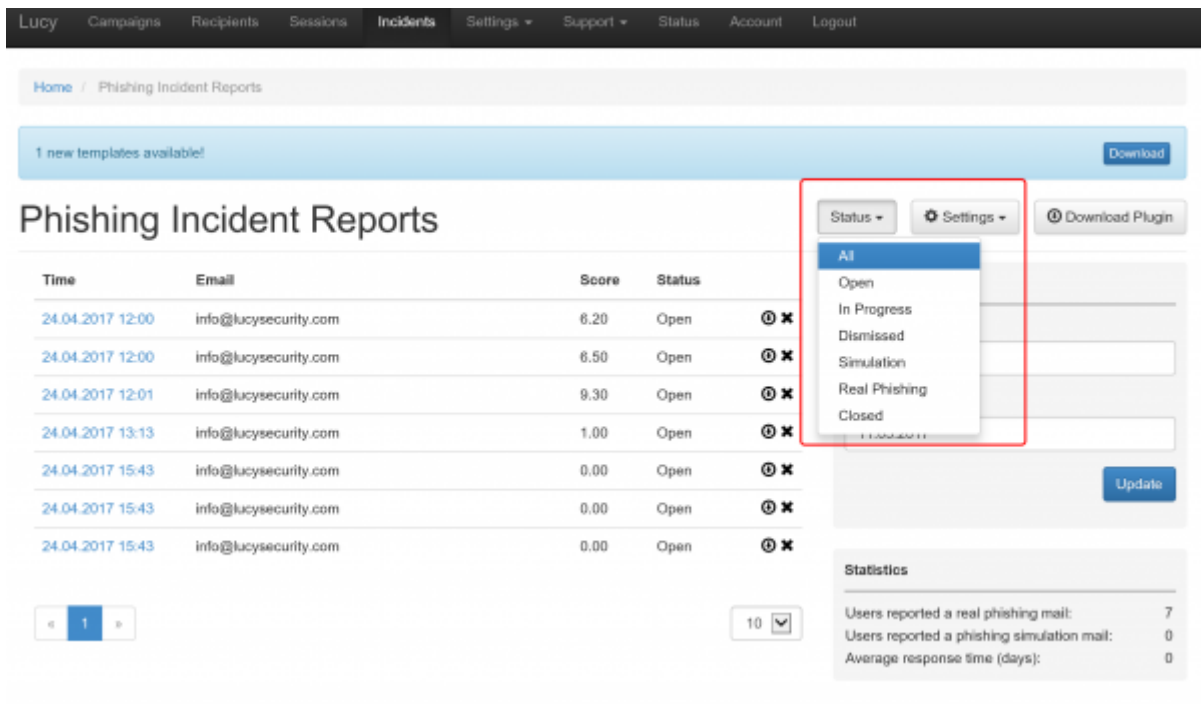


Phishing Incident Center Features (threat analyzer)

- **Dashboard Filter:** LUCY allows you to filter the incoming mails on the dashboard:



The screenshot shows the 'Phishing Incident Reports' dashboard. At the top, there's a navigation bar with links like 'Lucy', 'Campaigns', 'Recipients', 'Sessions', 'Incidents', 'Settings', 'Support', 'Status', 'Account', and 'Logout'. Below this, a breadcrumb trail shows 'Home / Phishing Incident Reports'. A blue banner indicates '1 new templates available!' with a 'Download' button. The main title 'Phishing Incident Reports' is followed by a table of reports. The table has columns for 'Time', 'Email', 'Score', and 'Status'. A red box highlights a 'Status' dropdown menu with options: 'All', 'Open', 'In Progress', 'Dismissed', 'Simulation', 'Real Phishing', and 'Closed'. To the right of the table, there's a 'Download Plugin' button and an 'Update' button. Below the table, there's a 'Statistics' section with the following data:

Statistics	
Users reported a real phishing mail:	7
Users reported a phishing simulation mail:	0
Average response time (days):	0

- **Centralized Analysis:** This feature allows you to analyse the incoming mails manually or automatically (see next chapter)
- **Centralized Campaign Reporting:** Any reported mail which is part of a phishing simulation will be processed within the campaign statistics
- **Threat Mitigation:** The Threat Mitigation (LUCY 3.5) allows you to take actions against legitimate phishing attacks
- **Custom Regex & Score:** LUCY allows you to define custom rules to scan mails for specific keywords and flag them with a individual threat score.

Detection of real phishing mails vs. Phishing simulations

The plugin automatically handles emails created in a phishing simulations 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 send as a part of a security awareness program. LUCY generated phishing mails 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 mails 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:

The screenshot shows the 'Campaigns' dashboard. At the top, there's a breadcrumb 'Home / Campaigns'. Below it, the title 'Campaigns' is followed by buttons: '+ New', 'Export', 'Select All', 'Actions', 'Type-Based', and 'Add Widget'. A widget titled 'Statistics Phish Alert' is highlighted with a red box. It contains the following data:

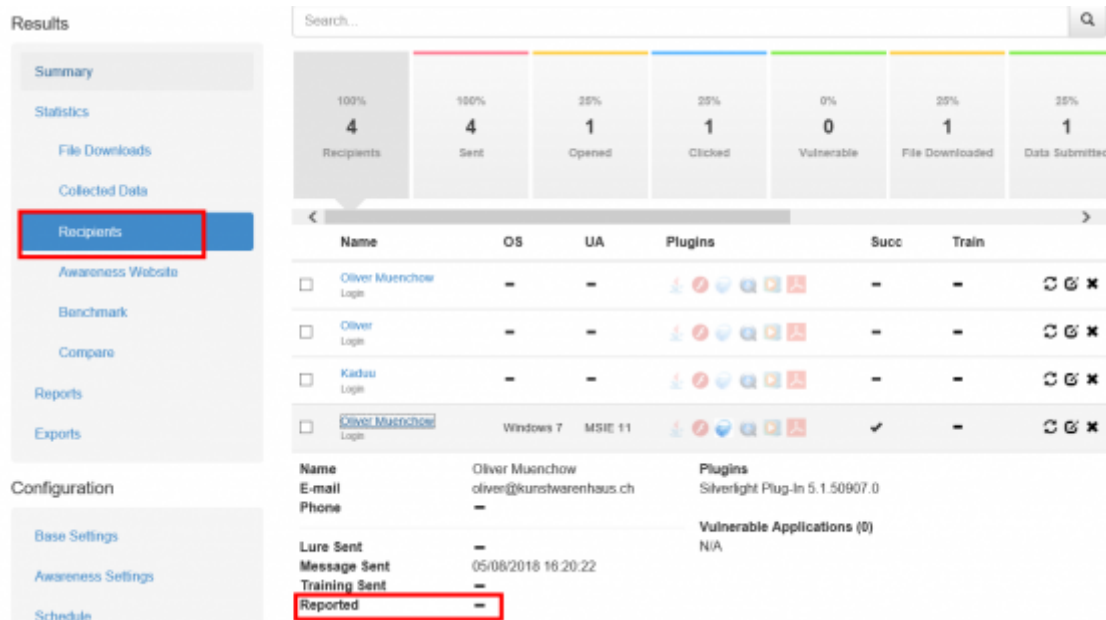
Statistics Phish Alert	
Users reported a real phishing mail:	24
Users reported a phishing simulation mail:	4
Average response time (days):	0

- Incident tab:

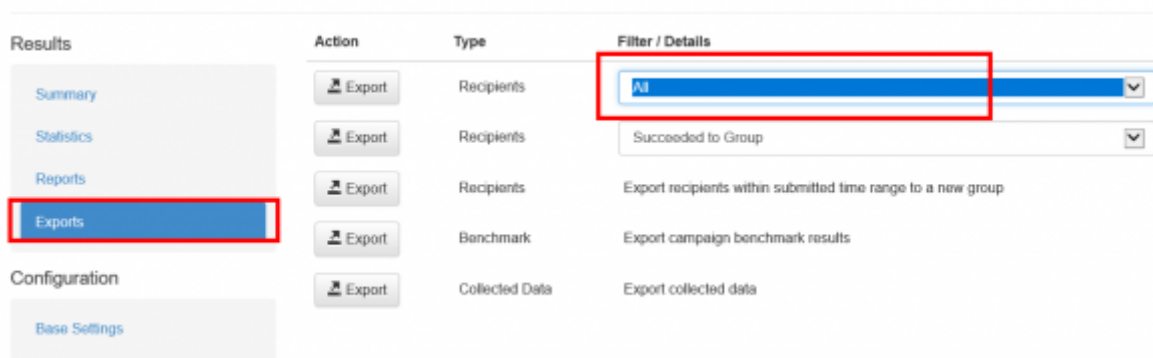
The screenshot shows the 'Incidents' tab in the application. The top navigation bar includes 'Lucy', 'Campaigns', 'Recipients', 'Sessions', 'Incidents' (highlighted), 'Settings', 'Support', 'Status', 'Account', and 'Logout'. Below the navigation bar, the breadcrumb is 'Home / Phishing Incident Reports'. The main title is 'Phishing Incident Reports', followed by buttons: 'Status', 'Delete', 'Settings', and 'Download Plugin'. A table lists the incidents with columns: Time, Email, Score, Status, and icons for report, delete, and settings. A 'Filter' sidebar on the right includes search, date range (From Date: 09.05.2017, To Date: 10.05.2018), domain (All), and min score filters. A pagination bar at the bottom shows '10 rows per page'.

Time	Email	Score	Status	Report	Delete	Settings
04/02/2018 11:14	oliver@muenchow.ch	10.00	Simulation			
03/23/2018 00:02	test.igor@hotmail.com	10.00	Simulation			
03/22/2018 23:52	test.igor@hotmail.com	10.00	Simulation			
03/22/2018 23:51	test.igor@hotmail.com	10.00	Simulation			
03/22/2018 15:57	oliver@muenchow.ch	10.00	Simulation			
03/22/2018 15:54	mailadmin@gaga.com	10.00	Simulation			
03/22/2018 11:10	mailadmin@gaga.com	10.00	Simulation			
03/15/2018 13:55	oliver@muenchow.ch	0.00	Open			
03/14/2018 13:35	oliver@muenchow.ch	10.00	Open			
03/14/2018 13:34	oliver@muenchow.ch	10.00	Simulation			

- 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:



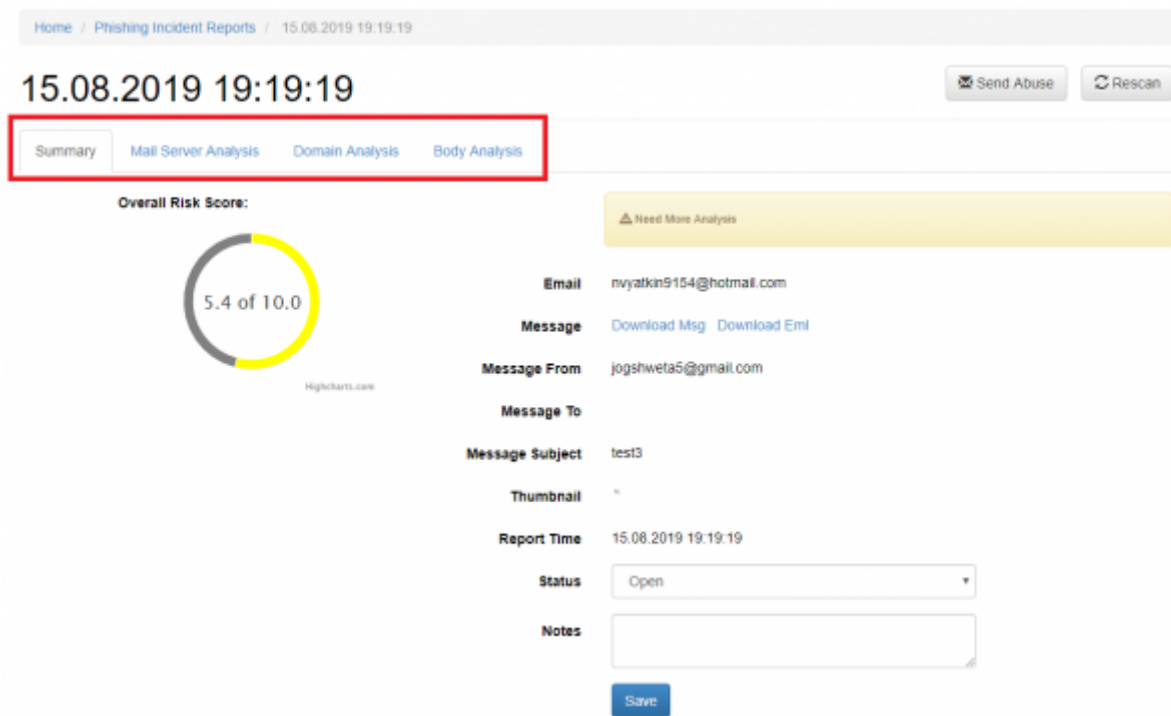
In LUCY 4.4, the incidents reports will also be integrated on the dashboard under the general statistics.

Centralized analysis

Once the mail has been reported by the user it will popup as an incident in LUCY in case you have enabled the HTTP option in LUCY. 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 mails can then be manually verified by the administrator. All mails 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:

24.04.2017 13:13

Summary Header Analysis Domain Analysis Body Analysis

Domain Source	Domain	PhishTank	Google Safebrowsing	Score
From	weltbild.ch	-	-	0.00
To	muenchow.ch	-	-	0.00
Return-path	bounce.mail.weltbild.ch	-	-	0.00
Received	unusunus.lambdas.ecm-cluster.com	-	-	0.00
Received	tux357.hoststar.ch	-	-	0.00
Received	app66.muc.ec-messenger.com	-	-	0.00
Received	app66.muc.domeus.com	-	-	0.00
Received	hp13mta041.muc.domeus.com	-	-	0.00
Dkim-signature	mail.weltbild.ch	-	-	0.00
List-Id	700002643.mail.weltbild.ch	-	-	0.00
List-unsubscribe	list_unsubscribe.jsp	-	-	0.00
List-help	shortest-route.com	-	-	0.00
X-csa-complaints	eco.de	✓	-	1.00

The current sources (LUCY 3.7) are:

- <https://safebrowsing.googleapis.com/v4/threatMatches:find> (port 443)
- <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.
- Palevo Blocklists (<https://palevotracker.abuse.ch/blocklists.php>) - Botnet C&C blocklists.
- 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:

24.04.2017 12:00 Rescan

Summary Header Analysis Domain Analysis Body Analysis

From	IP	By
v15708.1blu.de	178.254.23.25	tux165.hoststar.ch
tw124.tattooowida.com	178.254.23.25	v15708.1blu.de

Copyright © 2017 Lucy Phishing GmbH
All Rights Reserved

Lucy Campaigns Reports

24.04.2017 12:00

Summary Header Analysis Domain Analysis Body Analysis

From IP

v15708.1blu.de 178.254.23.25

tw124.tattooowida.com 178.254.23.25

Copyright © 2017 Lucy Phishing GmbH
All Rights Reserved

Whois

This is the RIPE Database query service.
The objects are in RPD format.
The RIPE Database is subject to Terms and Conditions.
See <http://www.ripe.net/gh/support/gh-term-conditions.pdf>
Notes this output has been filtered.
To receive output for a database update, use the "-u" flag.
Information related to '178.254.23.0 - 178.254.23.255'
Done output for '178.254.23.0 - 178.254.23.255' is 'abuse@tux165.ch'

last-as: 178.254.23.0 - 178.254.23.255
last-as-obj: RIPE-88-04
inet: 178.254.23.0/23
country: DE
admin-c: RIPE-RIPE
tech-c: RIPE-RIPE
org: ORG-RIPE-RIPE
status: ASSIGNED PA
mnt-routes: MNT-RIPE-RIPE
mnt-obj: MNT-RIPE-RIPE
created: 2017-03-04T13:18:50Z
last-modified: 2017-03-04T13:18:50Z
source: RIPE

Threat mitigation

The threat mitigation allows a LUCY admin to report reported phishing mails to according abuse contact of the provider's originating IP address taken from the message header. You can click on the mail symbol within the incident center to initiate the sending of the report. More info [here](#).

From:
<https://wiki.lucysecurity.com/> - LUCY

Permanent link:
https://wiki.lucysecurity.com/doku.php?id=threat_analyzer_-_mail_plugin&rev=1527142671

Last update: **2019/07/25 12:51**

