



LUCY WHITEPAPER



WAS BIETET LUCY?

Testen, schulen und beteiligen Sie Ihre Mitarbeiter!

Mit LUCY können Unternehmen die Rolle eines Angreifers übernehmen und vorhandene Schwachstellen, sowohl in der technischen Infrastruktur, als auch im Wissen der Mitarbeiter aufdecken und diese Mängel durch ein umfassendes E-Learning-Programm beseitigen.



MITARBEITERTEST

Angriffssimulationen (z. B. Phishing)



INFRASTRUKTURTEST

Malware-Simulation und Scanner



MITARBEITER-TRAINING

Integriertes Lern-Management-System



FORTSCHRITTS-ANALYSE

Bewertung Risiko und Lernfortschritte



INTEGRATION DER MITARBEITER

Reporting-System
(z. B. Mail Phish Button)



LUCY WHITEPAPER



INHALTSVERZEICHNIS

ALLGEMEINE MERKMALE

- Erinnerungen
- Antworterkennung
- Vollwertiger mail communication client
- Zeitplan-Randomisierung
- Leistungstools
- Mehrsprachige Admin-Oberfläche
- Zertifikat (SSL)
- Rollenbasierte Zugriffssteuerung
- Mehrschichtige Benutzergruppen
- Multi-Client-kompatibel
- Kampagnenvorlagen
- Setup-Assistent mit risikobasierter Anleitung
- Kampagnenprüfungen
- Approval Workflow
- DNS API

ANGRIFFSSIMULATION

- Angriffe auf tragbare Medien
- SMiShing
- Dateneingabe-Angriffe
- Hyperlink-Angriffe
- Leistungsstarkes Toolkit zur URL-Umleitung
- Gemischte Angriffe
- Dateibasierte Angriffe
- Double Barrel-Angriffe
- Java-basierte Angriffe
- PDF-basierte Angriffe
- Ransomware-Simulationsangriffe
- Toolkit zur Validierung der Dateneingabe
- Mehrsprachige Angriffsvorlagenbibliothek
- Sektor- und abteilungsspezifische Vorlagen
- Gleichzeitige Verwendung von Angriffsvorlagen
- Variationen von Angriffs-URLs
- URL-Verkürzung
- Pentest-Kit
- Webseiten-Kloner
- Level-basierte Angriffe
- Spear-Phishing-Simulation
- DKIM / S / MIME-Unterstützung für Phishing-E-Mails
- Mail-Scanner
- Benutzerdefinierte Homepage-Erstellung

INFRASTRUKTUR-TEST

- Malware Testing Toolkit
- E-Mail- und Webfiltertest
- Erkennen aktiver und passiver Client-Sicherheitslücken
- Spoofing-Test

TECHNISCHE TESTS

- Reputationsbasiertes E-Learning
- Endbenutzer-Schulungsportal
- Fortbildungsdiplom
- Sicherheitsbewusstsein
- e-Learning-Authoring-Toolkit
- Rich Media-Sensibilisierungstraining
- Schulungsbibliothek
- Unterstützung für statische Schulungen
- Schulungssupport offline
- Microlearning-Module
- Videoanpassung
- Mobile-Responsive-Format
- Videoimport / -export
- Dynamische Schulungshinweise

MITARBEITER MITEINBEZIEHEN

- E-Mails mit einem einzigen Klick melden
- Bestärkung im richtigen Verhalten
- Deep Inspection Request
- Automatische Vorfallsanalyse
- Automatisches Vorfalls-Feedback
- Bedrohungsminderung
- Benutzerdefinierte und regelbasierte Analyse
- Anpassungsoptionen für Plug-ins
- Integration von Drittanbietern
- Identifizieren von Angriffen nach einem gängigen Muster
- Reputationsprofile für Benutzer mit Vorfallshistorie
- Integration in Angriffssimulationen
- Einfache Installation

ALLGEMEINE MERKMALE

- **Erinnerungen:** Erinnerungsvorlagen können verwendet werden, um automatisch Nachrichten erneut an Benutzer zu senden, die nach einem vorbestimmten Zeitraum nicht auf einen Angriffslink oder einen Schulungskurs geklickt haben.

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

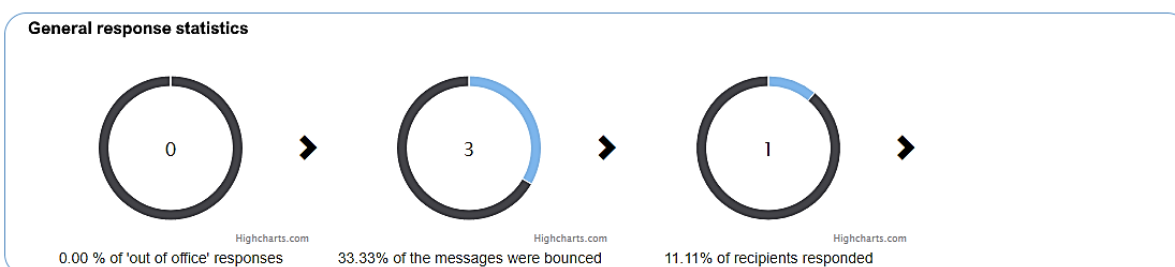
☐ Remind users who did not finish a training

3

days after training is started

Save

- **Antwarterkennung:** Die automatische Antwarterkennung ermöglicht das Definieren und Analysieren automatischer E-Mail-Antworten (z. B. bei Abwesenheit) sowie E-Mail-Zustellungsfehler (z. B. unbekannter Benutzer) innerhalb einer Kampagne.



User specific response statistics		
 No test	-	-
Name	No	
E-mail	doestntexist@doesntr-eallyexist.net	
Phone	-	
User History		
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

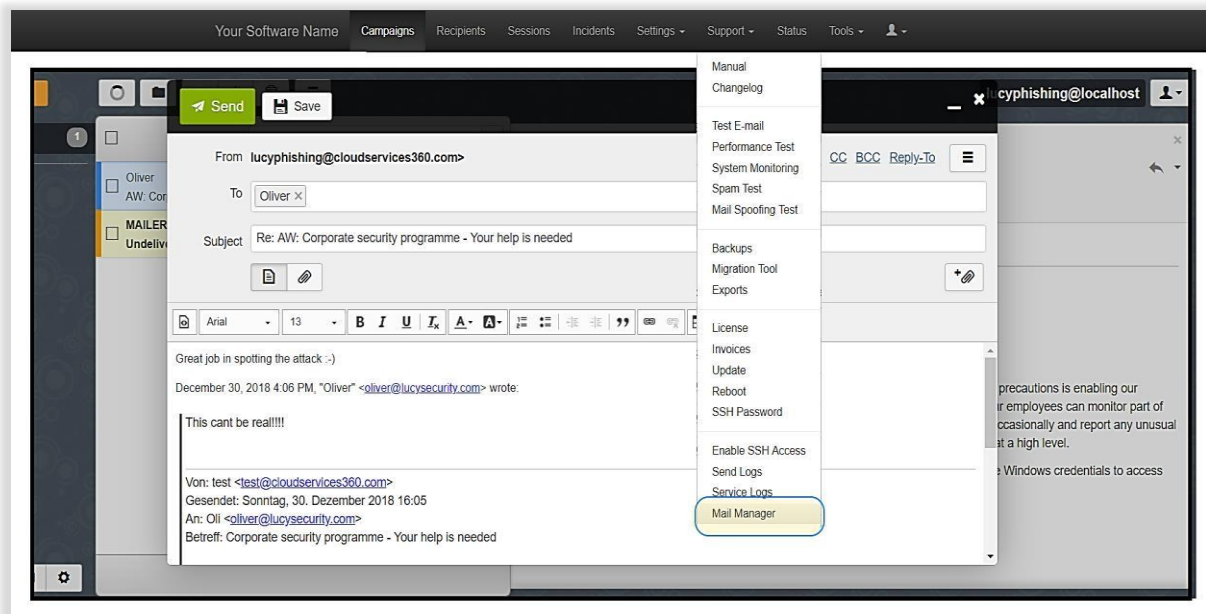
[Home](#) / Automated Response Detection

Automated Response Detection

Timeout	60	
Out Of Office Delay	1	
Out Of Office Pattern	out of office, away, vacation	
Bounced Pattern	User unknown, NoSuchUser, Host or domain name not found, does not exist	

Save

- **Vollwertiger mail communication client:** Eine integrierte Messaging-Plattform ermöglicht dem LUCY-Administrator die interaktive Kommunikation mit den Empfängern innerhalb oder außerhalb von LUCY-Kampagnen. Alle E-Mails werden archiviert und können ausgewertet werden.



- **Zeitplan-Randomisierung:** Die gezielte Sensibilisierung der Mitarbeiter ist der Schlüsselfaktor für ein effektives und nachhaltiges Sicherheitsbewusstsein innerhalb des Unternehmens. Das zufällige Fahren einiger Kampagnen gleichzeitig ist eines der besten Mittel, um Mitarbeiter zu schulen.

18.12.2018 ...

Campaign Status: Running

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

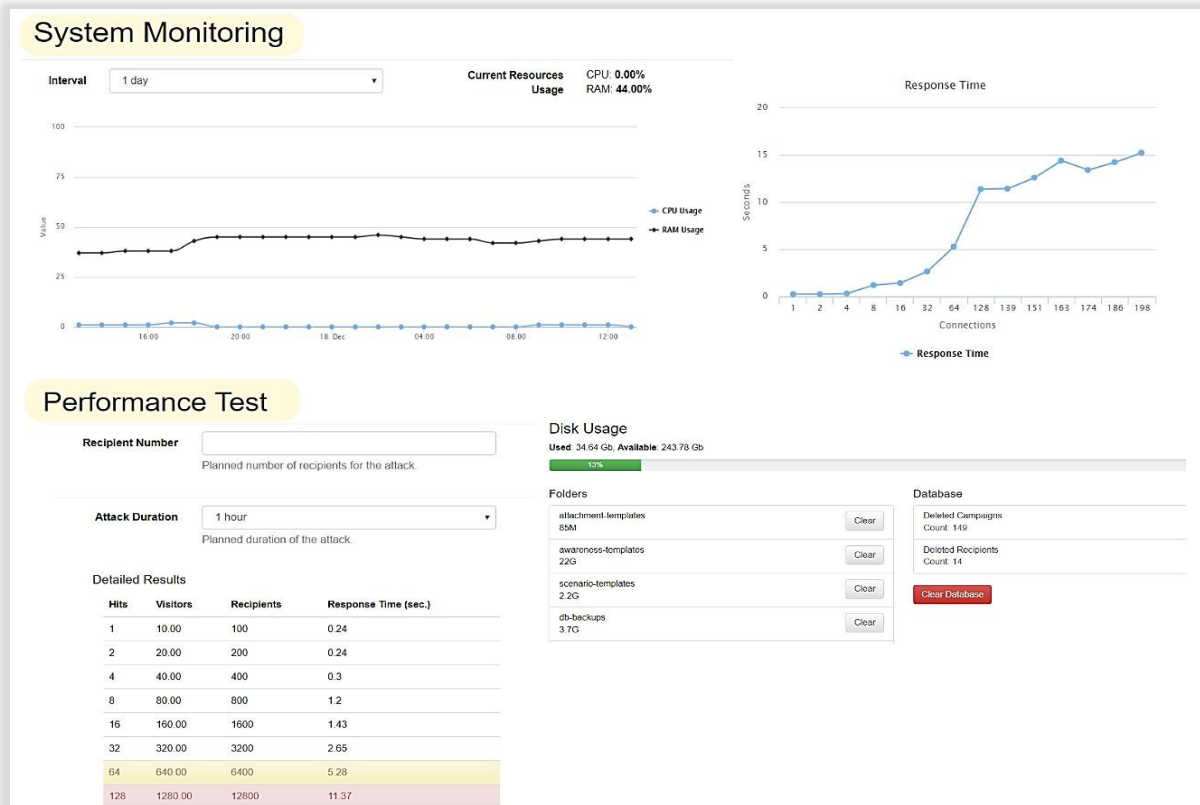
☒ Google Leaks (Web Based)
☒ DropBox (Web Based)
☒ LinkedIn (Hyperlink)
☒ eFax (Web Based)
☒ Private Message (Web Based)

Recipient Groups

☒ LUCY Test

Save

- **Leistungstools:** Die LUCY Smart Routines passen die Serverinstallation an die vorhandenen Ressourcen an. Anwendungsserver-, DBMS-Größen-, Speicher- und CPU-Auslastung werden während der Installation oder während des Betriebs berechnet. Sie können eine einzelne Cloud-basierte LUCY-Installation für mehr als 400.000 Benutzer skalieren.



- **Mehrsprachige Admin-Oberfläche:** Die LUCY Admin-Oberfläche ist in vielen verschiedenen Sprachen verfügbar und kann auf Anfrage auch in andere Sprachen übersetzt werden.

Your Software Name
Login

[your logo here]

Language
English
English
Deutsch
Español
Français
Italiano
Nederlands
Português
Türkçe

Login
E-mail
Password
Forgot?
Security Code
Login

(c) 2018 Your Company Name

- **Zertifikat (SSL):** Ermöglicht die automatische Erstellung offizieller und anerkannter Zertifikate durch den Administrator, das Back-End sowie für die Kampagnen. LUCY verwendet automatisch die im System konfigurierte Domain, um das Zertifikat zu generieren. Wenn Sie sich für die Verwendung von SSL für Ihre Kampagne entscheiden, können Sie ein benutzerdefiniertes Zertifikat oder ein CSR (Certificate Signing Request) generieren. Sie können auch offizielle vertrauenswürdige Zertifikate importieren.

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

- **Rollenbasierte Zugriffssteuerung:** LUCY bietet eine rollenbasierte Zugriffssteuerung (RBAC), die den Systemzugriff auf autorisierte Benutzer beschränkt. Die Berechtigungen zum Ausführen bestimmter Arbeitsabläufe werden in den Benutzereinstellungen an bestimmte Rollen gekoppelt. Mitarbeitern, Teilnehmern (oder anderen Systembenutzern) werden bestimmte Rollen zugeordnet, über die sie die erforderlichen Computerberechtigungen erwerben, um bestimmte LUCY-Funktionen auszuführen.

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

- **Mehrschichtige Benutzergruppen:** Laden Sie große Benutzergruppen schnell über eine CSV-, LDAP- oder Textdatei hoch. Erstellen Sie verschiedene Gruppen, die nach Arbeitsbereiche, Abteilung, Bezeichnung, usw. gegliedert sind. Aktualisieren Sie Benutzer in einer laufenden Kampagne. Erstellen Sie dynamische Benutzergruppen basierend auf den Ergebnissen der Phishing-Kampagne.

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-kompatibel:** „Client“ kann sich auf verschiedene Unternehmensbereiche, Abteilungen oder Gruppen beziehen, denen eine Kampagne in LUCY zugeordnet ist. Diese „Clients“ können beispielsweise verwendet werden, um einen kampagnenspezifischen Zugriff zu ermöglichen oder um teilnehmer-spezifische Analysen zu erstellen.

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	
☐ Test Client A	✕
☐ Tenant4	✕
☐ Client Inc USA	✕
☐ Tenant3	✕
☐ 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

- Kampagnenvorlagen:** Wenn Sie eine Kampagne in ähnlicher Form wiederverwenden möchten, können Sie eine solche Kampagne vollständig mit Angriffsvorlagen und E-Learning-Inhalte als Kampagnenvorlage speichern. Mit dieser Funktion können Sie vermeiden, ähnliche Konfigurationen immer wieder erstellen zu müssen.

The screenshot shows the Lucy campaign management interface. At the top, the breadcrumb navigation is 'Home / Campaigns / Max1'. The campaign name 'Max1' is displayed, along with its status 'Not Started', 'Reset Stats', 'Report', 'Save as Template' (highlighted with a yellow box and a blue arrow), 'Export', and 'Start' buttons. Below this, a table shows campaign details: 'Campaign' (Max1), 'Running Time' (4 days, 4 hours), and 'Created By' (N/A). The 'Results' section includes a 'Summary' button and a 'New Campaign' button. The 'Configuration' section shows 'Name' (Standard Test & Train Campaign Template), 'Client' (Lucy Test), 'Setup Mode' (Start with Default Campaign Template), and 'Template' (Max1). The 'Advanced Settings' section shows 'Successful Attacks' (1 of 3) and 'Vulnerable Victims' (0 of 3). On the right, there is a donut chart showing 'Awareness' and a 'Training Score (%)' bar chart.

- Setup-Assistent mit risikobasierter Anleitung:** LUCY bietet verschiedene Setup-Tools. Erstellen Sie mit den vordefinierten Kampagnenvorlagen in weniger als 3 Minuten eine vollständige Kampagne oder lassen Sie sich vom Setup-Assistenten durch die Konfiguration führen. Optional steht ein risikobasierter Einrichtungsmodus zur Verfügung, der - basierend auf Größe und Branche des Unternehmens - spezifische Vorschläge für die Auswahl von Angriffs- und Sensibilisierungsvorlagen enthält.

The screenshot shows the 'Campaign Wizard: Type' interface. It lists the steps: 1. Type, 2. Campaign, 3. Campaign Template, 4. Attack Settings, 5. Training Template, 6. Training Settings, 7. Recipients, 8. Review, and 9. Finish. The main area displays several campaign types with icons and descriptions:

- 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.

At the bottom, there are 'Close' and 'Next' buttons.

- **Kampagnenprüfungen:** Vorläufige Prüfungen vor dem Start einer LUCY-Kampagne: E-Mail-Zustellungsprüfung, MX-Datensatzprüfung, Zeitplanprüfung, Spamprüfung und andere.

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 Workflow:** Eine bestimmte Kampagne kann einem Vorgesetzten bei LUCY zur Bestätigung vorgelegt werden.

Results

- Summary
- Statistics
- Reports
- Exports

Configuration

- Base Settings
- Awareness Settings
- Schedule
- Recipients

Advanced Settings

- User Settings
- Custom Fields
- Reminders

Logs

- Supervision Log

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 "e-learning"

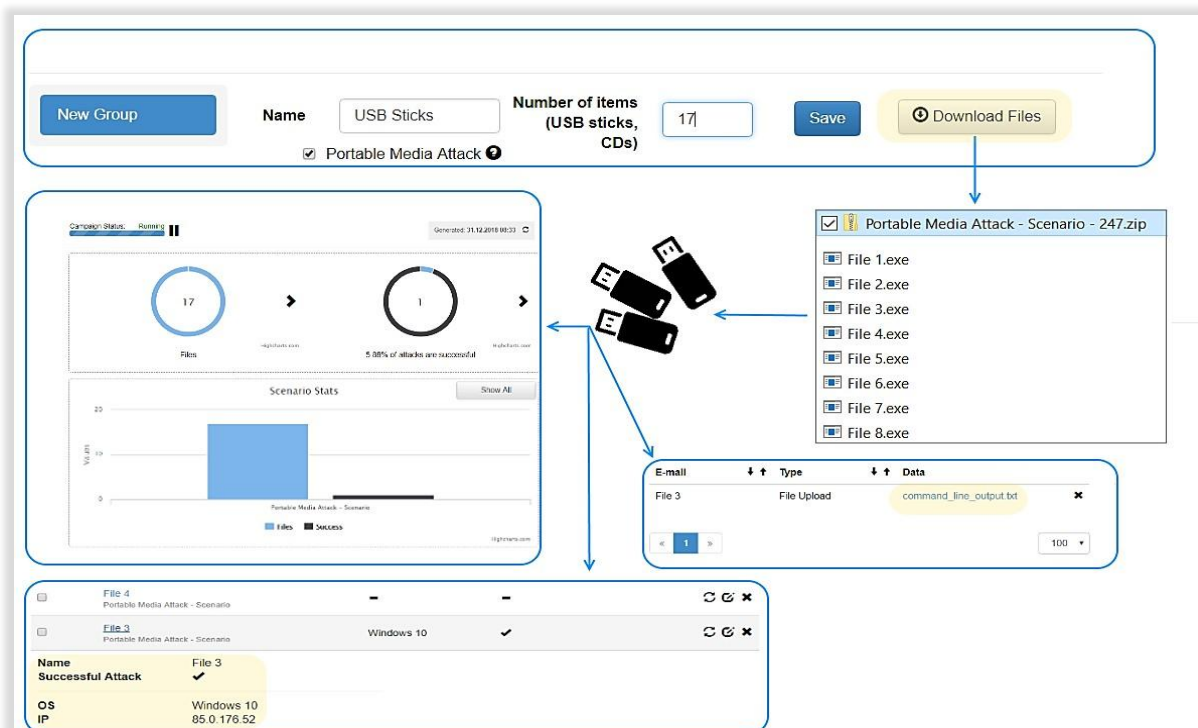
Reject

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

- DNS API:** Mit der DNS-API kann der Administrator innerhalb von Sekunden mit LUCY eine beliebige Domain erstellen. Da Angreifer sehr häufig ähnliche Domain-Schreibweise verwenden (Typosquatting genannt), kann dieses Risiko mit LUCY auch dargestellt werden. Wenn die ursprüngliche Domain des Unternehmens beispielsweise „onlinebanking.com“ lautet, kann der DNS-Assistent verwendet werden, um Domains wie „Onlinebanking.com“, „onl1nebanking.com“ oder „onlinebanking.services“ zu reservieren und später einer Kampagne zuzuweisen. LUCY erstellt dann automatisch die entsprechenden DNS-Einträge (MX, SPF, Whois Protection, usw.) für die IP, auf der LUCY installiert ist. Natürlich kann der Administrator auch die eigenen Domains seines Providers in LUCY verwenden.

ANGRIFFSSIMULATION

- Angriffe auf tragbare Medien:** Hacker können tragbare Medien verwenden, um auf vertrauliche Informationen zuzugreifen, die auf einem Computer oder in einem Netzwerk gespeichert sind. LUCY bietet die Möglichkeit, Angriffe auf tragbare Medien durchzuführen, bei denen eine Dateivorlage (z. B. ausführbare Datei, Archiv, Office-Dokument mit Makros, usw.) auf einem tragbaren Mediengerät wie USB-Stick, SD-Karte oder einer CD gespeichert werden kann. Die Aktivierung (Ausführung) dieser einzelnen Dateien kann mit LUCY verfolgt werden.



- **SMiShing:** Smishing ist gewissermaßen „SMS-Phishing“. Wenn Cyberkriminelle „Phishing“ betreiben, senden sie betrügerische E-Mails, die den Empfänger dazu verleiten sollen, einen mit Malware beladenen Anhang zu öffnen oder auf einen böswilligen Link zu klicken. Smishing verwendet einfach Textnachrichten anstelle von E-Mails.

The screenshot shows the 'Message Template' configuration page in the Lucy Webeditor. The 'Message Type' is set to 'Sms'. The 'Text' field contains the placeholder 'Check out this link here: %link%'. The 'Landing Domain' is 'cloudspace365.solutions' and the 'Subdomain' is 'sms'. The 'Url Shortener' is set to 'goo.gl'. A blue callout bubble points to the 'Text' field, showing a mobile phone screen with the message 'Check out this link here: goo.gl/KuraFG'. Other fields include 'Language' (English), 'Sender Name' (004550566166), 'Template' (Access to online surveillance portal / English), 'Name' (SMS), 'Login Regexp' (lw.*lw), and 'Password Regexp'. A 'Save' button is at the bottom.

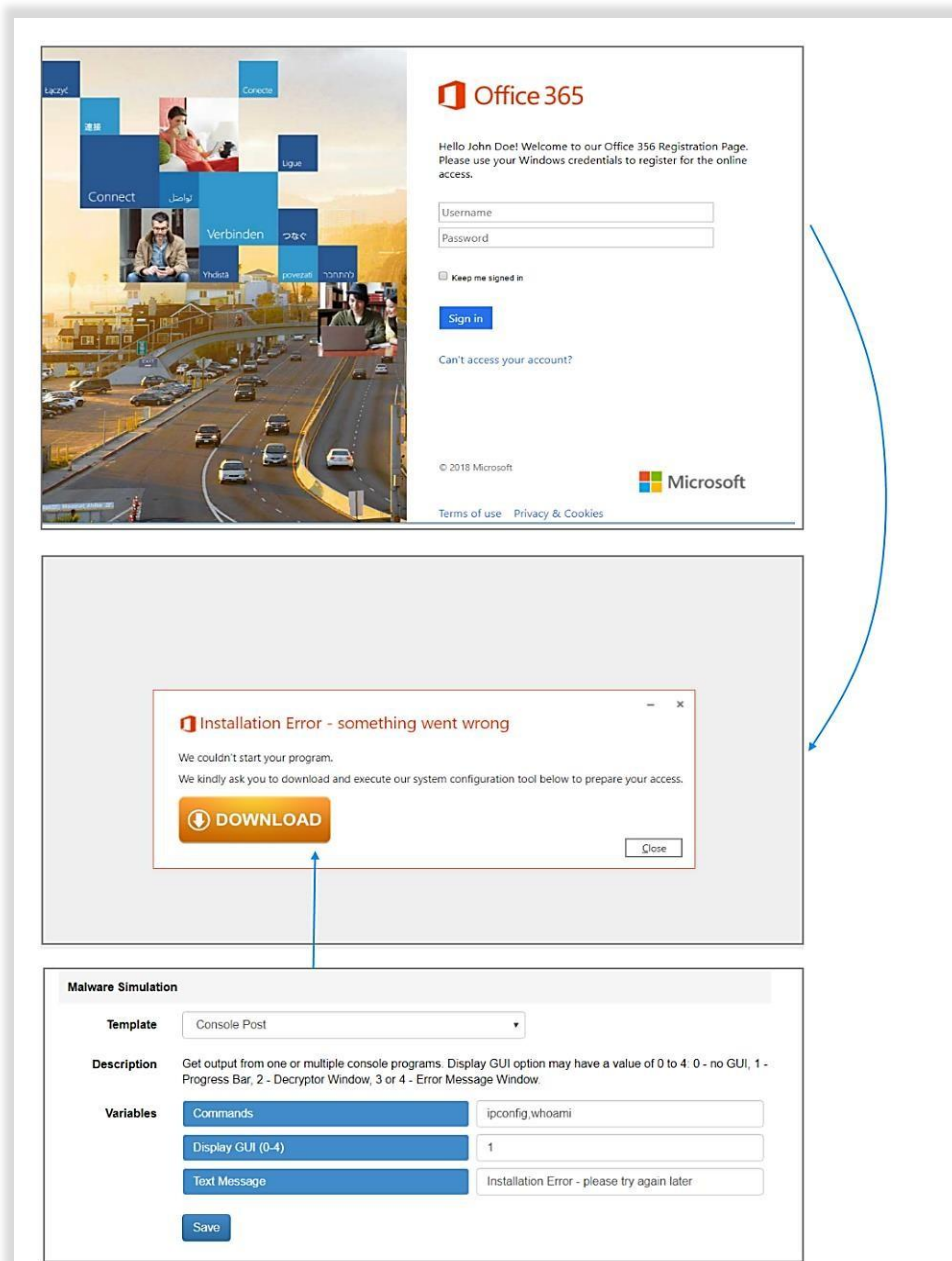
- **Dateneingabe-Angriffe:** Dateneingabeangriffe können eine oder mehrere Webseiten umfassen, welche die Eingabe vertraulicher Informationen abfangen. Die verfügbaren Webseiten können einfach mit dem LUCY-Webeditor angepasst werden. Mit zusätzlichen Bearbeitungs-Tools können Sie schnell Funktionen wie Anmeldeformulare, Downloadbereiche, usw. einrichten, auch ohne HTML-Kenntnisse.

The screenshot shows the Lucy Webeditor interface for inserting a login form. The 'Quick Tips' section on the left lists various variables like %static%, %link%, %name%, %email%, %message%, %link-awareness%, %division%, %location%, %staff-type%, %comment%, %gender%, and %time(FORMAT, OFFSET, ZONE)%. The 'Content' area shows a preview of a login form with fields for 'Email or phone' and 'Password'. The 'Insert Login Form' dialog box is open, showing the 'Login Form #3' selected. The 'File' dropdown menu is open, showing 'index.html' selected. The 'Insert Login Form' button is highlighted in the 'Content' area.

- **Hyperlink-Angriffe:** Eine Hyperlink-basierte Kampagne sendet Benutzern eine E-Mail mit einer zufälligen Tracking-URL.

- **Leistungsstarkes Toolkit zur URL-Umleitung:** Mit den flexiblen Umleitungsfunktionen von LUCY kann ein Benutzer zum richtigen Zeitpunkt zu den gewünschten Bereichen der Angriffssimulation oder der Schulung geführt werden. Nach Eingabe der ersten drei Zeichen eines Kennworts in einer Phishing-Simulation kann der Benutzer beispielsweise zu einer speziellen Schulungsseite zum Passwortschutz weitergeleitet werden.

- **Gemischte Angriffe:** Gemischte Angriffe ermöglichen die Kombination mehrerer Szenarienarten (dateibasiert, Dateneingabe, usw.) in derselben Kampagne.

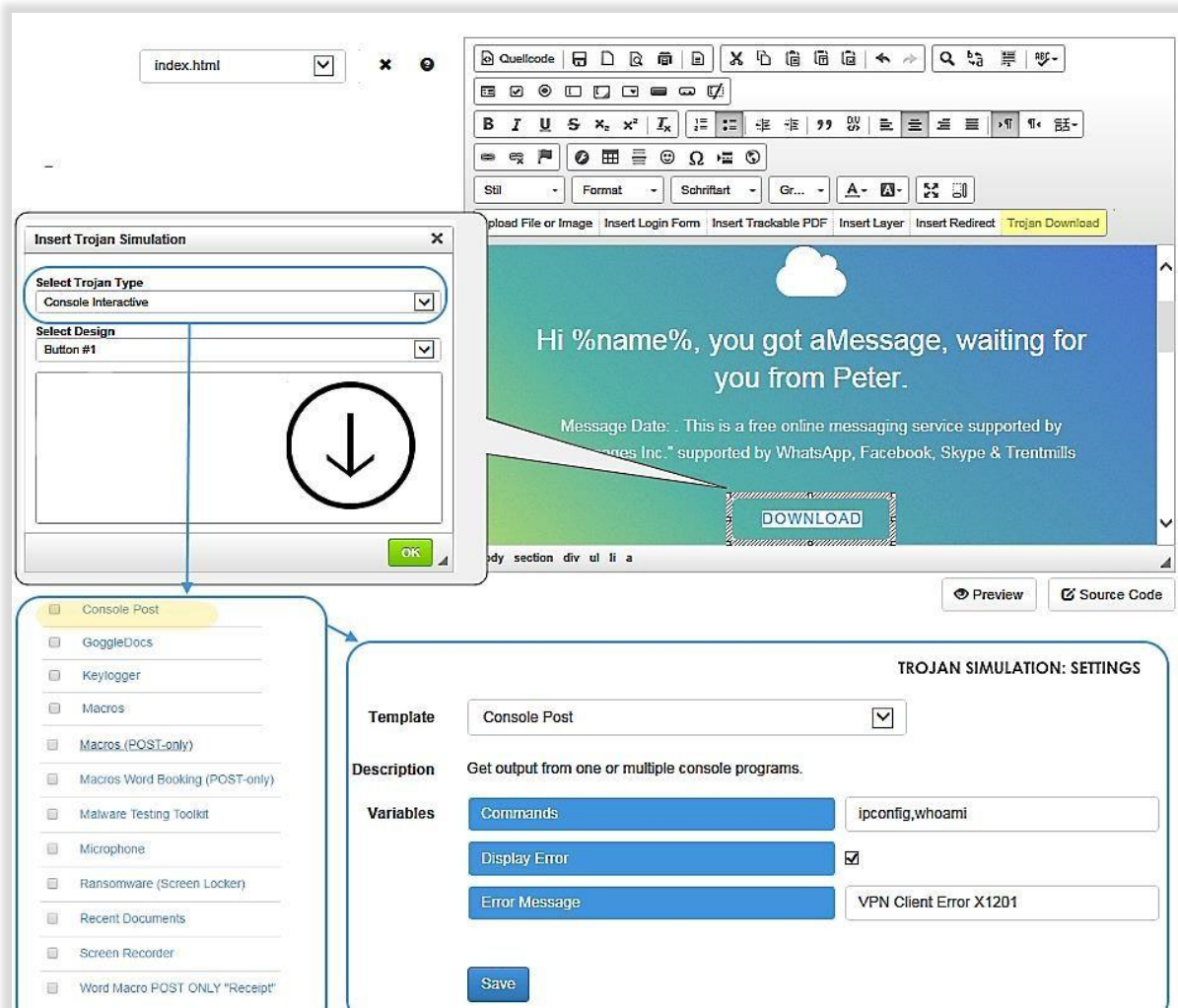


The diagram illustrates a mixed attack scenario involving three sequential steps:

- Office 365 Registration Page:** A user (John Doe) is prompted to register for Office 365. The page includes fields for Username and Password, a "Sign in" button, and a link for "Can't access your account?".
- Installation Error Dialog:** An error message appears: "Installation Error - something went wrong". It states: "We couldn't start your program. We kindly ask you to download and execute our system configuration tool below to prepare your access." A prominent orange "DOWNLOAD" button is shown.
- Malware Simulation Configuration:** A configuration window titled "Malware Simulation" is shown. It includes:
 - Template:** Console Post
 - Description:** 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.
 - Variables:**
 - Commands:** ipconfig, whoami
 - Display GUI (0-4):** 1
 - Text Message:** Installation Error - please try again later
 - Save** button

A blue arrow indicates the flow from the Office 365 page to the error dialog, and another blue arrow points from the error dialog to the Malware Simulation configuration window, showing how the error message is triggered by the simulated malware.

- **Dateibasierte Angriffe:** Mit dateibasierten Angriffen kann der LUCY-Administrator verschiedene Dateitypen (Office-Dokumente mit Makros, PDFs, ausführbaren Dateien, MP3s, usw.) in LUCY- generierte E-Mail-Anhänge oder Webseiten integrieren und deren Download- oder Ausführungsrate messen.



The screenshot displays the LUCY web editor interface. At the top, a file browser shows 'index.html'. The main editor area contains a message: 'Hi %name%, you got aMessage, waiting for you from Peter.' Below the message is a 'DOWNLOAD' button. A 'Trojan Download' button is also visible in the top right of the editor area.

The 'Insert Trojan Simulation' dialog is open, showing the 'Select Trojan Type' dropdown set to 'Console Interactive' and the 'Select Design' dropdown set to 'Button #1'. A large circular arrow icon is visible in the center of the dialog.

The 'Trojan Simulation: Settings' panel is also open, showing the 'Template' dropdown set to 'Console Post'. The 'Description' field contains the text 'Get output from one or multiple console programs.' The 'Variables' section includes three input fields: 'Commands' (containing 'ipconfig,whoami'), 'Display Error' (checked), and 'Error Message' (containing 'VPN Client Error X1201'). A 'Save' button is located at the bottom of the settings panel.

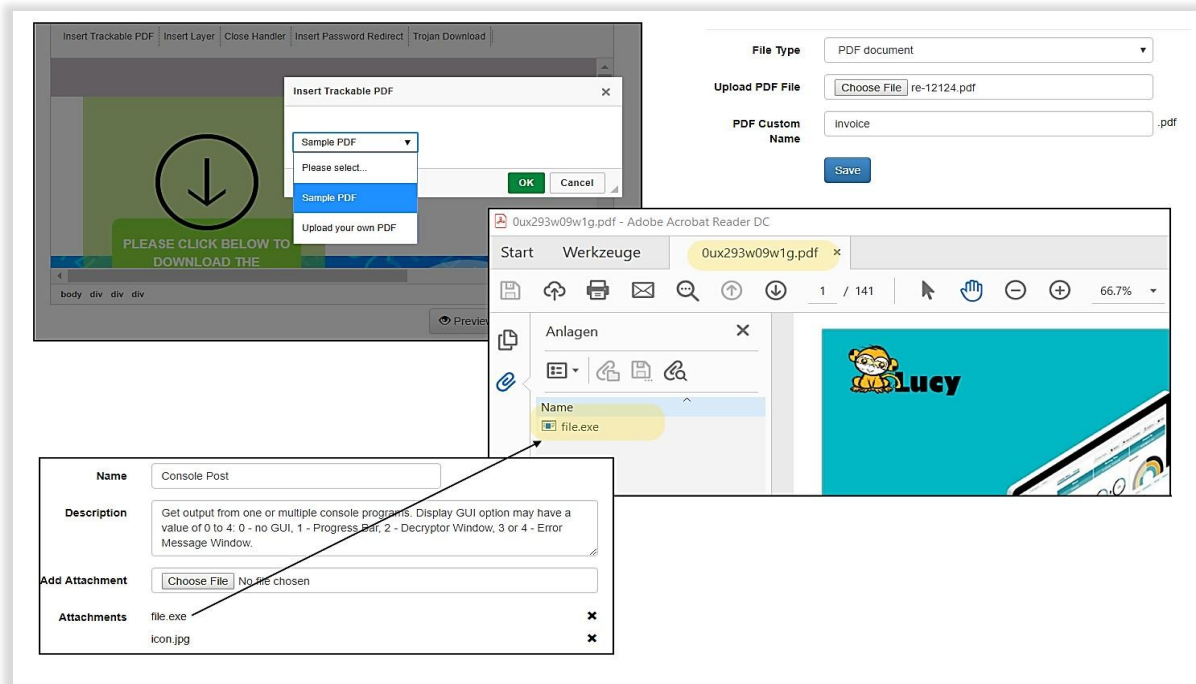
- **Double Barrel-Angriffe:** Mit dieser Funktion können in jeder Kampagne mehrere Phishing-E-Mails gesendet werden, wobei die erste harmlose E-Mail (der Köder) nichts Böses enthält und keine Antwort vom Empfänger verlangt.

The screenshot shows the 'Lure Template' configuration page in the Lucy web interface. The left sidebar contains a navigation menu with options: Summary, Scenario Settings, Landing Page Template, Message Template, Lure Template (highlighted), and Errors. Below this is a 'Quick Tips' section with a link to 'E-mail Message Variables'. The main content area is divided into two sections: 'Message Type' and 'Content'. The 'Message Type' section includes fields for 'Language' (English), 'Sender Name' (Security), and 'Sender E-mail' (Security@example.com). The 'Content' section features a rich text editor with a toolbar and a preview of the email content. The email content is a phishing message from the IT-Department, claiming a security program will be launched soon. Below the content editor, there are fields for 'Success Action' (Data Submit), 'Collect Data' (Partial), and 'Lure Delay' (3600). A 'Double Barrel Attack' checkbox is checked. At the bottom, there are fields for 'Url Shortener' (bit.ly), 'Login Regexp' (lw.*lw), and 'Password Regexp'. A 'Save' button is located at the bottom right.

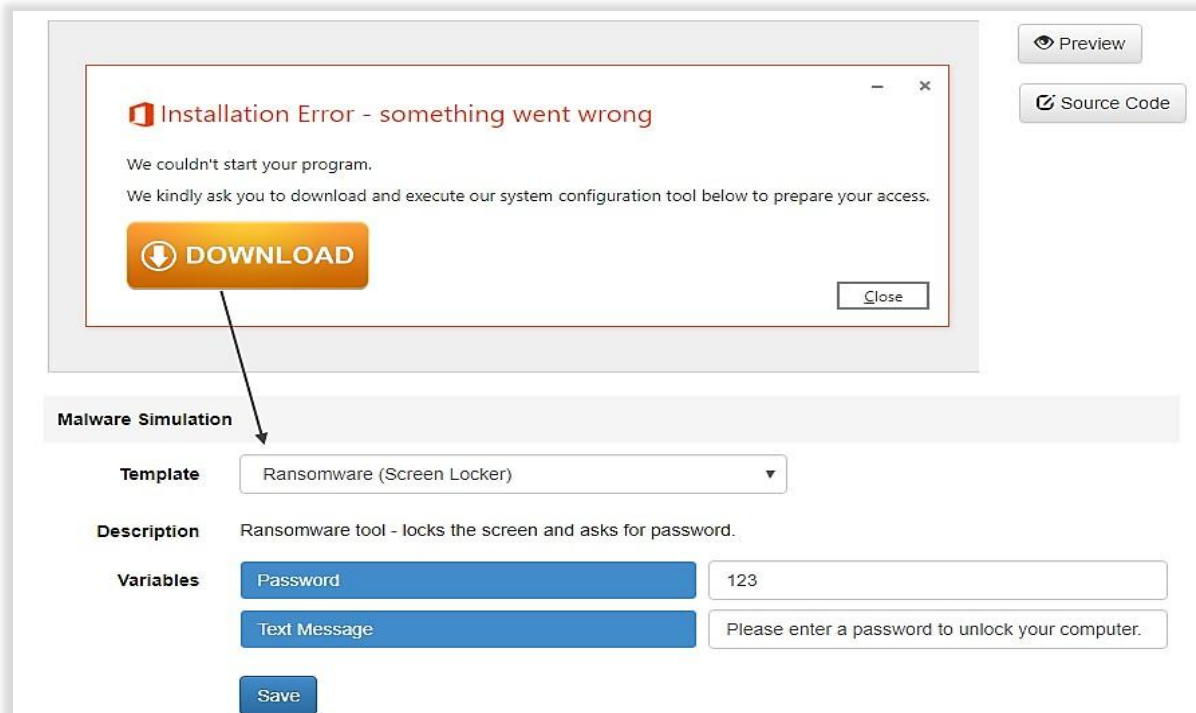
- **Java-basierte Angriffe:** Mit Java-basierten Angriffen kann der LUCY-Administrator ein vertrauenswürdiges Applet in die durch LUCY bereitgestellten dateibasierten oder gemischten Angriffsvorlagen integrieren und deren Ausführung durch den Benutzer messen.

The screenshot shows the 'Malware Simulation' configuration page in the Lucy web interface. The left sidebar contains a navigation menu with options: File Type, Tunnel Executable, and Malware Simulation (highlighted). The main content area is divided into two sections: 'File Type' and 'Malware Simulation'. The 'File Type' section includes a dropdown for 'File Type' (Java Applet) and a 'Save' button. The 'Malware Simulation' section includes a dropdown for 'Template' (Screen Recorder), a description of the simulation, and a list of variables: Desktop Video, Capture Webcam, Webcam Video, Video Length (seconds), Number of Snapshots, Interval Between Snapshots, Display GUI (0-4), and Text Message. A 'Save' button is located at the bottom right.

- PDF-basierte Angriffe:** Mit diesem Modul können PDF-basierte Phishing-Angriffe simuliert werden. Mit LUCY können Exe-Dateien als harmlose PDF-Anhänge „deklariert“ und deren Ausführung gemessen werden. Darüber hinaus können dynamische Phishing-Links auch in PDFs generiert werden.



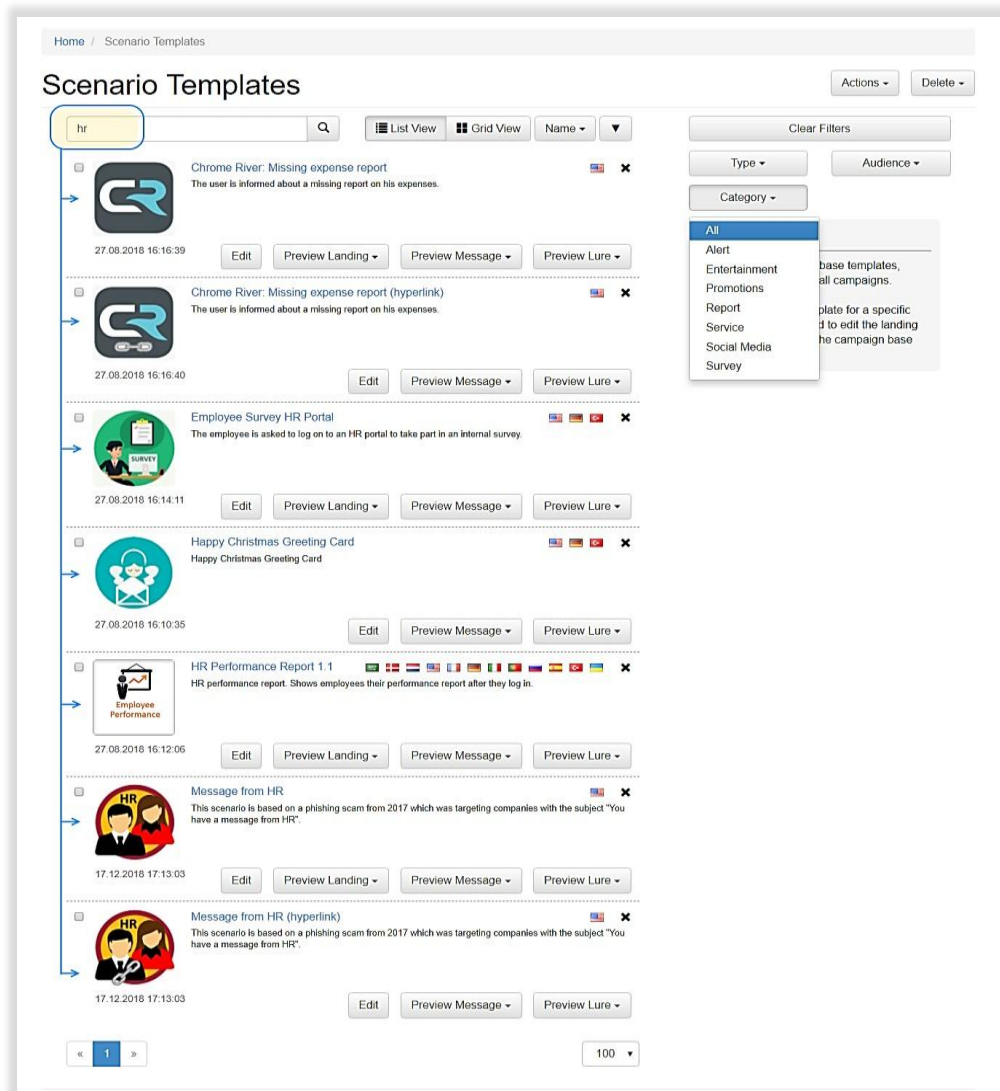
- Ransomware-Simulationsangriffe:** LUCY verfügt über zwei verschiedene Ransomware Simulationen, wobei eine das Personal und die andere die Infrastruktur testet.



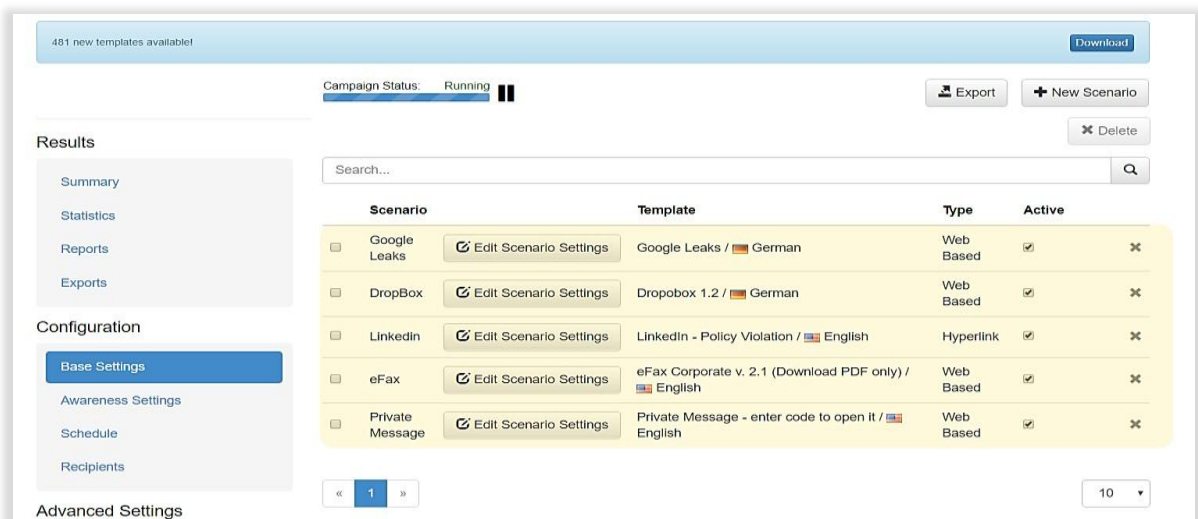
- Toolkit zur Validierung der Dateneingabe:** Bei der Phishing-Simulationen müssen fehlerhafte Akzeptanz für Anmeldefelder verhindert werden (z. B. Protokollierung mit ungültiger Syntax). Die Unternehmensrichtlinien können auch die Übertragung sensibler Daten wie Passwörter verbieten. Zu diesem Zweck bietet LUCY eine flexible Eingangsfilter-Engine, die für jede Anforderung eine geeignete Lösung bietet.

- Mehrsprachige Angriffsvorlagenbibliothek:** LUCY bietet Hunderte vordefinierte Angriffsvorlagen in mehr als 30 Sprachen in den Kategorien Dateneingabe (Vorlagen mit einer Webseite), dateibasiert (E-Mails oder Webseiten mit Dateidownload) und Hyperlink (E-Mails mit einem Link), gemischt (Kombination aus Dateneingabe und Download) und tragbaren Medien.

- **Sektor- und abteilungsspezifische Vorlagen:** Angriffsvorlagen sind für bestimmte Branchen oder Abteilungen verfügbar.



- **Gleichzeitige Verwendung von Angriffsvorlagen:** Mit LUCY können Sie mehrere simulierte Angriffsvorlagen in einer einzigen Kampagne verwenden. Mischen Sie die verschiedenen Typen (Hyperlink, dateibasiert, usw.) mit verschiedenen Angriffsthemen, um eine größtmögliche Risikoabdeckung und eine bessere Erkennungsrate der Mitarbeiter-Schwachstellen zu erzielen. In Kombination mit unserem Zufallsgenerator können komplexe Angriffsmuster über einen längeren Zeitraum ausgeführt werden.



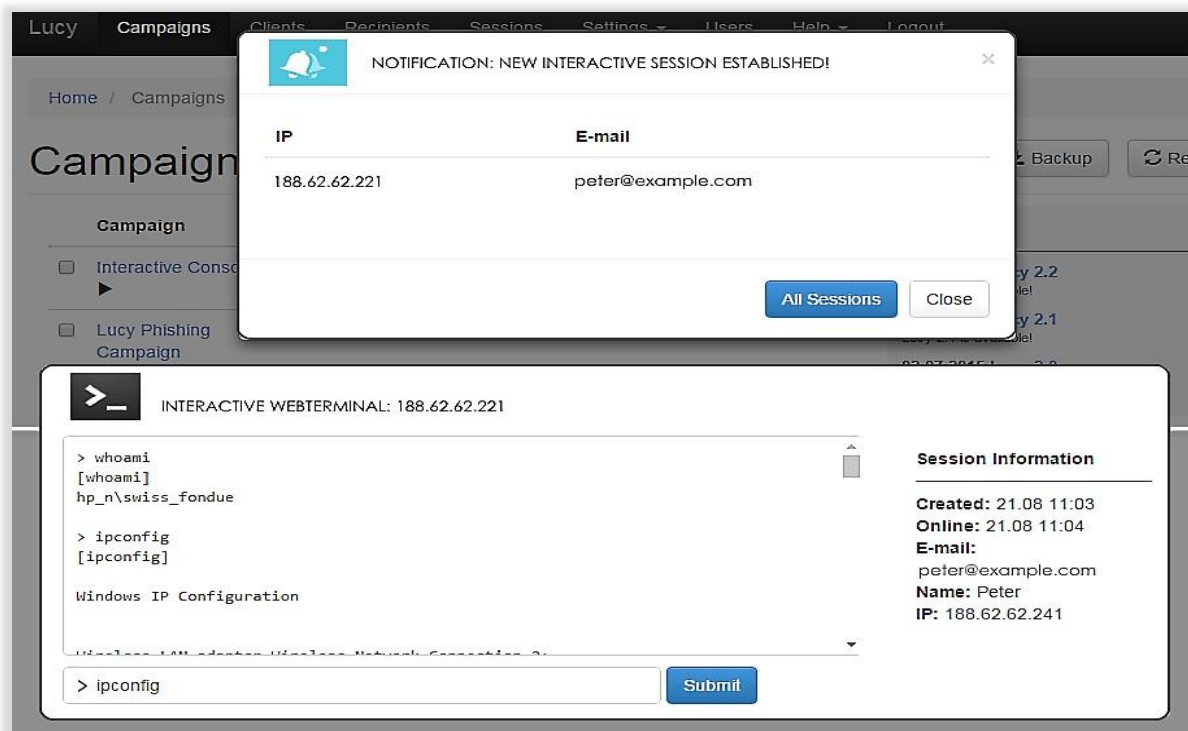
- **Variationen von Angriffs-URLs:** Übernehmen Sie die Kontrolle über die generierten URLs, um die Empfänger zu identifizieren. Verwenden Sie automatisierte kurze (<5 Zeichen) oder lange URL-Zeichenfolgen oder legen Sie für jeden Benutzer individuelle URLs fest. Mit der manuellen URL-Erstellung können Sie Links erstellen, an die sich ein Benutzer leicht erinnern kann. In einem Umfeld, in denen Link-Klicks in E-Mails deaktiviert sind, ist dies ein Muss.

The screenshot shows the 'LINK TEST' interface. On the left is a form with fields for Recipients, 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 an email from 'Test User <test@example.com>' with the subject 'Affordable car leasing for our employees'. The email body contains a message about a discounted leasing offer from 'CorporateCar-Leasing365' and a link to 'http://www.example.com/marketing-usa-1/'. A yellow box highlights the link, and a blue arrow points from the 'Link' field in the form to the link in the email preview.

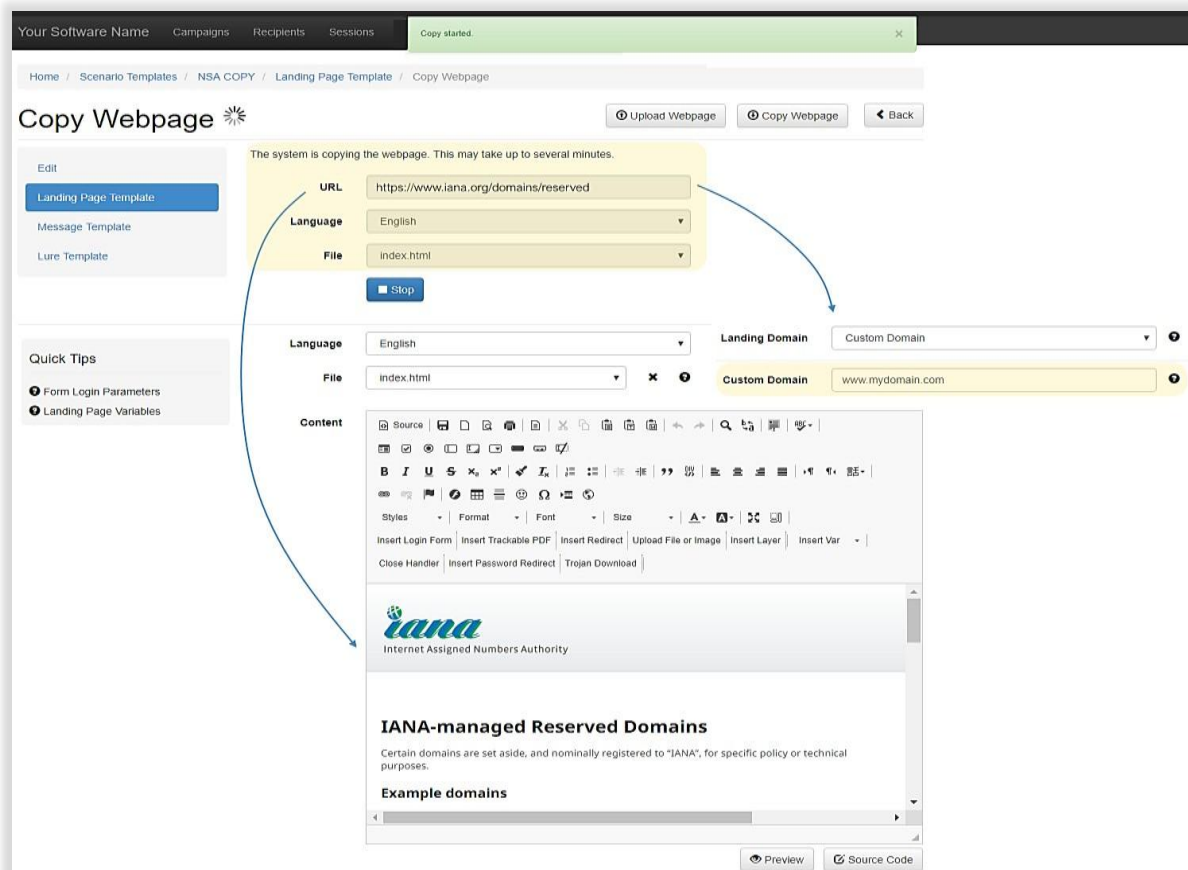
- **URL-Verkürzung:** URL-Verkürzungen sind ein relativ neuer Internetdienst. Da viele soziale Online-Dienste Zeichenbeschränkungen auferlegen (z. B. Twitter), sind diese URLs sehr praktisch. URL-Verkürzungen können jedoch von Cyberkriminellen verwendet werden, um das eigentliche Ziel eines Links zu verbergen, z. B. Phishing oder infizierte Webseiten. Aus diesem Grund bietet LUCY die Möglichkeit, verschiedene Verkürzungs-Services in eine Phishing- oder Smishing-Kampagne zu integrieren.

The screenshot shows the 'URL Shortener' interface. On the left is a form with fields for Landing Domain (cloudspace365.solutions), Subdomain (sms), Uri Shortener (N/A), Sender Name (004550776160), and Text (Check out this here %link%). A 'Save' button is at the bottom. On the right is a preview of a smartphone displaying a message that says 'Check out this link here: goo.gl/KuraFG'. A blue arrow points from the 'Uri Shortener' field in the form to the shortened URL in the preview.

- **Pentest-Kit:** Das Pentest-Kit ist ein Submodul des Malware-Simulations-Toolkits und trägt den Namen „Interaktive Sitzungen“. Sie können interaktiv mit einem Client-PC kommunizieren, der sich hinter einer Firewall befindet, indem Sie umgekehrte https-Verbindungen verwenden.



- **Webseiten-Kloner:** Erstellen Sie schnell hochprofessionelle Zielseiten für Ihre Kampagnen. Klonen Sie vorhandene Websites und fügen Sie zusätzliche Ebenen mit Dateneingabefeldern, Dateien zum Herunterladen und mehr hinzu.



- **Level-basierte Angriffe:** Level-basiertes Phishing-Training für Mitarbeiter dient dazu, das Risiko von Social Hacking messbar zu machen. Die wissenschaftliche Analyse sollte auch die wichtigsten Risikofaktoren identifizieren, damit einzelne Schulungsinhalte automatisch angeboten werden können.

Home / Campaigns / New Campaign

New Campa...

Campaign Status: Not Started

New Campaign

Name Please select a campaign name ...

Client Please select...

Industry N/A

Setup Mode

- ☐ Expert Setup (Manual Configuration)
- ☐ Pre-selected 5 minutes setup
- ☐ Launch a saved campaign template
- ☒ Level based campaign

Please choose a rule set

Go up one level No attack success & attack reported

Stay in level No attack success

Go down one level Attack was successful

Please choose start & end level

Minimum Start Level Please select...

Maximum End Level Please select...

Infrastructure testing

- ☐ Start a mail- and webfilter check campaign
- ☐ Start a local windows check campaign

E-Learning Settings

- ☐ Enduser Profiles Enabled
- ☐ Allow Awareness Rescheduling
- ☐ Ignore repeated answers in Awareness

Tracking

- ☐ Track Responses
- ☐ Email Tracking
- ☐ Automated Reporting

Template Please select... **Format** Please select...

Font Size 12 **Font Family** Helvetica

Antivirus/Firewall Protection Interval off

View Options ☐ Pinned

Save

- **Spear-Phishing-Simulation:** Die Spear-Phishing-Anpassung funktioniert mit dynamischen Variablen (Name, Geschlecht, E-Mail, Zeit, Links, Nachrichten, Abteilungen, Land, usw.), die Sie in Landing-Page und Nachrichtenvorlagen verwenden können.

Landing Domain cloudservices27.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

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:T:S", "6000")%. The document is only available for %division%, %location%, %staff-type%. I

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.

Save

Available Variables:

- %static%
- %link%
- %name%
- %email%
- %message%
- %link-awareness%
- %division%
- %location%
- %staff-type%
- %comment%
- %gender%
- %time(FORMAT, OFFSET, ZONE)%

- **DKIM / S / MIME-Unterstützung für Phishing-E-Mails:** Digitale Signaturen für E-Mails: Senden Sie signierte Phishing-Simulations-Mails (S / Mime). Verwenden Sie DKIM, um eine bessere Absenderbewertung zu erhalten.

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

☐ High Importance
☐ Receive Confirmation
☒ 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

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:** Möchten Sie wissen, welche E-Mail-Adressen Ihrer Organisation im Internet zu finden sind? Verwenden Sie den Mail-Scanner von LUCY und finden Sie heraus, was ein Hacker bereits über Ihr Unternehmen weiß.

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

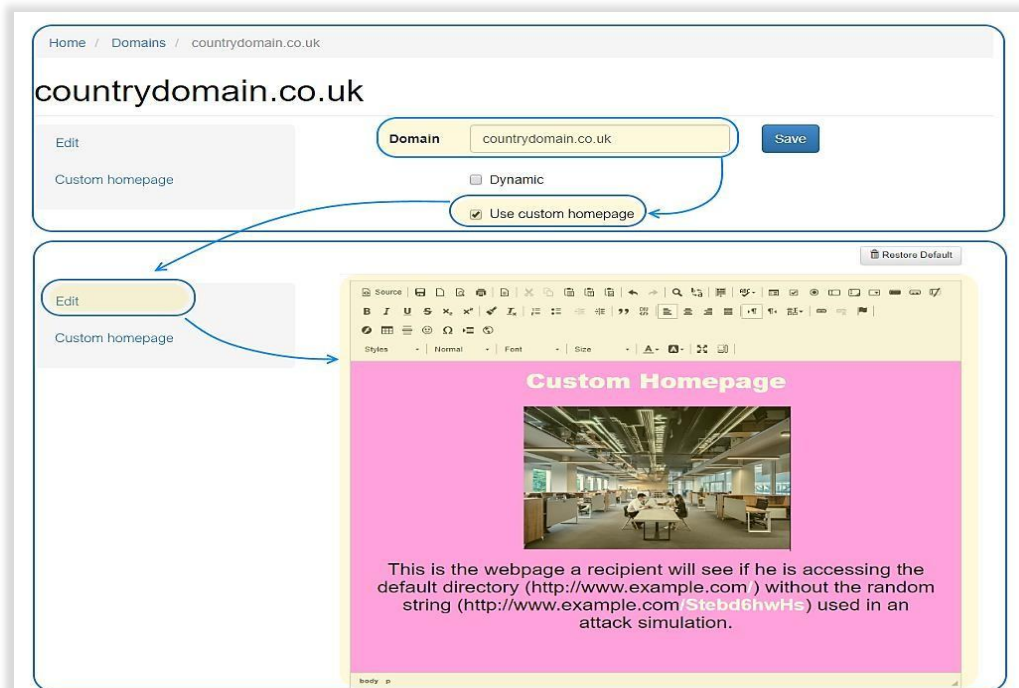
Maximum number of URLs to crawl

Maximum crawling time in minutes

☒ Yahoo
☒ Lixam
☒ Wotbox
☒ Yandex
☒ Bing
☒ Public Key Servers
☒ Additional Sources
☒ Paid Sources

Stop

- **Benutzerdefinierte Homepage-Erstellung:** Empfänger mit einem besseren technischen Verständnis können in ihrem Browser die Domain oder IP-Adresse aufrufen, die dem zufällig generierten Phishing-Link zugeordnet ist. Um zu verhindern, dass Fehlermeldungen angezeigt werden oder der Endbenutzer überhaupt in den Anmeldebereich der Administratorkonsole gelangt, können Sie in LUCY generische „Homepages“ für die in der Phishing-Simulation verwendeten Domains erstellen.



INFRASTRUKTUR-TEST

- **Malware Testing Toolkit:** Das Malware-Simulation-Toolkit ist eine erweiterte Malware-Simulationssuite, die verschiedene Bedrohungen nachbilden kann. Es ermöglicht einem Auditor den Zugriff auf eine Reihe erweiterter Funktionen, die vielen der von Cyberkriminellen verwendeten Tools entsprechen. Das Tool ermöglicht es dem LUCY-Administrator daher, Sicherheitsüberprüfungen durchzuführen, ohne Mitarbeiter außerhalb der IT-Abteilung einzubeziehen.

LUCY MALWARE TESTING SUITE

General Settings

☒ Enable Http Checks

☒ Http via IE

☒ Http with IE proxy

☒ Http with IE proxy and default credentials

☒ Http with proxy from Firefox

☒ Enable Net Checks

☒ DNS

☒ ICMP

☒ SMTP

☒ FTP

☒ SSH

☒ Enable Windows Checks

☒ OS Version

☒ Firewall

☒ Antivirus

☒ Virus downloading

☒ Hosts

LUCY MALWARE TESTING SUITE

General Settings

Test started: 10:18:40 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 antivirus FAIL

Send Save

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 ■

No	Test	Info	Result	Status	Risk	Solution
1	Command & IE access to st	View Details	Executed command: whoami (full output)	Success	■	View Details
2	Read recent document	View Details	C:\Users\lawis_\Favorites\Example-Communication\Emails.doc (full output)	Success	■	View Details
3	Access to last Outlook e-mail	View Details	Email: [john.doe@phishing-server.com] Subject: [VPN C] Only last mail and last 5 symbols of subject are displayed for privacy reasons	Success	■	View Details
4	Screenshot	View Details		Success	■	View Details
5	Webcam access test	View Details		Success	■	View Details
6	Access to the internet via IE	View Details	Received page url: http://www.google.com (full output)	Success	■	View Details
7	Access to the internet via a http	View Details	Error occurred: Invalid URI: The hostname could not be parsed. (full output)	Fail	■	View Details
8	Access to the internet via a http with IE proxy	View Details	Error occurred: Invalid URI: The hostname could not be parsed. (full output)	Fail	■	View Details
9	Access to the internet via a http with IE proxy	View Details	Error occurred: Invalid URI: The hostname could not be parsed. (full output)	Fail	■	View Details

LMPC

General Checks Templates

☒ Enable Advanced Dropper

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

Amount of sessions: [5]

Interval between sessions, minutes: [5]

☒ Enable Ransomware

Hours of work (0-23): From: [8] To: [17]

☒ Use dummy data ☐ Delete data

Extensions (separated by commas): .doc;.pdf;.txt

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

Crawl time, minutes: [120]

Amount of file operations: [100000]

- **E-Mail- und Webfiltertest:** Diese Funktion bietet die Antwort auf eine der wichtigsten Fragen zur Sicherung des Internet- und E-Mailverkehrs: Welche Dateitypen aus dem Web können heruntergeladen werden und welche E-Mail-Anhänge werden herausgefiltert und welche nicht?

[Home](#) / [Scenario Templates](#) / [Mail & Web Test](#) / [File List](#)

MWFT (1)

[Summary](#)
[Base Settings](#)
[Reports](#)

Advanced Settings
[User Settings](#)

Logs
[Supervision Log](#)
[Message Log](#)
[Errors](#)

Campaign Status: Not Started

[Reset Stats](#)
[Export](#)
[Start](#)

Mail & Web Test Overview

2

7% of files downloaded

27

96% of files submitted

1

4% of files downloaded successfully

1

4% of files submitted successfully

Dangerous File Types in archives

Name	Downloaded	Mailed	Download Result	Mail Result
Dll-archiv-1.gz2	✓	✓	✗	✓
Dll-archiv-1.tar	✗	✓	✗	✗
Dll-archiv-1.zip	✗	✓	✗	✗
exe-archiv-1.gz	✗	✓	✗	✗

File List

[Mime Types](#)
[+ New File](#)
[+ New Class](#)

[Edit](#)
[File List](#)

Search...

Dangerous File Types in archives

Profanity

Harmless Level 3 Files

Encrypted Class 1 Files

PDF & Office Exploits

Harmless Macros

Use Obfuscation technique to hide malware

Dangerous file types

Edit File

[Edit](#)
[File List](#)

Name

exe-archiv-1.tar

Mime Type

application/x-tar

Class

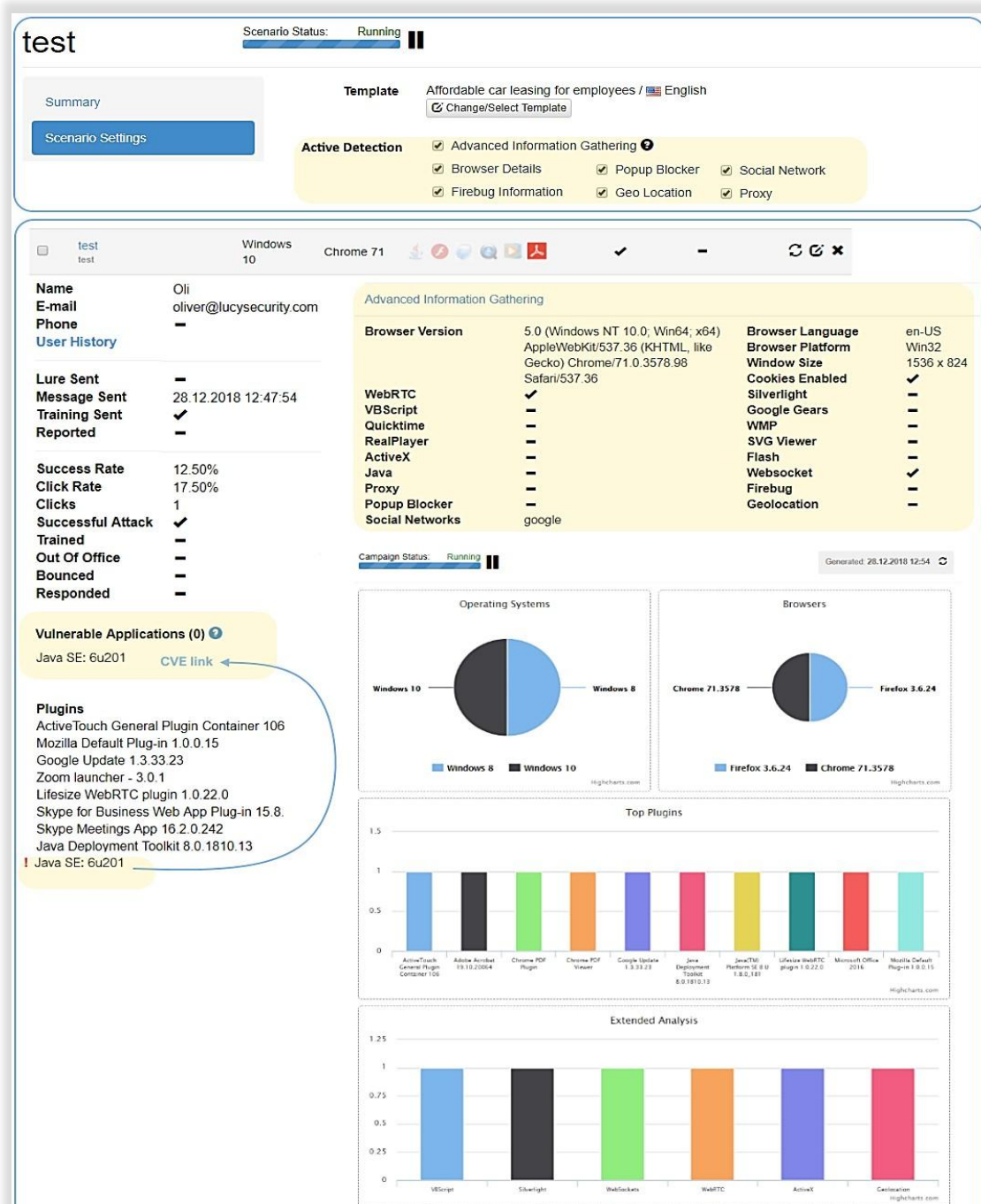
Dangerous File Types in archives

File

[Upload](#)
[Download](#)

[Save](#)

- **Erkennen aktiver und passiver Client-Sicherheitslücken:** Diese Funktion ermöglicht das lokale Testen des Client-Browsers und das Erkennen möglicher Sicherheitslücken basierend auf benutzerdefinierten Javascript-Bibliotheken und den Benutzeragentendaten des Browsers. Die erkannten Plug-ins können automatisch mit der Schwachstellendatenbank (CVE) verglichen werden, um anfällige Geräte zu identifizieren.



- **Spoofing-Test:** Testen Sie Ihre eigene Infrastruktur auf E-Mail-Spoofing-Schwachstellen.

Home / Mail Spoofing

Mail spoofing test

Domain
phishing-server.com
Start Test

Recipient Email
spoofing-test@phishing-server.com

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

TECHNISCHE TESTS

- **Reputationsbasiertes E-Learning:** Schulen Sie Ihre Mitarbeiter, den gebotenen Anforderungen entsprechend. Bewerten Sie die Fähigkeiten der Mitarbeiter und ermöglichen Sie einen gesunden Wettbewerb zwischen den Kollegen (Gamification). Basierend auf den Reputationsprofilen jedes Benutzers kann das System automatisch mehrere Schulungen durchführen. Die Reputationsprofile basieren unter anderem auf dem Verhalten des Benutzers in Phishing-Simulationen. Dies stellt sicher, dass Benutzer, die wiederholt in die Falle gegangen sind, andere Trainingsinhalte erhalten als Benutzer, die zum ersten Mal auf eine Angriffssimulation klicken.

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

Template
Affordable car leasing for employees / English
Change/Select Template
Name
test
Send Link to Awareness Website Automatically
Send Awareness By Click Rate
40 %
Send Awareness By Success Rate
20 %
Awareness Delay
0

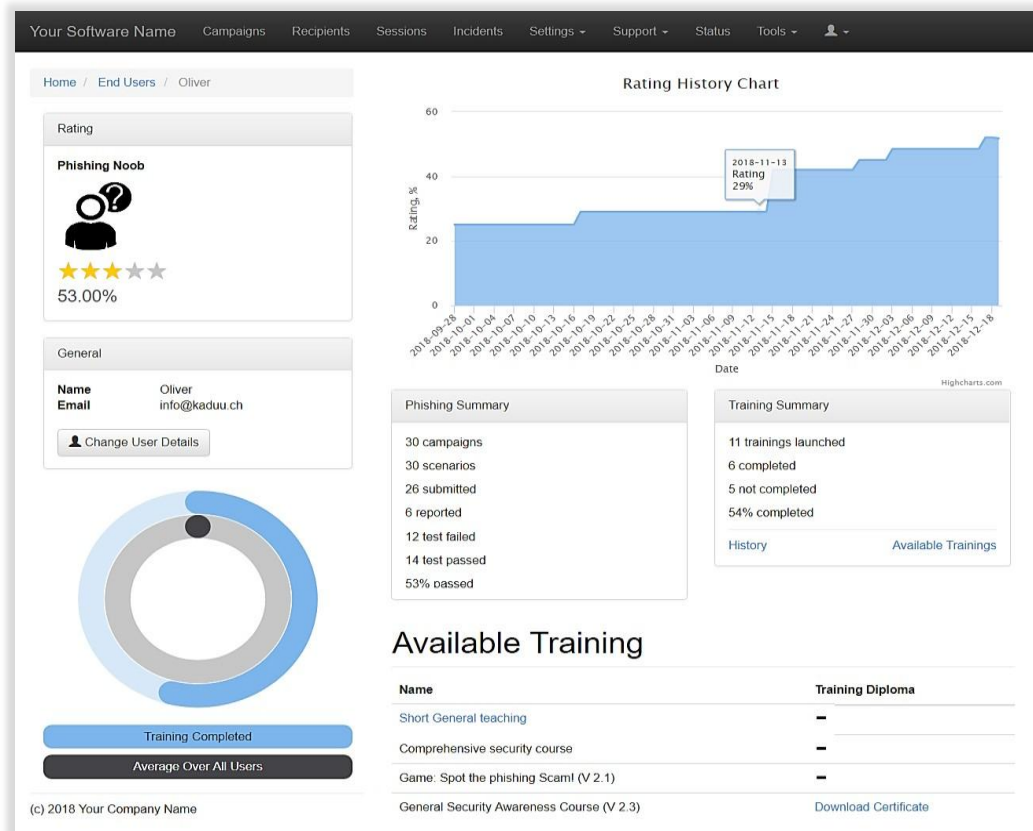
Configuration
Base Settings
Awareness Settings

Export
New Awareness

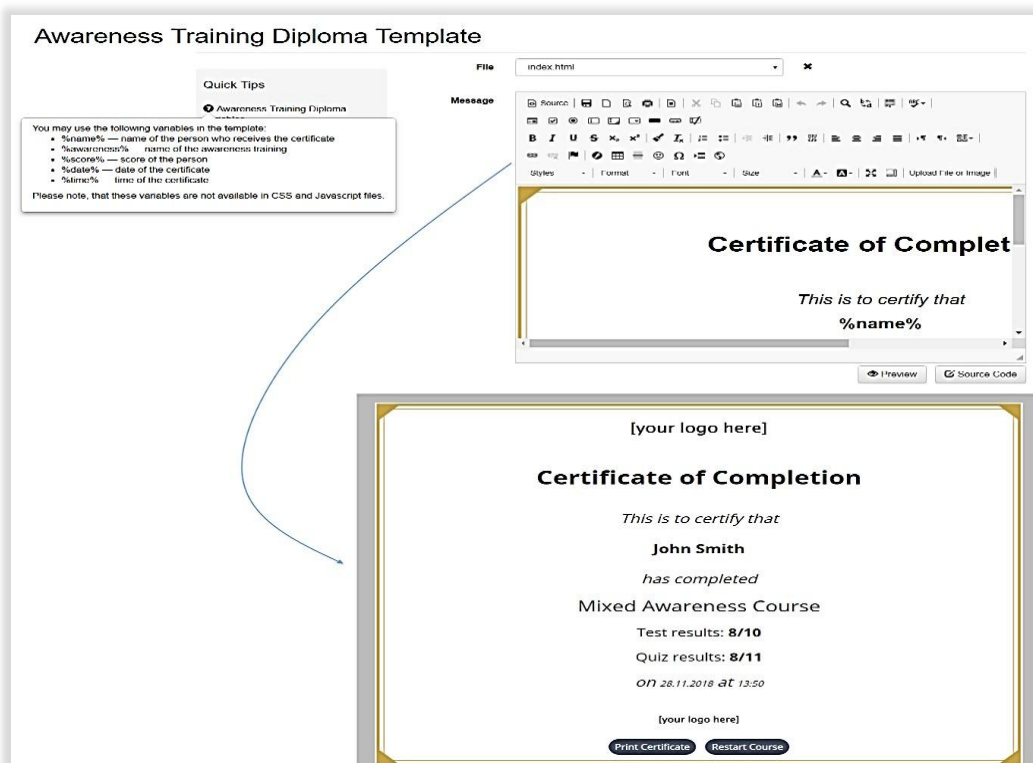
Awareness	Course	Risk Level
Comprehensive security course	Comprehensive security course	0
Repetition Course	Avoid & Recognize Phishing Attacks (V 2.3)	2
Short General teaching	Email Only - This was a phishing simulation & Tips	3

1
10

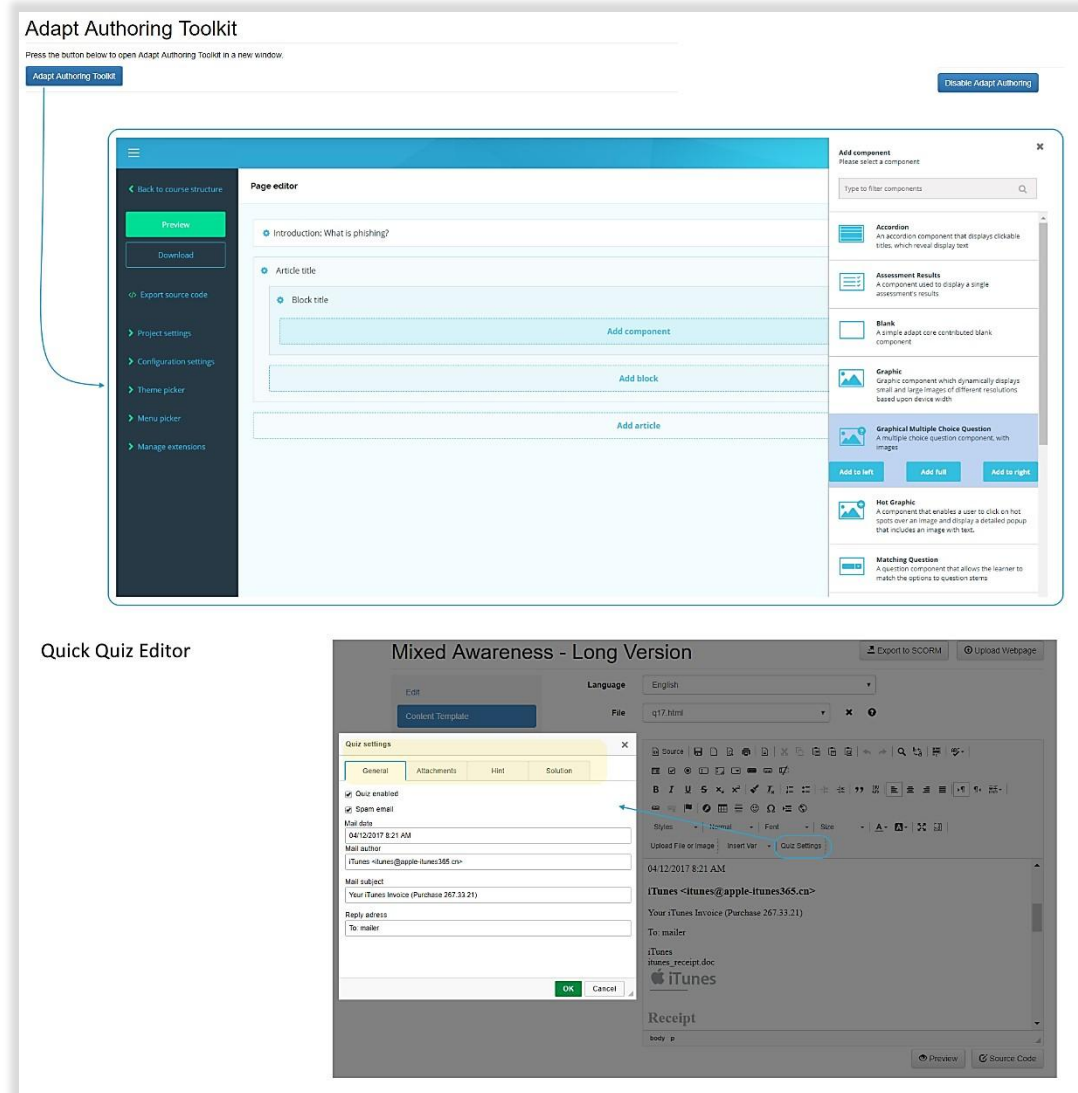
- **Endbenutzer-Schulungsportal:** LMS-Funktionalität (Learning Management System): Ermöglicht jedem Mitarbeiter permanenten Zugriff auf eine personalisierte Schulungshomepage, auf der eigene Kurse speziell auf ihn zugeschnitten sind. Auf dieser Homepage können Leistungsstatistiken angezeigt werden, das Training fortgesetzt oder wiederholt werden, Kurszertifikate können erstellt und Ergebnisse mit anderen Abteilungen oder Gruppen verglichen werden.



- **Fortbildungsdiplom Sicherheitsbewusstsein:** E-Learning-Zertifikate können vom Berechtigten entweder direkt im Rahmen einer Schulung oder im LMS-Portal erstellt und ausgedruckt werden.



- **e-Learning-Authoring-Toolkit:** Das E-Learning-Authoring-Toolkit (Adapt) ermöglicht die Erstellung individueller Lerninhalte. Ziehen Sie Videos oder andere Rich Media-Formate per „Drag und Drop“ an die gewünschte Stelle, fügen Sie Tests aus vordefinierten Menüs ein und erstellen Sie in kürzester Zeit interaktive E-Learning-Inhalte, von Grund auf neu.



- **Rich Media-Sensibilisierungstraining:** Integrieren Sie Rich Media (Video, Audio oder andere Elemente, welche den Zuseher zur Interaktion ermuntert und ihn mit dem Inhalt „fesselt“) in Ihre Sensibilisierungstrainings. Verwenden Sie die vorhandenen Lernvideos, passen Sie sie an oder fügen Sie Ihre eigenen Rich Media hinzu.

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", "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: 60-90 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://go.gihXW5G>. Duration: 5-10 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

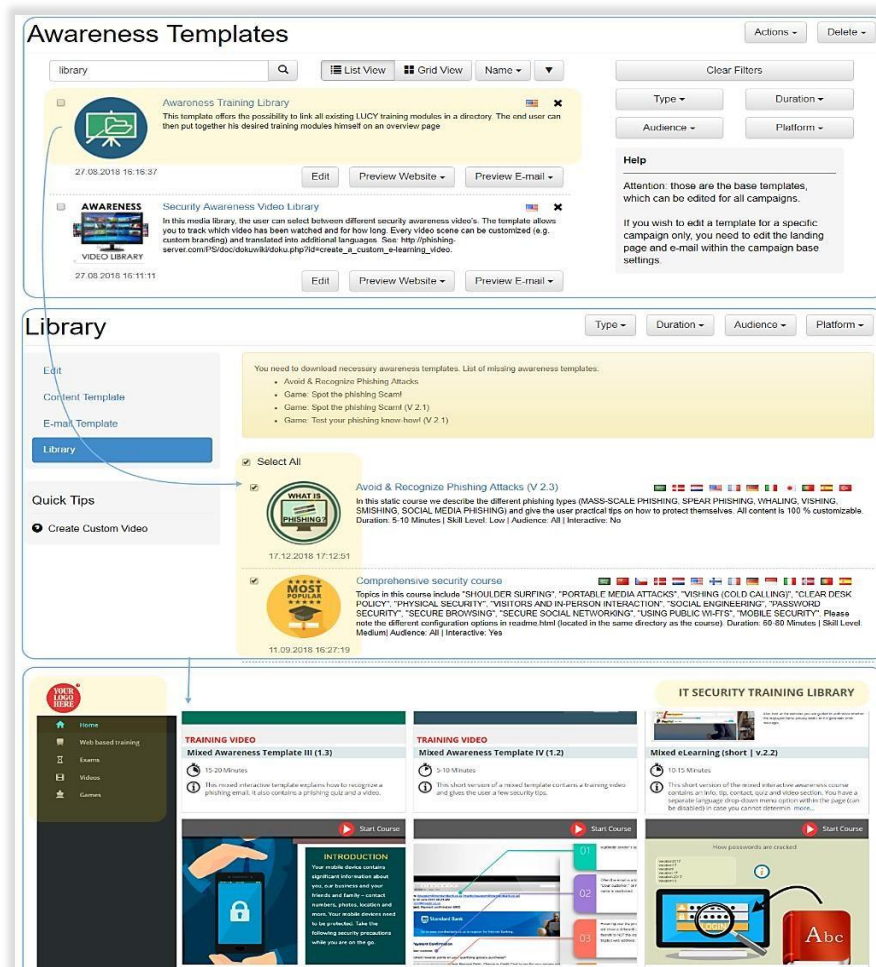
This course covers security incidents and the processes involved in reporting such incidents.

28.12.2018 14:48:47

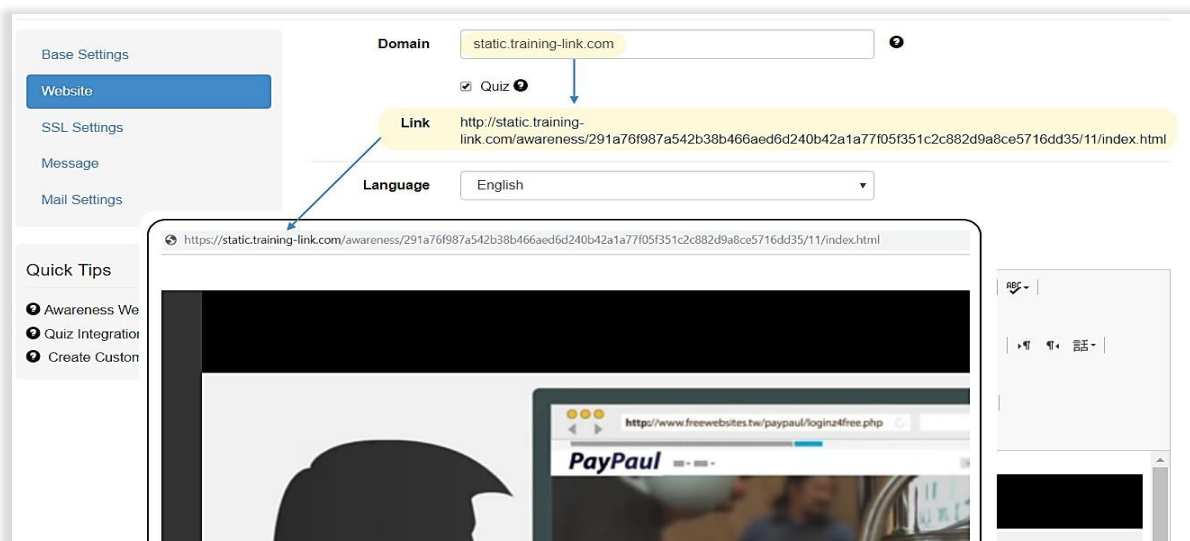
Edit Preview Website Preview E-mail

...and many more

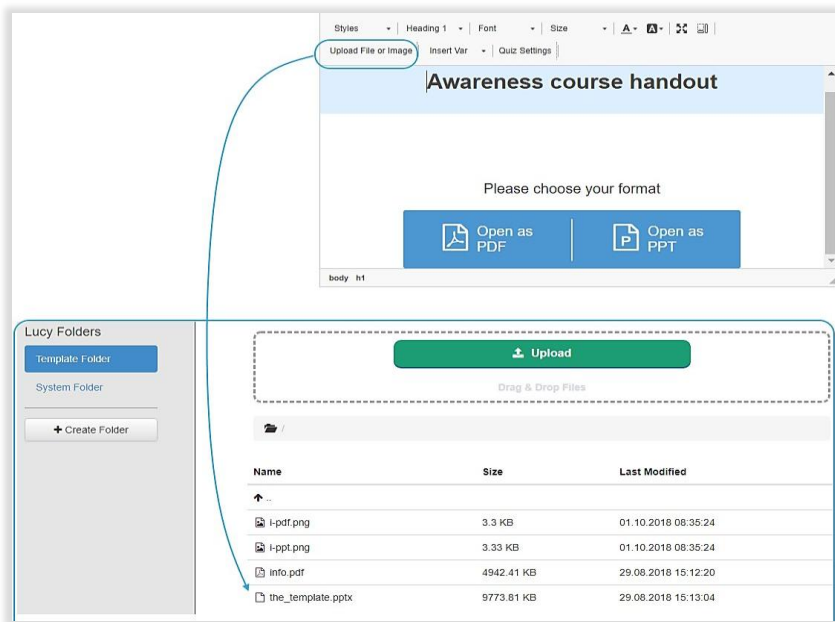
- **Schulungsbibliothek:** Ihre Mitarbeiter können über eine Übersichtsseite mit dem Namen „Schulungsbibliothek“ auf die Schulungsinhalte Ihres Unternehmens zugreifen. Es enthält eine große Auswahl der regulären E-Learning-Vorlagen von LUCY, die als Eingabe dienen. Die Übersichtsseite kann nach bestimmten Themen (Video, Quiz, Test, usw.) sortiert werden.



- **Unterstützung für statische Schulungen:** Schulungsinhalte können auch auf statischen Seiten in LUCY oder im Intranet veröffentlicht werden, sodass der Benutzer unabhängig von möglichen Angriffssimulationen permanent auf Schulungsinhalte zugreifen kann.



- **Schulungssupport offline:** LUCY bietet eine Reihe adaptierbarer Vorlagen (Adobe Photoshop oder Illustrator-Dateien) für Sensibilisierungs-Schulungen, wie Poster, Flyer, Bildschirmschoner, usw.



- **Microlearning-Module:** Wir haben Microlearning-Schulungsmodulare (z. B. 1-minütige Videos oder 1-Seiten-Module zur Sicherheits-Sensibilisierung) entwickelt, die auf die Branding- und Richtlinienanforderungen Ihres Unternehmens zugeschnitten werden können.

☐

Micro Module: Phishing

In this course the student will be guided through different lessons. These include tips, video, quizzes and a test. Each learning content is in a separate chapter. 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: 15-25 Minutes | Skill Level: Medium | Audience: All | Interactive: Yes

18.12.2018 13:05:47

Edit Preview Website Preview E-mail

☐

Micro Module: 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

18.12.2018 13:05:43

Edit Preview Website Preview E-mail

☐

Micro Module: Password security

In this course the participant learns how to navigate the Internet safely.

26.12.2018 15:08:18

Edit Preview Website Preview E-mail

☐

Micro Module: Secure Storage

Security topics related to mobile data storage devices and cloud-based storage services are presented in this course. At the end of the course a test will be carried out. If the participant passes the test, he or she can create a diploma and print it out.

21.12.2018 14:43:58

Edit Preview Website Preview E-mail

☐

Micro Module: Workplace Security

In this course the employee learns how to behave in the workplace. Topics include the disposal of data, cleaning up the workplace, locking the screen, printing data, etc. At the end of the course a test will be carried out. If the participant passes the test, he or she can create a diploma and print it out.

...and many more!

- **Videoanpassung:** Senden Sie uns Ihr Firmenlogo und wir integrieren es in die Schulungsvideos. Sie wünschen eine andere Sprache? Kein Problem. Wir passen das Video so an, dass es in der von Ihnen gewünschten Sprache läuft. Sie wünschen eine andere Szene? Laden Sie einfach die Videoskripte herunter und markieren Sie die gewünschten Änderungen



27.08.2018 16:12:23

Security Awareness Video: 7 Security Tips 1.3

In this short 3-minute security awareness video we have put together 7 security tips, which involve best practices and policies that promote security. The content (animation, language, script) is customizable. More info about customization can be found here: <https://goo.gl/HXN9SG>. Duration: 3 minutes | Skill Level: Low | Audience: All | Interactive: No

[Edit](#)
[Preview Website](#)
[Preview E-mail](#)



Drag & Drop Files

Name	Size	Last Modified
↑ ..		
 2018.06.11_Lucy Data Privacy.mp4	44094.42 KB	27.08.2018 16:16:28
 2018.06.11_Lucy Data Privacy.webm	34599.3 KB	27.08.2018 16:16:29

General Security Awareness Video

- **Example:** <https://youtu.be/i0iLy8racHI>
- **Current Language(s):** English, German, Spanisch, Dutch, French, Italian
- **Possible Translation in other Languages:** All* (*If you want to have the video in a different language you have the option to order this for USD 350)
- **Cost of scene changes:** See movie script* (*If you want to have the content changed (e.g. logo or different scenes altered) please download the movie script and send us back the desired changes within that document)
- **Movie Script:** [sample_lucy_movie_storyboard_general_awareness.docx](#)
- **Topics:** Social Engineering, Physical Security, Phishing, Clean Desk Policy etc.

- **Mobile-Responsive-Format:** Viele der in LUCY integrierten Module sind in einem Mobile-Responsive-Format verfügbar, das Ihren Benutzern die Flexibilität bietet, an jedem angeschlossenen Gerät die Schulungen zu durchlaufen.



- **Videoimport / -export:** Sie können LUCY-Videos auf Ihr eigenes System exportieren sowie Ihre eigenen Videos in LUCY importieren.

The screenshot shows 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 selected, showing its details: 'This video is dedicated to the topic "data privacy & GDPR". The content (animation, language, script) is customizable. More info about customization can be found here: <https://goo.gl/HXN9SG>. Duration: 5:50 Minutes | Skill Level: Low | Audience: All | Interactive: No'. On the left, there's a 'Lucy Folders' sidebar with options like 'Template Folder', 'System Folder', '+ Create Folder', 'Rename', 'Copy', 'Move', 'Download', and 'Delete'. The 'Download' button is highlighted. In the center, there's an 'Upload' button and a 'Drag & Drop Files' area. Below that, a table lists files: 'flowplayer', '2018.06.11_Lucy Data Privacy.mp4', '2018.06.11_Lucy Data Privacy.webm', and 'jquery.js'. The '2018.06.11_Lucy Data Privacy.mp4' file is highlighted.

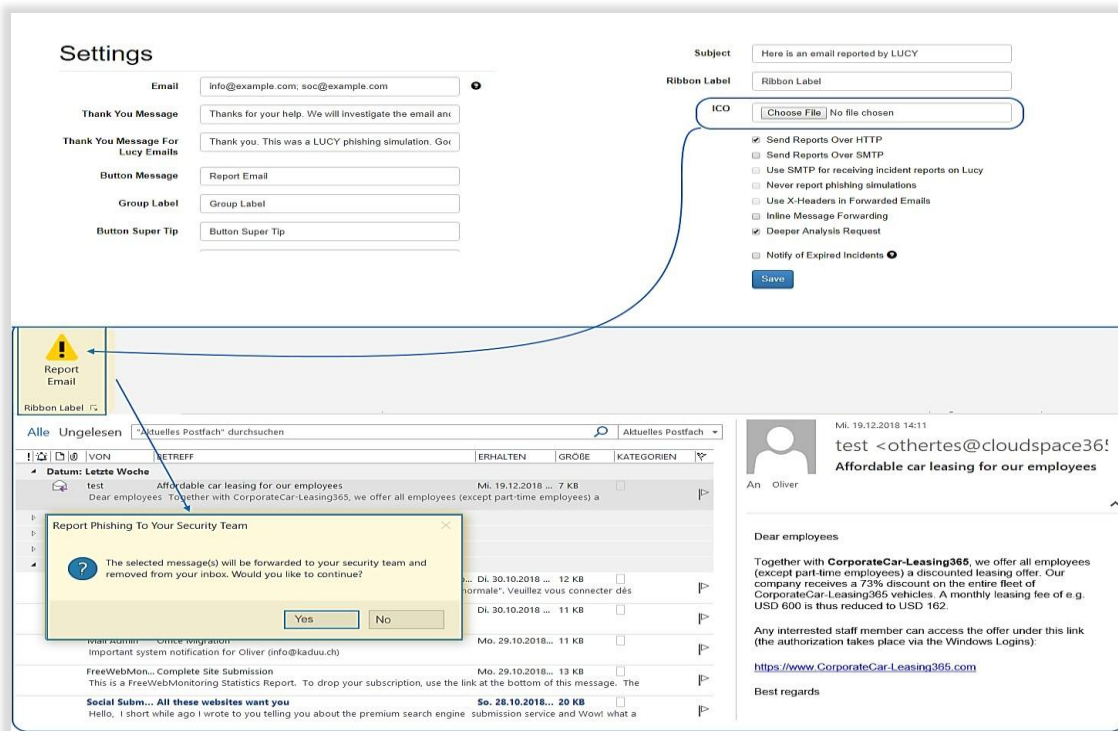
- **Dynamische Schulungshinweise:** Mit den implementierten dynamischen Hinweisen kann Ihr Administrator Markierungen an den Angriffsvorlagen setzen, die Ihren Mitarbeitern im E-Learning-Material anzeigen, wo der Phishing-Angriff möglicherweise erkannt wurde.

The screenshot shows the 'Comprehensive security course' interface. At the top, there's a breadcrumb trail: 'Home / Awareness Templates / Comprehensive security course / Content Template'. The main title is 'Comprehensive security course'. On the left, there's a sidebar with 'Edit', 'Content Template', and 'E-mail Template' buttons. The 'Content Template' button is highlighted. Below that, there's a 'Quick Tips' section with links to 'Awareness Website Variables', 'Quiz Integration', and 'Create Custom Video'. In the center, there's a 'Language' dropdown set to 'English' and a 'File' dropdown set to 'index.html'. Below that, there's a 'Content' section with a rich text editor. The 'Export to SCORM' button is highlighted. On the right, there's an 'Upload Webpage' button. Below the main content, there's an 'Exports' section with a table listing exports. The first export is highlighted: '31.12.2018 15:08:53', 'Awareness Template - Comprehensive security course'. To the right of the table, there's a 'scorm-export.zip' file icon.

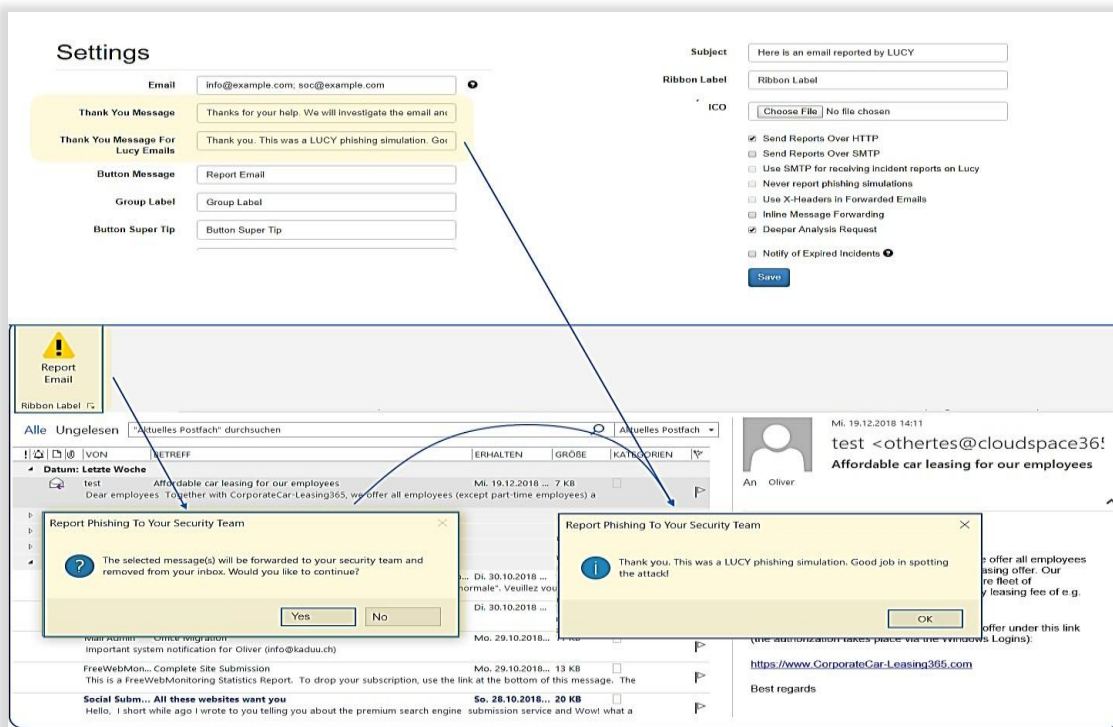
Date	Name	Extension	Status
31.12.2018 15:08:53	Awareness Template - Comprehensive security course		✓
29.12.2018 17:10:15	Campaign - BOUNCE TEST	csv	✓
28.12.2018 15:19:11	Awareness Template - Avoid & Recognize Phishing Attacks (V 2.3)		✓

MITARBEITER MITEINBEZIEHEN

- **E-Mails mit einem einzigen Klick melden:** Benutzer können verdächtige E-Mails mit einem einzigen Klick an eine oder mehrere E-Mail-Adressen melden und an die LUCY-Vorfallsanalyse weiterleiten lassen.



- **Bestärkung im richtigen Verhalten:** Unser Plug-in bietet automatisch eine Bestärkung des richtigen Verhaltens, indem es dem Benutzer mittels einer Nachricht aus Ihrem Unternehmen entsprechende Dankbarkeit ausdrückt.



- **Deep Inspection Request:** Manchmal möchten Benutzer wissen, ob die empfangene E-Mail sicher geöffnet werden kann. Der Benutzer kann optional den sog. „Deep Inspection Request“ im lokalen Plug-in verwenden, um dem Sicherheitsteam mitzuteilen, dass er Feedback zu der gemeldeten E-Mail erhalten möchte.

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
Datum: Vorletzte Woche				
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. 18.12.2018 ...	5 KB	
Hy there What we have here is an interesting offers Are you in? <http://red.studygood.com/WRLKMOAINNX> <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	Filter
29.12.2018 11:49	oliver@muenchow.ch	Lucy Test	BOUNCE TEST	0.00	Simulation	All
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 20:59	oliver@muenchow.ch	Lucy Test	Attack CS	0.00	Simulation	

Filter

Client: All

From Date: 29.12.2017

To Date:

Need more analysis

- Automatische Vorfallsanalyse:** Verwalten und Reagieren auf gemeldete verdächtige E-Mails über eine zentrale Verwaltungskonsole: Die LUCY-Analyse ermöglicht eine automatische Überprüfung der gemeldeten Nachrichten (Header und Text) und enthält eine individuelle Risikobewertung, die ein Echtzeit-Ranking der gemeldeten E-Mails liefert. Diese Bedrohungsanalyse entlastet die Arbeit des Sicherheitsteams spürbar.

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

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 address defined than the actual (more info...)	1.60	Active ☒ Inactive ☐
New Domain Domain has been reserved in the last 30 days (more info...)	20.00	Active ☒ Inactive ☐
Link Display mismatch link display name different from the actual link (more info...)	0.00	Active ☐ Inactive ☒

Summary
Mail Server Analysis
Domain Analysis
Body Analysis

Overall Risk Score:

2.5 of 10.0
Highcharts.com

Need More Analysis

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

- Automatisches Vorfalls-Feedback:** Mit diesem Vorfalls-Feedback kann eine automatische Benachrichtigung an den Benutzer mit den Ergebnissen der E-Mail-Bedrohungsanalyse gesendet werden. Der Nachrichtentext ist frei konfigurierbar, und bei Bedarf kann auch der sog. LUCY E-Mail Risk-Score hinzugefügt werden.

The screenshot shows the 'Autoresponder' configuration page. At the top, there's a navigation bar with 'Incidents' highlighted. Below it, a breadcrumb trail reads 'Home / Phishing Incident Reports / Autoresponder'. The main heading is 'Autoresponder'. On the right, there's a button 'Upload Message Template'. On the left, under 'Quick Tips', there's a link 'Autoresponder Email Variables'. The main form has a toggle 'Enable Autoresponder' (checked). Below it, fields for 'Subject' (Your email submission), 'Sender Name' (Security Team), and 'Sender E-mail' (soc@example.com) are visible. The 'Content' section features a rich text editor with a toolbar. The text in the editor reads: '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'. At the bottom right of the content area are 'Preview' and 'Source Code' buttons.

- Bedrohungsminderung:** Dieser verhaltensbezogene Bedrohungsminderer ist ein revolutionärer Ansatz zur Beseitigung von E-Mail-Risiken. Es unterstützt den Sicherheitsadministrator bei der Abwehr des Angriffs (z. B. Senden eines automatisierten Berichts an spezialisierte Teams bei den Anbietern, die für den Angriff genutzt wurden).

The screenshot shows a workflow for sending an abuse report. It starts with the 'Select Incident' panel, which has a table of incidents. A blue arrow points from the 'Send Abuse' button in the top right of this panel to the 'Select Abuse Domain/IP' panel. The 'Select Incident' panel includes a table with columns: Time, Email, Client, Campaign, Score, and Status. The second row is selected. To the right is a 'Filter' section with a 'Search' input and a 'Client' dropdown. The 'Select Abuse Domain/IP' panel has a 'MAIL HEADER' section with a table of domains/IPs and their associated abuse email addresses. A blue arrow points from the 'Send abuse report' button in this panel to the 'Select Abuse Template' panel. The 'Select Abuse Template' panel has fields for 'Subject', 'Sender Name', and 'Sender E-mail', and a 'Content' section with a rich text editor. The text in the editor starts with 'Dear Abuse Team,' and includes placeholders like '%email%', '%time%', '%domain%', and '%report%'. A 'Send abuse report' button is at the bottom of the 'Select Abuse Domain/IP' panel.

- **Benutzerdefinierte und regelbasierte Analyse:** Definieren Sie Ihre eigenen Regeln für die E-Mail-Analyse und Risikoberechnung.

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
From Date

Custom Rules
Score Factors
Abuse
Autoresponder
Plugin Settings

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 ☒ Inactive	⊗ ⓘ ✕
New Domain	Domain has been reserved in the last 30 days (more info...)	20.00	Active ☒ Inactive	⊗ ⓘ ✕
Link Display mismatch	link display name different from the actual link (more info...)	0.00	Active ☐ Inactive	⊗ ⓘ ✕

- **Anpassungsoptionen für Plug-ins:** LUCY ermöglicht eine einfache Anpassung und ein vollständiges „White labelling“ für verschiedene Plugin-Funktionen (angezeigte Symbole, Rückmeldungen, Kennzeichnungen, Übertragungsprotokolle, gesendete Header, usw.).

The screenshot shows the 'Phishing Incident Reports' interface. At the top, there's a table with columns: Time, Email, Client, Campaign, Score, Status, and icons. Two entries are visible, both from 'oliver@muenchow.ch'. To the right of the table is a 'Filter' section with 'Search' and 'Client' dropdowns. Above the table are buttons for 'Send Abuse', 'Delete', 'Delete All', 'Settings', and 'Download Plugin'. The 'Settings' dropdown is open, showing options: 'Custom Rules', 'Score Factors', 'Abuse', 'Autoreponder', and 'Plugin Settings'. Below the table is a 'Settings' panel with various input fields for messages (Email, Thank You, Report Title, Error Title, No Selection, Eval Error, Send Error, Unsupported, Subject, Ribbon Label, User Request) and checkboxes for reporting preferences (Send Reports Over HTTP, SMTP, X-Headers, etc.). A 'Save' button is at the bottom right of the settings panel. Below the settings panel is another instance of the 'Phishing Incident Reports' table and controls, with the 'Download Plugin' dropdown open, showing options for Microsoft Outlook (32-bit, 64-bit, 365) and Gmail Addon.

- **Integration von Drittanbietern:** Mithilfe der REST-API-Automatisierung von LUCY können wir gemeldete E-Mails verarbeiten und Ihrem Sicherheitsteam dabei helfen, aktive Phishing-Angriffe bereits während des Vorgangs zu stoppen.

The screenshot shows the 'API Whitelist' interface. At the top, there's a table with columns: IP, and a delete icon. Two entries are visible: '192.168.10.231' and '192.168.12.114'. Above the table are buttons for '+ New', 'Delete', and 'API Documentation'. Below the table is a section titled 'Resources' with a list of API endpoints. To the right of this is a section titled 'Endpoint List' with a list of API endpoints. Below these sections is a table with columns: Endpoint, Method, and Description. Three entries are visible: '/api/incidents' (GET), '/api/incidents/:id' (GET), and '/api/incidents/:id' (DELETE).

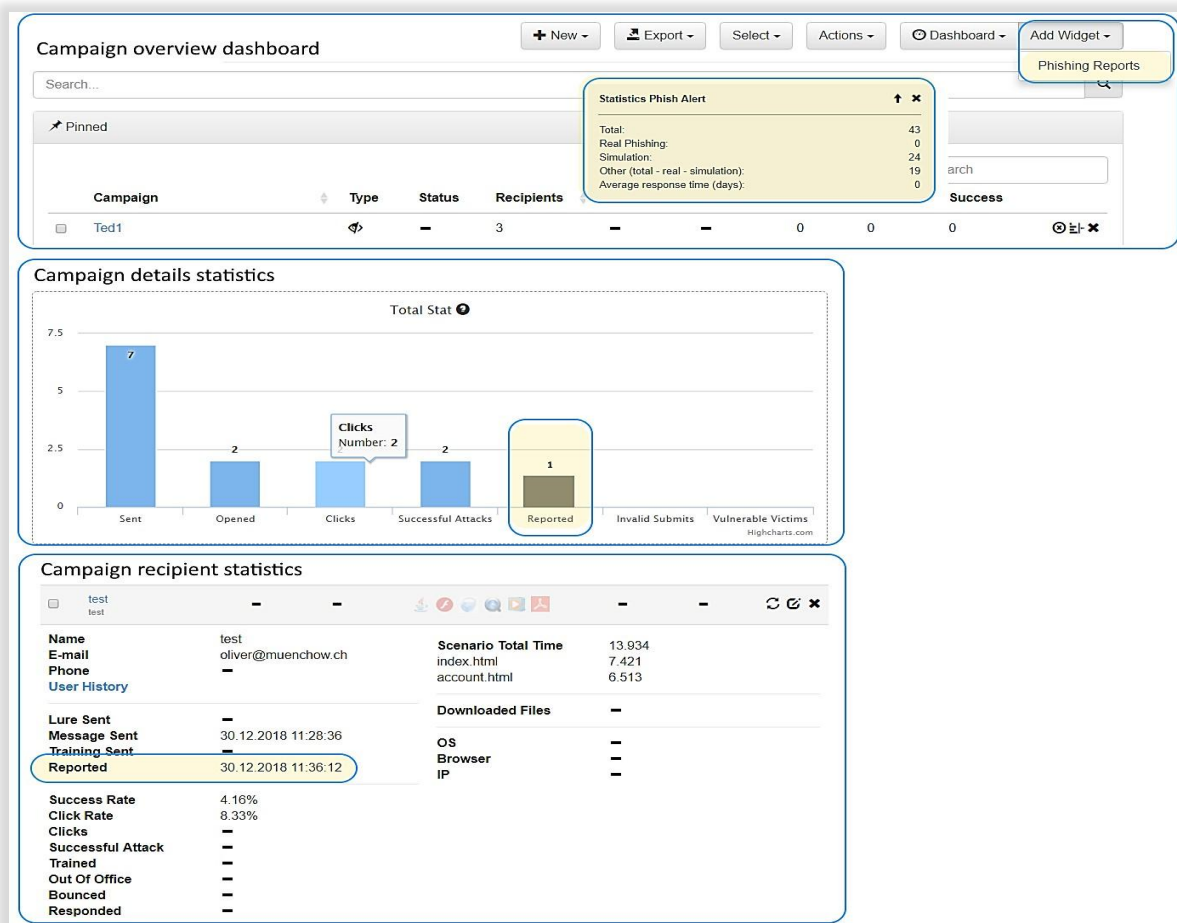
- **Identifizieren von Angriffen nach einem gängigen Muster:** Wenden Sie die Dashboard-Filter von LUCY an, um allgemeine Angriffsmethoden in Ihrem Unternehmen zu erkennen. Suchen Sie in allen gemeldeten E-Mails nach ähnlichen Bedrohungs-Indikatoren.

The screenshot shows the 'Incident Reports' dashboard in Lucy. The top section displays a table of reports with columns: Time, Email, Rating, Client, Campaign, Score, and Status. The table lists several reports, including one from sarah@test.com with a rating of 3.9. To the right of the table is a filter panel with options for Search, Reputation Filter, Client, From Date, To Date, Status, and Email Domain. Below the table, there is a 'Summary' tab and a 'Body Analysis' tab. The 'Body Analysis' tab shows a detailed view of the report for sarah@test.com, including a circular progress indicator for the 'Overall Risk Score' (3.9 of 10.0) and a list of message subjects. A blue box highlights the 'Behold is also able' link in the message subject list. A blue arrow points from this link to the 'Behold' search filter in the filter panel on the right.

- **Reputationsprofile für Benutzer mit Vorfallshistorie:** Klassifizieren Sie Benutzer mit einer Vorfallshistorie durch das Reputations-Score.

The screenshot shows the 'Incident Reports' dashboard in Lucy, similar to the previous one. The table of reports is visible, and the 'Rating' column is highlighted with a blue box. The filter panel on the right is also visible, showing options for Search, Reputation Filter, Client, From Date, To Date, Status, and Email Domain. The 'Behold' search filter is highlighted in the filter panel, and a blue arrow points from the 'Behold is also able' link in the message subject list of the report for sarah@test.com to this filter.

- **Integration in Angriffssimulationen:** Nahtlose Integration von Berichten und Dashboards in Phishing-Simulationen: Identifizieren Sie die Benutzer, die sich in einer Phishing-Simulation vorbildlich verhalten haben.



- **Einfache Installation:** Installieren Sie das Phishing Vorfalls-Plugin für Outlook, Gmail oder Office365.

