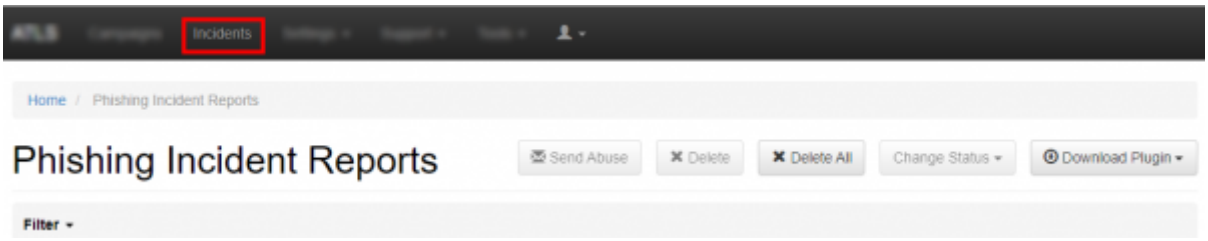
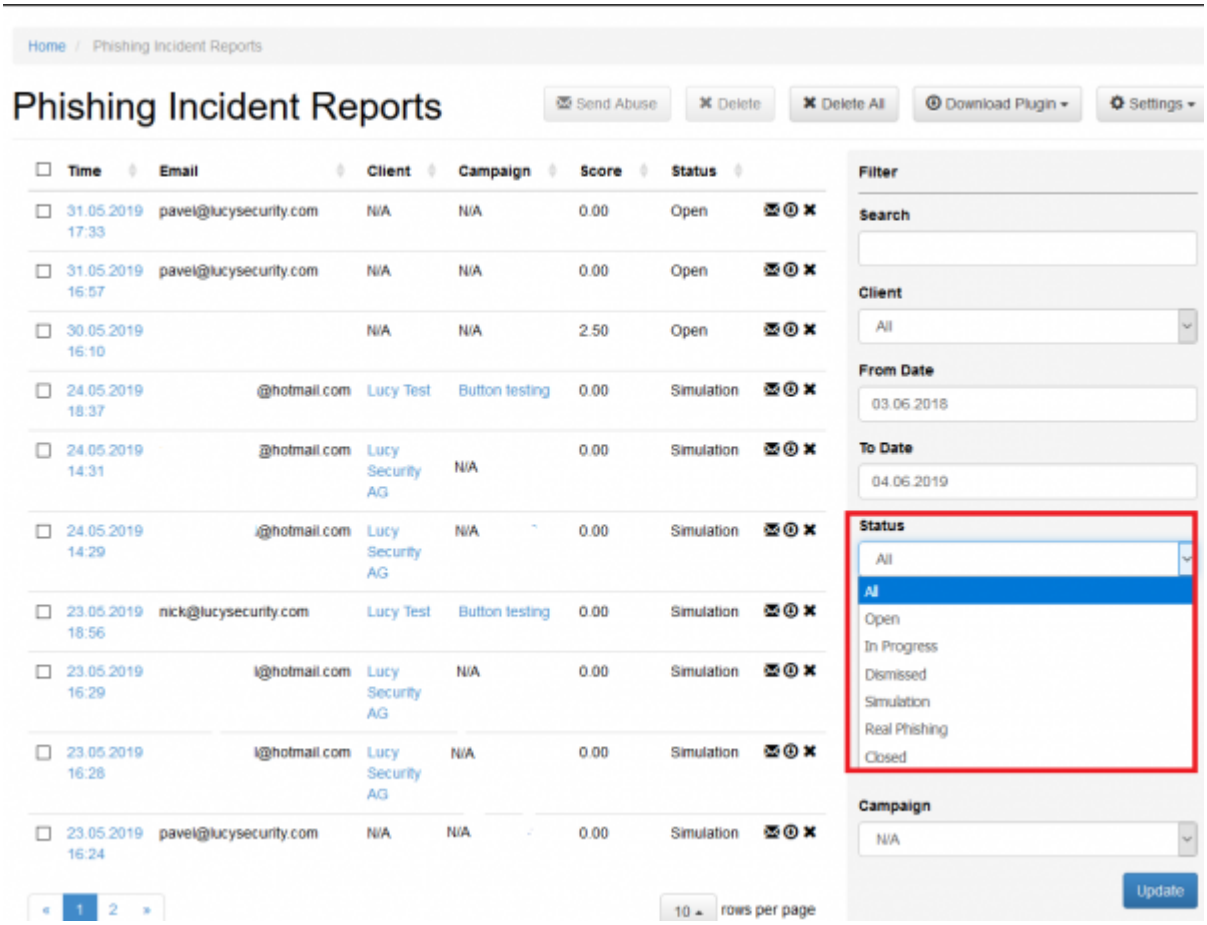
Phishing Incidents (threat analyzer)

LUCY comes with a “Phish Alert” plugin for mail clients. This add-in gives your users a safe way to forward suspected Emails with only one click and have them analyzed automatically by the threat analyzer in LUCY. The tool empowers users to proactively participate in an organization’s security program and makes it easy for your employees to report any suspicious email they receive. If you enabled "Send Reports Over HTTP", mail will get forwarded to LUCY. You will find them on the "incident" menu:



Incident Dashboard - Filters & Views

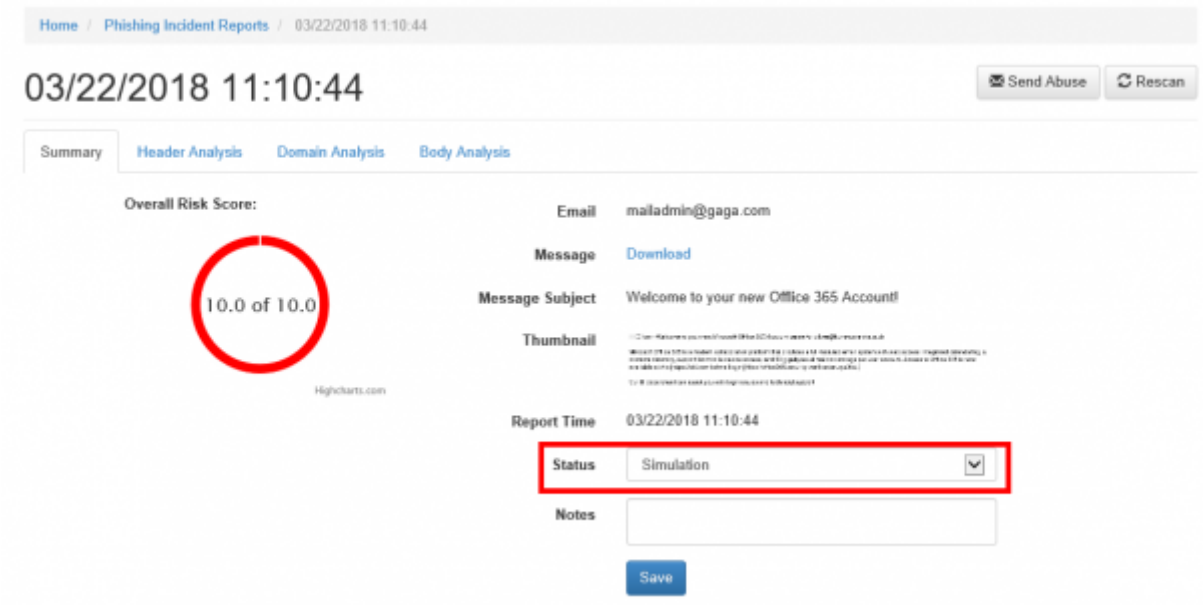
Filter by status: At the top level, LUCY allows you to filter the reported mails by the status of the ticket:



The default status is "open" unless it is a phishing simulation detected by LUCY. The other possible status are:

- Open
- In Progress
- Dismissed
- Simulation
- Real Phishing
- Closed

The status can be set by the LUCY administrator after clicking on the detail of a reported Email:



Lucy offers more filter and view options:

1. Search: You can search for any text from the mail subject or body. All emails that contain that exact search string will get displayed. This allows you to quickly identify similar attacks, even if the mail sender and recipients are different.
2. Client: Every campaign is associated with a client. This feature is helpful for MSSP's or companies with multiple legal entities to quickly identify submitted reports from different sources.
3. Date: You can use a date or date range to narrow down your search criteria
4. Domain: This field relates to the sender domain used in the reported email (not the user who reports the Email)
5. Minimum Score: The automatic risk score calculated in the system
6. Campaign: If the Email is associated with a specific campaign from LUCY
7. Select all View
8. All fields are sortable
9. Threat Details can be viewed by clicking on the date

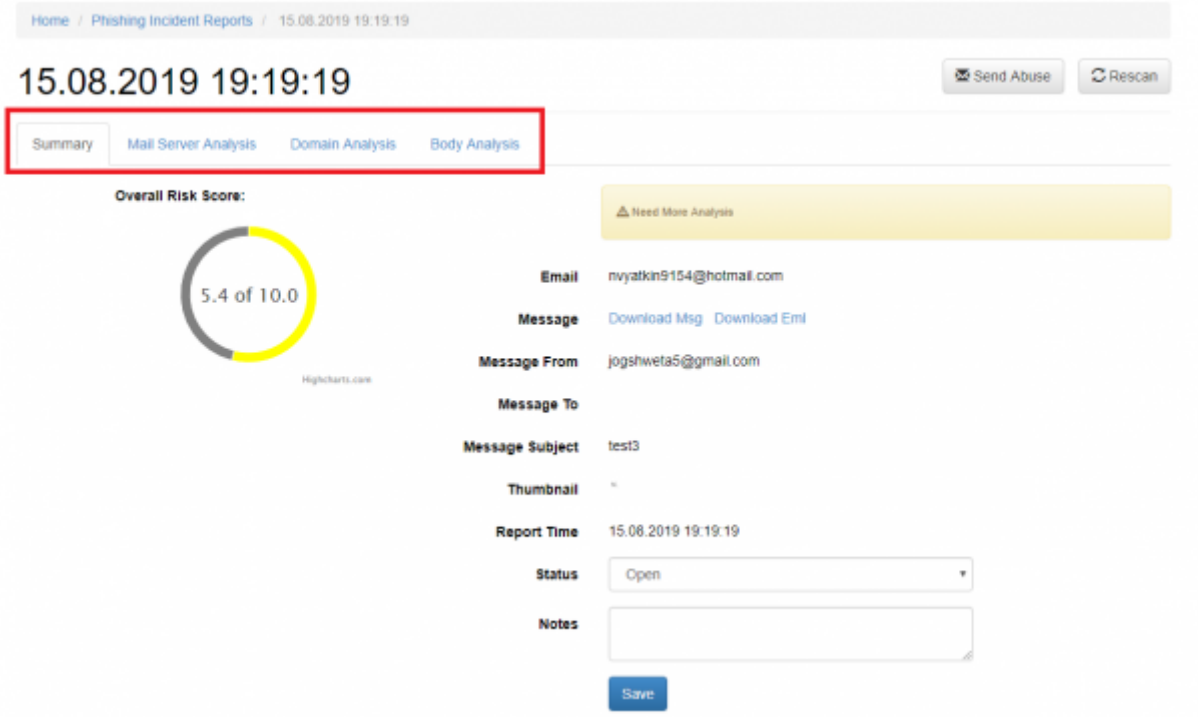
Automatic Incident Analysis (Threat Analyzer)

There are a few automatic analysis routines build into LUCY (e.g. check an IP in Google's Safe Browsing Database or Phishtank Database). More checks will follow in the upcoming versions.

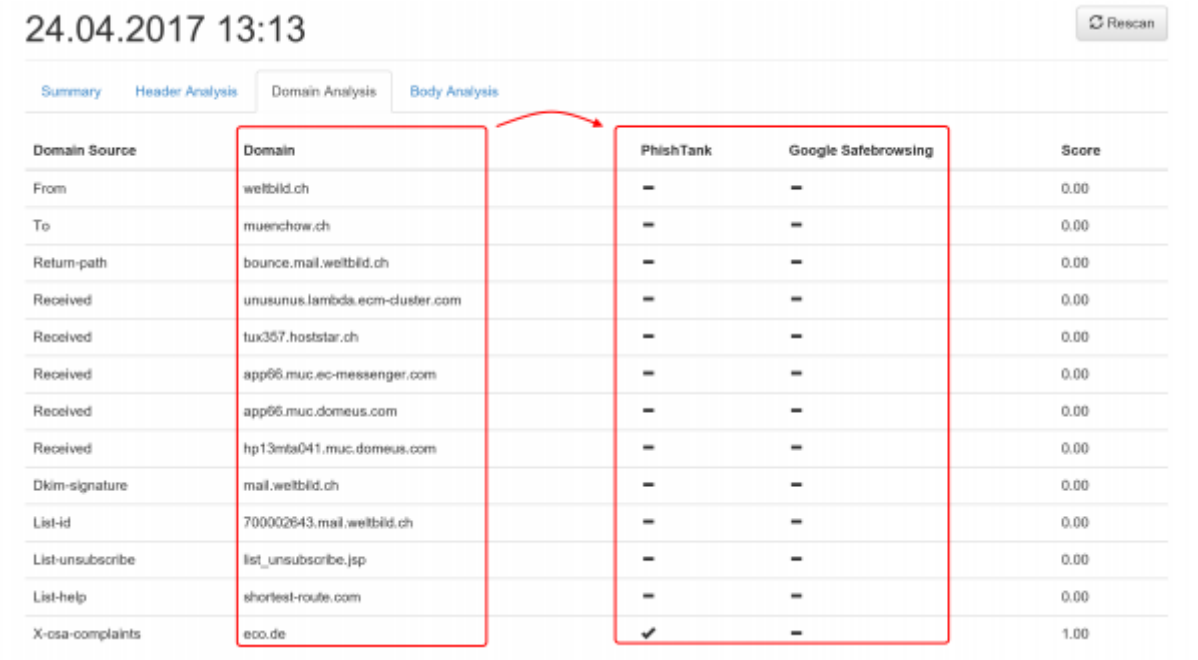
LUCY will automatically flag mail simulations. All other emails can then be manually verified by the

administrator. All emails can be downloaded as .msg file and/or add an incident report. When you click on a reported mail you will first see the overall risk score. The overall risk score is a weighted average of the following score from different scans:

- Header Analysis
- Domain Analysis
- Body Analysis



When a user forwards an email to LUCY all the domains and IP's from the mail header & body are extracted. For each IP and domain LUCY will then lookup public databases like google's safe browsing or phishtank, if any threat was reported:

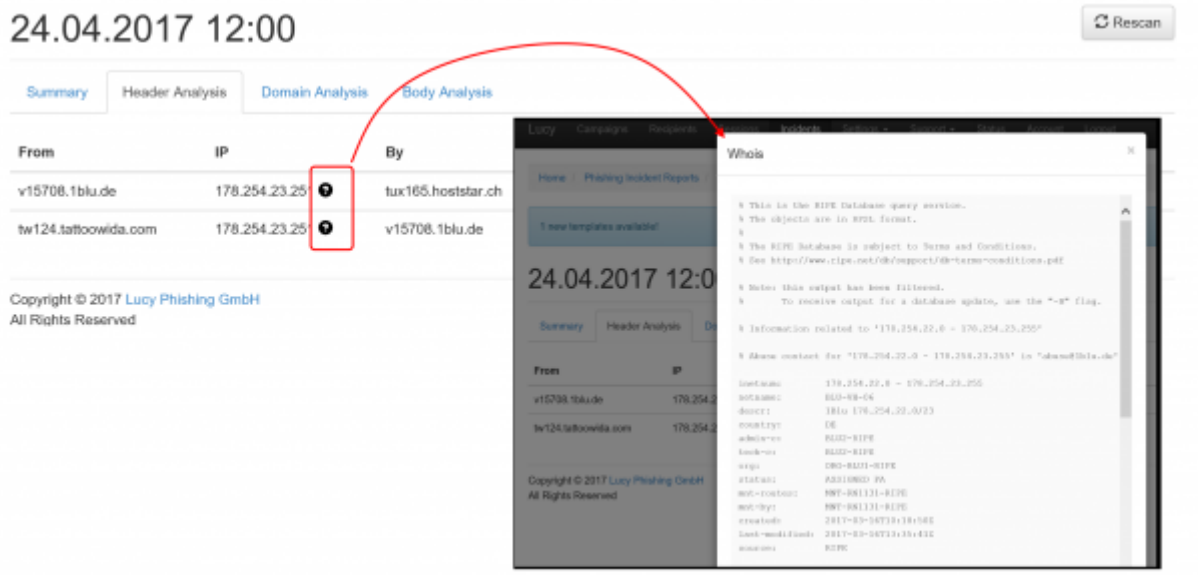


The current sources (LUCY 3.7) are:

- https://developers.google.com/safe-browsing/v4/lookup-api
- http://data.phishtank.com/data/online-valid.csv (port 80)
- DNS BL queries to bl.spamcop.net and zen.spamhaus.org
- CI Army (list) (http://cinsscore.com/) - Network security Block Lists.
- Cybercrime tracker (http://cybercrime-tracker.net/) -

More sources will be added with each new major release. Lucy will query those sources directly from the location where the software is installed. No data is transmitted back to our infrastructure.

The LUCY admin can also quickly just manually investigate the WHOIS records from the IP's by clicking on the help symbol:



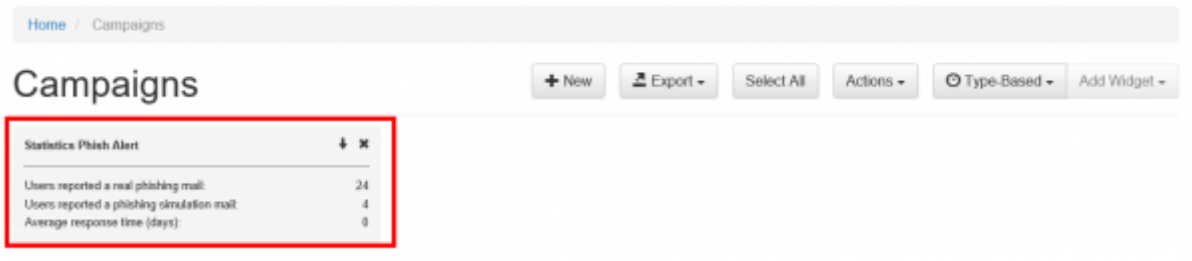
Detection of real phishing mails vs. Phishing simulations

The plugin automatically handles emails created in a phishing simulation from LUCY: it will ensure that only reports of potentially malicious emails are delivered to appropriate security staff. All emails created by LUCY itself will create a custom message to inform the user, that the mail has been sent as a part of a security awareness program. LUCY generated phishing emails won't be forwarded to the security team. But they will be reported back to LUCY in order to process the information within the campaign statistics. The reported emails will then be purged from the successful attack listings in LUCY.

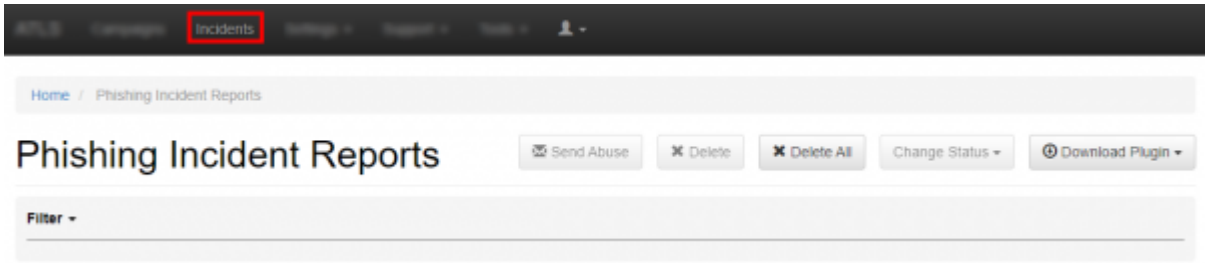
Where are incidents (LUCY generated emails) from the plugin reported?

If a user spots the phishing simulation and reports the email, you can see this information in various places:

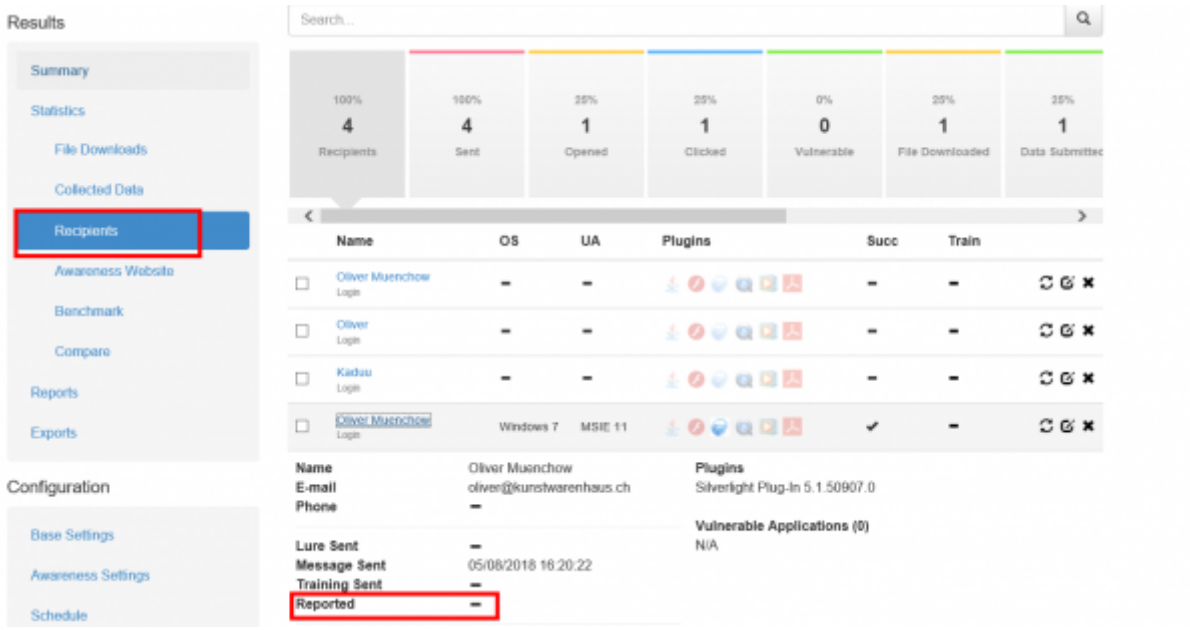
- Incident widget on the dashboard:



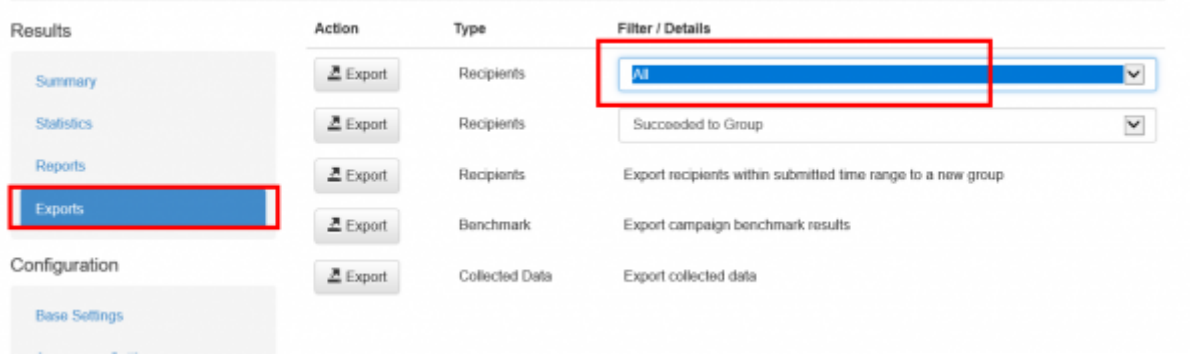
- Incident tab:



- Under the campaign statistics (recipients) under the "reported" item:



- If you want a comparison of all reported emails, you can export the whole campaign data via CSV. Within the CSV there is a reported column:



In LUCY, the incident reports will also be integrated on the dashboard under the general statistics.