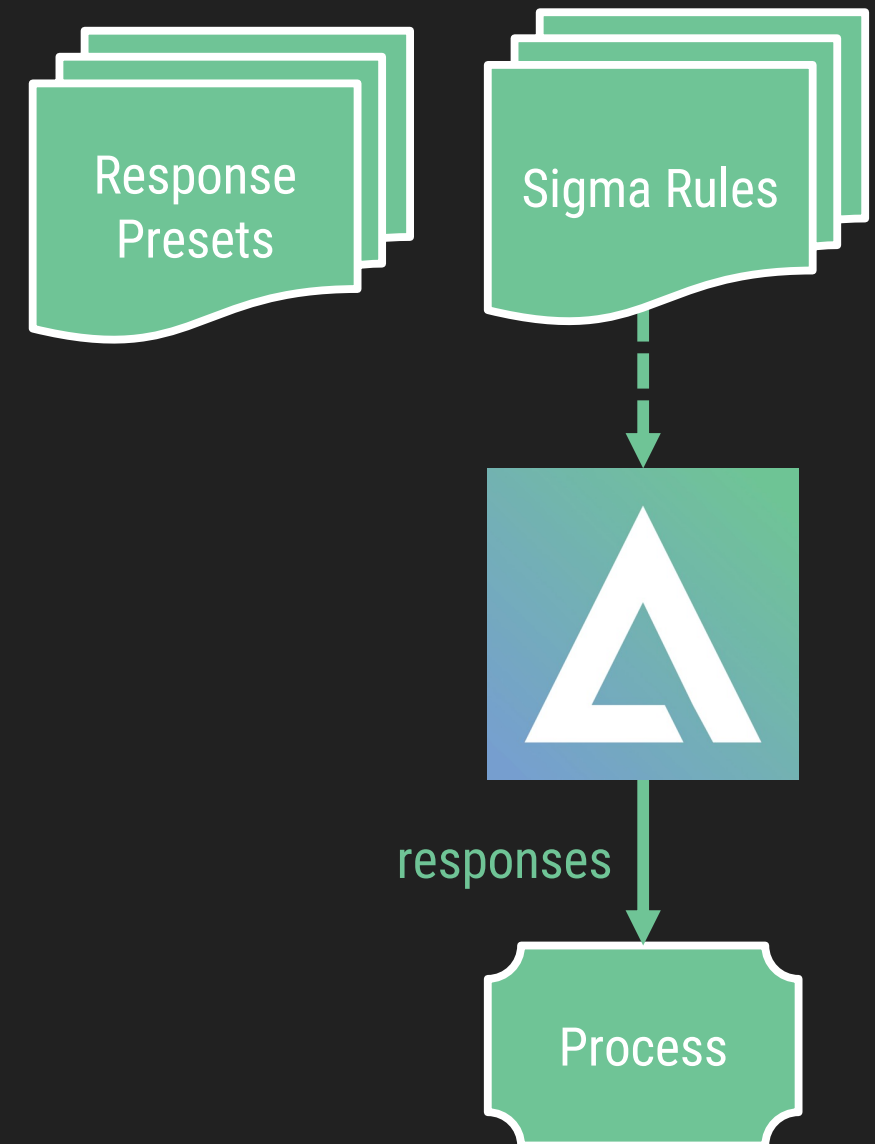


Response Presets

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
(?:i)\\AppData\\[^\\]{1,64}\.exe([^\._\\]|$);75
(?:i)\\AppData\\[^\\]{1,64}\.(dll|bat|vbs|ps1|js|hta);80
(?:i)\\AppData\\Local\\[^\\]{1,64}\.exe([^\._\\]|$);75
(?:i)\\AppData\\Local\\[^\\]{1,64}\.(dll|bat|vbs|ps1|hta);80
(?:i)\\AppData\\Roaming\\[^\\]{1,64}\.exe$;75
(?:i)\\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.”

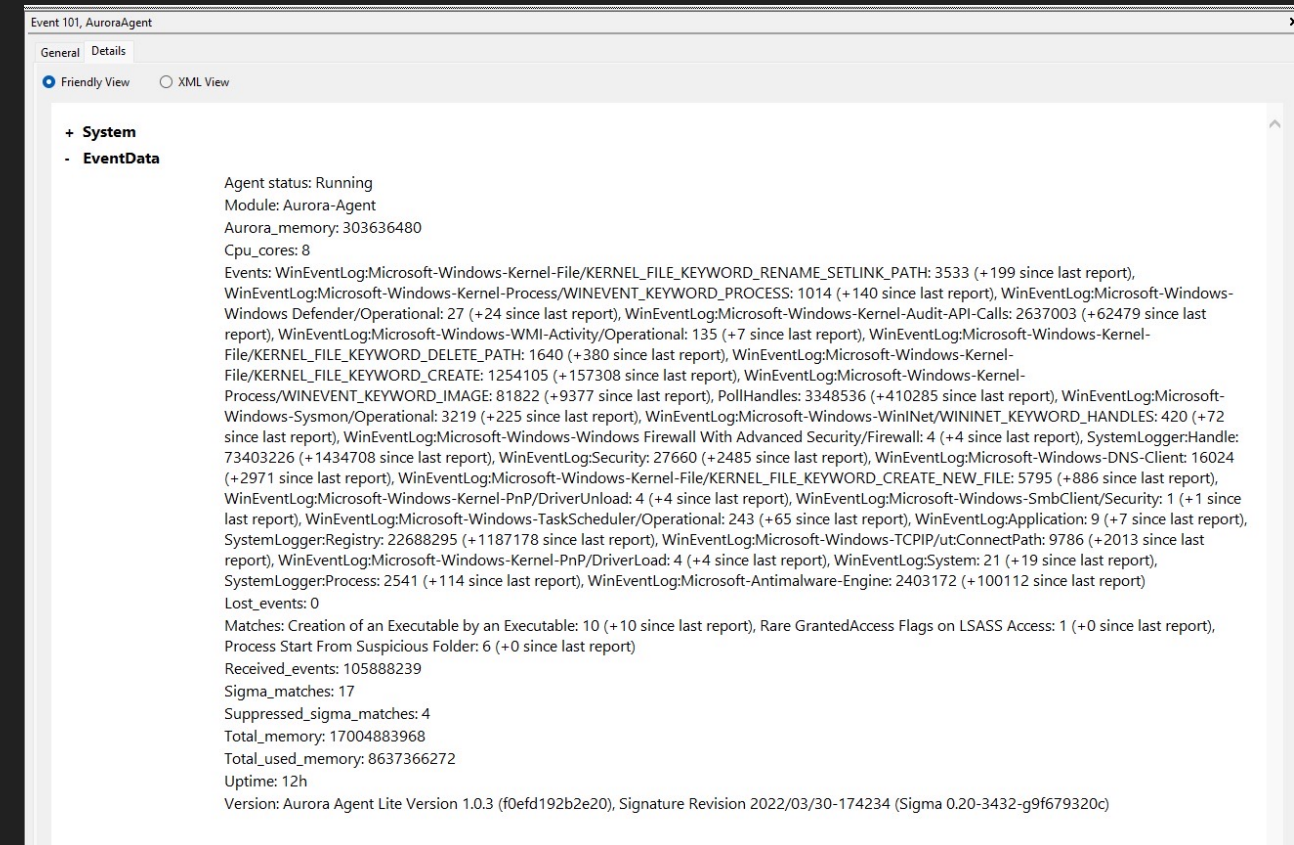
```
GrandparentCommandLine: c:\windows\system32\inet\w3wp.exe -ap "DefaultAppPool" -v
"v4.0" -l "webengine4.dll" -a \\.\pipe\iisipm8ff443c1-cfe8-4a0d-ac14-a9816f37bb80 -h
"C:\inetpub\temp\appools\DefaultAppPool\DefaultAppPool.config" -w "" -m 0 -t 20 -ta 0
GrandparentImage: C:\Windows\System32\inet\w3wp.exe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

Application Number of events: 2,484

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

Event 107, AuroraAgent

General Details

☒ Friendly View ☐ XML View

+ 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

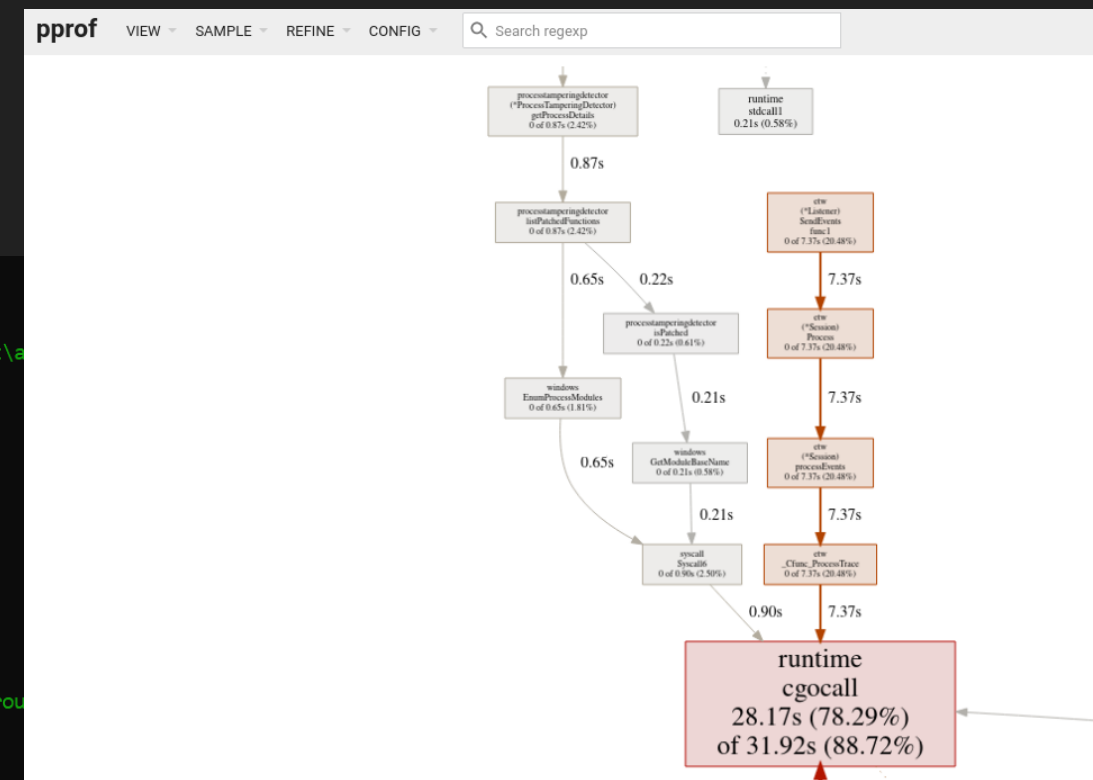
Diagnostics













- 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

This PC > Local Disk (C:) > aurora-beta > diagnostics

Name	Date modified
cpu.pprof	30/03/2022 14:46
diagnostics.log	30/03/2022 14:46
goroutine.pprof	30/03/2022 14:46
heap.pprof	30/03/2022 14:46
status.json	30/03/2022 14:46
status.txt	30/03/2022 14:46

```
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
```



- | | | |
|---|--------|-----------|
|  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 |

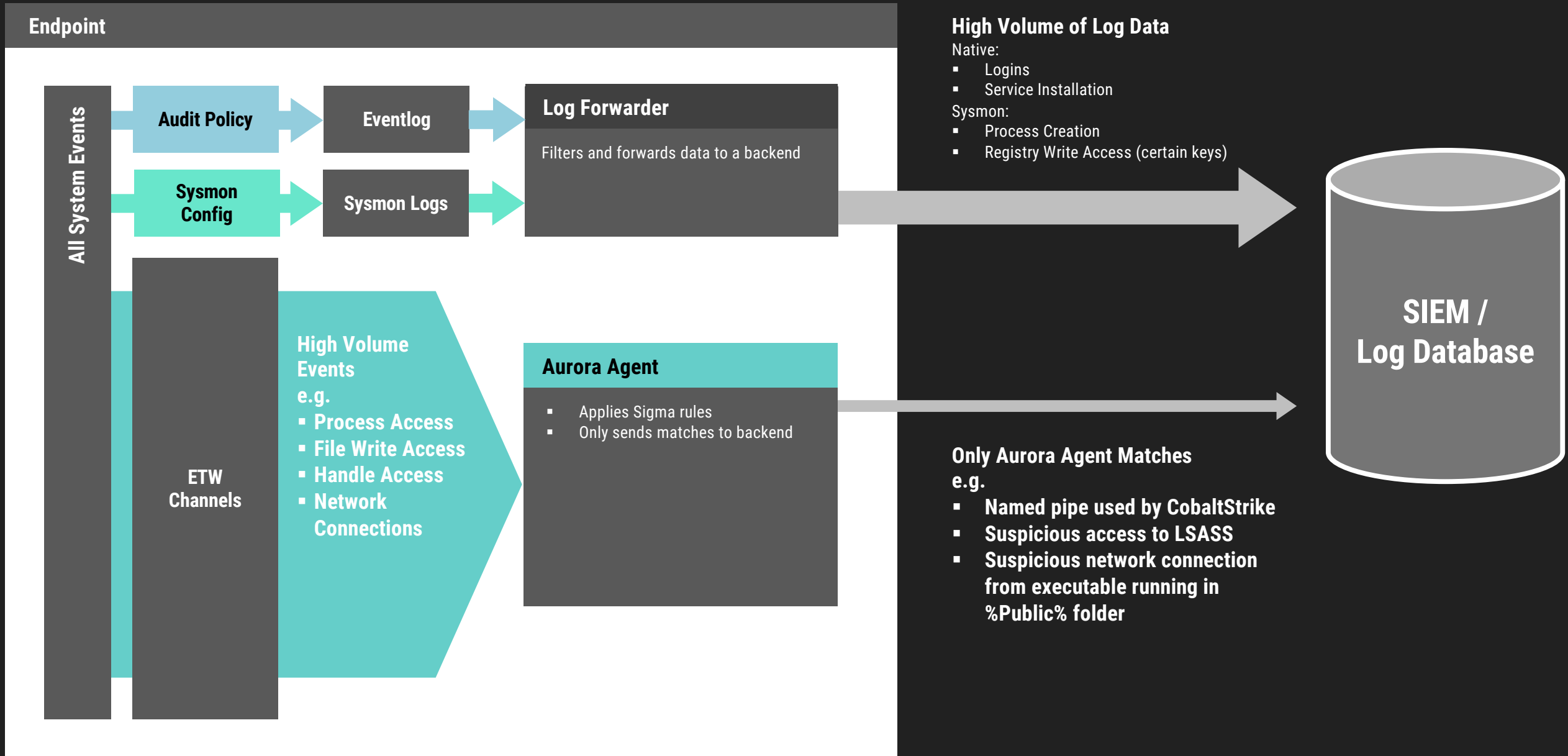
Getting Started

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

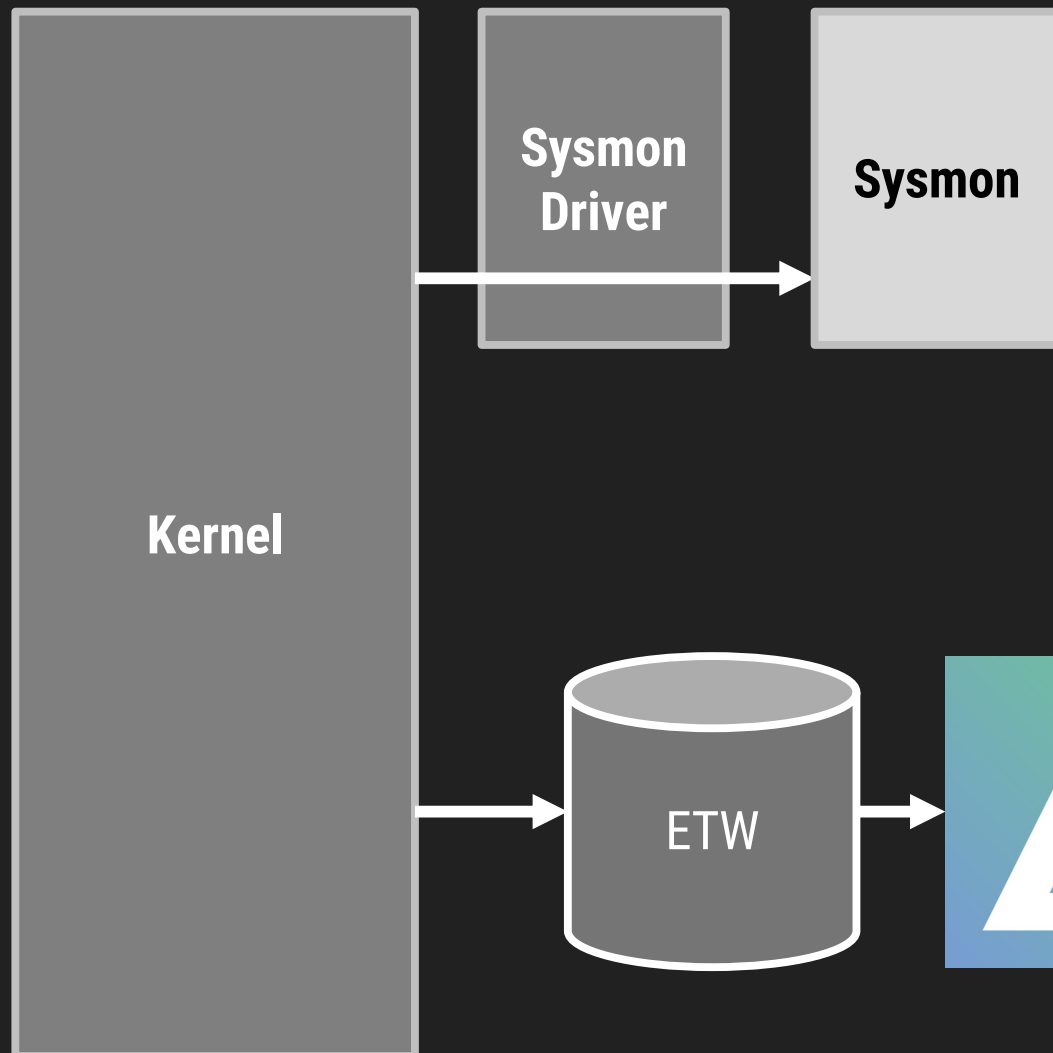
Extra Slides

Used for discussions regarding some of the features

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

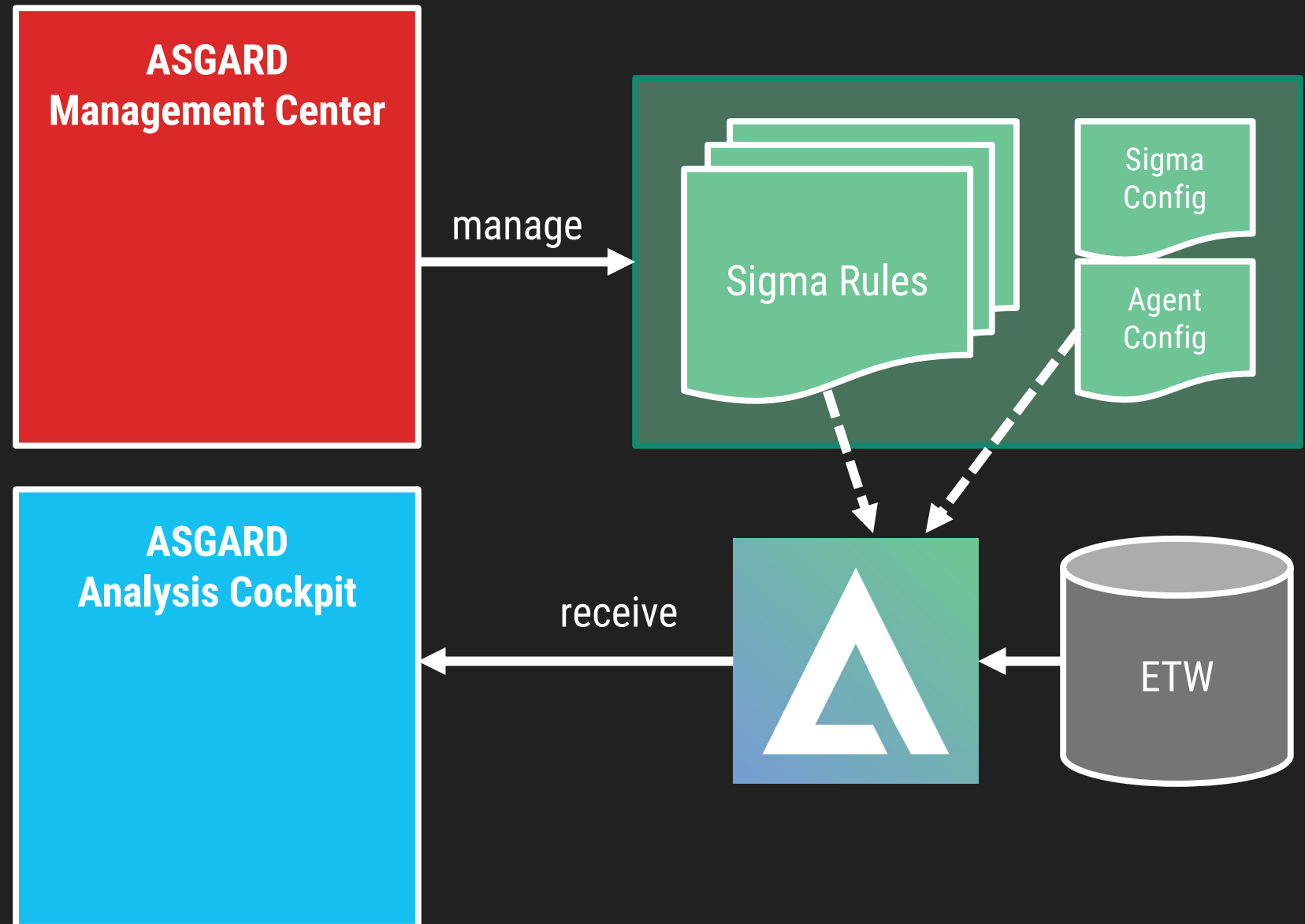
~70%

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

Aurora LogWatcher Sigma 57 Rules Help

[+ Add To Ruleset](#)
[- Remove From Ruleset](#)
[Upload Rules](#)
[Enable](#)
[Disable](#)
[Delete](#)

NOT Disabled Showing 1 - 100 of 1444 results Show 100 1 2 3 4 5 ... 15

	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			
>	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		
>	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	
>	PowerShell Web Download and Execution	high	Detects suspicious ways to download files or content using PowerShell		All high Sigma rules Nexttron Testing Setup		

Aurora LogWatcher Sigma 57 Rulesets 1 Help

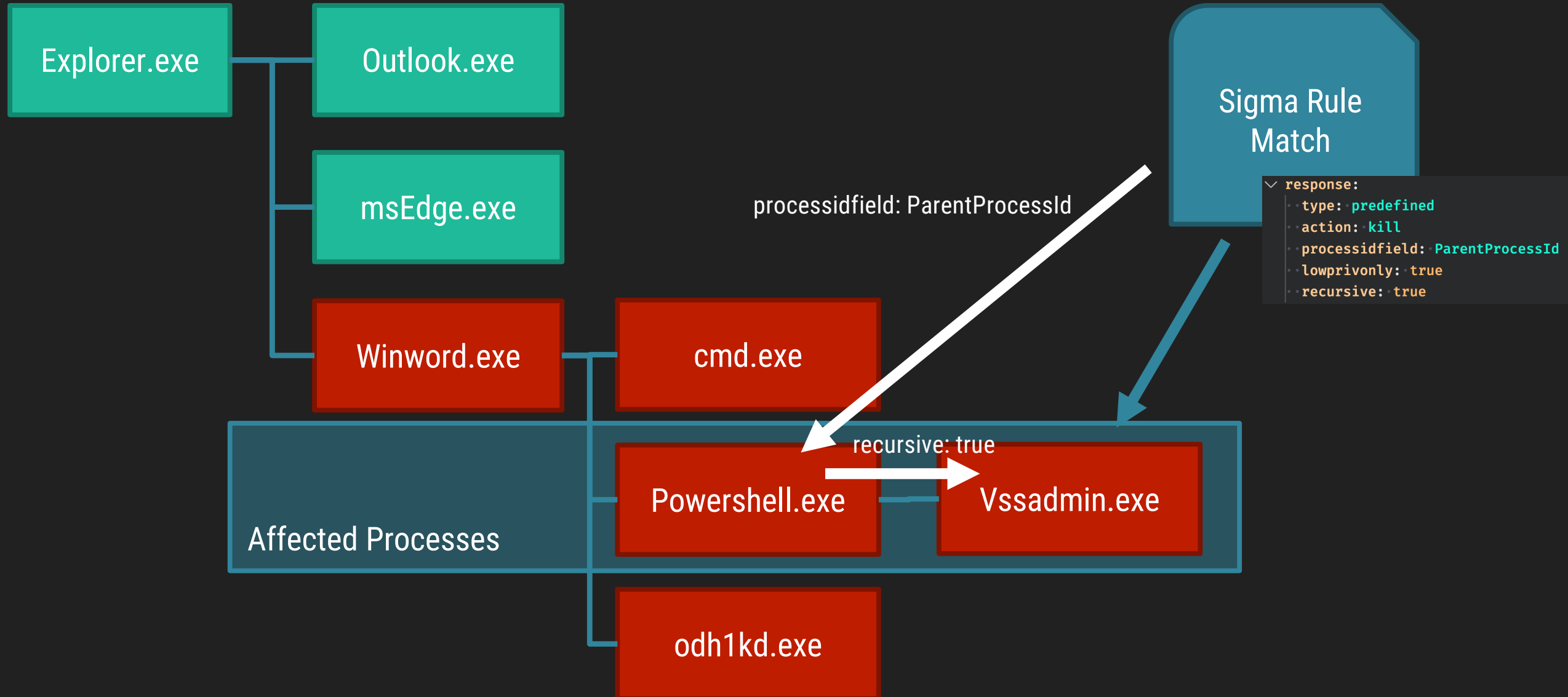
1 Sigma rulesets contain uncompiled changes

Create Ruleset

Showing 1 - 4 of 4 results Show 25 1

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	-	
> 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	
> 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	

Action: Kill, Recursive



Action: Kill, Recursive, LowPrivOnly, Ancestors: All

