LIVRE BLANC DE LUCY

QU'EST-CE QUE LUCY ?

Testez, formez et impliquez vos employés

LUCY permet aux entreprises de jouer le rôle d'un attaquant et de découvrir les faiblesses existantes de l'infrastructure technique et des connaissances du personnel, et de les éliminer grâce à un programme complet d'apprentissage en ligne.

TEST DES EMPLOYÉS
Simulations d'attaque (hameçonnage, p. ex.)

TEST DE L'INFRASTRUCTURE
Simulation de programmes malveillants & Scanner

FORMATION DES EMPLOYÉS
SGA intégré

ÉVALUATION DES PROGRÈS
Analyse des risques et de l'apprentissage

INTÉGRATION DES EMPLOYÉS
Système de reporting (p. ex. bouton mail d'hameçonnage)

LIVRE BLANC DE LUCY

TABLE DES MATIÉRES

FONCTIONNALITIÉS GÉNÉRALES

- Rappels
- Détection de réponse
- Logiciel client de messagerie complet
- Randomisation du planificateur
- Outils de gestion de la performance
- Interface d'administration multilingue
- Certificate (SSL)
- Contrôles d'accès basés sur rôles
- Groupes d'utilisateurs multicouches
- Compatible multi-clients
- Modèles de campagne
- Assistant d'installation guidée et basée sur le risque
- Contrôles de campagne
- Process d'approbation
- API DNS

SIMULATION D'ATTAQUE

- Attaques de supports amovibles
- SMiShing
- Attaques de saisie de données
- Attaques de liens hypertextes
- Boîte à outils performante de redirection d'URL
- Attaques mixtes
- Attaques basées sur des fichiers
- Attaques Double Barrel
- Attaques basées sur Java
- Attaques basées sur PDF
- Attaques simulant un logiciel rançonneur
- Boîte à outils de validation de la saisie de données
- Bibliothèque de modèles d'attaque multilingues
- Modèles spécifiques à des secteurs d'activité et à des divisions
- Utilisation simultanée de plusieurs modèles d'attaque
- Variantes des URL d'attaque
- Raccourcissement d'URL
- Kit de test d'intrusion Pentest
- Clonage de site Web
- Attaques basées sur les niveaux
- Simulation d'hameçonnage ciblé
- Prise en charge de DKIM / S /MIME pour les e-mails d'hameçonnage
- Scanner de messagerie
- Création de page d'accueil personnalisée

TESTEZ L'INFRASTRUCTURE

- Boite à outils de test programmes malveillants
- Test du filtrage de la messagerie et du Web
- Détection de la vulnérabilité active et passive du client
- Test d'usurpation d'identité

TEST TECHNIQUES

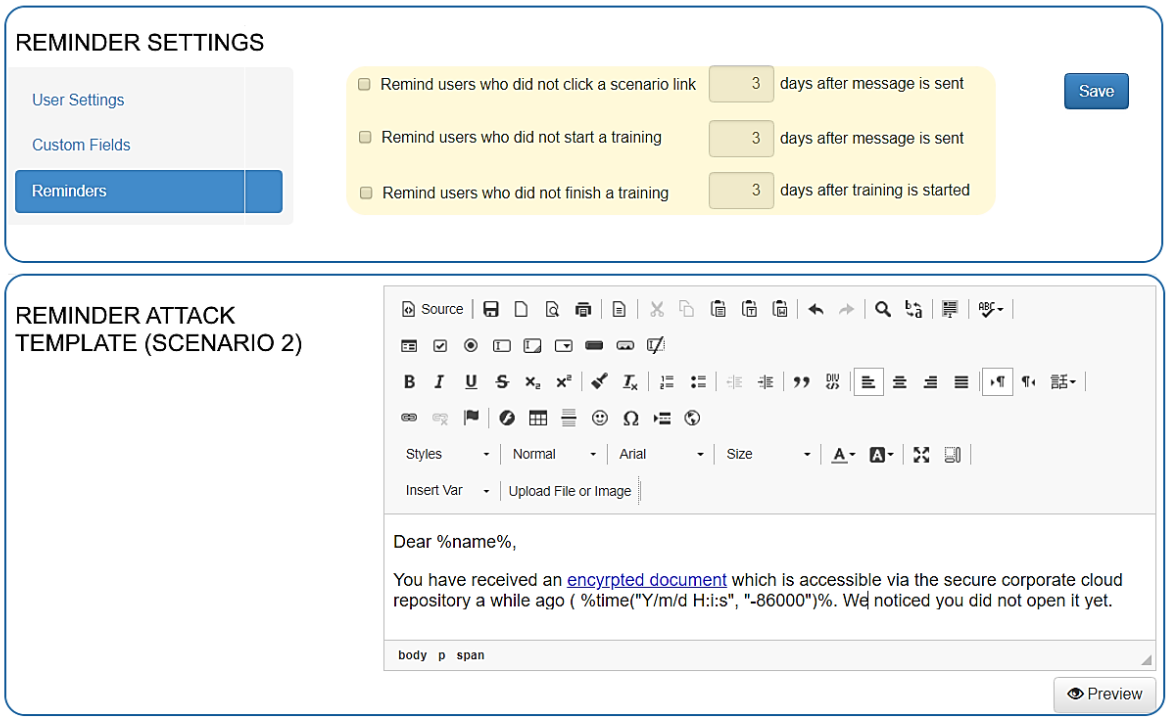
- Apprentissage en ligne basé sur la réputation
- Portail de formation des utilisateurs finaux
- Diplôme de sensibilisation
- Boîte à outils de création de contenu d'apprentissage en ligne
- Formation de sensibilisation au format interactif rich media
- Bibliothèque de formation
- Supports de formation statiques
- Supports de formation hors ligne
- Modules de micro-apprentissage
- Personnalisation de video
- Format optimisé pour appareils mobiles
- Importation/exportation de vidéo
- Indices de formation dynamiques

IMPLIQUEZ LES EMPLOYÉS

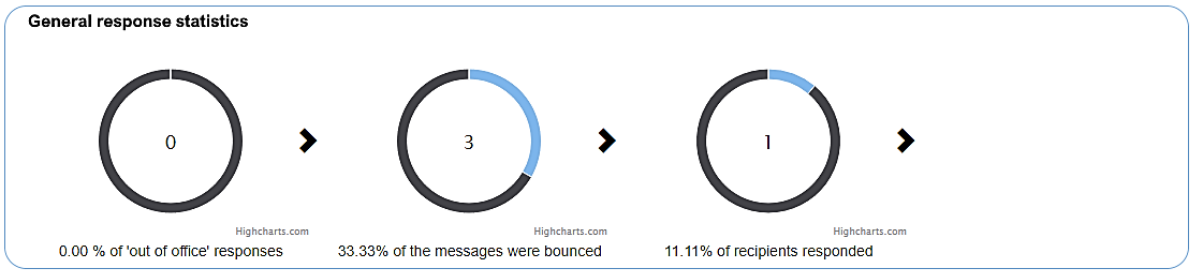
- Signaler des e-mails en un seul clic
- Appui aux bons comportements
- Demande d'analyse approfondie
- Analyse automatique d'incident
- Feed-back automatique sur les incidents
- Atténuation de la menace
- Analyse basée sur des règles personnalisées
- Options de personnalisation des plugins
- Intégration de tiers
- Identifier les attaques présentant des caractéristiques courantes
- Profils de réputation incidents des utilisateurs
- Intégration aux simulations d'attaque
- Installation facile

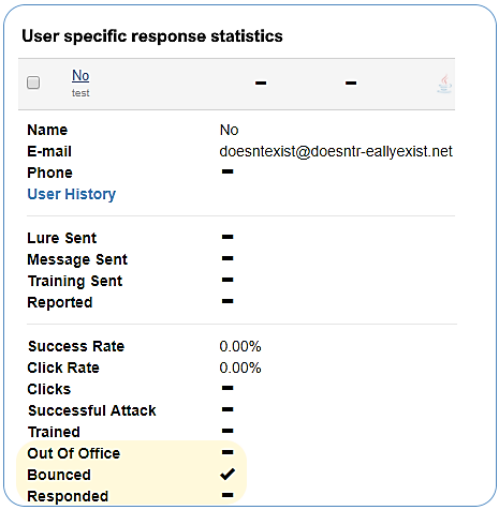
FONCTIONNALITÉS GÉNÉRALES

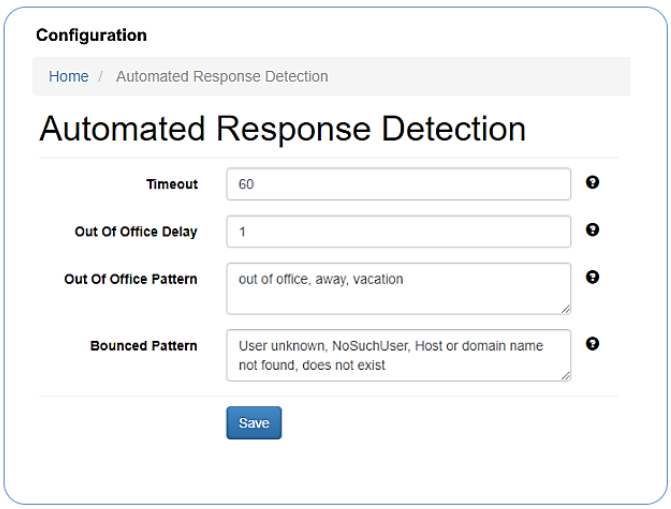
- **Rappels :** les modèles de rappel peuvent être utilisés pour renvoyer automatiquement des messages aux utilisateurs qui n'ont pas cliqué sur un lien d'attaque ou sur un cours de formation après une période de temps personnalisée.



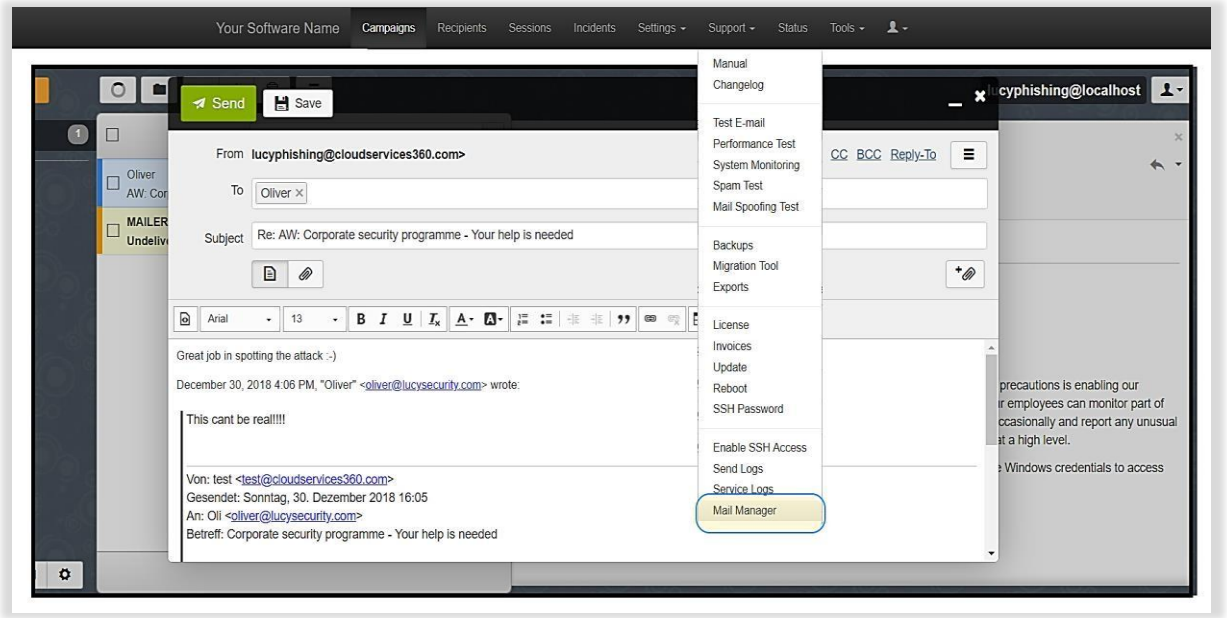
- **Détection de réponse :** la détection de réponse automatique permet de définir et d'analyser au sein de la campagne les réponses automatiques à e-mail (par exemple, absent du bureau) ainsi que les erreurs de remise du courrier (par exemple, utilisateur inconnu).



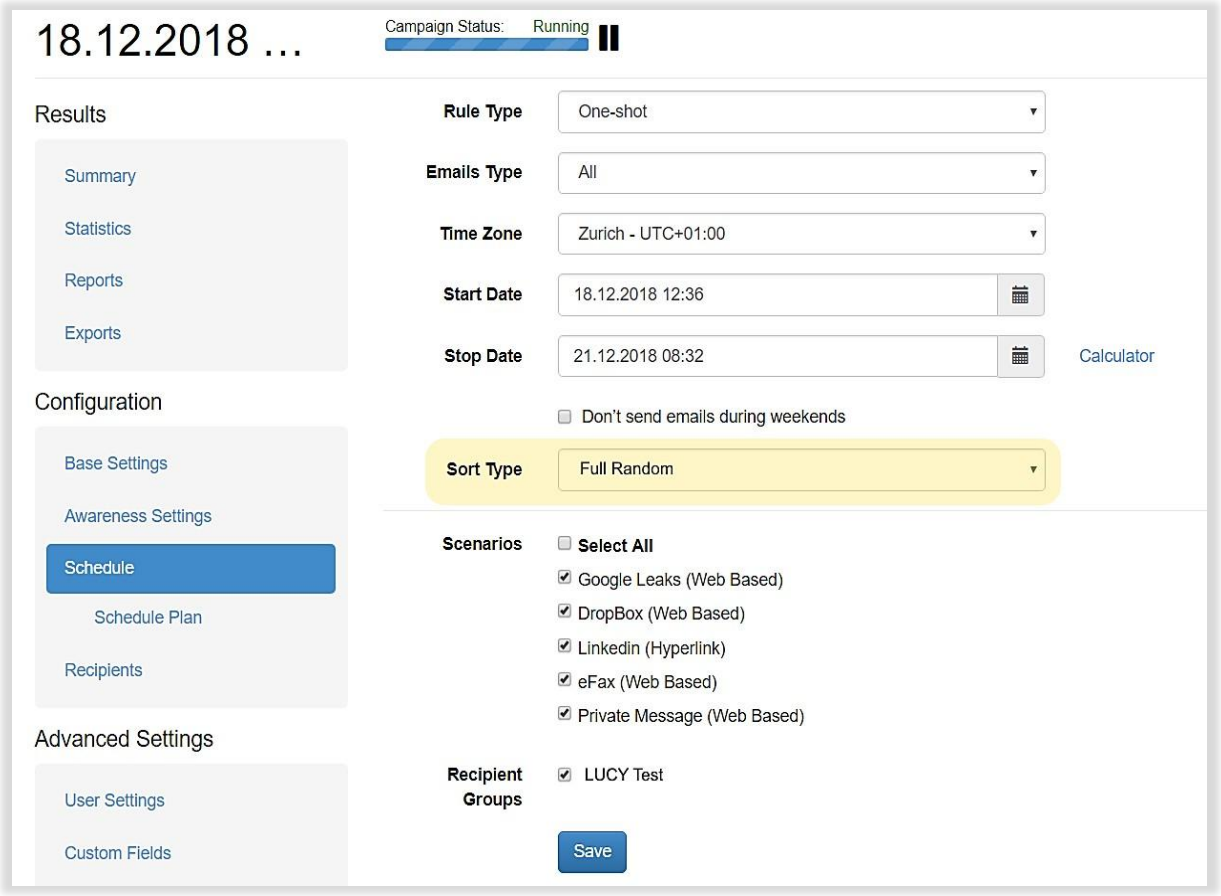




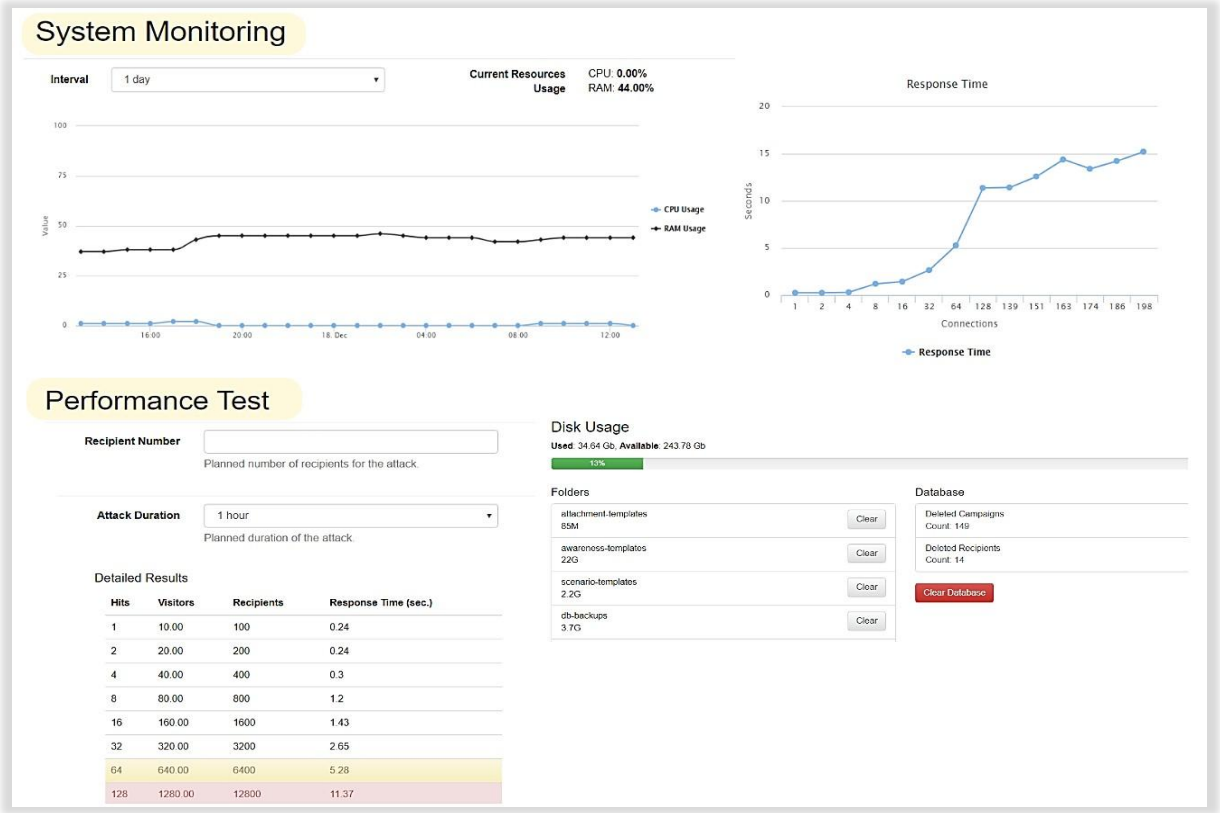
- **Logiciel client de messagerie complet :** une plate-forme de messagerie intégrée permet à l'administrateur de LUCY de communiquer de manière interactive avec les destinataires à l'intérieur ou à l'extérieur des campagnes de LUCY. Tous les e-mails sont archivés et peuvent être évalués.



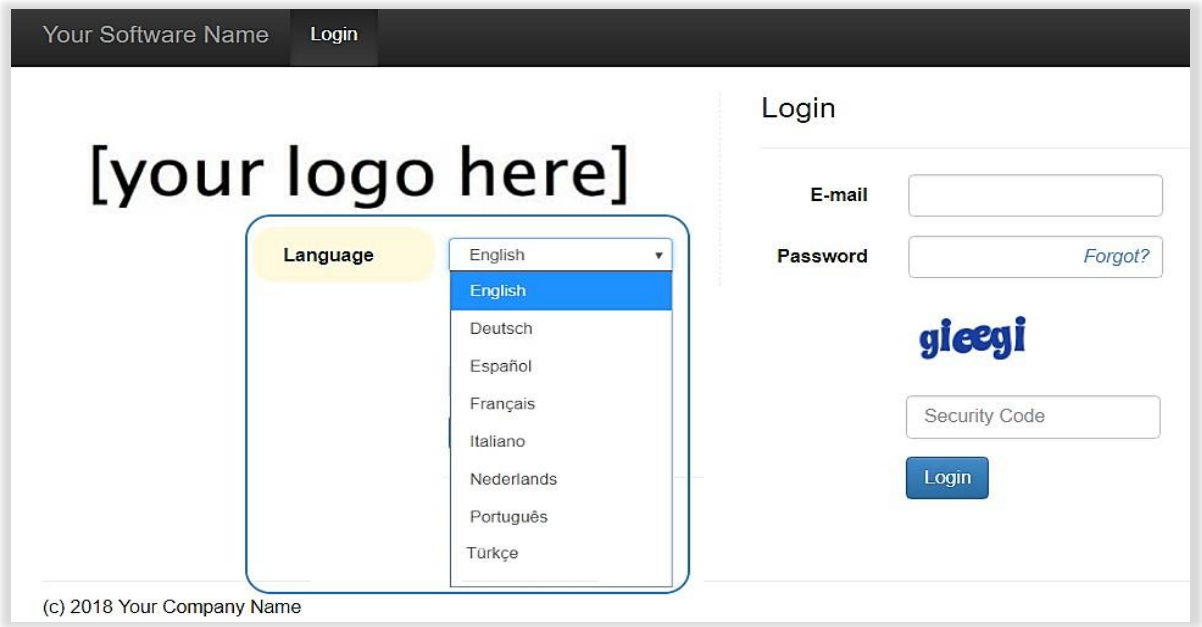
- **Randomisation du planificateur :** sensibiliser les employés de manière aléatoire est le facteur clé d'une sensibilisation efficace et durable au sein de l'entreprise. L'envoi aléatoire de nombreuses campagnes en simultané est l'un des meilleurs moyens de former les employés.



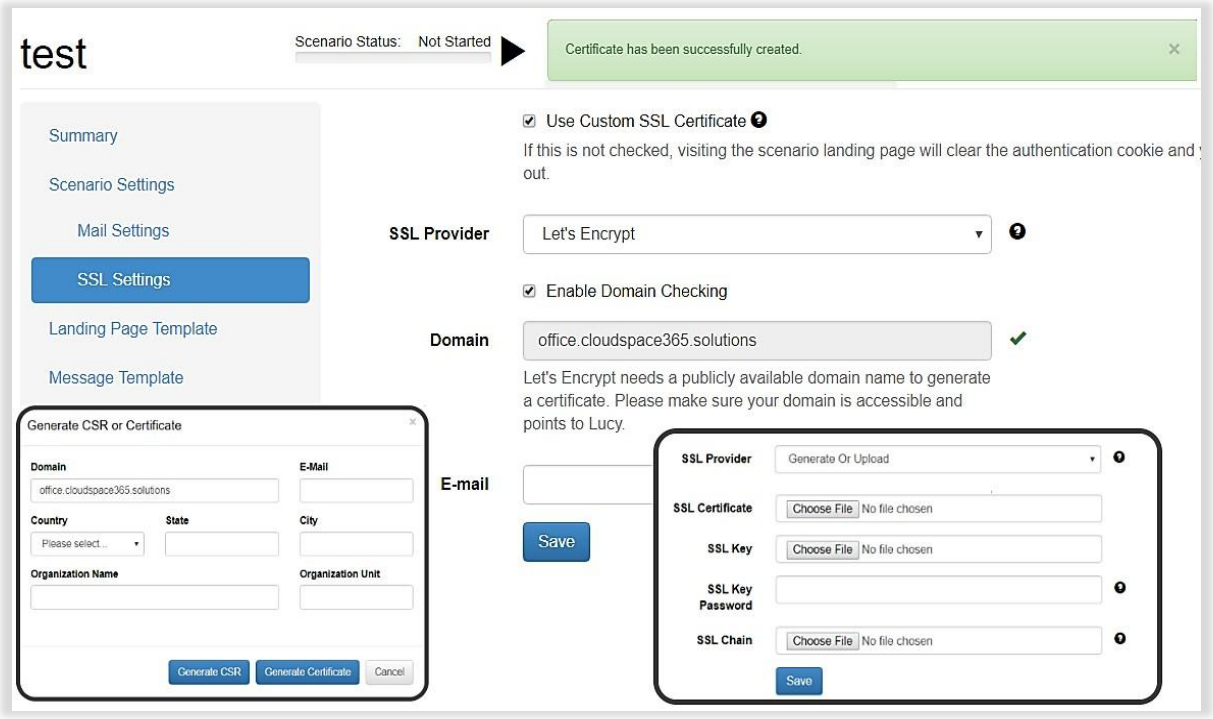
- **Outils de gestion de la performance :** les routines intelligentes de LUCY adaptent l'installation du serveur aux ressources disponibles. Le serveur d'applications, le dimensionnement du SGBD, l'utilisation de la mémoire et de la CPU, sont calculés durant l'installation ou pendant les opérations. Une installation LUCY unique en nuage (cloud) peut être dimensionnée pour plus de 400 000 utilisateurs.



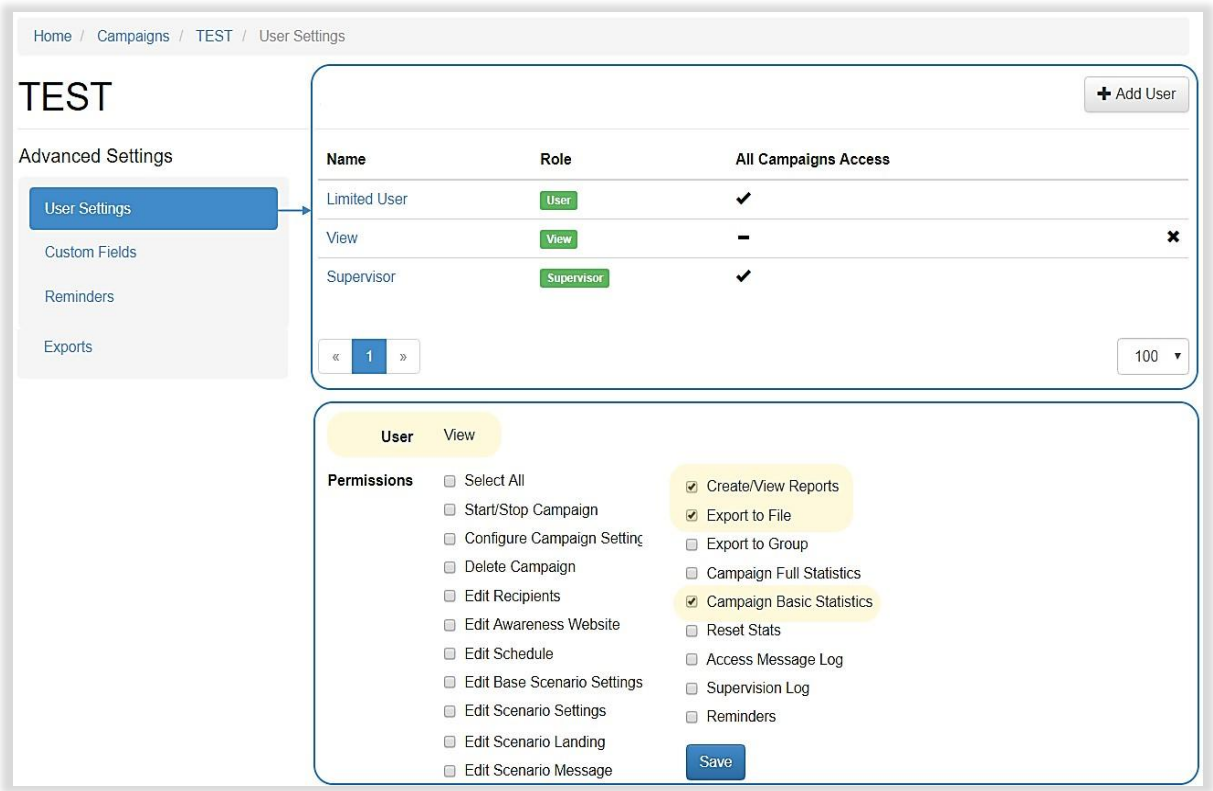
- **Interface d'administration multilingue :** l'interface d'administration de LUCY est disponible dans plusieurs langues et peut être traduite dans d'autres langues sur demande.



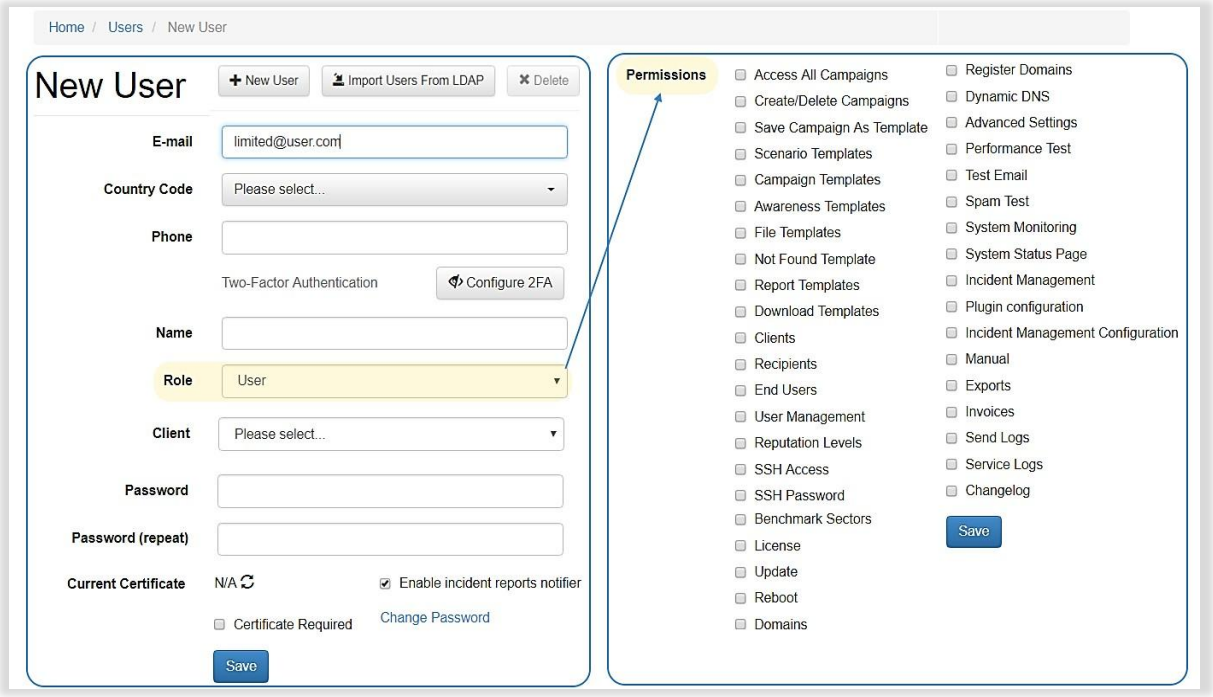
- **Certificate (SSL) :** permet la création automatique de certificats officiels et de confiance pour l'administrateur, le backend, ainsi que pour les campagnes. LUCY utilisera automatiquement le domaine configuré dans le système pour générer le certificat. Si vous décidez d'utiliser SSL pour la campagne, vous pouvez générer un certificat personnalisé ou une CSR (demande de signature du certificat). Vous pouvez également importer des certificats de confiance officiels.



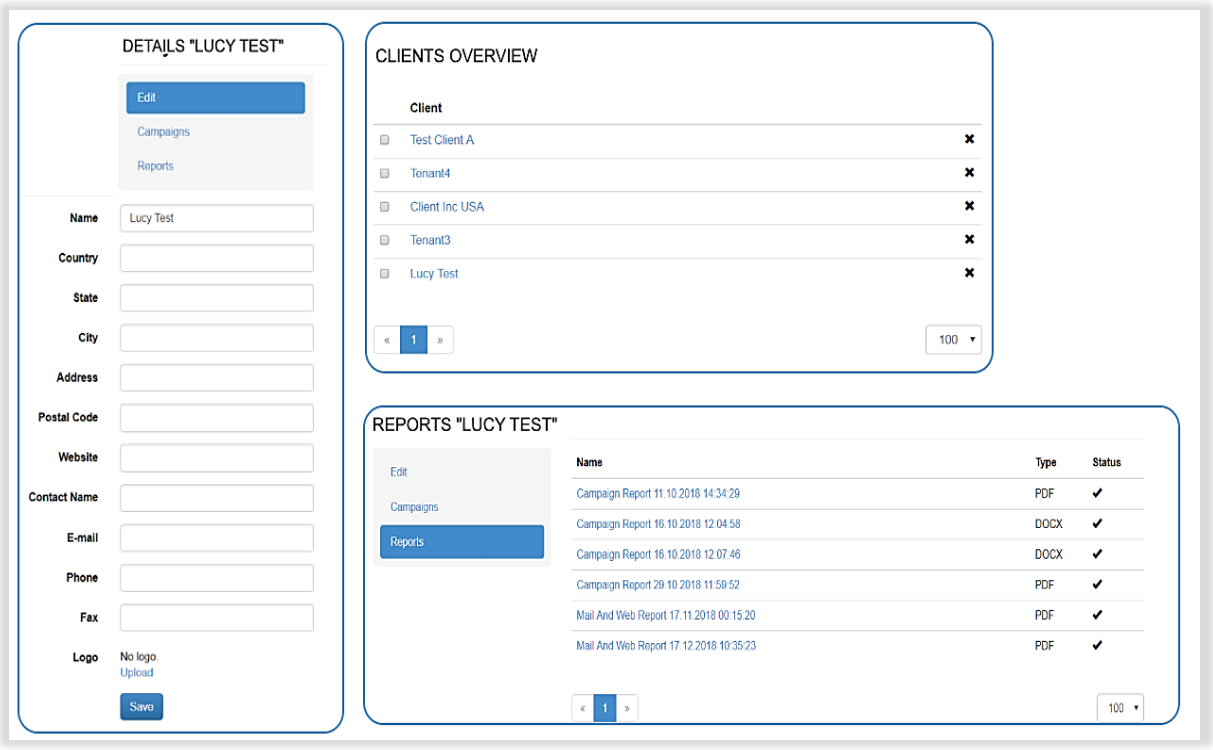
- **Contrôles d'accès basés sur les rôles :** LUCY offre un contrôle d'accès basé sur les rôles (RBAC) qui restreint l'accès au système aux seuls utilisateurs autorisés. Les autorisations permettant d'effectuer certaines opérations sont attribuées à des rôles spécifiques dans les paramètres utilisateur. Les membres ou le personnel (ou d'autres utilisateurs du système) se voient attribuer des rôles particuliers leur permettant d'acquérir les autorisations nécessaires pour exécuter des fonctions particulières de LUCY.



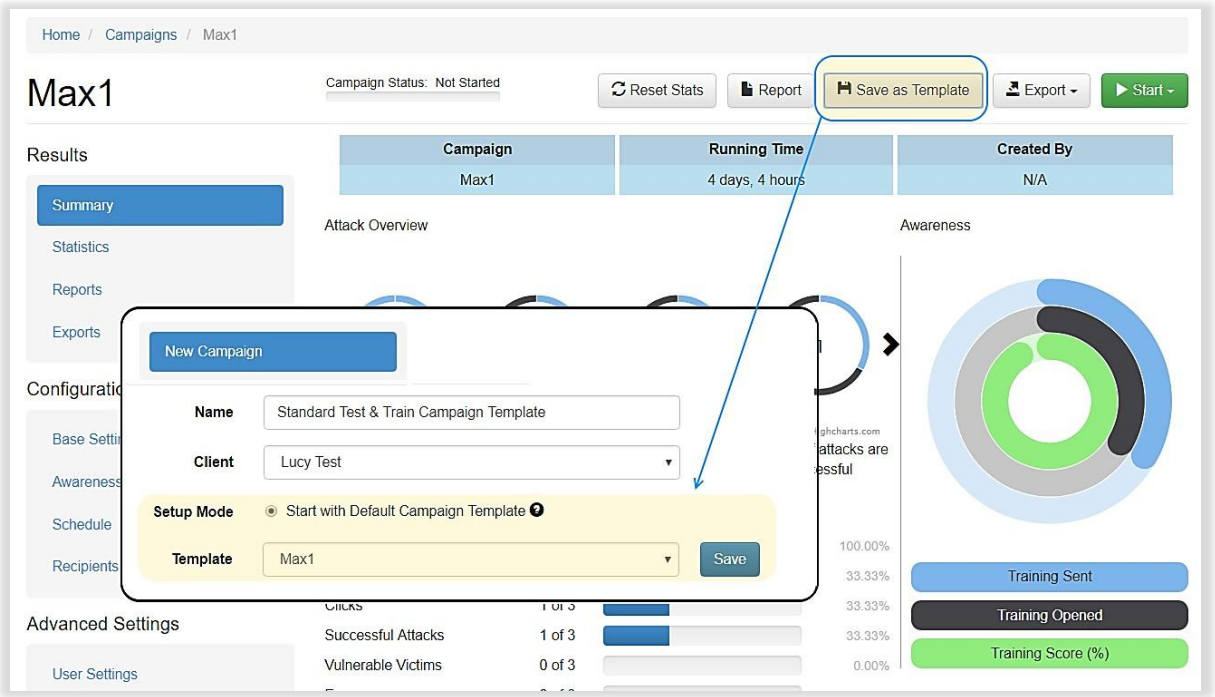
- **Groupes d'utilisateurs multicouches :** importez rapidement des utilisateurs en masse au moyen d'un fichier CSV, LDAP ou texte. Créez différents groupes, organisés par département, division, fonction, etc. Mettez à jour les utilisateurs dans une campagne en cours d'exécution. Créez dynamiquement des groupes d'utilisateurs basés sur les résultats de la campagne d'hameçonnage.



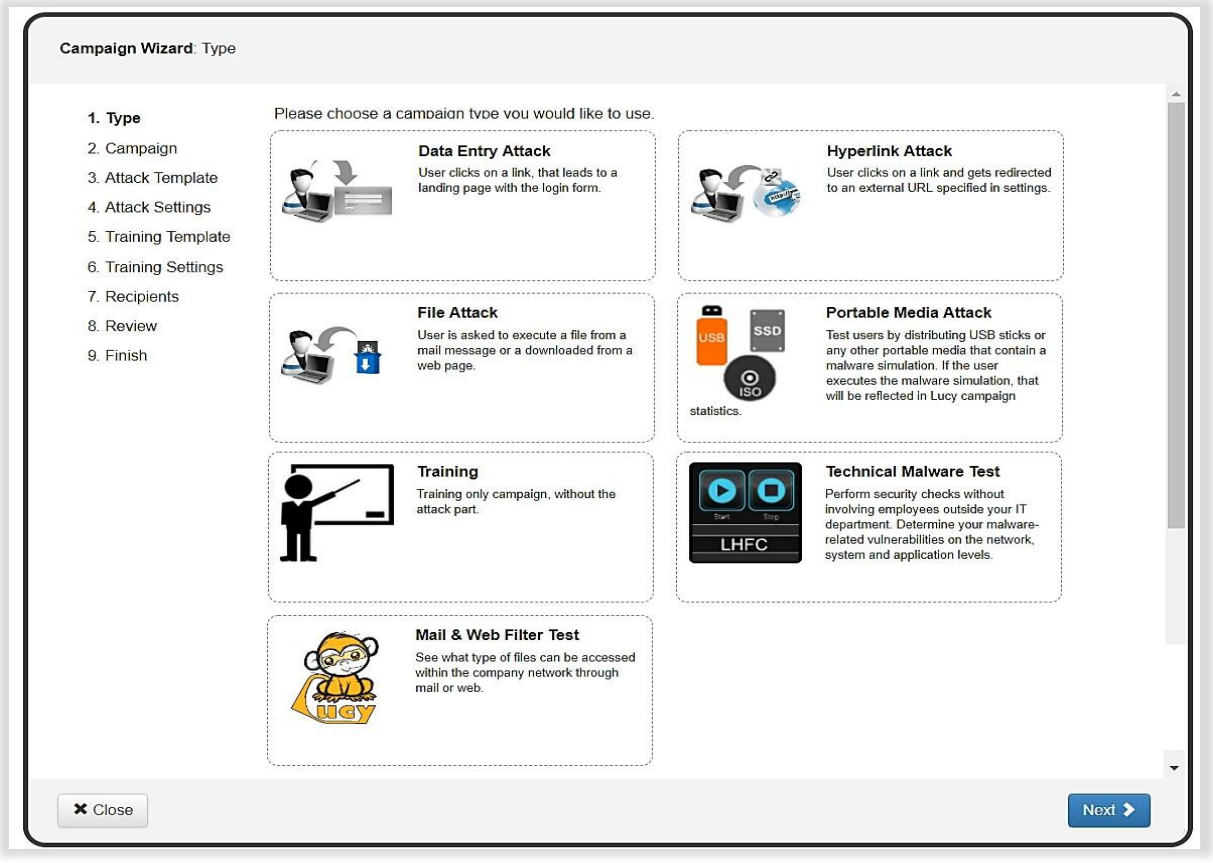
- **Compatible multi-clients :** les « clients » peuvent faire référence à différentes entreprises, départements ou groupes qui ont été associés à une campagne dans LUCY. Ces clients peuvent être utilisés, par exemple, pour autoriser un accès spécifique à une campagne ou pour générer une analyse spécifique à un client.



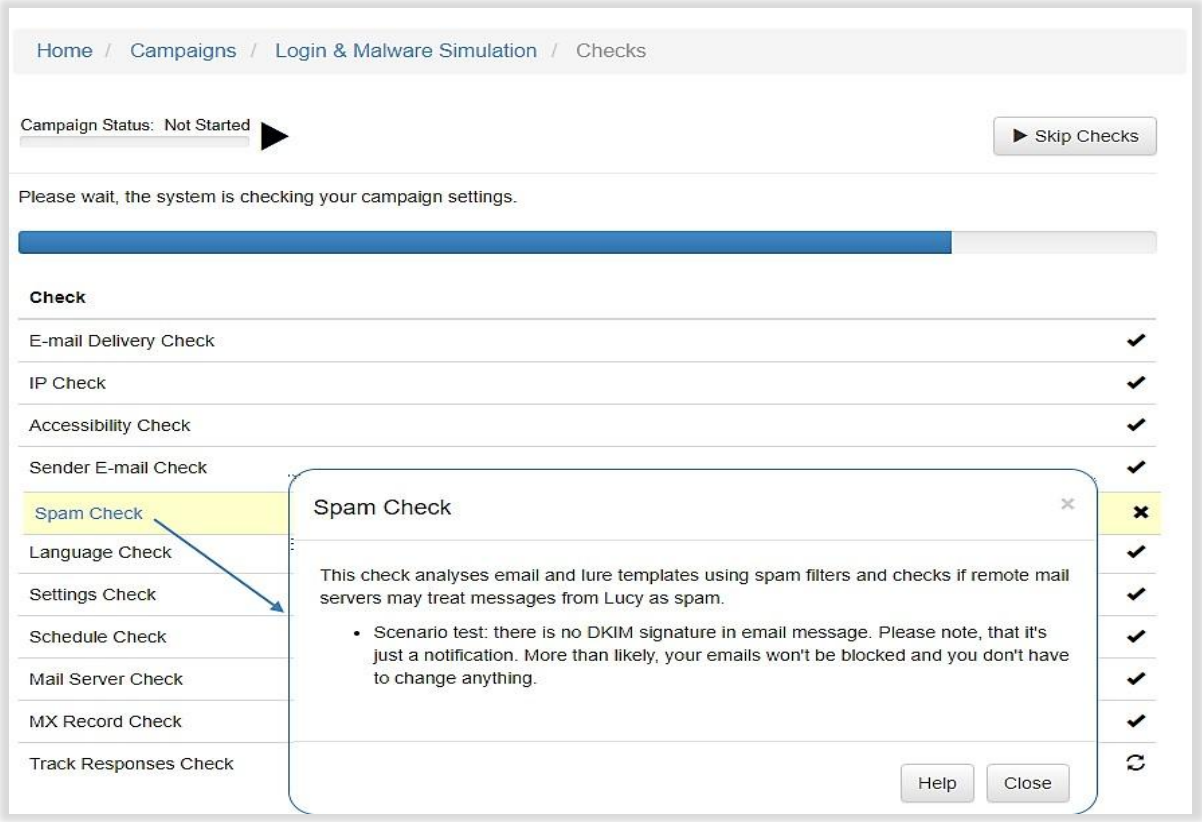
- **Modèles de campagne :** si vous souhaitez réutiliser des campagnes similaires, vous pouvez enregistrer une campagne complète avec ses modèles d'attaque et son contenu d'apprentissage en ligne en tant que modèle de campagne. Cette fonctionnalité vous permet d'éviter de créer sans cesse des configurations similaires.



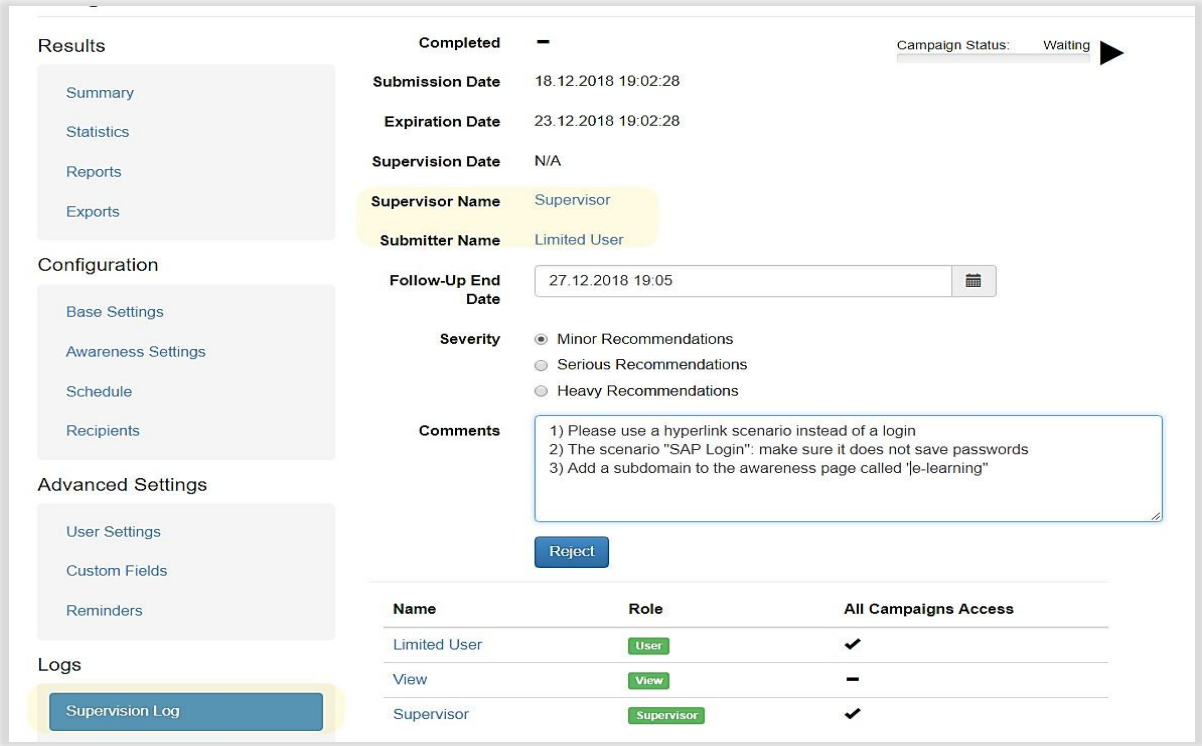
- **Assistant d'installation guidée et basée sur le risque :** LUCY propose plusieurs outils de configuration. Créez une campagne complète en moins de 3 minutes à l'aide des modèles de campagne prédéfinis ou laissez l'assistant de configuration vous guider dans la configuration. En option, vous pouvez utiliser un mode de configuration basé sur les risques qui émet des suggestions spécifiques pour la sélection des modèles d'attaque et de sensibilisation, basées sur la taille de l'entreprise et son secteur d'activité.



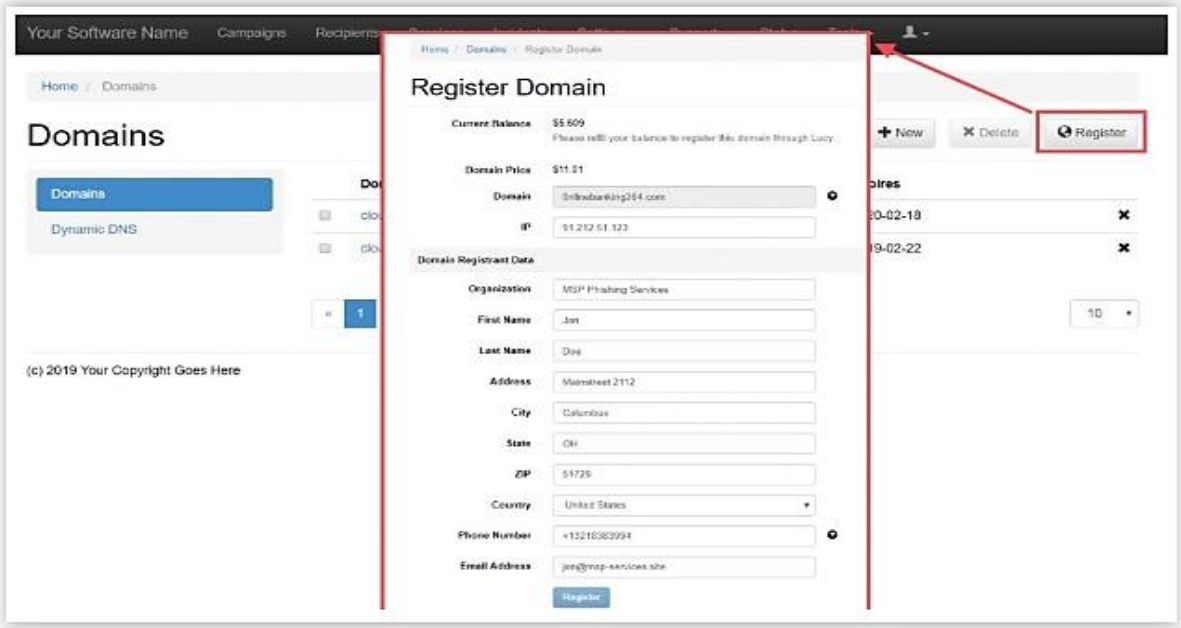
- **Contrôles de campagne :** contrôles préliminaires avant de lancer une campagne dans LUCY : contrôle de la remise des e-mails, contrôle de l'enregistrement MX, contrôle du planning, contrôle du courrier indésirable, etc.



- **Processus d'approbation :** une campagne donnée peut être soumise à un superviseur de LUCY pour son approbation.

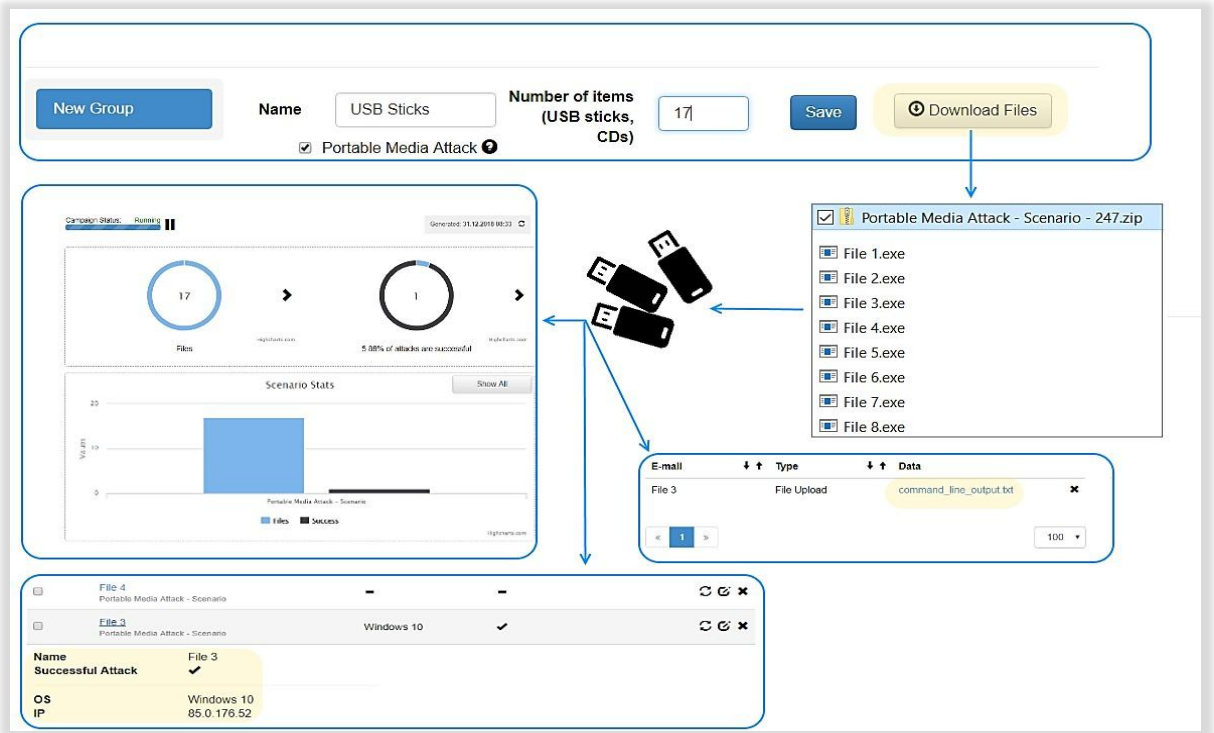


- **API DNS :** l'API DNS permet à l'administrateur de créer n'importe quel domaine sur LUCY en quelques secondes. Comme les attaquants utilisent très souvent des noms de domaine dont l'orthographe est similaire à celui du client (appelé Typosquattage), ce risque peut également être recréé dans LUCY. Si le domaine original du client est par exemple « onlinebanking.com », l'assistant du DNS peut être utilisé pour réserver des domaines tels que « 0nlinebanking.com », « onl1nebanking.com » ou « onlinebanking.services » et les affecter ultérieurement à une campagne. LUCY crée alors automatiquement les entrées DNS correspondantes (MX, SPF, Protection Whois, etc.) pour l'IP sur lequel LUCY est installé. Bien sûr, l'administrateur peut aussi utiliser dans LUCY les domaines propres de son fournisseur.

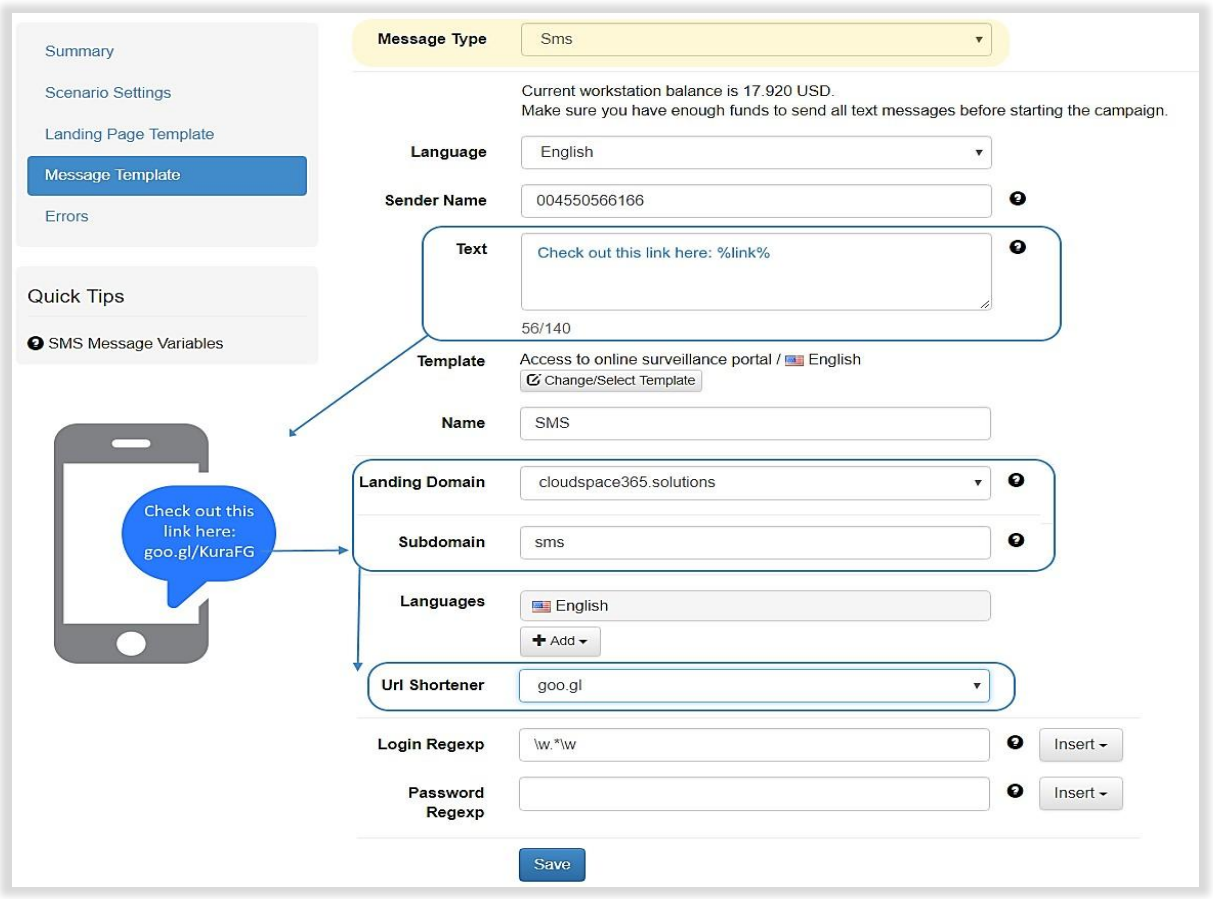


SIMULATION D'ATTAQUE

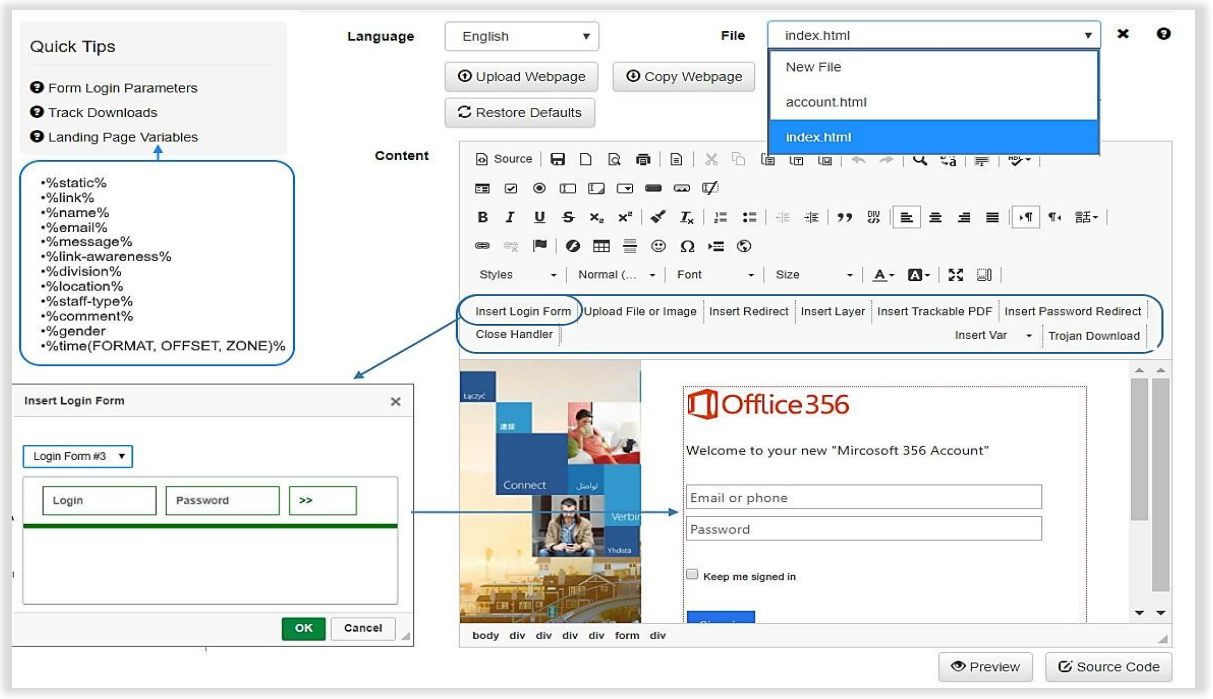
- **Attaques de supports amovibles :** les pirates informatiques peuvent utiliser les lecteurs de supports amovibles pour accéder aux informations sensibles stockées sur un ordinateur ou un réseau. LUCY offre la possibilité de lancer des attaques de supports amovibles dans lesquelles un modèle de fichier (par exemple, fichier exécutable, fichier archive, document bureautique contenant des macros, etc.) peut être stocké sur un périphérique de stockage amovible tel que clé USB, carte SD ou CD. L'activation (exécution) de ces fichiers individuels peut être suivie dans LUCY.



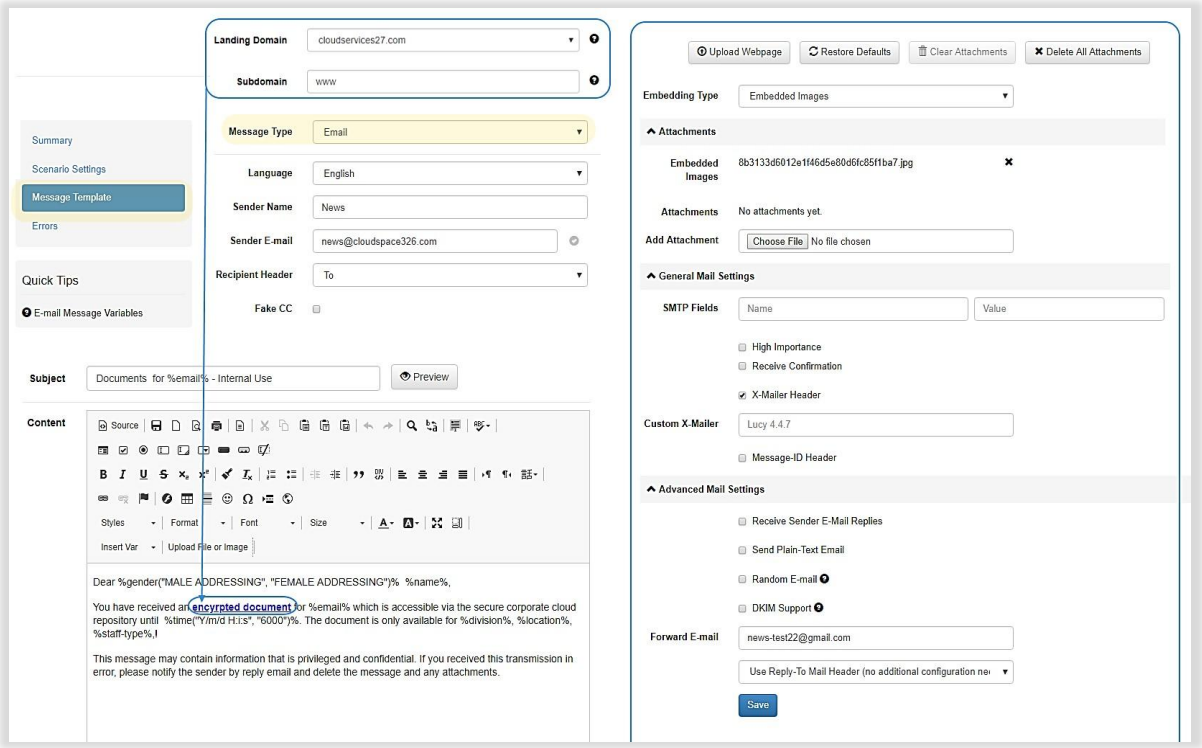
- **SMiShing :** le SMiShing est en quelque sorte un « hameçonnage par SMS ». Lorsque les cybercriminels « leurrent », ils envoient des e-mails frauduleux qui cherchent à amener le destinataire à ouvrir une pièce jointe truffée de programmes malveillants ou à cliquer sur un lien malveillant. Le SMiShing utilise simplement des messages de texte au lieu d'e-mails.



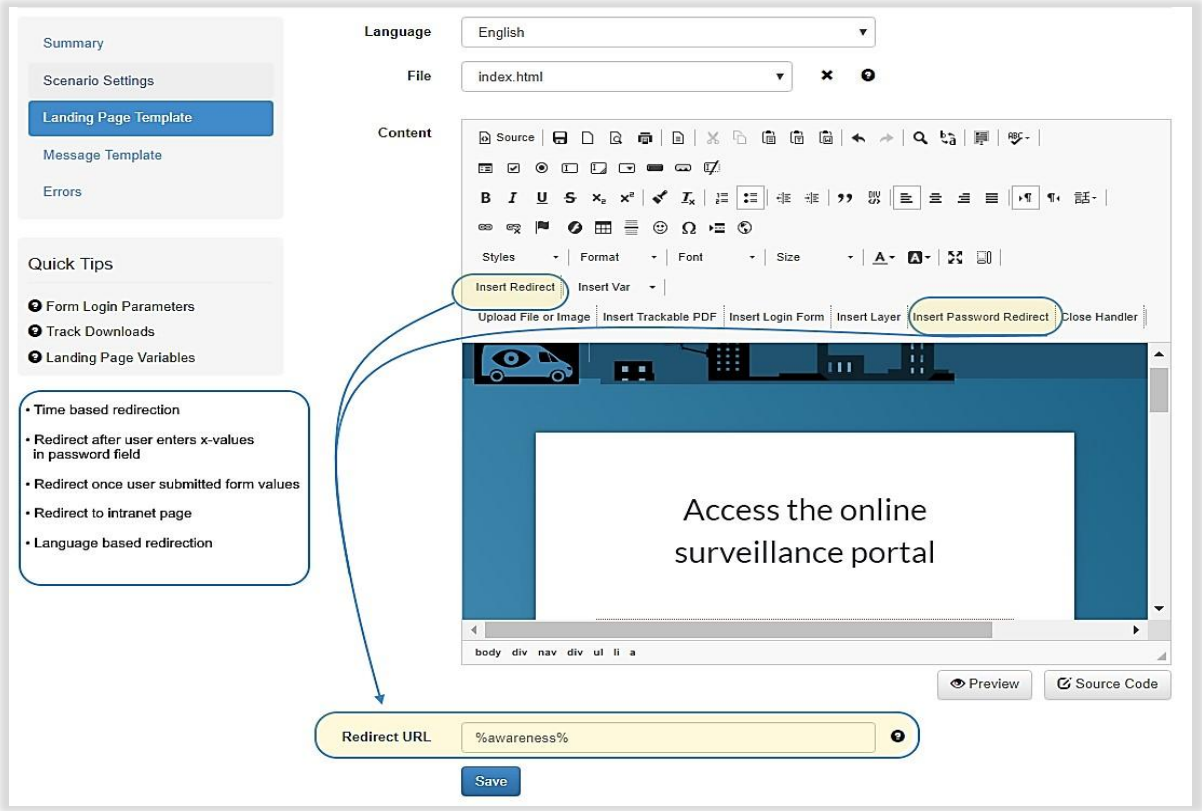
- **Attaques de saisie de données :** les attaques lors de la saisie de données peuvent inclure une ou plusieurs pages Web qui interceptent la saisie d'informations sensibles. Les pages Web à disposition peuvent être facilement personnalisées au moyen d'un éditeur Web de LUCY. Des outils d'édition supplémentaires vous permettent de configurer rapidement des éléments tels que des formulaires de connexion, des zones de téléchargement, etc., sans connaissance du langage HTML.



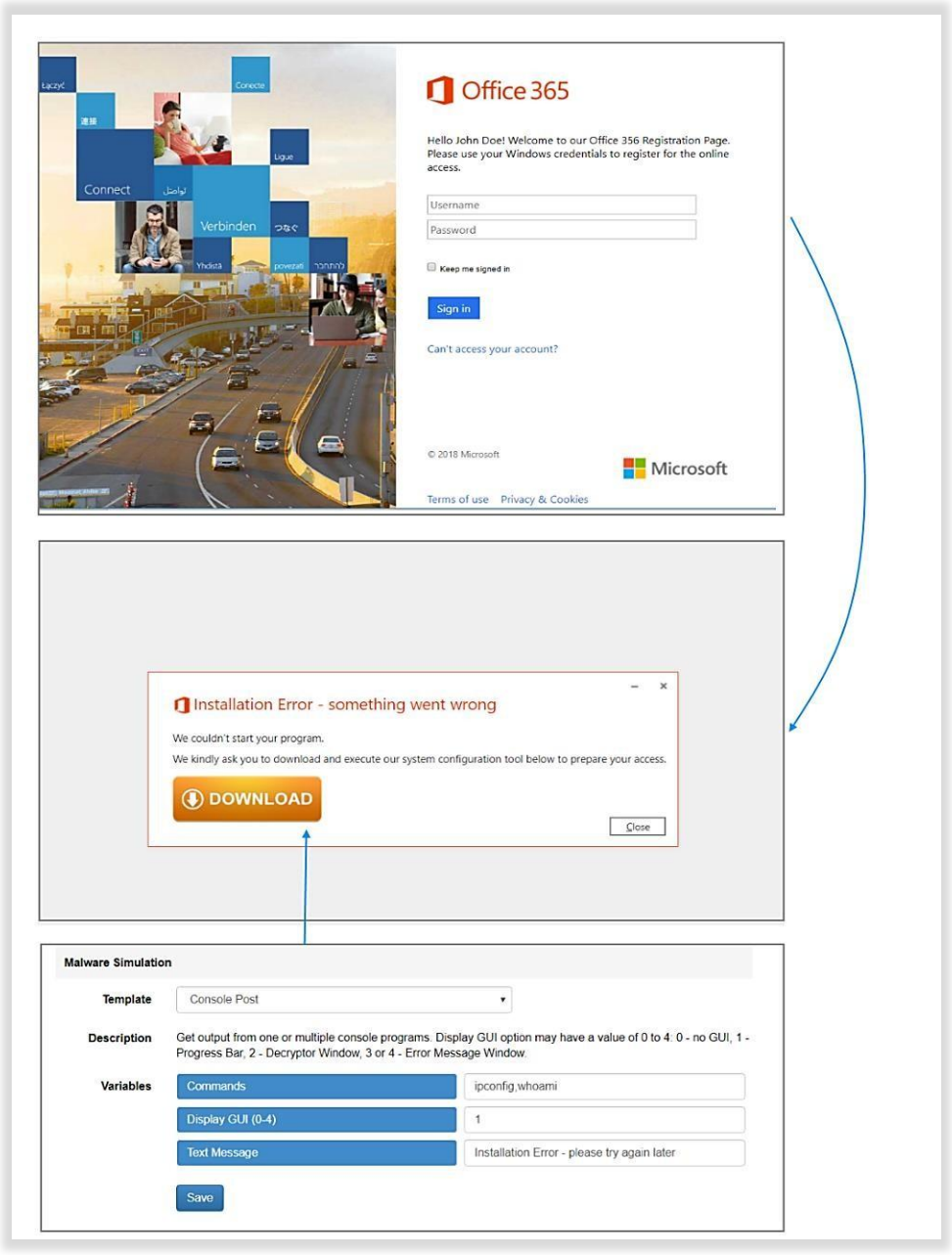
- **Attaques de liens hypertextes :** une campagne basée sur un lien hypertexte enverra aux utilisateurs un e-mail contenant une URL de suivi aléatoire.



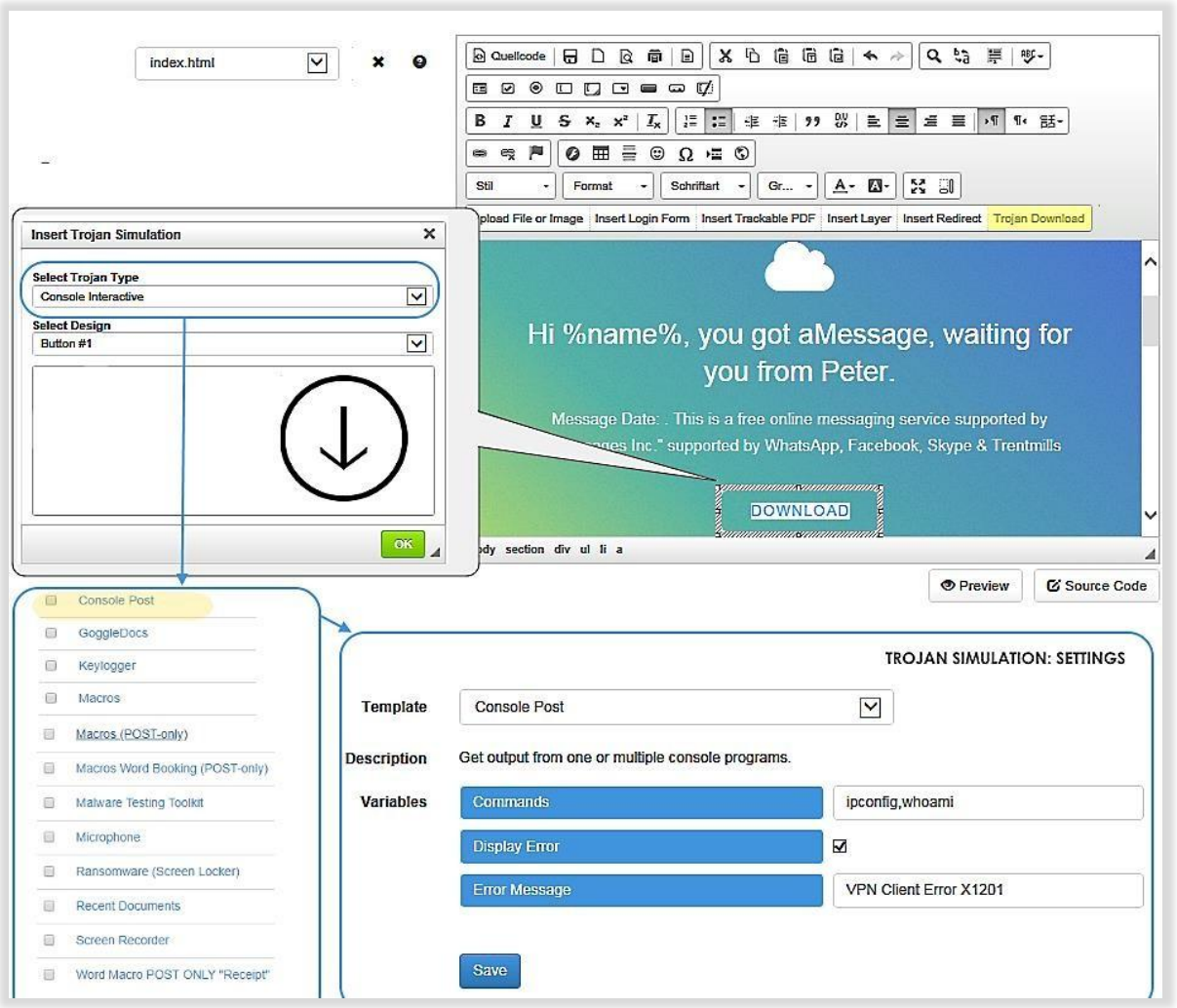
- **Boîte à outils performante de redirection d'URL :** les fonctions de redirection flexibles de LUCY permettent à l'utilisateur d'être guidé, au bon moment, vers les zones de simulation d'attaque ou de formation souhaitées. Par exemple, après avoir saisi les 3 premiers caractères d'un mot de passe dans une simulation d'hameçonnage, l'utilisateur peut être redirigé vers une page de formation axée sur la protection du mot de passe.



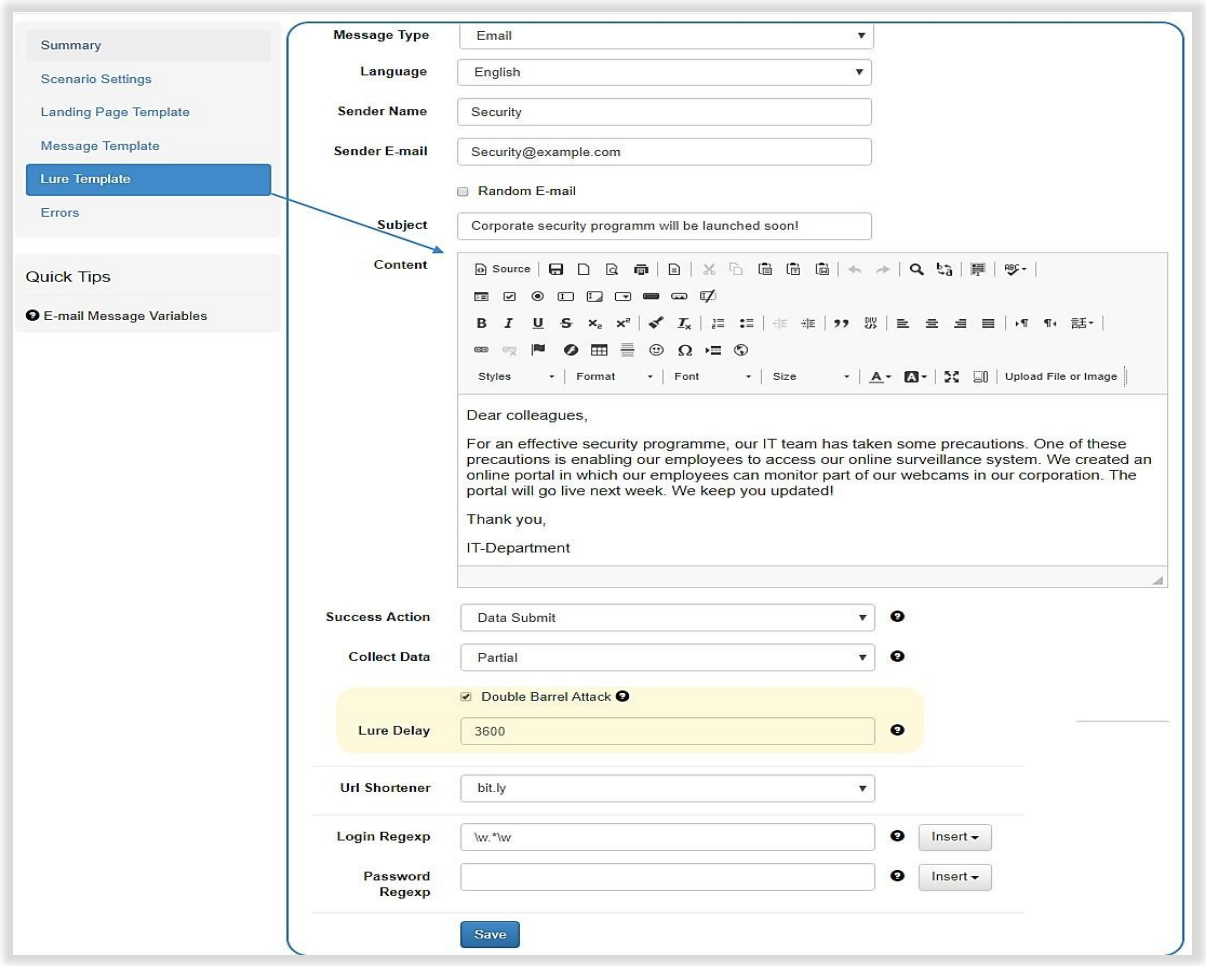
- **Attaques mixtes :** les attaques mixtes permettent de combiner plusieurs types de scénario (basé sur un fichier, saisie de données, etc.) dans une même campagne.



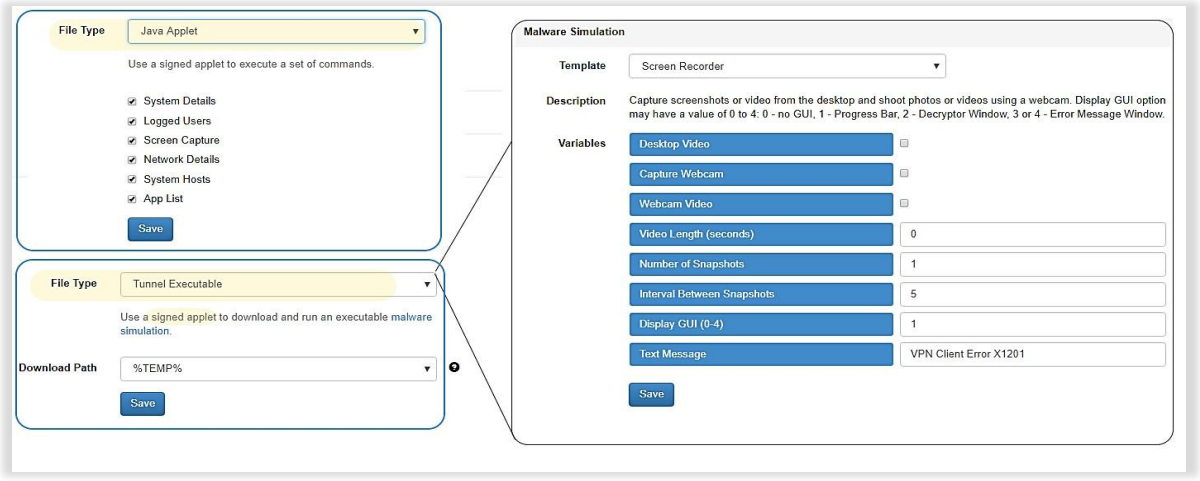
- **Attaques basées sur des fichiers :** la fonctionnalité des attaques basées sur des fichiers permet à l'administrateur de LUCY d'intégrer différents types de fichiers (documents bureautiques contenant des macros, PDF, exécutables, MP3, etc.) dans des pièces jointes ou sur des sites Web générés sur LUCY, et de mesurer leur taux de téléchargement ou d'exécution.



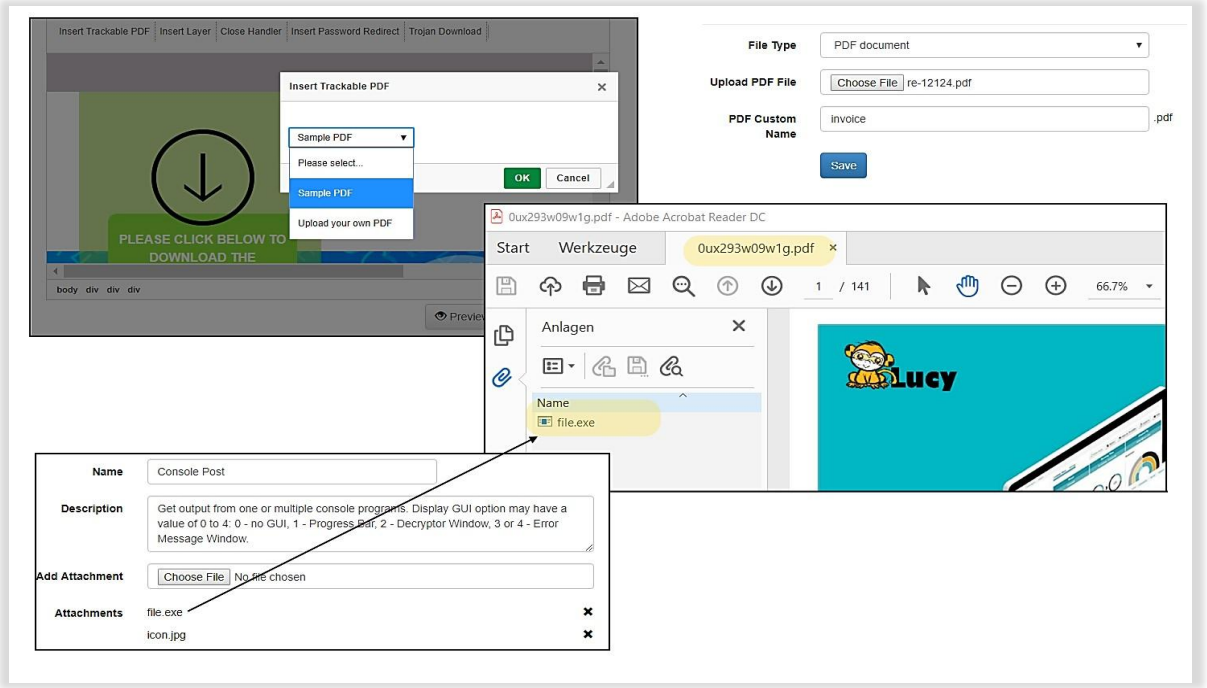
- **Attaques Double Barrel :** cette fonctionnalité permet d'envoyer plusieurs e-mails d'hameçonnage dans chaque campagne, le premier e-mail bénin (l'appât) ne contenant rien de malveillant et n'exigeant pas de réponse du destinataire.



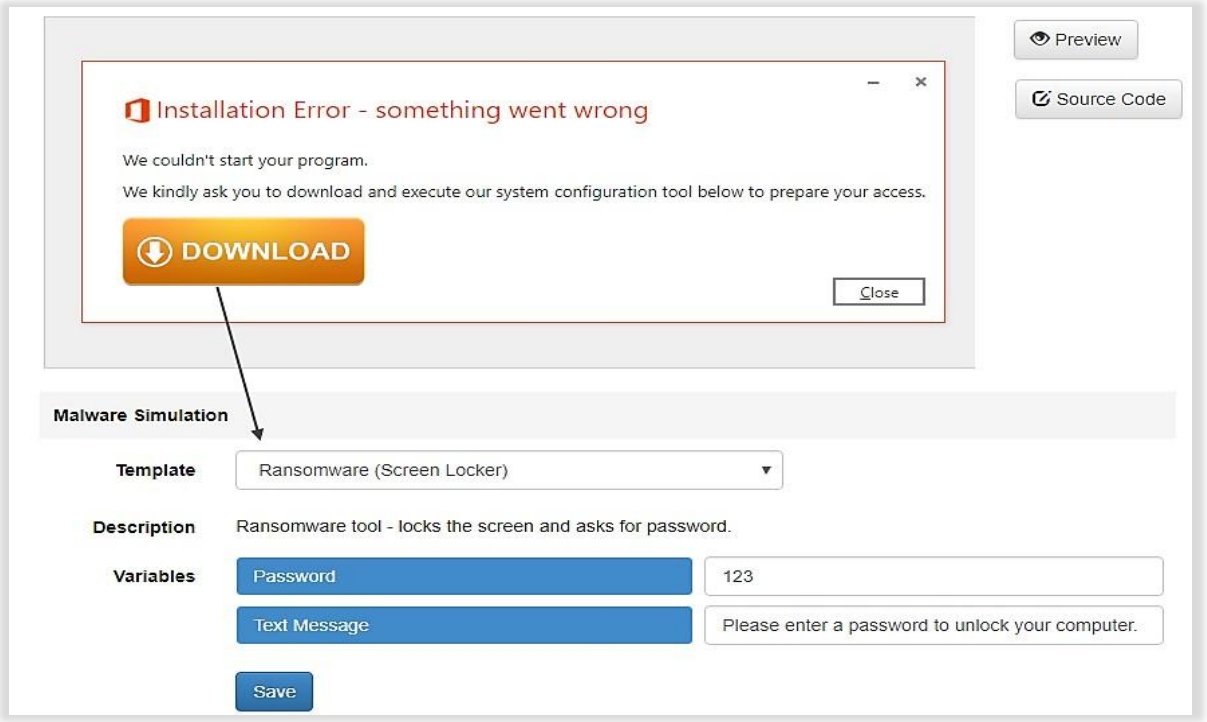
- **Attaques basées sur Java :** la fonctionnalité des attaques basées sur Java permet à l'administrateur de LUCY d'intégrer une applet de confiance dans les modèles d'attaques mixtes ou basées sur des fichiers fournis dans LUCY, et de mesurer leur exécution par l'utilisateur.



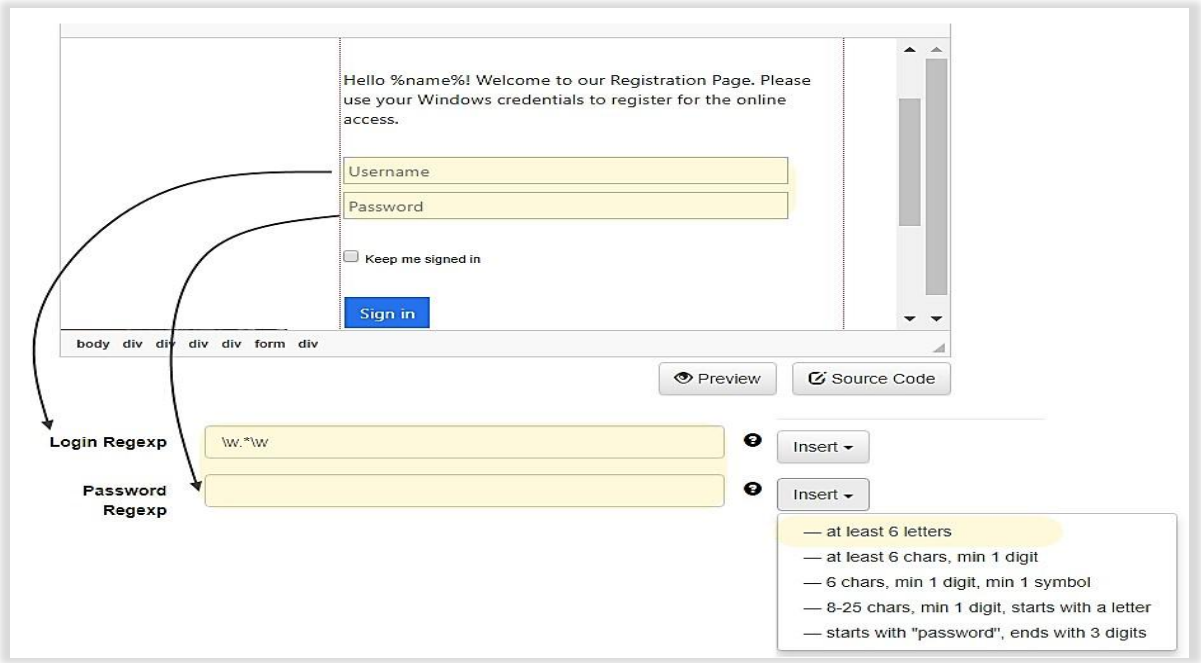
- **Attaques basées sur PDF :** les attaques d'hameçonnage basées sur des fichiers PDF peuvent être simulées avec ce module. LUCY permet de « dissimuler » des fichiers exécutables sous forme de pièces jointes PDF et de mesurer leur exécution. En outre, des liens d'hameçonnage dynamiques peuvent également être générés au sein des fichiers PDF.



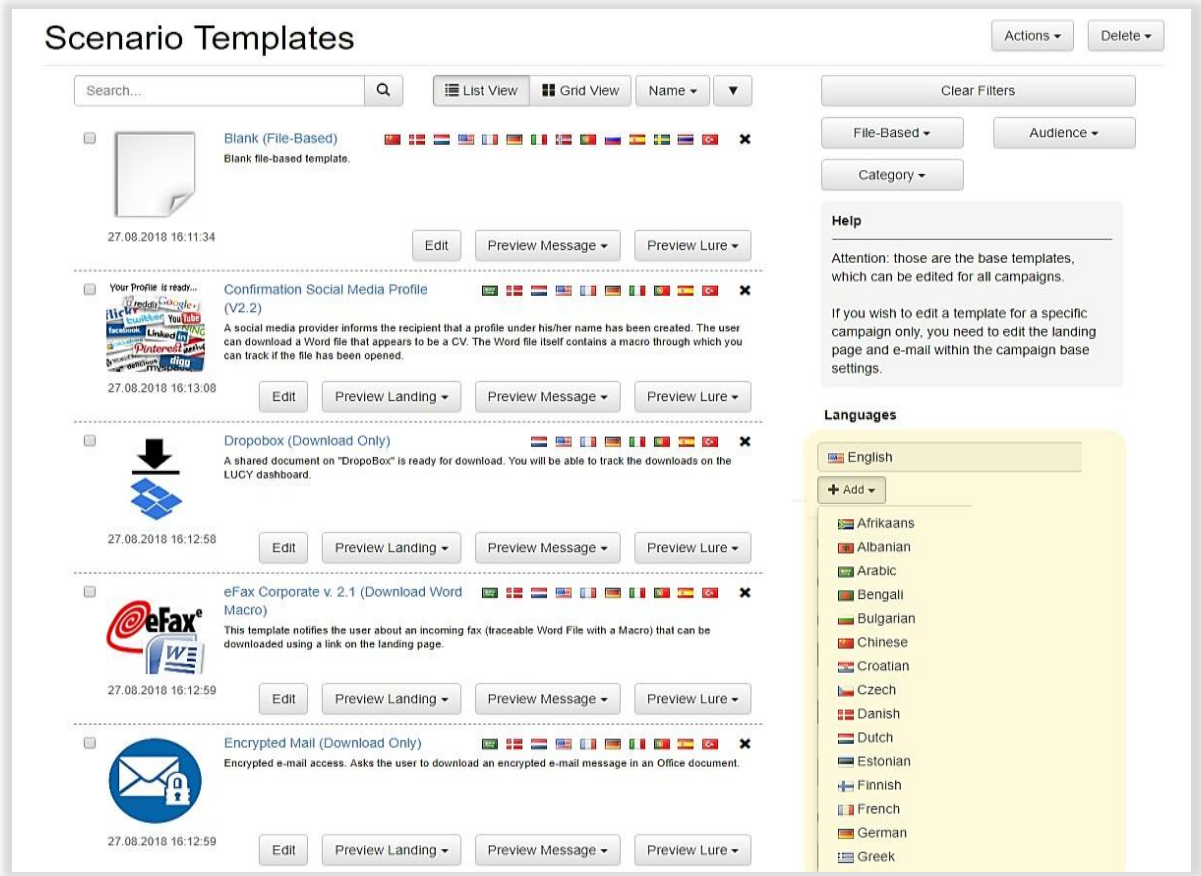
- **Attaques simulant un logiciel rançonneur :** LUCY propose deux simulations de logiciel rançonneur différentes, l'une testant le personnel et l'autre l'infrastructure.



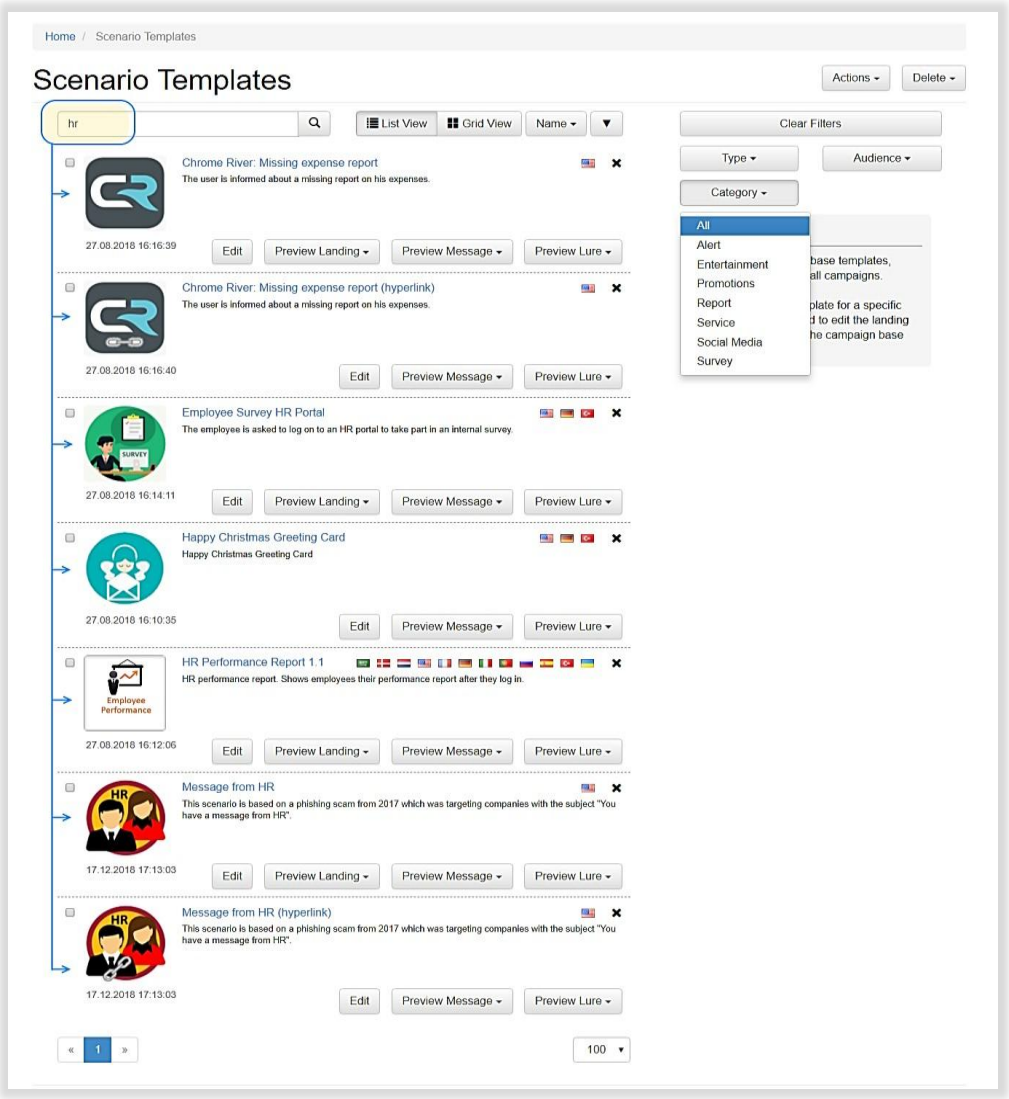
- **Boîte à outils de validation de la saisie de données :** dans les simulations d'hameçonnage, il faut éviter les faux positifs dans les champs de connexion (par exemple, l'identification avec une syntaxe non valide). Les directives de l'entreprise peuvent également interdire la transmission de données sensibles telles que les mots de passe. À cet effet, LUCY fournit un moteur de filtrage d'entrée flexible qui offre une solution adaptée à chaque exigence.



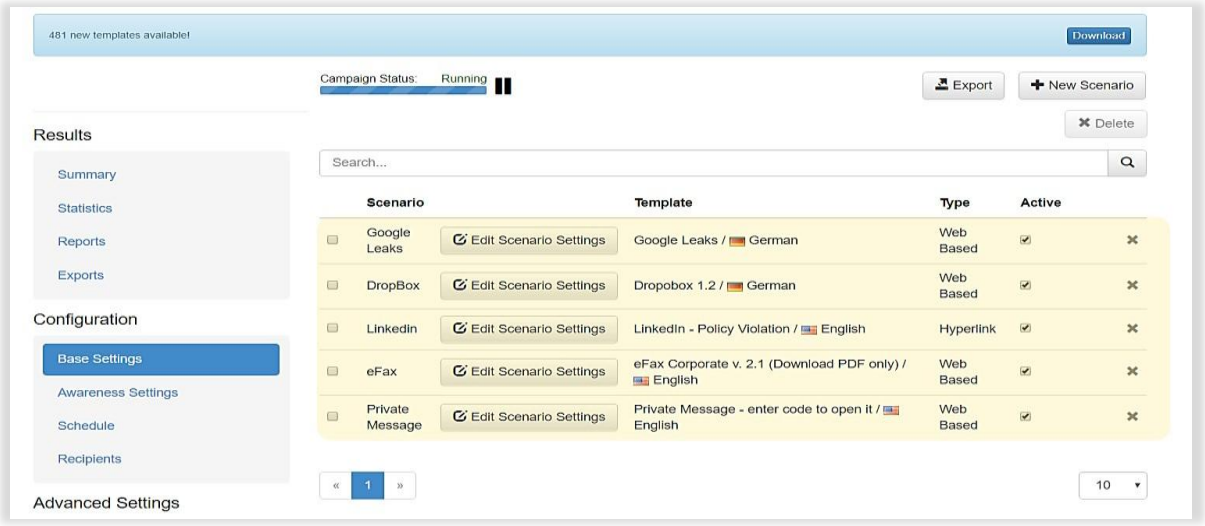
- **Bibliothèque de modèles d'attaque multilingues :** LUCY est livré avec des centaines de modèles d'attaques prédéfinis dans plus de 30 langues, dans les catégories de saisie de données (modèles avec site Web), basée sur des fichiers (e-mails ou sites Web avec téléchargement de fichier), lien hypertexte (e-mails avec un lien), mixtes (combinaison de saisie de données et de téléchargement) et supports amovibles.



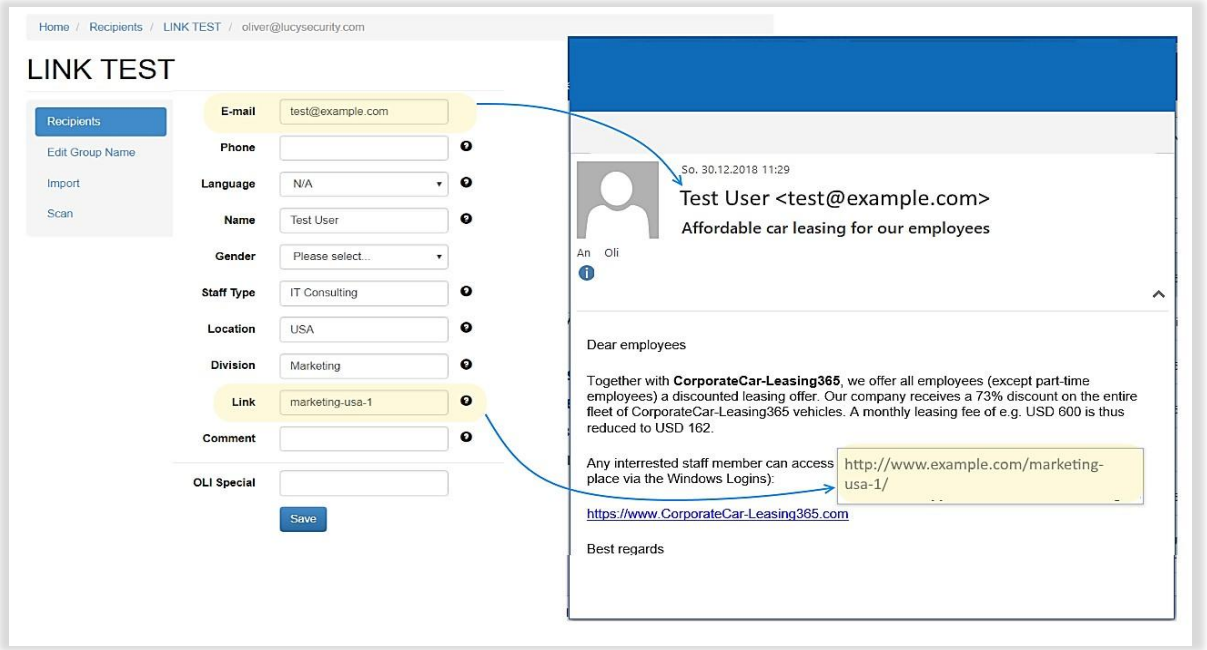
- **Modèles spécifiques à des secteurs d'activité et à des divisions :** les modèles d'attaque sont disponibles pour des secteurs d'activité ou des divisions spécifiques.



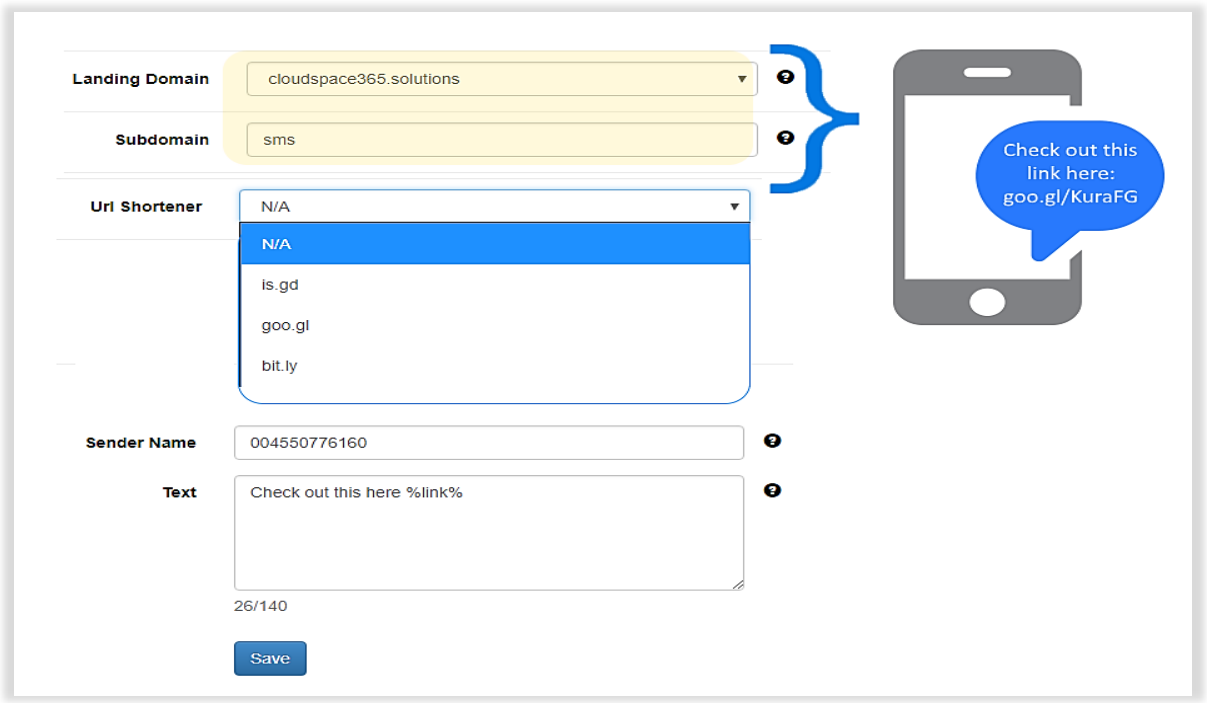
- **Utilisation simultanée de plusieurs modèles d'attaque :** LUCY vous offre la possibilité d'utiliser plusieurs modèles d'attaque simulée dans une même campagne. Mélangez les différents types (lien hypertexte, basée sur des fichiers, etc.) avec différents thèmes d'attaque, pour obtenir la couverture de risque la plus large possible et une meilleure compréhension des vulnérabilités des employés. En combinaison avec notre randomiseur de planification, des schémas d'attaque complexes peuvent être exécutés sur une période prolongée.



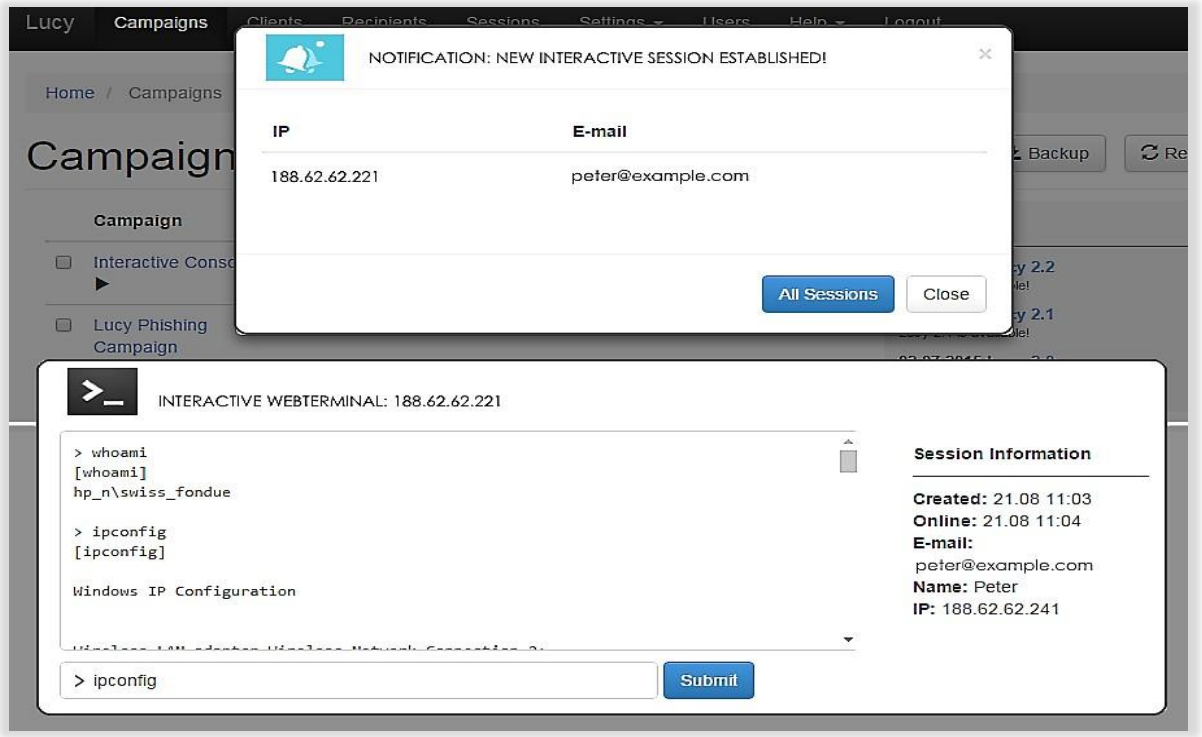
- **Variantes des URL d'attaque :** prenez le contrôle des URL générées pour identifier les destinataires. Utilisez des chaînes d'URL courtes (< 5 caractères) ou longues automatisées, ou définissez des URL individuelles pour chaque utilisateur. La création manuelle d'URL vous permet de créer des liens que l'utilisateur peut facilement mémoriser. Dans les environnements où les clics sur les liens sont désactivés dans les e-mails, ceci est impératif.



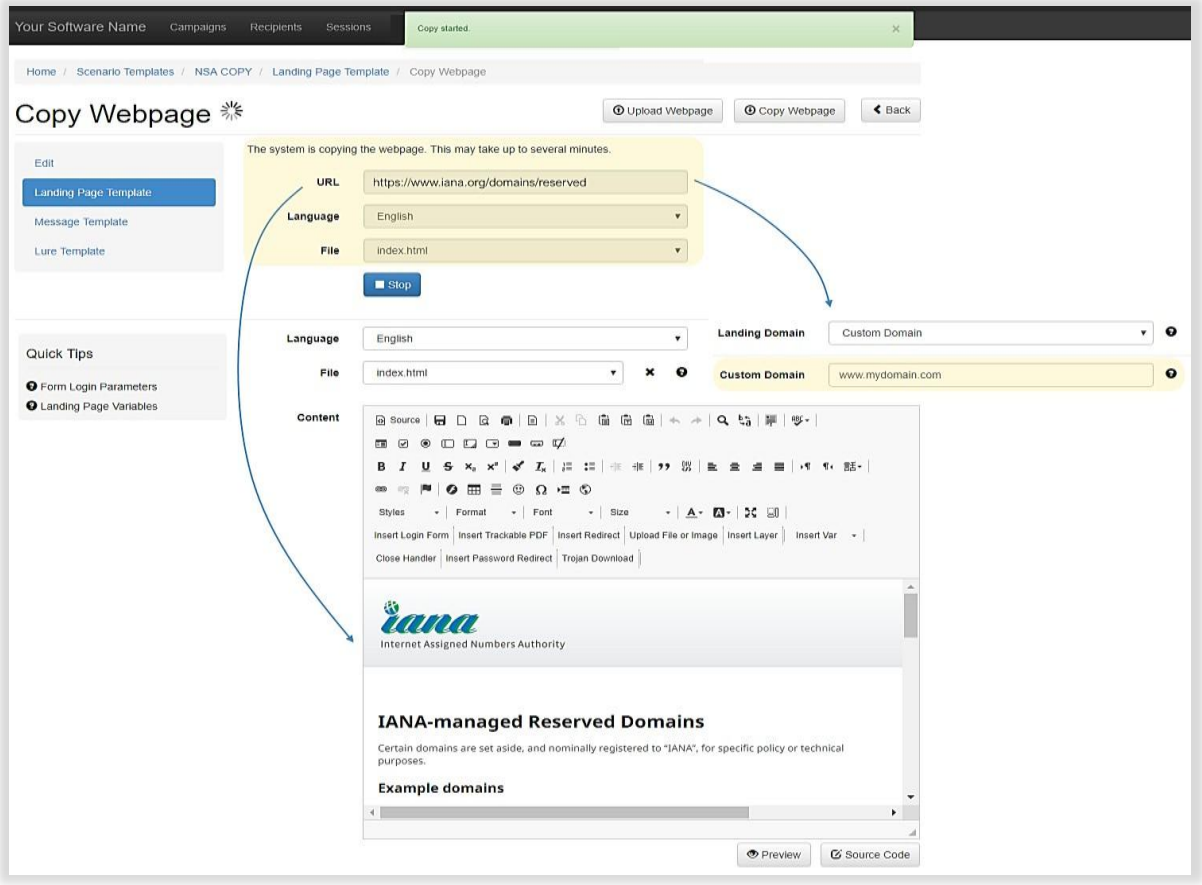
- **Raccourcissement d'URL :** le raccourcissement d'URL est un service Internet relativement nouveau. Comme de nombreux réseaux sociaux en ligne imposent des limitations de caractères (Twitter, par exemple), ces URL sont très pratiques. Néanmoins, le raccourcissement d'URL peut être utilisé par les cybercriminels pour masquer la cible réelle d'un lien, telle que des sites Web d'hameçonnage ou infectés. Pour cette raison, LUCY offre la possibilité d'intégrer différents services de raccourcissement dans une campagne d'hameçonnage ou de SMiShing.



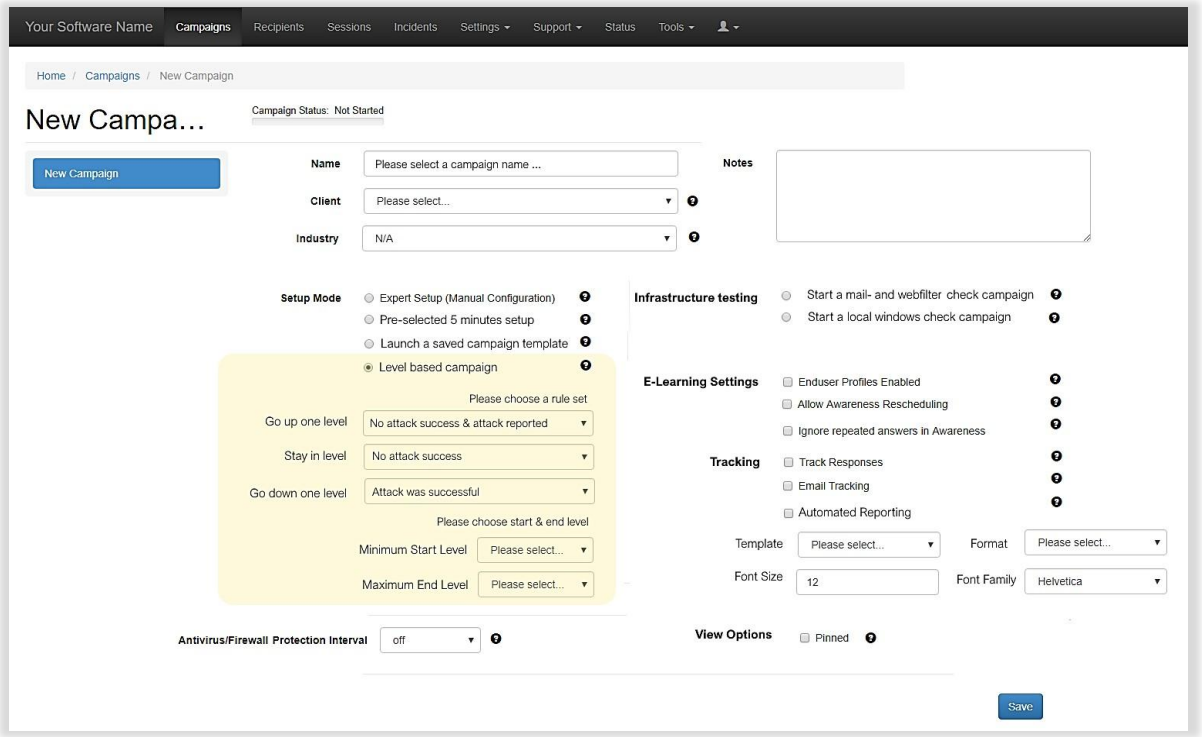
- **Kit de test d'intrusion Pentest :** le Kit de test d'intrusion Pentest est un sous-module de la boîte à outils de simulation de programmes malveillants et porte le nom de « Sessions Interactives ». Il vous permet de communiquer de manière interactive avec un ordinateur client installé derrière un pare-feu à l'aide de connexions http/s inversées.



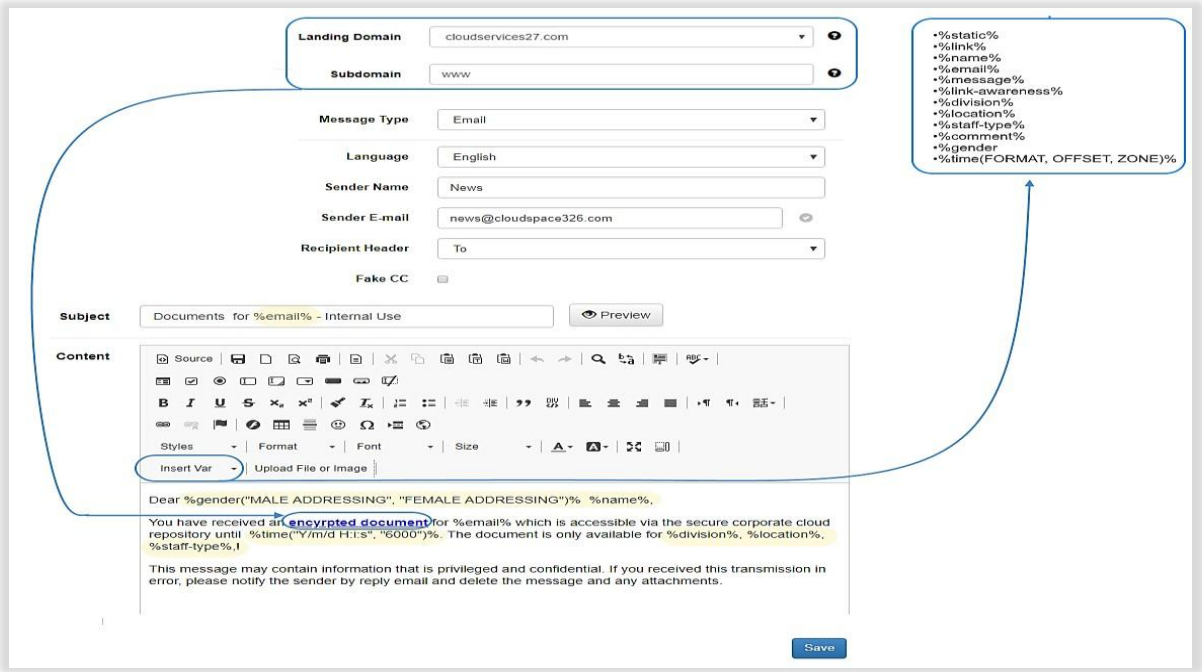
- **Clonage de site Web :** créez rapidement des pages de destination très professionnelles pour vos campagnes. Clonez des sites Web existants et ajoutez des couches supplémentaires avec des champs de saisie de données, des fichiers à télécharger, et plus encore.



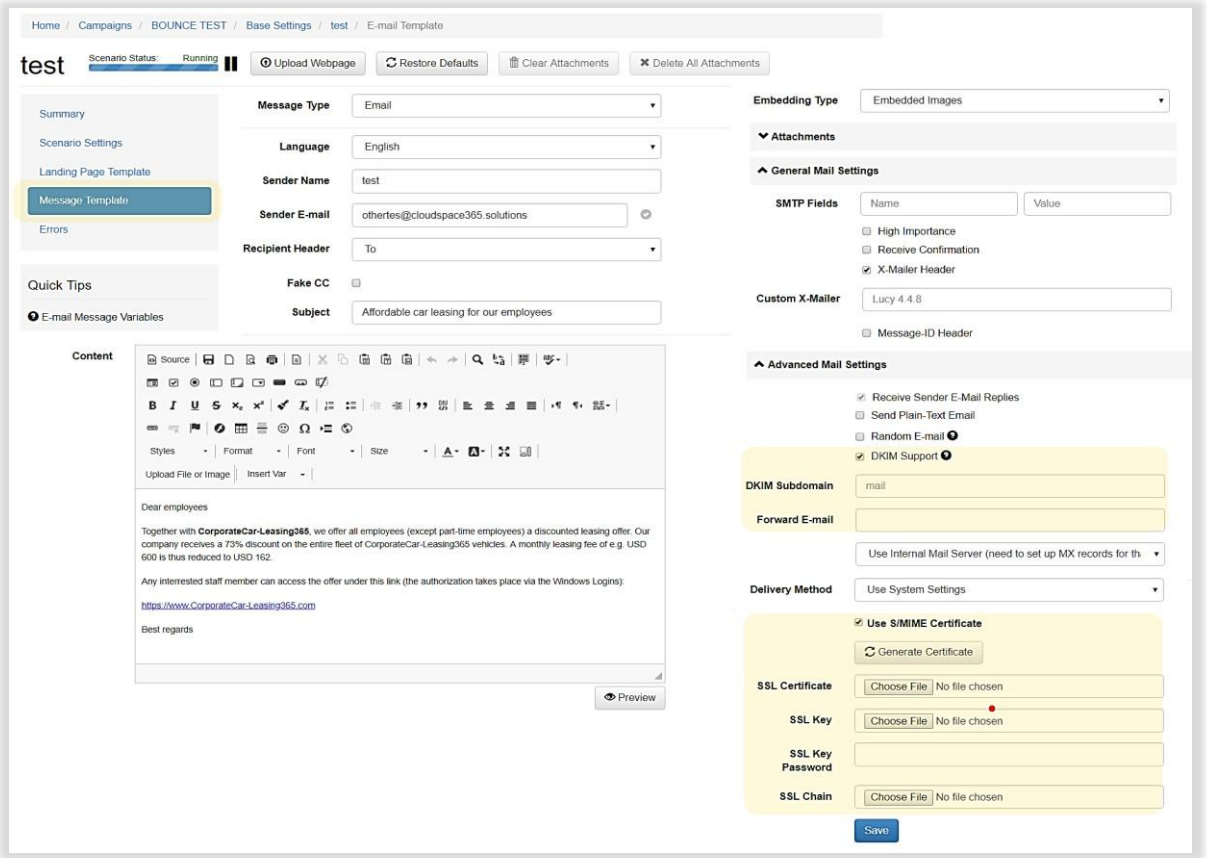
- **Attaques basées sur les niveaux :** la formation d'hameçonnage pour les employés basée sur les niveaux permet de mesurer le risque de piratage par le biais de l'ingénierie sociale. L'analyse scientifique devrait également identifier les facteurs de risque les plus importants, de sorte que le contenu de la formation individuelle puisse être proposé automatiquement.



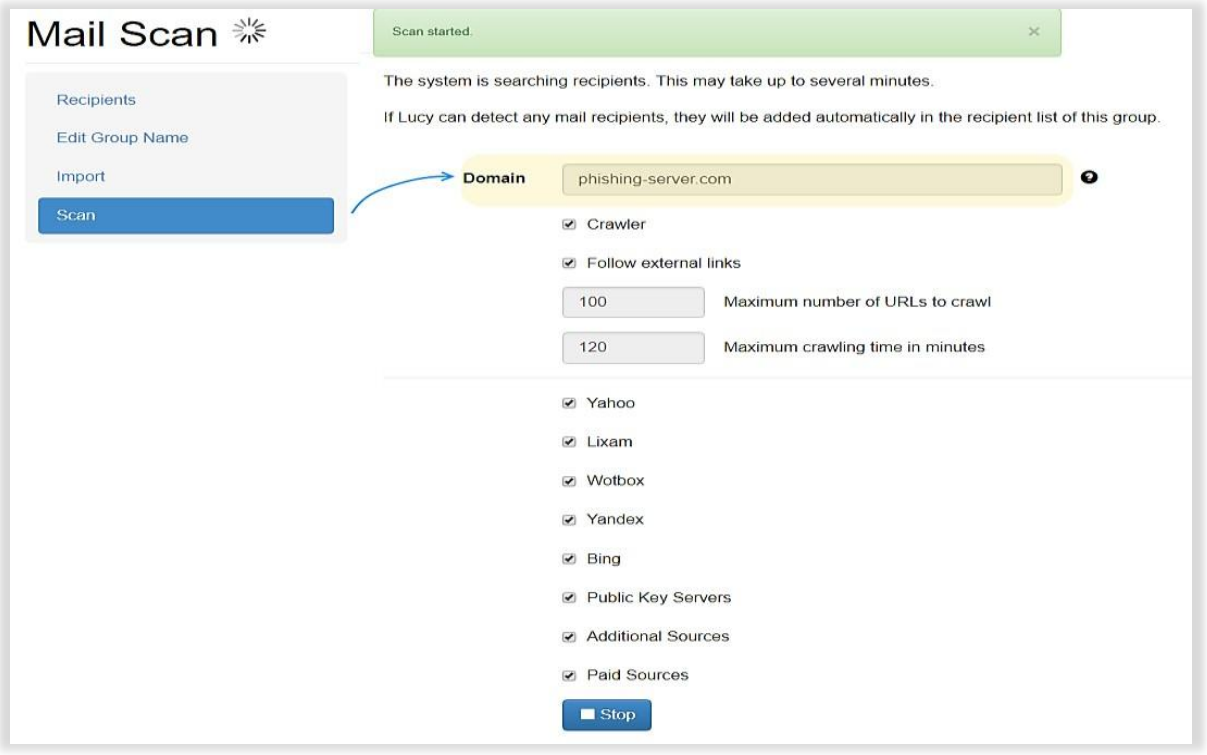
- **Simulation d'hameçonnage ciblé :** la personnalisation de l'hameçonnage ciblé s'effectue au moyen de variables dynamiques (sexe, heure, nom, e-mail, liens, messages, division, pays, etc.) que vous pouvez utiliser dans les modèles de destination et de messages.



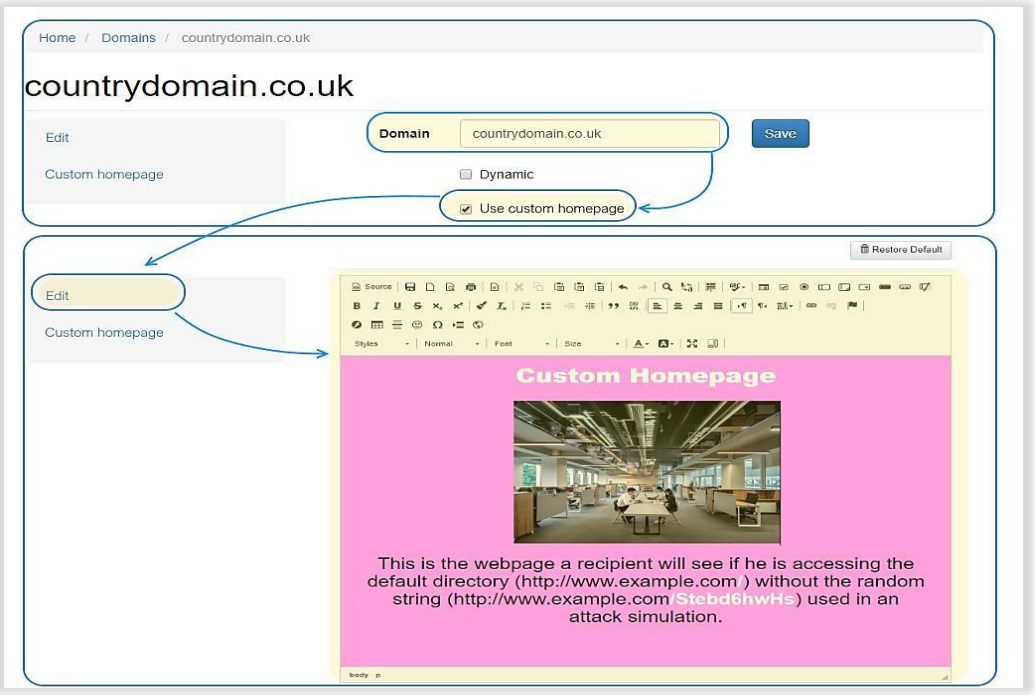
- **Prise en charge de DKIM / S / MIME pour les e-mails d'hameçonnage :** signatures numériques pour les e-mails : envoyez des e-mails de simulation d'hameçonnage signés (s / mime). Utilisez DKIM pour obtenir un meilleur score d'expéditeur.



- **Scanner de messagerie :** vous voulez savoir quelles adresses électroniques de votre entreprise peuvent être trouvées sur Internet ? Utilisez le scanner de messagerie de LUCY et découvrez ce qu'un pirate informatique sait déjà sur votre entreprise.

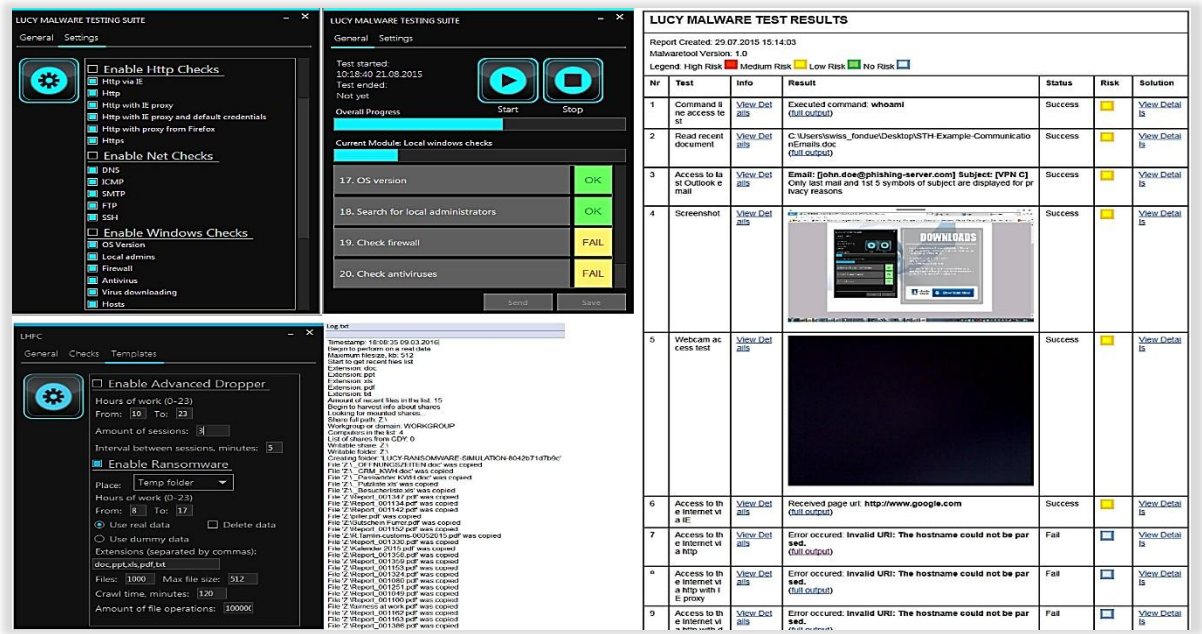


- **Création de page d'accueil personnalisée :** les destinataires ayant une meilleure connaissance technique pourraient utiliser leur navigateur pour appeler le domaine ou l'adresse IP associé au lien d'hameçonnage généré de manière aléatoire. Pour éviter que des messages d'erreur n'apparaissent ou que l'utilisateur final parvienne dans la zone de connexion de la console d'administration, vous pouvez créer des « pages d'accueil » génériques dans LUCY pour les domaines utilisés dans la simulation d'hameçonnage.

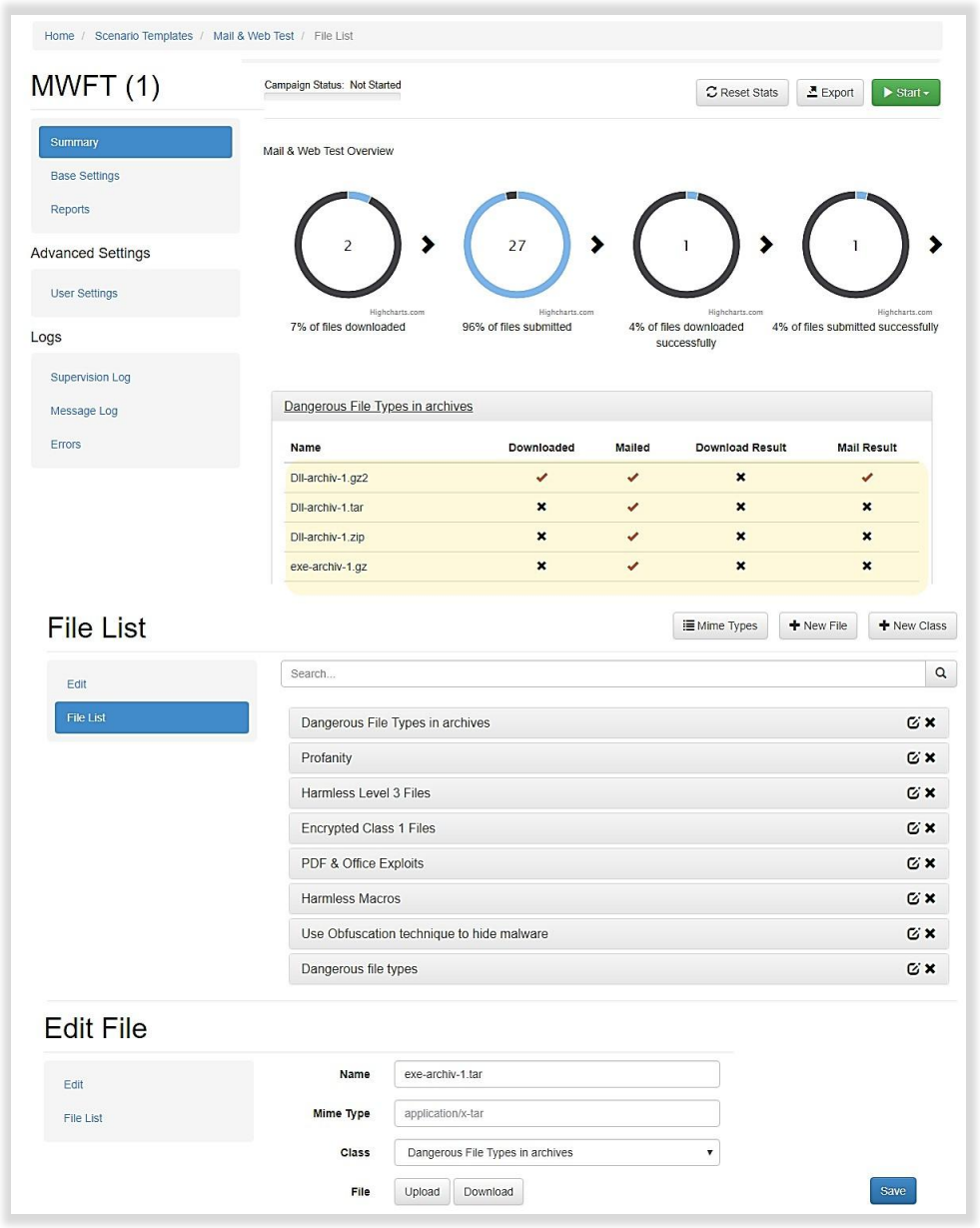


TESTEZ L'INFRASTRUCTURE

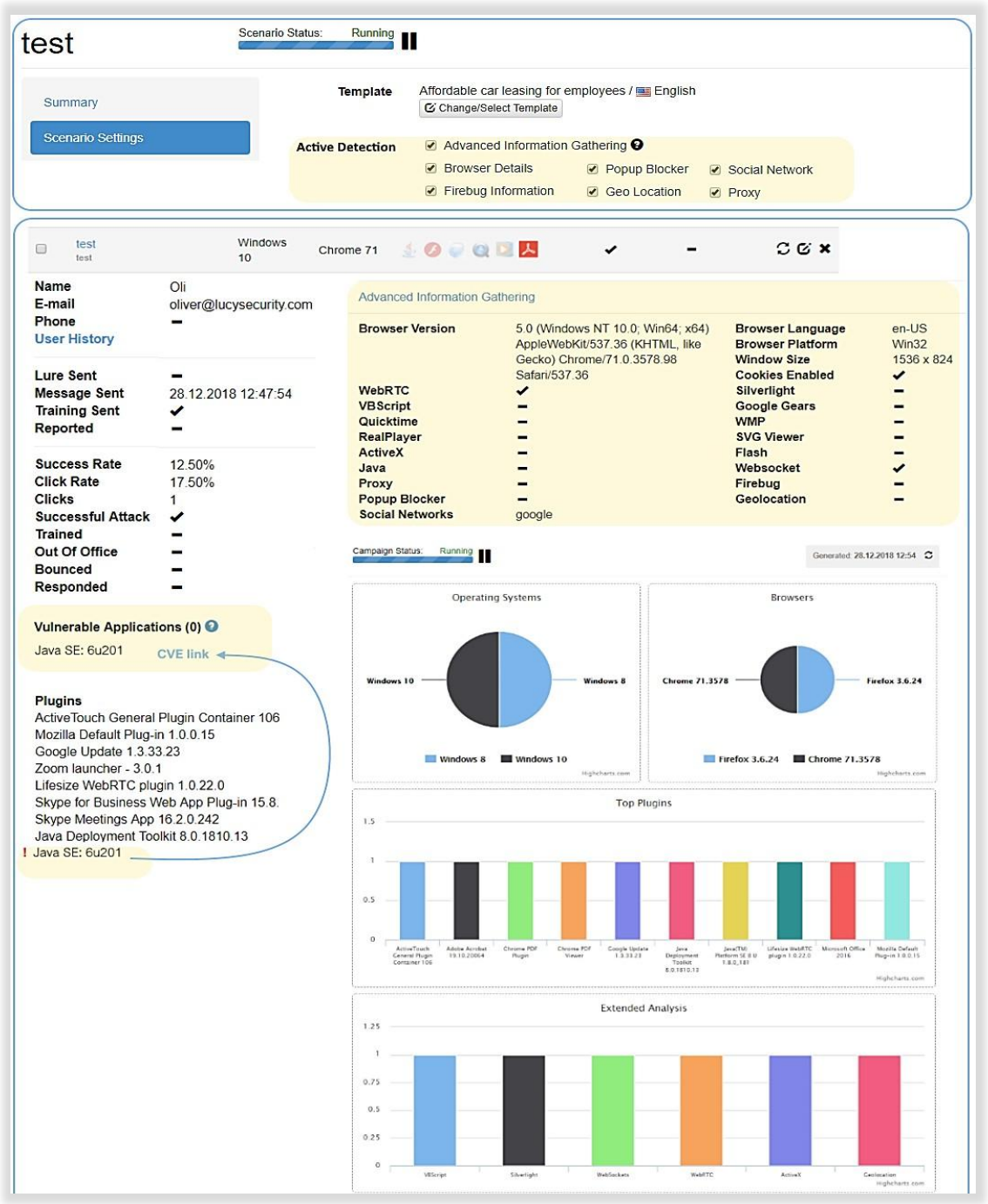
- **Boite à outils de test des programmes malveillants :** la boite à outils de simulation des programmes malveillants est une suite avancée de simulation de programmes malveillants, capable d'émuler diverses menaces. Elle permet à un auditeur d'accéder à un ensemble avancé de fonctionnalités équivalentes à de nombreux moyens utilisés par les cybercriminels. L'outil permet donc à l'administrateur de LUCY d'effectuer des contrôles de sécurité sans devoir impliquer des employés n'appartenant pas au Service Informatique.



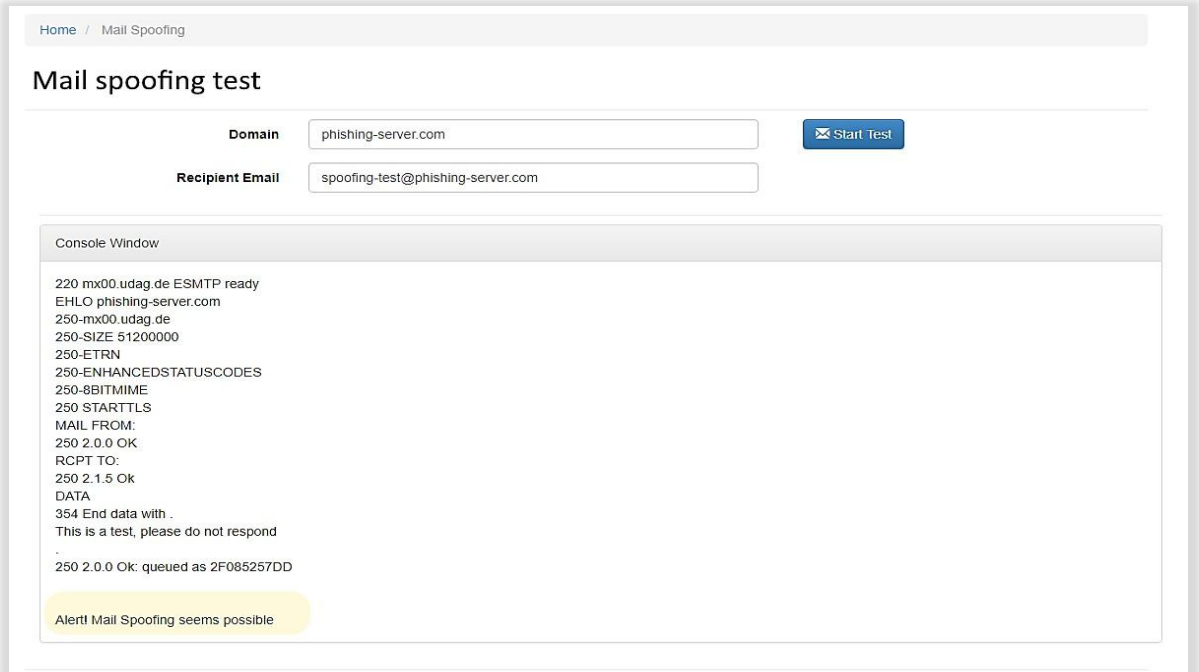
- **Test du filtrage de la messagerie et du Web :** cette fonctionnalité apporte une réponse à l'une des questions les plus importantes en matière de sécurisation du trafic Internet et du courrier électronique : quels types de fichiers peuvent être téléchargés à partir du Web et quelles pièces jointes à un e-mail sont filtrées ou non ?



- **Détection de la vulnérabilité active et passive du client :** cette fonctionnalité permet de tester en local le navigateur client et de détecter les vulnérabilités éventuelles sur la base des bibliothèques JavaScript personnalisées et des données de l'agent utilisateur du navigateur. Les plugins détectés peuvent être automatiquement comparés aux bases de données de vulnérabilité (CVE) pour identifier les dispositifs vulnérables.

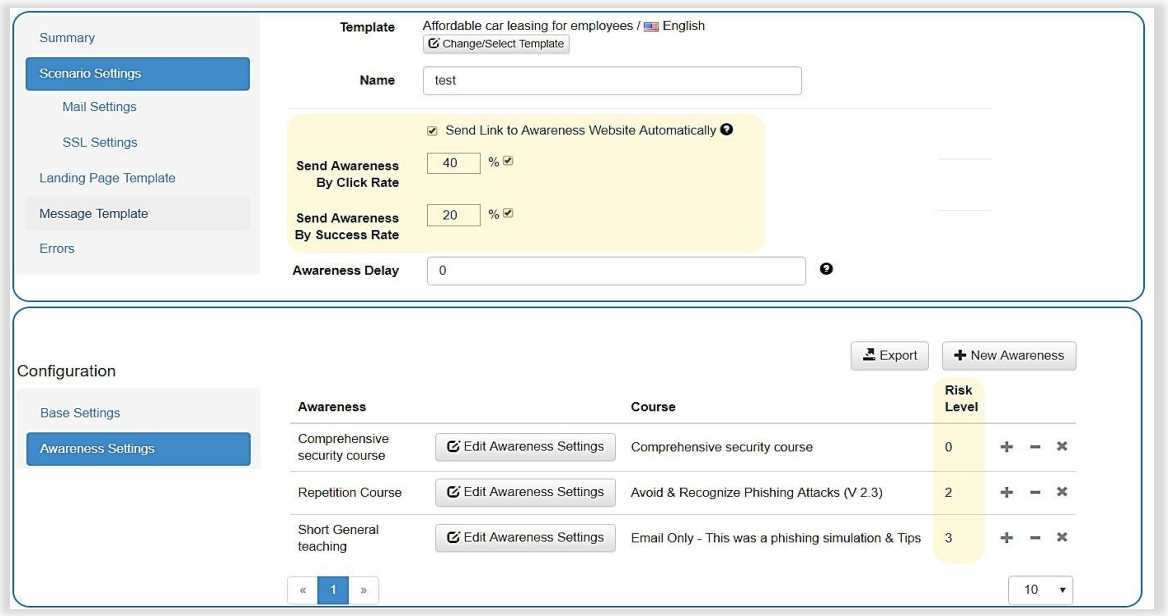


- **Test d'usurpation d'identité :** testez votre propre infrastructure pour détecter les vulnérabilités de votre messagerie à l'usurpation d'identité.

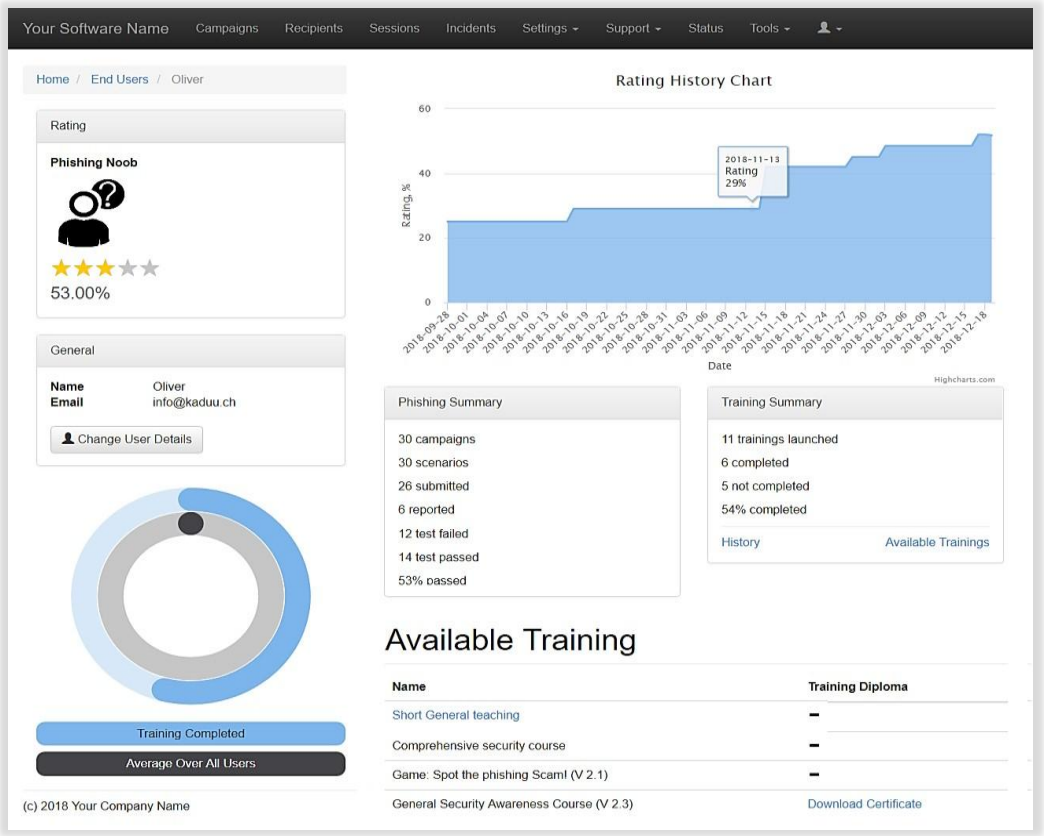


TESTS TECHNIQUES

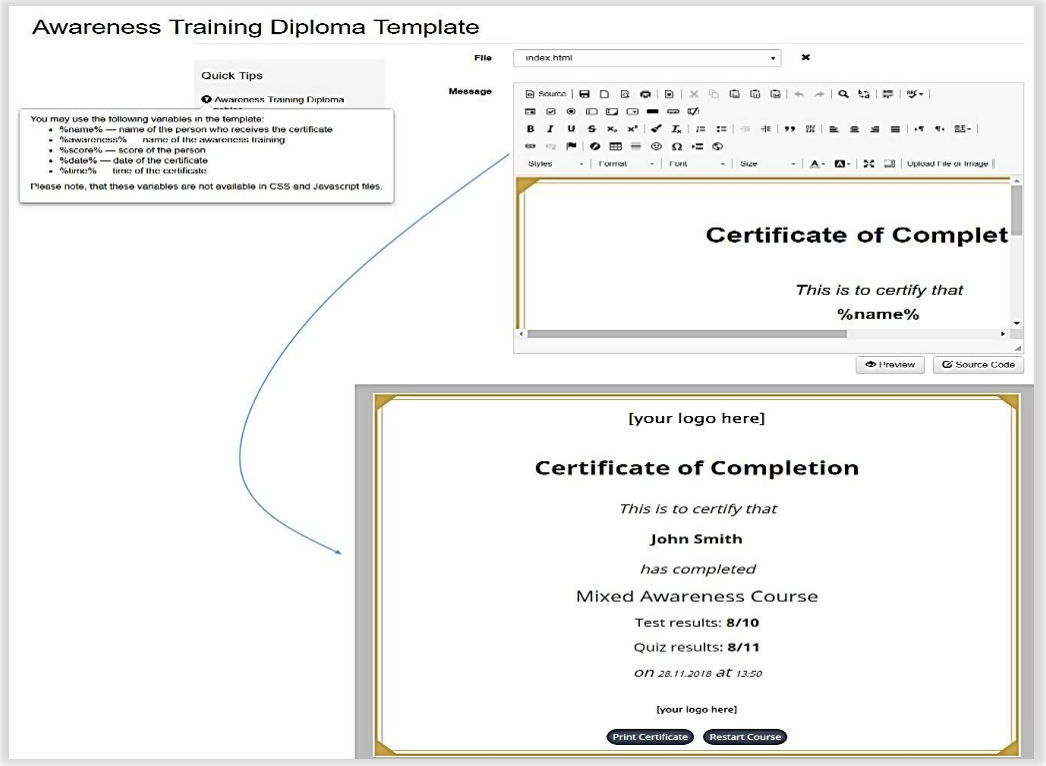
- **Apprentissage en ligne basé sur la réputation :** formez vos employés en fonction des compétences requises. Évaluez les aptitudes des employés et permettez une rivalité amicale entre collègues (ludification).
- Sur la base des profils de réputation de chaque utilisateur final, le système peut leur proposer automatiquement de multiples sessions de formation. Les profils de réputation reposent, entre autres facteurs, sur le comportement de l'utilisateur dans les simulations d'hameçonnage. Cela garantit que les « récidivistes » reçoivent un contenu de formation différent de ceux qui cliquent sur une simulation d'attaque pour la première fois.



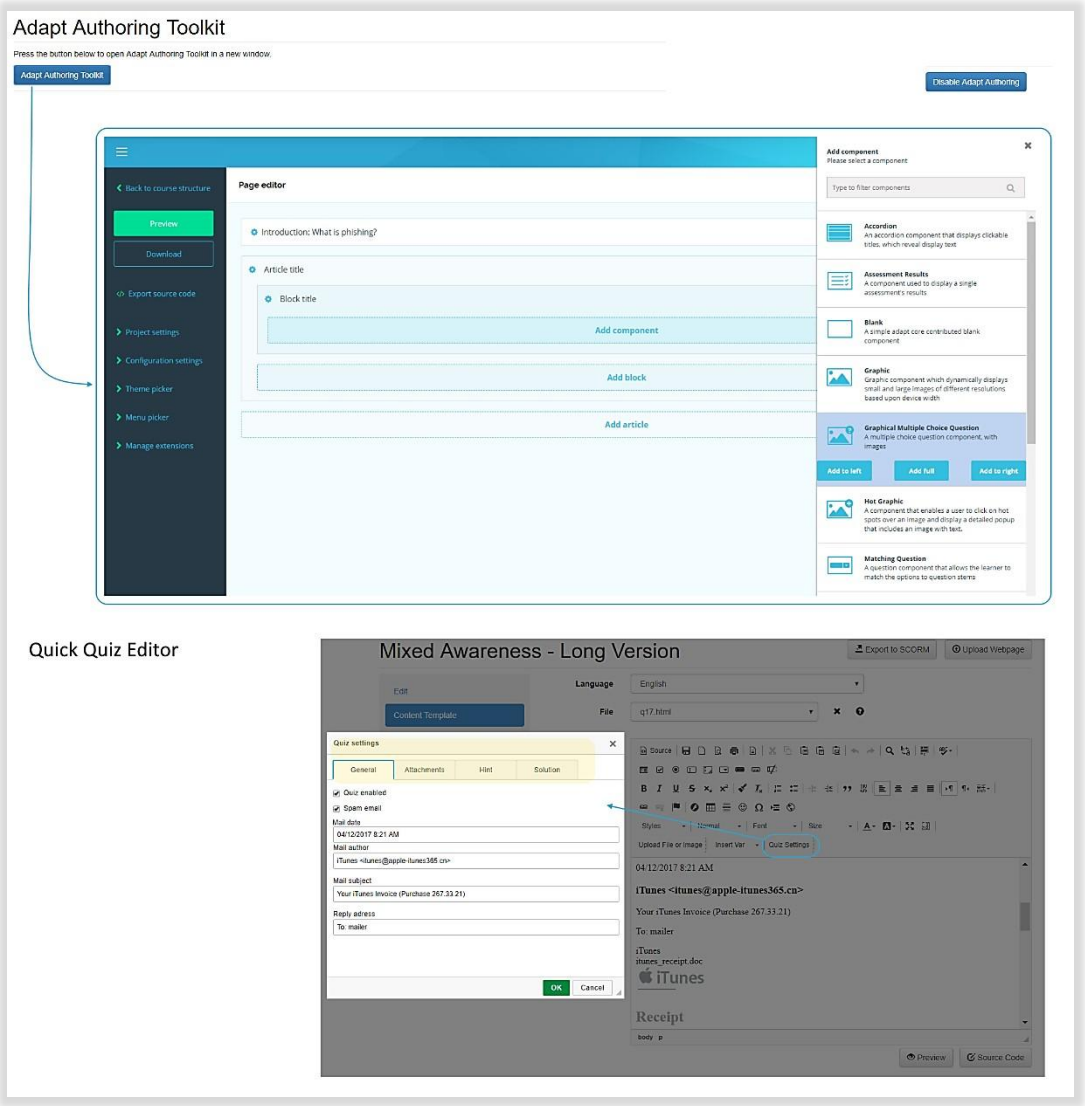
- **Portail de formation des utilisateurs finaux :** fonctionnalité du système de gestion de l'apprentissage (SGA) : les employés ont un accès permanent à une page d'accueil de formation personnelle qui présente vos propres cours adaptés à chacun d'entre eux. Sur cette page d'accueil, ils peuvent consulter leurs statistiques de performances, reprendre ou répéter la formation, créer des attestations de fin de formation et comparer leurs résultats avec ceux d'autres départements ou groupes.



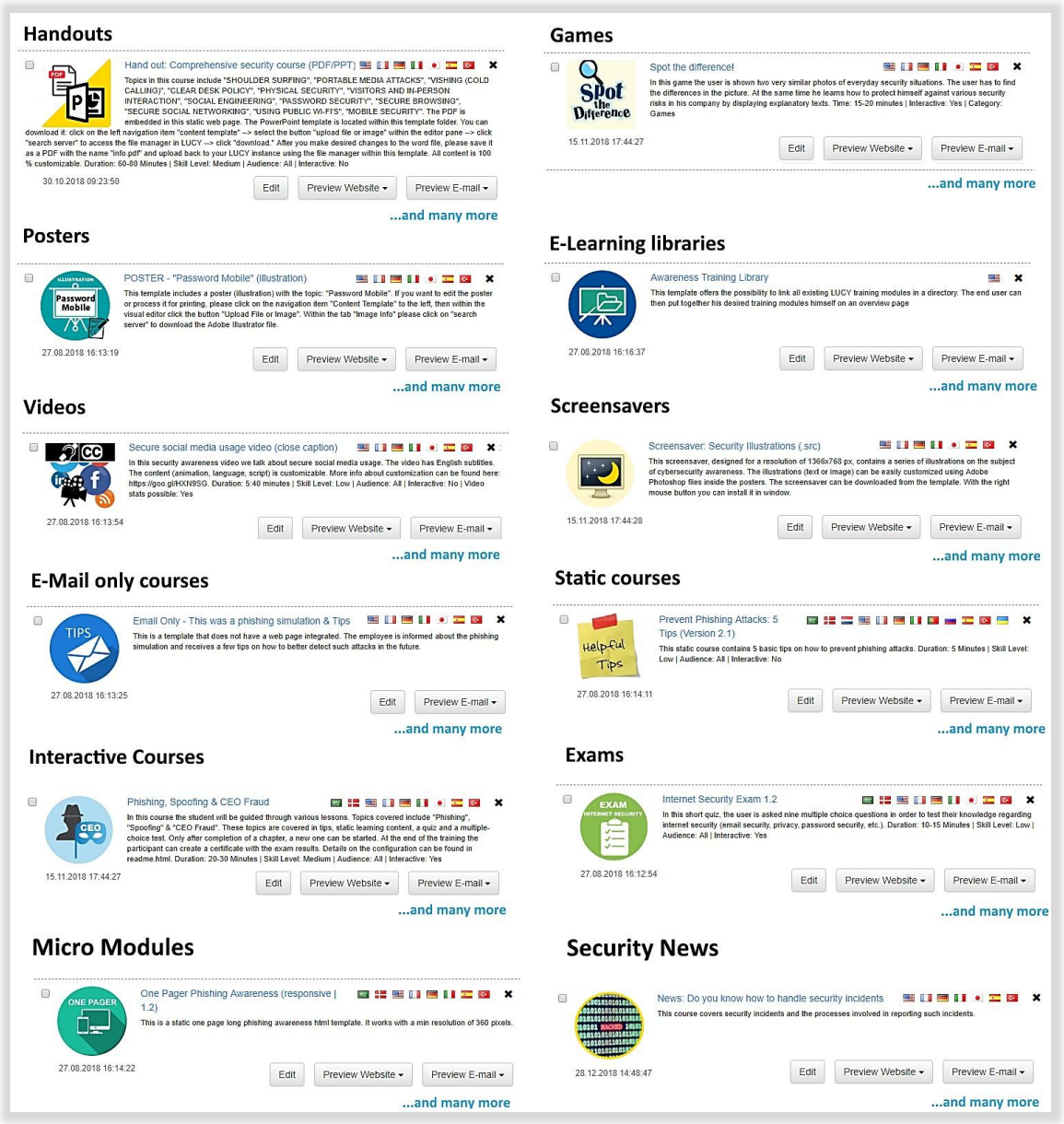
- **Diplôme de sensibilisation :** les certificats d'apprentissage en ligne peuvent être créés et imprimés par le destinataire à la fin de la formation ou depuis le portail SGA.



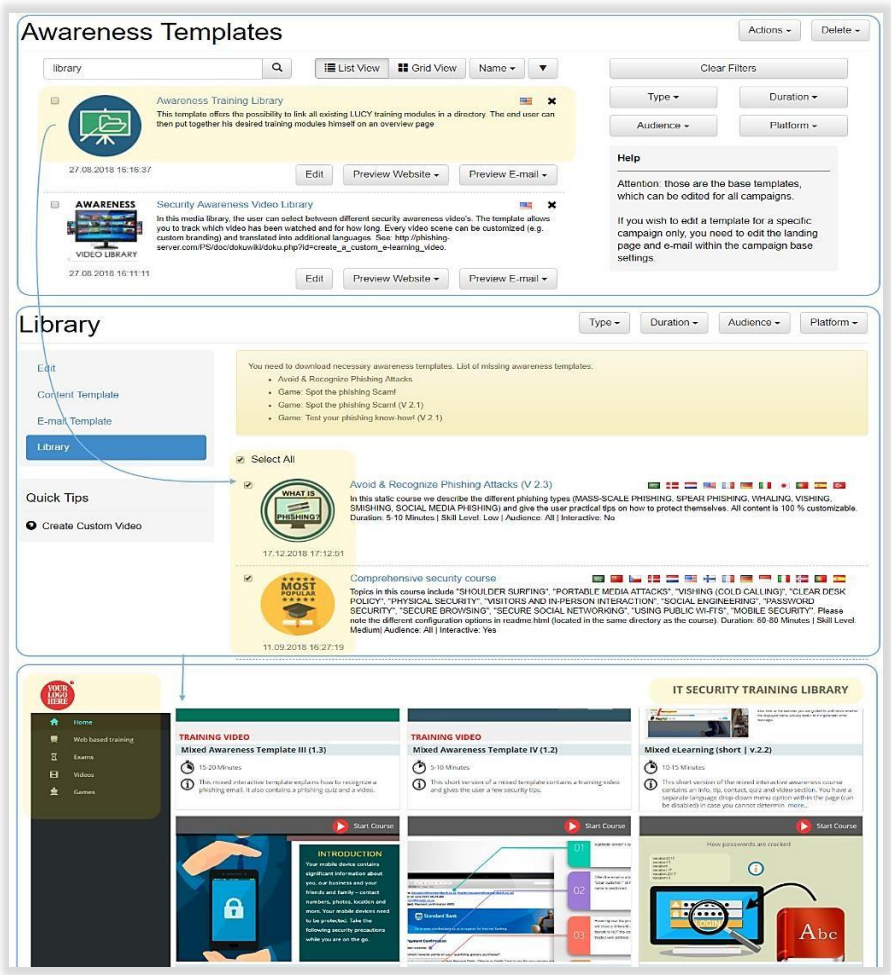
- **Boîte à outils de création de contenu d'apprentissage en ligne :** la boîte à outils de création de contenu d'apprentissage en ligne (Adapt) permet la création de contenu d'apprentissage individualisé. Glissez-déposez des vidéos ou tout autre format interactif rich media, insérez des examens à partir de menus prédéfinis, créez du contenu d'apprentissage en ligne interactif à partir de zéro en très peu de temps.



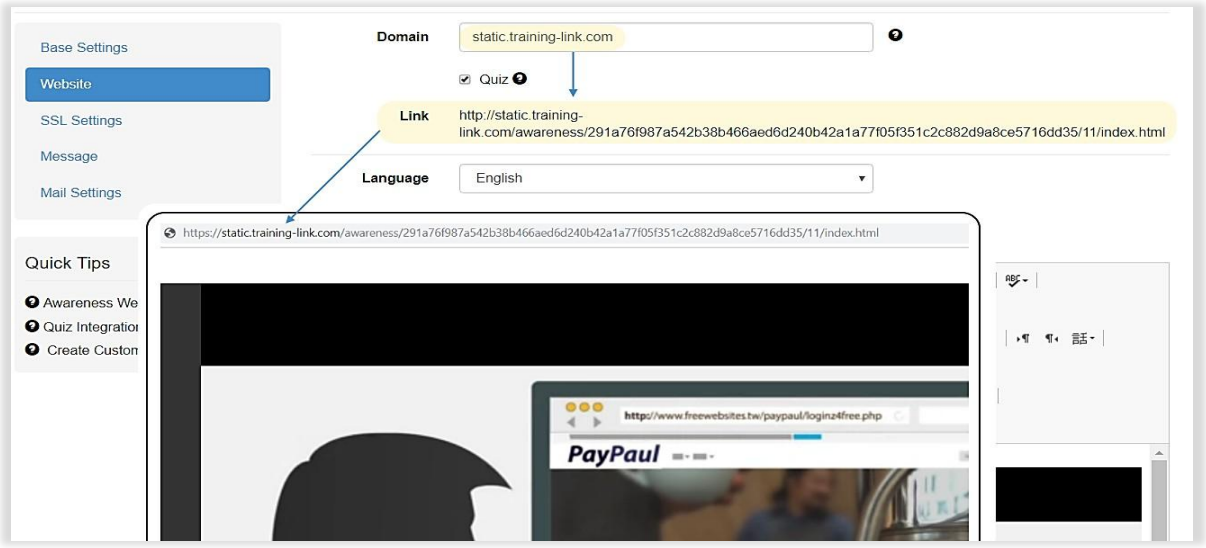
- **Formation de sensibilisation au format interactif rich media:** intégrez des éléments au format interactif rich media (vidéo, audio ou autres éléments qui encouragent les employés à interagir avec le contenu et à s'impliquer) dans vos formations de sensibilisation. Utilisez les vidéos pédagogiques existantes, adaptez-les ou ajoutez vos propres éléments au format interactif rich media.



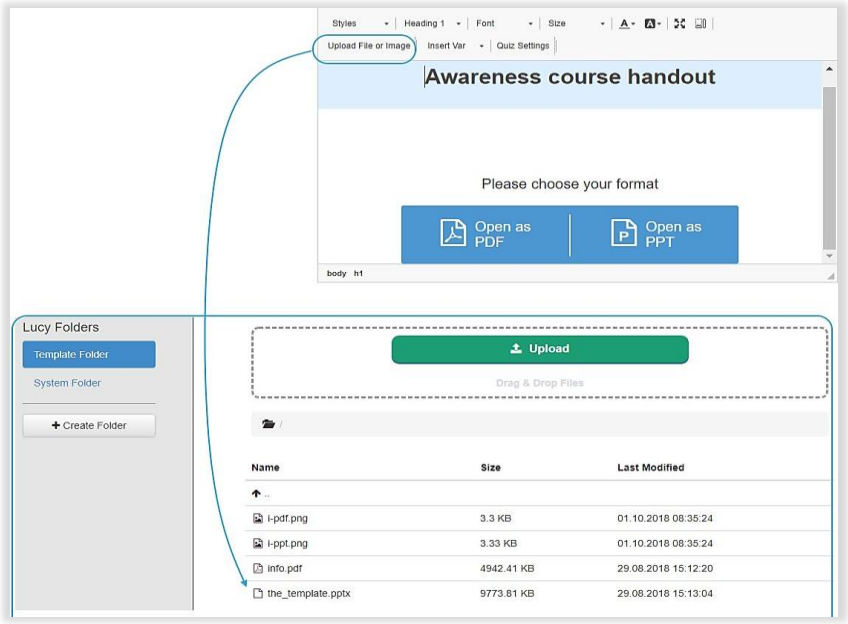
- **Bibliothèque de formation :** les employés peuvent accéder au contenu de formation de votre entreprise à partir d'une page récapitulative intitulée « bibliothèque de formation ». Elle contient une vaste sélection de modèles standards d'apprentissage en ligne de LUCY qui servent de référence. La page récapitulative peut être triée sur certains thèmes (vidéo, quiz, test, etc.).



- **Supports de formation statiques :** le contenu de la formation peut également être publié sur des pages statiques de LUCY ou sur l'intranet, donnant à l'utilisateur un accès permanent au contenu de la formation, indépendamment des éventuelles simulations d'attaque.

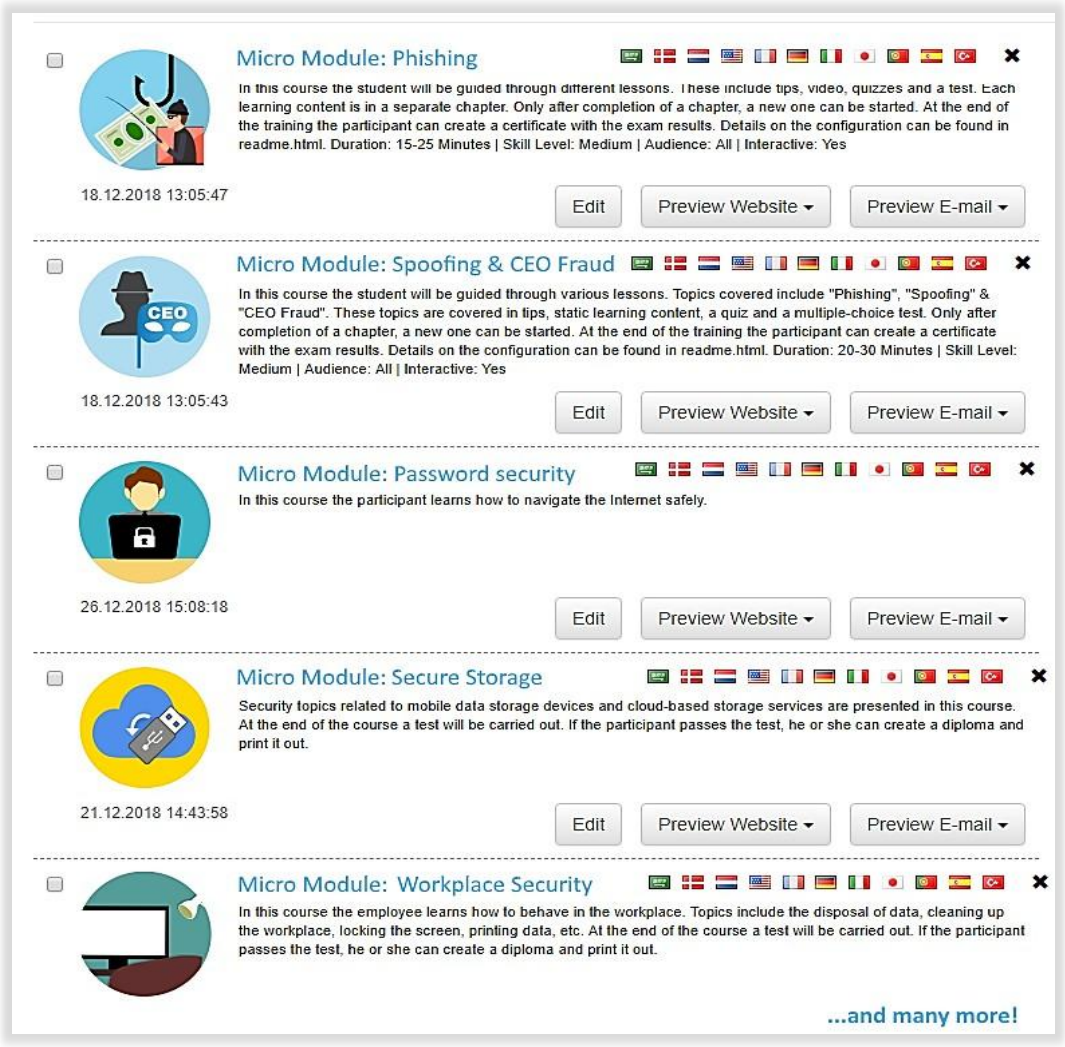


- **Supports de formation hors ligne :** LUCY est fourni avec une série de modèles modifiables (fichiers Adobe Photoshop ou Illustrator) destinés à la formation de sensibilisation, tels que des affiches, des écrans de veille, des dépliants, etc.

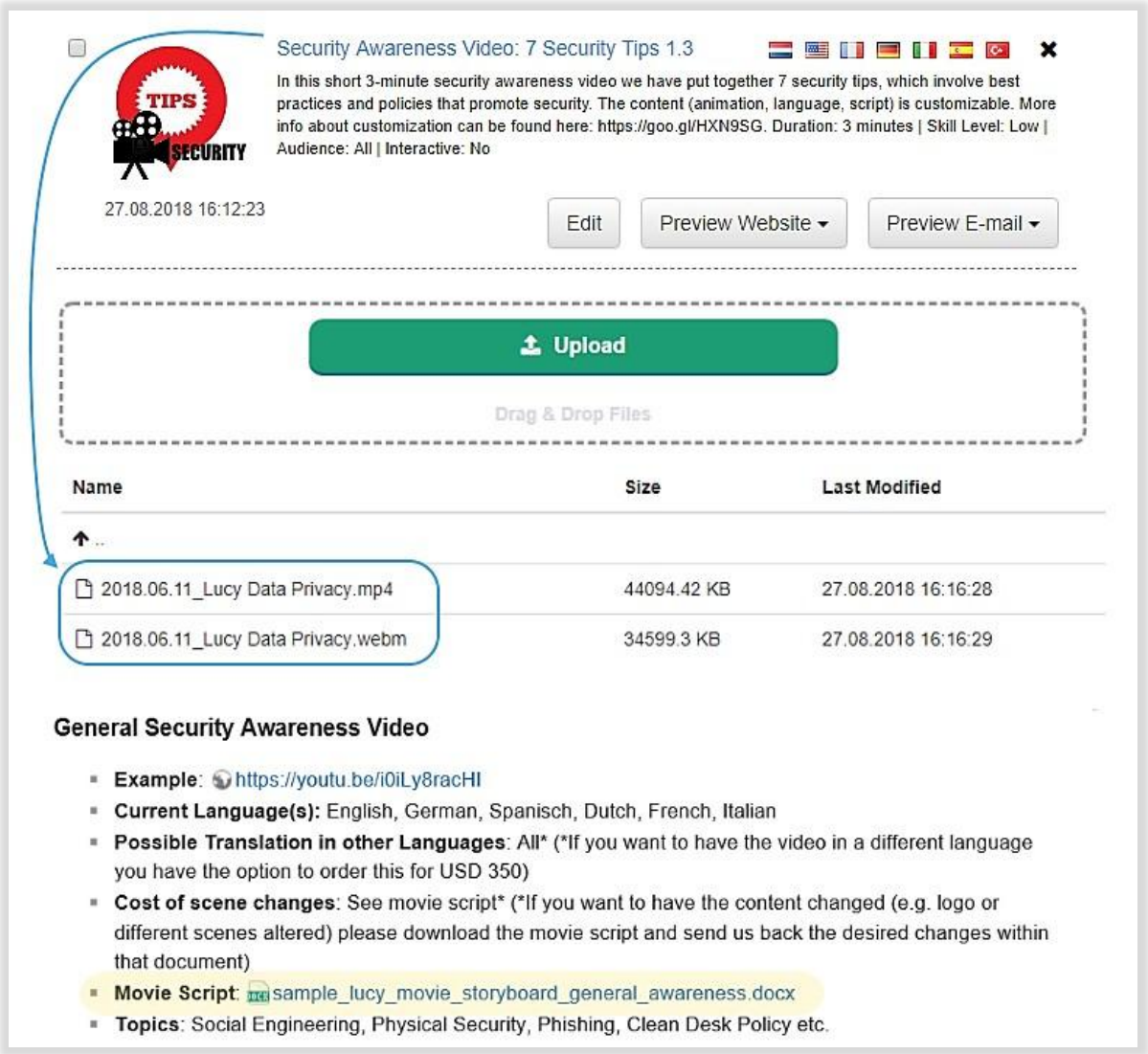


.

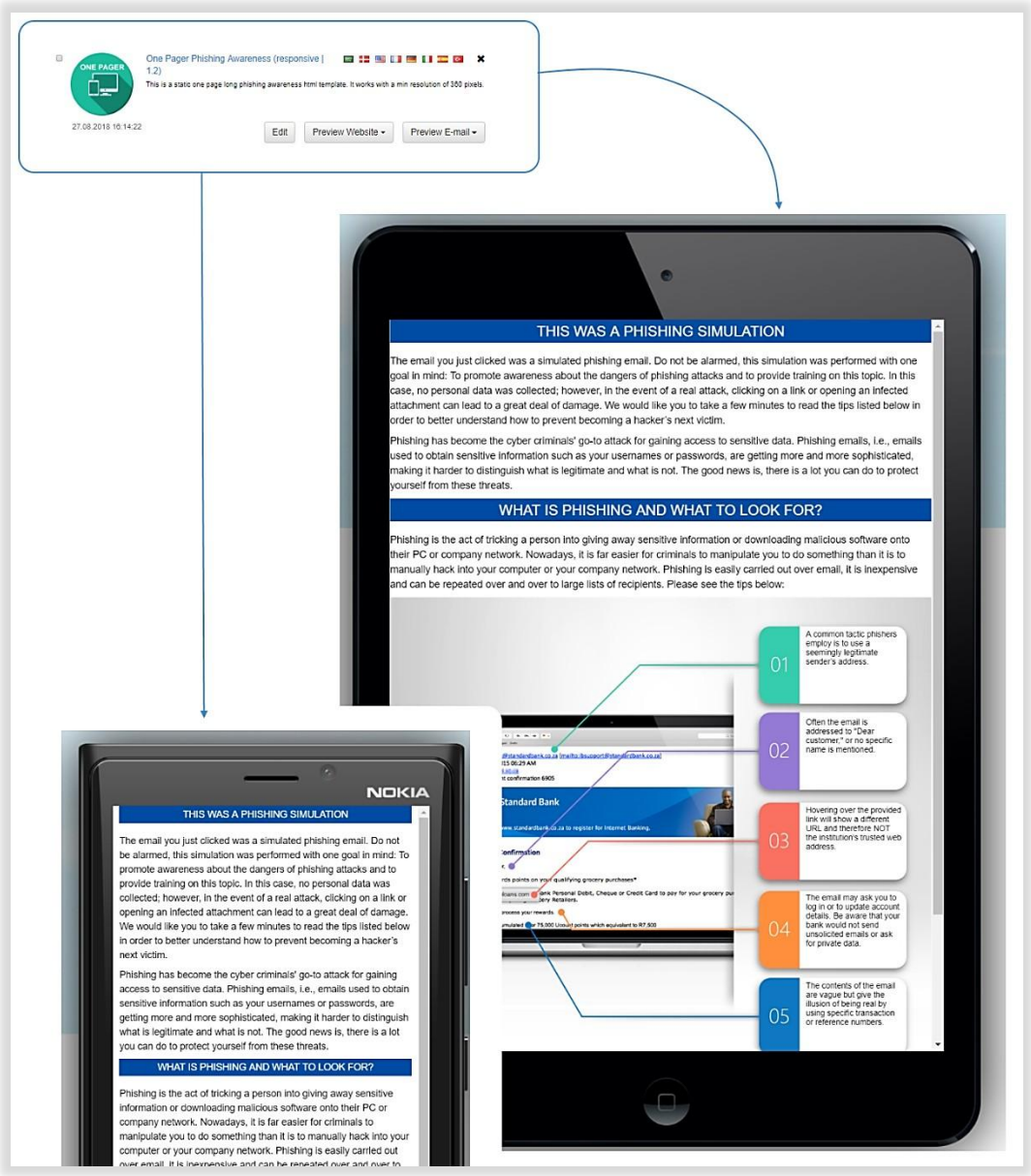
- **Modules de micro-apprentissage :** nous avons conçu des modules de formation pour le micro-apprentissage (vidéos d'une minute ou documents de sensibilisation sur une page, par exemple) pouvant être adaptés à la stratégie de marque et à la politique de votre entreprise.



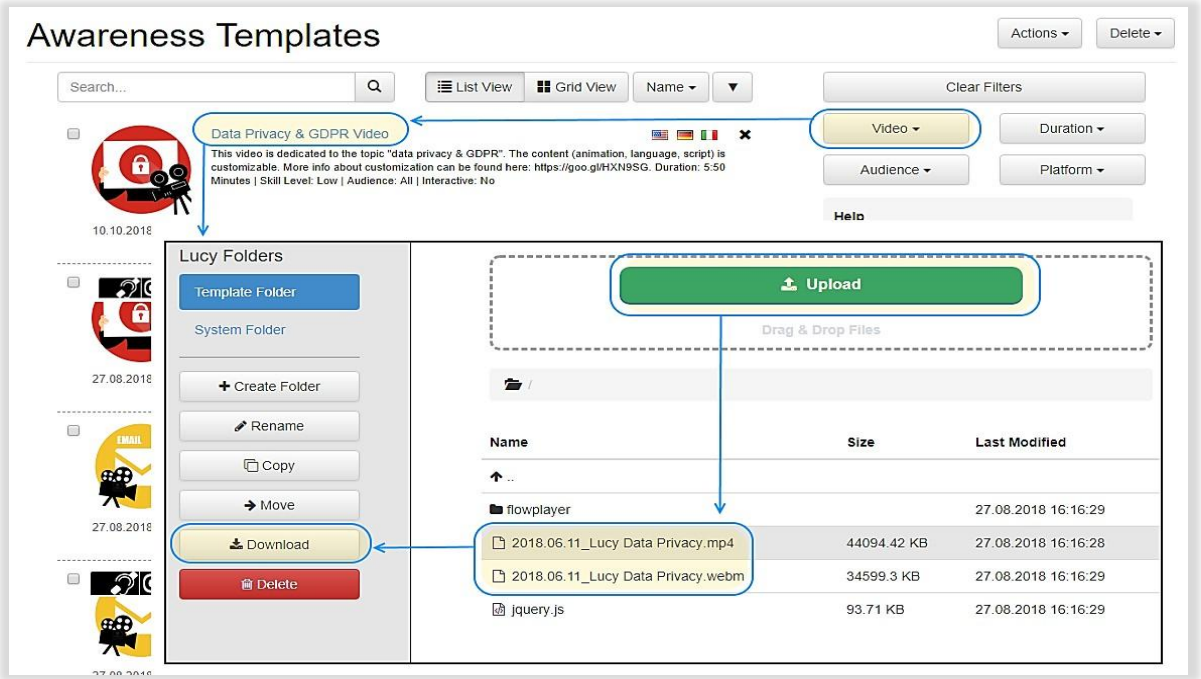
- **Personnalisation de vidéo :** envoyez-nous le logo de votre entreprise et nous l'inclurons dans les vidéos de formation. Vous souhaitez une autre langue ? Aucun problème. Nous paramétrerons la vidéo dans la langue de votre choix. Vous voulez une scène différente ? Il suffit de télécharger les scripts de la vidéo et de noter les modifications souhaitées.



- **Format optimisé pour appareils mobiles :** de nombreux modules intégrés de LUCY sont disponibles dans un format adapté aux appareils mobiles, ce qui donne à vos utilisateurs la possibilité de suivre une formation sur tout type d'appareil connecté.



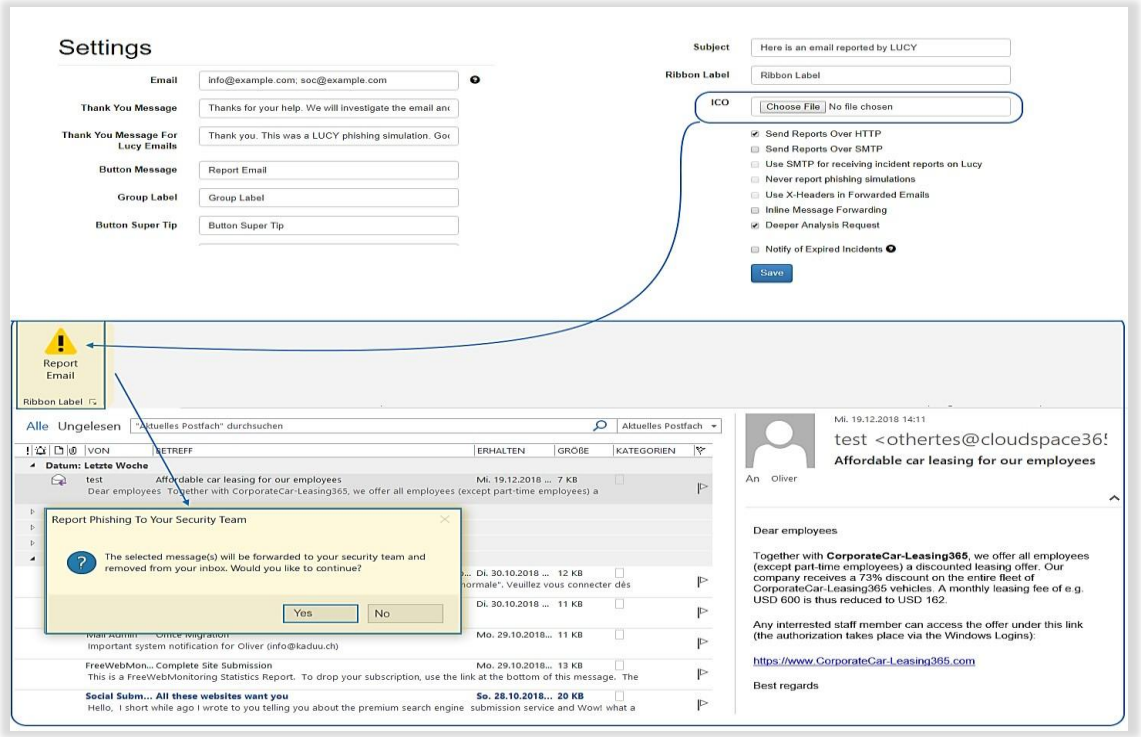
- **Importation/exportation de vidéo :** vous pouvez exporter des vidéos LUCY vers votre propre système et aussi importer vos propres vidéos dans LUCY.



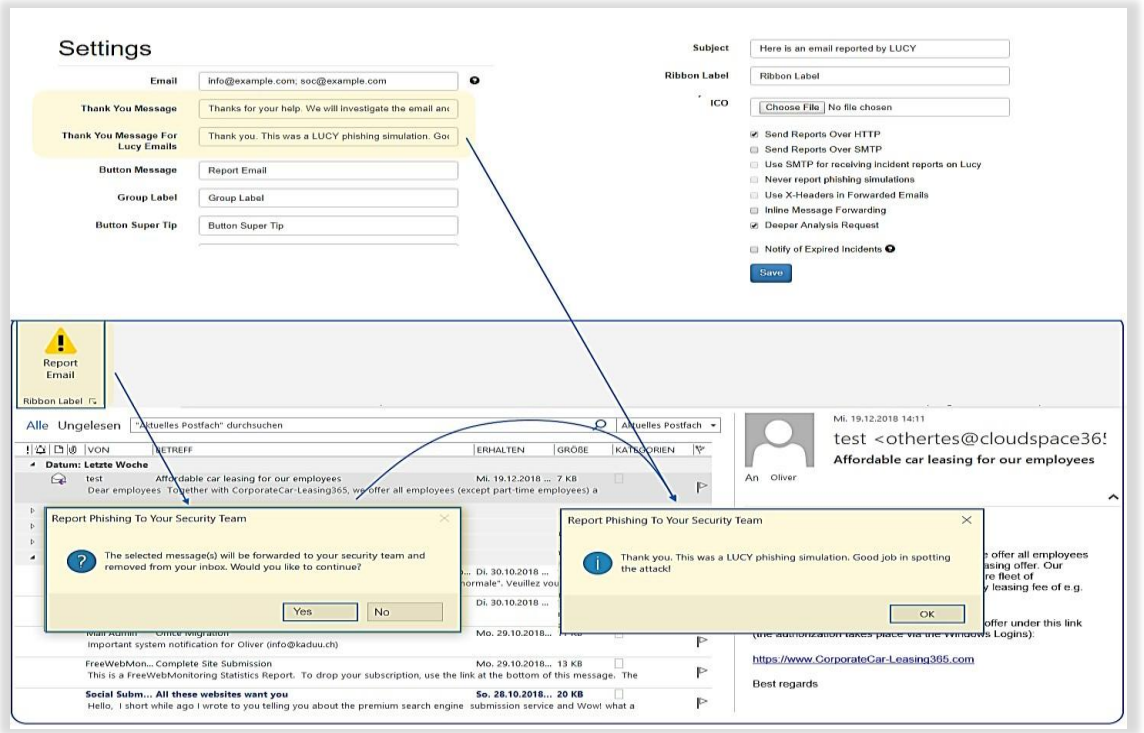
- **Indices de formation dynamiques :** les indices dynamiques implémentés permettent à votre administrateur de définir, dans les modèles d'attaque, des marqueurs pouvant indiquer à vos employés, dans le matériel d'apprentissage en ligne, où l'attaque d´hameçonnage peut avoir été détectée.

IMPLIQUEZ LES EMPLOYÉS

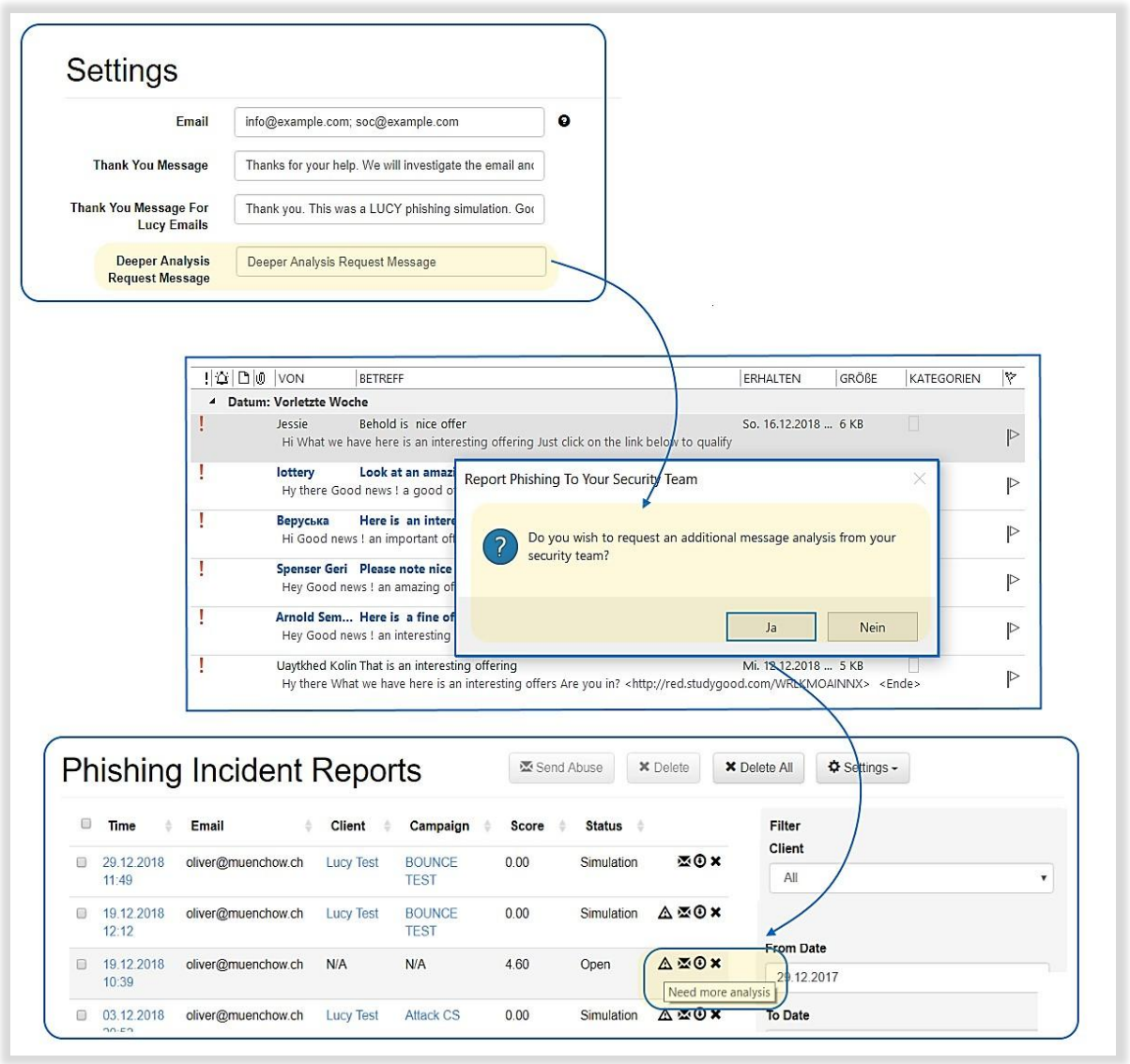
- **Signaler des e-mails en un seul clic :** les utilisateurs finaux peuvent signaler en un seul clic des e-mails suspects à un ou plusieurs comptes de messagerie afin qu'ils soient transmis à votre console d'analyse des incidents de LUCY.



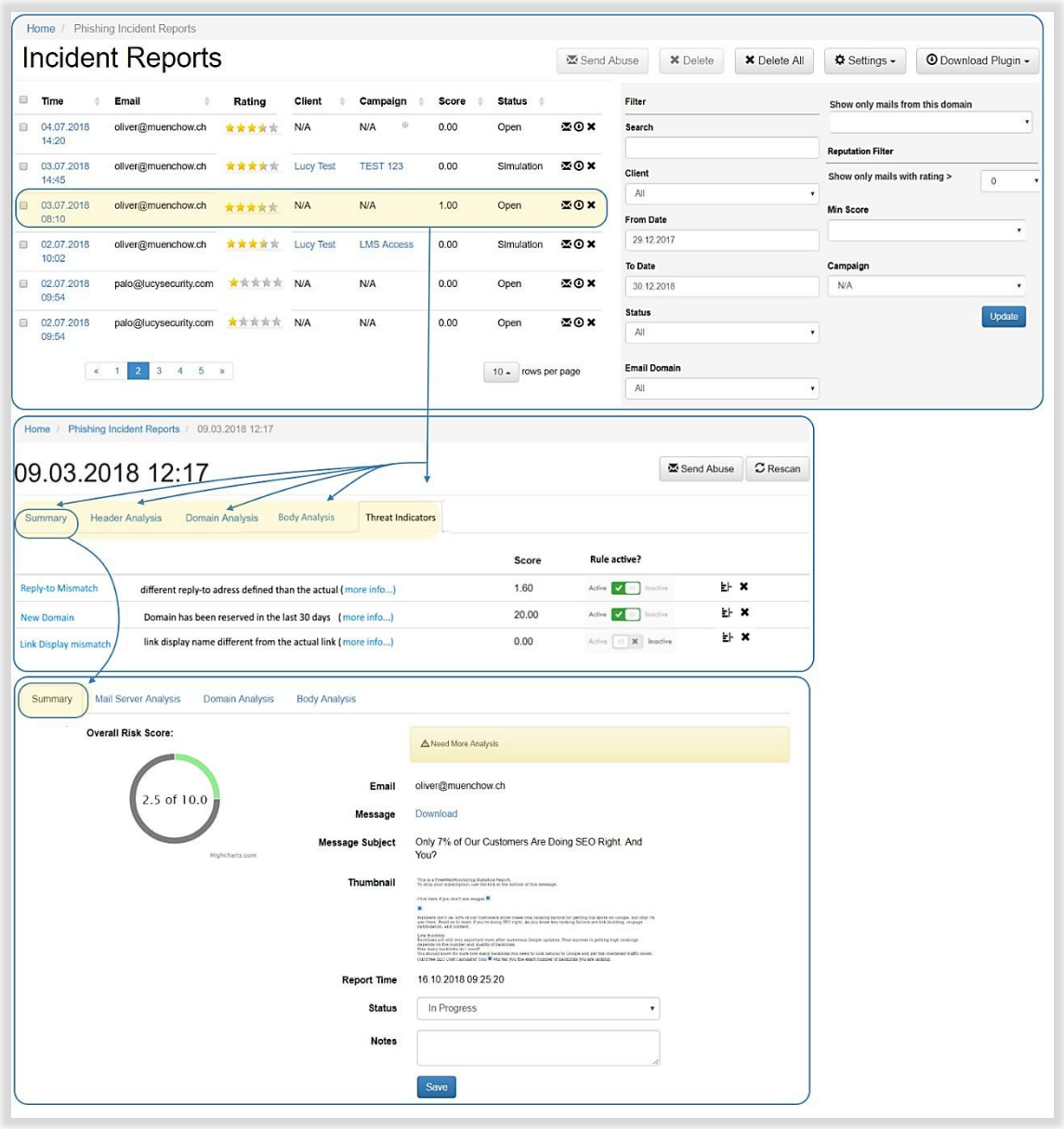
- **Appui aux bons comportements :** notre plugin apporte automatiquement un appui aux bons comportements en remerciant les utilisateurs finaux via l'envoi d'un message personnalisé défini par votre entreprise.



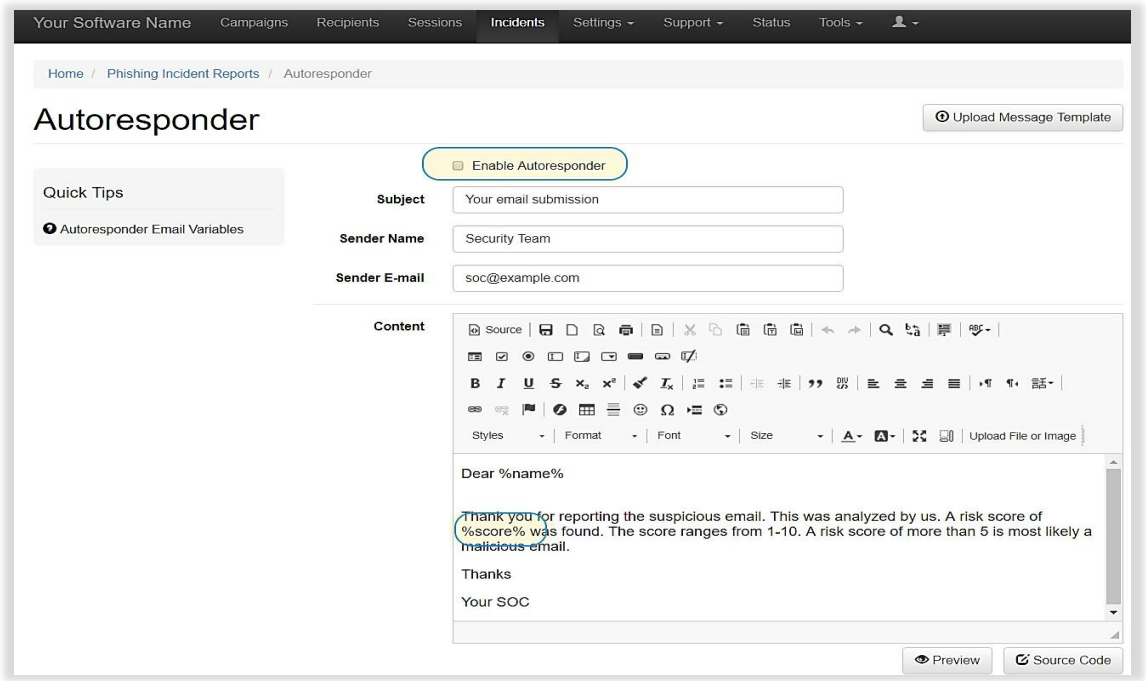
- **Demande d’analyse approfondie :** parfois, les utilisateurs veulent savoir si l’e-mail reçu peut être ouvert en toute sécurité. En option, l'utilisateur peut utiliser la « demande d’analyse approfondie » intégrée dans le plugin local pour demander à l'équipe de sécurité un retour d’information sur l’e-mail signalé.



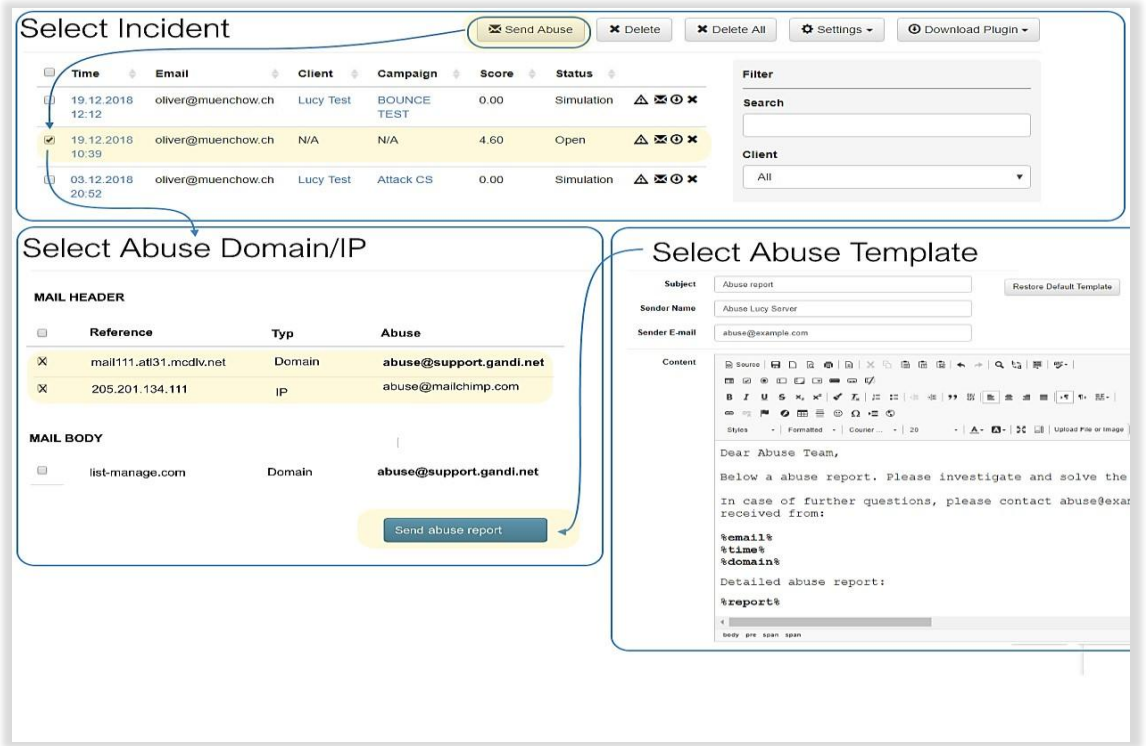
- **Analyse automatique d'incident :** gérez et répondre aux e-mails suspects signalés à l'aide d'une console de gestion centralisée : l'analyseur de LUCY permet une analyse automatisée des messages signalés (en-tête et corps). L'analyseur inclut un score de risque individuel, fournissant un classement en temps réel des e-mails signalés. L'Analyseur de Menaces permet de réduire notablement la charge de travail de l'équipe de sécurité.



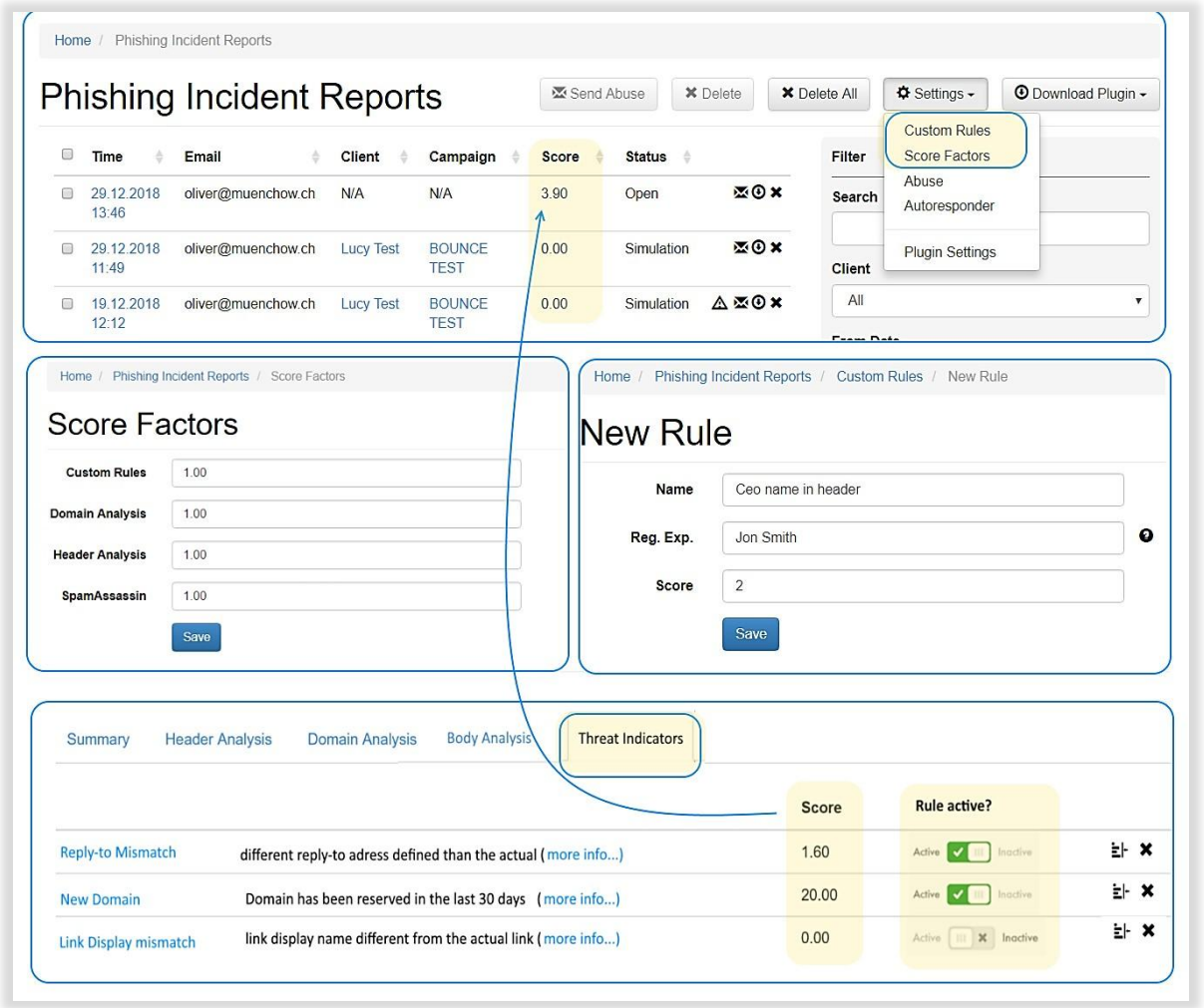
- **Feed-back automatique sur les incidents :** l'Autorépondeur d'incident permet d'envoyer automatiquement un message à l'utilisateur final pour lui communiquer les résultats de l'analyse des menaces de son e-mail. Le texte du message est librement configurable et le score de risque de l'e-mail calculé par LUCY peut être inclus, si cela est souhaité.



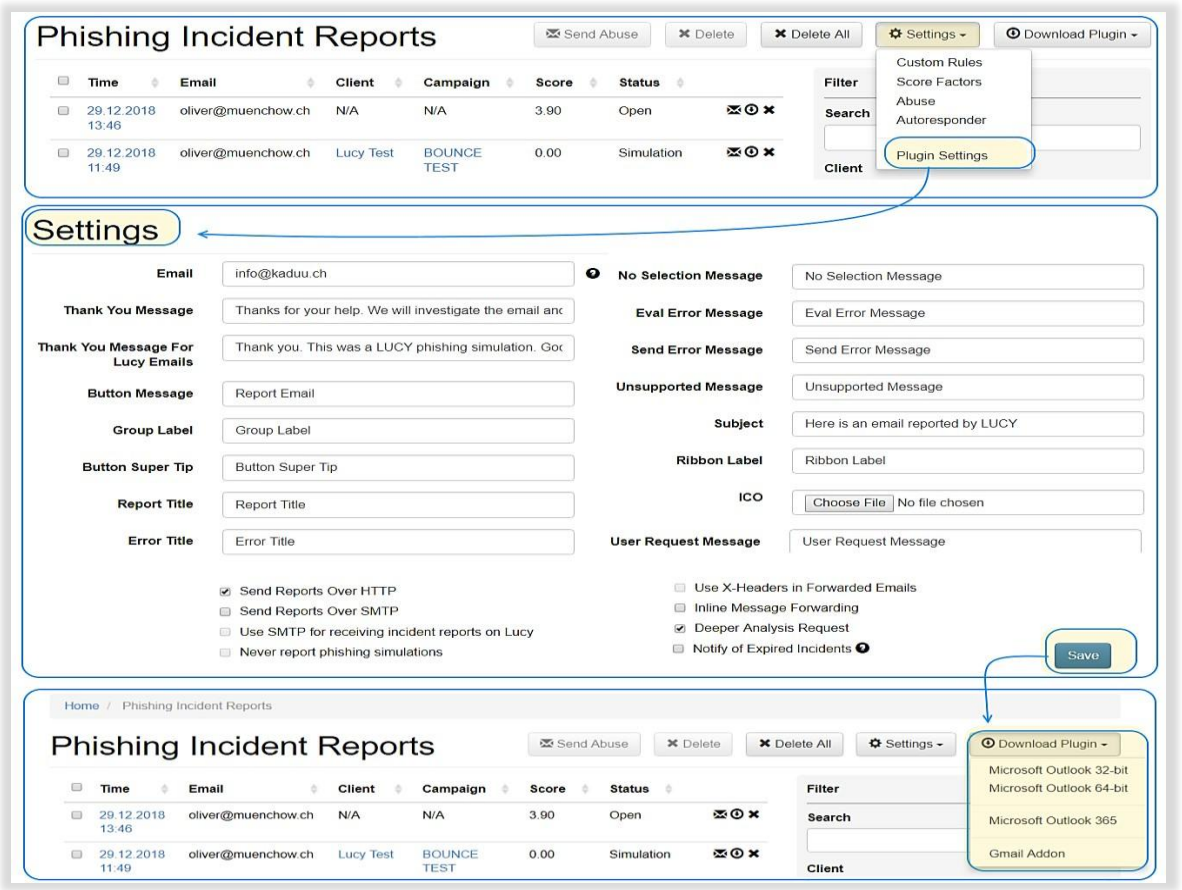
- **Atténuation de la menace :** l'Atténuateur de Menace Comportemental est une approche révolutionnaire pour éliminer les risques liés au courrier électronique. Il aidera l'administrateur sécurité à mettre fin à l'attaque (par exemple, en envoyant un rapport automatisé à l'équipe anti-abus des fournisseurs impliqués dans l'attaque).



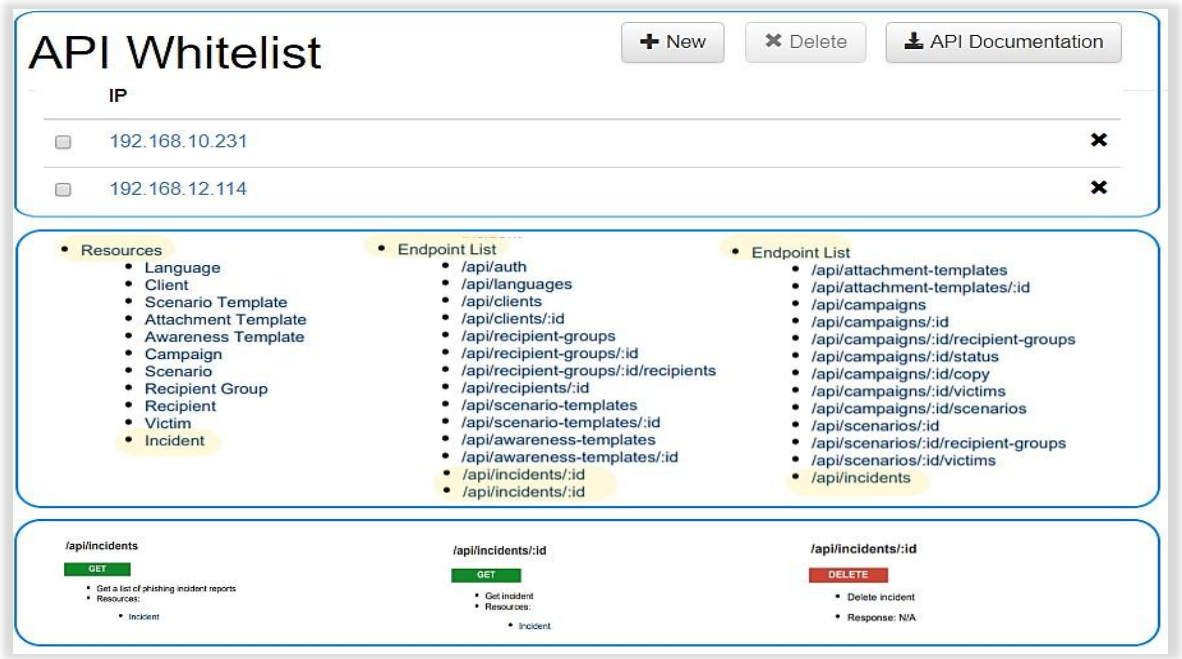
- **Analyse basée sur des règles personnalisées :** définissez vos propres règles pour l'analyse du courrier électronique et le calcul du risque.



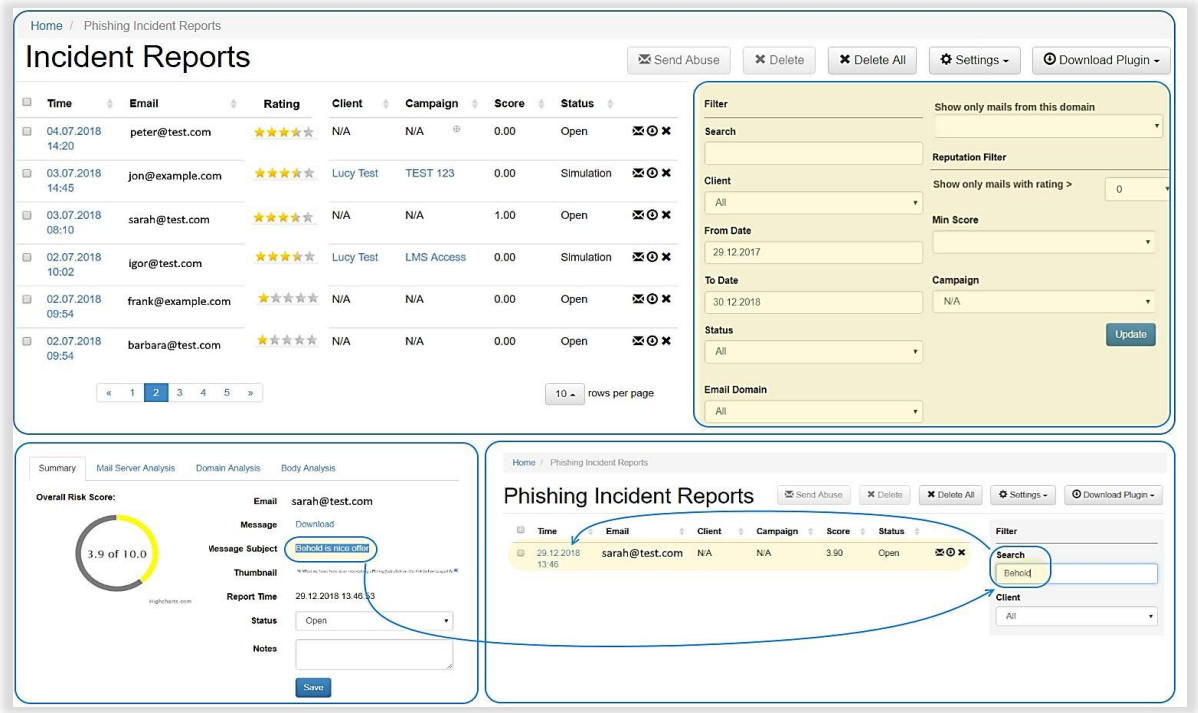
- **Options de personnalisation des plugins :** LUCY permet une personnalisation aisée et un mode marque blanche complet pour diverses fonctions des plugins (icône affichée, message de feed-back, étiquette de ruban, protocole de transmission, en-tête des envois, etc.).



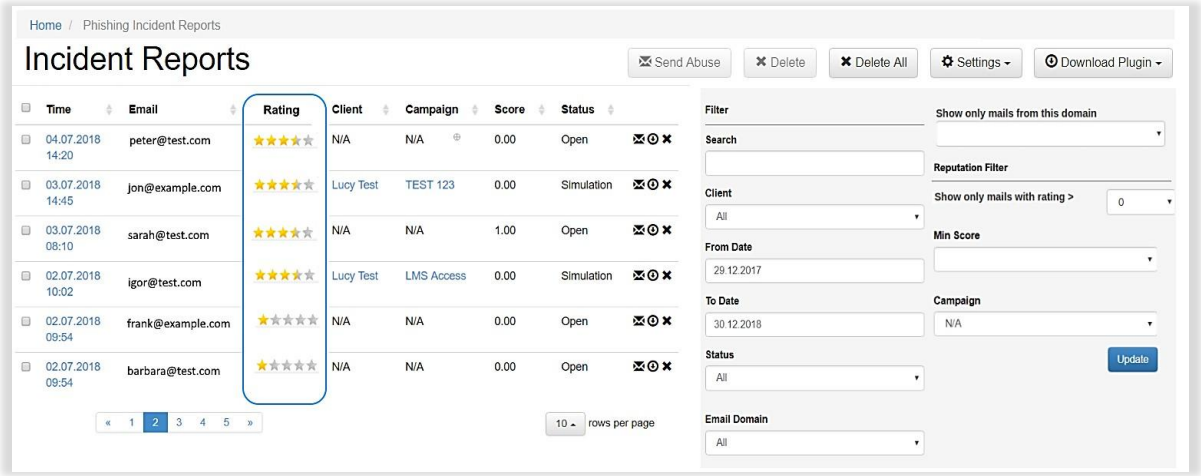
- **Intégration de tiers :** grâce à l'automatisation de l'API REST incident de LUCY, nous pouvons traiter les e-mails signalés et aider votre équipe de sécurité à mettre fin aux attaques d'hameçonnage actives pendant leur déroulement.



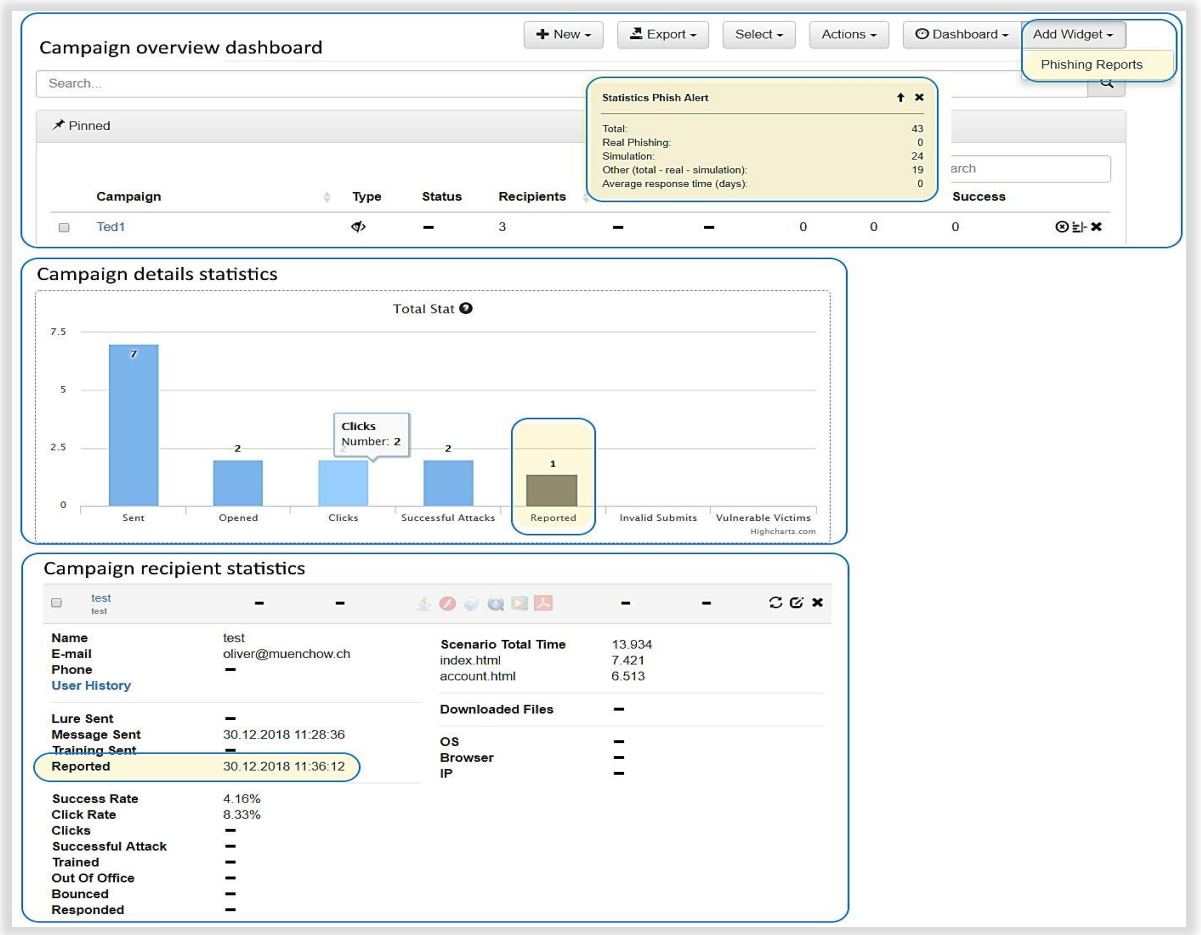
- **Identifier les attaques présentant des caractéristiques courantes :** appliquez les filtres du tableau de bord de LUCY pour détecter les vecteurs d'attaque courants au sein de votre entreprise. Recherchez dans tous les e-mails signalés des indicateurs de menace similaires.



- **Profils de réputation incidents des utilisateurs :** classer les utilisateurs en leur affectant un score de réputation basé sur les incidents



- **Intégration aux simulations d'attaque :** intégration parfaite de rapports et de tableaux de bord aux simulations d'hameçonnage : identifiez les utilisateurs qui se sont comportés de manière exemplaire dans une simulation d'hameçonnage.



- **Installation facile :** installez le plugin Incident d'hameçonnage pour Outlook, Gmail, Office365.