LUCY WHITEPAPER

CHE COS'È LUCY?

Metti alla prova, forma e coinvolgi i tuoi impiegati

LUCY permette alle società di prendere il ruolo di un aggressore e rivelare le debolezze esistenti in infrastruttura tecnica e competenze del personale, eliminandole attraverso un programma di e-learning completo.

TEST IMPIEGATI
Simulazione di attacchi (ad esempio phishing)

TEST INFRASTRUTTURE
Simulazione e scansione malware

FORMAZIONE IMPIEGATI
LMS integrato

MISURAZIONE RISULTATI
Progressi su rischi e apprendimento

INTEGRAZIONE PER IMPIEGATI
Sistema di segnalazione (ad esempio, pulsante per mail phishing)

LUCY WHITEPAPER

SOMMARIO

FUNZIONI GENERALI

- Promemoria
- Rilevamento Risposte
- Client di comunicazione e-m ail completo
- Schedulatore randomizzazione
- Strumenti di prestazione
- Interfaccia amministratore multilingue
- Certificato (SSL)
- Controllo degli accessi basato sui ruoli
- Gruppi di utenti a più livelli
- Compatibilità con più clienti
- Modelli di campagna
- Configurazione guidata basata sui rischi
- Verifica champagne
- Approvazione del flusso di lavoro
- API DNS

SIMULAZIONE DI ATTACCO

- Attacchi con dispositivi multimediali portatili
- SMiShing
- Attacchi di inserimento dati
- Attacchi con collegamenti ipertestuali
- Toolkit di reindirizzamento URL potente
- Attacchi misti
- Attacchi basati su file
- Attacchi doppietta
- Attacchi basati su Java
- Attacchi basati su PDF
- Attacchi di simulazione ransomware
- Toolkit di convalida inserimento dati
- Libreria di modelli di attacco multilingue
- Modelli specifici per settore e divisione
- Utilizzo simultaneo di modelli di attacco
- Variazioni degli URL di attacco
- Accorciamento URL
- Kit pentest
- Duplicatore siti web
- Attacchi basati su livelli
- Simulazione di spear phishing
- Supporto DKIM / S / MIME per email di phishing
- Scansione email
- Creazione homepage personalizzata

TEST INFRASTRUTTURE

- Toolkit test malware
- Test filtri email e web
- Rilevamento vulnerabilità client passiva e attiva
- Test di spoofing

TEST TECNICI

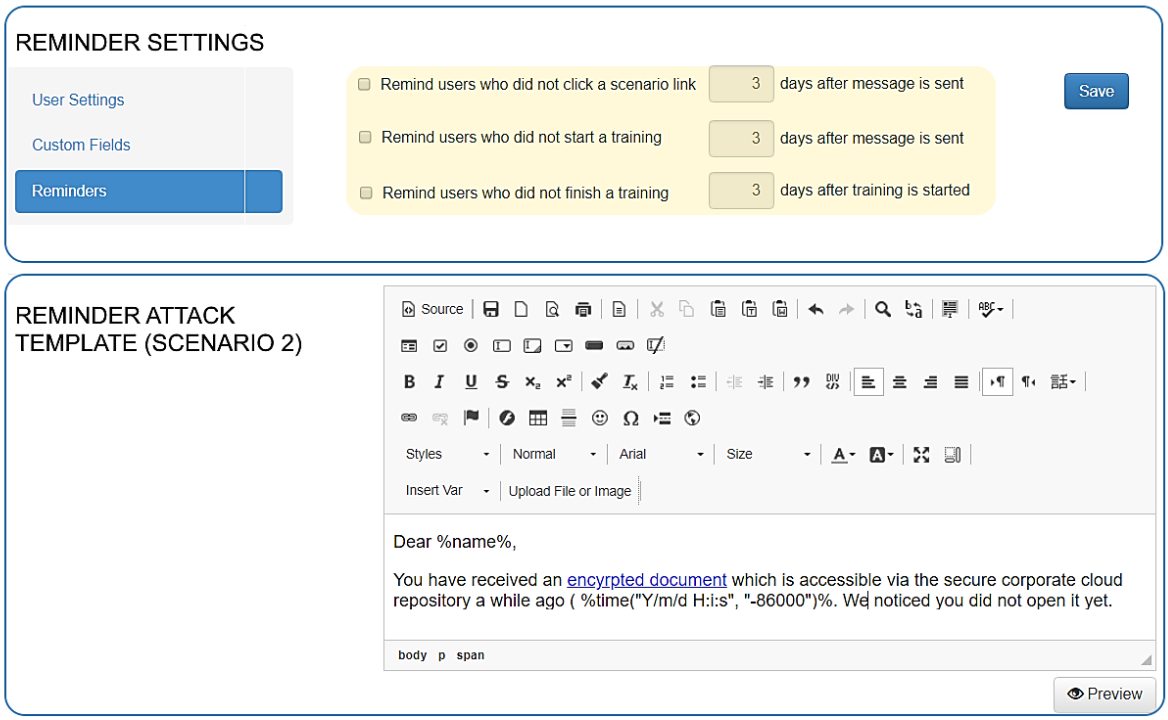
- e-Learning basato sulla reputazione
- Portale di formazione utente finale
- Diploma di formazione sulla sensibilizzazione
- Toolkit di creazione e-learning
- Formazione sulla sensibilizzazione su media interattivi
- Libreria di formazione
- Supporto per formazione statica
- Supporto per formazione offline
- Moduli di microapprendimento
- Personalizzazione video
- Formato adatto per dispositivi mobile
- Importazione / Esportazione video
- Suggerimenti di formazione dinamica

COINVOLGIMENTO IMPIEGATI

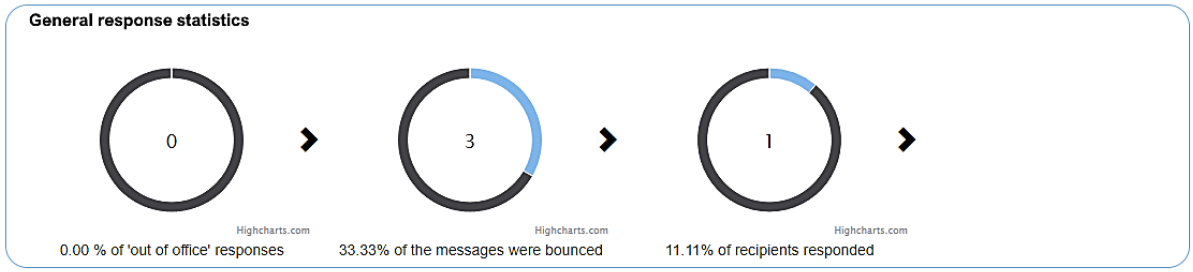
- Segnalazione delle email con un solo click
- Rafforzamento del comportamento positive
- Richiesta di ispezione approfondita
- Analisi degli incidenti automatica
- Feedback degli incidenti automatico
- Mitigazione minacce
- Analisi con regole personalizzate
- Opzioni di personalizzazione plugin
- Integrazione di terze parti
- Identificazione attacchi con schemi comuni
- Profili di reputazione degli utenti sugli incidenti
- Integrazione con attacchi simulati
- Installazione facile

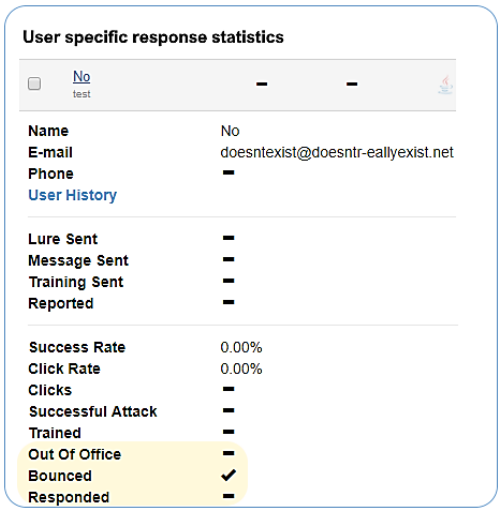
FUNZIONI GENERALI

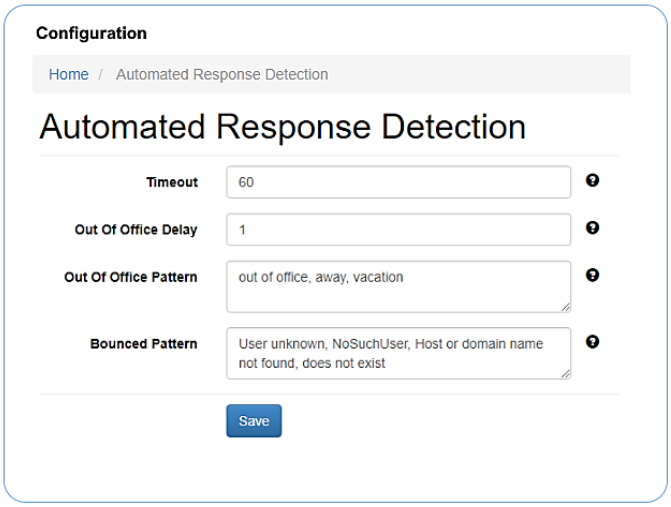
- **Npnrk ck mpg_ 8**i modelli di promemoria possono essere utilizzati per rispedire automaticamente messaggi agli utenti che non hanno cliccato su un link di attacco o su un corso di formazione dopo un periodo di tempo personalizzato.



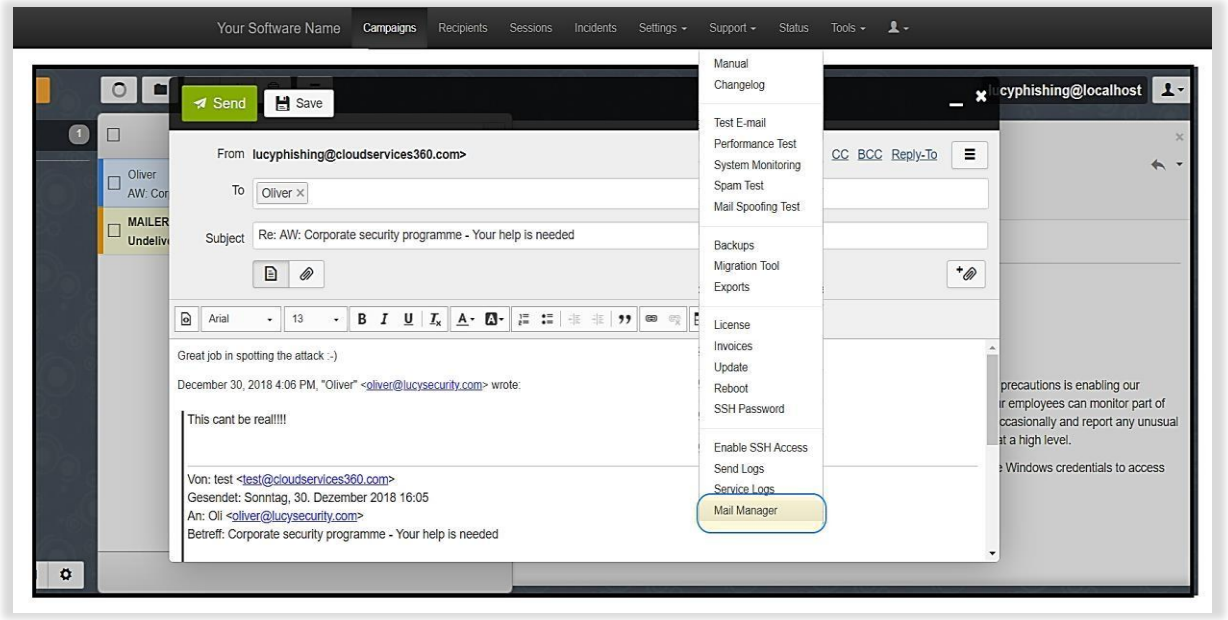
- **Pgct _k cl rmpggnnmqrc 8**il rilevamento automatico delle risposte permette di definire e analizzare le risposte automatiche alle email (ad es. fuori ufficio) e gli errori di consegna della posta (ad es. utente sconosciuto) all'interno della campagna.



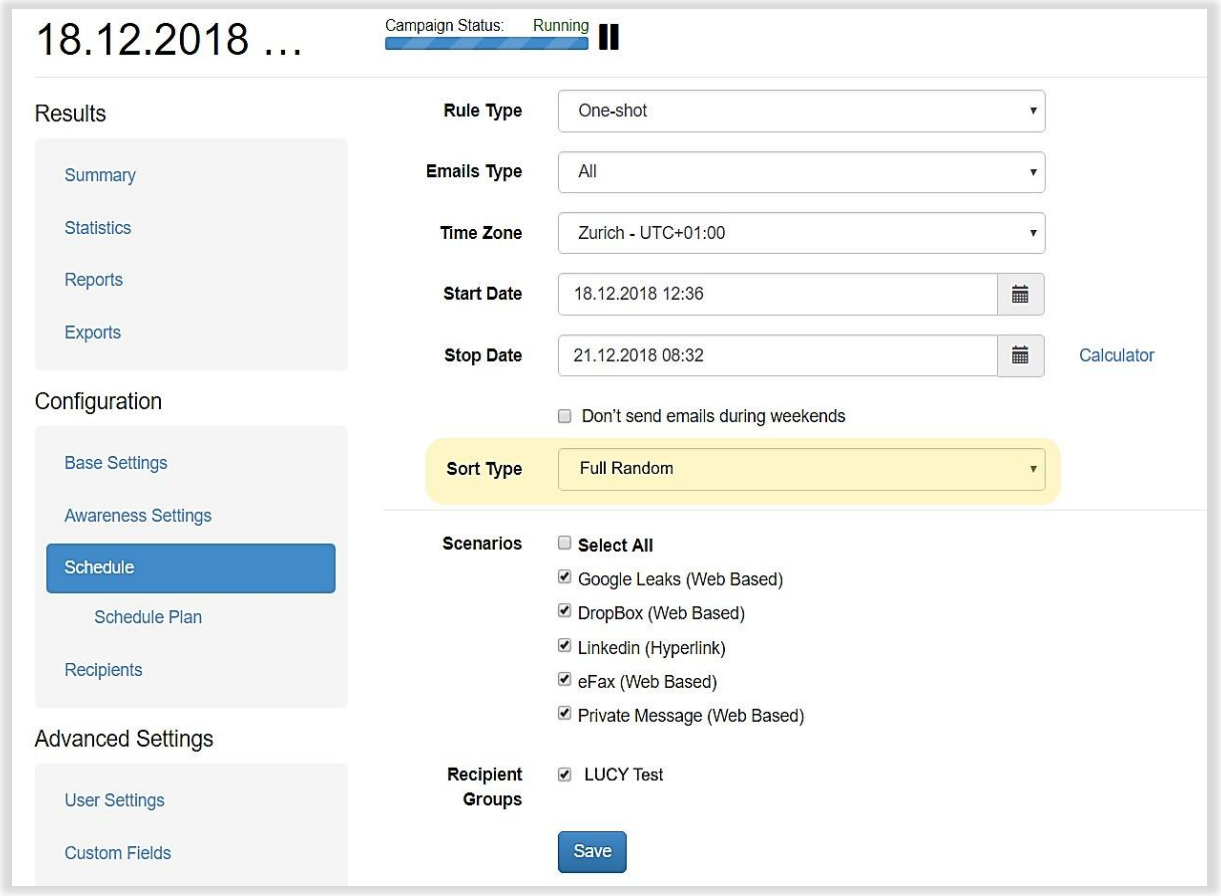




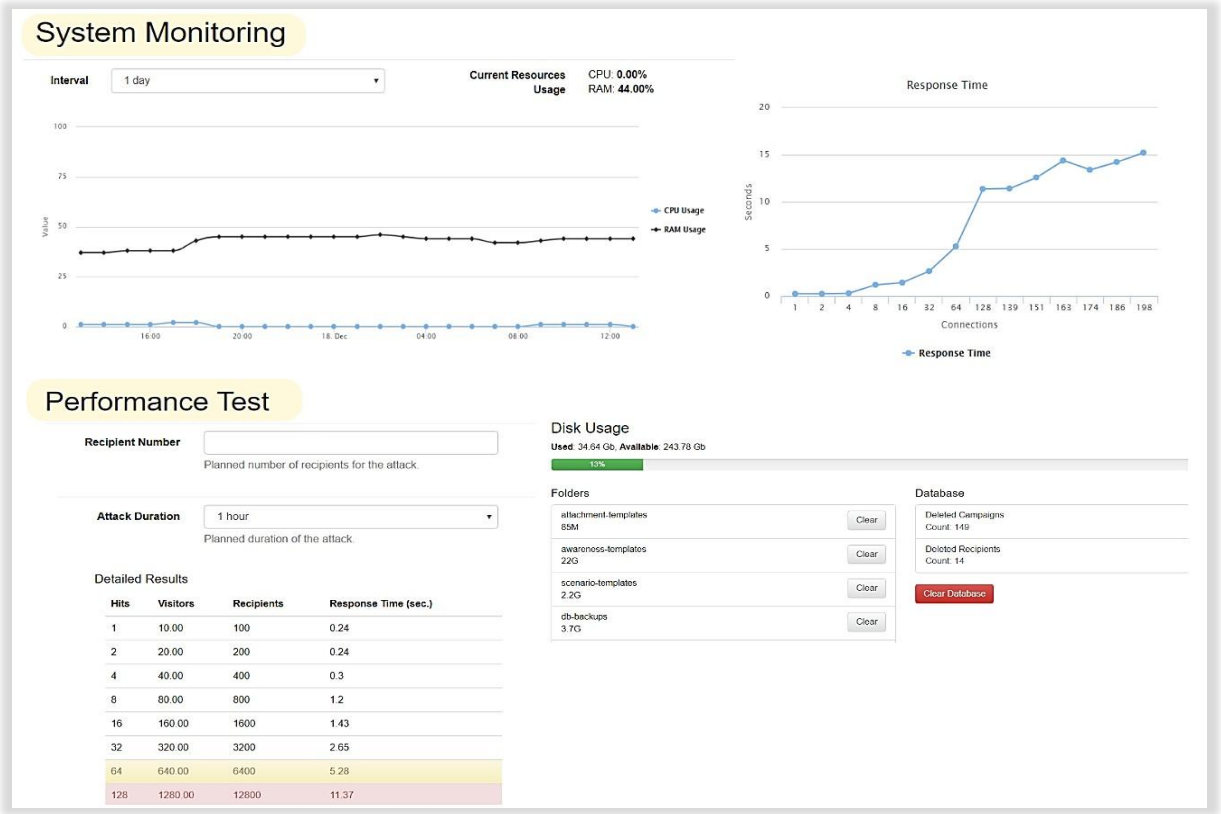
- **Ajgcl r bgamk sl ga_xgml c ck _g amk njcrm8** una piattaforma di messaggistica integrata permette all'amministratore LUCY di comunicare in modo interattivo con i destinatari all'interno o all'esterno delle campagne LUCY. Tutte le email vengono archiviate e possono essere esaminate.



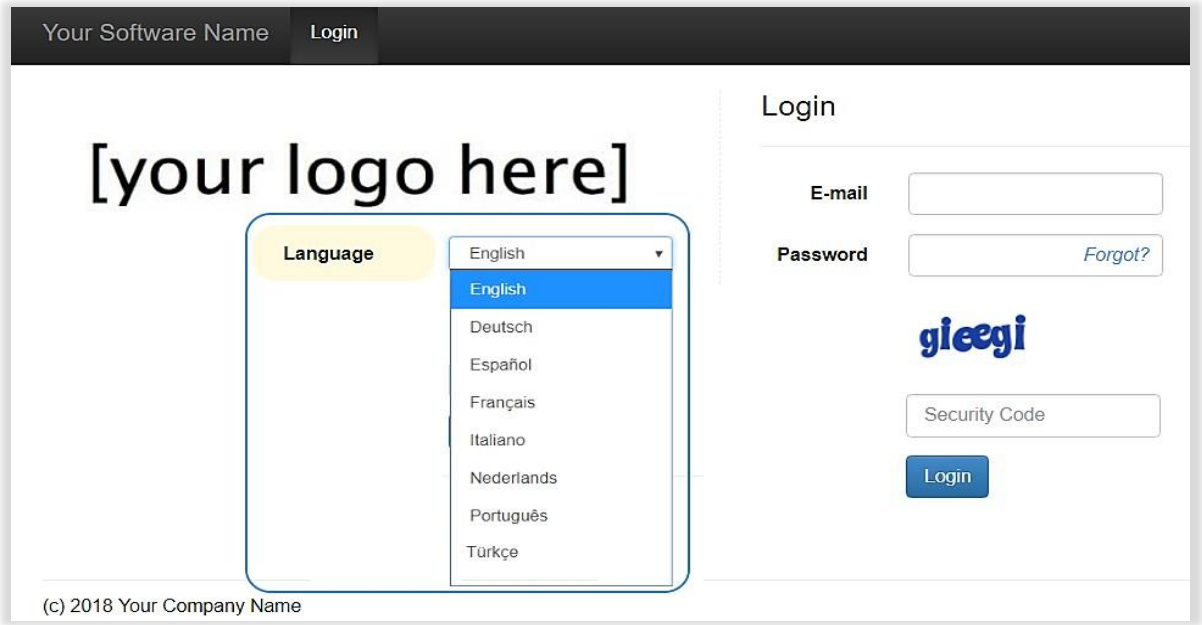
- **Schedulatore randomizzazione:** sensibilizzare gli impiegati in modo casuale è un fattore chiave per una sensibilizzazione efficace e sostenibile all'interno della società. Inviare più campagne simultanee in modo casuale è uno dei migliori mezzi per la formazione degli impiegati.



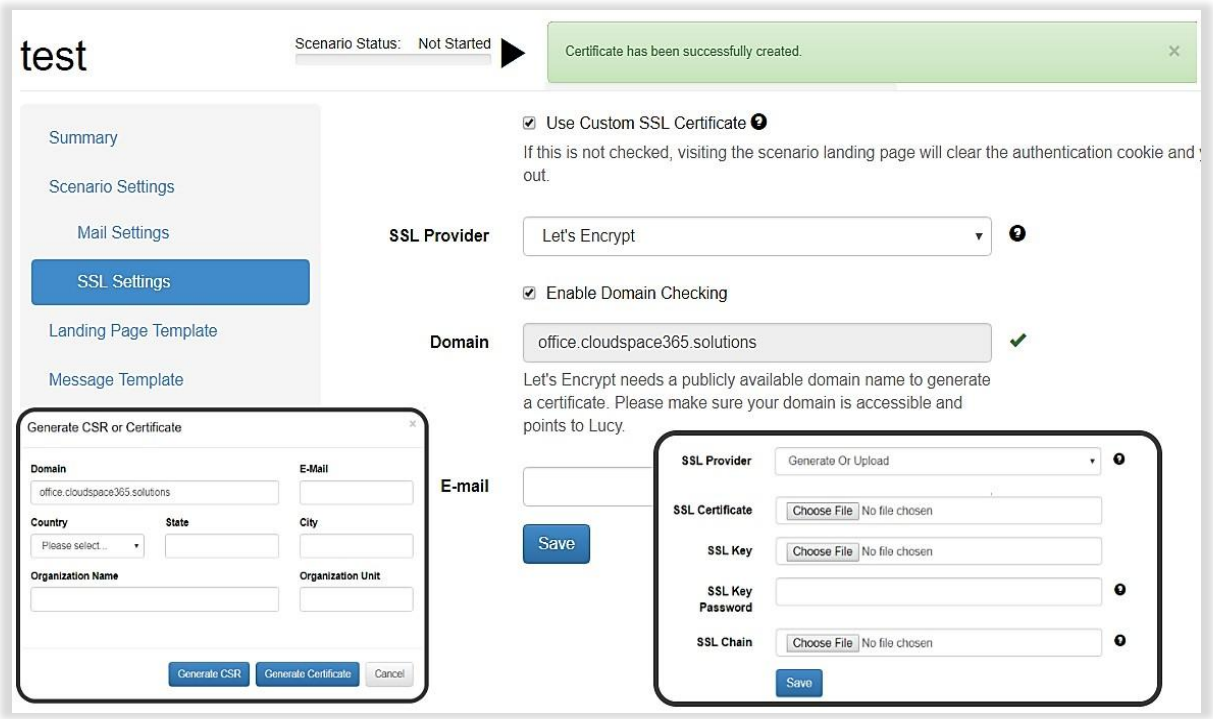
- **Strumenti di prestazione:** le routine smart LUCY adattano l'installazione del server alle risorse date. Durante installazioni o operazioni vengono calcolate operazioni server, dimensionamento DBMS, utilizzo memoria e CPU. Puoi dimensionare una singola installazione LUCY su cloud per oltre 400.000 utenti.



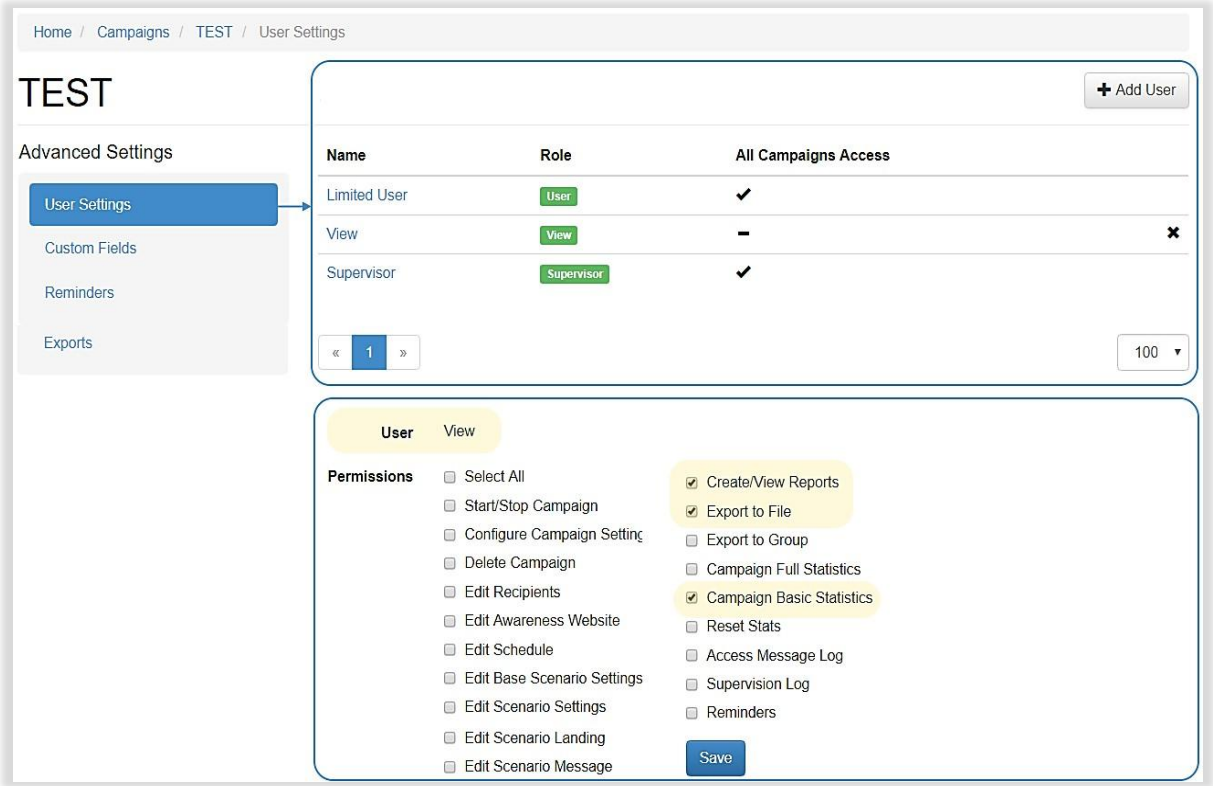
- **Interfaccia amministratore multilingue:** l'interfaccia amministratore LUCY è disponibile in diverse lingue e può essere tradotta in altre lingue su richiesta.



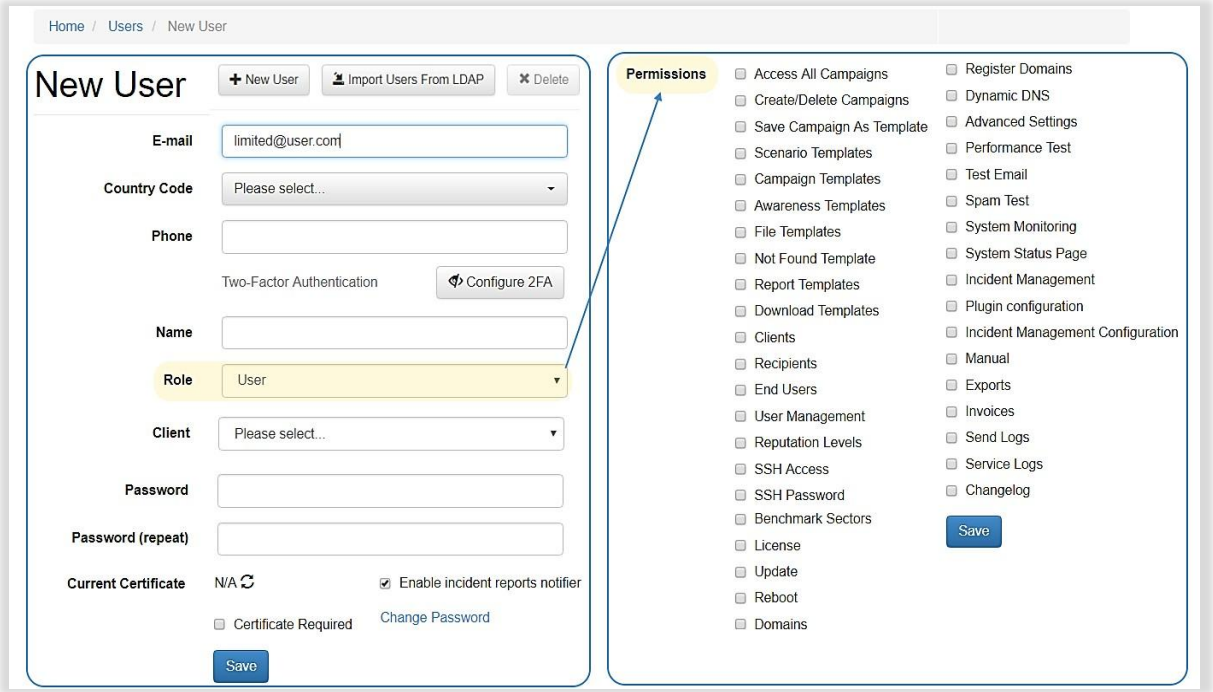
- **Certificato (SSL):** permette la creazione automatica di certificati ufficiali e verificati per amministratore, backend e campagne. LUCY utilizzerà automaticamente il dominio configurato nel sistema per generare il certificato. Se decidi di utilizzare SSL per la campagna, è possibile generare un certificato personalizzato o un CSR (certificate signing request). Puoi anche importare certificati ufficiali verificati.



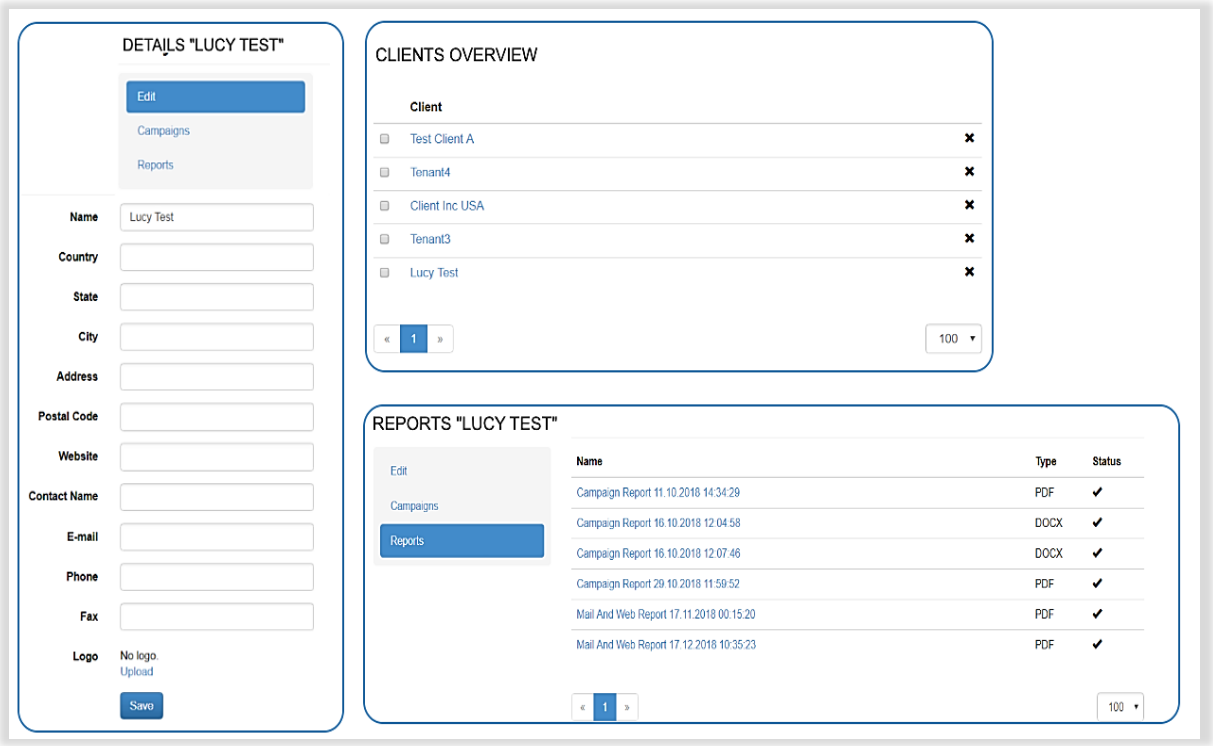
- **Controllo degli accessi basato sui ruoli:** LUCY offre un controllo di accesso basato sui ruoli (RBAC) che limita l'accesso al sistema solo agli utenti autorizzati. I permessi per eseguire determinate operazioni vengono assegnati a ruoli specifici all'interno delle impostazioni dell'utente. A membri o personale (o ad altri utenti del sistema) vengono assegnati ruoli particolari attraverso i quali acquisire i permessi necessari per eseguire particolari funzioni di LUCY.



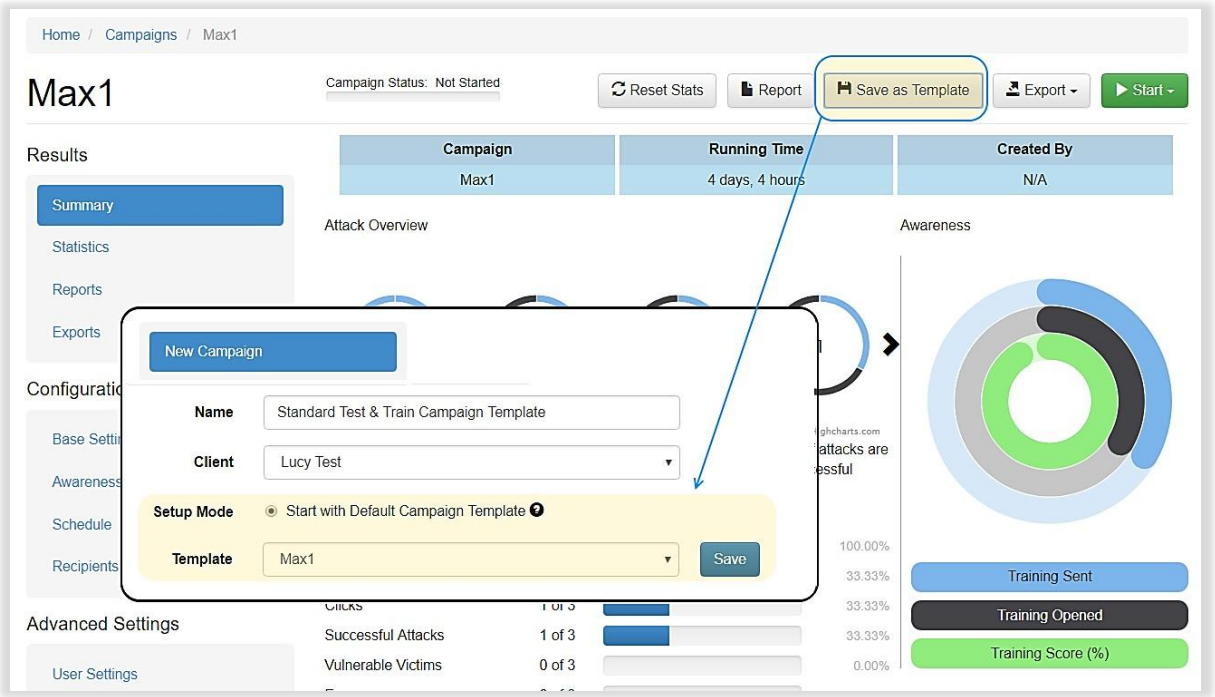
- **Gruppi di utenti a più livelli**: carica rapidamente utenti in gruppo tramite CSV, LDAP o file di testo. Crea diversi gruppi, organizzati per dipartimento, divisione, titolo ecc. Aggiorna gli utenti in una campagna in corso. Costruisci gruppi di utenti dinamici basati sui risultati della campagna di phishing.



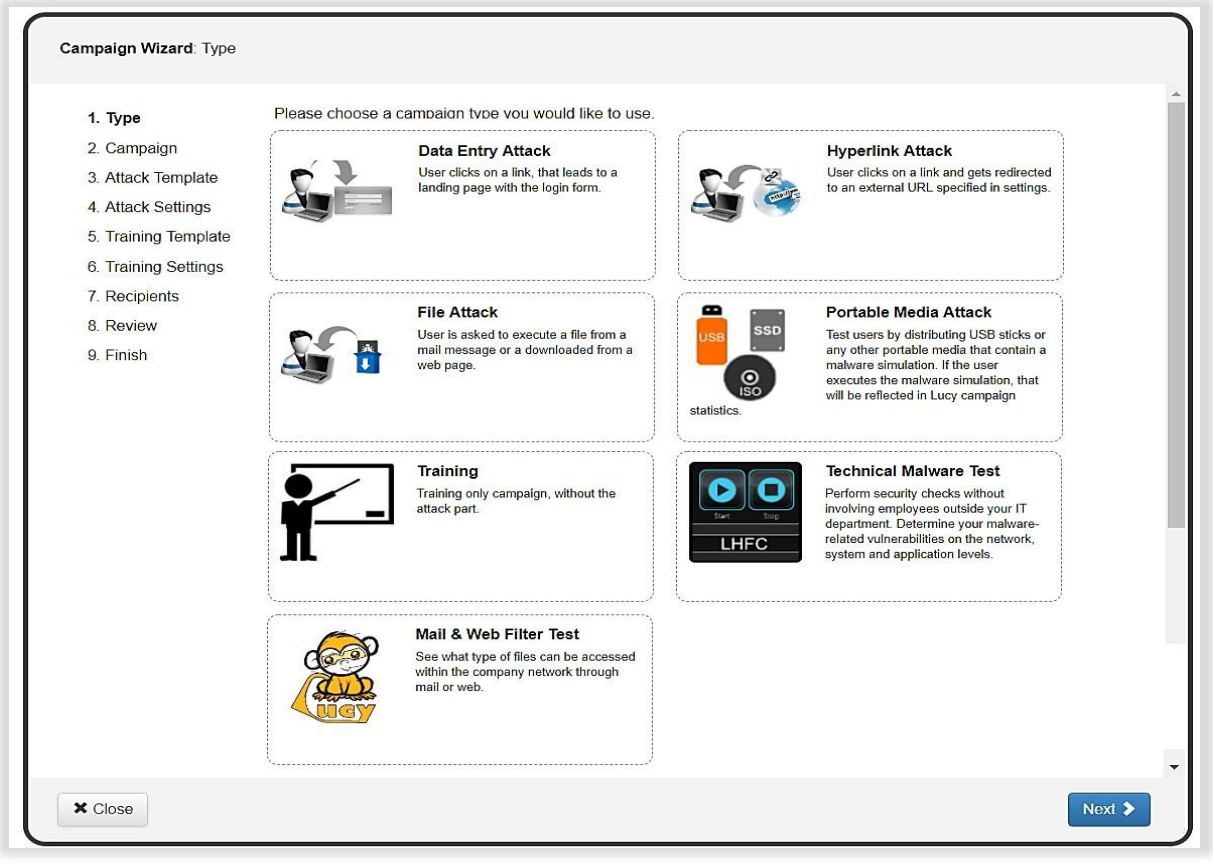
- **Compatibilità con più clienti:** "clienti" si riferisce a diverse società, dipartimenti o gruppi che hanno una campagna associata su LUCY. Questi clienti possono essere utilizzati, per esempio, per consentire accesso specifico alla campagna o per creare analisi specifiche per il cliente.



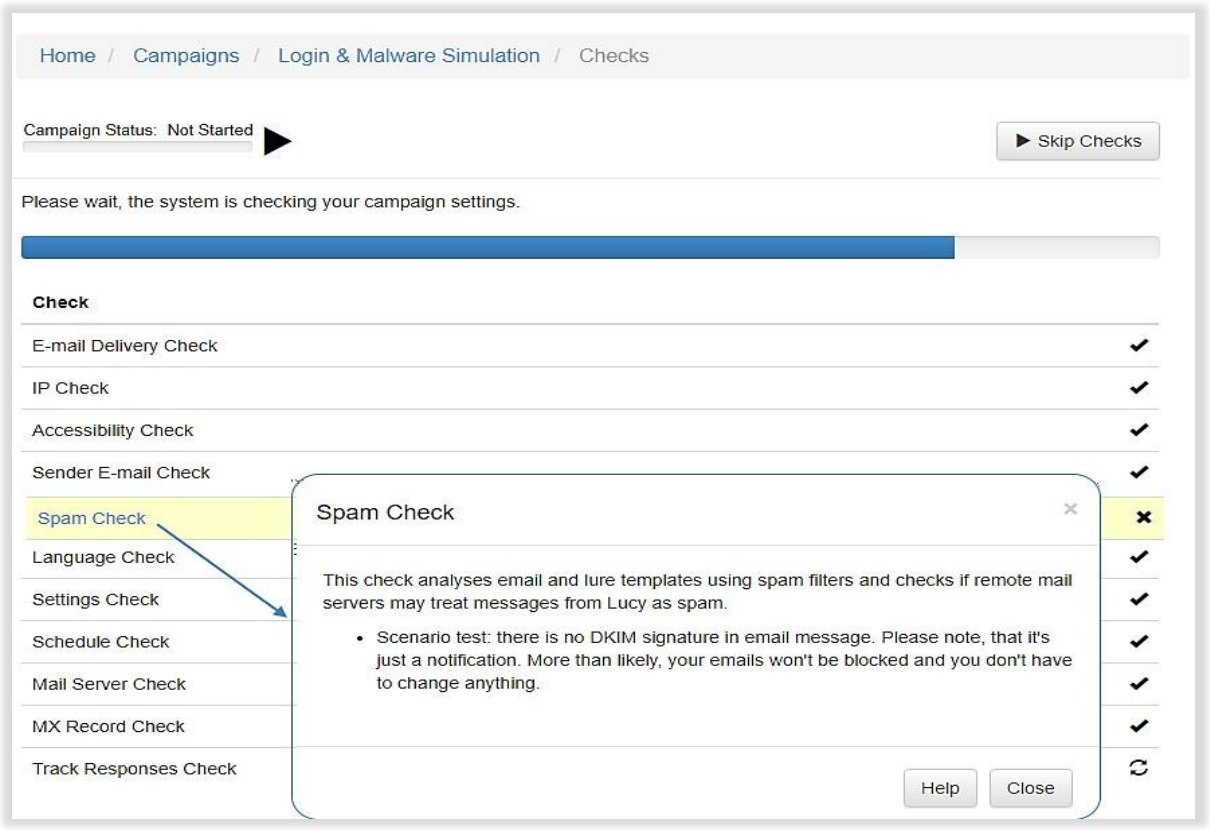
- **Modelli di campagna:** nel caso in cui voglia riutilizzare campagne simili, è possibile salvare una campagna completa con modelli di attacco e contenuti di e-learning come modello di campagna. Questa funzione consente di evitare di dover ripetere più volte configurazioni simili.



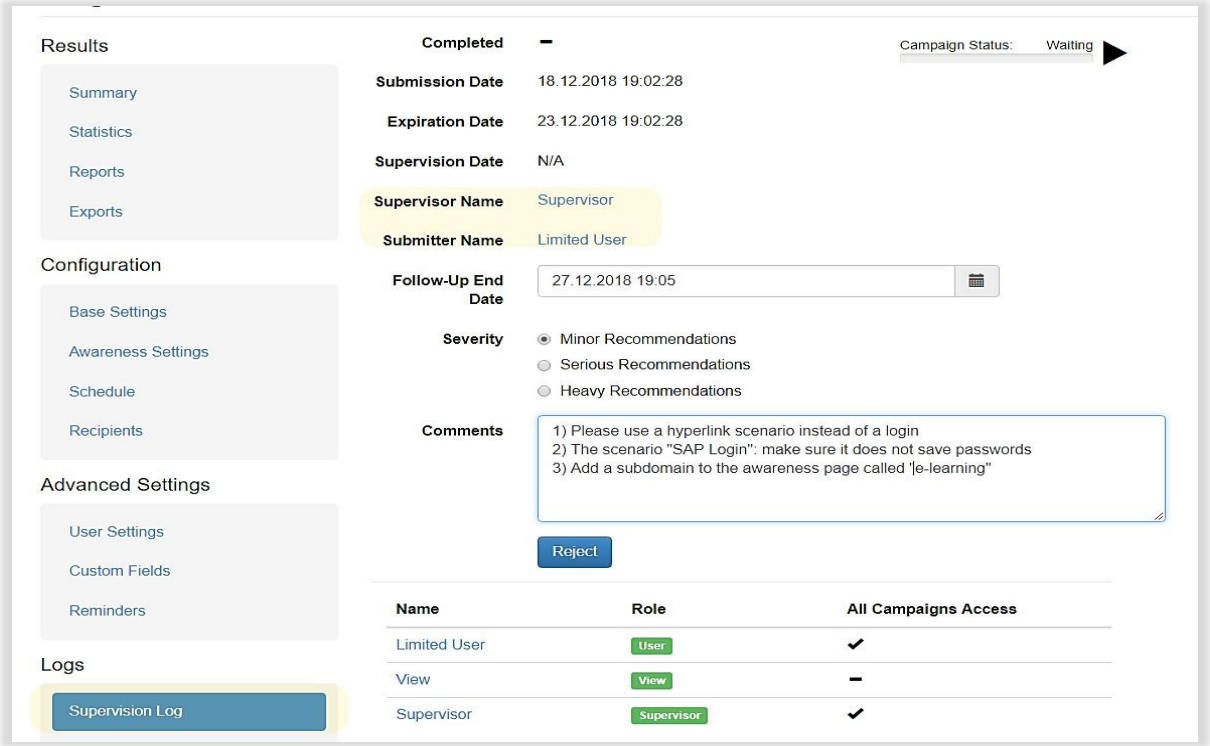
- **Configurazione guidata basata sui rischi:** LUCY offre diversi strumenti di configurazione. Crea una campagna completa in meno di 3 minuti utilizzando i modelli di campagna predefiniti o usufruisci della praticità della configurazione guidata. È disponibile una modalità di configurazione basata sui rischi opzionale, che fornisce suggerimenti specifici per la selezione di modelli di attacco e di sensibilizzazione in base alle dimensioni e al settore della società.



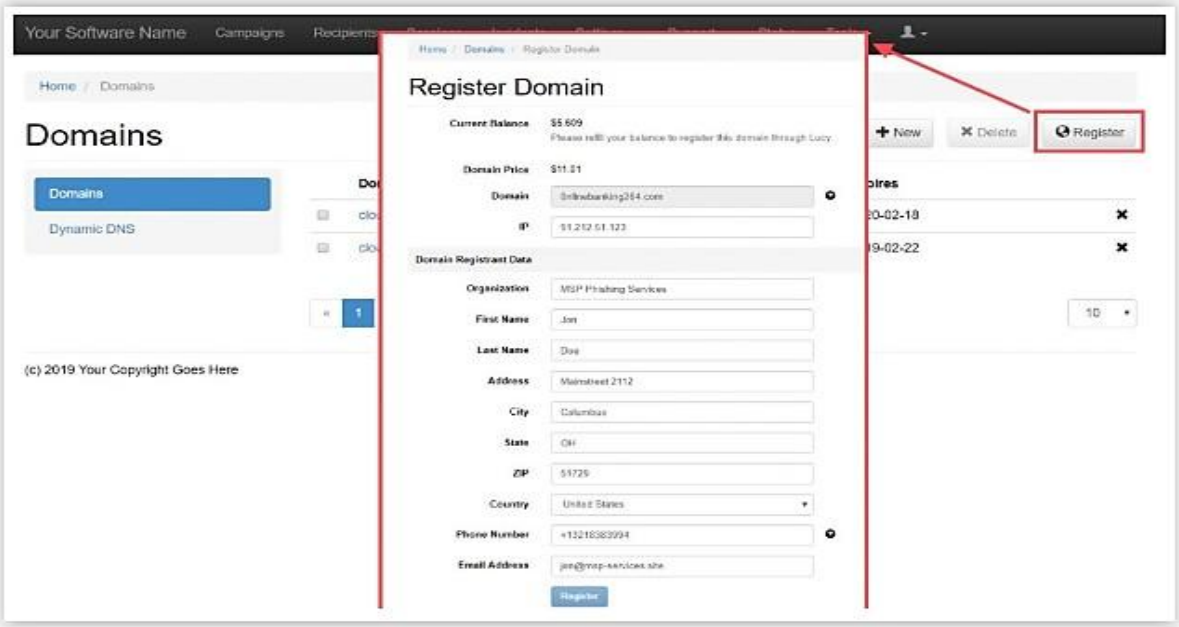
- **Verifica campagne:** effettua verifiche preliminari prima di avviare una campagna LUCY: verifica delle consegne via email, verifica dei record MX, verifica dei programmi, verifica di spam e altre.



- **Approvazione del flusso di lavoro:** una determinata campagna può essere sottoposto a un supervisore in LUCY per l'approvazione.

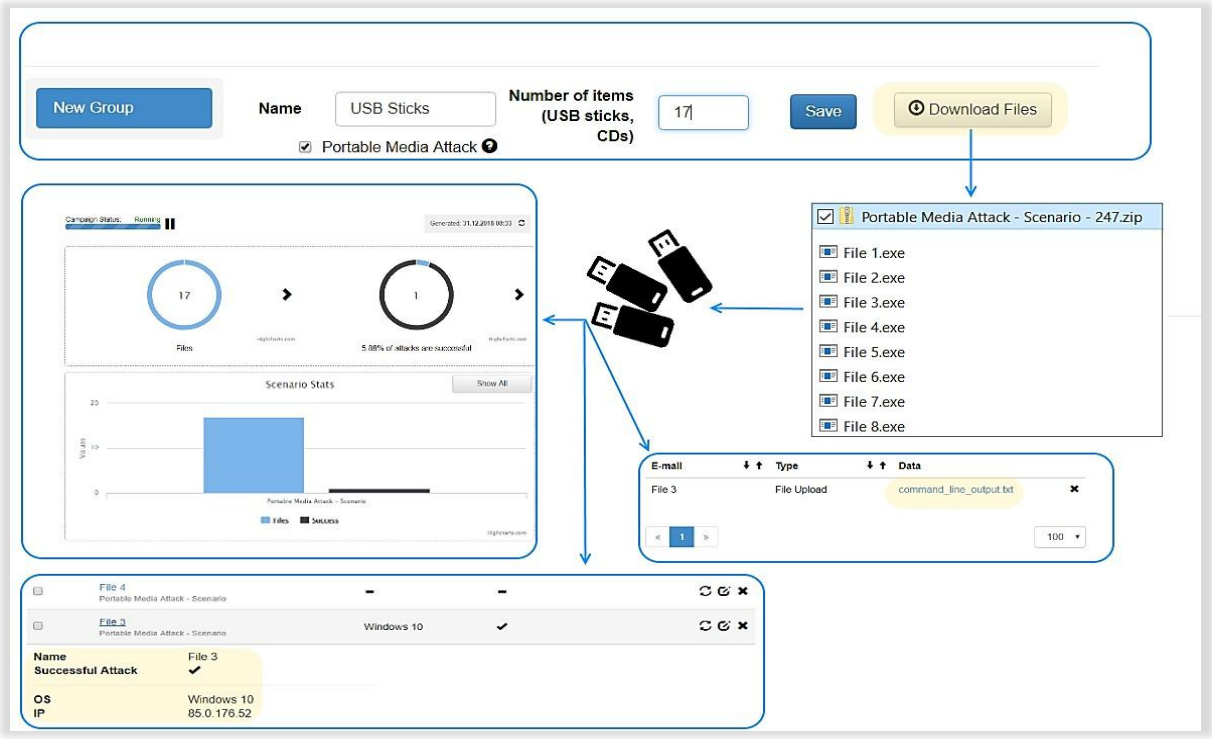


- **API DNS:** l'API DNS consente all'amministratore di creare qualsiasi dominio su LUCY in pochi secondi. Dato che gli aggressori utilizzano nomi di dominio simili a quelli di un cliente (pratica chiamata typosquatting), è possibile rappresentare questo rischio su LUCY. Se il dominio originale del cliente è, ad esempio, "onlinebanking.com", l'API DNS potrebbe essere utilizzato per riservare domini come "0nlinebanking.com", "onl1nebanking.com" o "onlinebanking.services" e assegnarlo successivamente a una campagna. LUCY crea quindi automaticamente le voci DNS corrispondenti (MX, SPF, protezione whois ecc.) per l'IP su cui è installato LUCY. Ovviamente, l'amministratore può utilizzare anche i domini del proprio provider su LUCY.

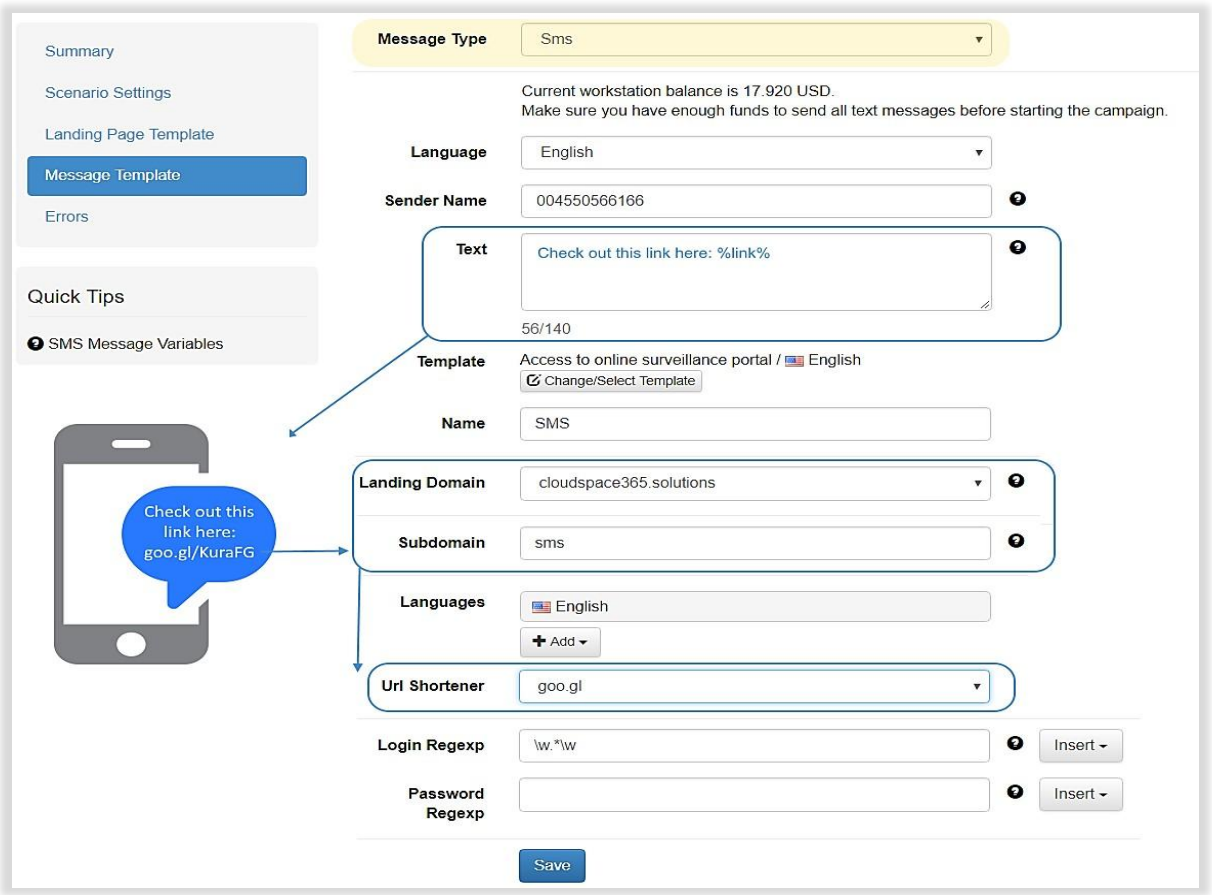


SIMULAZIONE DI ATTACCO

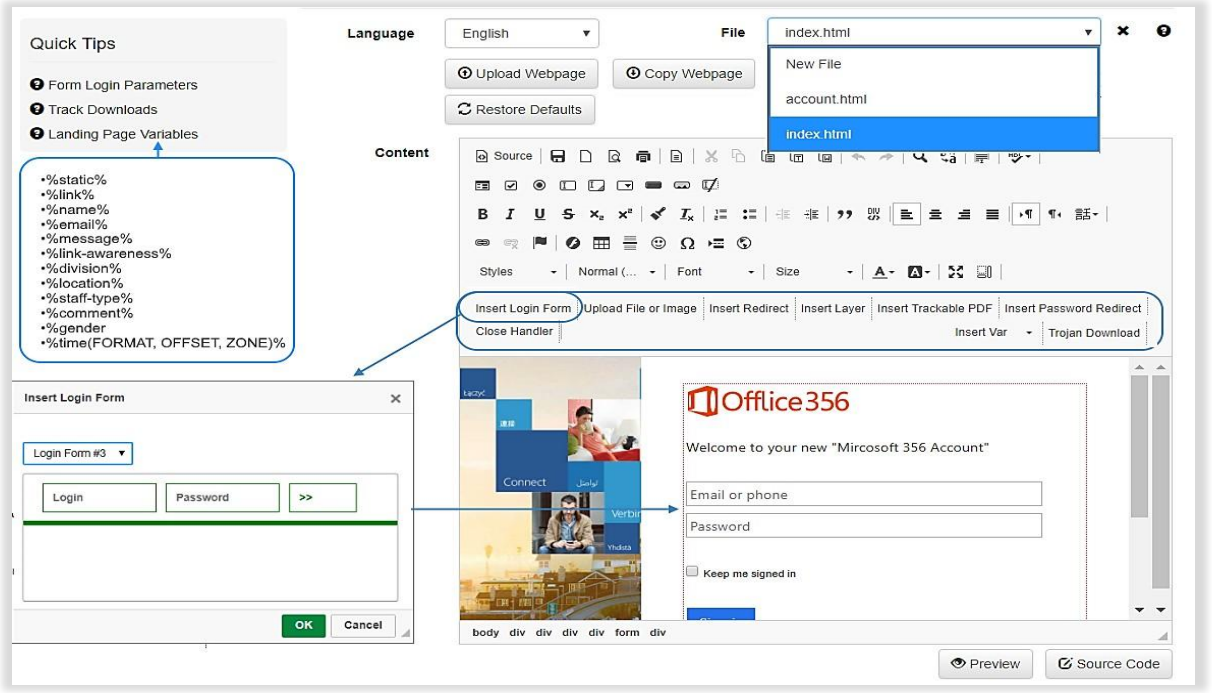
- **Attacchi con dispositivi multimediali portatili:** gli hacker possono utilizzare dispositivi multimediali portatili per accedere a informazioni sensibili memorizzate su un computer o una rete. LUCY offre la possibilità di eseguire attacchi con dispositivi multimediali portatili in cui un file modello (ad esempio, file eseguibile, archivio, documento word con macro ecc.) può essere memorizzato su un dispositivo multimediale portatile come USB, scheda SD o CD. È possibile monitorare attivazione (esecuzione) di questi singoli file su LUCY.



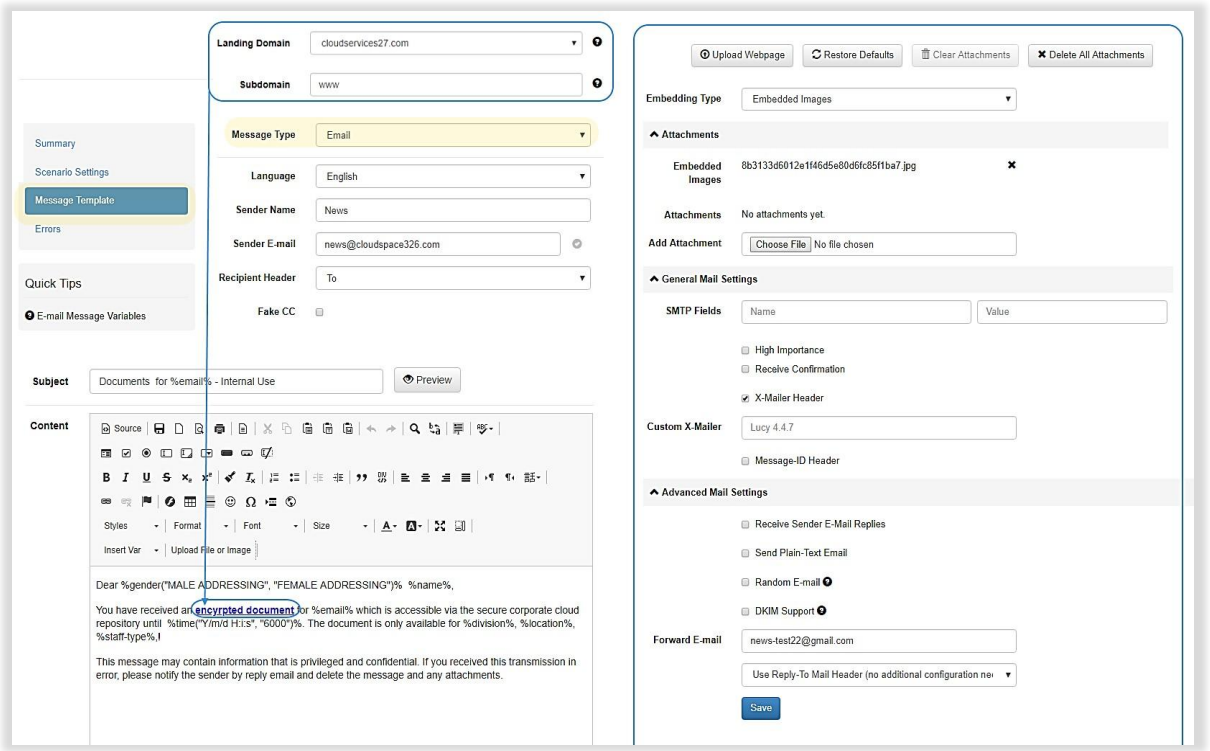
- **SMiShing:** lo smishing è, in un certo senso, "phishing SMS". Quando i criminali informatici effettuano "phishing", inviano email fraudolente per ingannare il destinatario ad aprire un allegato con malware o cliccare su un link malevole. Lo smishing utilizza i messaggi di testo anziché le email.



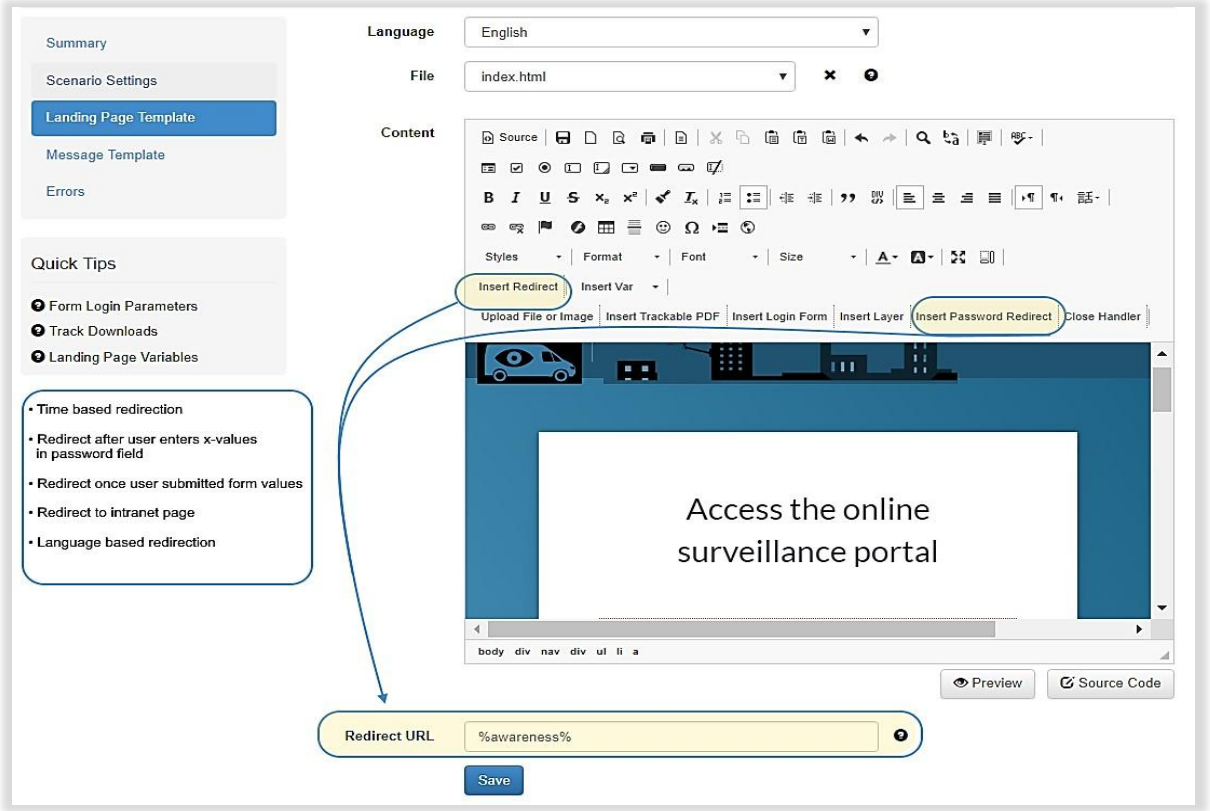
- **Attacchi di inserimento dati:** gli attacchi di inserimento dati possono comprendere una o più pagine web che intercettano l'inserimento di informazioni sensibili. Le pagine web disponibili possono essere facilmente personalizzate con l'editor web LUCY. Altri strumenti di editing consentono di impostare rapidamente funzioni come moduli di login, aree di download ecc. senza dover conoscere codice HTML.



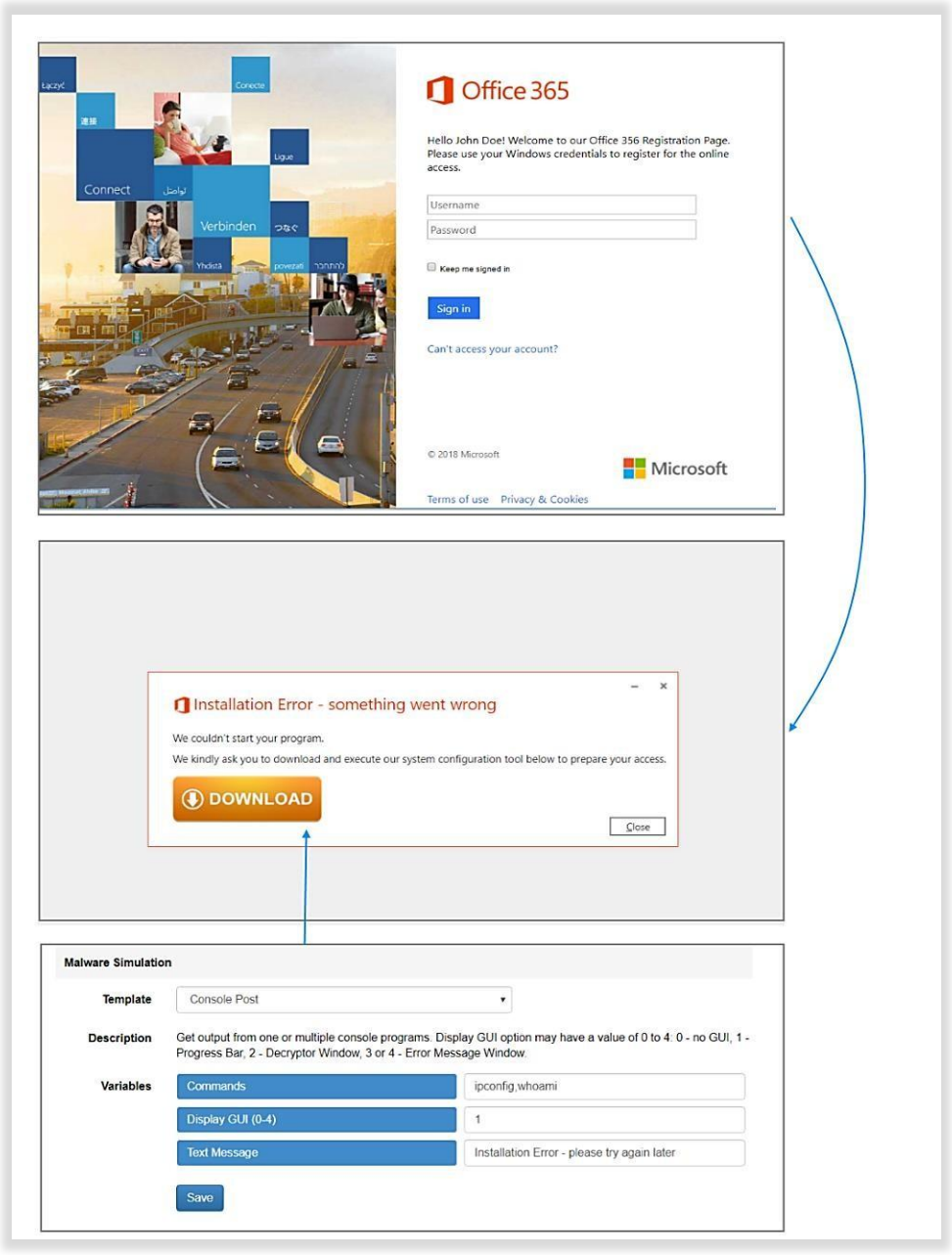
- **Attacchi con collegamenti ipertestuali:** una campagna basata su collegamenti ipertestuali invia agli utenti un'email contenente un URL di tracciamento randomizzato.



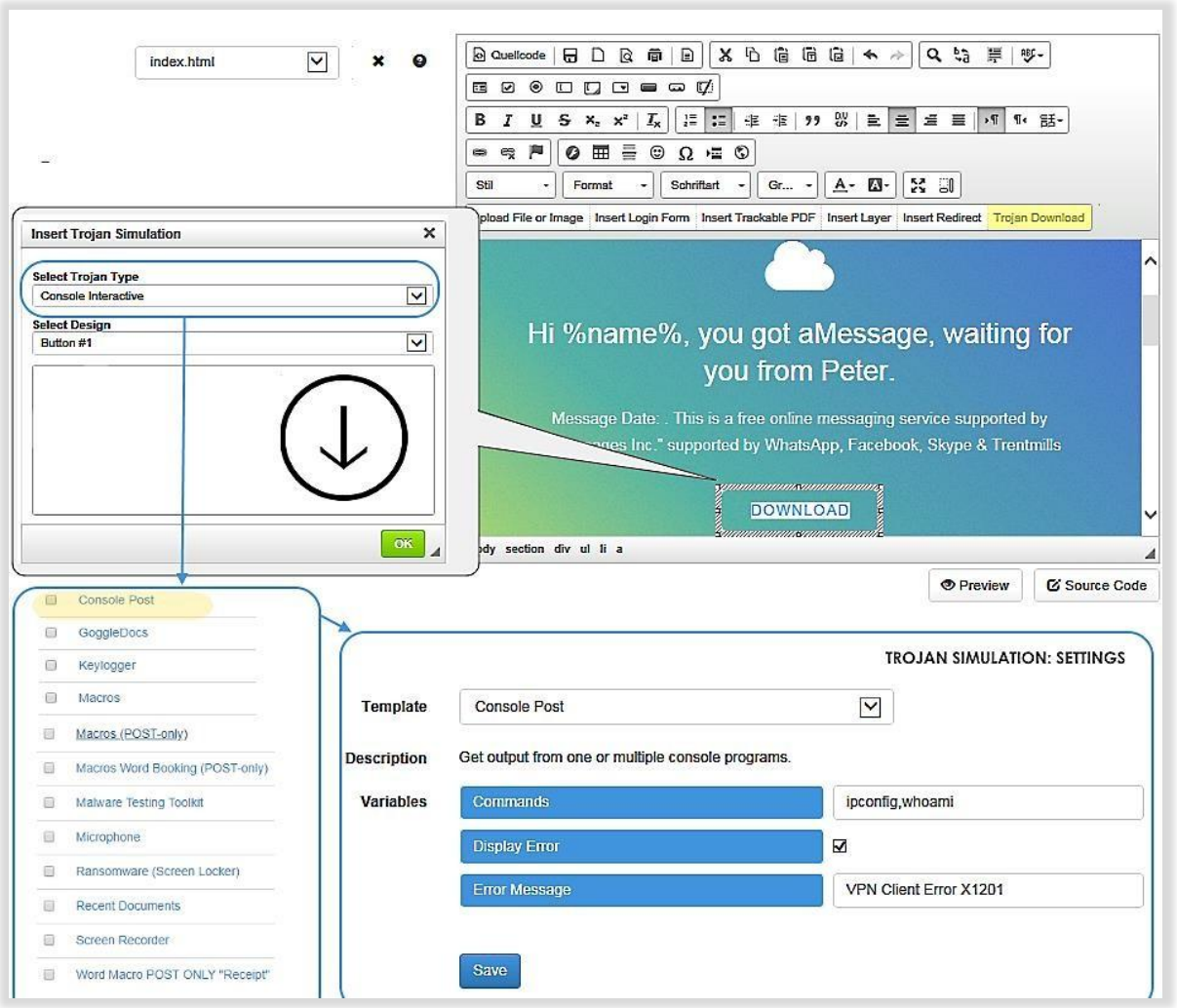
- **Toolkit di reindirizzamento URL potente:** le funzioni di reindirizzamento flessibili di LUCY consentono all'utente di essere guidato, al momento giusto, nell'area desiderata della simulazione di attacco o del corso di formazione. Per esempio, dopo aver inserito i primi 3 caratteri di una password in una simulazione di phishing, l'utente può essere reindirizzato alla pagina di formazione speciale relativa alla protezione delle password.



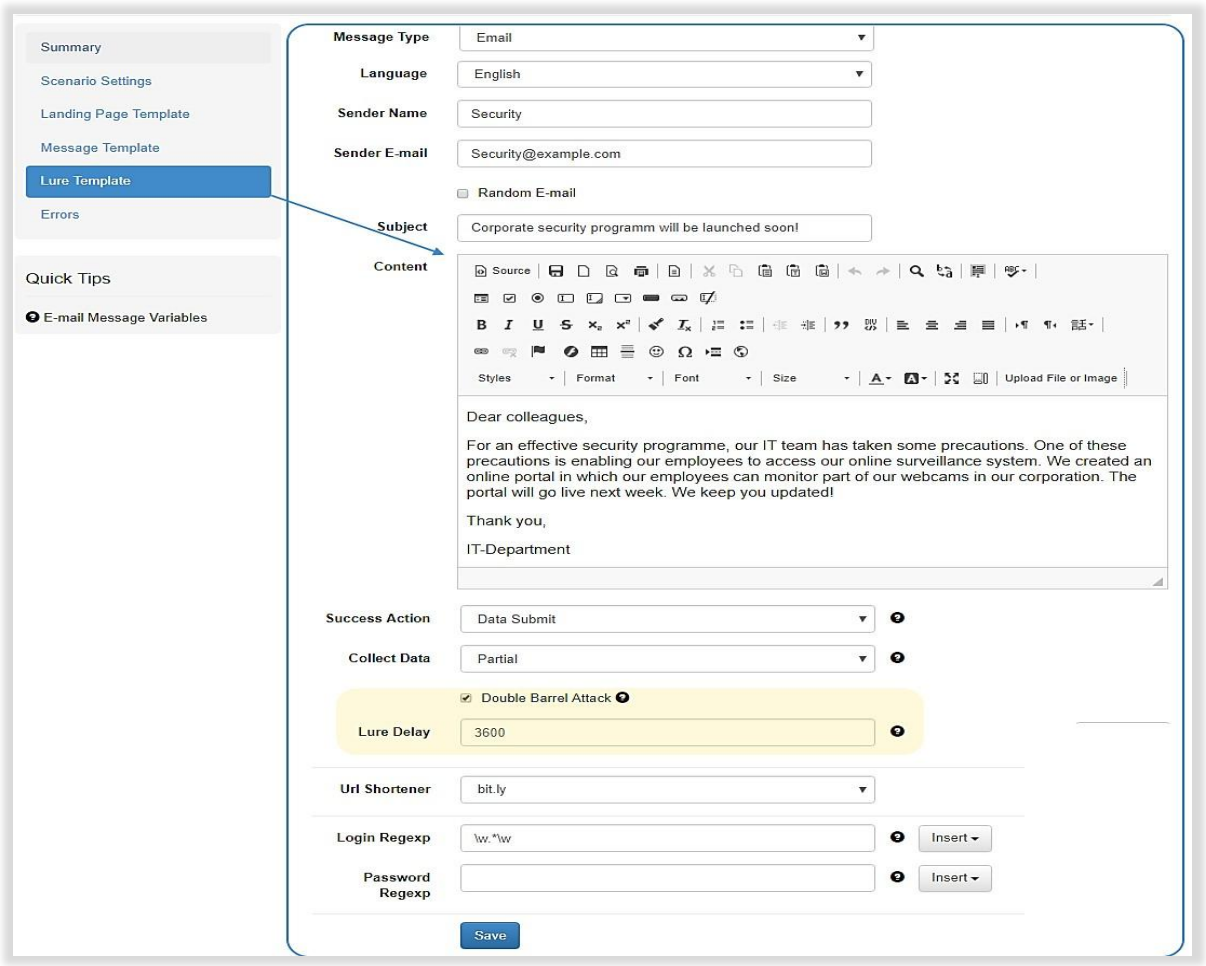
- **Attacchi misti:** gli attacchi misti consentono una combinazione di tipi di scenario multipli (basati su file, inserimento dati ecc.) nella stessa campagna.



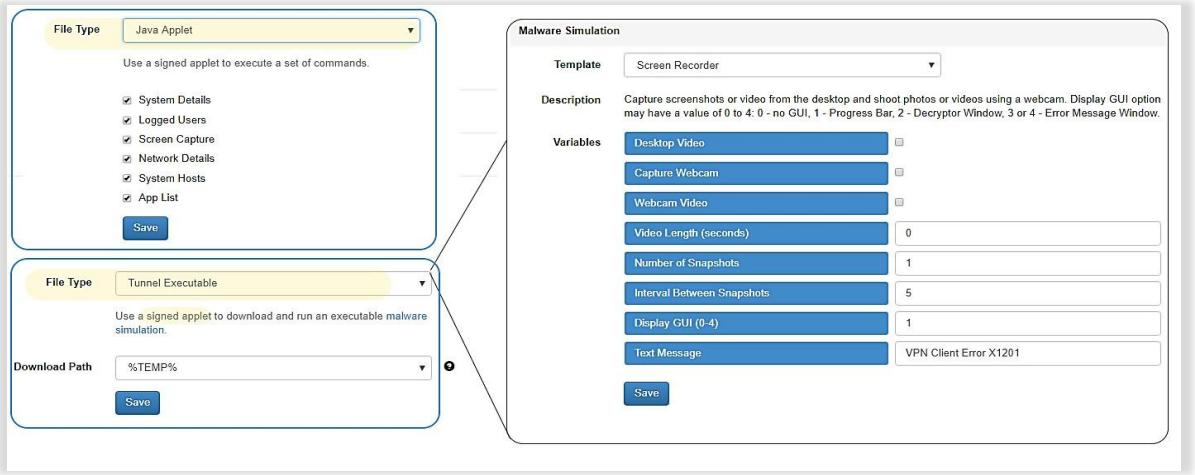
- **Attacchi basati su file:** gli attacchi basati su file consentono all'amministratore LUCY di integrare diversi tipi di file (documenti word con macro, PDF, eseguibili, MP3 ecc.) in allegati email o siti web generati su LUCY e di misurarne la velocità di download o esecuzione.



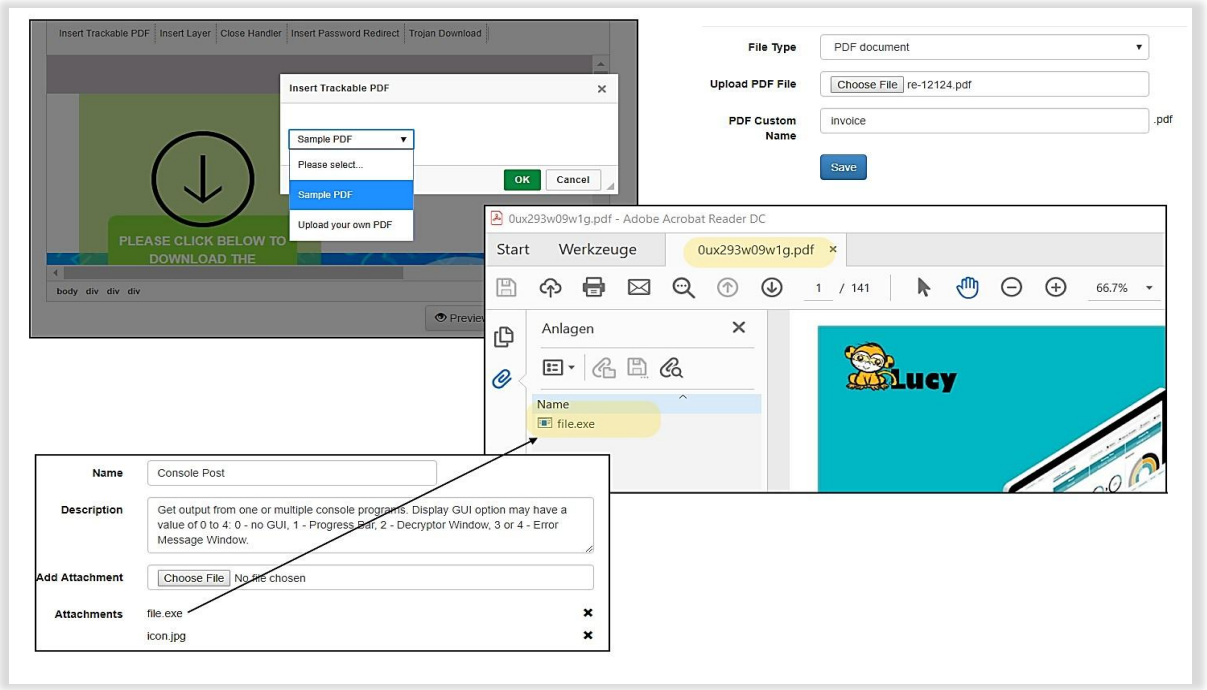
- **Attacchi doppietta:** questa funzione permette di inviare più email di phishing in ogni campagna, tra cui una prima email benigna (l'esca) che non contiene nulla di maligno e che non richiede una risposta da parte del destinatario.



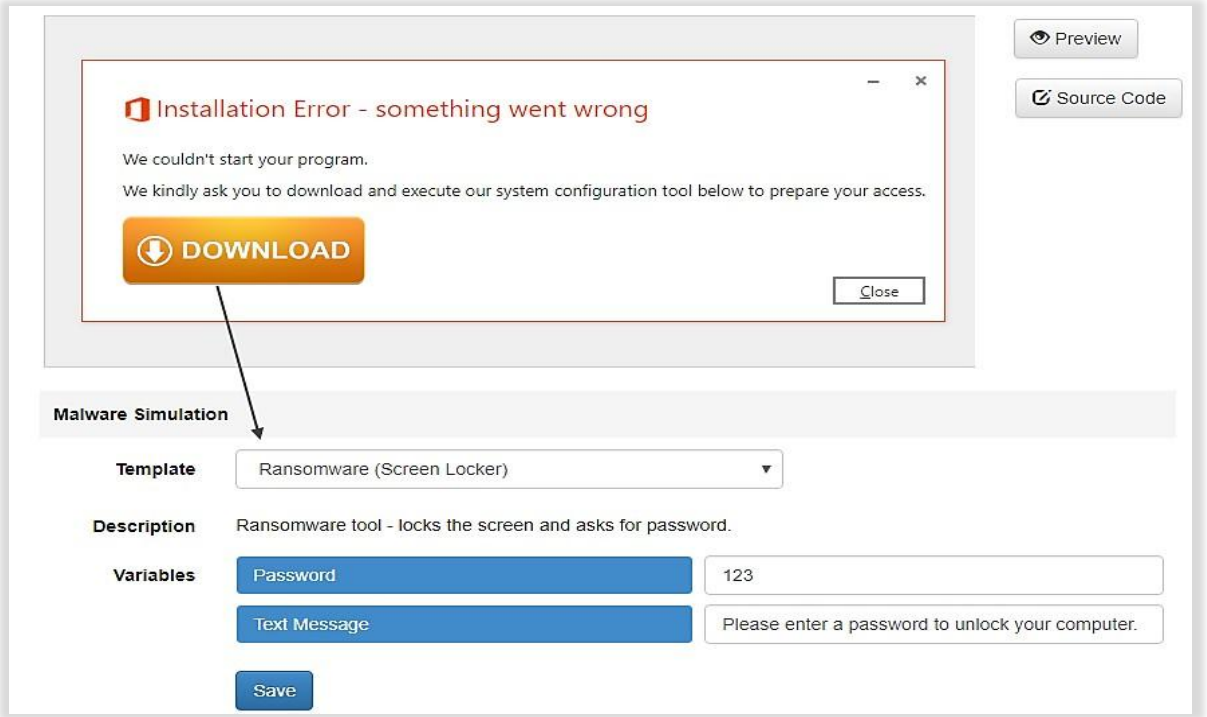
- **Attacchi basati su Java:** gli attacchi basati su Java consentono all'amministratore LUCY di integrare un applet verificato all'interno dei modelli di attacco basati su file o misti forniti su LUCY e di misurarne l'esecuzione da parte degli utenti.



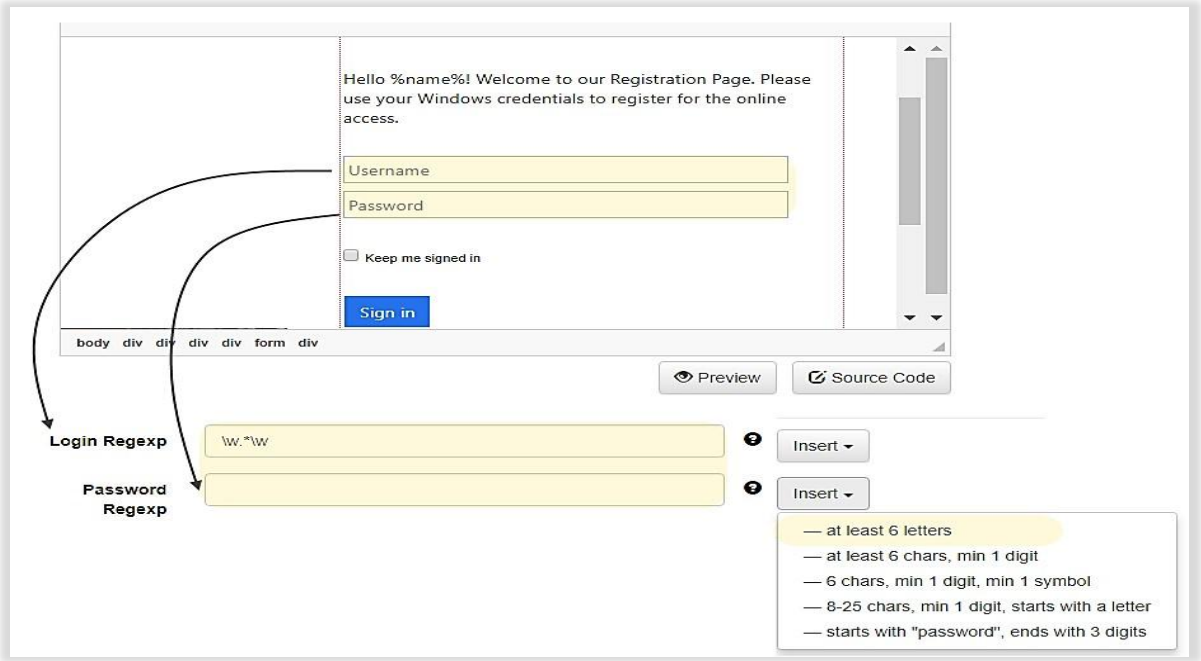
- **Attacchi basati su PDF:** con questo modulo è possibile simulare attacchi di phishing basati su PDF. LUCY consente di "nascondere" file eseguibili come allegati PDF e di misurarne l'esecuzione. Inoltre, è possibile generare collegamenti di phishing dinamici all'interno dei PDF.



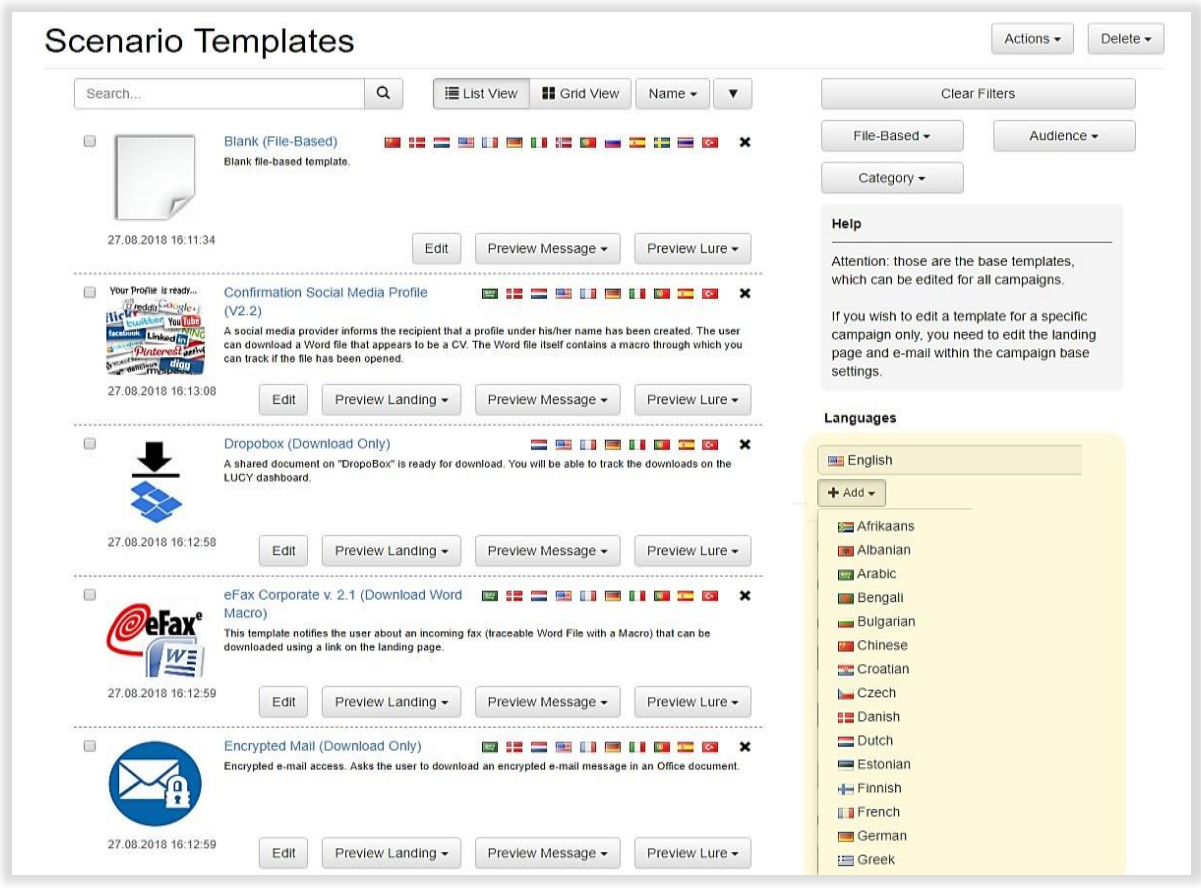
- **Attacchi di simulazione ransomware:** LUCY offre due diverse simulazioni di ransomware, una per mettere alla prova gli impiegati e l'altra l'infrastruttura.



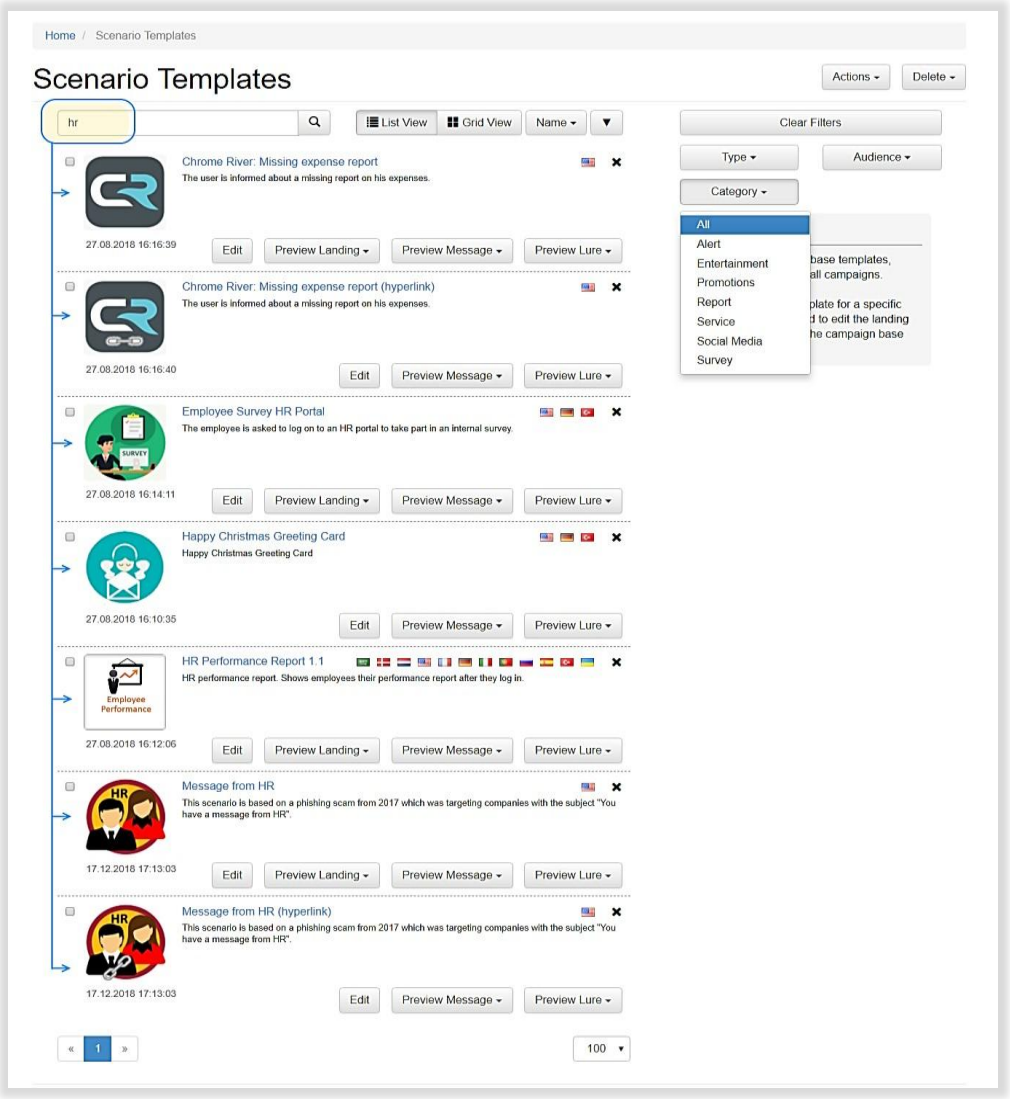
- **Toolkit di convalida inserimento dati:** nelle simulazioni di phishing, è importante prevenire falsi positivi nei campi di accesso (ad esempio, accesso con sintassi non valida). Le direttive societarie possono anche vietare la trasmissione di dati sensibili come password. Per questo motivo, LUCY mette a disposizione un motore di filtraggio dei dati inseriti flessibile che offre una soluzione adatta ad ogni esigenza.



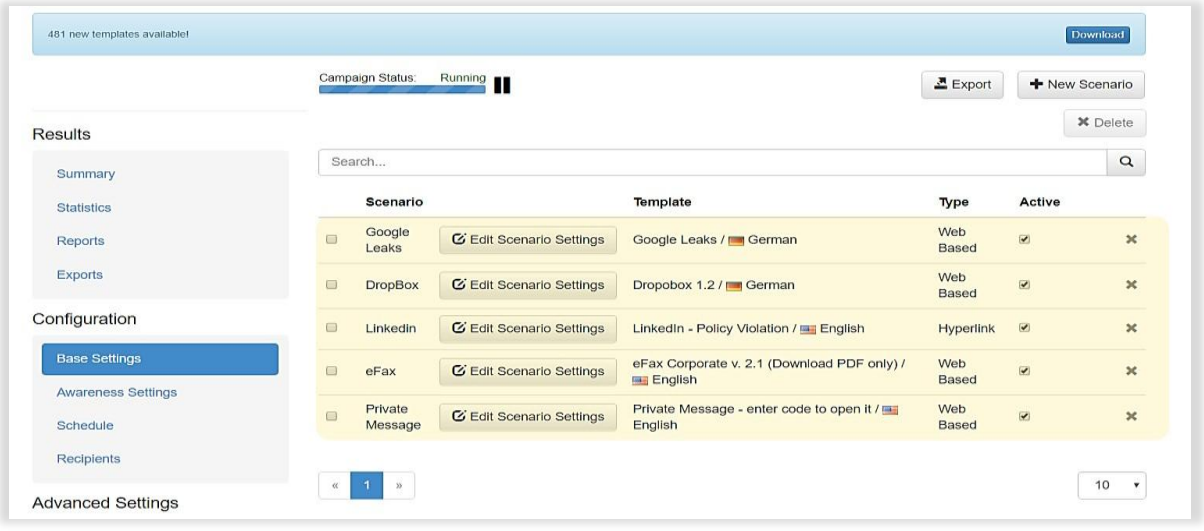
- **Libreria di modelli di attacco multilingue:** LUCY dispone di centinaia di modelli di attacco predefiniti in più di 30 lingue nelle categorie di inserimento dati (modelli con un sito web), basati su file (email o siti web con un download di file), collegamenti ipertestuali (email con un link), misti (combinazione di inserimento dati e download) e dispositivi multimediali portatili.



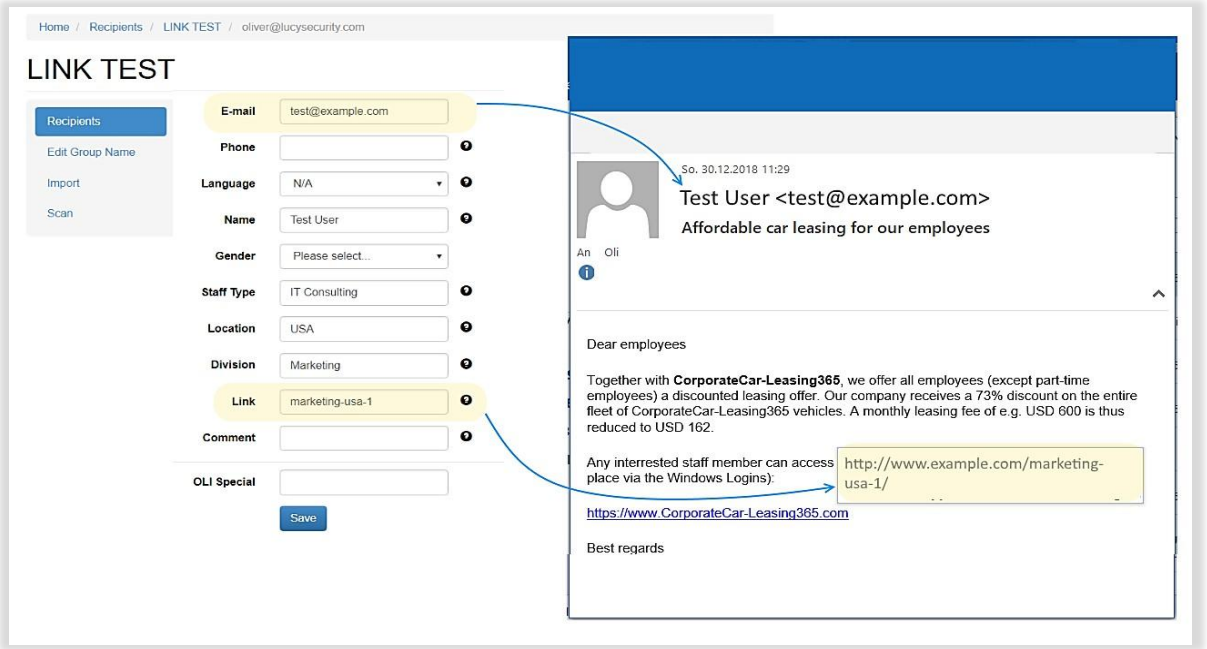
- **Modelli specifici per settore e divisione:** sono disponibili modelli di attacco specifici per settore o divisione.



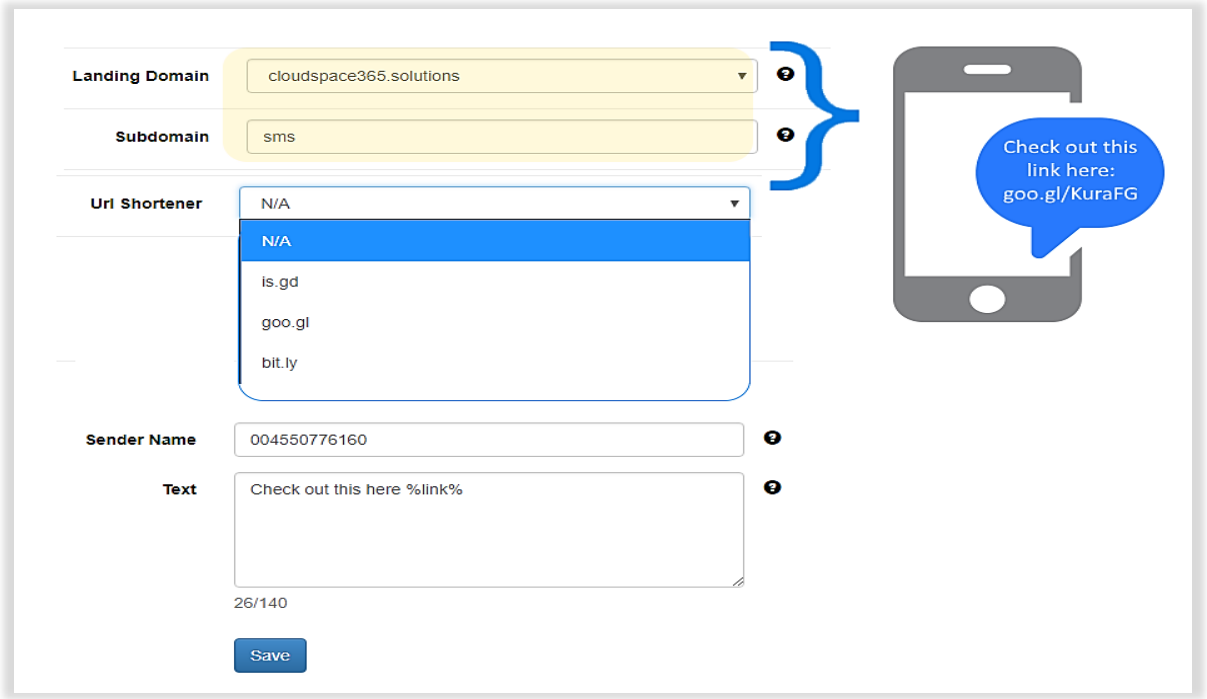
- **Utilizzo simultaneo di modelli di attacco:** LUCY ti offre la possibilità di utilizzare più modelli di attacco simulato in una singola campagna. Combina diversi tipi (collegamenti ipertestuali, basati su file ecc.) con diversi temi di attacco per ottenere la più ampia copertura di rischio possibile e una migliore comprensione delle vulnerabilità degli impiegati. In combinazione con il nostro schedulatore randomizzato, è possibile eseguire modelli di attacco complessi per un periodo di tempo più lungo.



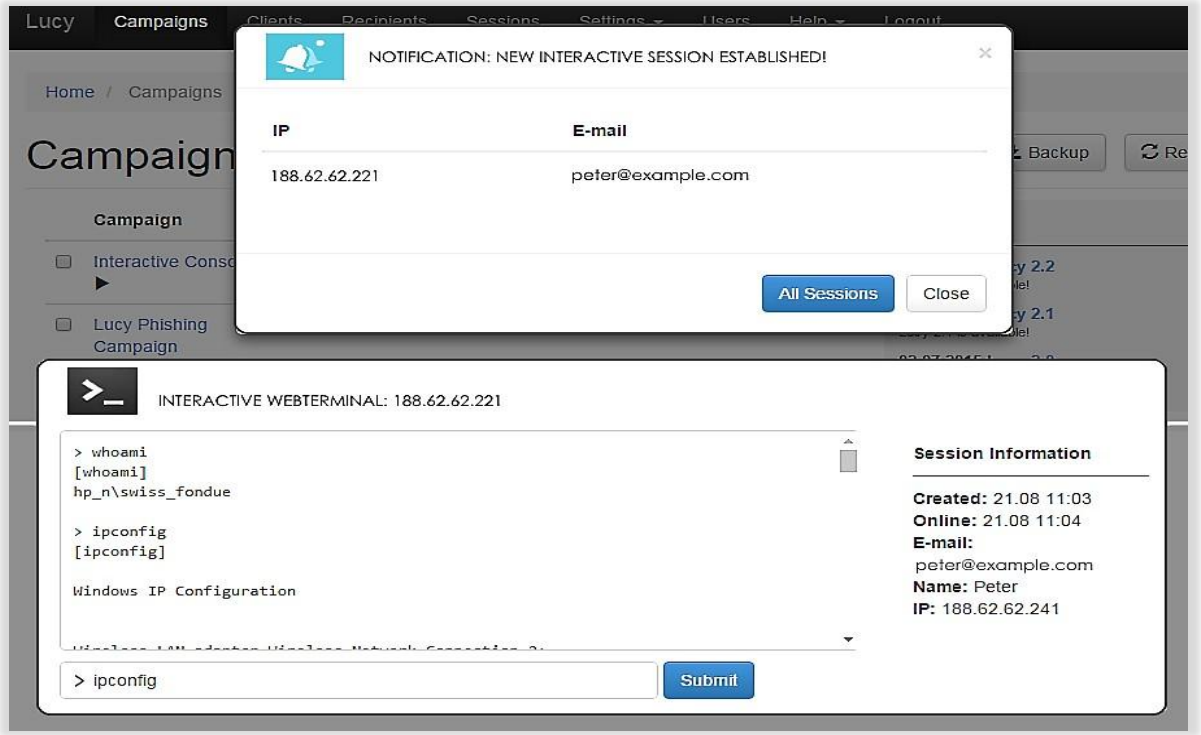
- **Variazioni degli URL di attacco:** prendi il controllo degli URL generati per identificare i destinatari. Utilizza stringhe di URL brevi (< 5 caratteri) o lunghe automatizzate o imposta URL singoli per ogni utente. La creazione manuale di URL consente di formare link che un utente può facilmente ricordare. Questo è indispensabile negli ambienti in cui i click sui link sono disabilitati nelle email.



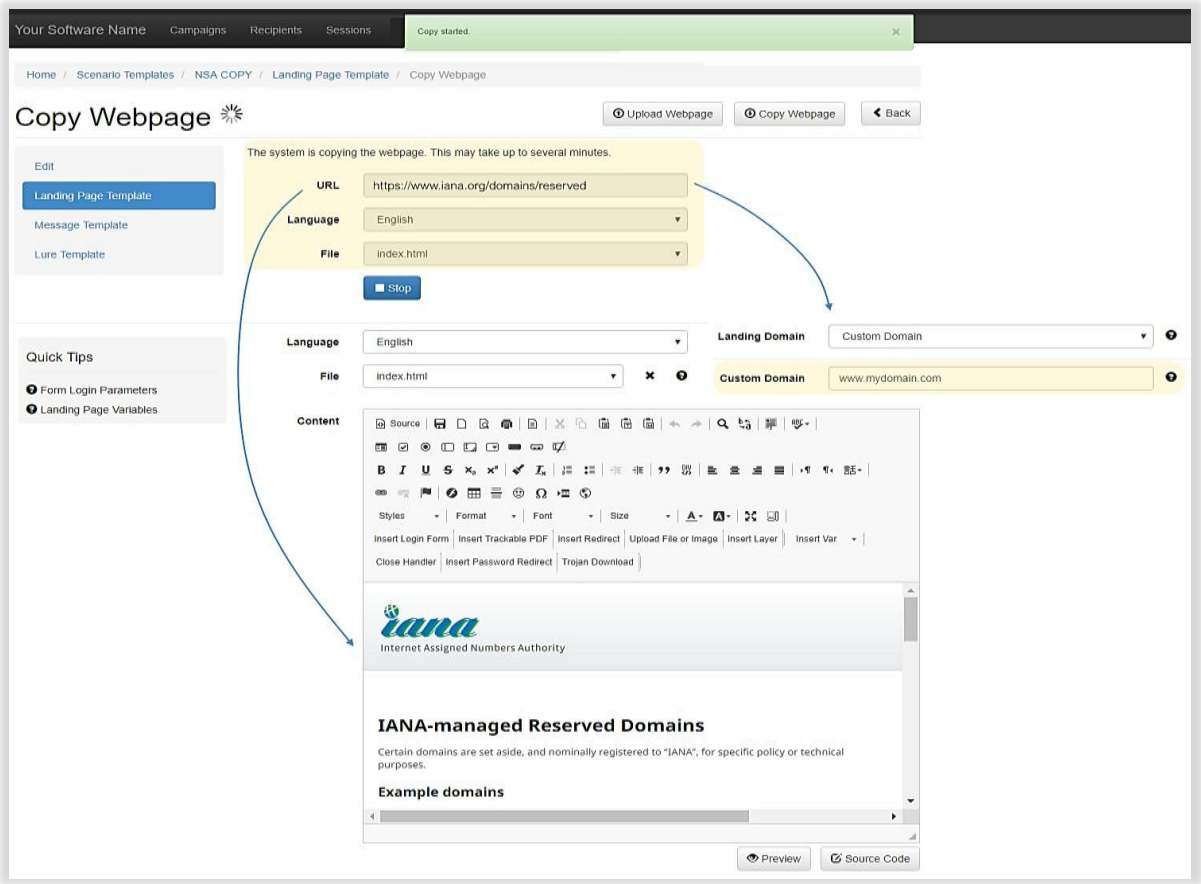
- **Accorciamento URL:** l'accorciamento degli URL è un servizio internet relativamente nuovo. Dato che molti servizi social online impongono limitazioni sui caratteri (ad es. Twitter), questi URL sono molto pratici. L'accorciamento di URL può, tuttavia, essere utilizzato da criminali informatici per nascondere il vero obiettivo di un link, come ad esempio phishing o siti web infetti. Per questo motivo LUCY offre la possibilità di integrare diversi servizi di accorciamento all'interno di una campagna di phishing o smishing.



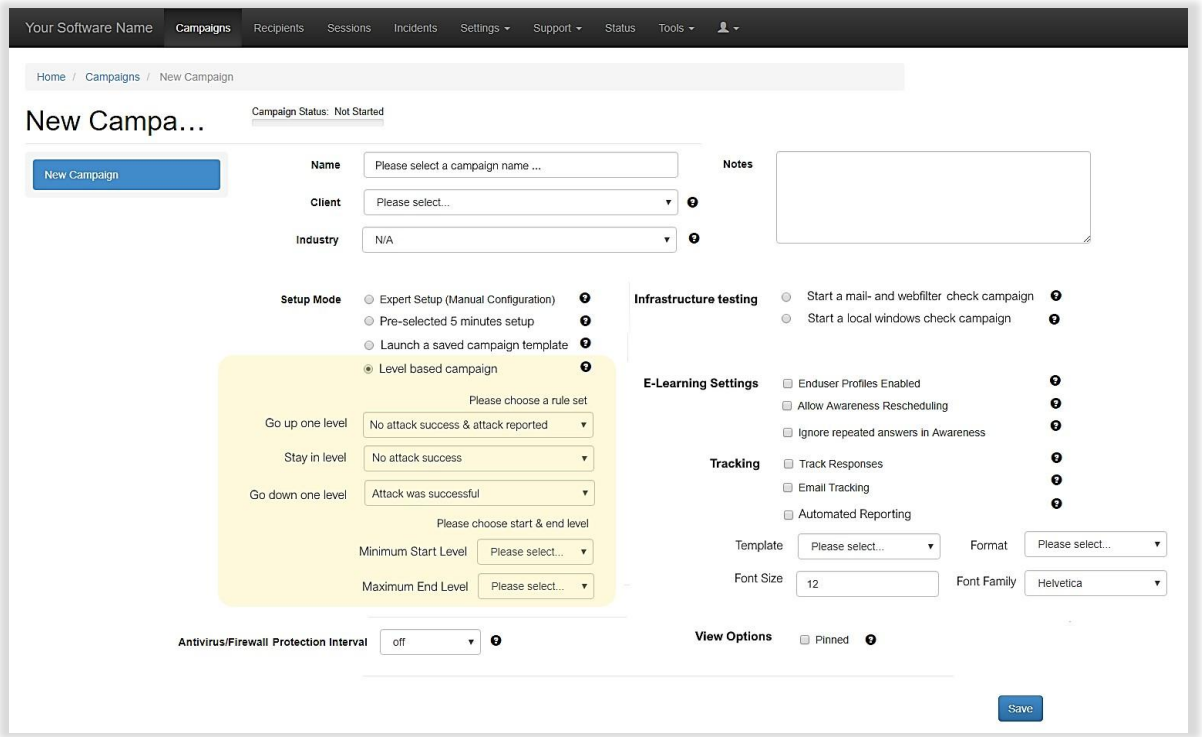
- **Kit pentest:** il kit pentest è un sottomodulo di un toolkit di simulazione malware ed è indicato con il nome di "sessioni interattive". Consente di comunicare in modo interattivo con un pc client che si trova dietro i firewall usando connessioni http/s inverse.



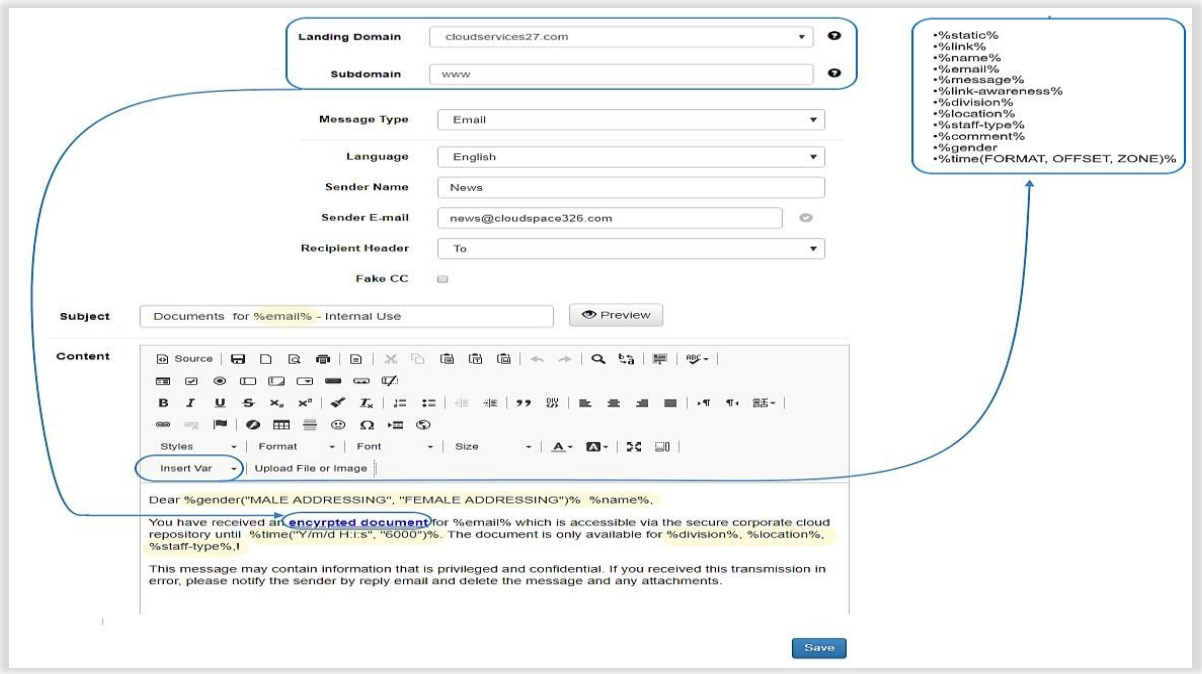
- **Duplicatore siti web:** crea rapidamente delle landing page altamente professionali per le tue campagne. Duplica siti web esistenti e aggiungi ulteriori livelli con campi di inserimento dati, file da scaricare e altro.



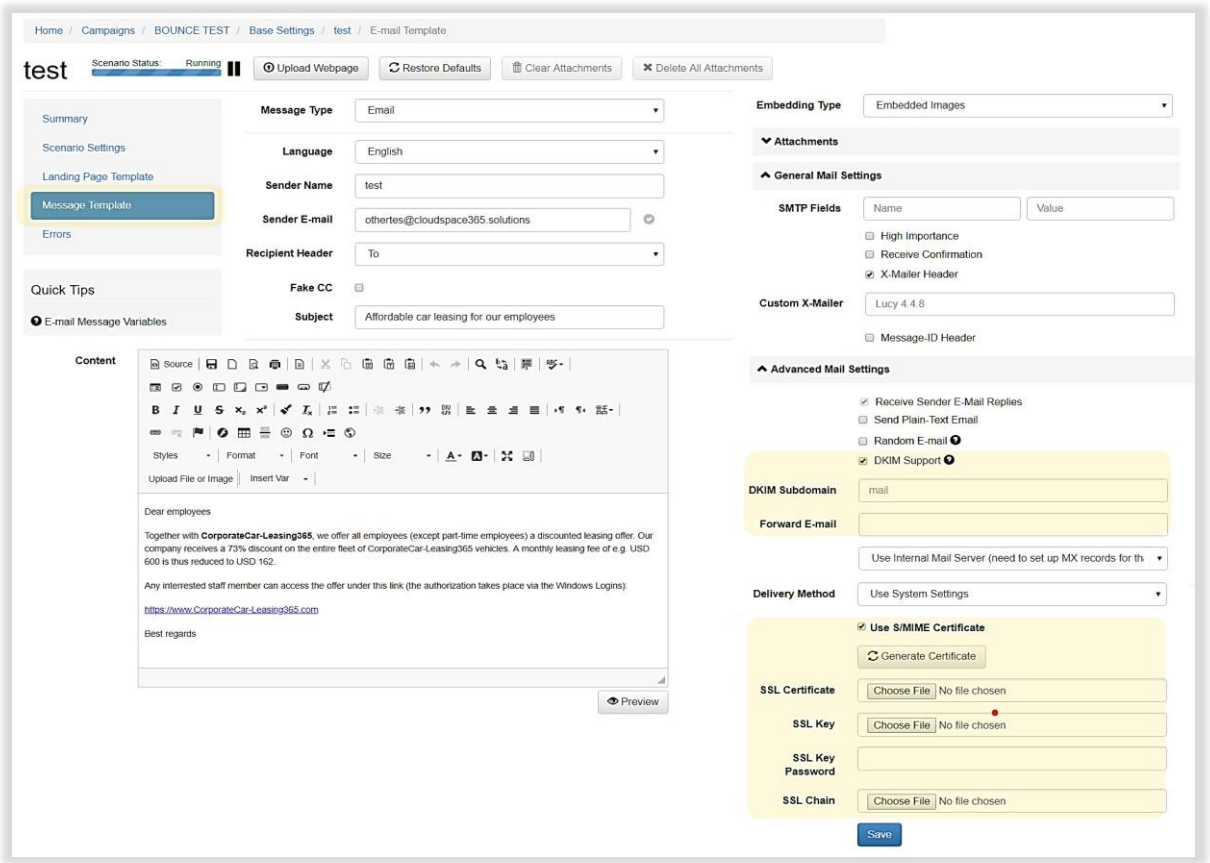
- **Attacchi basati su livelli:** il programma di formazione sul phishing basato su livelli per gli impiegati serve per rendere misurabile il rischio di hackeraggio sociale. Le analisi scientifiche permettono di identificare i fattori di rischio in modo da poter offrire contenuti di formazione individuali automaticamente.



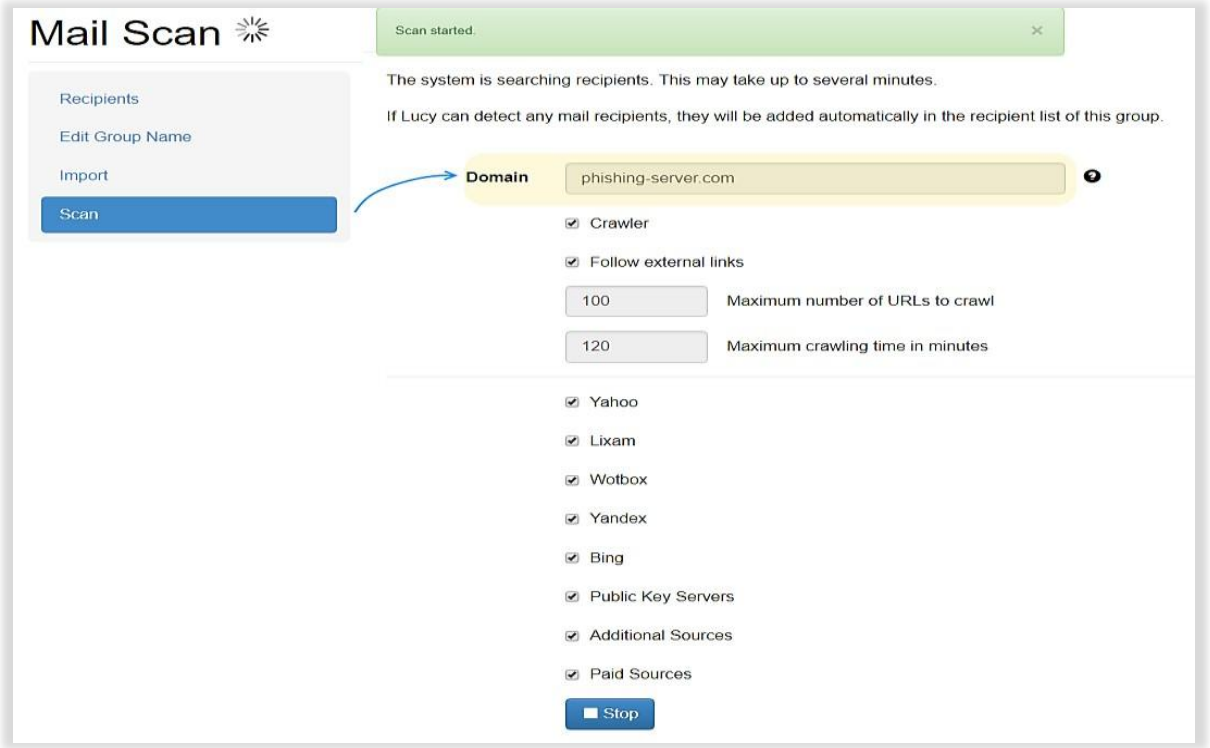
- **Simulazione di spear phishing:** il sistema di simulazione spear phishing funziona con variabili dinamiche (genere, orario, nome, email, link, messaggi, divisione, nazione ecc.) utilizzabili in modelli di landing o messaggi.



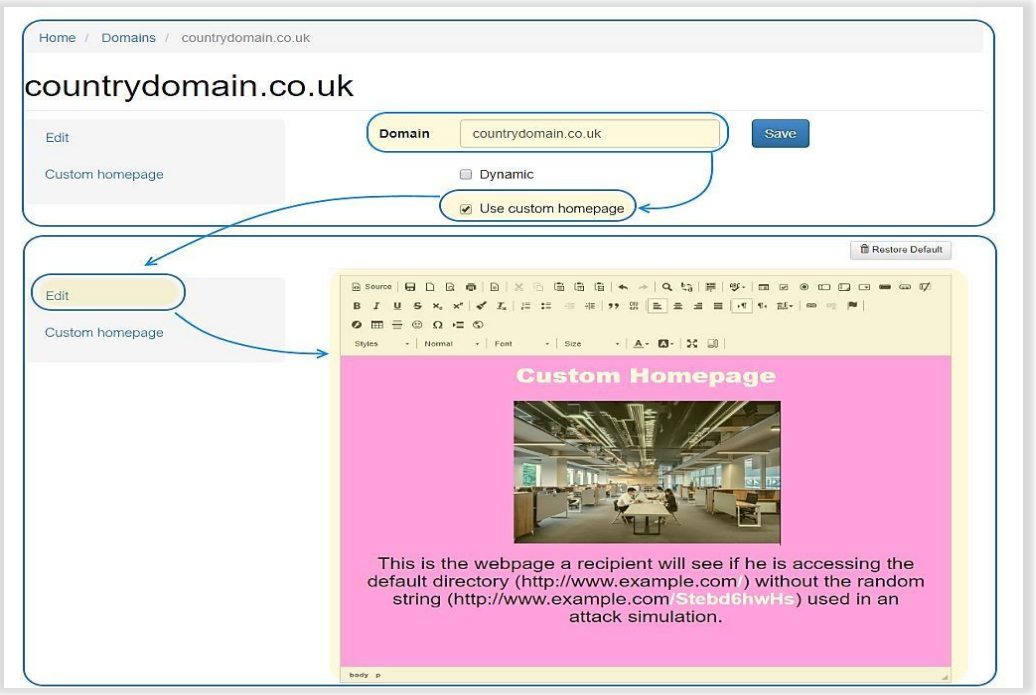
- **Supporto DKIM / S / MIME per email di phishing:** firme digitali per email: invia email di phishing simulato firmate (s/mime). Usa DKIM per ottenere un punteggio mittente migliore.



- **Scansione email:** vuoi scoprire quali indirizzi email della tua società si possono trovare su Internet? Utilizza il sistema di scansione email LUCY e scopri cosa un hacker conosce già sulla tua società.

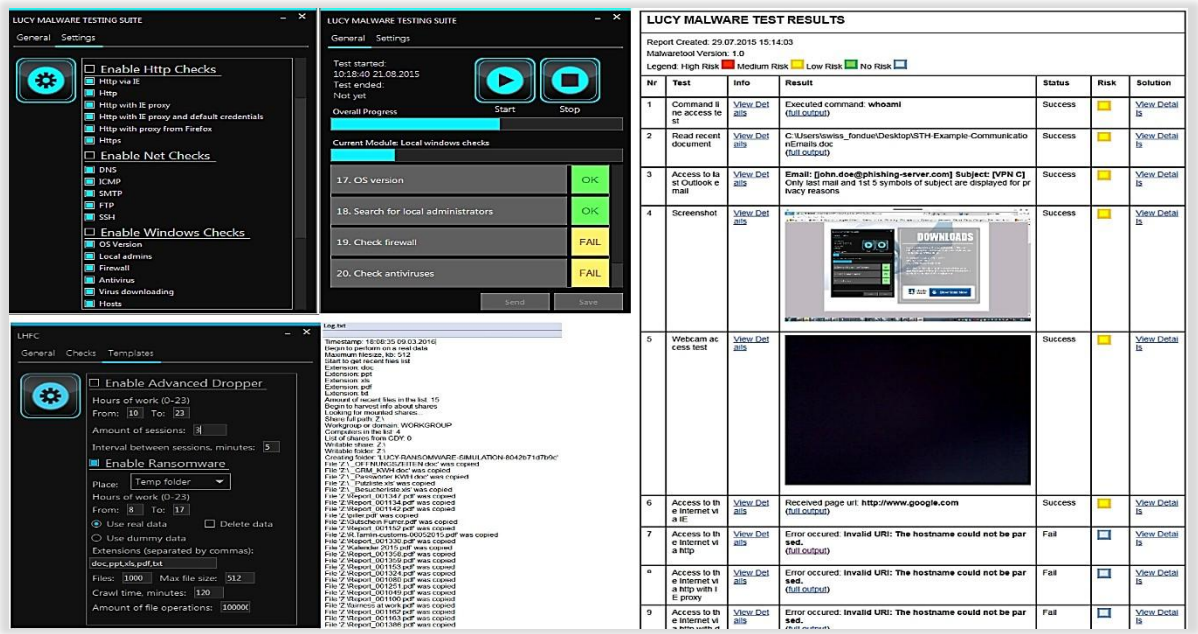


- **Creazione homepage personalizzata:** i destinatari con migliori competenze tecniche potrebbero usare il loro browser per trovare il dominio o l'indirizzo IP associato al link di phishing generato in modo casuale. Per evitare che compaiano messaggi di errore o che l'utente finale arrivi addirittura nell'area di accesso della console amministratore, è possibile creare delle "homepage" generiche all'interno di LUCY per i domini utilizzati nella simulazione di phishing.

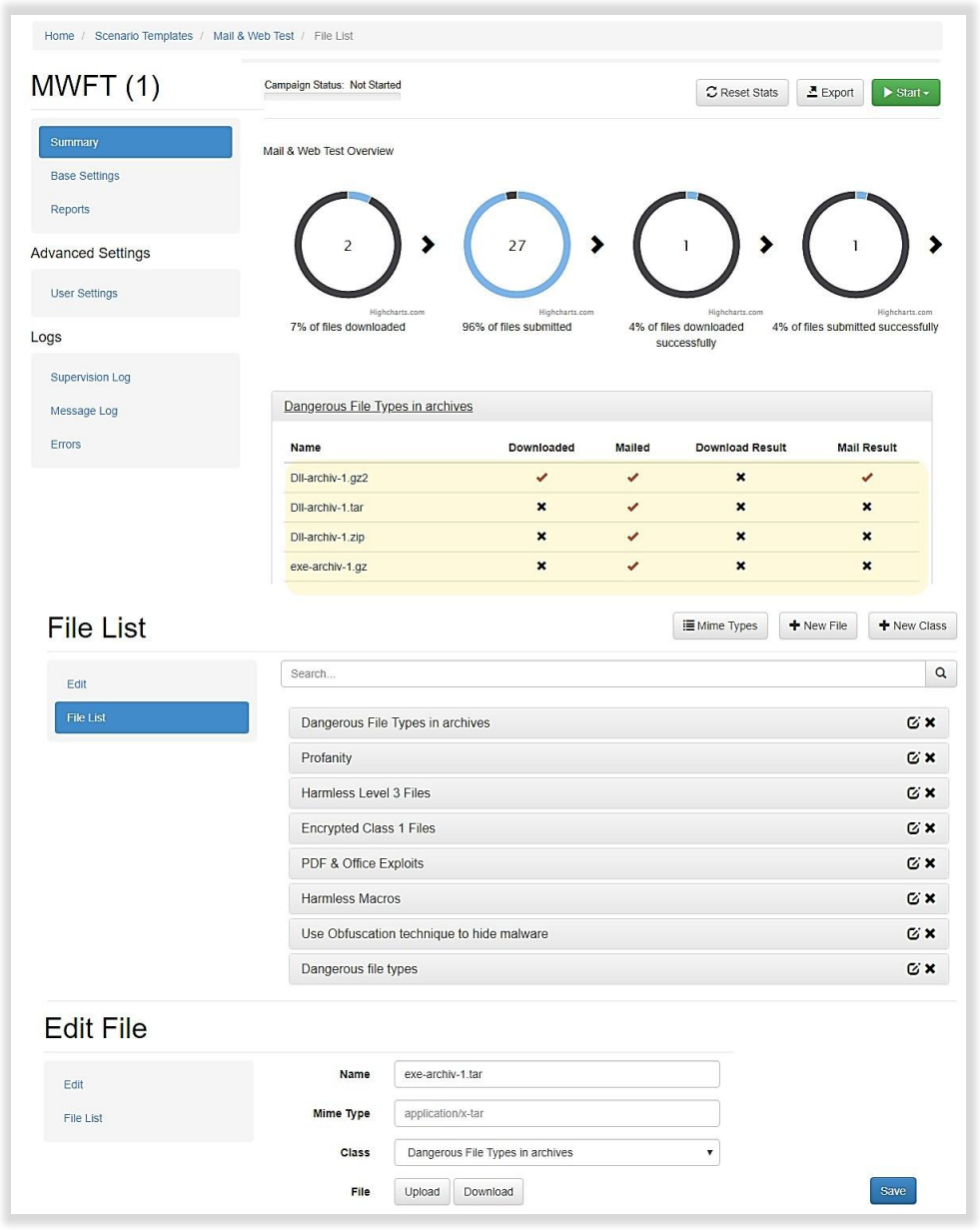


TEST INFRASTRUTTURE

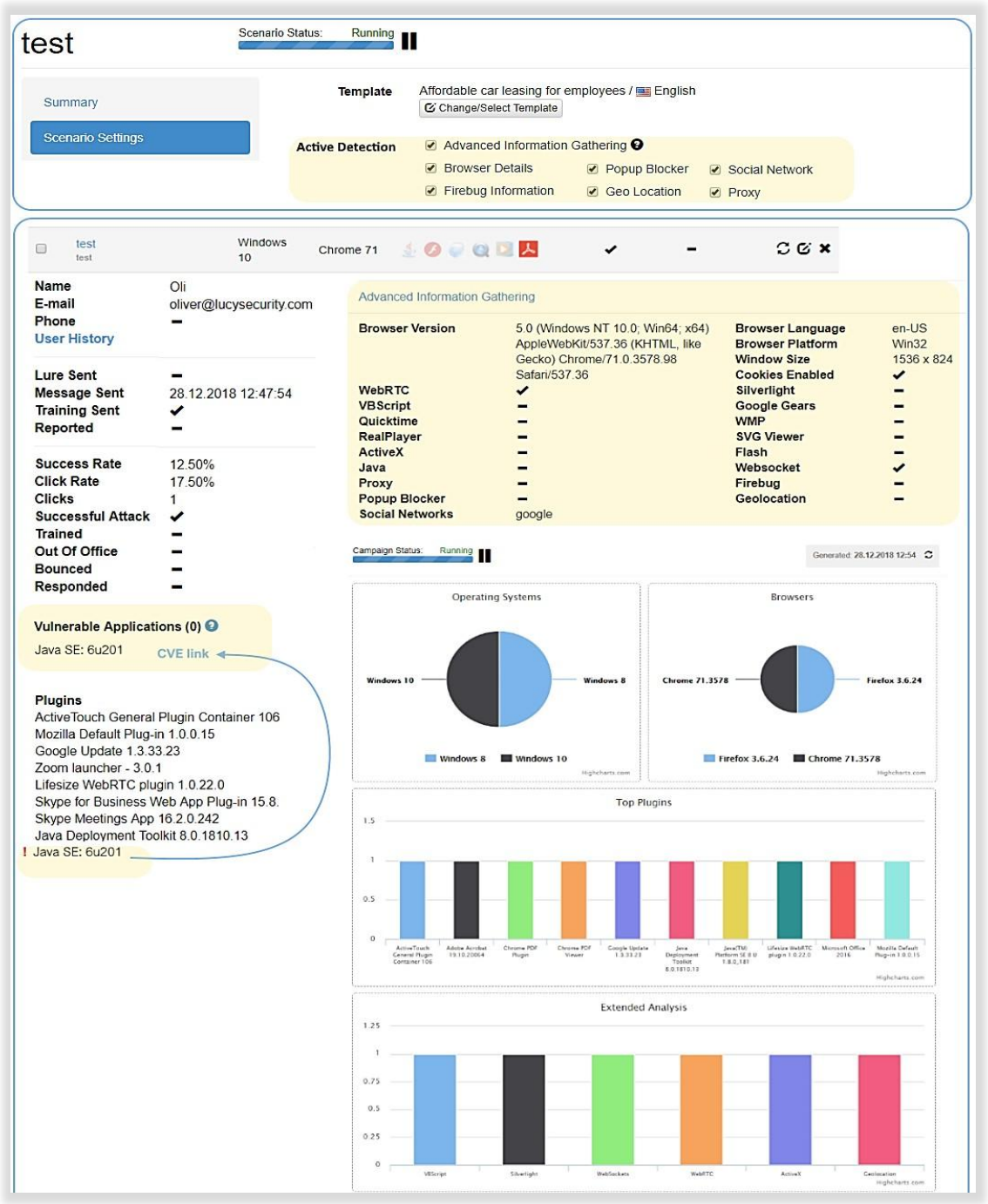
- **Toolkit test malware:** il toolkit di simulazione malware è un programma di simulazione malware avanzato in grado di emulare varie minacce. Consente a un revisore di accedere a un set di funzioni avanzate equivalente a tanti strumenti utilizzati da criminali informatici. Lo strumento, pertanto, consente all'amministratore LUCY di effettuare delle verifiche di sicurezza senza coinvolgere gli impiegati al di fuori del dipartimento informatico.



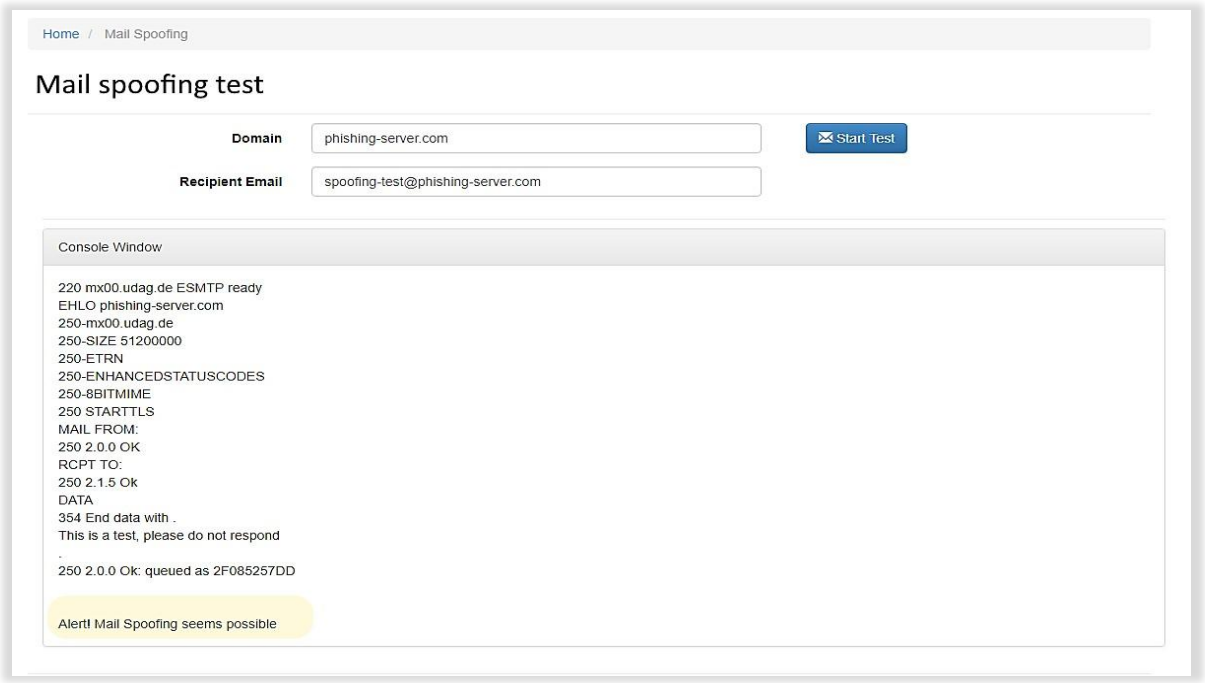
- **Test filtri email e web:** questa funzionalità fornisce una risposta a una delle questioni più importanti della protezione di traffico internet ed email: quali tipi di file possono essere scaricati dal web e quali allegati email vengono filtrati o meno?



- **Rilevamento vulnerabilità client passiva e attiva:** questa funzione consente di testare in modo locale il browser client e rilevare le possibili vulnerabilità basate su librerie JavaScript personalizzate e dati dell'user agent del browser. I plugin trovati possono essere automaticamente comparati con database di vulnerabilità (CVE) per identificare dispositivi vulnerabili.

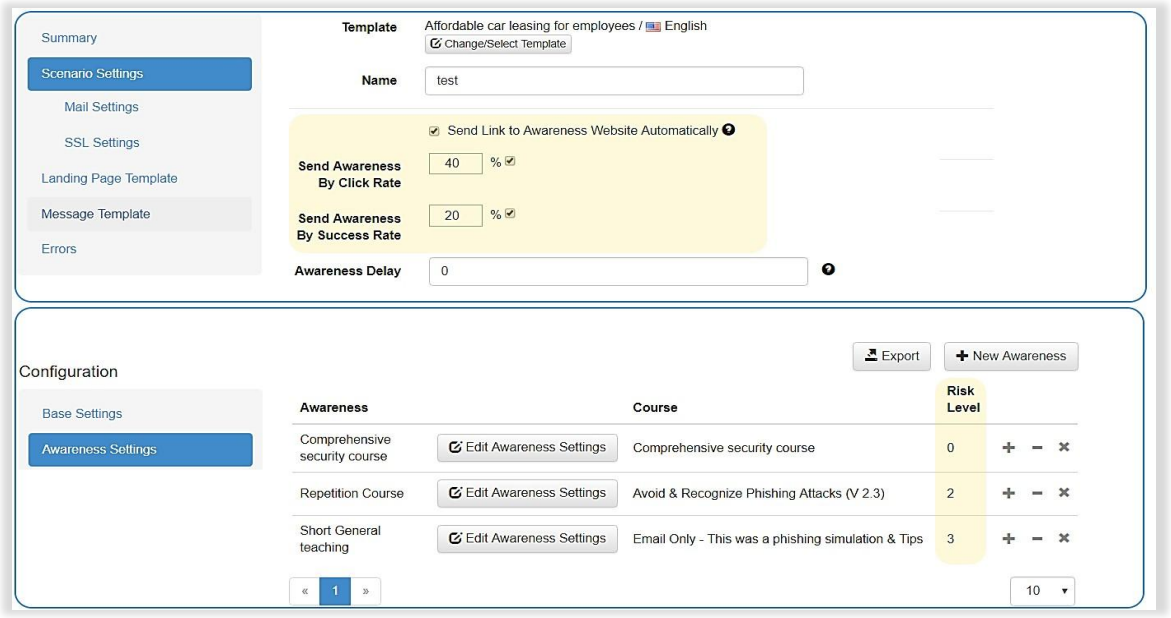


- **Test di spoofing:** esamina le tue infrastrutture per individuare vulnerabilità di spoofing email.

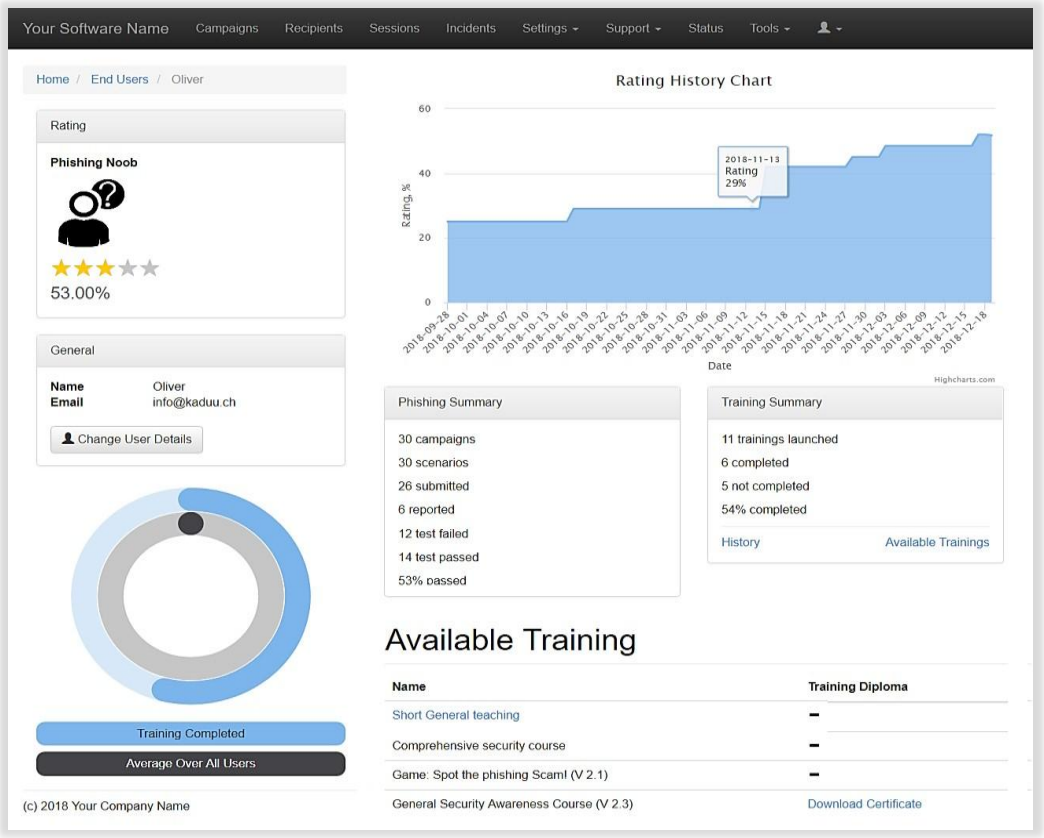


TEST TECNICI

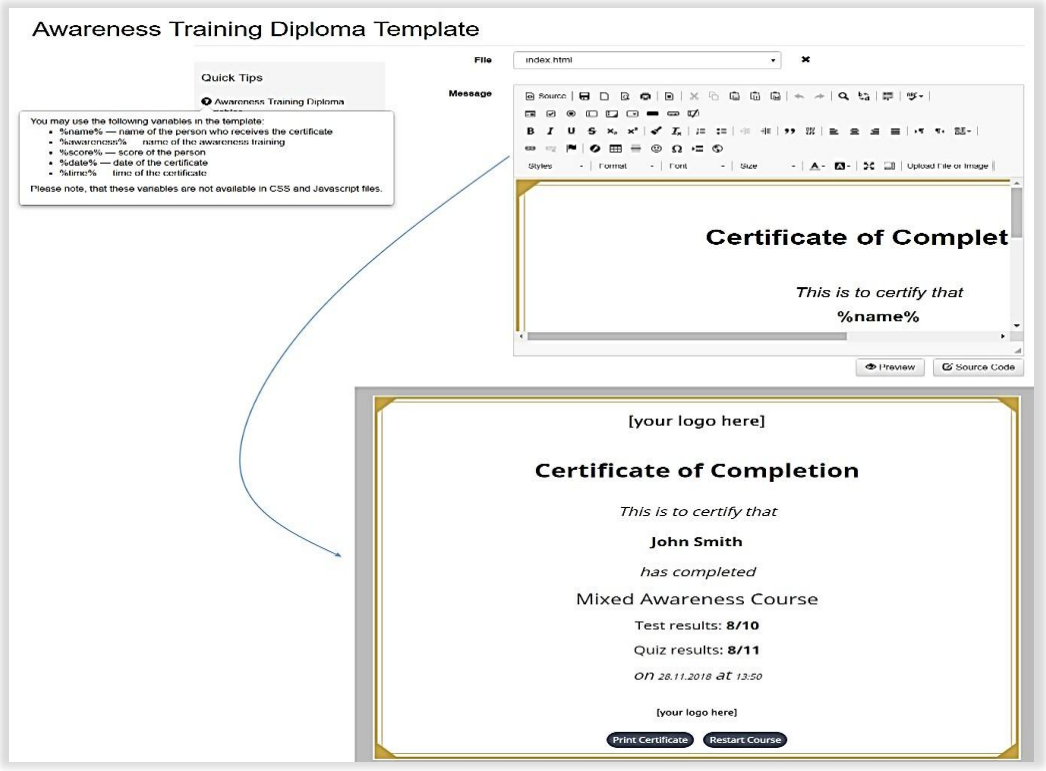
- **e-Learning basato sulla reputazione:** forma i tuoi impiegati secondo le competenze richieste. Misura le abilità degli impiegati e favorisci una competizione amichevole tra colleghi (gamification).
  Sulla base della reputazione di ogni utente, il sistema è in grado di fornire sessioni di formazione multiple. La reputazione è basata sul comportamento dell'utente nelle simulazioni di phishing, oltre che altri fattori. Questo assicura che gli utenti recidivi ricevano contenuti di formazione diversi rispetto a coloro che cliccano su una simulazione di attacco per la prima volta.



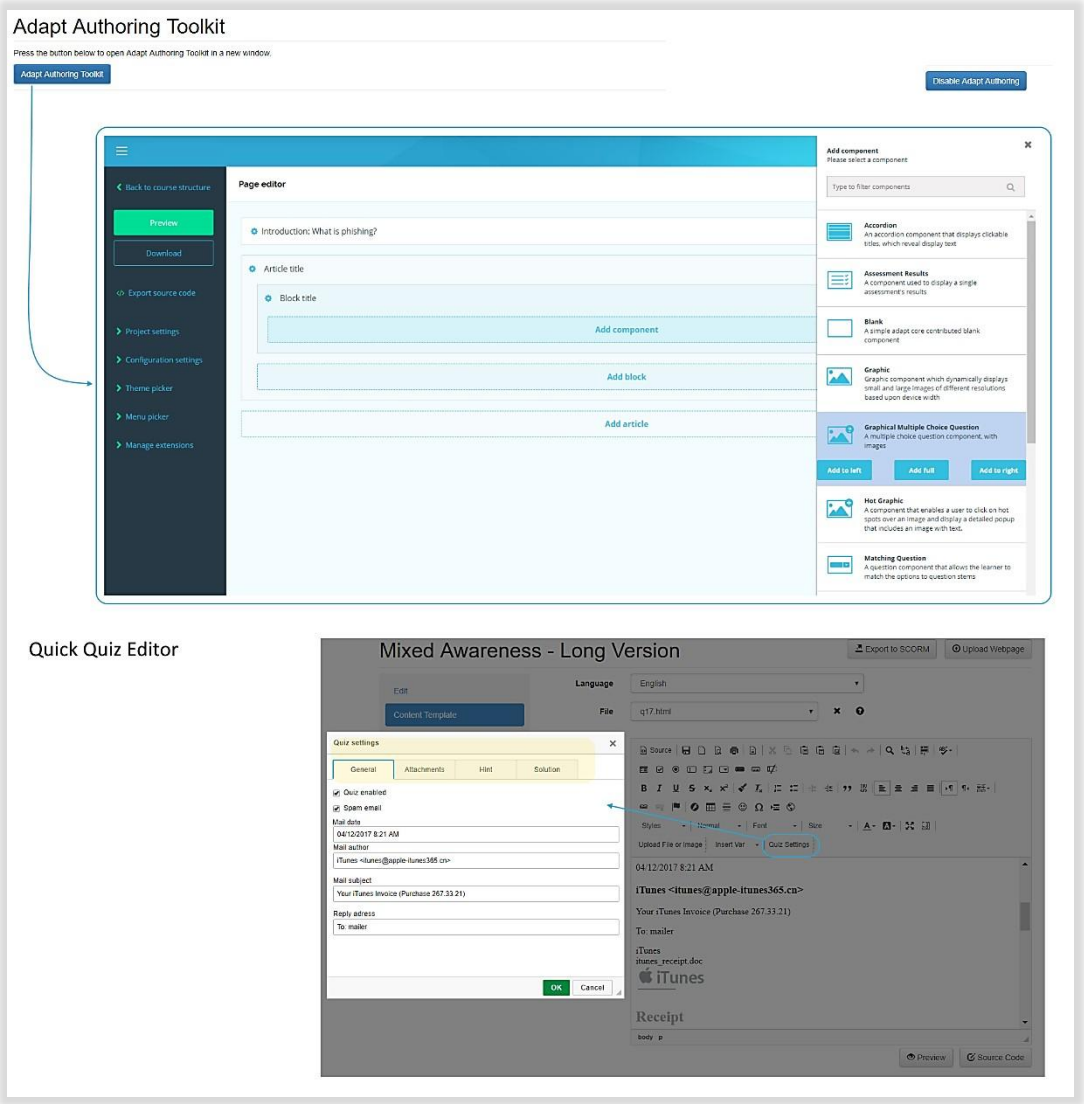
- **Portale di formazione utente finale:** learning management system (LMS): permette a tutti gli utenti di accedere in modo permanente a una homepage di formazione personalizzata che include i tuoi corsi su misura per loro. Su questa homepage possono vedere le statistiche prestazionali, riprendere o ripetere corsi di formazione, creare certificati dei corsi e comparare i loro risultati con altri dipartimenti o gruppi.



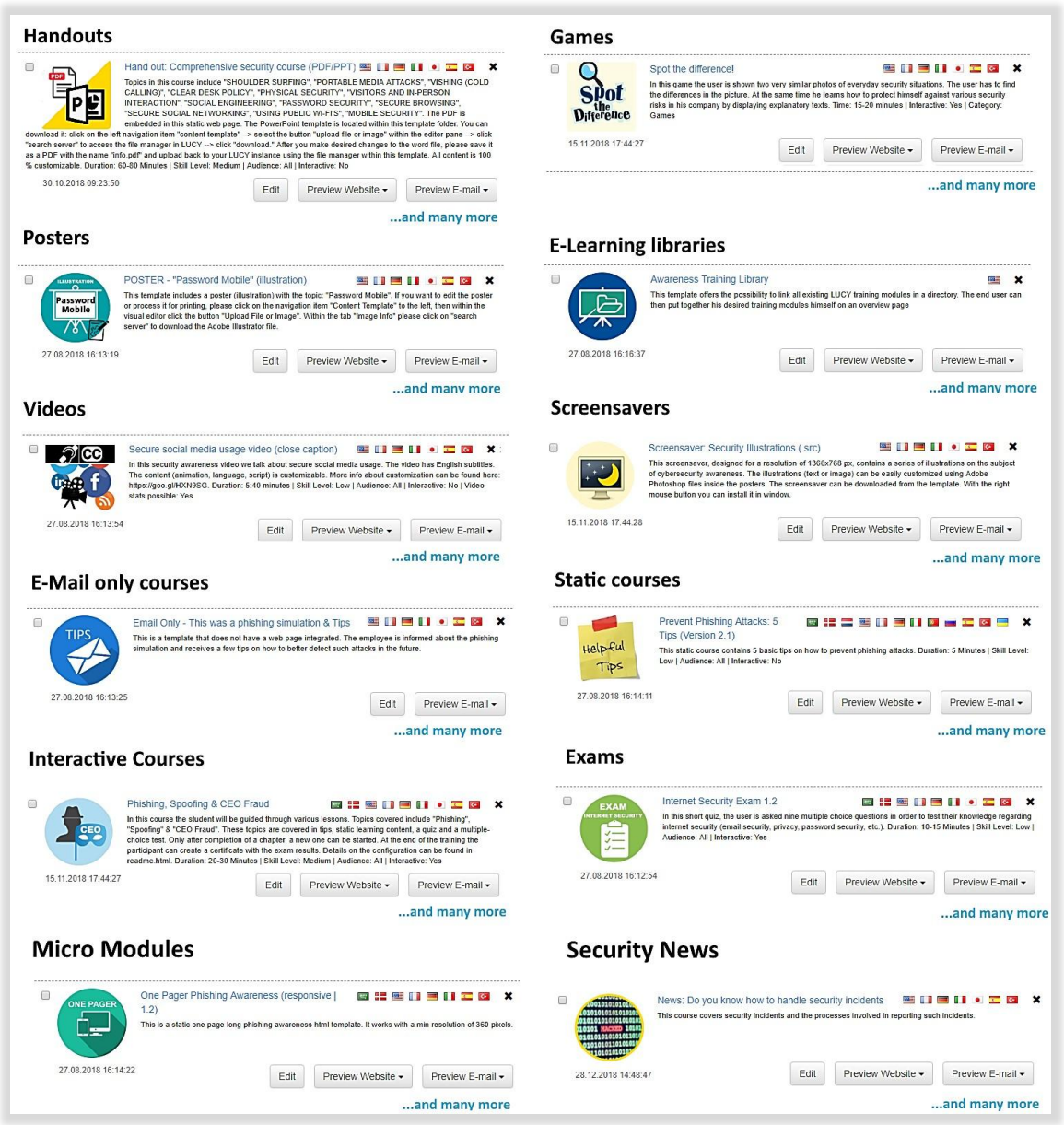
- **Diploma di formazione sulla sensibilizzazione:** è possibile creare dei certificati di e-learning, stampabili dai destinatari direttamente dentro un corso di formazione o il portale LMS.



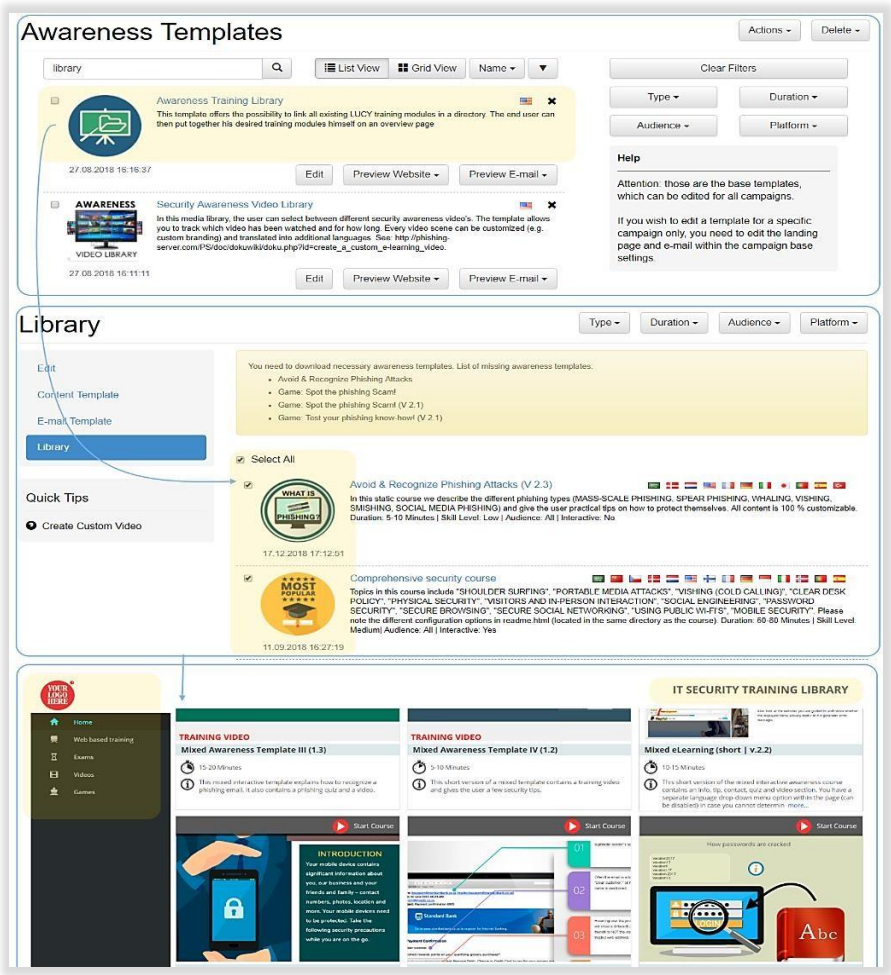
- **Toolkit di creazione e-learning:** il toolkit di creazione e-learning (Adapt) permette di creare contenuti di formazione individualizzati. Copia e incolla video o altri media interattivi, inserisci esami da menu predefiniti, crea contenuti di e-learning interattivo da zero in breve tempo.



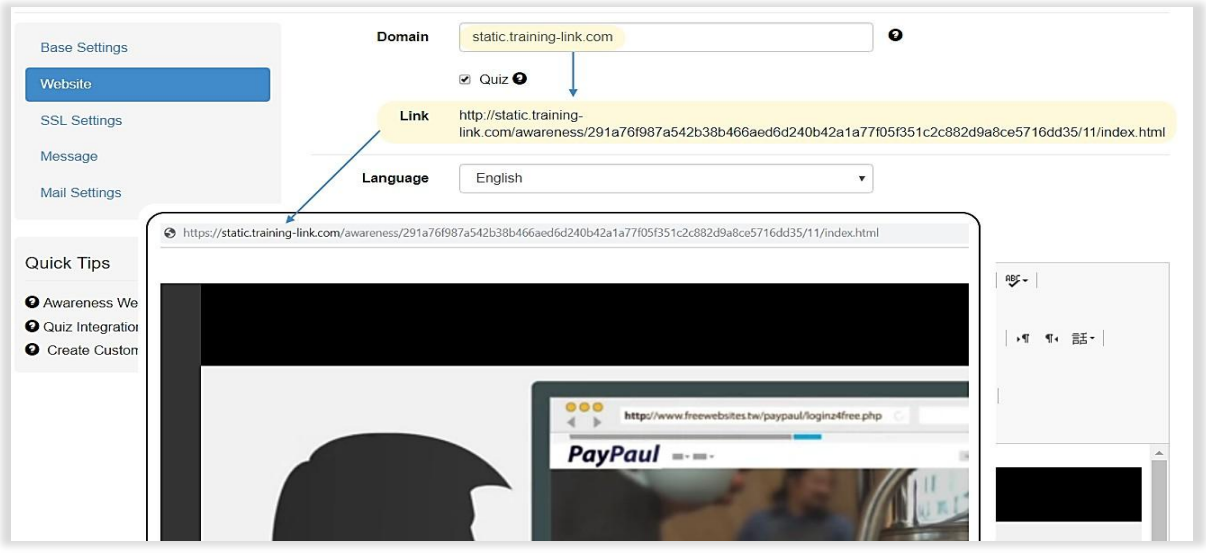
- **Formazione sulla sensibilizzazione su media interattivi:** integra media interattivi (video, audio o altri elementi che incoraggiano gli spettatori a interagire con i contenuti) nei corsi di formazione sulla sensibilizzazione. Usa video di formazione esistenti, adattali o aggiunti i tuoi media interattivi personali.



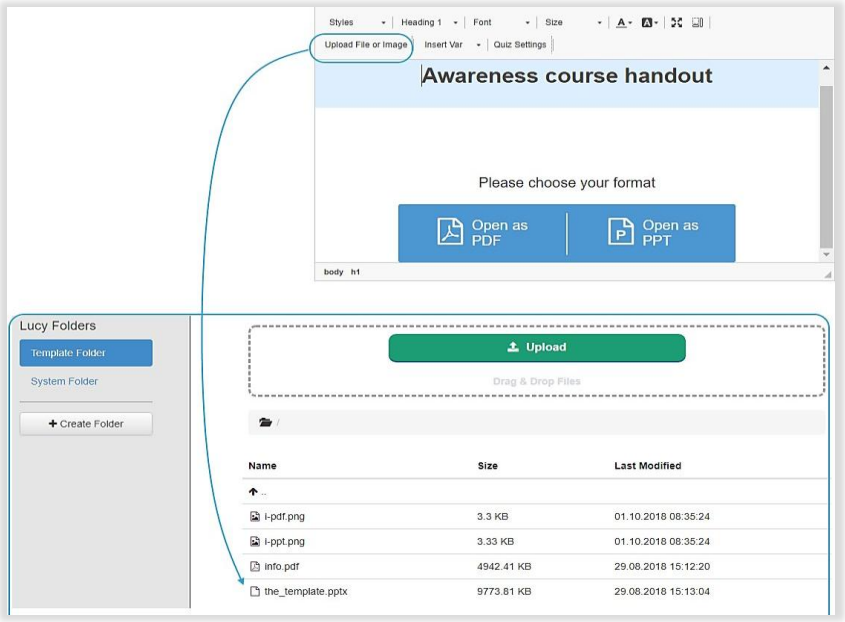
- **Libreria di formazione:** i tuoi impiegati possono accedere ai contenuti di formazione della società da una pagina di panoramica chiamata "libreria di formazione". Contiene una vasta selezione di modelli di e-learning regolari di LUCY, che servono come input. La pagina di panoramica può essere ordinata secondo certi argomenti (video, quiz, test ecc.).



- **Supporto per formazione statica:** i contenuti di formazione possono essere pubblicati anche su pagine statiche all'interno di LUCY o dell'intranet, conferendo all'utente un accesso permanente, indipendentemente da possibili simulazioni di attacco.

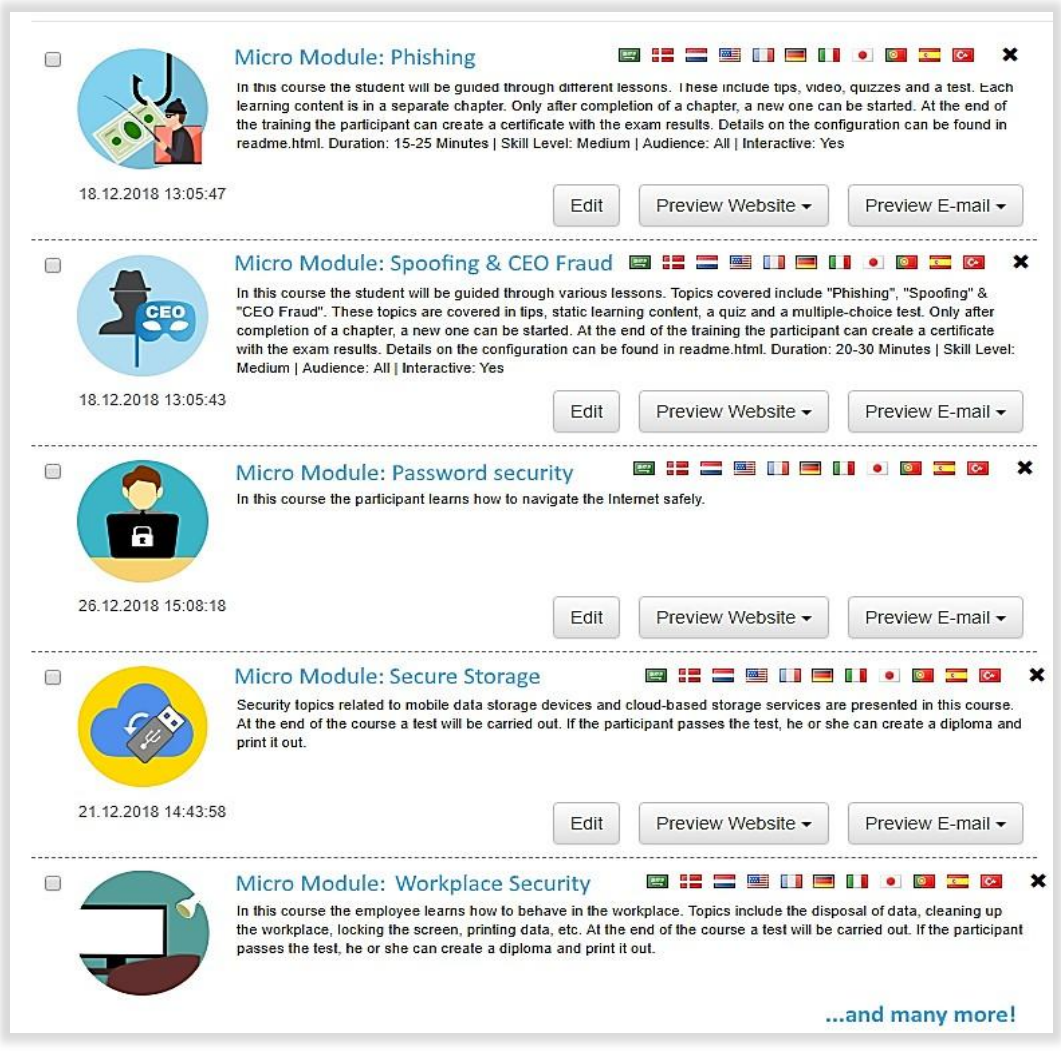


- **Supporto per formazione offline:** LUCY viene fornito con una serie di modelli modificabili (file Adobe Photoshop o Illustrator) per formazione su sensibilizzazione, come poster, screensaver, volantini ecc.

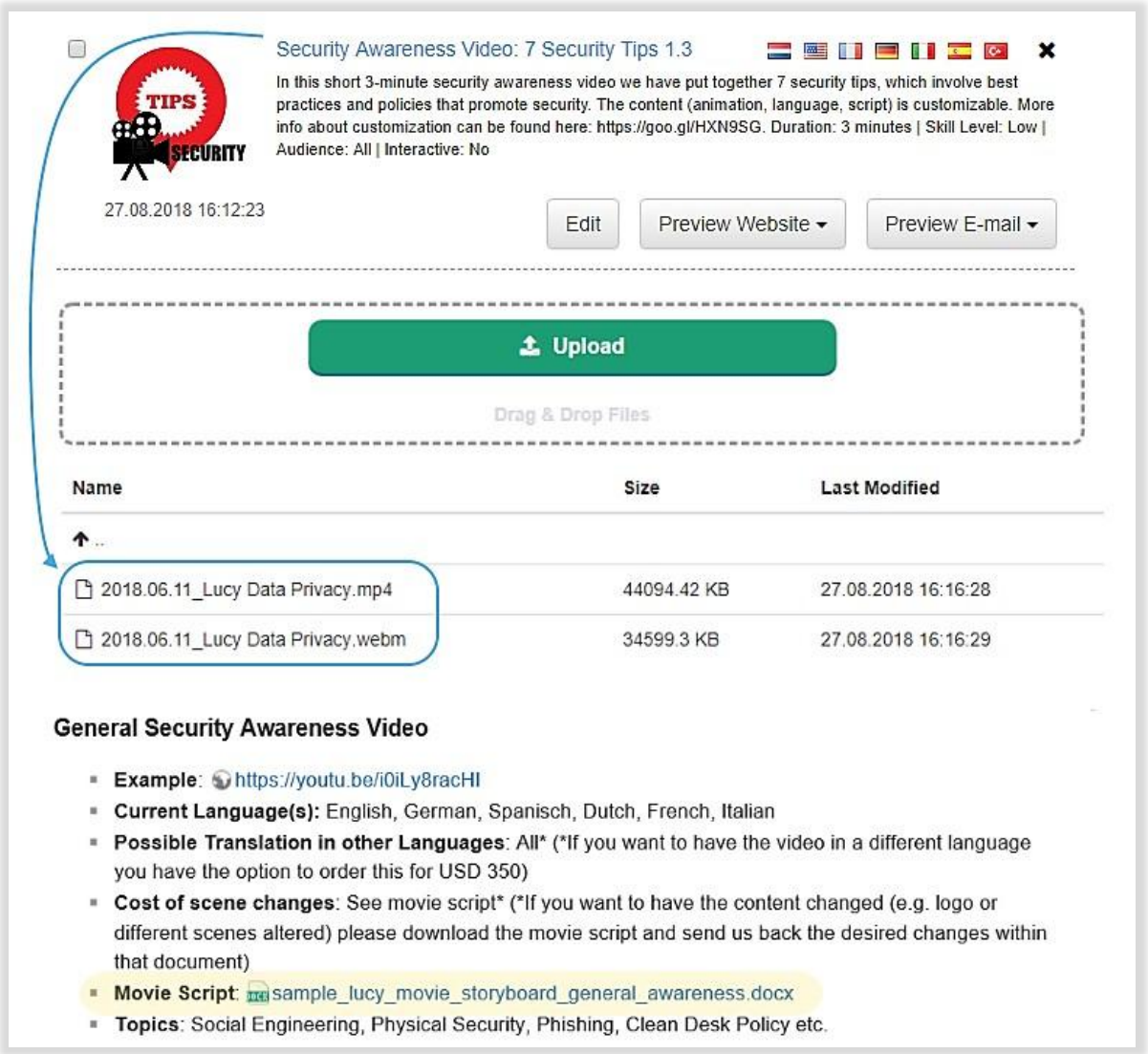


.

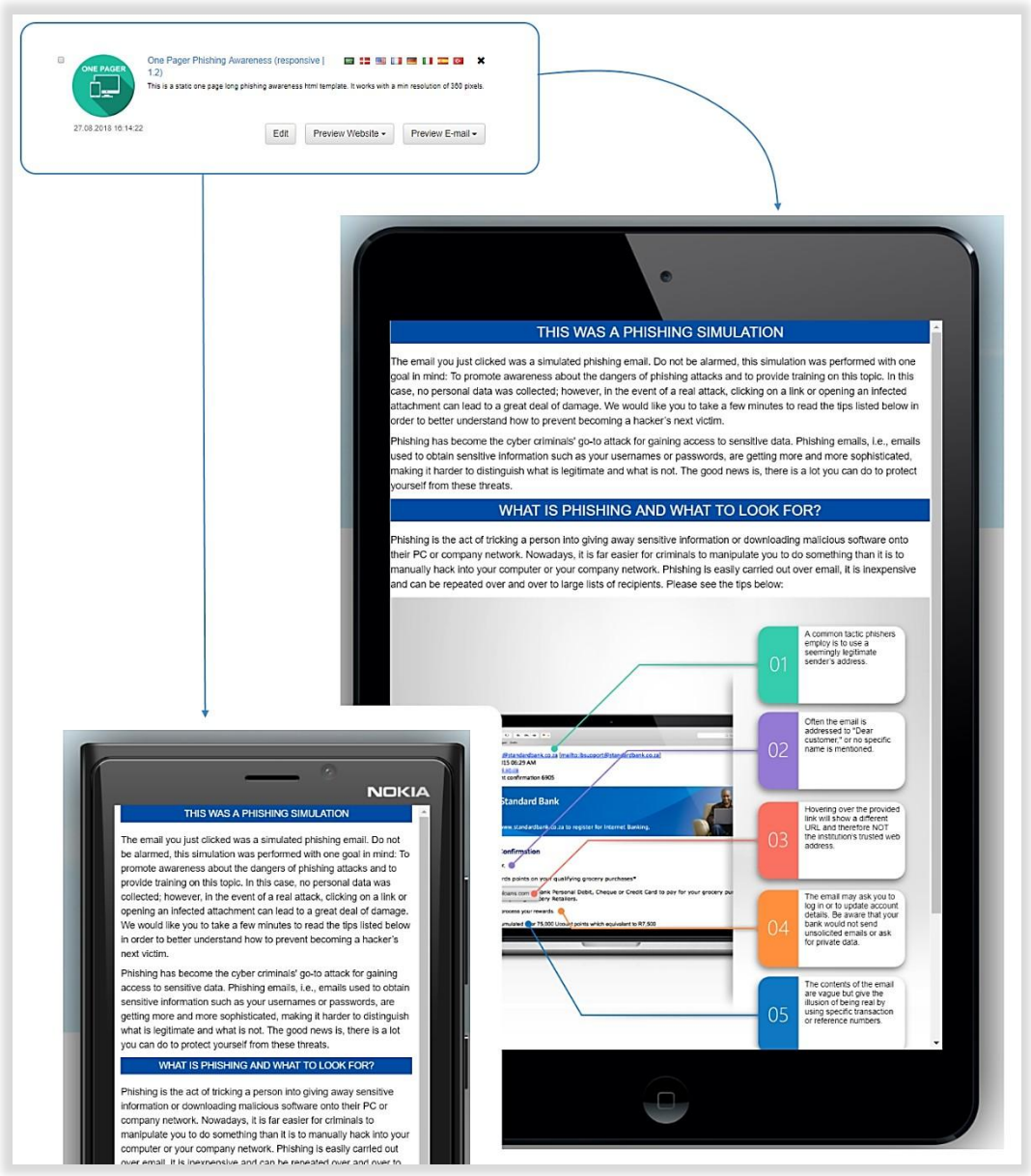
- **Moduli di microapprendimento:** abbiamo progettato dei moduli di microapprendimento (ad esempio, video di 1 minuto o testi di sensibilizzazione di 1 pagina) che possono essere adattati alle esigenze del marchio e alle politiche della tua società.



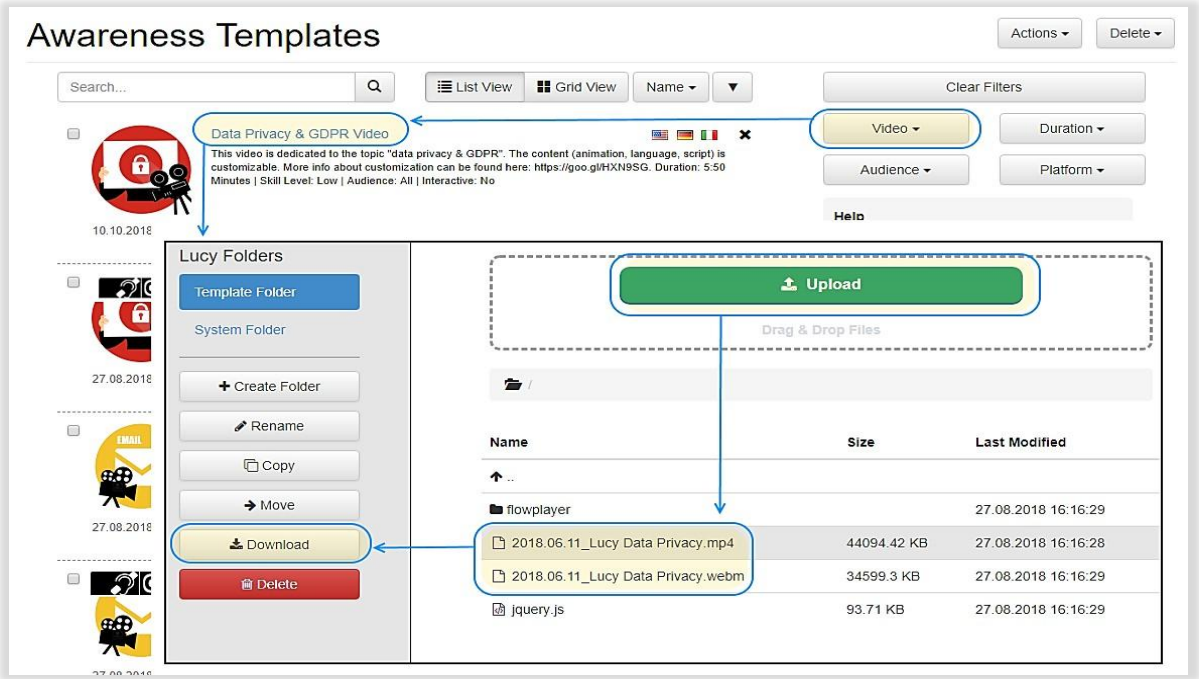
- **Personalizzazione video:** inviaci il logo della tua società e lo includeremo nei video di formazione. Vuoi un'altra lingua? Nessun problema. Imposteremo il video nella lingua che preferisci. Vuoi una scena diversa? Basta scaricare gli script del video e contrassegnare le modifiche desiderate.



- **Formato adatto per dispositivi mobile:** molti moduli integrati di LUCY sono disponibili in un formato adatto a dispositivi mobile che offre ai tuoi utenti la possibilità di seguire il corso di formazione sul qualsiasi dispositivo collegato.



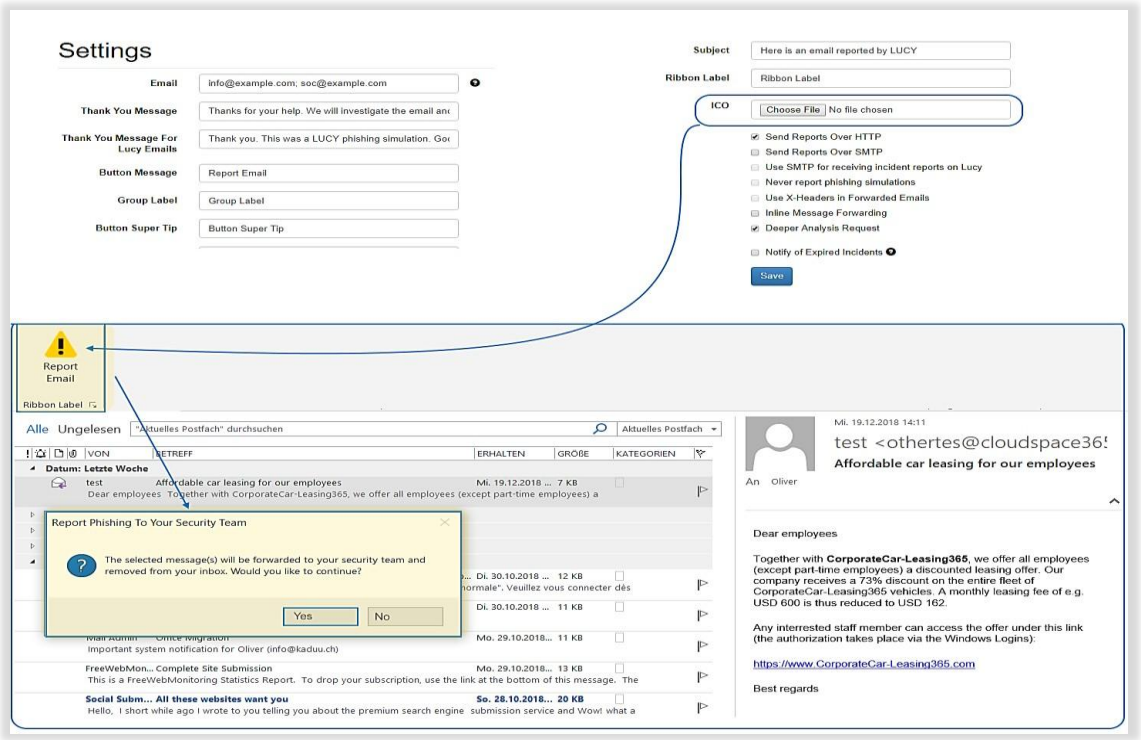
- **Importazione / Esportazione video:** puoi esporta i video LUCY sui tuoi sistemi oltre che importare i tuoi video su LUCY.



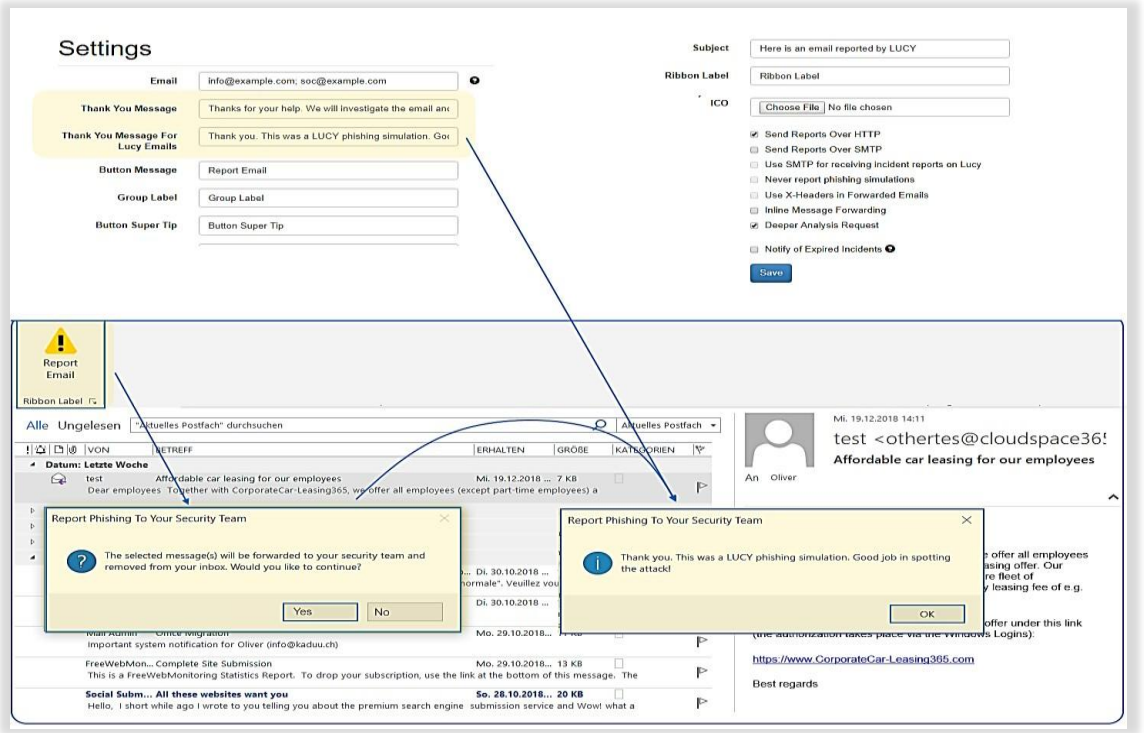
- **Suggerimenti di formazione dinamica:** i suggerimenti dinamici integrati permettono all'amministratore di impostare dei marcatori all'interno dei modelli di attacco che potrebbero indicare ai tuoi impiegati il punto dove è possibile rilevare l'attacco di phishing, nel materiale di e-learning.

COINVOLGIMENTO IMPIEGATI

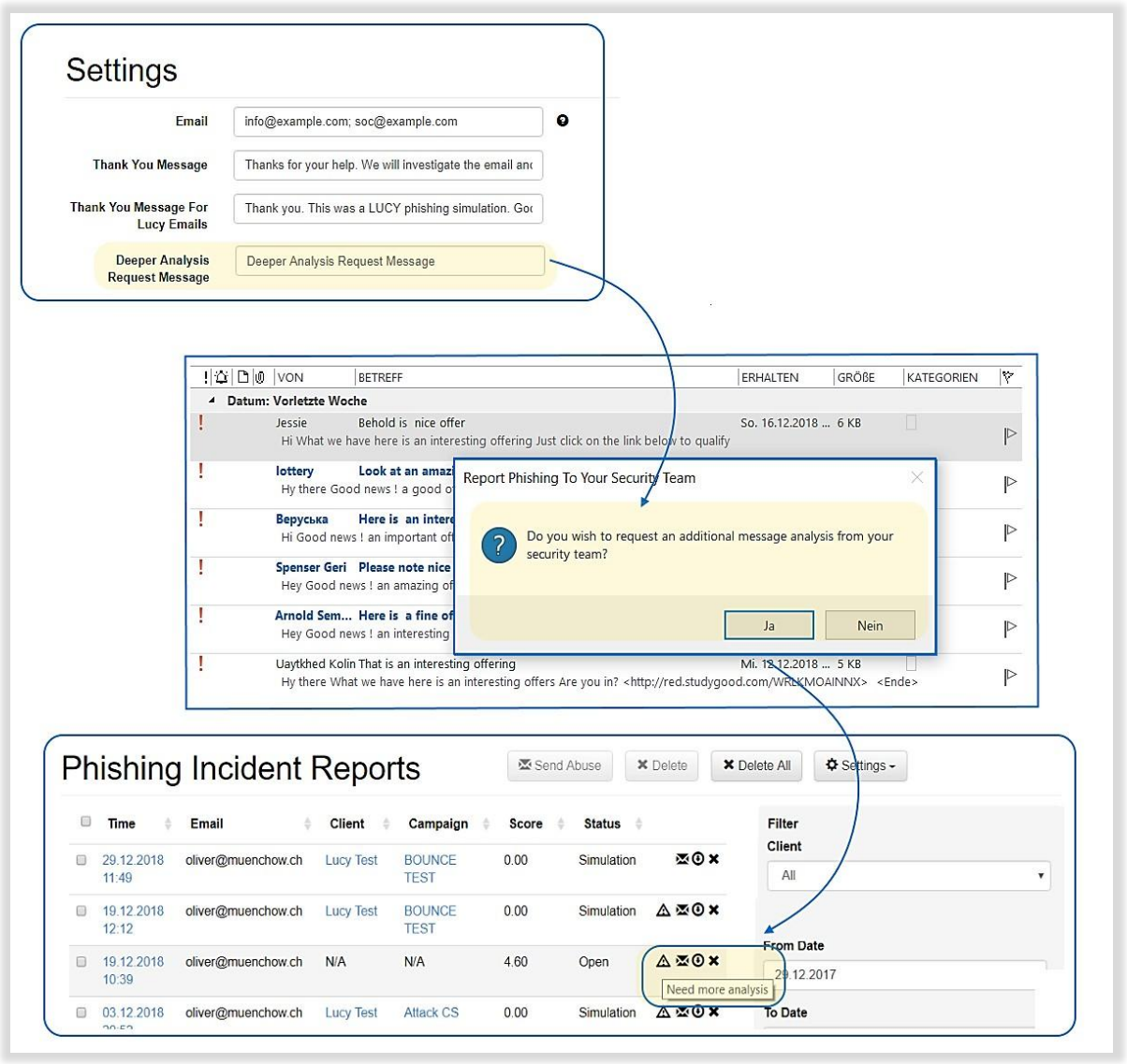
- **Segnalazione delle email con un solo click:** gli utenti finali possono segnalare email sospette con un solo click su uno o più account email e inoltrarle alla console di analisi incidenti LUCY.



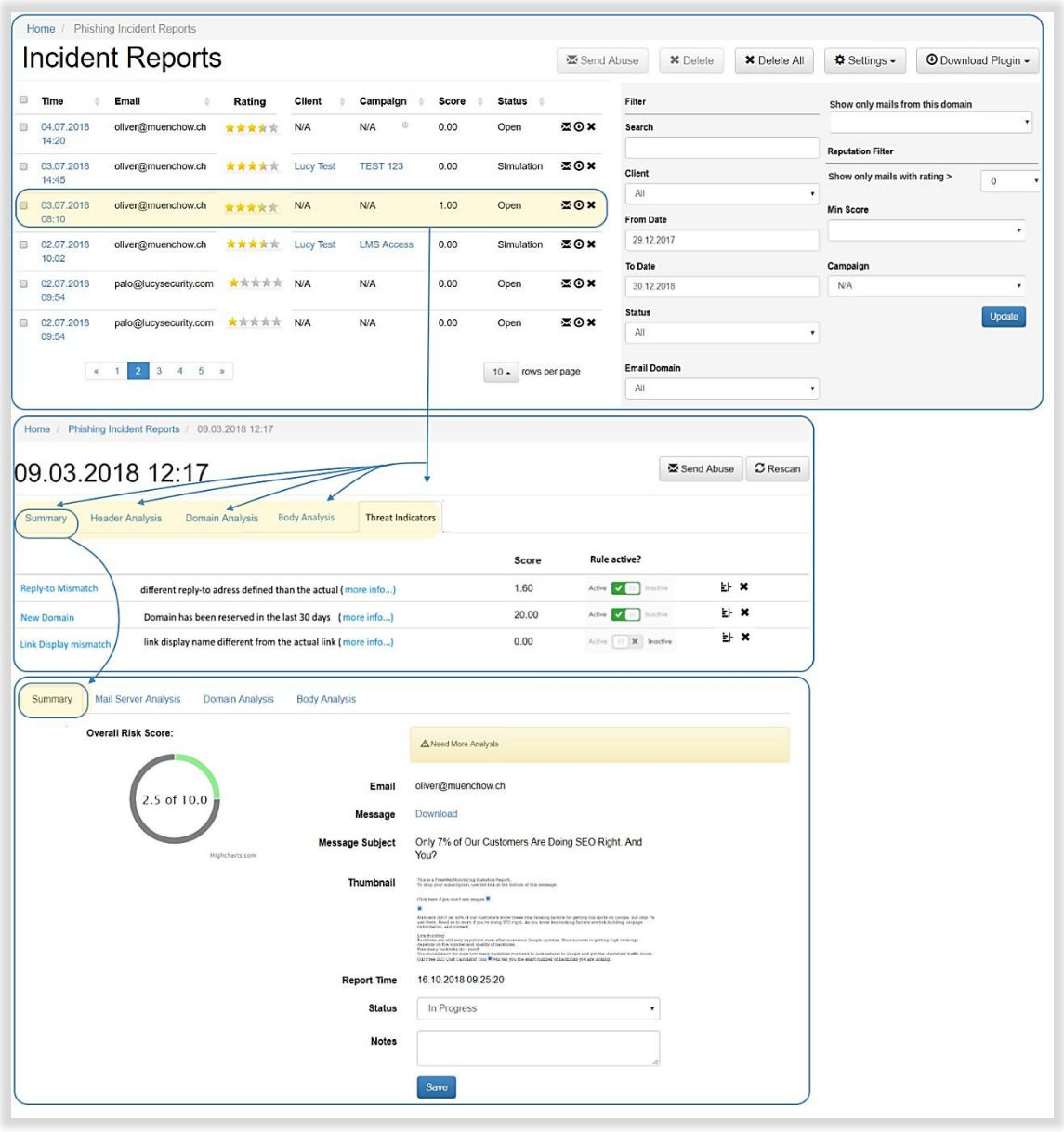
- **Rafforzamento del comportamento positivo:** il nostro plugin fornisce automaticamente rafforzamento del comportamento positivo mostrando gratitudine agli utenti finali tramite un messaggio personalizzato definito dalla tua società.



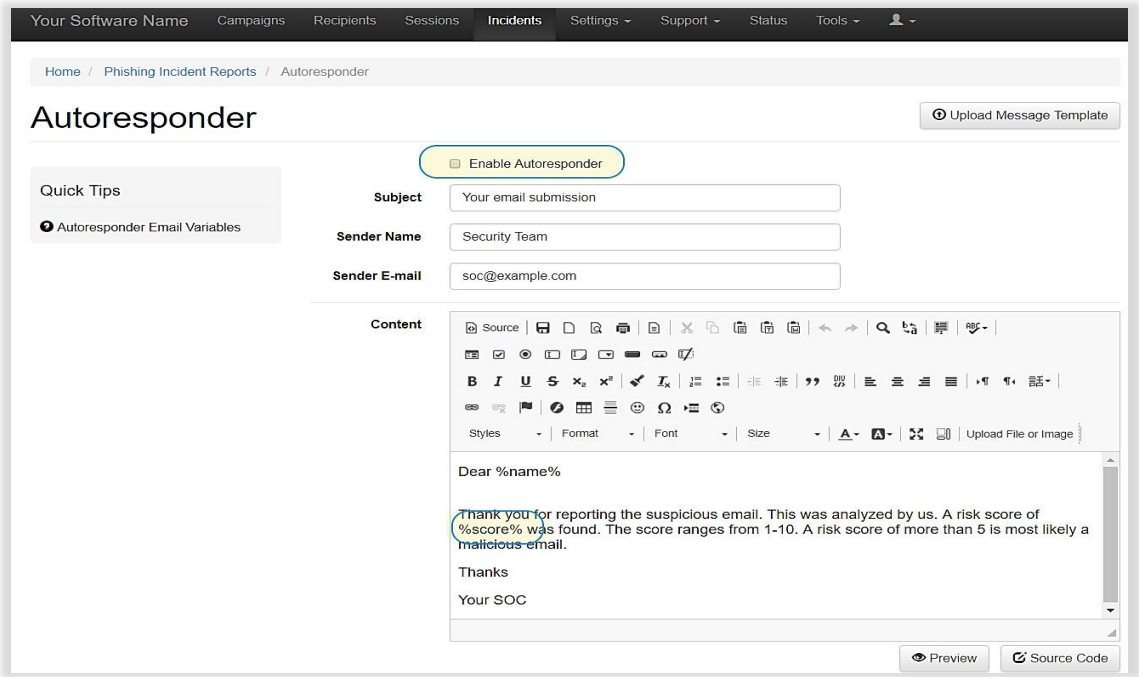
- **Richiesta di ispezione approfondita:** a volte gli utenti vogliono sapere se l'email ricevuta può essere aperta in sicurezza. L'utente può utilizzare la "richiesta di ispezione approfondita" nel plugin locale per informare il team di sicurezza che desidera ricevere un feedback sull'email segnalata.



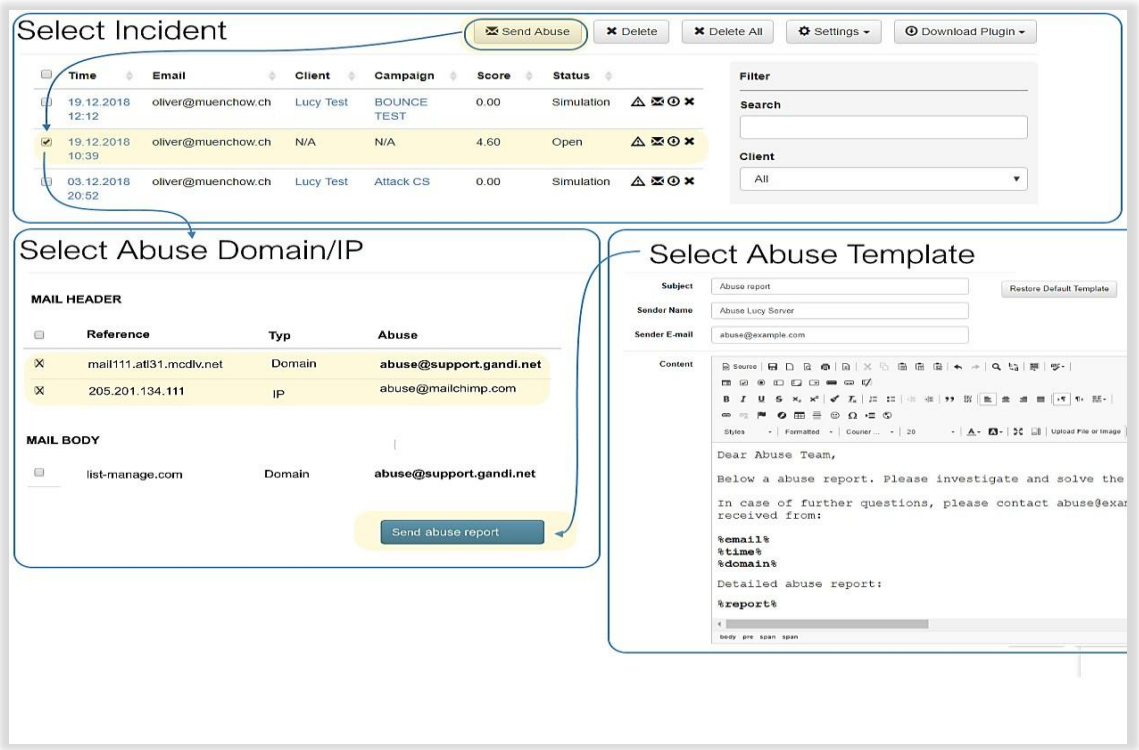
- **Analisi degli incidenti automatica:** Gestisci e rispondi alle email sospette segnalate utilizzando una console di gestione centralizzata. Il sistema di analisi LUCY permette di ispezionare automaticamente i messaggi segnalati (intestazione e corpo). Il sistema di analisi include un punteggio di rischio individuale, fornendo una classifica in tempo reale delle email segnalate. Inoltre, riduce il carico di lavoro del team di sicurezza.



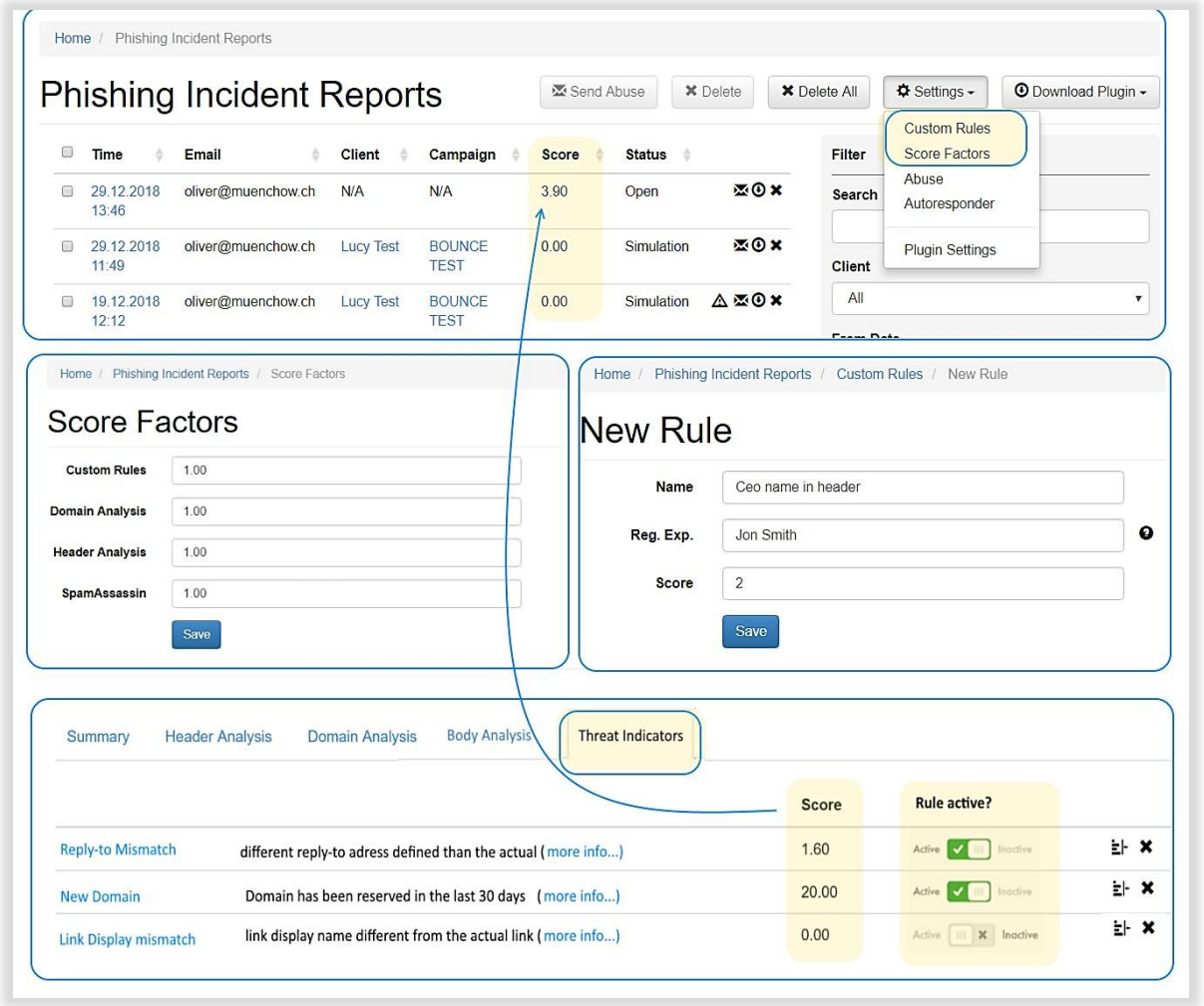
- **Feedback degli incidenti automatico:** il sistema di risposta incidenti automatico permette di inviare una notifica automatica all'utente finale fornendo i risultati di un'analisi delle minacce. Il messaggio di testo è configurabile liberamente ed è possibile includere anche il punteggio di rischio email LUCY, se richiesto.



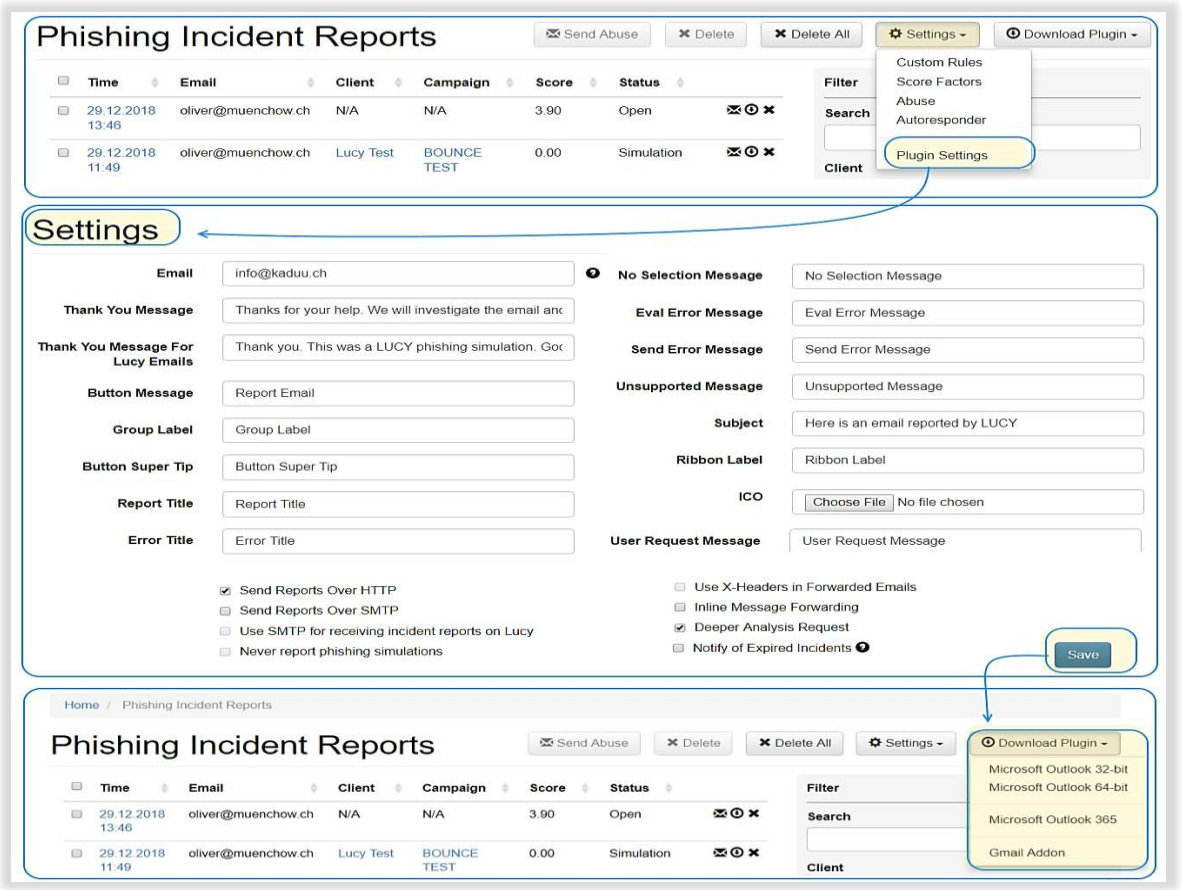
- **Mitigazione minacce:** il sistema di mitigazione minacce è un approccio rivoluzionario per eliminare i rischi delle email. Supporta l'amministratore di sicurezza in relazione al bloccare l'attacco (ad es. inviando un report automatico al gruppo di provider specifico coinvolto nell'attacco).



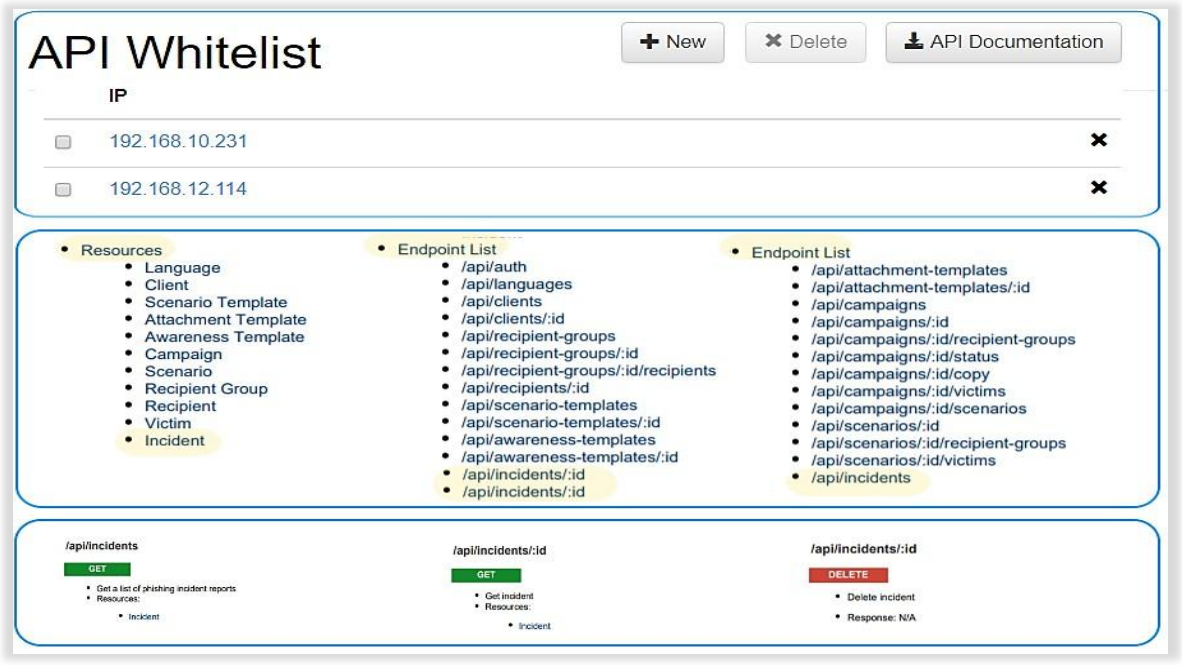
- **Analisi con regole personalizzate:** definisci le tue regole per analisi email e calcolo dei rischi.



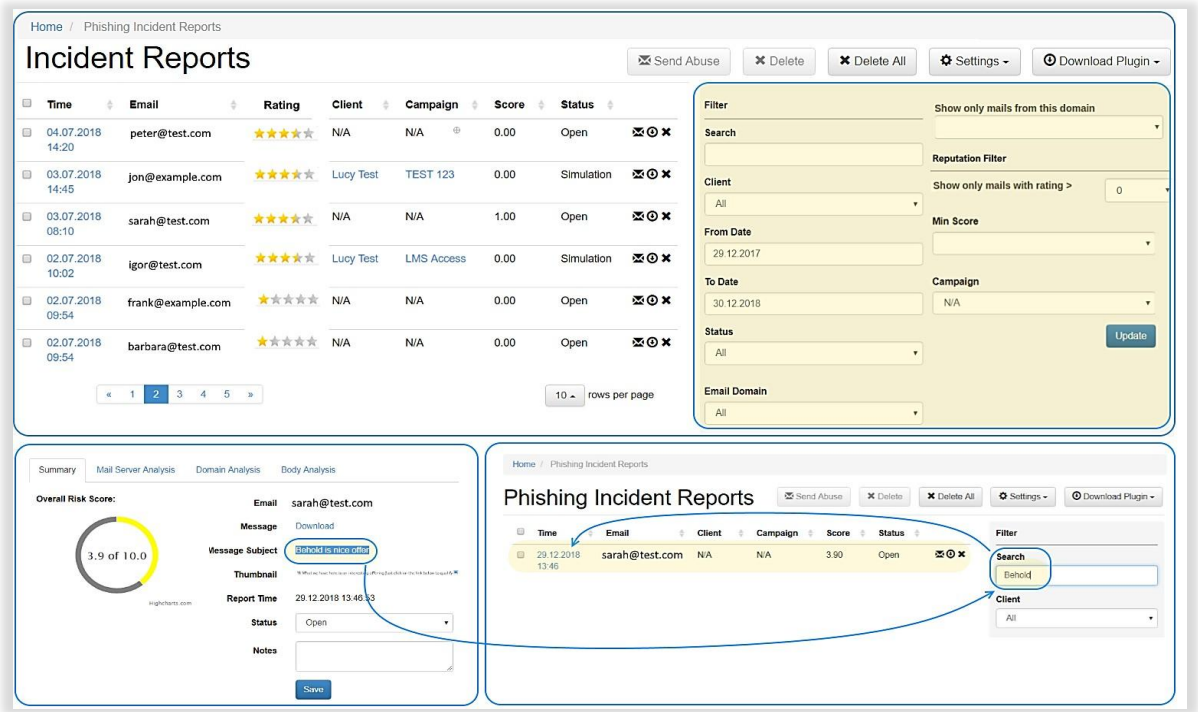
- **Opzioni di personalizzazione plugin:** LUCY permette di personalizzare facilmente diverse funzioni e plugin (icone mostrate, messaggi di feedback, etichette, protocolli di trasmissione, intestazioni ecc.).



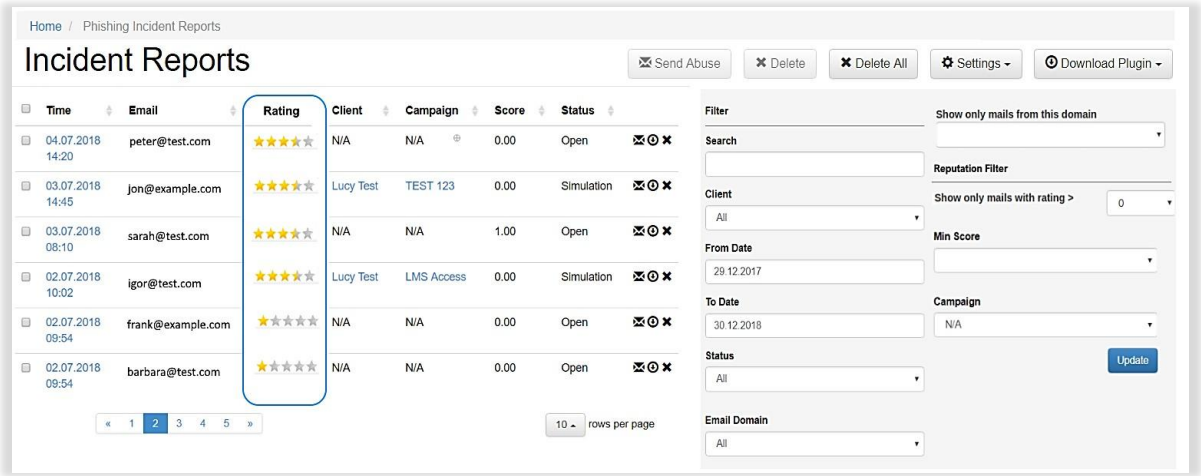
- **Integrazione di terze parti:** utilizzano l'automazione API REST incidenti LUCY, siamo in grado di elaborare email segnalate e aiutare il team di sicurezza a fermare attacchi di phishing in corso.



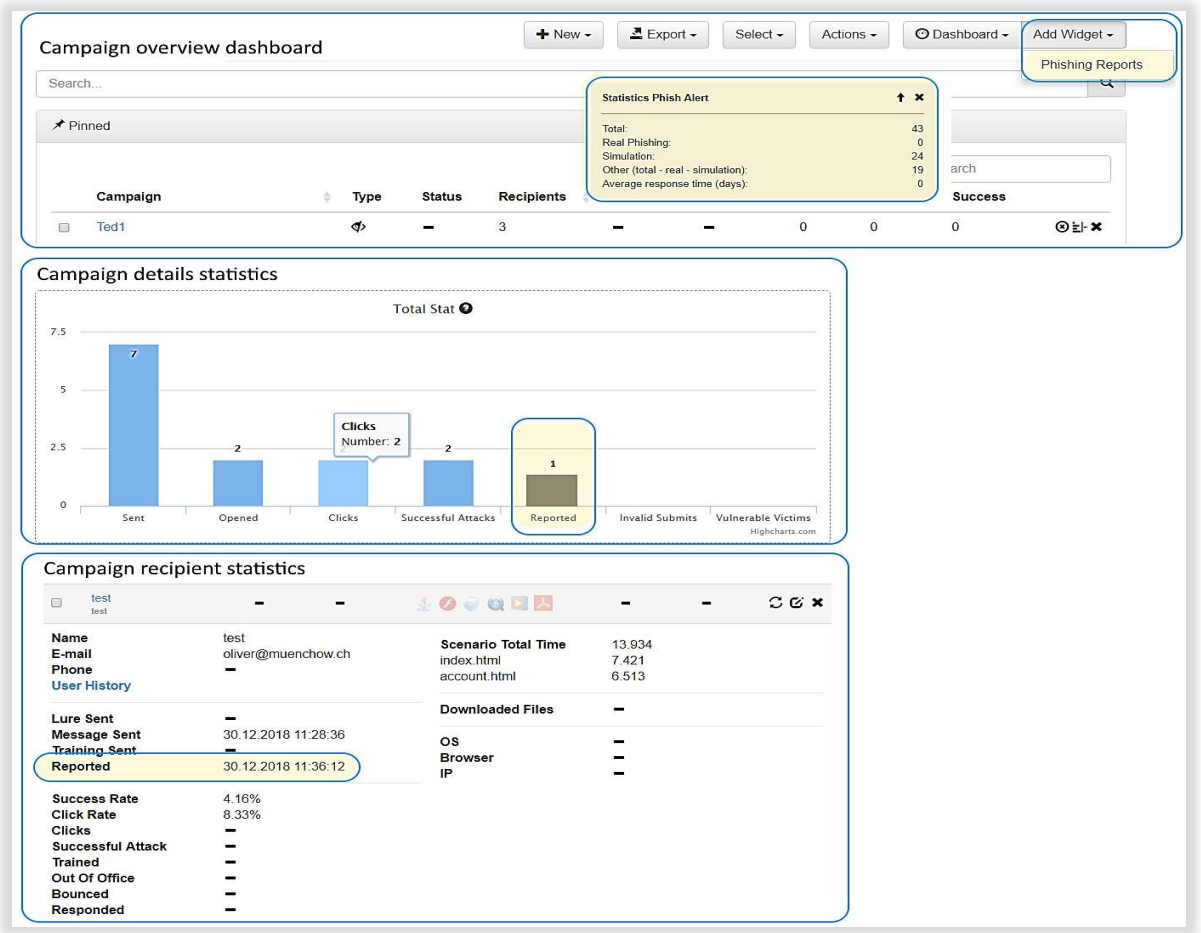
- **Identificazione attacchi con schemi comuni:** applica i filtri della dashboard LUCY per rilevare vettori di attacco comuni nella tua società. Ricerca tra tutte le email segnalate indicatori di compromissione simili.



- **Profili di reputazione degli utenti sugli incidenti:** classifica gli utenti con un punteggio di reputazione incidenti.



- **Integrazione con attacchi simulati:** report illimitati e integrazioni dashboard per simulazioni di phishing: identifica gli utenti che si sono comportati meglio in una simulazione di phishing.



- **Installazione facile:** installa il plugin per incidenti di phishing su Outlook, Gmail e Office365.