
ASGARD_Analysis_Cockpit_3_Manual Documentation

Nexttron

Feb 21, 2024

CONTENTS:

1	Introduction	1
2	Requirements	3
2.1	Hardware Requirements	3
2.2	Network Requirements	3
2.3	Internet Access during Installation	5
2.4	Verify the Downloaded ISO (Optional)	5
2.5	Other Optional Requirements	7
2.6	Architecture	7
3	Setup Guide	9
3.1	Create a New ESX VM and Mount the ISO	9
3.2	Analysis Cockpit Installation	9
3.3	Network Configuration	9
3.4	Choosing a password	17
3.5	Partitioning of the Hard Disk	17
3.6	Proxy Configuration	19
3.7	Install the Analysis Cockpit Services	19
3.8	Changing Passwords	20
3.9	Changing the IP-Address	21
4	Administration	23
4.1	License Installation	23
4.2	System Update	23
4.3	Set Users and User Rights	23
4.4	Configure Canned Recommendations	25
4.5	Syslog Forwarding	26
4.6	TLS Certificate Installation	26
4.7	Configure LDAP	28
4.8	Configure Notifications	28
4.9	Log File Import	31
4.10	Connect to ASGARD Management Center	35
4.11	Asset View	35
4.12	Sandbox Integration	37
4.13	API	43
5	Basic Concepts	45
5.1	Events	45
5.2	Baselining	46
5.3	Cases and Log Processing	49

5.4	Understanding Users, Roles, Rights and Case Status	54
6	Baselining Best Practices	61
6.1	Customize Your View	62
6.2	Manual Case Creation	65
6.3	Create Cases Automatically	71
6.4	Add to Case	73
6.5	Customizing the Detailed View of Log Lines	73
6.6	Usage of the Context Menu	74
7	Case Management Best Practices	77
7.1	Open a Case for Editing	77
7.2	Case Dispatching	78
7.3	Closing a Case	78
7.4	Generate and Review auto_case_ids	79
7.5	More Information about Cases	80
7.6	Bulk Edit / Bulk Delete	82
8	Maintenance	83
8.1	System Updates	83
8.2	Configuration Backup & Restore	83
8.3	Regain Disk Space	84
9	Typical Pitfalls	87
9.1	Certificate Validation Failed	87
9.2	Log File Import of Previous Years	87
9.3	Recover from a Full Disk	87
9.4	ElasticSearch Index Locked Due to Low Free Disk Space	88
9.5	Debug Failed File Imports	90
9.6	Fixing a Broken Proxy Configuration	90
10	FAQs	93
10.1	Disabling Assignment Logs	93
10.2	No Events visible	93
10.3	No new Events in Case	94
10.4	Location of Scan Logs	94
10.5	Default password for file downloads	95
10.6	Disk Space filling up quickly	95
10.7	Reverse Proxy to access the Analysis Cockpit	95
10.8	Internet Explorer	96
10.9	Admin Password reset	96
10.10	Multi Factor Authentication reset	96
11	Known Issues	97
11.1	AAC#006: Scan stuck at Status "Unknown"	97
11.2	AAC#005: Could not get table data: Data too large	98
11.3	AAC#004: Multiple Sandbox Issues	99
11.4	AAC#003: Case Management - onDelete is not defined	99
11.5	AAC#002: Context Deadline Exceeded	100
11.6	AAC#001: Nested LDAP Groups not working	101
12	Migrate from Cockpit v2.8.x to Cockpit v3.x	103
13	Glossary	105
13.1	Baselining	105

13.2	Cases	106
13.3	Invisible (Backend)	108
14	Changelog	109
14.1	Analysis Cockpit 3.10	109
14.2	Analysis Cockpit 3.8	110
14.3	Analysis Cockpit 3.7	111
14.4	Analysis Cockpit 3.5	112
14.5	Analysis Cockpit 3.4	113
14.6	Analysis Cockpit 3.3	113
14.7	Analysis Cockpit 3.2	114
14.8	Analysis Cockpit 3.1	115
14.9	Analysis Cockpit 3.0	116
14.10	Analysis Cockpit 3.0 unstable	117
15	Indices and tables	125

INTRODUCTION

Analysis Cockpit is the central platform for analyzing THOR events and SIGMA matches generated by ASGARDs real time agents.

It can be used in an environment where scans results can be automatically collected from ASGARD Management Centers or environments in which THOR is executed by scripts or any other 3rd party solution.

It is available as a virtual appliance on VMWare and also as a dedicated hardware appliance.

While THOR can also be seen or used as hunting solution THOR is optimized to avoid false negatives – meaning optimized to not miss an indicator of compromise. On the other side this clearly leads to more anomalies and false positives being reported.

In a scenario where you scan your infrastructure frequently you would either be seeing the same anomalies again and again or you would need to create many rules to filter out these anomalies in order to save analysis time.

Analysis Cockpit is designed to facilitate this process and help you generate these rules automatically, so that you can set your baseline-filters after the first scan. After setting the first baseline it is now easy to focus on relevant Alerts and Warnings as only differences between the first and second scans are shown.

Analysis Cockpit comes with an integrated and highly configurable ticketing system that helps organizing your analysis workflow and – if required – interfaces to your existing ticketing system through a configurable connector. If ASGARD's Bifrost_2 Service is used to collect suspicious samples, the Analysis Cockpit can submit the samples to various Sandbox systems and include the report in the graphical frontend.

Furthermore, Analysis Cockpit comes with a rule-based alert forwarding and SIEM integration that makes it easy for your organization to react quickly on new incidents. For organizations or projects where a SIEM system is not available, Analysis Cockpit features a separate notification section to deal with alerts and notifications you would normally process in a SIEM system.

The following document describes requirements, the installation process and best practices to group, classify and dispatch events for further analysis.

REQUIREMENTS

2.1 Hardware Requirements

There are a few things to consider, before you start with the installation.

If you install on VMWare, the minimum requirements for the virtual machine are as follows:

- System memory: 16 GB
- Hard disk: 200 GB
- CPU cores: 2

The disk size of 200 GB is fine in scenarios where you import only Alerts and Warnings into the Cockpit, scan less than 1.000 systems on a weekly basis and want to keep the logs for less than one year. If you also import Notices and Info messages for these 1.000 servers, we recommend a disk size of at least 500 GB.

For an Installation of up to 20.000 endpoints the following specifications are recommended:

- System memory: 32 GB
- Hard disk: 2 TB SSD
- CPU cores: 4

2.2 Network Requirements

The Analysis Cockpit and other systems which will have to communicate with each other, need the following ports opened within the network. For a detailed and up to date list of our update and licensing servers, please visit <https://www.nextron-systems.com/hosts/>.

The Analysis Cockpit requires the following open ports (incoming).

2.2.1 From Management Workstation to Analysis Cockpit

Description	Ports
Administrative Web Interface	443/tcp
Command Line Access	22/tcp

2.2.2 From Analyst Workstation to Analysis Cockpit

Description	Ports
Administrative Web Interface	443/tcp

2.2.3 From ASGARD Management Center to Analysis Cockpit

Description	Ports
Syslog Forwarding	514/tcp, 514/udp
Asset Synchronization	7443/tcp

2.2.4 From Analysis Cockpit to SIEM (optional)

Description	Ports
Syslog Forwarding	514/tcp, 514/udp

2.2.5 From Analysis Cockpit to the Internet

The Analysis Cockpit is configured to retrieve updates from the following URLs:

- Analysis Cockpit packages: <https://update3.nexttron-systems.com>

A proxy system should be configured to allow access to these URLs without TLS/SSL interception (Analysis Cockpit uses client-side SSL certificates for authentication). It is possible to configure a proxy server, username and password during the setup process of the Analysis Cockpit platform. It only supports BASIC authentication, not NTLM Authentication.

2.2.6 From Analysis Cockpit to Sandbox Systems (optional)

Depending on the Sandbox system and your individual configuration.

Description	Ports
Sandbox (typically)	443/tcp, 8080/tcp

2.2.7 Time Synchronization

Analysis Cockpit tries to reach the public Debian time servers by default.

Server	Port
0.debian.pool.ntp.org	123/udp
1.debian.pool.ntp.org	123/udp
2.debian.pool.ntp.org	123/udp

The NTP server configuration can be changed in the settings.

2.2.8 DNS

Analysis Cockpit needs to be able to resolve internal and external IP addresses.

Warning: Please make sure that you install your Analysis Cockpit with a **domain name** (see *Network Configuration*). If you do not set the domain name and install the ASGARD package, you will have problems connecting your ASGARD(s) to the Analysis Cockpit.

All components you install should have a proper domain name configured to avoid issues further during the configuration.

2.3 Internet Access during Installation

The Analysis Cockpit installer requires Internet access during the setup. The installation process will fail if required packages cannot be loaded from <https://update3.nexttron-systems.com>

2.3.1 SSL/TLS Interception

The installation and update processes do not accept an unknown but valid SSL/TLS certificate presented by an intercepting entity and therefore don't support SSL/TLS interception.

Since our products are usually used in possibly compromised environments, the integrity of our software and update packages has highest priority.

2.4 Verify the Downloaded ISO (Optional)

You can do a quick hash check to verify that the download was not corrupted. We recommend to verify the downloaded ISO's signature as this is the cryptographically sound method.

The hash and signature file are both part of the ZIP archive you download from our [portal server](#).

2.4.1 Via Hash

Extract the ZIP and check the sha256 hash:

On Linux

```
user@unix:~/nextron-universal-installer$ sha256sum -c nextron-universal-installer.iso.
↳ sha256
nextron-universal-installer.iso: OK
```

or in Windows command prompt

```
C:\temp\nextron-universal-installer>type nextron-universal-installer.iso.sha256
efccb4df0a95aa8e562d42707cb5409b866bd5ae8071c4f05eec6a10778f354b nextron-universal-
↳ installer.iso
C:\temp\nextron-universal-installer>certutil -hashfile nextron-universal-installer.iso.
↳ SHA256
SHA256 hash of nextron-universal-installer.iso:
efccb4df0a95aa8e562d42707cb5409b866bd5ae8071c4f05eec6a10778f354b
CertUtil: -hashfile command completed successfully.
```

or in Powershell

```
PS C:\temp\nextron-universal-installer>type .\nextron-universal-installer.iso.sha256
efccb4df0a95aa8e562d42707cb5409b866bd5ae8071c4f05eec6a10778f354b nextron-universal-
↳ installer.iso
PS C:\temp\nextron-universal-installer>Get-FileHash .\nextron-universal-installer.iso

Algorithm      Hash
↳ Path
-----
--
↳ --
SHA256          EFCCB4DF0A95AA8E562D42707CB5409B866BD5AE8071C4F05EEC6A10778F354B
↳ C:\Users\user\Desktop\asgard2-installer\nextron-universal-installer.iso
```

2.4.2 Via Signature (Recommended)

Extract the ZIP, download the public signature and verify the signed ISO:

On Linux

```
use@unix:~/temp$ wget https://www.nextron-systems.com/certs/codesign.pem
use@unix:~/temp$ openssl dgst -sha256 -verify codesign.pem -signature nextron-universal-
↳ installer.iso.sig nextron-universal-installer.iso
Verified OK
```

or in Powershell

```
PS C:\temp\nextron-universal-installer>Invoke-WebRequest -Uri https://www.nextron-
↳ systems.com/certs/codesign.pem -OutFile codesign.pem
PS C:\temp\nextron-universal-installer>"C:\Program Files\OpenSSL-Win64\bin\openssl.exe"
↳ dgst -sha256 -verify codesign.pem -signature nextron-universal-installer.iso.sig
↳ nextron-universal-installer.iso
Verified OK
```


Note: If openssl is not present on your system you can easily install it using winget: `winget install openssl`.

2.5 Other Optional Requirements

2.5.1 Usage of a Reverse Proxy

If you are planing to make the Analysis Cockpit available through a reverse proxy, see [Reverse Proxy to access the Analysis Cockpit](#).

2.6 Architecture

The following image shows an architecture overview with all products and their communication relationships.

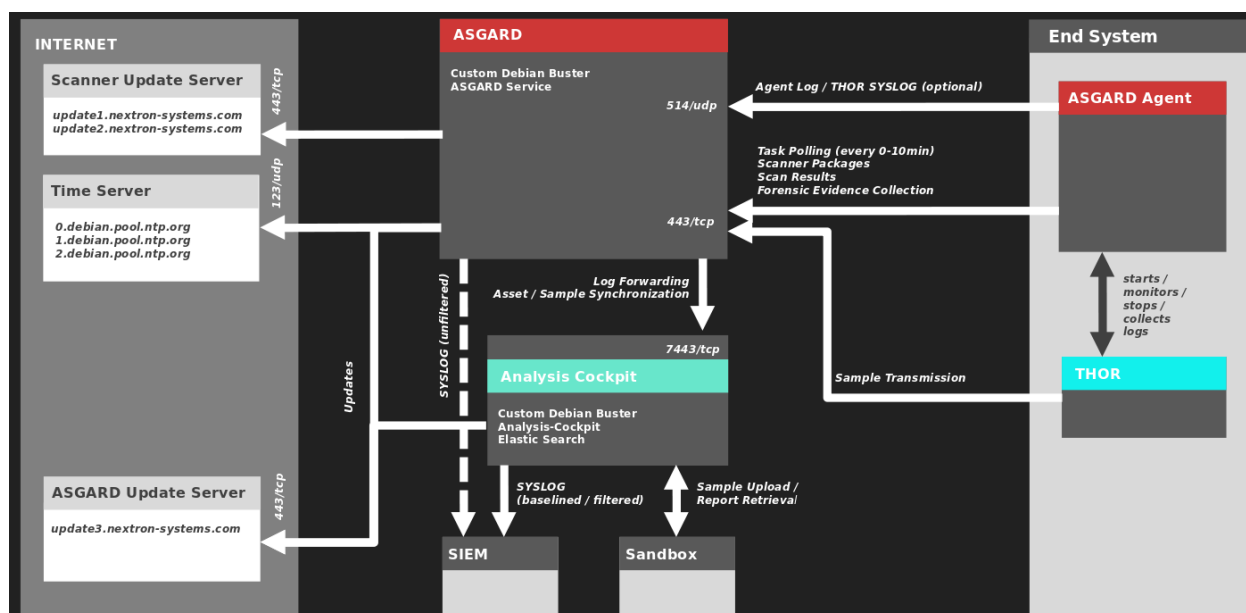


Fig. 1: Full Architecture

SETUP GUIDE

3.1 Create a New ESX VM and Mount the ISO

Create a new VM with your virtualization software. In this case, we will use VMWare ESX managed through a VMWare VCenter.

The new VM must be configured with a Linux base system and Debian GNU/Linux 10 (64 bits) as target version. It is recommended to upload the Nextron Universal Installer ISO to an accessible datastore and mount the same to your newly created VM.

Please make sure to select a suitable v-switch or physical interface that reflects the IP address scheme you are planning to use for the new Analysis Cockpit. Only use one Hard Disk for the installation.

3.2 Analysis Cockpit Installation

Start the installation confirming the only available option in the boot loader screen.

The installer then loads the additional components from the ISO image and lets you select a location and language.

If DHCP is available, network parameters will be configured automatically.

Without DHCP, ASGARD proceeds with the manual network configuration dialogue.

3.3 Network Configuration

The next step prompts for a hostname for the device. After entering a hostname and clicking **Continue**, it also prompts for the Domain Name. After this Information is submitted, the Installer tries to get network configurations from a DHCP-Server. If there is none to be found, it will prompt for a static IP-Configuration.

Enter the IP address that Analysis Cockpit should use and optimally directly add a netmask in CIDR notation. (see below) If you don't append the netmask, you'll be asked for a network mask in the following dialogue.

Important: Important: Make sure that the combination of hostname and domain creates an FQDN that can be resolved from the ASGARD Management Center(s) you want to connect with your Analysis Cockpit. If you've configured a FQDN (hostname + domain) that cannot be resolved, your ASGARDS will encounter an error during connection.

This is especially important since your Analysis Cockpit will create some certificates during the installation, which will not contain an IP Address as its Subject Alternative Name (SAN), but only the FQDN! You will not be able to connect your ASGARD Management Center with your Analysis Cockpit via IP Address.

New Virtual Machine

1 Select a creation type

- 2 Select a name and folder
- 3 Select a compute resource
- 4 Select storage
- 5 Select compatibility
- 6 Select a guest OS
- 7 Customize hardware
- 8 Ready to complete

Select a creation type

How would you like to create a virtual machine?

- Create a new virtual machine
- Deploy from template
- Clone an existing virtual machine
- Clone virtual machine to template
- Clone template to template
- Convert template to virtual machine

This option guides you through creating a new virtual machine. You will be able to customize processors, memory, network connections, and storage. You will need to install a guest operating system after creation.

CANCEL

BACK

NEXT

New Virtual Machine

✓ 1 Select a creation type

2 Select a name and folder

- 3 Select a compute resource
- 4 Select storage
- 5 Select compatibility
- 6 Select a guest OS
- 7 Customize hardware
- 8 Ready to complete

Select a name and folder

Specify a unique name and target location

Virtual machine name: asgard.nexttron

Select a location for the virtual machine.

▼  vcenter

CANCEL

BACK

NEXT

New Virtual Machine

- ✓ 1 Select a creation type
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Select storage
- ✓ 5 Select compatibility
- 6 Select a guest OS**
- 7 Customize hardware
- 8 Ready to complete

Select a guest OS

Choose the guest OS that will be installed on the virtual machine

Identifying the guest operating system here allows the wizard to provide the appropriate defaults for the operating system installation.

Guest OS Family:

Guest OS Version:

Compatibility: ESXi 6.7 and later (VM version 14)

CANCEL

BACK

NEXT

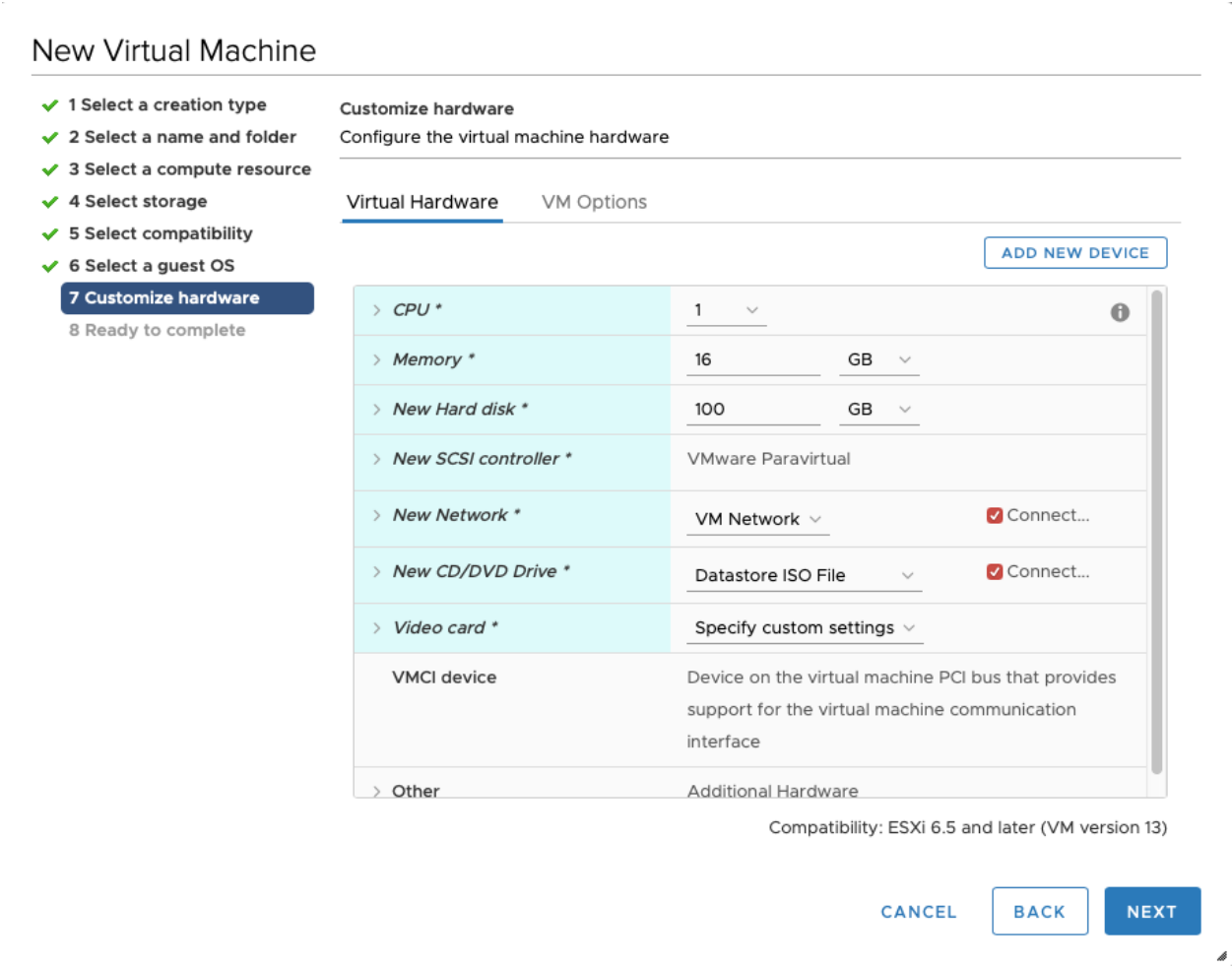


Fig. 1: Create a new virtual Machine

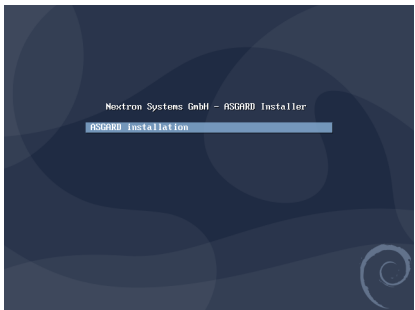


Fig. 2: Starting the installation

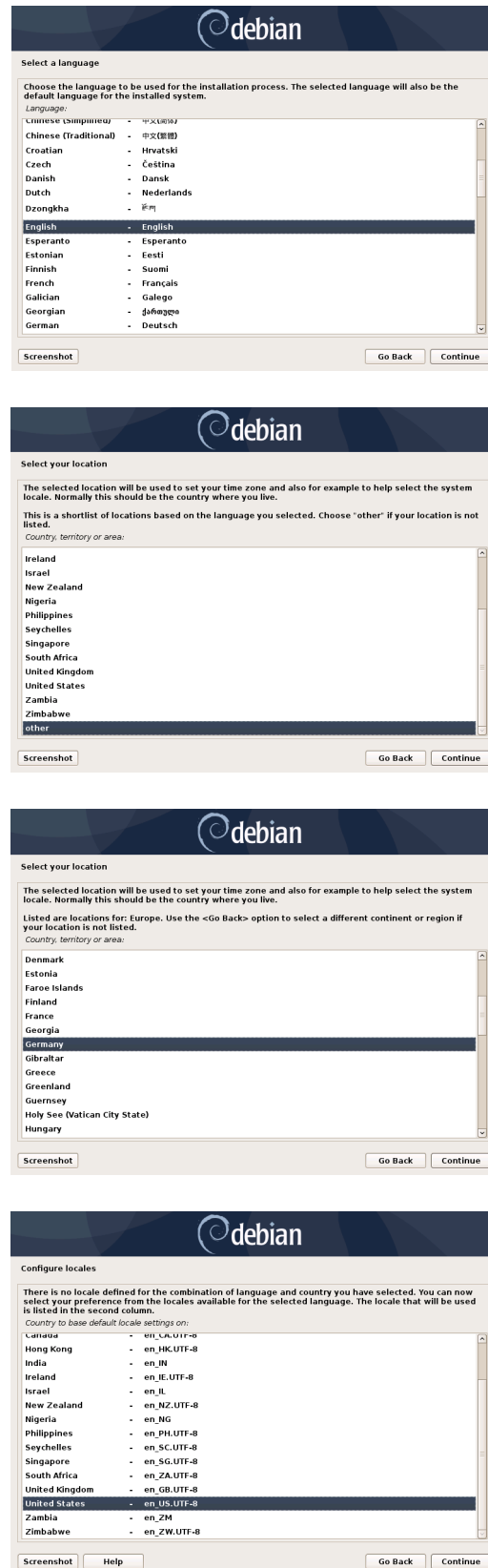


Fig. 3: Choosing language, location and locales

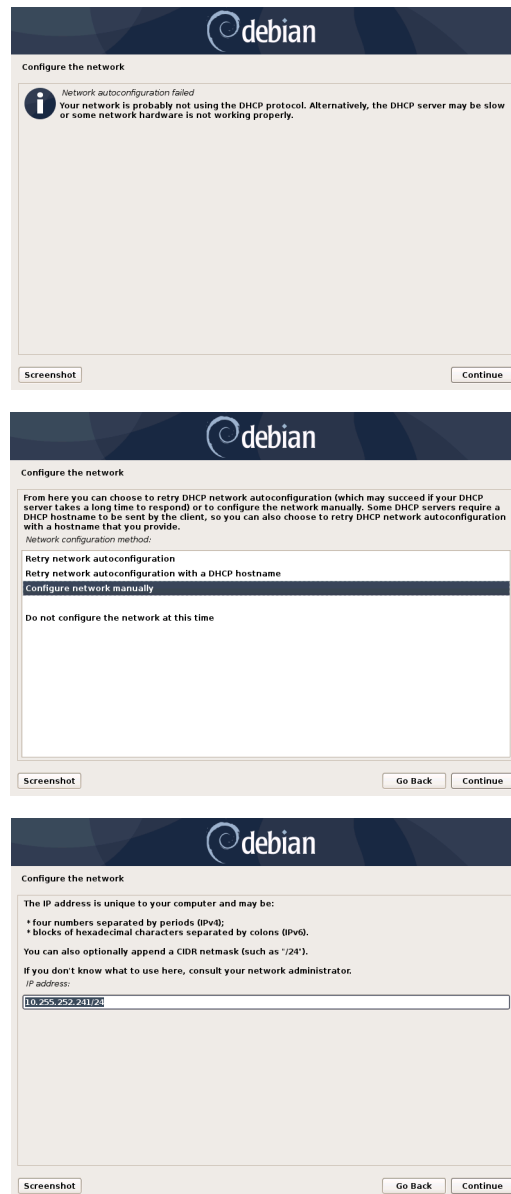


Fig. 4: Network Configuration - IP addresses



Fig. 5: Network Configuration – Enter the DNS server addresses



Fig. 6: Network Configuration - Enter the Gateway



Fig. 7: Network Configuration - Enter the Hostname



Configure the network

The domain name is the part of your Internet address to the right of your host name. It is often something that ends in .com, .net, .edu, or .org. If you are setting up a home network, you can make something up, but make sure you use the same domain name on all your computers.

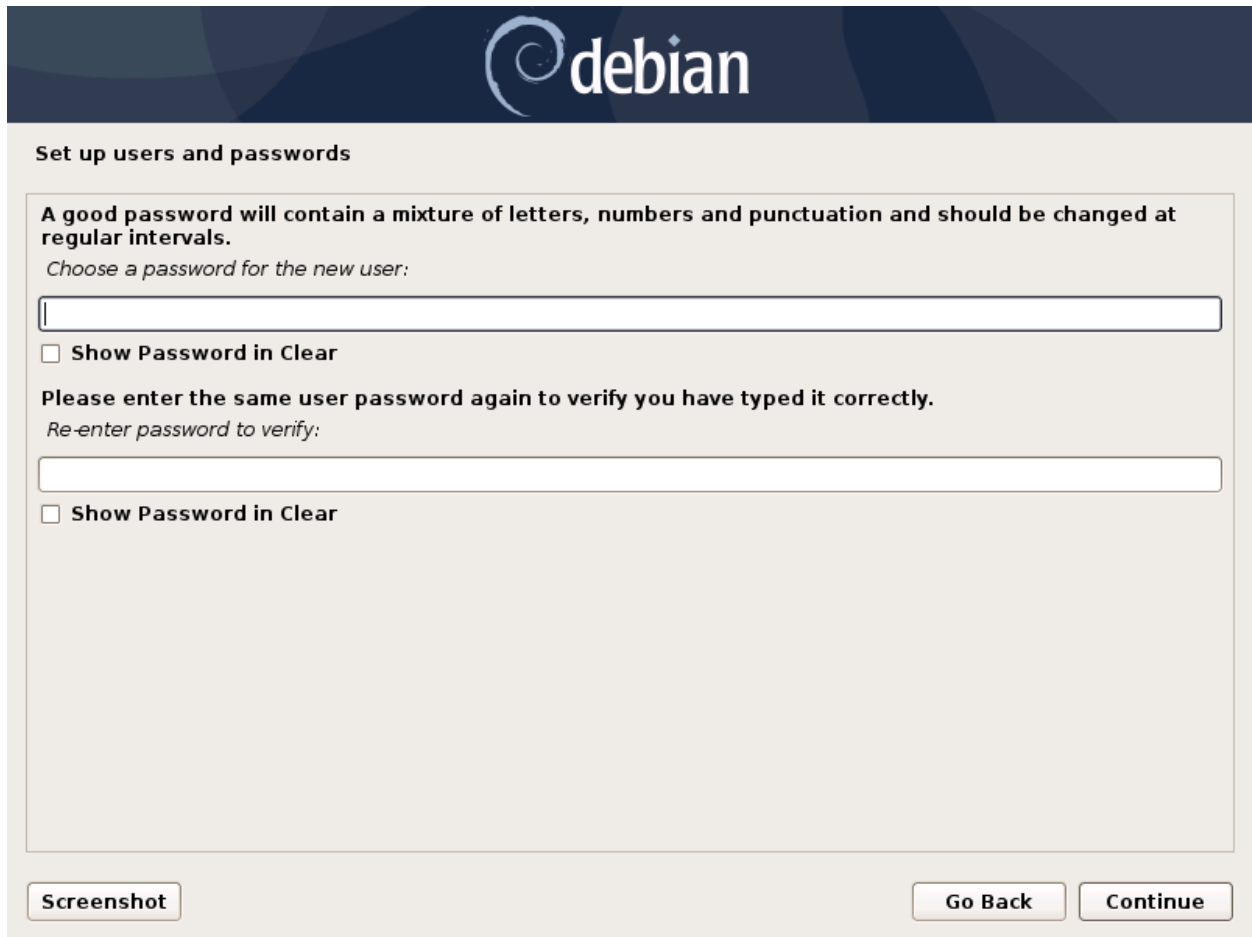
Domain name:

Screenshot

Go Back Continue

Fig. 8: Network Configuration - Enter the Domain name

3.4 Choosing a password



Set up users and passwords

A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.

Choose a password for the new user:

☐ **Show Password in Clear**

Please enter the same user password again to verify you have typed it correctly.

Re-enter password to verify:

☐ **Show Password in Clear**

Screenshot **Go Back** **Continue**

Fig. 9: Choosing a password for the nextron user

3.5 Partitioning of the Hard Disk

Warning: The Analysis Cockpit is intended to be installed with only one disk. Do not configure your server with multiple disks. The system won't configure additional disks. Make sure that your disk has the recommended size. See [Hardware Requirements](#) for more information.

Finally, confirm the settings, select “Yes” and click “Continue”.

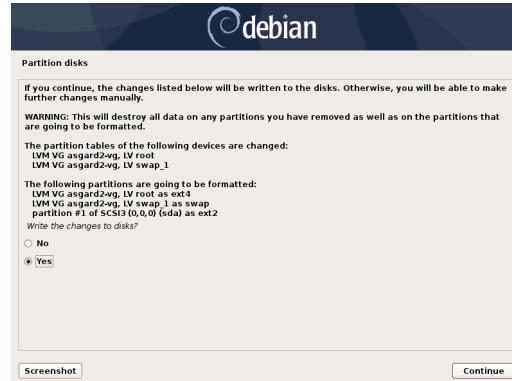


Fig. 10: Partition Disks – Write changes to disks

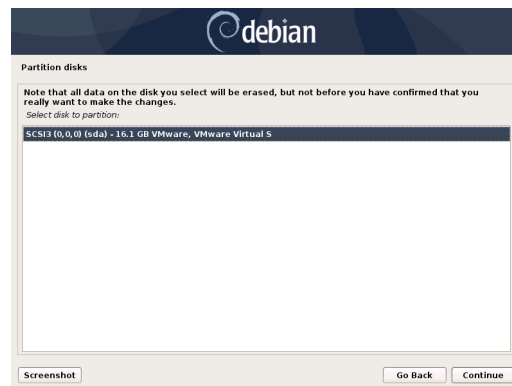


Fig. 11: Partition disks – Select disk to partition

3.6 Proxy Configuration

If you are using a proxy to access the Internet, enter the proxy details in the next step. Please note, Internet connectivity is required for the next step – the installation of the ASGARD Analysis Cockpit service.



Fig. 12: Proxy Configuration

The proxy configuration supports unauthorized access and HTTP Auth, for example `http://our-proxy.local:8080` and `http://username:password@our-proxy.local:8000`

3.7 Install the Analysis Cockpit Services

The base installation is now complete. In the next step we'll install the Analysis Cockpit service.

Important:

- Internet connectivity is required for this step.
 - Use an upper case **i** in the word `nextronInstaller`.
-

Use the VMWare console or SSH to the appliance using the user `nextron`.

To start the Analysis Cockpit installation run the following command:

```
nextron@asgard-ac:~$ sudo nextronInstaller -cockpit
```

After the installer has completed its operations successfully, the system is ready to be used.

```
Installation of Analysis Cockpit 3 completed.
Use https://analysis3-iso to connect to the web frontend
nextron@analysis3-iso:~$
```

Fig. 13: Message upon successful completion

Note that the FQDN shown after `https://` has to be resolvable by the connected ASGARD Management Centers and users that try to access the Analysis Cockpit.

3.8 Changing Passwords

3.8.1 Console

The password for the linux system can be changed by opening a command line on the Analysis Cockpit. Log into the Analysis Cockpit via SSH with the user **nextron**.

Simply type the following command after logging into the system, to set a new password for the **nextron** user.

```
nextron@asgard-ac:~$ passwd
Changing password for nextron.
Current password:
New password:
Retype new password:
passwd: password updated successfully
```

Make sure to write that new password down or better save it into a password safe.

Note: On older installations default password is **nextron**.

3.8.2 Web UI

Log into the web-based frontend with user **admin** and password **admin** and change the initial password.

The Analysis Cockpit Web interface password can be changed by clicking your username in the top right corner and selecting **User Settings**. From here you can change your password.

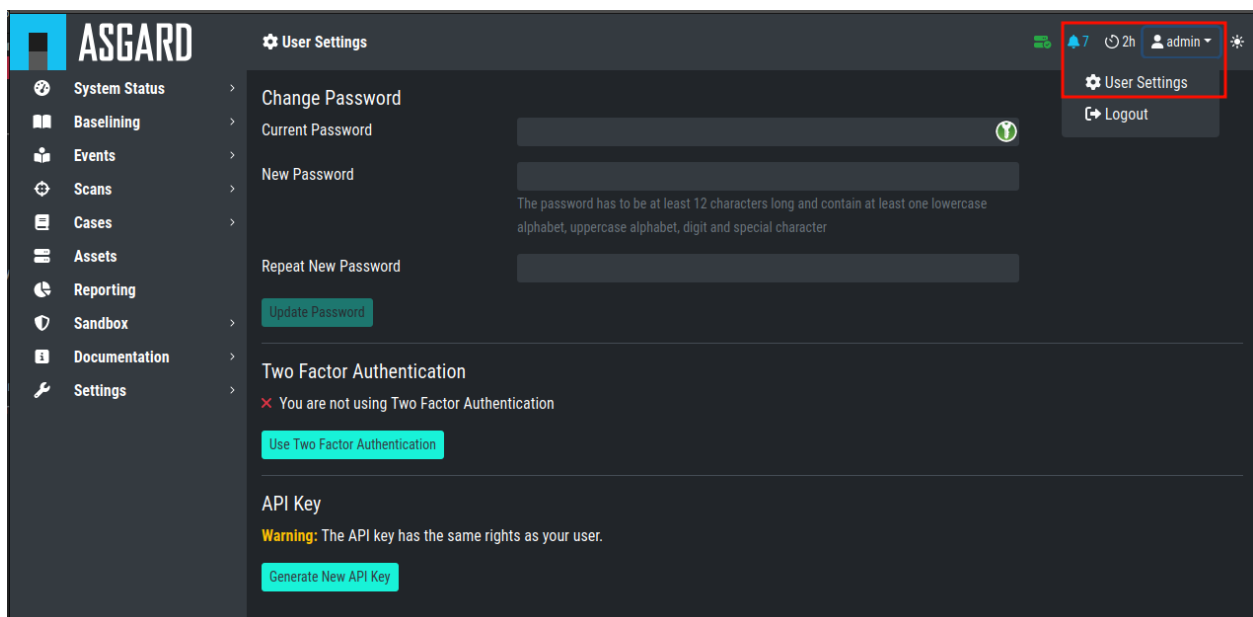


Fig. 14: User Settings

3.9 Changing the IP-Address

The Analysis Cockpit's IP-Address can be changed in `/etc/network/interfaces`. The IP is configured with the address variable.

```
nexttron@asgard-ac:~$ sudo vi /etc/network/interfaces
```

```
auto ens32
iface ens32 inet static
    address 172.16.2.7/24
    gateway 172.16.2.254
    dns-nameservers 172.16.20.20
```

You can now restart `networking.service` to apply the changes.

```
nexttron@asgard-ac:~$ sudo systemctl restart networking.service
```

Important:

- The network interface might have a different name, so pay attention to the name (in this example `ens32`).
 - If restarting the `networking.service` is throwing an error, you can restart the server
-

The new IP can be applied with the command **`sudo systemctl restart networking`**

3.9.1 Verifying DNS Settings

To verify if ASGARD is using the correct DNS Server, you can inspect the file `/etc/resolv.conf`:

```
nexttron@asgard-ac:~$ cat /etc/resolv.conf
search example.org
nameserver 172.16.200.2
```

If you see errors in this configuration, you can change it with the following command:

```
nexttron@asgard-ac:~$ sudoedit /etc/resolv.conf
```


ADMINISTRATION

This chapter assumes, that you have read chapter *Basic Concepts*.

In order to configure the Analysis Cockpit for the first use, the following steps need to be done:

- License installation
- System update
- Set users and set user rights
- Define canned responses
- Decide about syslog forwarding
- Integrate your log source

These steps are described in detail in the following sections.

4.1 License Installation

Before you can use the cockpit, you must install a license. Navigate to the Licensing section, click the Upload License Button, select your license file and click the Upload Button.

4.2 System Update

All updates can be done from the Web GUI. Simply navigate to the Updates section, review the release notes and click the update button. You can also check for new updates by clicking the Check for Updates Button.

4.3 Set Users and User Rights

The chapter *Understanding Users, Roles, Rights and Case Status* already described how to set up a 2-level analyst model for working with cases. The roles defined in that section are non-administrative roles, meaning they are only allowed to access cases based on the respective status of a ticket.

Additionally, roles can have the following rights:

- Administrator
- Universal
- View Notifications

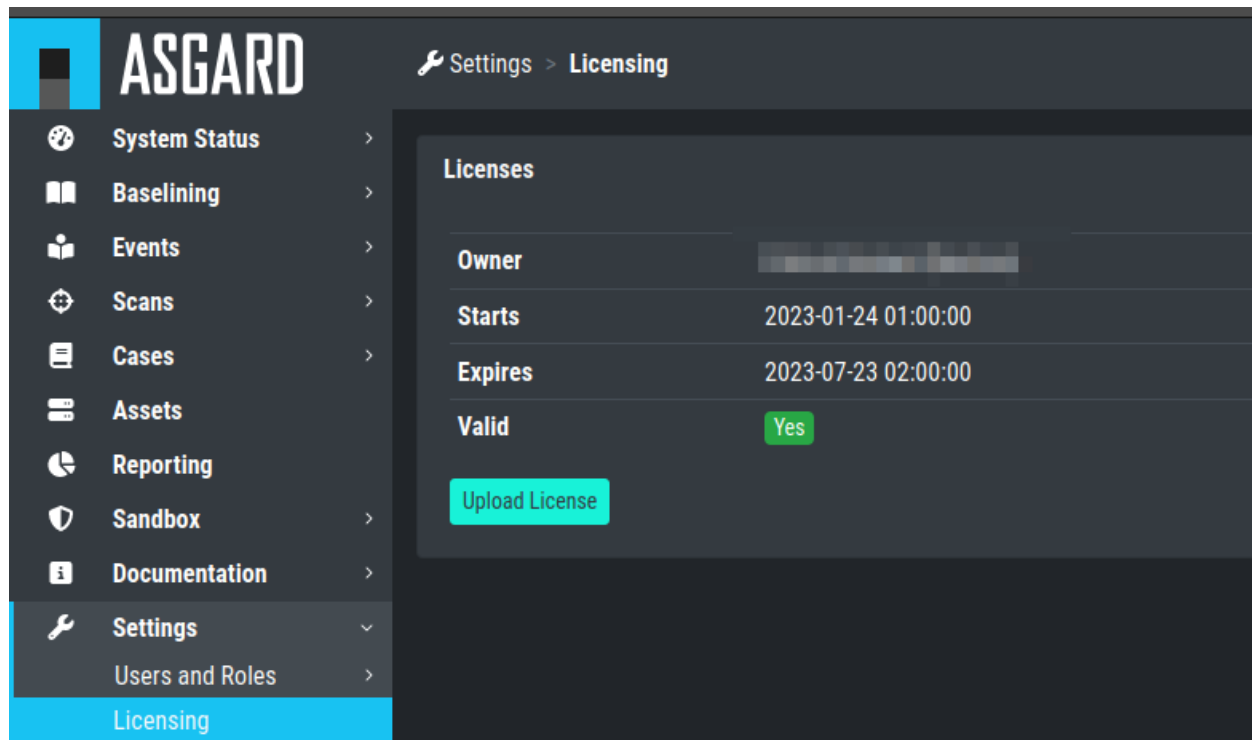


Fig. 1: Licensing

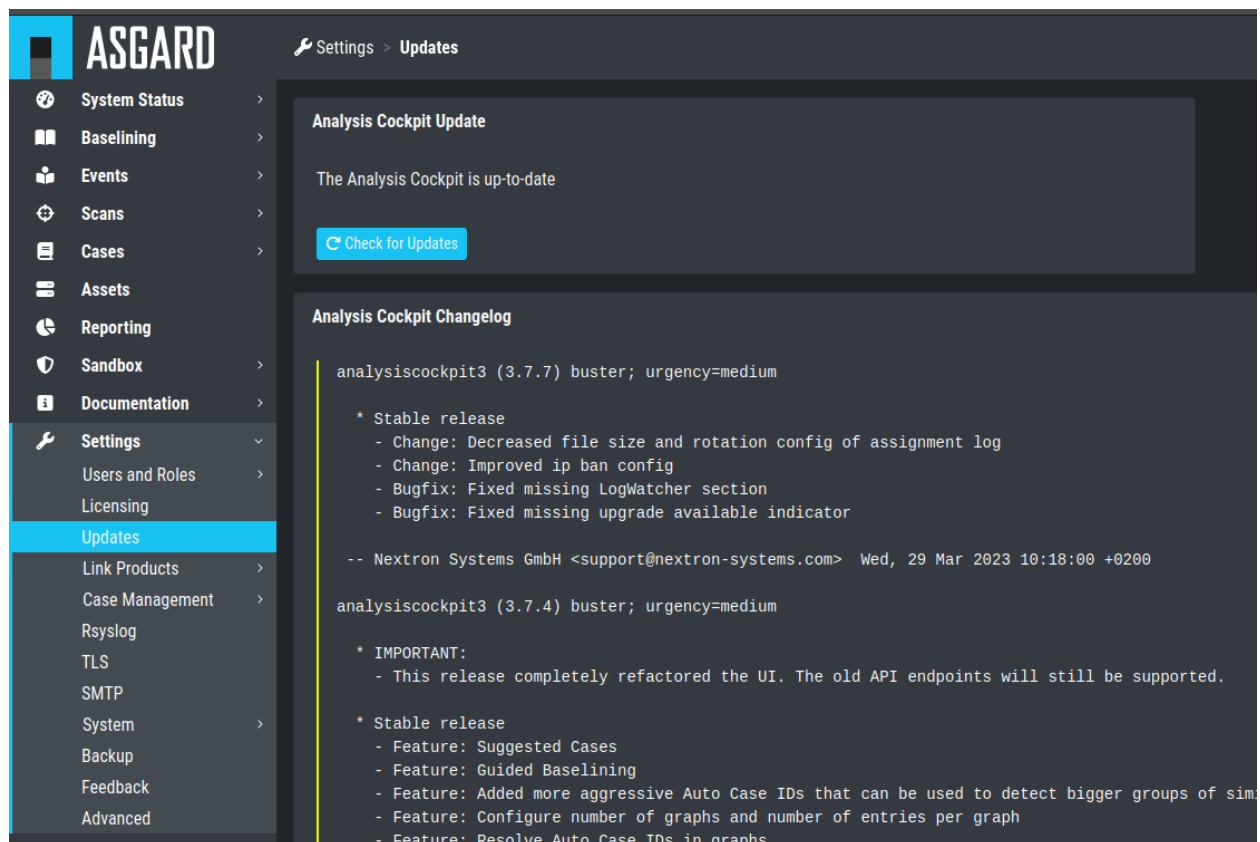


Fig. 2: Updating the System

- Acknowledge Notifications
- Upload Events
- Delete Events
- Upload File(s) for Sandbox Analysis
- Download File(s) for Sandbox Analysis

Roles can be granted these privileges by choosing them in the New Role dialogue.

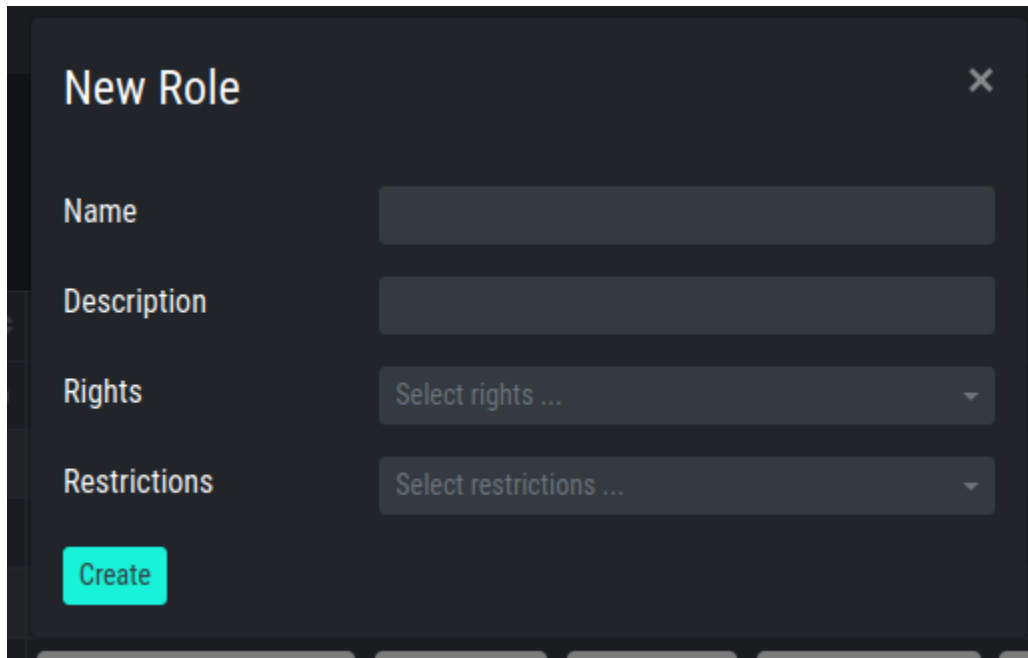


Fig. 3: New Role

4.4 Configure Canned Recommendations

Canned recommendations are predefined actions that can be used within a case. The recommendations are fully configurable and are aimed to facilitate choice making regarding the action that should be applied for a specific case. There is no need to set this up, but we suggest doing some planning and provide recommendations that are suitable for your organization. Some recommendations such as Verify Legitimacy, Provide Sample File / Sample Directory, Run full Antivirus Scan are already generated by default. You are free to use, modify or delete them. Recommendations can also be added by any user from within a case.

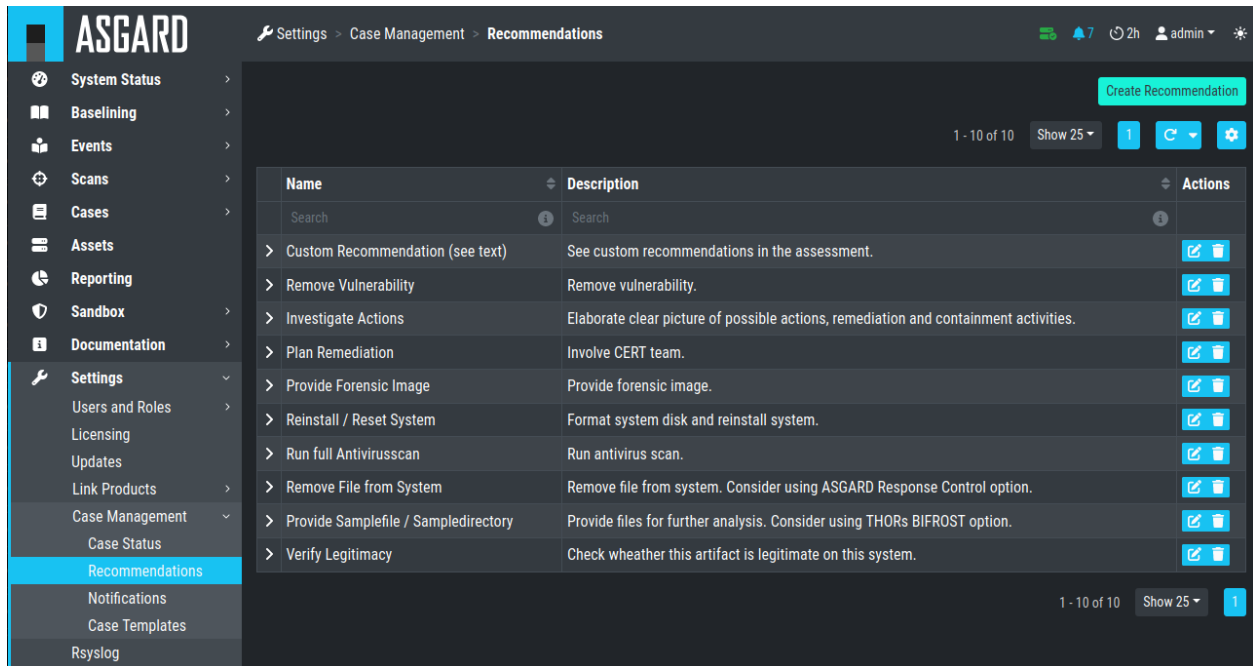


Fig. 4: Case Management- Recommendations

4.5 Syslog Forwarding

The Rsyslog Tab in the Settings section allows forwarding of all incoming THOR events along with all audit logs and all other cockpit related logs.

Please note, that forwarding THOR Logs through syslog might lead to a certain loss of information as THOR events might exceed syslog length restrictions.

4.6 TLS Certificate Installation

Instead of using the pre-installed self-signed TLS Certificate, users can upload their own TLS Certificate for ASGARD.

In order to achieve the best possible compatibility with the most common browsers, we recommend using the system's FQDN in both fields Common Name AND Hostnames.

Hint: Please note that generating a CSR on the command line is not supported.

The generated CSR can be used to generate a TLS Certificate. Subsequently, this TLS Certificate can be uploaded in the Settings > TLS section.

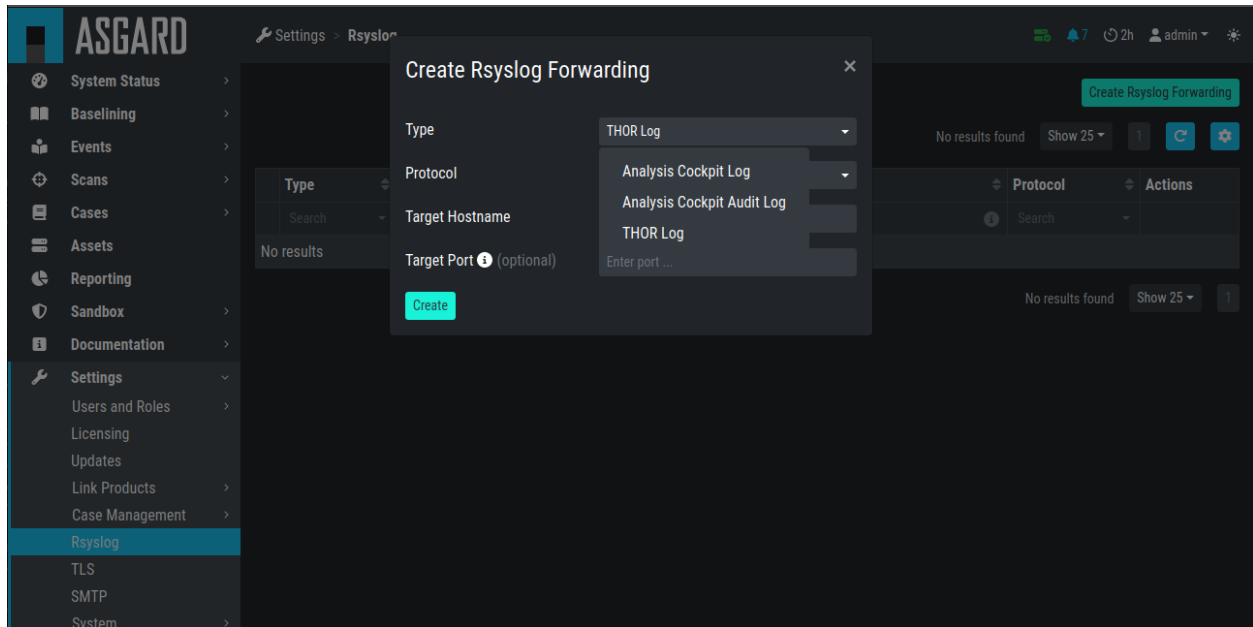


Fig. 5: Add Rsyslog Forwarding II

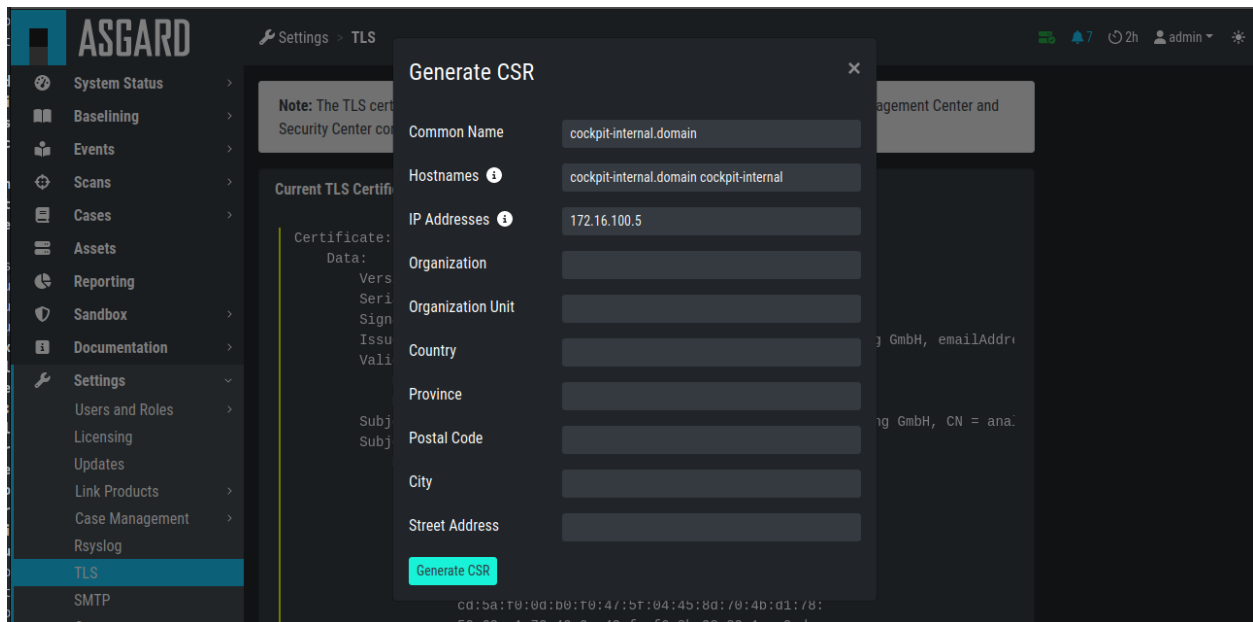


Fig. 6: Generate a Certificate Signing Request (CSR)

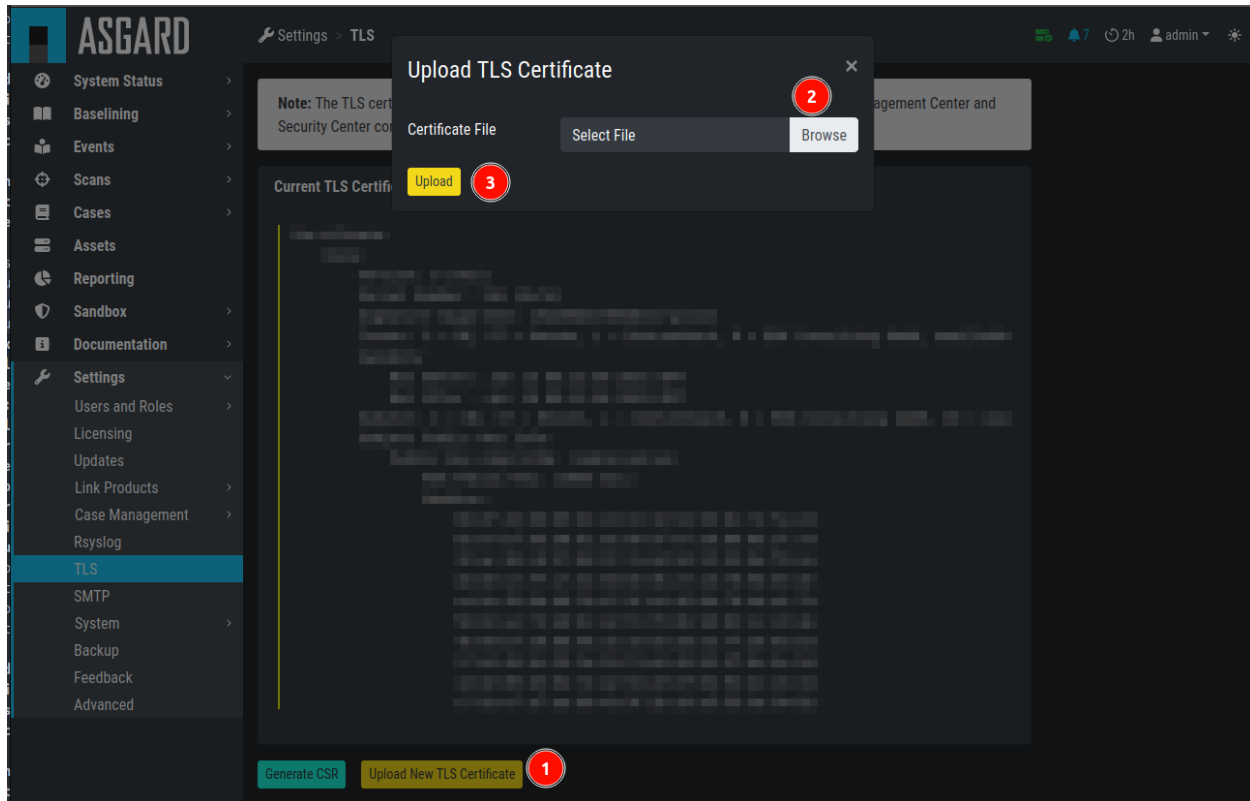


Fig. 7: Upload a TLS Certificate

4.7 Configure LDAP

The LDAP tab in the Users and Roles section lets you configure an LDAP server and define mappings for LDAP groups to roles within the Analysis Cockpit.

The figures below illustrate options of a possible LDAP configuration.

4.8 Configure Notifications

As described in *Cases and Log Processing*, the Analysis Cockpit is able to forward logs to a SIEM system in case this particular log line was added automatically to a case with the type "Incident".

The Notifications tab allows you to define custom notifications for event assignments (Event Assignment Notifications). It is recommended to at least configure an Event Assignment Notification for events that get added to existing Incident cases.

Additionally, notifications can be defined for changes to cases (Case Change Notifications), so Level 2 analysts can get notified if a case gets added to their in-queue (e.g., Finished Level 1).

The notification itself can be a syslog message or an email. In order to use email for notifications you have to setup an email account in the Mail Account Tab. Additionally webhook support has been added to facilitate interfacing to services like Slack.

Note: The Analysis Cockpit will collect all triggering events and send only one email every 15 minutes. Syslog and

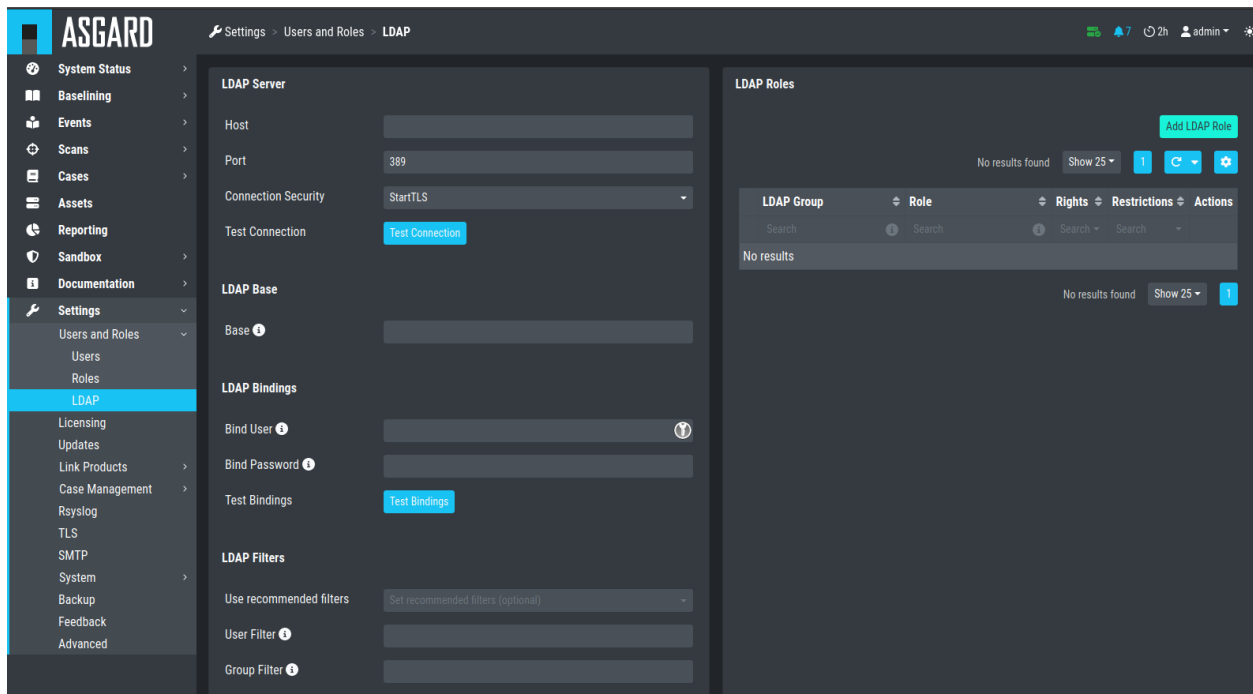


Fig. 8: Configure LDAP

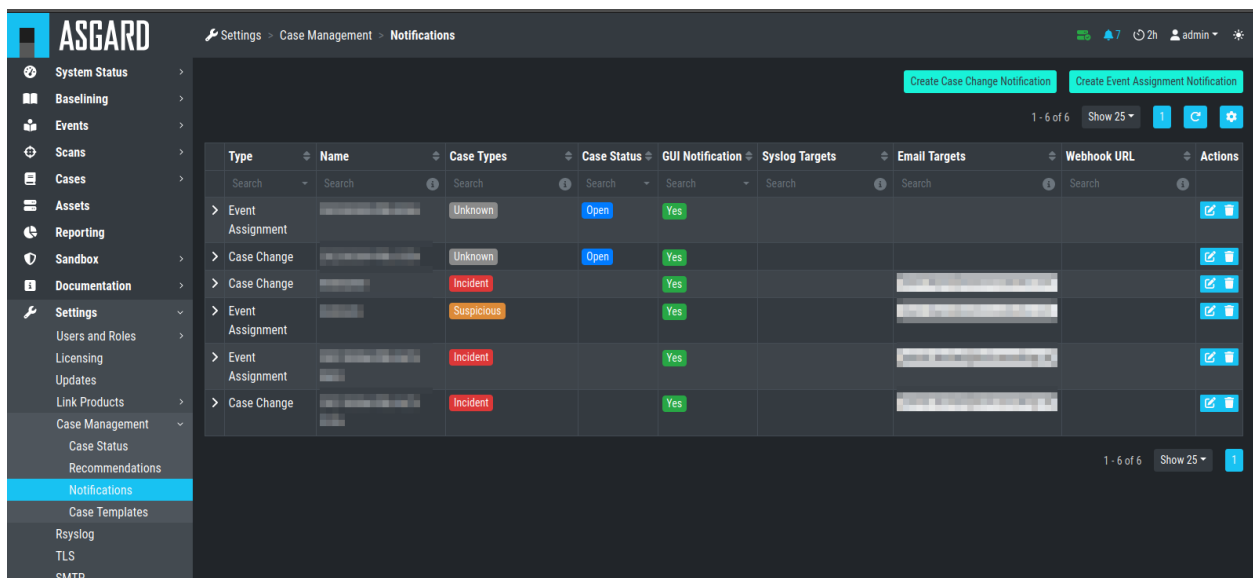


Fig. 9: Case Management- Notifications

Webhooks are triggered in real time for every single event.

Additionally, you can see the notifications in the top right corner (bell icon) and inspect them. You will see all Unread notifications, which can be Acknowledged by selecting one or more notification and clicking Acknowledge. Only Unread notifications will show up in the top right status bar of the Cockpit.

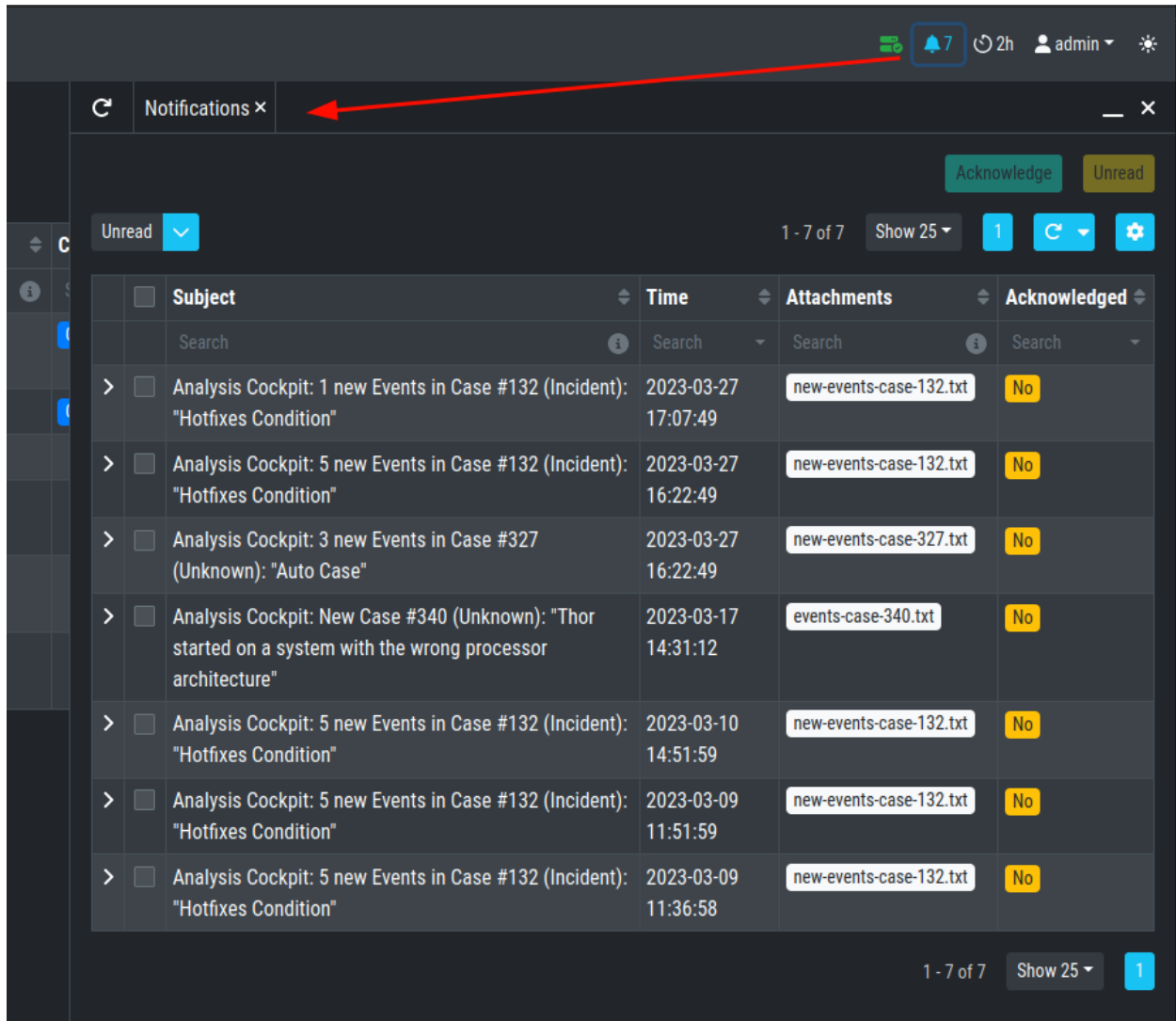


Fig. 10: UI Notifications

4.8.1 Configure Event Assignment Notifications

To configure log notifications, click the **Add Event Assignment Notification** button in the Notifications Tab of the **Settings** section. This leads you to a form that allows you to set a name for your notification, the notification type (syslog, email, webhook or notification within the Analysis Cockpit) and the condition that will trigger your notification.

Fig. 11: Event Assignment Notification

4.8.2 Configure Case Change Notifications

To configure Case Change Notifications, click the **Add Case Change Notification** button in the Notifications Tab of the **Settings** section. This leads you to a form that allows setting a name for your notification, the notification type (syslog, email, webhook or notification within the Analysis Cockpit) and the condition that will trigger your notification.

4.9 Log File Import

4.9.1 Basic Concepts

In general, all logs show up in the Events section. Additionally, all Alerts and Warnings that are not matching a particular case will show up in the Baselining section. Notices and informational events will NOT show up in the Baselining Section as they match the predefined default cases for these events.

All logs are tagged with a specific scan id – regardless of how the log was integrated. This enables filtering down to all logs contained in a specific scan.

If ASGARD Management Center is connected and the events was generated as part of a group scan the event is also tagged with this particular group scan id. This allows for filtering down to all logs a particular group scan.

Assets are identified through the asset ID that was issued by ASGARD Management Center during the setup of the ASGARD Agent. If this ID is not available to the Analysis Cockpit (e.g. log has been uploaded manually or sent

Fig. 12: Case Change Notification

through syslog) the hostname (NOT the FQDN) will be used instead.

4.9.2 Direct Integration with ASGARD Management Center

If the Analysis Cockpit is linked to one or more ASGARD Management Centers, all THOR logs get integrated automatically and will show up in the Baselining and/or the Events section. Aurora Events will also automatically show up.

To see how to connect an ASGARD Management Center with your Analysis Cockpit, follow the instructions in the chapter [Connect to ASGARD Management Center](#).

You can retrieve old scans performed by ASGARD Management Center before connecting it to Analysis Cockpit using the Request Events button in the Scans section.

4.9.3 Syslog Input

Another way to import log data is by using SYSLOG messages.

The ANALYSIS COCKPIT listens on port 514/udp and 514/tcp for incoming log data and all logs will show up in the Baselining and/or the Events section.

Incoming syslog messages get assigned to single scan using the "ScanID" value that's unique in each scan.

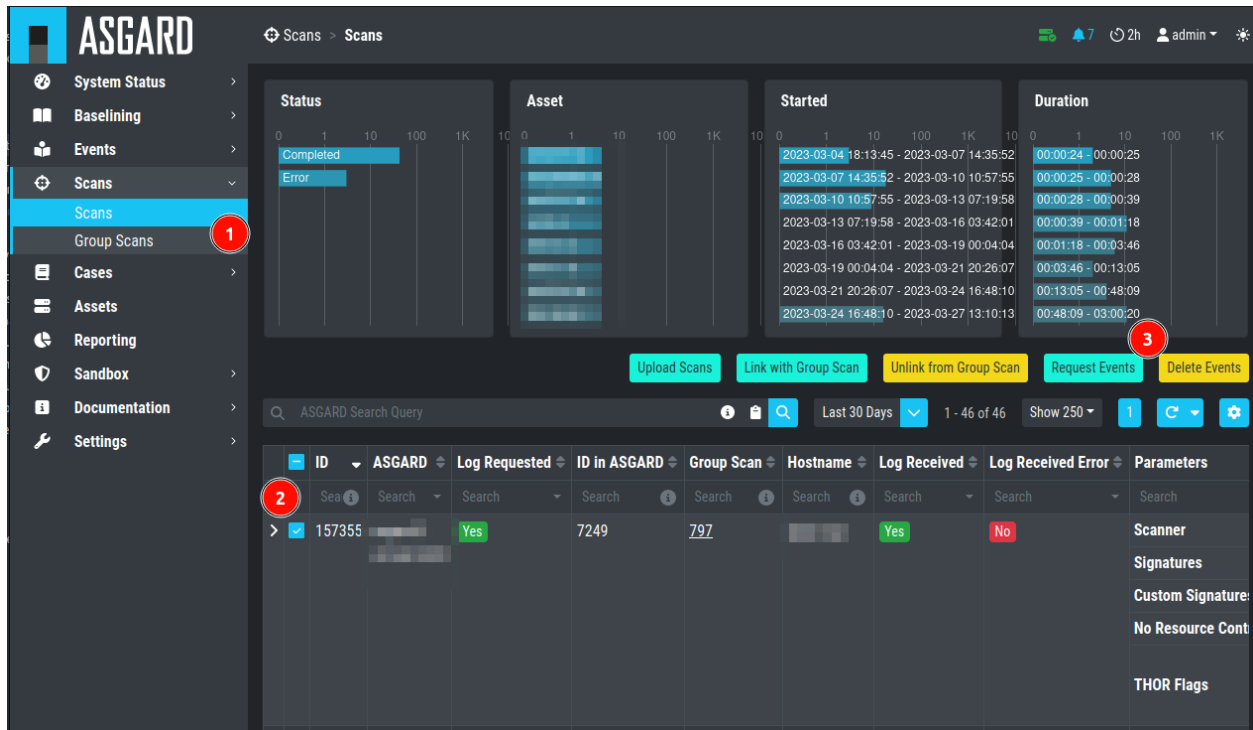


Fig. 13: Request Events from Scan

4.9.4 File Import Through Web-Based GUI

Alternatively, logs can be uploaded through the web-based interface by selecting the particular log file (must be the .txt format, html import is not supported) and clicking the Upload Scans button within the Scans section.

Note: You can upload one or more THOR scans in one or more text files. The Analysis Cockpit will automatically generate scans in the database, based on the scanned assets and the SCAN_IDs in the events. Only .txt, .log, .txt.gz and .log.gz files are supported.

After a successful upload, the scans should appear in the list below.

Important: If you can not see events in the Events or Baselining views, please make sure that you've selected the correct time frame as filter. Often times manually uploaded scans happened days or weeks before the upload. The log data gets indexed with the timestamp of their creation and not the import, and can therefore be hidden in the default view.

After the upload, you're able to link the recently uploaded scans with an existing or new group scan. You can also unlink scans from a group scan.

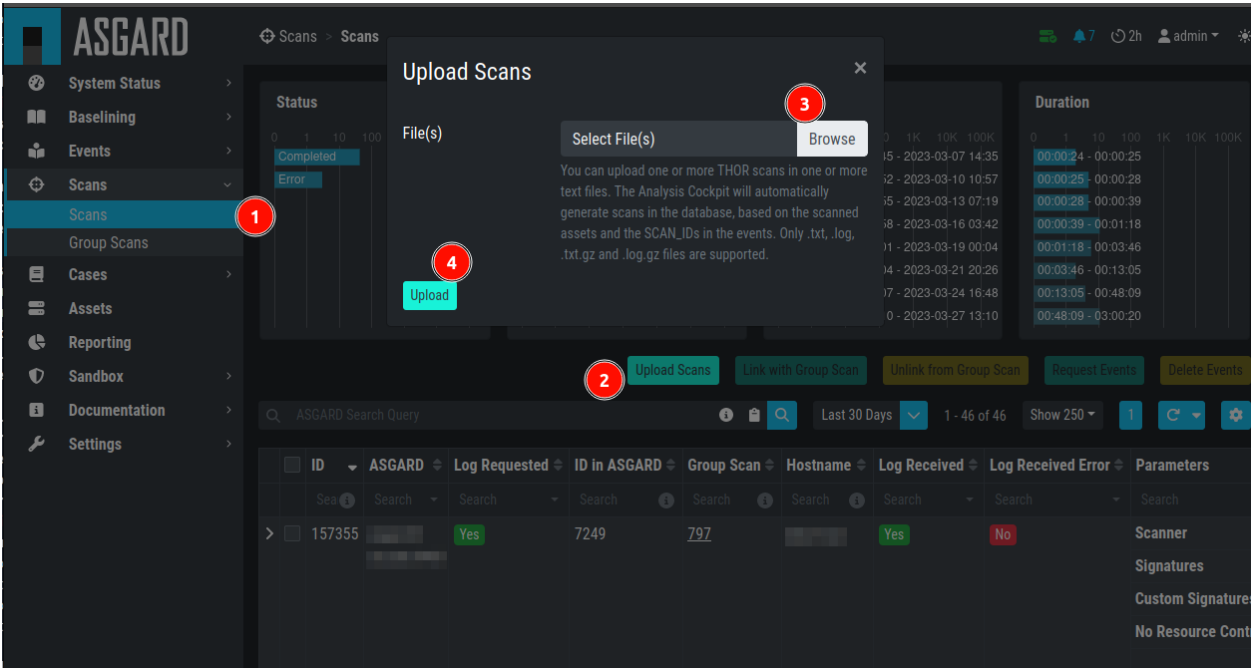


Fig. 14: Upload logs using the web-based interface

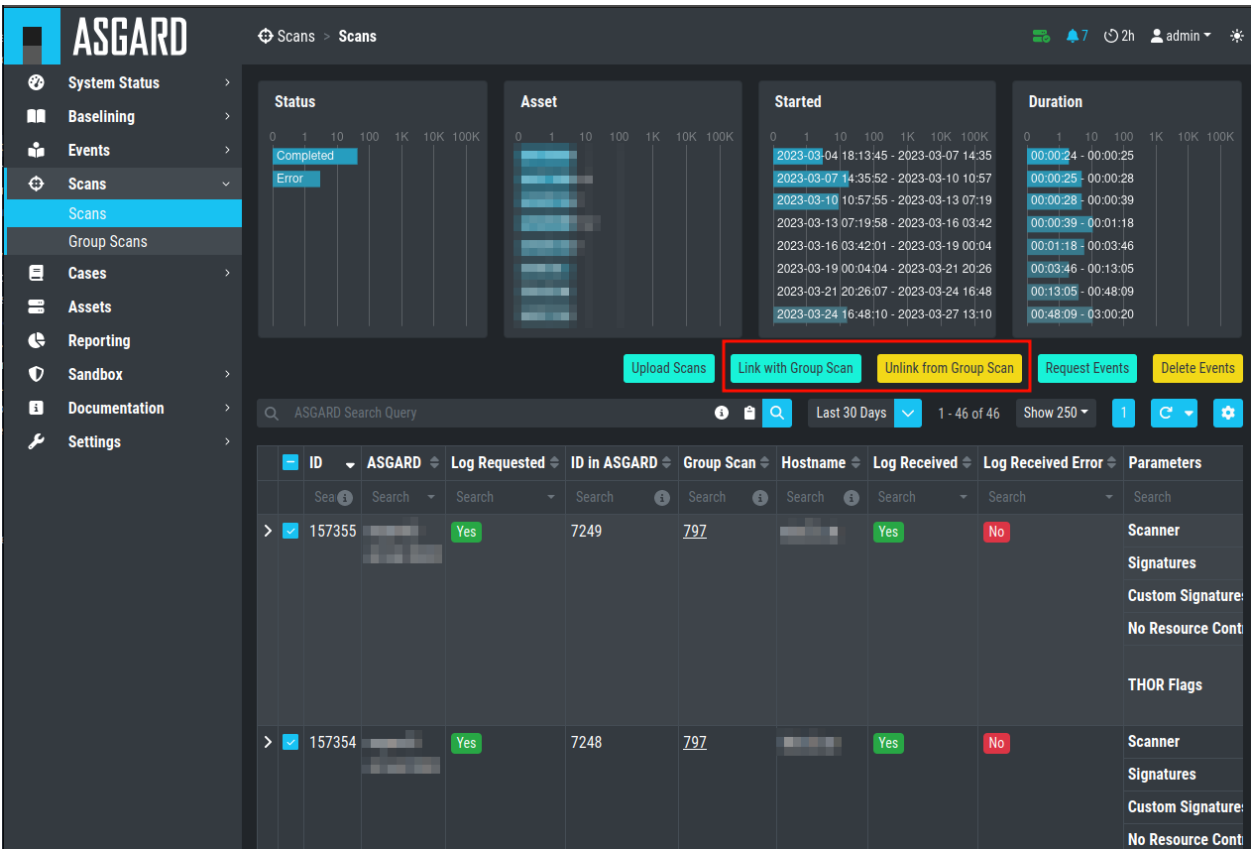


Fig. 15: Link/Unlink scans with an existing or new group scan

4.9.5 File Import Using the Command Line

This option can be helpful in an environment where you scan without ASGARD Management Center but want to automate analysis by dropping the log data into that import directory.

Log files can be imported by placing the files in the following directory:

```
/var/lib/nextron/analysiscockpit3/events
```

Make sure that user and group of these files is set to `cockpit`.

You can change the owner and group manually by using:

```
nexttron@asgard-ac:~$ sudo chown cockpit:cockpit <file>
```

Successfully imported files get a new extension named `.ok`.

When the file is moved to that folder with the wrong permissions, Analysis Cockpit tries to handle these situations in the appropriate way. If the Analysis cockpit had read access but no rights to write/delete/rotate/rename the file, the file gets blacklisted in memory and will not be imported as long as the service doesn't get restarted. A restart of the service would cause the service to re-index the log data placed in that folder.

Important: We highly recommend not to directly copy (`scp`, `rsync`) files into that folder, but use a staging folder in which you set the right permissions and then copy the files to the import folder.

Copying files directly to that folder has many problematic side effects, e.g. files partly composed of binary zeros because the file transfer is still in progress.

4.10 Connect to ASGARD Management Center

In order to receive log data from ASGARD Management Center systems, add them in the corresponding section in the system settings.

Settings > Link Products > Management Center

After you have connected the two components, all assets along with additional information from ASGARD will show up in the **Assets** section of your Analysis Cockpit.

4.11 Asset View

In most cases working with the **Baselining** section and the **Cases** section can be seen as the best practice approach for setting baselines and dealing with alerts and warnings.

However, in some cases it makes sense to change perspective and rather go for a host centric approach. The Analysis Cockpit will calculate numbers of lines in different case types (Incident, Suspicious, Anomaly, etc.) on a per host basis for a given time frame. Along with information from ASGARD on last scan dates, labels, host availability etc. this gives an entirely different perspective.

By using the "Asset View" you can e.g., easily answer questions like:

- Which systems appear most often in "Incident" cases?
- Which systems haven't reported a single event for more than a month?
- Which Domain Controllers have not been scanned yet?

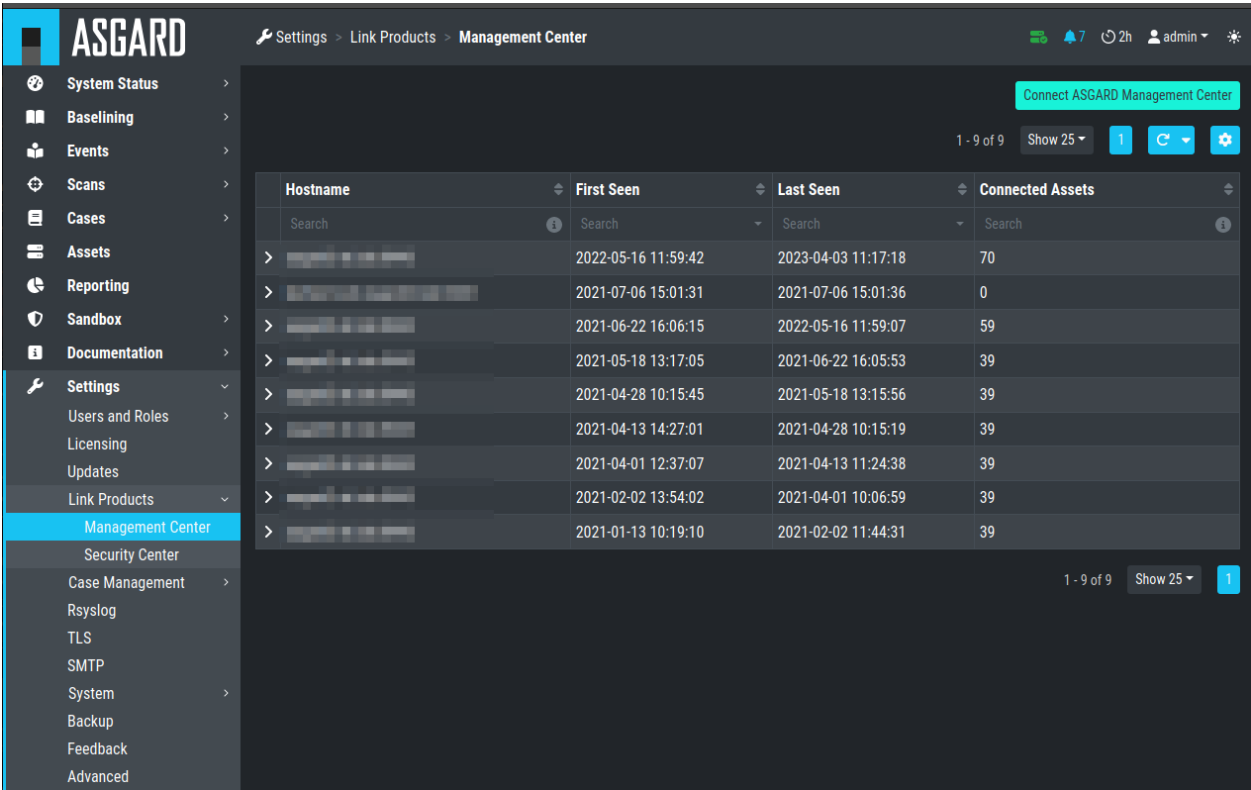


Fig. 16: Link ASGARD Management Center

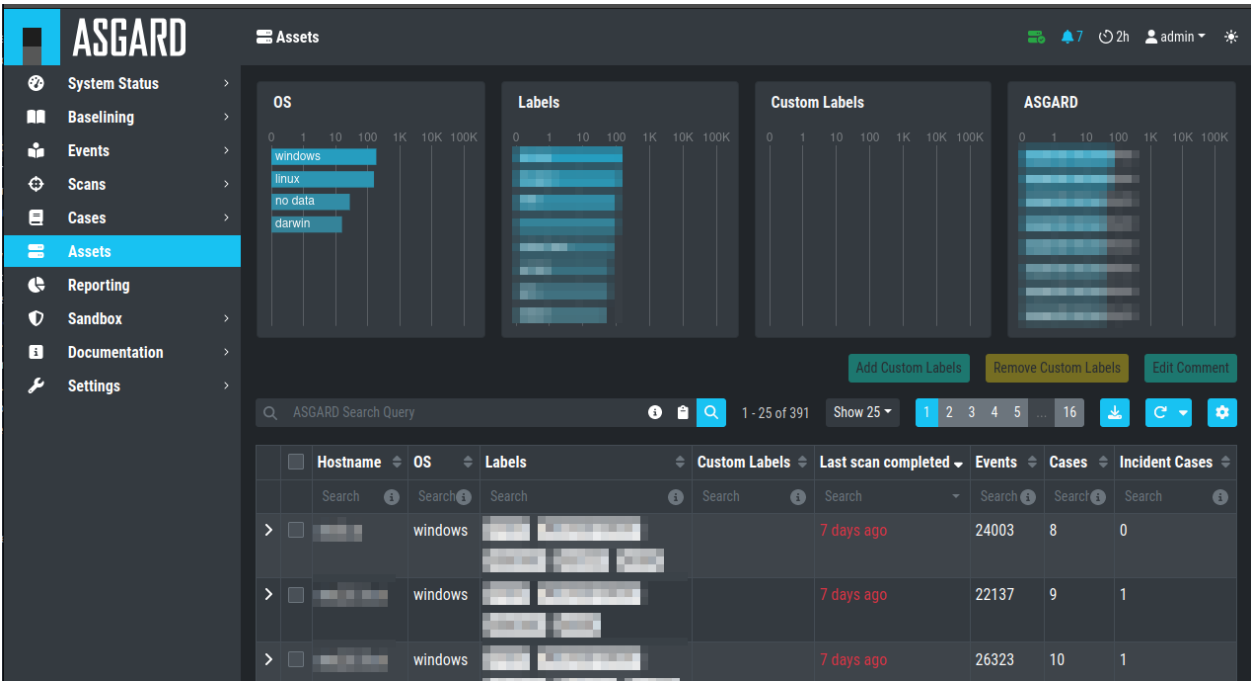


Fig. 17: Asset View after a Successful Connection

- Which systems with IP addresses starting "192.168." appear in "Incident" cases?

In combination with the ASGARD Query and Labels, which are identical to your ASGARD, you can even narrow down the events by system group (e.g., Domain Controllers, or certain locations).

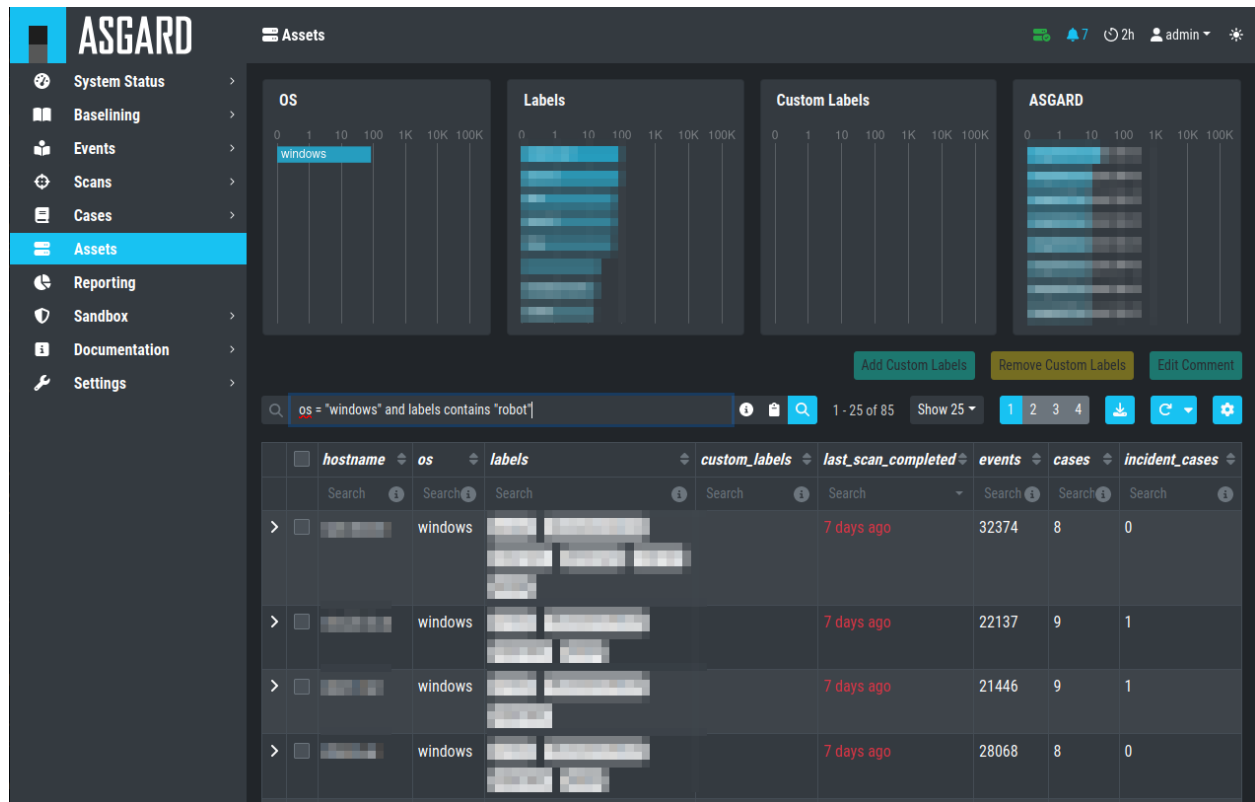


Fig. 18: Filtering within the Assets view

4.12 Sandbox Integration

You can configure your Analysis Cockpit to upload files to a local sandbox. Currently you can use [CAPEv2](#) (recommended) or [Cuckoo](#).

Additionally, you can look at the following `python` file and write your own connector, for a different sandbox, if you need to: `/etc/nextron/analysiscockpit3/sandbox/connector/capev2.py`

Note: This section only focuses on the integration of your Analysis Cockpit with an existing sandbox. We will not cover how to set up the sandbox.

4.12.1 Analysis Cockpit Sandbox Configuration

In the web view of your Analysis Cockpit, navigate to Sandbox > Sandboxes. Click Add Sandbox in the top right corner. Keep the Name short and add a proper Description.

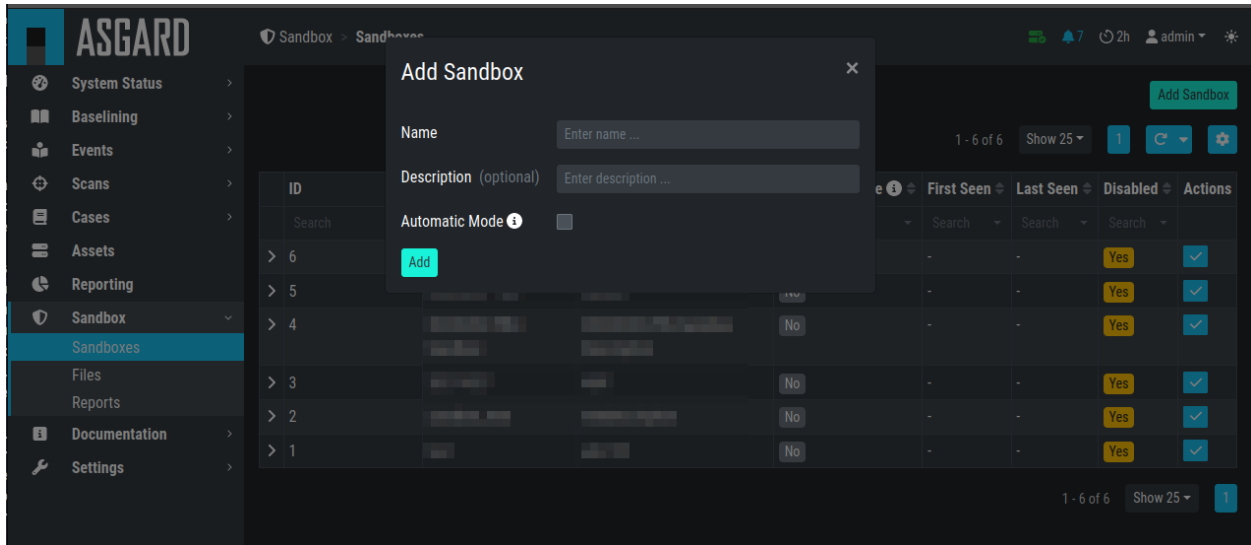


Fig. 19: Adding a new Sandbox

Once you click Add the page will display an API token. Copy this token, we will need it later.

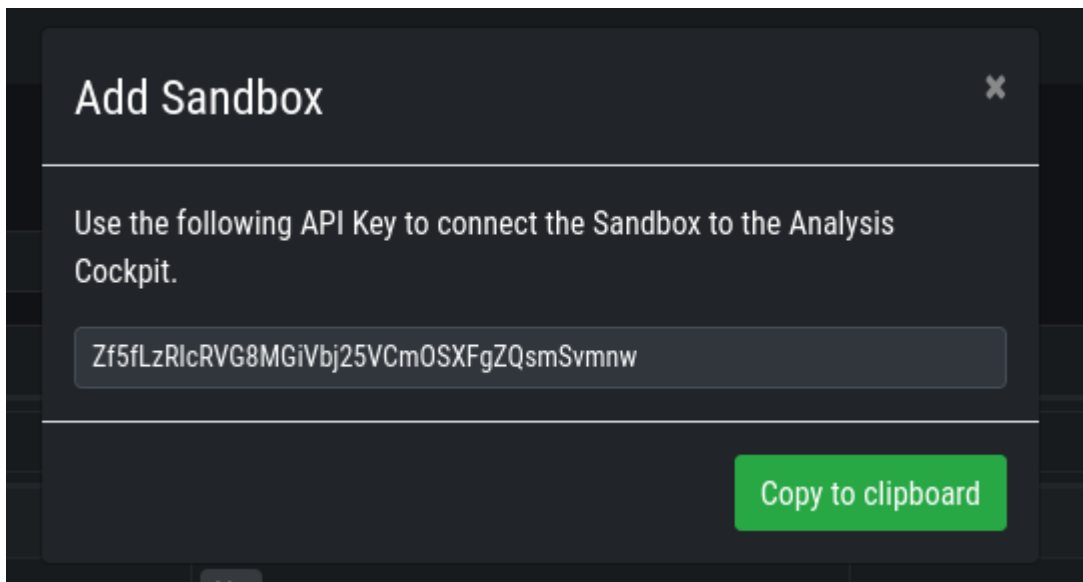


Fig. 20: Sandbox API Token

Connect to your Analysis Cockpit via SSH and follow the steps below.

Change the user to the root user:

```
nextron@cockpit:~$ sudo su -
[sudo] password for nextron:
```

(continues on next page)

(continued from previous page)

```
root@cockpit:~#
```

We change into the configuration directory of the sandbox:

```
root@cockpit:~# cd /etc/nextron/analysiscockpit3/sandbox/connector
root@cockpit:/etc/nextron/analysiscockpit3/sandbox/connector#
```

Here you can find multiple files and folders. The .py and .ini files represent each the type of sandbox you want to integrate. In this example, we will configure the CAPv2 sandbox with our Analysis Cockpit.

```
root@cockpit:/etc/nextron/analysiscockpit3/sandbox/connector# ls -lA
total 36
drwxr-xr-x 2 analysiscockpit3 analysiscockpit3 4096 Apr 21 15:27 analysiscockpit
-rw-r--r-- 1 analysiscockpit3 analysiscockpit3 253 Mär 3 11:20 capev2.ini
-rw-r--r-- 1 analysiscockpit3 analysiscockpit3 4934 Mär 3 11:20 capev2.py
-rw-r--r-- 1 analysiscockpit3 analysiscockpit3 278 Mär 28 2021 cuckoo.ini
-rw-r--r-- 1 analysiscockpit3 analysiscockpit3 9867 Nov 17 2020 cuckoo.py
drwxr-xr-x 2 analysiscockpit3 analysiscockpit3 4096 Apr 14 15:29 sandboxapi
```

Here we have two files which are of relevance for us:

- capev2.ini
 - This holds the configuration for both the sandbox and your Analysis Cockpit
- capev2.py
 - This has the systemd configuration to create the actual service on the system (we don't change anything in here)

Change the capev2.ini with a text editor. The important lines, which need to be changed accordingly to your environment, are marked:

```
root@cockpit:/etc/nextron/analysiscockpit3/sandbox/connector# nano capev2.ini
```

```
1 [DEFAULT]
2 debug = yes
3 tmp_directory = /var/lib/nextron/analysiscockpit3/sandbox/capev2
4
5 [capev2]
6 protocol = http
7 host = 192.168.0.50
8 port = 8000
9 token = <your CAPEv2 API token here>
10 verify = no
11 all = yes
12 html = yes
13
14 [analysis-cockpit]
15 host = localhost:443
16 apikey = <your API Key here>
17 verify = no
```

For lines 6-10, please fill the information accordingly. host is the IP/FQDN of your sandbox. port is the listening port of the web interface of your sandbox. token is the API token generated in the user management of your sandbox.

verify is for verification of the TLS certificate (if you don't use TLS or don't want to verify the certificate, set this option to no).

For lines 16-17 you have to set the apikey of your Analysis Cockpit (see "Add Sandbox" step in the beginning of this section) and verify, which can be set to no; this will verify the TLS certificate.

Save your files after you made your changes.

Now you have to create a new directory and give the analysiscockpit3 user permission:

```
root@cockpit:/etc/nextron/analysiscockpit3/sandbox/connector# mkdir -p /var/lib/nextron/
↳ analysiscockpit3/sandbox/capev2
root@cockpit:/etc/nextron/analysiscockpit3/sandbox/connector# chown -R analysiscockpit3:
↳ /var/lib/nextron/analysiscockpit3
```

We need to create a systemd service file in order to run the CAPEv2 connector on your Analysis Cockpit. Below you can find a predefined service file which we will use:

```
1 [Unit]
2 Description=CAPEv2 Sandbox Connector
3 After=network.target
4
5 [Service]
6 ExecStart=/usr/bin/python3 /etc/nextron/analysiscockpit3/sandbox/connector/capev2.py
7 Restart=on-failure
8 User=analysiscockpit3
9 Group=analysiscockpit3
10 SyslogIdentifier=capev2_connector
11
12 [Install]
13 WantedBy=multi-user.target
```

Now we run the following command and paste the content from the output earlier into it:

```
root@cockpit:/etc/nextron/analysiscockpit3/sandbox/connector# nano /lib/systemd/system/
↳ capev2-connector.service
```

The file should now look like this:

```
root@cockpit:/etc/nextron/analysiscockpit3/sandbox/connector# cat /lib/systemd/system/
↳ capev2-connector.service
[Unit]
Description=CAPEv2 Sandbox Connector
After=network.target

[Service]
ExecStart=/usr/bin/python3 /etc/nextron/analysiscockpit3/sandbox/connector/capev2.py
Restart=on-failure
User=analysiscockpit3
Group=analysiscockpit3
SyslogIdentifier=capev2_connector

[Install]
WantedBy=multi-user.target

root@cockpit:/etc/nextron/analysiscockpit3/sandbox/connector#
```

Now that the systemd service file is created, we need to activate it. Run the following command:

```
root@cockpit:/etc/nextron/analysiscockpit3/sandbox/connector# systemctl daemon-reload &&
↳ systemctl enable capev2-connector && systemctl start capev2-connector
Created symlink /etc/systemd/system/multi-user.target.wants/capev2-connector.service → /
↳ lib/systemd/system/capev2-connector.service.
root@cockpit:/etc/nextron/analysiscockpit3/sandbox/connector#
```

The connection to your sandbox should work now. You can see the capev2.log for debug output and troubleshooting:

```
root@cockpit:~# tail /var/lib/nextron/analysiscockpit3/sandbox/capev2/capev2.log
22-11-15 12:07:46 DEBUG: Starting new HTTPS connection (1): localhost:443
22-11-15 12:07:46 DEBUG: https://localhost:443 "GET /api/sandboxes/a/reports/pending?
↳ limit=10&offset=0 HTTP/1.1" 200 13
22-11-15 12:07:46 DEBUG: no pending references found
22-11-15 12:08:46 DEBUG: Starting new HTTP connection (1): 192.168.0.50:8000
22-11-15 12:08:46 DEBUG: http://192.168.0.50:8000 "GET /apiv2/cuckoo/status/ HTTP/1.1"
↳ 200 289
22-11-15 12:08:46 DEBUG: Starting new HTTPS connection (1): localhost:443
22-11-15 12:08:46 DEBUG: https://localhost:443 "GET /api/sandboxes/a/get-sha256s-without-
↳ report?limit=10 HTTP/1.1" 200 13
22-11-15 12:08:46 DEBUG: Starting new HTTPS connection (1): localhost:443
22-11-15 12:08:46 DEBUG: https://localhost:443 "GET /api/sandboxes/a/reports/pending?
↳ limit=10&offset=0 HTTP/1.1" 200 13
22-11-15 12:08:46 DEBUG: no pending references found
root@cockpit:~#
```

4.12.2 Analysis Cockpit Sandbox Usage

Once your sandbox is set up and running, you can see the status of it in the sandbox view (Last Seen):

ID	Name	Description	Automatic Mode	First Seen	Last Seen	Disabled	Actions
6			No	-	-	Yes	✓
5			No	-	-	Yes	✓
4			No	-	-	Yes	✓
3			No	-	-	Yes	✓
2			No	-	-	Yes	✓
1			No	-	-	Yes	✓

If you wish to enable automatic scanning for uploaded files (Bifrost), you can do so by pressing the play button to the right hand side.

In the Files view you can see previously analyzed files or upload files for analysis by yourself:

SHA256	Name	Description	Size	Type	Received First
04e9a4a330b64e81819d5de6f226019912f372c1262735da42541e7cabdded31	custom-events.template		350 B	(custom upload)	2023-03-07 14:37:18
25d4f2a86deb5e2574bb3210b67bb24fcc4afb19f93a7b65a057daa874a9d18e	11.txt		3 B	(custom upload)	2022-08-30 11:48:29
917df3320d778dbaa5c5c7742bc4046bf803c36ed2b050f30844ed206783469	10.txt		3 B	(custom upload)	2022-07-18 16:21:22
2e6d31a5983a91251bfae5aefa1c0a19d8ba3cf601d0e8a706b4cfa9661a6b8a	9.txt		2 B	(custom upload)	2022-05-16 15:52:01
35ea08f857a5e2c5a131a7149b6cbcb381bc6de067abda8bca92b6da3a5ccd05	(missing)		4 KB	UNKNOWN	2021-01-13 10:19:12
521c38abbbb94536b928e06164a1557de83b7fd688c826f66551eacca7193ae	(missing)		6 B	UNKNOWN	2021-01-13 10:19:12
e2b17c49ee7c7d88550213ade1d4e267b83fea26d55d7f1d9b3a075c98ac1ac9	(missing)		5 KB	UNKNOWN	2021-07-06

Note: If you did not enable auto mode of your configured sandbox, you have to manually add the file for scanning in here. You can do this by pressing the Scan file with sandbox button to the right of your file.

After your file has been uploaded, you have to wait until your sandbox is finished with analyzing the file. Change to the Reports view to see the status of the files.

SHA256	Sandbox Name	Prioritize	Created	Started	Completed	Status	Threat Score	Updated	Download
912018ab3c6b16b39ee84f17745f0c80a33cee241013ec35d0281e40c0658d9	CAPEv2	No	2022-11-15 13:18:47 +01:00	2022-11-15 13:18:48 +01:00	-	PENDING	0	2022-11-15 13:18:48 +01:00	REPORT HTML JSON

Once the file was analyzed and the reports are ready, you will see that the status of the file changed to SUCCESS and the buttons REPORT, JSON and HTML can be clicked.

You can now download the report.

The screenshot shows the ASGARD Analysis Cockpit interface. The left sidebar contains navigation links: Overview, Baselineing, Events, Scans, Cases, Assets, Reporting, Sandbox, Downloads, Licensing, Notifications, API Documentation, Updates, Settings, User Settings, Logout (admin), and Elasticsearch Status. The main content area is titled 'Reports' and shows a table of analysis results. The table has columns for SHA256, Sandbox Name, Prioritize, Created, Started, Completed, Status, Threat Score, Updated, and Download. A single entry is displayed for a SHA256 hash starting with '912018ab3c6b16b39ee84f17745ff0c80a33cee2410'. The Status is 'SUCCESS' and the Threat Score is '3'. The Download column contains links for 'REPORT', 'HTML', and 'JSON', which are highlighted with a red box.

SHA256	Sandbox Name	Prioritize	Created	Started	Completed	Status	Threat Score	Updated	Download
912018ab3c6b16b39ee84f17745ff0c80a33cee2410 13ec35d0281e40c0658d9	CAPEv2	No	2022-11-15 13:18:47 +01:00	2022-11-15 13:18:48 +01:00	2022-11-15 13:23:49 +01:00	SUCCESS	3	2022-11-15 13:23:49 +01:00	REPORT HTML JSON

4.13 API

The API documentation has been integrated into the web interface.

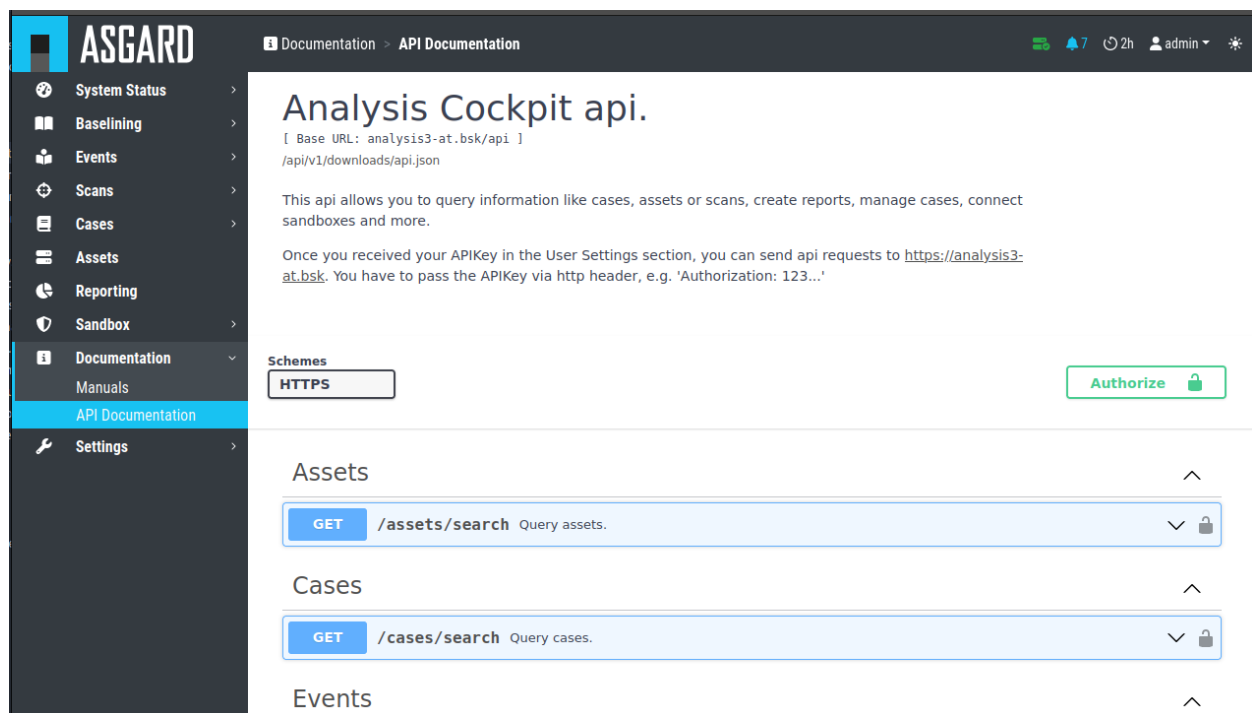


Fig. 21: API Documentation

BASIC CONCEPTS

5.1 Events

All events that have been stored in your Analysis Cockpit – regardless if they are assigned to a particular case or not – are displayed in the section **Events**. This section can be seen as your threat hunting pool. The section provides powerful filtering options. The Events Section is split into the different sources of your Events:

- THOR Events
- Aurora Events
- Log Watcher Events (deprecated)

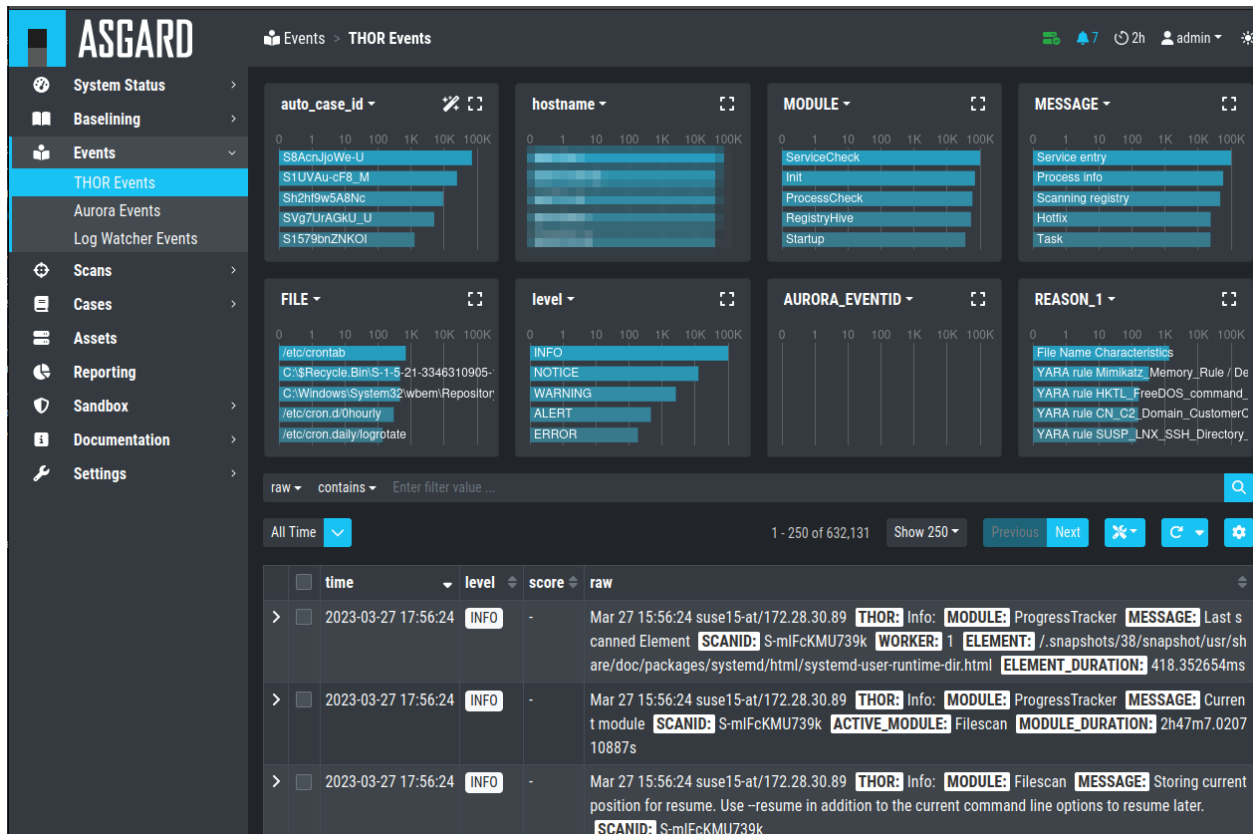


Fig. 1: Events Section

5.2 Baselining

All events that have **not** been assigned to a particular case are displayed in the Baselining section of the Analysis Cockpit.

Again, the Baselining Section is split into the different sources of our events. Additionally, you can see the Suggested Cases, which will suggest cases based on predefined *Case Templates*.

- THOR Events
- Aurora Events
- Log Watcher Events (deprecated)
- Suggested Cases

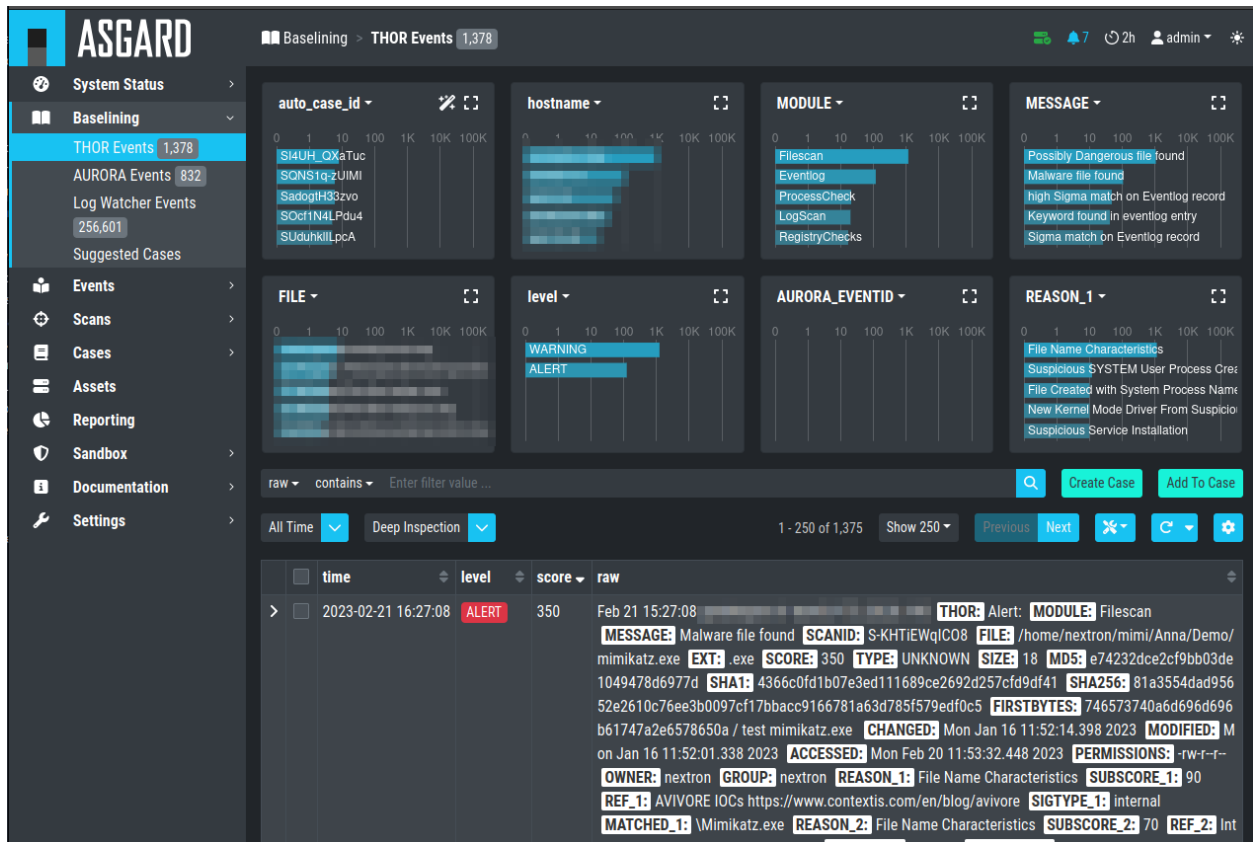


Fig. 2: Baselining Section

Logs that represent the same type of anomaly or incident can be grouped together using the various filters and then be stored in a Case for further analysis. Grouping can be done manually by filtering and clicking **Create Case**, selecting individual Events and clicking **Create Case**, or automatically by simply clicking the **Advanced Tools** button and **Auto Baselining**. With **Auto Baselining**, the Cockpit automatically calculates groups of "similar" log lines.

Once stored in a case, the logs will disappear from the Baselining section.

The Analysis Cockpit can automatically check for events that can be added to existing cases. By clicking the **Optimize** button, the Analysis Cockpit will iterate through all unassigned events and check if there is a matching case.

Note: The optimization will iterate through all unassigned events and assign them to cases if a match were found.

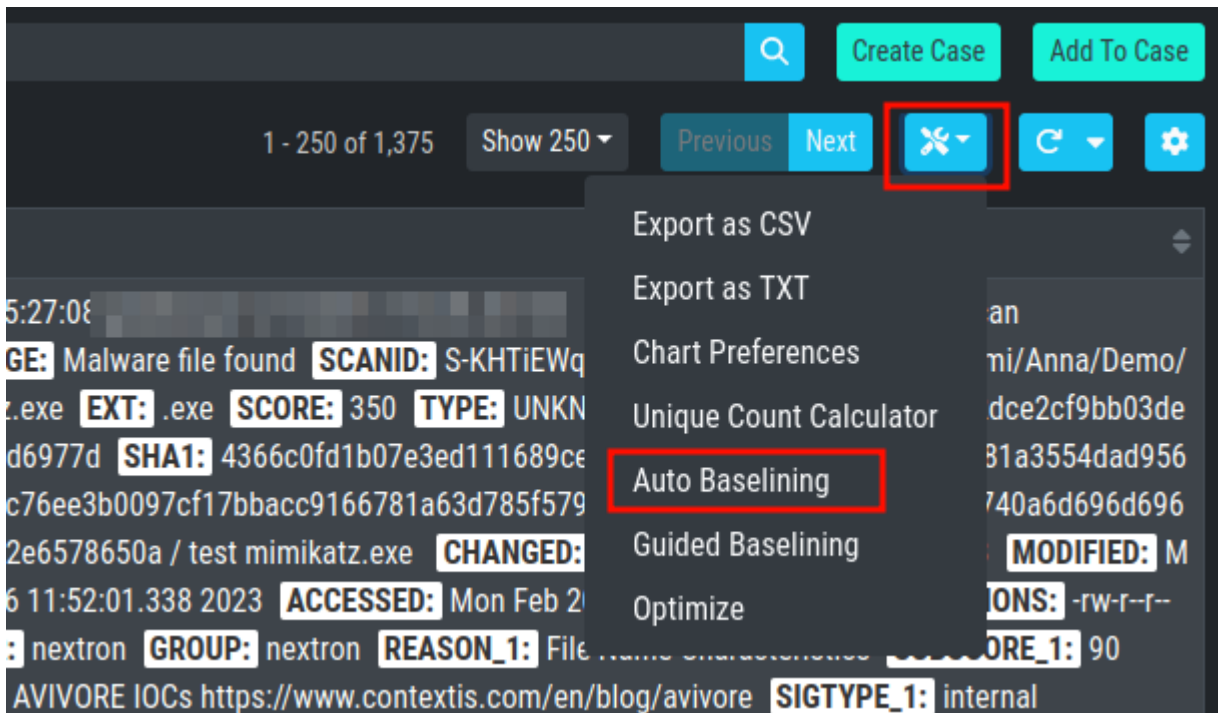


Fig. 3: Auto Baseline

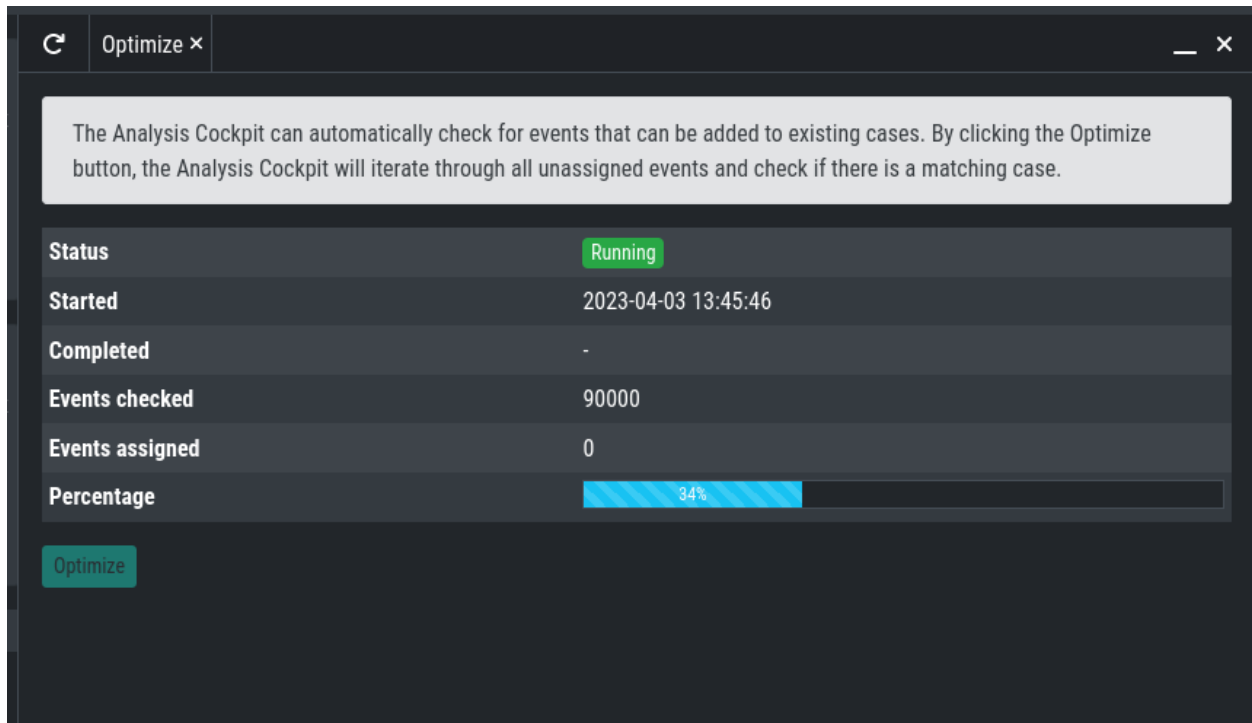


Fig. 4: Optimize Function

This may take a while.

In an ideal organization, the Baselining section should always be empty at the end of a day, as these logs represent suspicious elements that have not yet been looked at.

5.2.1 Baselining Views

In the Baselining section there are two main views, the Compromise Assessment Mode and the Deep Inspection Mode. Additionally, you can find the Custom Signatures Only Mode, which will only show events found by custom signatures. This can be helpful if you scanned your environment with customer signatures, for example during or after an incident.

By default, the Analysis Cockpit Baselining Mode is set to Compromise Assessment.

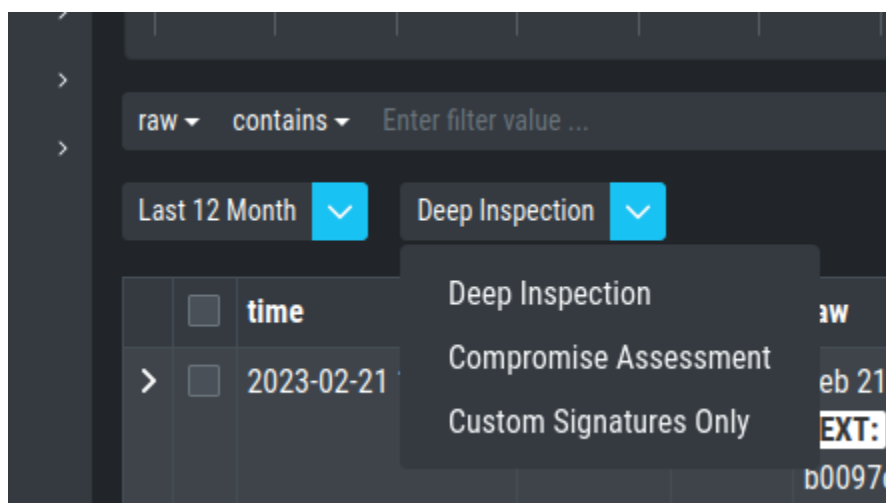


Fig. 5: Select your view

5.2.2 Compromise Assessment Mode

The Compromise Assessment Mode is a new filter/representation of events created and reviewed by our security experts.

It includes our most successful detections. In this context "success" means, that the detection uncovered malicious activity in the wild and at the same time had a low anomaly and false positive rate. Additionally we also consider a detection to be successful that caused little or no false positives or anomalies.

The new view will combine and apply different techniques and filters to all the unclassified events in the Baselining section, providing a reduced set of logs which proved to be relevant from an analyst perspective.

This new "Compromise Assessment Mode" dramatically reduces your baselining effort. In our tests we noticed a decrease of events in the Baselining section of more than 90%. We believe that especially entities that follow our "Continuous Compromise Assessment" approach should switch into this new mode. We've also challenged the new mode with the post exploitation tools and techniques found in the context of HAFNIUM / Exchange exploitations in March 2021 and covered almost every aspect of the attacks in the new view.

Note: In case of an Incident Response, the Deep Inspection Mode is always recommended, since nothing is filtered

here.

5.2.3 Deep Inspection Mode

This view is basically how it used to be (the old default view). It shows all Alerts and Warnings unless they are already part of an existing case.

5.2.4 Custom Signatures Only Mode

The Custom Signatures Only view will only show you events, which:

- Are not part of a case
- Where found by a custom signature

This view can be helpful if you only want to see events found by one of your custom signatures during a THOR scan. This can be helpful if you want to see only those events and nothing else.

5.3 Cases and Log Processing

The Cases section gives a good overview regarding the existing cases and also provides various filtering options. Column visibility can be configured by clicking on the Columns button of this section.

The Cases Section is split into the different sources of your Cases:

- THOR Cases
- Aurora Cases
- Log Watcher Cases (deprecated)

Additionally, you can find more information regarding:

- Grouping Criteria
- Case Changes
- Security Center

When a case is created, the state will be "Open" and the type will be set to "Noteworthy" by default.

The following states can be set (by default):

- Open
- Level 1 Finished
- Level 1 Working
- Level 2 Working
- Closed

It is possible to configure custom states.

The following types can be set:

- Incident
- Suspicious

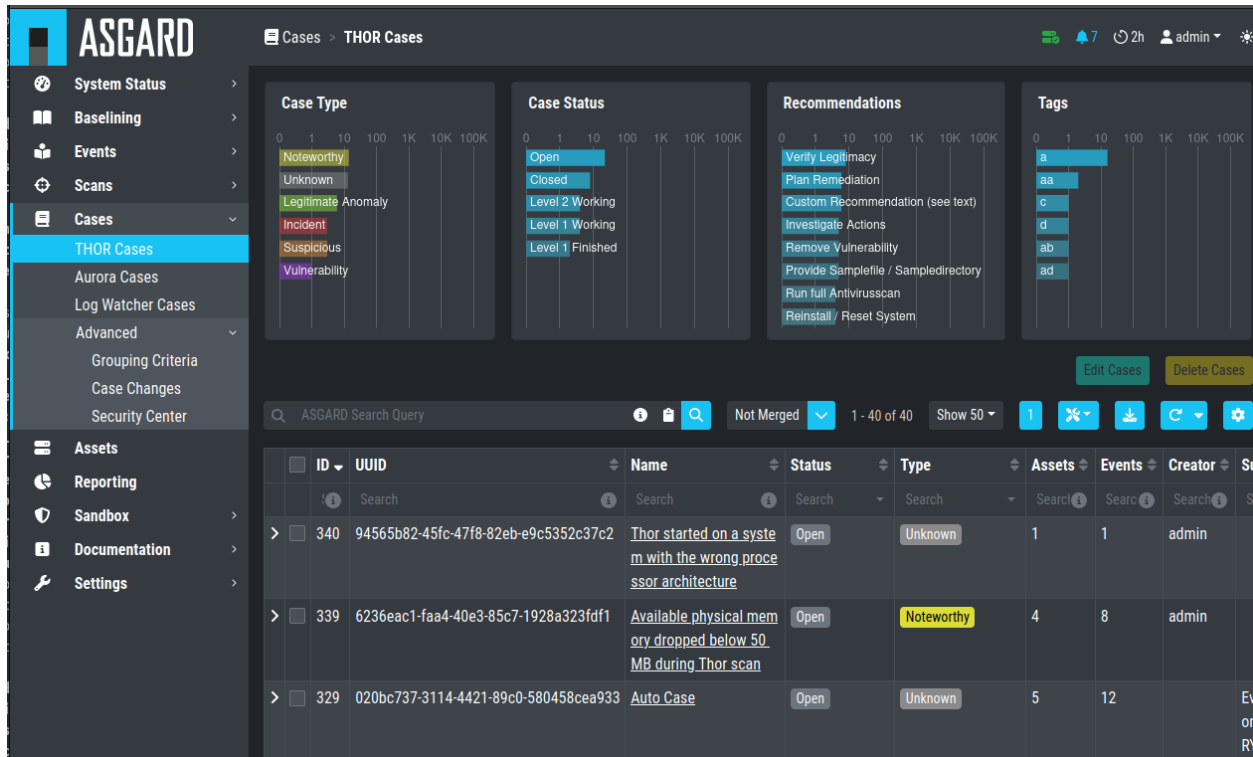


Fig. 6: Cases Section

- Vulnerability
- Noteworthy
- Unknown
- Legitimate Anomaly
- False Positive

See chapter [Glossary](#) for a detailed description of these terms.

Within a case, it is possible to add various information, write a summary, provide canned recommendations or add assessment information.

The log lines contained in the case can of course be analyzed in detail and changes to the case are tracked automatically.

The cockpit will automatically calculate rules (auto_case_id), that make sure, future incoming logs that are similar to the log lines in this particular case are automatically assigned to this case and **will not show up** in the Baselineing section.

Important: Automatically assign newly incoming events to this case needs to be selected during case creation to automatically assign new events to an existing case.

In order to understand this better, let's assume you have decided a group of logs are legitimate anomalies. Then all future logs that are similar to these anomalies will automatically be added to this case and not show up in the Baselineing section.

In case you have decided a group of log lines represent a security incident, the same thing will happen. Future log lines that represent a security incident will show up only in the case and not in the Baselineing section.

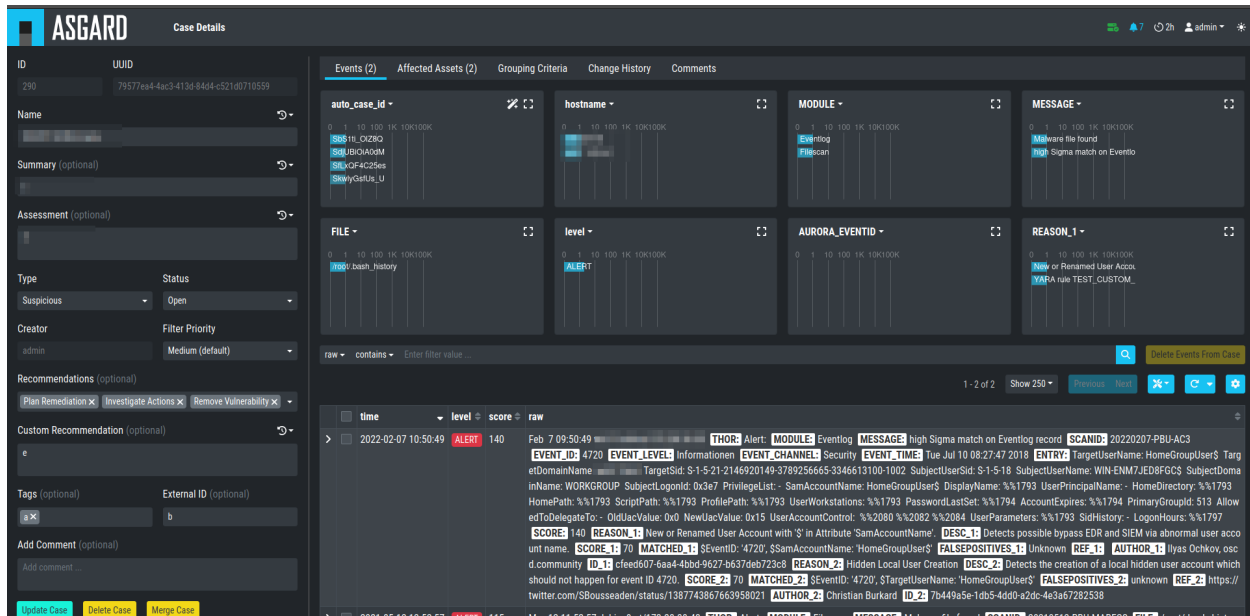


Fig. 7: Case Details

Most organizations want to be alerted in case of a security incident. The Cockpit can be configured to forward all logs that are automatically assigned to an incident case to the organizations' SIEM System via syslog. Organizations that prefer to handle THOR Events entirely within the Analysis Cockpit and not forward anything to a SIEM system may choose to configure a notification that shows up in the Cockpit's Notification Section.

The following picture shows the recommended log processing.

As one can see, an incoming log line only shows up in the Baselining section when it matches no existing case.

This behavior is highly configurable and can be changed in the Settings section of the Analysis Cockpit. One can even decide not to forward anything to a SIEM System or may decide to also forward suspicious elements in addition.

In other Words:

Cases represent the means of setting and maintaining the log baseline within the Cockpit. When you scan your infrastructure once, assign all logs to cases and then scan it for the second time, the Baselining section should be empty if nothing has changed. All incoming logs should be similar to the ones in the first scan and therefore be assigned to the respective cases and not show up in the Baselining section.

Working with cases is explained in detail in the sections below.

5.3.1 Case Templates

Case Templates can be used to suggest new cases in the Suggested Cases section. If there are no Suggested Cases in the view, no events match the Case Templates in your Analysis Cockpit.

To import new Case Templates, you need to create a .yaml file with the conditions first. This can be done by navigating to the Cases view and exporting your search results as Case Templates. You will be able to download a .yaml file from here, which can be used to import as a Case Template.

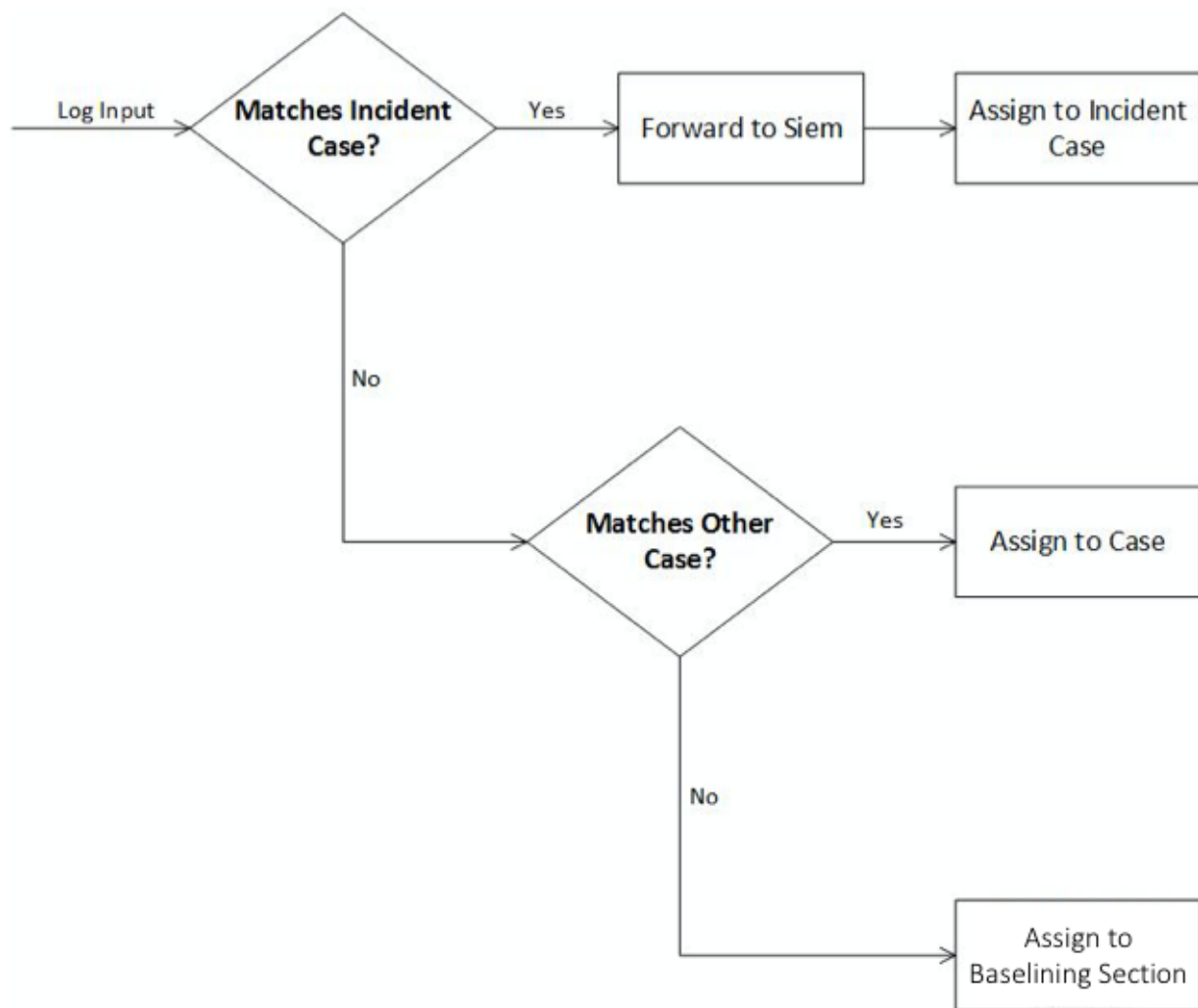


Fig. 8: Log Processing

Name	Type	Summary	Creator	Last Checked
Office Documents with VBA and/or Templates (maybe malicious but also widely used in a legitimate way)	Unknown		Nextron Systems GmbH	2023-04-03 13:17:19
User login on a sunday	Unknown		Nextron Systems GmbH	2023-04-03 13:17:29
Allows local admin group members to login remotely with highest privileges	Unknown		Nextron Systems GmbH	2023-04-03 13:17:39
Remote Control Software: AnyDesk	Unknown		Nextron Systems GmbH	2023-04-03 13:17:49
Network share is freely writable from the outside	Unknown		Nextron Systems GmbH	2023-04-03 13:17:59
Users Download Directories (findings are often related to legitimate downloads)	Unknown		Nextron Systems GmbH	2023-04-03 13:18:09
Web Browser Cache	Unknown		Nextron Systems GmbH	2023-04-03 13:18:19
Remote Control Software: TeamViewer Portable	Unknown		Nextron Systems GmbH	2023-04-03 13:18:29
Hosts File with reference to local IPs / localhost / "0-host" (no resolution)	Unknown		Nextron Systems GmbH	2023-04-03 13:18:40
Process integrity checks are only relevant for Forensics (not activated in default)	Unknown		Nextron Systems GmbH	2023-04-03 13:18:50
Available physical memory dropped below 50 MB during Thor scan	Unknown		Nextron Systems GmbH	2023-04-03 13:19:00
Found executable file in /tmp directory on Linux systems	Unknown		Nextron Systems GmbH	2023-04-03 13:19:10
Service that is not owned by root user (often found when function users for the services are used)	Unknown		Nextron Systems GmbH	2023-04-03 13:19:20
Service configurations that will allow privilege escalation	Unknown		Nextron Systems GmbH	2023-04-03 13:19:30
Burpsuite pentesting software	Unknown		Nextron Systems GmbH	2023-04-03 13:19:50
Detection of Avast software	Unknown		Nextron Systems GmbH	2023-04-03 13:20:00
Found a user named "test"	Unknown		Nextron Systems GmbH	2023-04-03 13:20:10
Folders that contain signatures of various security software	Unknown		Nextron Systems GmbH	2023-04-03 13:20:20
OneNote cache	Unknown		Nextron Systems GmbH	2023-04-03 13:20:30
Exe file in Start Menu / Startup folder (high amount of anomalies)	Unknown		Nextron Systems GmbH	2023-04-03 13:20:40

Fig. 9: Case Templates Overview

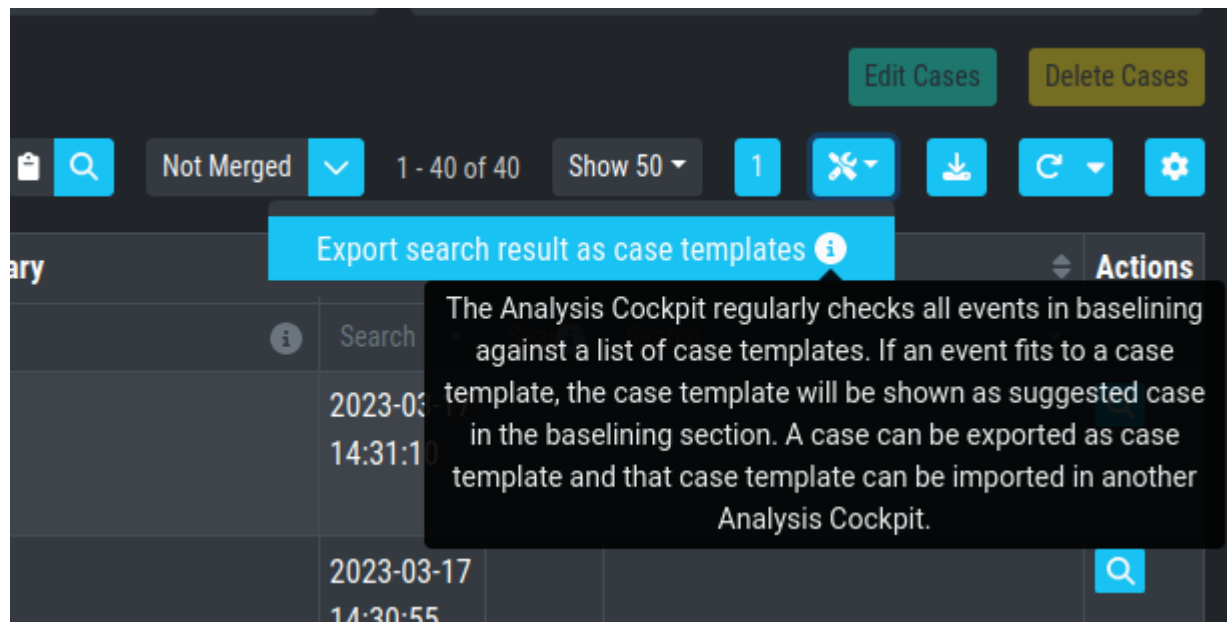


Fig. 10: Exporting Search Results as Case Templates

Listing 1: Exported Case Template

```

1 uuid: 94565b82-45fc-47f8-82eb-e9c5352c37c2
2 name: Thor started on a system with the wrong processor architecture
3 summary: ""
4 type: 5
5 scanner: THOR
6 creator: admin
7 condition: "\"MODULE: Startup\" AND \"MESSAGE: 32 bit THOR was executed on 64 bit
8   system. For improved results, use the 64 bit version of THOR.\"\\r\\n"

```

After you downloaded the Case Templates, you can import them in the Case Templates view.

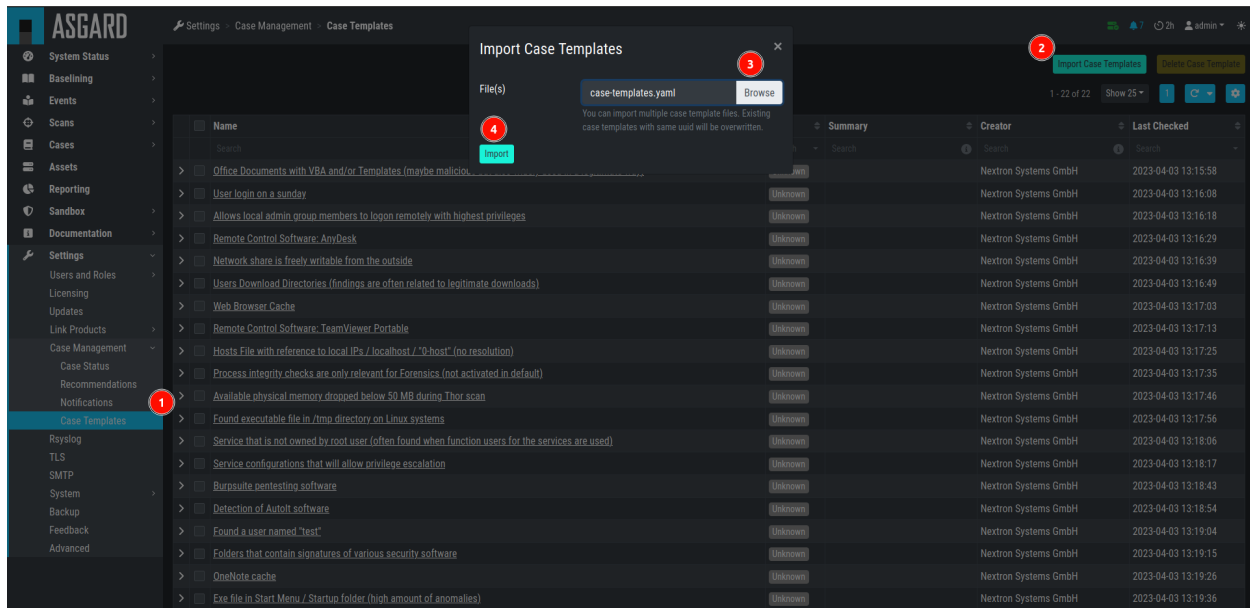


Fig. 11: Import Case Template

You can now inspect the Case Template. You can find it by either looking for the name or filter by who created it. You can see that the conditions match the contents of your exported Case Template (.yaml file).

5.4 Understanding Users, Roles, Rights and Case Status

The rights and roles model within the cockpit is aimed to support large multinational organizations with different independent users working with the case management at the same time. An organization responsible for analyzing THOR logs might be split up in groups of analysts.

Within the cockpit, all users have the right to access the logs and create cases. Within the Case Management section, access rights are granted depending on the particular state the case is in.

In order to setup your rights management you must first decide about the states you want your cases to have, then assign rights for a particular state to a role and after that you add users to that particular role.

In order to understand this better, let's look at an example.

Let's assume we have an organization where a Level 1 analyst group located in Frankfurt is responsible for creating cases and providing an initial assessment for cases, while a Level 2 analyst group located in Hamburg is responsible

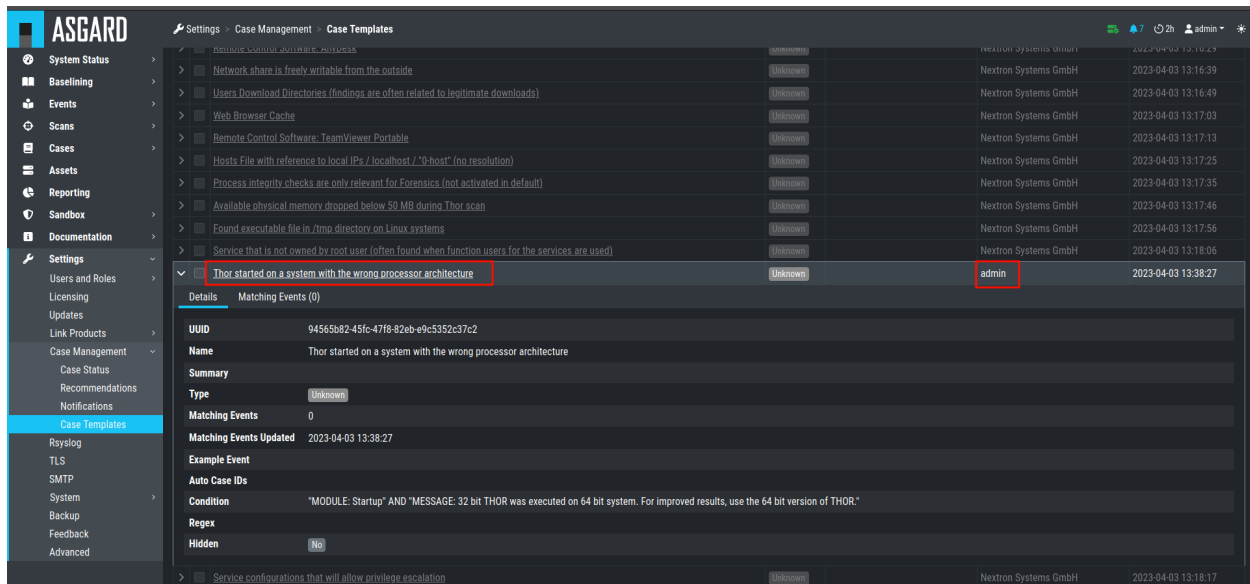


Fig. 12: Inspect Imported Case Template

for reviewing, final decision and closing of cases. In order to support an efficient workflow, you would at least need the following states for your cases:

- Open (nobody is yet working on this case)
- Level 1 Working (Level 1 is working on this case)
- Level 1 Finished (Level 1 has finished and nobody is now working on this case)
- Level 2 Working (Level 2 is working on this case)
- Closed (Case closed)

A workflow could look like this:

For your convenience, we already did the setup for this example and ship all Analysis Cockpit with this workable template by default. You are free to use, modify or delete the corresponding rights, statuses and roles.

However, in order to explain the concepts and the setup of roles and statuses better we assume for a while, we had an empty cockpit with no roles and statuses pre-configured.

In order to set up our pre-configured example, we navigate to the **Settings** section and create the following roles:

Every role can have different rights. We will explain this in detail in the next section. Firstly, we create Level 1 Analyst and Level 2 Analyst without rights at all.

After that we define the following statuses:

In the lower table you can manage the access rights for every role and every Case Status. We can give the suitable rights to our generated roles by clicking the **New Rights for Case Status** button on the right.

For Level 1 Analyst we add the right to read and write all "Open" cases and change the case status to this status (set).

Additionally, we grant Level 1 Analyst the rights to read, write and set all cases for "Level 1 Working".

Finally, we grant the right to read and set cases for the status Level1 Finished. This allows Level 1 Analysts to set a particular case to "Level 1 Finished" and restricts them from modifying this case once they have passed it to this status.

For Level 2 we now add the rights to read and write cases for "Level 1 Finished" and the rights to read, write and set cases for "Level 2 Working". This allows Level 2 analysts to pick cases from the "Level 1 Finished" status and start

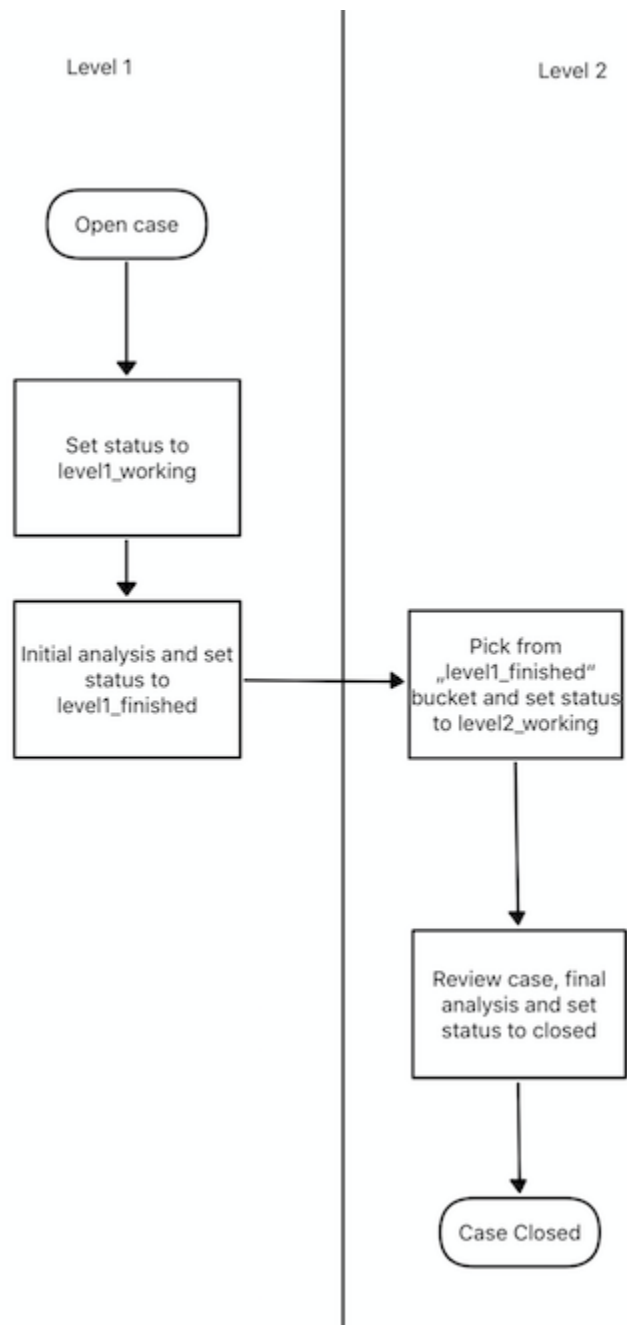


Fig. 13: Workflow open Cases

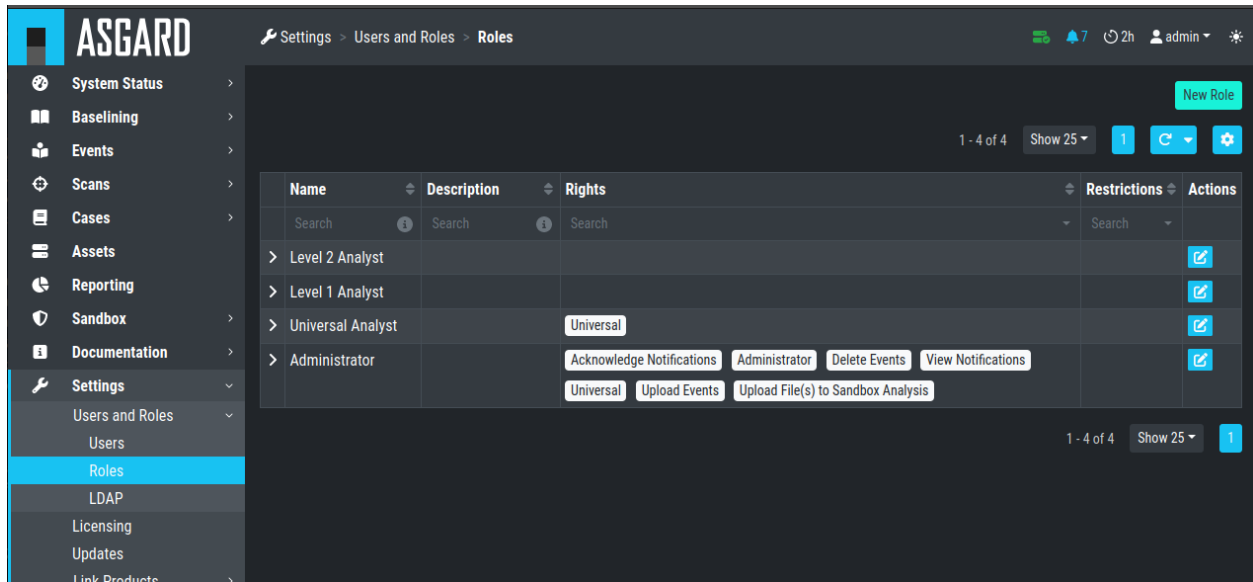


Fig. 14: Settings – adding additional roles

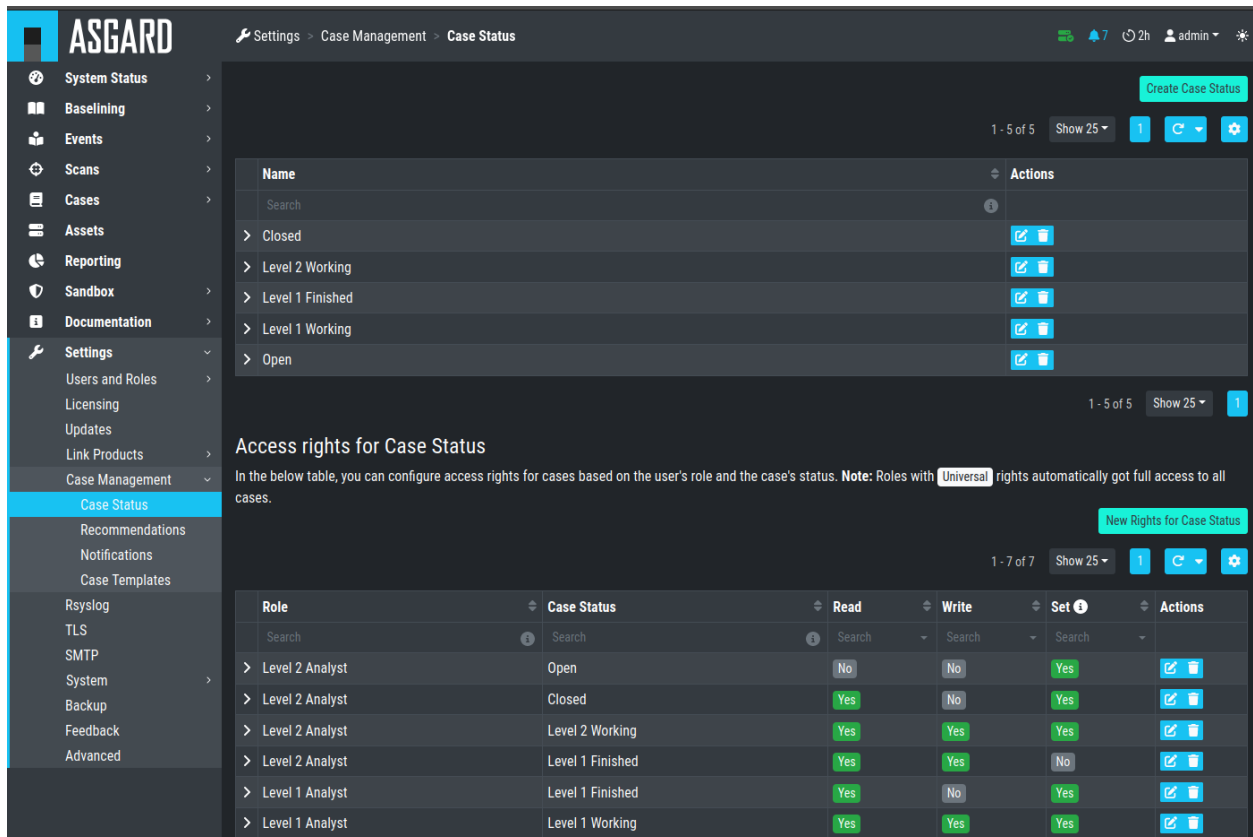


Fig. 15: Settings – Case Status

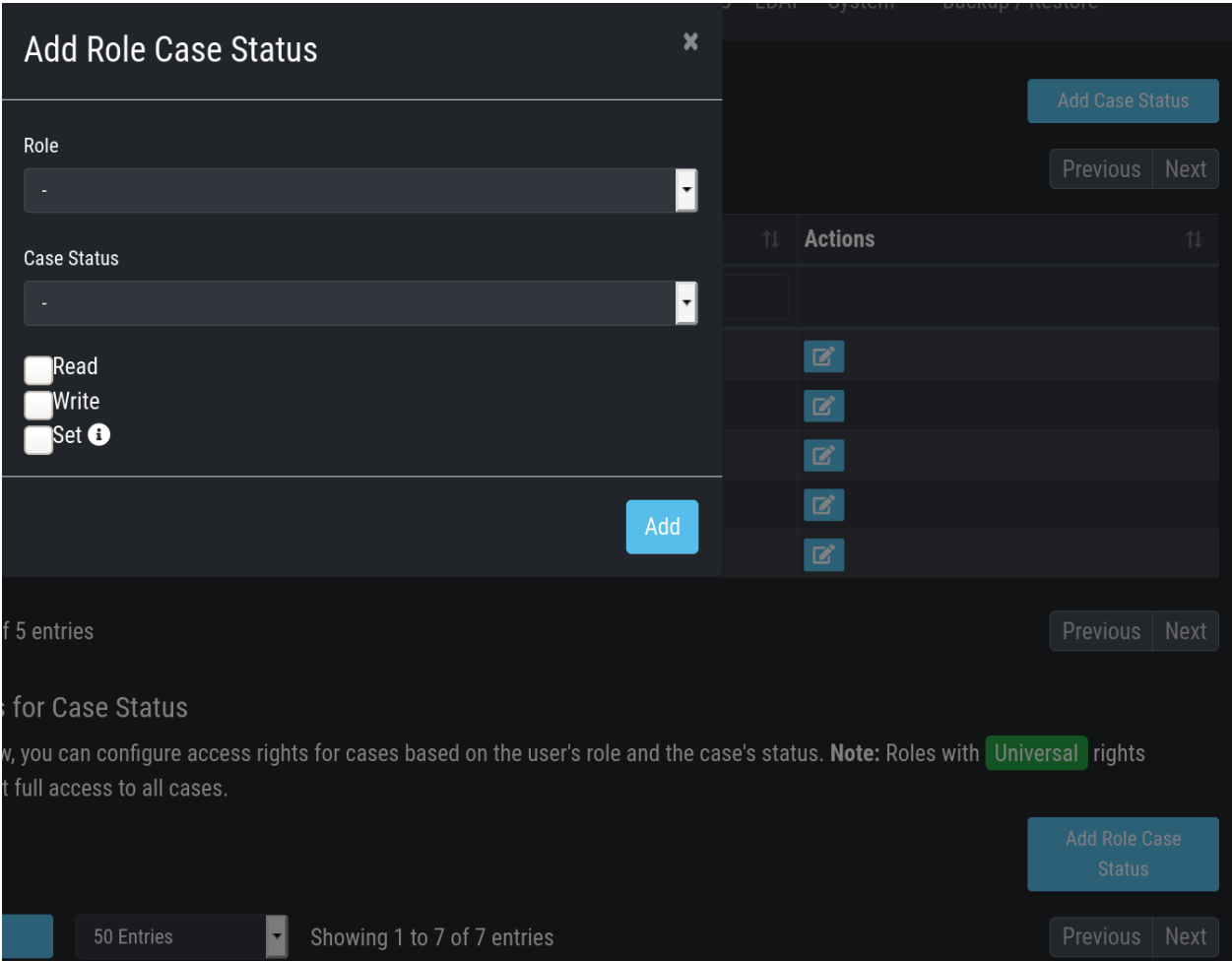


Fig. 16: Edit Rights – Read, Write, Set

working on them.

As we do not want Level 2 Analysts to reopen cases, that have already been closed we only grant them rights to read and set for the status "Closed".

Additionally, we give Level 2 Analyst the right to set the case status to "Open".

After that, the Access rights for Case Status section looks like this:

Access rights for Case Status

In the table below, you can configure access rights for cases based on the user's role and the case's status. **Note:** Roles with **Universal** rights automatically got full access to all cases.

[Add Role Case Status](#)

Columns ▾ 50 Entries ▾ Showing 1 to 7 of 7 entries [Previous](#) [Next](#)

Role Name	Case Status Name	Read	Write	Set ⓘ	Actions
<input type="text" value="Search"/>	<input type="text" value="Search"/>	<input type="text" value="Search"/>	<input type="text" value="Search"/>	<input type="text" value="Search"/>	
Level 1 Analyst	Open	Yes	Yes	Yes	
Level 1 Analyst	Level 1 Working	Yes	Yes	Yes	
Level 1 Analyst	Level 1 Finished	Yes	No	Yes	
Level 2 Analyst	Level 1 Finished	Yes	Yes	No	
Level 2 Analyst	Level 2 Working	Yes	Yes	Yes	
Level 2 Analyst	Closed	Yes	No	Yes	
Level 2 Analyst	Open	No	No	Yes	

Showing 1 to 7 of 7 entries [Previous](#) [Next](#)

Fig. 17: Settings – Access rights for Case Status

Of course, this is only an example. You may of course decide to give Level 2 full access to all cases, and it may also be a good means of training to grant Level 1 Analysts the right to see the "Level 2 Working" and "Closed" cases. You may also want Level 2 Analysts to reopen "Closed" cases or may restrict this right to an additional role. This just illustrates, that the system is highly configurable with an almost infinite number of statuses, roles and rights.

Finally, you simply add users and add them to their particular role.

BASELINING BEST PRACTICES

This section assumes, that you have read the *Basic Concepts*.

All incoming logs, that do not match an existing case, will show up in the Baselineing section.

While importing the logs, the cockpit will already try to find logs are that similar and represent the same type of alert or warning. It will group these logs and assign an `auto_case_id`.

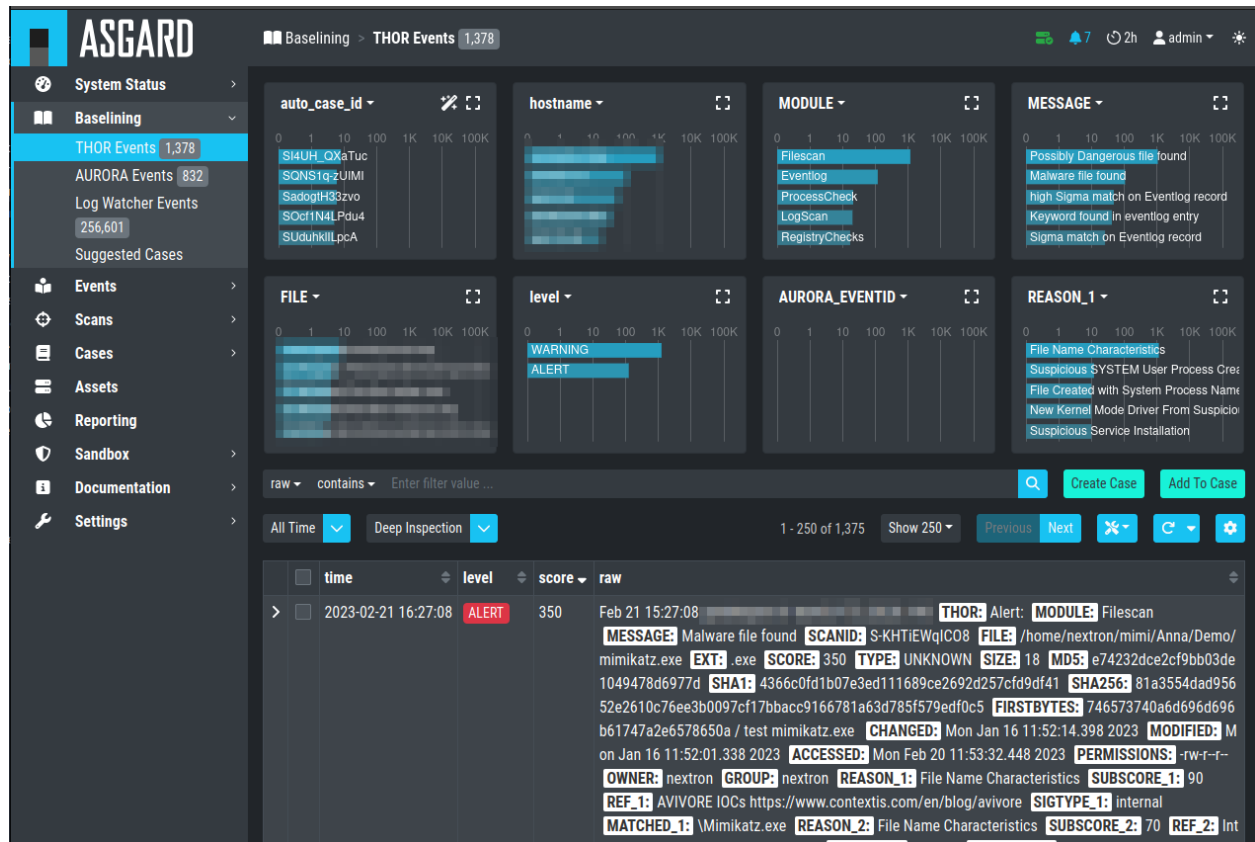
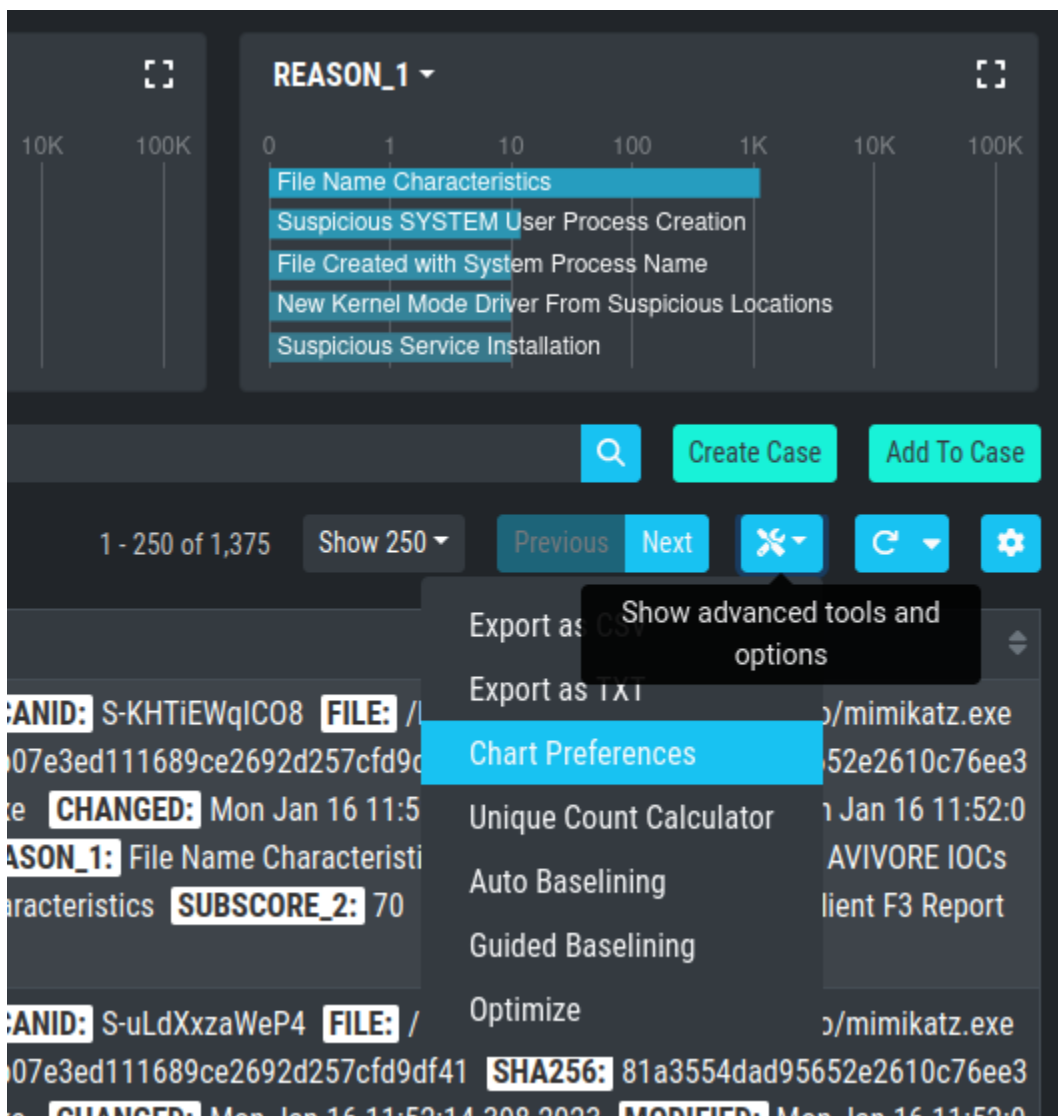


Fig. 1: Baselineing Overview

6.1 Customize Your View

By default, the Analysis Cockpit Baselineing view ships with multiple bar charts and a table with the most relevant columns in order to help you find meaningful groups of logs. You can add additional bar charts by clicking on the Advanced Tools button and selecting Chart Preferences.



You can also modify which bar charts are shown by the name/field-name of the chart and choose the category you want to see. To get more details about a bar chart, you can click on square symbol in the heading of the bar chart.

Click the Columns button to manage which columns are shown.

Hint: All views are personalized and changes will only affect your user.

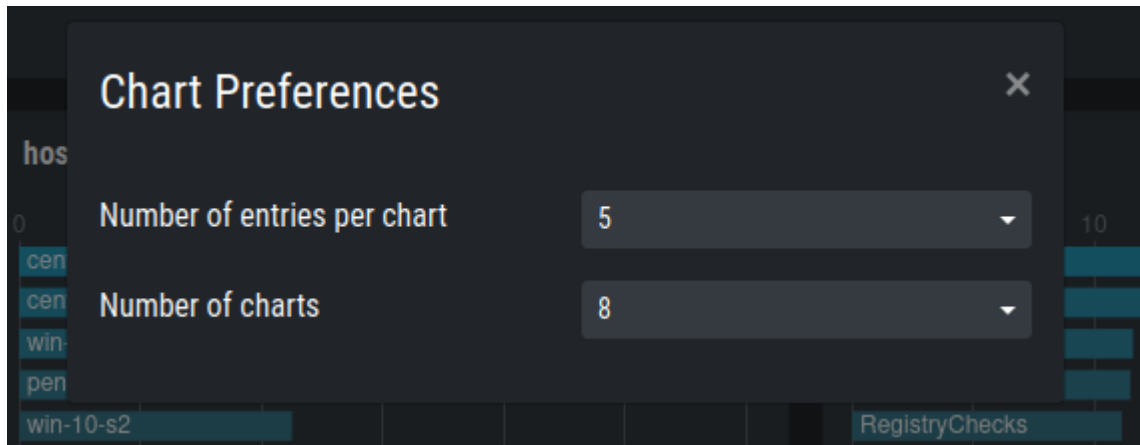


Fig. 2: Chart Preferences

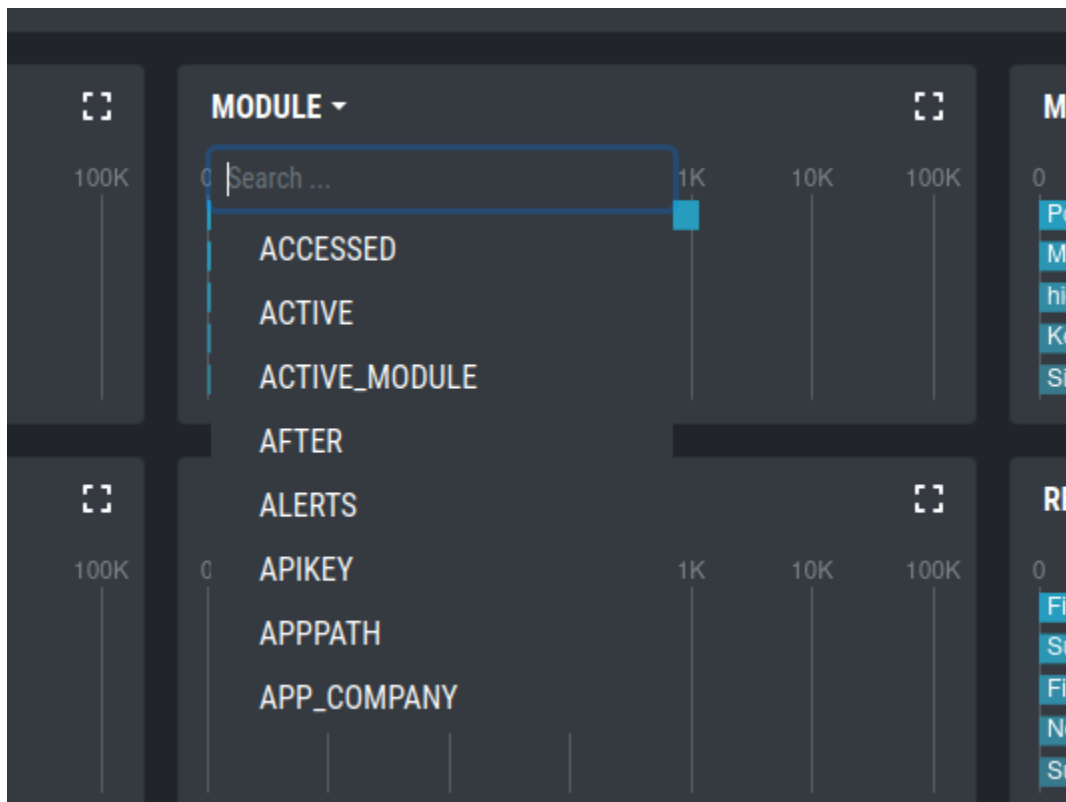


Fig. 3: Bar Chart Selector

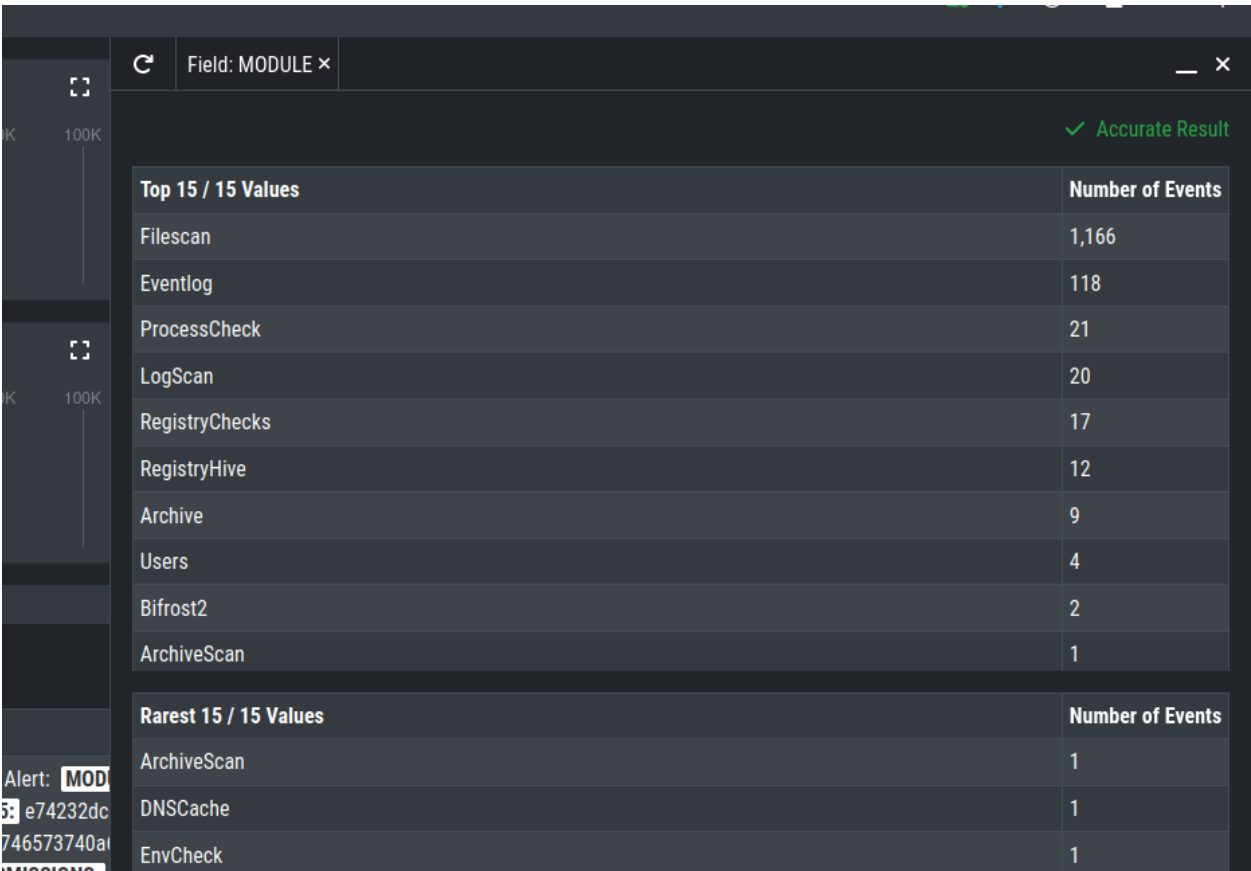


Fig. 4: Bar Chart Details

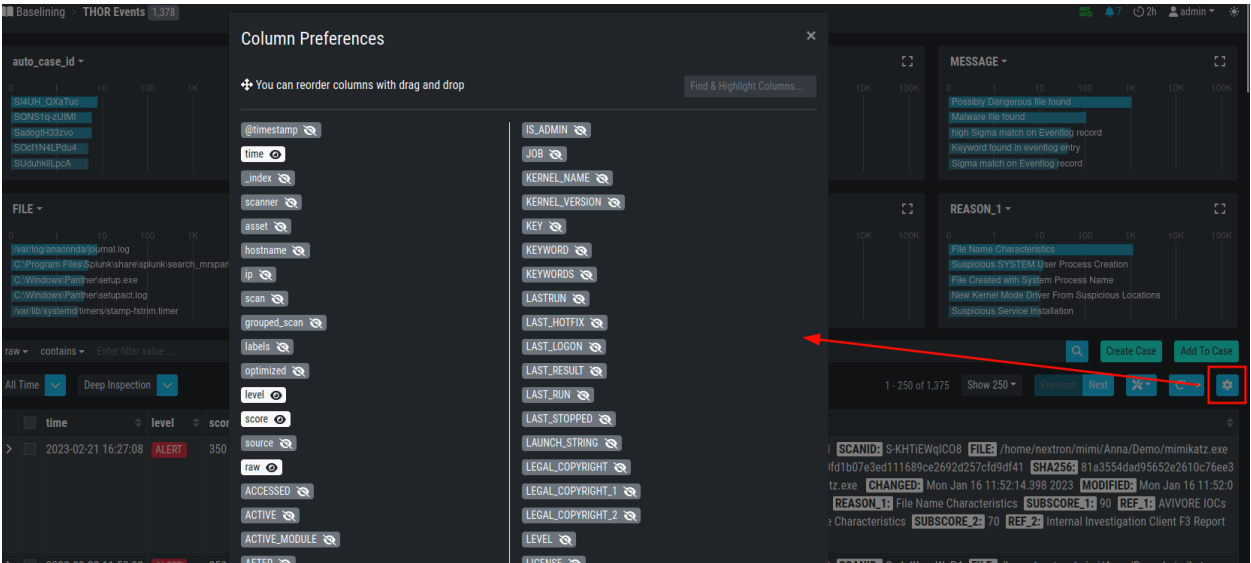


Fig. 5: Column Preferences

6.2 Manual Case Creation

6.2.1 Case Creation Basics

Create a new case following these steps:

1. Select on which conditions the case should be built

2. Inspect the Case Assignment and Conditions. Set Auto Assign if needed.

3. Set a case **name**, which serves as title - use keywords that make it easy for other analysts to find it based on a few terms (e.g. if a false positive was caused by matches in **savedsearch.conf**, use this filename in the title of your case)
4. Select a sample event for the **summary** field
5. Add your **assessment**
6. Choose one or more **recommendations**
7. Select a **case type** (see the [Glossary](#) for a detailed description of every case type)
8. Select a **case status** (usually used to mark it as 'work in progress' or to forward it to the next team)
9. Submit case by clicking the **Create Case** button

Create Case

Events (2) Case Assignment Case Details

Example Events (2 of 2)

Feb 21 15:27:08 gatekeeper-s1-test01/172.28.28.143 **THOR:** Alert: **MODULE:** Filescan **MESSAGE:** Malware file found **SCANID:** S-KHTiEWqIC08 **FILE:** /home/nextron/mimi/Anna/Demo/mimikatz.exe **EXT:** exe **SCORE:** 350 **TYPE:** UNKNOWN **SIZE:** 18 **MD5:** e74232dce2cf9bb03de1049478d6977d **SHA1:** 4366c0fd1b07e3ed111689ce2692d257cfd9df41 **SHA256:** 81a3554dad95652e2610c76ee3b0097cf17bbacc9166781a63d785f579edf0c5 **FIRSTBYTES:** 746573740a6d696d696b61747a2e6578650a / test mimikatz.exe **CHANGED:** Mon Jan 16 11:52:14.398 2023 **MODIFIED:** Mon Jan 16 11:52:01.338 2023 **ACCESSED:** Mon Feb 20 11:53:32.448 2023 **PERMISSIONS:** -rw-r--r-- **OWNER:** nextron **GROUP:** nextron **REASON_1:** File Name Characteristics **SUBSCORE_1:** 90 **REF_1:** AVIVORE IOCs https://www.contextis.com/en/blog/avivore **SIGTYPE_1:** internal **MATCHED_1:** \Mimikatz.exe **REASON_2:** File Name Characteristics **SUBSCORE_2:** 70 **REF_2:** Internal Investigation Client F3 Report **SIGTYPE_2:** internal **MATCHED_2:** \mimikatz.exe

Feb 20 10:53:32 gatekeeper-s1-test01/172.28.28.143 **THOR:** Alert: **MODULE:** Filescan **MESSAGE:** Malware file found **SCANID:** S-uLdXrzaWeP4 **FILE:** /home/nextron/mimi/Anna/Demo/mimikatz.exe

Name: Mimikatz.exe found on endpoint

Summary (optional): Filescan Malware file found FILE: /home/nextron/mimi/Anna/Demo/mimikatz.exe

Assessment (optional): mimikatz.exe was found on endpoints, further inspection is needed.

Type: Suspicious Status: Open

Recommendations (optional): Run full Antivirus scan x Investigate Actions x

Custom Recommendation (optional): Enter custom recommendation ...

Tags (optional): Enter tags ...

External ID (optional): Enter external ID ...

Add Comment (optional): Add comment ...

Create Case

6.2.2 Select Log Messages for a Case

In order to create a meaningful case, you typically start with selecting logs or groups of logs that you want to be contained in the case. This can be done in various ways:

- by adding a custom filter in the search bar
- by clicking on one of the bars in the bar chart
- by clicking on the filter symbol in a field in a log line
- by using the Lucene Search Query

You can generate a filter condition using an expression in the search field, choosing a category, deciding whether the expression should be contained, equal etc. and clicking the search button. Clicking on one of the bars in the bar chart or on the filter symbol in a field in a log line will generate a filter condition, too.

FILE contains Enter filter value ...

All Time Deep Inspection FILE contains mimikatz.exe

time level score raw

Fig. 6: Active Filters

Hint: Filters can be negated by clicking on the two arrows symbol or delete it by clicking on the cross symbol.

Using the built-in custom filters is the most common and easiest way to select groups of logs.

For those who prefer Lucene, an additional Lucene search bar can be activated and can even be combined with the built-in custom search.

In order to activate the Lucene Query search just click the contains button and choose Lucene Query.

The screenshot displays the ASGARD Analysis Cockpit interface. At the top, there are four filter panels: FILE, level, AURORA_EVENTID, and REASON_1. The FILE panel shows a list of files, including '/home/nextron/mimi/Anna/Demo/mimikatz.exe'. The level panel shows a bar chart with 'ALERT' highlighted. The AURORA_EVENTID and REASON_1 panels show bar charts with 'File Name Characteristics' highlighted. Below the filter panels is a search bar with the text 'FILE:*mimikatz*'. To the right of the search bar are buttons for 'Create Case' and 'Add To Case'. Below the search bar is a table with columns for 'time', 'level', 'score', and 'raw'. The table contains two rows of log data. The first row is from Feb 21 15:27:08 and the second row is from Feb 20 10:53:32. Both rows are marked as 'ALERT' and have a score of 350. The raw data for each row is a detailed file scan report for 'mimikatz.exe'.

Fig. 7: Lucene Query

Note: You can Alt/Shift click items in the top field view to add them as a NOT filter to your search.

6.2.3 Case Creation from Search Results

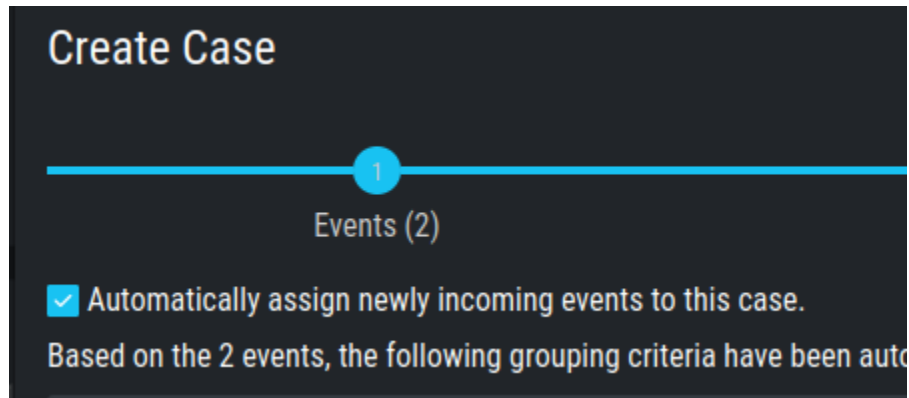
This is the most relevant way to create a case. Create the filters, so that you only see the logs you want to be contained in your case. Then click the **Create Case** button, select **Search results** and add a name, that makes sense to you.

If you want future incoming logs with the same log lines automatically assigned to this case, you have to tick the checkbox **Automatically assign newly incoming events to this case..**

You may add a summary to your case.

You may or may not add assessment, case type, recommendations or a comment. After closing you will find the log section empty, as it is still using your filter, but the matching log lines have been removed from this section and added to the case.

Simply remove the filter and the remaining log lines will show up.



Create Case

1

2

3

Events (2)Case AssignmentCase Details

BackNext

Example Events (2 of 2)

Feb 21 15:27:08 gatekeeper-s1-test01/172.28.28.143 THOR: Alert: MODULE: Filescan MESSAGE: Malware file found SCANID: S-KHTiEWqlC08 FILE: /home/nextron/mimi/Anna/Demo/mimikatz.exe EXT: .exe SCORE: 350 TYPE: UNKNOWN SIZE: 18 MD5: e74232dce2cf9bb03de1049478d6977d SHA1: 4366c0fd1b07e3ed111689ce2692d257cfd9df41 SHA256: 81a3554dad95652e2610c76ee3b0097cf17bbacc9166781a63d785f579edf0c5 FIRSTBYTES: 746573740a6d696d696b61747a2e6578650a / test mimikatz.exe CHANGED: Mon Jan 16 11:52:14.398 2023 MODIFIED: Mon Jan 16 11:52:01.338 2023 ACCESSED: Mon Feb 20 11:53:32.448 2023 PERMISSIONS: -rw-r--r-- OWNER: nextron GROUP: nextron REASON_1: File Name Characteristics SUBSCORE_1: 90 REF_1: AVIVORE IOCs https://www.contextis.com/en/blog/avivore SIGTYPE_1: Internal MATCHED_1: \Mimikatz.exe REASON_2: File Name Characteristics SUBSCORE_2: 70 REF_2: Internal Investigation Client F3 Report SIGTYPE_2: Internal MATCHED_2: \mimikatz.exe

Feb 20 10:53:32 gatekeeper-s1-test01/172.28.28.143 THOR: Alert: MODULE: Filescan MESSAGE: Malware file found SCANID: S-uLdXxaWeP4 FILE: /home/nextron/mimi/Anna/Demo/mimikatz.exe

Name

mimikatz.exe found on endpoint

Recommendations (optional)

Select recommendations ...

Summary (optional)

Filescan Malware file found FILE: /home/nextron/mimi/Anna/Demo/mimikatz.exe

Custom Recommendation (optional)

Enter custom recommendation ...

Assessment (optional)

Enter assessment ...

Tags (optional)

Enter tags ...

External ID (optional)

Enter external ID ...

Type

Noteworthy

Status

Open

Add Comment (optional)

Add comment ...

Create Case

Fig. 8: Baselining – Create Case

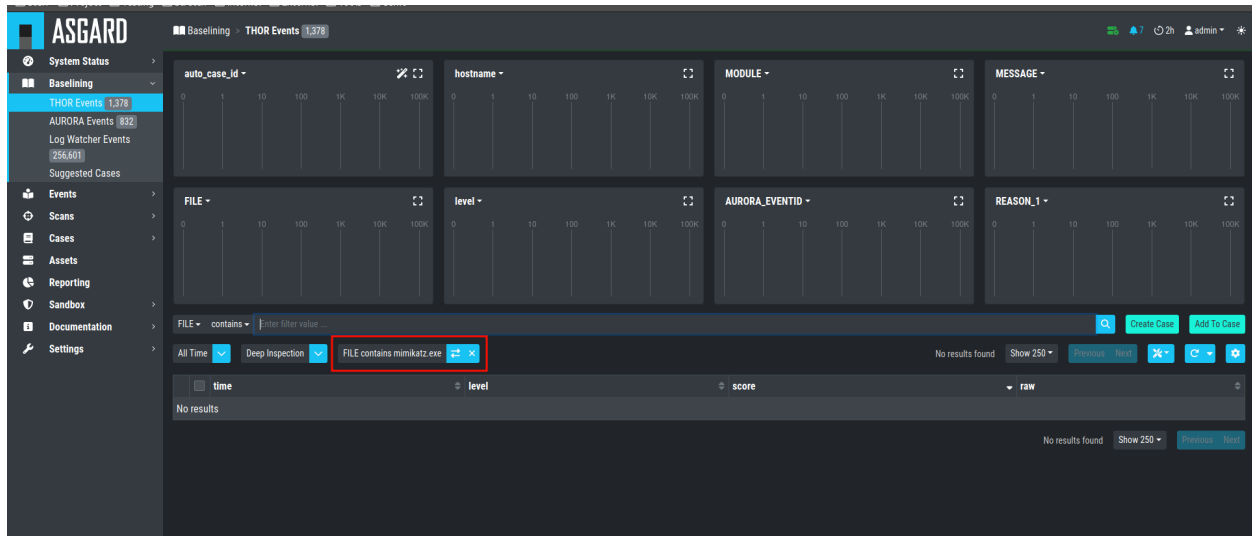


Fig. 9: Log Section empty

6.2.4 Case Creation from Selection

In order to create a case from a specific selection of logs simply use the checkboxes at the very left side of the table and click the **Create Case** button select **Selected events** and add a name, that makes sense to you.

After closing you will find the selected logs have been removed from the logs section.

6.2.5 Case Creation Using a Custom Condition

To create a case with a condition, click the **Create Case** button and select **Condition**. Now you can build a condition by entering keywords in the field.

Keywords in the same field are combined by **OR**, you can negate them by clicking the **NOT** button or combine them with **AND** by clicking the **Add AND Condition** button. The filter bubbles you have generated before will be used as default. You are free to use, modify or delete them. Conditions only match on the **raw** field.

The **Test Condition / Regular Expression** button will calculate the numbers of hits and return some matching and some non-matching events as an example.

Again, you may or may not add auto assignment for future incoming log lines, summary, assessment, case type, recommendations or a comment. After closing you will find the selected logs have been removed from the logs section.

6.2.6 Case Creation Using a Regular Expressions

In order to create a case from a regular expression just click the **Create Case** button and select **Regular Expression**. This lets you write and test your regular expression.

The **Test Condition / Regular Expression** button will calculate the numbers of hits and return some matching and some non-matching events as an example.

Again, you may or may not add auto assignment for future incoming log lines, summary, assessment, case type, recommendations or a comment. After clicking the **Create Case** button, the matching lines will get removed from the log management view.

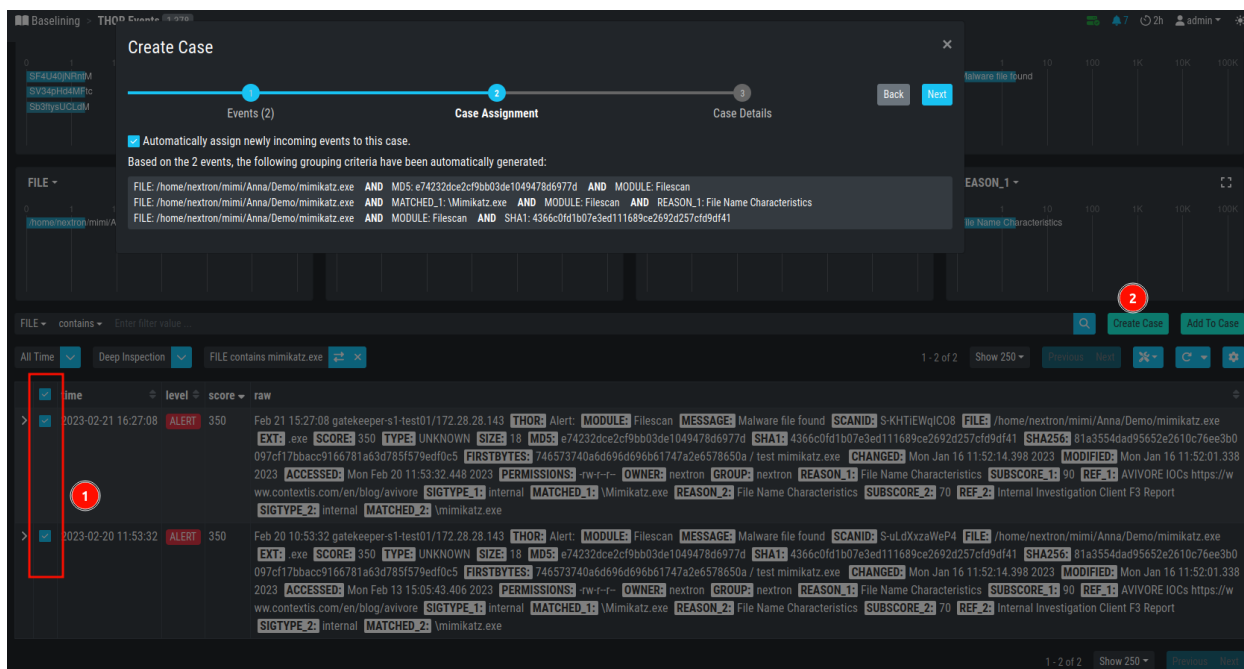


Fig. 10: Creating Cases from Selection

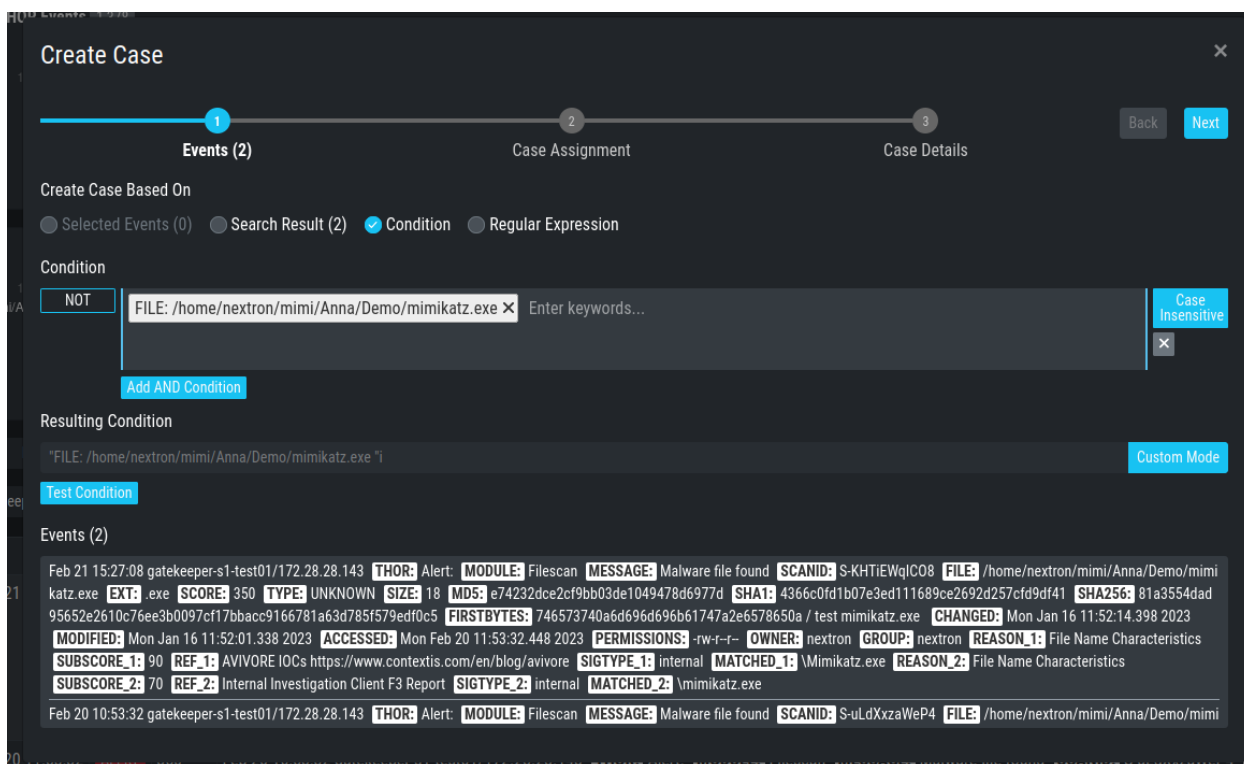


Fig. 11: Creating Cases through Condition

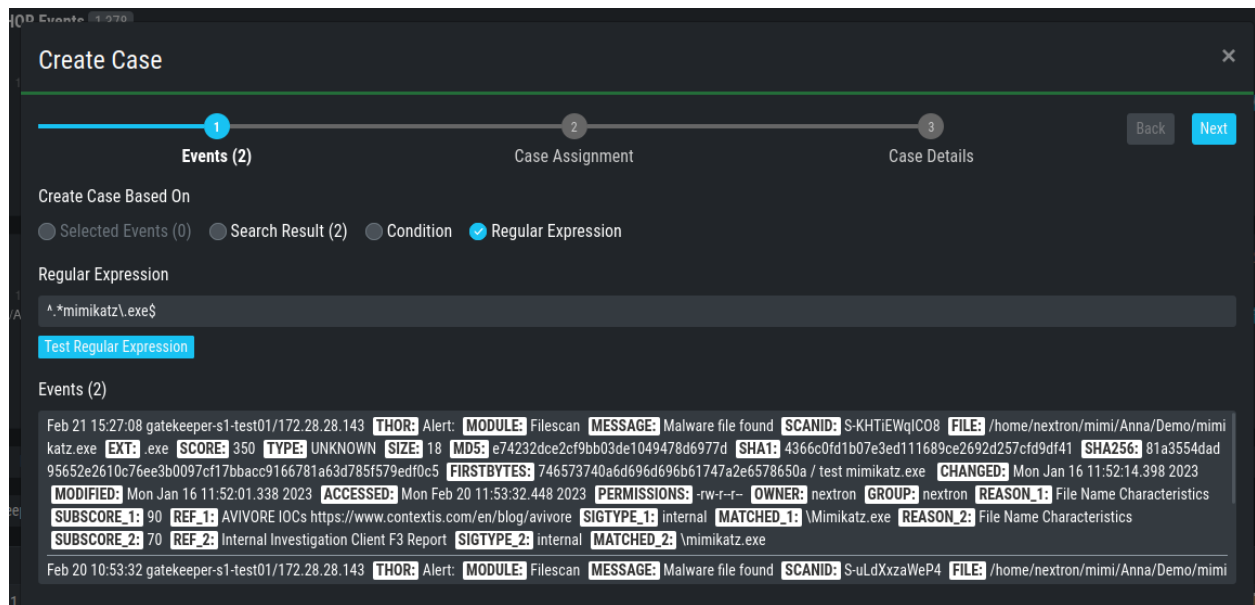


Fig. 12: Creating Cases through Regular Expressions

Warning: It is recommended to use regular expressions only rarely and with caution. This feature can severely impact the performance of the system.

6.3 Create Cases Automatically

With Auto Baselining, the Cockpit will automatically generate cases for groups of logs that are similar, or in other words: Have the same `auto_case_id`.

After clicking the button **Automatically generate Cases** button in the **Auto Baselining** tab you will be prompted for a threshold. This means: Do only create a case when you find at least that many similar logs. In our example below the Cockpit will now generate cases for all groups of at least 2000 similar events.

After pressing the **Start** button, the Cockpit will start calculating and create cases. Depending on the data volume this may take a while and you will be presented a page that shows that Auto Cases is still running along with the current number of cases.

It is safe to leave this page, once the status in **Running**. It will continue in the background.

Important: The Analysis Cockpit generates `auto_case_ids` only for Alerts and Warnings. Don't use the Autocase feature for Notice and Info level events.

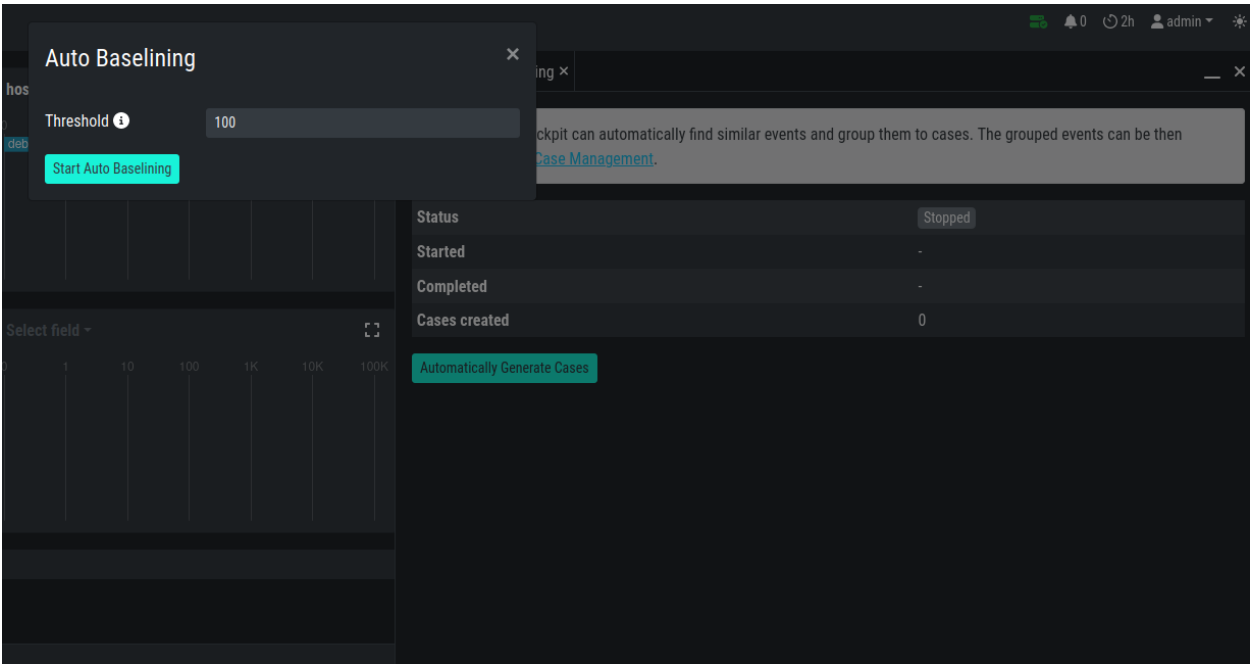


Fig. 13: Automatically create cases

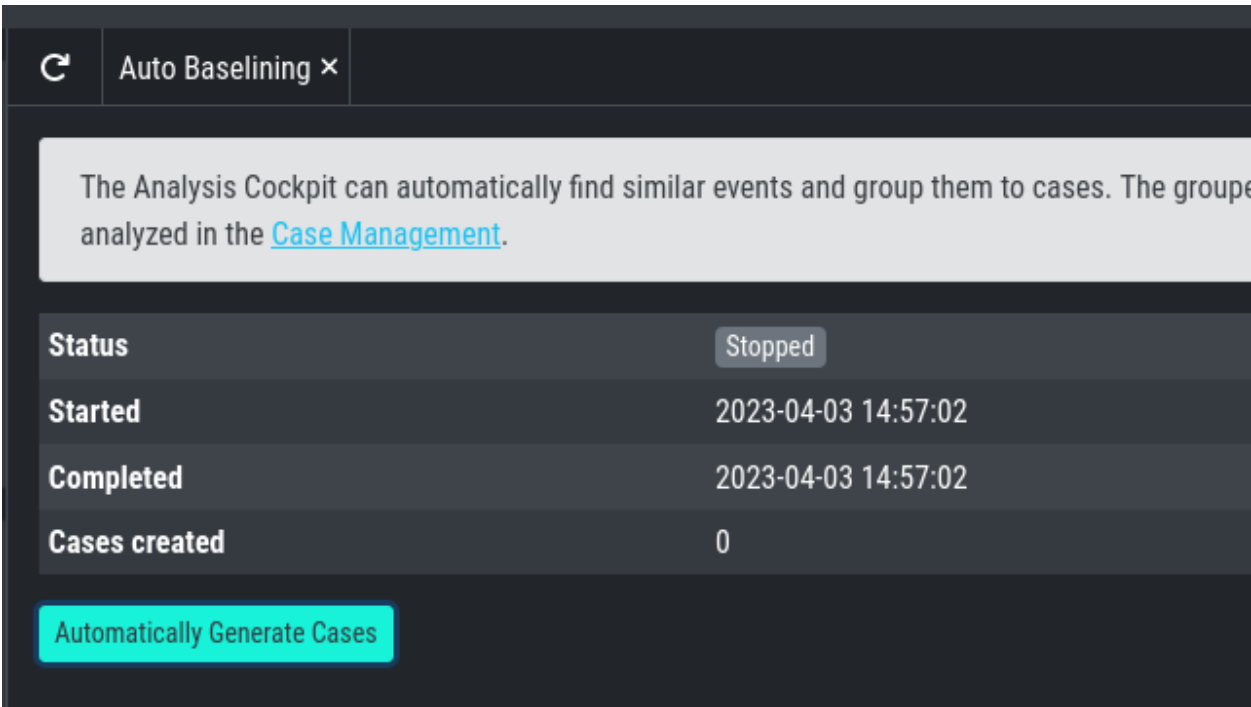


Fig. 14: Auto Cases Status

6.4 Add to Case

Sometimes you may want to add log lines to an already existing case because they represent the same security context. To do this you can just click the Add to Case button and select the suitable case. It is also possible to add an additional comment to this case for the addition.

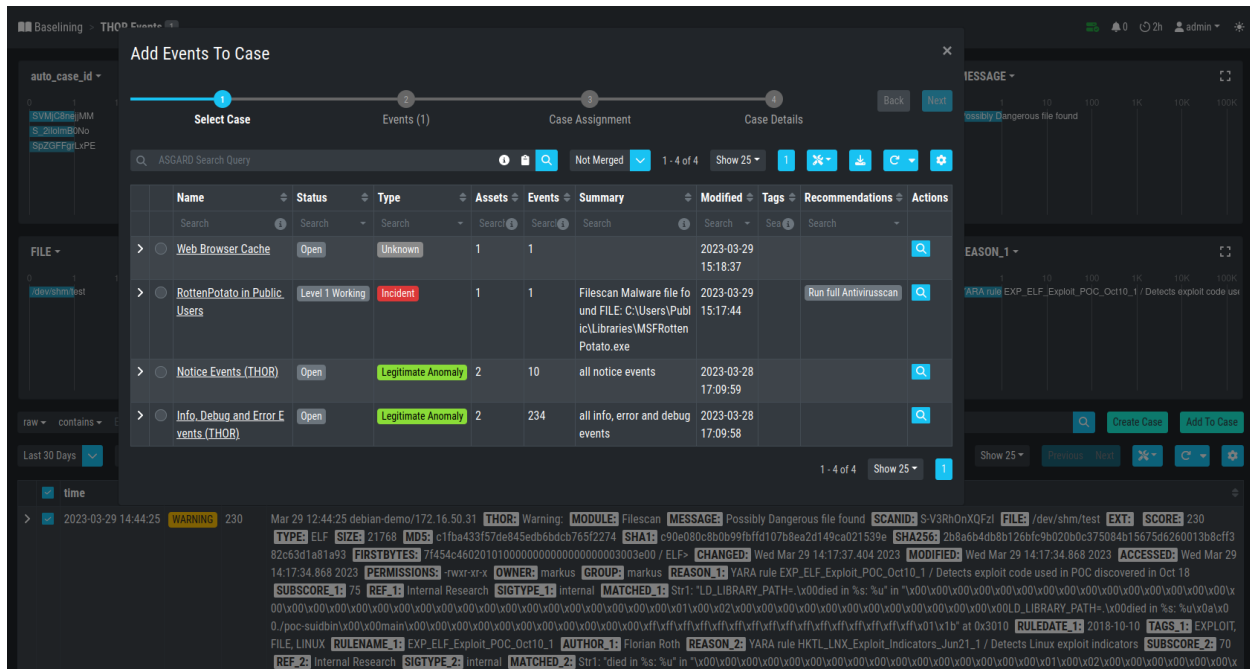


Fig. 15: Add to Case

6.5 Customizing the Detailed View of Log Lines

The detailed view for log lines opens by clicking on a log line. Within this view you can select some fields as favorite fields by clicking on the star symbol. They will always be shown at the top of this view. MESSAGE, MODULE and hostname are selected by default.

To search for all log lines with the same entry as this log line in a particular field, you can click the dropdown on the left hand side of the field.

Additionally, you can find a VIRUSTOTAL button in every hash field and a VALHALLA button in every reason field. By clicking VIRUSTOTAL the hash will be searched on Virustotal. By clicking VALHALLA you will get more information about the matching rule from valhalla.nexttron-systems.com.

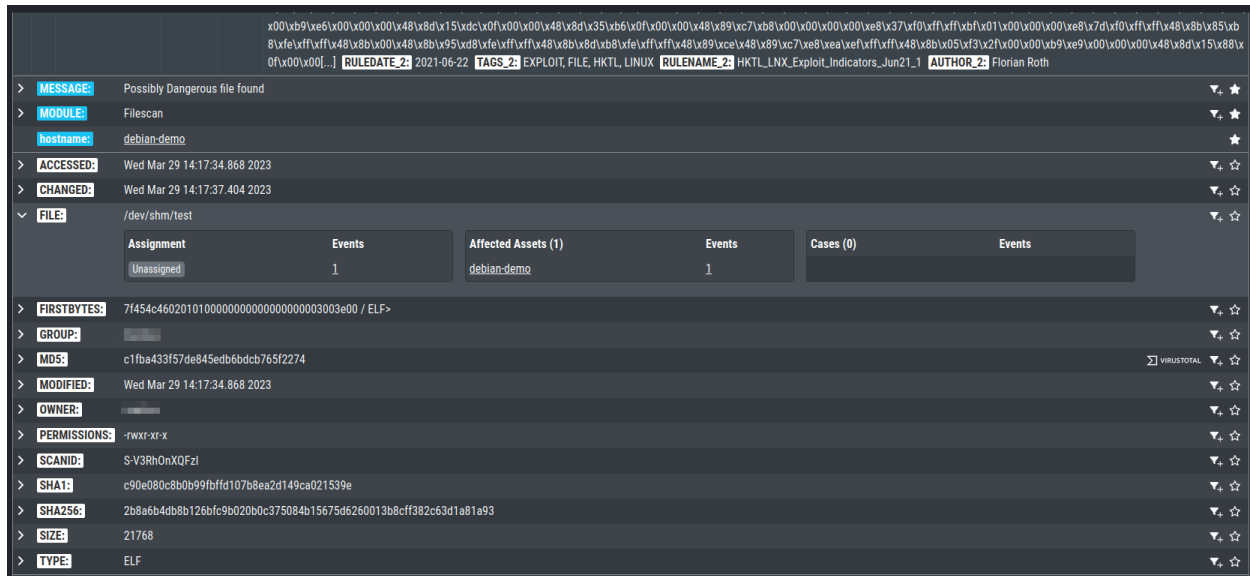


Fig. 16: Customizing the detailed view for log lines

6.6 Usage of the Context Menu

You can use the context menu on any **value** in your logs to get an action menu. Within this menu, you can do different actions:

You can filter, search for similar events, or even create cases based on the value you right-clicked.

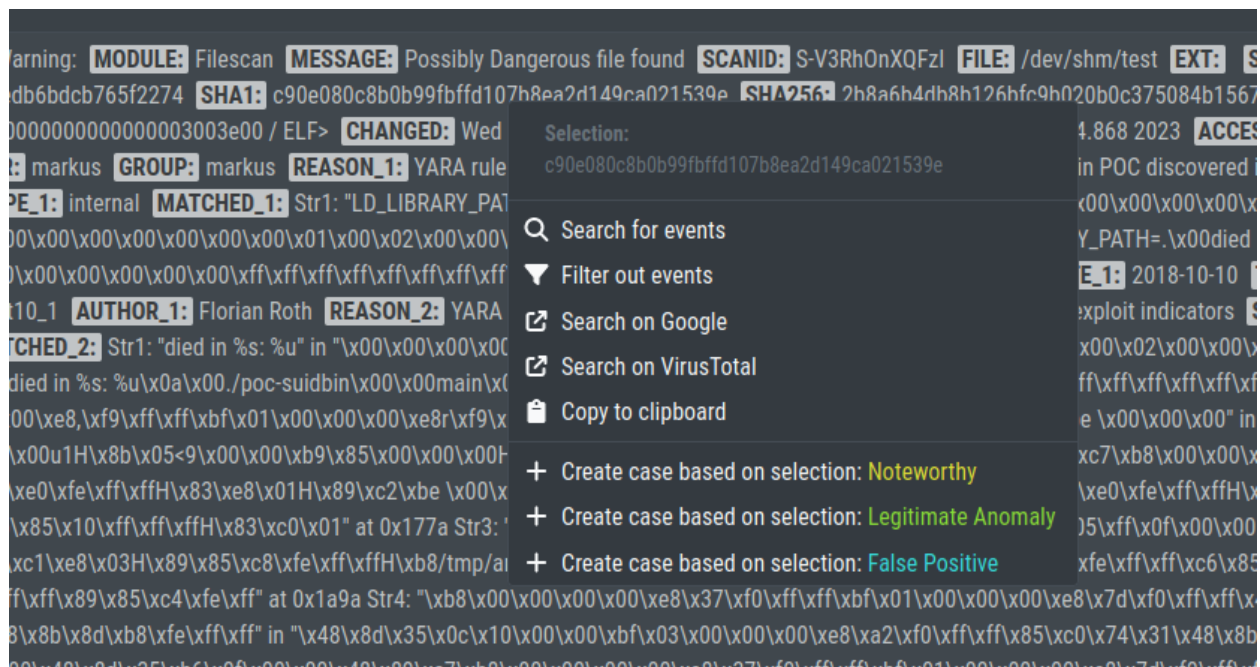


Fig. 17: Context Menu

CASE MANAGEMENT BEST PRACTICES

This section assumes, that a 2-Level model as described in *Understanding Users, Roles, Rights and Case Status* is used.

The following actions will be explained:

- Opening a case
- Handing a case over to the next level
- Closing a case
- Reviewing the rules that add future logs to this case (Grouping Criteria)

7.1 Open a Case for Editing

The picture below shows the Case Management view with cases that have been created with the Auto Case feature. You can see those cases by filtering the Name column to only contain the Auto Case value and the Status column to only contain the Open value.

The screenshot displays the ASGARD Case Management interface. The top navigation bar includes 'System Status', 'Baselining', 'Events', 'Scans', 'Cases', 'Assets', 'Reporting', 'Sandbox', 'Documentation', and 'Settings'. The 'Cases' section is expanded, showing 'THOR Cases', 'Aurora Cases', 'Log Watcher Cases', and 'Advanced'. The main content area shows a list of cases with columns for ID, UUID, Name, Status, Type, Assets, Events, Creator, Summary, Modified, Tags, Recommendations, and Actions. The search bar at the top filters for 'name CONTAINS "Auto Case" AND status = "Open"'. The table lists four cases, all with 'Auto Case' as the name and 'Open' as the status. The first case (ID 329) has a summary of 'Eventlog Sigma match on Eventlog record ENTRY: E ventID: 1116 Provider_Name: Microsoft-Windows-W indows Defender Provider_Guid: {11cd958a-c507-4e f3-b3f2-5fd9fbd2c78} Version: 0 Level: 3 Task: 0 Opcode: 0 Keywords: 0 TimeCreated_SystemTime: 2022-07-12T07:57:03.7693772Z Even... (truncated)'. The second case (ID 328) has a summary of 'RegistryHive Suspicious file name in registry hive on tities found ELEMENT: (1151787C-E79D-4e20-9618-75A811715A0D)\Root\InventoryApplicationFile\do c.exe\435a52aff220a2bcLongPathHash.doc.exe\43 5a52aff220a2bc'. The third case (ID 327) has a summary of 'Filescan Possibly Dangerous file found FILE: C:\tho r\custom-signatures\otx-hash-hocs.txt'. The fourth case (ID 326) has a summary of 'ServiceCheck Service that is not owned by root user'.

ID	UUID	Name	Status	Type	Assets	Events	Creator	Summary	Modified	Tags	Recommendations	Actions
329	020bc737-3114-4421-89c0-580458cea933	Auto Case	Open	Unknown	5	12		Eventlog Sigma match on Eventlog record ENTRY: E ventID: 1116 Provider_Name: Microsoft-Windows-W indows Defender Provider_Guid: {11cd958a-c507-4e f3-b3f2-5fd9fbd2c78} Version: 0 Level: 3 Task: 0 Opcode: 0 Keywords: 0 TimeCreated_SystemTime: 2022-07-12T07:57:03.7693772Z Even... (truncated)	2023-03-09 11:27:21		Verify Legitimacy	
328	ea0956e7-ad67-4299-aad0-795104518d05	Auto Case	Open	Unknown	1	17		RegistryHive Suspicious file name in registry hive on tities found ELEMENT: (1151787C-E79D-4e20-9618-75A811715A0D)\Root\InventoryApplicationFile\do c.exe\435a52aff220a2bcLongPathHash.doc.exe\43 5a52aff220a2bc	2023-03-07 15:00:20			
327	a6a3be94-345f-4625-b92d-7c4894614b03	Auto Case	Open	Unknown	10	24		Filescan Possibly Dangerous file found FILE: C:\tho r\custom-signatures\otx-hash-hocs.txt	2023-03-07 15:00:19			
326	e2085300-13f6-4308-95c0-928536c8a425	Auto Case	Open	Unknown	9	30		ServiceCheck Service that is not owned by root user	2023-03-07 15:00:18			

Fig. 1: Opening a Case for editing

In our example a Level 1 Analyst would now pick one of these open cases and set the Status to "Level 1 Working". To do this, they would open the case by clicking on the magnifier button and modify the status to Level 1 Working and

then click Update.

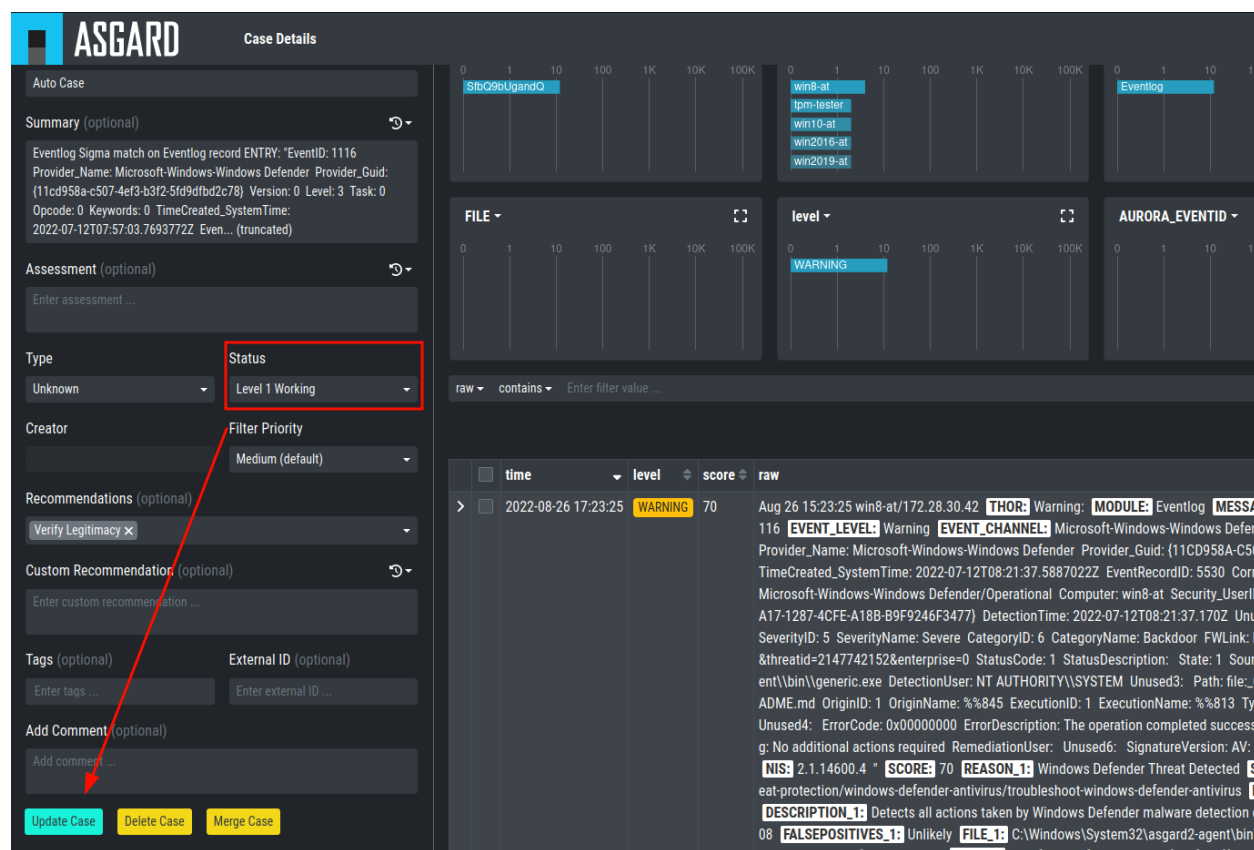


Fig. 2: Change Status

Now the logs within the case can be analyzed and results can be documented in the assessment field. Recommendations can be set from the canned recommendations list. Columns can be faded in and out and comments can be added.

7.2 Case Dispatching

Let's assume, our Level 1 Analyst concludes, that this is a "Legitimate Anomaly". They will now set the status to "Level 1 Finished" and update the case. After setting the case to "Level 1 Finished" the case becomes visible to the Level 2 Analyst.

7.3 Closing a Case

Let's assume, that a Level 2 Analyst now picks one of the cases in status "Level 1 Finished" and starts working on this case.

In this respect we assume, that something suspicious has been found, that needs further analysis by the system administration team. In most organizations this will be controlled through the organization's action request or ticketing system. So, we assume, that we will close the case in the Analysis Cockpit as it is progressed in another system. Thus, the status is changed to closed and the case gets updated.

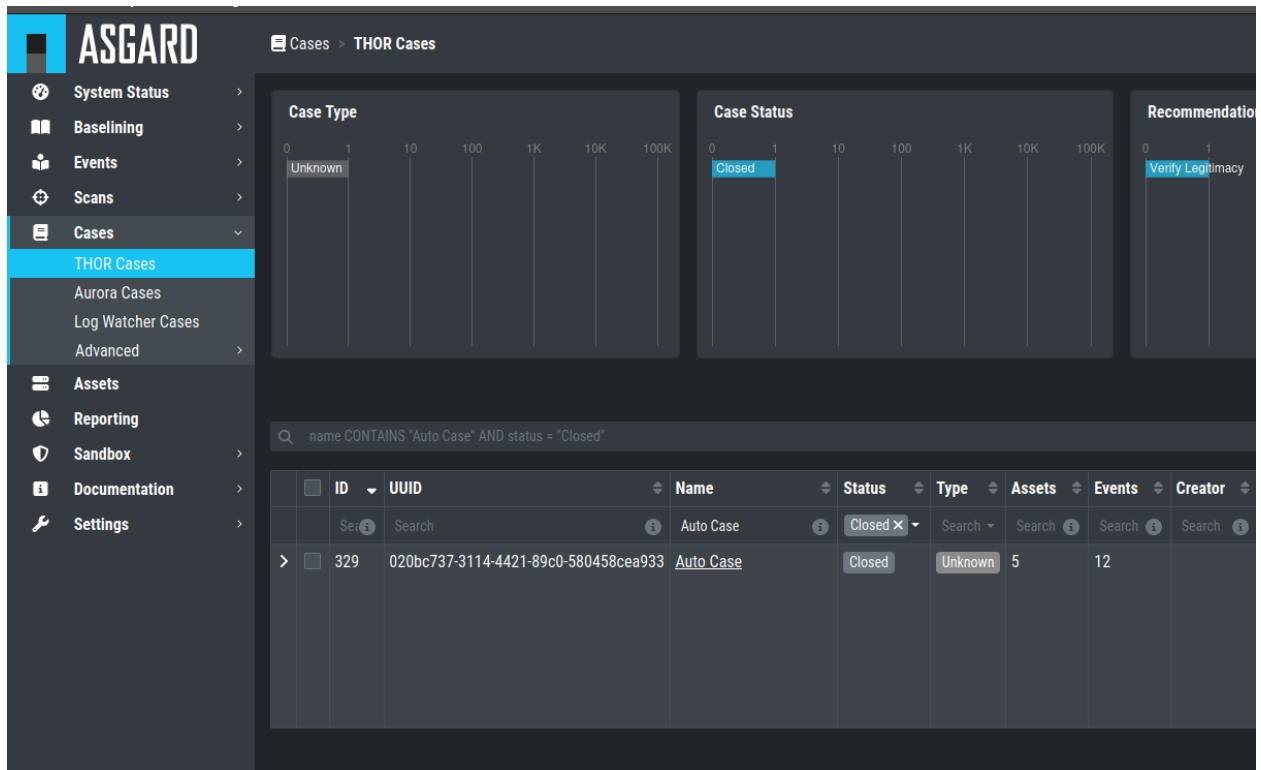


Fig. 3: Closing a Case

Note: The Analysis Cockpit provides interfacing to action-request and external ticketing systems using the API.

7.4 Generate and Review auto_case_ids

These auto_case_ids can be reviewed in the Grouping Criteria section of the case.

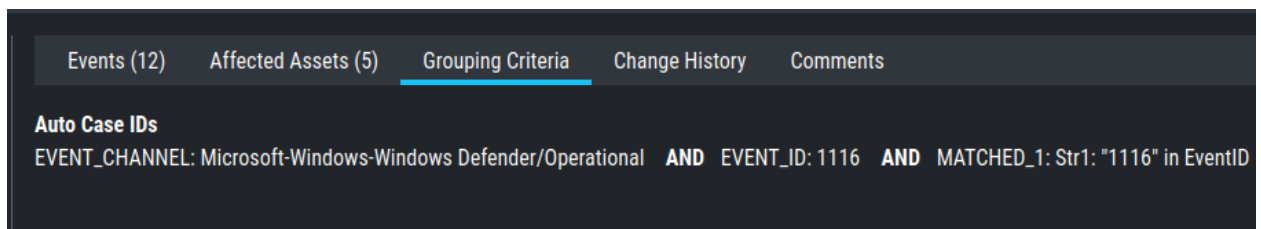


Fig. 4: Reviewing Grouping Criteria

In our example, three auto_case_ids were added that match all 1,000 log lines. In the future all incoming logs, that match one of the three “Detailed Reasons” will be added to this case directly and will not show up in the Log Management section.

7.4.1 Limitations

There are limitations to the visibility of grouping criteria. Grouping Criteria are only calculated for Alerts and Warnings. For all other types of logs (Notices, Info, Error) auto_case_ids are not calculated, so every log line gets its own highly specific filter that matches future occurrences of exactly the same log line but will not do any kind of generic matching. These highly specific filters are not displayed in the case for simplicities sake.

In rare cases the Analysis Cockpit will find it difficult to calculate auto_case_ids even for Alerts and Warnings. These logs will get tagged with optimized_template=false. In this case, the behavior is like for Notices, Info and Error messages. Grouping Criteria will not show up as it will be one highly specific filter per log line.

7.5 More Information about Cases

The Affected Assets tab of a case shows assets that have contributed at least one log line to this case. In this example 5 assets are affected. All of them have the same operating system "windows".

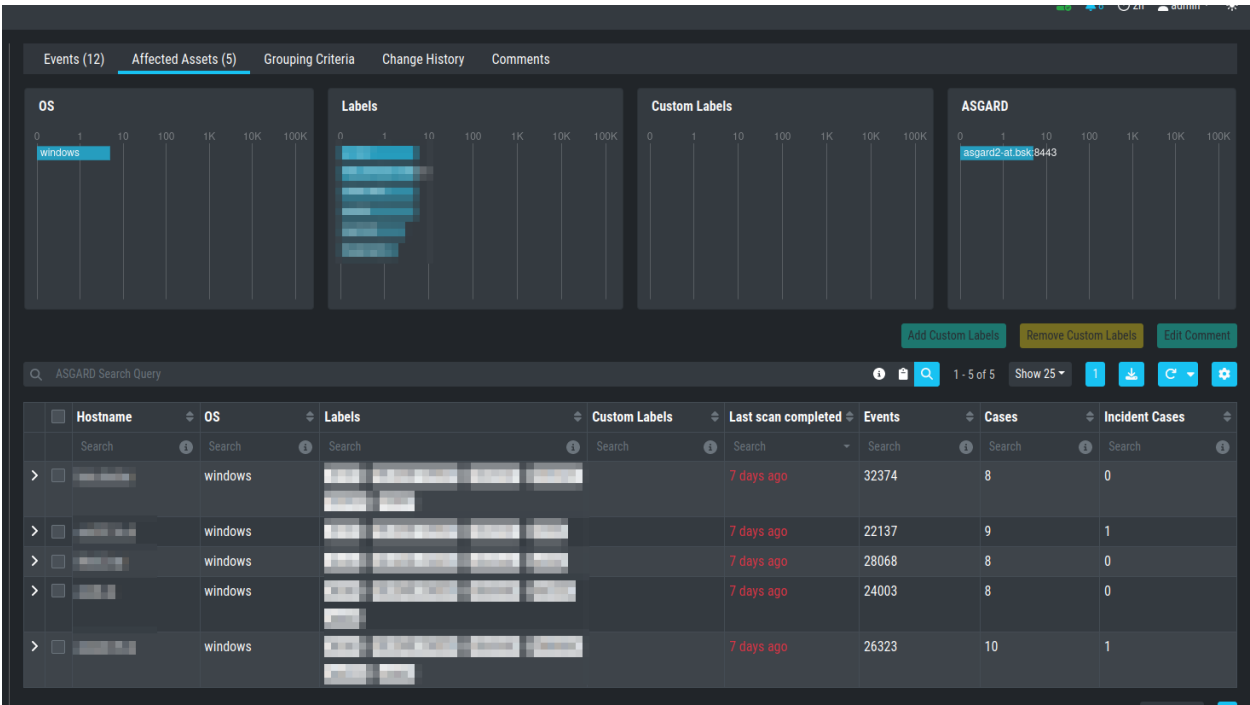


Fig. 5: Case – Assets Tab

In the Comments tab you can add comments and attachments to this case. Attachments can be used to pass additional information to members of the analysis team (e.g. memory dump for further analysis).

The Changes tab shows information about changes to this case.

In other words: This is your case audit log.

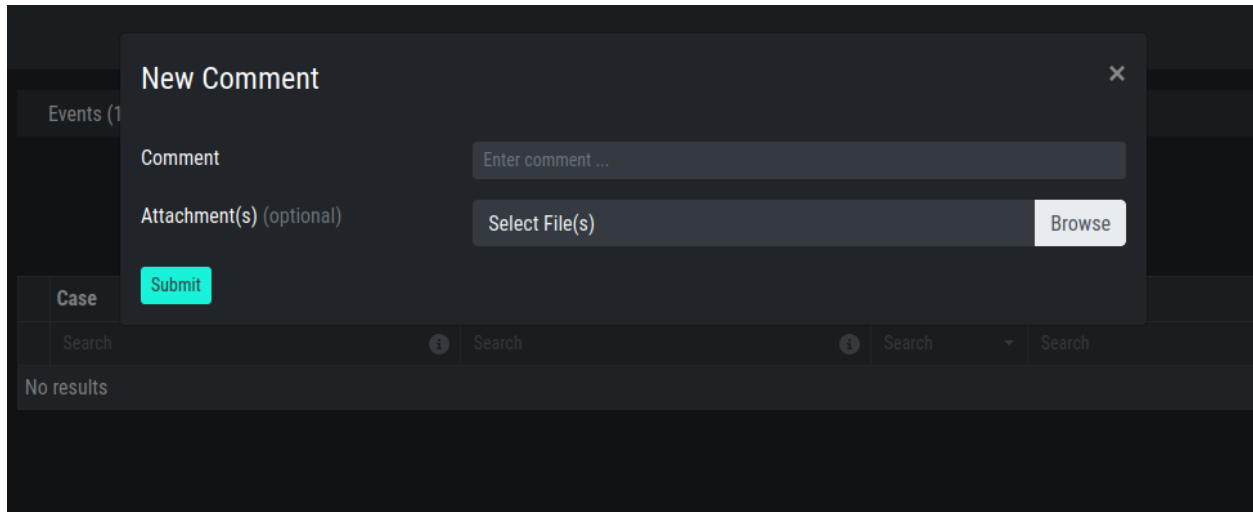


Fig. 6: Case – Comments

Events (12)

Affected Assets (5)

Grouping Criteria

Change History

Comments

1 - 7 of 7

Show 25

Case ID	User	Time	Changes	Current Name	Current Type	Current Status
<div>Search</div>	<div>Search</div>	<div>Search</div>	<div>Search</div>	<div>Search</div>	<div>Search</div>	<div>Search</div>
> 329		2023-04-03 15:28:01	Updated Status from Closed to Open	Auto Case	Unknown	Open
> 329	admin	2023-04-03 15:26:50	Updated Status from Open to Closed	Auto Case	Unknown	Open
> 329	admin	2023-03-09 11:27:21	Updated Recommendations from to Verify Legitimacy	Auto Case	Unknown	Open
> 329	admin	2023-03-09 11:11:59	Updated Recommendations from to test	Auto Case	Unknown	Open
> 329	admin	2023-03-09 11:06:16	Updated Status from Level 1 Working to Open	Auto Case	Unknown	Open
> 329	20230306-PBU	2023-03-09 11:05:49	Updated Status from Open to Level 1 Working	Auto Case	Unknown	Open
> 329		2023-03-07 15:00:22	Created case	Auto Case	Unknown	Open

1 - 7 of 7

Show 25

Fig. 7: Case – Changes tab

7.6 Bulk Edit / Bulk Delete

The Analysis Cockpit features a convenient way to make certain changes to groups of cases. Just select the case in the left column and click the `Edit Cases` or `Delete Cases` button.

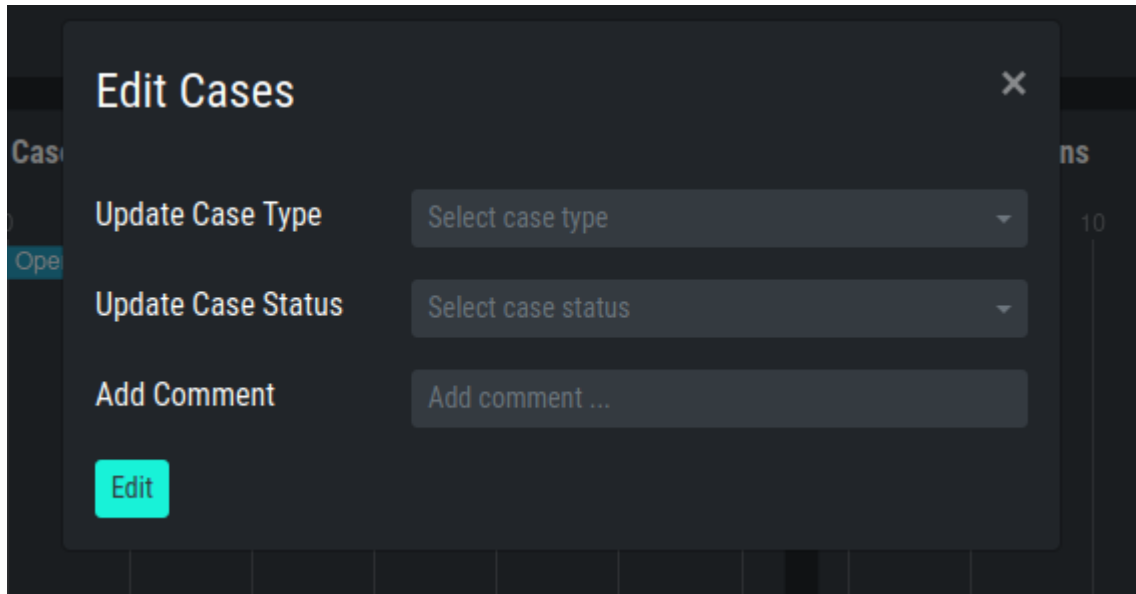


Fig. 8: Bulk Edit

MAINTENANCE

8.1 System Updates

Since the release of version 4 of the Analysis Cockpit, the update section only contains instructions on how to update to the newest major version. If you wish to keep using version 3 of the Analysis Cockpit, but still receive bugfix updates, you can run the following commands via SSH:

```
nexttron@analysis:~$ sudo apt update
nexttron@analysis:~$ sudo apt upgrade
```

Please note that you have to do that for every bugfix which is released. So please make sure to run those commands sporadically on your Analysis Cockpit.

8.2 Configuration Backup & Restore

The Analysis Cockpit comes with a backup and restore function for its configuration. The Configuration Backup contains the following data:

- Cases, Grouping Criteria, Recommendations, Case Changes, Case Comments
- Users, Roles, LDAP Roles, Role Rights
- User Configurations

To perform a backup, you can simply go to **Settings > Backup** and click **Create Configuration Backup**. To restore from an old backup, it is important to understand the implications of the restore. From the Backup page of the Analysis Cockpit:

The restore procedure will install a previously generated configuration backup on this Analysis Cockpit. All data on this Analysis Cockpit will be deleted before. This can only be done on newly installed Analysis Cockpits and not on an Analysis Cockpit that is already in use. Do not use the restore to rollback to an earlier point in time, this will cause inconsistent data.

Warning: Installing a configuration backup of an earlier Analysis Cockpit Release Version is not supported and may fail. The currently installed version is 3.5.6. The version of the configuration backup can be found in the file name. The backup's file name has the following pattern: `analysis_cockpit_%VERSION%_backup_%DATE%.sql.gz`

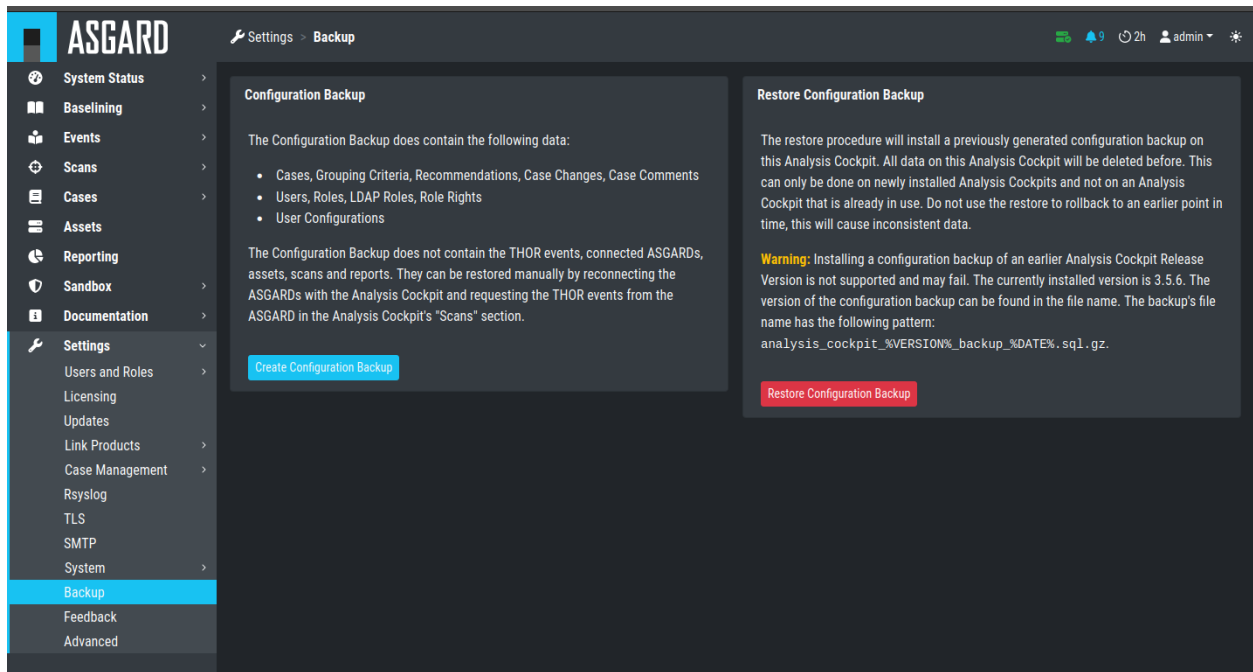


Fig. 1: Configuration Backup & Restore

8.3 Regain Disk Space

If your disk is already at or close to 100% and AC no longer works properly, see section [Recover from a Full Disk](#).

If your disk usage is growing too fast and free disk space is running out, you have several options:

1. Increase the size of your disk
2. Delete files that are not needed for operation
3. Delete files that are used by AC but are unneeded / dated

8.3.1 Safe-to-Delete Files

The following files are safe to delete. They are not needed for AC to operate.

- `/var/lib/nextron/analysiscockpit3/log/*.gz`
- `/var/lib/nextron/analysiscockpit3/events/*.ok`

They are only kept on the system if needed for further processing. E.g. saving/sending the log files to another system or keeping the THOR scans (found in events) for backup reasons. If you do not need or plan to use those, they can be deleted. If you are unsure make a copy to another system before deleting them.

More details can be found in section [Recover from a Full Disk](#).

8.3.2 Potentially Unneeded / Dated Files

This method is only advised as a last resort if increasing your disk space is not an option.

If your AC is running for a long time, there might be data ingested that you no longer need and therefore can be deleted to regain disk space. This includes:

- Scans
- Reports

Deleting Unneeded Scans

Warning: Deleting old scans deletes information ASGARD Analysis Cockpit uses.

As an example: If you delete a scan with which an asset was marked in an incident case, this connection is no longer made and the asset will be shown with 0 incident cases.

Therefore only delete scans you no longer need. This can be done under Scans > Scans by selecting the scans with check marks and clicking **Delete Events**.

You can filter events for deletion with the time range picker in the completed column and e.g. selecting only scans with 0 incident and 0 suspicious cases. (Add columns using the **Columns** button).

<input checked="" type="checkbox"/>	ASGARD	ID in	Asset	Scanner	Parameters	Status	Started	Completed	Took	Events	Cases	Incident	Suspicious
Sea	Search	Search	Search	THOR	Search	Select	Search	1970-01-01 - :	Search	Search	Search	0	0
<input checked="" type="checkbox"/>	1	95	workstation-04	THOR	THOR 10 quick syslog: %asgar.. IOC Rulesets: default	Completed	2021-05-17 10:12:08 +02:00	2021-05-17 10:15:19 +02:00	3 minutes	1577	12	0	0
<input checked="" type="checkbox"/>	1	31	workstation-02	THOR	THOR 10 quick syslog: %asgar.. IOC Rulesets: default	Completed	2021-04-01 14:51:00 +02:00	2021-04-01 14:56:47 +02:00	6 minutes	1515	14	0	0

Fig. 2: Possible Filter for Selecting Scans for Deletion

Another possibility is searching for assets which are no longer part of your infrastructure and deleting their scans.

Deleting Unneeded Reports

Old unneeded reports can be deleted via command line and are found at `/var/lib/nextron/analysiscockpit3/reports`.

Note: The reports are still listed in the UI after removal, but a download attempt will fail.

TYPICAL PITFALLS

9.1 Certificate Validation Failed

If you receive the following error, SSL/TLS interception interrupted the installation process.

```
nextron@cockpit:~$ sudo nextronInstaller -cockpit
[sudo] password for nextron:
Ign:1 https://update3.nextron-systems.com analysis InRelease
Err:2 https://update3.nextron-systems.com analysis Release
Certificate verification failed: The certificate is NOT trusted. The certificate issuer
↳ is unknown. Could not handshake: Error in the certificate verification. [IP: 192.168.3.
↳ 21 8080]
```

Since we do not support setups in which the connections to our update servers are intercepted (see chapter *Requirements*), the only way to resolve this problem is to deactivate SSL/TLS interception for our update servers.

9.2 Log File Import of Previous Years

The log file format of (old) THOR scan logs is the original SYSLOG format, which contains no year value in the timestamp of the message header.

You can modify the timestamp of old THOR logs by using the following script:

<https://github.com/NextronSystems/nextron-helper-scripts/blob/master/asgard-analysis-cockpit/thor-timestamp-converter.py>

9.3 Recover from a Full Disk

If your disk is full or near full, ASGARD Analysis Cockpit will not work properly. In order to resume its operation you need to make free space on the disk.

We suggest to save the files to another system beforehand, if you want to keep the information for future usage. ASGARD will not need the following files to function and they can be removed safely:

- /var/lib/nextron/analysiscockpit3/log/*.gz
- /var/lib/nextron/analysiscockpit3/events/*.ok

Especially the assignment log can grow big in production environments. If deleting the logs is not enough, deleting the already read-in events (ending on .ok) is the next best location to regain disk space. If there are too many files for a simple `rm *.ok`, you can use `find` to delete them:

```

nexttron@cockpit:~$ sudo su -
[sudo] password for nexttron:
root@cockpit:~# find /var/lib/nexttron/analysiscockpit3/events -name "*.ok" -print0 |
↪xargs -0 -I'{}' rm '{}'

```

If Elasticsearch does not automatically work again after cleaning up some disk space, restart it under Settings > System > Services or with `sudo systemctl restart elasticsearch.service`. If this is not working either, you may need to disable Elasticsearch's read-only mode. See [ElasticSearch Index Locked Due to Low Free Disk Space](#) for a how-to.

Deleting the files given above should be enough to resume operation. If the disk on your ASGARD Analysis Cockpit is full because of growing data over time, the disk space should be increased. If that is not an option you can delete old scans as described in section [Potentially Unneeded / Dated Files](#).

9.4 ElasticSearch Index Locked Due to Low Free Disk Space

```

Mar 26 09:48:09 analysis-cockpit[22732]: [ERROR] could not update log:
could not update logs: could not update documents: http status 403

```

```

{
  "took": 48,
  "timed_out": false,
  "total": 136,
  "updated": 0,
  "deleted": 0,
  "batches": 1,
  "version_conflicts": 0,
  "noops": 0,
  "retries":
  {
    "bulk": 0,
    "search": 0
  },
  "throttled_millis": 0,
  "requests_per_second": -1.0,
  "throttled_until_millis": 0,
  "failures":
  [
    {
      "index": "logs-2019-03-21",
      "type": "doc",
      "id": "L11527716281914854515",
      "cause":
      {
        "type": "cluster_block_exception",
        "reason": "blocked by: [FORBIDDEN/12/index read-only / allow delete
↪(api)];"
      },
      "status": 403
    },
    {

```

(continues on next page)

(continued from previous page)

```

        "index": "logs-2019-03-21",
        "type": "doc",
        "id": "L12526619521231613944",
        "cause":
        {
            "type": "cluster_block_exception",
            "reason": "blocked by: [FORBIDDEN/12/index read-only / allow delete
↪(api)];"
        },
        "status": 403
    },
    {
        "index": "logs-2019-03-21",
        "type": "doc",
        "id": "L10726191995274581682",
        "cause":
        {
            "type": "cluster_block_exception",
            "reason": "blocked by: [FORBIDDEN/12/index read-only / allow delete
↪(api)];"
        },
        "status": 403
    },
    {
        "index": "logs-2019-03-21",
        "type": "doc",
        "id": "L17340155165061572392",
        "cause":
        {
            "type": "cluster_block_exception",
            "reason": "blocked by: [FORBIDDEN/12/index read-only / allow delete
↪(api)];"
        },
        "status": 403
    },
    {
        "index": "logs-2019-03-21",
        "type": "doc",
        "id": "L10064611600393832220",
        "cause":
        {
            "type": "cluster_block_exception",
            "reason": "blocked by: [FORBIDDEN/12/index read-only / allow delete
↪(api)];"
        },
        "status": 403
    }
}
]
}

```

This happens when Elasticsearch thinks the disk is running low on space so it puts itself into read-only mode.

By default, Elasticsearch's decision is based on the percentage of disk space that's free, so on big disks this can happen

even if you have many gigabytes of free space.

The flood stage watermark is 95% by default, so on a 1TB drive you need at least 50GB of free space or Elasticsearch will put itself into read-only mode.

You can fix that issue with the following command using the command line on ASGARD:

```
nextron@asgard:~$ curl -XPUT -H "Content-Type: application/json" http://localhost:9200/_all/_settings -d '{"index.blocks.read_only_allow_delete": null}'
```

9.5 Debug Failed File Imports

Check for reported problems using this command:

```
nextron@cockpit:~$ sudo su -  
[sudo] password for root:  
nextron@cockpit:~$ find /var/lib/nextron/analysiscockpit3/events -name "\*.problem"
```

Make sure that you're able to see the imported log data and review the selected time range in the time range picker in whatever view you're reviewing the data. Be aware that the log data gets indexed with the creation timestamp of the log lines not the time of their import.

This means that if you're importing log data that is old, the default date range set in the date range picker may be too narrowly defined so that you're just unable to see the imported data.

9.6 Fixing a Broken Proxy Configuration

Sometimes during installation, proxy settings get mixed up or a typo in the proxy URL leads to a broken Internet connection.

It is not trivial to fix this situation, since the proxy settings collected during installation are changed in so many different locations on a Linux system for all the different services and command line tools.

9.6.1 Broken before Analysis Cockpit Installation

If you have set a wrong proxy before the package installation using the **sudo nextronInstaller -cockpit** command and the installer failed to fetch the required packages from our update servers, perform the following steps.

Fix the proxy string in the file `/etc/apt/apt.conf.d/00proxy`

```
nextron@cockpit:~$ sudoedit /etc/apt/apt.conf.d/00proxy
```

Then rerun the installer.

9.6.2 Broken after the Analysis Cockpit Installation

If your infrastructure has changed and you have to change the proxy server sometime later, edit the proxy settings in the Web GUI.

Settings > System > Proxy

This section has frequently asked questions and answers to them. You will find that the format of this section is split into a question as the introduction of each chapter and the explanation right after.

10.1 Disabling Assignment Logs

Q: My assignment Logs on the server are growing quickly, how can I turn them off

The assignment logs located at `/var/lib/nextron/analysiscockpit3/log/assignment.log` write warnings and errors for the Optimize function of the Cockpit.

If you have the feeling that the log is filling up too quickly, you can turn off those logs completely. It is advised to try and see what the problem is before turning off the log completely, as this might indicate an underlying issue.

Run the following command on your Analysis Cockpit (warning: this will restart your Analysis Cockpit. If you do not want to restart the Analysis Cockpit, you can run the second command at a later time):

```
nexttron@cockpit:~$ echo "REPLACE INTO config VALUES ('write-assignment-log','false')" | \
↳ sudo mysql analysiscockpit3
nexttron@cockpit:~$ sudo systemctl restart analysiscockpit3.service
```

To turn back on the `assignment.log`, run the following command:

```
nexttron@cockpit:~$ echo "REPLACE INTO config VALUES ('write-assignment-log','true')" | \
↳ sudo mysql analysiscockpit3
nexttron@cockpit:~$ sudo systemctl restart analysiscockpit3.service
```

10.2 No Events visible

Q: It seems that events are not visible or have been lost. What can I do to verify that they're still in the database?

If you think that some events are not visible or have been lost, you can do the following to verify that they still exist in the database.

First, check your date range picker.

Very often, analysts forget to set it to the right time frame and old events accidentally disappear from the view.

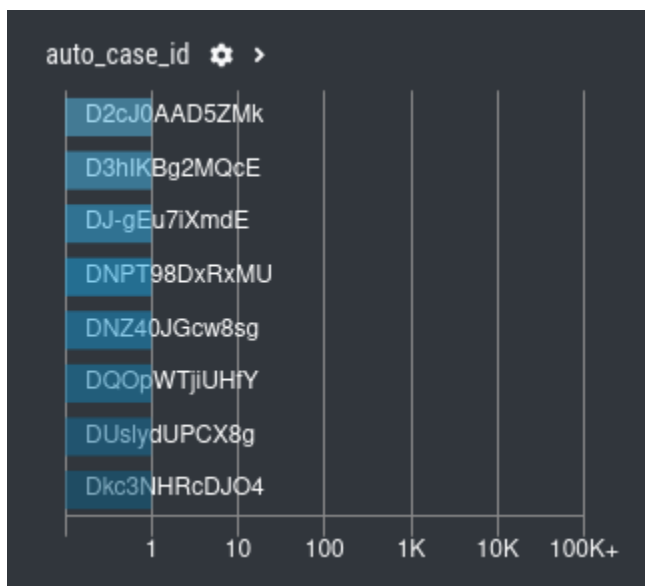
Secondly, make sure you're using the search in the Events section and not the Baselining section.

10.3 No new Events in Case

Q: I have created a case but it seems that no new incoming events are assigned to that existing case. How can I check what's wrong?

The first thing that you should check are the `auto_case_ids` of the events in that case (Cases > Open Case > Events > `auto_case_id` Panel).

If they are distributed as in the following screenshot, it seems that auto-casing doesn't work on this case.



This case doesn't have groupable contents and uses only so-called "Dynamic Auto Case IDs", which are used whenever the Analysis cockpit was unable to find a suitable filter template to create usable filters for this type of events.

Also check the grouping criteria of that case:

Cases > Open Case > Tab Grouping Criteria

What are the conditions defined to assign new events to that case?

10.4 Location of Scan Logs

Q: Where are Scan Logs on the system located?

You can find the Scan Logs in `/var/lib/nextron/analysiscockpit3/events`. In this folder you will find three different naming schemes:

- **.txt.gz** - Logs which are not imported yet
- **.txt.gz.ok** - Logs which were imported successfully
- **.txt.gz.problem** - Logs which could not be imported correctly due to an error

If you need to manually investigate logs which failed during the import (`.gz.problem`), you can do so by copying the files to a different location (`/tmp` for example) and remove the suffix `.problem`. After that you can use `gunzip` to extract the log and inspect it. Most likely you will find that the file did not transfer correctly over to the Analysis Cockpit. This can be seen if you open the file and scroll to the very end. In this case the file will just end in the middle of a log line.

The Logs can be imported into the Cockpit via the Scans menu. Select the Asset which had a problem with the log transfer and click **Request Events**. This will transfer the Events from the corresponding ASGARD. You can also use the Fields **Log Requested**, **Log Received** and **Log Received Error** to filter and look for other failed log transmissions.

10.5 Default password for file downloads

Q: What is the password used to protect file downloads?

Artifacts uploaded to a case might be malware. To ensure the file is not automatically deleted by antivirus or executed by an unknowing user, we zip all files in the attachments and encrypt the ZIP file with a default password. The default password **infected** can be used to extract the file.

10.6 Disk Space filling up quickly

Q: My disk is getting full soon. What options do I have?

If your disk is already at or close to 100% and AC no longer works properly, see section *Recover from a Full Disk*.

In other cases check section *Regain Disk Space*.

10.7 Reverse Proxy to access the Analysis Cockpit

Q: I am using a Reverse Proxy to access the Analysis Cockpit. What do I have to take care of?

The Analysis Cockpit partially uses large URLs to communicate with its backend. Proxy server usually do not allow arbitrary large URLs.

In case of nginx the default header size is 8k (see http://nginx.org/en/docs/http/nginx_http_core_module.html#large_client_header_buffers). If you want to use the Analyst Cockpit behind a nginx reverse proxy, you need to increase the *large_client_header_buffer*. A size of 100k should be sufficient. Also the HTTP2 protocol has to be disabled.

A minimal example configuration for nginx looks as follows:

```
server {
    listen 443 ssl; # !! no http2 !!
    ssl_certificate /path/to/your/certificate.crt;
    ssl_certificate_key /path/to/your/private.key;
    location / {
        proxy_pass https://analysis-cockpit.your.org;
        proxy_set_header Host $http_host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    }
    large_client_header_buffers 4 100k; # increase maximal allowed URL length
}
```

10.8 Internet Explorer

Q: I am using Internet Explorer and the Analyst Cockpit seems to run into a timeout. What can I do?

Modern browsers (e.g. Firefox, Chrome, Edge, Safari) support large URLs. Internet Explorer does not. If you want to access the Analyst Cockpit and all its features, you need to switch your browser.

10.9 Admin Password reset

Q: I forgot my admin password and lost access to the WebUI. How do I reset the admin user password?

If you've lost the password of the local admin user (Web GUI) but still have access the system via SSH, you can reset it via command line using the following command.

```
nexttron@cockpit:~$ sudo mysql analysiscockpit3 -e "UPDATE users SET password =  
↪ '7951GYqdAjLAo01NaQu1ManJDik' WHERE name = 'admin';"
```

This resets the password to admin. You should then change that password immediately.

10.10 Multi Factor Authentication reset

Q: How do I reset Multi Factor Authentication for a specific user

If you or another user lost their second factor (MFA) to log into the ASGARD Web UI, you can reset the users MFA Settings with the following command (in this example we assume that the user is called john):

```
nexttron@cockpit:~$ sudo mysql analysiscockpit3 --execute "UPDATE users SET tfa_valid = 0  
↪ WHERE name = 'john';"
```

KNOWN ISSUES

11.1 AAC#006: Scan stuck at Status "Unknown"

Introduced Version	Fixed Version
<= 3.10.1	3.10.3

There is currently a bug in the Analysis Cockpit which prevents some Scans from being imported correctly.

This is caused by very big events (a single event bigger than 64 Kb), which will cause the parser to error. The Analysis Cockpit can never finish importing this Scan.

Note: If you are unable to see the Update button in the update section (because of the major upgrade text), run the following commands via ssh on your Analysis Cockpit to install the update:

```
nextron@analysis:~$ sudo apt update
nextron@analysis:~$ sudo apt upgrade
```

11.1.1 AAC#006: Check

You can check if one of your scan logs is effected if the following conditions are met:

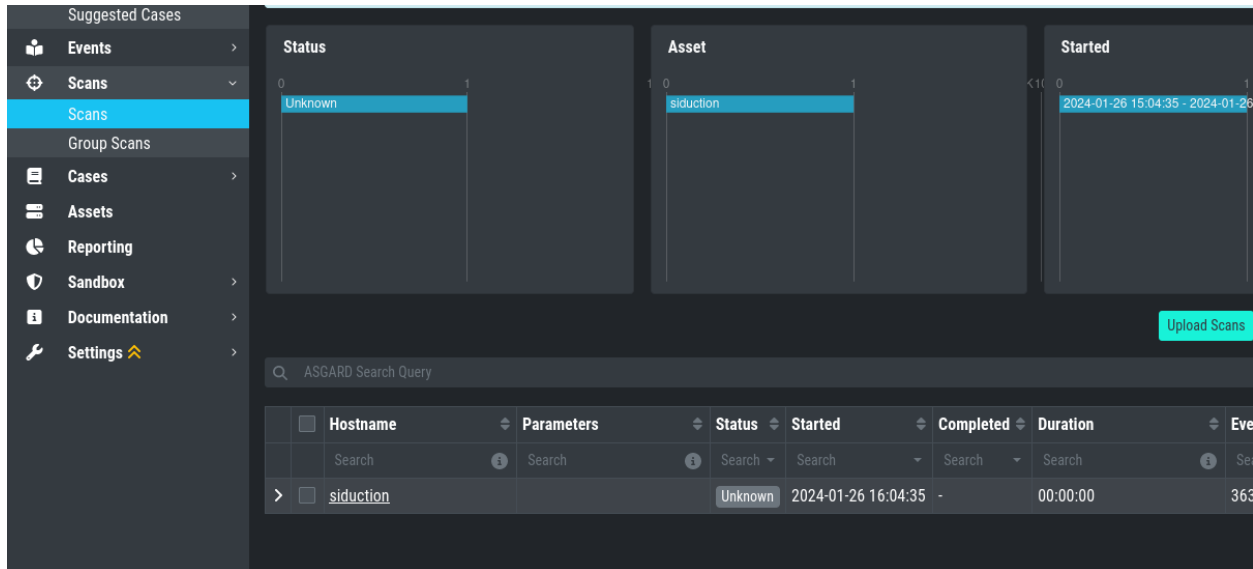
You will see a scan which has the Status **Unknown**

When you connect to your Analysis Cockpit via SSH and enter a root session, you can execute the following command to see if the error occurred on one or more log files:

```
root@analysis:# grep -R "ERROR: bufio.Scanner: token too long" /var/lib/nextron/
↳ analysiscockpit3/log
Jan 26 16:18:49 analysis analysiscockpit4[29459]: 2024-01-26T15:18:49Z [ERR] could not
↳ read events from file PATH: /var/lib/nextron/analysiscockpit3/events/upload_siduction_
↳ thor_2024-01-06.txt ERROR: bufio.Scanner: token too long
```

You should see from the above output which log had problems, which should also be reflected in the filename:

```
root@analysis:# ls /var/lib/nextron/analysiscockpit3/events
upload_siduction_thor_2024-01-06.txt.problem
```



The file has the `.problem` suffix, which indicates a problem during the import.

If you encounter this problem with one or more scan files, update your system and re-import the scans.

You can either upload them manually, or rename them by removing the `.problem` suffix in the end. They should then get correctly imported.

11.2 AAC#005: Could not get table data: Data too large

This issue is related to Elasticsearch, which stores your Analysis Cockpit's events. Elasticsearch calculates the required RAM for operations before executing them.

The below error might occur on complex searches or aggregations (e.g. for the graphs in the baselining view). To fix this issue, you have to increase the RAM of your Analysis Cockpit and reconfigure Elasticsearch to actually use more RAM.

11.2.1 AAC#005: Fix

To actually fix the problem, you have to allocate more RAM to your Analysis Cockpit. You should be able to do this via your hypervisor.

To increase heap space for Elasticsearch, edit the following configuration file on your Analysis Cockpit:

```
nextron@cockpit:~$ sudoedit /etc/elasticsearch/jvm.options.d/10-cockpit.options
```

You should see the following default values:

```
-Xms2g
-Xmx2g
```

- Xms represents the initial size of total heap space
- Xmx represents the maximum size of total heap space

The 2g part of the values indicates the heap space in gigabytes. We advise to use 50% of your system's memory for ElasticSearch. On a system with a maximum of 8 GB of RAM, this would be 4g:

```
-Xms4g
-Xmx4g
```

After you saved your changes, restart the elasticsearch service (this could take a few seconds!):

```
nexttron@cockpit:~$ sudo systemctl restart elasticsearch.service
```

Make sure the service is in active (running) state after you restarted it:

```
nexttron@cockpit:~$ sudo systemctl status elasticsearch.service
```

11.3 AAC#004: Multiple Sandbox Issues

Introduced Version	Fixed Version
<= 3.7.8	3.8.2

There are currently three issues with the sandbox integration:

1. Wrong python script capev2.py
2. Reports can't be downloaded
3. Files coming from the Bifrost Quarantine have no Name (missing)

Those issues will be fixed with the next release.

11.3.1 AAC#004: Workarounds

1. To fix the capev2.py file, contact support. We can provide you with the correct file
2. No workaround - upgrade needed
3. No workaround - upgrade needed

11.4 AAC#003: Case Management - onDelete is not defined

Introduced Version	Fixed Version
3.7.4	3.8.2

Version 3.7.4 of the Analysis Cockpit introduced a bug, which occurs when trying to edit Access rights for Case Status in the **Case Management** settings. The following error appears along with a visual bug on the right side of your browser window which says **"Retry"**:

```
Error: Error: Something went wrong
onDelete is not defined
```

There is currently no workaround for this bug, you need to upgrade to version **3.8.2 or higher** to fix this.

11.5 AAC#002: Context Deadline Exceeded

Introduced Version	Fixed Version
N/A	Ongoing

When debugging GRPC connectivity issues between your components (for example Management Center to Analysis Cockpit), you might encounter an error similar to the following one:

```

1 {
2   "LEVEL":"Warning",
3   "MESSAGE":"could not dial grpc",
4   "MODULE":"api",
5   "REQUEST_IP":"172.16.30.20",
6   "TIME":"2023-03-06T12:35:37Z",
7   "USER":"admin",
8   "error":"context deadline exceeded",
9   "host":"cockpit3.domain.local:7443"
10 }
```

11.5.1 AAC#002: Workaround

There is no workaround for this type of error. The error usually occurs because one of the following things are preventing proper communication between your components:

- Firewall is using TLS Inspection
- Proxy is using TLS Inspection
- DNS Issues

Note: Your components expect specific certificates from each other when communicating. If a device is trying to inspect TLS traffic, the certificate will change and you receive the above error.

To help you figuring out what is causing the problem, you can try the following. You can use openssl on your source system to see which certificate is presented by the destination host (change the host and port values as needed)

```

nexttron@asgard2:~$ openssl s_client -host cockpit3.domain.local -port 7443
CONNECTED(000000005)
depth=0 0 = Nextron Systems GmbH, CN = cockpit3.domain.local
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 0 = Nextron Systems GmbH, CN = cockpit3.domain.local
verify error:num=21:unable to verify the first certificate
verify return:1
write W BLOCK
---
Certificate chain
```

(continues on next page)

(continued from previous page)

```
0 s:0 = Nextron Systems GmbH, CN = cockpit3.domain.local
  i:0 = Nextron Systems GmbH, CN = Analysis Cockpit 3
---
Server certificate
-----BEGIN CERTIFICATE-----
```

The marked lines show you the certificate which is presented by the destination host. If this certificate is different from the one you installed, then the problem might be a device trying to do TLS Inspection.

We are currently working on improving the presented error message, to give a better understanding what might be the issue at hand.

11.6 AAC#001: Nested LDAP Groups not working

Introduced Version	Fixed Version
3.0.0	Open

Using nested groups in your LDAP/AD will result in no users because the query will fail.

11.6.1 AAC#001: Workaround

Change your LDAP GroupFilter to the following:

```
(&(objectCategory=group)(objectClass=group)(member:1.2.840.113556.1.4.1941:=%s))
```


MIGRATE FROM COCKPIT V2.8.X TO COCKPIT V3.X

In order to migrate an old Cockpit Version 2.x to a newly installed Cockpit 3.x proceed as follows

Make sure you have installed the latest updates.

On the command line of your Analysis Cockpit v2.x type:

```
nextron@cockpitv2:~$ sudo /etc/analysis-cockpit/ac2toac3 export -o export.ac2
```

This will create the output file `export.ac2` that will contain the entire Cockpit V2.x configuration including, users, rights, cases and case content but it WILL NOT contain any logs.

Copy the file `export.ac2` to your newly installed Cockpit v3.x.

On the command line type of your Analysis Cockpit v3.x type:

```
nextron@cockpitv3:~$ sudo /etc/analysis-cockpit/ac2toac3 import -f export.ac2
```

This will import the entire Cockpit 2.x configuration into your Cockpit V3.x.

Caution: This will overwrite your existing configuration.

Now your cockpit v3.x contains all v2.x configuration including all users, roles and cases.

As the cases also contain all grouping criteria, group IDs and rules, incoming logs will from now on be moved to the respective cases – just like your cockpit V2.x would have done.

If you also require logs to be migrated from Cockpit v2.x to your new Cockpit v3.x proceed as follows:

In ASGARD Management Center Version 2:

- Link your new Cockpit v3 to your ASGARD Management Center(s)

In Cockpit v3 navigate to Scans.

- Select the Scans you want to import into Cockpit
- Click Request Events

Events will show up in Analysis Cockpit shortly. Of course, this also works for “Group Scans”.

ASGARD Management Center Version 1:

- On ASGARD navigate to `/var/lib/bsk/asgard/log`
- **Copy and upload scan.log into Analysis Cockpit via web-based GUI (see below)**

Note: Scan.log rotates every month. Be sure to import older logs as needed.

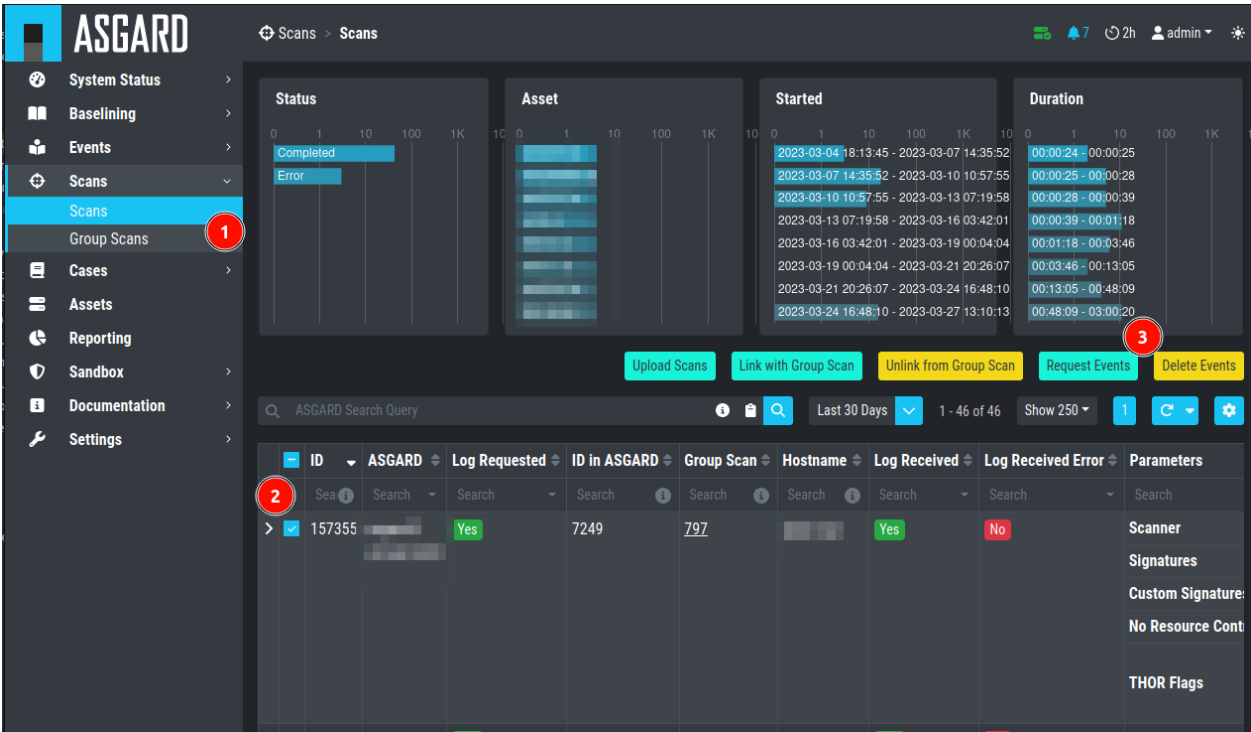


Fig. 1: Request Events from ASGARD Management Center 2.x

To import old log data, see [Log File Import](#).

GLOSSARY

13.1 Baselining

The **Baselining** section is meant to assign all unassigned events to cases, so that newly incoming events are immediately assigned to existing cases and only differences to the last scan have to be reviewed. (new malware, new signatures)

13.1.1 Auto Baselining

The Auto Baselining feature can be used to assign events to new and automatically generated cases. Auto Casing makes use of the so-called Auto Case ID, which is the same for all events of a certain type (see Glossary > Cases > Auto Case ID for details).

Auto Baselining is typically used to quickly reduce the remaining events in the Baselining section. It reduced the burden to manually group together events of a similar type.

Automatically cased events can then be reviewed in the Cases section.

Auto Baselining uses a threshold that defines the minimum number of events required in each of these automatically generated cases. A threshold of 10 instructs the process to create only cases for groups of at least 10 similar events. Obviously, we do not recommend using threshold of 1, but everything higher than 1 can be reasonable.

The best practice is to start the Auto Baselining process with a relatively high threshold (e.g., 10) and then subsequently perform iterations with lower thresholds.

13.1.2 Optimization

The Optimization is used to assign unassigned events to cases based on their filters.

Usually, an analyst selects events and creates a case with these events. During the case creation a set of filters gets generated to automatically assign newly incoming events to this case.

Often, characteristics of existing older events also align with the criteria described in the filters of the new case. However, they do not get assigned to that case, because they're already in the database and the case assignment only happens when new events arrive.

Optimization is used to assign unassigned events to existing cases.

13.2 Cases

13.2.1 Auto Case ID (formerly Group ID)

The Auto Case ID is an automatically generated ID for a group of events.

This group has been formed automatically by the use filters generated from predefined filter templates (see Glossary > Invisible > Filter Templates).

Auto Case IDs identify a groupable set of events.

The Auto Case IDs are used in case creation as the default method to assign new events to a case. You can review the Auto Case IDs used to assign new events to a case in the **Tab Grouping Criteria** of each case.

They are also used in "Auto Casing" and "Optimization". (see [Baselining](#))

13.2.2 Dynamic Auto Case ID

The Dynamic Auto Case IDs are generated for events that don't have a corresponding filter template defined. This is often the case for very rare event types or events of a low level (Info, Notice).

You can think of them as a fallback in form of a less efficient grouping method.

They are usually created of all fields of an event except the ones that are highly specific, like the HOSTNAME field.

If your case uses many Dynamic Auto Case IDs, distinguishable by the leading uppercase "D", then automatic event assignment is nearly impossible. In these cases, you should rather use a string conditions to group events into that case and assign new incoming events automatically.

13.2.3 Filter Priority

It is possible that two or more cases include filters that would assign a new incoming event to them. This often happens when one case uses Auto Case ID (see Glossary section) and another case uses a string selection (String Condition).

The filter priority can be used to prioritize the filters of a case so that newly incoming events go to that prioritized case and not the one with the default priority.

You could also create fallback cases, e.g., for all events of the level "Notice" and intentionally reduce the priority of this case so that other cases that select events of that level always come first.

The full prioritization process looks like:

- Case with higher priority takes the event
- If both cases have the same priority, the case with the higher "Type" takes the event (Incident > Noteworthy)
- If both cases have the same priority and the same type, the case with the smaller case ID (older case) takes the events

13.2.4 External ID

This field is optional and can be used to refer to an ID that you use in a different system, like a ticket management system or an incident response platform.

13.2.5 Difference between Summary and Assessment

The field **Summary** is meant to include the elements (fields) of events that are used as characteristics to perform an assessment. You can think of it as the values that you as an analyst want to highlight for other analysts that review that specific case. It's often a special file name and location or a process name and YARA rule match on that process.

You can use the "Auto Summary" feature to get an auto-recommended content for this field.

The field **Assessment** is the one that requires the most effort. It contains the findings of the analyst's review.

13.2.6 Case Types

The following table describes the cases types taxonomy used in Analysis Cockpit.

Type	Description
Incident	Incident cases report a clear threat, indicated by a hard match and verified by research of an analyst. Analysts create incident cases to indicate the highest possible certainty and risk. Incident cases are also characterized by the fact that they do not need to be verified by someone else. They either indicate malware, a threat group or penetration testing activity and should trigger immediate response.
Suspicious	Suspicious cases are based on significant indicators that require a review by someone within the organization or more evidence to come to a final conclusion. Often, file samples or process memory dumps are required to verify/falsify a verdict. Cases of this type usually trigger evidence collection or review actions.
Noteworthy	Noteworthy cases are based on soft indicators or elements that should be reviewed whenever there is time to do that. They include all kinds of events that cannot be dismissed as false positives or anomalies but are likely uncritical. Noteworthy cases don't trigger an immediate response but should be reviewed whenever there is time to do that.
Vulnerability	Vulnerability cases contain detected software or configuration weaknesses that compromise system integrity. The reported vulnerabilities often include easy to exploit weaknesses that are frequently used by threat groups to execute code remotely, gain access or escalate privileges on affected systems. Cases classified as Vulnerability are typically integrated into a vulnerability management process as an additional input channel.
Legitimate Anomaly	Legitimate Anomaly cases contain events that are related to legitimate elements that are suspicious, but an ordinary finding in the context of the analyzed organization. The reason for an anomaly is not a malfunction of the scanner but a peculiarity within the analyzed environment. Legitimate Anomalies don't trigger any further activity.
False Positive	False Positive cases contain events that indicate suspicious or malicious activity, but the review revealed that it is actually legitimate software or other elements. The only reason for a false positive is a scanner malfunction or signatures that falsely report a threat (see section <i>Difference between False Positive and Legitimate Anomaly</i> for details). A false positive usually triggers a review by Nextron Systems and a signature adjustment.
Unknown	The default state of newly created cases.

13.2.7 Difference between False Positive and Legitimate Anomaly

We use "False Positive" and "Legitimate Anomaly" to distinguish between situations in which the scanner (THOR) made an error and situations in which a customer environment contains suspicious or malicious elements that are known.

E.g., a Winrar used by admins as `r.exe` in `C:\users\public` for software rollout purposes is not considered a "False Positive" but a "Legitimate Anomaly". It is a finding which doesn't have to be fixed in THOR's signature set but is simply a specific situation in the analyzed environment.

Matches that are clearly an error in THOR signatures should be classified as "False Positive".

Examples for "Legitimate Anomalies":

- Procdump.exe findings
- Suspicious RUN Key entries that use customer software
- Custom software that uses suspicious folders, e.g. `C:\Users\Public,%AppData%`
- Process memory match with a "ReflectiveLoader" YARA rule on a third party EDR agent process

Examples for "False Positives":

- YARA rule match on Bloomberg or SAP software
- Filename IOC match `w64.exe` on a Perl for Windows build tool
- YARA rule match with "Putty_Anomaly" on a legitimate and signed `putty.exe`

Another good example is one of the many anomaly signatures that triggers on an XORed MS-DOS Stub. A match with such a signature only qualifies as false positives when there is no XORed MS-DOS stub in that file and not when it turns out to be a legitimate file. The signature detects what it is designed to detect.

A signature with a rule named `MAL_Xrat_Mar21_1` that triggers on a legitimate and signed executable, however, is a false positive.

13.3 Invisible (Backend)

13.3.1 Filter Templates

The Analysis Cockpit uses so-called filter templates that describe which fields in which event types are specific enough to be used in a filter that can be used to automatically group events.

These groups can be identified by a common so-called "Auto Case ID" (formerly Group ID). See the respective entry in this Glossary.

The filter templates are static and predefined.

E.g., a typical filter template states that for events in the Module `Filescan`, the fields **FILE** and **SHA1** are sufficiently specific to group events based on equal values in these two fields.

CHANGELOG

This chapter contains all the changes of the ASGARD Analysis Cockpit.

14.1 Analysis Cockpit 3.10

14.1.1 Analysis Cockpit 3.10.3

Release Date
Fri, 26 Jan 2024 17:18:00 +0200

Type	Description
Bugfix	Fixed import of THOR logfiles with very long lines
Feature	Configure max. line length for THOR logfiles

14.1.2 Analysis Cockpit 3.10.1

Release Date
Mon, 20 Nov 2023 08:37:00 +0200

Type	Description
Major	Prepare for Debian 12 Upgrade

14.2 Analysis Cockpit 3.8

14.2.1 Analysis Cockpit 3.8.5

Release Date
Thu, 28 Sep 2023 15:03:00 +0200

Type	Description
Bugfix	Fixed synchronization issues between Management Center and Analysis Cockpit caused by Bifrost file collection

14.2.2 Analysis Cockpit 3.8.4

Release Date
Thu, 17 Aug 2023 09:49:00 +0200

Type	Description
Feature	Synchronize Aurora Agent cases and events with Security Center
Feature	Synchronize deleted assets with Management Center, hide deleted assets per default
Feature	Reconnect Management Center
Feature	Added uuids for scans, cases and more
Security	OS Security Fix
Bugfix	Removed auto_case_id template for Eventlog/EVTX that caused event assignments solely by Event ID causing unwanted assignments. The template was removed. New events of the affected type will be shown in the baselining section once they are identified again.
Bugfix	Fixed issues with syslog receiver
Bugfix	Fixed smtp login issues with some smtp servers
Bugfix	Fixed issues with create case / add to case for LogWatcher events
Bugfix	Fixed download issues with sandbox reports
Bugfix	Fixed corrupt CapeV2 sandbox connector script
Bugfix	Fixed asset label deletion via Management Center
Bugfix	Fixed some missing meta columns in event table
Bugfix	Fixed missing VirusTotal link for some SHA256/SHA1
Bugfix	Fixed "no results" in some tables when applying filters during pagination
Bugfix	Fixed missing 'Show matching assets' and 'Show matching cases' in events table

14.3 Analysis Cockpit 3.7

14.3.1 Analysis Cockpit 3.7.8

Release Date
Fri, 14 Apr 2023 10:42:00 +0200

Type	Description
Bugfix	Fixed non-working "add role case status"
Bugfix	Fixed issues with LogWatcher cases

14.3.2 Analysis Cockpit 3.7.7

Release Date
Wed, 29 Mar 2023 10:18:00 +0200

Type	Description
Change	Decreased file size and rotation config of assignment log
Change	Improved ip ban config
Bugfix	Fixed missing LogWatcher section
Bugfix	Fixed missing upgrade available indicator

14.3.3 Analysis Cockpit 3.7.4

Important: This release completely refactored the UI. The old API endpoints will still be supported.

Release Date
Fri, 17 Mar 2023 16:18:00 +0100

Type	Description
Feature	Suggested Cases
Feature	Guided Baselining
Feature	Added more aggressive Auto Case IDs that can be used to detect bigger groups of similar events
Feature	Configure number of graphs and number of entries per graph
Feature	Resolve Auto Case IDs in graphs
Feature	Switch between light and dark mode
Feature	Added 'ASGARD Search Query' to most tables
Feature	Select an assessment based on your previous assessments
Feature	Highlight favorite fields in event table
Feature	Added new context menu when right-clicking on events, can be used to create fast filters, cases and more.
Feature	Added baselining count per asset
Feature	Added detailed event field view containing the top 1000 and rarest 1000 values of the selected field
Feature	Send automated YARA rule feedback to Nextron Systems (disabled per default, can be enabled in UI)
Feature	Automatically run an Baselining Optimize in background once per day (disabled per default, can be enabled in UI)
Feature	Delete users
Feature	Added Cape v2 sandbox connector
Feature	Automatically block ip for a few minutes on many bad requests / login requests
Change	Improved our engine for generating Auto Case IDs
Change	Completely refactored UI
Bugfix	Fixed non-working asset label filter in timeframe-based reports
Bugfix	Reduced occurrence of "trying to create too many scroll contexts" error
Bugfix	Fixed corrupt 'To:' mail header in some notification mails
Bugfix	Fixed missing ntp restrictions in ntp config

14.4 Analysis Cockpit 3.5

14.4.1 Analysis Cockpit 3.5.6

Release Date
Tue, 23 Aug 2022 14:28:00 +0200

Type	Description
Feature	Baselining Modes 'Compromise Assessment' and 'Deep Inspection'
Feature	UUID for assets that are synchronized from ASGARD Management Center
Feature	Label events with the asset's labels
Change	Hide static search bubbles
Change	Load total count of baselining events in background to improve ui performance
Bugfix	Fixed non-working counter links in additional key value information
Bugfix	Fixed non-working sync between Management Center and Analysis Cockpit due to very large Bifrost quarantine files
Bugfix	Fixed non-working last seen filter in asset table

14.5 Analysis Cockpit 3.4

14.5.1 Analysis Cockpit 3.4.7

Release Date
Mon, 30 May 2022 11:30:00 +0200

Type	Description
Security	OS Security Fix

14.5.2 Analysis Cockpit 3.4.6

Release Date
Thu, 17 May 2022 10:09:00 +0200

Type	Description
Feature (Beta)	use Elasticsearch clusters instead of single-node setup
	script to add Elasticsearch cluster nodes
	script to configure number of replicas for each index
	check Elasticsearch status before API calls
	improved Elasticsearch error detection (disallow searches when shards are down)
	automatic update while installing cluster nodes
Fix	improved Active Directory support in ldap configuration
Fix	collect individual bulk indexer errors and report on close
Fix	remove unused kernel versions from boot partition
Change	use file timestamp when loading events from events directory

14.6 Analysis Cockpit 3.3

14.6.1 Analysis Cockpit 3.3.7

Release Date
Thu, 17 Feb 2022 12:09:00 +0200

Type	Description
Bugfix	Fixed a bug in 'add to case' by similar case name

14.6.2 Analysis Cockpit 3.3.6

Important: The previous update routine interrupted some case assignments. Use of Optimize function after the update is recommended.

Release Date
Fri, 11 Feb 2022 09:30:00 +0200

Type	Description
Bugfix	Fixed a bug in the update routine

14.6.3 Analysis Cockpit 3.3.5

Release Date
Tue, 8 Feb 2022 09:01:00 +0200

Type	Description
Feature	Aurora Support
Feature	Add comment to assets
Feature	Custom labels for assets
Feature	Download reports as yaml
Change	Assigned each case to a scanner / agent, e.g. THOR, Aurora, LogWatcher
Bugfix	Fixed a bug in the condition engine in combination with merged cases
Bugfix	Fixed a bug that caused some cases to break case priority
Bugfix	Fixed escaping of ldap usernames with special characters
Bugfix	Fixed 'too many scroll contexts' error, when creating large regex cases
Bugfix	Fixed non-working 'add filter' button in group scans section
Bugfix	Fixed ntp configuration

14.7 Analysis Cockpit 3.2

14.7.1 Analysis Cockpit 3.2.2

Release Date
Thu, 28 Oct 2021 14:23:00 +0200

Type	Description
Feature	Merge Cases
Feature	Import statistics on overview page
Change	Separate events in baselining and event view between THOR- and Log Watcher events
Bugfix	Fixed recommendations and custom recommendations in csv export
Bugfix	Fixed a bug in the condition engine that caused some events to not match the specific condition in rare cases

14.8 Analysis Cockpit 3.1

14.8.1 Analysis Cockpit 3.1.5

Release Date
Thu, 16 Sep 2021 11:49:00 +0200

Type	Description
Bugfix	Fixed a bug in the new condition engine that caused some events to not match the specified condition in rare cases.

14.8.2 Analysis Cockpit 3.1.4

Release Date
Wed, 21 Jul 2021 11:13:00 +0200

Type	Description
Security	OS Security Fix

14.8.3 Analysis Cockpit 3.1.3

Release Date
Fri, 2 Jul 2021 14:29:00 +0200

Type	Description
Feature	Added support for new ASGARD Security Center
Change	Regenerated TLS certificate with SAN extension for ASGARD Management Center synchronization
Change	Toggle between "show" and "hide" additional asset information in asset table to improve performance
Change	Cosmetics and wordings
Change	Highly reduced length of server-side table urls due to issues with older browsers and reverse proxies
Bugfix	Fixed non-working text highlighting in some table cells (also text highlighting will not trigger a click event anymore)
Bugfix	Allow import of .log files in scan section

14.9 Analysis Cockpit 3.0

14.9.1 Analysis Cockpit 3.0.4

Release Date
Mon, 7 Jun 2021 09:09:00 +0200

Type	Description
Bugfix	Fixed an issue that caused synchronization of Log Watcher events to not work anymore in specific cases
Bugfix	Fixed "trying to create too many scroll contexts" error that sporadically occurred during case creation or regex testing

14.9.2 Analysis Cockpit 3.0.2

Release Date
Thu, 6 May 2021 09:14:00 +0200

Type	Description
Feature	Added new "similar cases" feature in Add Case form
Feature	Added pagination to additional asset information
Change	Improved API documentation
Change	Refactored condition engine to be more performant in some cases
Change	Cosmetics
Bugfix	Fixed missing events of some scans that were collected by an additional "log collection" job
Bugfix	Fixed default values in cuckoo config
Bugfix	Fixed missing MATCH_STRINGS field in the search bar
Bugfix	Removing events from a case caused the scan- and asset table of this case to be inconsistent for a few hours

14.9.3 Analysis Cockpit 3.0.0

Release Date
Fri, 19 Mar 2021 09:52:00 +0200

Type	Description
Major Release	Initial release

14.10 Analysis Cockpit 3.0 unstable

14.10.1 Analysis Cockpit 3.0.0~pre+20210319.0

Release Date
Fri, 19 Mar 2021 09:36:00 +0200

Type	Description
Change	Renamed ASGARD's new Log Scanner to Log Watcher

14.10.2 Analysis Cockpit 3.0.0~pre+20210315.0

Release Date
Mon, 15 Mar 2021 10:22:00 +0200

Type	Description
Bugfix	Fixed corrupt case-insensitive search for 'contains' search
Bugfix	Increased ~tls certificate validity (between ASGARD and Analysis Cockpit)

14.10.3 Analysis Cockpit 3.0.0~pre+20210309.1

Release Date
Tue, 9 Mar 2021 11:28:00 +0200

Type	Description
Feature	Support Eventlog Scanner

14.10.4 Analysis Cockpit 3.0.0~pre+20210308.1

Release Date
Fri, 5 Mar 2021 08:42:00 +0200

Type	Description
Feature	New column 'last scan completed' per asset
Security	Fixed smaller security issues (Added more CSP headers, added logout headers, improved yaml decoder, jquery upgrade, ..)

14.10.5 Analysis Cockpit 3.0.0~pre+20210305.1

Release Date
Fri, 5 Mar 2021 08:42:00 +0200

Type	Description
Feature	Receive additional asset information from ASGARD, e.g. installed software, local users, ...
Feature	Request THOR logs of group scan from ASGARD
Feature	Create empty case (in Case Management)
Change	Added THOR key whitelisting - Only known THOR keys will be parsed from THOR events and added to ElasticSearch
Change	The collapse button in the Baselining / All Events section will only collapse the timeline and keep all bar charts expanded
Change	Cosmetics
Change	Updated templates in filter engine
Bugfix	Added timeout for LDAP requests
Bugfix	Fixed noteworthy cases of group scans in suspicious cases column
Bugfix	Fixed missing grouping criteria for initial cases

14.10.6 Analysis Cockpit 3.0.0~pre+20210222.0

Release Date
Mon, 22 Feb 2021 08:55:00 +0200

Type	Description
Change	Updated min. TLS version and TLS cipher suites
Bugfix	Automatically reconnect to LDAP server on broken pipe
Bugfix	Fixed CSRF protection
Bugfix	Do not show 'undefined' in some cells in Baselining- and All Events Section
Bugfix	Fixed corrupt 'continue' button in 'Your session will expire soon' popup

14.10.7 Analysis Cockpit 3.0.0~pre+20210218.0

Release Date
Thu, 18 Feb 2021 10:13:00 +0200

Type	Description
Change	Improved performance
Bugfix	Fixed corrupt GUI notification table

14.10.8 Analysis Cockpit 3.0.0~pre+20210212.0

Release Date
Fri, 12 Feb 2021 11:35:00 +0200

Type	Description
Bugfix	Some newly created cases had corrupt grouping criteria. This release will remove all automatically assigned events from the affected cases and reassign them with an automatically started Optimize. There might be more events in the Baselining section after this upgrade due to events that were accidentally assigned to a case before.

14.10.9 Analysis Cockpit 3.0.0~pre+20210205.0

Release Date
Fri, 5 Feb 2021 09:12:00 +0200

Type	Description
Bugfix	Increased limit of total fields in Elasticsearch from 1000 to 8000

14.10.10 Analysis Cockpit 3.0.0~pre+20210204.0

Release Date
Thu, 4 Feb 2021 10:29:00 +0200

Type	Description
Feature	Auto-Resize for some textareas, e.g. Summary, Assessment, Comment
Feature	Bulk Delete Cases
Feature	Added hide button to additionally loaded event information
Feature	Made 'Events Assigned' clickable in 'Optimize' section to show all events that were assigned in the current optimize run
Change	Automatically focus inputs in some popups
Change	Allow 'Shift + Click' for negated search, too (instead of 'Alt + Click')
Change	Improved performance of 'Remove Events from Case'
Change	Added VirusTotal URL to MD5 and SHA1, too
Change	Improved MOTD config
Change	Increased time-based default filters from 'Last 7 Days' to 'Last 30 Days'
Change	Truncated summary in case table
Change	Sort users by user name instead of creation date
Bugfix	Fixed corrupt generation of conditions based on current query
Bugfix	Fixed reduction of multiple whitespaces to one whitespace of THOR events in GUI (caused some filters to not work)

14.10.11 Analysis Cockpit 3.0.0~pre+20210203.1

Release Date
Wed, 3 Feb 2021 08:11:00 +0200

Type	Description
Bugfix	Removing events from condition cases caused them to be corrupt until reboot
Bugfix	Fixed typo in filter engine
Bugfix	Fixed security issues with LDAP

14.10.12 Analysis Cockpit 3.0.0~pre+20210201.1

Release Date
Mon, 1 Feb 2021 08:59:00 +0200

Type	Description
Feature	Persistent page length per section per user
Feature	Completely refactored the 'Create Case' dialog
Feature	Remove events from case
Feature	Added Log Analysis Guide and THOR Manual to downloads section
Feature	Favorite Fields per user in event section
Feature	Persistent time range filter in event-, asset- and scan section
Feature	Resolve asset- and case ids in event details to hostname and case name
Feature	New button 'Valhalla' in event detail fields that contain a YARA rule name that will lookup the rule in Valhalla
Feature	Backup configuration (cases, grouping criteria, users, ...) and Restore on a fresh Analysis Cockpit
Feature	Replaced all graphs in several sections with horizontal bar charts
Feature	Added 'Download Sandbox Sample' button in sandbox samples table
Feature	Added 'Origin' column in sandbox samples table
Change	Removed 'Close' button from all dialogs
Change	Cosmetics
Change	Wordings
Change	Added more tooltips
Change	Sort by score in baselining section and by timestamp in event section
Change	Added refresh button in report section
Change	Prevent users from creating duplicate bubble filters
Change	Files that could not be imported will now be rotated to .problem
Change	Highly improved performance of case creation and condition tests based on condition
Change	Added more configurable LDAP settings
Bugfix	Fixed corrupt search for integers in ElasticSearch
Bugfix	Redirect to case table if case detail page was opened without case id in URL
Bugfix	Fixed corrupt mysql config that occurs on >30 GB systems due to a wrong installation script
Bugfix	Fixed wrong scan duration in scan table
Bugfix	Removed revise of THOR events in import procedure that added fields that do not exist in original event, e.g. BASENAME

14.10.13 Analysis Cockpit 3.0.0~pre+20210121.2

Release Date
Thu, 21 Jan 2021 15:45:00 +0200

Type	Description
Feature	Two Factor Authentication
Feature	New filter bar in baselining and event section
Feature	New icon in aggregation graphs that counts unique values
Feature	Added progress bar for optimizer
Feature	Add comments to cases in 'Create Case', 'Add to Case', 'Update Case' and 'Bulk Update Case' dialogs
Feature	Auto-Summary in 'Create Case' dialog
Change	Improved column visibility selection
Change	Added 'Notification Name' to notifications table
Change	Cosmetics
Change	Wordings
Bugfix	Restrict users to create or change 'Open' or 'Closed' case status in settings section
Bugfix	Fixed ntp configuration issues
Bugfix	'equals' and 'not equals' searches in baselining and event section are now case insensitive
Bugfix	Added 'Disabled' column in user table
Bugfix	Added 'Unknown' to scan status selection

14.10.14 Analysis Cockpit 3.0.0~pre+20210118.2

Release Date
Mon, 18 Jan 2021 15:28:00 +0200

Type	Description
Change	Improved performance of THOR events import
Bugfix	Add group ids of manually added events to case engine
Bugfix	Fixed assignment of events to already deleted cases
Bugfix	Fixed wrong suspicious cases count of scans in scan table
Bugfix	Fixed wrong include path in rsyslog config for port 514 listener
Bugfix	Fixed upgrade via GUI

14.10.15 Analysis Cockpit 3.0.0~pre+20210114.0

Release Date
Thu, 14 Jan 2021 06:40:00 +0200

Type	Description
Bugfix	Fixed wrong API base path for Update section
Bugfix	LDAP Fixes
Bugfix	Fixed typo in case assignment engine for THOR's "ProcessCheck" module
Bugfix	Added missing dependency

14.10.16 Analysis Cockpit 3.0.0~pre+20201207.1

Release Date
Mon, 7 Dec 2020 13:13:00 +0200

Type	Description
Beta release	

INDICES AND TABLES

- search