LUCY WHITEPAPER

WAS BIETET LUCY?

Testen, schulen und beteiligen Sie Ihre Mitarbeiter!

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

MITARBEITERTEST
Angriffssimulationen (z. B. Phishing)

INFRASTRUKTURTEST
Malware-Simulation und Scanner

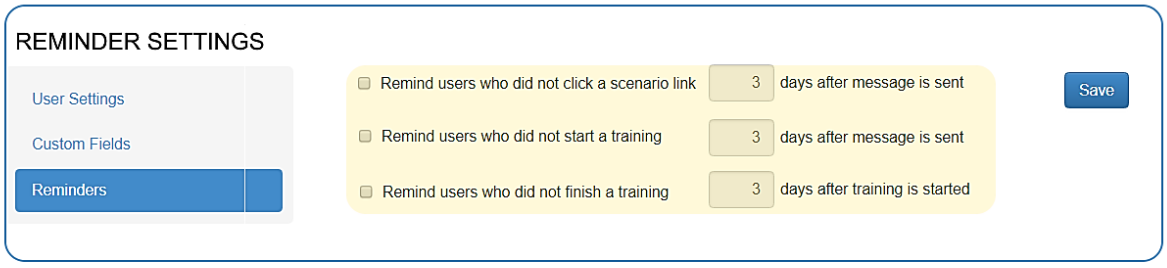
MITARBEITER-TRAINING
Integriertes Lern-Management-System

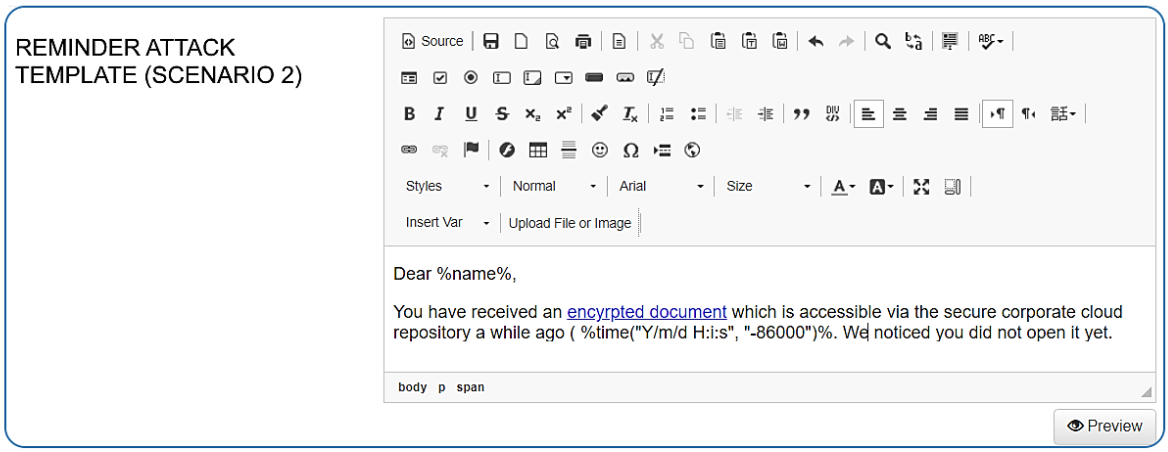
FORTSCHRITTS-ANALYSE
Bewertung Risiko und Lernfortschritte

INTEGRATION DER MITARBEITER
Reporting-System
(z. B. Mail Phish Button)

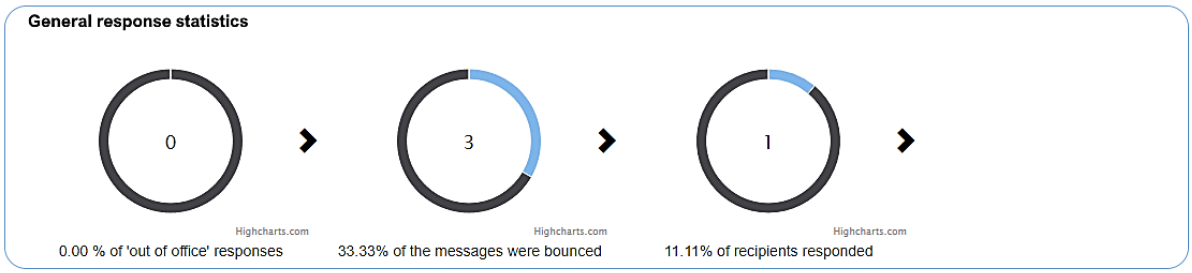
ALLGEMEINE MERKMALE

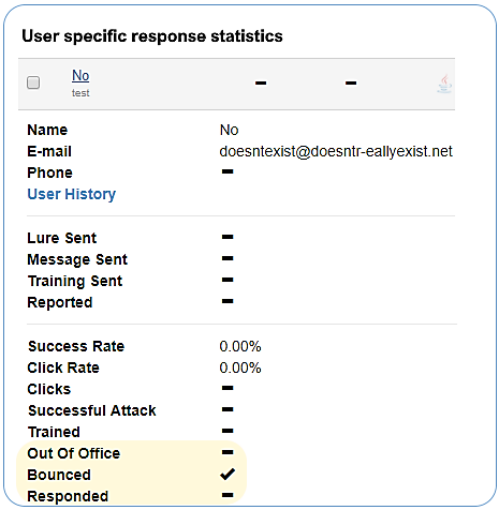
- **ERINNERUNGEN:** Erinnerungsvorlagen können verwendet werden, um automatisch Nachrichten erneut an Benutzer zu senden, die nach einem vorbestimmten Zeitraum nicht auf einen Angriffslink oder einen Schulungskurs geklickt haben.

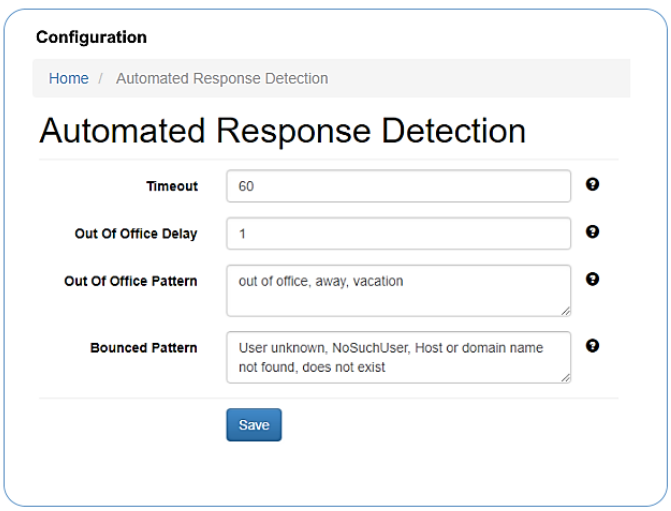




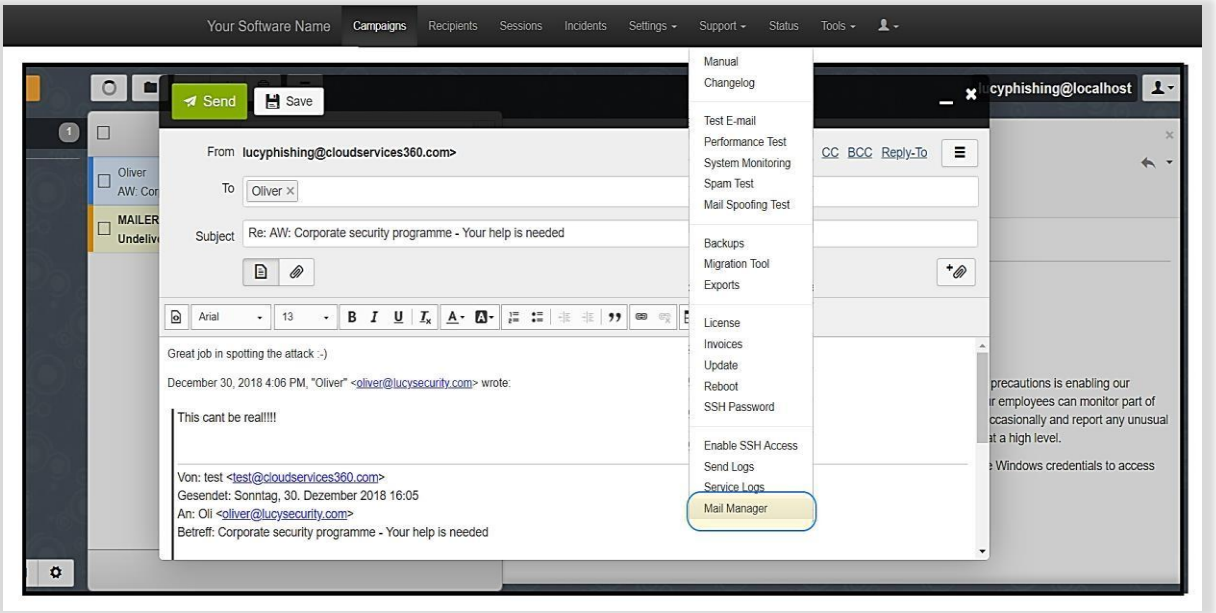
- **ANTWORTERKENNUNG:** Die automatische Antworterkennung ermöglicht das Definieren und Analysieren automatischer E-Mail-Antworten (z. B. bei Abwesenheit) sowie E-Mail-Zustellungsfehler (z. B. unbekannter Benutzer) innerhalb einer Kampagne.



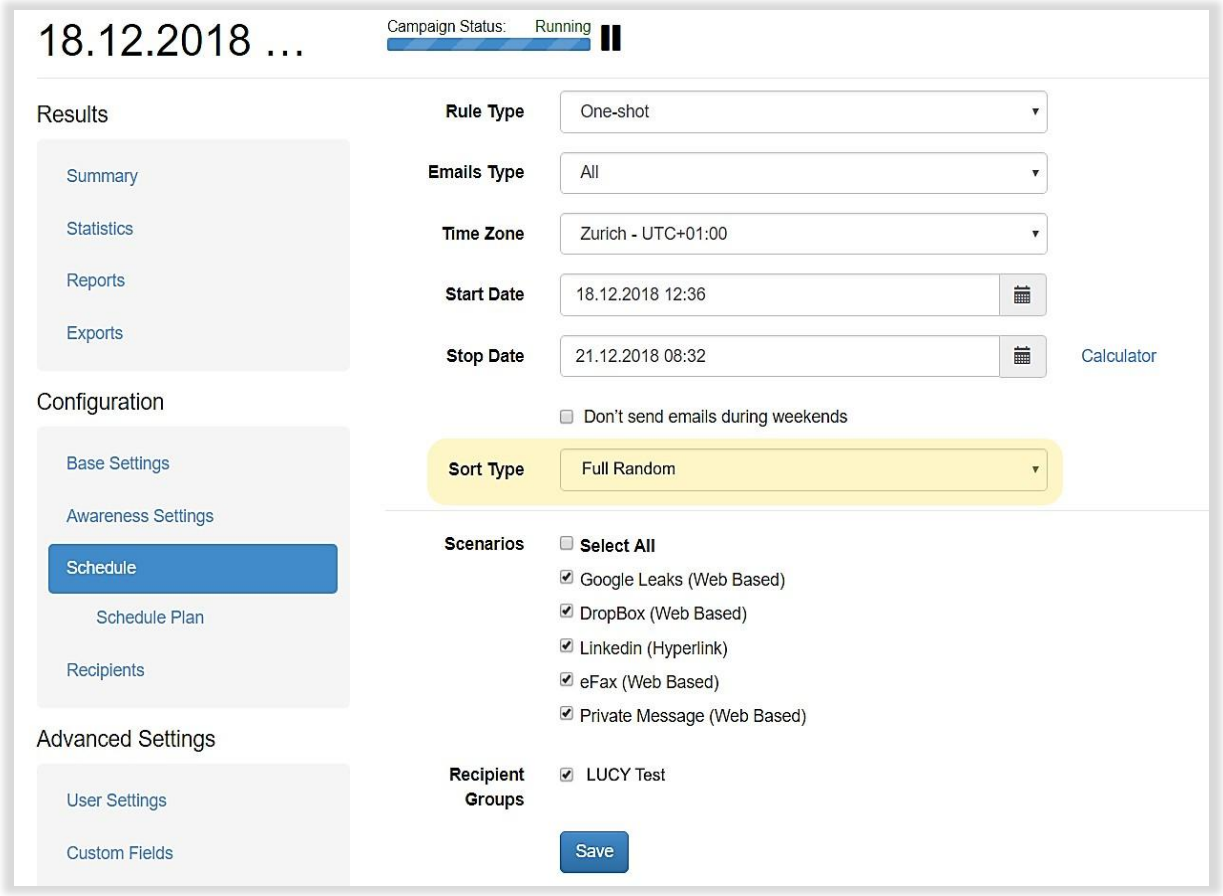




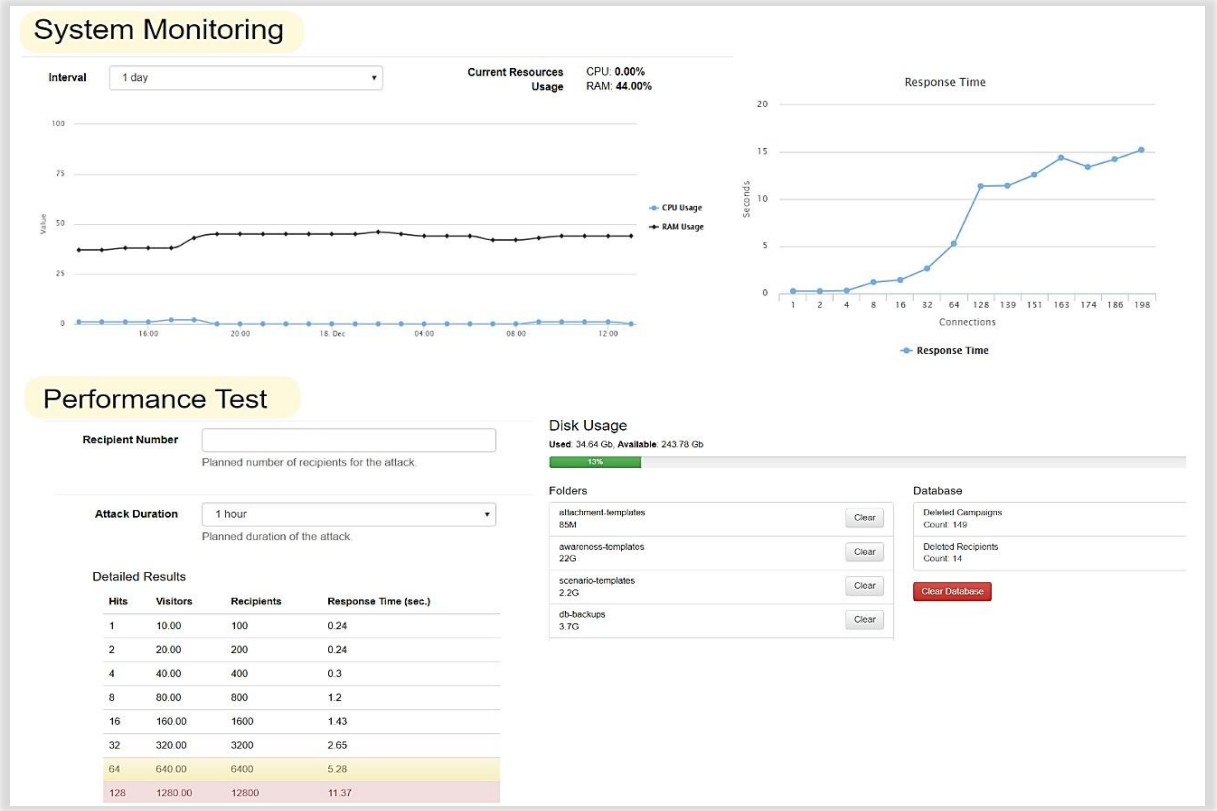
- **VOLLWERTIGER MAIL COMMUNICATION CLIENT:** Eine integrierte Messaging-Plattform ermöglicht dem LUCY-Administrator die interaktive Kommunikation mit den Empfängern innerhalb oder außerhalb von LUCY-Kampagnen. Alle E-Mails werden archiviert und können ausgewertet werden.



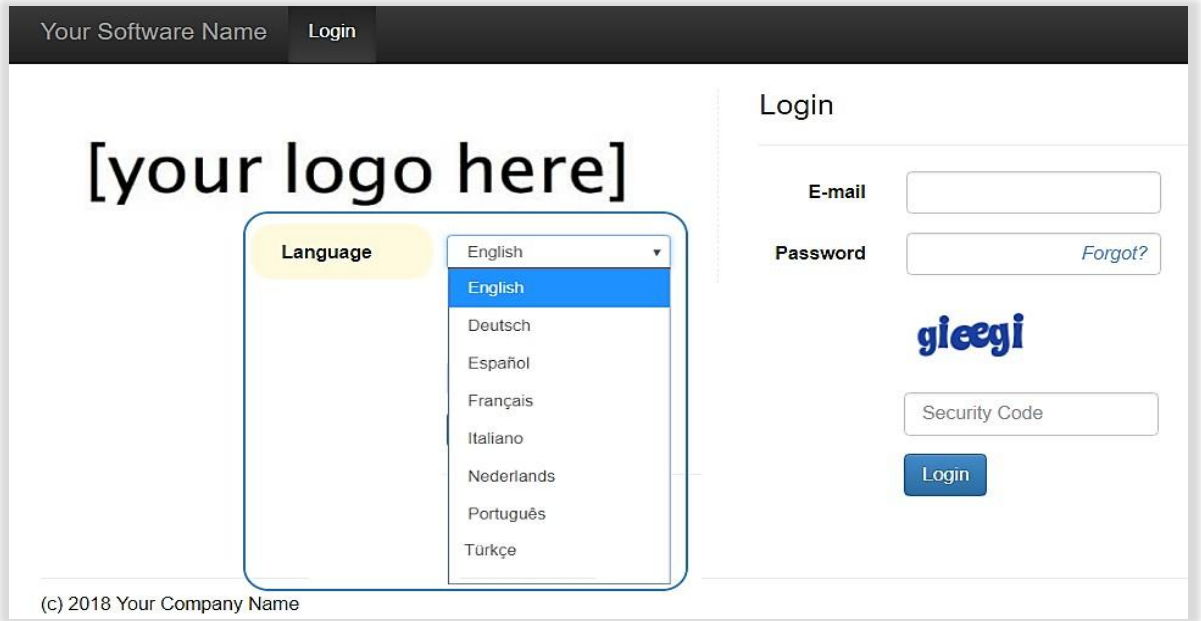
- **Zeitplan-Randomisierung:** Die gezielte Sensibilisierung der Mitarbeiter ist der Schlüsselfaktor für ein effektives und nachhaltiges Sicherheitsbewusstsein innerhalb des Unternehmens. Das zufällige Fahren einiger Kampagnen gleichzeitig ist eines der besten Mittel, um Mitarbeiter zu schulen.



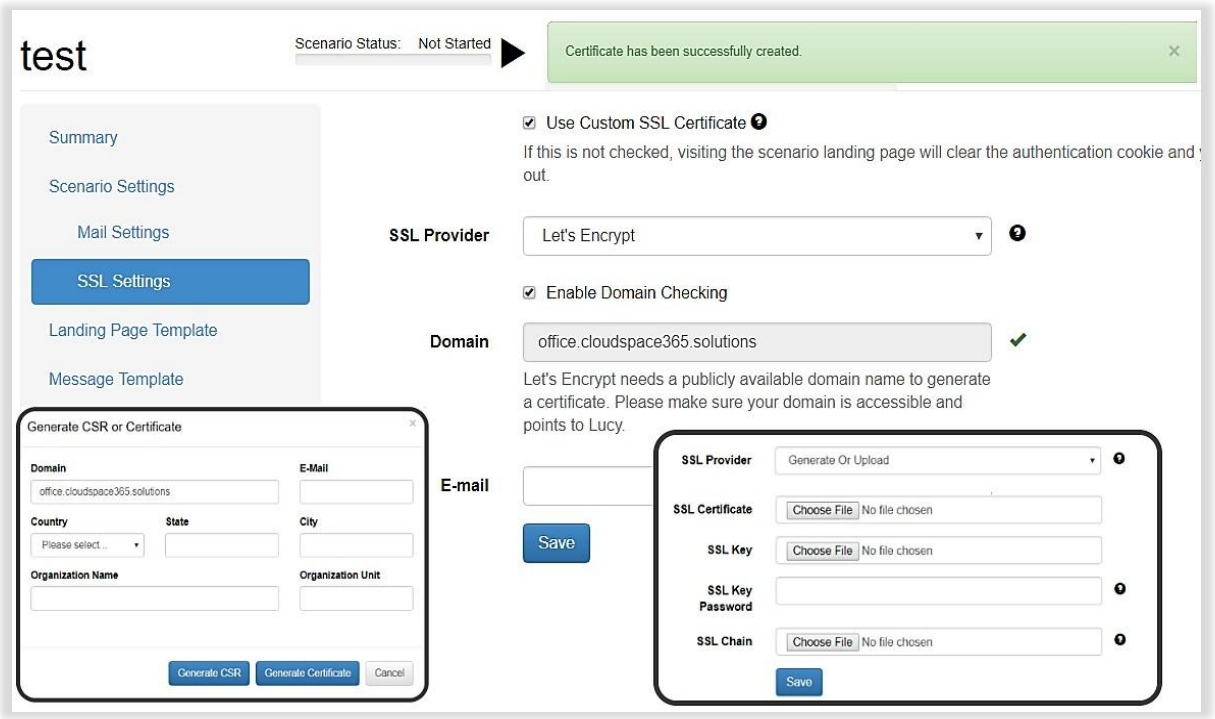
- **Leistungstools:** Die LUCY Smart Routines passen die Serverinstallation an die vorhandenen Ressourcen an. Anwendungsserver-, DBMS-Größen-, Speicher- und CPU-Auslastung werden während der Installation oder während des Betriebs berechnet. Sie können eine einzelne Cloud-basierte LUCY-Installation für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



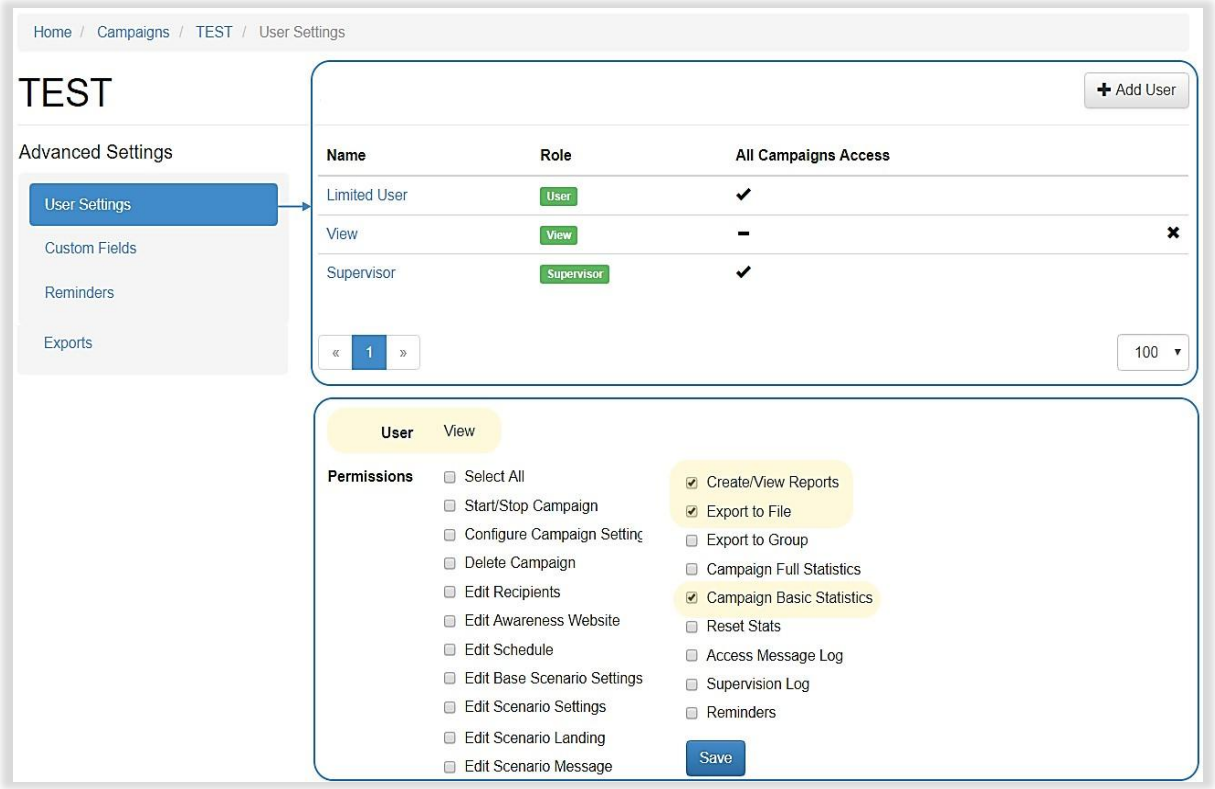
- **Mehrsprachige Admin-Oberfläche:** Die LUCY Admin-Oberfläche ist in vielen verschiedenen Sprachen verfügbar und kann auf Anfrage auch in andere Sprachen übersetzt werden.



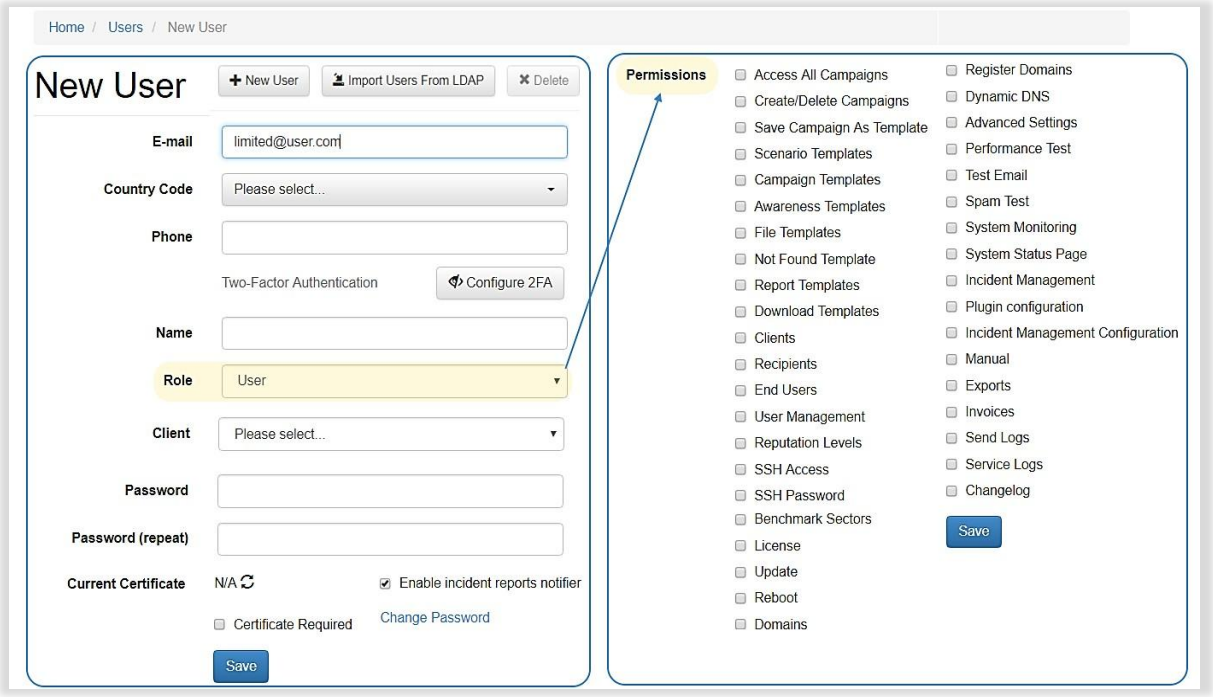
- **Zertifikat (SSL):** Ermöglicht die automatische Erstellung offizieller und anerkannter Zertifikate durch den Administrator, das Back-End sowie für die Kampagnen. LUCY verwendet automatisch die im System konfigurierte Domain, um das Zertifikat zu generieren. Wenn Sie sich für die Verwendung von SSL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



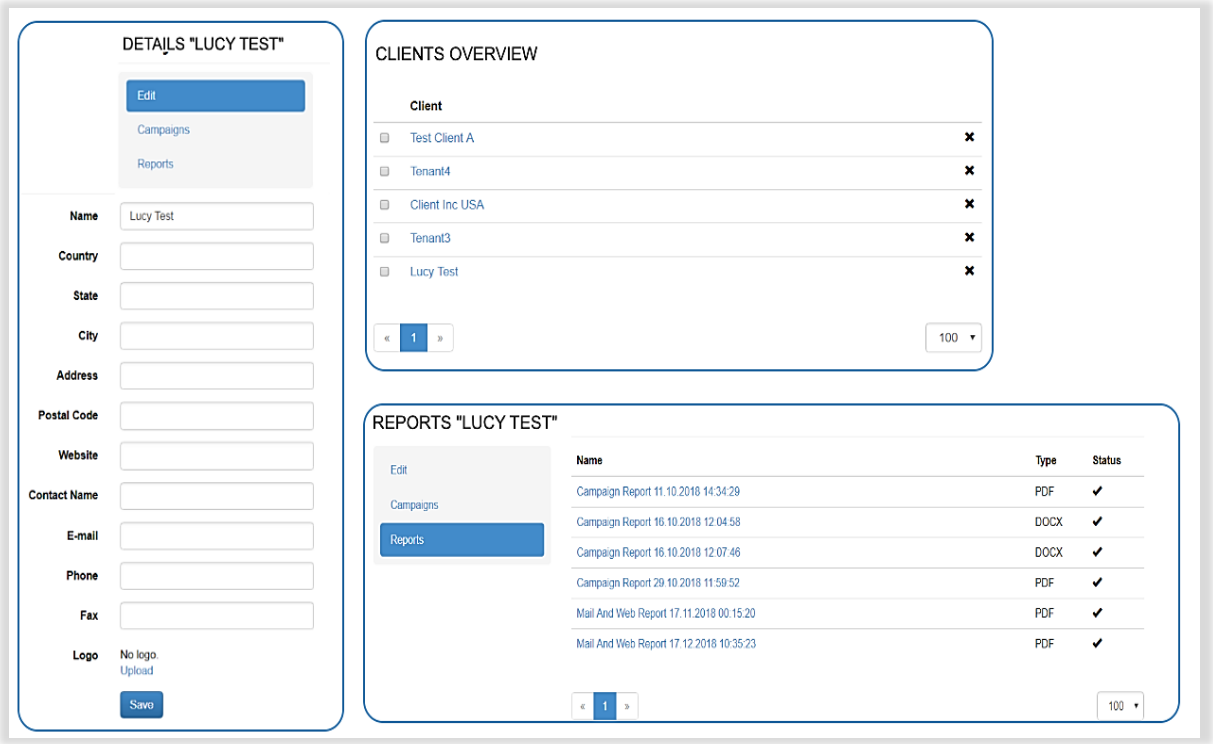
- **Rollenbasierte Zugriffssteuerung:** LUCY bietet eine rollenbasierte Zugriffssteuerung (RBAC), die den Systemzugriff auf autorisierte Benutzer beschränkt. Die Berechtigungen zum Ausführen bestimmter Arbeitsabläufe werden in den Benutzereinstellungen an bestimmte Rollen gekoppelt. Mitarbeitern, Teilnehmern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



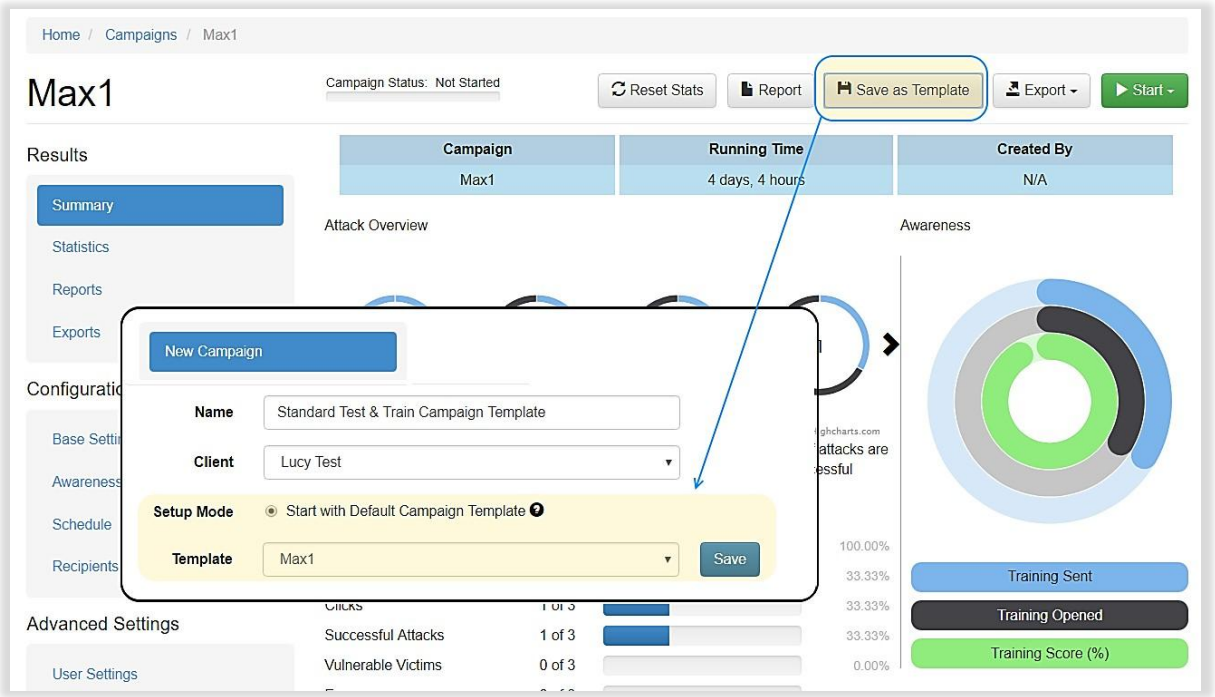
- **Mehrschichtige Benutzergruppen**: Laden Sie große Benutzergruppen schnell über eine CSV-, LDAP- oder Textdatei hoch. Erstellen Sie verschiedene Gruppen, die nach Arbeitsbereiche, Abteilung, Bezeichnung, usw. gegliedert sind. Aktualisieren Sie Benutzer in einer laufenden Kampagne. Erstellen Sie dynamische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



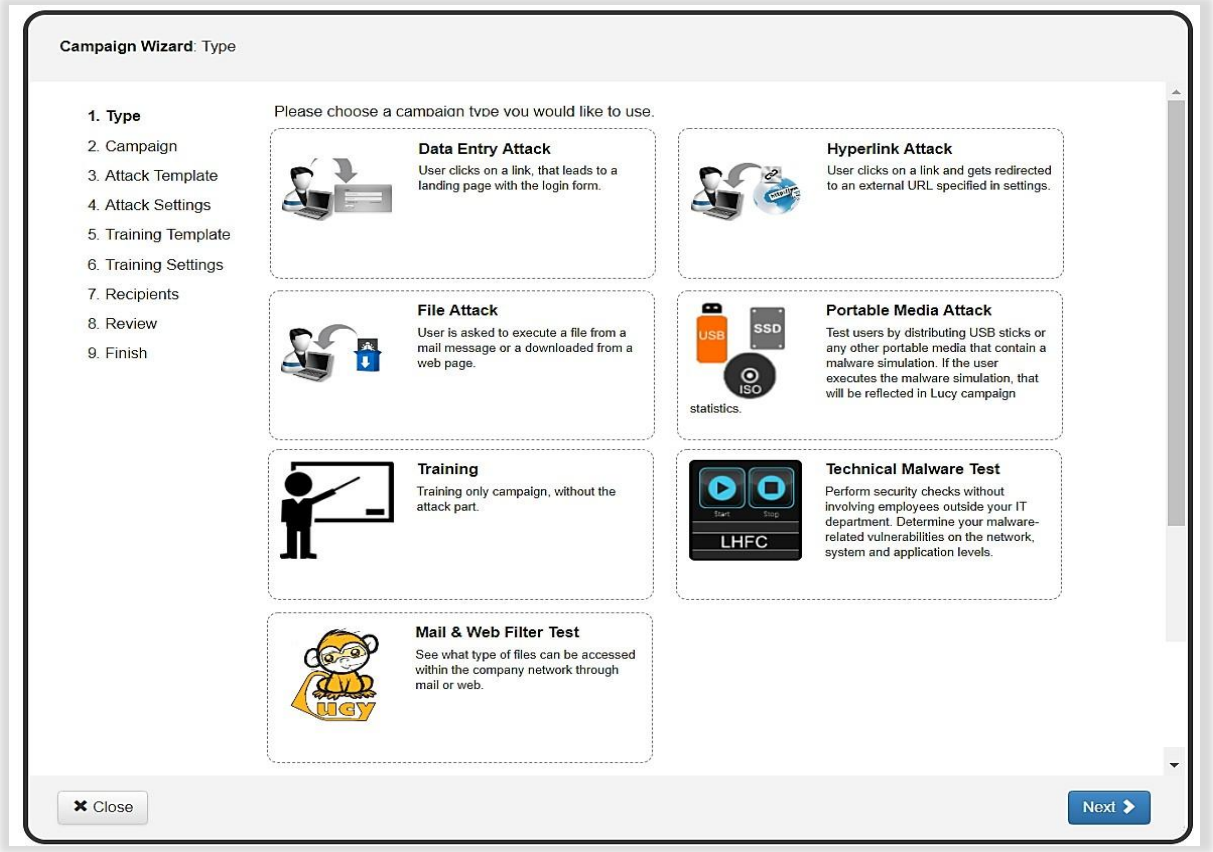
- **Multi-Client-kompatibel:** „Client“ kann sich auf verschiedene Unternehmensbereiche, Abteilungen oder Gruppen beziehen, denen eine Kampagne in LUCY zugeordnet ist. Diese „Clients“ können beispielsweise verwendet werden, um einen kampagnenspezifischen Zugriff zu ermöglichen oder um teilnehmer-spezifische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



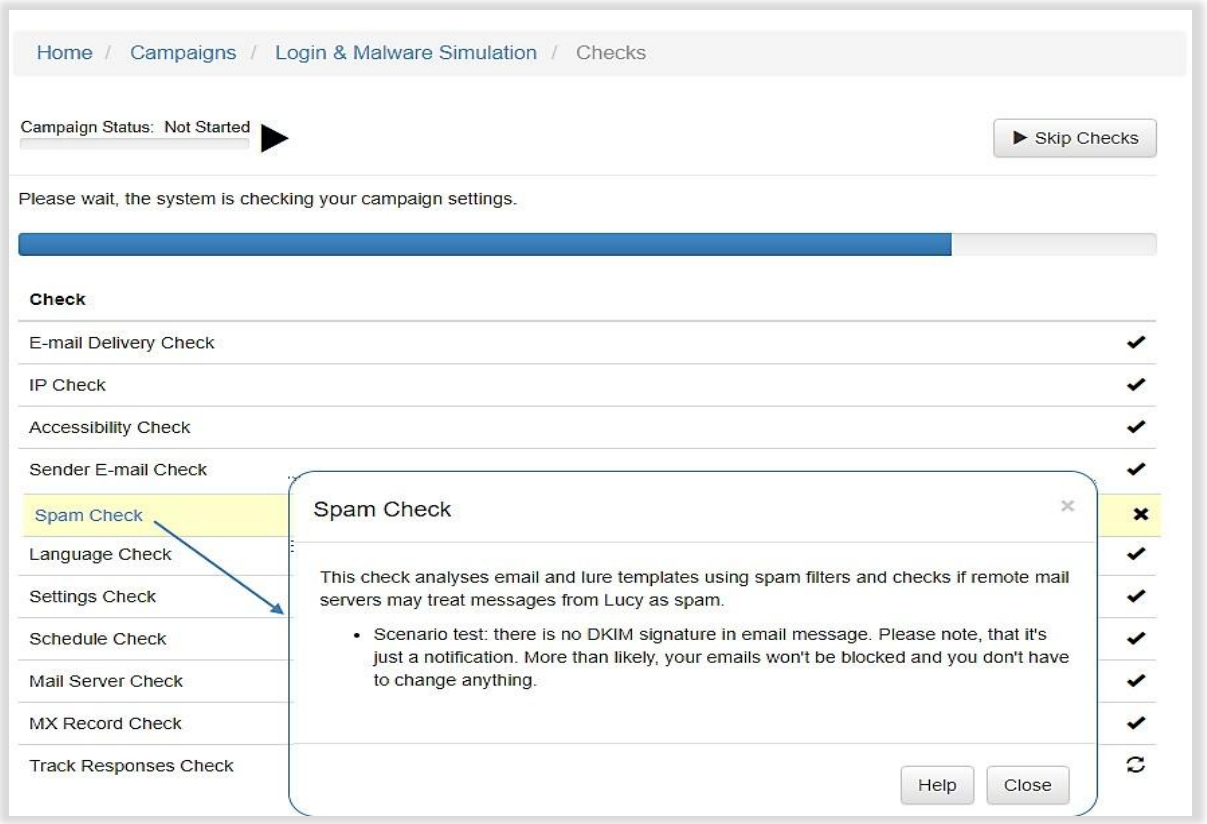
- **Kampagnenvorlagen:** Wenn Sie eine Kampagne in ähnlicher Form wiederverwenden möchten, können Sie eine solche Kampagne vollständig mit Angriffsvorlagen und E-Learning-Inhalte als Kampagnenvorlage speichern. Mit dieser Funktion können Sie vermeiden, ähnliche Konfigurationen immer wieder erstellen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



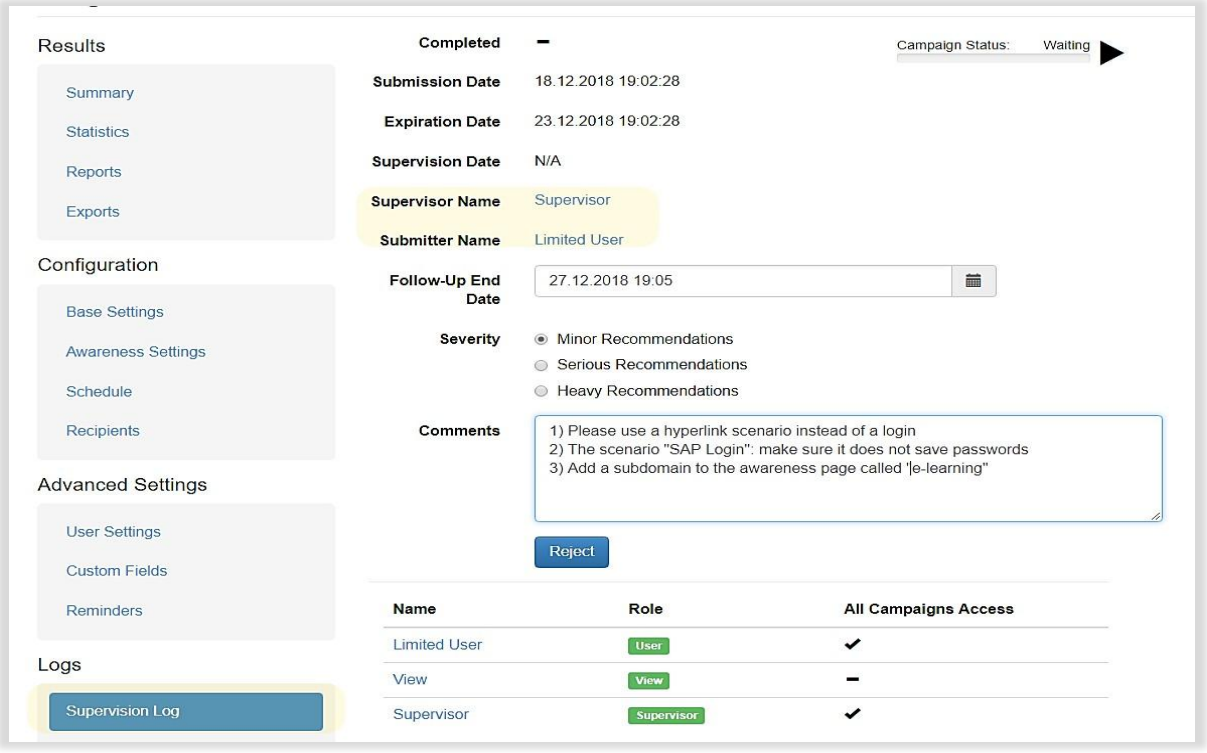
- **Setup-Assistent mit risikobasierter Anleitung:** LUCY bietet verschiedene Setup-Tools. Erstellen Sie mit den vordefinierten Kampagnenvorlagen in weniger als 3 Minuten eine vollständige Kampagne oder lassen Sie sich vom Setup-Assistenten durch die Konfiguration führen. Optional steht ein risikobasierter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



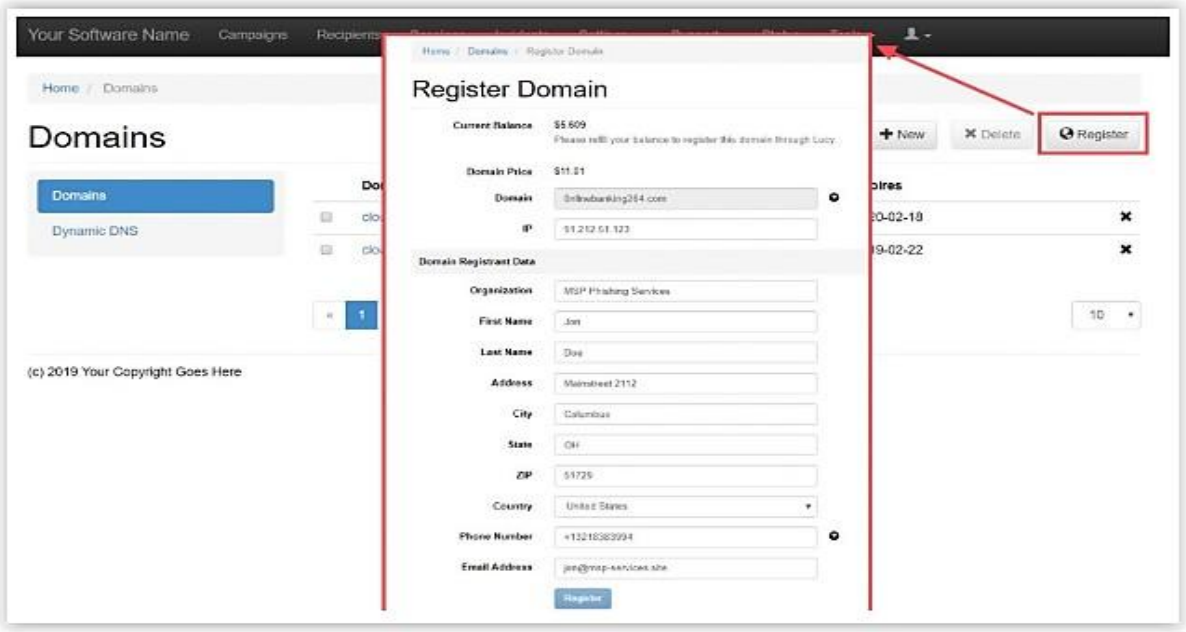
- **Kampagnenprüfungen:** Vorläufige Prüfungen vor dem Start einer LUCY-Kampagne: E-Mail-Zustellungsprüfung, MX-Datensatzprüfung, Zeitplanprüfung, Spamprüfung und andere.



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

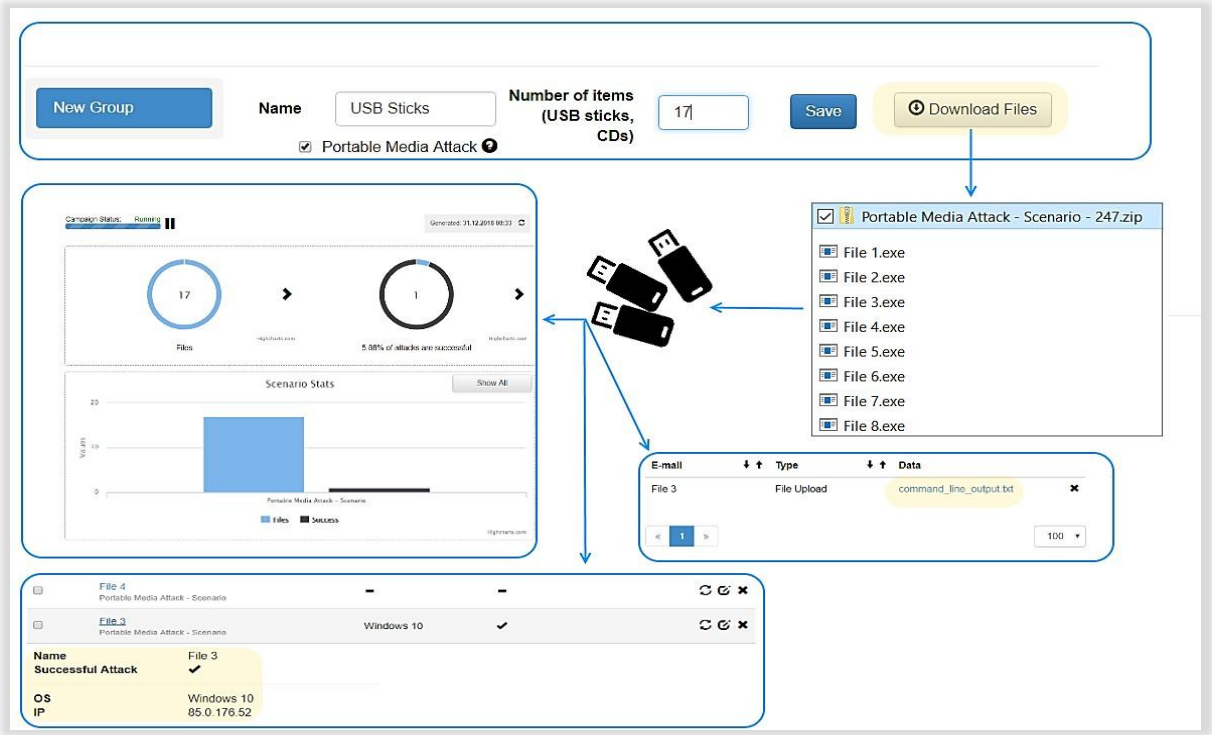


- **DNS API:** Mit der DNS-API kann der Administrator innerhalb von Sekunden mit LUCY eine beliebige Domain erstellen. Da Angreifer sehr häufig ähnliche Domain-Schreibweise verwenden (Typosquatting genannt), kann dieses Risiko mit LUCY auch dargestellt werden. Wenn die ursprüngliche Domain des Unternehmens beispielsweise „onlinebanking.com“ lautet, kann der DNS-Assistent verwendet werden, um Domains wie „0nlinebanking.com“, „onl1nebanking.com“ oder „onlinebanking.services“ zu reservieren und später einer Kampagne zuweisen. LUCY erstellt dann automatisch die entsprechenden DNS-Einträge (MX, SPF, Whois Protection, usw.) für die IP, auf der LUCY installiert ist. Natürlich kann der Administrator auch die eigenen Domains seines Providers in LUCY verwenden.

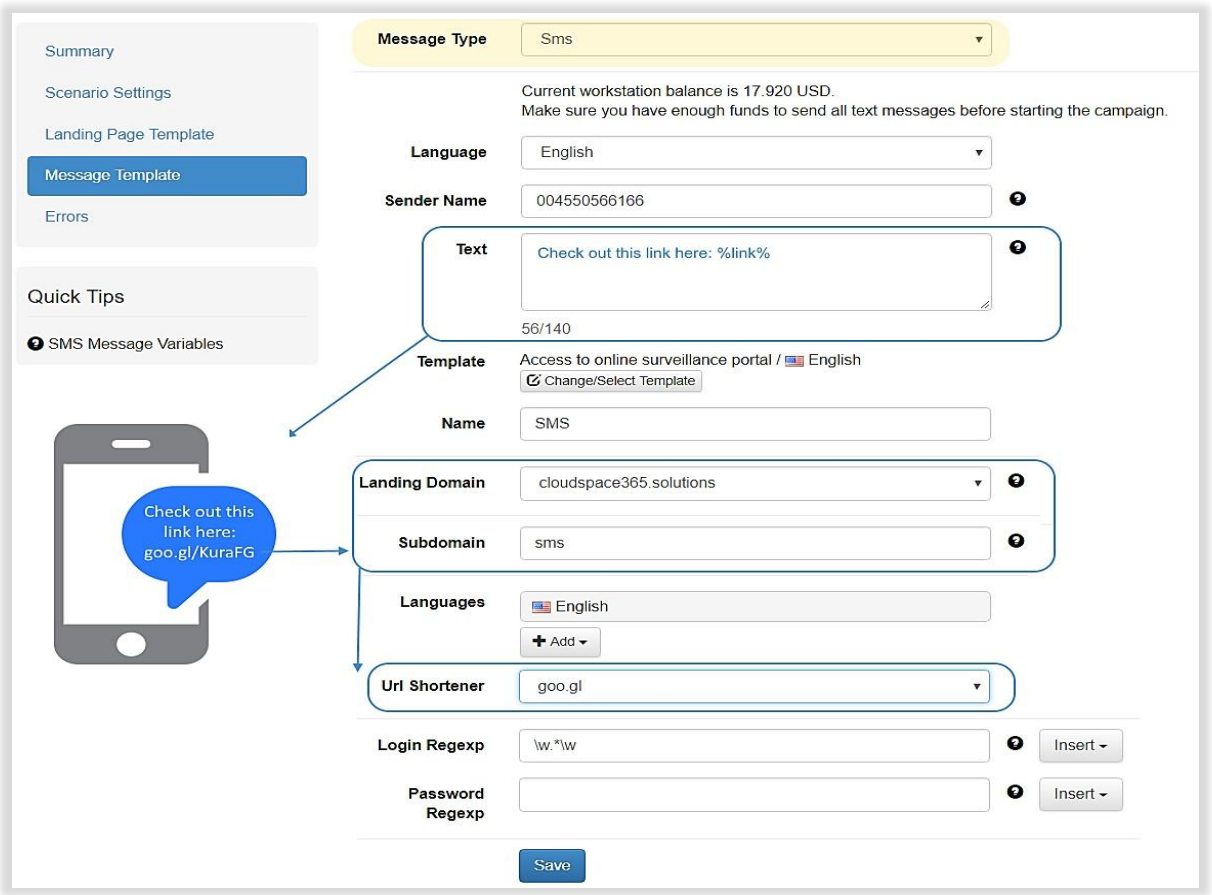


ANGRIFFSSIMULATION

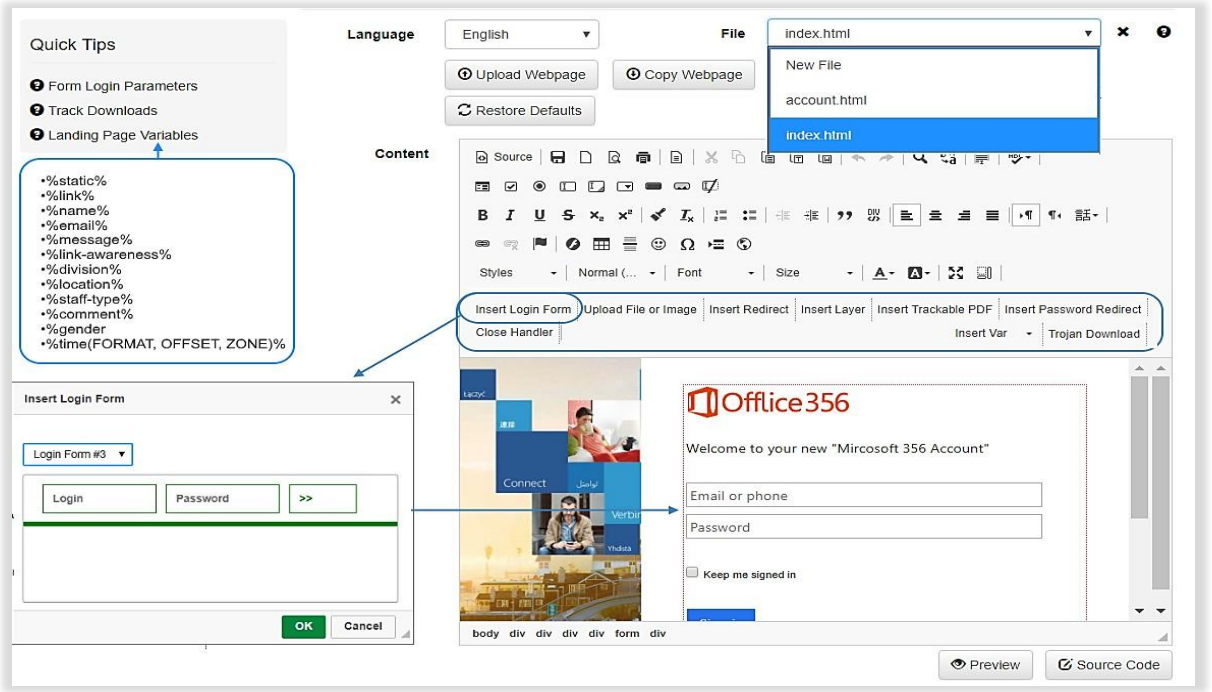
- **Angriffe auf tragbare Medien:** Hacker können tragbare Medien verwenden, um auf vertrauliche Informationen zuzugreifen, die auf einem Computer oder in einem Netzwerk gespeichert sind. LUCY bietet die Möglichkeit, Angriffe auf tragbare Medien durchzuführen, bei denen eine Dateivorlage (z. B. ausführbare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



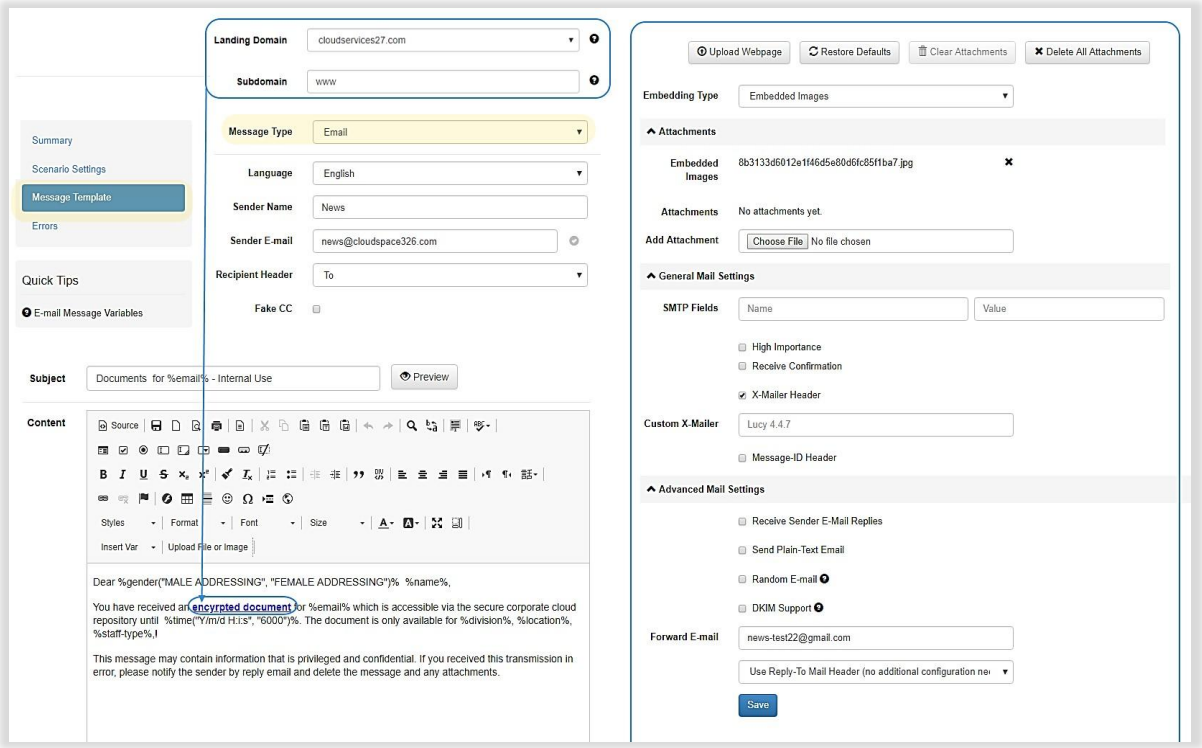
- **SMiShing:** Smishing ist gewissermaßen „SMS-Phishing“. Wenn Cyberkriminelle „Phishing“ betreiben, senden sie betrügerische E-Mails, die den Empfänger dazu verleiten sollen, einen mit Malware beladenen Anhang zu öffnen oder auf einen böswilligen Link zu klicken. Smishing verwendet einfach Textnachrichten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



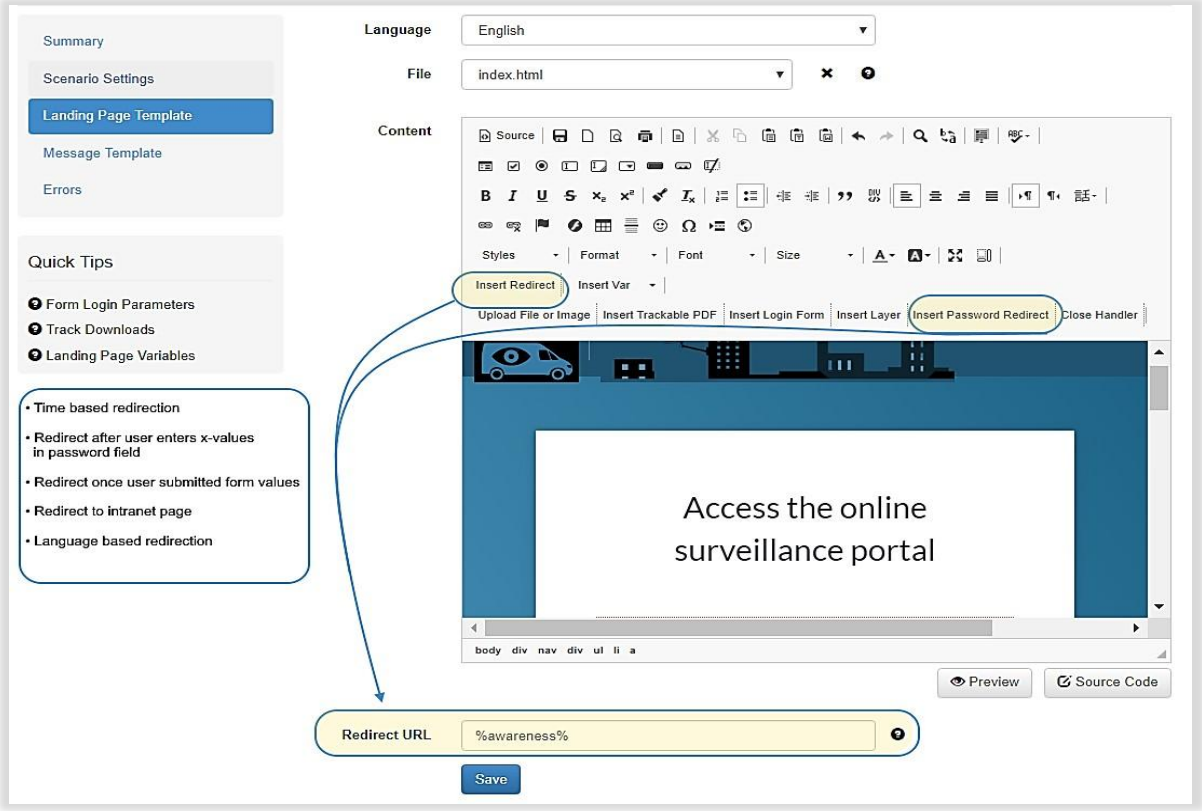
- **Dateneingabe-Angriffe:** Dateneingabeangriffe können eine oder mehrere Webseiten umfassen, welche die Eingabe vertraulicher Informationen abfangen. Die verfügbaren Webseiten können einfach mit dem LUCY-Webeditor angepasst werden. Mit zusätzlichen Bearbeitungs-Tools können Sie schnell Funktionen wie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



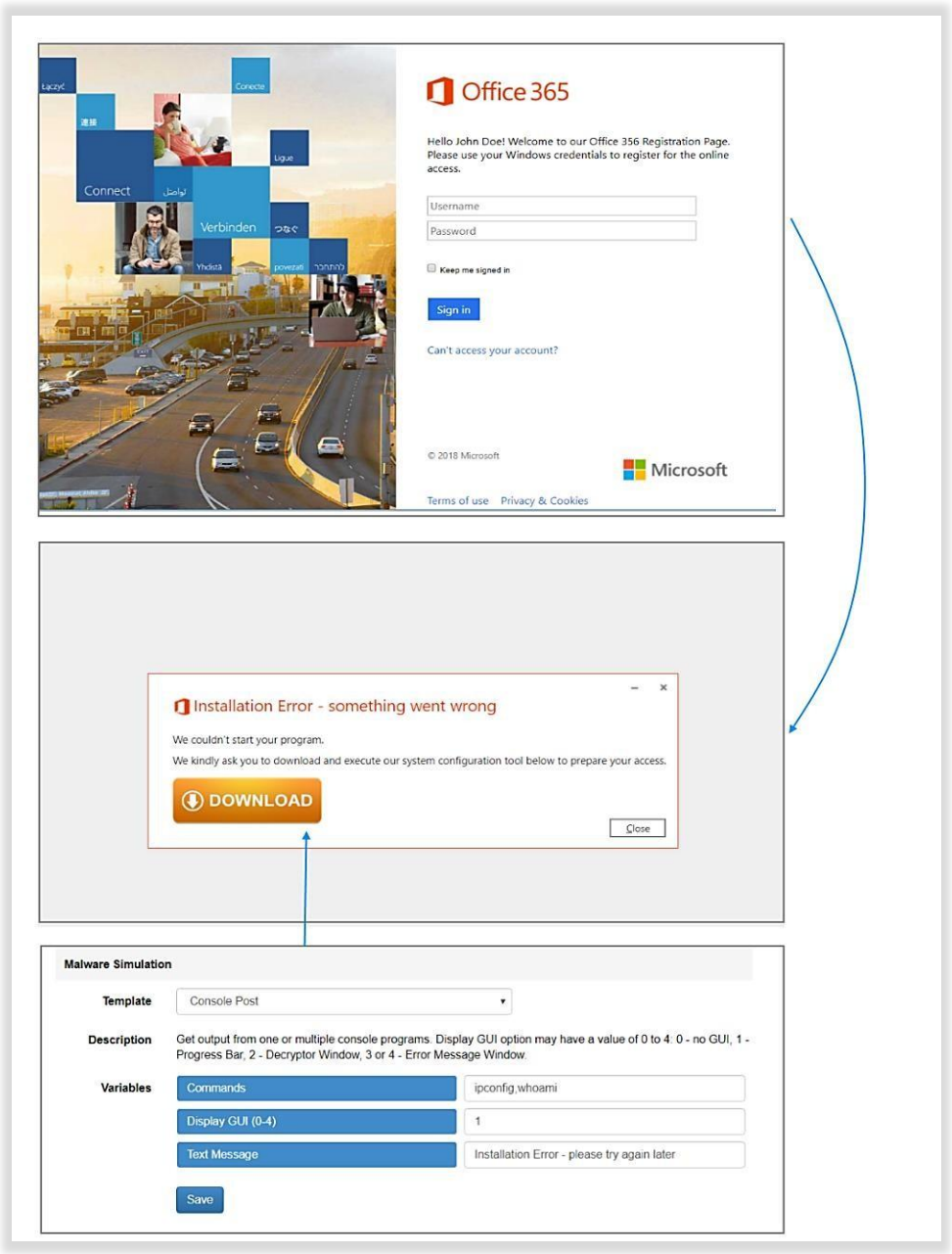
- **Hyperlink-Angriffe:** Eine Hyperlink-basierte Kampagne sendet Benutzern eine E-Mail mit einer zufälligen Tracking-URL.



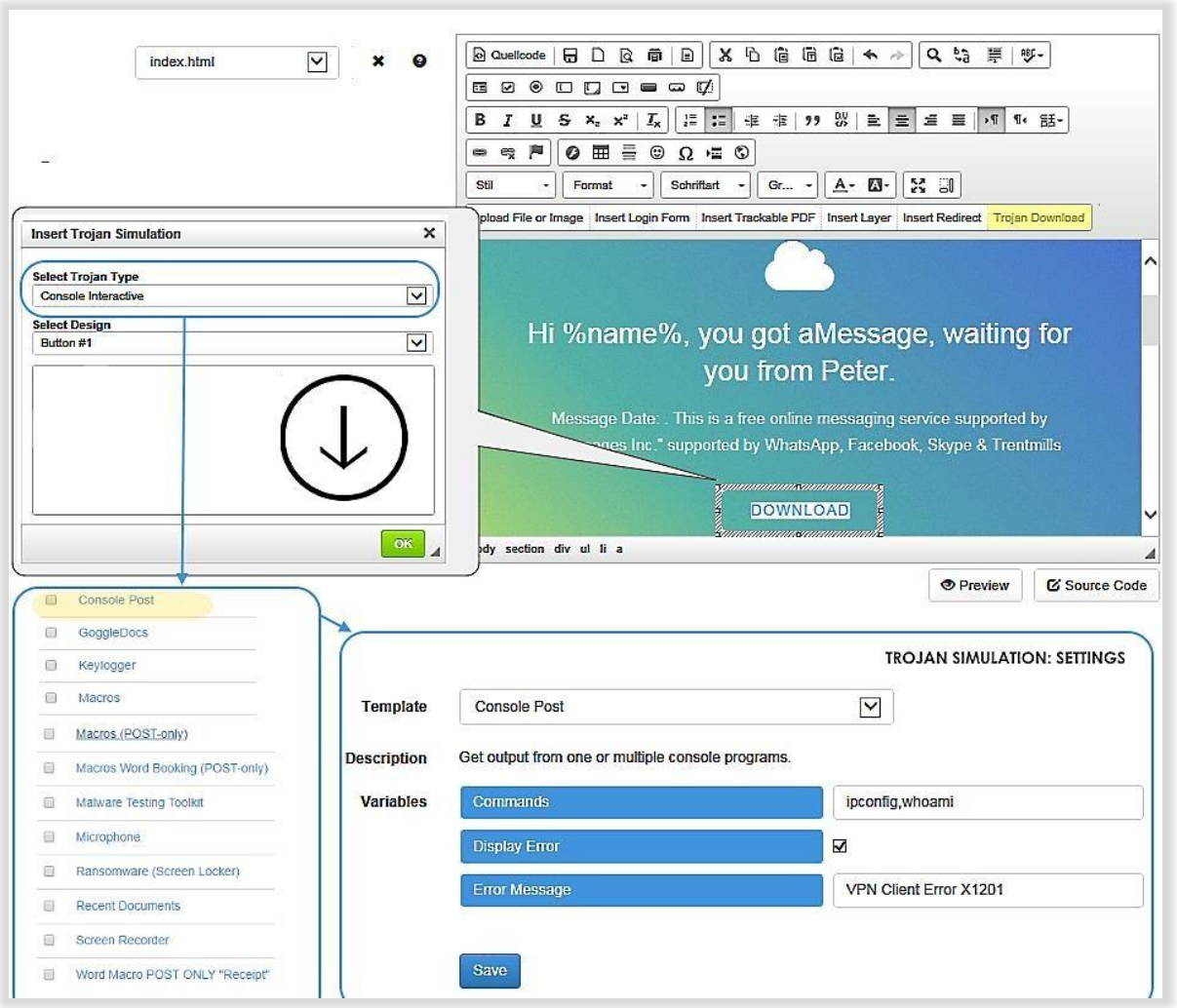
- **Leistungsstarkes Toolkit zur URL-Umleitung:** Mit den flexiblen Umleitungsfunktionen von LUCY kann ein Benutzer zum richtigen Zeitpunkt zu den gewünschten Bereichen der Angriffssimulation oder der Schulung geführt werden. Nach Eingabe der ersten drei Zeichen eines Kennworts in einer Phishing-Simulation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



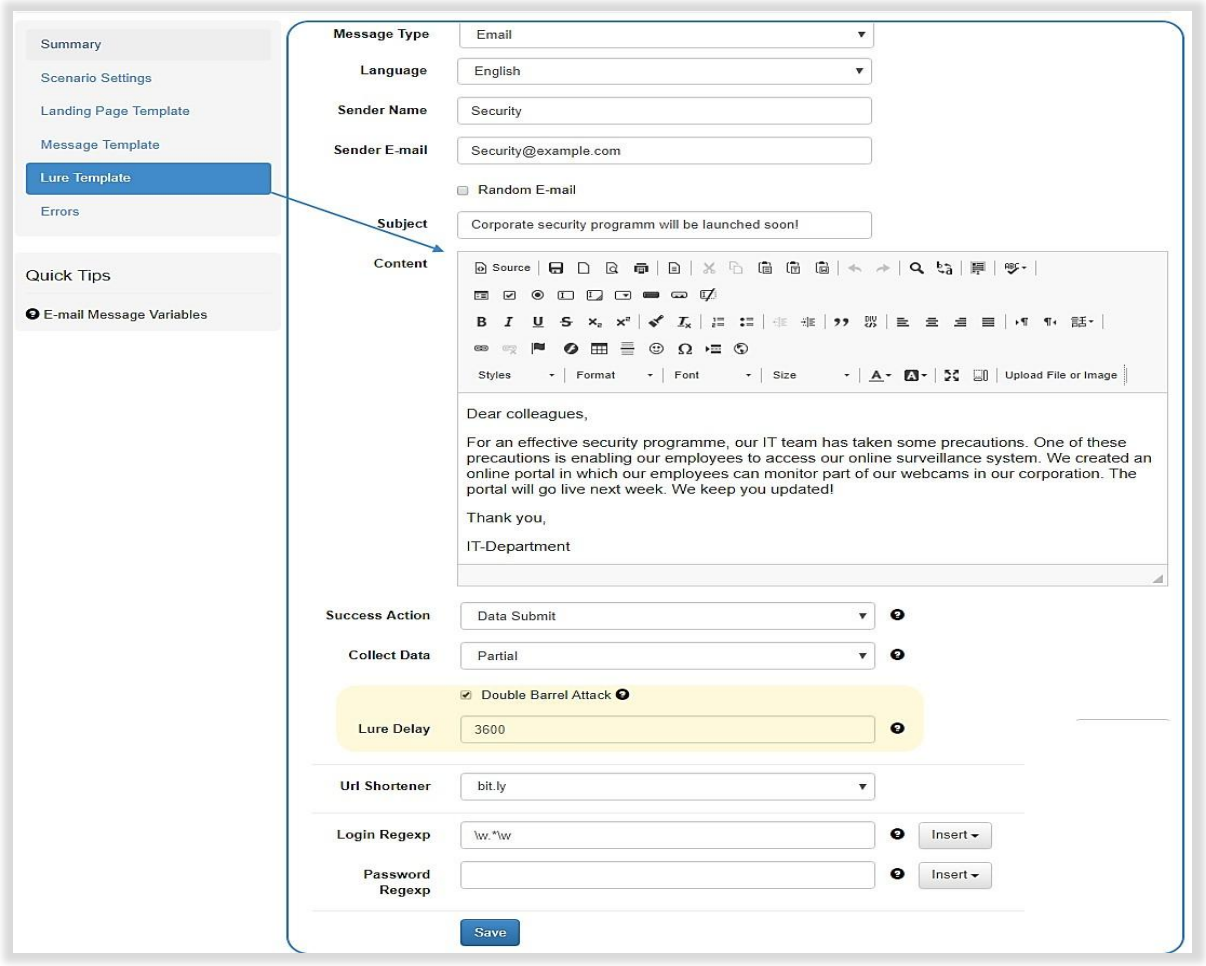
- **Gemischte Angriffe:** Gemischte Angriffe ermöglichen die Kombination mehrerer Szenarienarten (dateibasiert, Dateneingabe, usw.) in derselben Kampagne.



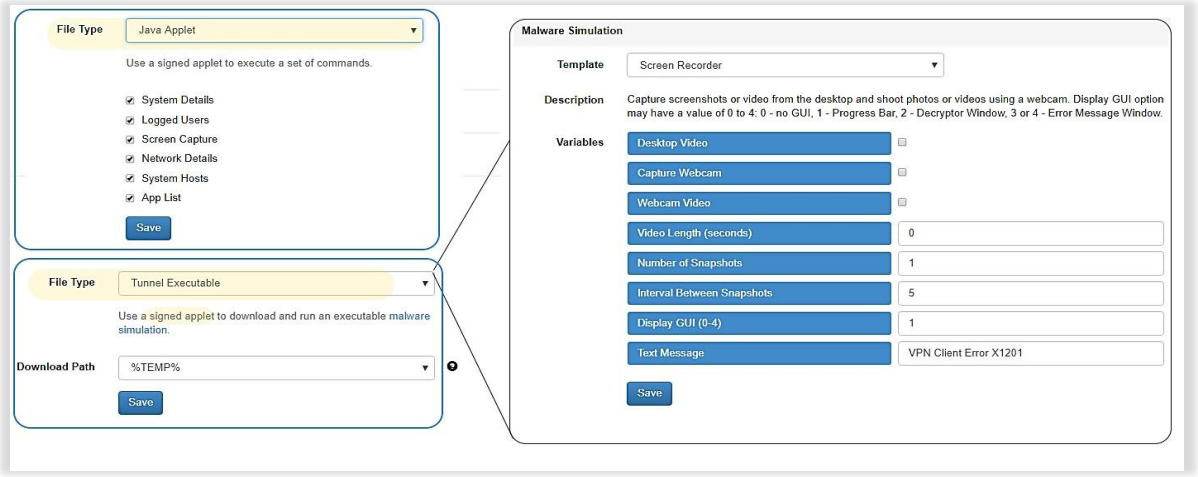
- **Dateibasierte Angriffe:** Mit dateibasierten Angriffen kann der LUCY-Administrator verschiedene Dateitypen (Office-Dokumente mit Makros, PDFs, ausführbaren Dateien, MP3s, usw.) in LUCY- generierte E-Mail-Anhänge oder Webseiten integrieren und deren Download- oder Ausführungsrate messen.



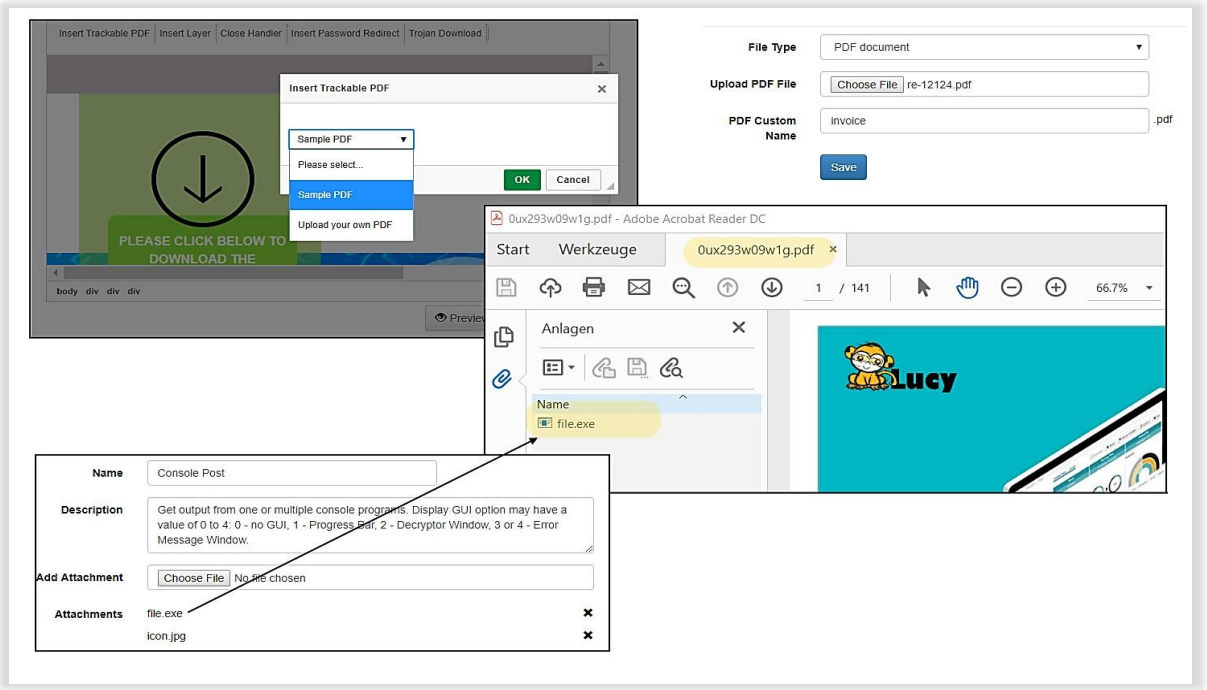
- **Double Barrel-Angriffe:** Mit dieser Funktion können in jeder Kampagne mehrere Phishing-E-Mails gesendet werden, wobei die erste harmlose E-Mail (der Köder) nichts Bösartiges enthält und keine Antwort vom Empfänger verlangt.



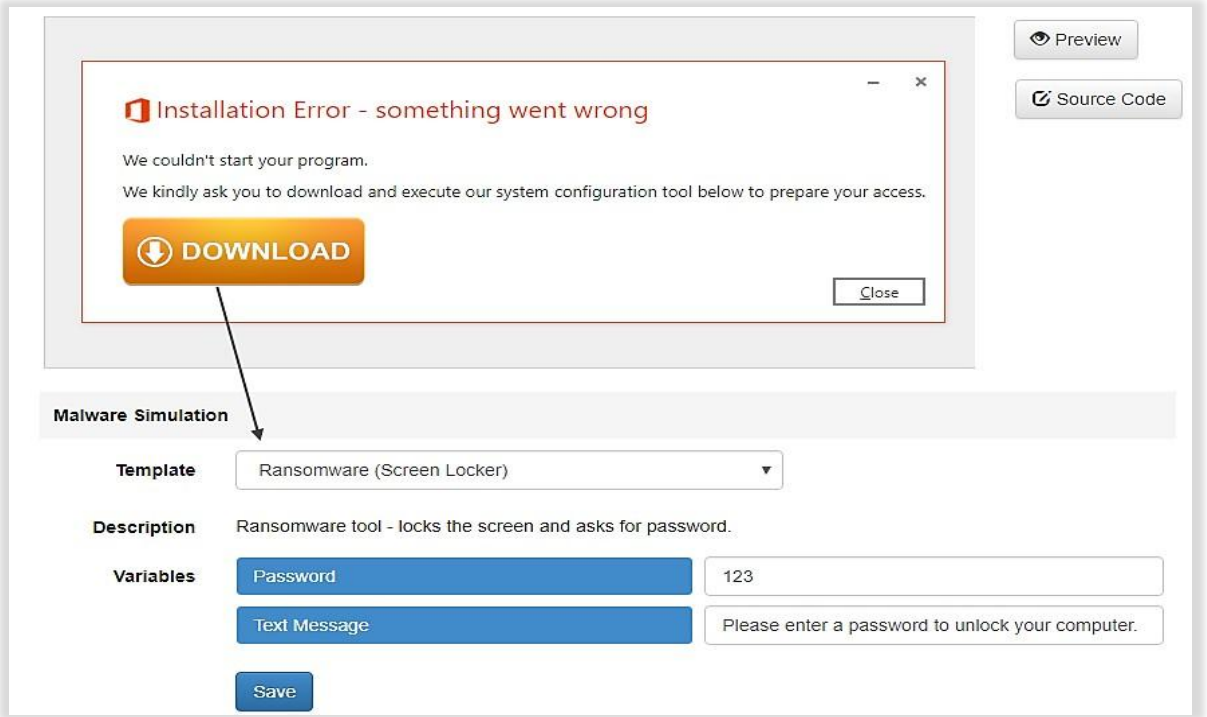
- **Java-basierte Angriffe:** Mit Java-basierten Angriffen kann der LUCY-Administrator ein vertrauenswürdiges Applet in die durch LUCY bereitgestellten dateibasierten oder gemischten Angriffsvorlagen integrieren und deren Ausführung durch den Benutzer messen.



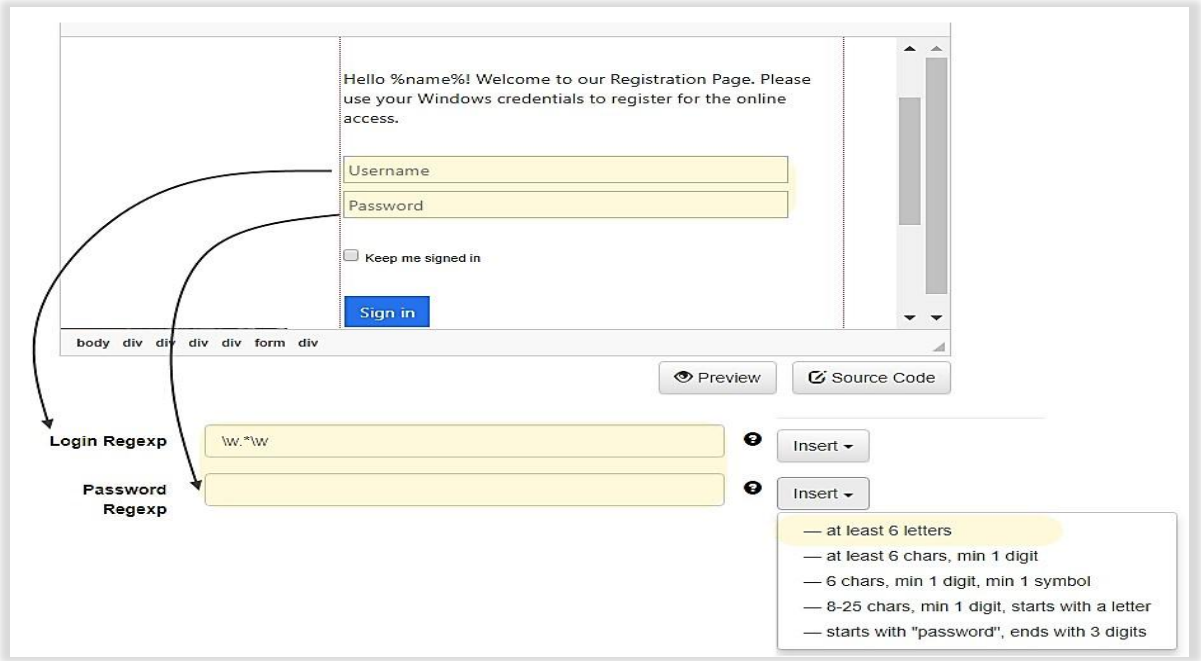
- **PDF-basierte Angriffe:** Mit diesem Modul können PDF-basierte Phishing-Angriffe simuliert werden. Mit LUCY können Exe-Dateien als harmlose PDF-Anhänge „deklariert“ und deren Ausführung gemessen werden. Darüber hinaus können dynamische Phishing-Links auch in PDFs generiert werden.



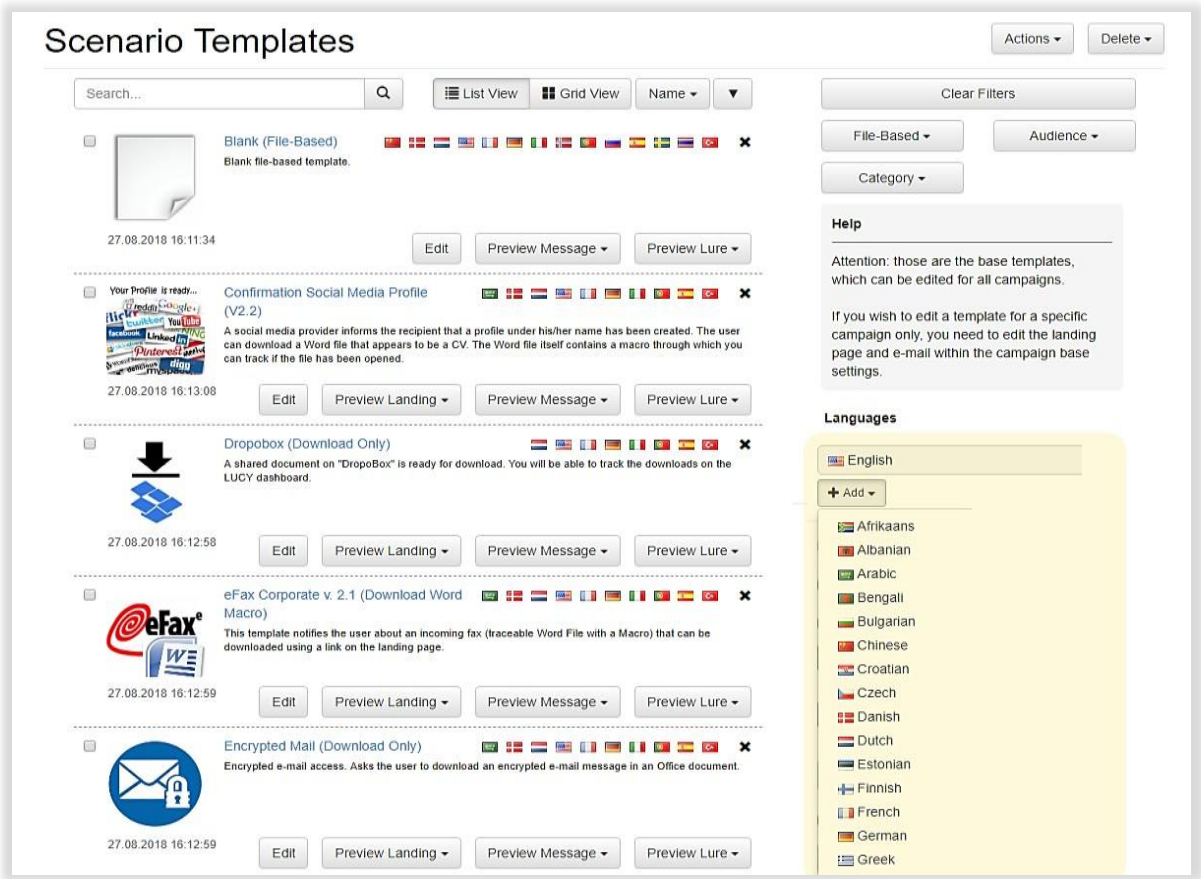
- **Ransomware-Simulationsangriffe:** LUCY verfügt über zwei verschiedene Ransomware Simulationen, wobei eine das Personal und die andere die Infrastruktur testet.



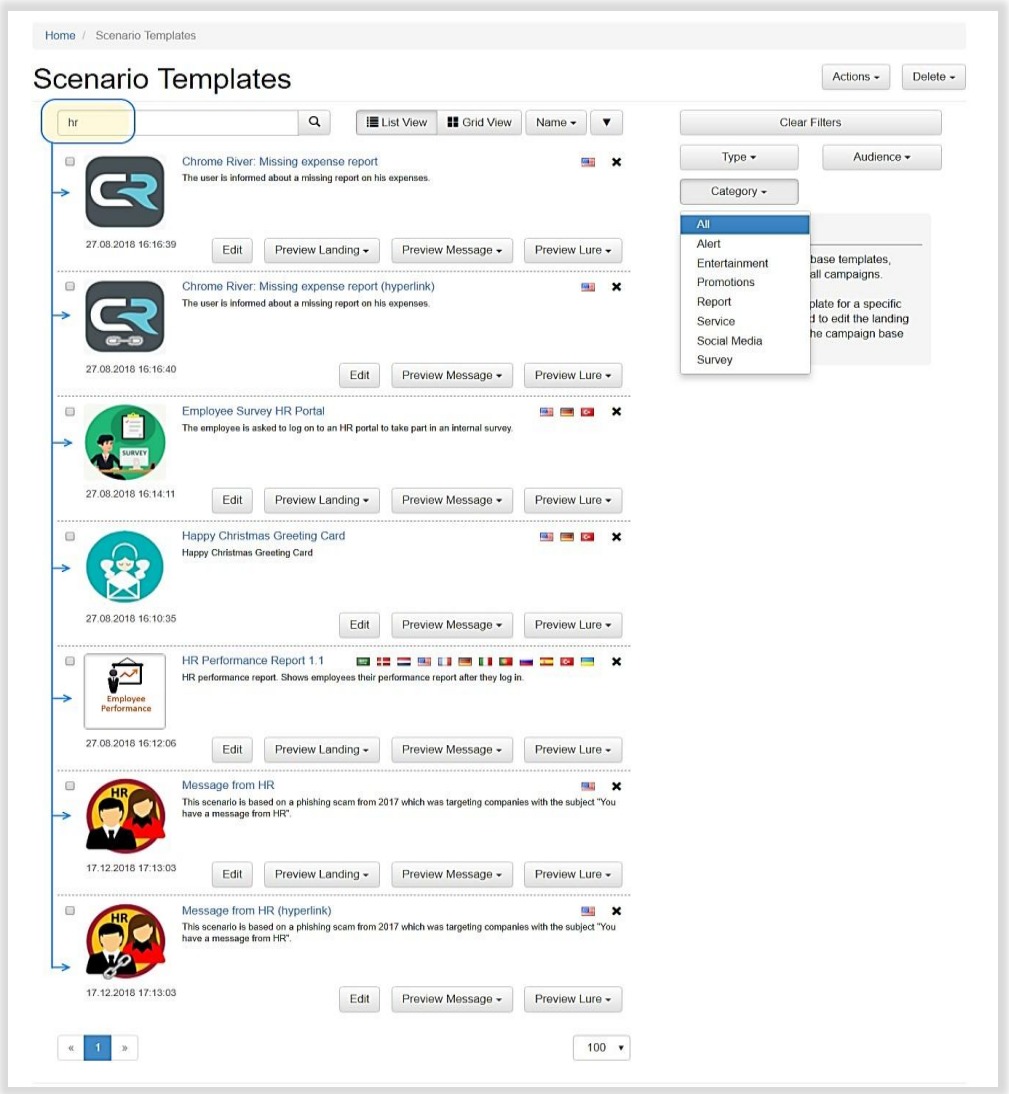
- **Toolkit zur Validierung der Dateneingabe:** Bei der Phishing-Simulationen müssen fehlerhafte Akzeptanz für Anmeldefelder verhindert werden (z. B. Protokollierung mit ungültiger Syntax). Die Unternehmensrichtlinien können auch die Übertragung sensibler Daten wie Passwörter verbieten. Zu diesem Zweck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



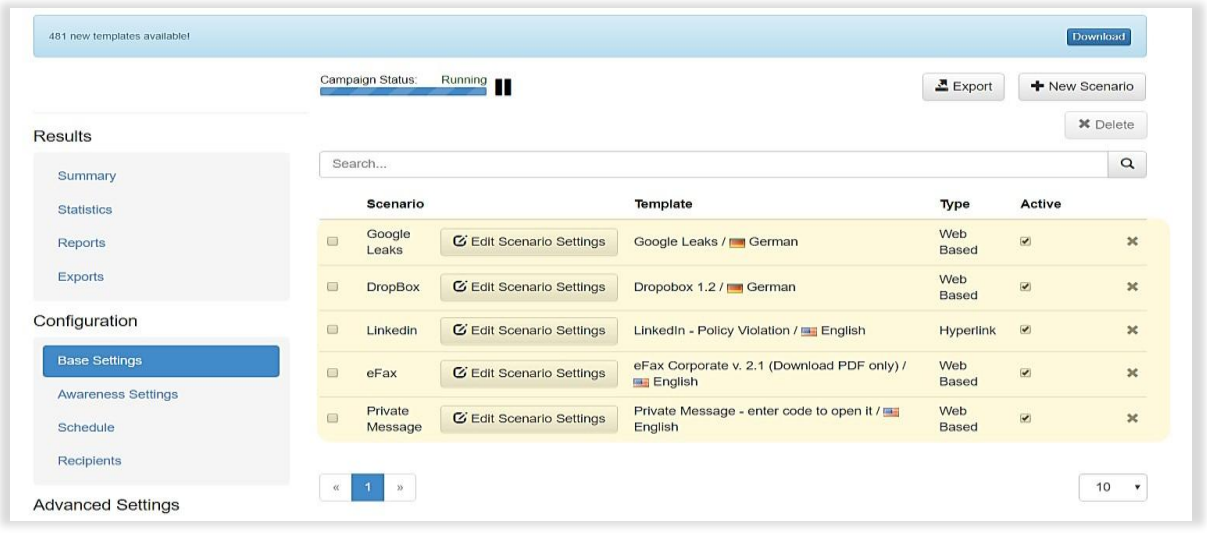
- **Mehrsprachige Angriffsvorlagenbibliothek:** LUCY bietet Hunderte vordefinierte Angriffsvorlagen in mehr als 30 Sprachen in den Kategorien Dateneingabe (Vorlagen mit einer Webseite), dateibasiert (E-Mails oder Webseiten mit Dateidownload) und Hyperlink (E-Mails mit einem Link), gemischt (Kombination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



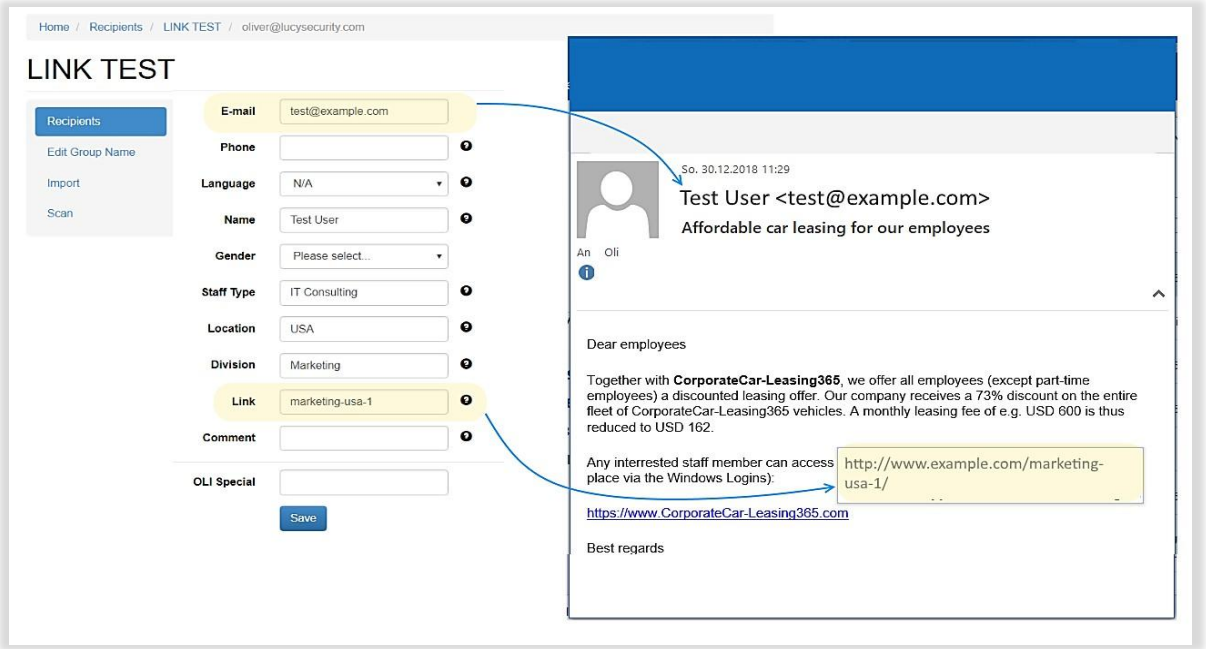
- **Sektor- und abteilungsspezifische Vorlagen:** Angriffsvorlagen sind für bestimmte Branchen oder Abteilungen verfügbar.



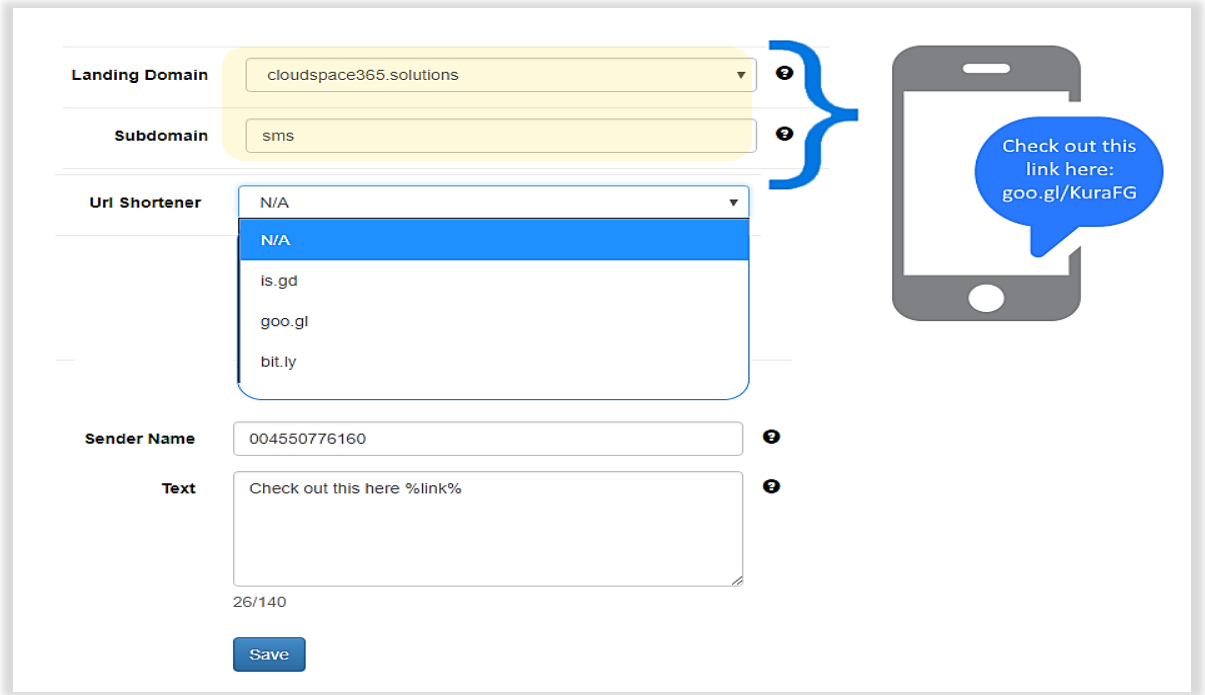
- **Gleichzeitige Verwendung von Angriffsvorlagen:** Mit LUCY können Sie mehrere simulierte Angriffsvorlagen in einer einzigen Kampagne verwenden. Mischen Sie die verschiedenen Typen (Hyperlink, dateibasiert, usw.) mit verschiedenen Angriffsthemen, um eine größtmögliche Risikoabdeckung und eine bessere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



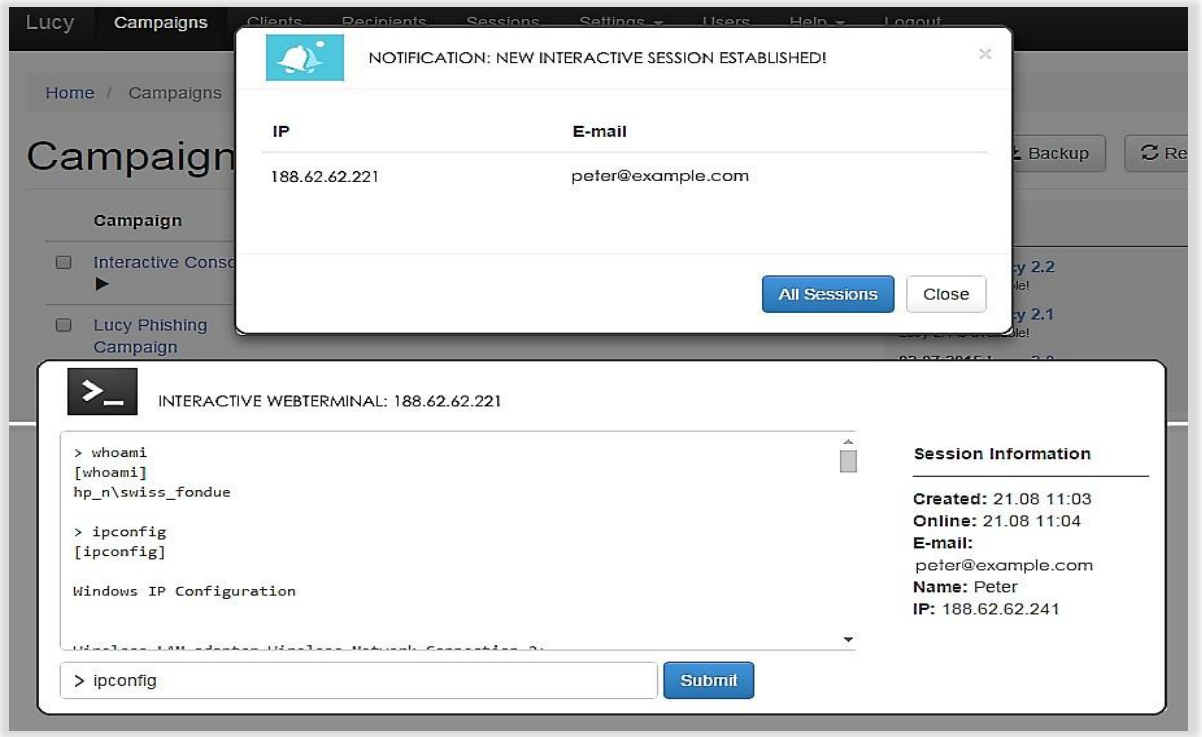
- **Variationen von Angriffs-URLs:** Übernehmen Sie die Kontrolle über die generierten URLs, um die Empfänger zu identifizieren. Verwenden Sie automatisierte kurze (<5 Zeichen) oder lange URL-Zeichenfolgen oder legen Sie für jeden Benutzer individuelle URLs fest. Mit der manuellen URL-Erstellung können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



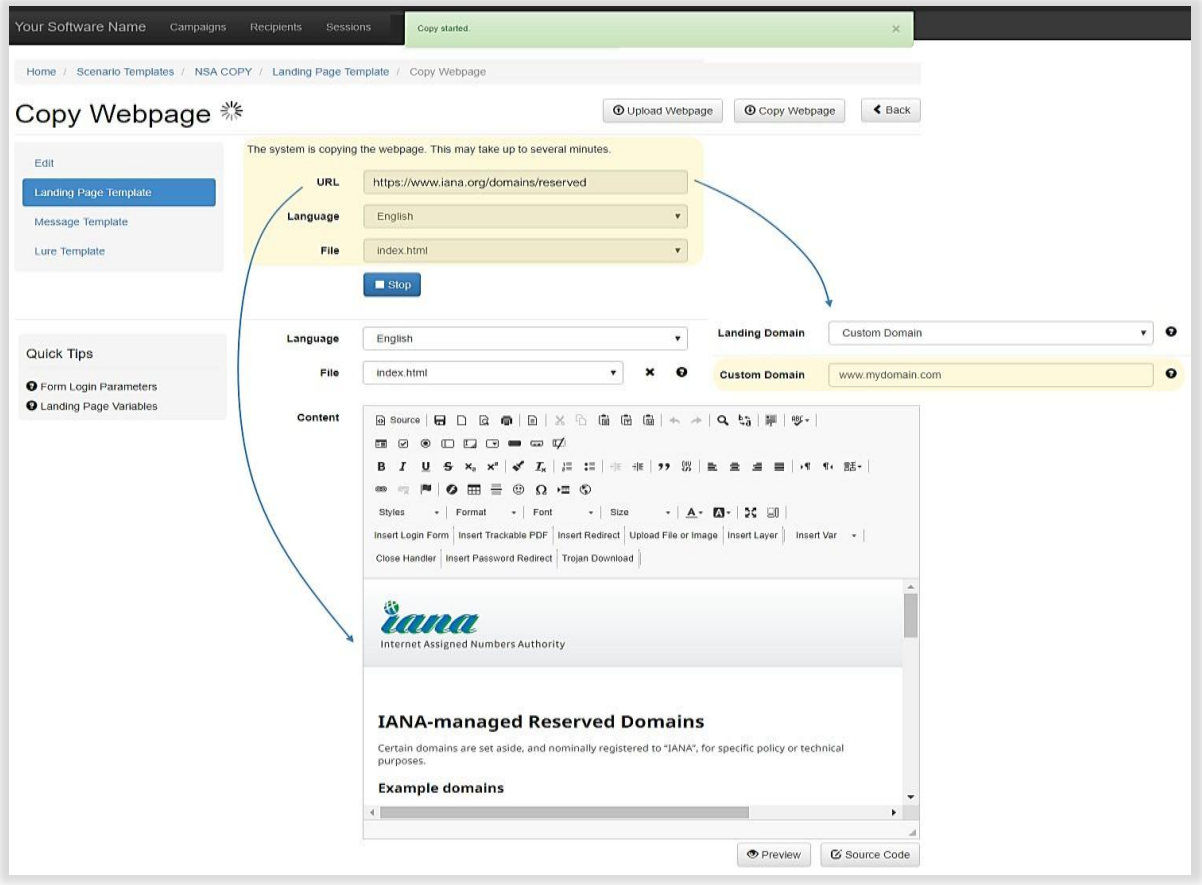
- **URL-Verkürzung:** URL-Verkürzungen sind ein relativ neuer Internetdienst. Da viele soziale Online-Dienste Zeichenbeschränkungen auferlegen (z. B. Twitter), sind diese URLs sehr praktisch. URL-Verkürzungen können jedoch von Cyberkriminellen verwendet werden, um das eigentliche Ziel eines Links zu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



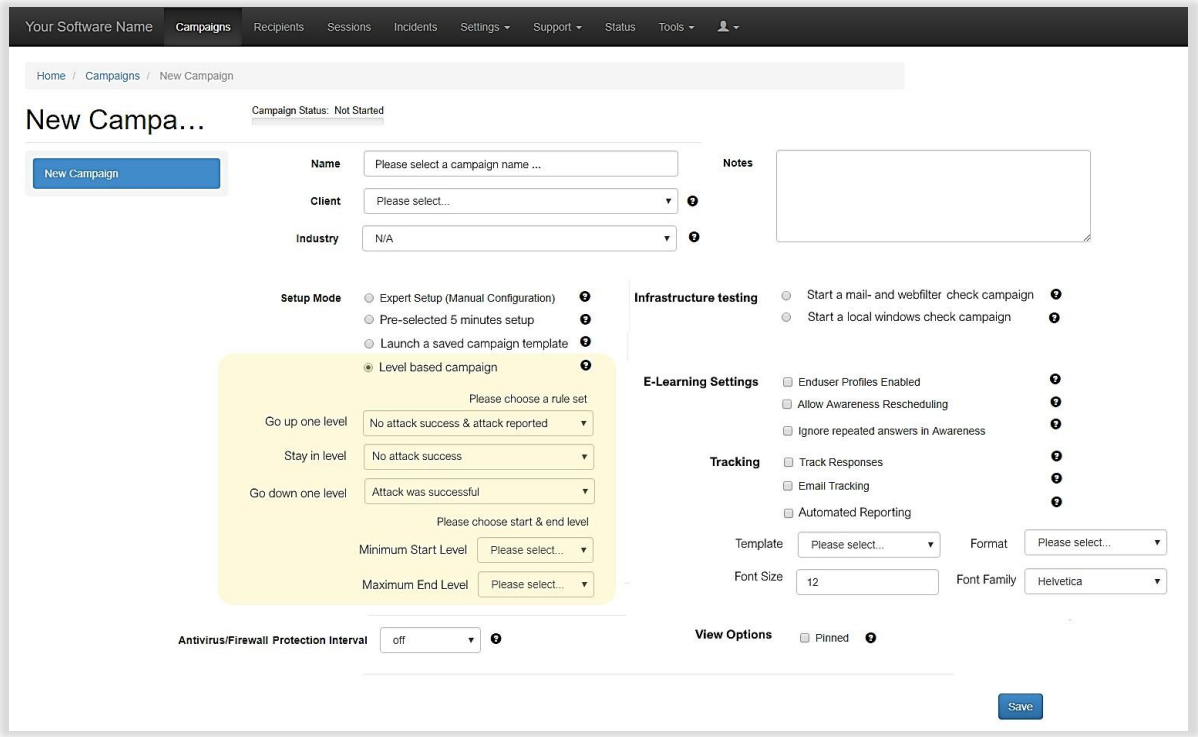
- **Pentest-Kit:** Das Pentest-Kit ist ein Submodul des Malware-Simulations-Toolkits und trägt den Namen „Interaktive Sitzungen“. Sie können interaktiv mit einem Client-PC kommunizieren, der sich hinter einer Firewall befindet, indem Sie umgekehrte https-Verbindungen verwenden.



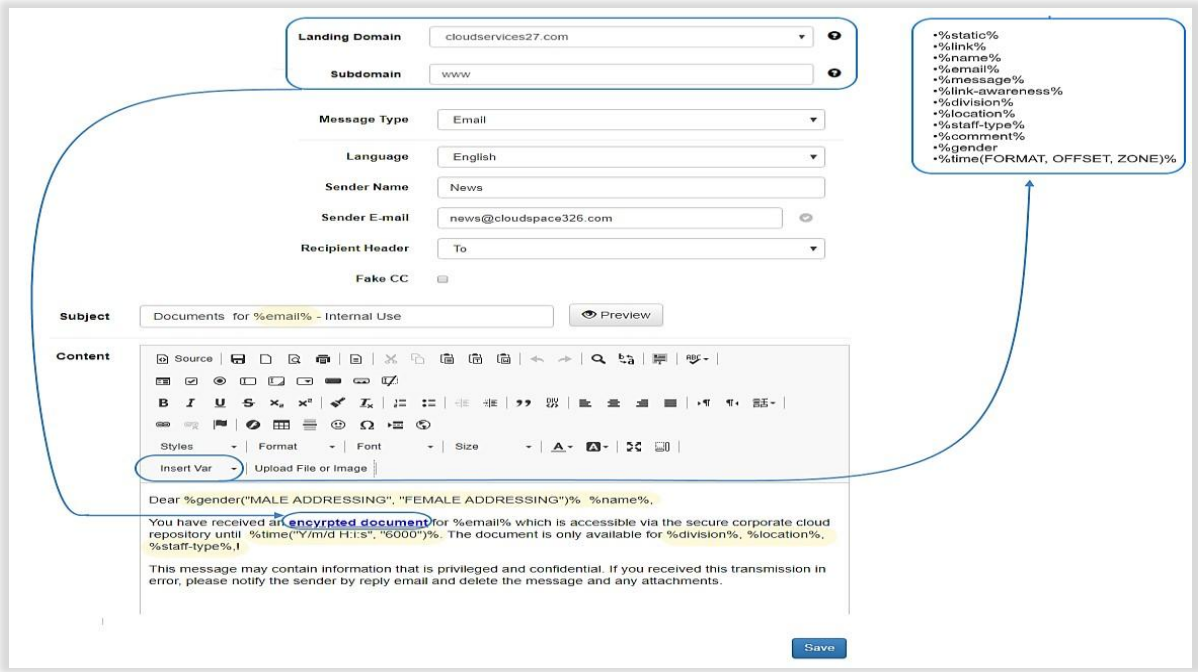
- **Webseiten-Kloner:** Erstellen Sie schnell hochprofessionelle Zielseiten für Ihre Kampagnen. Klonen Sie vorhandene Websites und fügen Sie zusätzliche Ebenen mit Dateneingabefeldern, Dateien zum Herunterladen und mehr hinzu.



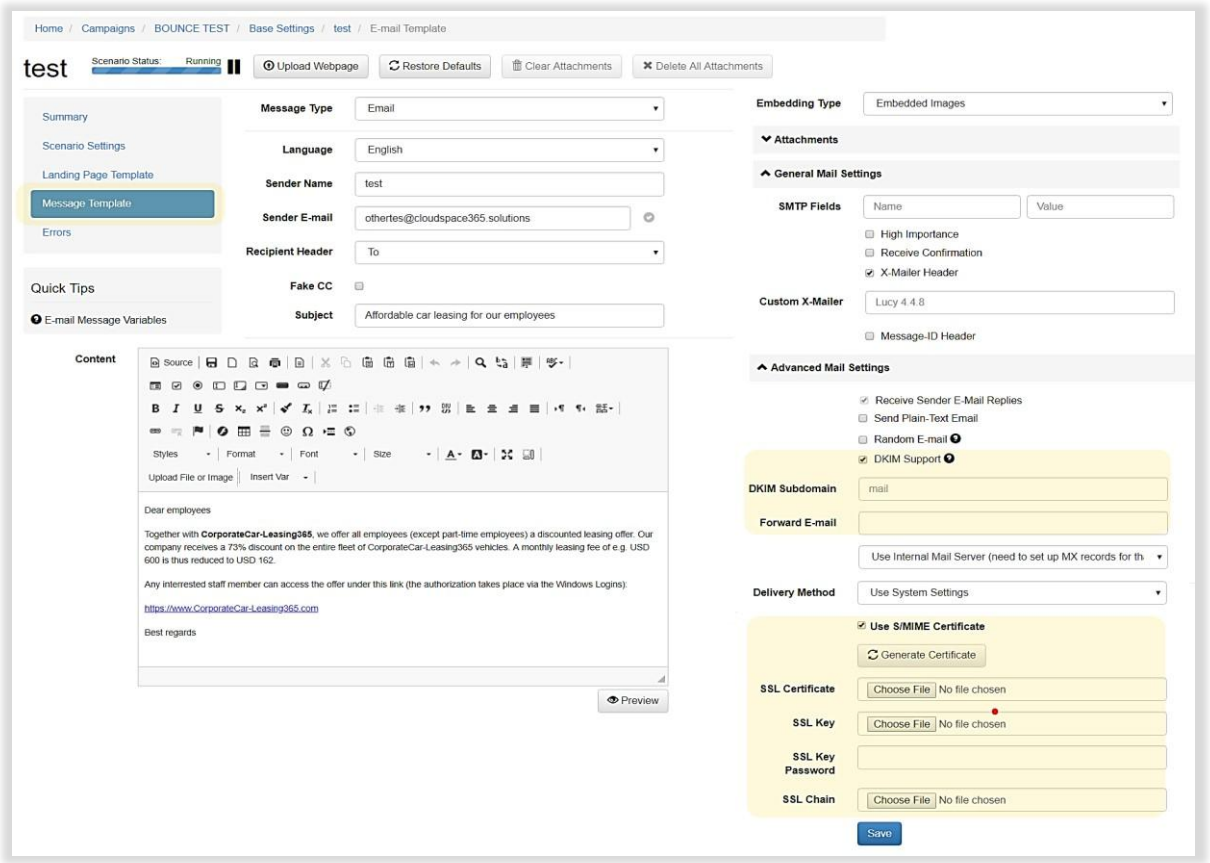
- **Level-basierte Angriffe:** Level-basiertes Phishing-Training für Mitarbeiter dient dazu, das Risiko von Social Hacking messbar zu machen. Die wissenschaftliche Analyse sollte auch die wichtigsten Risikofaktoren identifizieren, damit einzelne Schulungsinhalte automatisch angeboten werden können.



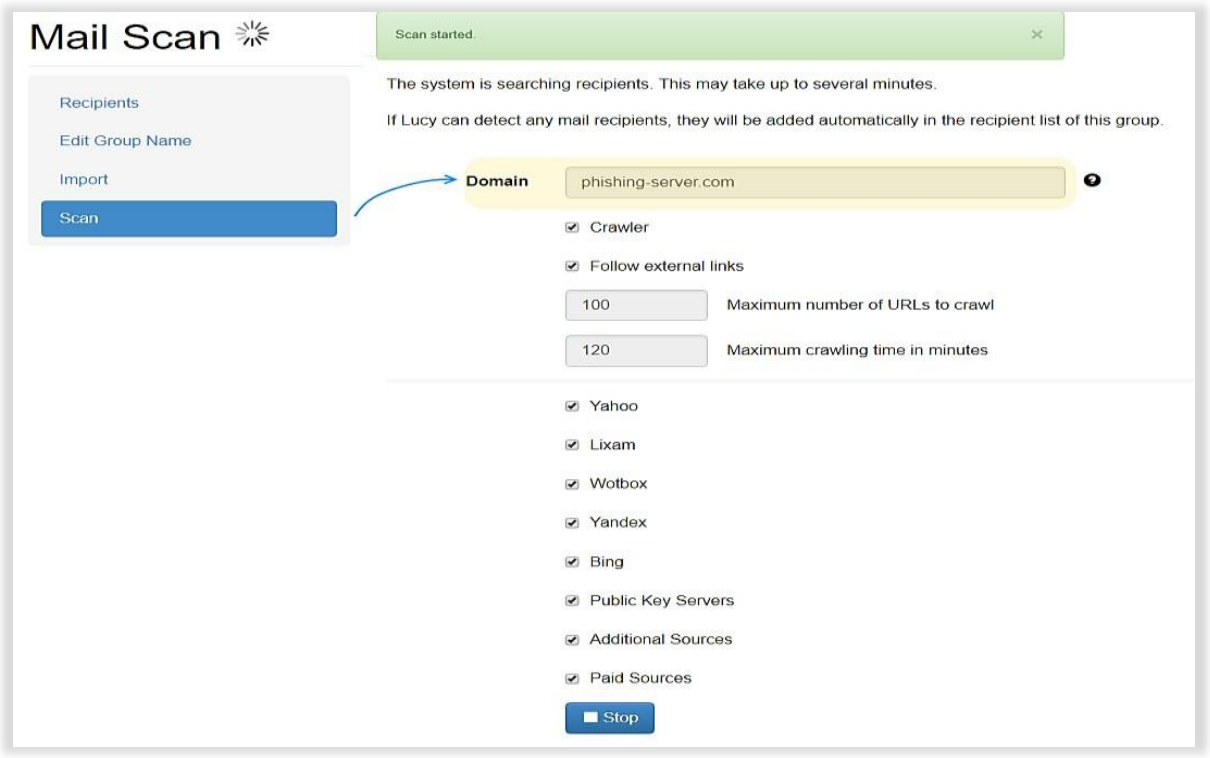
- **Spear-Phishing-Simulation:** Die Spear-Phishing-Anpassung funktioniert mit dynamischen Variablen (Name, Geschlecht, E-Mail, Zeit, Links, Nachrichten, Abteilungen, Land, usw.), die Sie in Landing-Page und Nachrichtenvorlagen verwenden können.



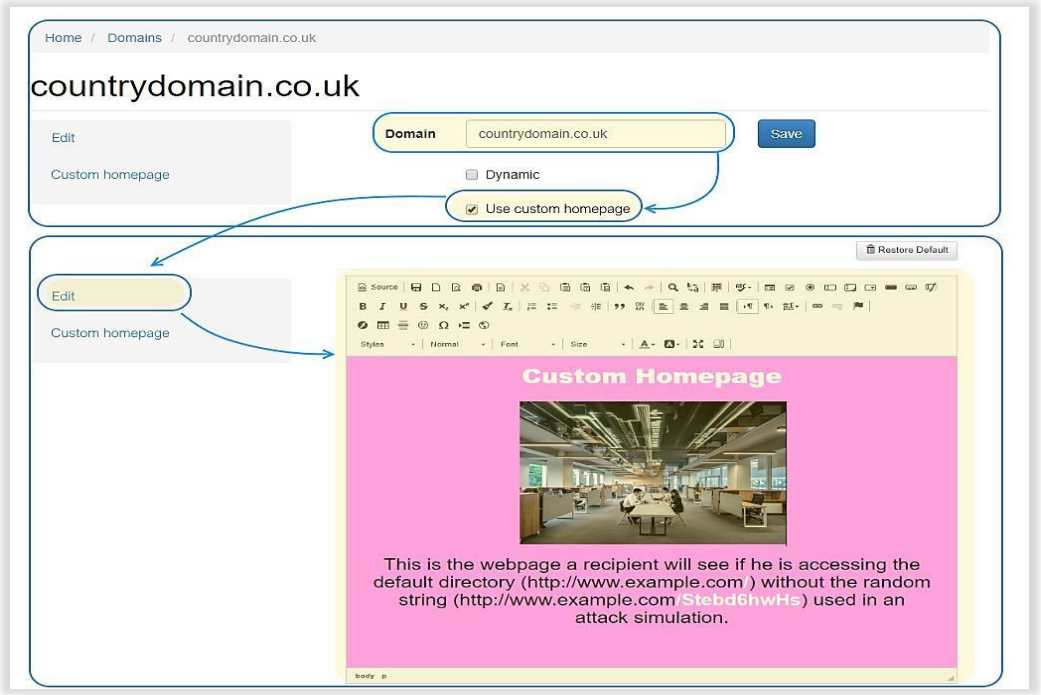
- **DKIM / S / MIME-Unterstützung für Phishing-E-Mails:** Digitale Signaturen für E-Mails: Senden Sie signierte Phishing-Simulations-Mails (S / Mime). Verwenden Sie DKIM, um eine bessere Absenderbewertung zu erhalten.



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

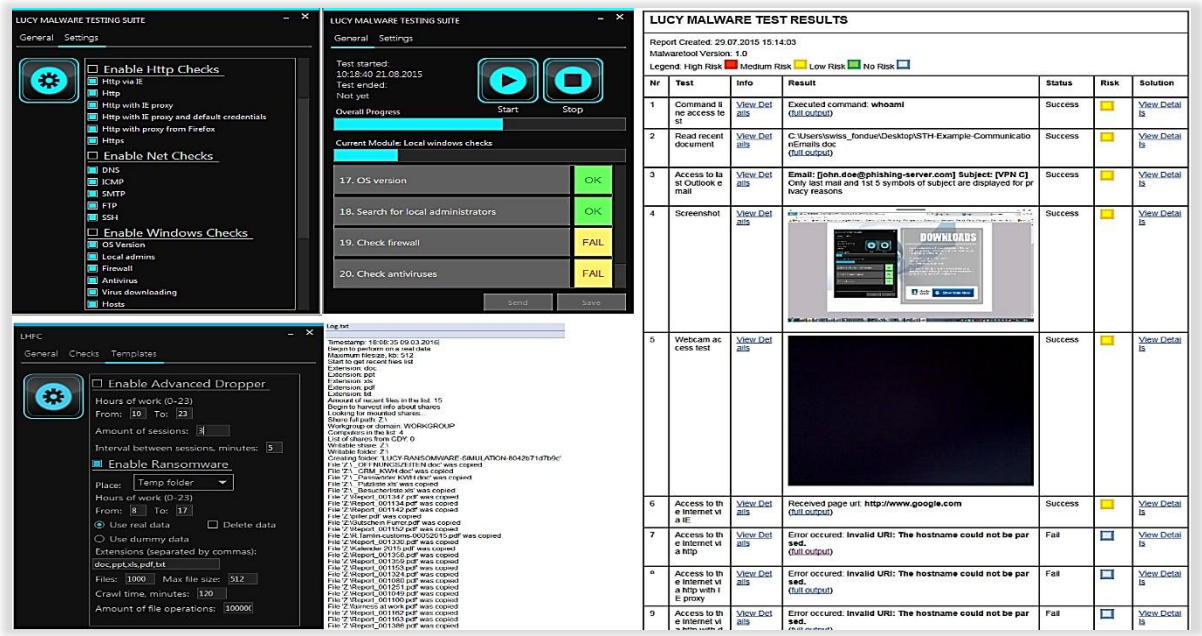


- **Benutzerdefinierte Homepage-Erstellung:** Empfänger mit einem besseren technischen Verständnis können in ihrem Browser die Domain oder IP-Adresse aufrufen, die dem zufällig generierten Phishing-Link zugeordnet ist. Um zu verhindern, dass Fehlermeldungen angezeigt werden oder der Endbenutzer überhaupt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

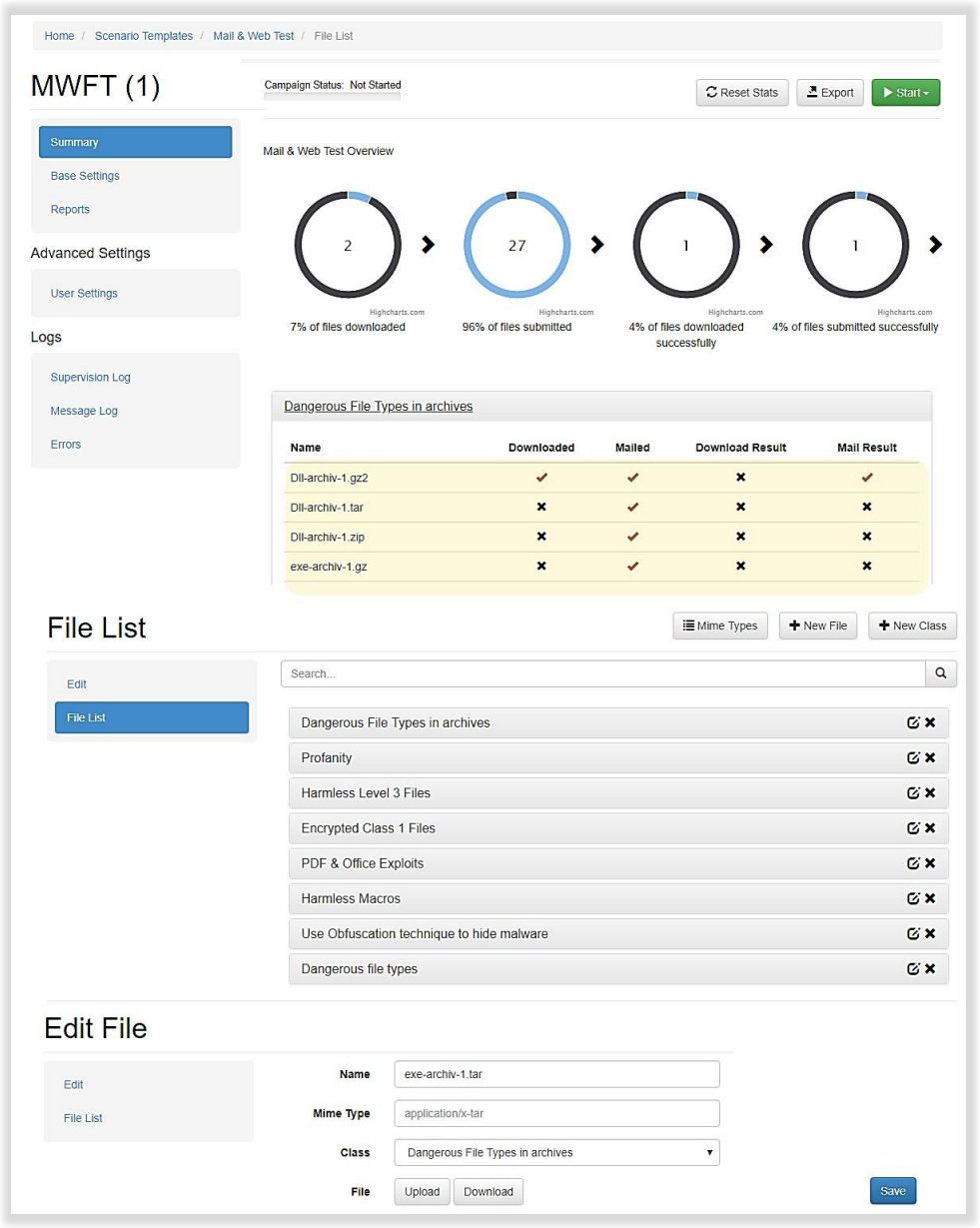


INFRASTRUKTUR-TEST

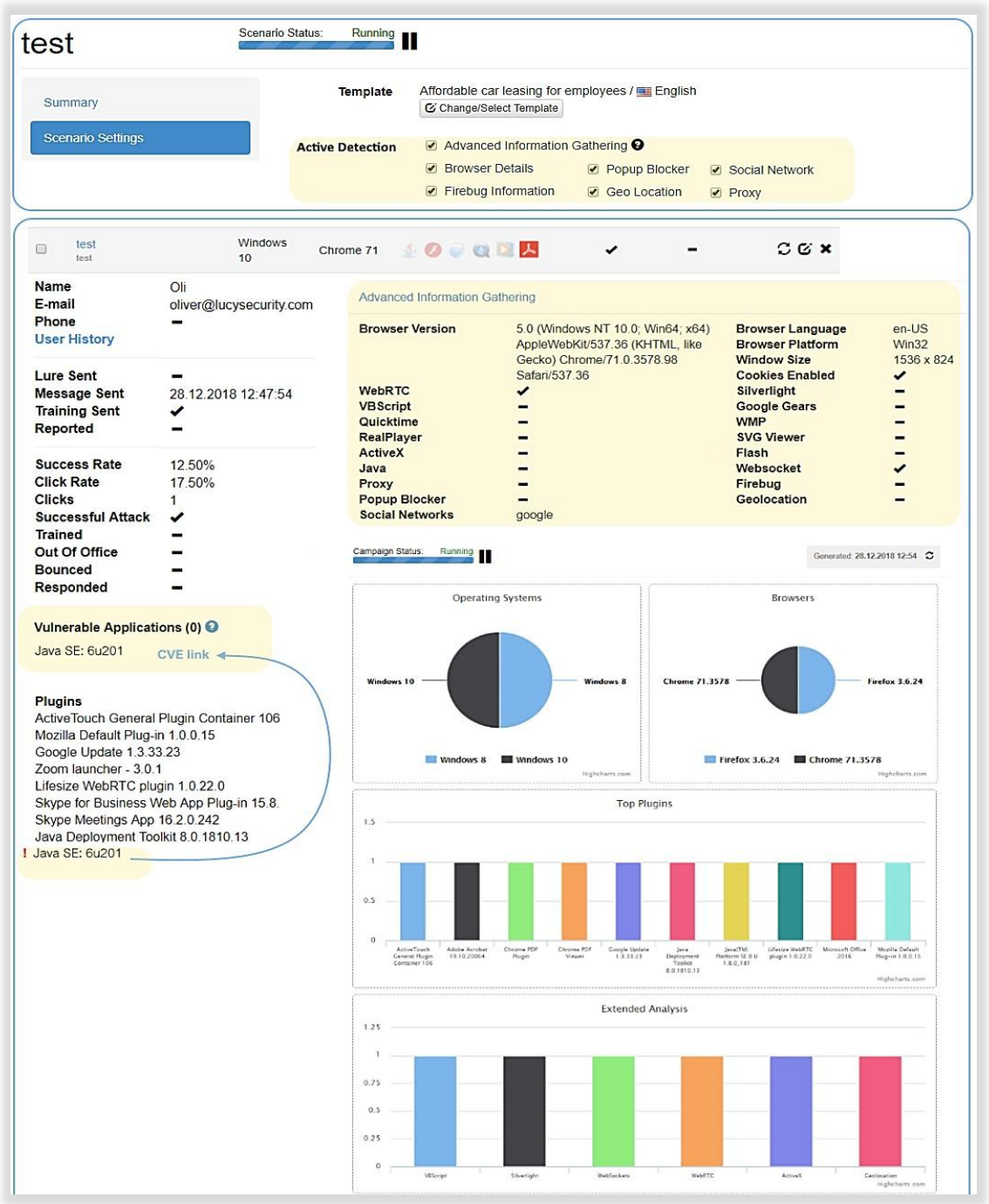
- **Malware Testing Toolkit:** Das Malware-Simulation-Toolkit ist eine erweiterte Malware-Simulationssuite, die verschiedene Bedrohungen nachbilden kann. Es ermöglicht einem Auditor den Zugriff auf eine Reihe erweiterter Funktionen, die vielen der von Cyberkriminellen verwendeten Tools entsprechen. Das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



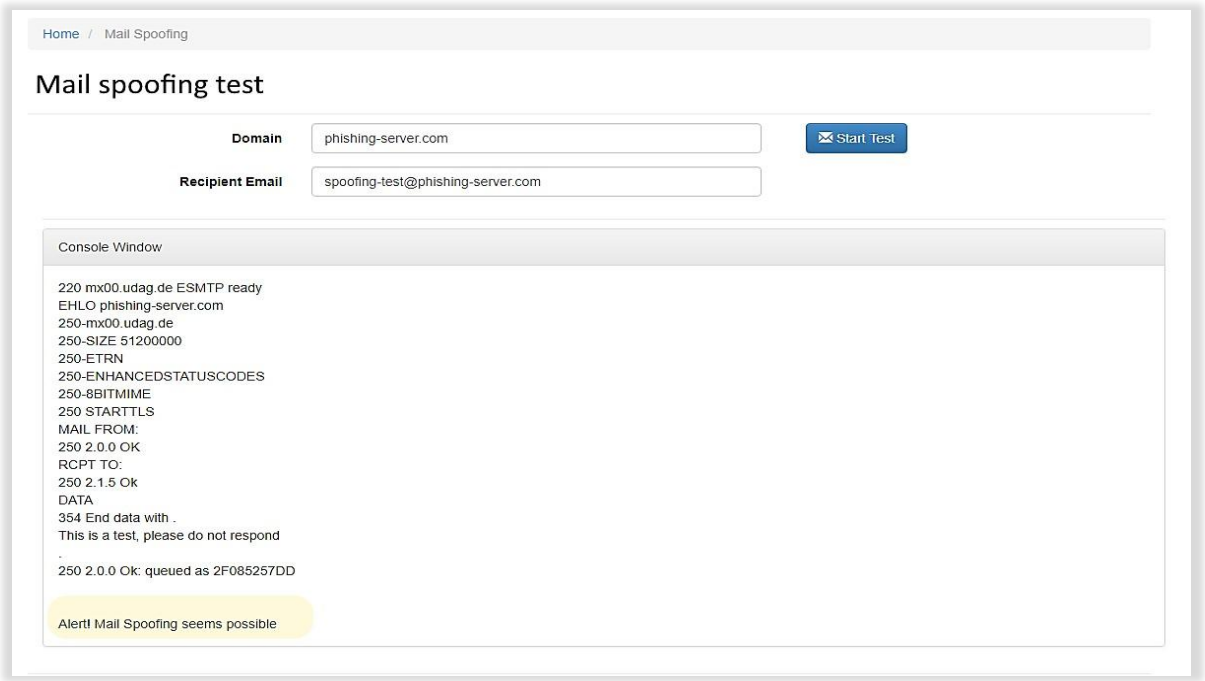
- **E-Mail- und Webfiltertest:** Diese Funktion bietet die Antwort auf eine der wichtigsten Fragen zur Sicherung des Internet- und E-Mailverkehrs: Welche Dateitypen aus dem Web können heruntergeladen werden und welche E-Mail-Anhänge werden herausgefiltert und welche nicht?



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

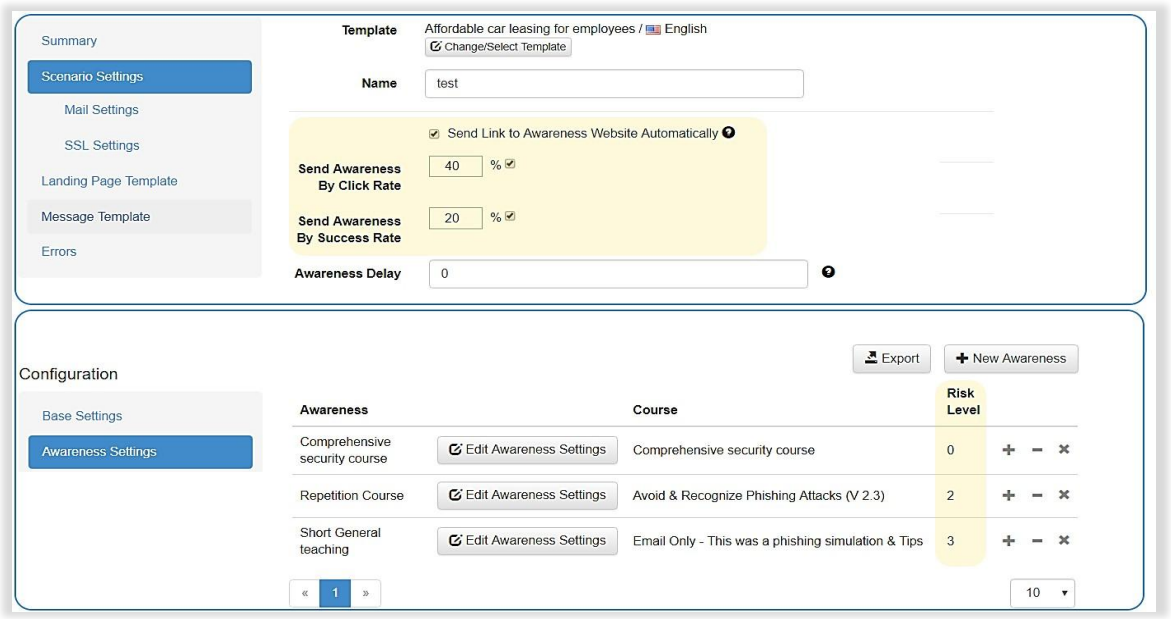


- **Spoofing-Test:** Testen Sie Ihre eigene Infrastruktur auf E-Mail-Spoofing-Schwachstellen.

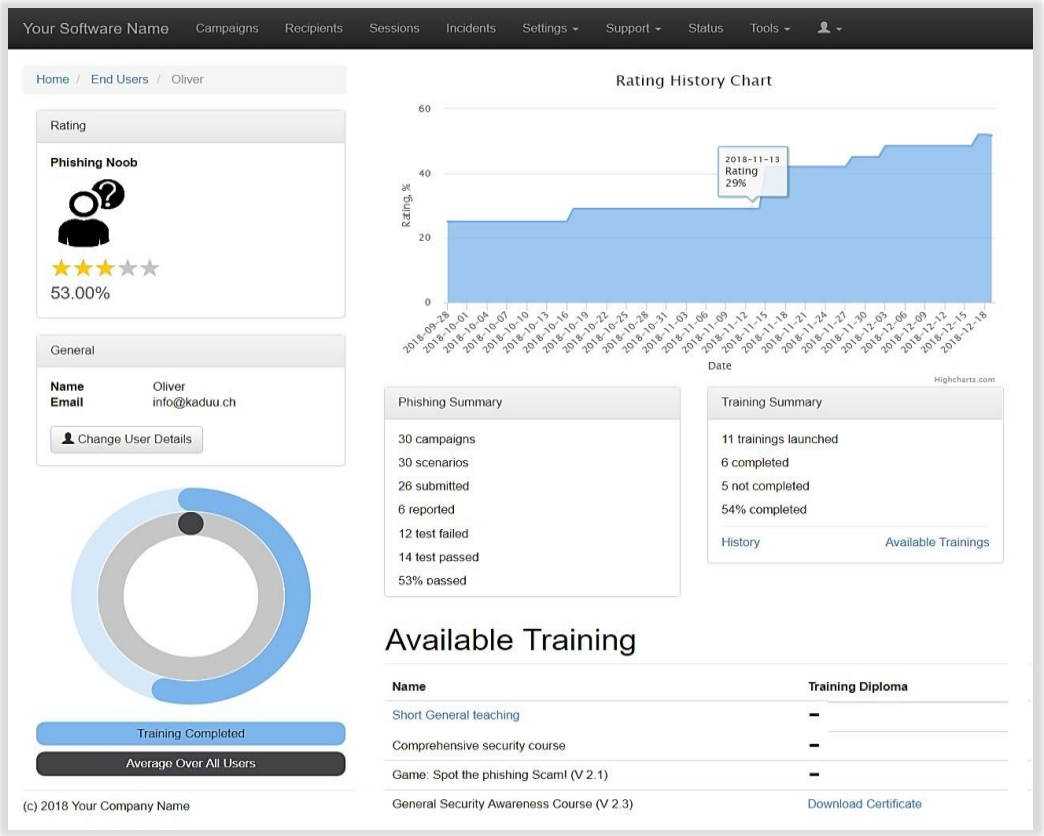


TECHNISCHE TESTS

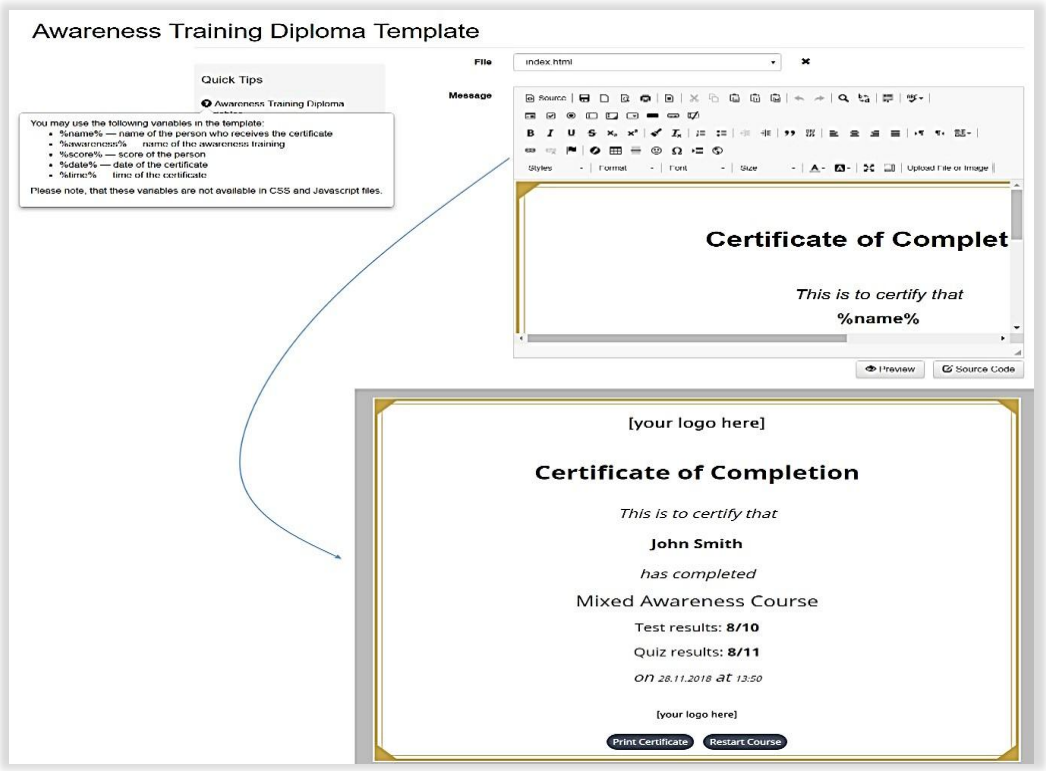
- **Reputationsbasiertes E-Learning:** Schulen Sie Ihre Mitarbeiter, den gebotenen Anforderungen entsprechend. Bewerten Sie die Fähigkeiten der Mitarbeiter und ermöglichen Sie einen gesunden Wettbewerb zwischen den Kollegen (Gamification). Basierend auf den Reputationsprofilen jedes Benutzers kann das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



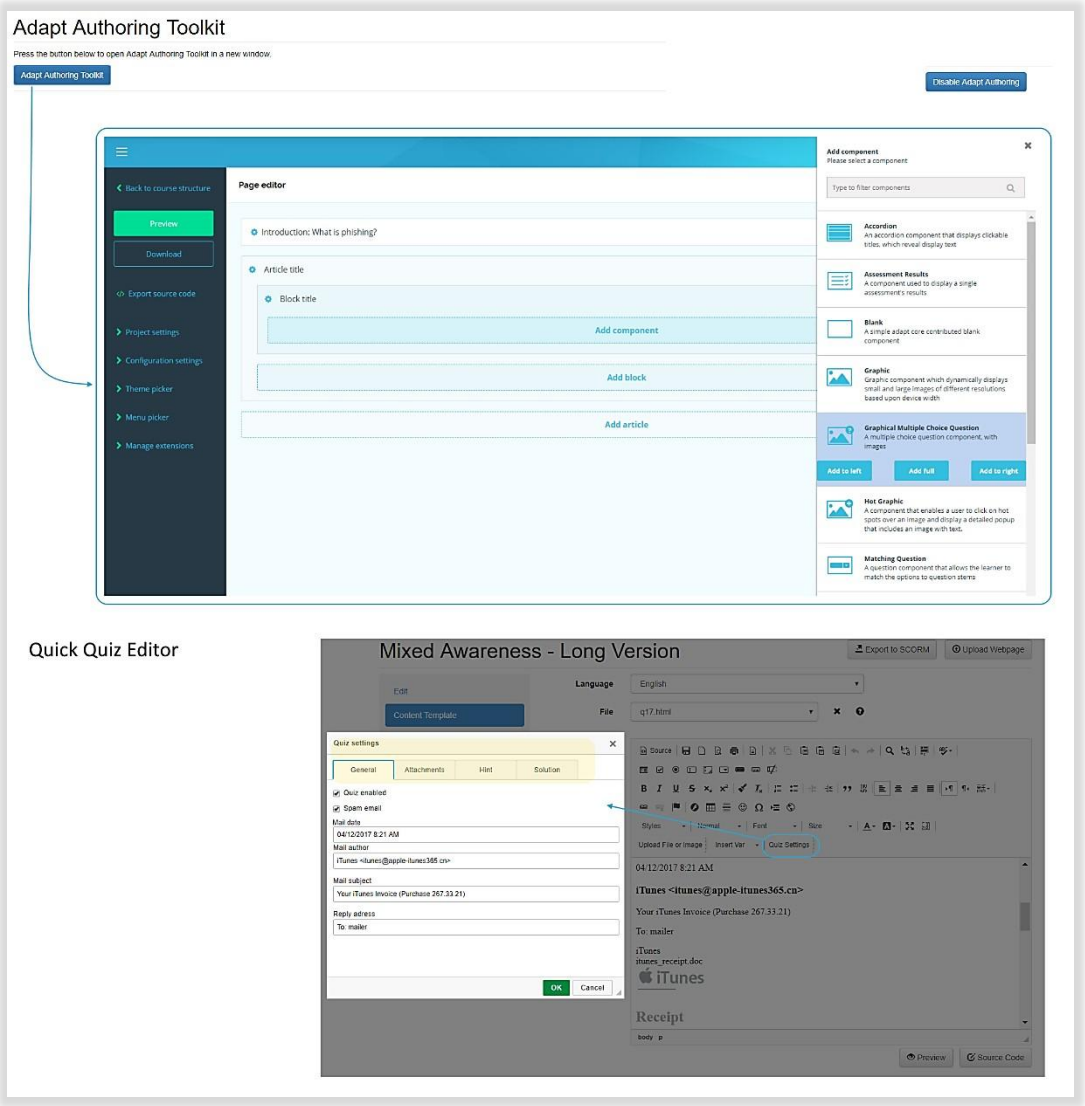
- **Endbenutzer-Schulungsportal:** LMS-Funktionalität (Learning Management System): Ermöglicht jedem Mitarbeiter permanenten Zugriff auf eine personalisierte Schulungshomepage, auf der eigene Kurse speziell auf ihn zugeschnitten sind. Auf dieser Homepage können Leistungsstatistiken angezeigt werden,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



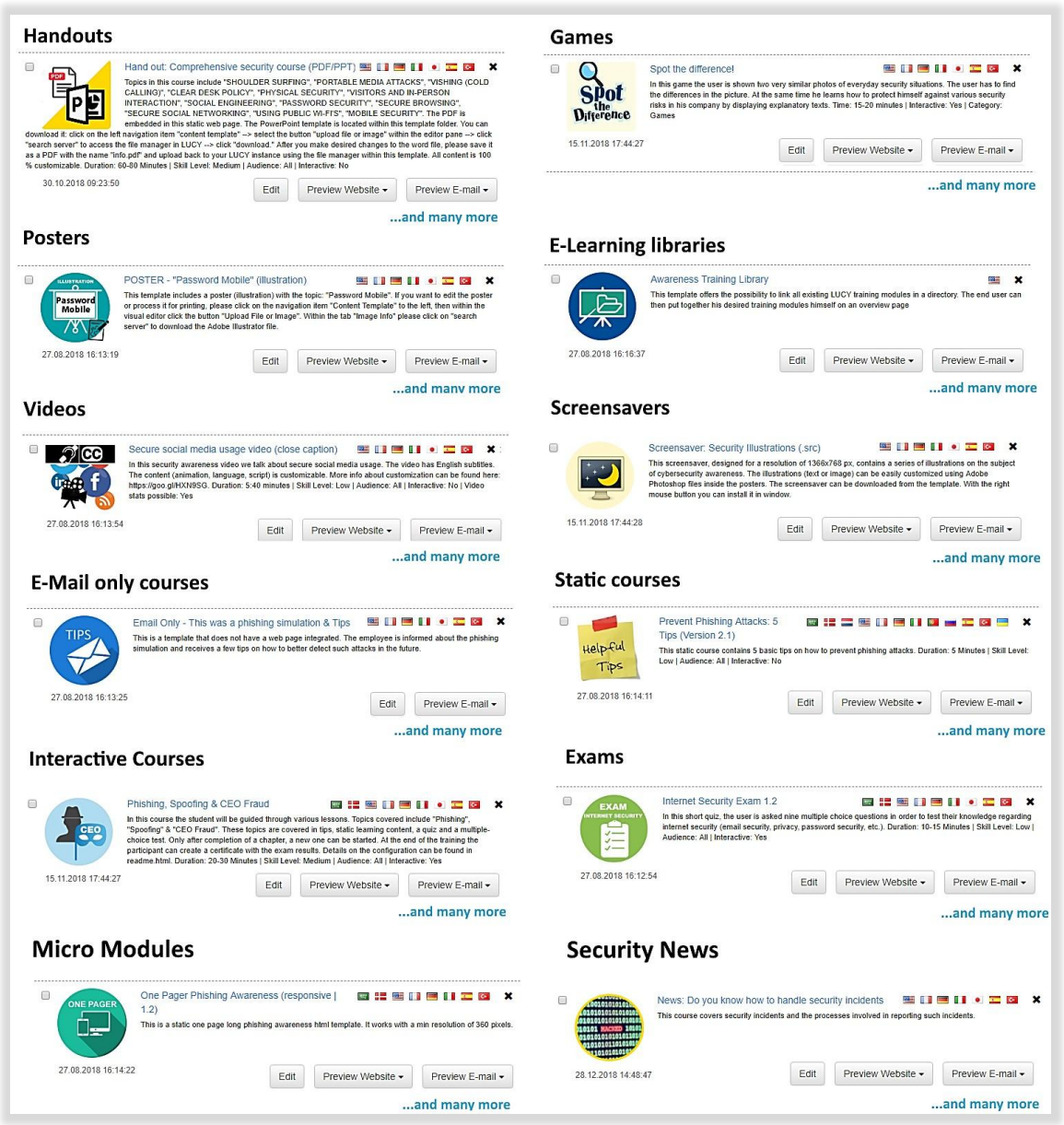
- **Fortbildungsdiplom Sicherheitsbewusstsein:** E-Learning-Zertifikate können vom Berechtigten entweder direkt im Rahmen einer Schulung oder im LMS-Portal erstellt und ausgedruckt werden.



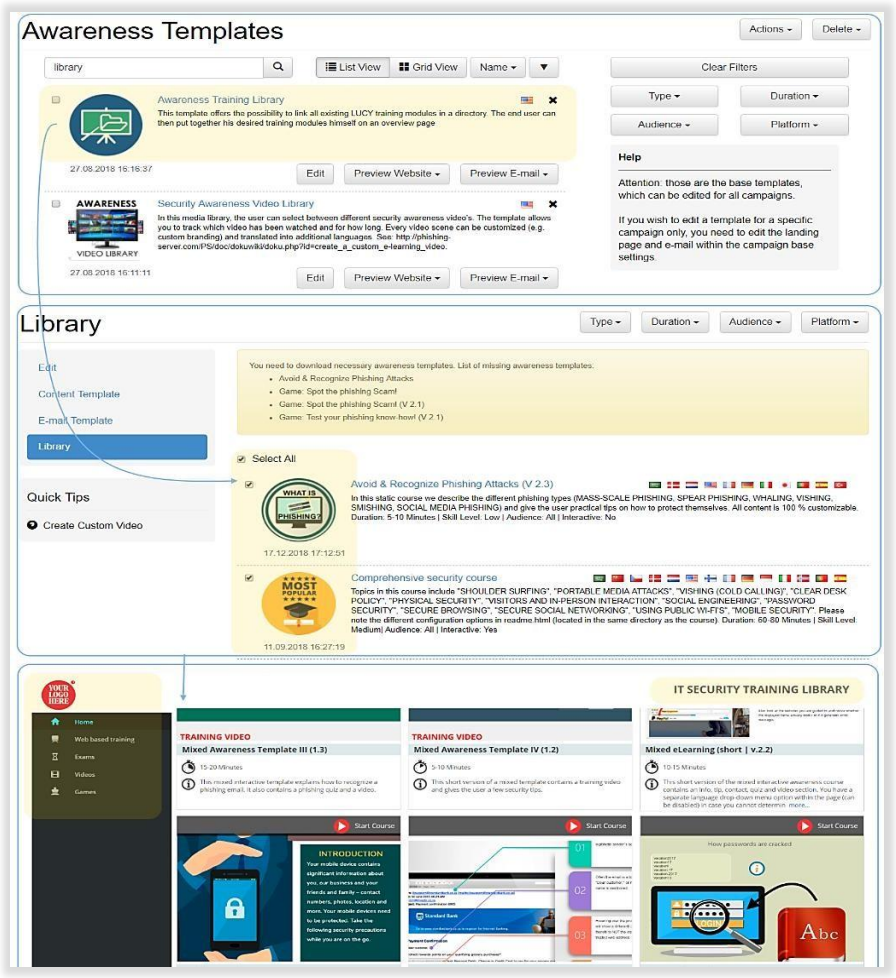
- **E-Learning-Authoring-Toolkit:** Das E-Learning-Authoring-Toolkit (Adapt) ermöglicht die Erstellung individueller Lerninhalte. Ziehen Sie Videos oder andere Rich Media-Formate per „Drag und Drop“ an die gewünschte Stelle, fügen Sie Tests aus vordefinierten Menüs ein und erstellen Sie in kürzester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



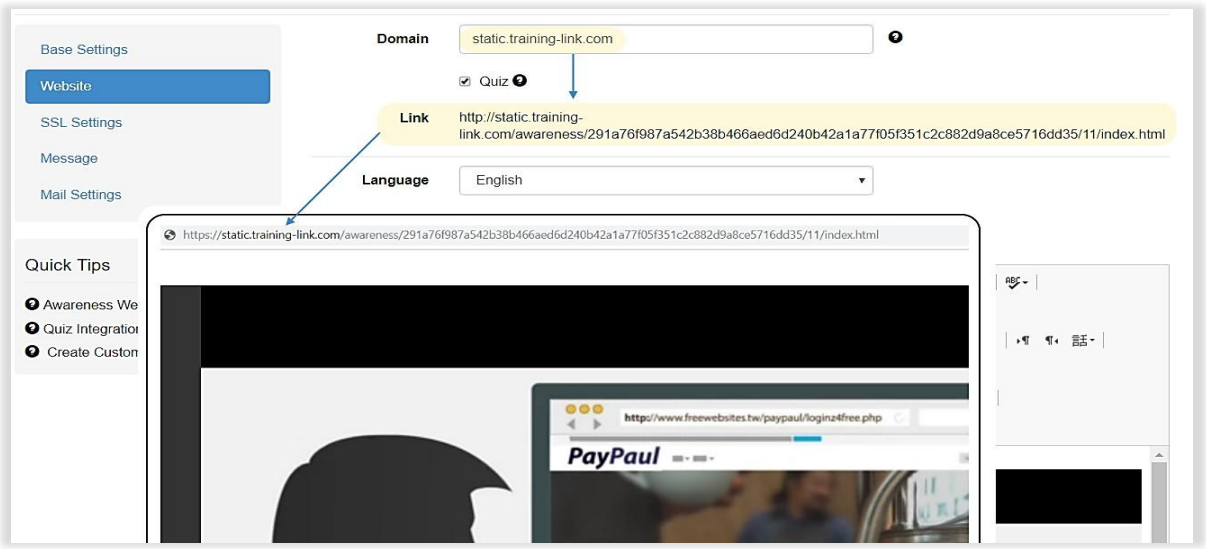
- **Rich Media-Sensibilisierungstraining:** Integrieren Sie Rich Media (Video, Audio oder andere Elemente, welche den Zuseher zur Interaktion ermuntert und ihn mit dem Inhalt „fesselt“) in Ihre Sensibilisierungstrainings. Verwenden Sie die vorhandenen Lernvideos, passen Sie sie an oder fügen Sie Ihre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



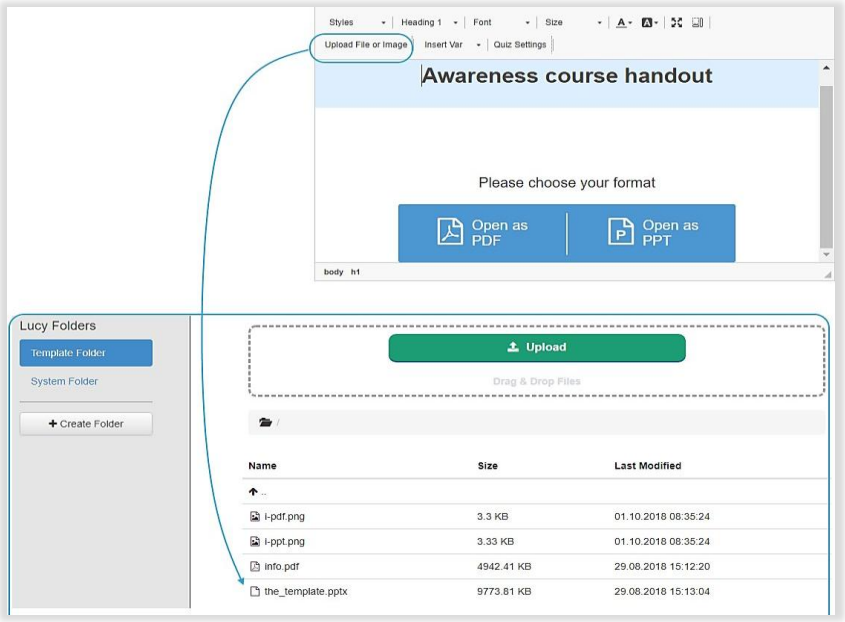
- **Schulungsbibliothek:** Ihre Mitarbeiter können über eine Übersichtsseite mit dem Namen „Schulungsbibliothek“ auf die Schulungsinhalte Ihres Unternehmens zugreifen. Es enthält eine große Auswahl der regulären E-Learning-Vorlagen von LUCY, die als Eingabe dienen. Die Übersichtsseite kann nach bestimmten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



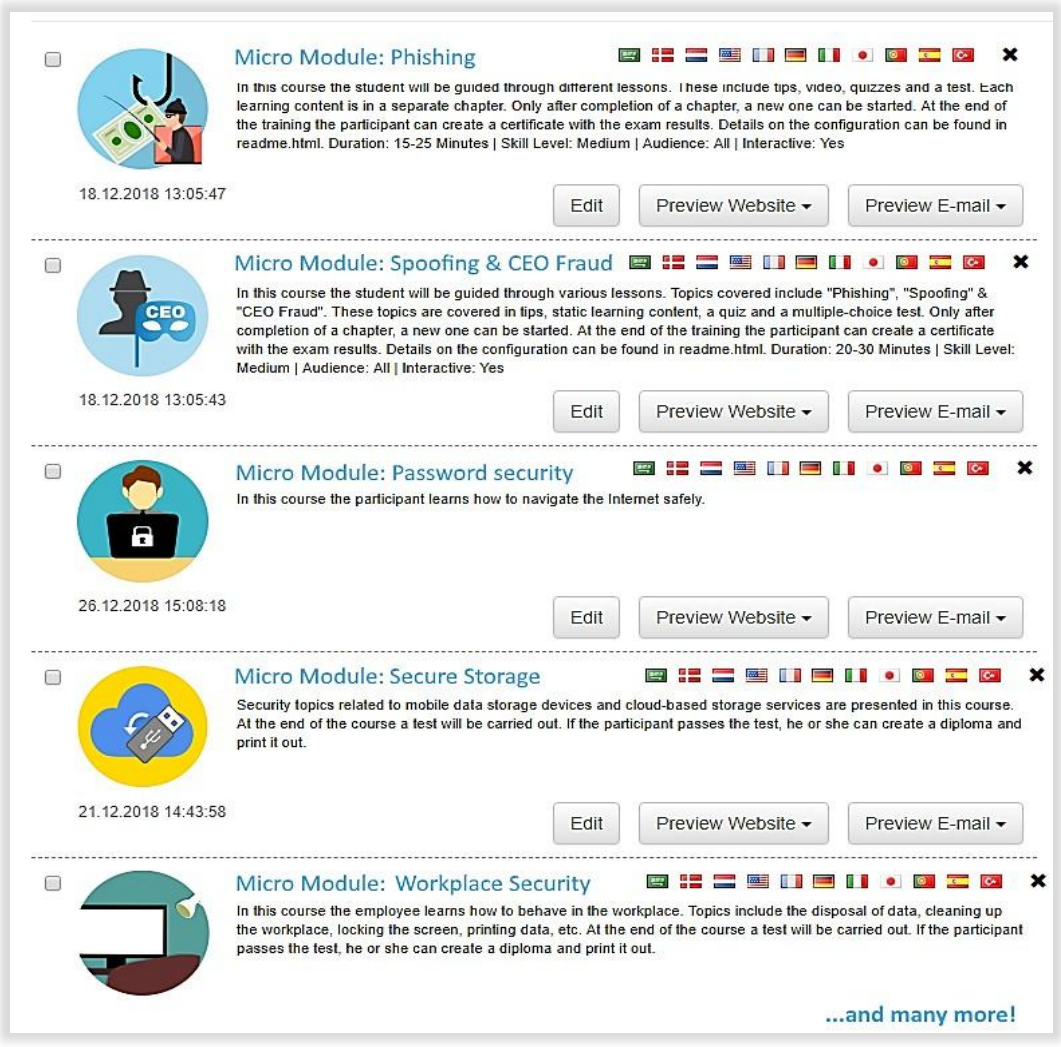
- **Unterstützung für statische Schulungen:** Schulungsinhalte können auch auf statischen Seiten in LUCY oder im Intranet veröffentlicht werden, sodass der Benutzer unabhängig von möglichen Angriffssimulationen permanent auf Schulungsinhalte zugreifen kann.



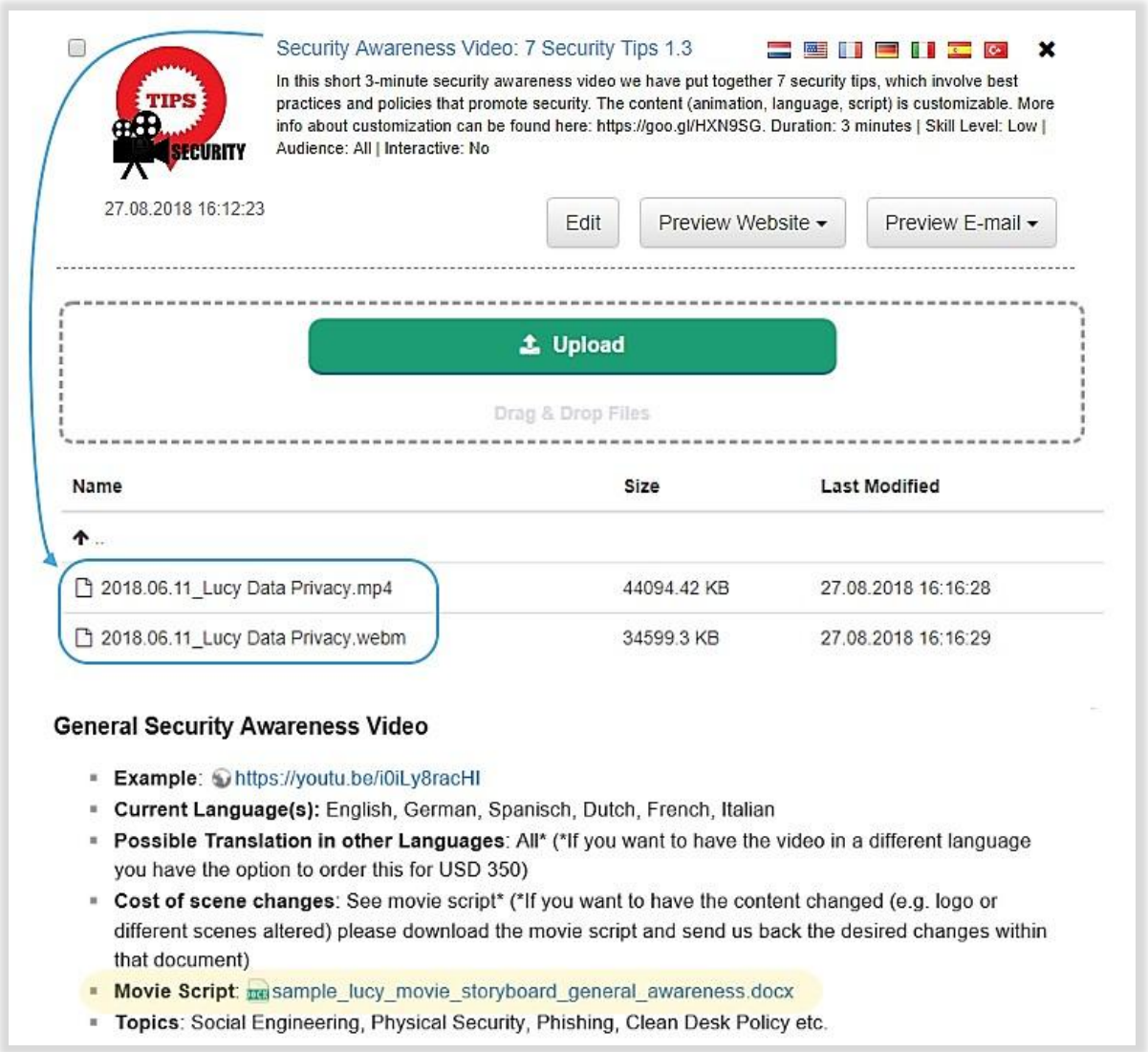
- **Schulungssupport offline:** LUCY bietet eine Reihe adaptierbarer Vorlagen (Adobe Photoshop oder Illustrator-Dateien) für Sensibilisierungs-Schulungen, wie Poster, Flyer, Bildschirmschoner, usw.



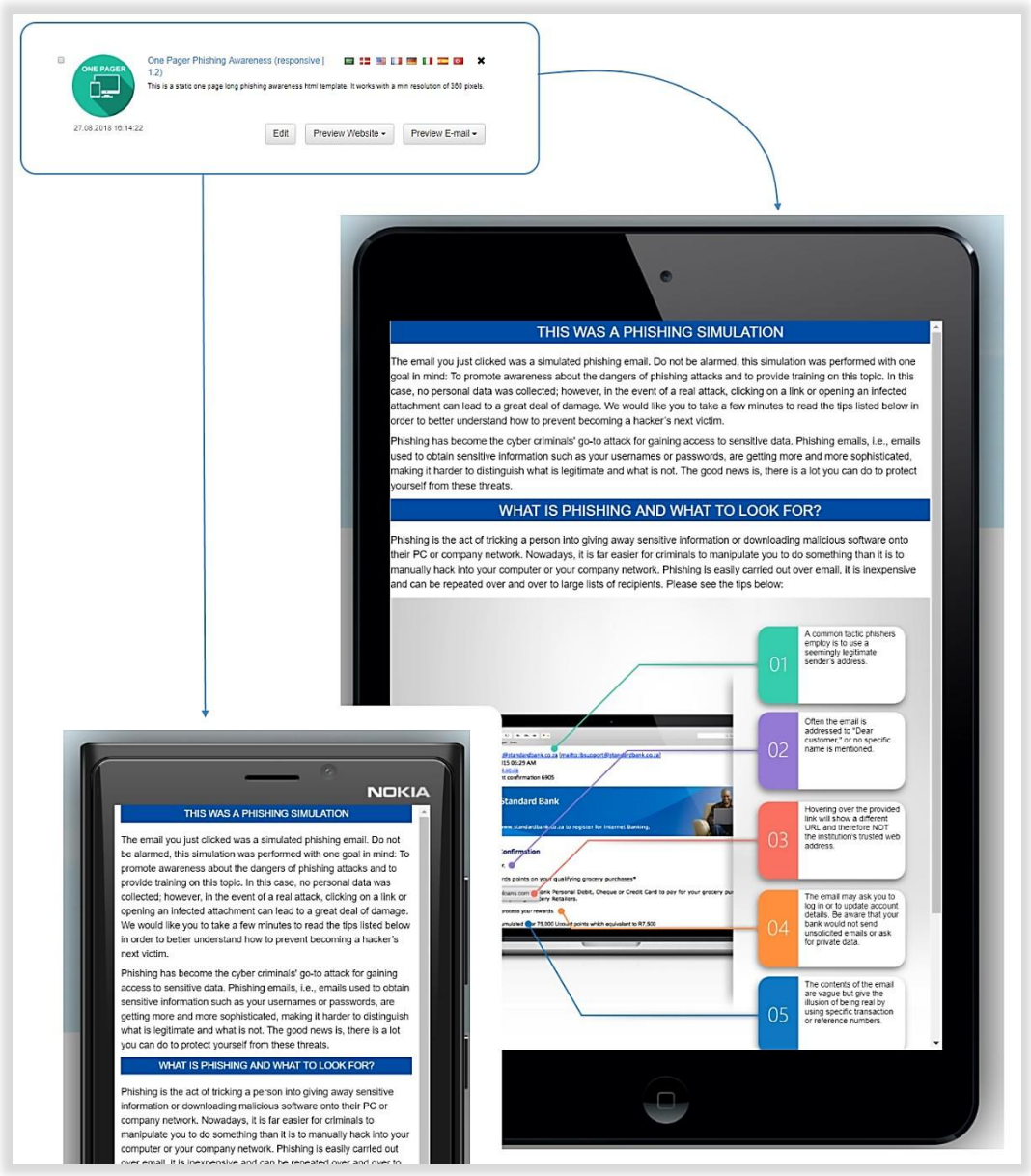
- **Microlearning-Module:** Wir haben Microlearning-Schulungsmodule (z. B. 1-minütige Videos oder 1-Seiten-Module zur Sicherheits-Sensibilisierung) entwickelt, die auf die Branding- und Richtlinienanforderungen Ihres Unternehmens zugeschnitten werden können.



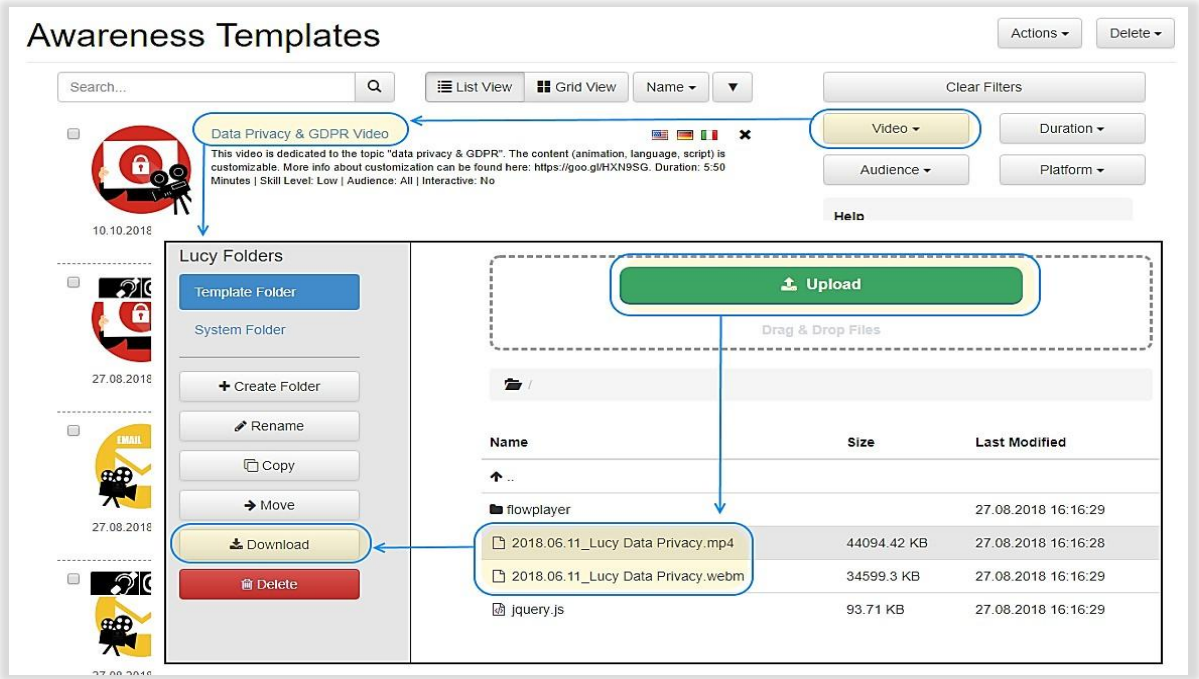
- **Videoanpassung:** Senden Sie uns Ihr Firmenlogo und wir integrieren es in die Schulungsvideos. Sie wünschen eine andere Sprache? Kein Problem. Wir passen das Video so an, dass es in der von Ihnen gewünschten Sprache läuft. Sie wünschen eine andere Szene? Laden Sie einfach die Videoskripte herunter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



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



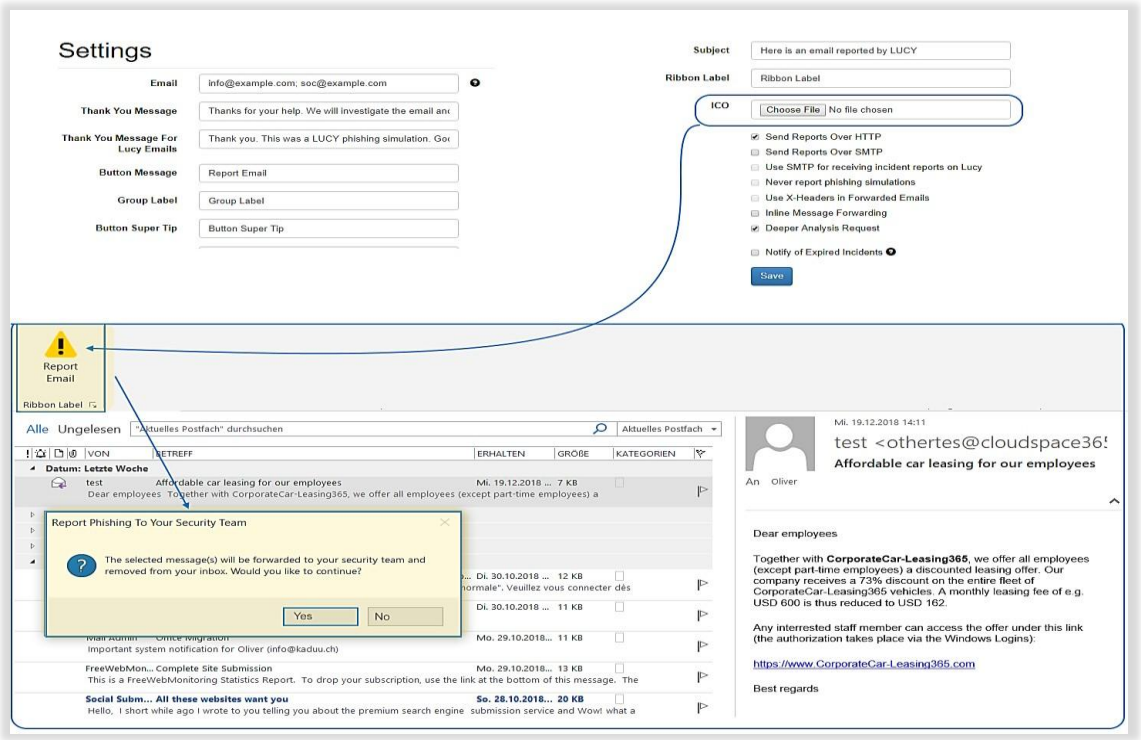
- **Videoimport / -export:** Sie können LUCY-Videos auf Ihr eigenes System exportieren sowie Ihre eigenen Videos in LUCY importieren.



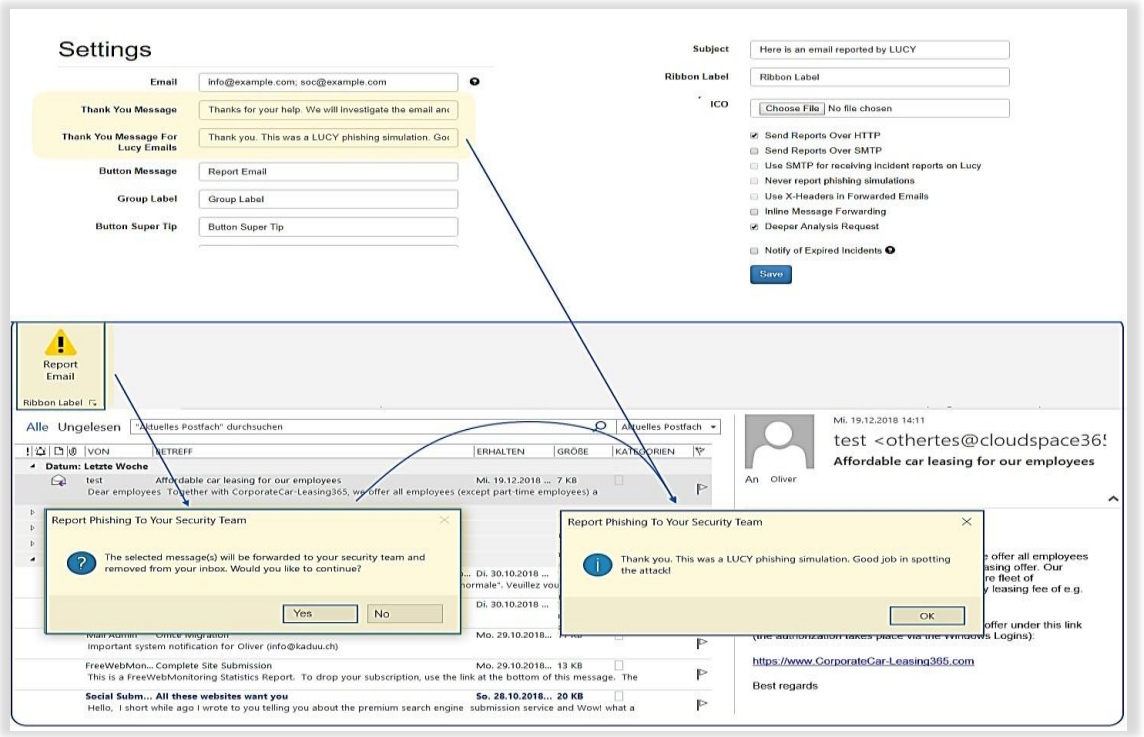
- **Dynamische Schulungshinweise:** Mit den implementierten dynamischen Hinweisen kann Ihr Administrator Markierungen an den Angriffsvorlagen setzen, die Ihren Mitarbeitern im E-Learning-Material anzeigen, wo der Phishing-Angriff möglicherweise erkannt wurde.

MITARBEITER MITEINBEZIEHEN

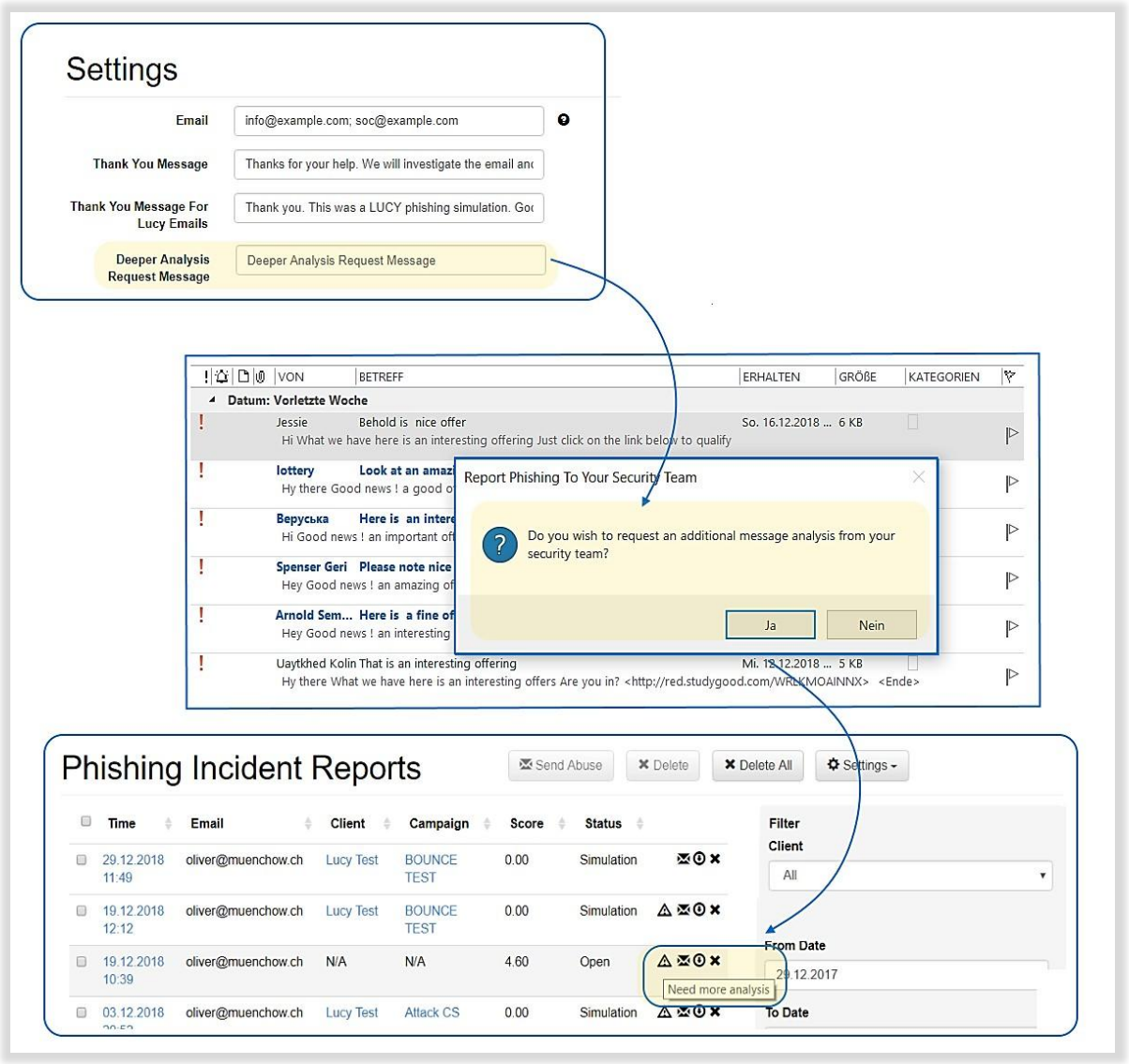
- **E-Mails mit einem einzigen Klick melden:** Benutzer können verdächtige E-Mails mit einem einzigen Klick an eine oder mehrere E-Mail-Adressen melden und an die LUCY-Vorfallsanalyse weiterleiten lassen.



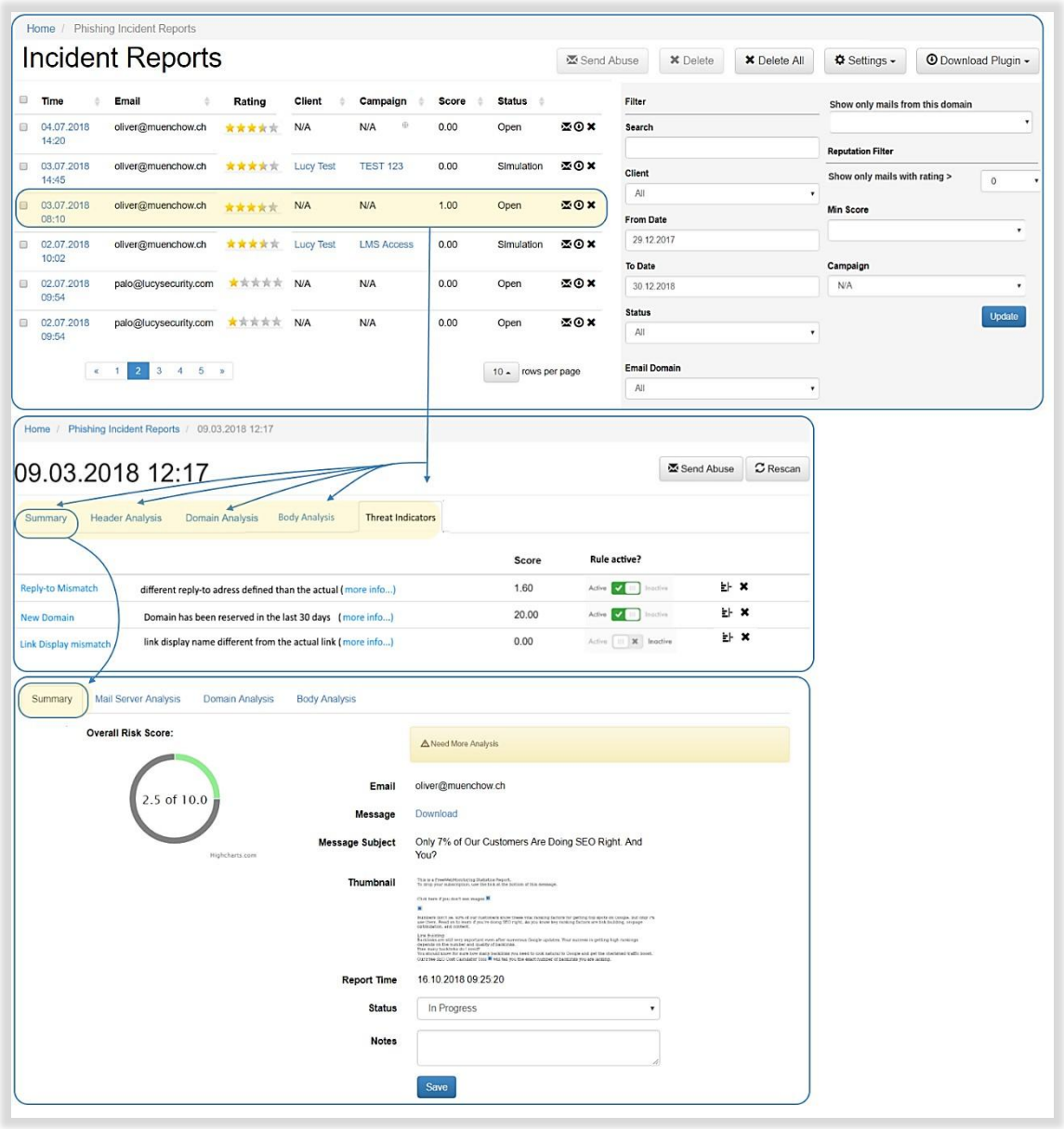
- **Bestärkung im richtigen Verhalten:** Unser Plug-in bietet automatisch eine Bestärkung des richtigen Verhaltens, indem es dem Benutzer mittels einer Nachricht aus Ihrem Unternehmen entsprechende Dankbarkeit ausdrückt.



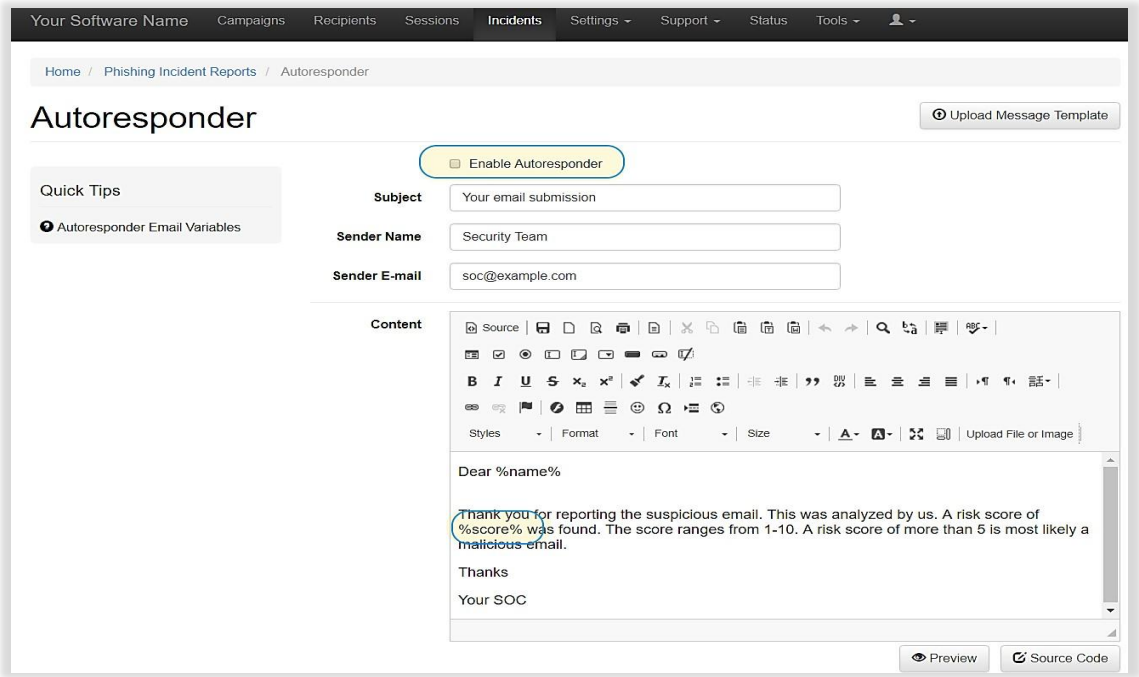
- **Deep Inspection Request:** Manchmal möchten Benutzer wissen, ob die empfangene E-Mail sicher geöffnet werden kann. Der Benutzer kann optional den sog. „Deep Inspection Request“ im lokalen Plug-in verwenden, um dem Sicherheitsteam mitzuteilen, dass er Feedback zu der gemeldeten E-Mail erhalten möchte.



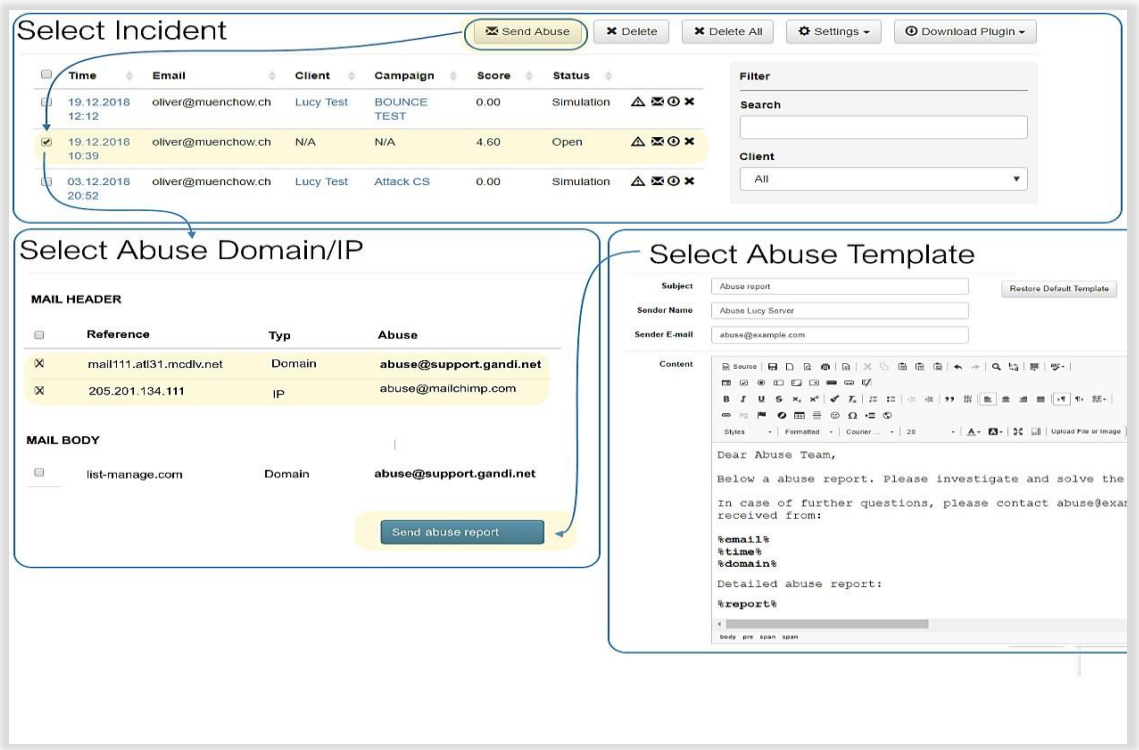
- **Automatische Vorfallsanalyse:** Verwalten und Reagieren auf gemeldete verdächtige E-Mails über eine zentrale Verwaltungskonsole: Die LUCY-Analyse ermöglicht eine automatische Überprüfung der gemeldeten Nachrichten (Header und Text) und enthält eine individuelle Risikobewertung, die ein Echtzeit-Ranking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



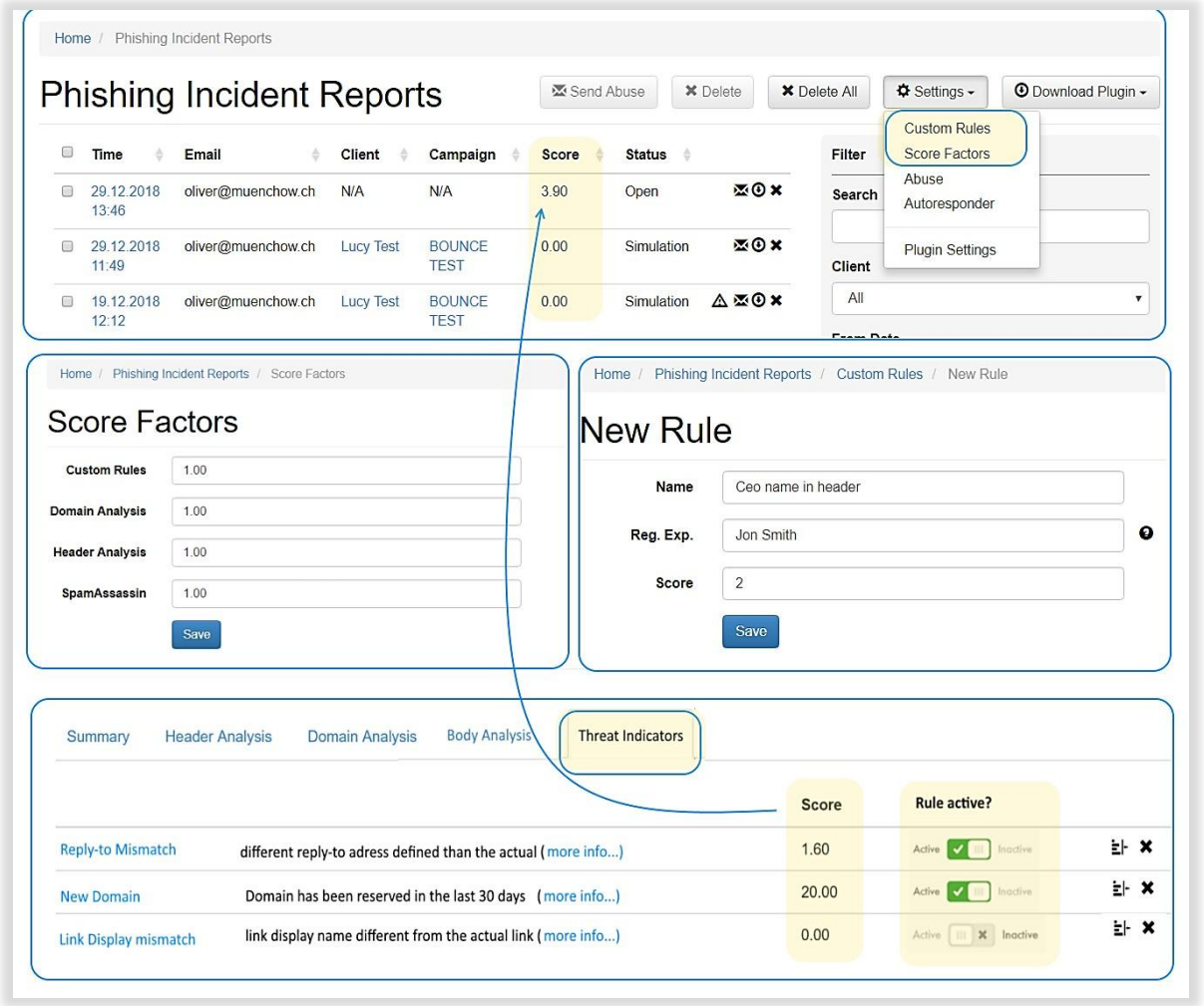
- **Automatisches Vorfalls-Feedback:** Mit diesem Vorfalls-Feedback kann eine automatische Benachrichtigung an den Benutzer mit den Ergebnissen der E-Mail-Bedrohungsanalyse gesendet werden. Der Nachrichtentext ist frei konfigurierbar, und bei Bedarf kann auch der sog. LUCY E-Mail Risk-Score hinzugefügt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



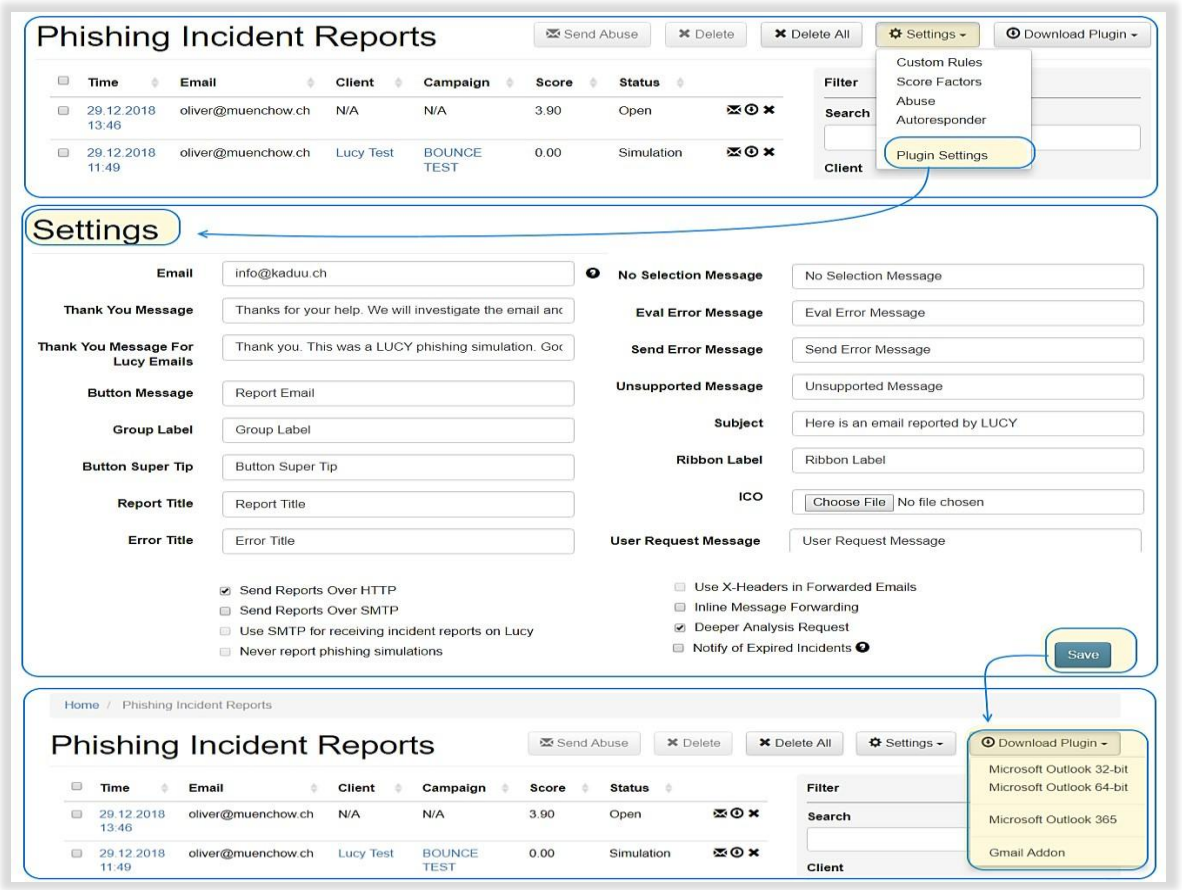
- **Bedrohungsminderung:** Dieser verhaltensbezogene Bedrohungsminderer ist ein revolutionärer Ansatz zur Beseitigung von E-Mail-Risiken. Es unterstützt den Sicherheitsadministrator bei der Abwehr des Angriffs (z. B. Senden eines automatisierten Berichts an spezialisierte Teams bei den Anbietern, die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



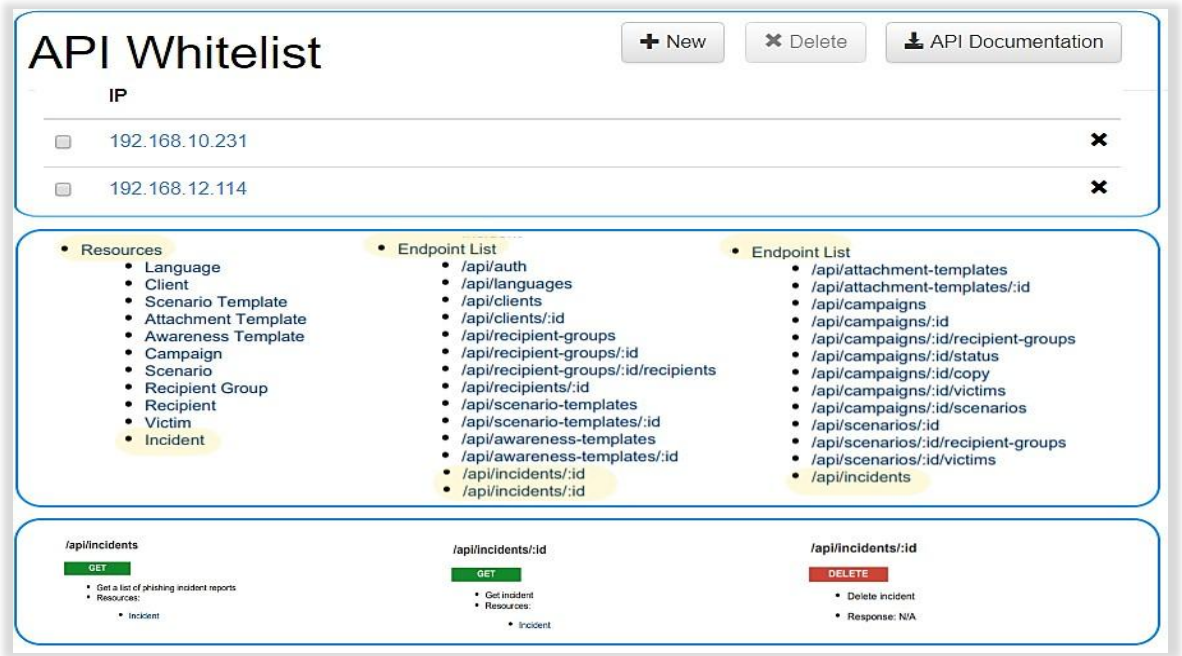
- **Benutzerdefinierte und regelbasierte Analyse:** Definieren Sie Ihre eigenen Regeln für die E-Mail-Analyse und Risikoberechnung.



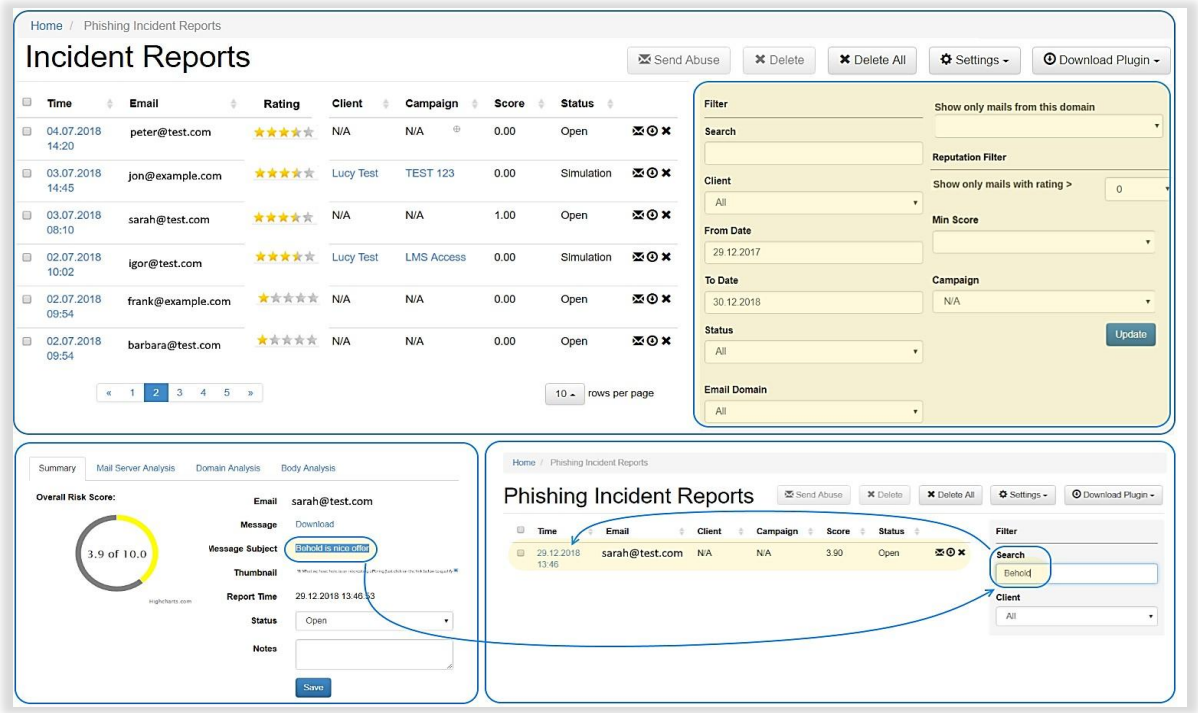
- **Anpassungsoptionen für Plug-ins:** LUCY ermöglicht eine einfache Anpassung und ein vollständiges „White labelling“ für verschiedene Plugin-Funktionen (angezeigte Symbole, Rückmeldungen, Kennzeichnungen, Übertragungsprotokolle, gesendete Header, usw.).



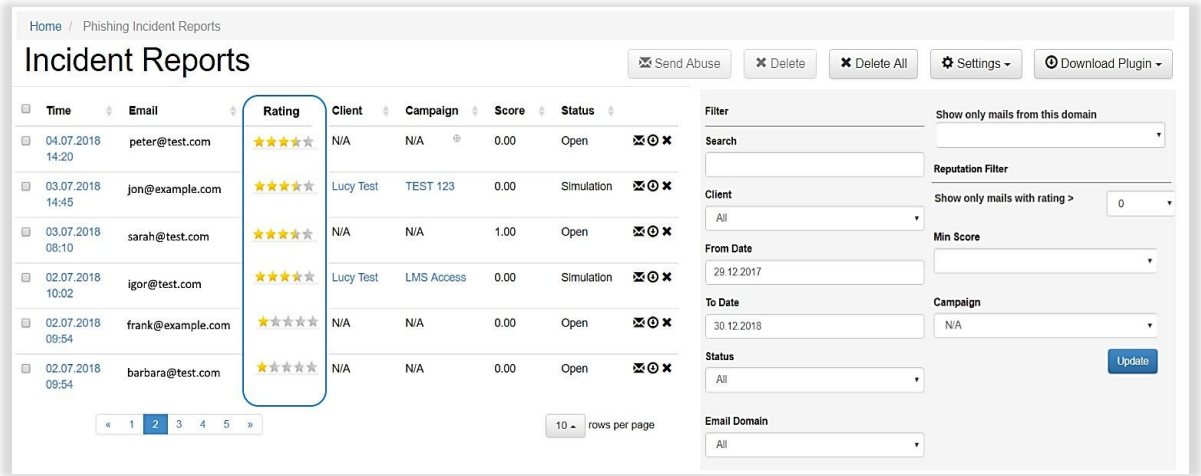
- **Integration von Drittanbietern:** Mithilfe der REST-API-Automatisierung von LUCY können wir gemeldete E-Mails verarbeiten und Ihrem Sicherheitsteam dabei helfen, aktive Phishing-Angriffe bereits während des Vorgangs zu stoppen.



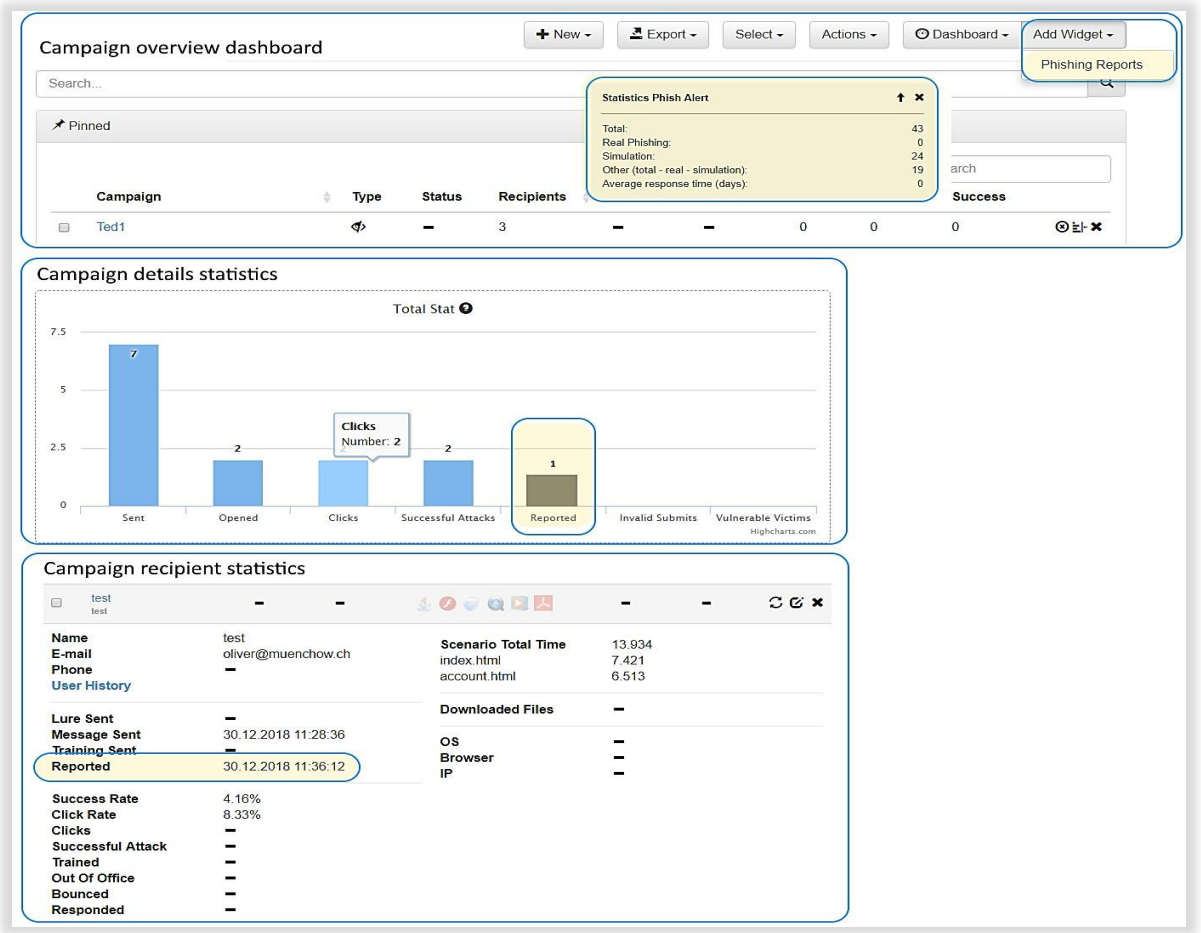
- **Identifizieren von Angriffen nach einem gängigen Muster:** Wenden Sie die Dashboard-Filter von LUCY an, um allgemeine Angriffsmethoden in Ihrem Unternehmen zu erkennen. Suchen Sie in allen gemeldeten E-Mails nach ähnlichen Bedrohungs-Indikatoren.



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



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



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