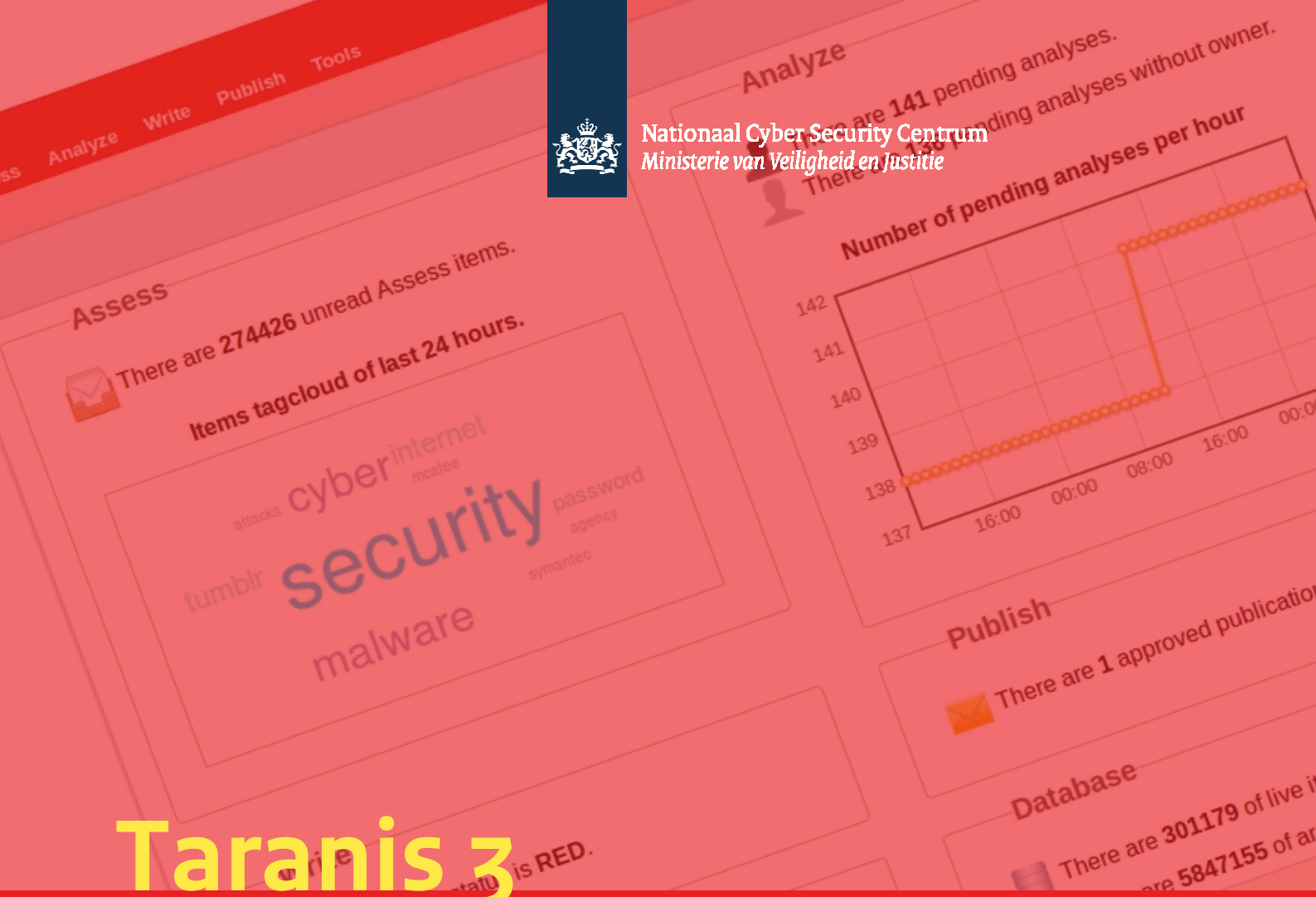


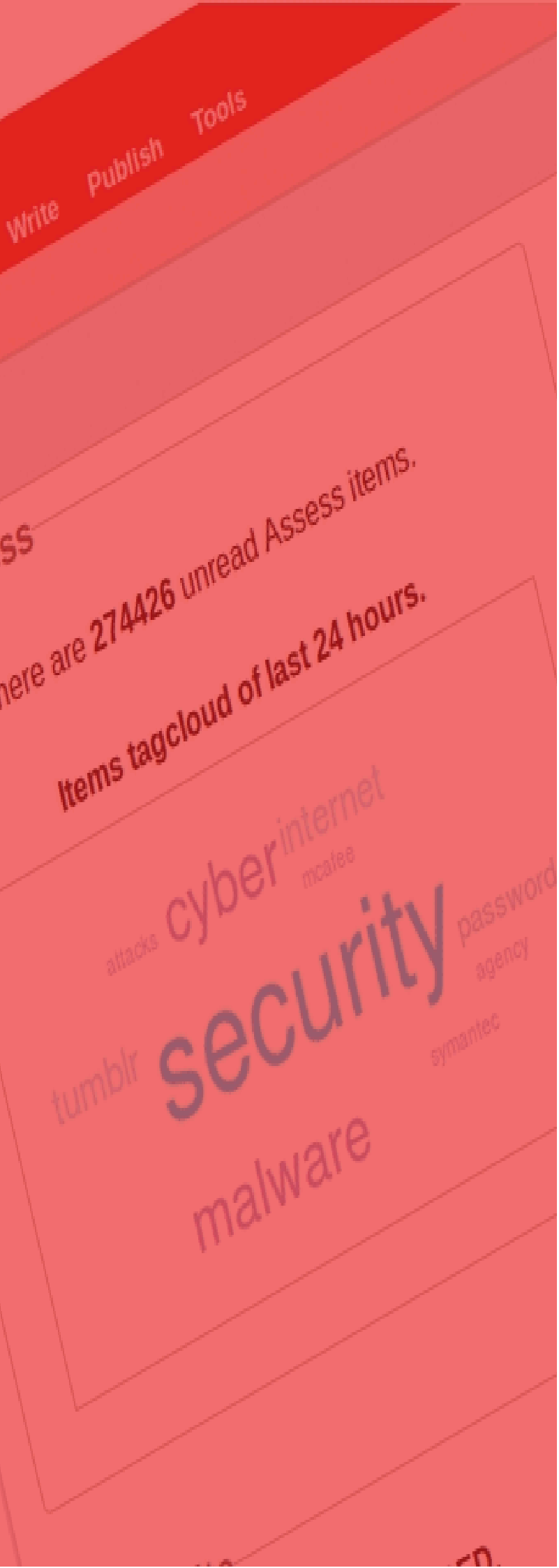
Taranis 3

Taranis 3.3.3 Release Notes

Taranis 3

Taranis 3.3.3 Release Notes

National Cyber Security Centre
Turfmarkt 147 | 2511 DP The Hague
PO box 117 | 2501 CC The Hague
T +31 70 751 55 55 | F +31 70 888 75 50
www.ncsc.nl | info@ncsc.nl



Index

1 New features and enhancements

Taranis 3.3.3 is the successor to version 3.1.2 and this new version contains a lot of new features and enhancements. This chapter describes these new features and enhancements shortly. For a complete overview, please consult the Taranis 3.3.3 user and administration guides.

1.1 New tool: Feed Digest

Taranis contains a new tool called "Feed Digest". This tool allows you to send out daily automated email updates based on the contents of one or more XML-based feeds. You can influence the look and feel of these emails based on a template that you can define. It's possible to send out both text-based and HTML-based emails.

1.2 Screenshot functionality

Screenshot functionality was added to Taranis and is used in multiple Taranis functions. Formerly, you could only add a new source to Taranis after which Taranis would put hyperlinks to new items from this source in the database. You can now choose to not only place a link to resulting web based items in the database but also a screenshot of resulting items. This means that if you have a possible malicious website, users will not automatically be redirected to these websites but will be shown a screenshot of the website instead after clicking on the link in Taranis.

This screenshot functionality is also incorporated into the Phishing Checker tool. Every time the contents of a phishing website changes, the Phishing Checker will take a screenshot of the current status so that you'll have a good overview of the history of such a site.

Finally, screenshot functionality is also part of the new Dossier-functionality that was added to this version of Taranis.

1.3 Collector enhancements

Quite a few changes were made to the Collector component. First of all, it's now possible to add multiple Collector instances to one Taranis installation. This allows you e.g. to collect information over different physical networks. The Collector can be placed on a separate machine and doesn't need to be on the Taranis main server anymore. You must connect every source to one of the collectors that you've defined.

Next to that, the Collector is now multi-threaded. This improves the performance of the Collector drastically and allows you to check a lot more sources within the same timeframe.

It is now also possible to create a custom collector module. This is especially useful for hard to parse sites or sites that have a public API for accessing content, like Twitter.
Please see Twitter.pm and TemplateModule.pm in /opt/taranis/pm/Taranis/Collector/ for creating your own collector modules.

The Collector now supports a Minimum Time Between Checks (MTBC) and a random delay. This makes retrieving sources look more random.

Lastly the collector will send a notification if the collector fails to finish 2 or more times during last 4 runs.

1.4 Wordlists

Taranis now supports the use of wordlists in combination with your sources. Several users of Taranis requested this functionality that will allow you to add more sources and only see resulting items that are of interest to you based on standard wordlists. This way you can add a source that results in a lot of items and only see the items that contain a specific keyword (or combination of keywords) that you're interested in. All items that do *not* match these keywords will still be inserted into the Taranis database but are automatically set to "read". This way you can still look these items up through Taranis, but your operational process will not be "polluted" with irrelevant items.

1.5 Extensive user actions logging

Transparency of user actions is greatly improved by logging more types of user actions (e.g. creation of an analysis, linking to an analysis, editing of products, bad login attempts, etc.). The actions can only be seen by Taranis administrators and help these administrators in

finding out who performed a specific action at what time. The latest user activity is shown on the Dashboard. A history of user actions can be requested through the "User actions logging" option on the Taranis configuration page.

1.6 Changes to the dashboard

The Taranis dashboard now also shows the current user activity (user actions) if the logged-in user is allowed to see that information. The Collect-graphs have been adjusted to accommodate more collectors all reporting to the same Taranis instance (see 1.3).

New settings were added to taranis.conf.dashboard.xml to allow you to further configure the Assess-information on the dashboard. Through the settings you can now control:

- The news categories to be included in the tag cloud.
- The news categories to be included to calculate the number of unread items.

Icons on minified dashboard are clickable and have been expanded with icons for indicating the oldest unread assess item.

1.7 Dossier functionality

The existing "Analyze" functionality of Taranis is ideal for issues with a short turnaround time. However we found that this functionality is less suitable for issues with a much longer turnaround time. That's why we introduced the Dossier functionality in this new version of Taranis. The dossier functionality allows you to group different types of information (items, analyses, products, etc) into one dossier. By connecting tags to your dossiers you can automatically get hints of new items for dossier when another user adds such a tag to e.g. a news item.

1.8 Advisory forward

Next to advisories, Taranis now also supports advisory *forwards*. With advisory forwards, it's possible to use an advisory from a source as is and then add some metadata to it before sending it out to your constituents. This functionality is aimed at security teams that don't want to write a full advisory but instead want to inform their constituents based on external advisories.

1.9 Rebranding of End-of-Shift to End-of-Day and new End-of-Shift

The End-of-Shift publication has been rebranded to End-of-Day to make way for a new End-of-Shift.
With the new End-of-Shift comes the new Report functionality which is the bases for content of the End-of-Shift.
With Report handlers can log incidents and contact information during their shift. These log entries can be added to the End-of-Shift automatically.
Besides logging functionality users can add to-dos and 'special interests' during their shift.
Optionally, an End-of-Shift can be sent automatically with the added report.pl backend tool.

1.10 BigScreen revised

The BigScreen has been rewritten to accommodate several feature requests:

- Easier customization options
- No log-in required / or alternative means for authentication
- Stand-alone-usage (run on separate server)
- Possibility to view one page with auto-refresh capabilities.

To make the stand-alone-usage feature request possible Taranis has been expanded with RESTful interface.

1.11 Further CVE integration

CVE descriptions can now be viewed and translated in Taranis Configuration → 'Other configuration'.
The translations can be created with the usage of CVE templates.
The created translations can be used in advisories as templates.

1.12 Documentation enhancements

The documentation of Taranis is updated to contain a description of all new functionalities. A new guide called the "Taranis 3.3.3 Administration Guide" has been added to describe functionalities specifically aimed at technical and functional administrators of Taranis. Formerly this information was part of the Taranis User Guide but multiple users of Taranis informed us that this made the user guide too complex. The User Guide is now specifically aimed at end users and all information related to the

administration of Taranis is transferred into the Administration Guide.

1.13 Security enhancements

We have implemented a number of security enhancements in Taranis and fixed a number of security issues. Taranis now has CSRF protection and cryptographically secure session tokens.

User passwords were formerly hashed based on MD5. Because this is a weak hashing algorithm, passwords are now salted hashes based on the SHA-512 algorithm. Passwords are automatically rehashed for every user logging in to this new version of Taranis.

The Collector now refuses to connect with servers that present an invalid certificate when retrieving HTTPS or IMAPS sources.

Thanks to Dirk van Veen from The S-Unit for reporting a SQL injection vulnerability!

1.14 Miscellaneous

Following is a list of small features added to this new version of Taranis:

- Analysis statuses can now be sorted based on configuration. This way you can influence the default status you want to present to the user when e.g. creating a new analysis.
- When adding a news item to the End-of-Day (EoD), you now also have the option to add it to the "Community News" section of the EoD. In previous versions of Taranis you could only link to "Vulnerabilities and Threats" and "Media Exposure".
- Because tags get more important if you decide to use the new Dossier functionality, it's now easier to add new tags by using the new tag icon next to e.g. analyses and products.
- The Phishing Checker now supports the use of ticket numbers and campaign description with every phishing website you add. This eases the process of correlating a Phishing Checking alert with an incident in your incident tracking system.
- The Phishing Checker GUI now has an auto-refresh option and column sorting.
- Searching through e.g. items and advisories based on date is now simplified. If you leave the "from" or "to" date in your search empty, Taranis will now consider this as infinite (in previous versions these fields were both required and could not be left empty).
- Some IMAPS servers require the use of STARTTLS before setting up an encrypted session. Sending STARTTLS is now added as an optional extra during the definition of an (IMAPS-)source.
- The data type for constituent phone numbers was changed from INT to TEXT in order to support the usage of phone numbers starting with '+'.
- When sending out an End-of-Week, the current date is now automatically added to the subject of the mail.
- Advisories can now be searched through based on probability and/or damage rating and 'only search products in use'.
- Advisory preview has been expanded with a tab with selected software/hardware.
- A rating of sources can be set, which will result to assess items from higher rated sources being put at the top of the list.
- PostgreSQL SSL mode can be set in main config file (dbsslmode).
- Keyboard shortcuts have been added to the Assess page.
- The width of Taranis GUI can be set in main config file (screen_width).
- F5 page refresh has been restored and will not return to dashboard but refreshes the current page.
- The header of Taranis can now be customized with the banner_html configuration option.
- It is now possible to run Taranis outside /opt/taranis, making it possible to run multiple Taranis instances on the same host.
- The notbefore and notafter configuration options have been removed. Use crontab instead to determine when the collector should run.
- Browsing through the Taranis web interface is simplified by the support of the "Back" button.

1.15 Bugfixes

In addition to the new features, many small bugs were fixed. See the CHANGES file for a list.

2 Installation

2.1 How to get Taranis 3.3.3

Taranis 3.3.3 is distributed through the Taranis download server of NCSC-NL. The download server can be found at: https:// 147.181.97.149/.

Mind that the server contains a self-signed certificate. Your browser will show you a message indicating that the certificate is not trusted. On the server, you will find a set of install files and accompanying documentation.

To access this server you need a valid username/password combination. Should you not have these credentials, please send your request for access to the Taranis download server to info@ncsc.nl.

2.2 How to upgrade your installation

If you are already using an older version of Taranis you can upgrade your version to 3.3.3. If you're currently using Taranis 3.1.X you can upgrade to 3.3.3 directly. See the Taranis 3.3.3 Migration Guide on the steps you have to take to update to 3.3.3. If you're using an older version of Taranis (pre 3.1.X) you first have to upgrade your Taranis installation one version at the time (e.g. from 2.2.0 to 3.0.0, then from 3.0.0 to 3.1.0 and finally from 3.1.0 to 3.3.3). Please contact us on info@ncsc.nl for more information should that be the case.

2.3 How to do a clean installation

In case you're not currently running a version of Taranis or don't mind losing the information in your current installation, you can choose to do a clean installation of Taranis. We offer installation guides for the installation of Taranis on Ubuntu (16.04 LTS) and CentOS (7). These two guides should help you install Taranis on these Linux-distributions as well as on related distributions like Debian, Red Hat and Fedora Linux. «