



LIBRO BLANCO DE LUCY



¿QUÉ ES LUCY?

Pruebe, entrene e involucre a sus empleados

LUCY permite a las organizaciones asumir el papel de atacantes para descubrir las debilidades existentes tanto en la infraestructura técnica como en el conocimiento del personal y eliminarlas a través de un completo programa de aprendizaje online.



PRUEBA DE EMPLEADOS

Simulaciones de ataques (p. ej., phishing)



PRUEBA DE INFRAESTRUCTURAS

Simulación de malware y Escáner



FORMACIÓN DE EMPLEADOS

LMS integrado



MEDICIÓN DEL PROGRESO

Análisis de riesgos y aprendizaje



INTEGRACIÓN DE EMPLEADOS

Sistema de reporte (p. ej., botón de aviso de phishing)





LIBRO BLANCO DE LUCY



TABLA DE CONTENIDO

CARACTERÍSTICAS GENERALES

- Recordatorios
- Detección de respuesta
- Cliente completo de comunicación por correo
- Aleatorización del programador
- Herramientas de rendimiento
- Interfaz de administración multilingüe
- Certificado (SSL)
- Controles de acceso basado en roles
- Grupos de usuarios de múltiples capas
- Compatibilidad multi-cliente
- Plantillas de campañas
- Asistente de configuración con orientación basada en el riesgo
- Verificaciones de campaña
- Proceso de aprobación
- API de DNS

SIMULACIÓN DE ATAQUE

- Ataques de medios portátiles
- SMiShing
- Ataques de entrada de datos
- Ataques de hipervínculos
- Potente kit de herramientas para la redirección de URLs
- Ataques mixtos
- Ataques basados en archivos
- Ataques Double Barrel
- Ataques basados en Java
- Ataques basados en PDF
- Ataques de simulación de ransomware
- Kit de herramientas de validación de entrada de datos
- Biblioteca de plantillas de ataque multilingüe
- Plantillas específicas de industrias y divisiones
- Uso simultáneo de plantillas de ataque
- Variaciones de URL de ataque
- Acortador de URL
- Kit de Pentest
- Clonación de sitios Web
- Ataques basados en niveles
- Simulación de Spear Phishing
- Soporte DKIM / S / MIME para los correos electrónicos de phishing
- Escáner de correos electrónicos
- Creación de página de inicio personalizada

PRUEBE LA INFRAESTRUCTURA

- Kit de herramientas para pruebas de malware
- Prueba de filtro web y correo
- Detección de vulnerabilidades activas y pasivas de los clientes
- Prueba de spoofing

PRUEBAS TÉCNICAS

- Aprendizaje online basado en la reputación
- Portal de formación para usuarios finales
- Diploma de concienciación
- Kit de herramientas de creación de contenidos de aprendizaje online
- Entrenamiento de concienciación en formato interactivo rich media
- Biblioteca de formación
- Soporte de entrenamiento estático
- Soporte de entrenamiento fuera de Internet
- Módulos de microaprendizaje
- Personalización de video
- Formato adaptativo a móviles
- Importar y exportar video
- Pistas dinámicas de entrenamiento

INVOLUCRE A LOS EMPLEADOS

- Reportar correos electrónicos con un solo clic
- Refuerzo de comportamiento positivo
- Solicitud de inspección profunda
- Análisis automático de incidentes
- Feedback automático del incidente
- Mitigación de amenazas
- Análisis basado en reglas personalizadas
- Opciones de personalización de los plugins
- Integración de terceros
- Identificar ataques con patrones comunes
- Perfiles de reputación de usuarios de incidentes
- Integración con simulaciones de ataque
- Fácil instalación

CARACTERÍSTICAS GENERALES

- **Recordatorios:** Las plantillas de los recordatorios pueden utilizarse para reenviar automáticamente mensajes a los usuarios que no hayan hecho clic en un vínculo de ataque o en un curso de formación después de un período de tiempo personalizado.

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

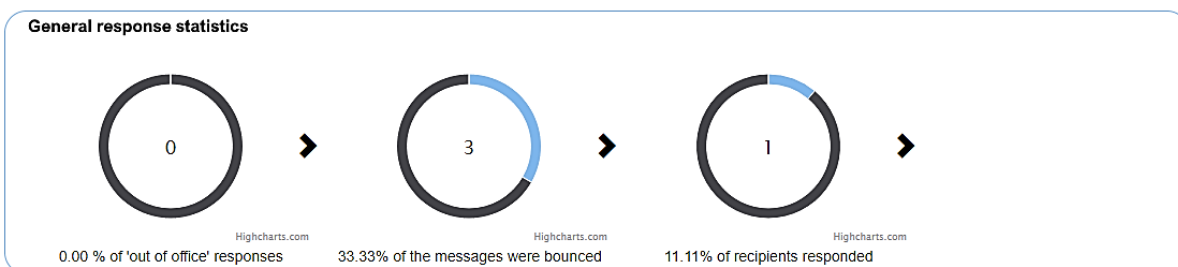
☐ Remind users who did not finish a training

3

days after training is started

Save

- **Detección de respuesta:** La detección de respuestas automáticas permite definir y analizar las respuestas automáticas de correo electrónico (p. ej., fuera de la oficina), así como los errores de entrega de correo (p. ej., usuario desconocido) dentro de la compañía.



User specific response statistics		
	No	
	test	
Name	No	
E-mail	doestextist@doesntreallyexist.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	—	

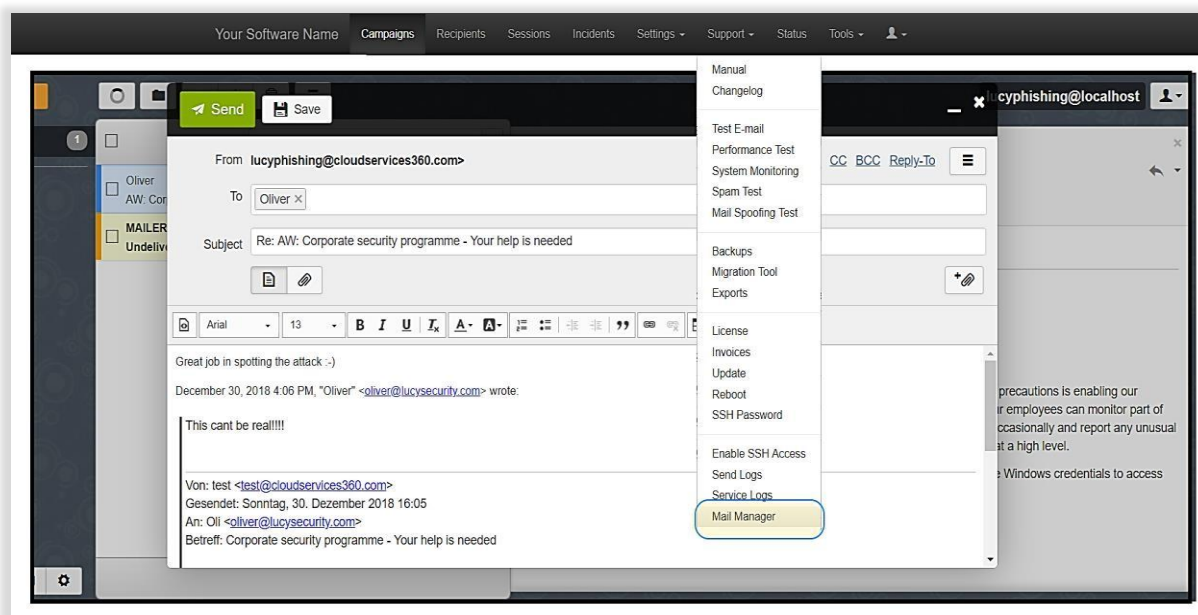
[Home](#) / Automated Response Detection

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

- **Cliente completo de comunicación por correo:** Una plataforma de mensajería integrada permite al administrador de LUCY comunicarse interactivamente con los destinatarios dentro o fuera de las campañas de LUCY. Todos los correos electrónicos se archivan y pueden ser evaluados.



- **Aleatorización del programador:** Concienciar a los empleados al azar es el factor clave para una concienciación efectiva y sostenible dentro de la organización. El envío aleatorio de muchas campañas simultáneas es uno de los mejores medios para capacitar a los empleados.

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)

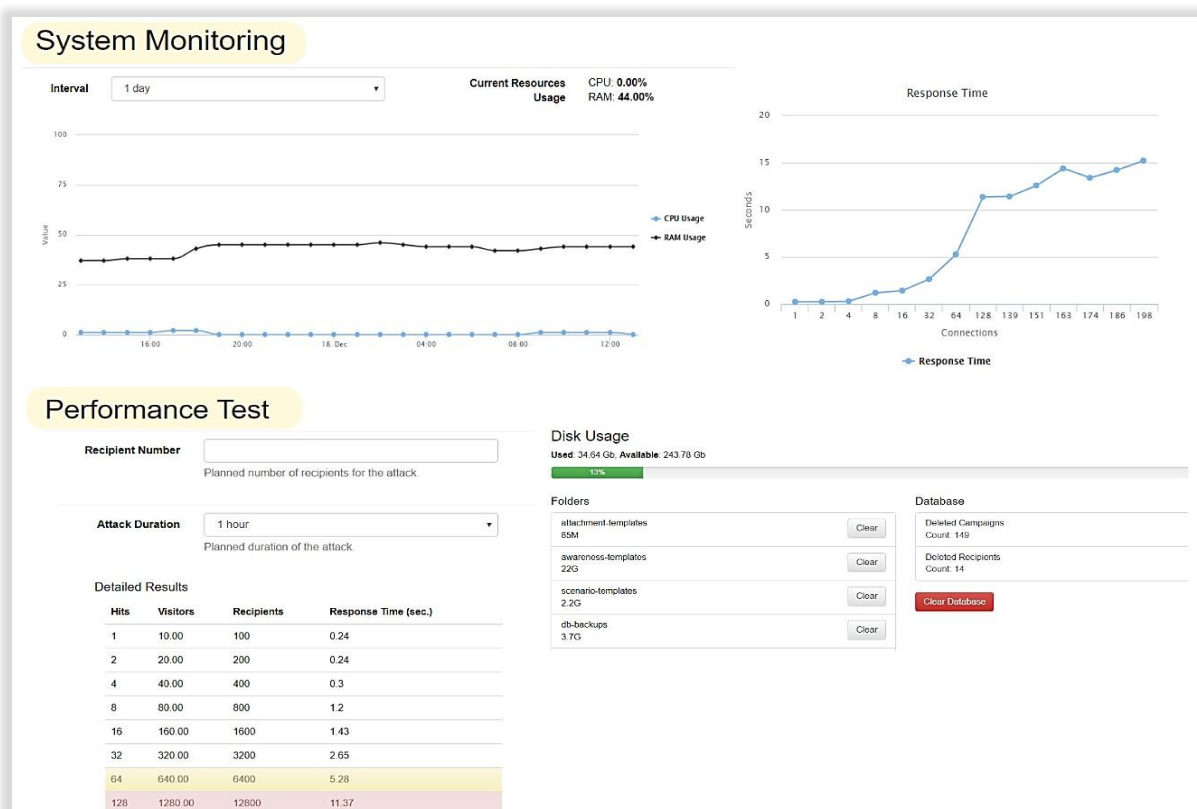
Recipient Groups

☒ LUCY Test

Save

Calculator

- **Herramientas de rendimiento:** Las rutinas inteligentes de LUCY adaptan la instalación del servidor a los recursos disponibles. El servidor de aplicaciones, el dimensionamiento del SGBD y el uso de CPU y memoria se calculan durante la instalación o durante las operaciones. Puede escalar una única instalación LUCY basada en la nube para más de 400.000 usuarios.



- **Interfaz de administración multilingüe:** La interfaz de administración de LUCY está disponible en diferentes idiomas y puede traducirse a otros idiomas si se solicita.

- Certificado (SSL):** Permite la creación automática de certificados oficiales y de confianza para el administrador, el backend y las campañas. LUCY utilizará automáticamente el dominio configurado en el sistema para generar el certificado. Si decide utilizar SSL para la campaña, puede generar un certificado personalizado o un CSR (solicitud de firma de certificado). También puede importar certificados de confianza oficiales.

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** 2
If this is not checked, visiting the scenario landing page will clear the authentication cookie and out.

SSL Provider Let's Encrypt 2

☒ **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 [Empty field] **Save**

Generate CSR or Certificate

Domain: office.cloudspace365.solutions
Country: Please select... State: City: Organization Name: Organization Unit:

Generate CSR **Generate Certificate** **Cancel**

SSL Provider Generate Or Upload 2

SSL Certificate Choose File No file chosen

SSL Key Choose File No file chosen

SSL Key Password 2

SSL Chain Choose File No file chosen 2

Save

- Controles de acceso basado en roles:** LUCY ofrece un control de acceso basado en roles (RBAC) que restringe el acceso al sistema solo a usuarios autorizados. Los permisos para realizar ciertas operaciones se asignan a roles específicos dentro de la configuración del usuario. A los miembros o al personal (u otros usuarios del sistema) se les asignan roles específicos a través de las cuales pueden adquirir los permisos informáticos necesarios para ejecutar determinadas funciones de LUCY.

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

- **Grupos de usuarios de múltiples capas:** Cargue rápidamente usuarios de forma masiva mediante un archivo CSV, LDAP o de texto. Cree diferentes grupos, organizados por departamento, división, título, etc. Actualice a los usuarios en una campaña en curso. Cree grupos de usuarios dinámicos basados en los resultados de la campaña de phishing.

Home / Users / New User

New User

[+ New User](#) [Import Users From LDAP](#) [Delete](#)

E-mail

Country Code

Phone

Two-Factor Authentication [Configure 2FA](#)

Name

Role

Client

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](#)

- **Compatibilidad multi-cliente:** Los «clientes» pueden referirse a diferentes empresas, departamentos o grupos que tengan una campaña asociada en LUCY. Estos clientes pueden utilizarse, por ejemplo, para permitir el acceso específico a una campaña o para crear análisis específicos del cliente.

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

- **Plantillas de campañas:** En caso de que desee reutilizar campañas similares, puede guardar una campaña completa con plantillas de ataque y contenido de aprendizaje online como plantilla de campaña. Esta característica le permite evitar tener que repetir configuraciones similares una y otra vez.

The screenshot shows the Lucy Campaigns interface for a campaign named 'Max1'. The campaign status is 'Not Started'. The 'Running Time' is '4 days, 4 hours'. The 'Created By' is 'N/A'. The 'Attack Overview' section shows a progress bar for 'Successful Attacks' (1 of 3) and 'Vulnerable Victims' (0 of 3). The 'Awareness' section shows a progress bar for 'Training Sent' (33.33%), 'Training Opened' (33.33%), and 'Training Score (%)' (0.00%). A 'New Campaign' modal is open, showing the 'Standard Test & Train Campaign Template' with the 'Client' set to 'Lucy Test'. The 'Setup Mode' is 'Start with Default Campaign Template' and the 'Template' is 'Max1'. The 'Save' button is highlighted. A blue arrow points from the 'Save as Template' button in the top right to the 'Save' button in the modal.

- **Asistente de configuración con orientación basada en el riesgo:** LUCY ofrece varias herramientas de configuración. Cree una campaña completa en menos de 3 minutos utilizando las plantillas de campaña predefinidas o deje que el asistente de configuración le guíe a través de la configuración. Opcionalmente, existe un modo de configuración basado en el riesgo, que da sugerencias específicas para la selección de plantillas de ataque y concienciación basadas en el tamaño de la empresa y la industria.

The screenshot shows the 'Campaign Wizard: Type' interface. It lists the steps: 1. Type, 2. Campaign, 3. Attack Template, 4. Attack Settings, 5. Training Template, 6. Training Settings, 7. Recipients, 8. Review, 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.

- **Verificaciones de campaña:** Controles preliminares antes de iniciar una campaña de LUCY: Comprobación de entrega de correo electrónico, comprobación del registro MX, comprobación de programación, comprobación de spam y otros.

Home / Campaigns / Login & Malware Simulation / Checks

Campaign Status: Not Started 



Please wait, the system is checking your campaign settings.



Check	Status
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.

- **Proceso de aprobación:** Puede enviarse una campaña dada a un supervisor de LUCY para su aprobación.

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 

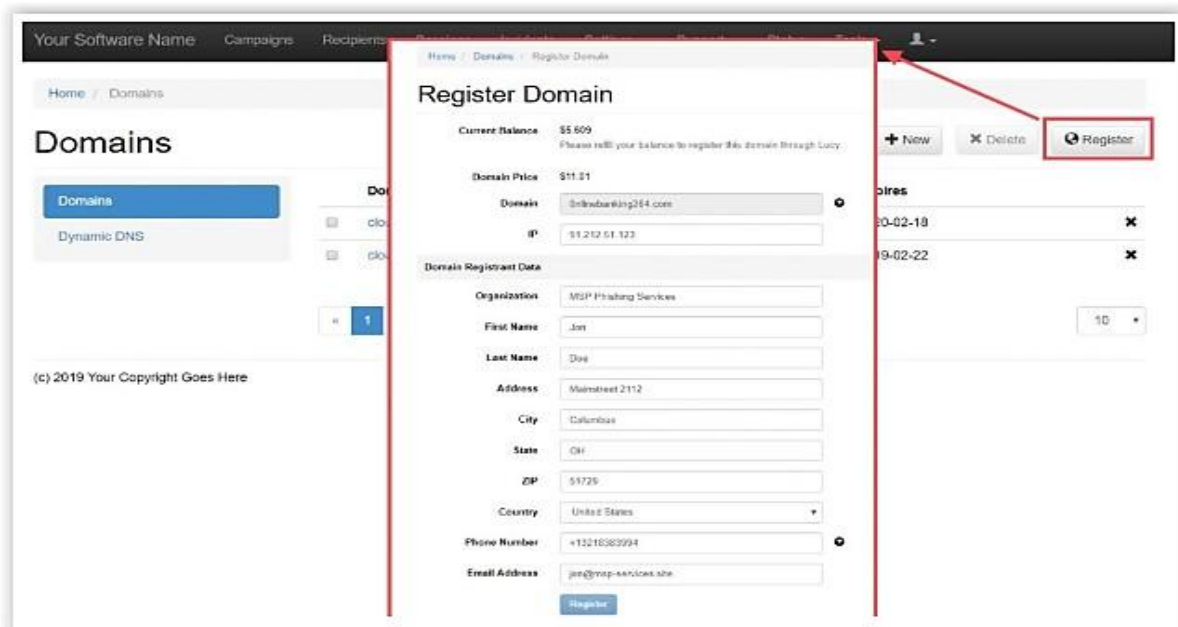
Severity: ☒ Minor Recommendations ☐ Serious Recommendations ☐ Heavy Recommendations

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"



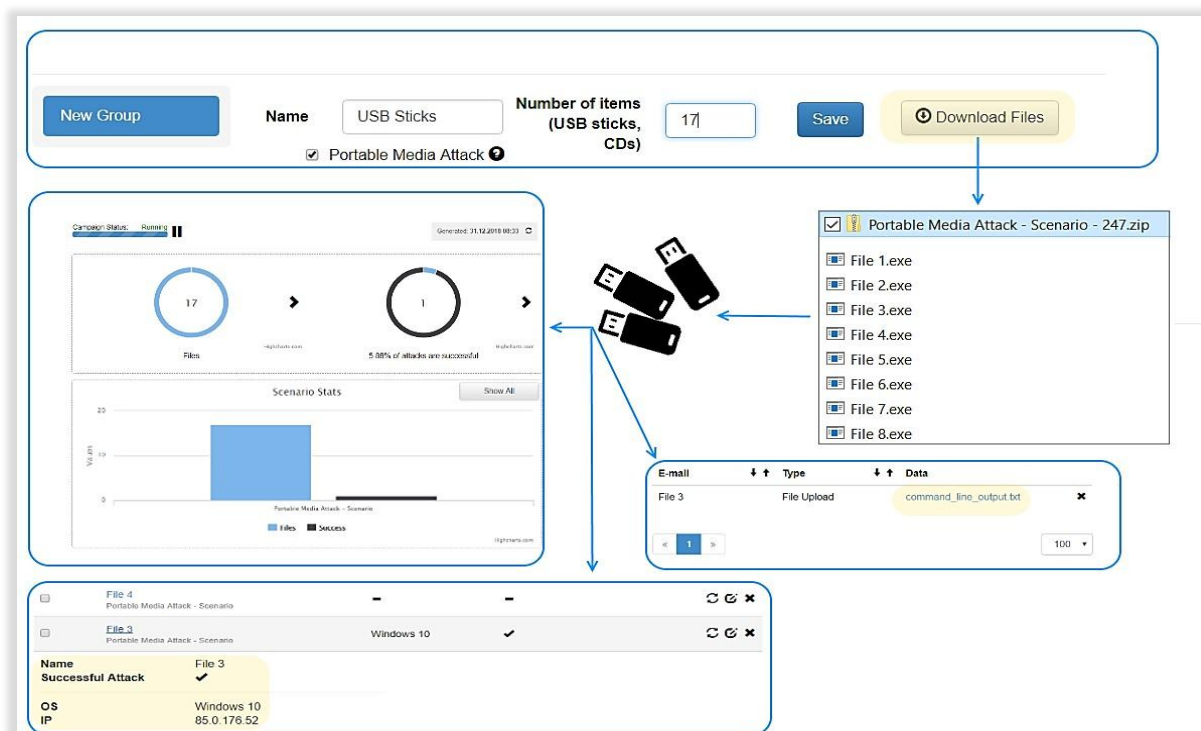
Name	Role	All Campaigns Access
Limited User	User	✓
View	View	—
Supervisor	Supervisor	✓

- API de DNS:** La API de DNS permite al administrador crear cualquier dominio en LUCY en cuestión de segundos. Dado que los atacantes suelen utilizar dominios con palabras similares de los clientes (lo que se conoce como typosquatting), este riesgo también puede representarse en LUCY. Si el dominio original del cliente es, por ejemplo, "onlinebanking.com", el asistente del DNS podría usarse para reservar un dominio como "Onlinebanking.com", "onl1nebanking.com" o "onlinebanking.services", y asignarlo posteriormente a una campaña. LUCY crea automáticamente las entradas DNS correspondientes (MX, SPF, Protección Whois, etc.) para la IP donde está instalado LUCY. Por supuesto, el administrador también puede utilizar los propios dominios de su proveedor en LUCY.

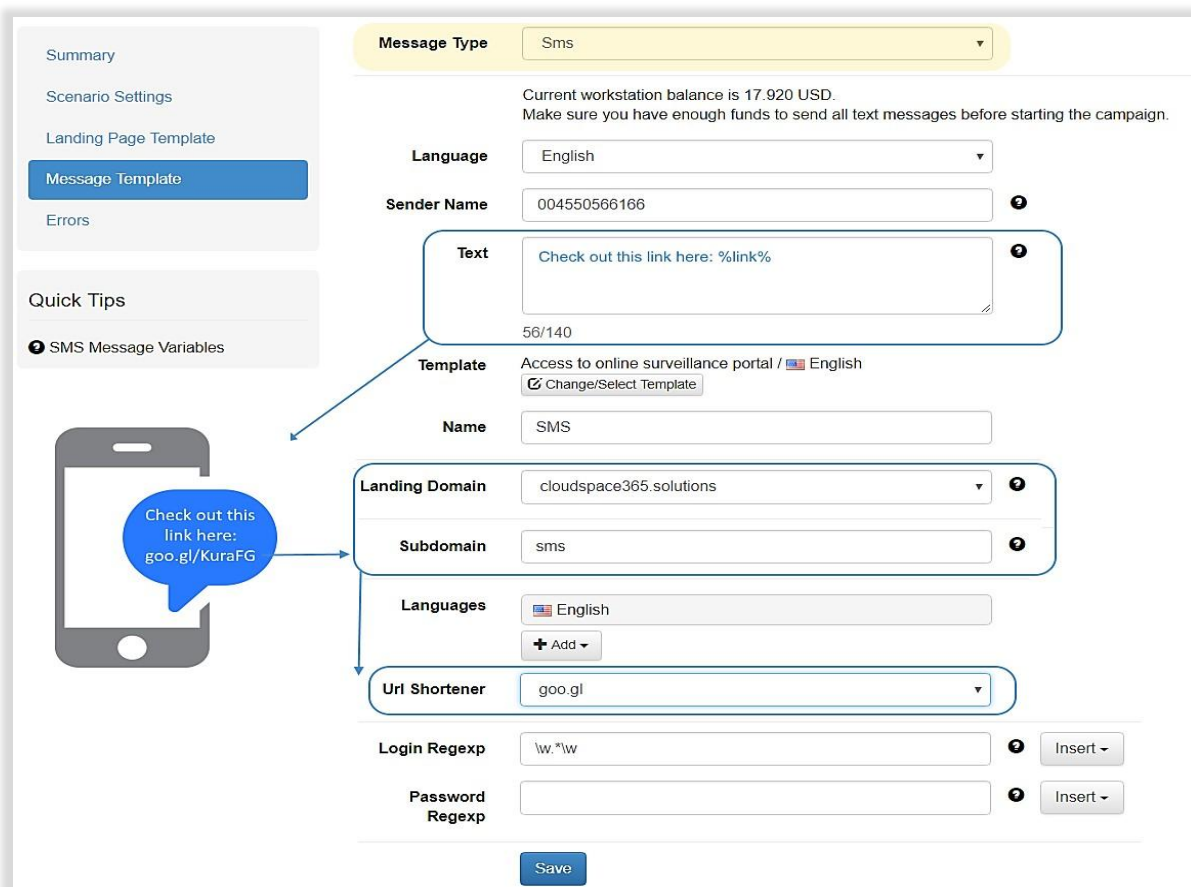


SIMULACIÓN DE ATAQUE

- Ataques de medios portátiles:** Los hackers pueden utilizar unidades de medios portátiles para acceder a información confidencial almacenada en un ordenador o en una red. LUCY ofrece la opción de realizar ataques de medios portátiles en los que se puede guardar una plantilla de archivo (p. ej., ejecutable, archivo, documento de oficina con macros, etc.) en un dispositivo multimedia portátil como USB, tarjeta SD o CD. La activación (ejecución) de estos archivos individuales puede ser rastreada en LUCY.

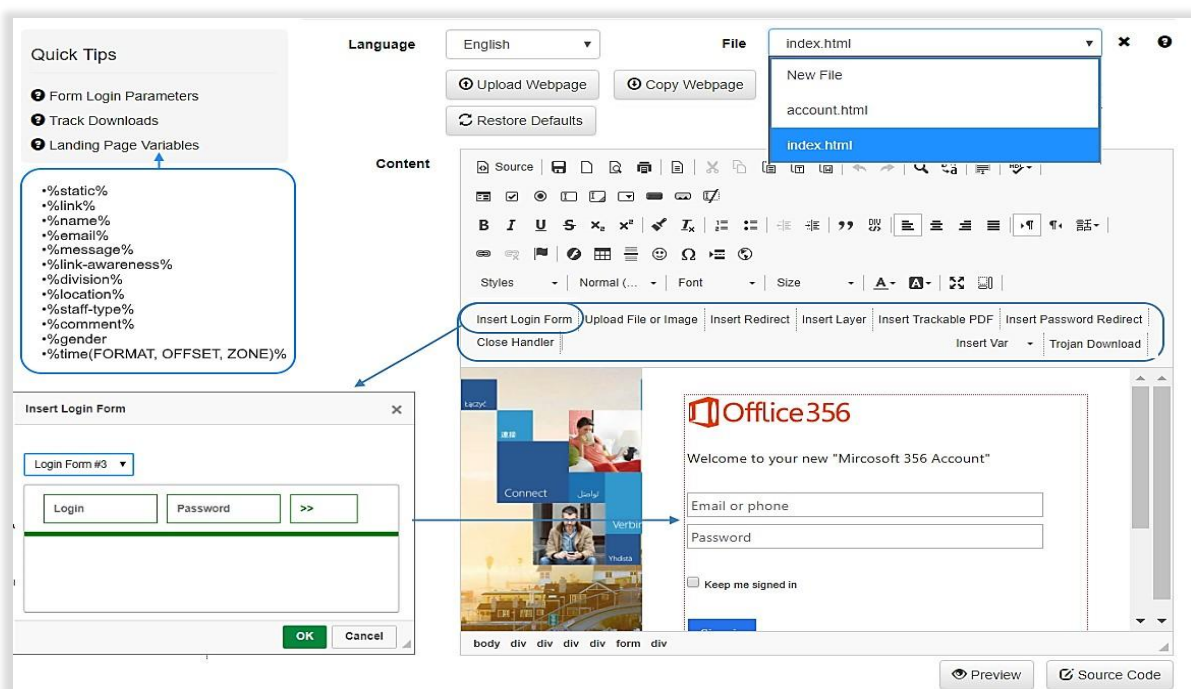


- SMiShing:** SMiShing es, en cierto sentido, «phishing por SMS». Cuando los delincuentes cibernéticos «hacen phishing», envían correos electrónicos fraudulentos que intentan engañar al destinatario para que abra un archivo adjunto cargado de malware o haga clic en un enlace malicioso. El SMiShing simplemente utiliza mensajes de texto en lugar de correo electrónico.



The screenshot shows the 'Message Template' configuration page in the Lucy web editor. On the left, a sidebar contains 'Summary', 'Scenario Settings', 'Landing Page Template', 'Message Template' (selected), and 'Errors'. Below this is a 'Quick Tips' section with a link to 'SMS Message Variables'. The main area is titled 'Message Type' and 'Sms'. It includes a warning about workstation balance, a 'Language' dropdown set to 'English', a 'Sender Name' field with '004550566166', and a 'Text' field with 'Check out this link here: %link%'. Below these are fields for 'Template' (Access to online surveillance portal / English), 'Name' (SMS), 'Landing Domain' (cloudspace365.solutions), 'Subdomain' (sms), 'Languages' (English), and 'Url Shortener' (goo.gl). At the bottom, there are 'Login Regexp' and 'Password Regexp' fields, each with an 'Insert' button, and a 'Save' button at the very bottom.

- Ataques de entrada de datos:** Los ataques de entradas de datos pueden incluir una o más páginas web que interceptan la entrada de información sensible. Las páginas web disponibles se pueden personalizar fácilmente con un editor web de LUCY. Las herramientas de edición adicionales le permiten configurar rápidamente funciones, como formularios de inicio de sesión, áreas de descarga, etc., sin conocimientos de HTML.



The screenshot shows the 'Content' editor in the Lucy web editor. On the left, a sidebar contains 'Quick Tips' with links to 'Form Login Parameters', 'Track Downloads', and 'Landing Page Variables'. Below this is a list of variables: %static%, %link%, %name%, %email%, %message%, %link-awareness%, %division%, %location%, %staff-type%, %comment%, %gender%, and %time(FORMAT, OFFSET, ZONE)%. The main area shows a 'File' dropdown set to 'index.html' and buttons for 'Upload Webpage', 'Copy Webpage', and 'Restore Defaults'. Below these is a 'Content' toolbar with various icons. A 'Insert Login Form' button is highlighted, and a modal window titled 'Insert Login Form' is open, showing a 'Login Form #3' with 'Login', 'Password', and '>>' buttons. The main content area displays a preview of a login form with the 'Office365' logo and fields for 'Email or phone' and 'Password', with a 'Keep me signed in' checkbox. At the bottom, there are 'Preview' and 'Source Code' buttons.

- **Ataques de hipervínculos:** Una campaña basada en hipervínculos enviará a los usuarios un correo electrónico que contiene una URL de seguimiento aleatoria.

- **Potente kit de herramientas para la redirección de URLs:** Las flexibles funciones de redireccionamiento de LUCY permiten al usuario ser guiado en el momento adecuado a las áreas deseadas de simulación de ataques o entrenamiento. Por ejemplo, después de introducir los 3 primeros caracteres de una contraseña en una simulación de phishing, el usuario puede ser redirigido a una página de formación especial sobre protección de contraseñas.

- **Ataques mixtos:** Los ataques mixtos permiten una combinación de múltiples tipos de escenarios (basado en archivos, entrada de datos, etc.) en la misma campaña.



Malware Simulation

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)

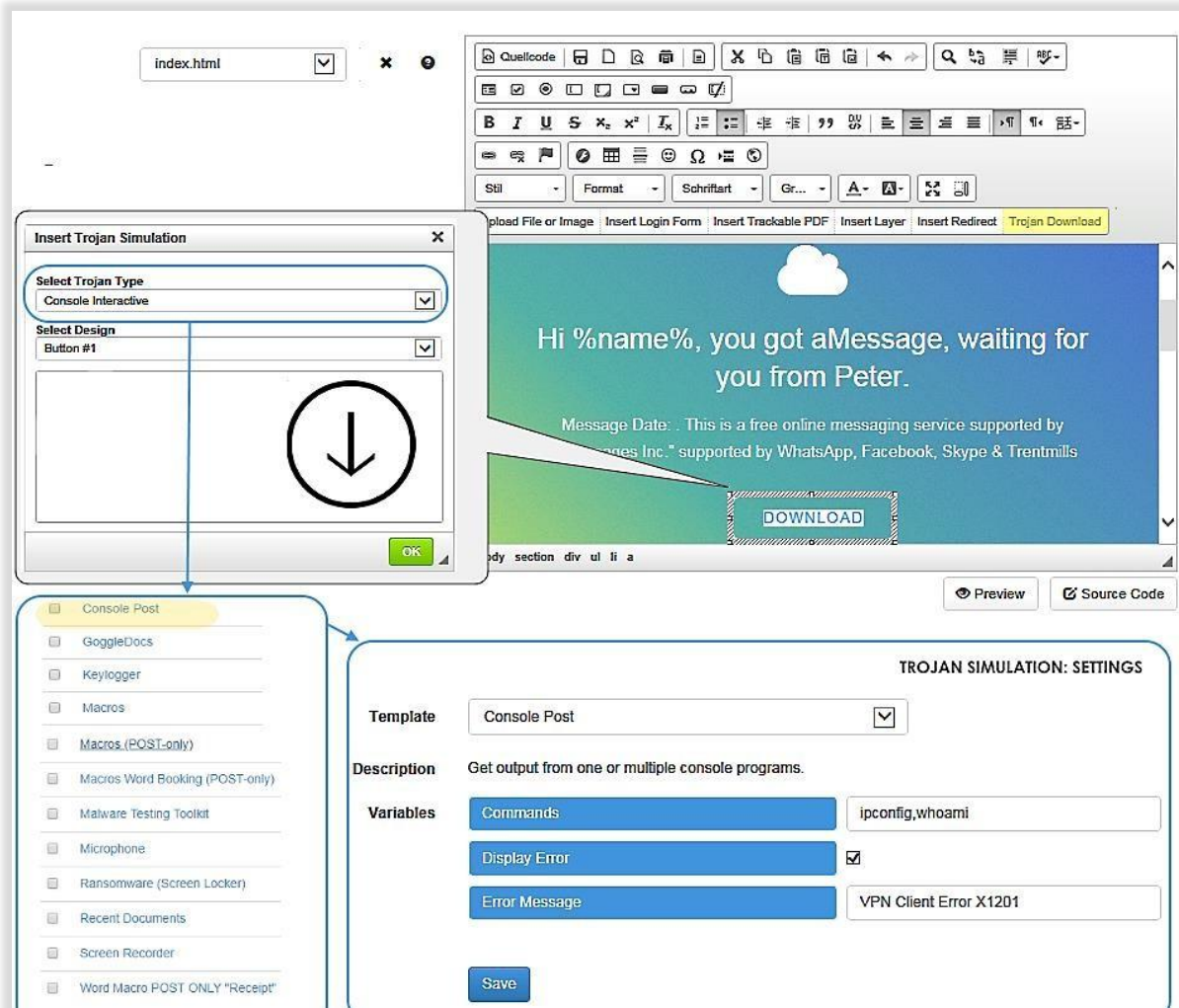
1

Text Message

Installation Error - please try again later

Save

- **Ataques basados en archivos:** Los ataques basados en archivos permiten al administrador de LUCY integrar diferentes tipos de archivos (documentos de oficina con macros, PDF, ejecutables, MP3, etc.) en adjuntos de correo o sitios web generados en LUCY y medir su tasa de descarga o ejecución.



The screenshot displays the LUCY web application interface. At the top, there is a file manager showing 'index.html'. Below it, a rich text editor is visible with a toolbar and a preview of a message that says 'Hi %name%, you got aMessage, waiting for you from Peter.' and includes a 'DOWNLOAD' button. A dialog box titled 'Insert Trojan Simulation' is open, showing 'Select Trojan Type' as 'Console Interactive' and 'Select Design' as 'Button #1'. Below the dialog, a list of templates is shown, 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"'. The 'Console Post' template is selected, and its settings are shown in the 'TROJAN SIMULATION: SETTINGS' panel. The settings include a 'Template' dropdown set to 'Console Post', a 'Description' field with the text 'Get output from one or multiple console programs.', and three 'Variables' fields: 'Commands' with the value 'ipconfig,whoami', 'Display Error' with a checked checkbox, and 'Error Message' with the value 'VPN Client Error X1201'. A 'Save' button is at the bottom of the settings panel.

- **Ataques Double Barrel:** Esta función permite enviar varios correos electrónicos de phishing en cada campaña, con un primer correo electrónico benigno (el cebo) que no contiene nada malicioso y no exige una respuesta del destinatario.

Message Type Email

Language English

Sender Name Security

Sender E-mail Security@example.com

☐ Random E-mail

Subject Corporate security program 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.*\w

Password Regexp

Save

- **Ataques basados en Java:** Los ataques basados en Java permiten al administrador de LUCY integrar un applet de confianza dentro de las plantillas de ataque basadas en archivos o mixtas proporcionadas en LUCY y medir su ejecución por el usuario.

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

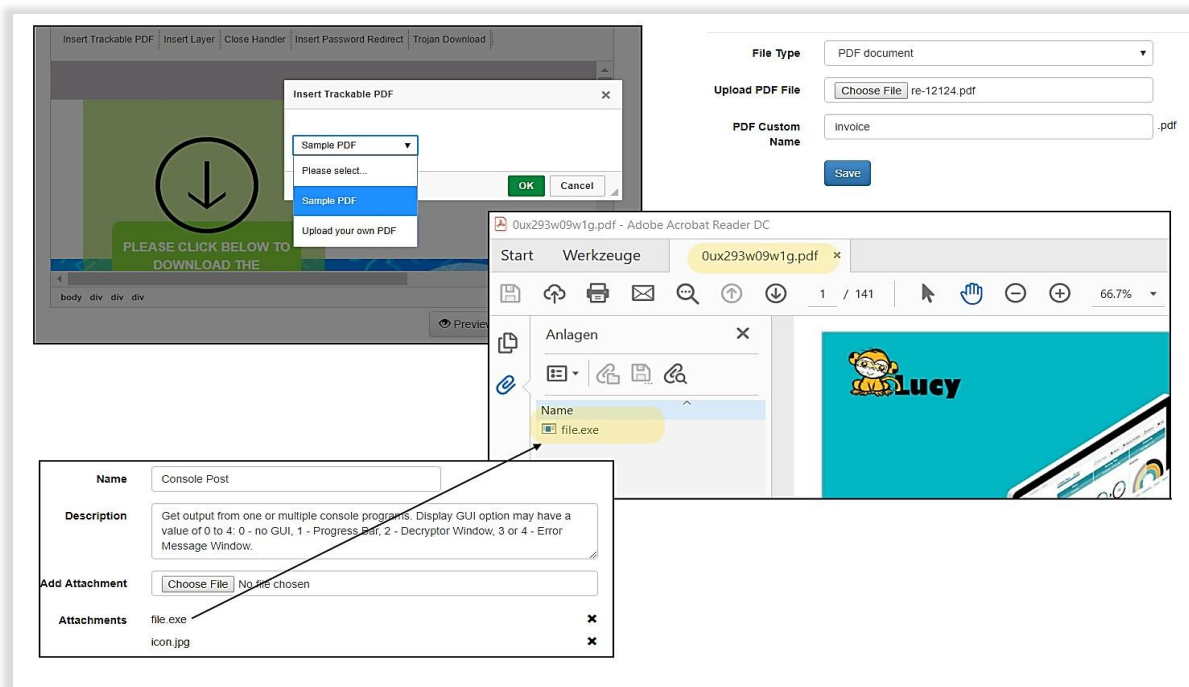
Description Capture screenshots or video from the desktop and shoot photos or videos using a webcam. Display GUI option may have a value of 0 to 4: 0 - no GUI, 1 - Progress Bar, 2 - Decryptor Window, 3 or 4 - Error Message Window.

Variables

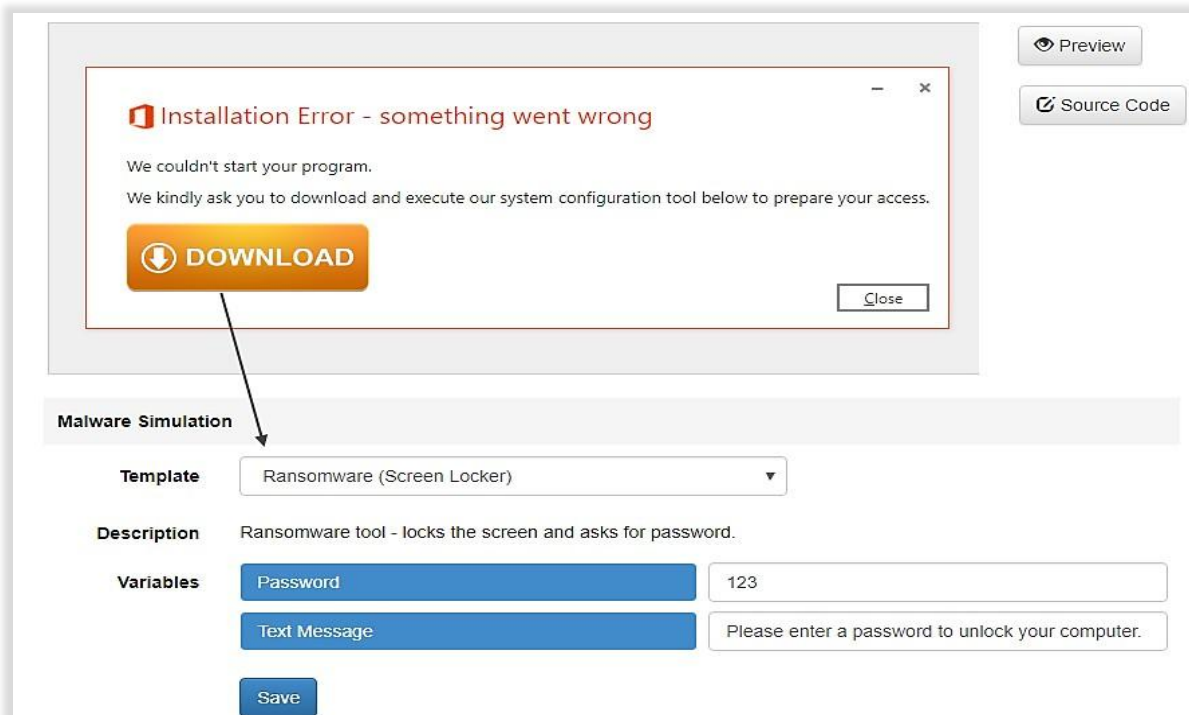
Desktop Video	☐
Capture Webcam	☐
Webcam Video	☐
Video Length (seconds)	0
Number of Snapshots	1
Interval Between Snapshots	5
Display GUI (0-4)	1
Text Message	VPN Client Error X1201

Save

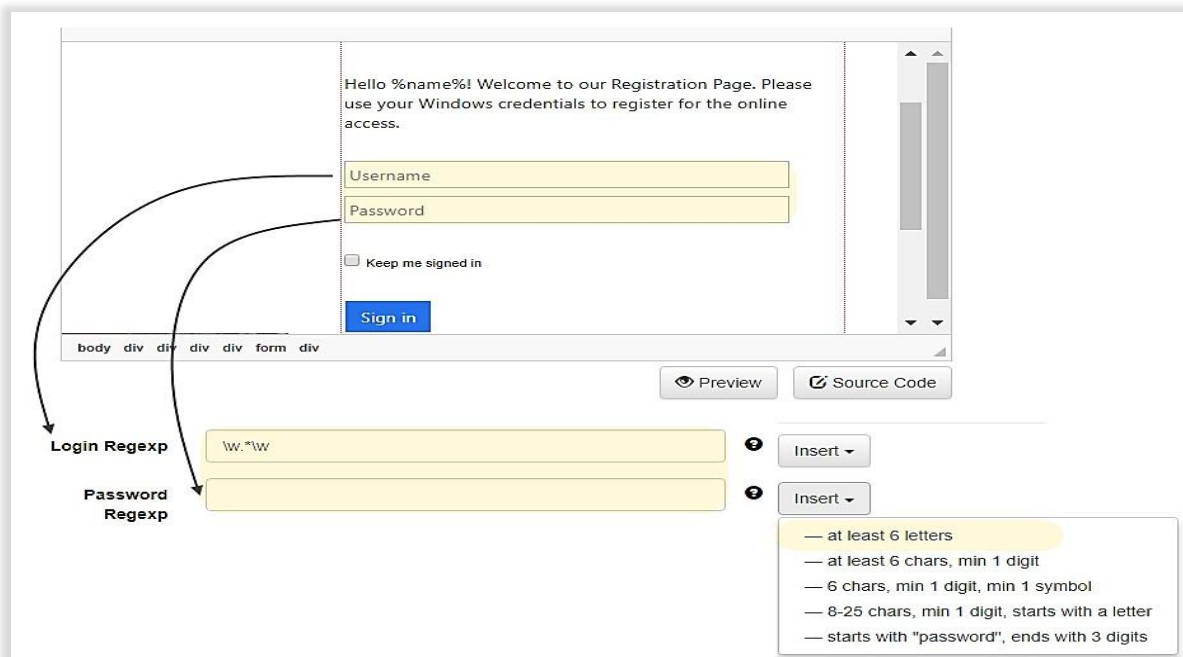
- **Ataques basados en PDF:** Los ataques de phishing basados en PDF pueden simularse con este módulo. LUCY permite «ocultar» archivos ejecutables en archivos adjuntos PDF y medir su ejecución. Además, también se pueden generar enlaces dinámicos de phishing dentro de los PDF.



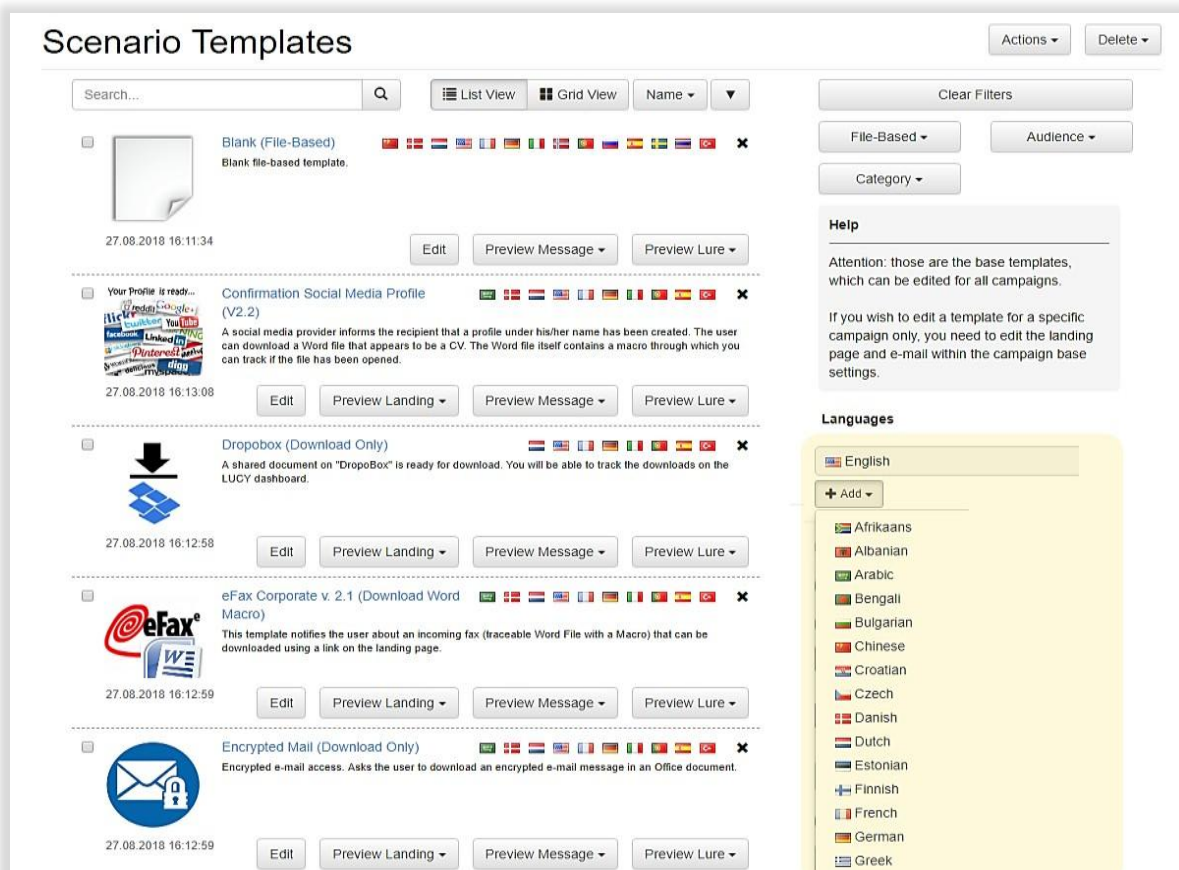
- **Ataques de simulación de ransomware:** LUCY tiene dos simulaciones de ransomware diferentes, una de las cuales prueba al personal y la otra, la infraestructura.



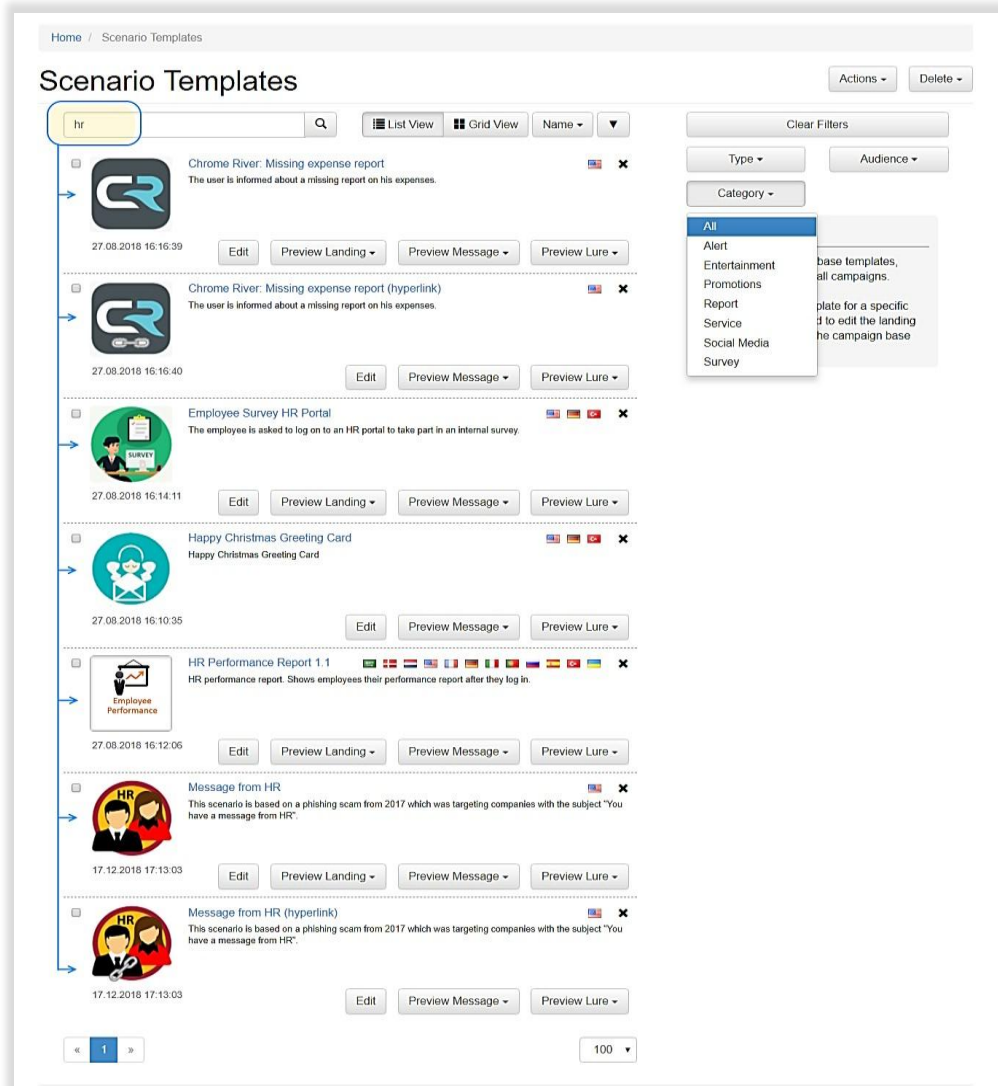
- Kit de herramientas de validación de entrada de datos:** En las simulaciones de phishing, se deben evitar los falsos positivos en los campos de inicio de sesión (p. ej., el registro con sintaxis no válida). Las directrices de la empresa también pueden prohibir la transmisión de datos sensibles como las contraseñas. Para ello, LUCY ofrece un motor de filtrado de entrada flexible que ofrece una solución adecuada para cada necesidad.



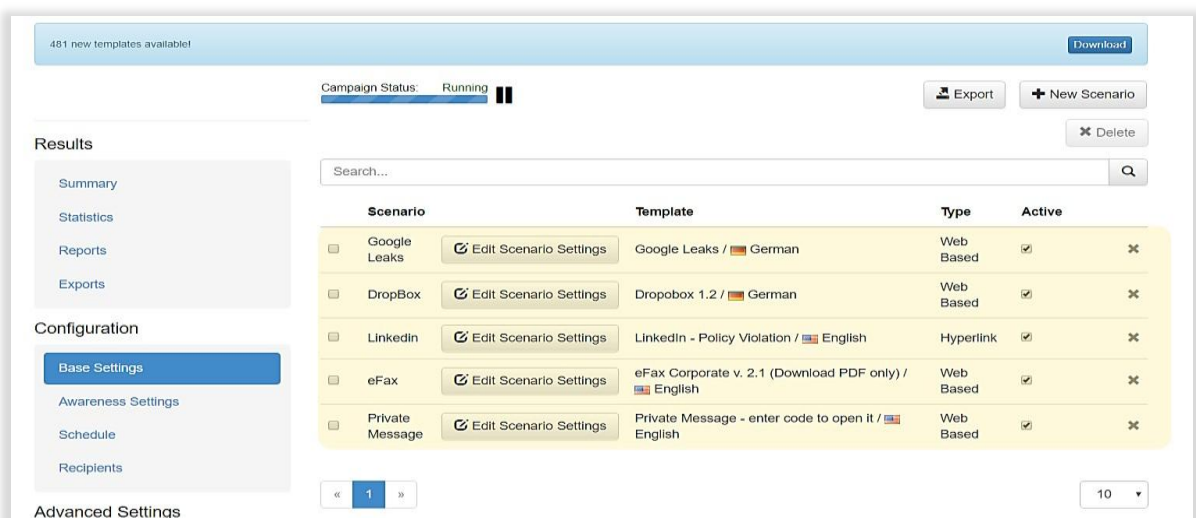
- Biblioteca de plantillas de ataque multilingüe:** LUCY viene con cientos de plantillas de ataque predefinidas en más de 30 idiomas en las categorías de entrada de datos (plantillas con un sitio web), basadas en archivos (correos electrónicos o sitios web con descarga de archivos), hipervínculos (correos electrónicos con un enlace), mixtas (combinación de entrada de datos y descarga) y medios portátiles.



- **Plantillas específicas de industrias y divisiones:** Las plantillas de ataque están disponibles para industrias o divisiones específicas.



- **Uso simultáneo de plantillas de ataque:** LUCY le ofrece la opción de utilizar varias plantillas de ataque simulado en una campaña. Mezcle los diferentes tipos (hipervínculos, basados en archivos, etc.) con diferentes temas de ataque para lograr la mayor cobertura de riesgos posible y una mejor comprensión de las vulnerabilidades de los empleados. En combinación con nuestro aleatorizador de programación, se pueden ejecutar patrones de ataque complejos durante un período de tiempo más largo.



- **Variaciones de URL de ataque:** Tome el control de las URL generadas para identificar a los destinatarios. Utilice cadenas de URL cortas (<5 caracteres) o largas automatizadas o establezca URLs individuales para cada usuario. La creación manual de URL le permite formar enlaces que un usuario puede recordar fácilmente. En los entornos en los que los clics de los enlaces están deshabilitados en los correos electrónicos, esto es una necesidad.

Home / Recipients / LINK TEST / oliver@lucysecurity.com

LINK TEST

Recipients
Edit Group Name
Import
Scan

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
OLI Special
Save

So, 30.12.2018 11:29

Test User <test@example.com>
Affordable car leasing for our employees

An Oli

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): <http://www.example.com/marketing-usa-1/>

<https://www.CorporateCar-Leasing365.com>

Best regards

- **Acortador de URL:** Los acortadores de URL son un servicio de Internet relativamente nuevo. Como muchos servicios sociales en línea imponen limitaciones de caracteres (p. ej., Twitter), estas URL son muy prácticas. Sin embargo, los delincuentes cibernéticos pueden utilizar los acortadores de URL para ocultar el destino real de un enlace, como sitios web infectados o de phishing. Por esta razón, LUCY ofrece la posibilidad de integrar diferentes servicios de acortadores dentro de una campaña de phishing o SMiShing.

Landing Domain cloudspace365.solutions

Subdomain sms

Url Shortener N/A

Sender Name 004550776160

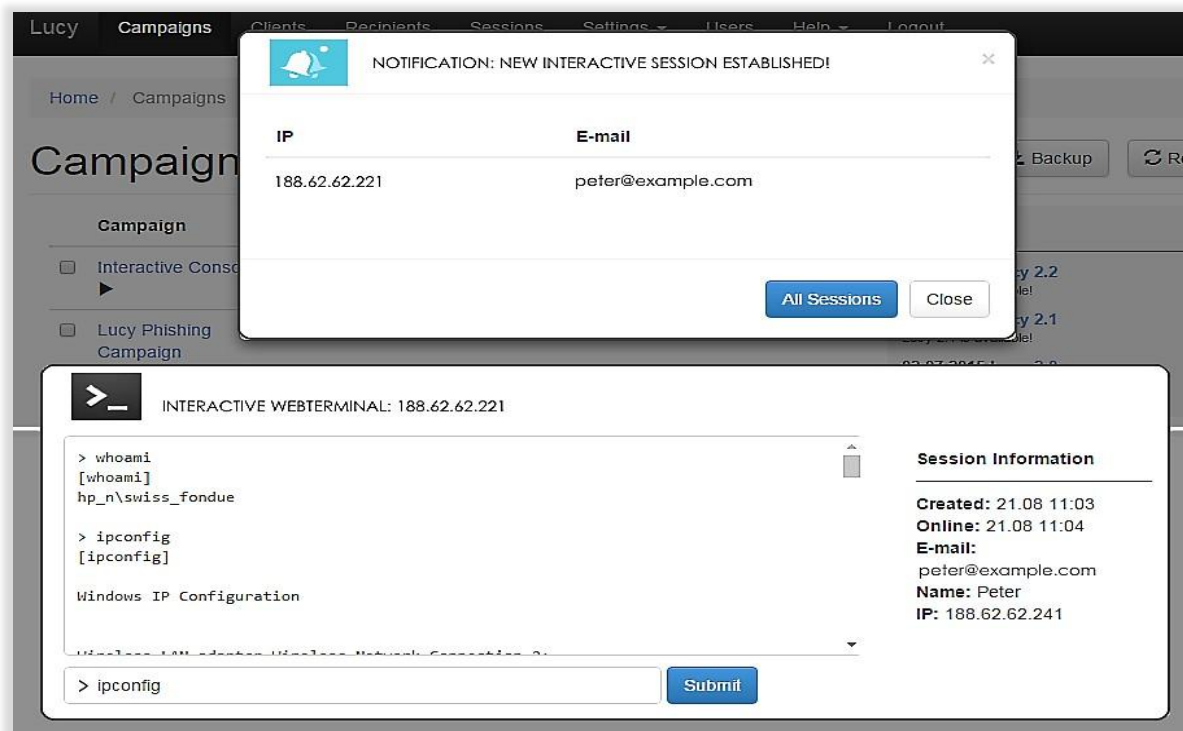
Text Check out this here %link%

26/140

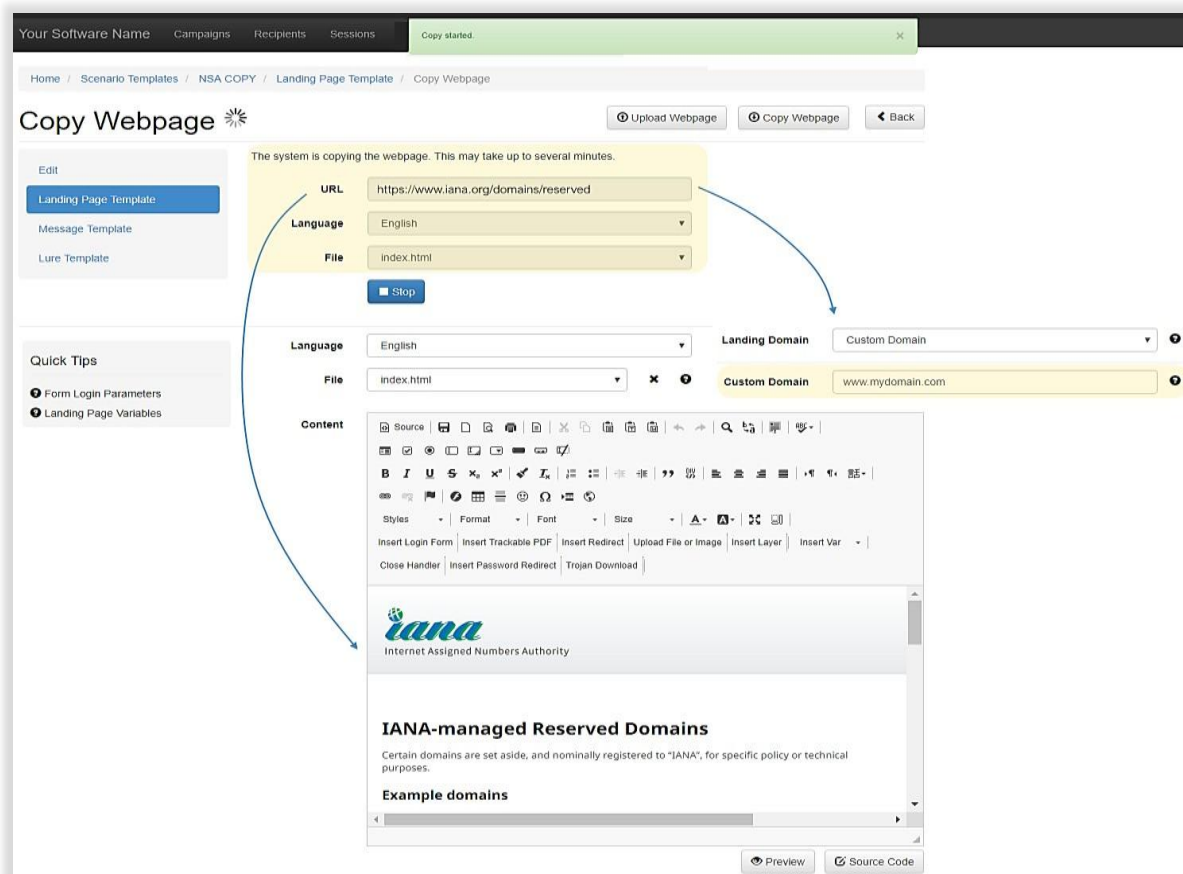
Save

Check out this link here: goo.gl/KuraFG

- **Kit de Pentest:** El kit de Pentest es un submódulo del kit de simulación de malware y se llama «Sesiones Interactivas». Le permite comunicarse interactivamente con un PC cliente que se encuentra detrás de cortafuegos usando conexiones http/s inversas.



- **Clonación de sitios Web:** Cree rápidamente páginas de destino altamente profesionales para sus campañas. Clone sitios web existentes y añada capas adicionales con campos de entrada de datos, archivos para descargar y mucho más.



- **Ataques basados en niveles:** El entrenamiento de phishing para empleados se basa en niveles y sirve para medir el riesgo de hackeo con ingeniería social. El análisis científico también debería identificar los factores de riesgo más importantes para que el contenido formativo individual pueda ofrecerse automáticamente.

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...

Antivirus/Firewall Protection Interval: off

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

View Options

- ☐ Pinned

Save

- **Simulación de Spear Phishing:** La personalización de Spear Phish funciona con variables dinámicas (género, hora, nombre, correo electrónico, enlaces, mensajes, división, país, etc.) que se pueden utilizar en plantillas de destino y de mensajes.

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:i:s", "6000")%. The document is only available for %division%, %location%, %staff-type%.

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

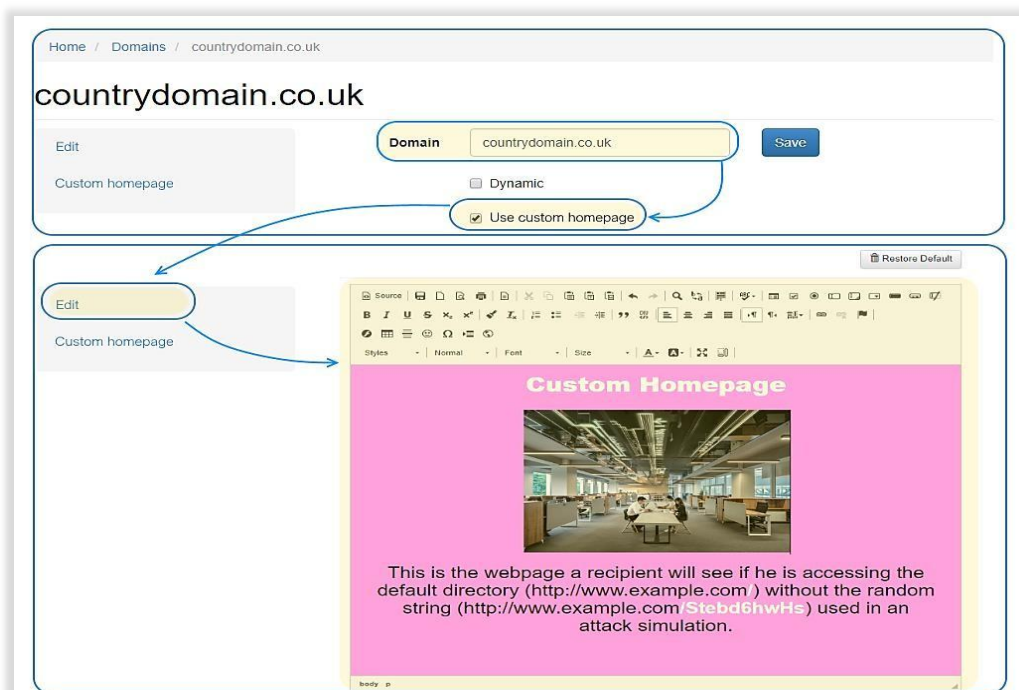
Available Variables:

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

- **Soporte DKIM / S / MIME para los correos electrónicos de phishing:** Firmas digitales para correos electrónicos: Envíe correos de simulación de phishing firmados (s/mime). Utilice DKIM para obtener una mejor puntuación de remitente.

- **Escáner de correos electrónicos:** ¿Tiene curiosidad por saber qué direcciones de correo electrónico de su organización se pueden encontrar en Internet? Utilice el escáner de correos de LUCY y descubra lo que un hacker ya sabe sobre su empresa.

- **Creación de página de inicio personalizada:** Los destinatarios con una mejor comprensión técnica podrían utilizar su navegador para llamar al dominio o dirección IP asociados con el enlace del phishing generado de forma aleatoria. Para evitar que aparezcan mensajes de error o que el usuario final llegue al área de inicio de sesión de la consola de administración, puede crear «páginas de inicio» genéricas en LUCY para los dominios utilizados en la simulación de phishing.



PRUEBE LA INFRAESTRUCTURA

- **Kit de herramientas para pruebas de malware:** El kit de herramientas de simulación de malware es una suite de simulación de malware avanzada capaz de emular varias amenazas. Permite a un auditor acceder a un conjunto avanzado de funciones equivalentes a muchas de las herramientas empleadas por los delincuentes cibernéticos. La herramienta, por lo tanto, permite al administrador de LUCY realizar comprobaciones de seguridad sin involucrar a los empleados ajenos al departamento informático.

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 admin
- ☐ Firewall
- ☐ Antivirus
- ☐ Virus downloading
- ☐ Hosts

LUCY MALWARE TESTING SUITE

General Settings

Test started: 10:16:40 21.08.2015

Test ended: Not yet

Overall Progress:

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 TEST RESULTS

Report Created: 20.07.2015 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 & no access to	View Details	Executed command: whoami (full output)	Success	Low Risk	View Details
2	Read recent document	View Details	C:\Users\jdoe\Desktop\STH-Example-Communication.docx	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 last 5 symbols of subject are displayed for privacy reasons	Success	Low Risk	View Details
4	Screenshot	View Details		Success	Low Risk	View Details
5	Webcam access test	View Details		Success	Low Risk	View Details
6	Access to the internet via IE	View Details	Received page URL: http://www.google.com (full output)	Success	Low Risk	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	Medium Risk	View Details
8	Access to the internet via a https	View Details	Error occurred: Invalid URI: The hostname could not be parsed. (full output)	Fail	Medium Risk	View Details
9	Access to the internet via a https	View Details	Error occurred: Invalid URI: The hostname could not be parsed. (full output)	Fail	Medium Risk	View Details

LHFC

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

Place: Temp folder

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

☐ Use real data ☐ Delete data

☐ Use dummy data

Extensions (separated by commas): doc, ppt, xls, pdf, txt

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

Crawl time, minutes: [120]

Amount of file operations: [10000]

- **Prueba de filtro web y correo:** Esta funcionalidad proporciona la respuesta a una de las preguntas más importantes a la hora de proteger el tráfico de Internet y de correo: ¿Qué tipos de archivos se pueden descargar de la web y qué archivos adjuntos de correo electrónico se filtran o no?

[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

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

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

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

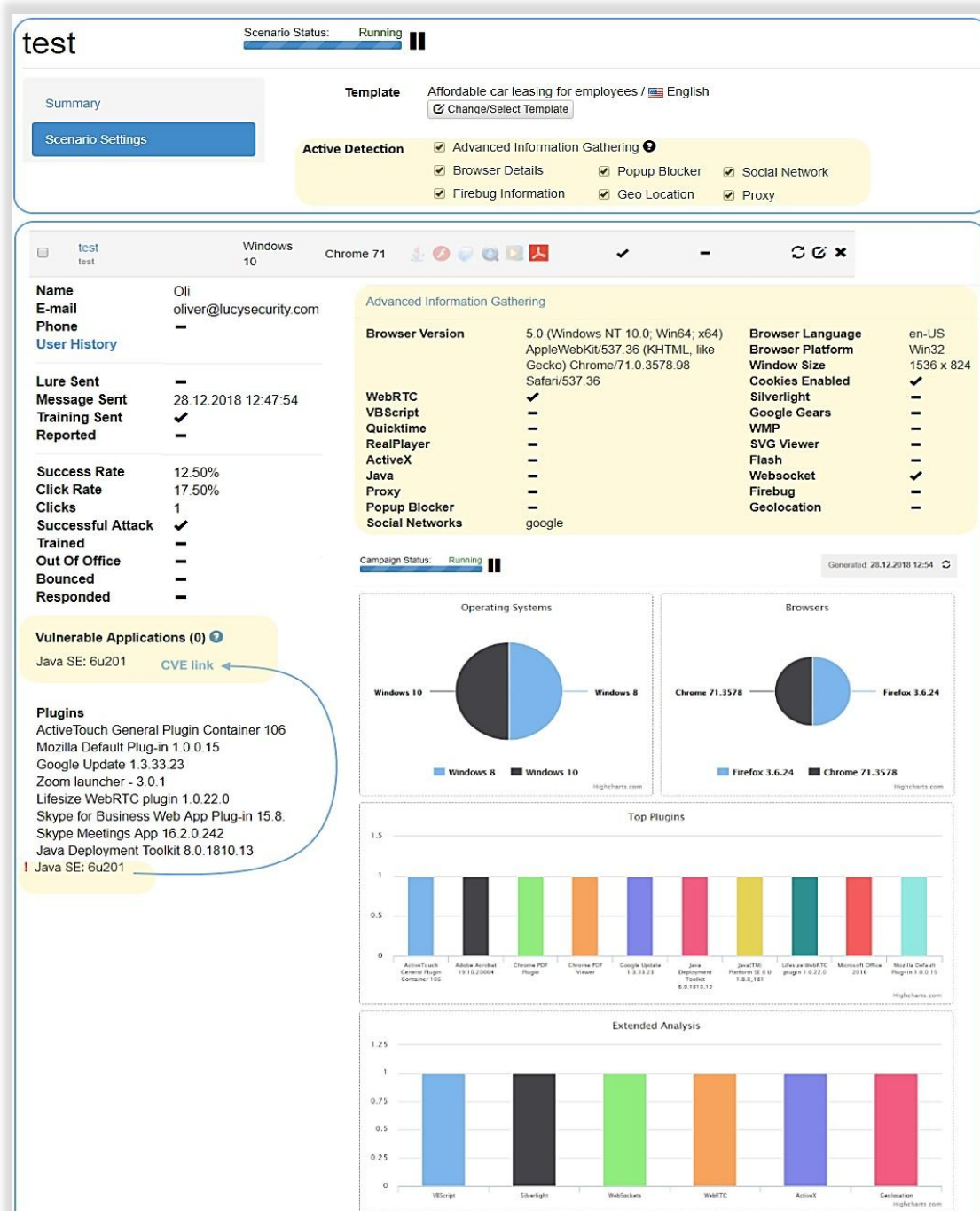
Mime Type

Class

Dangerous File Types in archives

File

- Detección de vulnerabilidades activas y pasivas de los clientes:** Esta función permite realizar pruebas locales del navegador del cliente y detectar posibles vulnerabilidades basándose en bibliotecas JavaScript personalizadas y en los datos del agente de usuario del navegador. Los plugins descubiertos se pueden comparar automáticamente con las bases de datos de vulnerabilidades (CVE) para identificar dispositivos vulnerables.



- **Prueba de spoofing:** Pruebe su propia infraestructura para detectar vulnerabilidades de spoofing de correo.

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

PRUEBAS TÉCNICAS

- **Aprendizaje online basado en la reputación:** Entrene a sus empleados de acuerdo a sus habilidades requeridas. Mida las habilidades de los empleados y permita una competición amistosa entre colegas (ludificación). Basándose en los perfiles de reputación de cada usuario final, el sistema puede proporcionarles automáticamente múltiples sesiones formativas. Los perfiles de reputación se basan, entre otros factores, en el comportamiento del usuario en las simulaciones de phishing. Esto asegura que los usuarios reincidentes reciban un contenido formativo diferente al de los que hacen clic en una simulación de ataque por primera vez.

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

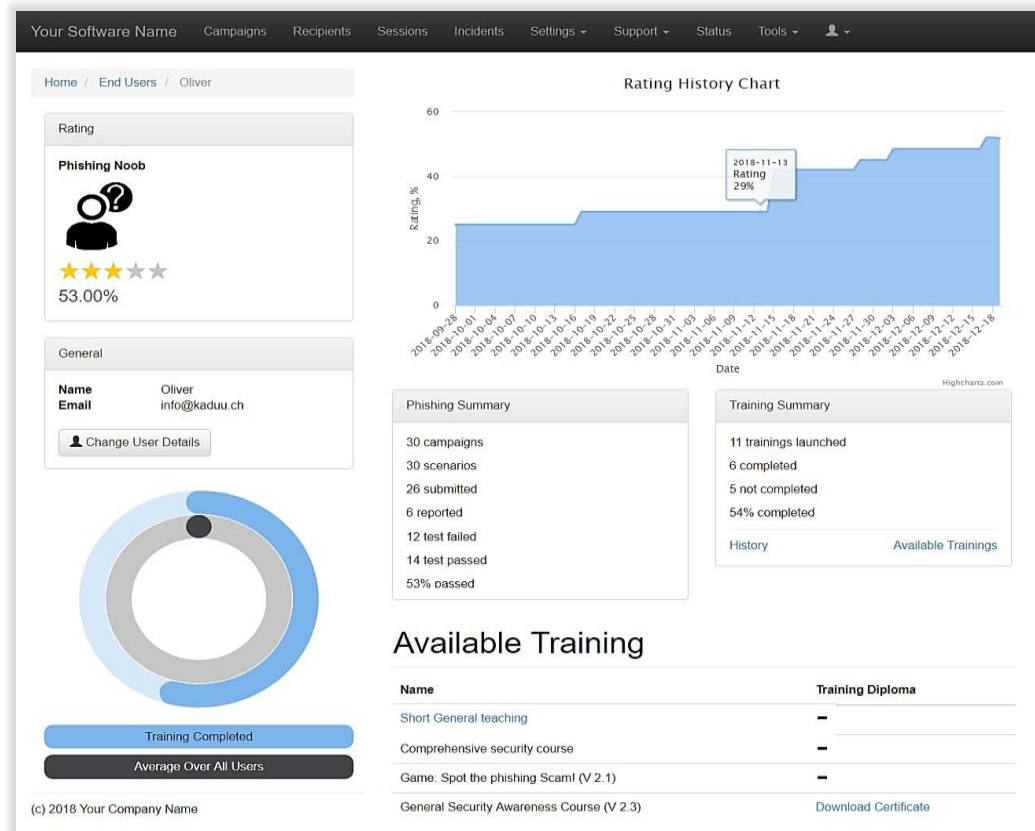
Configuration
Base Settings
Awareness Settings

Export
New Awareness

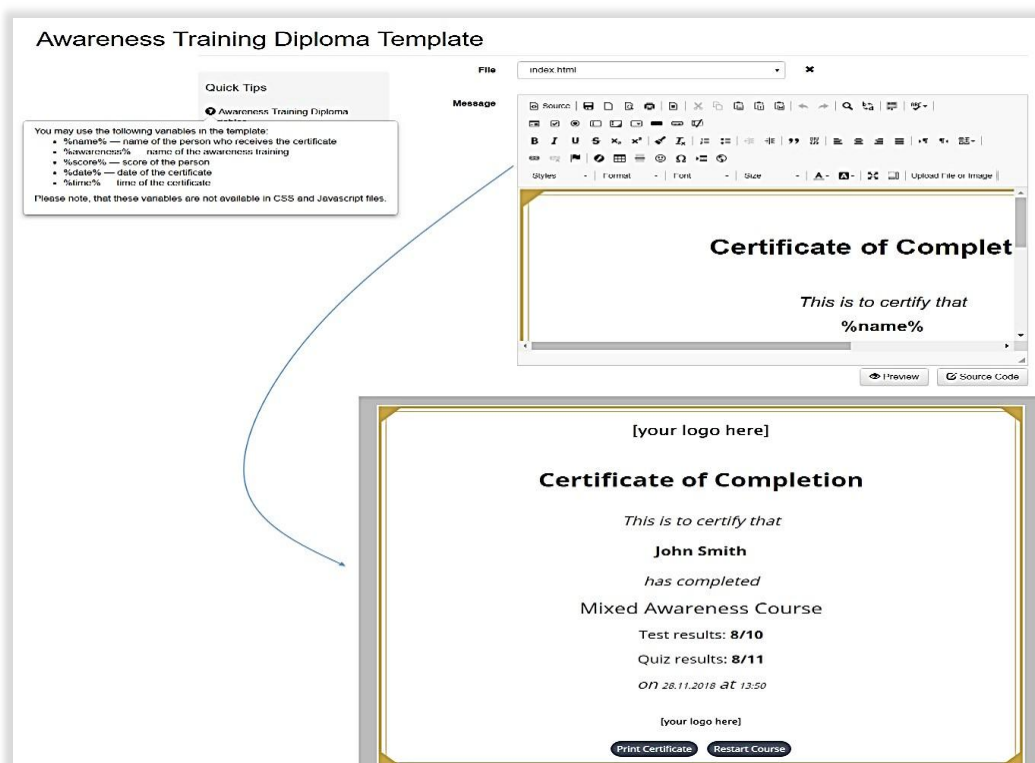
Awareness	Course	Risk Level			
Comprehensive security course	Edit Awareness Settings	Comprehensive security course	0	+	- x
Repetition Course	Edit Awareness Settings	Avoid & Recognize Phishing Attacks (V 2.3)	2	+	- x
Short General teaching	Edit Awareness Settings	Email Only - This was a phishing simulation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

1
10

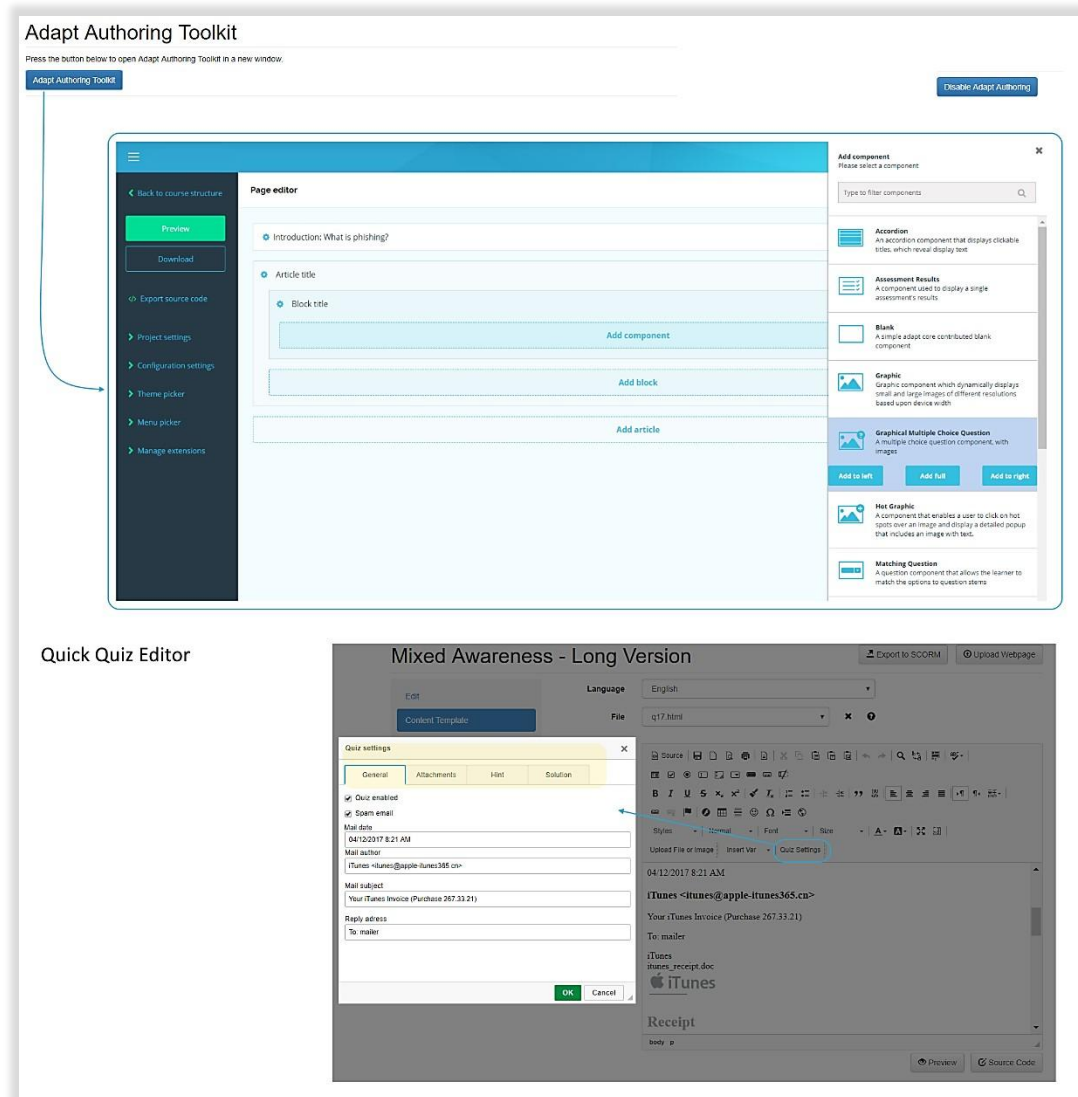
- Portal de formación para usuarios finales:** Funcionalidad del sistema de gestión de aprendizaje (LMS): Ofrece a cada empleado acceso permanente a una página de inicio formativa personalizada que incluye sus propios cursos específicamente diseñados para ellos. En esta página de inicio pueden ver sus estadísticas de rendimiento, reanudar o repetir la formación, crear certificados de cursos y comparar sus resultados con otros departamentos o grupos.



- Diploma de concienciación:** El destinatario puede crear e imprimir los certificados de aprendizaje online, ya sea directamente dentro de una formación o dentro del portal LMS.



- Kit de herramientas de creación de contenidos de aprendizaje online:** El kit de herramientas de creación de contenidos de aprendizaje online (Adapt) permite la creación de contenidos de aprendizaje individualizados. Arrastre y suelte vídeos o cualquier otro formato interactivo rich media, inserte exámenes desde menús predefinidos, cree contenido de aprendizaje electrónico interactivo desde cero en poco tiempo.



- **Entrenamiento de concienciación en formato interactivo rich media:** Integre elementos en formato interactivo rich media (vídeo, audio u otros elementos que animen a los empleados a interactuar y comprometerse con el contenido) en sus formaciones de concienciación. Utilice los vídeos educativos existentes, adáptelos o añada sus propios elementos en formato interactivo 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 INTERACTIVITY", "SOCIAL ENGINEERING", "PASSWORD SECURITY", "SECURE BROWSING", "SECURE SOCIAL NETWORKING", "USING PUBLIC WIFIS", "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

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

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.glnXN8SD>. 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

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

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

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

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

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

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

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

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: 16-15 Minutes | Skill Level: Low | Audience: All | Interactive: Yes

27.08.2018 16:12:54

Edit Preview Website Preview E-mail

...and many more

Security News

News: Do you know how to handle security incidents

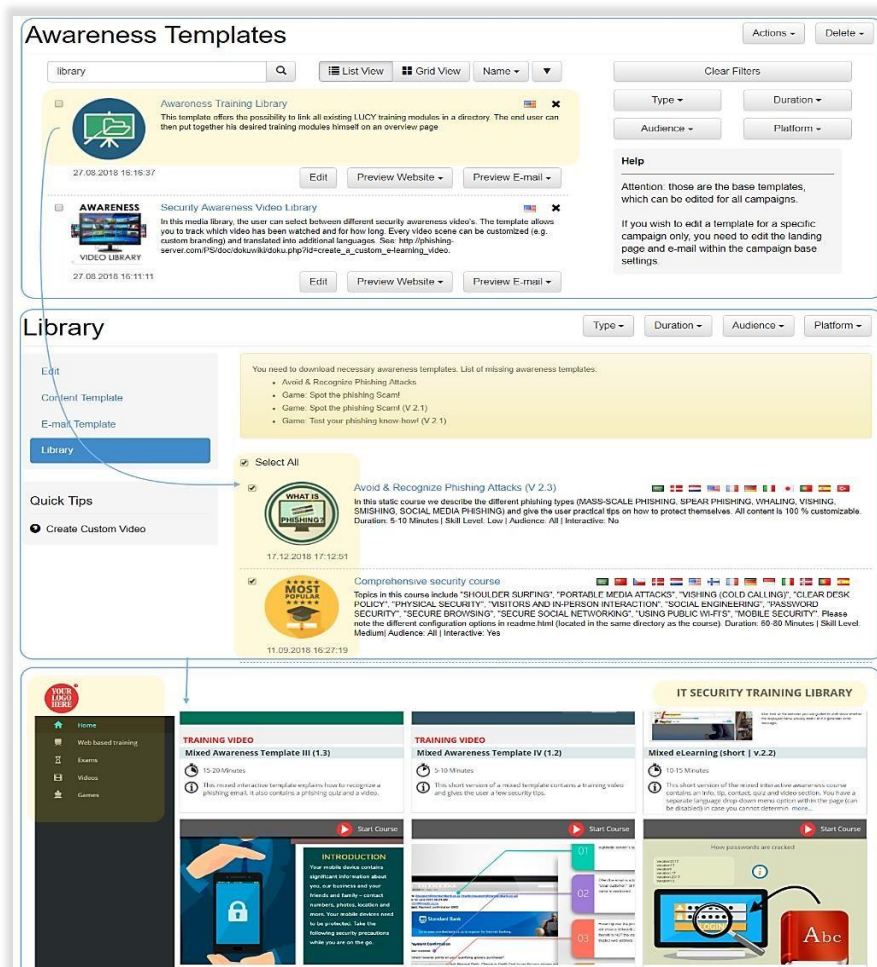
This course covers security incidents and the processes involved in reporting such incidents.

28.12.2018 14:48:47

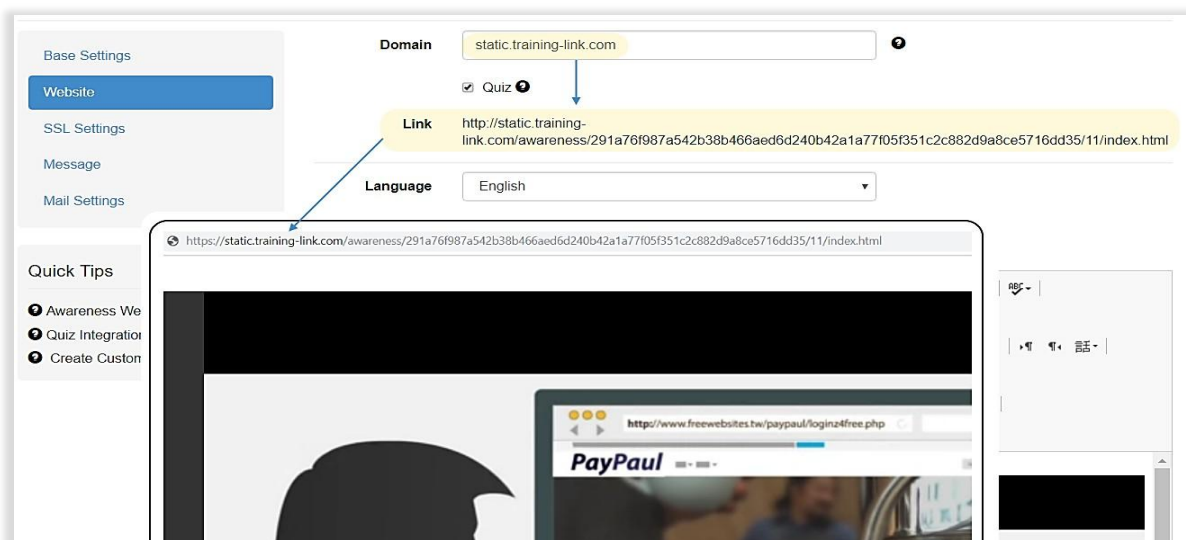
Edit Preview Website Preview E-mail

...and many more

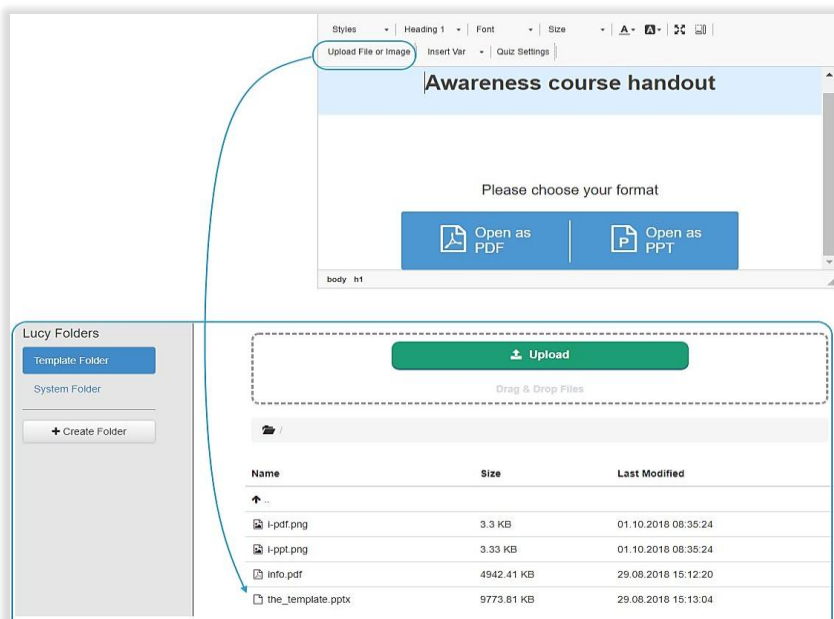
- **Biblioteca de formación:** Los empleados pueden acceder al contenido de formación de su organización desde una página de resumen llamada «biblioteca de formación». Contiene una gran selección de plantillas de aprendizaje online regulares de LUCY, que sirven como referencia. La página de resumen puede ordenarse por ciertos temas (vídeo, cuestionario, test, etc.).



- **Soporte de entrenamiento estático:** El contenido de la formación también puede publicarse en páginas estáticas en LUCY o en la Intranet, dando al usuario acceso permanente al contenido de la formación, independiente de posibles simulaciones de ataques.



- **Soporte de entrenamiento fuera de Internet:** LUCY se suministra con una serie de plantillas editables (archivos de Adobe Photoshop o Illustrator) para la formación de concienciación, como carteles, salvapantallas, folletos, etc.



- **Módulos de microaprendizaje:** Hemos diseñado módulos de formación para el microaprendizaje (p. ej., vídeos de 1 minuto o documentos de concienciación de una página) que pueden adaptarse a las necesidades de marca y políticas de su organización.

☐

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!

- **Personalización de vídeo:** Envíenos el logo de su empresa y lo incluiremos en los vídeos formativos. ¿Quiere otro idioma? No hay problema. Configuraremos el vídeo para que se reproduzca en el idioma que prefiera. ¿Quiere una escena diferente? Simplemente descargue los scripts de vídeo y marque los cambios deseados.



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 ▾

Upload

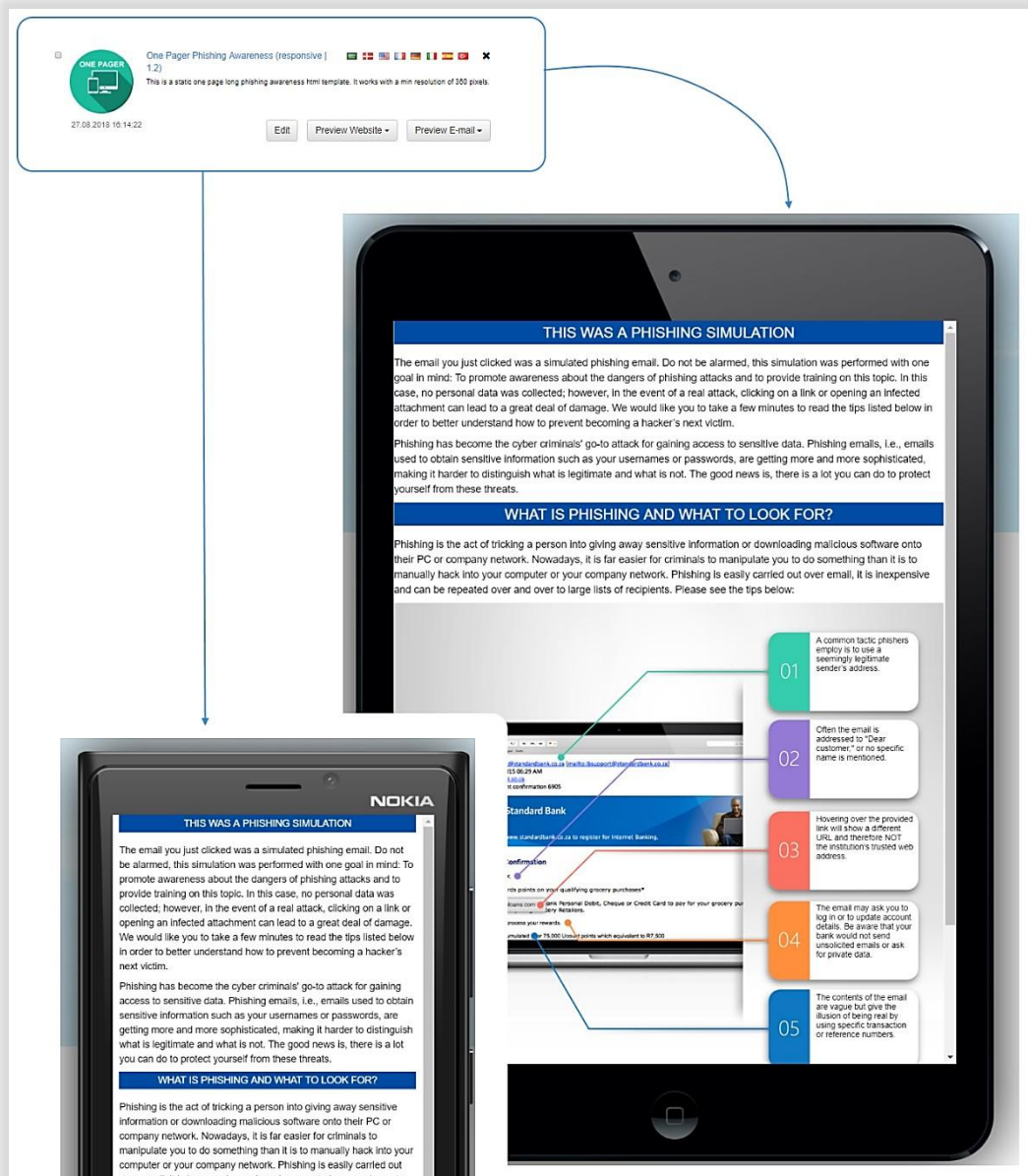
Drag & Drop Files

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.

- **Formato adaptativo a móviles:** Muchos de los módulos incorporados de LUCY están disponibles en un formato adaptado a los móviles que ofrece a sus usuarios la flexibilidad de realizar la formación con cualquier tipo de dispositivo conectado.



- **Importar y exportar vídeo:** Puede exportar vídeos de LUCY a su propio sistema, así como importar sus propios vídeos a LUCY.

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 highlighted. Below it, a 'Lucy Folders' sidebar shows 'Template Folder' and 'System Folder'. The main area displays an 'Upload' button and a table of files. A blue arrow points from the 'Download' button in the sidebar to the '2018.06.11_Lucy Data Privacy.mp4' file in the table.

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
jquery.js	93.71 KB	27.08.2018 16:16:29

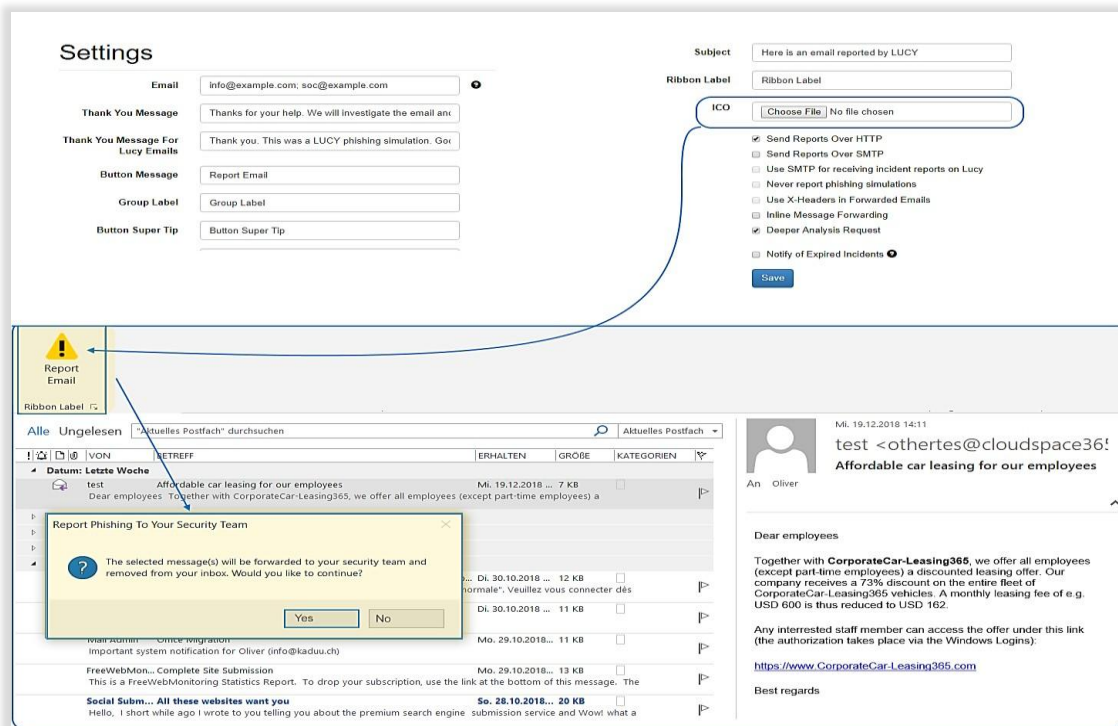
- **Pistas dinámicas de entrenamiento:** Las pistas dinámicas implementadas permiten a su administrador establecer marcadores dentro de las plantillas de ataque que podrían indicar a sus empleados, dentro del material de aprendizaje online, dónde se puede haber detectado el ataque de phishing.

The screenshot shows the 'Comprehensive security course' interface. It includes a sidebar with 'Edit', 'Content Template', and 'E-mail Template' options. The main area has a 'Language' dropdown set to 'English' and a 'File' dropdown set to 'index.html'. A blue arrow points from the 'Export to SCORM' button to the 'Exports' table. Another blue arrow points from the 'Content Template' button to the 'General Security Awareness Course' banner. A third blue arrow points from the 'Exports' table to the 'scorm-export.zip' file icon.

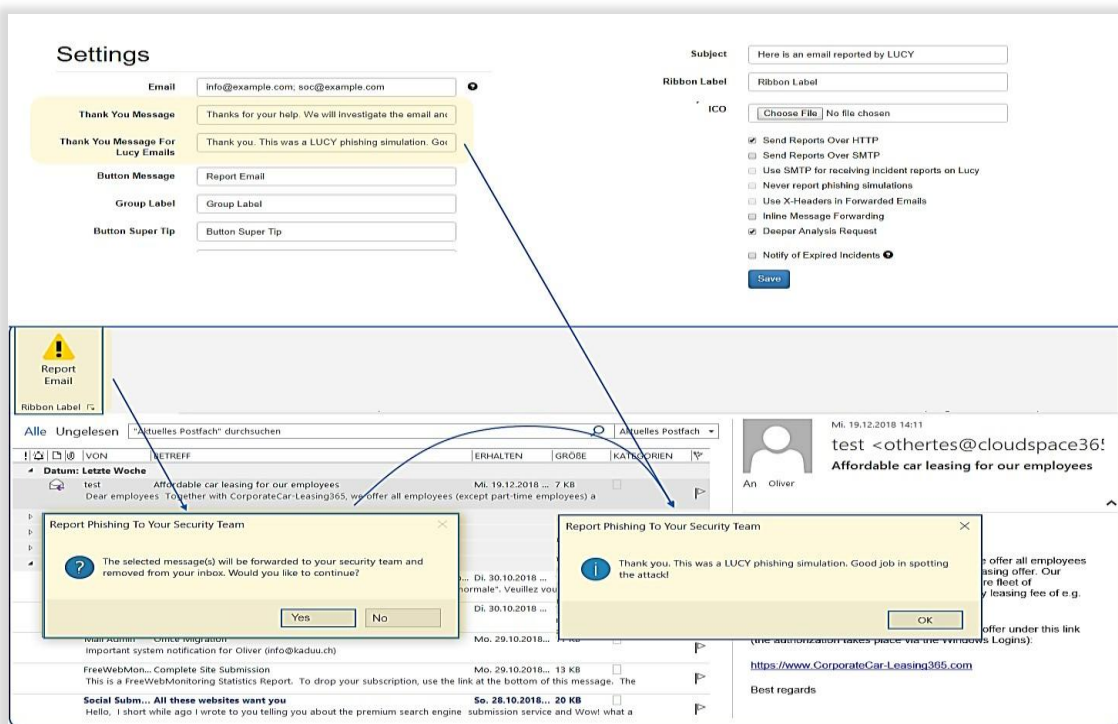
Date	Name	Extension	Status
31.12.2018 15:08:53	Awareness Template - Comprehensive security course		✓
29.12.2018 17:10:15	Campaign - BOUNCE TEST	csv	✓
28.12.2018 15:19:11	Awareness Template - Avoid & Recognize Phishing Attacks (V 2.3)		✓

INVOLUCRE A LOS EMPLEADOS

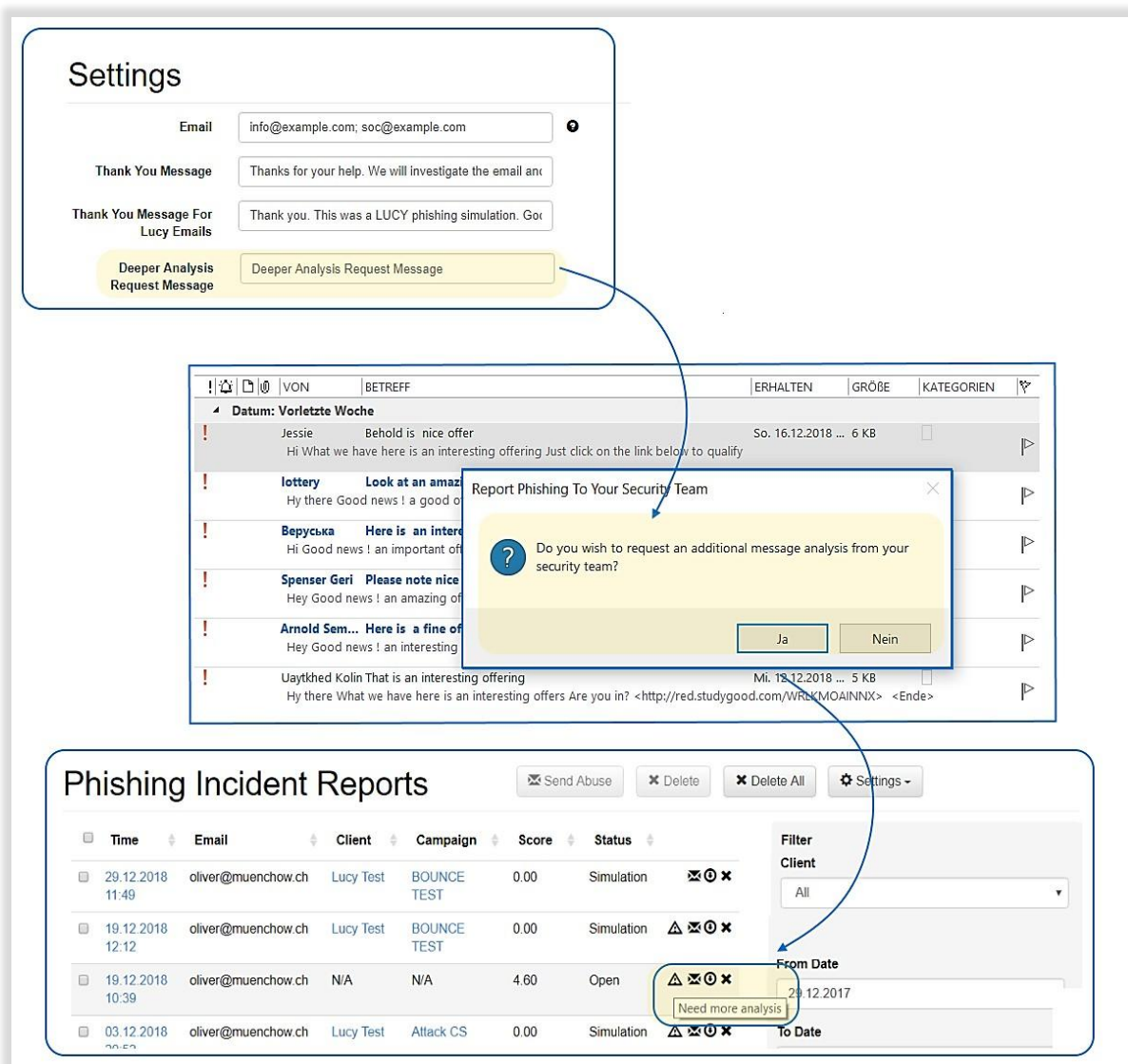
- **Reportar correos electrónicos con un solo clic:** Los usuarios finales pueden reportar correos electrónicos sospechosos con un solo clic a una o varias cuentas de correo electrónico y hacer que sean reenviados a su consola de análisis de incidentes LUCY.



- **Refuerzo de comportamiento positivo:** Nuestro plugin proporciona automáticamente un refuerzo positivo del comportamiento mostrando gratitud a los usuarios finales mediante un mensaje personalizado definido por su organización.



- Solicitud de inspección profunda:** A veces los usuarios quieren saber si el correo electrónico recibido se puede abrir de forma segura. Opcionalmente, el usuario puede utilizar la «solicitud de inspección profunda» dentro del plugin local para informar al equipo de seguridad de que desea recibir información sobre el correo electrónico reportado.



The screenshot illustrates the Lucy interface for managing phishing incidents. It is divided into three main sections:

Settings

This section allows users to configure their email and message templates. The "Email" field is set to "info@example.com; soc@example.com". The "Thank You Message" is "Thanks for your help. We will investigate the email and...". The "Thank You Message For Lucy Emails" is "Thank you. This was a LUCY phishing simulation. Go...". The "Deeper Analysis Request Message" is "Deeper Analysis Request Message".

Phishing Incident Reports

This section displays a list of phishing incidents. The table below shows the data for the incidents:

Time	Email	Client	Campaign	Score	Status	Actions
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 20:55	oliver@muenchow.ch	Lucy Test	Attack CS	0.00	Simulation	⚠️ 📧 🗑️

The "Need more analysis" button is highlighted in the "Actions" column for the incident on 19.12.2018 10:39.

Report Phishing To Your Security Team

This modal dialog asks the user if they wish to request an additional message analysis from their security team. The user can click "Ja" (Yes) or "Nein" (No).

- Análisis automático de incidentes:** Gestione y responda a los mensajes de correo electrónico sospechosos reportados mediante una consola de gestión centralizada: El analizador de LUCY permite una inspección automatizada de los mensajes reportados (encabezado y cuerpo). El analizador incluye una puntuación de riesgo individual, que proporciona una clasificación en tiempo real de los mensajes de correo electrónico reportados. El Analizador de Amenazas supone un notable alivio para la carga de trabajo del equipo de seguridad.

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	ⓧ ⓧ ⓧ

10 rows per page

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 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 ☒	ⓧ ⓧ ⓧ

Summary
Mail Server Analysis
Domain Analysis
Body Analysis

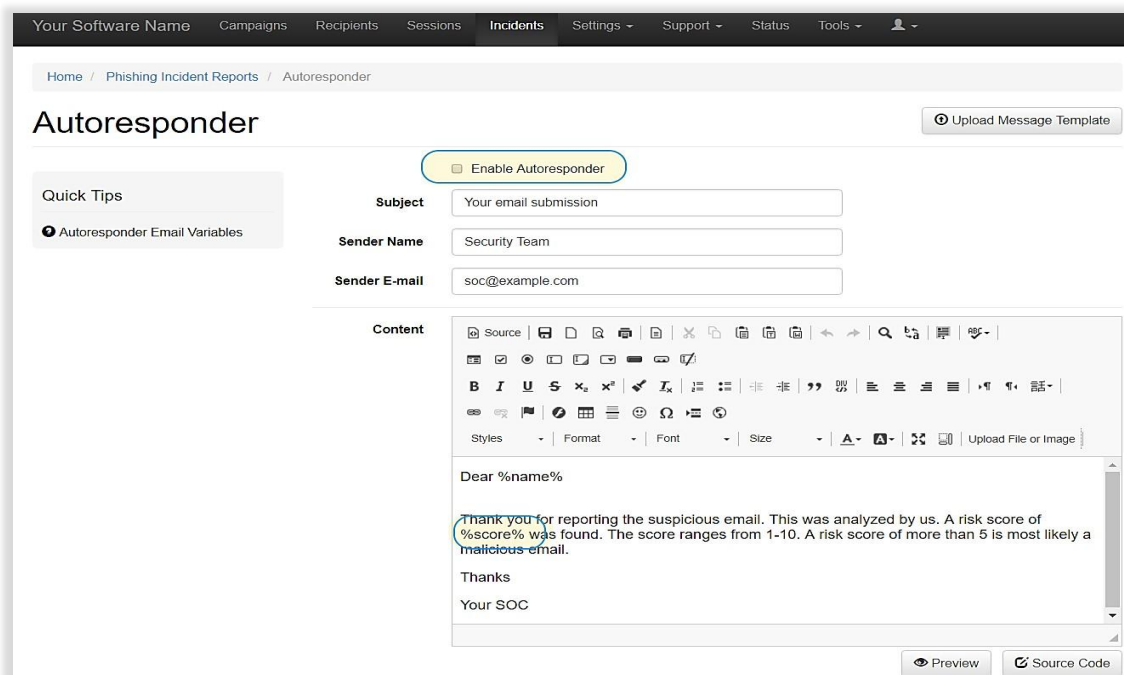
Overall Risk Score:

2.5 of 10.0
highcharts.com

Need More Analysis

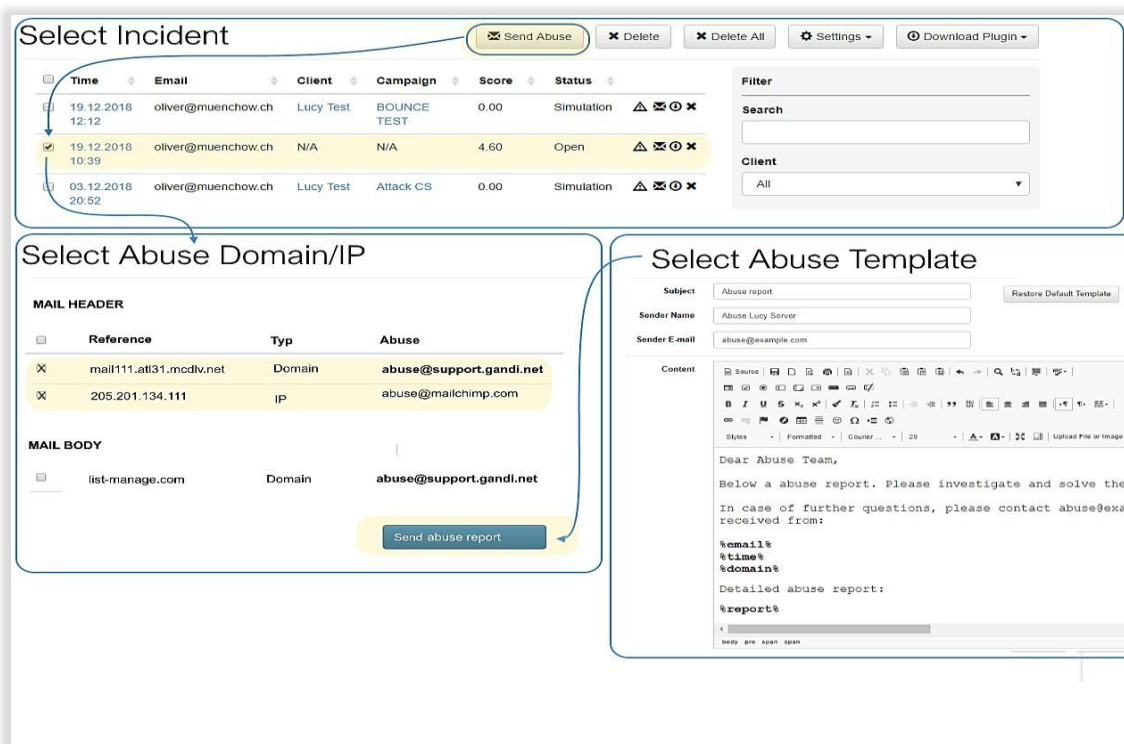
Email: oliver@muenchow.ch
Message: Download
Message Subject: Only 7% of Our Customers Are Doing SEO Right. And You?
Thumbnail:
Report Time: 16.10.2018 09:25:20
Status: In Progress
Notes:
Save

- Feedback automático del incidente:** El Autorespondedor de Incidentes permite enviar una notificación automatizada al usuario final proporcionando los resultados del análisis de las amenazas de su correo electrónico. El texto del mensaje es libremente configurable, y la puntuación de riesgo del correo electrónico de LUCY también puede incluirse si es necesario.



The screenshot shows the 'Autoresponder' configuration page. At the top, there's a navigation bar with 'Incidents' selected. Below it, a breadcrumb trail reads 'Home / Phishing Incident Reports / Autoresponder'. The main heading is 'Autoresponder', with an 'Upload Message Template' button on the right. On the left, there's a 'Quick Tips' section with a link to 'Autoresponder Email Variables'. The main form includes a toggle for 'Enable Autoresponder', and fields for 'Subject' (Your email submission), 'Sender Name' (Security Team), and 'Sender E-mail' (soc@example.com). The 'Content' section features a rich text editor with a toolbar and a preview of the email body. The preview shows a personalized message: 'Dear %name%', followed by a thank you for reporting a suspicious email, a risk score of '%score%' (with a tooltip explaining the score range from 1-10), and a closing 'Thanks, Your SOC'. At the bottom right, there are 'Preview' and 'Source Code' buttons.

- Mitigación de amenazas:** El Mitigador de Amenazas de Comportamiento es un enfoque revolucionario para eliminar los riesgos del correo electrónico. Apoyará al administrador de seguridad a parar el ataque (p. ej., enviando un informe automatizado al equipo antiabuso de los proveedores implicados en el ataque).



The screenshot illustrates the workflow for sending an abuse report. It starts with the 'Select Incident' screen, which has a table of incidents. A blue arrow points from the 'Send Abuse' button to the 'Select Abuse Domain/IP' screen. This screen shows a table with incident details, including 'Reference', 'Type', and 'Abuse'. A blue arrow points from the 'Send abuse report' button to the 'Select Abuse Template' screen. This final screen shows a form for the abuse report, including 'Subject' (Abuse report), 'Sender Name' (Abuse Lucy Sender), and 'Sender E-mail' (abuse@example.com). The 'Content' section shows a template for the abuse report, with placeholders for email, time, domain, and report details. The template text reads: 'Dear Abuse Team, Below a abuse report. Please investigate and solve the In case of further questions, please contact abuse@example.com received from: %email% %time% %domain% Detailed abuse report: %report%'. At the bottom, there's a 'body pre span span' label.

- **Análisis basado en reglas personalizadas:** 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
From Date

Custom Rules
Score Factors
Abuse
Autoreponder
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

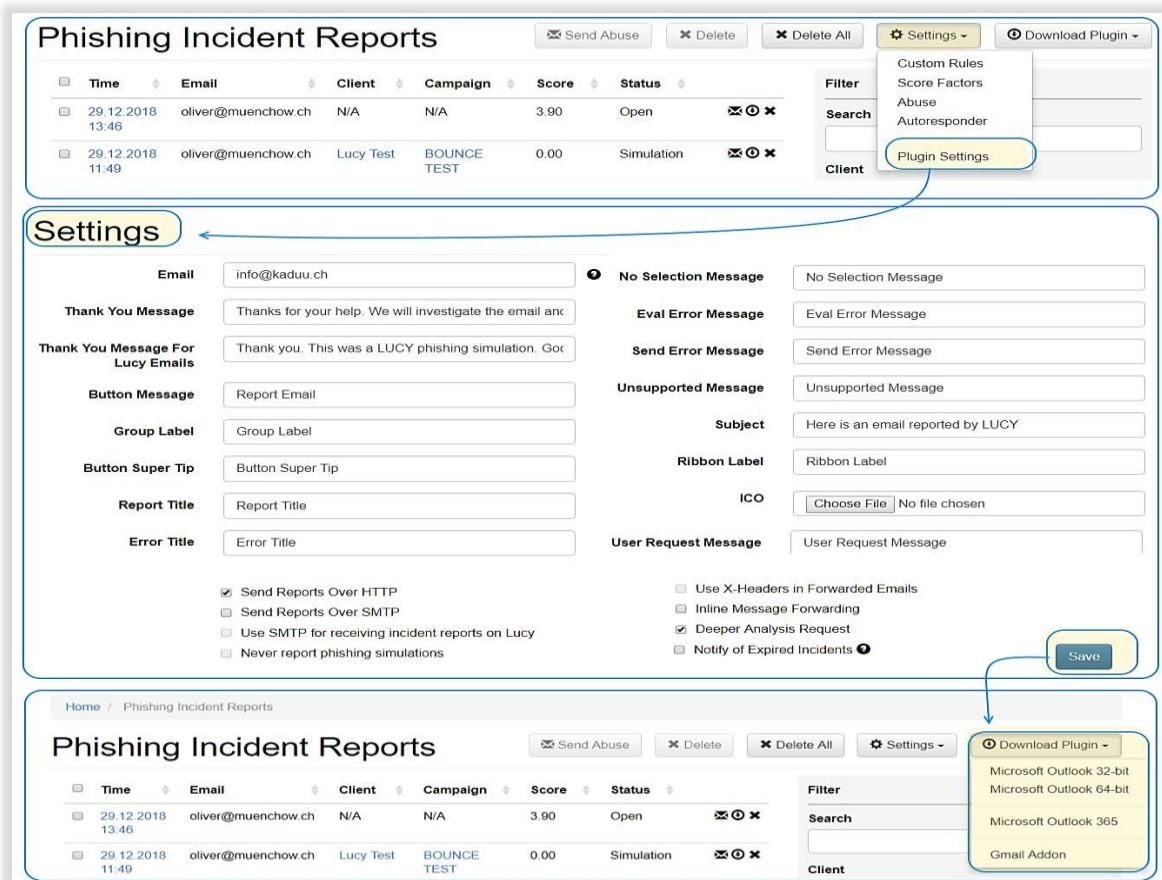
Name Ceo name in header
Reg. Exp. Jon Smith
Score 2

Save

Summary
Header Analysis
Domain Analysis
Body Analysis
Threat Indicators

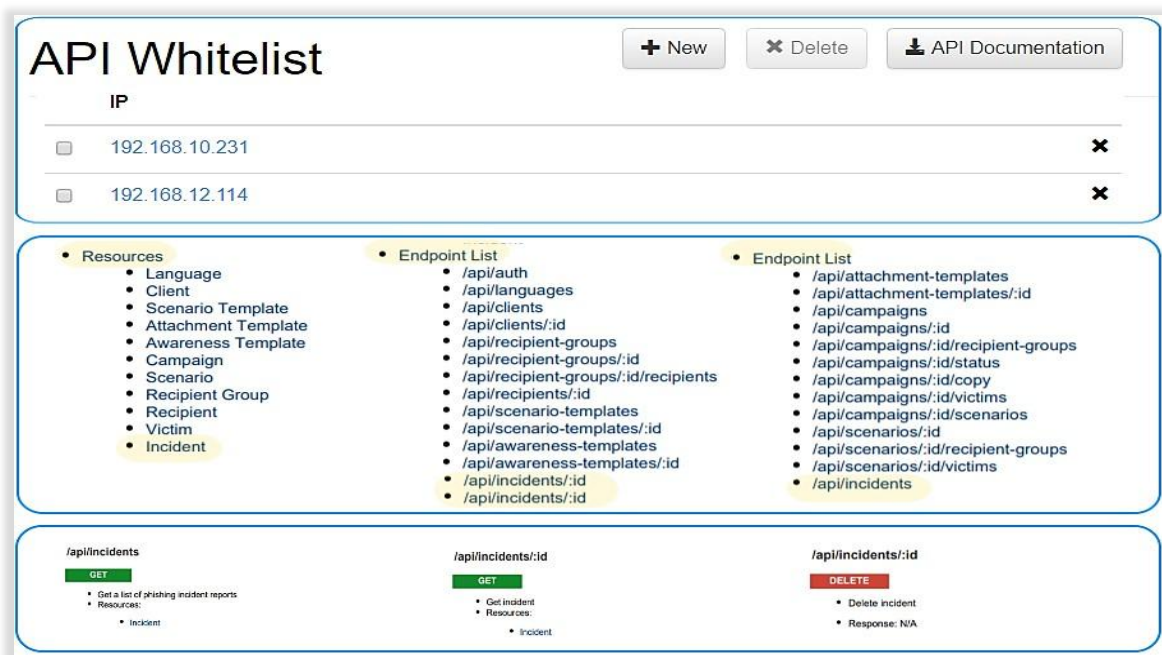
		Score	Rule active?	
Reply-to Mismatch	different reply-to adress defined than the actual (more info...)	1.60	Active ☒ Inactive	🔍✖️
New Domain	Domain has been reserved in the last 30 days (more info...)	20.00	Active ☒ Inactive	🔍✖️
Link Display mismatch	link display name different from the actual link (more info...)	0.00	Active ☐ Inactive	🔍✖️

- **Opciones de personalización de los plugins:** LUCY permite una fácil personalización y una marca blanca por completo de las diferentes funciones de los plugins (icono visualizado, mensajes de feedback, etiqueta de cinta, protocolo de transmisión, cabecera enviada, etc.).



The screenshot shows the 'Phishing Incident Reports' interface. At the top, there's a table with columns: Time, Email, Client, Campaign, Score, Status, and Filter. Below the table, there's a 'Settings' section with various input fields for messages (No Selection Message, Eval Error Message, Send Error Message, Unsupported Message, Subject, Ribbon Label, ICO, User Request Message) and checkboxes for reporting options (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, Notify of Expired Incidents). A 'Save' button is at the bottom right. A callout box shows the 'Settings' dropdown menu with options: Custom Rules, Score Factors, Abuse, Autoresponder, and Plugin Settings.

- **Integración de terceros:** Gracias a la automatización de la API REST de incidentes de LUCY, podemos procesar los mensajes de correo electrónico notificados y ayudar a su equipo de seguridad a detener los ataques de phishing activos mientras están en curso.



The screenshot shows the 'API Whitelist' interface. It has a table with columns: IP, and a 'New' button. Below the table, there's a 'Resources' section with a list of endpoints: /api/auth, /api/languages, /api/clients, /api/clients/:id, /api/recipient-groups, /api/recipient-groups/:id, /api/recipient-groups/:id/recipients, /api/recipients/:id, /api/scenario-templates, /api/scenario-templates/:id, /api/awareness-templates, /api/awareness-templates/:id, /api/incidents/:id, /api/incidents/:id. There's also an 'Endpoint List' section with a list of endpoints: /api/attachment-templates, /api/attachment-templates/:id, /api/campaigns, /api/campaigns/:id, /api/campaigns/:id/recipient-groups, /api/campaigns/:id/status, /api/campaigns/:id/copy, /api/campaigns/:id/victims, /api/campaigns/:id/scenarios, /api/scenarios/:id, /api/scenarios/:id/recipient-groups, /api/scenarios/:id/victims, /api/incidents. At the bottom, there's a section for '/api/incidents' with a 'GET' button and a description: 'Get a list of phishing incident reports. Resources: Incident'. There's also a section for '/api/incidents/:id' with a 'GET' button and a description: 'Get incident. Resources: Incident'. There's also a section for '/api/incidents/:id' with a 'DELETE' button and a description: 'Delete incident. Response: N/A'.

- **Identificar ataques con patrones comunes:** Aplique los filtros del panel de control de LUCY para detectar los vectores de ataque comunes en toda su organización. Busque en todos los correos electrónicos reportados indicadores similares de amenazas.

The screenshot displays the 'Incident Reports' interface in the Lucy application. The top section shows a list of incident reports with columns for Time, Email, Rating, Client, Campaign, Score, and Status. The bottom section shows a detailed view of a specific report for the email 'sarah@test.com', including a circular risk score gauge (3.9 of 10.0) and a 'Behold' button. A blue arrow points from the 'Behold' button in the detailed view to the 'Behold' button in the filter section of the 'Phishing Incident Reports' panel on the right.

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

Phishing Incident Reports

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

Filter

Show only mails from this domain: [dropdown]

Search: [input]

Reputation Filter: [dropdown]

Show only mails with rating >: [input]

Client: [dropdown]

Min Score: [input]

From Date: [input]

To Date: [input]

Campaign: [dropdown]

Status: [dropdown]

Email Domain: [dropdown]

Update

- **Perfiles de reputación de usuarios de incidentes:** Clasifique a los usuarios con una puntuación de reputación basada en los incidentes.

The screenshot displays the 'Incident Reports' interface in the Lucy application. The top section shows a list of incident reports with columns for Time, Email, Rating, Client, Campaign, Score, and Status. The 'Rating' column is highlighted with a blue box. The bottom section shows a detailed view of a specific report for the email 'sarah@test.com', including a circular risk score gauge (3.9 of 10.0) and a 'Behold' button. A blue arrow points from the 'Behold' button in the detailed view to the 'Behold' button in the filter section of the 'Phishing Incident Reports' panel on the right.

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

Phishing Incident Reports

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

Filter

Show only mails from this domain: [dropdown]

Search: [input]

Reputation Filter: [dropdown]

Show only mails with rating >: [input]

Client: [dropdown]

Min Score: [input]

From Date: [input]

To Date: [input]

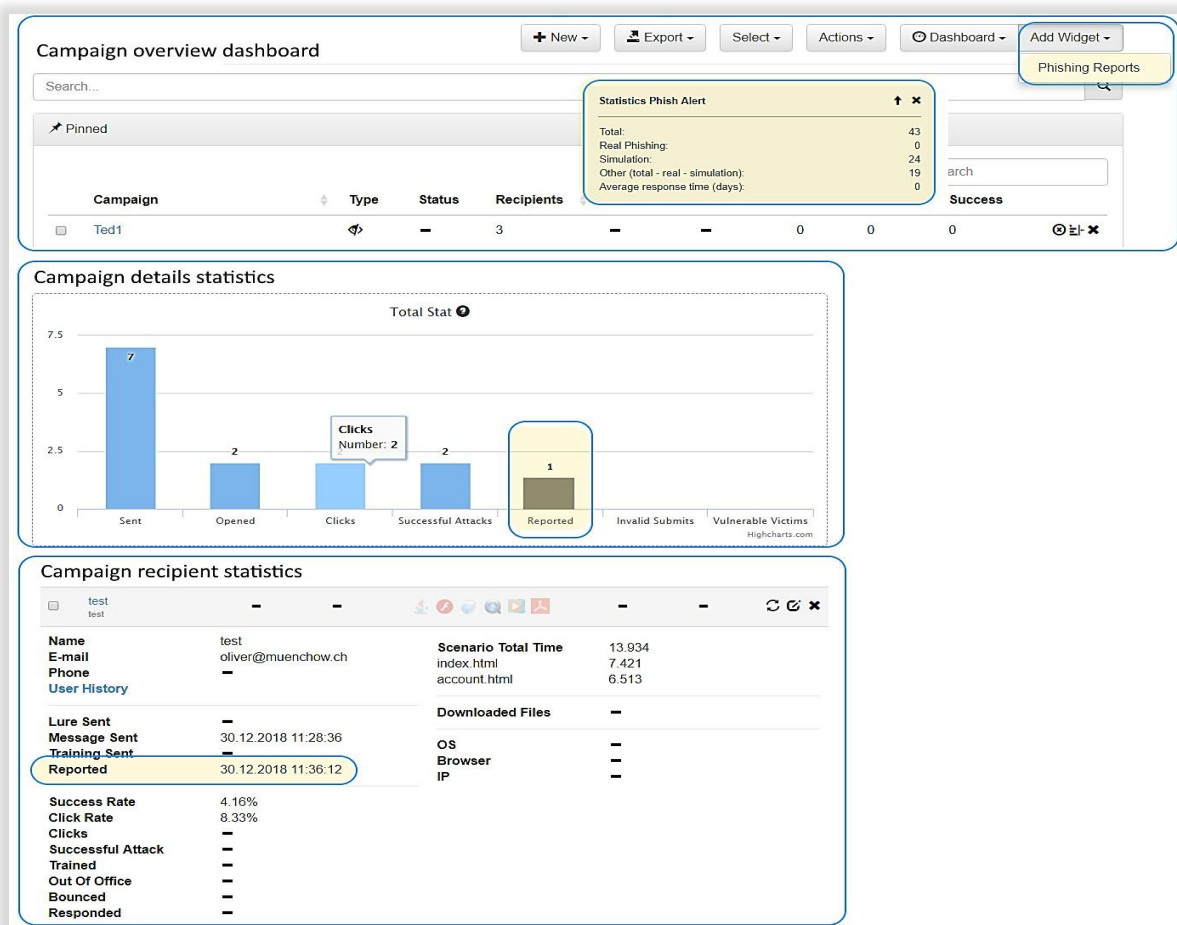
Campaign: [dropdown]

Status: [dropdown]

Email Domain: [dropdown]

Update

- **Integración con simulaciones de ataque:** Integración perfecta de reportes y panel de control con simulaciones de phishing: identifique a los usuarios que se han comportado de forma ejemplar en una simulación de phishing.



- **Fácil instalación:** Instale el plugin de incidentes de phishing para Outlook, Gmail, Office365.

