



# THOR Cloud Updates - May 2020

Feature Overview and Use Cases

# THOR Cloud



## No Requirements - No Hustle

No local servers, no local management system, no local update tools, no local licensing servers – all that you need is a script with your preset API token. Everything else is retrieved at runtime.



## In-Depth Investigations

With THOR Cloud you can easily extend your analysis with in-depth forensic scans. These scans give your analysts a second opinion on security events and thus speed up analysis and avoid costly manual investigations.



## Easy Integration

You can easily integrate THOR cloud into your existing infrastructure and toolset. The scripts and THOR itself are extremely flexible and feature-rich.

# THOR Cloud – The Idea


- User downloads nothing but a small script
- This script (seed) serves as
  - Downloader
  - License Retriever
  - Managed Executor
  - Configuration Helper
- Windows:                   thor-seed.ps1
- Linux / macOS:           thor-seed.sh
- This script communicates with Nextron Cloud and retrieves a THOR package and license
- Includes all configs: scan config, false positive filters etc
- Easy integration into any EDR or endpoint management solution (MDATP, Tanium, Intune ...)



## THOR Cloud Script Download

Owner	John Connor
Starts On	2020-04-21 00:00:00
Expires On	2021-02-28 23:59:59
License Lifetime	3 day(s)
Quota	1000
Used	0

Accept the EULA to show the download links.

I hereby agree with the terms and conditions stated in the [End User License Agreement \(EULA\)](#). 

Do not upload the software to public platforms like [virustotal.com](#), [hybrid-analysis.com](#) or [malwr.com](#) as those platforms allow the download for registered users.

[Download THOR Seed for Windows](#)

[Download THOR 10 for Linux / MacOS \(coming soon\)](#)

## THOR CLOUD Script Download Page

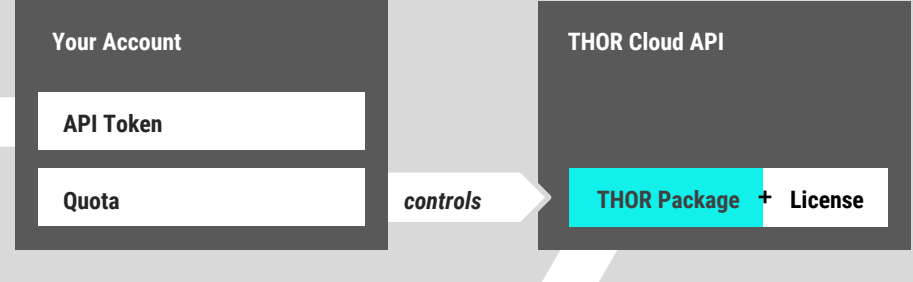


**THOR Cloud Script Download**

Owner: Marcel Gebhardt  
Starts On: 2020-04-20 00:00:00  
Expires On: 2021-04-27 23:59:59  
License Lifetime: 1 day(s)  
Quota: 10000  
Used: 5

[Download THOR-Seed.ps1 \(Windows\)](#)

## THOR CLOUD



**Your Account**

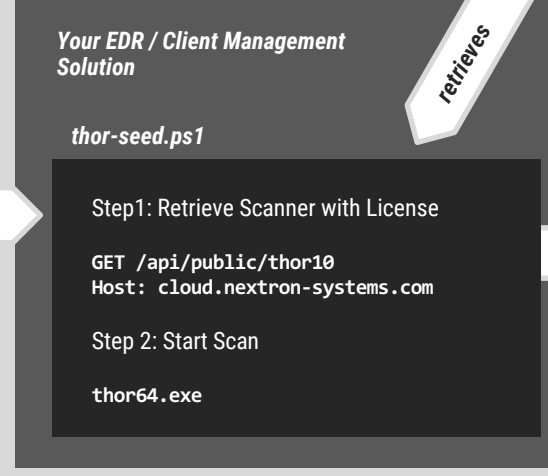
- API Token
- Quota

**THOR Cloud API**

**THOR Package + License**

Arrows: **preset** (from Account to API), **controls** (from Account to Package)

## END SYSTEM



**Your EDR / Client Management Solution**

*thor-seed.ps1*

Step1: Retrieve Scanner with License

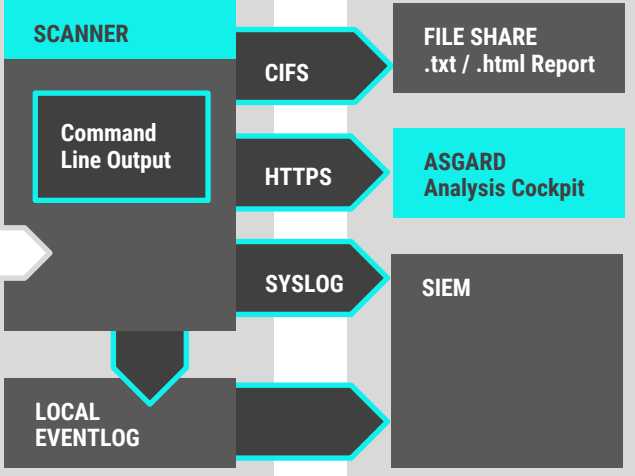
```
GET /api/public/thor10  
Host: cloud.nexttron-systems.com
```

Step 2: Start Scan

thor64.exe

Arrow: **retrieves** (from THOR Cloud API to Step 1)

## OUTPUT OPTIONS



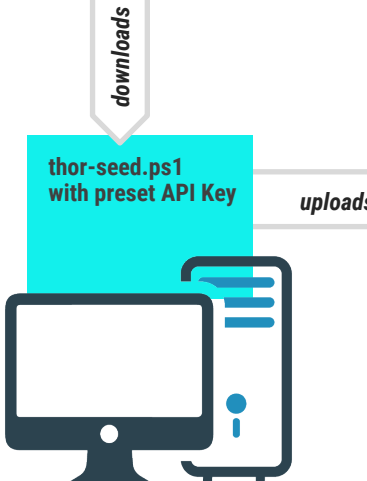
**SCANNER**

Command Line Output

Arrows from SCANNER:

- CIFS** → **FILE SHARE** (.txt / .html Report)
- HTTPS** → **ASGARD** Analysis Cockpit
- SYSLOG** → **SIEM**
- LOCAL EVENTLOG**

Arrow: **runs** (from END SYSTEM to SCANNER)



**downloads** (from THOR Cloud Script Download Page to thor-seed.ps1)

**thor-seed.ps1 with preset API Key**

**uploads** (from thor-seed.ps1 to END SYSTEM)

# THOR Cloud – Quota and Licensing

## A. Vouchers for Trial Runs

## B. Customer Portal


1. Download pages linked to a certain contract
  2. Download pages linked to a user account and all user contracts (automatically picks the most suitable)
- THOR Seed script gets prefilled with such a custom download token (maximum convenience)
  - Download page shows remaining quota



### THOR Cloud Script Download

Owner	John Connor
Starts On	2020-04-21 00:00:00
Expires On	2021-02-28 23:59:59
License Lifetime	3 day(s)
Quota	1000
Used	0

Accept the EULA to show the download links.

I hereby agree with the terms and conditions stated in the [End User License Agreement \(EULA\)](#). 

Do not upload the software to public platforms like virustotal.com, hybrid-analysis.com or malwr.com as those platforms allow the download for registered users.

Download THOR Seed for Windows

Download THOR 10 for Linux / MacOS (coming soon)

# THOR Seed

- PowerShell script (bash script N/A yet)
  - Runs with version 3 of PowerShell
  - Fully commented source code
- Three modes of operation
  1. with THOR Cloud
  2. with ASGARD server (on-premise)
  3. with custom URL (e.g. THOR Lite on local web server)
- Two ways to get it
  1. Download from github.com  
<https://github.com/NextronSystems/nextron-helper-scripts/tree/master/thor-seed>
  2. Download via Nextron Download page with prefilled Download token (API Key) to use it with THOR Cloud (trial voucher or customer contract)

```
thor-seed.ps1 x README.md
1  # Script Title: THOR Download and Execute Script
2  # Script File Name: thor-seed.ps1
3  # Author: Florian Roth
4  # Version: 0.13.0
5  # Date Created: 25.05.2020
6  # Requires -Version 3
7  # Synopsis
8  # Description
9  # Parameter AsgardServer
10 # Parameter UseThorCloud
11 # Parameter TakeToken
12 # Synopsis
13 The "thor-seed" script downloads THOR and executes it
14 # Description
15 The "thor-seed" script downloads THOR from an ASGARD instance, the M
16 executes THOR on the local system writing log files or transmitting
17 # Parameter AsgardServer
18 Enter the server name or IP address of your ASGARD instance.
19 # Parameter UseThorCloud
20 Use the official Nextron cloud systems instead of an ASGARD instance
21 # Parameter TakeToken
```

## Windows PowerShell 3.0

Windows PowerShell 3.0 runs on the following versions of Windows. To run Windows PowerShell 3.0, install the specified version of the Windows Management Framework for your operating system.

Windows version	System requirement
Windows 8	Installed by default
Windows Server 2012	Installed by default
Windows® 7 with Service Pack 1	Install Windows Management Framework 3.0
Windows Server® 2008 R2 with Service Pack 1	Install Windows Management Framework 3.0
Windows Server 2008 with Service Pack 2	Install Windows Management Framework 3.0

Nextron's cloud service inste  
 which the THOR package is ret  
 de it as ZIP archive and add  
 will automaticall find the TH  
 remote SYSLOG server to send  
 ept any value, but rather is  
 wnloaded to.  
 an starts. This is helpful wh  
 ) or network (package retrie

# THOR Seed – Usage Examples

## Usage with THOR Cloud

```
powershell.exe
  -executionpolicy bypass .\thor-seed.ps1
  -UseThorCloud
  -Token oF25AhL8gYbJBE
```

## Usage with ASGARD server

```
powershell.exe
  -executionpolicy bypass .\thor-seed.ps1
  -AsgardServer asgard1.local
  -Token oF25AhL8gYbJBE
```

## Usage with custom THOR package

```
powershell.exe
  -executionpolicy bypass .\thor-seed.ps1
  -CustomUrl https://serv1/share/thor.zip
```

```
Y:\>powershell.exe -ep bypass .\thor-seed.ps1 -UseThorCloud -Tok
```

```
=====
THOR Seed
=====
Nextron Systems, by Florian Roth
```

```
=====
[+] Started thor-seed with PowerShell v5.1.18362.752
[.] Adding random delay to the scan start (max. 10): sleeping fo
[.] Attempting to download THOR from Nextron cloud portal, pleas
[+] Download URL: https://cloud.nextron-systems.com/api/public/t
[+] Successfully downloaded THOR package to C:\Users\neo\AppData
age.zip
[.] Extracting THOR package
[.] Trying to find THOR binary in location C:\Users\neo\AppData\
[+] Using THOR binaries in location C:\Users\neo\AppData\Local\T
[+] Using preset config defined in script header due to $UsePres
[.] Writing temporary config to C:\Users\neo\AppData\Local\Temp\
[+] Using preset false positive filters due to $UseFalsePositive
[.] Writing temporary false positive filter file to C:\Users\neo
onfig\false_positive_filters.cfg
[.] Starting THOR scan ...
[+] Command Line: C:\Users\neo\AppData\Local\Temp\1zmu33po.za0\t
Local\Temp\1zmu33po.za0\config.yml
[+] Writing output files to Y:\
```



# THOR Seed Config Sections

## Integrated Config Section

- Different presets
- Default preset with quick scan setup

Find all command line flags here:

<https://github.com/NextronSystems/nextron-helper-scripts/tree/master/thor-help>

```
# SELECTIVE
# Preset template for a selective scan
# Run time: 1 to 3 minutes
# Specifics:
# - runs a reduced quick scan
# - skips Registry and Process memory checks
$PresetConfig_Selective = @"
module:
- Autoruns
- Rootkit
- ShimCache
- DNSCache
# - RegistryChecks
- ScheduledTasks
- FileScan
# - ProcessCheck
- Eventlog
nosoft: true      # Don't throttle the scan, even on single core system
lookback: 1       # Log and Eventlog look back time in days
sigma: true       # Activate Sigma scanning on Eventlogs
quick: true       # Quick scan mode
nofserrors: true  # Don't print an error for non-existing directories
nocsv: true       # Don't create CSV output file with all suspicious files
noscanid: true    # Don't print a scan ID at the end of each line (only for quick scan)
nothoradb: true   # Don't create a local SQLite database for different
"@
```



# THOR Seed False Positive Filters

## Integrated False Positive Filters

- Each filter gets applied to each output log line
- Strings are interpreted as regular expressions
- Section has some examples

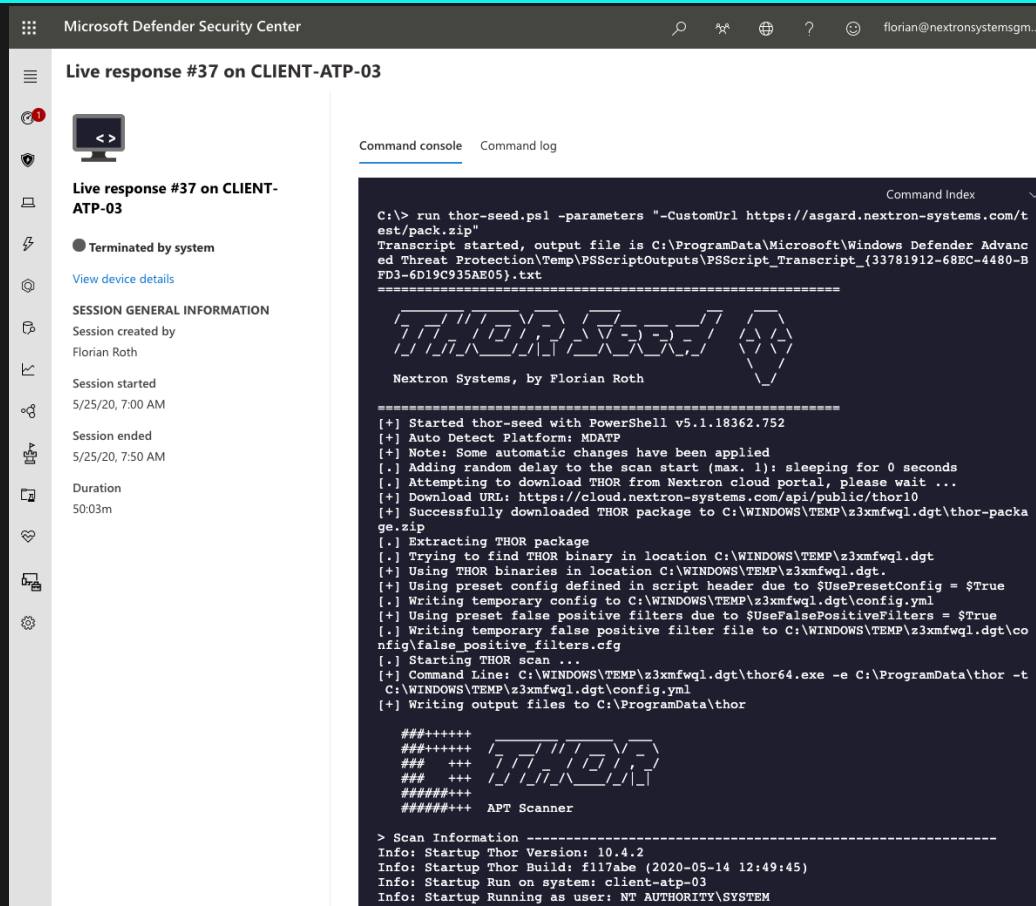
*Users can adjust them to their custom environment and tools that get falsely flagged by THOR*

```
# False Positive Filters
$UseFalsePositiveFilters = $True
# The following new line separated false positive
# applied to all log lines as regex values.
$PresetFalsePositiveFilters = @
Could not get files of directory
Signature file is older than 60 days
\\Our-Custom-Software\\v1.[0-9]+\
"@
```

# THOR Seed Integration: Windows Defender ATP

## First Showcase with Microsoft Defender ATP

- Upload THOR Seed to Live Response script library
- Run THOR Seed with “run” command
- THOR Seed auto-detects environment and makes some adjustments (output path changed to C:\ProgramData\thor)
- Retrieve reports with “getfile” command



Microsoft Defender Security Center

Live response #37 on CLIENT-ATP-03

Terminated by system

View device details

SESSION GENERAL INFORMATION

Session created by  
Florian Roth

Session started  
5/25/20, 7:00 AM

Session ended  
5/25/20, 7:50 AM

Duration  
50.03m

Command console

Command log

Command Index

```
C:\> run thor-seed.ps1 -parameters "-CustomUrl https://asgard.nextron-systems.com/test/pack.zip"
Transcript started, output file is C:\ProgramData\Microsoft\Windows Defender Advanced Threat Protection\Temp\PSScriptOutputs\PSScript_Transcript_(33781912-68EC-4480-BFD3-6D19C935AE05).txt
=====
THOR Seed
Nextron Systems, by Florian Roth
=====
[+] Started thor-seed with PowerShell v5.1.18362.752
[+] Auto Detect Platform: MDATP
[+] Note: Some automatic changes have been applied
[.] Adding random delay to the scan start (max. 1): sleeping for 0 seconds
[.] Attempting to download THOR from Nextron cloud portal, please wait ...
[+] Download URL: https://cloud.nextron-systems.com/api/public/thor10
[+] Successfully downloaded THOR package to C:\WINDOWS\TEMP\z3xmfqw1.dgt\thor-package.zip
[.] Extracting THOR package
[.] Trying to find THOR binary in location C:\WINDOWS\TEMP\z3xmfqw1.dgt
[+] Using THOR binaries in location C:\WINDOWS\TEMP\z3xmfqw1.dgt
[+] Using preset config defined in script header due to $UsePresetConfig = $True
[.] Writing temporary config to C:\WINDOWS\TEMP\z3xmfqw1.dgt\config.yml
[+] Using preset false positive filters due to $UseFalsePositiveFilters = $True
[.] Writing temporary false positive filter file to C:\WINDOWS\TEMP\z3xmfqw1.dgt\config\false_positive_filters.cfg
[.] Starting THOR scan ...
[+] Command Line: C:\WINDOWS\TEMP\z3xmfqw1.dgt\thor64.exe -e C:\ProgramData\thor -t C:\WINDOWS\TEMP\z3xmfqw1.dgt\config.yml
[+] Writing output files to C:\ProgramData\thor

#####
#####
###  ++
###  ++
#####
#####  APT Scanner

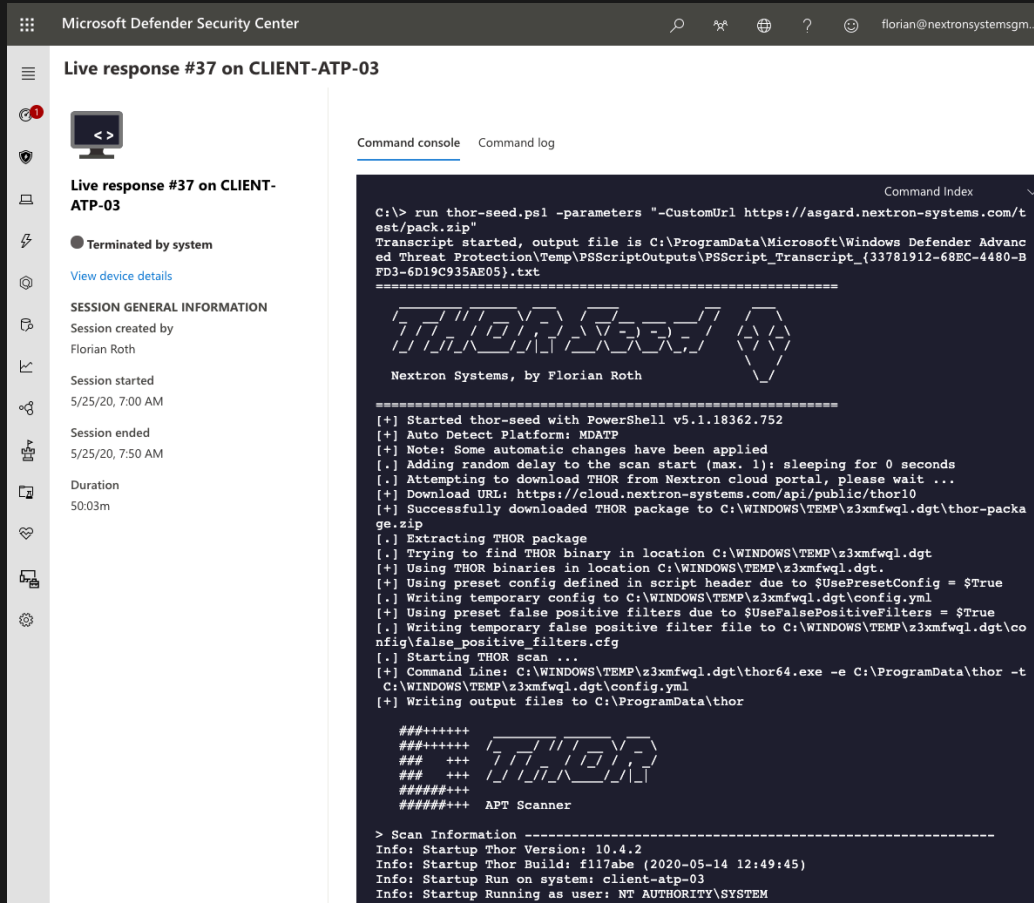
> Scan Information -----
Info: Startup Thor Version: 10.4.2
Info: Startup Thor Build: fl17abe (2020-05-14 12:49:45)
Info: Startup Run on system: client-atp-03
Info: Startup Running as user: NT AUTHORITY\SYSTEM
```

# THOR Seed Integration: Windows Defender ATP

## Pitfalls

- Live Response is only available on Windows 10
- No progress indication
  - After starting the script, all you see is a spinning command line cursor until the script ends. You can't see the usual scrolling text and get all output at the end of the scan.
- Script runtime is limited to 30 min
  - make sure to adjust config accordingly (default should do it, but be careful adding long running modules)
  - script runtime via API call is limited to 4 hours
- Note the special way to pass the command line flags

```
run thor-seed.ps1 -parameters "-
UseThorCloud -Token of25AhL8gYbJBE"
```



Microsoft Defender Security Center

Live response #37 on CLIENT-ATP-03

Terminated by system

View device details

SESSION GENERAL INFORMATION

Session created by  
Florian Roth

Session started  
5/25/20, 7:00 AM

Session ended  
5/25/20, 7:50 AM

Duration  
50.03m

Command console

Command Index

```
C:\> run thor-seed.ps1 -parameters "-CustomUrl https://asgard.nextron-systems.com/test/pack.zip"
Transcript started, output file is C:\ProgramData\Microsoft\Windows Defender Advanced Threat Protection\Temp\PSScriptOutputs\PSScript_Transcript_{33781912-68EC-4480-BFD3-6D19C935AE05}.txt
=====
THOR SEED
Nextron Systems, by Florian Roth
=====
[+] Started thor-seed with PowerShell v5.1.18362.752
[+] Auto Detect Platform: MDATP
[+] Note: Some automatic changes have been applied
[.] Adding random delay to the scan start (max. 1): sleeping for 0 seconds
[.] Attempting to download THOR from Nextron cloud portal, please wait ...
[+] Download URL: https://cloud.nextron-systems.com/api/public/thor10
[+] Successfully downloaded THOR package to C:\WINDOWS\TEMP\z3xmfwql.dgt\thor-package.zip
[.] Extracting THOR package
[.] Trying to find THOR binary in location C:\WINDOWS\TEMP\z3xmfwql.dgt
[+] Using THOR binaries in location C:\WINDOWS\TEMP\z3xmfwql.dgt
[+] Writing preset config defined in script header due to $UsePresetConfig = $True
[.] Writing temporary config to C:\WINDOWS\TEMP\z3xmfwql.dgt\config.yml
[+] Writing preset false positive filters due to $UseFalsePositiveFilters = $True
[.] Writing temporary false positive filter file to C:\WINDOWS\TEMP\z3xmfwql.dgt\config\false_positive_filters.cfg
[.] Starting THOR scan ...
[+] Command Line: C:\WINDOWS\TEMP\z3xmfwql.dgt\thor64.exe -e C:\ProgramData\thor -t C:\WINDOWS\TEMP\z3xmfwql.dgt\config.yml
[+] Writing output files to C:\ProgramData\thor

#####
#####
###  +++
###  +++
#####
#####  APT Scanner

> Scan Information -----
Info: Startup Thor Version: 10.4.2
Info: Startup Thor Build: fl17abe (2020-05-14 12:49:45)
Info: Startup Run on system: client-atp-03
Info: Startup Running as user: NT AUTHORITY\SYSTEM
```

# THOR Cloud Roadmap

- Support Custom Signatures / IOCs
  - Retrieved via HTTP(S) from some location in the local network or Internet
  - Retrieve from MISP at runtime (?)
- Use of `--global-lookback`
  - Available in upcoming THOR v10.5
  - Allows to limit the scan to elements (file, registry, eventlog) that have been created or modified during the last X days
  - Reduces scan duration significantly and is the perfect option for SOC related use cases (suspicious case evaluation)
- Improved HTML Reports
  - Layout & design