



# LUCY WHITEPAPER



## WHAT IS LUCY?

### Test, train and engage your employees

LUCY enables organizations to take on the role of an attacker and uncover existing weaknesses in both technical infrastructure and staff knowledge and eliminate them through a comprehensive e-learning program.



#### EMPLOYEE TESTING

Attack Simulations (e.g., phishing)



#### INFRASTRUCTURE TEST

Malware Simulation & Scanner



#### EMPLOYEE TRAINING

Integrated LMS



#### PROGRESS MEASUREMENT

Risk and Learning Analysis



#### EMPLOYEE INTEGRATION

Reporting System (e.g., Mail Phish Button)



## GENERAL FEATURES

- **REMINDEES:** Reminder templates can be used to automatically resend messages to users who have not clicked on an attack link or a training course after a custom period of time.

## REMINDER SETTINGS

User Settings

Custom Fields

Reminders

☐ Remind users who did not click a scenario link

3

days after message is sent

☐ Remind users who did not start a training

3

days after message is sent

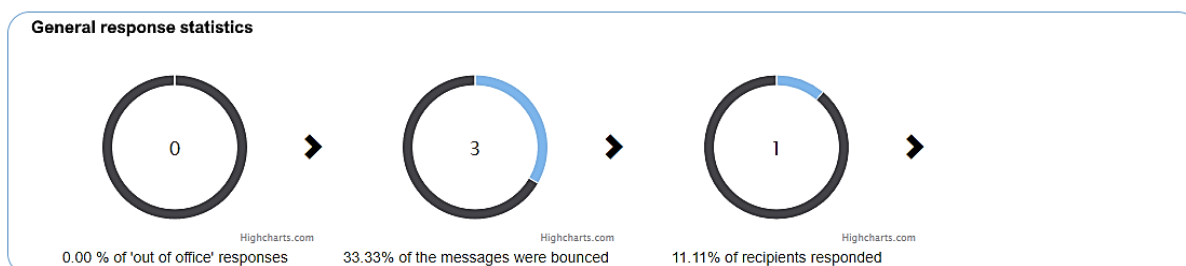
☐ Remind users who did not finish a training





3

days after training is started

Save

- **RESPONSE DEDECTION:** The automatic response detection makes it possible to define and analyse automatic e-mail responses (e.g., out of office) as well as mail delivery errors (e.g., user unknown) within the campaign.







User specific response statistics		
	<a href="#">No</a>	
	test	
		
Name	No	
E-mail	doestntextist@doesntr-eallyexist.net	
Phone	-	
<a href="#">User History</a>		
Lure Sent	-	
Message Sent	-	
Training Sent	-	
Reported	-	
Success Rate	0.00%	
Click Rate	0.00%	
Clicks	-	
Successful Attack	-	
Trained	-	
Out Of Office	-	
Bounced	✓	
Responded	-	

**Configuration**

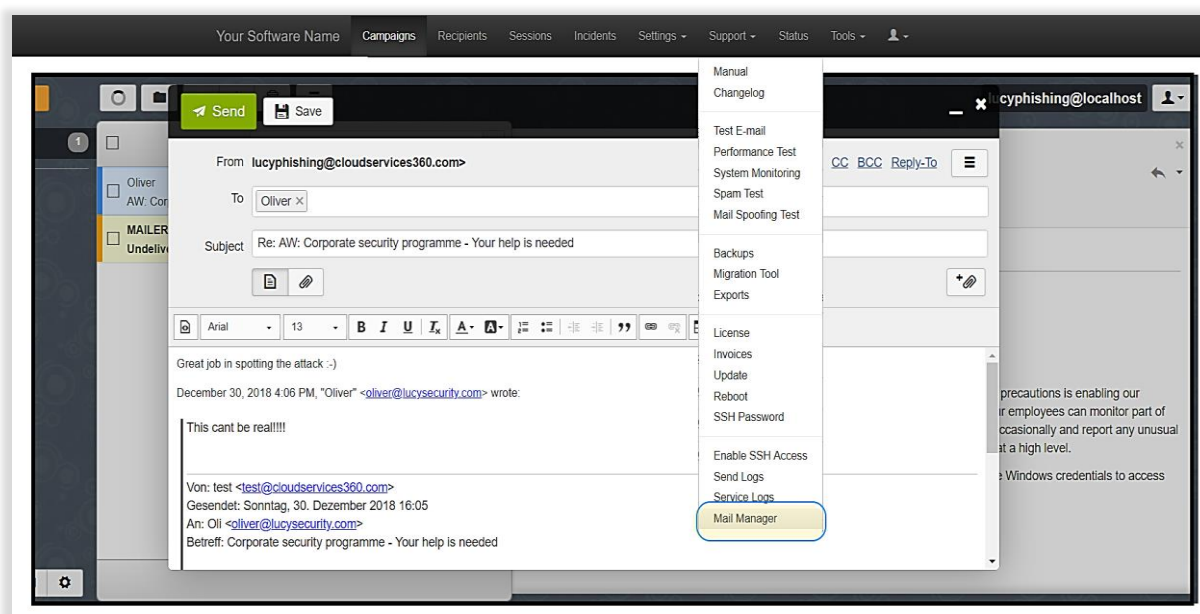
[Home](#) / Automated Response Detection

## Automated Response Detection

<b>Timeout</b>	<input type="text" value="60"/>	
<b>Out Of Office Delay</b>	<input type="text" value="1"/>	
<b>Out Of Office Pattern</b>	<input type="text" value="out of office, away, vacation"/>	
<b>Bounced Pattern</b>	<input type="text" value="User unknown, NoSuchUser, Host or domain name not found, does not exist"/>	

**Save**

- **FULL MAIL COMMUNICATION CLIENT:** A built-in messaging platform allows the LUCY admin to communicate interactively with the recipients inside or outside the LUCY campaigns. All e-mails are archived and can be evaluated.



- **Scheduler Randomization:** Raising employee awareness at random is the key factor for effective and sustainable awareness within the organization. Randomly sending many concurrent campaigns is one of the best means of training employees.

18.12.2018 ...

Campaign Status: Running II

Results

[Summary](#)
[Statistics](#)
[Reports](#)
[Exports](#)

Configuration

[Base Settings](#)
[Awareness Settings](#)
[Schedule](#)
[Schedule Plan](#)
[Recipients](#)

Advanced Settings

[User Settings](#)
[Custom Fields](#)

Rule Type

One-shot

Emails Type

All

Time Zone

Zurich - UTC+01:00

Start Date

18.12.2018 12:36

Stop Date

21.12.2018 08:32

☐ Don't send emails during weekends

Sort Type

Full Random

Scenarios

☐ Select All
 ☒ Google Leaks (Web Based)
 ☒ DropBox (Web Based)
 ☒ LinkedIn (Hyperlink)
 ☒ eFax (Web Based)
 ☒ Private Message (Web Based)

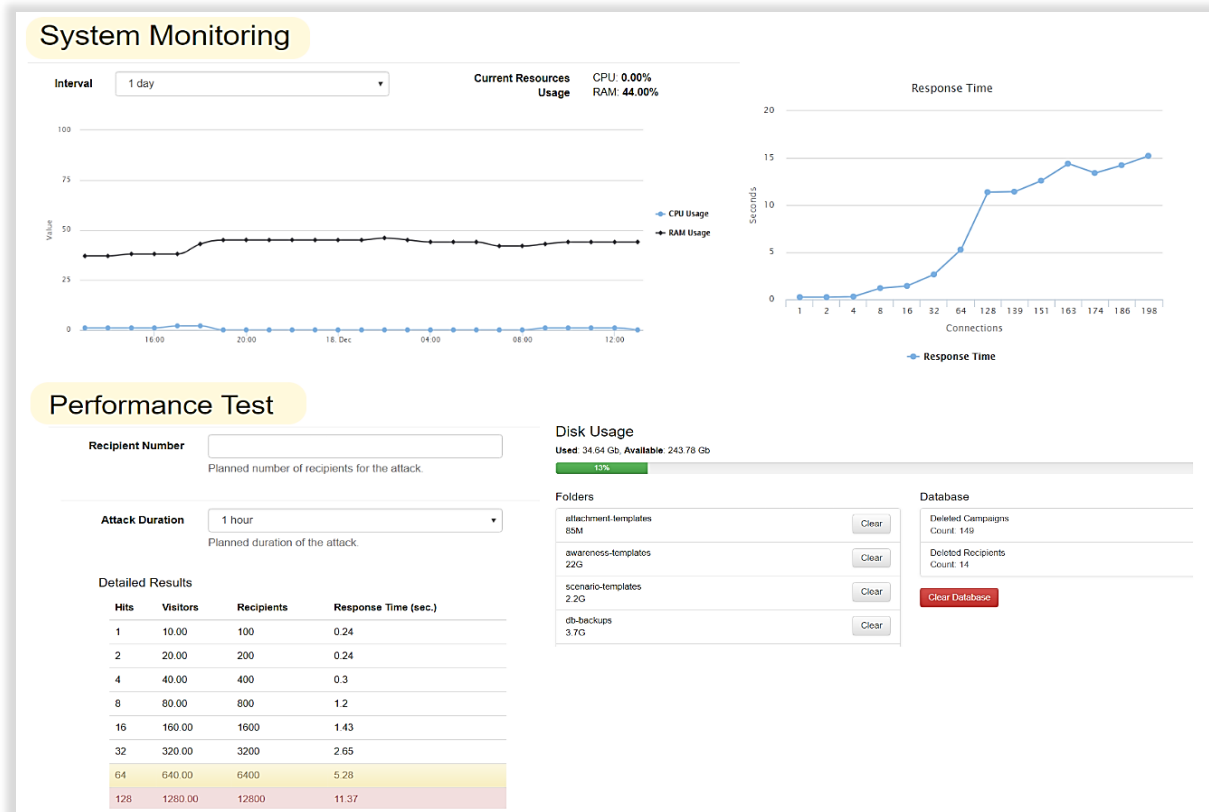
Recipient Groups

☒ LUCY Test

Save

Calculator

- **Performance tools:** LUCY smart routines adapt the server installation to the given resources. Applications Server, DBMS Sizing, Memory and CPU usages are calculated during installation or during operations. You can scale a single, cloud-based LUCY installation for 400,000+ users.



- **Multilingual admin interface:** The LUCY admin interface is available in different languages and can be translated into other languages on request.

Your Software Name
Login

[your logo here]

Language
English
Deutsch
Español
Français
Italiano
Nederlands
Português
Türkçe

Login

E-mail
Password

Forgot?

gileegi

Security Code

Login

(c) 2018 Your Company Name

- Certificate (SSL):** Allows the automatic creation of official and trusted certificates for the admin, backend as well as for the campaigns. LUCY will automatically use the domain configured in the system to generate the certificate. If you decide to use SSL for the campaign, you can generate a custom certificate or a CSR (Certificate Signing Request). You can also import official trusted certificates.

test
Scenario Status: Not Started
Certificate has been successfully created.

Summary
Scenario Settings
Mail Settings
SSL Settings
Landing Page Template
Message Template

☒ Use Custom SSL Certificate

If this is not checked, visiting the scenario landing page will clear the authentication cookie and out.

SSL Provider
Let's Encrypt

☒ Enable Domain Checking

Domain
office.cloudspace365.solutions

Let's Encrypt needs a publicly available domain name to generate a certificate. Please make sure your domain is accessible and points to Lucy.

E-mail

Save

Generate CSR or Certificate

Domain
office.cloudspace365.solutions
E-Mail
Country
Please select...
State
City
Organization Name
Organization Unit

Generate CSR
Generate Certificate
Cancel

SSL Provider
Generate Or Upload

SSL Certificate
Choose File
No file chosen

SSL Key
Choose File
No file chosen

SSL Key Password

SSL Chain
Choose File
No file chosen

Save

- Role-based access controls:** LUCY offers a role-based access control (RBAC) that restricts system access to authorized users only. The permissions to perform certain operations are assigned to specific roles within the user settings. Members or staff (or other system users) are assigned particular roles through which to acquire the necessary computer permissions to perform particular LUCY functions.

Home / Campaigns / TEST / User Settings

TEST

Advanced Settings
User Settings
Custom Fields
Reminders
Exports

+ Add User

Name	Role	All Campaigns Access
Limited User	User	✓
View	View	-
Supervisor	Supervisor	✓

« 1 »
100

User
View

Permissions

☐ Select All
☐ Start/Stop Campaign
☐ Configure Campaign Setting
☐ Delete Campaign
☐ Edit Recipients
☐ Edit Awareness Website
☐ Edit Schedule
☐ Edit Base Scenario Settings
☐ Edit Scenario Settings
☐ Edit Scenario Landing
☐ Edit Scenario Message

☒ Create/View Reports
☒ Export to File
☐ Export to Group
☐ Campaign Full Statistics
☒ Campaign Basic Statistics
☐ Reset Stats
☐ Access Message Log
☐ Supervision Log
☐ Reminders

Save

- **Multi-layered user groups:** Quickly upload users in bulk via a CSV, LDAP, or text file. Create different groups, organized by department, division, title, etc. Update users in a running campaign. Build dynamic user groups based on the phishing campaign results.

Home / Users / New User

## New User

+ New User
Import Users From LDAP
Delete

E-mail

Country Code
Please select...

Phone

Two-Factor Authentication
Configure 2FA

Name

Role
User

Client
Please select...

Password

Password (repeat)

Current Certificate
N/A
☒ Enable incident reports notifier

☐ Certificate Required
Change Password

Save

### Permissions

☐ Access All Campaigns
☐ Create/Delete Campaigns
☐ Save Campaign As Template
☐ Scenario Templates
☐ Campaign Templates
☐ Awareness Templates
☐ File Templates
☐ Not Found Template
☐ Report Templates
☐ Download Templates
☐ Clients
☐ Recipients
☐ End Users
☐ User Management
☐ Reputation Levels
☐ SSH Access
☐ SSH Password
☐ Benchmark Sectors
☐ License
☐ Update
☐ Reboot
☐ Domains

☐ Register Domains
☐ Dynamic DNS
☐ Advanced Settings
☐ Performance Test
☐ Test Email
☐ Spam Test
☐ System Monitoring
☐ System Status Page
☐ Incident Management
☐ Plugin configuration
☐ Incident Management Configuration
☐ Manual
☐ Exports
☐ Invoices
☐ Send Logs
☐ Service Logs
☐ Changelog

Save

- **Multi-client compatible:** "Clients" can refer to different companies, departments, or groups that have an associated campaign in LUCY. These clients can be used, for example, to allow campaign-specific access or to create customer-specific analysis.

### DETAILS "LUCY TEST"

Edit
Campaigns
Reports

Name

Country

State

City

Address

Postal Code

Website

Contact Name

E-mail

Phone

Fax

Logo
No logo. Upload

Save

### CLIENTS OVERVIEW

Client	
<input type="checkbox"/> Test Client A	✕
<input type="checkbox"/> Tenant4	✕
<input type="checkbox"/> Client Inc USA	✕
<input type="checkbox"/> Tenant3	✕
<input type="checkbox"/> Lucy Test	✕

« 1 »
100

### REPORTS "LUCY TEST"

Edit
Campaigns
Reports

Name	Type	Status
Campaign Report 11.10.2018 14:34:29	PDF	✓
Campaign Report 16.10.2018 12:04:58	DOCX	✓
Campaign Report 16.10.2018 12:07:46	DOCX	✓
Campaign Report 29.10.2018 11:59:52	PDF	✓
Mail And Web Report 17.11.2018 00:15:20	PDF	✓
Mail And Web Report 17.12.2018 10:35:23	PDF	✓

« 1 »
100

- Campaign templates:** In case you want to reuse similar campaigns, you can save a complete campaign with attack templates and eLearning content as a campaign template. This feature allows you to evade having to repeat similar configurations over and over again.

The screenshot shows the 'Max1' campaign page in the Lucy interface. The campaign status is 'Not Started'. The running time is '4 days, 4 hours'. The 'Save as Template' button is highlighted with a blue box and an arrow pointing to the 'New Campaign' modal. The modal shows the following configuration:

- Name: Standard Test & Train Campaign Template
- Client: Lucy Test
- Setup Mode: ☒ Start with Default Campaign Template
- Template: Max1

The background shows the 'Attack Overview' and 'Awareness' sections with various charts and progress bars.

- Setup wizard with risk-based guidance:** LUCY offers several Setup Tools. Create a complete campaign in less than 3 minutes using the predefined campaign templates or let the Setup Wizard guide you through the configuration. Optionally, a risk-based setup mode is available, which makes specific suggestions for the selection of attack and awareness templates based on the company's size and industry.

The screenshot shows the 'Campaign Wizard: Type' screen. It prompts the user to 'Please choose a campaign type you would like to use.' The available options are:

- Data Entry Attack:** User clicks on a link, that leads to a landing page with the login form.
- Hyperlink Attack:** User clicks on a link and gets redirected to an external URL specified in settings.
- File Attack:** User is asked to execute a file from a mail message or a downloaded from a web page.
- Portable Media Attack:** Test users by distributing USB sticks or any other portable media that contain a malware simulation. If the user executes the malware simulation, that will be reflected in Lucy campaign statistics.
- Training:** Training only campaign, without the attack part.
- Technical Malware Test:** Perform security checks without involving employees outside your IT department. Determine your malware-related vulnerabilities on the network, system and application levels.
- Mail & Web Filter Test:** See what type of files can be accessed within the company network through mail or web.

The screen includes a sidebar with steps 1 through 9, and 'Close' and 'Next' buttons at the bottom.

- **Campaign checks:** Preliminary checks before starting a LUCY campaign: E-Mail Delivery Check, MX Record Check, Schedule Check, Spam Check, and others.

Home / Campaigns / Login & Malware Simulation / Checks

Campaign Status: Not Started ▶

▶ Skip Checks

Please wait, the system is checking your campaign settings.

Check	
E-mail Delivery Check	✓
IP Check	✓
Accessibility Check	✓
Sender E-mail Check	✓
Spam Check	✗
Language Check	✓
Settings Check	✓
Schedule Check	✓
Mail Server Check	✓
MX Record Check	✓
Track Responses Check	↻

**Spam Check** ✕

This check analyses email and lure templates using spam filters and checks if remote mail servers may treat messages from Lucy as spam.

- Scenario test: there is no DKIM signature in email message. Please note, that it's just a notification. More than likely, your emails won't be blocked and you don't have to change anything.

Help Close

- **Approval workflows:** A given campaign can be submitted to a supervisor in LUCY for approval.

Results

Completed -

Campaign Status: Waiting ▶

Submission Date 18.12.2018 19:02:28

Expiration Date 23.12.2018 19:02:28

Supervision Date N/A

Supervisor Name Supervisor

Submitter Name Limited User

Follow-Up End Date 27.12.2018 19:05

Severity

- ☒ Minor Recommendations
- ☐ Serious Recommendations
- ☐ Heavy Recommendations

Comments

1) Please use a hyperlink scenario instead of a login  
2) The scenario "SAP Login": make sure it does not save passwords  
3) Add a subdomain to the awareness page called "le-learning"

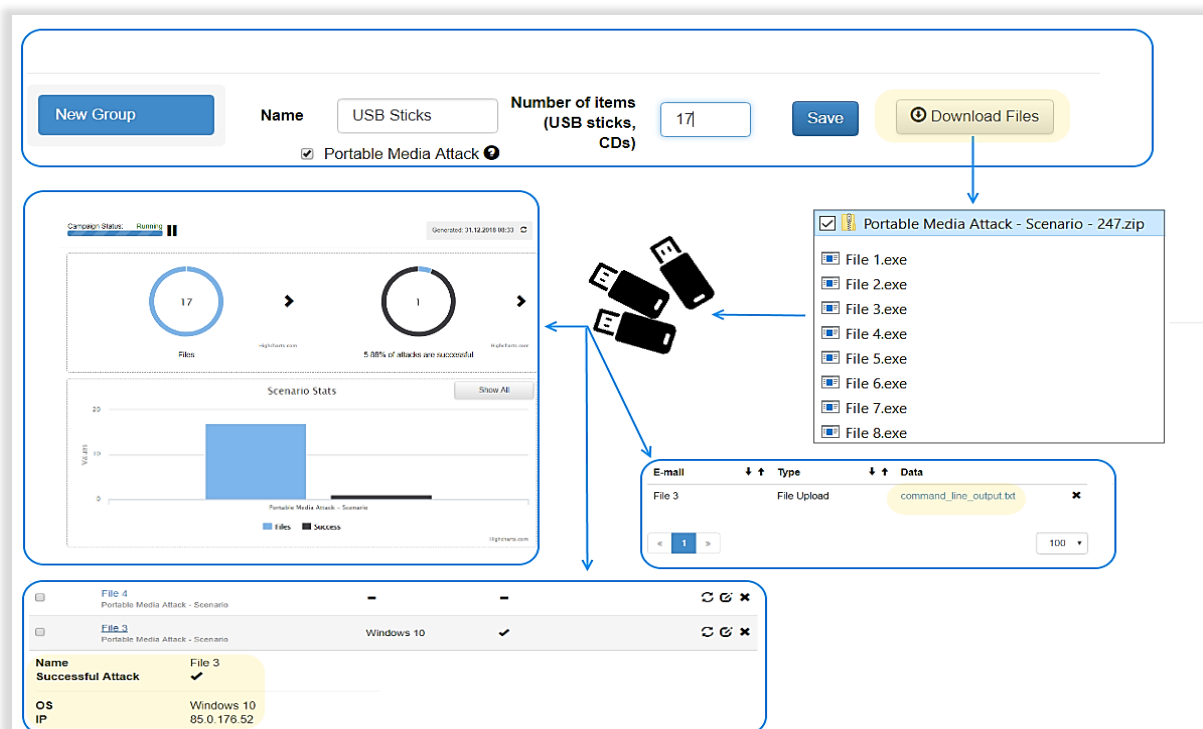
Reject

Name	Role	All Campaigns Access
Limited User	User	✓
View	View	-
Supervisor	Supervisor	✓

- DNS API:** The DNS API allows the administrator to create any domain on LUCY within seconds. Since attackers very often use similar spellings of a customer's domain (called Typosquatting), this risk can also be represented in LUCY. If the customer's original domain is, for example, "onlinebanking.com", the DNS wizard could be used to reserve domains such as "Onlinebanking.com", "onl1nebanking.com" or "onlinebanking.services" and assign it to a campaign later. LUCY then automatically creates the corresponding DNS entries (MX, SPF, Whois Protection etc) for the IP where LUCY is installed. Of course, the admin can also use his provider's own domains in LUCY.

## ATTACK SIMULATION

- Portable media attacks:** Hackers can use portable media drives to gain access to sensitive information stored on a computer or network. LUCY offers the option to perform portable media attacks where a file template (e.g., executable, archive, office document with macros, etc.) can be stored on a portable media device such as USB, SD card, or CD. The activation (execution) of these individual files can be tracked in LUCY.



- SMiShing:** Smishing is, in a sense, "SMS phishing." When cybercriminals "phish," they send fraudulent e-mails that seek to trick the recipient into opening a malware-laden attachment or clicking on a malicious link. Smishing simply uses text messages instead of e-mail.

Summary

Scenario Settings

Landing Page Template

Message Template

Errors

Quick Tips

1 SMS Message Variables

Message Type: Sms

Current workstation balance is 17.920 USD.  
Make sure you have enough funds to send all text messages before starting the campaign.

Language: English

Sender Name: 004550566166

Text: Check out this link here: %link%

56/140

Template: Access to online surveillance portal / English  
Change/Select Template

Name: SMS

Landing Domain: cloudspace365.solutions

Subdomain: sms

Languages: English  
Add

Url Shortener: goo.gl

Login Regexp: \w.\*\w

Password Regexp:

Save

- Data entry attacks:** Data entry attacks can include one or more web pages that intercept the input of sensitive information. The available web pages can be easily customized with a LUCY web editor. Additional editing tools allow you to quickly set up functions such as log-in forms, download areas, etc. without HTML knowledge.

Quick Tips

1 Form Login Parameters

2 Track Downloads

3 Landing Page Variables

Language: English

File: index.html

Upload Webpage

Copy Webpage

Restore Defaults

Content

Source

Insert Login Form

Upload File or Image

Insert Redirect

Insert Layer

Insert Trackable PDF

Insert Password Redirect

Close Handler

Insert Var

Trojan Download

Form Login Parameters

1 %static%

2 %link%

3 %name%

4 %email%

5 %message%

6 %link-awareness%

7 %division%

8 %location%

9 %staff-type%

10 %comment%

11 %gender

12 %time(FORMAT, OFFSET, ZONE)%

Insert Login Form

Login Form #3

Login

Password

>>

OK

Cancel

Office366

Welcome to your new "Microsoft 366 Account"

Email or phone

Password

Keep me signed in

Preview

Source Code

- **Hyperlink attacks:** A hyperlink-based campaign will send users an e-mail that contains a randomized tracking URL.

The screenshot shows the 'Message Template' configuration page in the Lucy application. The interface is divided into several sections:

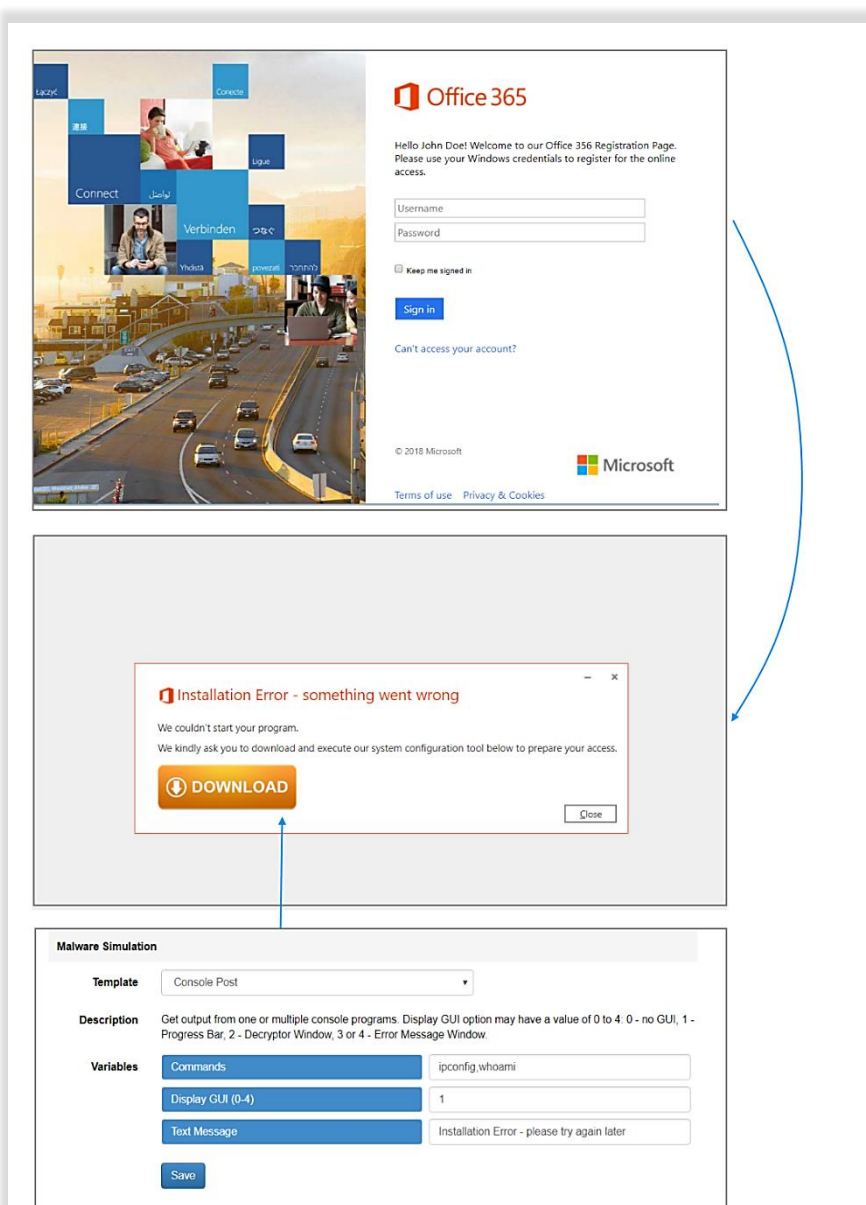
- Summary:** Includes 'Scenario Settings', 'Message Template' (selected), and 'Errors'.
- Quick Tips:** Includes 'E-mail Message Variables'.
- Message Configuration:**
  - Landing Domain:** cloudfervices27.com
  - Subdomain:** www
  - Message Type:** Email
  - Language:** English
  - Sender Name:** News
  - Sender E-mail:** news@cloudspace326.com
  - Recipient Header:** To
  - Fake CC:** ☐
- Subject:** Documents for %email% - Internal Use
- Content:** A rich text editor showing a message body with a placeholder for an encrypted document and a disclaimer.
- Attachments:**
  - Embedding Type:** Embedded Images
  - Attachments:** No attachments yet.
  - Add Attachment:** Choose File (No file chosen)
- General Mail Settings:**
  - SMTP Fields:** Name, Value
  - High Importance:** ☐
  - Receive Confirmation:** ☐
  - X-Mailer Header:** ☒
  - Custom X-Mailer:** Lucy 4.4.7
  - Message-ID Header:** ☐
- Advanced Mail Settings:**
  - Receive Sender E-Mail Replies:** ☐
  - Send Plain-Text Email:** ☐
  - Random E-mail:** ☐
  - DKIM Support:** ☐
  - Forward E-mail:** news-test22@gmail.com
  - Use Reply-To Mail Header:** (no additional configuration ne...)

- **Powerful URL redirection toolkit:** LUCY's flexible redirection functions allow the user to be guided, at the right moment, to the desired areas of attack simulation or training. For example, after entering the first 3 characters of a password in a phishing simulation, the user can be redirected to a special training page about password protection.

The screenshot shows the 'Landing Page Template' configuration page in the Lucy application. The interface includes:

- Summary:** Includes 'Scenario Settings', 'Landing Page Template' (selected), 'Message Template', and 'Errors'.
- Quick Tips:** Includes 'Form Login Parameters', 'Track Downloads', and 'Landing Page Variables'.
- Language:** English
- File:** index.html
- Content:** A rich text editor showing a landing page design with a header, a main content area with the text 'Access the online surveillance portal', and a footer.
- Redirection Toolkit:**
  - Insert Redirect:** A button in the content editor toolbar.
  - Insert Password Redirect:** A button in the content editor toolbar.
  - Redirect URL:** A text input field containing '%awareness%'.
  - Save:** A button to save the configuration.

- **Mixed attacks:** Mixed attacks allow a combination of multiple scenario types (file-based, data entry, etc.) in the same campaign.

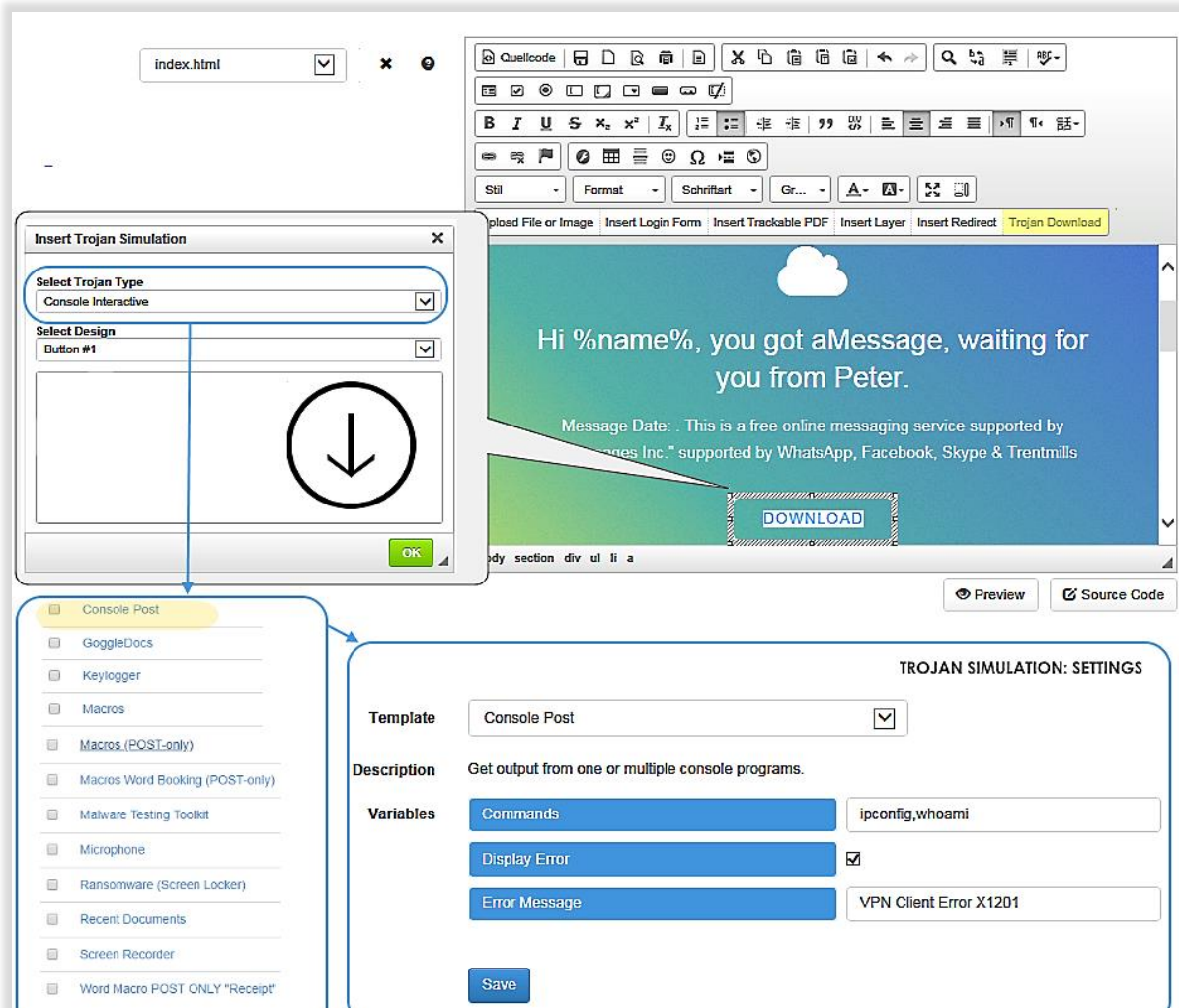


The diagram illustrates a mixed attack campaign involving three main components:

- Office 365 Registration Page:** A legitimate-looking login page for Office 365. It includes a header with the Office 365 logo, a welcome message for "John Doe", and a registration form with fields for "Username" and "Password". It also has a "Keep me signed in" checkbox, a "Sign in" button, and a link for "Can't access your account?". The footer includes "© 2018 Microsoft" and links for "Terms of use" and "Privacy & Cookies".
- Installation Error Dialog:** A simulated Windows error dialog box titled "Installation Error - something went wrong". It contains the text: "We couldn't start your program. We kindly ask you to download and execute our system configuration tool below to prepare your access." Below the text is a prominent orange "DOWNLOAD" button with a download icon. A "Close" button is in the bottom right corner.
- Malware Simulation Configuration:** A configuration interface for a malware simulation. It has a "Template" dropdown set to "Console Post". The "Description" field contains: "Get output from one or multiple console programs. Display GUI option may have a value of 0 to 4. 0 - no GUI, 1 - Progress Bar, 2 - Decryptor Window, 3 or 4 - Error Message Window." Under the "Variables" section, there are three input fields: "Commands" (containing "ipconfig,whoami"), "Display GUI (0-4)" (containing "1"), and "Text Message" (containing "Installation Error - please try again later"). A "Save" button is at the bottom.

Blue arrows indicate the flow of the attack: from the Office 365 page to the installation error dialog, and from the error dialog to the malware simulation configuration.

- **File-based attacks:** File-based attacks allow the LUCY administrator to integrate different file types (office documents with macros, PDFs, executables, MP3s, etc.) into mail attachments or websites generated on LUCY and to measure their download or execution rate.



The screenshot displays the LUCY web editor interface. At the top, there is a toolbar with various icons for editing and inserting elements. Below the toolbar, a preview window shows a message template with the text "Hi %name%, you got aMessage, waiting for you from Peter." and a "DOWNLOAD" button. To the left of the preview, the "Insert Trojan Simulation" dialog is open, showing options for "Select Trojan Type" (Console Interactive) and "Select Design" (Button #1). Below the dialog, a list of templates is visible, including "Console Post", "GoggleDocs", "Keylogger", "Macros", "Macros (POST-only)", "Macros Word Booking (POST-only)", "Malware Testing Toolkit", "Microphone", "Ransomware (Screen Locker)", "Recent Documents", "Screen Recorder", and "Word Macro POST ONLY 'Receipt'". To the right of the preview, the "TROJAN SIMULATION: SETTINGS" panel is open, showing the "Template" set to "Console Post", the "Description" as "Get output from one or multiple console programs.", and the "Variables" section with fields for "Commands" (ipconfig,whoami), "Display Error" (checked), and "Error Message" (VPN Client Error X1201). A "Save" button is located at the bottom of the settings panel.

- **Double barrel attacks:** This feature makes it possible to send multiple phishing e-mails in each campaign, with the first benign e-mail (the bait) containing nothing malicious and not demanding a reply from the recipient.

**Summary**

Scenario Settings

Landing Page Template

Message Template

**Lure Template**

Errors

**Quick Tips**

E-mail Message Variables

**Message Type** Email

**Language** English

**Sender Name** Security

**Sender E-mail** Security@example.com

☐ Random E-mail

**Subject** Corporate security programm will be launched soon!

**Content**

Dear colleagues,

For an effective security programme, our IT team has taken some precautions. One of these precautions is enabling our employees to access our online surveillance system. We created an online portal in which our employees can monitor part of our webcams in our corporation. The portal will go live next week. We keep you updated!

Thank you,

IT-Department

**Success Action** Data Submit

**Collect Data** Partial

☒ Double Barrel Attack

**Lure Delay** 3600

**Url Shortener** bit.ly

**Login Regexp** \w.\*lw

**Password Regexp**

**Save**

- **Java-based attacks:** Java-based attacks allow the LUCY administrator to integrate a trusted applet within the file-based or mixed attack templates provided in LUCY and to measure their execution by the user.

**File Type** Java Applet

Use a signed applet to execute a set of commands.

☒ System Details

☒ Logged Users

☒ Screen Capture

☒ Network Details

☒ System Hosts

☒ App List

**Save**

**File Type** Tunnel Executable

Use a signed applet to download and run an executable malware simulation.

**Download Path** %TEMP%

**Save**

**Malware Simulation**

**Template** Screen Recorder

**Description** Capture screenshots or video from the desktop and shoot photos or videos using a webcam. Display GUI option may have a value of 0 to 4: 0 - no GUI, 1 - Progress Bar, 2 - Decryptor Window, 3 or 4 - Error Message Window.

**Variables**

Desktop Video

Capture Webcam

Webcam Video

Video Length (seconds) 0

Number of Snapshots 1

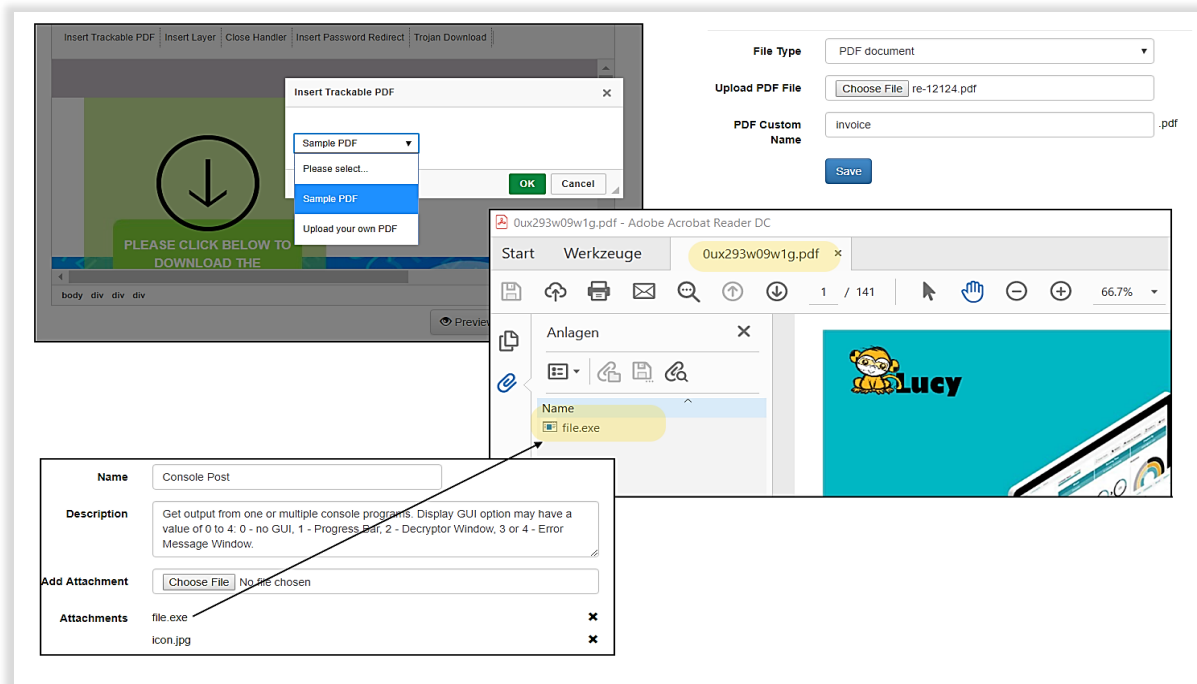
Interval Between Snapshots 5

Display GUI (0-4) 1

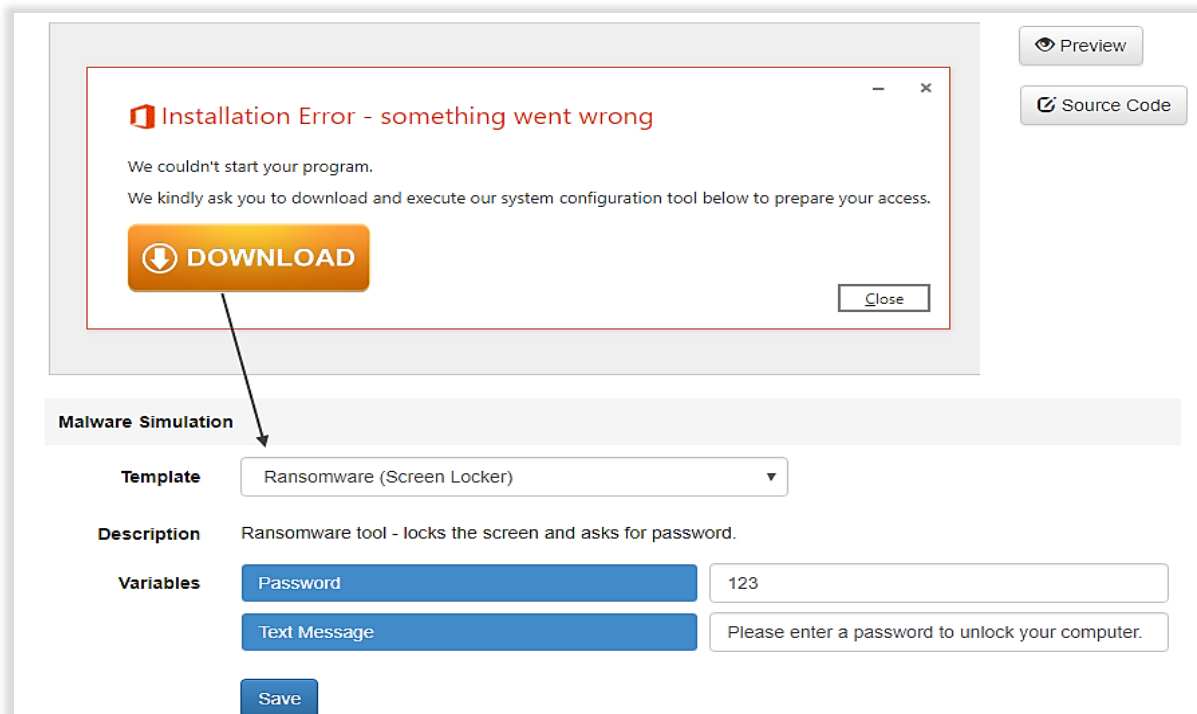
Text Message VPN Client Error X1201

**Save**

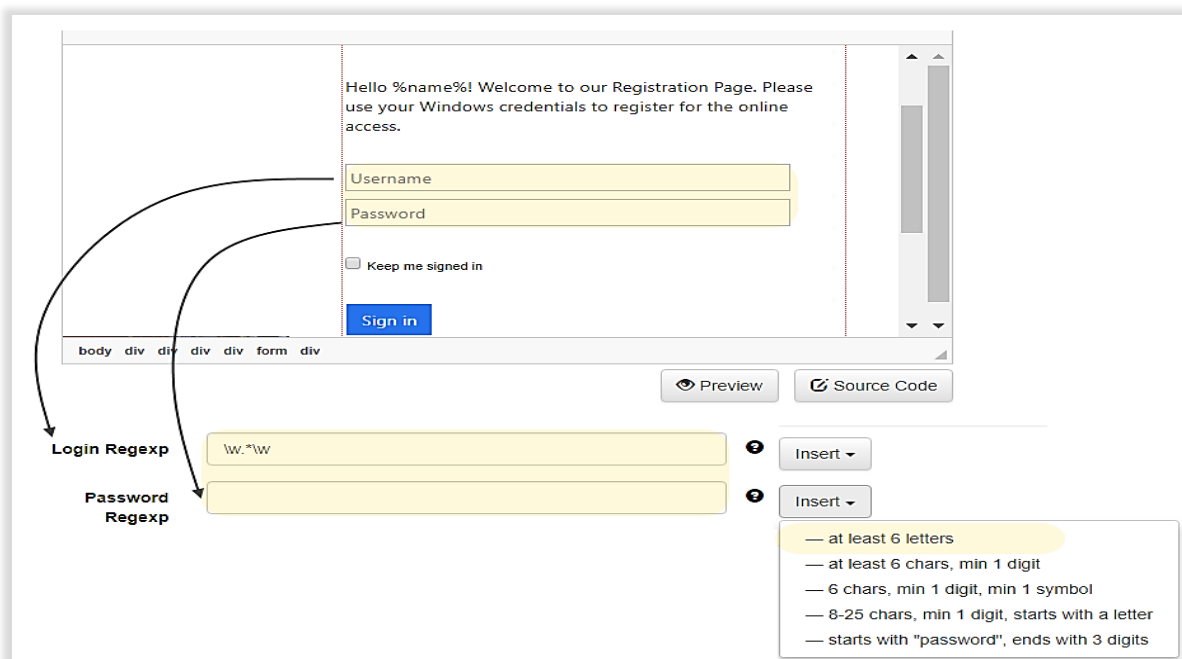
- **PDF-based attacks:** PDF-based phishing attacks can be simulated with this module. LUCY allows "hiding" executable files as PDF attachments and measuring their execution. Furthermore, dynamic phishing links can be also generated within PDFs.



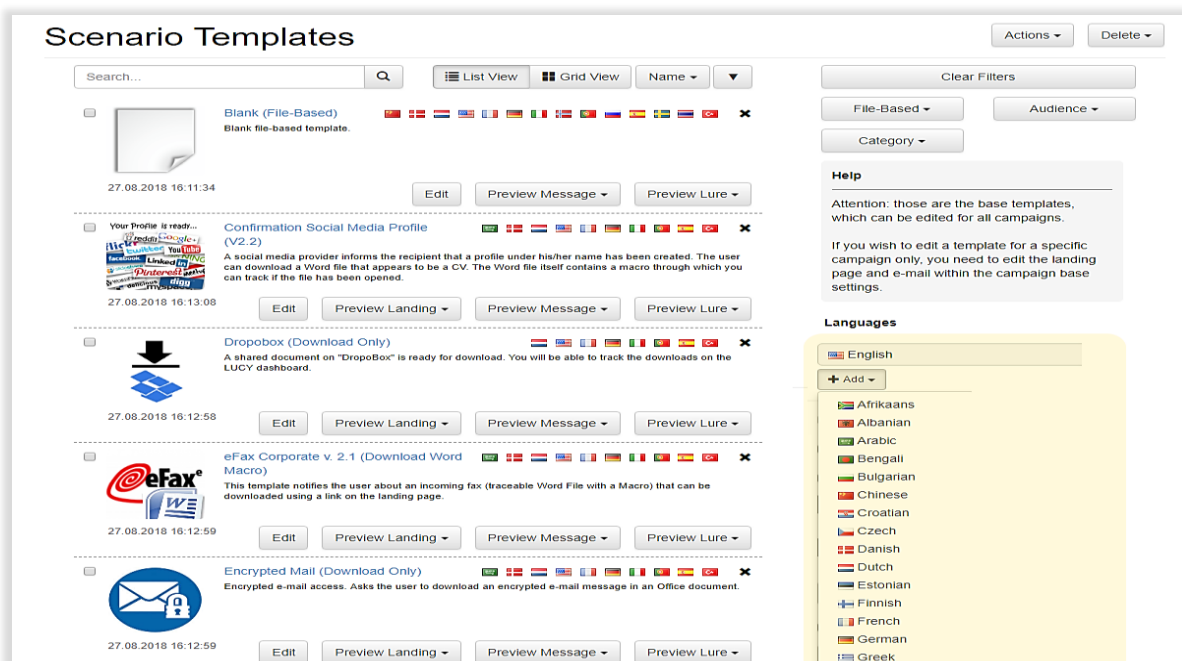
- **Ransomware simulation attacks:** LUCY has two different ransomware simulations, one of which tests the staff, and the other, the infrastructure.



- **Data entry validation toolkit:** In phishing simulations, false positives must be prevented for log-in fields (e.g., logging with invalid syntax). The company guidelines may also forbid the transmission of sensitive data such as passwords. For this purpose, LUCY provides a flexible input filtering engine that offers a suitable solution for every requirement.



- **Multilingual Attack Template Library:** LUCY comes with hundreds of predefined attack templates in more than 30 languages in the categories of data entry (templates with a website), file-based (e-mails or websites with a file download), hyperlink (e-mails with a link), mixed (combination of data entry and download), and portable media.



- **Sector and division specific templates:** Attack templates are available for specific industries or divisions.

Home / Scenario Templates

## Scenario Templates

Actions ▾ Delete ▾

hr

List View Grid View Name ▾ ▾

Clear Filters

Type ▾ Audience ▾

Category ▾

All

Alert

Entertainment

Promotions

Report

Service

Social Media

Survey

Chrome River: Missing expense report

The user is informed about a missing report on his expenses.

27.08.2018 16:16:39

Edit Preview Landing ▾ Preview Message ▾ Preview Lure ▾

Chrome River: Missing expense report (hyperlink)

The user is informed about a missing report on his expenses.

27.08.2018 16:16:40

Edit Preview Message ▾ Preview Lure ▾

Employee Survey HR Portal

The employee is asked to log on to an HR portal to take part in an internal survey.

27.08.2018 16:14:11

Edit Preview Landing ▾ Preview Message ▾ Preview Lure ▾

Happy Christmas Greeting Card

Happy Christmas Greeting Card

27.08.2018 16:10:35

Edit Preview Message ▾ Preview Lure ▾

HR Performance Report 1.1

HR performance report. Shows employees their performance report after they log in.

27.08.2018 16:12:06

Edit Preview Landing ▾ Preview Message ▾ Preview Lure ▾

Message from HR

This scenario is based on a phishing scam from 2017 which was targeting companies with the subject "You have a message from HR".

17.12.2018 17:13:03

Edit Preview Landing ▾ Preview Message ▾ Preview Lure ▾

Message from HR (hyperlink)

This scenario is based on a phishing scam from 2017 which was targeting companies with the subject "You have a message from HR".

17.12.2018 17:13:03

Edit Preview Message ▾ Preview Lure ▾

1 100 ▾

- **Simultaneous attack template usage:** LUCY gives you the option to use multiple simulated attack templates in a single campaign. Mix the different types (hyperlink, file-based, etc.) with different attack themes to achieve the largest possible risk coverage and a better understanding of employee vulnerabilities. In combination with our scheduling randomizer, complex attack patterns can be executed over a longer period of time.

481 new templates available! Download

Campaign Status: Running

Export New Scenario

Delete

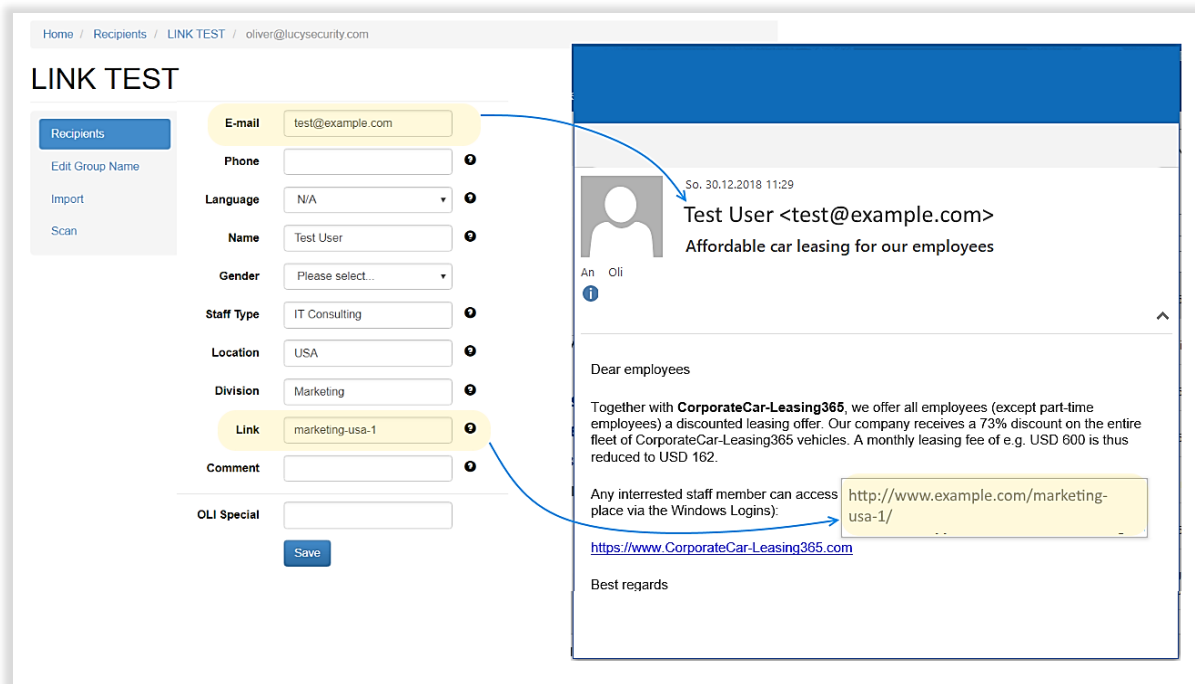
Search...

Scenario	Template	Type	Active
Google Leaks	Google Leaks / German	Web Based	✓
DropBox	Dropbox 1.2 / German	Web Based	✓
Linkedin	Linkedin - Policy Violation / English	Hyperlink	✓
eFax	eFax Corporate v. 2.1 (Download PDF only) / English	Web Based	✓
Private Message	Private Message - enter code to open it / English	Web Based	✓

1 10 ▾

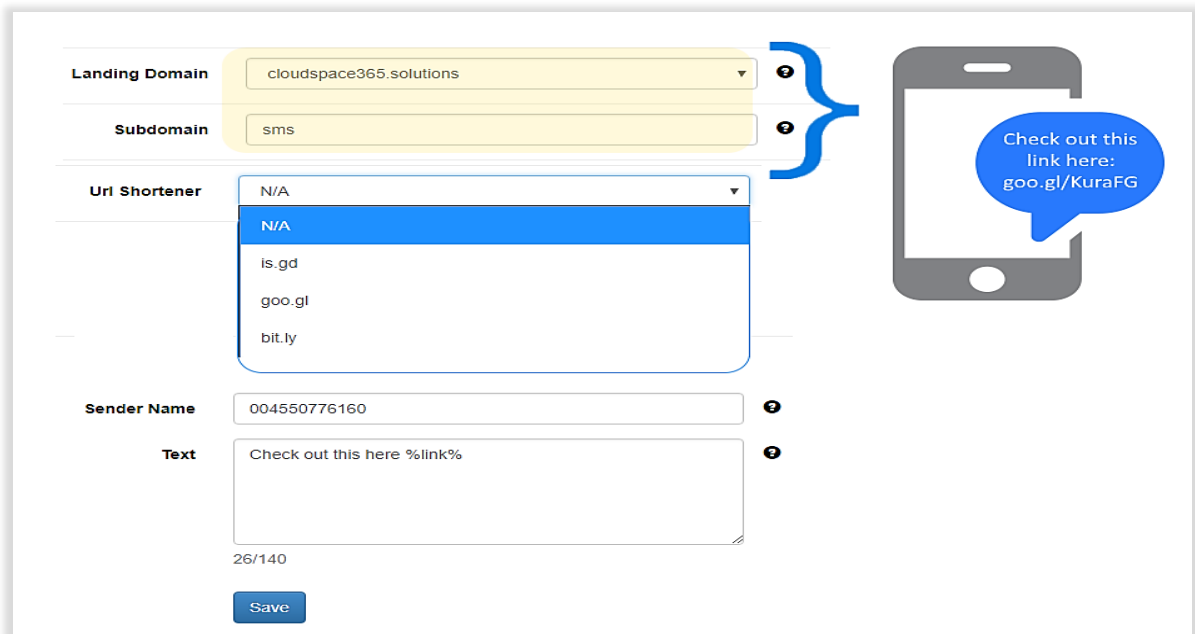
Advanced Settings

- Attack URL variations:** Take control of the generated URLs to identify the recipients. Use automated short (< 5 characters) or long URL strings or set individual URLs for each user. The manual URL creation allows you to form links that a user can easily remember. In environments where link clicks are disabled in e-mails, this is a must.



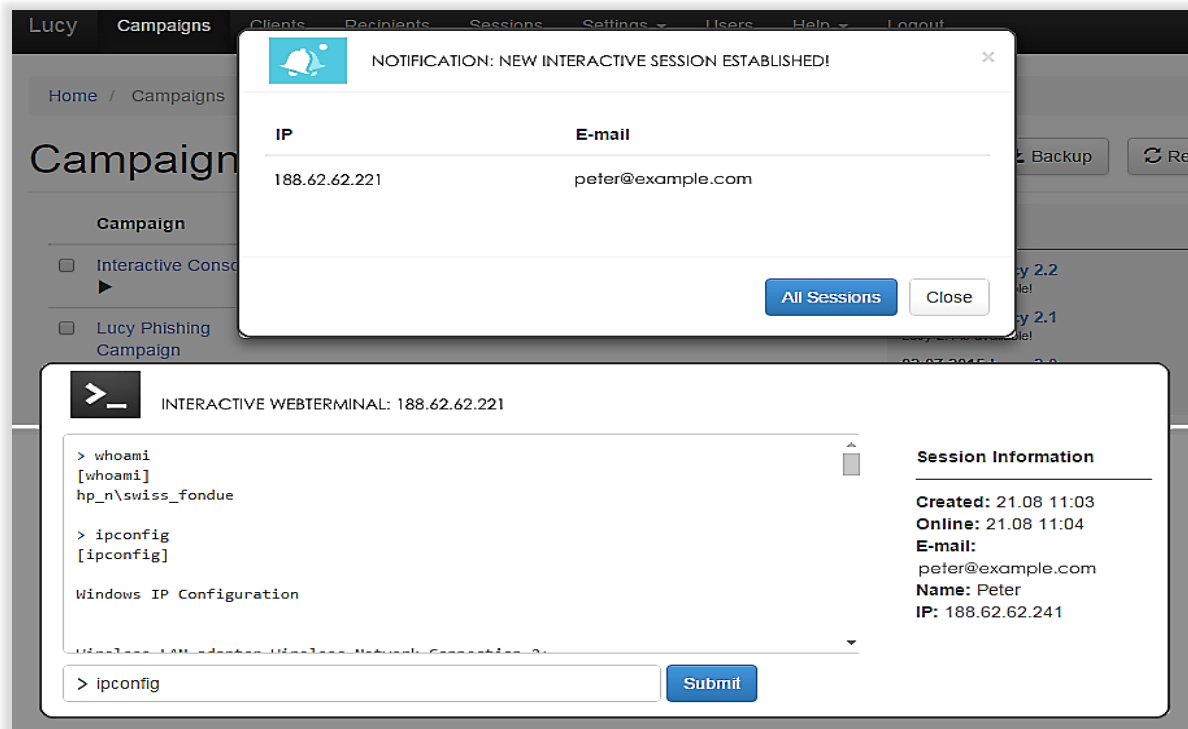
The screenshot shows the 'LINK TEST' interface. On the left is a sidebar with 'Recipients' and options like 'Edit Group Name', 'Import', and 'Scan'. The main form contains fields for 'E-mail' (test@example.com), 'Phone', 'Language' (N/A), 'Name' (Test User), 'Gender' (Please select...), 'Staff Type' (IT Consulting), 'Location' (USA), 'Division' (Marketing), 'Link' (marketing-usa-1), 'Comment', and 'OLI Special'. A 'Save' button is at the bottom. On the right is a preview of the generated email. The email header shows 'Test User <test@example.com>' and 'Affordable car leasing for our employees'. The body text reads: 'Dear employees', 'Together with CorporateCar-Leasing365, we offer all employees (except part-time employees) a discounted leasing offer. Our company receives a 73% discount on the entire fleet of CorporateCar-Leasing365 vehicles. A monthly leasing fee of e.g. USD 600 is thus reduced to USD 162.', 'Any interested staff member can access place via the Windows Logins:', and two links: 'http://www.example.com/marketing-usa-1/' and 'https://www.CorporateCar-Leasing365.com'. A blue box highlights the first link, and a blue arrow points from the 'Link' field in the form to this link in the preview.

- URL shortening:** URL shorteners are a relatively new Internet service. As many online social services impose character limitations (e.g., Twitter), these URLs are very practical. URL shorteners, however, can be used by cyber criminals to hide the real target of a link, such as phishing or infected websites. For this reason, LUCY offers the possibility to integrate different shortener services within a phishing or smishing campaign.

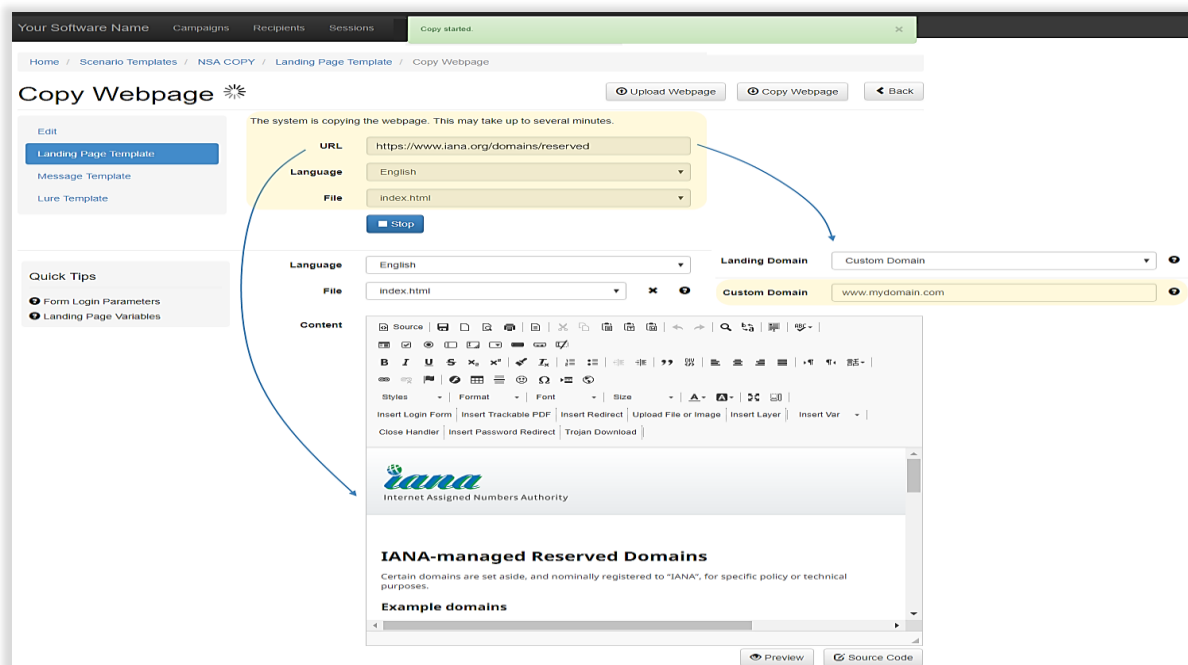


The screenshot shows the 'URL Shortener' interface. The form has fields for 'Landing Domain' (cloudspace365.solutions), 'Subdomain' (sms), 'Uri Shortener' (N/A), 'Sender Name' (004550776160), and 'Text' (Check out this here %link%). A dropdown menu for 'Uri Shortener' is open, showing options: N/A, is.gd, goo.gl, and bit.ly. A blue box highlights the 'Uri Shortener' field, and a blue arrow points from this box to a smartphone icon on the right. The smartphone screen displays a blue speech bubble with the text: 'Check out this link here: goo.gl/KuraFG'.

- **Pentest kit:** The pentest kit is a submodule of the malware simulation toolkit and goes by the name "Interactive Sessions." It allows you to communicate interactively with a client pc that sits behind firewalls by using reverse http/s connections.



- **Website cloner:** Quickly create highly professional landing pages for your campaigns. Clone existing websites and add additional layers with data entry fields, files for download, and more.



- **Level-based attacks:** Level-based phishing training for employees serves to make the risk of social hacking measurable. Scientific analysis should also identify the most important risk factors so that individual training content can be offered automatically.

The screenshot shows the 'New Campaign' setup interface. The top navigation bar includes 'Your Software Name', 'Campaigns', 'Recipients', 'Sessions', 'Incidents', 'Settings', 'Support', 'Status', 'Tools', and a user profile icon. The breadcrumb trail is 'Home / Campaigns / New Campaign'. The main heading is 'New Campa...' with a sub-header 'Campaign Status: Not Started'. A 'New Campaign' button is on the left. The form includes fields for 'Name', 'Client', and 'Industry'. A 'Notes' text area is on the right. The 'Setup Mode' section has radio buttons for 'Expert Setup (Manual Configuration)', 'Pre-selected 5 minutes setup', 'Launch a saved campaign template', and 'Level based campaign' (selected). Below this, a yellow box contains 'Please choose a rule set' with dropdowns for 'Go up one level', 'Stay in level', and 'Go down one level'. Another yellow box contains 'Please choose start & end level' with dropdowns for 'Minimum Start Level' and 'Maximum End Level'. The 'Infrastructure testing' section has radio buttons for 'Start a mail- and webfilter check campaign' and 'Start a local windows check campaign'. The 'E-Learning Settings' section has checkboxes for 'Enduser Profiles Enabled', 'Allow Awareness Rescheduling', and 'Ignore repeated answers in Awareness'. The 'Tracking' section has checkboxes for 'Track Responses', 'Email Tracking', and 'Automated Reporting'. There are dropdowns for 'Template', 'Format', 'Font Size', and 'Font Family'. An 'Antivirus/Firewall Protection Interval' dropdown is set to 'off'. A 'View Options' section has a 'Pinned' checkbox. A 'Save' button is at the bottom right.

- **Spear phishing simulation:** The Spear Phish Tailoring works with dynamic variables (gender, time, name, e-mail, links, messages, division, country, etc.) which you can use in landing and message templates.

The screenshot shows the 'Spear Phishing Tailoring' interface. It includes fields for 'Landing Domain' (cloudservices27.com), 'Subdomain' (www), 'Message Type' (Email), 'Language' (English), 'Sender Name' (News), 'Sender E-mail' (news@cloudspace326.com), 'Recipient Header' (To), and 'Fake CC'. The 'Subject' field contains 'Documents for %email% - Internal Use'. The 'Content' field shows a rich text editor with a toolbar. A blue box highlights the 'Insert Var' button in the toolbar. A blue arrow points from the 'Insert Var' button to a list of dynamic variables: '%static%', '%link%', '%name%', '%email%', '%message%', '%link-awareness%', '%division%', '%location%', '%staff-type%', '%comment%', '%gender%', and '%time(FORMAT, OFFSET, ZONE)%'. The preview text in the content area includes: 'Dear %gender("MALE ADDRESSING", "FEMALE ADDRESSING")% %name%', 'You have received an encrypted document for %email% which is accessible via the secure corporate cloud repository until %time("Y/m/d H:i:s", "6000")%. The document is only available for %division%, %location%, %staff-type%.', and 'This message may contain information that is privileged and confidential. If you received this transmission in error, please notify the sender by reply email and delete the message and any attachments.' A 'Save' button is at the bottom right.

- **DKIM / S / MIME Support for Phishing e-Mails:** Digital signatures for e-mails: Send signed phishing simulation mails (s/mime). Use DKIM to get a better sender score.

Home / Campaigns / BOUNCE TEST / Base Settings / test / E-mail Template

**test** Scenario Status: Running Upload Webpage Restore Defaults Clear Attachments Delete All Attachments

**Summary**  
 Scenario Settings  
 Landing Page Template  
**Message Template**  
 Errors

**Quick Tips**  
 E-mail Message Variables

**Message Type** Email

**Language** English

**Sender Name** test

**Sender E-mail** otheres@cloudspace365.solutions

**Recipient Header** To

**Fake CC** ☐

**Subject** Affordable car leasing for our employees

**Embedding Type** Embedded Images

**Attachments**

**General Mail Settings**

**SMTP Fields**

Name	Value
<input type="checkbox"/> High Importance	
<input type="checkbox"/> Receive Confirmation	
<input checked="" type="checkbox"/> X-Mailer Header	

**Custom X-Mailer** Lucy 4.4.8

☐ Message-ID Header

**Advanced Mail Settings**

☒ Receive Sender E-Mail Replies

☐ Send Plain-Text Email

☐ Random E-mail

☒ DKIM Support

**DKIM Subdomain** mail

**Forward E-mail**

**Delivery Method** Use System Settings

☒ Use S/MIME Certificate

Generate Certificate

**SSL Certificate** Choose File No file chosen

**SSL Key** Choose File No file chosen

**SSL Key Password**

**SSL Chain** Choose File No file chosen

Save

**Content**

Source |

Dear employees

Together with **CorporateCar-Leasing365**, we offer all employees (except part-time employees) a discounted leasing offer. Our company receives a 73% discount on the entire fleet of CorporateCar-Leasing365 vehicles. A monthly leasing fee of e.g. USD 600 is thus reduced to USD 162.

Any interested staff member can access the offer under this link (the authorization takes place via the Windows Logins): <https://www.CorporateCar-Leasing365.com>

Best regards

Preview

- **Mail scanner:** Curious which e-mail addresses in your organization can be found on the Internet? Use LUCY's mail scanner and find out what a hacker already knows about your company.

**Mail Scan**

Scan started. ×

The system is searching recipients. This may take up to several minutes.

If Lucy can detect any mail recipients, they will be added automatically in the recipient list of this group.

**Recipients**  
 Edit Group Name  
 Import  
**Scan**

**Domain** phishing-server.com ?

☒ Crawler

☒ Follow external links

Maximum number of URLs to crawl

Maximum crawling time in minutes

☒ Yahoo

☒ Lixam

☒ Wotbox

☒ Yandex

☒ Bing

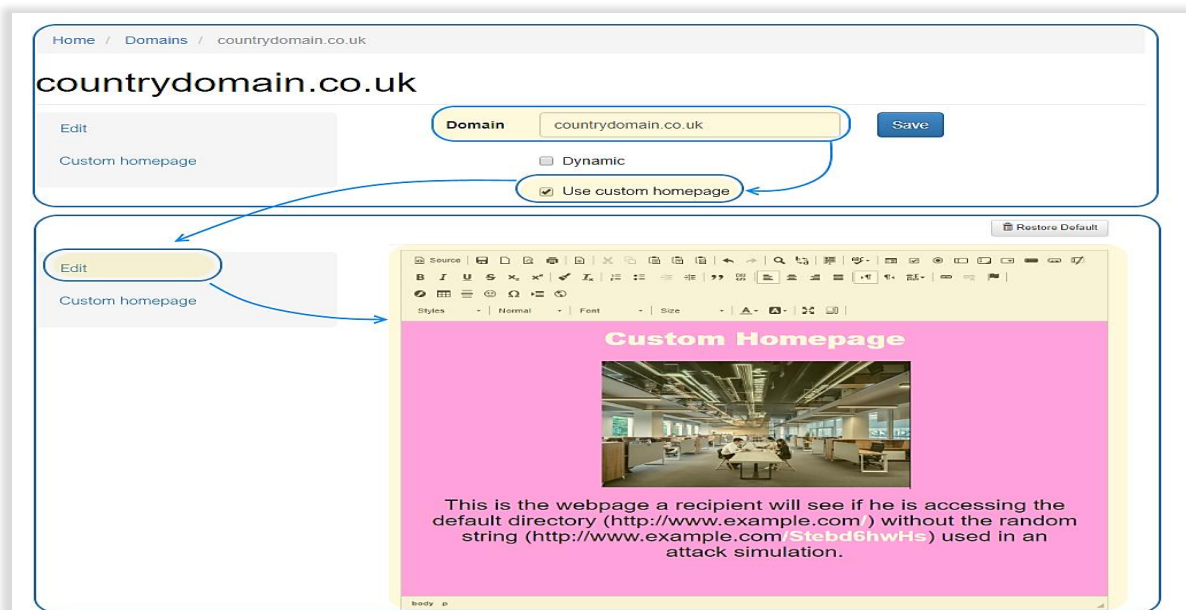
☒ Public Key Servers

☒ Additional Sources

☒ Paid Sources

Stop

- **Custom homepage creation:** Recipients with a better technical understanding could use their browser to call the domain or IP address associated with the randomly generated phishing link. To prevent error messages from appearing or the end user from even coming to the login area of the admin console, you can create generic "homepages" within LUCY for the domains used in the phishing simulation.



## TEST INFRASTRUCTURE

- **Malware Testing Toolkit:** The Malware Simulation Toolkit is an advanced malware simulation suite capable of emulating various threats. It allows an auditor to access an advanced set of features equivalent to many of the tools employed by cyber criminals. The tool, therefore, allows the LUCY administrator to perform security checks without involving employees outside the IT department.

**LUCY MALWARE TESTING SUITE**

General Settings

☐ Enable Http Checks

☐ Http via IE

☐ Http

☐ Http with IE proxy

☐ Http with IE proxy and default credentials

☐ Http with proxy from Firefox

☐ Https

☐ Enable Net Checks

☐ DNS

☐ ICMP

☐ SMTP

☐ FTP

☐ SSH

☐ Enable Windows Checks

☐ OS Version

☐ Local admins

☐ Firewall

☐ Antivirus

☐ Virus downloading

☐ Hosts

**LUCY MALWARE TESTING SUITE**

General Settings

Test started: 10-10-2015 21:08:2015

Test ended: Not yet

Overall Progress:

Start Stop

Current Module: Local windows checks

17. OS version: OK

18. Search for local administrators: OK

19. Check firewall: FAIL

20. Check antiviruses: FAIL

Send Save

**LUCY MALWARE TESTING SUITE**

General Checks Templates

☐ Enable Advanced Dropper

Hours of work (0-23): From: [10] To: [23]

Amount of sessions: [1]

Interval between sessions, minutes: [5]

☐ Enable Ransomware

Place: Temp folder

☐ Use real data ☐ Delete data

☐ Use dummy data

Extensions (separated by commas): docx,pptx,pdf,txt

Files: [1000] Max file size: [512]

Crawl time, minutes: [120]

Amount of file operations: [100000]

**LUCY MALWARE TEST RESULTS**

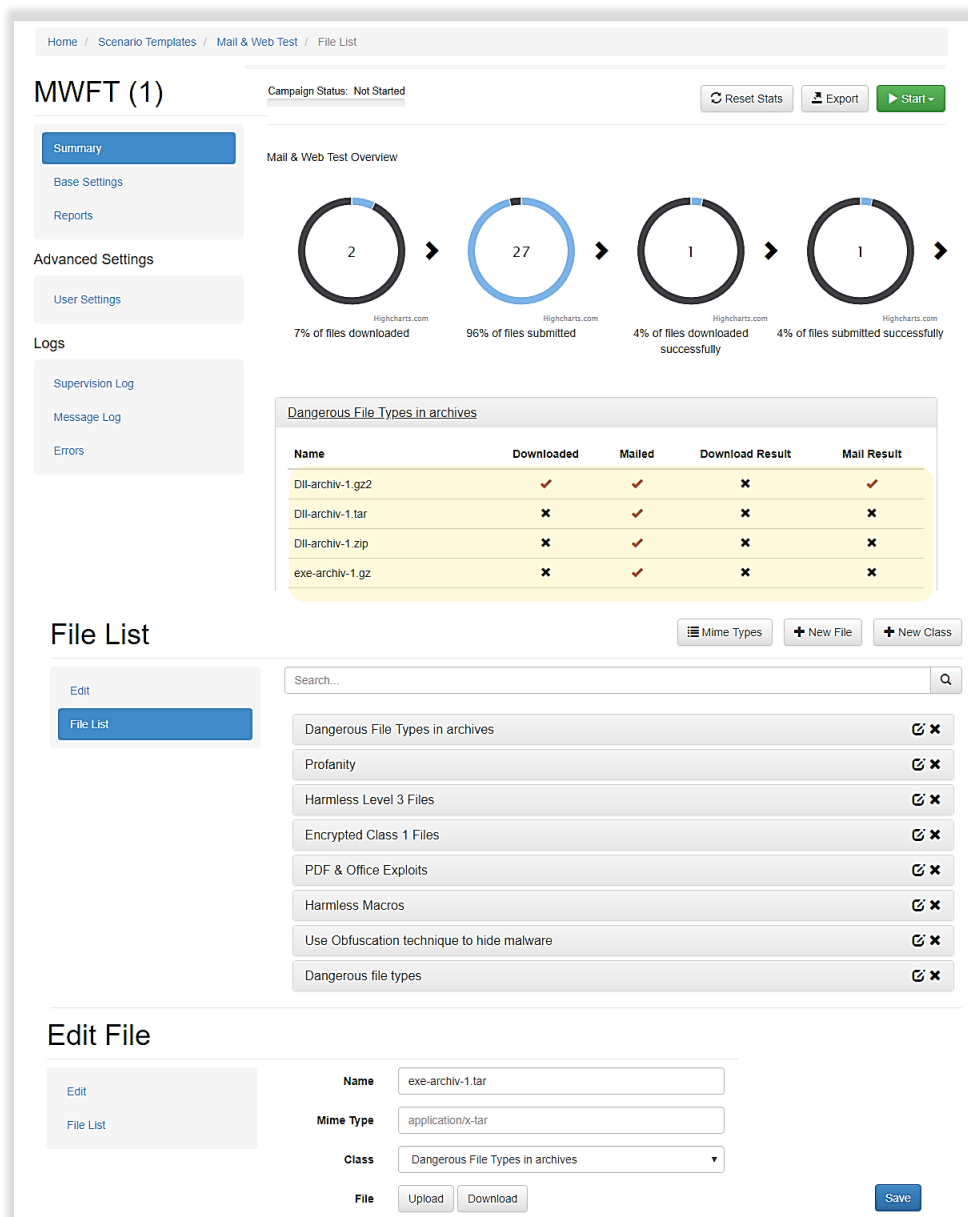
Report Created: 29.07.2015 15:14:03

Malwaretest Version: 1.0

Legend: High Risk Medium Risk Low Risk No Risk

Nr	Test	Info	Result	Status	Risk	Solution
1	Command line access test	View Details	Executed command: whoami (Full output)	Success	Low Risk	View Details
2	Read recent document	View Details	C:\Users\twixw_fundus\Desktop\STH-Example-CommunicationEmails.doc (Full output)	Success	Low Risk	View Details
3	Access to last Outlook e-mail	View Details	Email: john.doe@phishing-server.com Subject: [VPN C] Only last mail and 1st 5 symbols of subject are displayed for privacy reasons	Success	Low Risk	View Details
4	Screenshot	View Details	View Details	Success	Low Risk	View Details
5	Webcam access test	View Details	View Details	Success	Low Risk	View Details
6	Access to Internet via IE	View Details	Received page url: http://www.google.com (Full output)	Success	Low Risk	View Details
7	Access to Internet via a http	View Details	Error occurred: Invalid URI: The hostname could not be parsed. (Full output)	Fail	Medium Risk	View Details
8	Access to Internet via a http with IE proxy	View Details	Error occurred: Invalid URI: The hostname could not be parsed. (Full output)	Fail	Medium Risk	View Details
9	Access to Internet via a http with IE proxy	View Details	Error occurred: Invalid URI: The hostname could not be parsed. (Full output)	Fail	Medium Risk	View Details

- Mail and Web Filter Test:** This functionality provides the answer to one of the most important questions in securing Internet and mail traffic: Which file types can be downloaded from the Web, and which e-mail attachments are filtered out or not?



- **Active and Passive Client Vulnerability Detection:** This feature allows local testing of the client browser and detection of possible vulnerabilities based on custom JavaScript libraries and the browser's user agent data. The discovered plugins can be automatically compared with the vulnerability databases (CVE) to identify vulnerable devices.

test

Scenario Status: Running

Summary

Scenario Settings

Template

Affordable car leasing for employees / English

Change/Select Template

Active Detection

☒ Advanced Information Gathering
 ☒ Browser Details
 ☒ Firebug Information
 ☒ Popup Blocker
 ☒ Geo Location
 ☒ Social Network
 ☒ Proxy

test

Windows 10

Chrome 71

Name

Oli

E-mail

oliver@lucysecurity.com

Phone

—

User History

—

Lure Sent

—

Message Sent

28.12.2018 12:47:54

Training Sent

✓

Reported

—

Success Rate

12.50%

Click Rate

17.50%

Clicks

1

Successful Attack

✓

Trained

—

Out Of Office

—

Bounced

—

Responded

—

Vulnerable Applications (0)

Java SE: 6u201

CVE link

Plugins

ActiveTouch General Plugin Container 106  
 Mozilla Default Plug-in 1.0.0.15  
 Google Update 1.3.33.23  
 Zoom launcher - 3.0.1  
 Lifesize WebRTC plugin 1.0.22.0  
 Skype for Business Web App Plug-in 15.8  
 Skype Meetings App 16.2.0.242  
 Java Deployment Toolkit 8.0.1810.13  
 Java SE: 6u201

Advanced Information Gathering

Browser Version

5.0 (Windows NT 10.0; Win64; x64)

Browser Language

en-US

Browser Platform

Win32

Window Size

1536 x 824

Cookies Enabled

✓

Silverlight

—

Google Gears

—

WMP

—

SVG Viewer

—

Flash

—

Websocket

✓

Firebug

—

Geolocation

—

WebRTC

✓

VBScript

—

Quicktime

—

RealPlayer

—

ActiveX

—

Java

—

Proxy

—

Popup Blocker

—

Social Networks

google

Campaign Status: Running

Generated: 28.12.2018 12:54

Operating Systems

Browsers

Top Plugins

Extended Analysis


- **Spoofing Test:** Test your own infrastructure for mail spoofing vulnerabilities.

[Home](#) / [Mail Spoofing](#)

## Mail spoofing test

**Domain**

**Recipient Email**



Console Window

```

220 mx00.udag.de ESMTP ready
EHLO phishing-server.com
250-mx00.udag.de
250-SIZE 51200000
250-ETRN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-STARTTLS
MAIL FROM:
250 2.0.0 OK
RCPT TO:
250 2.1.5 Ok
DATA
354 End data with .
This is a test, please do not respond
.
250 2.0.0 Ok: queued as 2F085257DD


```

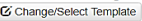
Alert! Mail Spoofing seems possible

## TECHNICAL TESTING


- **Reputation-Based e-Learning:** Train your employees according to their required skills. Measure employee abilities and enable friendly competition between colleagues (gamification). Based on the reputation profiles of each end user, the system can automatically provide them with multiple training sessions. The reputation profiles are based, among other factors, on the user's behaviour in phishing simulations. This ensures that users who are repeated offenders receive different training content from those who click on an attack simulation for the first time.


[Summary](#)
[Scenario Settings](#)
[Mail Settings](#)
[SSL Settings](#)
[Landing Page Template](#)
[Message Template](#)
[Errors](#)


**Template**
Affordable car leasing for employees /  English




**Name**

☒ Send Link to Awareness Website Automatically 

**Send Awareness By Click Rate**
 % 

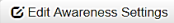
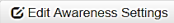
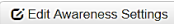
**Send Awareness By Success Rate**
 % 

**Awareness Delay**
 

[Export](#)
[+ New Awareness](#)

**Configuration**

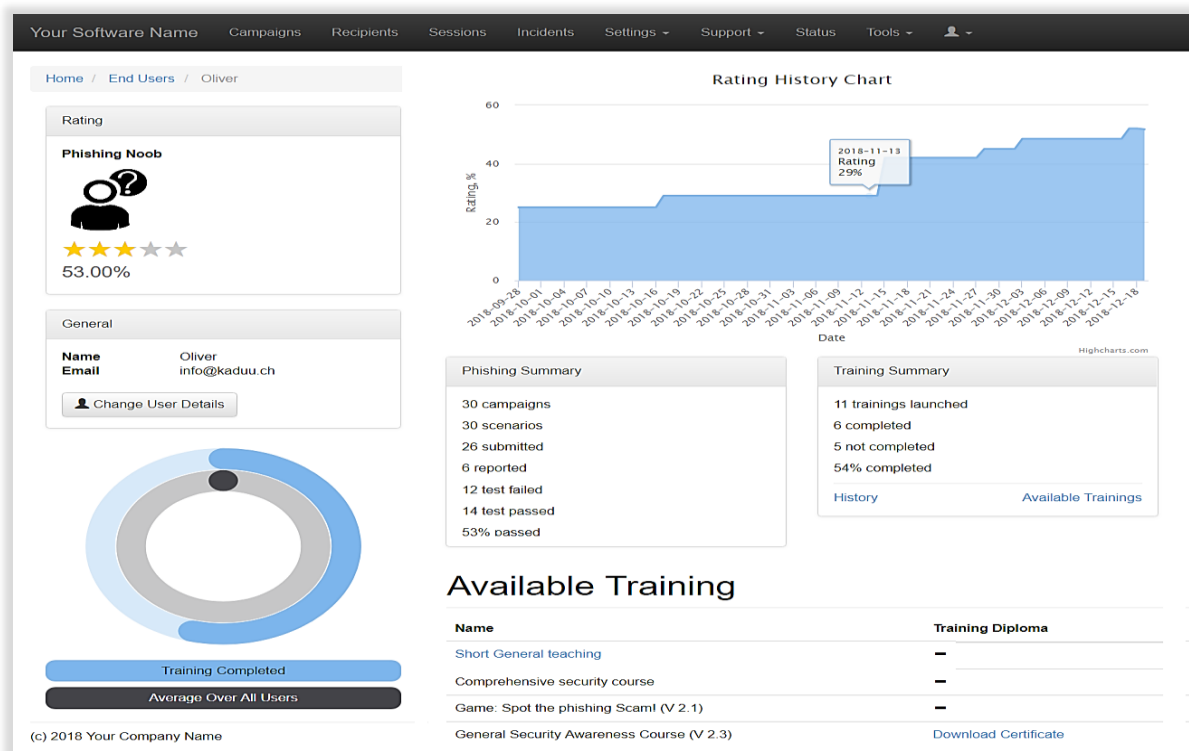
[Base Settings](#)
[Awareness Settings](#)

Awareness		Course	Risk Level			
Comprehensive security course		Comprehensive security course	0	+	-	x
Repetition Course		Avoid & Recognize Phishing Attacks (V 2.3)	2	+	-	x
Short General teaching		Email Only - This was a phishing simulation & Tips	3	+	-	x

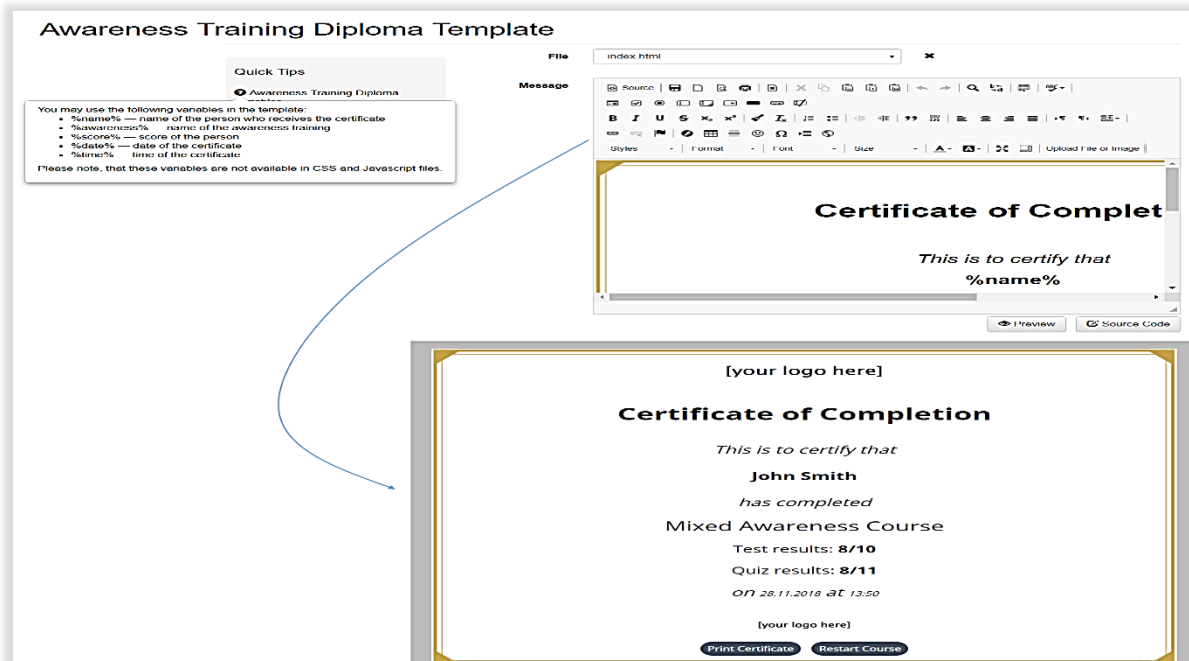
< 1 >

10

- **End user Training Portal:** Learning Management System (LMS) functionality: Gives each employee permanent access to a personalized training homepage that features your own courses specifically tailored for them. On this homepage they can view their performance statistics, resume or repeat training, create course certificates, and compare their results with other departments or groups.



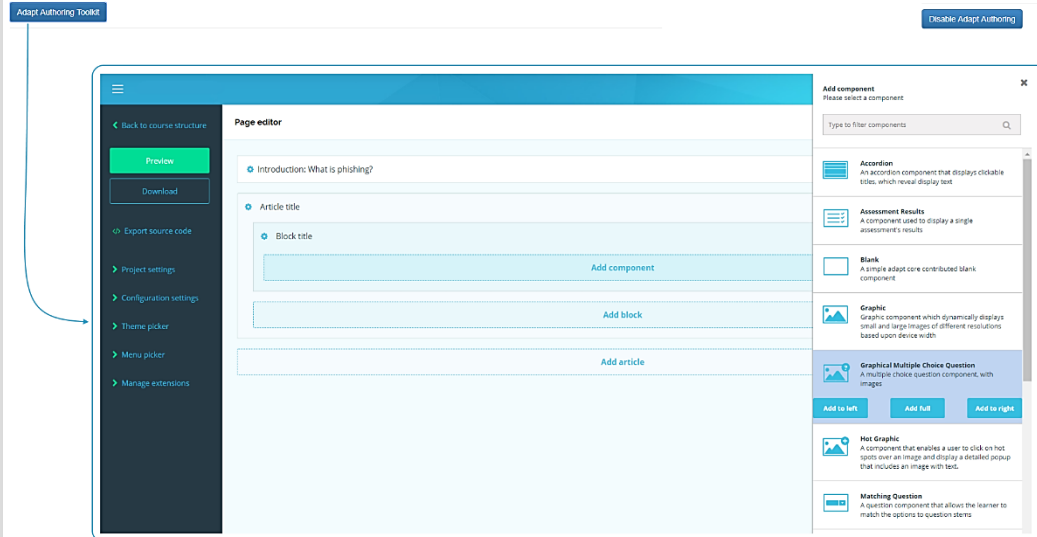
- **Awareness Education Diploma:** Certificates of e-Learning can be created and printed out by the recipient either directly within a training or inside the LMS portal.



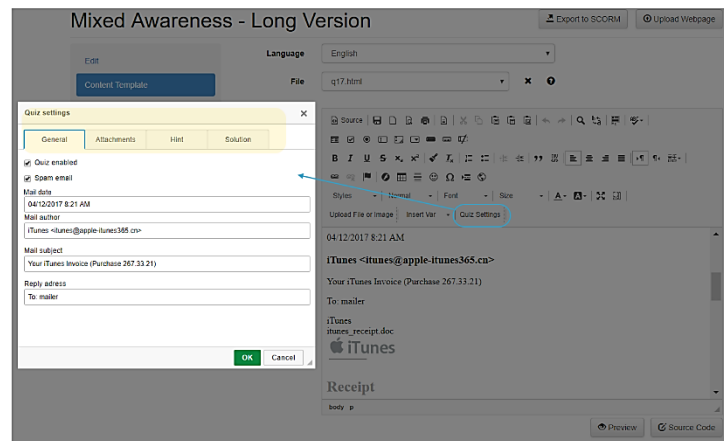
- **e-Learning Authoring Toolkit:** The e-Learning Authoring Toolkit (Adapt) allows the creation of individualized learning content. Drag and drop videos or any other rich media format, insert exams from pre-defined menus, create interactive e-learning content from scratch in a short time.

## Adapt Authoring Toolkit

Press the button below to open Adapt Authoring Toolkit in a new window.





## Quick Quiz Editor



- **Rich Media Awareness Training:** Integrate rich media (video, audio, or other elements that encourage viewers to interact and engage with the content) in your awareness trainings. Use the existing educational videos, adapt them, or add your own rich media.

### Handouts



**Hand out: Comprehensive security course (PDF/PPT)** 


Topics in this course include "SHOULDER SURFING", "PORTABLE MEDIA ATTACKS", "VISHING (COLD CALLING)", "CLEAR DESK POLICY", "PHYSICAL SECURITY", "VISITORS AND IN-PERSON INTERACTION", "SOCIAL ENGINEERING", "PASSWORD SECURITY", "SECURE BROWSING", "SECURE SOCIAL NETWORKING", "USING PUBLIC WI-FI'S", "MOBILE SECURITY". The PDF is embedded in this static web page. The PowerPoint template is located within this template folder. You can download it: click on the left navigation item "content template" -> select the button "upload file or image" within the editor pane -> click "search server" to access the file manager in LUCY -> click "download". After you make desired changes to the word file, please save it as a PDF with the name "Info.pdf" and upload back to your LUCY instance using the file manager within this template. All content is 100 % customizable. Duration: 60-80 Minutes | Skill Level: Medium | Audience: All | Interactive: No


30.10.2018 09:23:50

Edit Preview Website Preview E-mail

...and many more

### Games



**Spot the difference!** 


In this game the user is shown two very similar photos of everyday security situations. The user has to find the differences in the picture. At the same time he learns how to protect himself against various security risks in his company by displaying explanatory texts. Time: 15-20 minutes | Interactive: Yes | Category: Games


15.11.2018 17:44:27

Edit Preview Website Preview E-mail

...and many more

### Posters



**POSTER - "Password Mobile" (illustration)** 


This template includes a poster (illustration) with the topic: "Password Mobile". If you want to edit the poster or process it for printing, please click on the navigation item "Content Template" to the left, then within the visual editor click the button "Upload File or Image". Within the tab "Image Info" please click on "search server" to download the Adobe Illustrator file.


27.08.2018 16:13:19

Edit Preview Website Preview E-mail

...and many more

### E-Learning libraries



**Awareness Training Library** 


This template offers the possibility to link all existing LUCY training modules in a directory. The end user can then put together his desired training modules himself on an overview page


27.08.2018 16:16:37

Edit Preview Website Preview E-mail

...and many more

### Videos



**Secure social media usage video (close caption)** 


In this security awareness video we talk about secure social media usage. The video has English subtitles. The content (animation, language, script) is customizable. More info about customization can be found here: <https://goo.gl/1XN9SG>. Duration: 5:40 minutes | Skill Level: Low | Audience: All | Interactive: No | Video stats possible: Yes


27.08.2018 16:13:54

Edit Preview Website Preview E-mail

...and many more

### Screensavers



**Screensaver: Security Illustrations (.src)** 


This screensaver, designed for a resolution of 1366x768 px, contains a series of illustrations on the subject of cybersecurity awareness. The illustrations (text or image) can be easily customized using Adobe Photoshop files inside the posters. The screensaver can be downloaded from the template. With the right mouse button you can install it in window.


15.11.2018 17:44:28

Edit Preview Website Preview E-mail

...and many more

### E-Mail only courses



**Email Only - This was a phishing simulation & Tips** 


This is a template that does not have a web page integrated. The employee is informed about the phishing simulation and receives a few tips on how to better detect such attacks in the future.


27.08.2018 16:13:25

Edit Preview E-mail

...and many more

### Static courses



**Prevent Phishing Attacks: 5 Tips (Version 2.1)** 


This static course contains 5 basic tips on how to prevent phishing attacks. Duration: 5 Minutes | Skill Level: Low | Audience: All | Interactive: No


27.08.2018 16:14:11

Edit Preview Website Preview E-mail

...and many more

### Interactive Courses



**Phishing, Spoofing & CEO Fraud** 


In this course the student will be guided through various lessons. Topics covered include "Phishing", "Spoofing" & "CEO Fraud". These topics are covered in tips, static learning content, a quiz and a multiple-choice test. Only after completion of a chapter, a new one can be started. At the end of the training the participant can create a certificate with the exam results. Details on the configuration can be found in readme.html. Duration: 20-30 Minutes | Skill Level: Medium | Audience: All | Interactive: Yes


15.11.2018 17:44:27

Edit Preview Website Preview E-mail

...and many more

### Exams



**Internet Security Exam 1.2** 


In this short quiz, the user is asked nine multiple choice questions in order to test their knowledge regarding internet security (email security, privacy, password security, etc.). Duration: 10-15 Minutes | Skill Level: Low | Audience: All | Interactive: Yes


27.08.2018 16:12:54

Edit Preview Website Preview E-mail

...and many more

### Micro Modules



**One Pager Phishing Awareness (responsive | 1.2)** 


This is a static one page long phishing awareness html template. It works with a min resolution of 360 pixels.


27.08.2018 16:14:22

Edit Preview Website Preview E-mail

...and many more

### Security News



**News: Do you know how to handle security incidents** 

This course covers security incidents and the processes involved in reporting such incidents.

28.12.2018 14:48:47

Edit Preview Website Preview E-mail

...and many more

- **Training Library:** Your employees can access your organization's training content from an overview page called "training library." It contains a large selection of LUCY's regular e-learning templates, which serve as input. The overview page can be sorted by certain topics (video, quiz, test, etc.).

**Awareness Templates**

library

Awareness Training Library

Security Awareness Video Library

**Library**

Quick Tips

Create Custom Video

**IT SECURITY TRAINING LIBRARY**

- **Static Training Support:** Training content can also be published on static pages within LUCY or the intranet, giving the user permanent access to training content, independent of possible attack simulations.

**Base Settings**

Website

SSL Settings

Message

Mail Settings

**Quick Tips**

Awareness We

Quiz Integration

Create Custom

**Domain** static.training-link.com

☒ Quiz

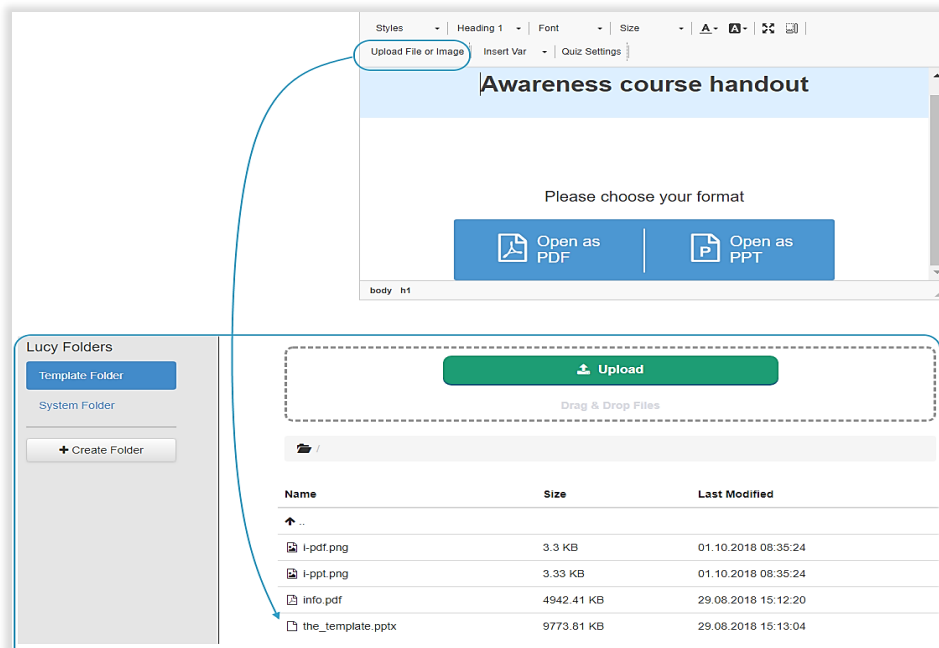
**Link** http://static.training-link.com/awareness/291a76f987a542b38b466aed6d240b42a1a77f05f351c2c882d9a8ce5716dd35/11/index.html

**Language** English

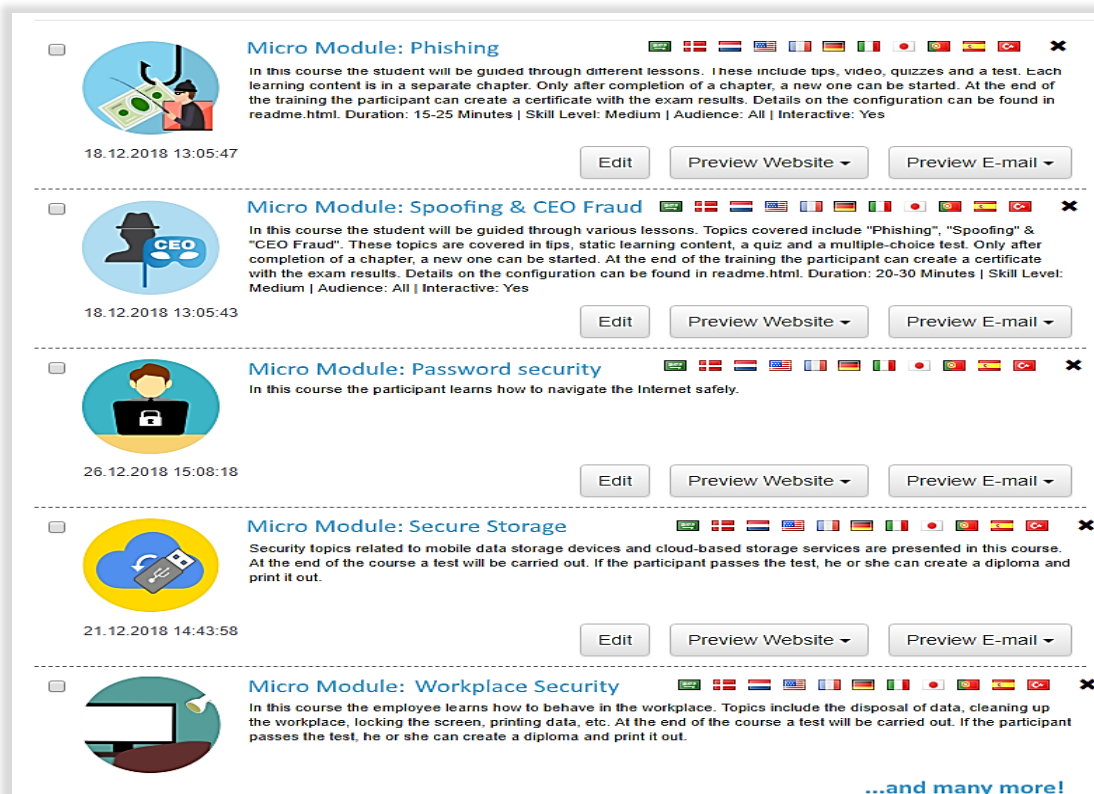
https://static.training-link.com/awareness/291a76f987a542b38b466aed6d240b42a1a77f05f351c2c882d9a8ce5716dd35/11/index.html

PayPaul

- **Offline Training Support:** LUCY is supplied with a series of editable templates (Adobe Photoshop or Illustrator files) for awareness training, such as posters, screensavers, fliers, etc.

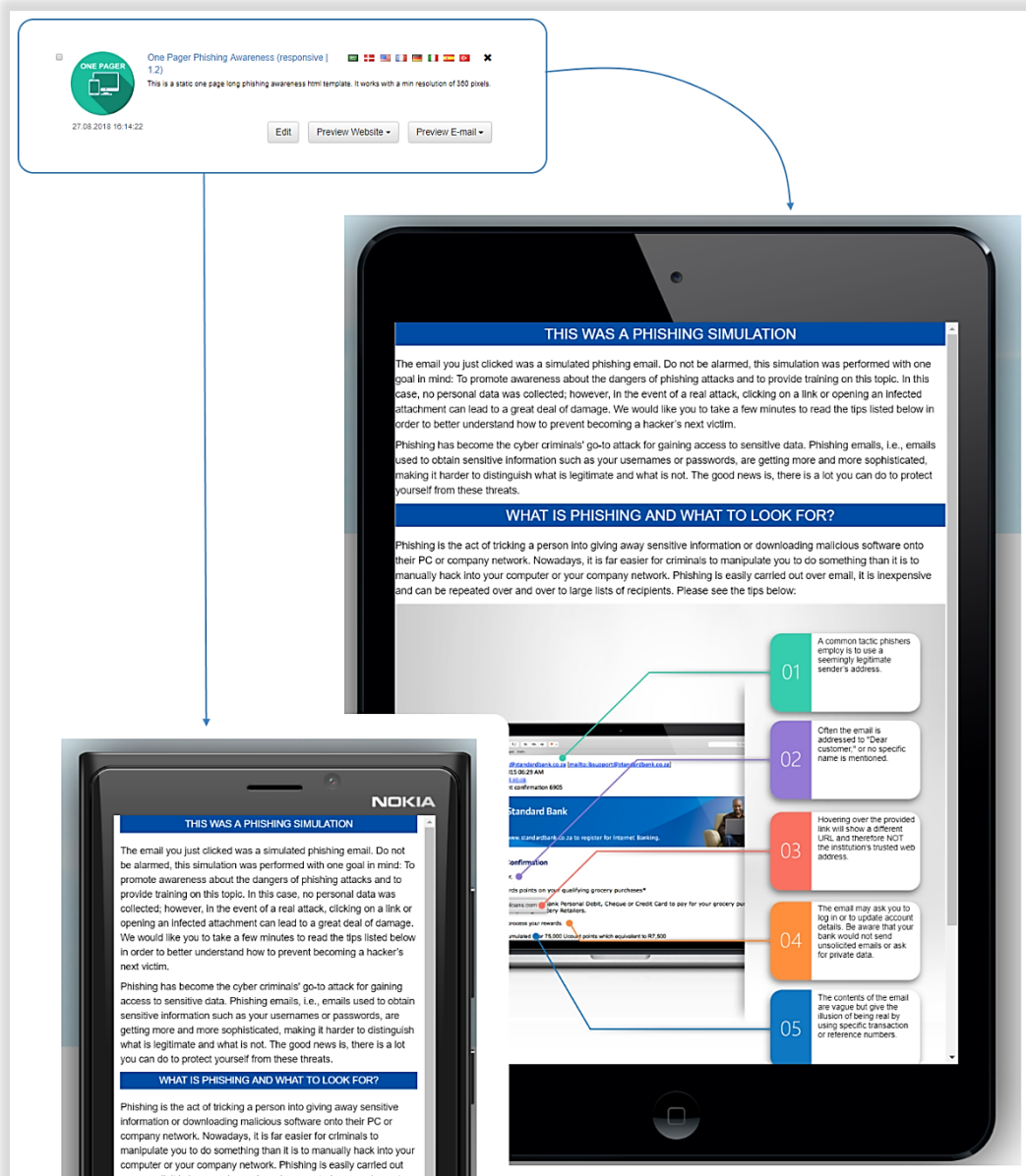


- **Microlearning Modules:** We have designed microlearning training modules (e.g., 1-minute videos or awareness 1-pagers) that can be tailored to the branding and policy needs of your organization.





- Mobile-Responsive Format:** Many of LUCY's built-in modules are available in a mobile-responsive format that gives your users the flexibility to take the training on any type of connected device.



- **Video Import/Export:** You can export LUCY videos to your own system as well as import your own videos into LUCY.

The screenshot displays the 'Awareness Templates' interface. At the top, there's a search bar and view toggles (List View, Grid View). A video titled 'Data Privacy & GDPR Video' is highlighted. Below it, a 'Lucy Folders' sidebar shows options like 'Template Folder', 'System Folder', 'Create Folder', 'Rename', 'Copy', 'Move', 'Download', and 'Delete'. The 'Download' button is circled. The main area shows a file list with columns 'Name', 'Size', and 'Last Modified'. Files listed include 'flowplayer', '2018.06.11\_Lucy Data Privacy.mp4', '2018.06.11\_Lucy Data Privacy.webm', and 'jquery.js'. An 'Upload' button and a 'Drag & Drop Files' area are also visible.

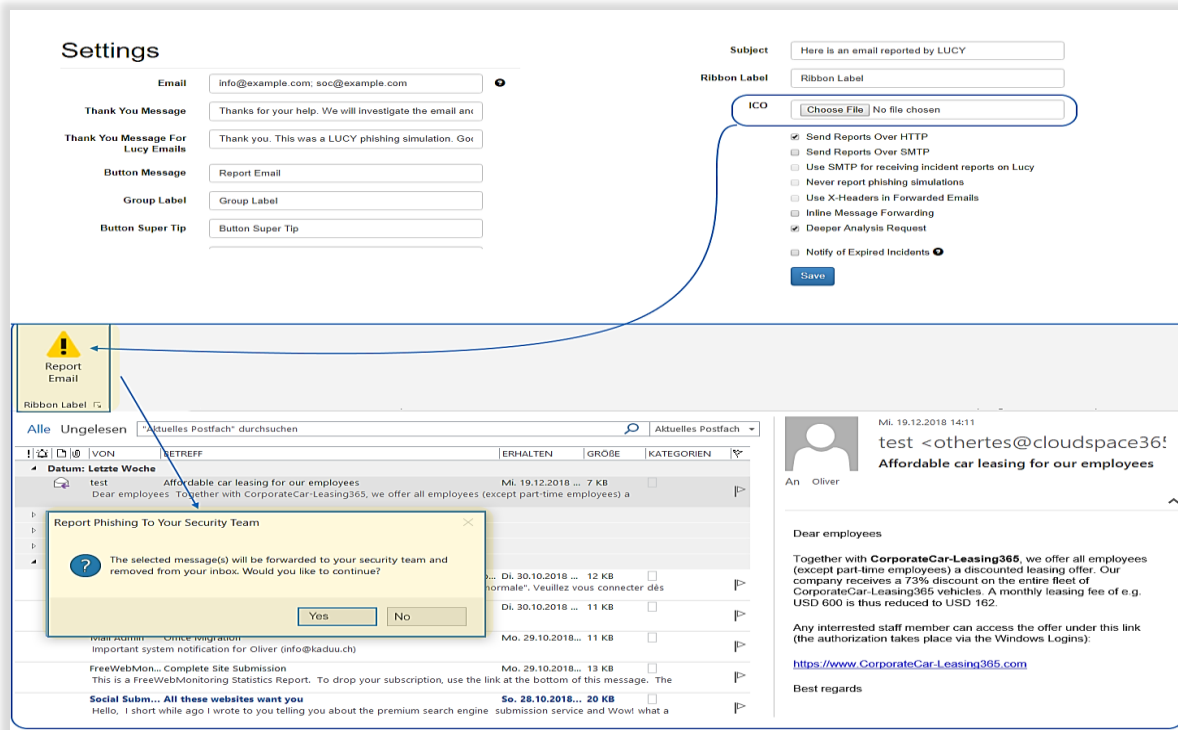
- **Dynamic Training Hints:** The implemented dynamic hints allow your administrator to set markers within the attack templates that could indicate to your employees, inside the e-learning material, where the phishing attack may have been detected.

The screenshot shows the 'Comprehensive security course' interface. On the left, there's a sidebar with 'Edit', 'Content Template', and 'E-mail Template' options. The 'Content Template' option is circled. The main area displays course details like 'Language' (English) and 'File' (index.html). A toolbar with various editing tools is visible. At the bottom, there's an 'Exports' section with a table listing export records. The 'Export to SCORM' button is circled. A 'scorm-export.zip' file is shown as a download icon.

Date	Name	Extension	Status
31.12.2018 15:08:53	Awareness Template - Comprehensive security course		✓
29.12.2018 17:10:15	Campaign - BOUNCE TEST	csv	✓
28.12.2018 15:19:11	Awareness Template - Avoid & Recognize Phishing Attacks (V 2.3)		✓

## ENGAGE EMPLOYEES

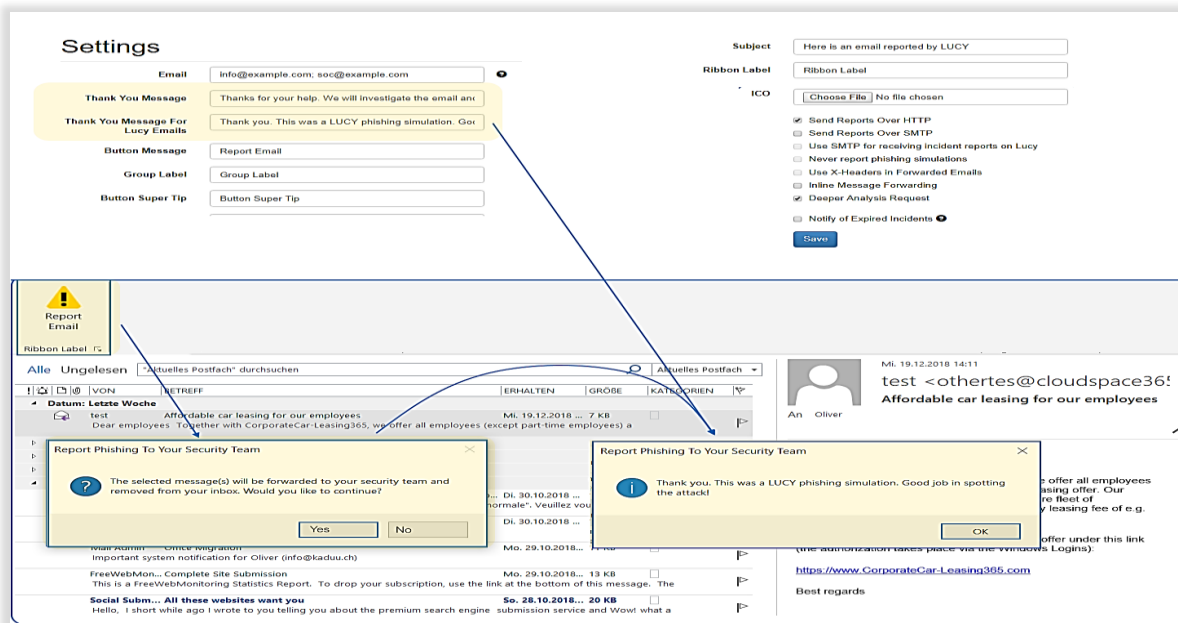
- Report E-mails with a single click:** End users can report suspicious e-mails with a single click to one or multiple e-mail accounts and have them forwarded to your LUCY incident analysis console. Your employees, inside the e-learning material, where the phishing attack may have been detected.



The screenshot displays the LUCY Settings and Email interface. On the left, the 'Settings' panel includes fields for 'Email' (info@example.com, soc@example.com), 'Thank You Message', 'Thank You Message For Lucy Emails', 'Button Message' (Report Email), 'Group Label', and 'Button Super Tip'. On the right, the 'Subject' field is set to 'Here is an email reported by LUCY', and the 'Ribbon Label' is 'Ribbon Label'. Below these, there are checkboxes for various reporting options: 'Send Reports Over HTTP' (checked), 'Send Reports Over SMTP' (unchecked), 'Use SMTP for receiving incident reports on Lucy' (unchecked), 'Never report phishing simulations' (unchecked), 'Use X-Headers in Forwarded Emails' (unchecked), 'Inline Message Forwarding' (checked), 'Deeper Analysis Request' (checked), and 'Notify of Expired Incidents' (checked). A 'Save' button is at the bottom right of the settings panel.

The main email interface shows a list of emails. A 'Report Email' button is visible in the top left corner. A confirmation dialog box titled 'Report Phishing To Your Security Team' is open, asking: 'The selected message(s) will be forwarded to your security team and removed from your inbox. Would you like to continue?'. The dialog has 'Yes' and 'No' buttons. A blue arrow points from the 'Report Email' button in the settings panel to the 'Report Email' button in the email interface.

- Positive Behavior Reinforcement:** Our plugin automatically provides positive behaviour reinforcement by showing gratitude to end users via a custom message defined by your organization.



This screenshot shows the LUCY Settings and Email interface with a custom message defined for positive behavior reinforcement. The 'Settings' panel on the left is identical to the previous screenshot, but the 'Thank You Message' field is now set to 'Thank you. This was a LUCY phishing simulation. Good job in spotting the attack!'. The 'Button Message' field is still 'Report Email'.

The main email interface shows the same list of emails. A confirmation dialog box titled 'Report Phishing To Your Security Team' is open, displaying the custom message: 'Thank you. This was a LUCY phishing simulation. Good job in spotting the attack!'. The dialog has 'Yes' and 'No' buttons. A blue arrow points from the 'Report Email' button in the settings panel to the 'Report Email' button in the email interface.

- **Deep inspection request:** Sometimes users want to know if the received e-mail can be opened safely. The user can optionally use the “deep inspection request” within the local plugin to tell the security team that he wants feedback on the reported e-mail.

**Settings**

Email: info@example.com; soc@example.com ⓘ

Thank You Message: Thanks for your help. We will investigate the email and

Thank You Message For Lucy Emails: Thank you. This was a LUCY phishing simulation. Go

Deeper Analysis Request Message: Deeper Analysis Request Message

**Email List**

VON	BETREFF	ERHALTEN	GRÖÖE	KATEGORIEN
<b>Datum: Vorletzte Woche</b>				
Jessie	Behold is nice offer	So. 16.12.2018 ...	6 KB	
Hi What we have here is an interesting offering Just click on the link below to qualify				
lottery	Look at an amaz			
Hy there Good news ! a good o				
Верська	Here is an intere			
Hi Good news ! an important of				
Spenser Geri	Please note nice			
Hey Good news ! an amazing of				
Arnold Sem...	Here is a fine of			
Hey Good news ! an interesting				
Uaytkhed Kolin	That is an interesting offering	Mi. 13.12.2018 ...	5 KB	
Hy there What we have here is an interesting offers Are you in? <http://red.studygood.com/WRKMOAINNX> <Ende>				

**Report Phishing To Your Security Team**

Do you wish to request an additional message analysis from your security team?

Ja Nein

**Phishing Incident Reports**

Send Abuse Delete Delete All Settings

Time	Email	Client	Campaign	Score	Status	
29.12.2018 11:49	oliver@muenchow.ch	Lucy Test	BOUNCE TEST	0.00	Simulation	⚠️ ⓘ ⓧ
19.12.2018 12:12	oliver@muenchow.ch	Lucy Test	BOUNCE TEST	0.00	Simulation	⚠️ ⓘ ⓧ
19.12.2018 10:39	oliver@muenchow.ch	N/A	N/A	4.60	Open	⚠️ ⓘ ⓧ ⓧ
03.12.2018 20:53	oliver@muenchow.ch	Lucy Test	Attack CS	0.00	Simulation	⚠️ ⓘ ⓧ ⓧ

**Filter**

Client: All

From Date: 29.12.2017

To Date:

**Need more analysis**

- Automatic Incident Analysis:** Manage and respond to reported suspicious e-mails using a centralized management console: LUCY analyzer allows an automated inspection of reported messages (header & body). The analyzer includes an individual risk score, providing a real-time ranking of reported e-mails. The Threat Analyzer brings a noticeable relief for the safety team's work load.

Home / Phishing Incident Reports

## Incident Reports

Send Abuse
Delete
Delete All
Settings
Download Plugin

Time	Email	Rating	Client	Campaign	Score	Status
04.07.2018 14:20	oliver@muenchow.ch	★★★★☆	N/A	N/A	0.00	Open
03.07.2018 14:45	oliver@muenchow.ch	★★★★☆	Lucy Test	TEST 123	0.00	Simulation
03.07.2018 08:10	oliver@muenchow.ch	★★★★☆	N/A	N/A	1.00	Open
02.07.2018 10:02	oliver@muenchow.ch	★★★★☆	Lucy Test	LMS Access	0.00	Simulation
02.07.2018 09:54	palo@lucysecurity.com	★★★★☆	N/A	N/A	0.00	Open
02.07.2018 09:54	palo@lucysecurity.com	★★★★☆	N/A	N/A	0.00	Open

Filter
Show only mails from this domain
Search
Reputation Filter
Show only mails with rating > 0
Min Score
From Date
To Date
Status
Email Domain
Update

1 2 3 4 5
10 rows per page

Home / Phishing Incident Reports / 09.03.2018 12:17

### 09.03.2018 12:17

Send Abuse
Rescan

Summary
Header Analysis
Domain Analysis
Body Analysis
Threat Indicators

		Score	Rule active?
Reply-to Mismatch	different reply-to adress defined than the actual (more info...)	1.60	Active <input checked="" type="checkbox"/> Inactive <input type="checkbox"/>
New Domain	Domain has been reserved in the last 30 days (more info...)	20.00	Active <input checked="" type="checkbox"/> Inactive <input type="checkbox"/>
Link Display mismatch	link display name different from the actual link (more info...)	0.00	Active <input type="checkbox"/> Inactive <input checked="" type="checkbox"/>

Summary
Mail Server Analysis
Domain Analysis
Body Analysis

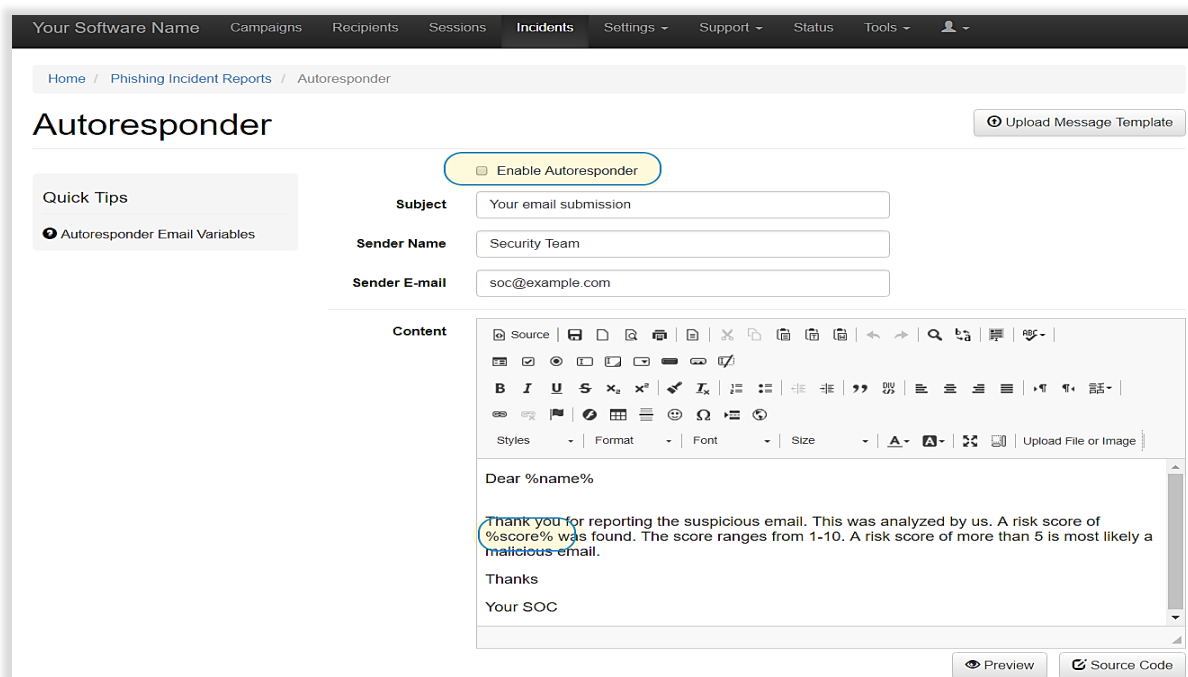
Overall Risk Score:

Need More Analysis

2.5 of 10.0
highcharts.com

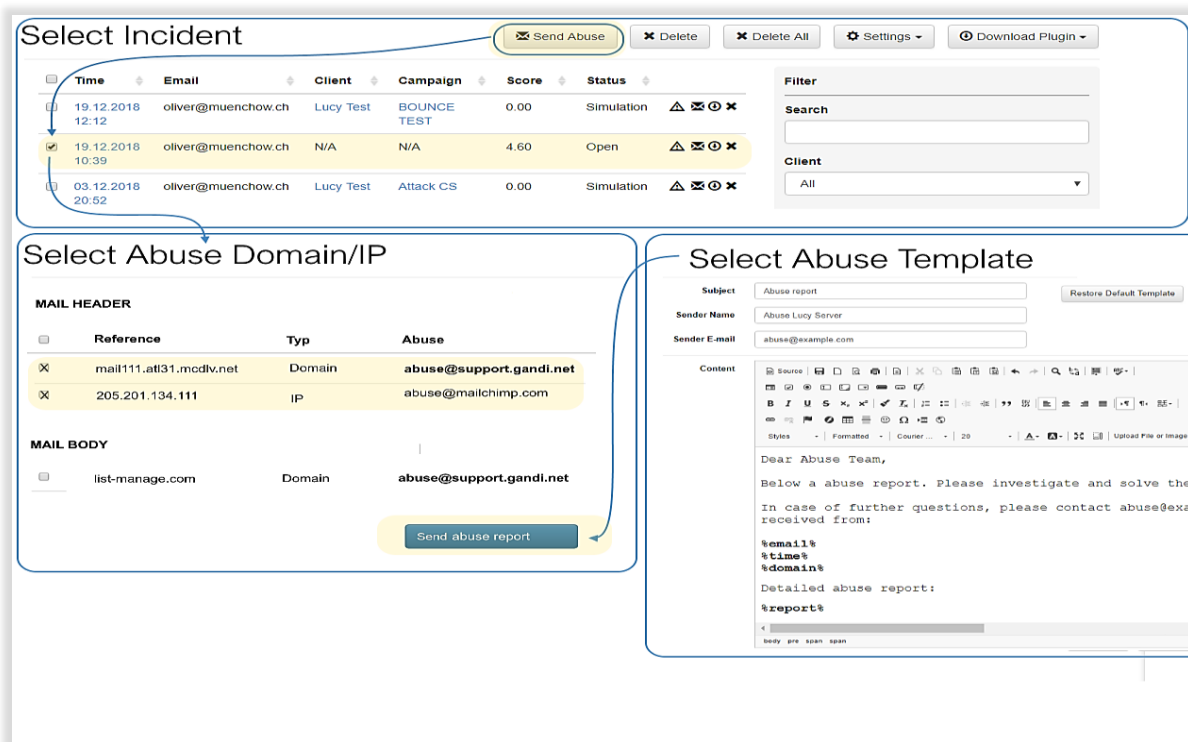
Email: oliver@muenchow.ch
Message: Download
Message Subject: Only 7% of Our Customers Are Doing SEO Right. And You?
Thumbnail:
Report Time: 16.10.2018 09:25:20
Status: In Progress
Notes:
Save

- Incident Auto Feedback:** The Incident Autoresponder allows sending an automated notification to the end user providing the results of the e-mail threat analysis. The message text is freely configurable, and the LUCY E-mail Risk Score can also be included, if required.



The screenshot shows the 'Incidents' tab in the Lucy interface. The 'Autoresponder' section is active, displaying a configuration form. A yellow box highlights the 'Enable Autoresponder' checkbox, which is checked. The form includes fields for 'Subject' (Your email submission), 'Sender Name' (Security Team), and 'Sender E-mail' (soc@example.com). The 'Content' field contains a rich text editor with the following text: 'Dear %name%', 'Thank you for reporting the suspicious email. This was analyzed by us. A risk score of %score% was found. The score ranges from 1-10. A risk score of more than 5 is most likely a malicious email.', 'Thanks', and 'Your SOC'. A yellow box highlights the placeholder '%score%' in the text. The bottom right of the form has 'Preview' and 'Source Code' buttons.

- Threat Mitigation:** The behavioural threat mitigator is a revolutionary approach to eliminating e-mail risks. It will support the security admin in shutting down the attack (e.g., sending an automated report to specified abuse team of providers involved in the attack).



The screenshot shows the 'Threat Mitigation' workflow in the Lucy interface. It consists of three main steps: 'Select Incident', 'Select Abuse Domain/IP', and 'Select Abuse Template'.  
 1. **Select Incident:** A table lists incidents with columns: Time, Email, Client, Campaign, Score, and Status. A yellow box highlights the 'Send Abuse' button above the table. The second row is selected, showing an incident from 19.12.2018 at 10:39, email oliver@muenchow.ch, client N/A, campaign N/A, score 4.60, and status Open.  
 2. **Select Abuse Domain/IP:** A table lists abuse domains and IPs with columns: Reference, Typ, and Abuse. A yellow box highlights the 'Send abuse report' button at the bottom. The first row shows a domain mail111.atl31.mcdlv.net with an abuse email abuse@support.gandi.net.  
 3. **Select Abuse Template:** A form for configuring the abuse report. It includes fields for Subject (Abuse report), Sender Name (Abuse Lucy Server), and Sender E-mail (abuse@example.com). The Content field contains a rich text editor with the following text: 'Dear Abuse Team,', 'Below a abuse report. Please investigate and solve the', 'in case of further questions, please contact abuse@exar', 'received from:', '%email%', '%time%', '%domain%', 'Detailed abuse report:', and '%report%'. A yellow box highlights the 'Send Abuse' button from the first step, which points to this form.

- **Custom rule-based analysis:** Define your own rules for e-mail analysis and risk calculations.

Home / Phishing Incident Reports

## Phishing Incident Reports

Send Abuse
Delete
Delete All
Settings
Download Plugin

Time	Email	Client	Campaign	Score	Status	
29.12.2018 13:46	oliver@muenchow.ch	N/A	N/A	3.90	Open	ⓧ Ⓜ ⓧ
29.12.2018 11:49	oliver@muenchow.ch	Lucy Test	BOUNCE TEST	0.00	Simulation	ⓧ Ⓜ ⓧ
19.12.2018 12:12	oliver@muenchow.ch	Lucy Test	BOUNCE TEST	0.00	Simulation	⚠ ⓧ Ⓜ ⓧ

Filter
Search
Client

Home / Phishing Incident Reports / Score Factors

### Score Factors

Custom Rules: 1.00
Domain Analysis: 1.00
Header Analysis: 1.00
SpamAssassin: 1.00

Save

Home / Phishing Incident Reports / Custom Rules / New Rule

### New Rule

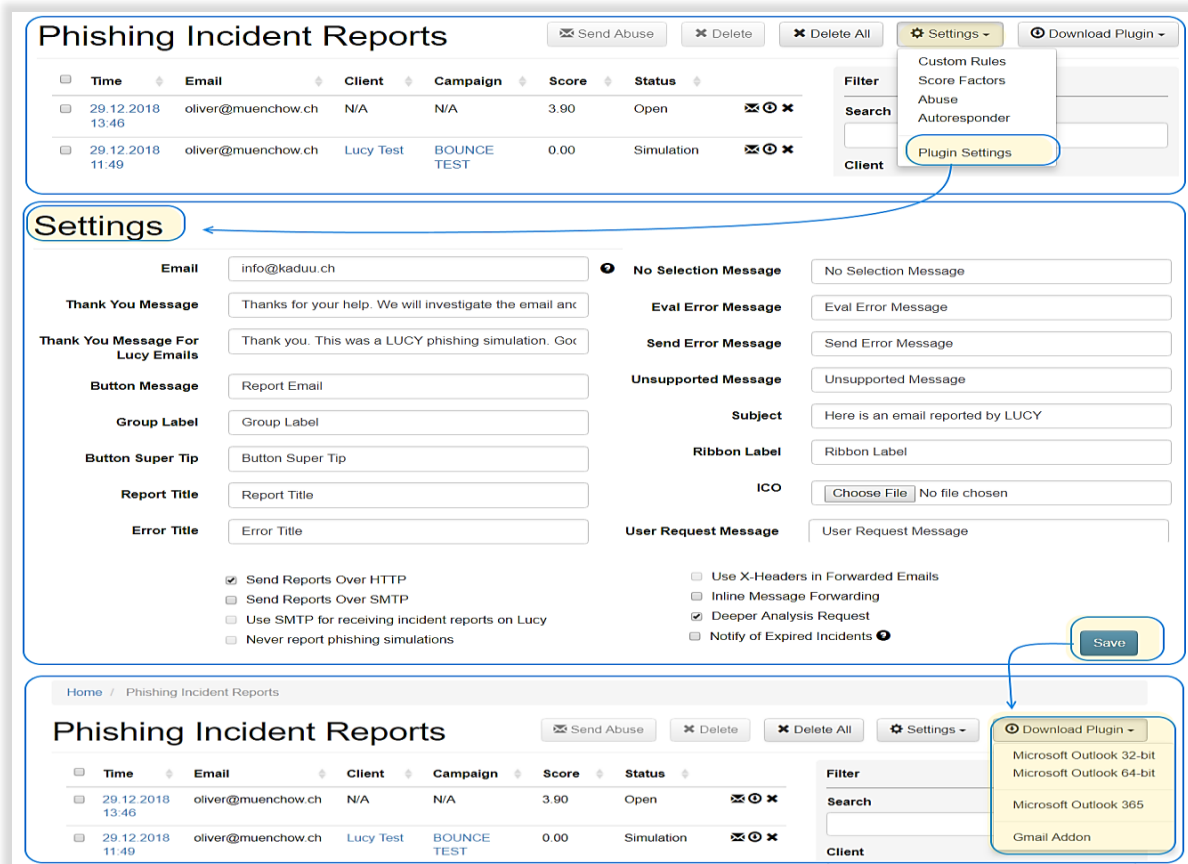
Name: Ceo name in header
Reg. Exp.: Jon Smith
Score: 2

Save

Summary
Header Analysis
Domain Analysis
Body Analysis
Threat Indicators

		Score	Rule active?	
Reply-to Mismatch	different reply-to adress defined than the actual ( more info...)	1.60	Active <input checked="" type="checkbox"/> Inactive	ⓧ Ⓜ ⓧ
New Domain	Domain has been reserved in the last 30 days ( more info...)	20.00	Active <input checked="" type="checkbox"/> Inactive	ⓧ Ⓜ ⓧ
Link Display mismatch	link display name different from the actual link ( more info...)	0.00	Active <input type="checkbox"/> Inactive	ⓧ Ⓜ ⓧ

- **Plugin customization options:** LUCY allows an easy customization and a complete white labelling of various plugin functions (displayed icon, feedback messages, ribbon label, transmission protocol, sent header, etc.).

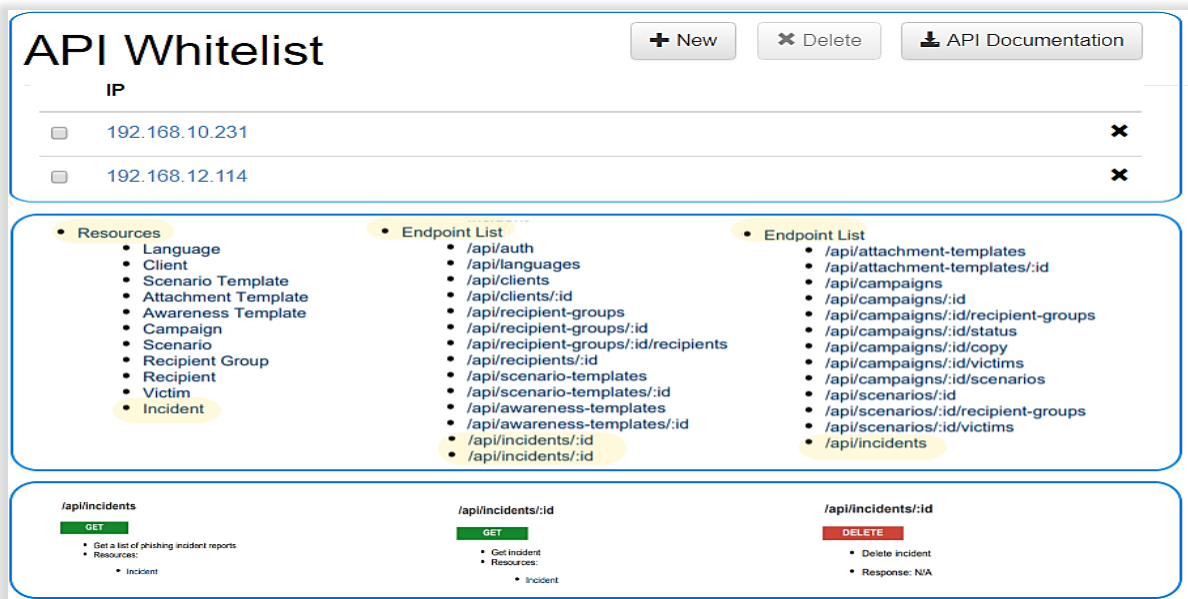


The screenshot displays the 'Phishing Incident Reports' interface. At the top, there's a header with buttons for 'Send Abuse', 'Delete', 'Delete All', 'Settings', and 'Download Plugin'. Below this is a table of incident reports with columns: Time, Email, Client, Campaign, Score, Status, and icons for Filter, Search, and Client. The table shows two entries for 'oliver@muenchow.ch'.

The 'Settings' page is shown below the table, with a 'Save' button. It contains various configuration options for messages and reports, such as 'Email', 'Thank You Message', 'Report Title', 'Error Title', 'No Selection Message', 'Eval Error Message', 'Send Error Message', 'Unsupported Message', 'Subject', 'Ribbon Label', 'ICO', and 'User Request Message'. There are also checkboxes for 'Send Reports Over HTTP', 'Send Reports Over SMTP', 'Use SMTP for receiving incident reports on Lucy', 'Never report phishing simulations', 'Use X-Headers in Forwarded Emails', 'Inline Message Forwarding', 'Deeper Analysis Request', and 'Notify of Expired Incidents'.

The 'Download Plugin' dropdown menu is open, showing options for 'Microsoft Outlook 32-bit', 'Microsoft Outlook 64-bit', 'Microsoft Outlook 365', and 'Gmail Addon'.

- **Third party integration:** Using LUCY's incident REST API automation, we can process reported e-mails and help your security team stop active phishing attacks while in progress.



The screenshot displays the 'API Whitelist' interface. At the top, there's a header with buttons for '+ New', 'Delete', and 'API Documentation'. Below this is a table of whitelisted IP addresses with columns: IP and a delete icon. The table shows two entries: '192.168.10.231' and '192.168.12.114'.

The 'Resources' section lists various API endpoints, including 'Language', 'Client', 'Scenario Template', 'Attachment Template', 'Awareness Template', 'Campaign', 'Scenario', 'Recipient Group', 'Recipient', 'Victim', and 'Incident'.

The 'Endpoint List' section shows a list of API endpoints, including '/api/auth', '/api/languages', '/api/campaigns', '/api/recipients', '/api/scenarios', and '/api/incidents'.

The bottom section shows the details for the '/api/incidents' endpoint, including the 'GET' method and the response structure.

- **Identify attacks with common patterns:** Apply LUCY's dashboard filters to detect common attack vectors across your organization. Search within all reported e-mails for similar indicators of compromise.

The screenshot displays the LUCY dashboard's 'Incident Reports' section. The top panel shows a list of incidents with columns for Time, Email, Rating, Client, Campaign, Score, and Status. A filter sidebar on the right allows for refining results by domain, reputation, rating, date, and campaign. Below the list, a detailed view for a specific incident (Email: sarah@test.com, Score: 3.9) is shown, including a risk score gauge, message details, and a 'Phishing Incident Reports' sub-section with its own filters.

Time	Email	Rating	Client	Campaign	Score	Status
04.07.2018 14:20	peter@test.com	★★★★★	N/A	N/A	0.00	Open
03.07.2018 14:45	jon@example.com	★★★★★	Lucy Test	TEST 123	0.00	Simulation
03.07.2018 08:10	sarah@test.com	★★★★★	N/A	N/A	1.00	Open
02.07.2018 10:02	igor@test.com	★★★★★	Lucy Test	LMS Access	0.00	Simulation
02.07.2018 09:54	frank@example.com	★★★★★	N/A	N/A	0.00	Open
02.07.2018 09:54	barbara@test.com	★★★★★	N/A	N/A	0.00	Open

**Incident Details (sarah@test.com):**

- Overall Risk Score: 3.9 of 10.0
- Message Subject: **Standard is more better**
- Report Time: 29.12.2018 13:46:43
- Status: Open

**Phishing Incident Reports (sarah@test.com):**

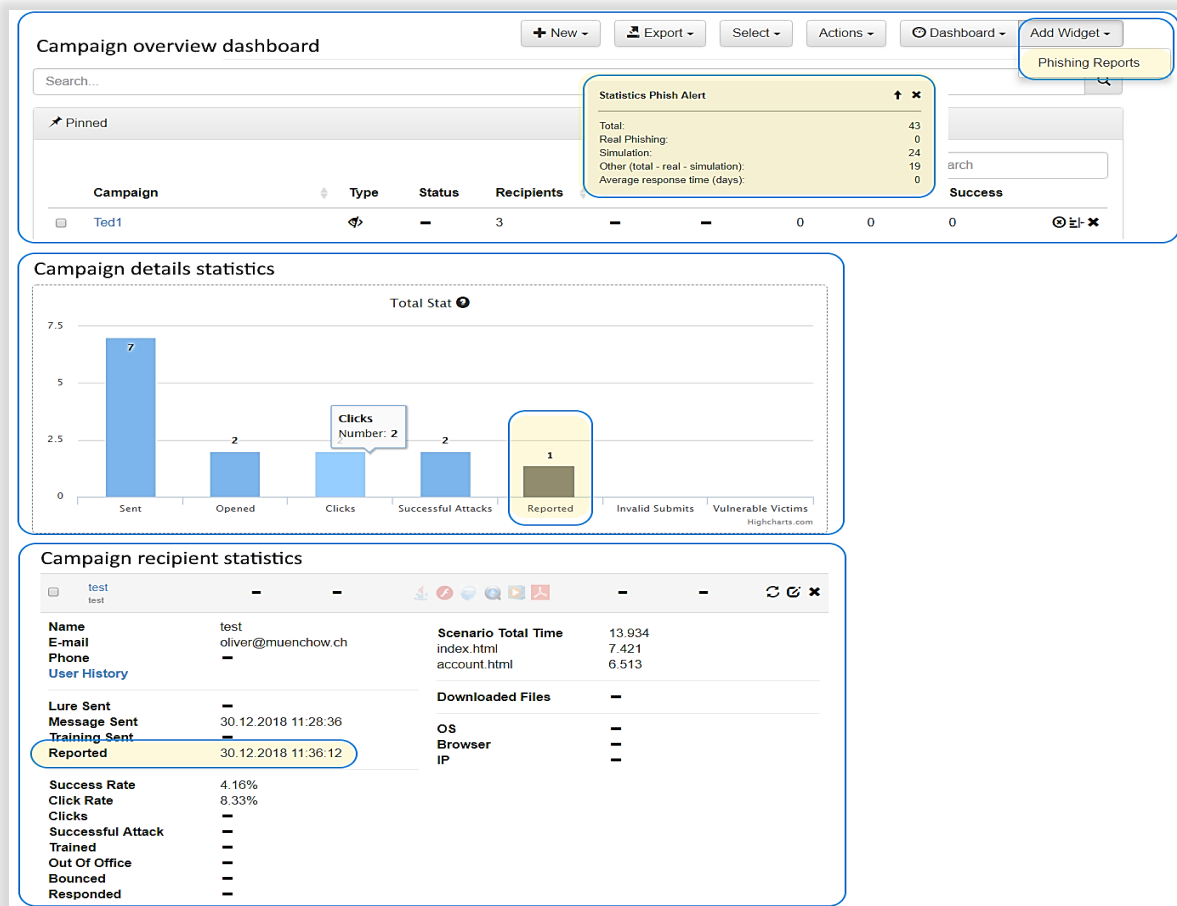
Time	Email	Client	Campaign	Score	Status
29.12.2018 13:46	sarah@test.com	N/A	N/A	3.90	Open

- **Incident user reputation profiles:** Classify users with an incident reputation score.

This screenshot shows the 'Incident Reports' table with a focus on the 'Rating' column. The table lists various incidents, and the 'Rating' column uses star icons to represent scores. A red box highlights the 'Rating' column header and the star ratings for several rows.

Time	Email	Rating	Client	Campaign	Score	Status
04.07.2018 14:20	peter@test.com	★★★★★	N/A	N/A	0.00	Open
03.07.2018 14:45	jon@example.com	★★★★★	Lucy Test	TEST 123	0.00	Simulation
03.07.2018 08:10	sarah@test.com	★★★★★	N/A	N/A	1.00	Open
02.07.2018 10:02	igor@test.com	★★★★★	Lucy Test	LMS Access	0.00	Simulation
02.07.2018 09:54	frank@example.com	★★★★★	N/A	N/A	0.00	Open
02.07.2018 09:54	barbara@test.com	★★★★★	N/A	N/A	0.00	Open

- **Integration with attack simulations:** Seamless report and dashboard integration with phishing simulations: identify the users who have behaved exemplarily in a phishing simulation.



- **Easy Installation:** Install the Phishing Incident Plugin for Outlook, Gmail, Office365.

