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

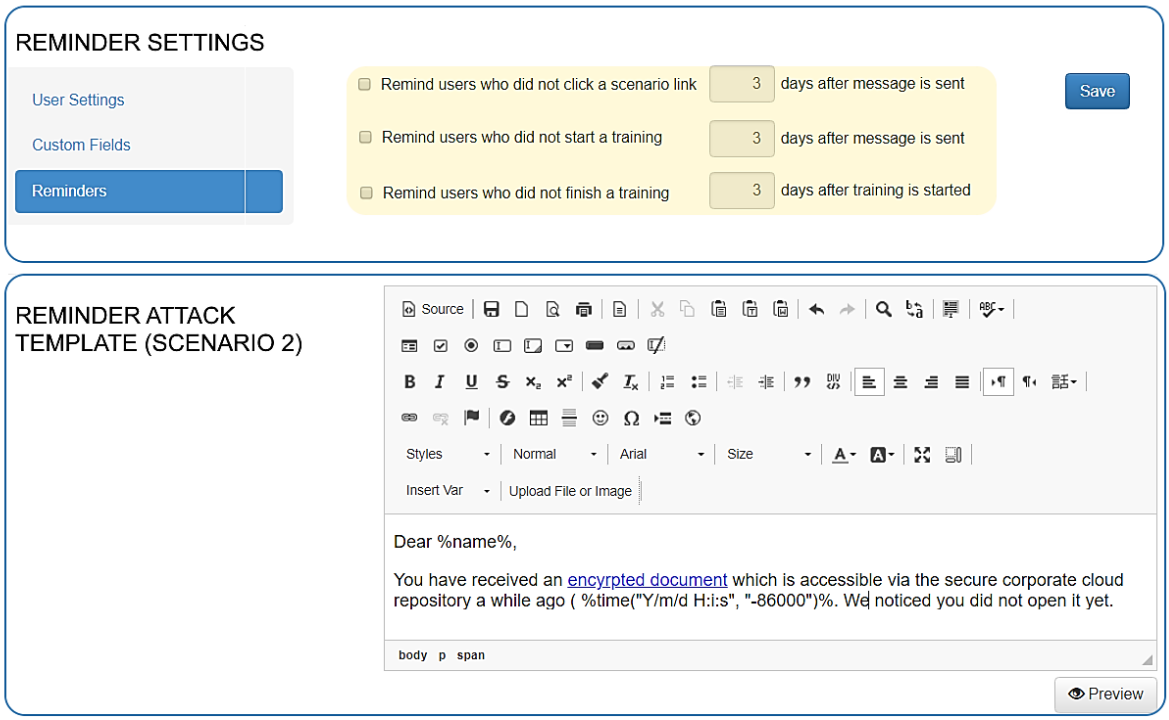
- Aprendizaje online basado en la reputación
- Portal de formación para usuarios finales
- Diploma de concienciación
- Kit de herramientas de creación de contenidos de aprendizaje online
- Entrenamiento de concienciación en formato interactivo rich media
- Biblioteca de formación
- Soporte de entrenamiento 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

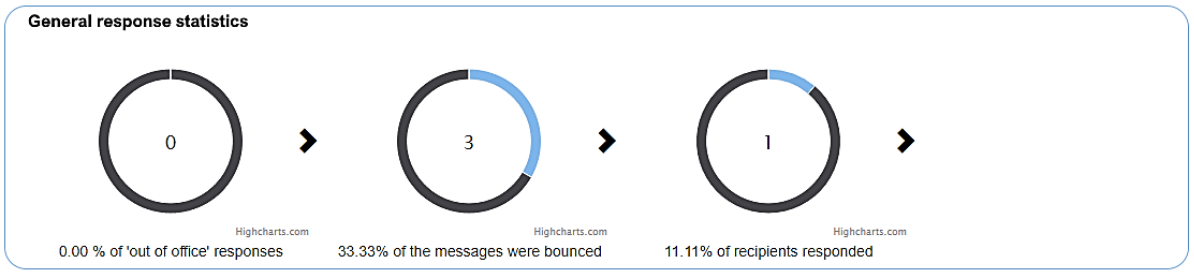
- Reportar correos electrónicos con un solo clic
- Refuerzo de comportamiento positive
- Solicitud de inspección profunda
- Análisis automático de incidentes
- Feedback automático del incidente
- Mitigación de amenazas
- Análisis basado en reglas personalizadas
- Opciones de personalización de los plugins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

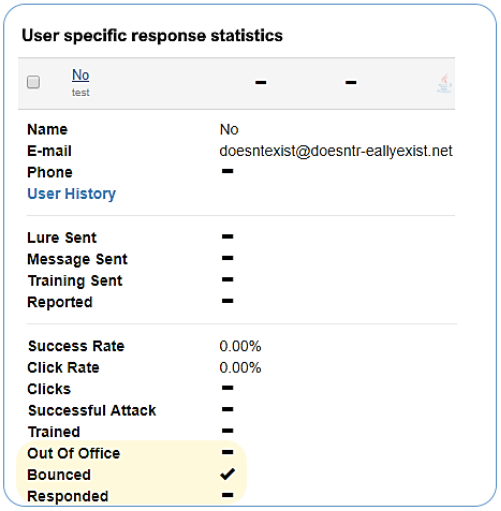
CARACTERÍSTICAS GENERALES

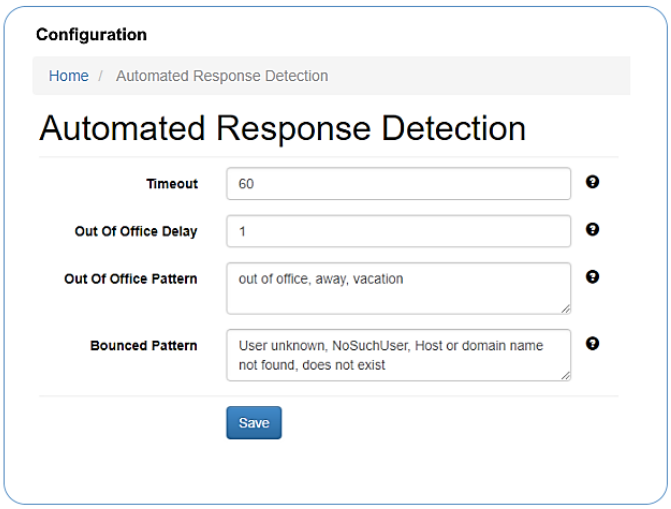
- **Recordatorios:** Las plantillas de los recordatorios pueden utilizarse para reenviar automáticamente mensajes a los usuarios que no hayan hecho clic en un vínculo de ataque o en un curso de formación después de un período de tiempo personalizado.



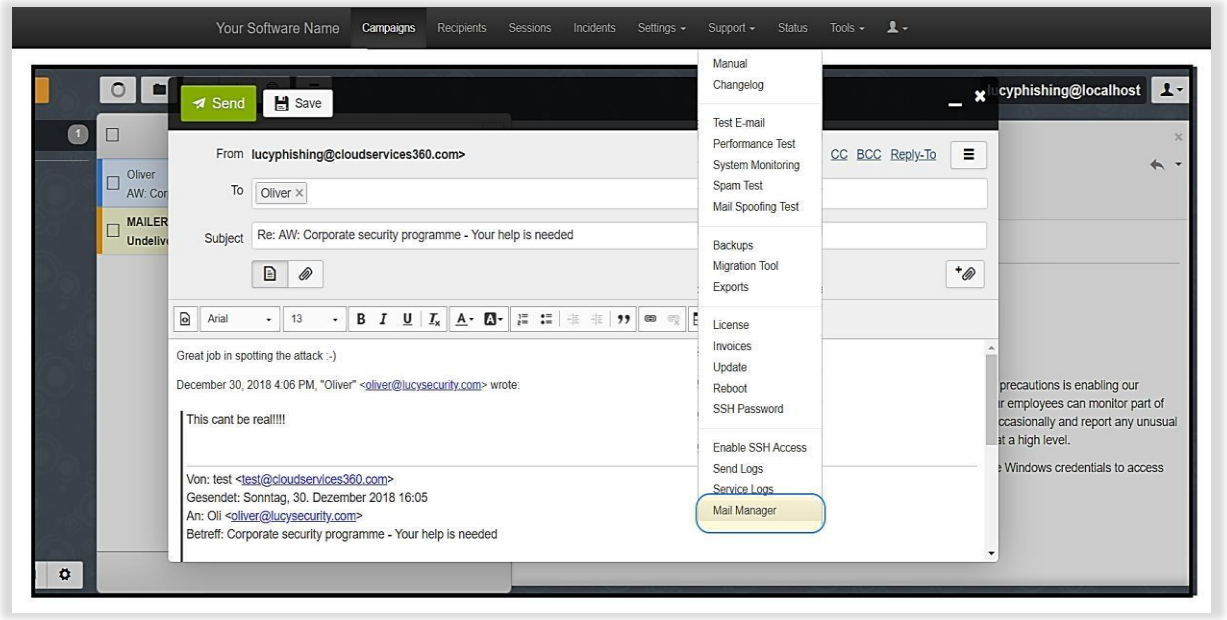
- **Detección de respuesta:** La detección de respuestas automáticas permite definir y analizar las respuestas automáticas de correo electrónico (p. ej., fuera de la oficina), así como los errores de entrega de correo (p. ej., usuario desconocido) dentro de la compaña.



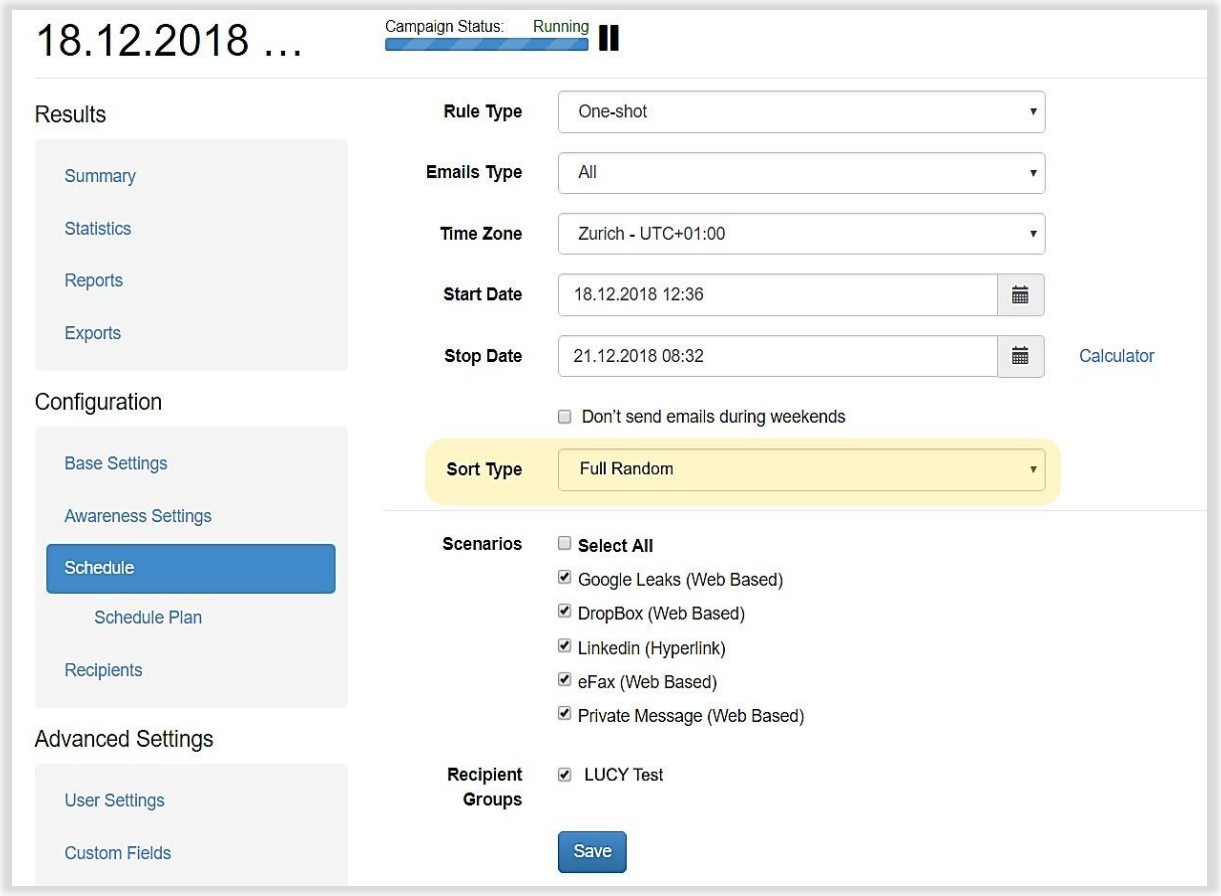




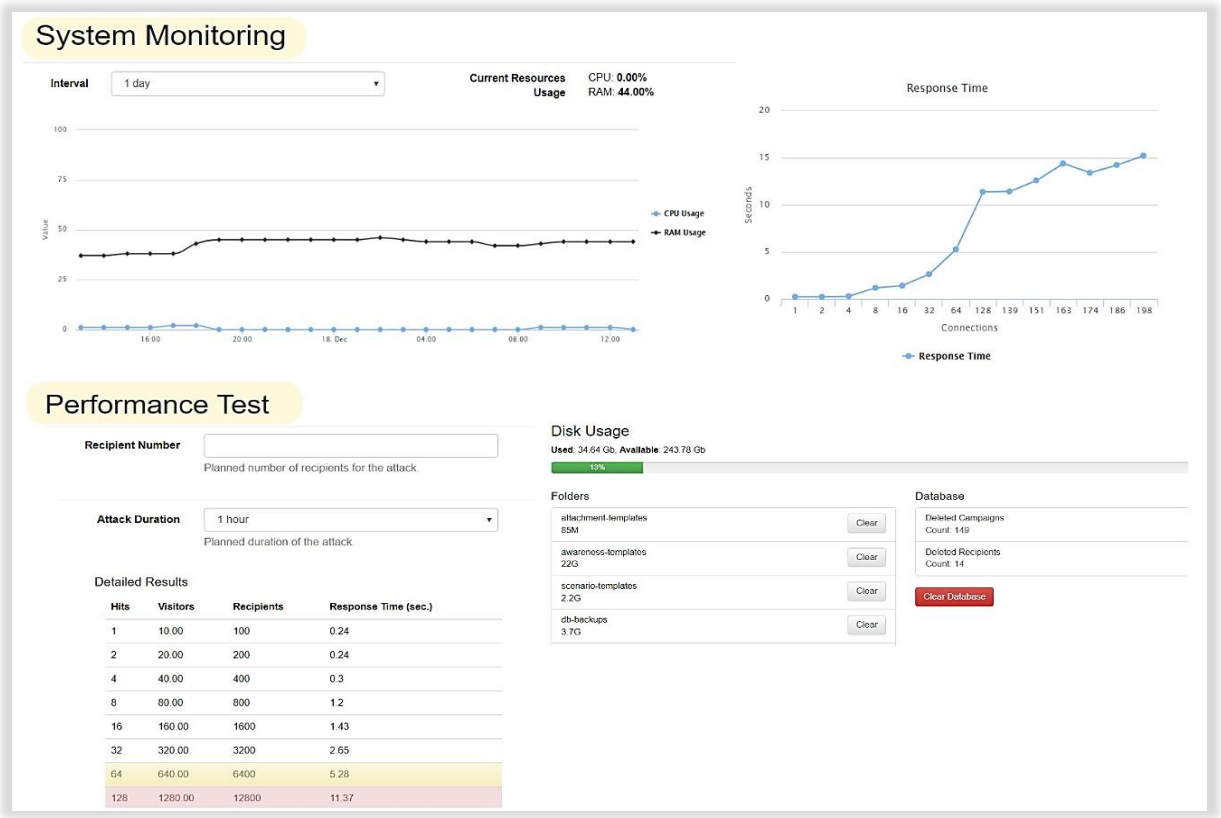
- **Cliente completo de comunicación por correo:** Una plataforma de mensajería integrada permite al administrador de LUCY comunicarse interactivamente con los destinatarios dentro o fuera de las campañas de LUCY. Todos los correos electrónicos se archivan y pueden ser evaluados.



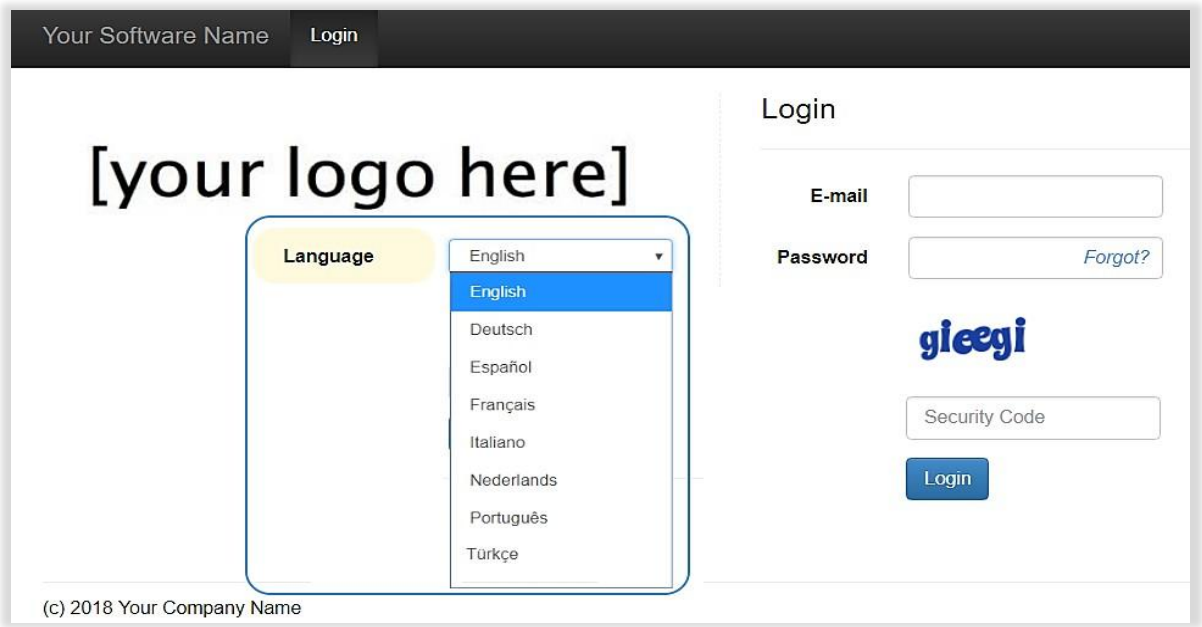
- **Aleatorización del programador:** Concienciar a los empleados al azar es el factor clave para una concienciación efectiva y sostenible dentro de la organización. El envío aleatorio de muchas campañas simultáneas es uno de los mejores medios para capacitar a los empleados.



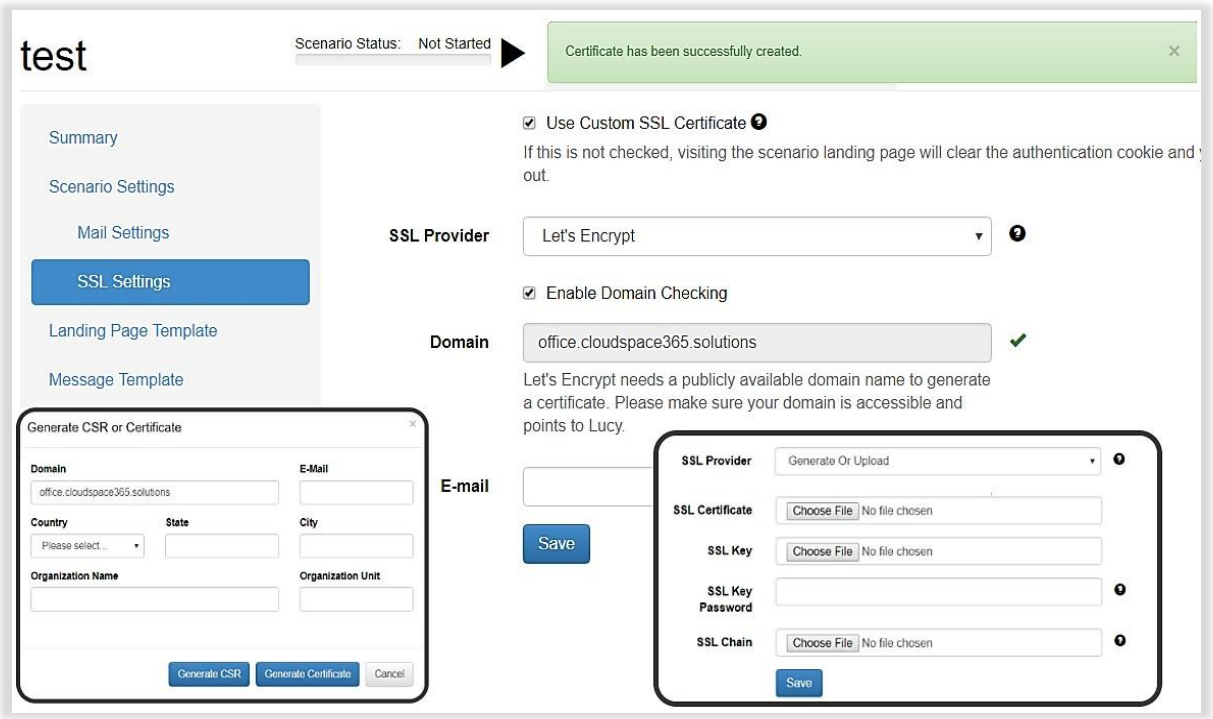
- **Herramientas de rendimiento:** Las rutinas inteligentes de LUCY adaptan la instalación del servidor a los recursos disponibles. El servidor de aplicaciones, el dimensionamiento del SGBD y el uso de CPU y memoria se calculan durante la instalación o durante las operaciones. Puede escalar una única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



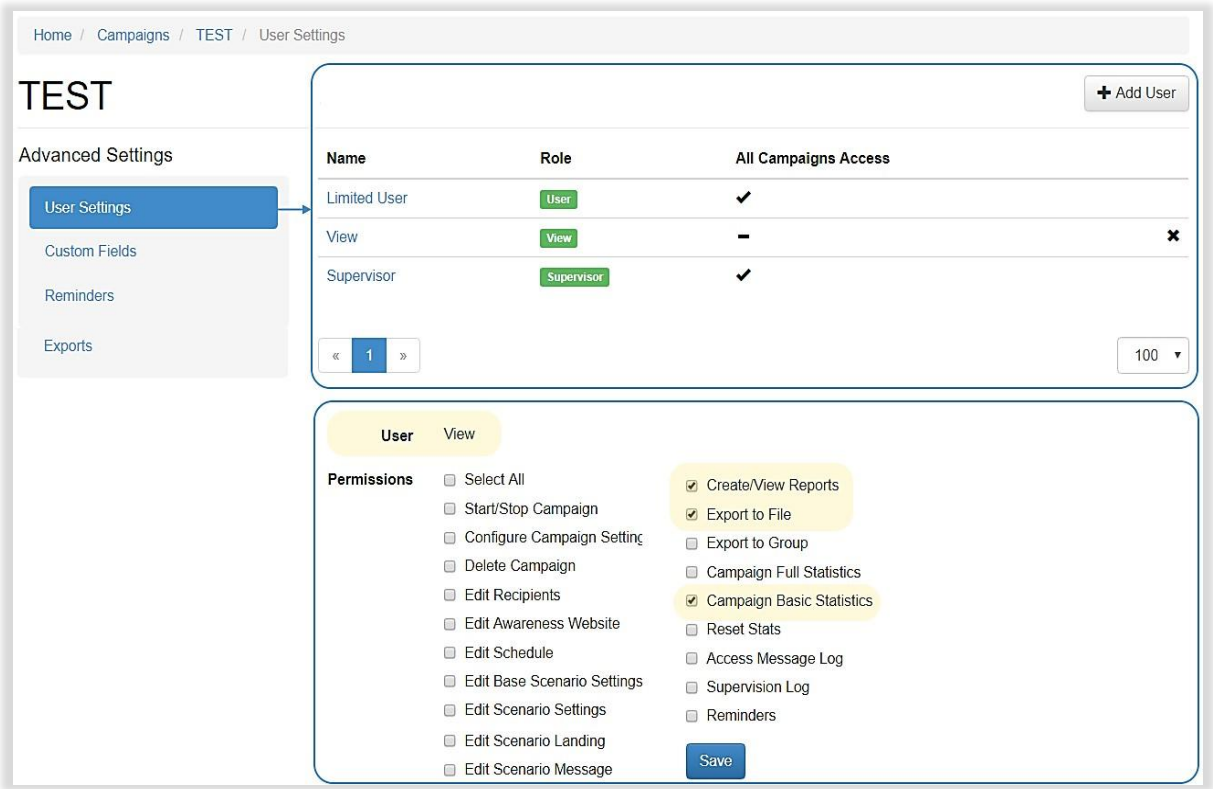
- **Interfaz de administración multilingüe:** La interfaz de administración de LUCY está disponible en diferentes idiomas y puede traducirse a otros idiomas si se solicita.



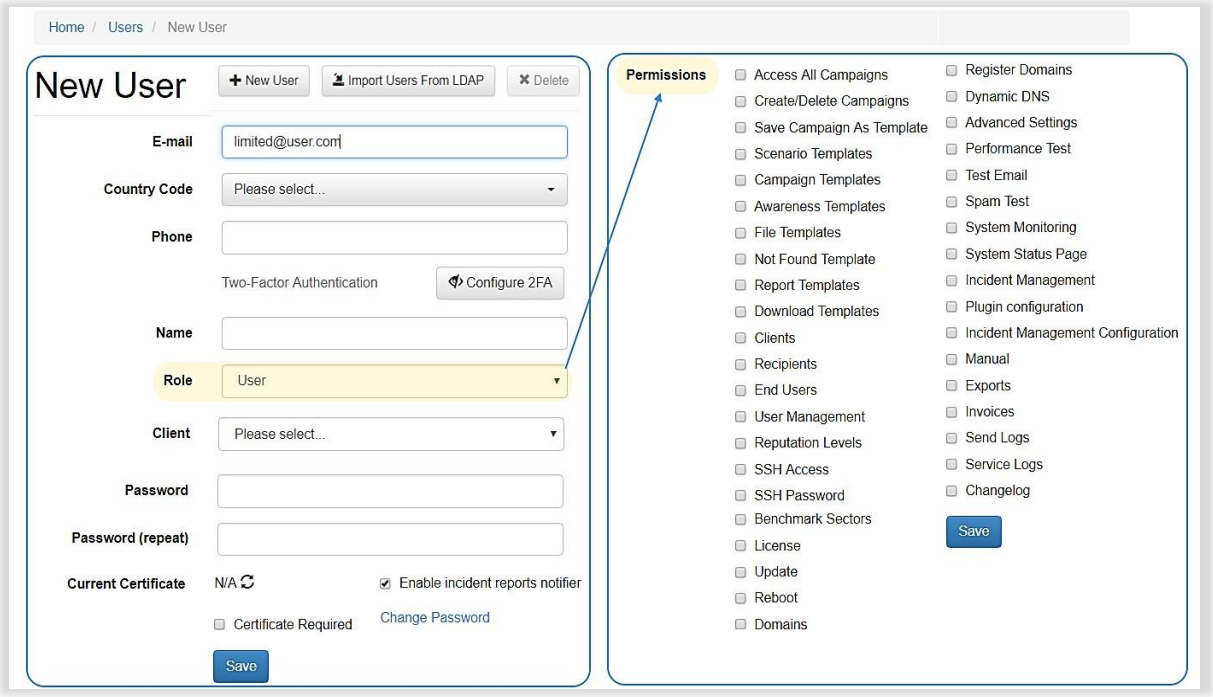
- **Certificado (SSL):** Permite la creación automática de certificados oficiales y de confianza para el administrador, el backend y las campañas. LUCY utilizará automáticamente el dominio configurado en el sistema para generar el certificado. Si decide utilizar SSL para la campaña, puede generar un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



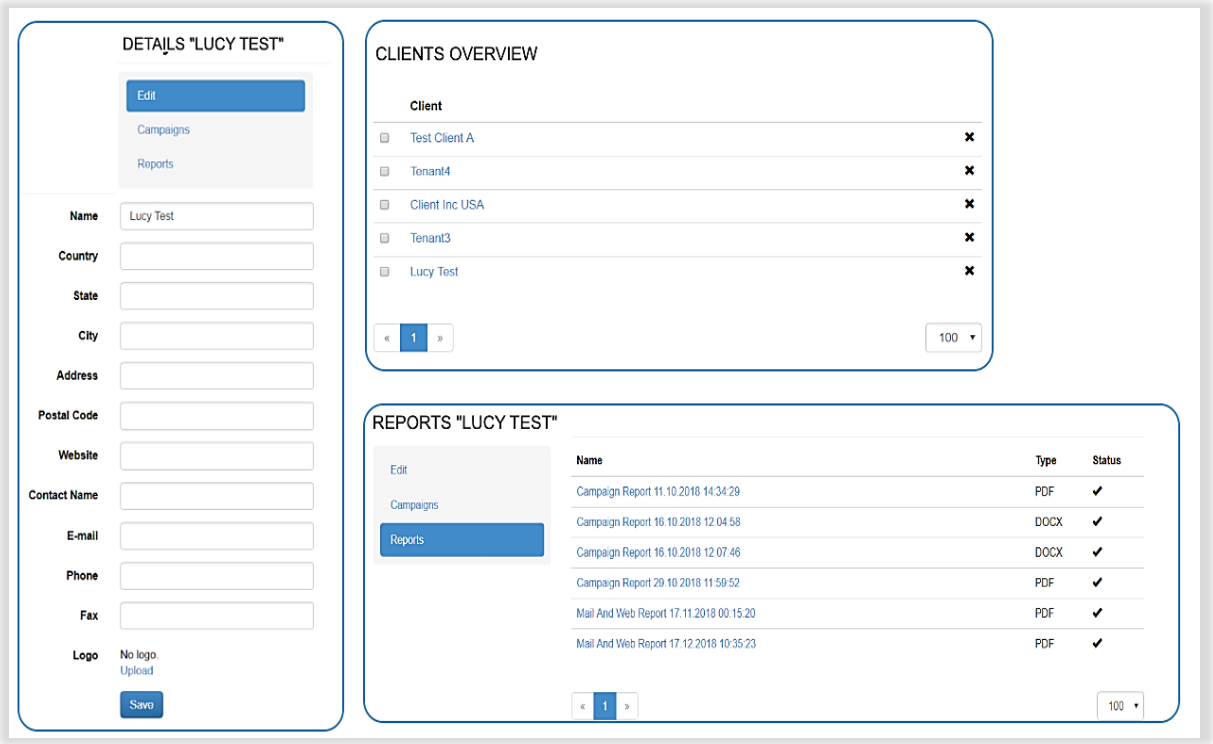
- **Controles de acceso basado en roles:** LUCY ofrece un control de acceso basado en roles (RBAC) que restringe el acceso al sistema solo a usuarios autorizados. Los permisos para realizar ciertas operaciones se asignan a roles específicos dentro de la configuración del usuario. A los miembros o al 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.



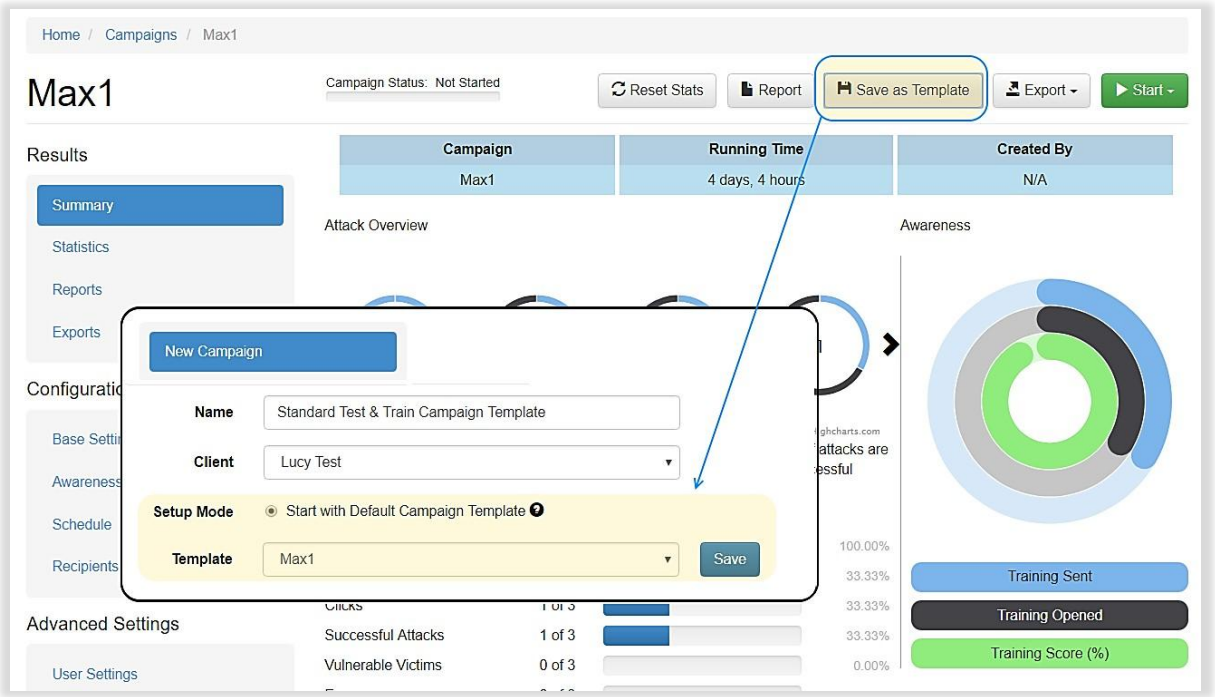
- **Grupos de usuarios de múltiples capas**: Cargue rápidamente usuarios de forma masiva mediante un archivo CSV, LDAP o de texto. Cree diferentes grupos, organizados por departamento, división, título, etc. Actualice a los usuarios en una campaña en curso. Cree grupos de usuarios dinámicos basados en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



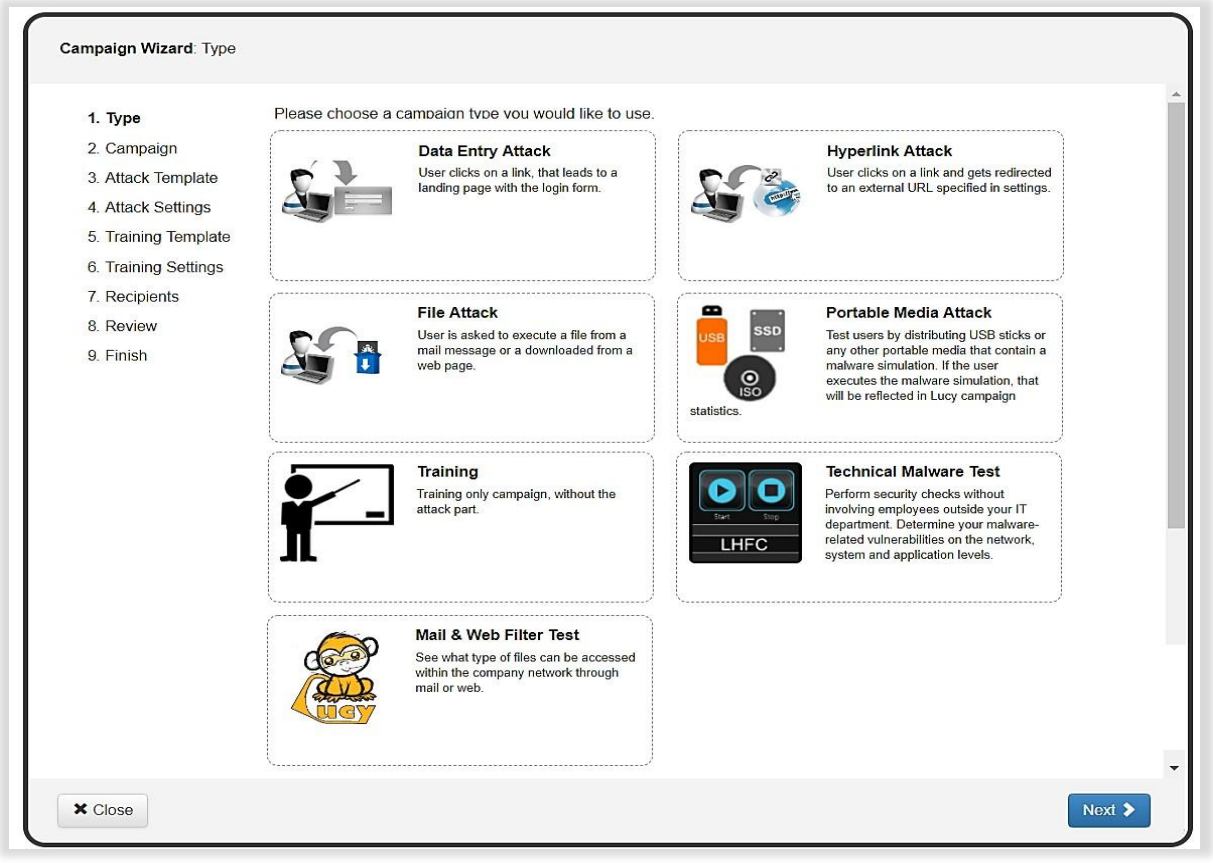
- **Compatibilidad multi-cliente:** Los «clientes» pueden referirse a diferentes empresas, departamentos o grupos que tengan una campaña asociada en LUCY. Estos clientes pueden utilizarse, por ejemplo, para permitir el acceso específico a una campaña o para crear análisis específicos del cliente.



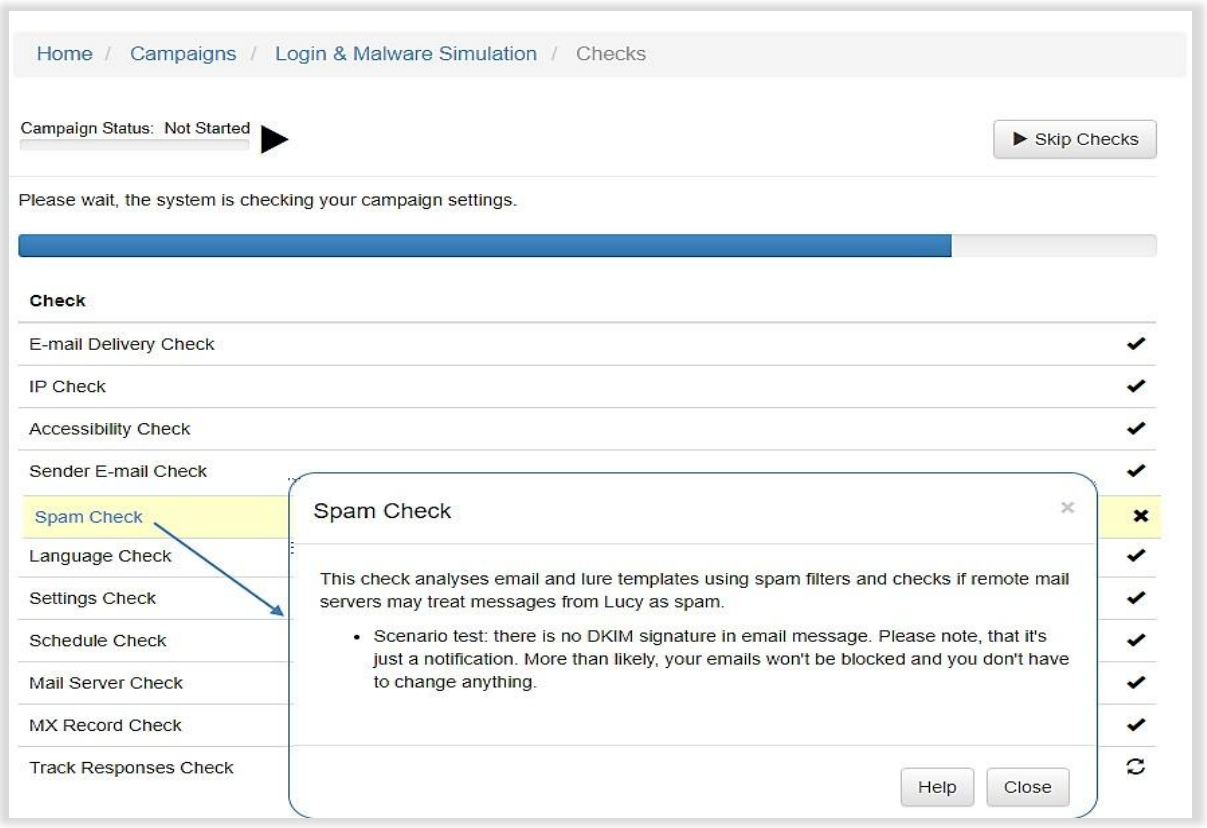
- **Plantillas de campañas:** En caso de que desee reutilizar campañas similares, puede guardar una campaña completa con plantillas de ataque y contenido de aprendizaje online como plantilla de campaña. Esta característica le permite evitar tener que repetir configuraciones similares una y otra vez.



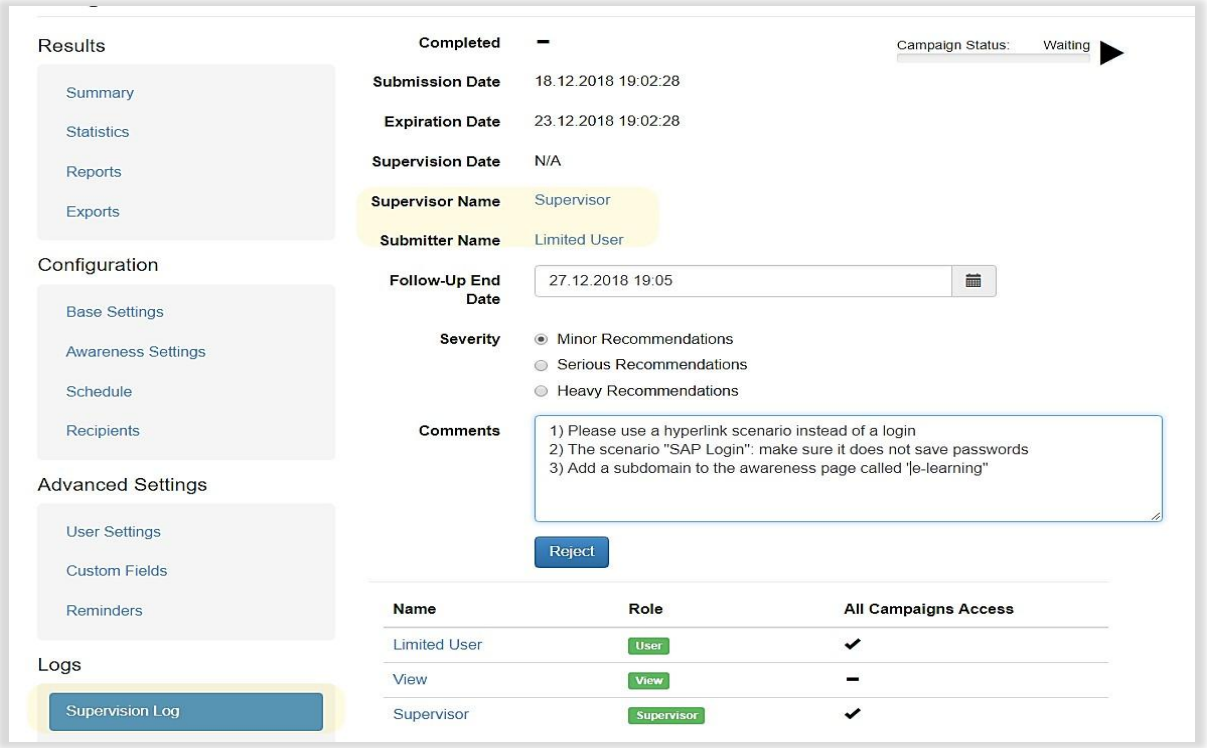
- **Asistente de configuración con orientación basada en el riesgo:** LUCY ofrece varias herramientas de configuración. Cree una campaña completa en menos de 3 minutos utilizando las plantillas de campaña predefinidas o deje que el asistente de configuración le guíe a través de la configuración. Opcionalmente, 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.



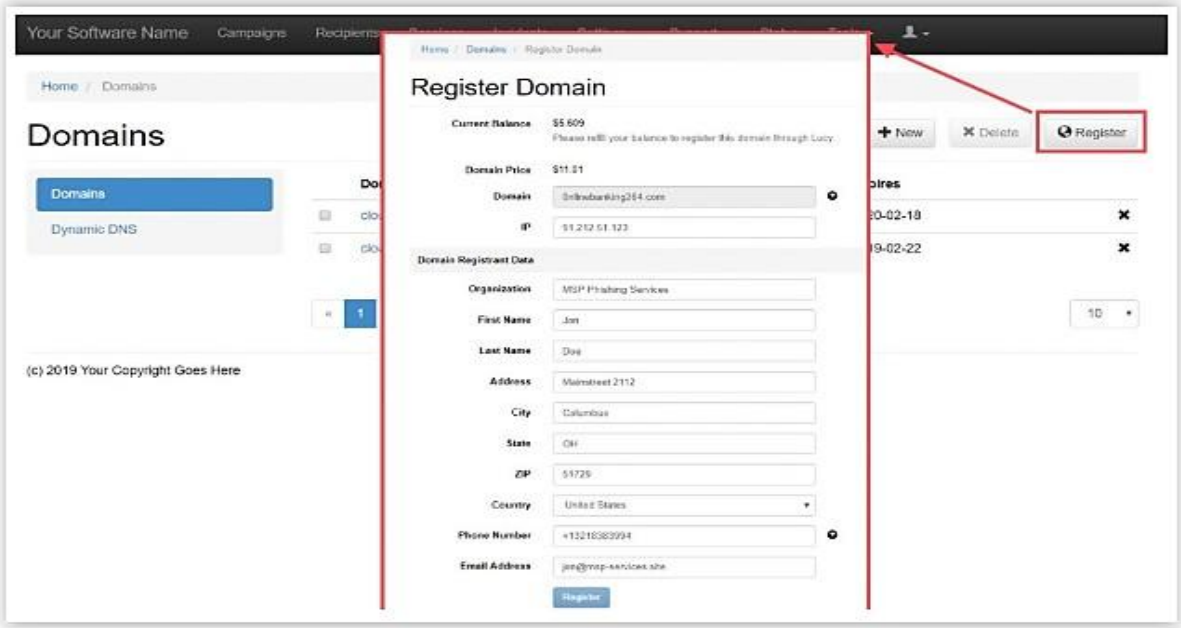
- **Verificaciones de campaña:** Controles preliminares antes de iniciar una campaña de LUCY: Comprobación de entrega de correo electrónico, comprobación del registro MX, comprobación de programación, comprobación de spam y otros.



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

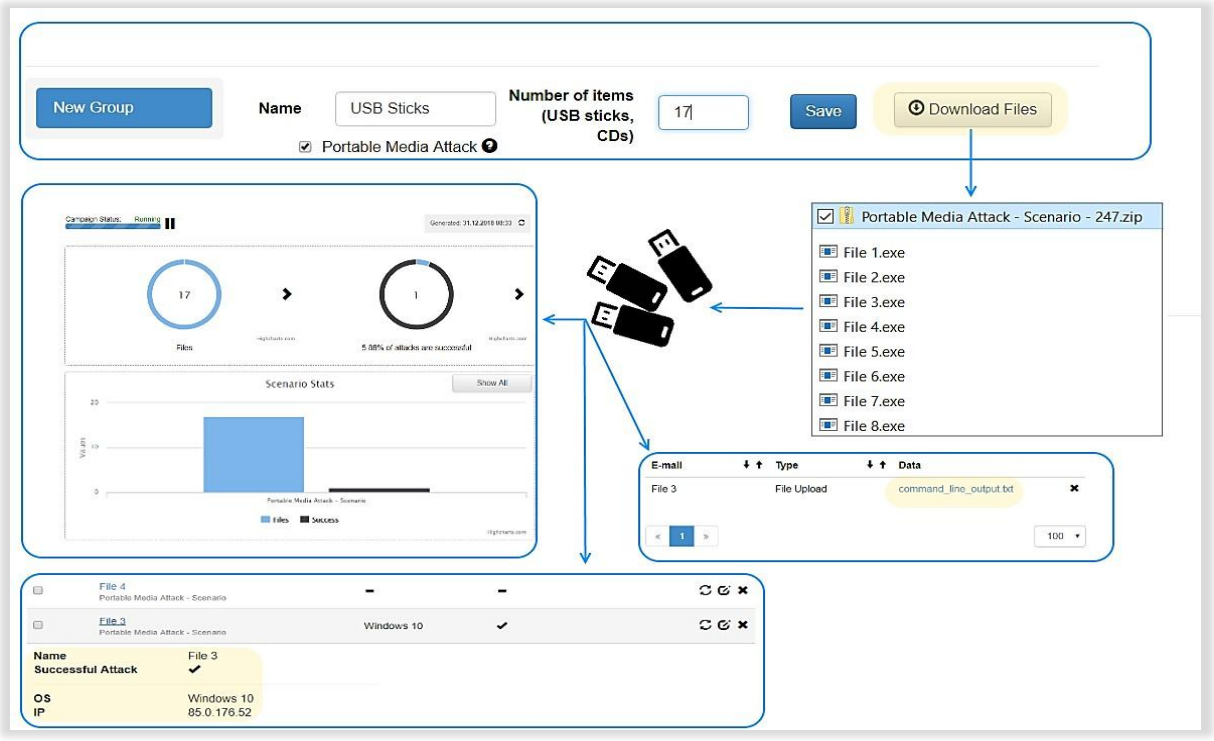


- **API de DNS:** La API de DNS permite al administrador crear cualquier dominio en LUCY en cuestión de segundos. Dado que los atacantes suelen utilizar dominios con palabras similares de los clientes (lo que se conoce como typosquatting), este riesgo también puede representarse en LUCY. Si el dominio 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.

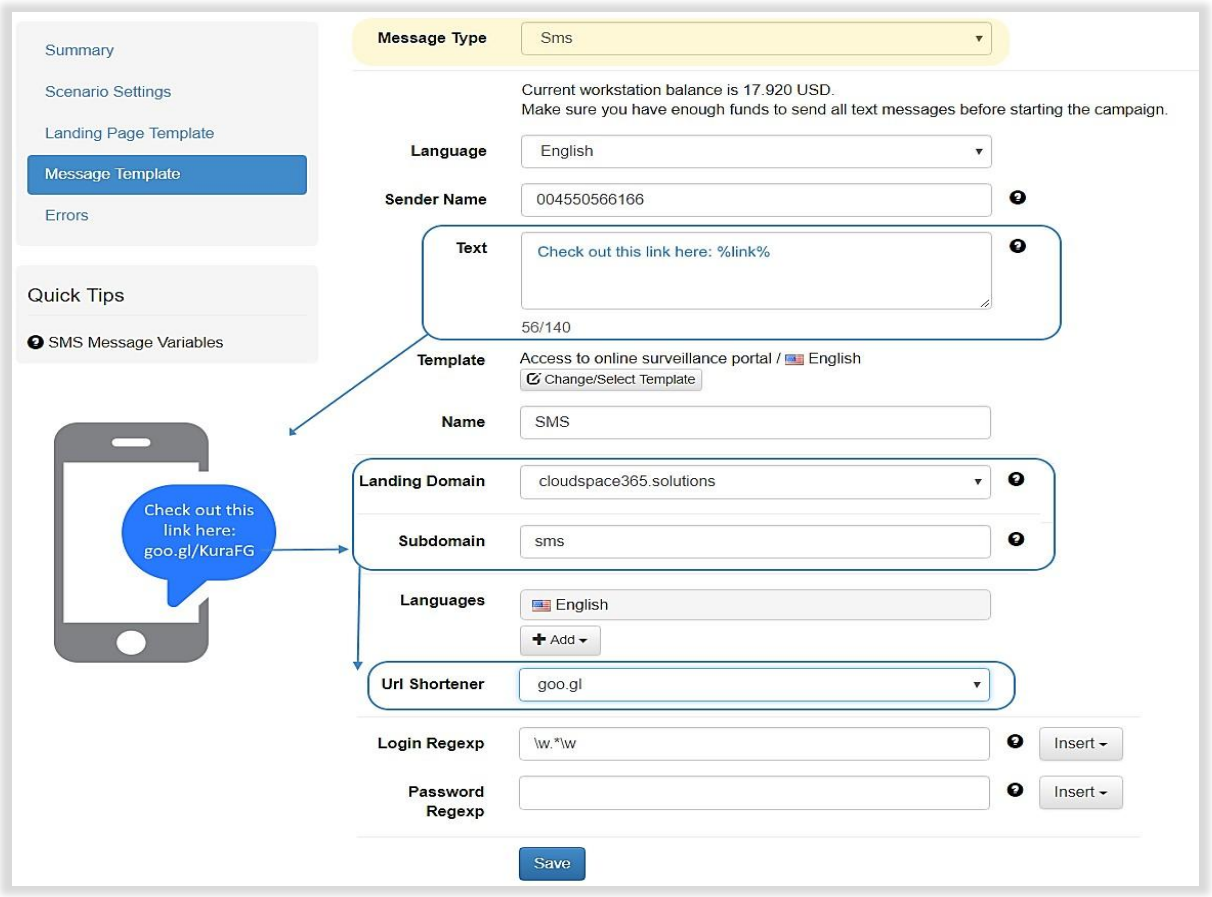


SIMULACIÓN DE ATAQUE

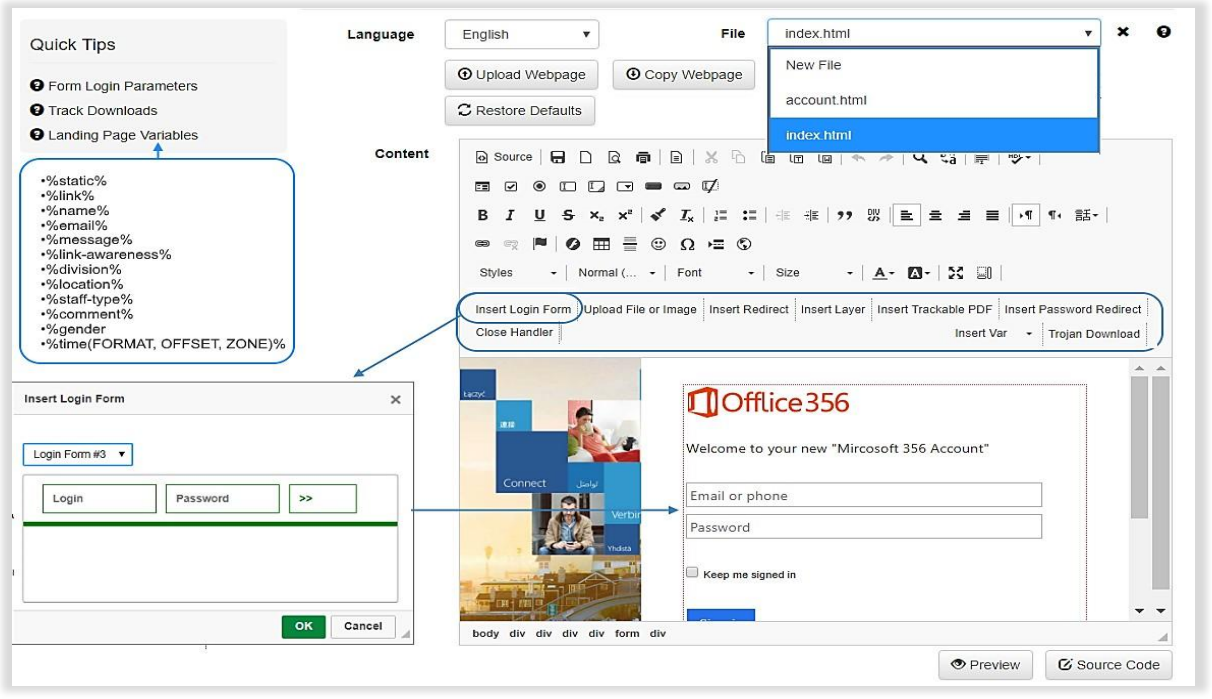
- **Ataques de medios portátiles:** Los hackers pueden utilizar unidades de medios portátiles para acceder a información confidencial almacenada en un ordenador o en una red. LUCY ofrece la opción de realizar ataques de medios portátiles en los que se puede guardar una plantilla de archivo (p. ej., ejecutable, 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.



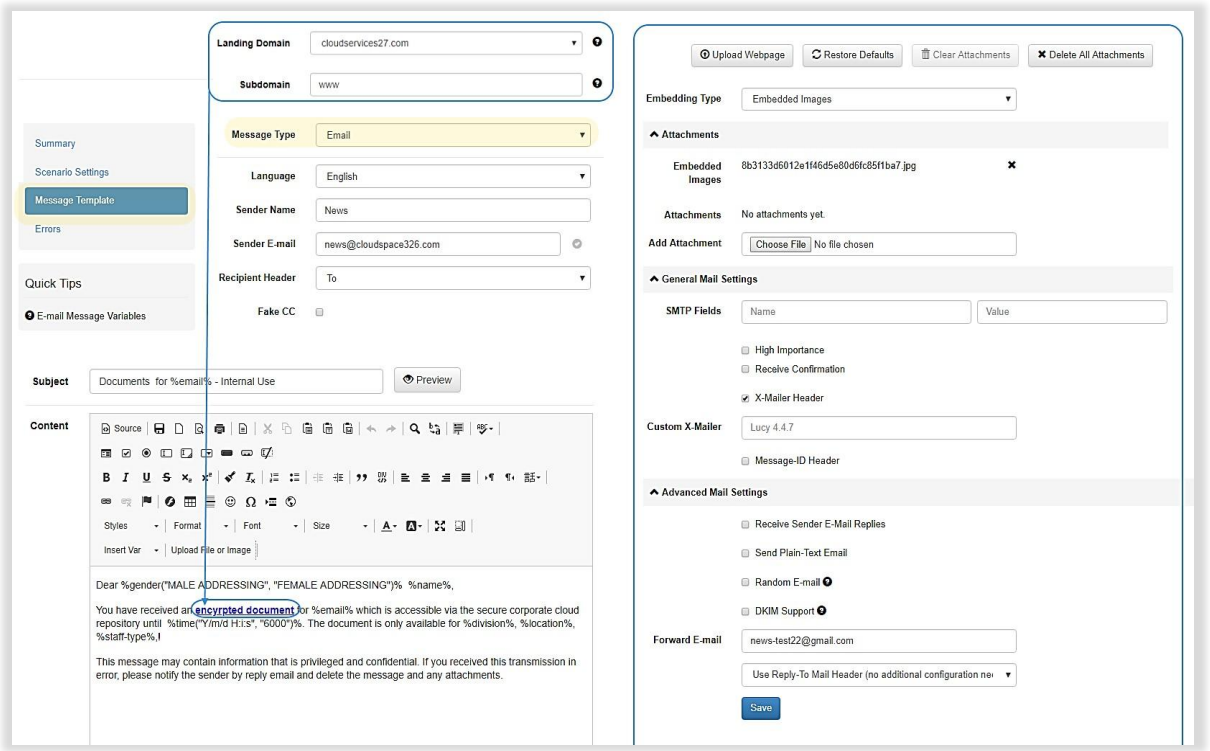
- **SMiShing:** SMiShing es, en cierto sentido, «phishing por SMS». Cuando los delincuentes cibernéticos «hacen phishing», envían correos electrónicos fraudulentos que intentan engañar al destinatario para que abra un archivo adjunto cargado de malware o haga clic en un enlace malicioso. El SMiShing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



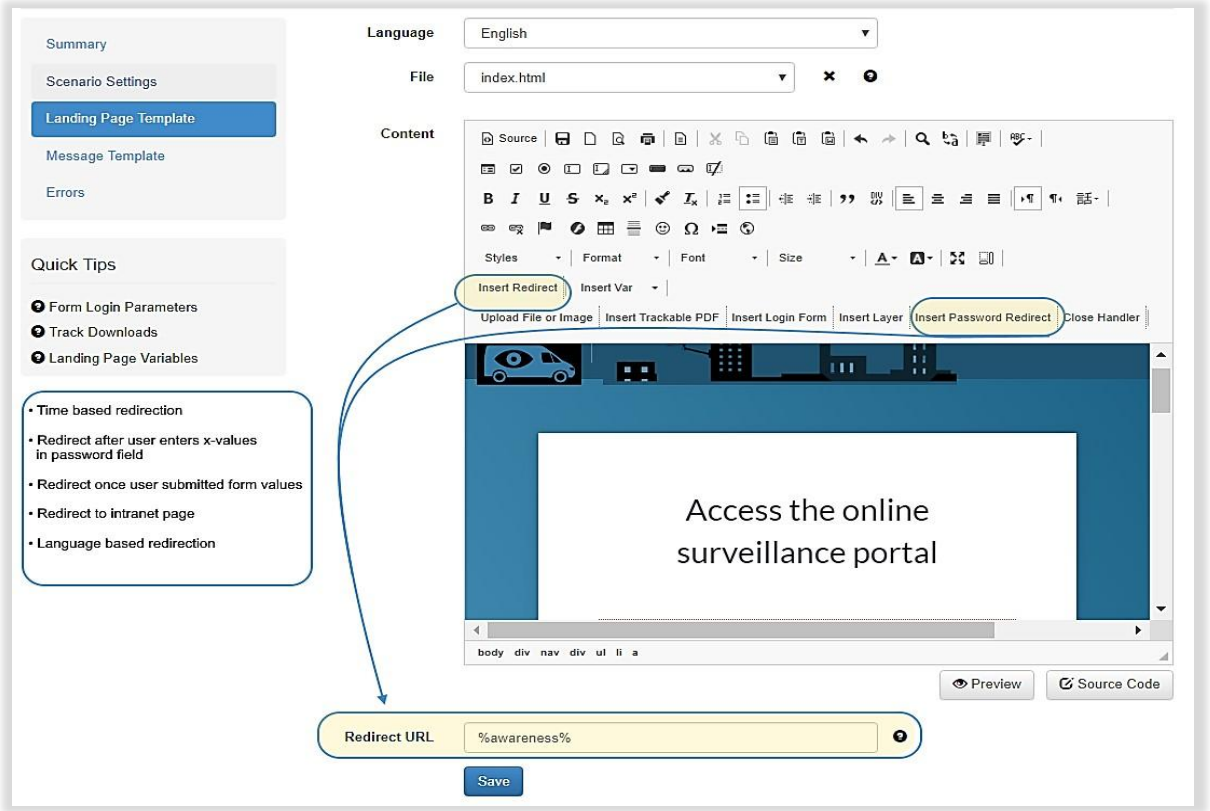
- **Ataques de entrada de datos:** Los ataques de entradas de datos pueden incluir una o más páginas web que interceptan la entrada de información sensible. Las páginas web disponibles se pueden personalizar fácilmente con un editor web de LUCY. Las herramientas de edición adicionales le permiten configurar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



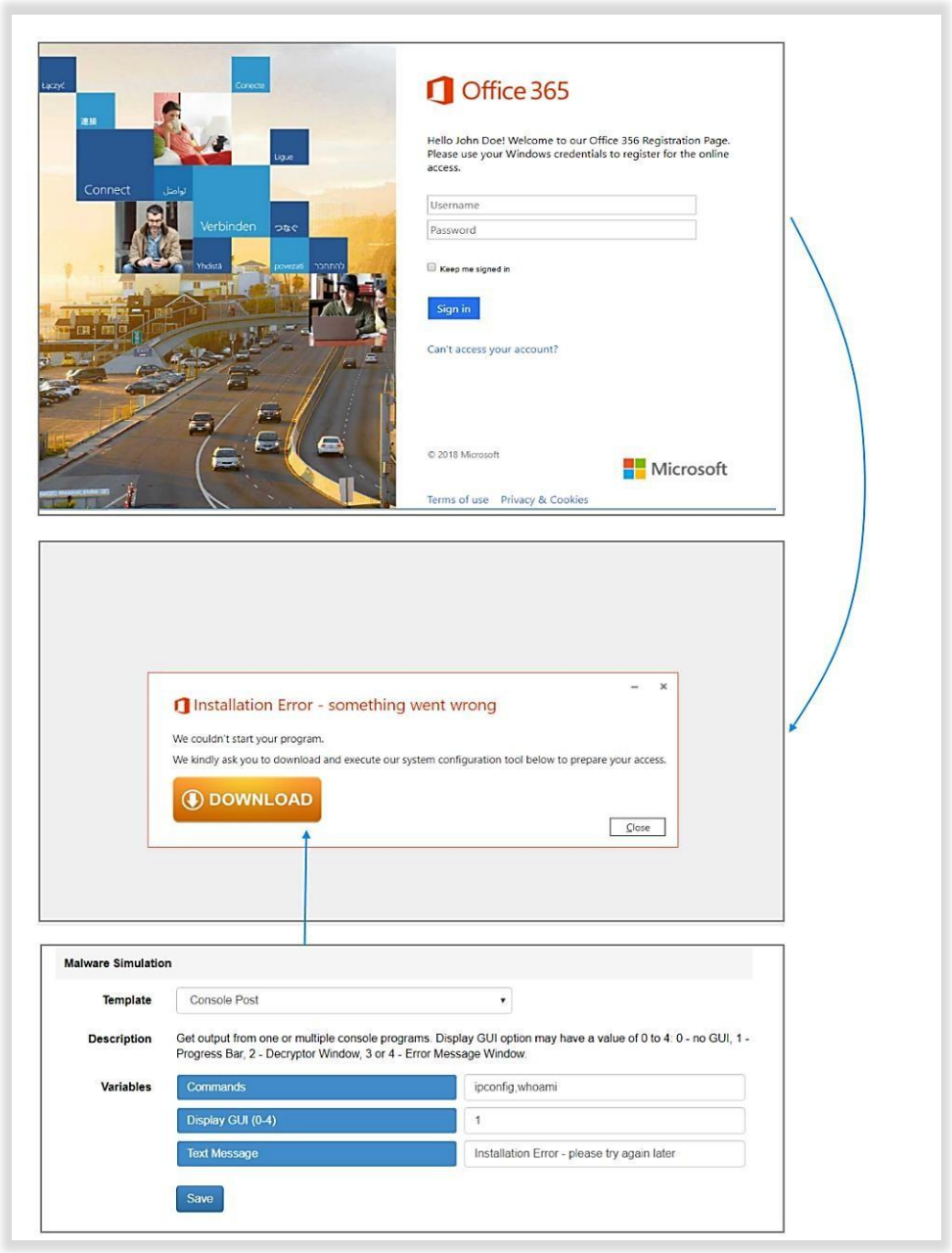
- **Ataques de hipervínculos:** Una campaña basada en hipervínculos enviará a los usuarios un correo electrónico que contiene una URL de seguimiento aleatoria.



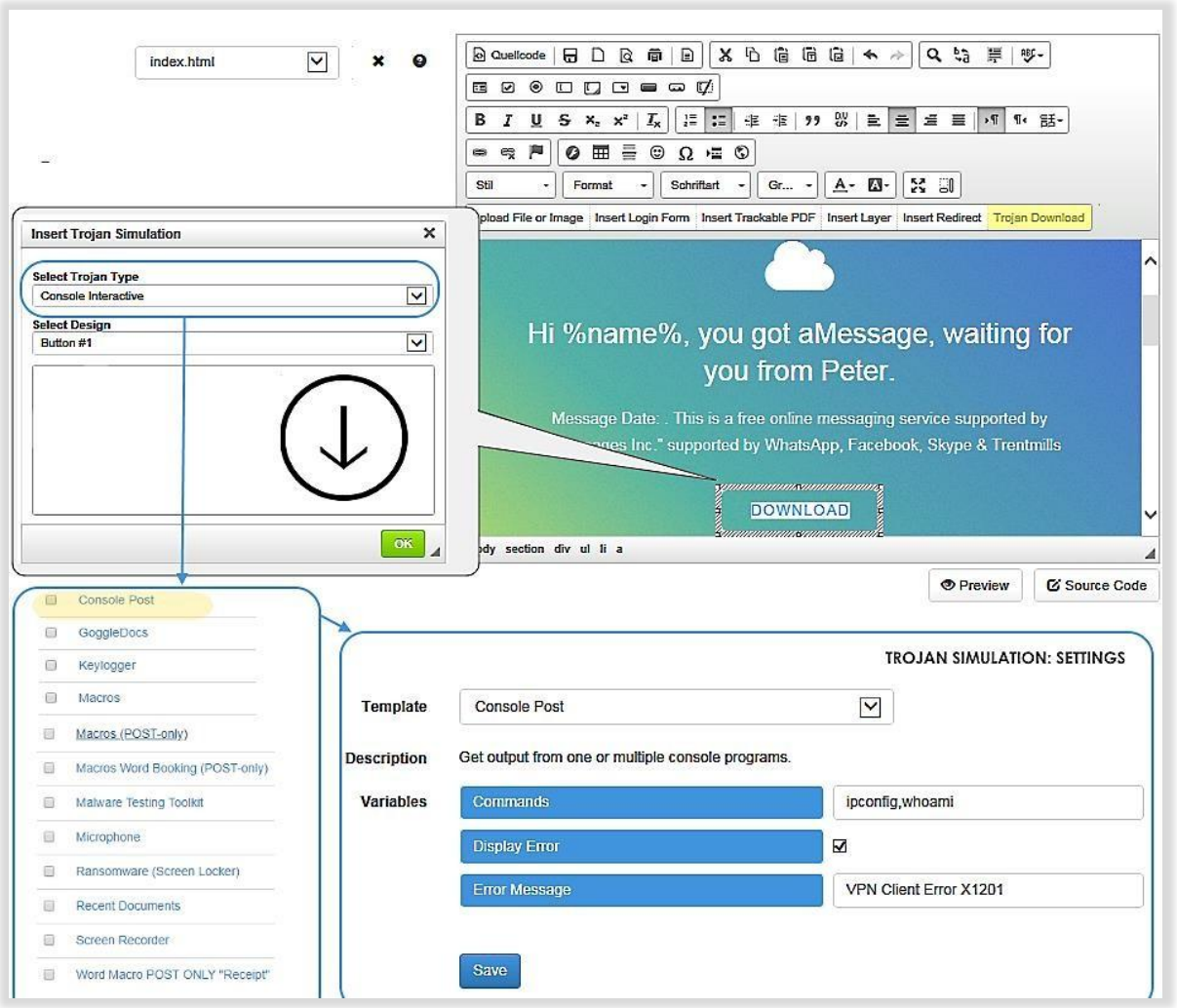
- **Potente kit de herramientas para la redirección de URLs:** Las flexibles funciones de redireccionamiento de LUCY permiten al usuario ser guiado en el momento adecuado a las áreas deseadas de simulación de ataques o entrenamiento. Por ejemplo, después de introducir los 3 primeros caracteres de una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



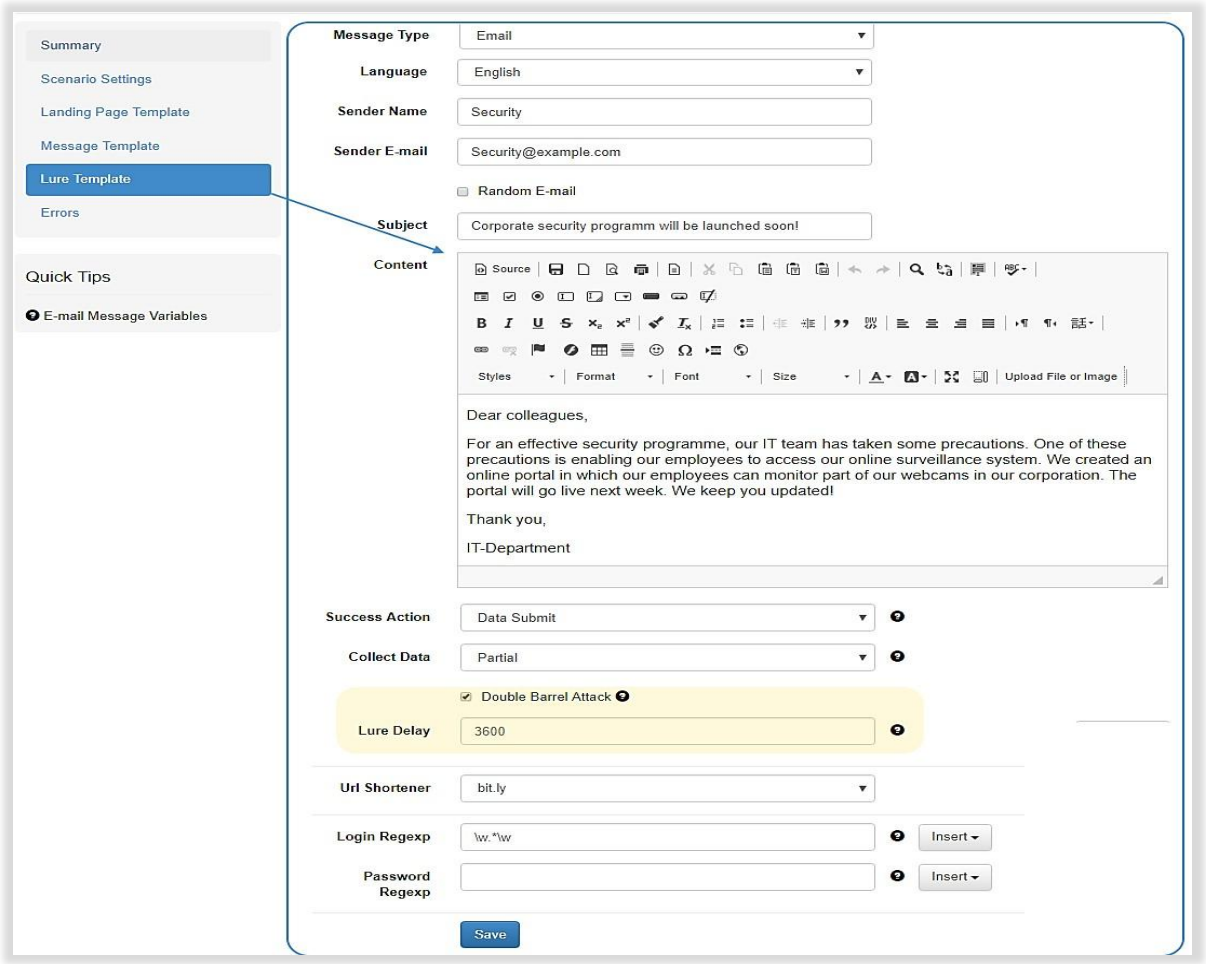
- **Ataques mixtos:** Los ataques mixtos permiten una combinación de múltiples tipos de escenarios (basado en archivos, entrada de datos, etc.) en la misma campaña.



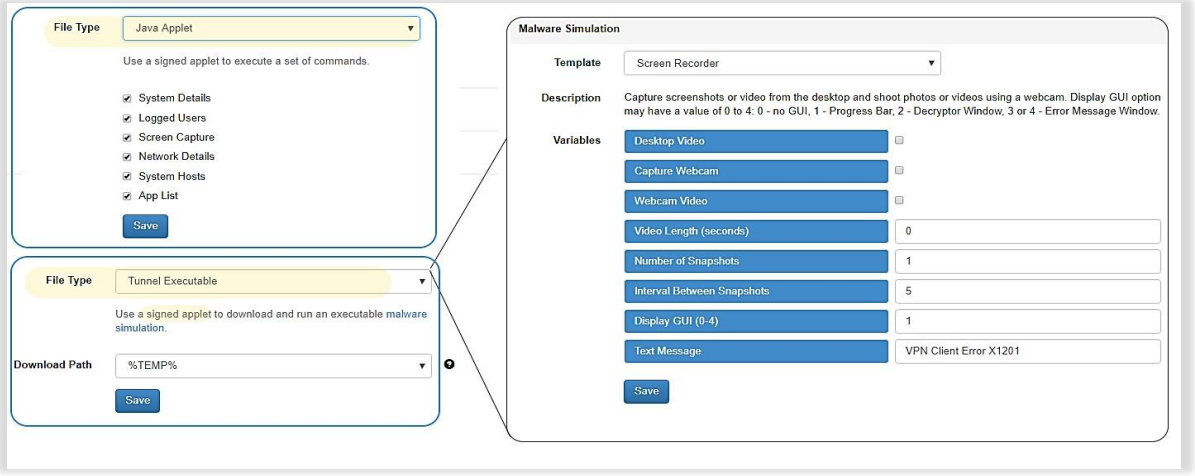
- **Ataques basados en archivos:** Los ataques basados en archivos permiten al administrador de LUCY integrar diferentes tipos de archivos (documentos de oficina con macros, PDF, ejecutables, MP3, etc.) en adjuntos de correo o sitios web generados en LUCY y medir su tasa de descarga o ejecución.



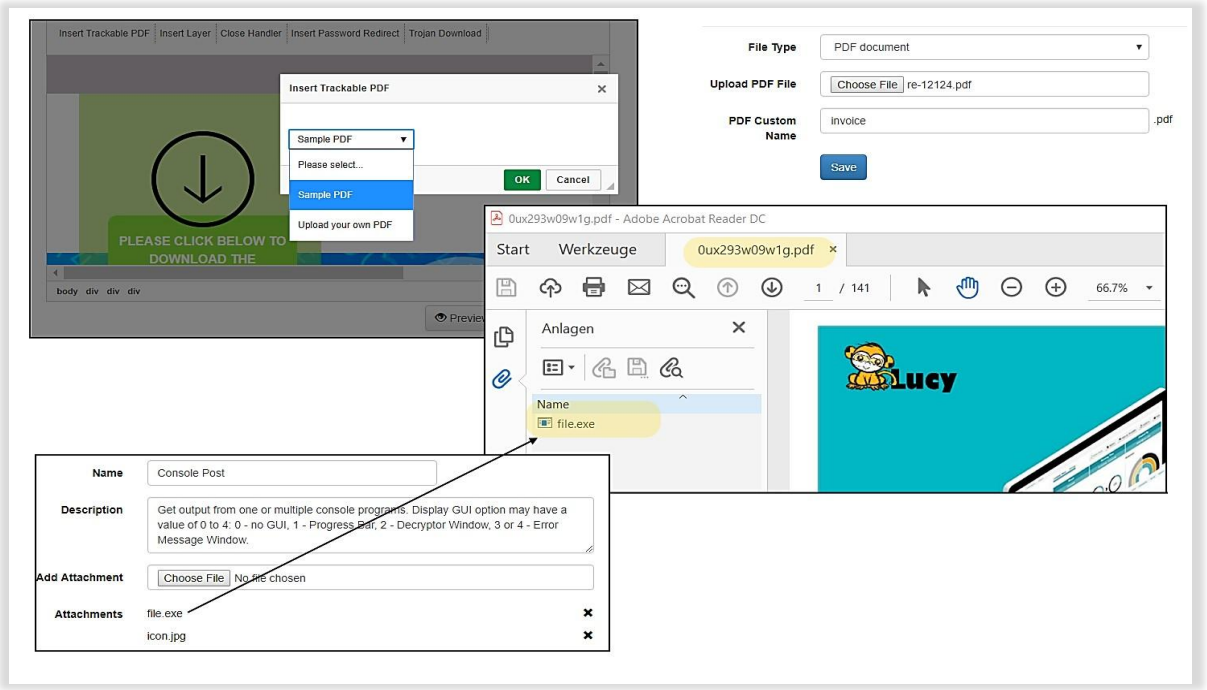
- **Ataques Double Barrel:** Esta función permite enviar varios correos electrónicos de phishing en cada campaña, con un primer correo electrónico benigno (el cebo) que no contiene nada malicioso y no exige una respuesta del destinatario.



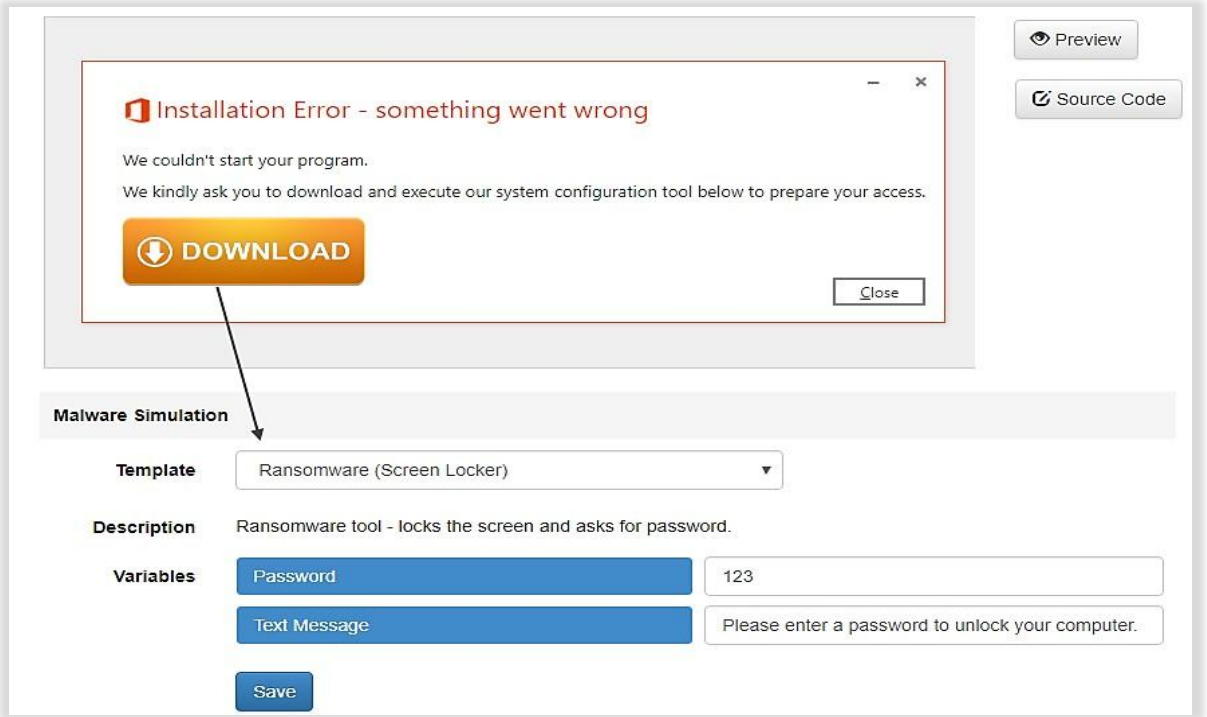
- **Ataques basados en Java:** Los ataques basados en Java permiten al administrador de LUCY integrar un applet de confianza dentro de las plantillas de ataque basadas en archivos o mixtas proporcionadas en LUCY y medir su ejecución por el usuario.



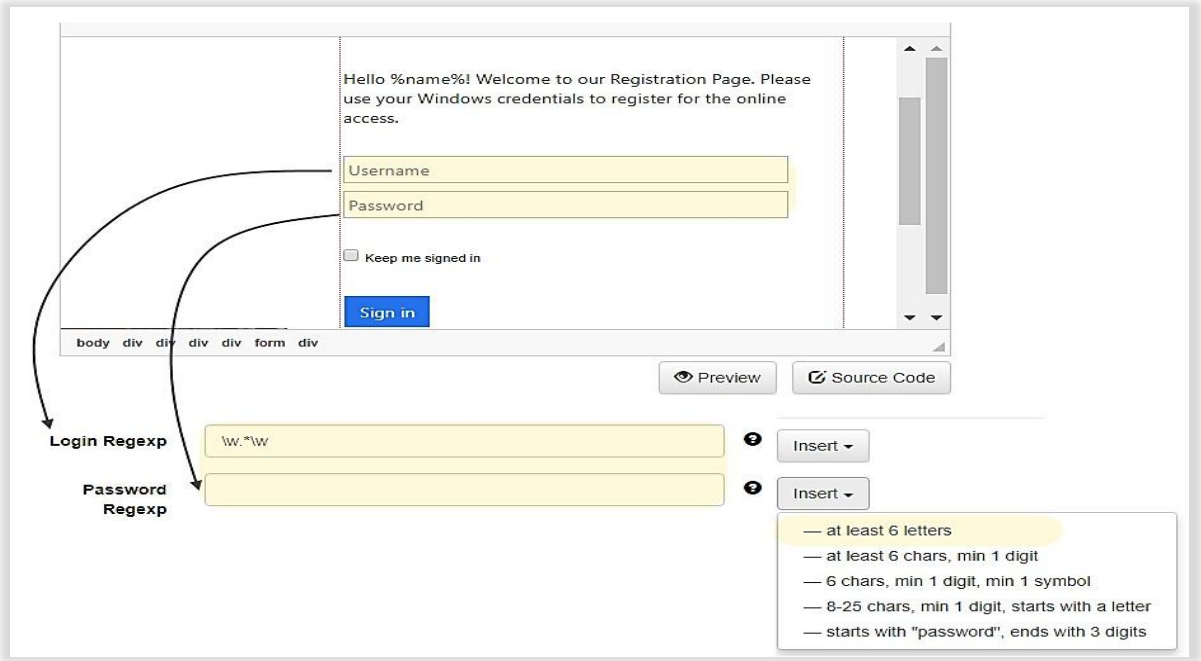
- **Ataques basados en PDF:** Los ataques de phishing basados en PDF pueden simularse con este módulo. LUCY permite «ocultar» archivos ejecutables en archivos adjuntos PDF y medir su ejecución. Además, también se pueden generar enlaces dinámicos de phishing dentro de los PDF.



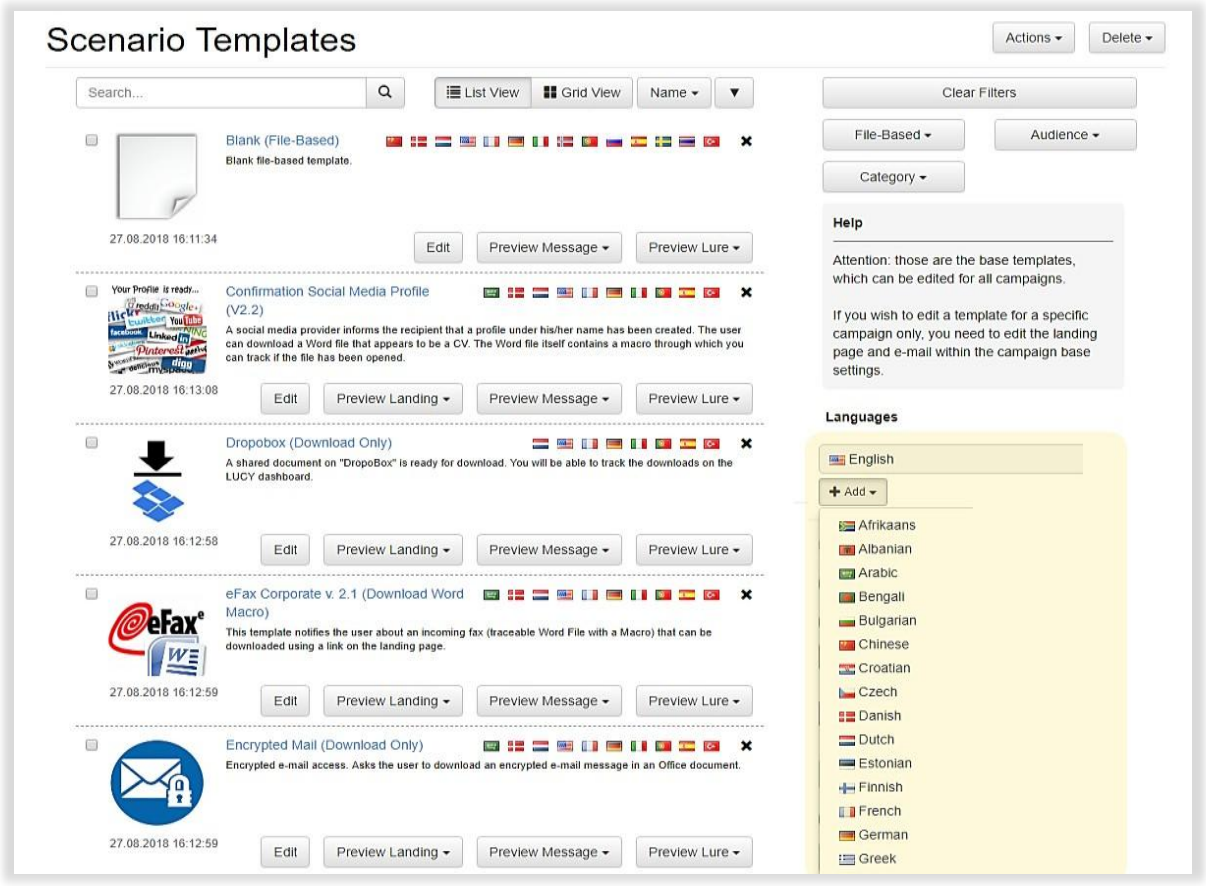
- **Ataques de simulación de ransomware:** LUCY tiene dos simulaciones de ransomware diferentes, una de las cuales prueba al personal y la otra, la infraestructura.



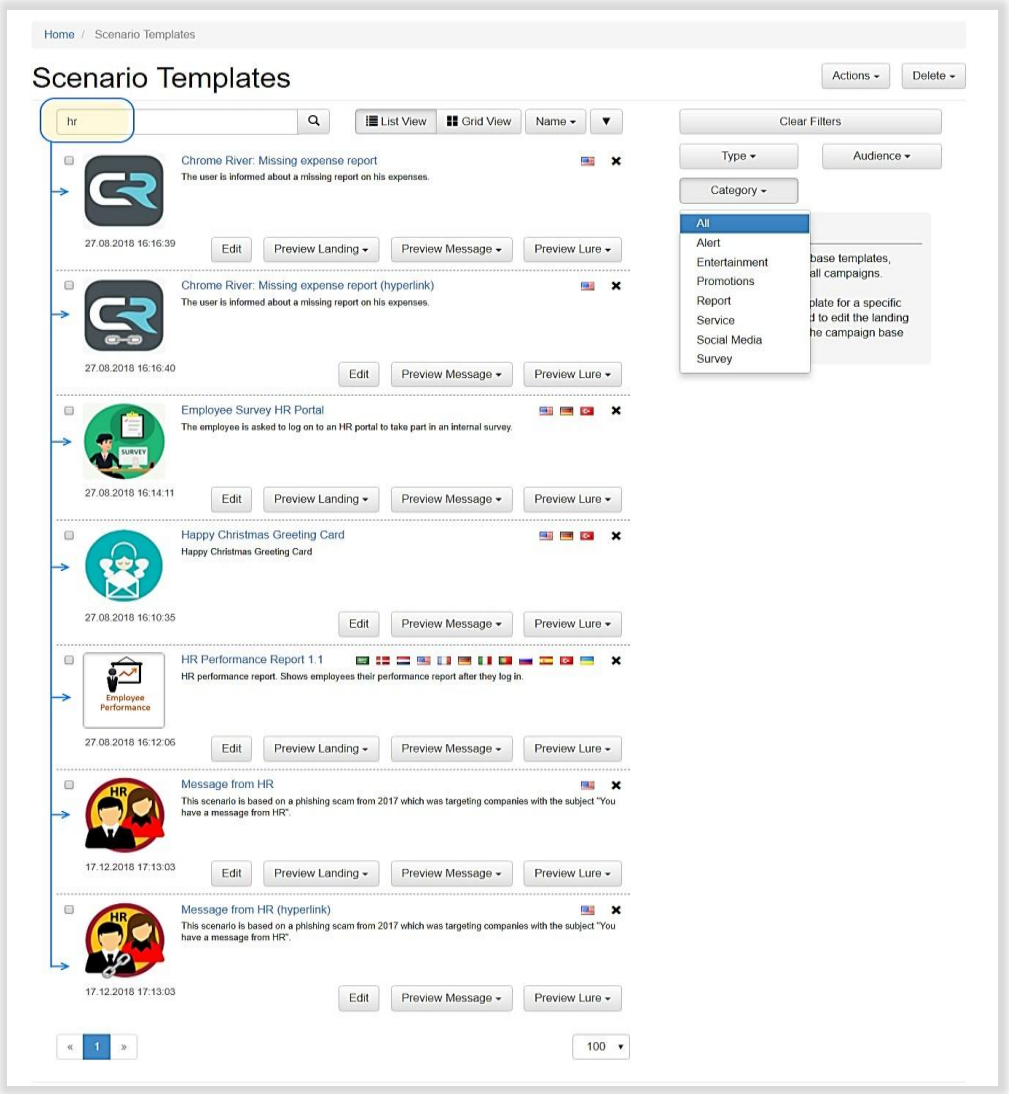
- **Kit de herramientas de validación de entrada de datos:** En las simulaciones de phishing, se deben evitar los falsos positivos en los campos de inicio de sesión (p. ej., el registro con sintaxis no válida). Las directrices de la empresa también pueden prohibir la transmisión de datos sensibles como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



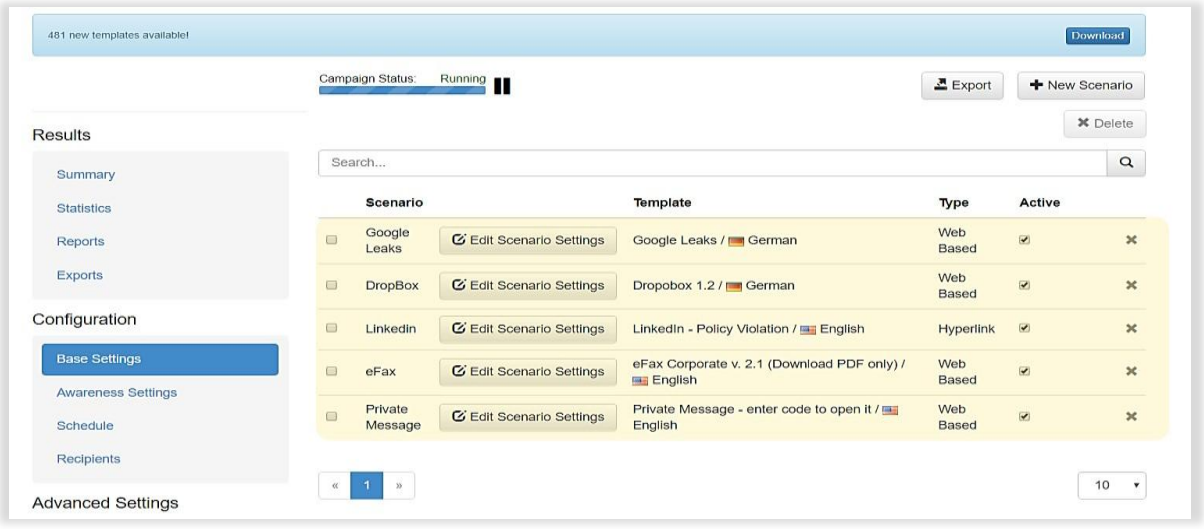
- **Biblioteca de plantillas de ataque multilingüe:** LUCY viene con cientos de plantillas de ataque predefinidas en más de 30 idiomas en las categorías de entrada de datos (plantillas con un sitio web), basadas en archivos (correos electrónicos o sitios web con descarga de archivos), hipervínculos (correos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



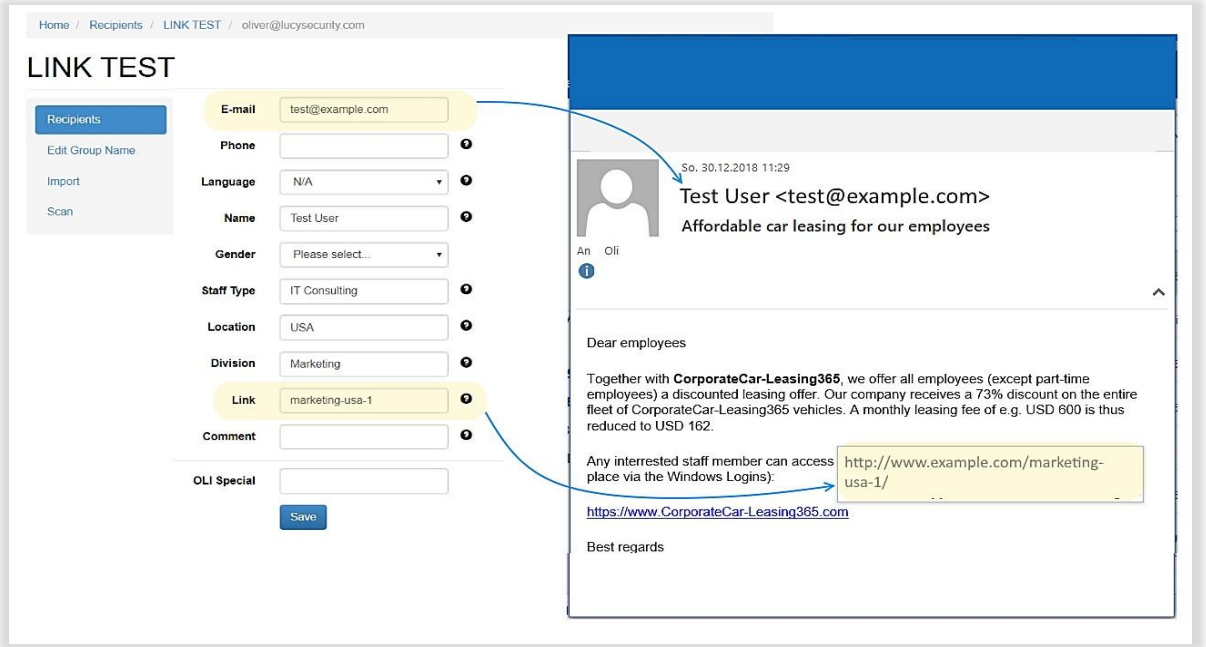
- **Plantillas específicas de industrias y divisiones:** Las plantillas de ataque están disponibles para industrias o divisiones específicas.



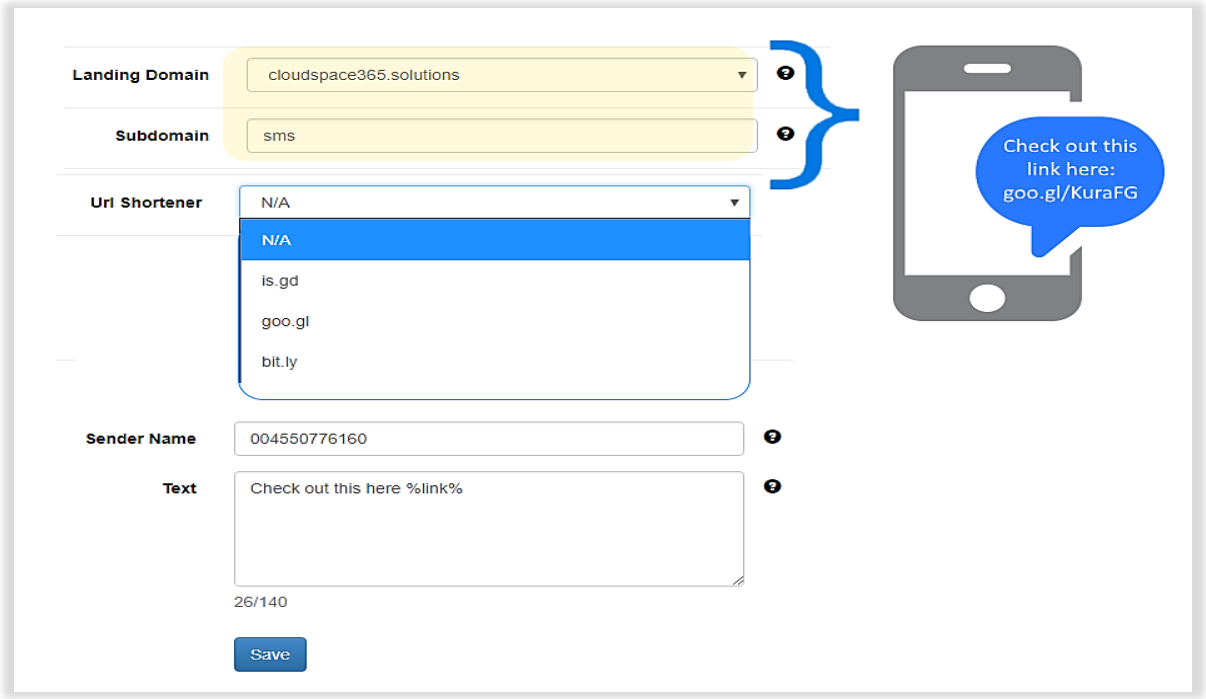
- **Uso simultáneo de plantillas de ataque:** LUCY le ofrece la opción de utilizar varias plantillas de ataque simulado en una sola campaña. Mezcle los diferentes tipos (hipervínculos, basados en archivos, etc.) con diferentes temas de ataque para lograr la mayor cobertura de riesgos posible y una mejor 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.



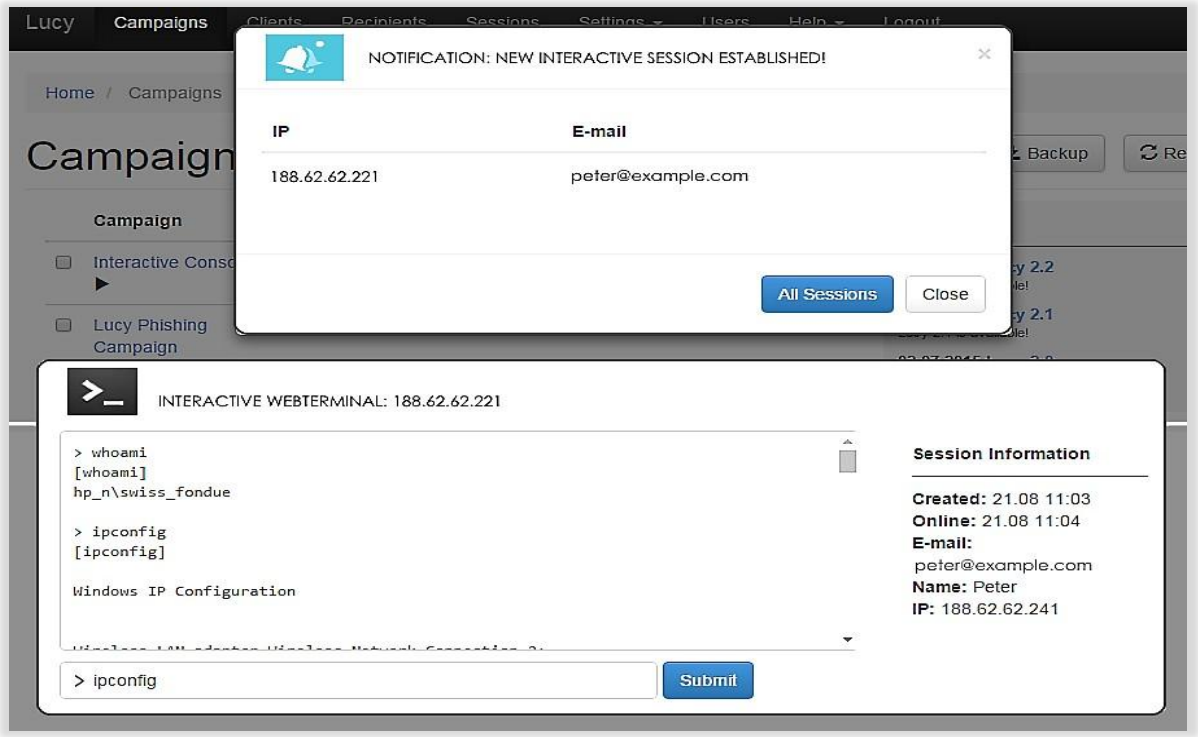
- **Variaciones de URL de ataque:** Tome el control de las URL generadas para identificar a los destinatarios. Utilice cadenas de URL cortas (<5 caracteres) o largas automatizadas o establezca URLs individuales para cada usuario. La creación manual de URL le permite formar enlaces que un usuario puede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



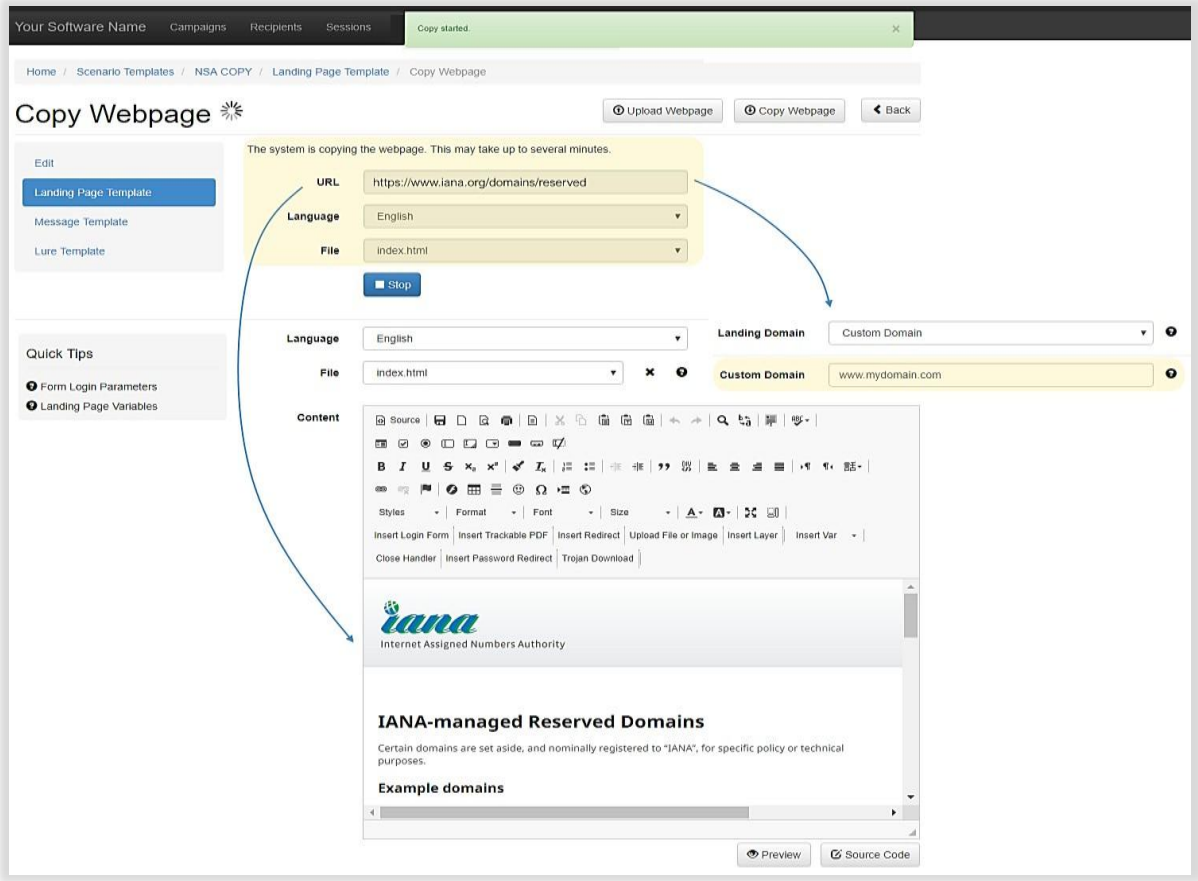
- **Acortador de URL:** Los acortadores de URL son un servicio de Internet relativamente nuevo. Como muchos servicios sociales en línea imponen limitaciones de caracteres (p. ej., Twitter), estas URL son muy prácticas. Sin embargo, los delincuentes cibernéticos pueden utilizar los acortadores de URL 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.



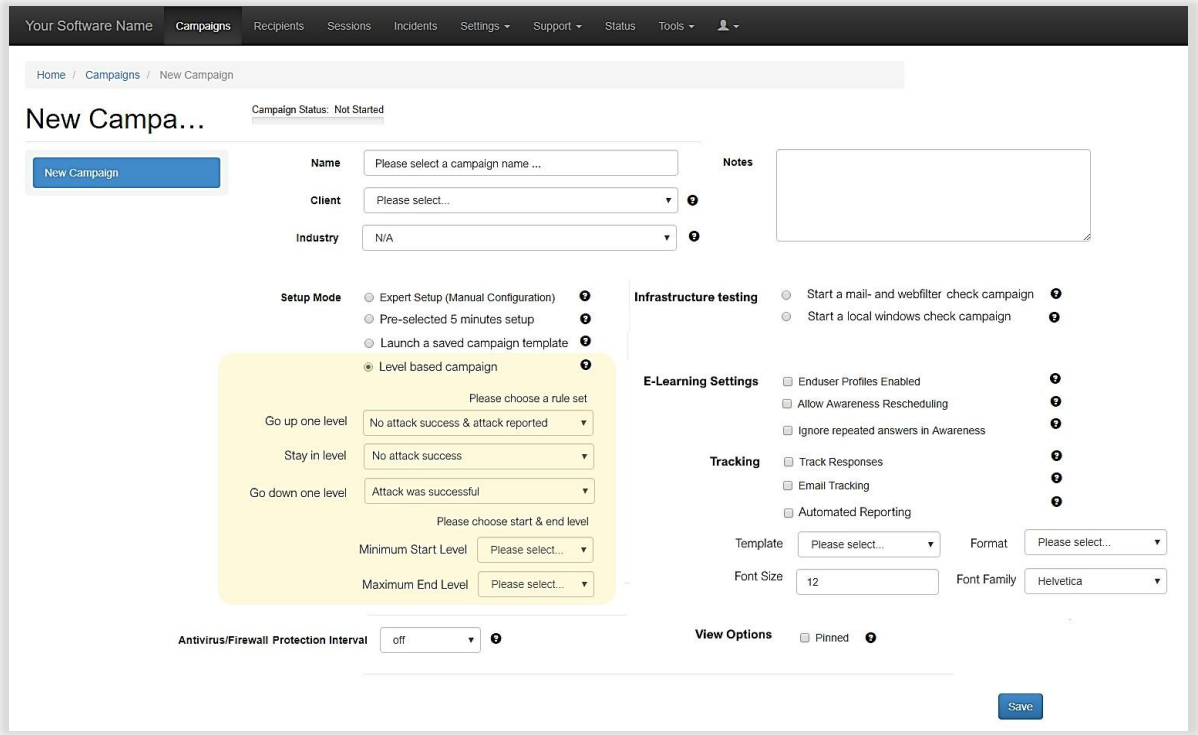
- **Kit de Pentest:** El kit de Pentest es un submódulo del kit de simulación de malware y se llama «Sesiones Interactivas». Le permite comunicarse interactivamente con un PC cliente que se encuentra detrás de cortafuegos usando conexiones http/s inversas.



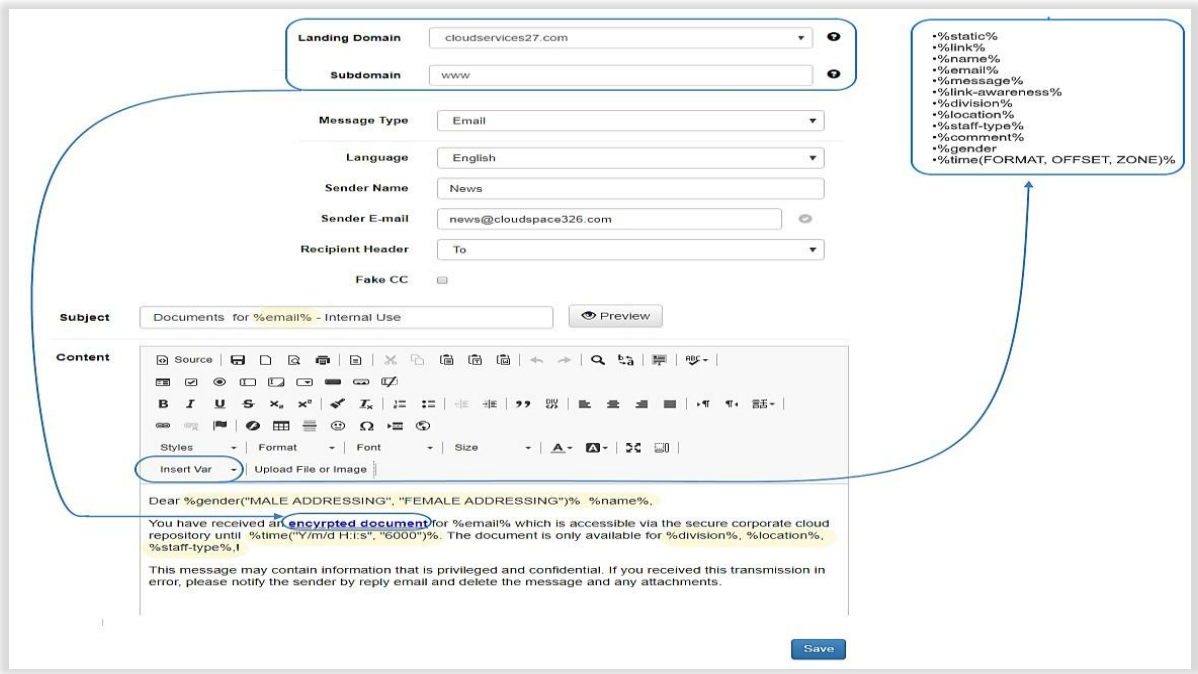
- **Clonación de sitios Web:** Cree rápidamente páginas de destino altamente profesionales para sus campañas. Clone sitios web existentes y añada capas adicionales con campos de entrada de datos, archivos para descargar y mucho más.



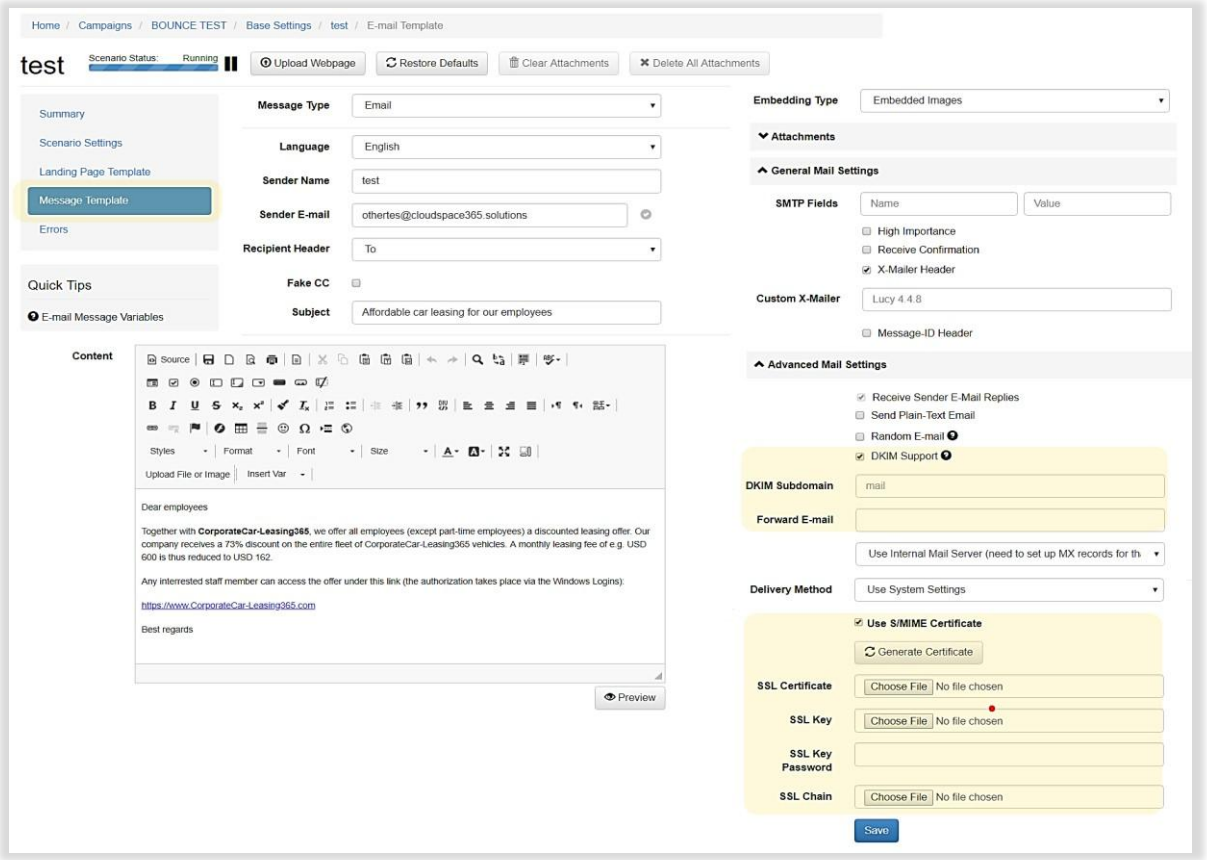
- **Ataques basados en niveles:** El entrenamiento de phishing para empleados se basa en niveles y sirve para medir el riesgo de hackeo con ingeniería social. El análisis científico también debería identificar los factores de riesgo más importantes para que el contenido formativo individual pueda ofrecerse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



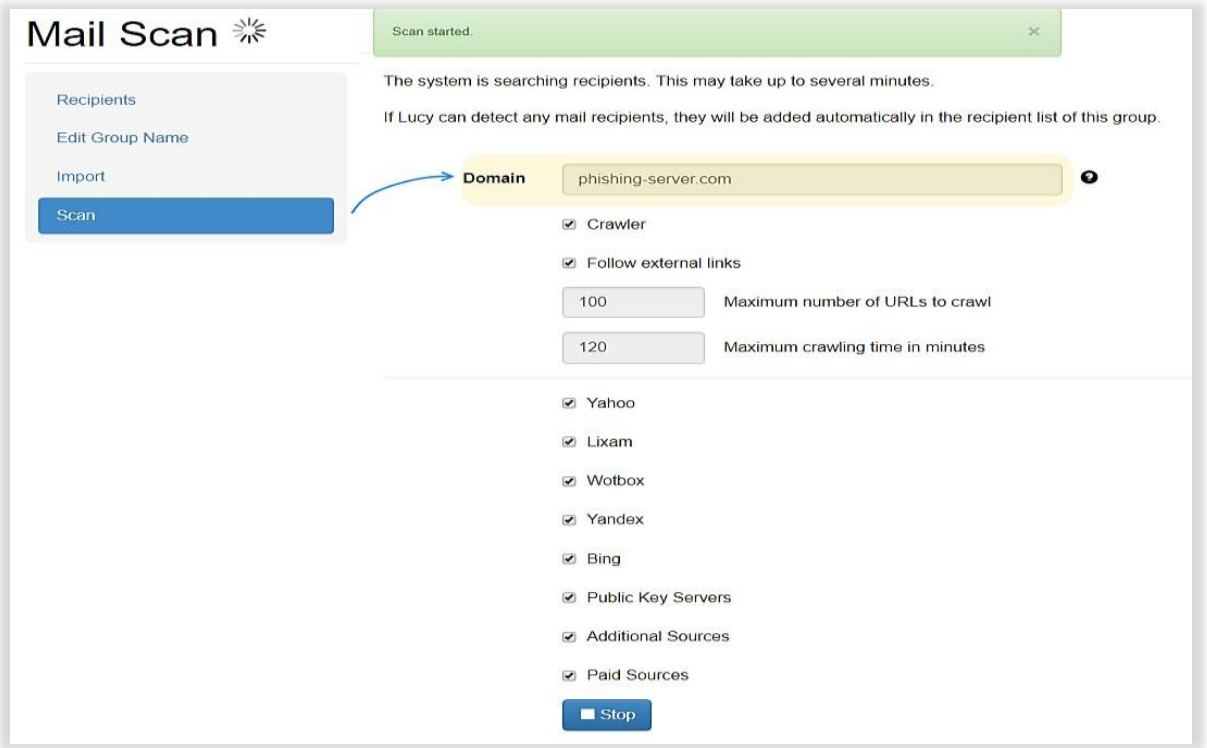
- **Simulación de Spear Phishing:** La personalización de Spear Phish funciona con variables dinámicas (género, hora, nombre, correo electrónico, enlaces, mensajes, división, país, etc.) que se pueden utilizar en plantillas de destino y de mensajes.



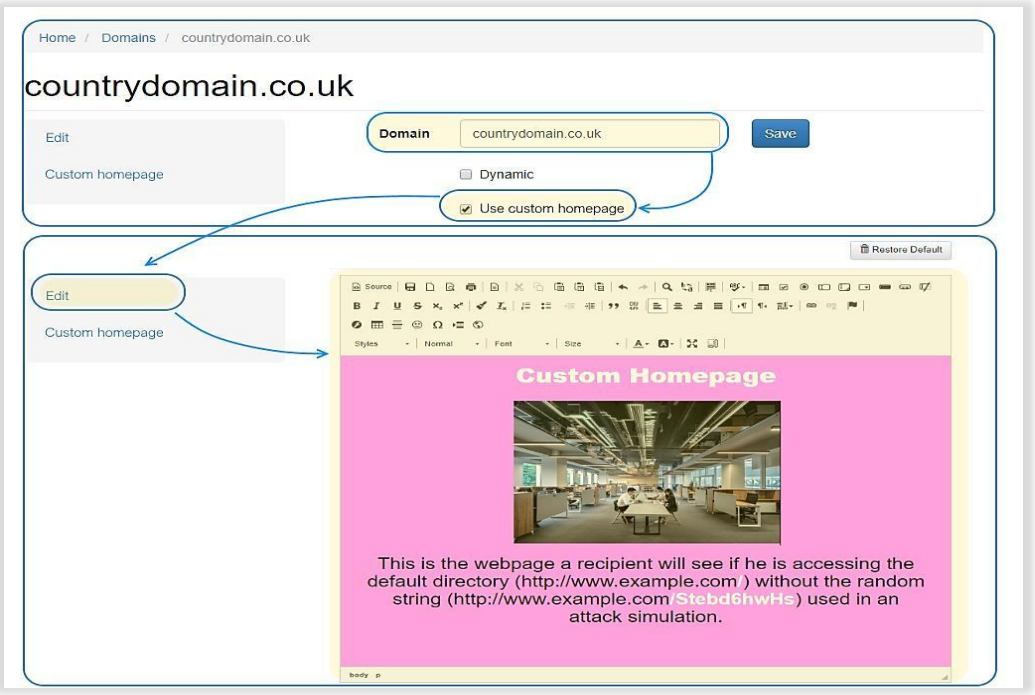
- **Soporte DKIM / S / MIME para los correos electrónicos de phishing:** Firmas digitales para correos electrónicos: Envíe correos de simulación de phishing firmados (s/mime). Utilice DKIM para obtener una mejor puntuación de remitente.



- **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.

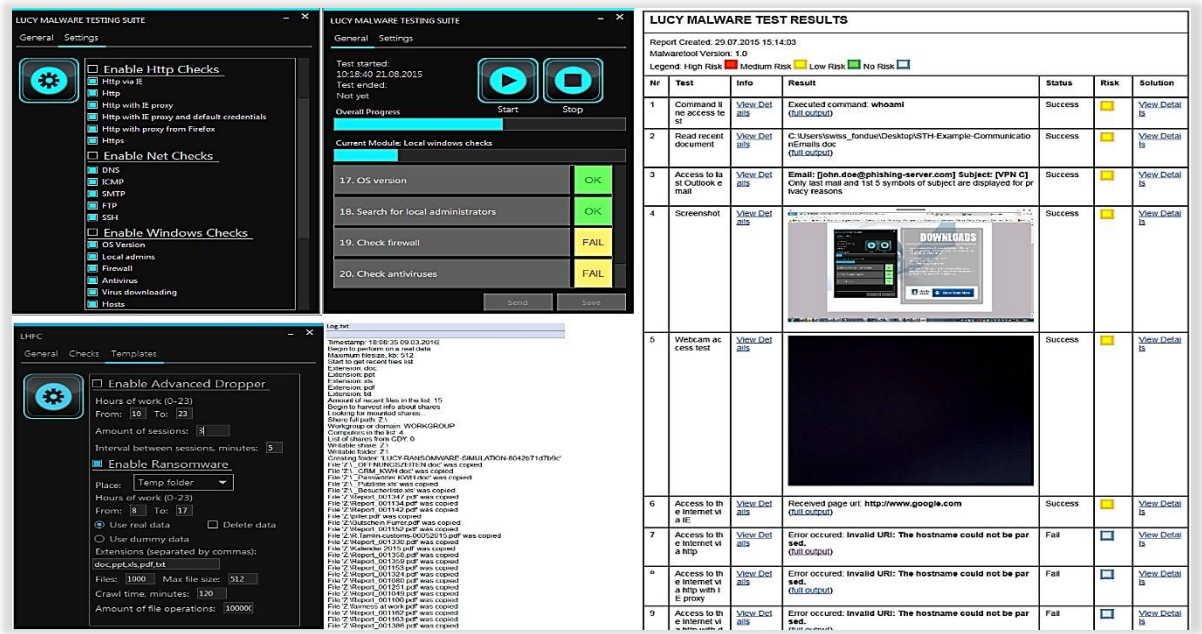


- **Creación de página de inicio personalizada:** Los destinatarios con una mejor comprensión técnica podrían utilizar su navegador para llamar al dominio o dirección IP asociados con el enlace del phishing generado de forma aleatoria. Para evitar que aparezcan mensajes de error o que el usuario final 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.

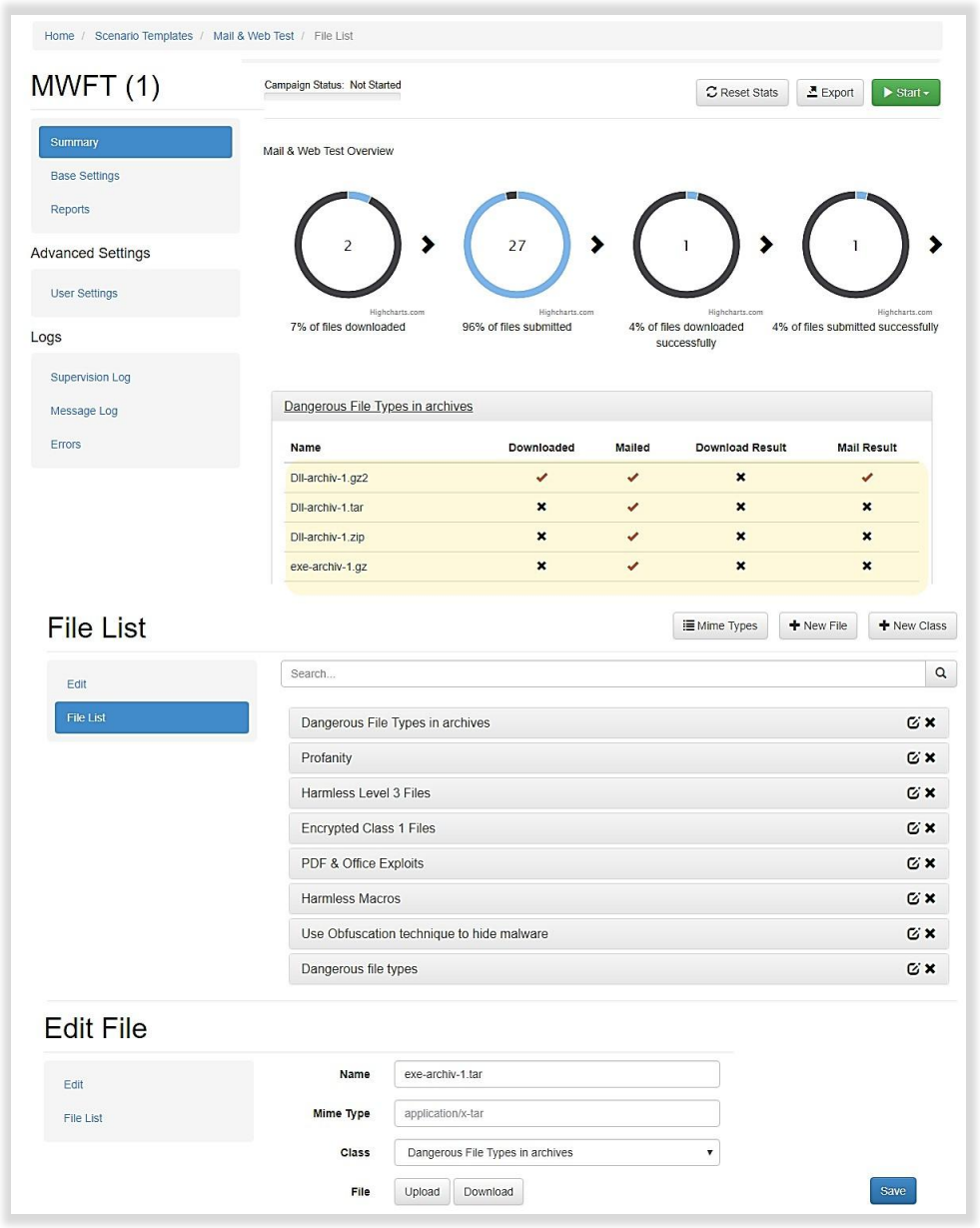


PRUEBE LA INFRAESTRUCTURA

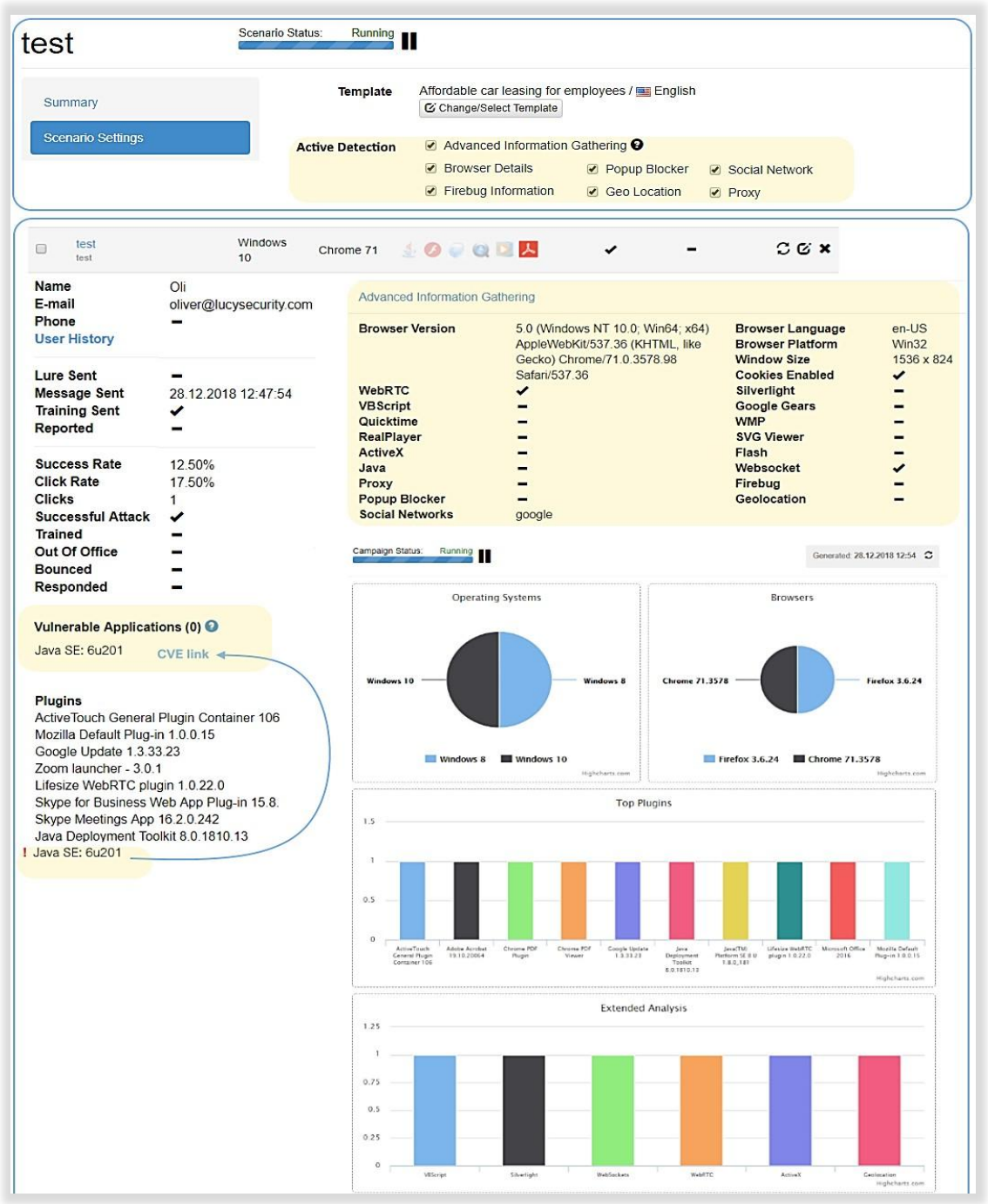
- **Kit de herramientas para pruebas de malware:** El kit de herramientas de simulación de malware es una suite de simulación de malware avanzada capaz de emular varias amenazas. Permite a un auditor acceder a un conjunto avanzado de funciones equivalentes a muchas de las herramientas empleadas por los 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.



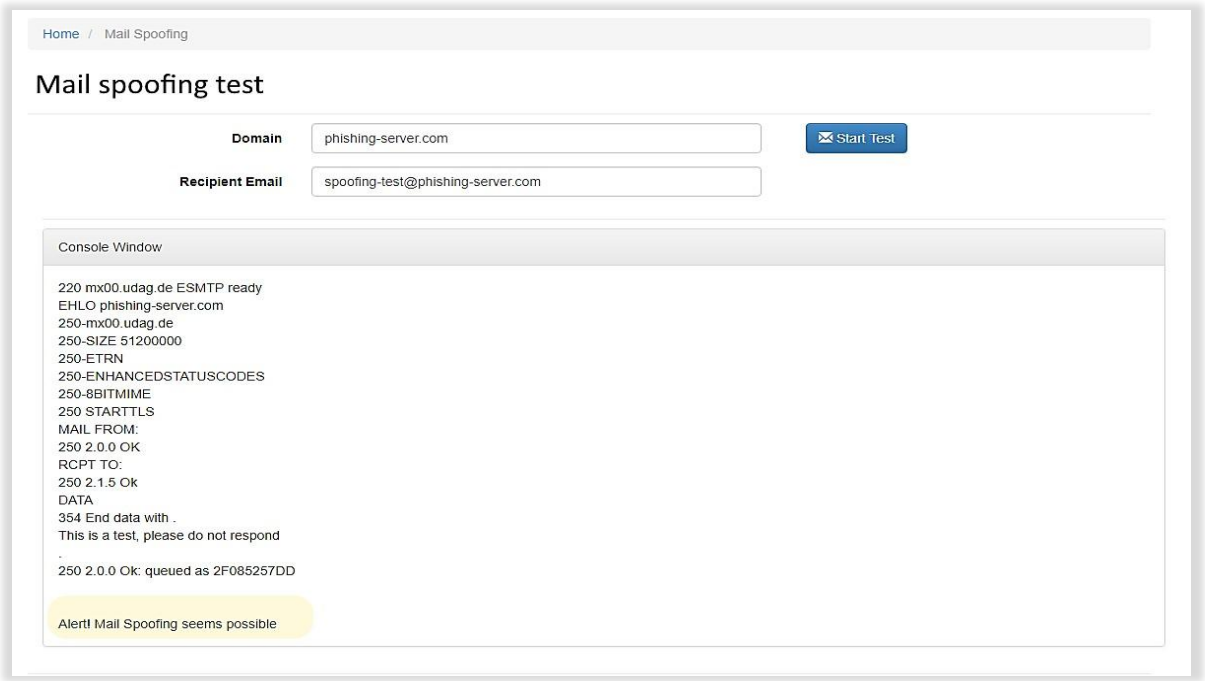
- **Prueba de filtro web y correo:** Esta funcionalidad proporciona la respuesta a una de las preguntas más importantes a la hora de proteger el tráfico de Internet y de correo: ¿Qué tipos de archivos se pueden descargar de la web y qué archivos adjuntos de correo electrónico se filtran o no?



- **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.

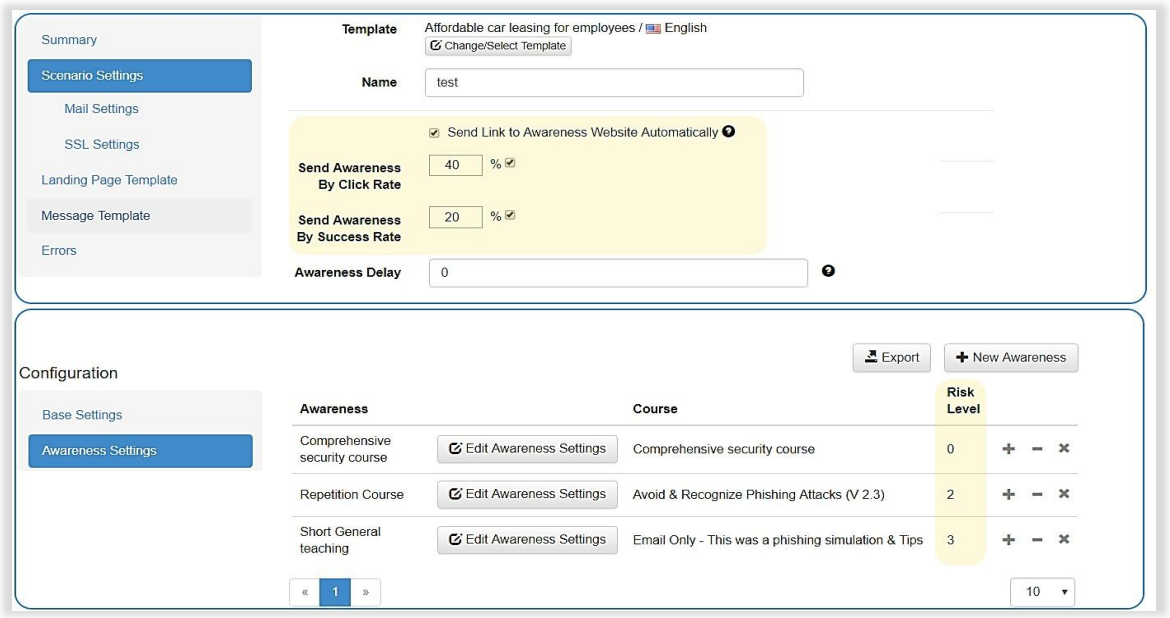


- **Prueba de spoofing:** Pruebe su propia infraestructura para detectar vulnerabilidades de spoofing de correo.

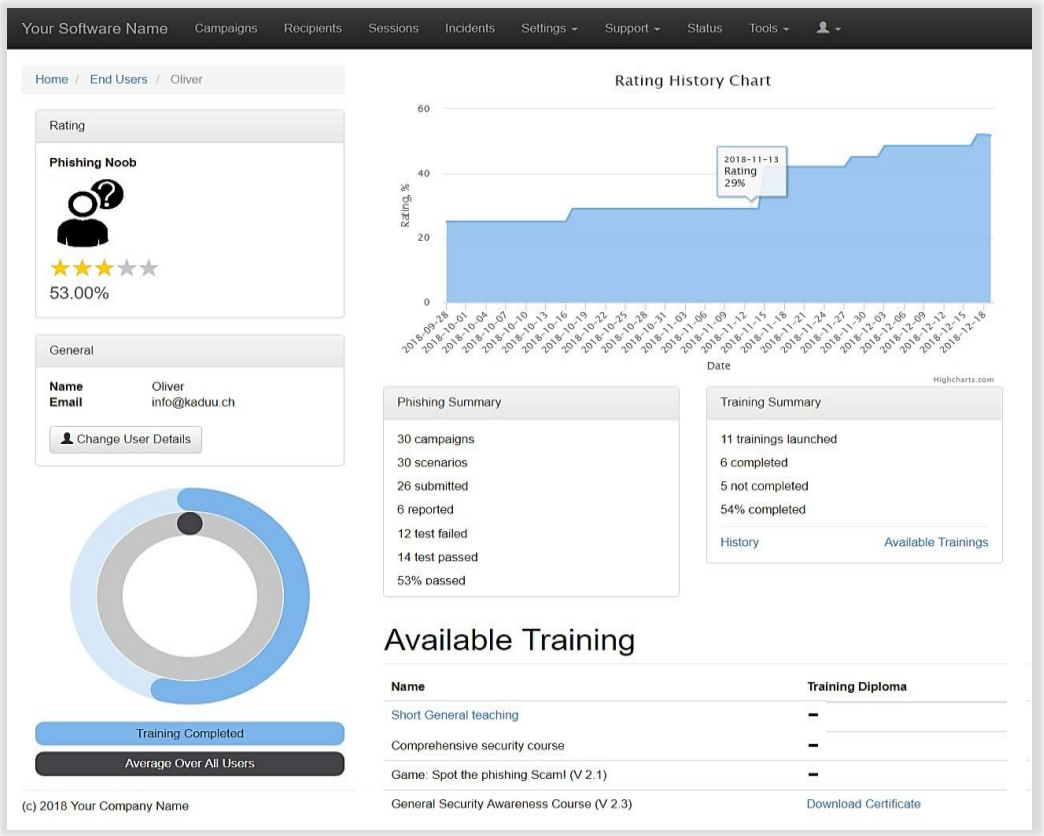


PRUEBAS TÉCNICAS

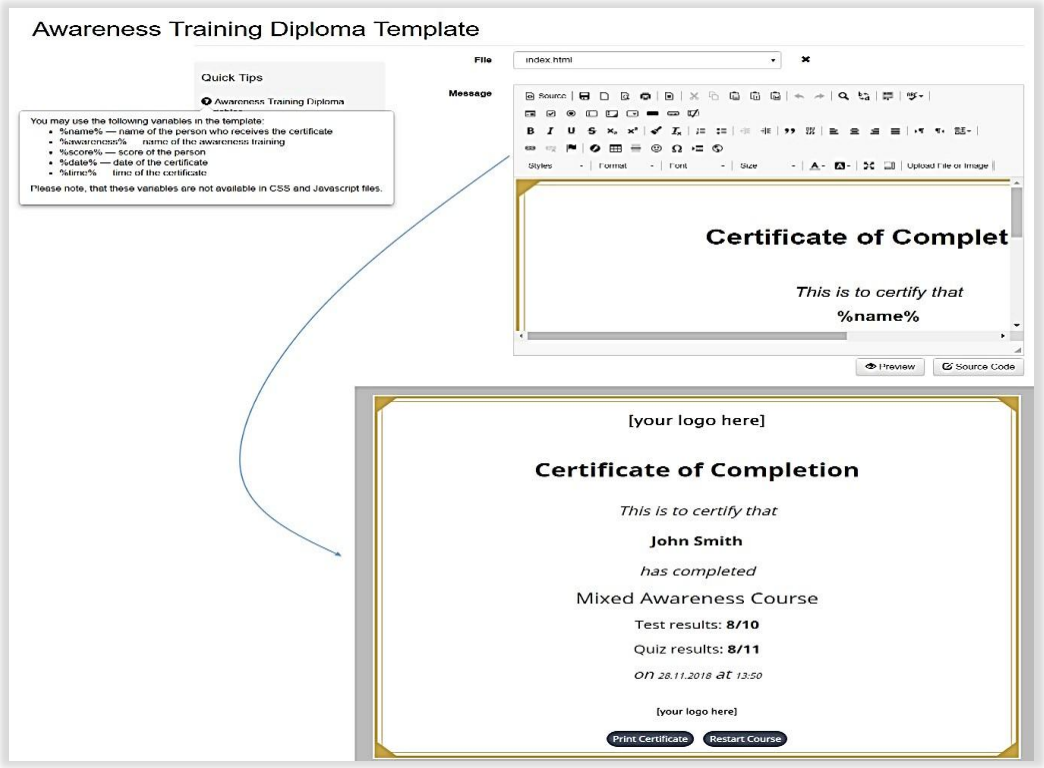
- **Aprendizaje online basado en la reputación:** Entrene a sus empleados de acuerdo a sus habilidades requeridas. Mida las habilidades de los empleados y permita una competición amistosa entre colegas (ludificación). Basándose en los perfiles de reputación de cada usuario final, el sistema puede proporcionarles 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.



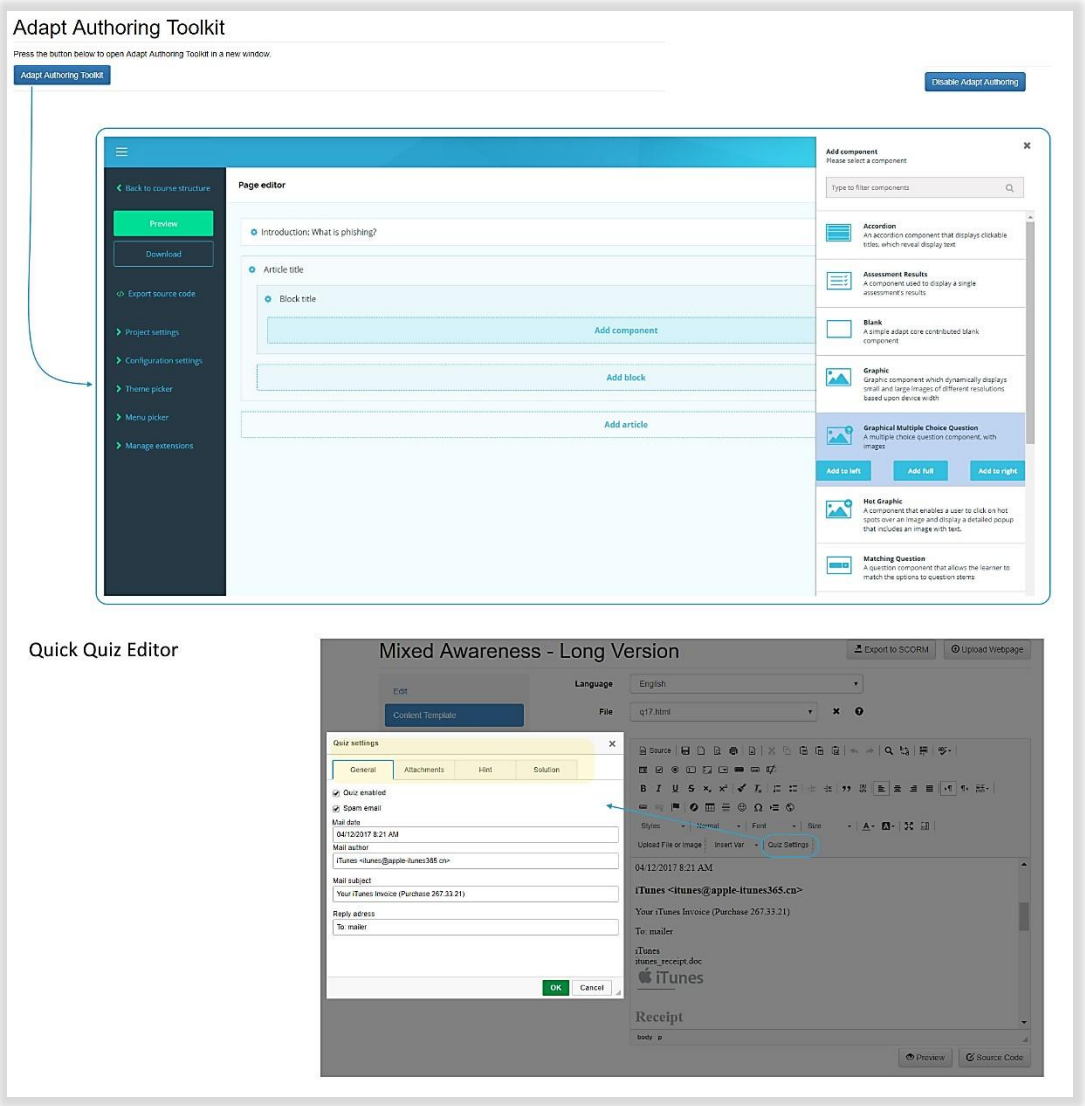
- **Portal de formación para usuarios finales:** Funcionalidad del sistema de gestión de aprendizaje (LMS): Ofrece a cada empleado acceso permanente a una página de inicio formativa personalizada que incluye sus propios cursos específicamente diseñados para ellos. En esta página de inicio pueden ver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



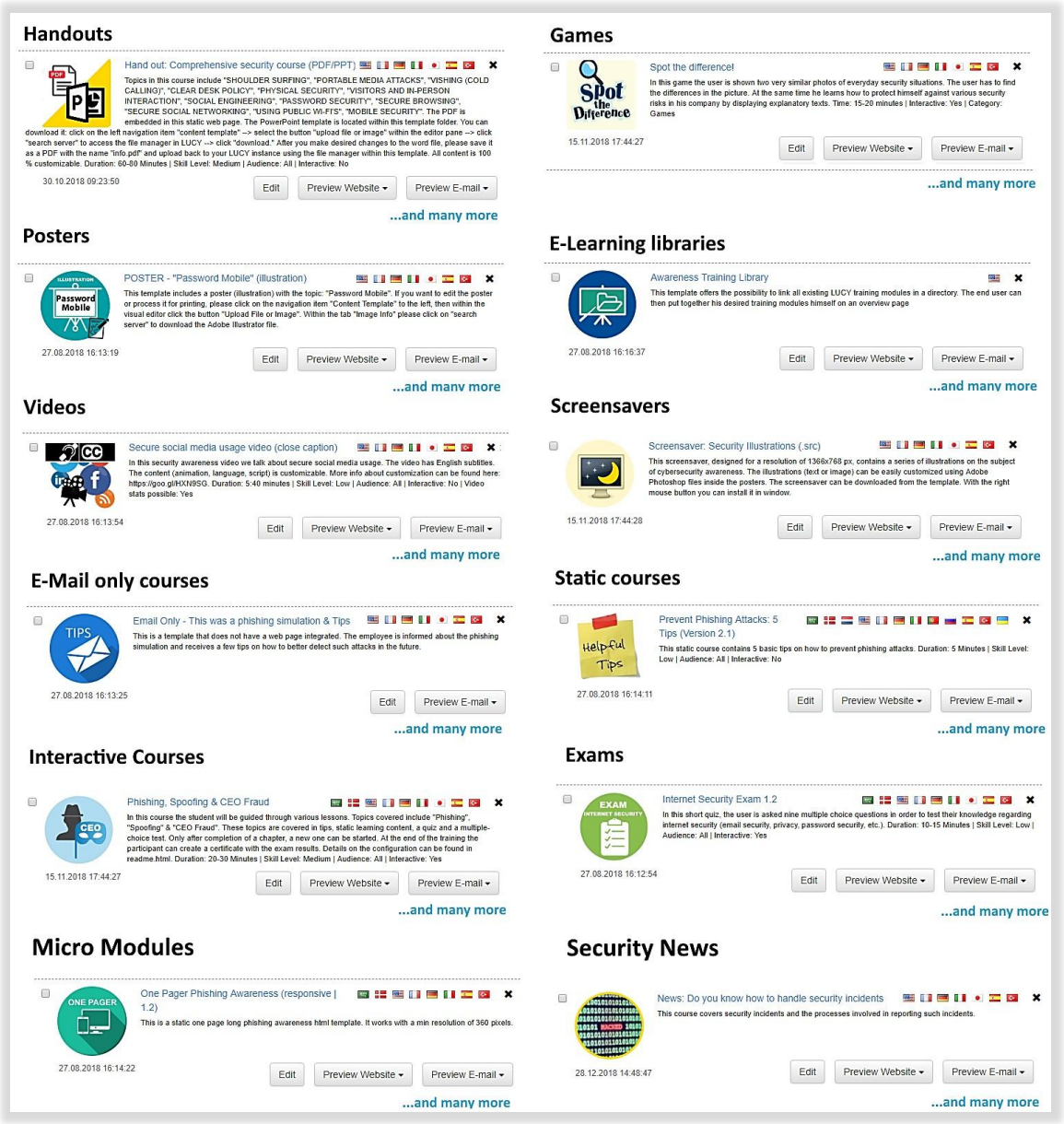
- **Diploma de concienciación:** El destinatario puede crear e imprimir los certificados de aprendizaje online, ya sea directamente dentro de una formación o dentro del portal LMS.



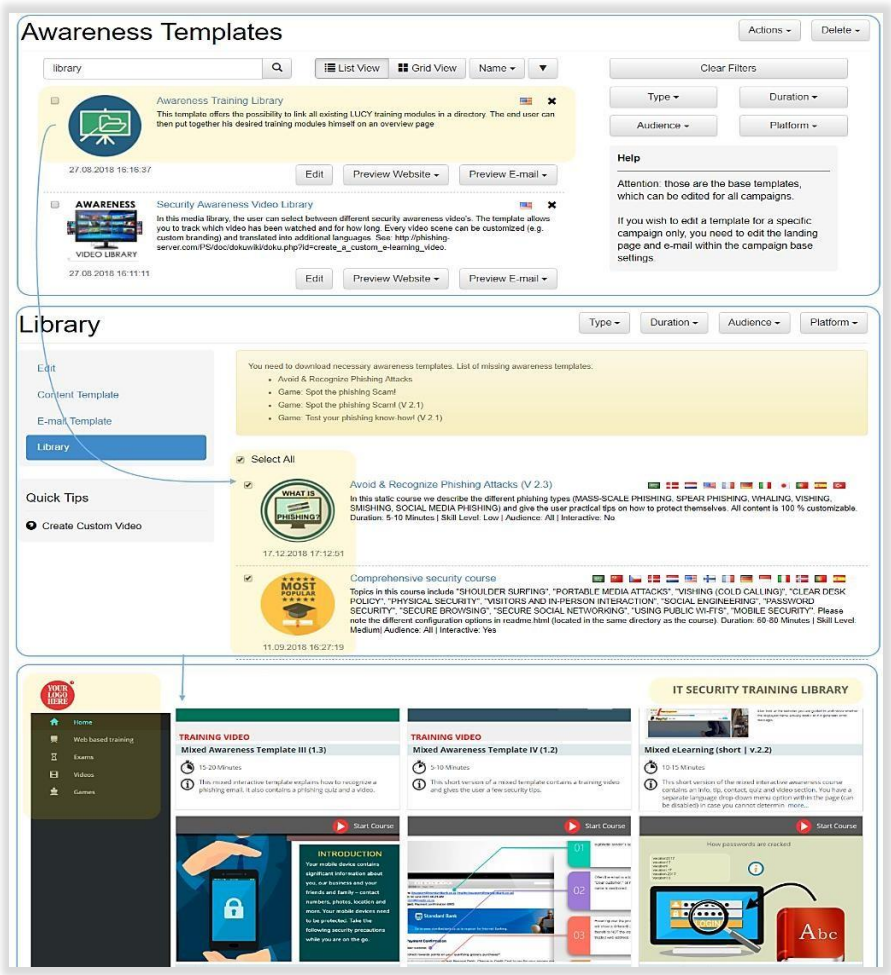
- **Kit de herramientas de creación de contenidos de aprendizaje online:** El kit de herramientas de creación de contenidos de aprendizaje online (Adapt) permite la creación de contenidos de aprendizaje individualizados. Arrastre y suelte vídeos o cualquier otro formato interactivo rich media, inserte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



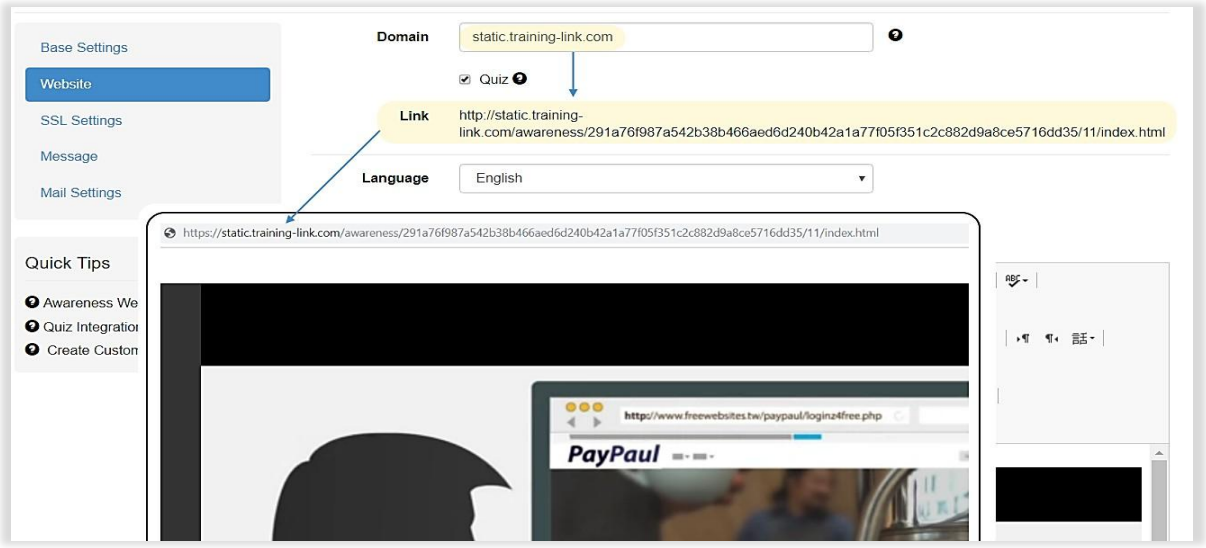
- **Entrenamiento de concienciación en formato interactivo rich media:** Integre elementos en formato interactivo rich media (vídeo, audio u otros elementos que animen a los empleados a interactuar y comprometerse con el contenido) en sus formaciones de concienciación. Utilice los vídeos educativos existentes, adáptelos o añada sus propios elementos en formato interactivo rich media.



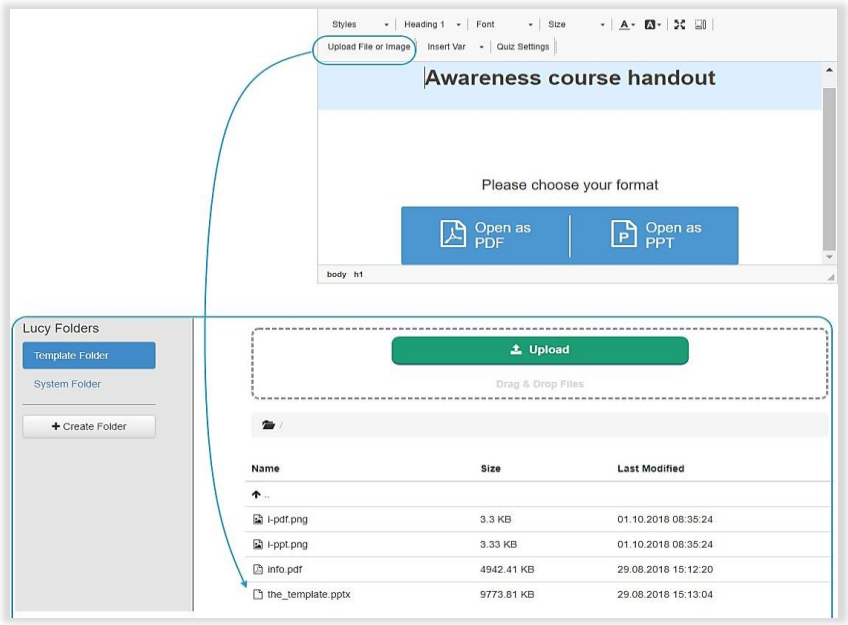
- **Biblioteca de formación:** Los empleados pueden acceder al contenido de formación de su organización desde una página de resumen llamada «biblioteca de formación». Contiene una gran selección de plantillas de aprendizaje online regulares de LUCY, que sirven como referencia. La página de resumen puede 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.

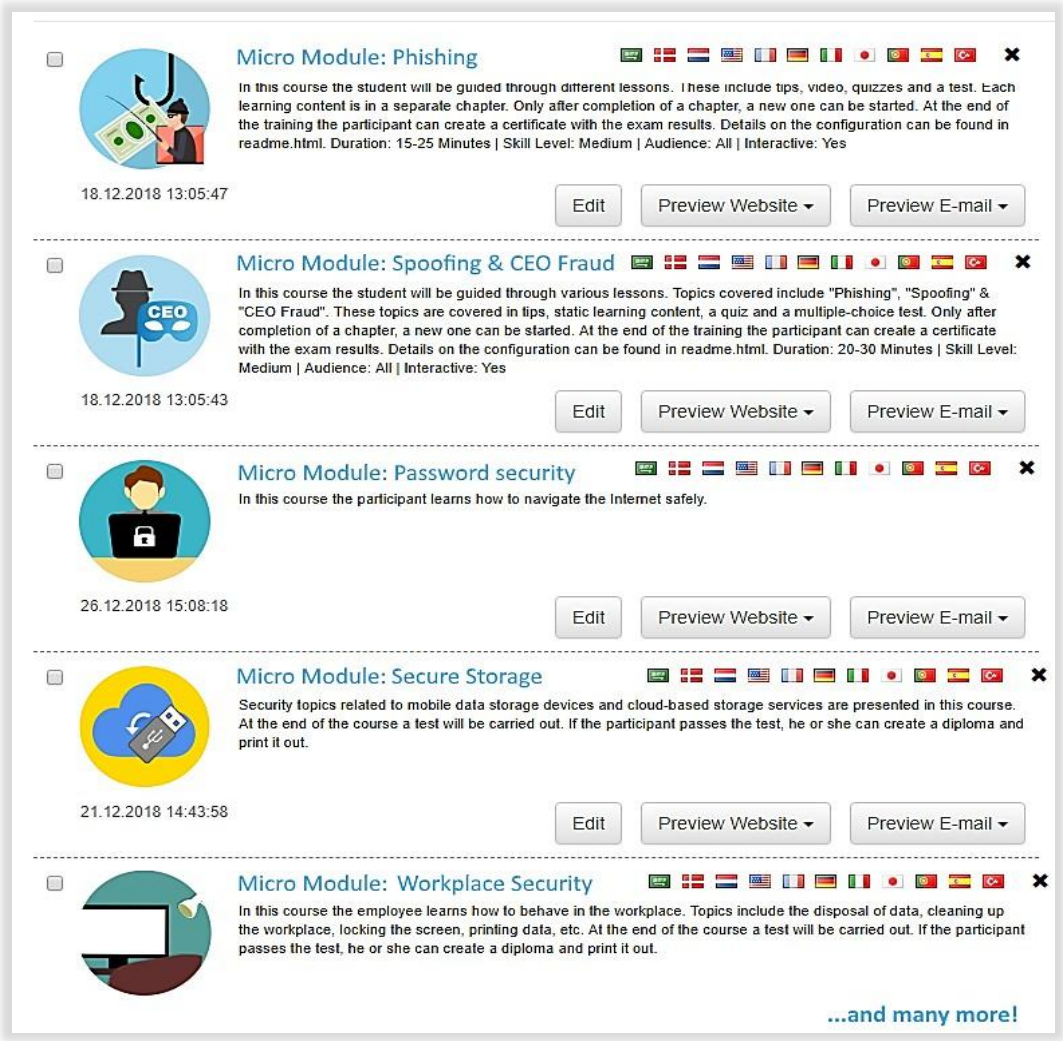


- **Soporte de entrenamiento fuera de Internet:** LUCY se suministra con una serie de plantillas editables (archivos de Adobe Photoshop o Illustrator) para la formación de concienciación, como carteles, salvapantallas, folletos, etc.

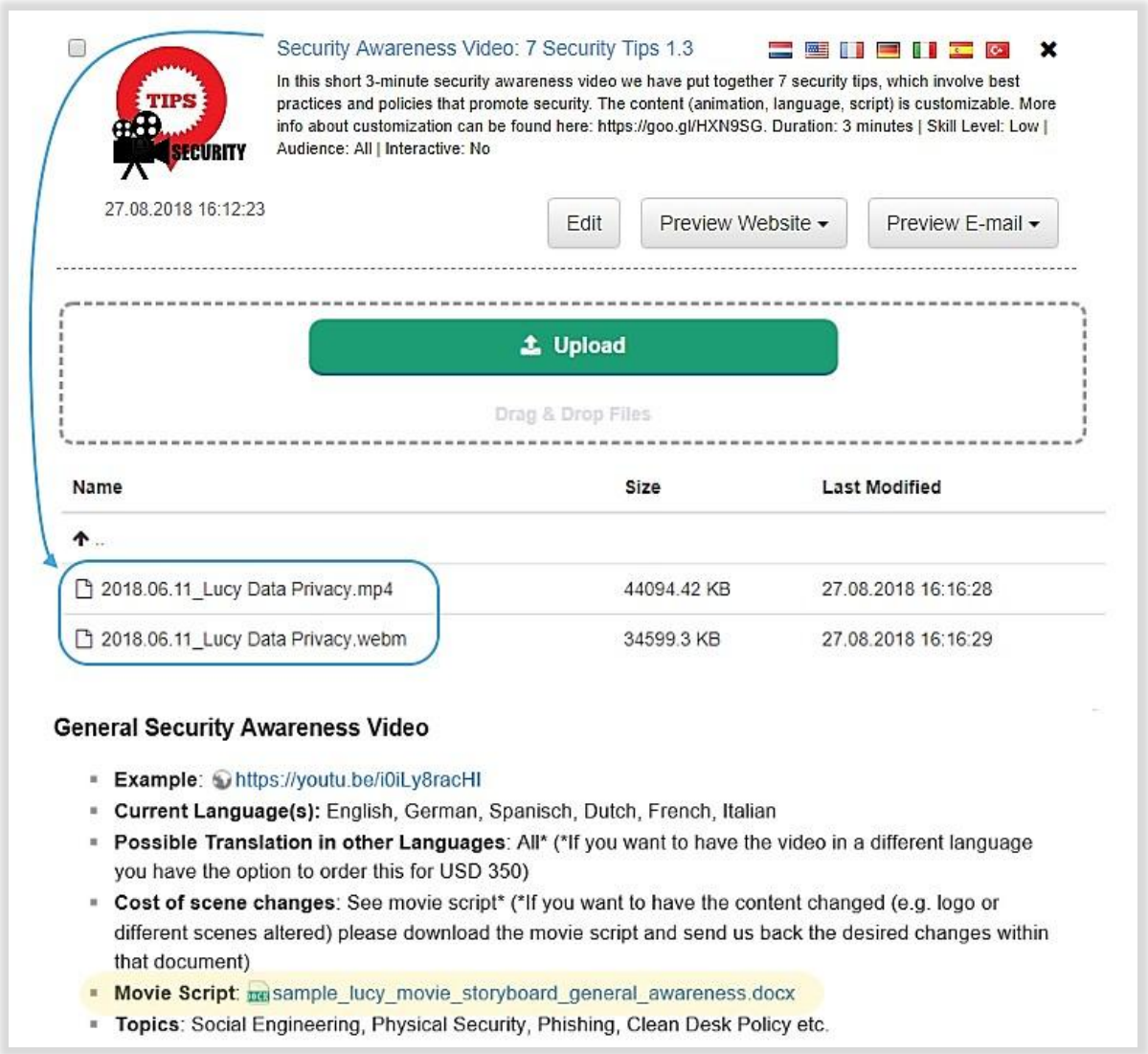


.

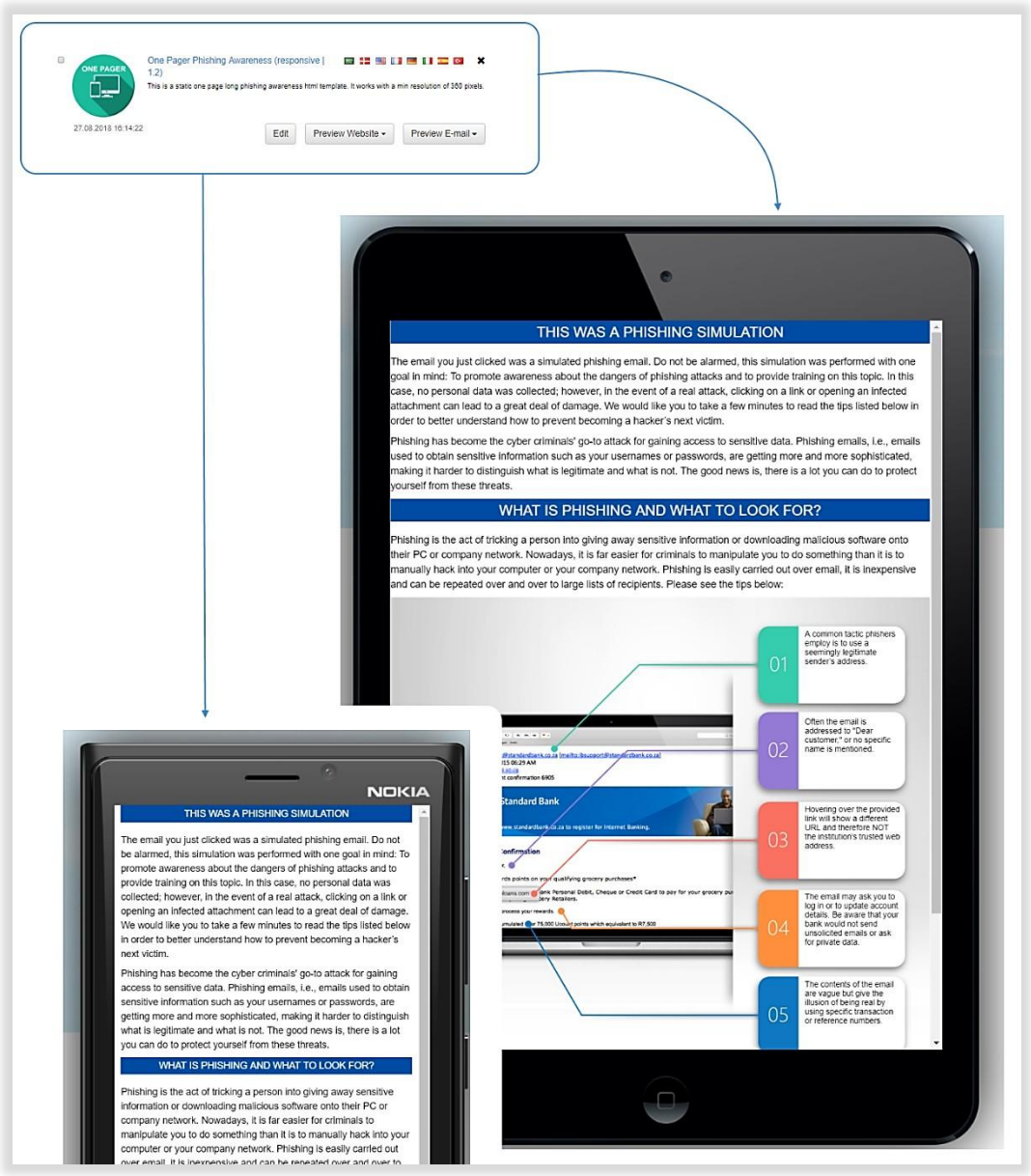
- **Módulos de microaprendizaje:** Hemos diseñado módulos de formación para el microaprendizaje (p. ej., vídeos de 1 minuto o documentos de concienciación de una página) que pueden adaptarse a las necesidades de marca y políticas de su organización.



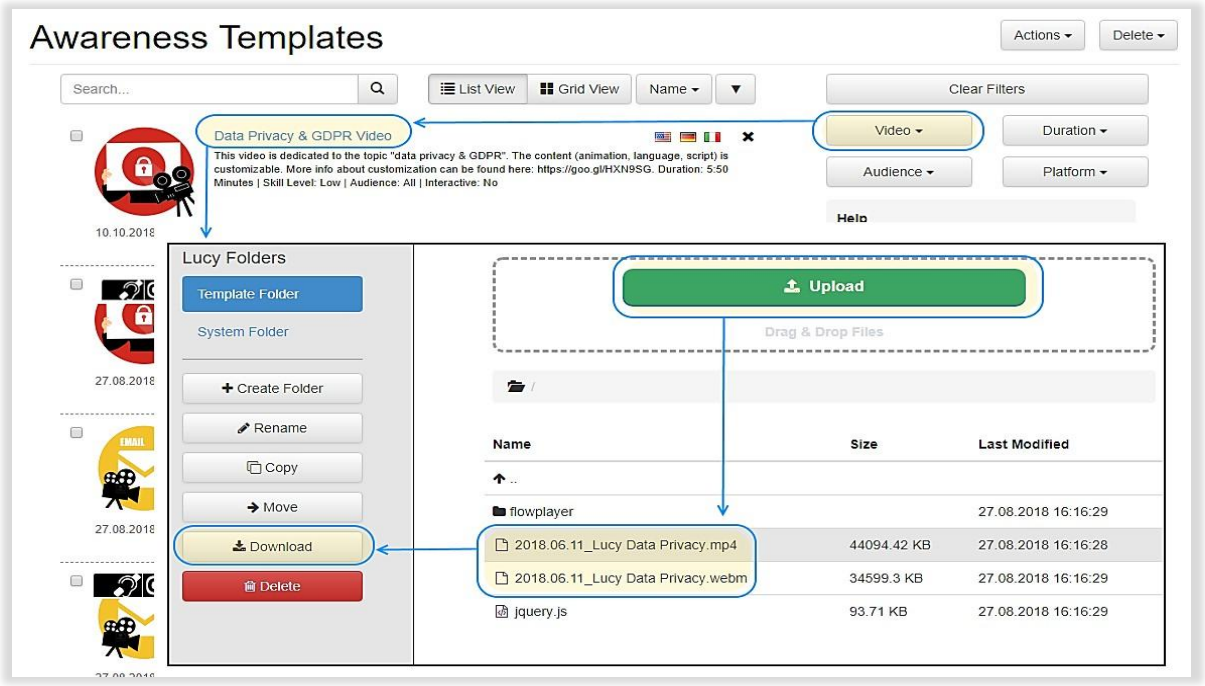
- **Personalización de vídeo:** Envíenos el logo de su empresa y lo incluiremos en los vídeos formativos. ¿Quiere otro idioma? No hay problema. Configuraremos el vídeo para que se reproduzca en el idioma que prefiera. ¿Quiere una escena diferente? Simplemente descargue los scripts de vídeo y marque los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



- **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.



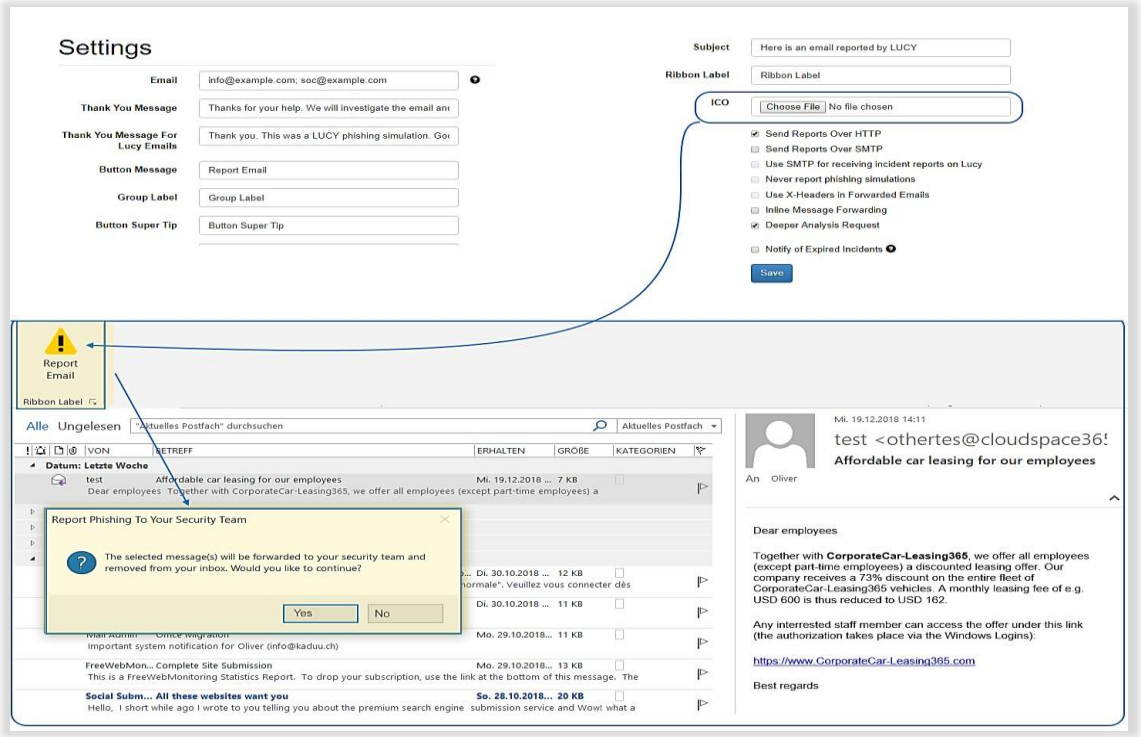
- **Importar y exportar vídeo:** Puede exportar vídeos de LUCY a su propio sistema, así como importar sus propios vídeos a LUCY.



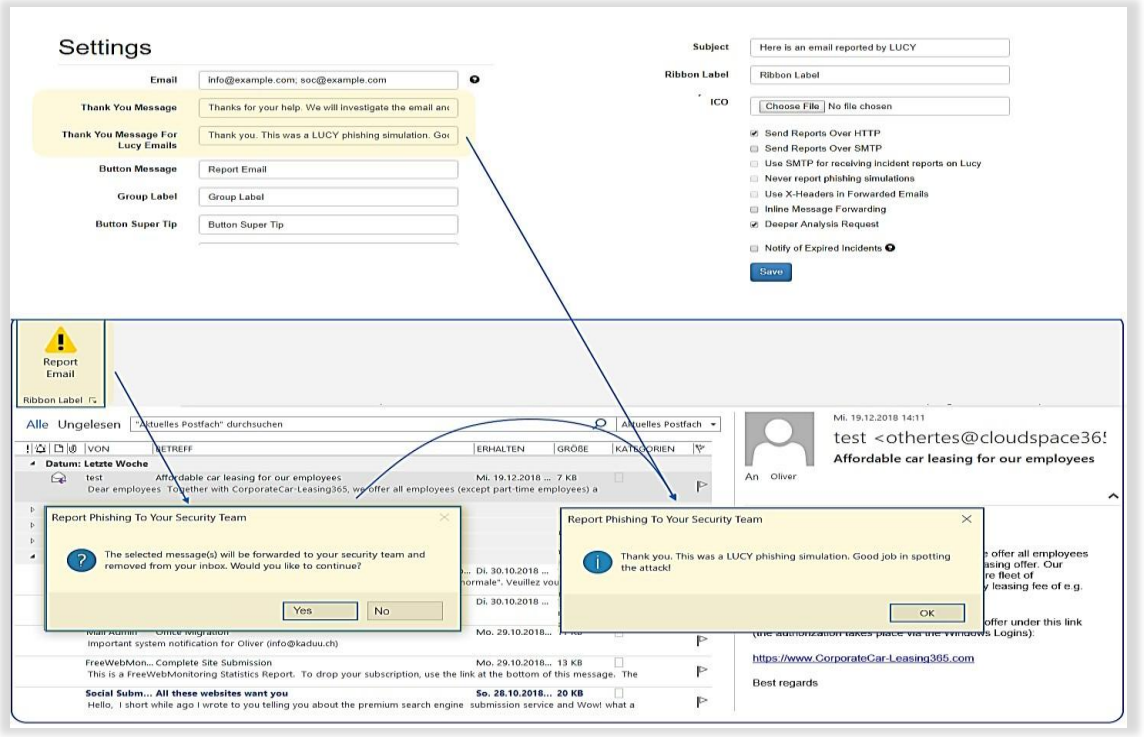
- **Pistas dinámicas de entrenamiento:** Las pistas dinámicas implementadas permiten a su administrador establecer marcadores dentro de las plantillas de ataque que podrían indicar a sus empleados, dentro del material de aprendizaje online, dónde se puede haber detectado el ataque de phishing.

INVOLUCRE A LOS EMPLEADOS

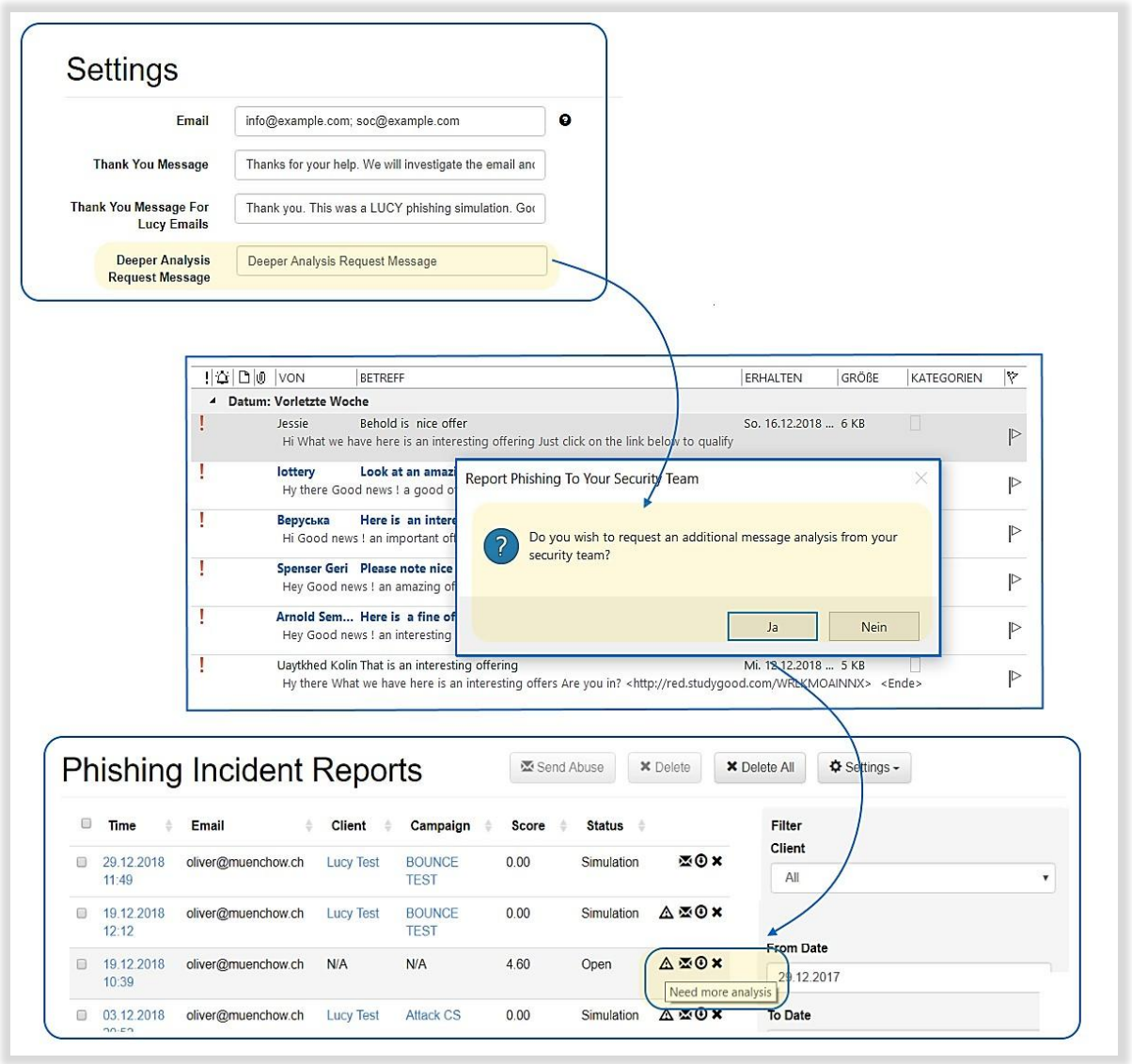
- **Reportar correos electrónicos con un solo clic:** Los usuarios finales pueden reportar correos electrónicos sospechosos con un solo clic a una o varias cuentas de correo electrónico y hacer que sean reenviados a su consola de análisis de incidentes LUCY.



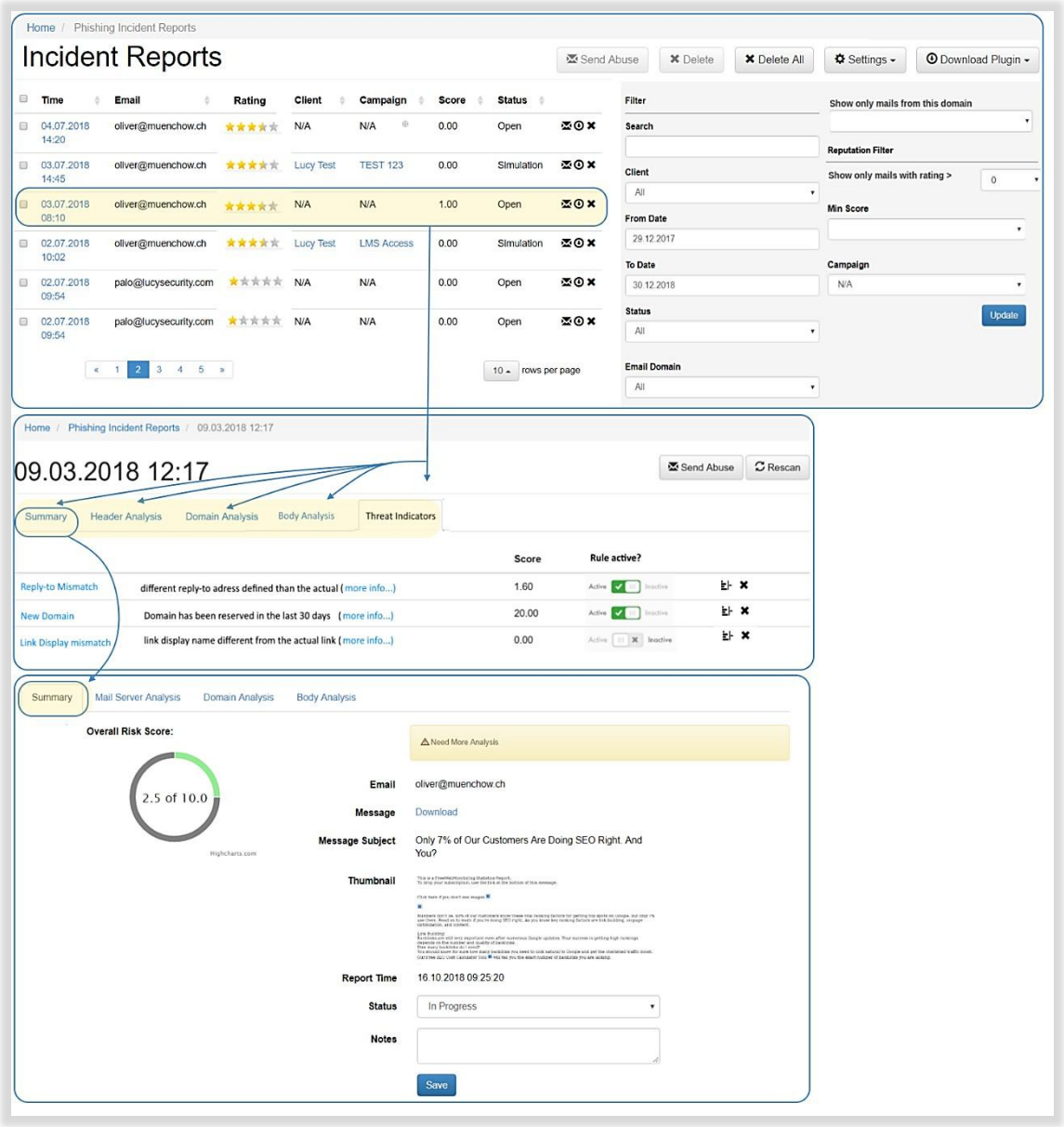
- **Refuerzo de comportamiento positivo:** Nuestro plugin proporciona automáticamente un refuerzo positivo del comportamiento mostrando gratitud a los usuarios finales mediante un mensaje personalizado definido por su organización.



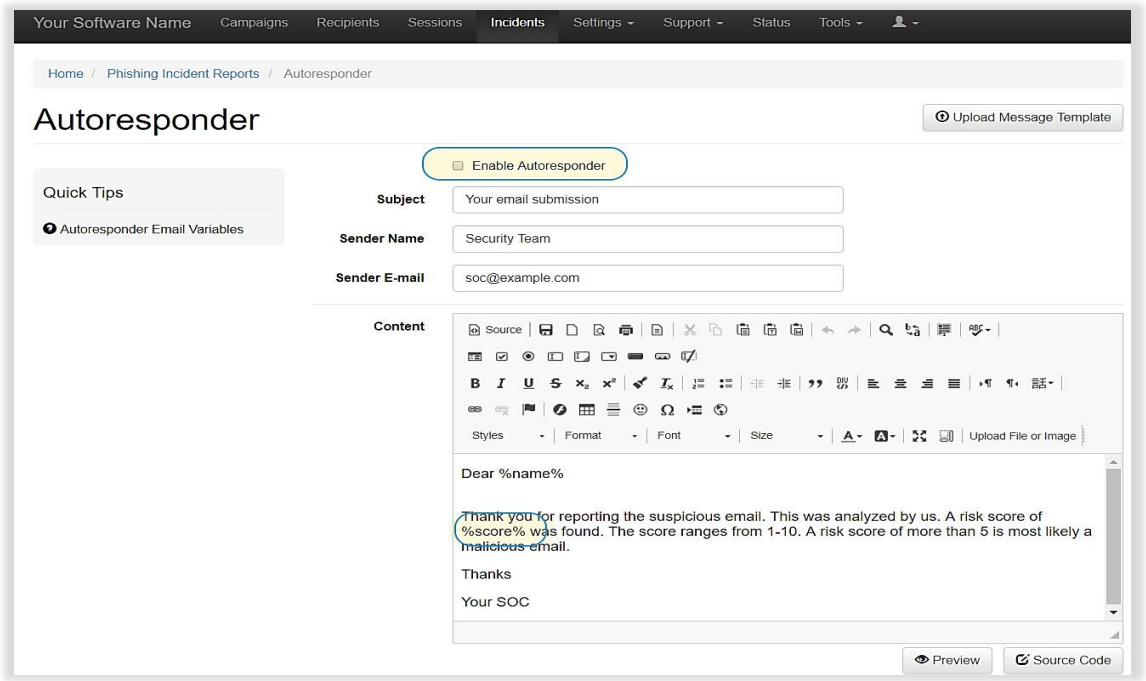
- **Solicitud de inspección profunda:** A veces los usuarios quieren saber si el correo electrónico recibido se puede abrir de forma segura. Opcionalmente, el usuario puede utilizar la «solicitud de inspección profunda» dentro del plugin local para informar al equipo de seguridad de que desea recibir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



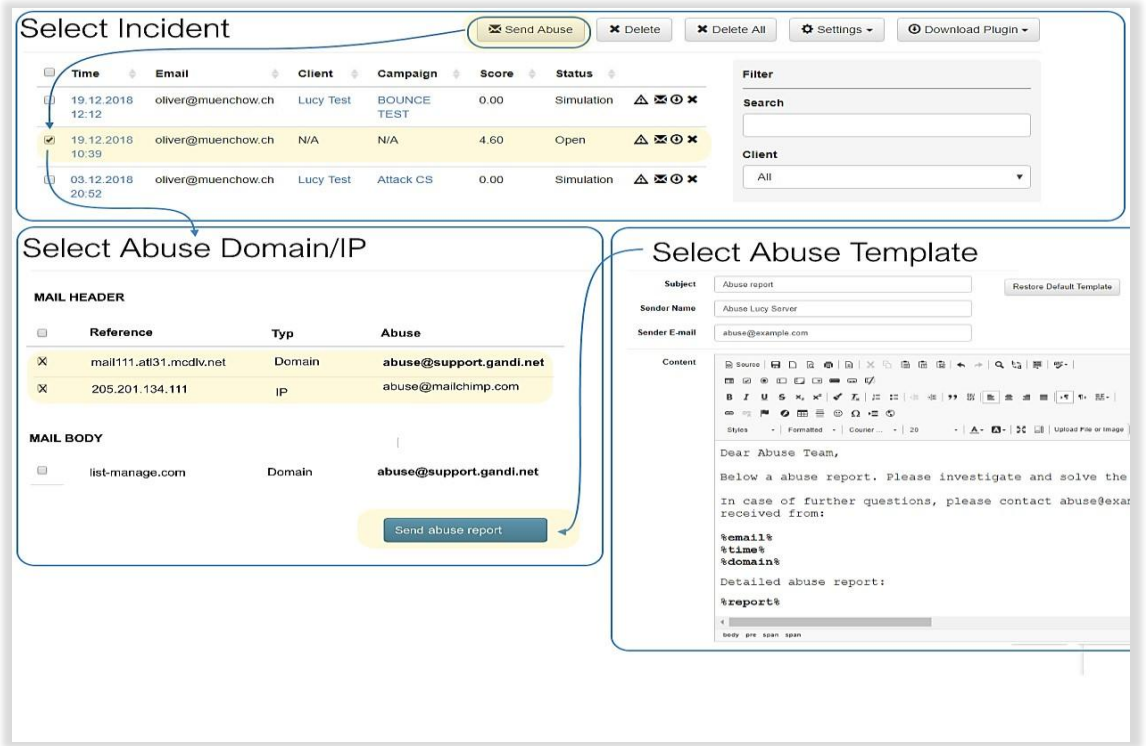
- **Análisis automático de incidentes:** Gestione y responda a los mensajes de correo electrónico sospechosos reportados mediante una consola de gestión centralizada: El analizador de LUCY permite una inspección automatizada de los mensajes reportados (encabezado y cuerpo). El analizador incluye una 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.



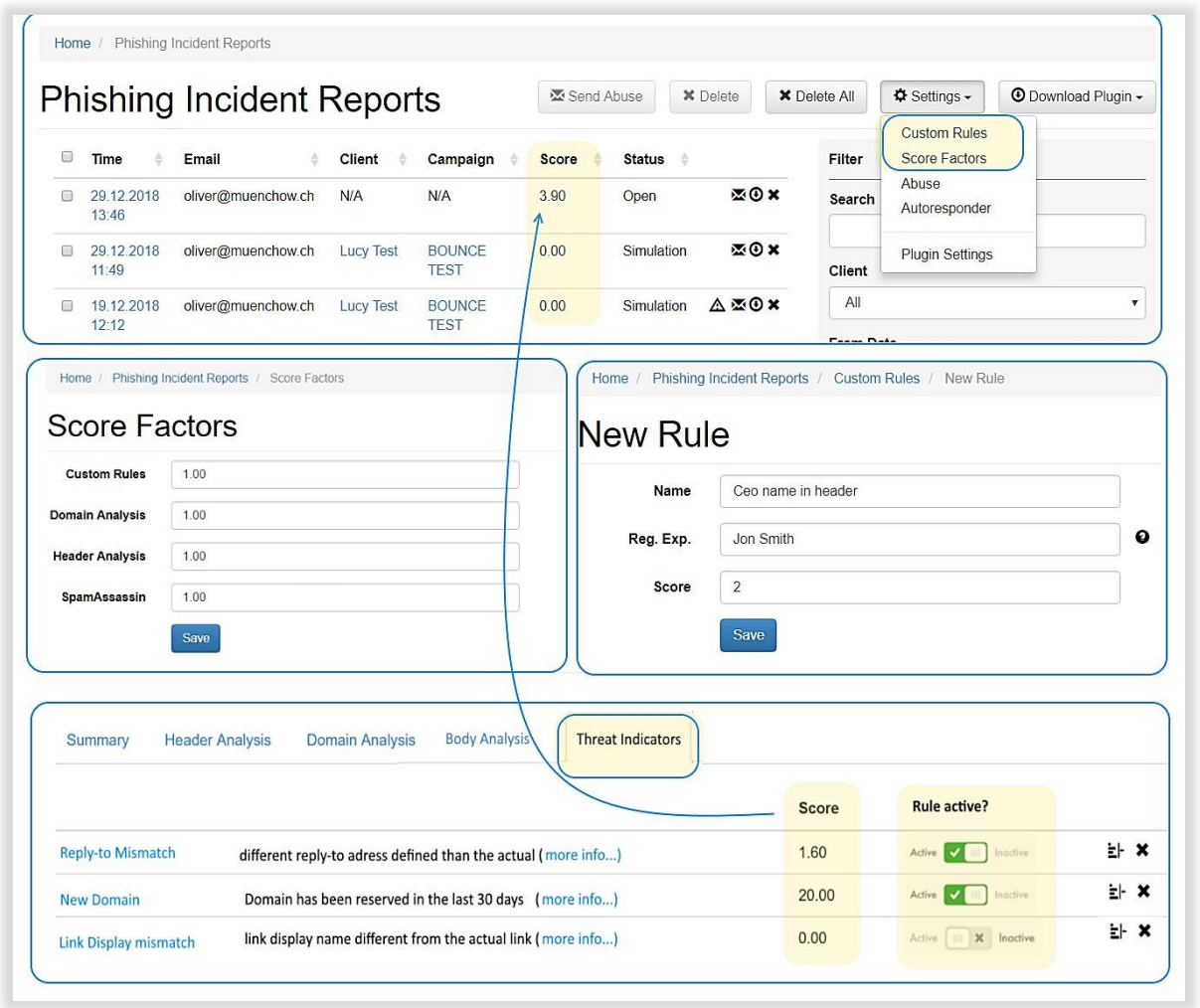
- **Feedback automático del incidente:** El Autorespondedor de Incidentes permite enviar una notificación automatizada al usuario final proporcionando los resultados del análisis de las amenazas de su correo electrónico. El texto del mensaje es libremente configurable, y la puntuación de riesgo del correo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



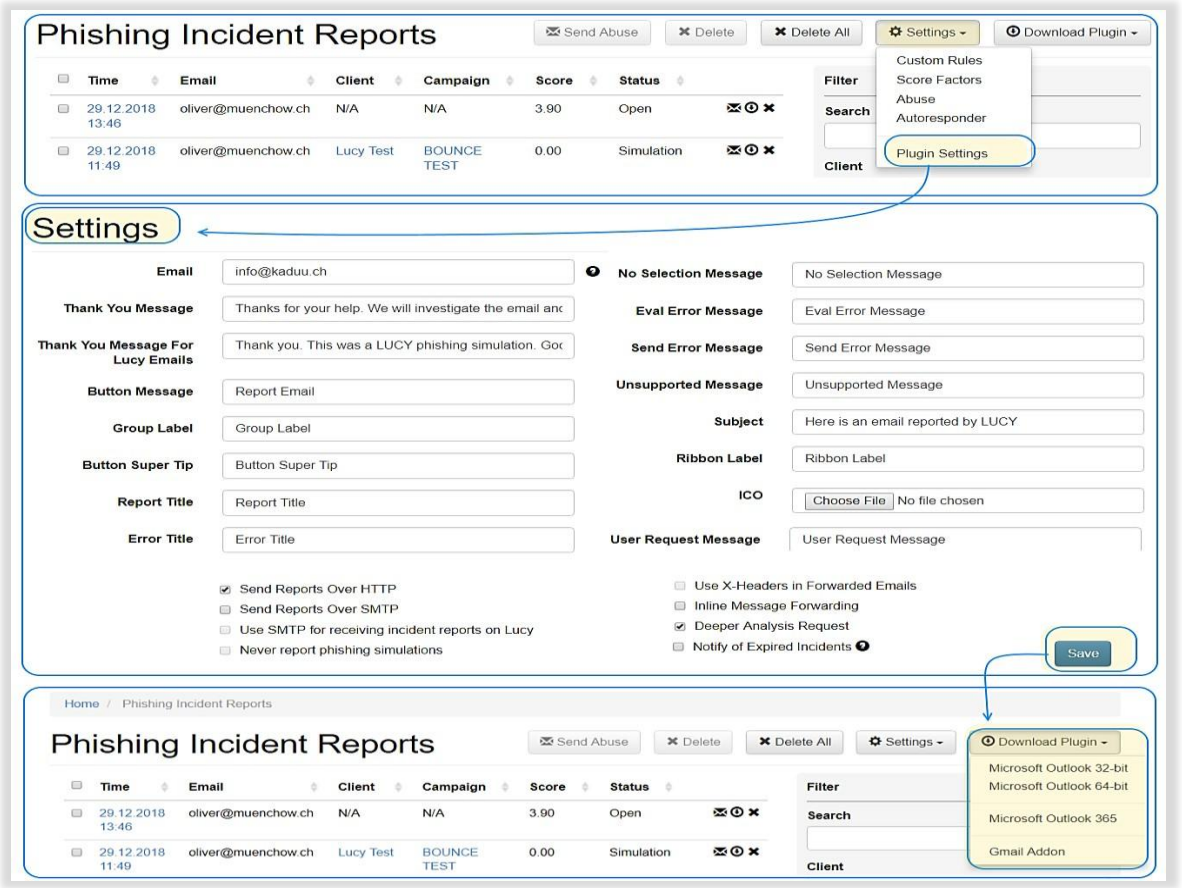
- **Mitigación de amenazas:** El Mitigador de Amenazas de Comportamiento es un enfoque revolucionario para eliminar los riesgos del correo electrónico. Apoyará al administrador de seguridad a parar el ataque (p. ej., enviando un informe automatizado al equipo antiabuso de los proveedores implicados en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



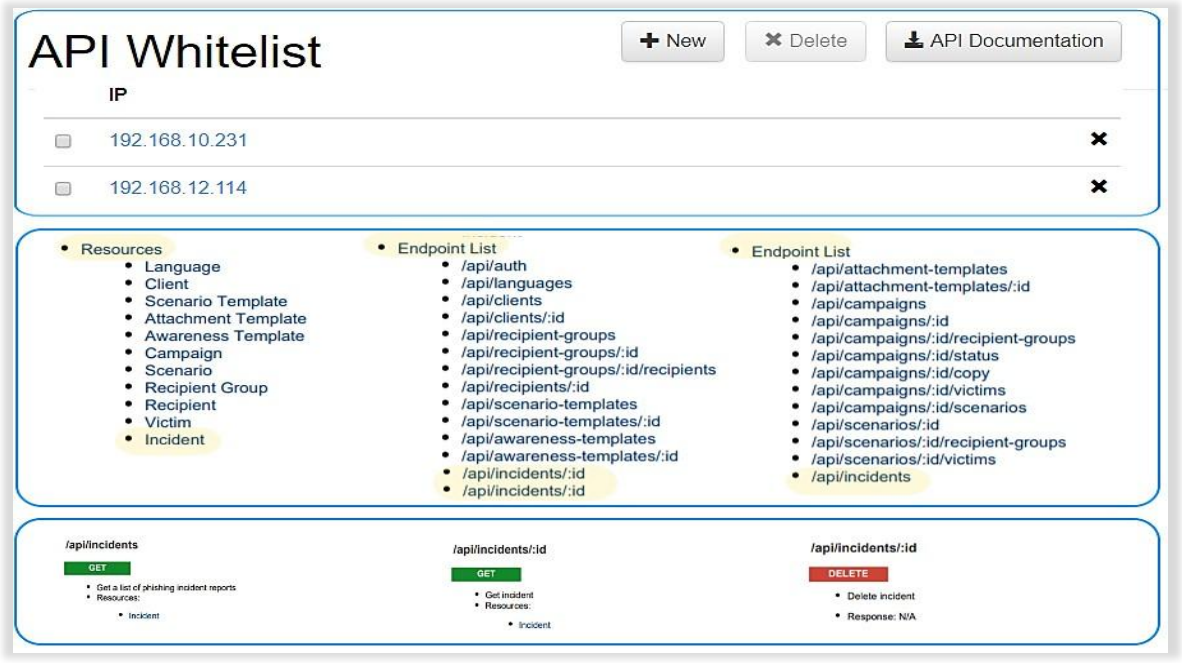
- **Análisis basado en reglas personalizadas:** Define your own rules for e-mail analysis and risk calculations.



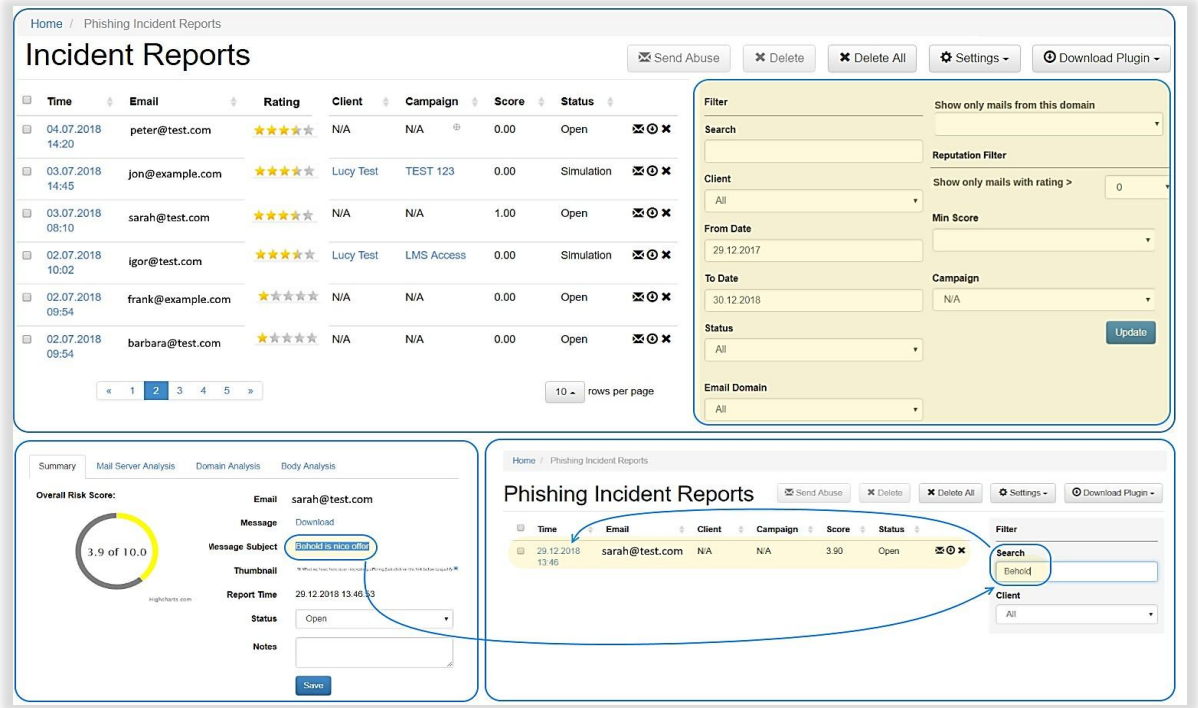
- **Opciones de personalización de los plugins:** LUCY permite una fácil personalización y una marca blanca por completo de las diferentes funciones de los plugins (icono visualizado, mensajes de feedback, etiqueta de cinta, protocolo de transmisión, cabecera enviada, etc.).



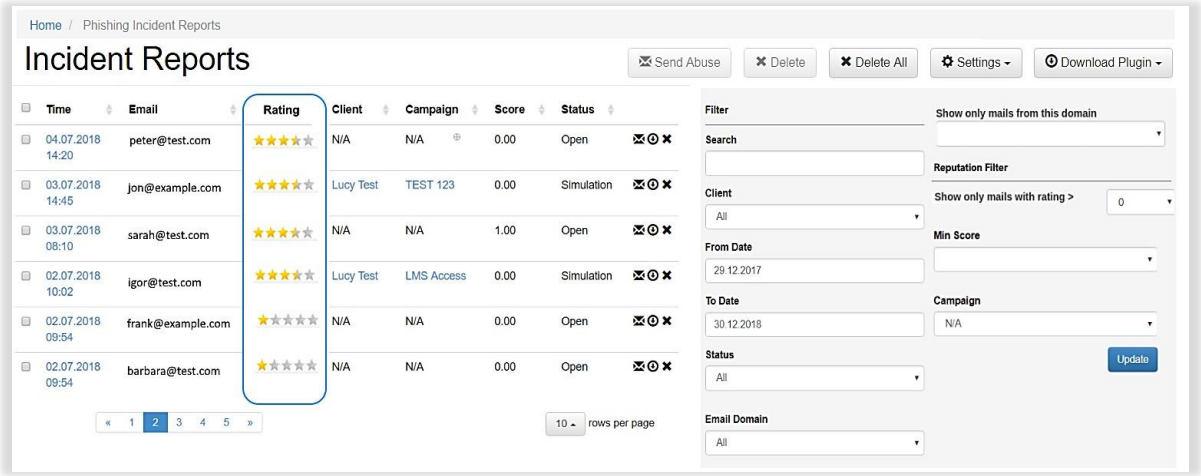
- **Integración de terceros:** Gracias a la automatización de la API REST de incidentes de LUCY, podemos procesar los mensajes de correo electrónico notificados y ayudar a su equipo de seguridad a detener los ataques de phishing activos mientras están en curso.



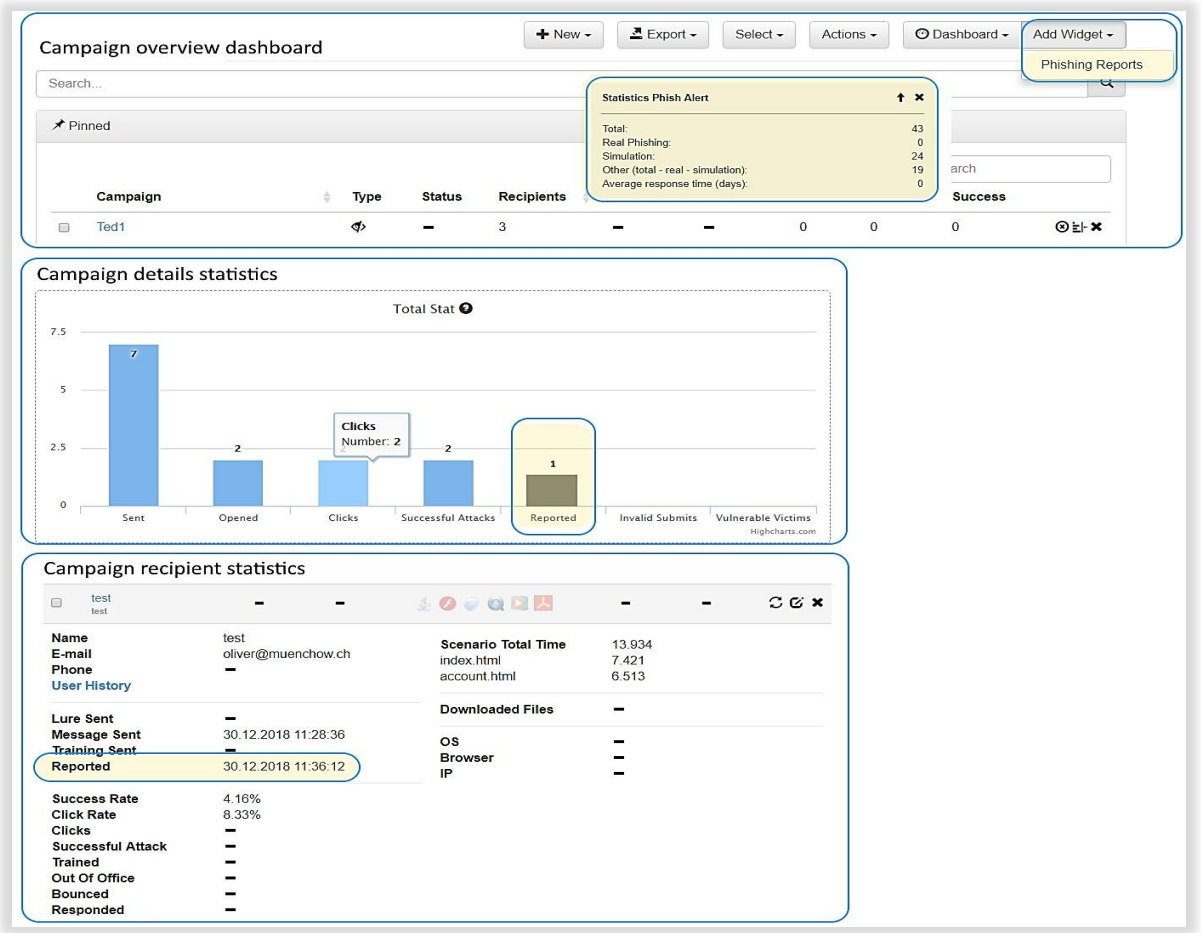
- **Identificar ataques con patrones comunes:** Aplique los filtros del panel de control de LUCY para detectar los vectores de ataque comunes en toda su organización. Busque en todos los correos electrónicos reportados indicadores similares de amenazas.



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



- **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.