LIVRO BRANCO DO LUCY

O QUE É O LUCY?

Teste, forme e envolva os seus funcionários

O LUCY permite que as organizações desempenhem o papel de um atacante e revelem fragilidades existentes, tanto na infraestrutura técnica como nos conhecimentos da equipa, eliminando-as por meio de programas abrangentes de elearning.

TESTE DOS FUNCIONÁRIOS
Simulações de Ataque (por exemplo, phishing)

TESTE DA INFRAESTRUTURA
Simulação de Scanner de Malware

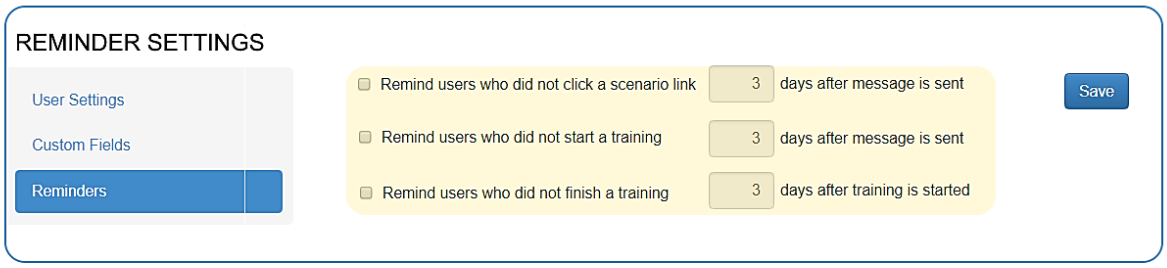
FORMAÇÃO DOS FUNCIONÁRIOS
SGA Integrado

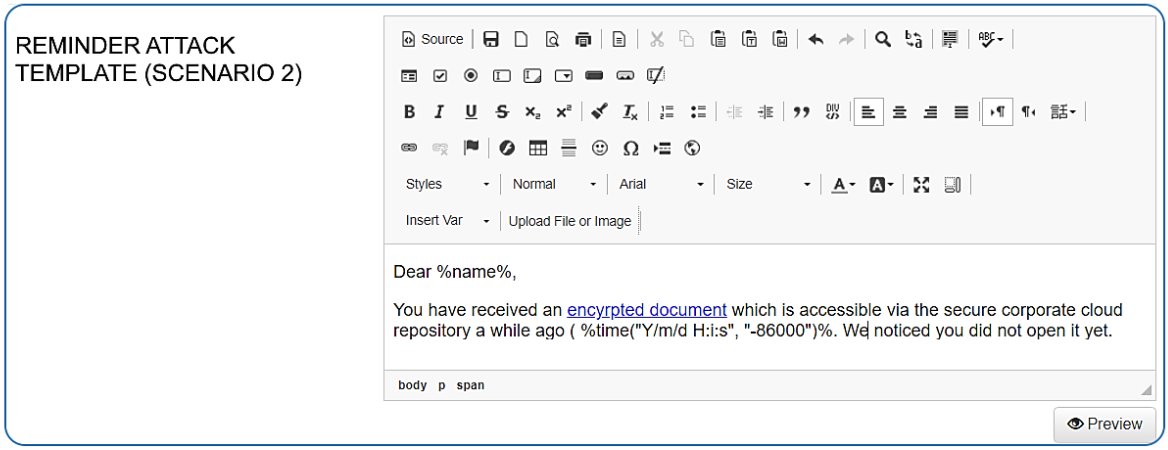
MEDIÇÃO DO PROGRESSO
Análise do Risco e da Aprendizagem

INTEGRAÇÃO DOS FUNCIONÁRIOS
Sistema de Denúncia (por exemplo, Botão de e-mail com Phishing)

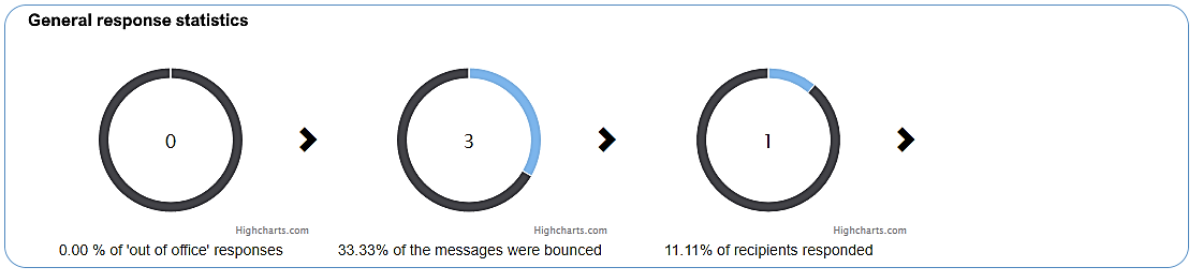
CARACTERÍSTICAS GERAIS

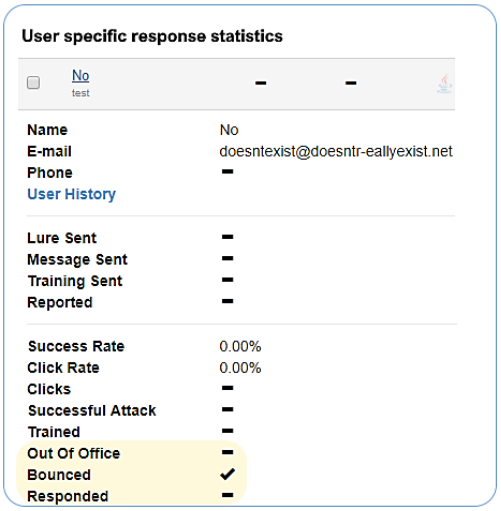
- **LEMBRETES:** Podem utilizar-se modelos de lembretes para reenviar mensagens automaticamente para utilizadores que não tenham clicado num link de ataque ou para realizar um curso de formação após um período de tempo personalizado.

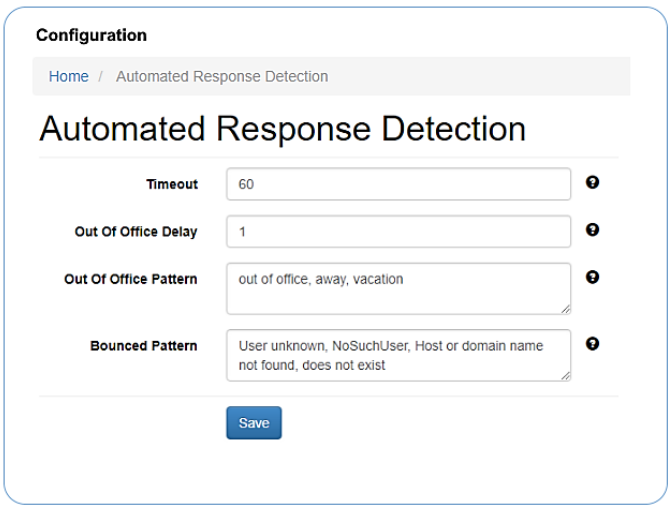




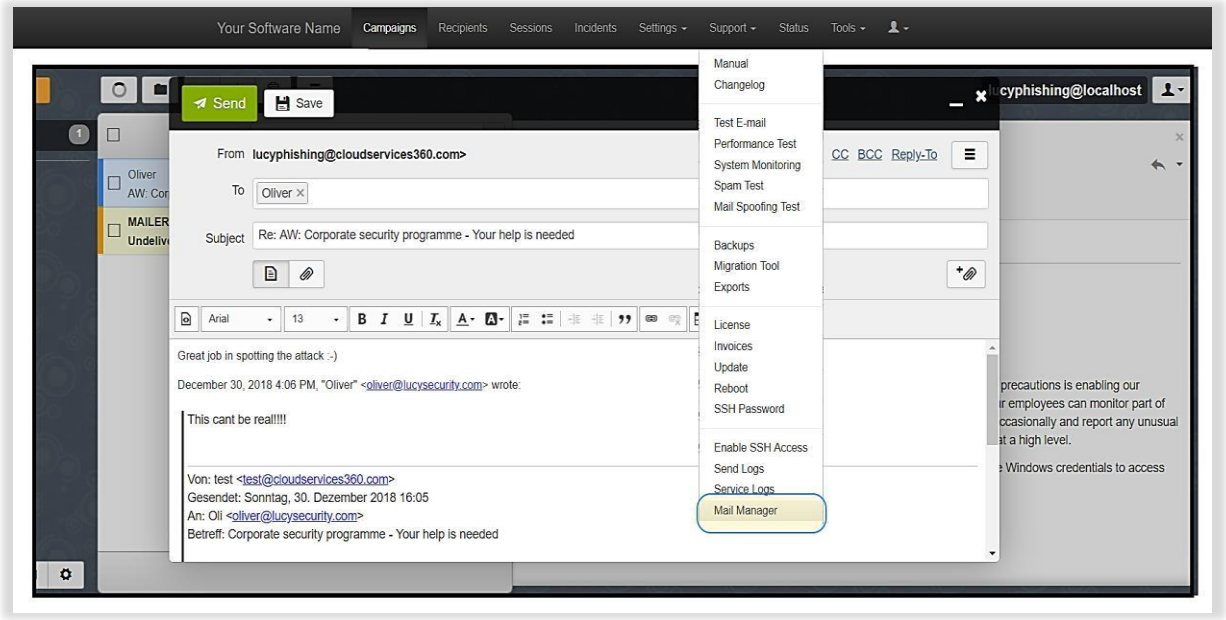
- **DETEÇÃO DE RESPOSTA:** A deteção automática de resposta permite definir e analisar respostas automáticas por e-mail (por exemplo, fora do escritório), bem como erros de entrega de e-mail (por exemplo, utilizador desconhecido) dentro da campanha.



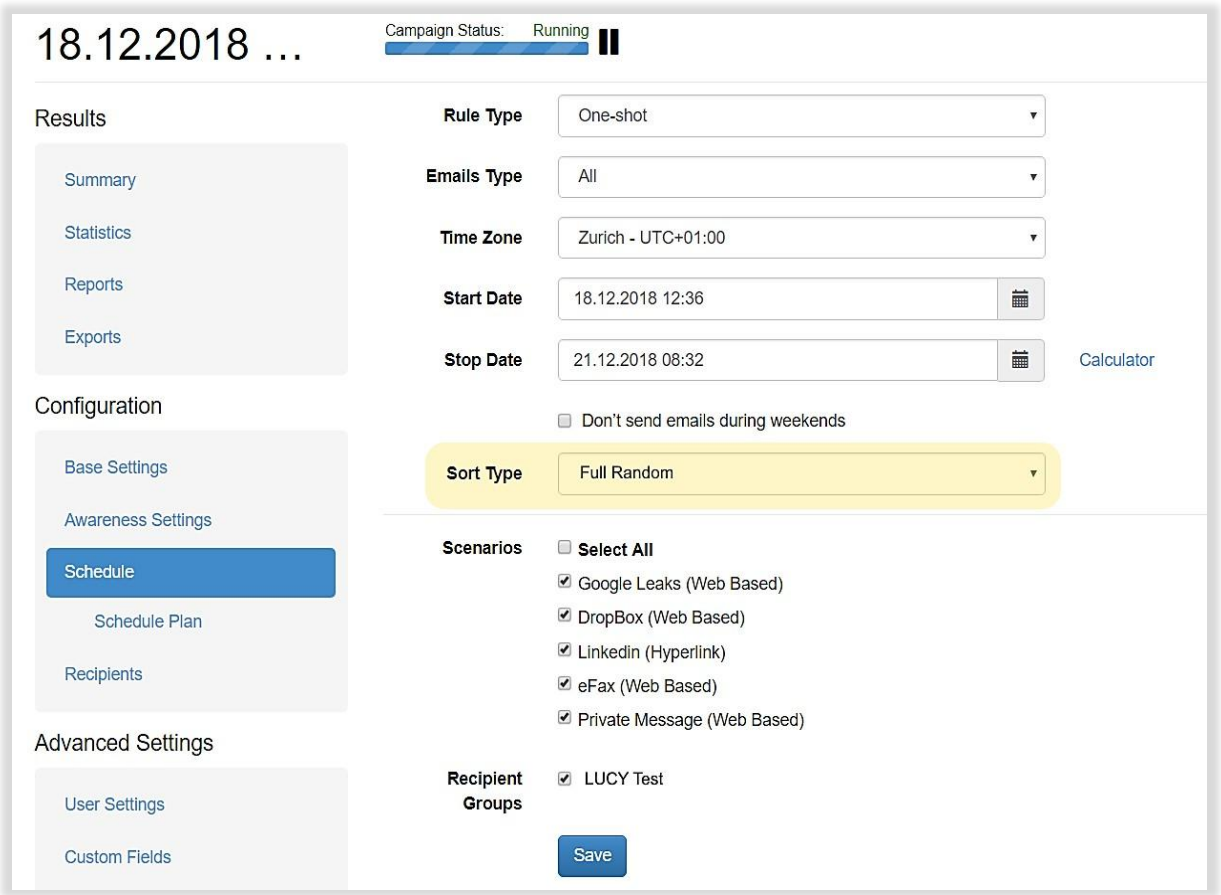




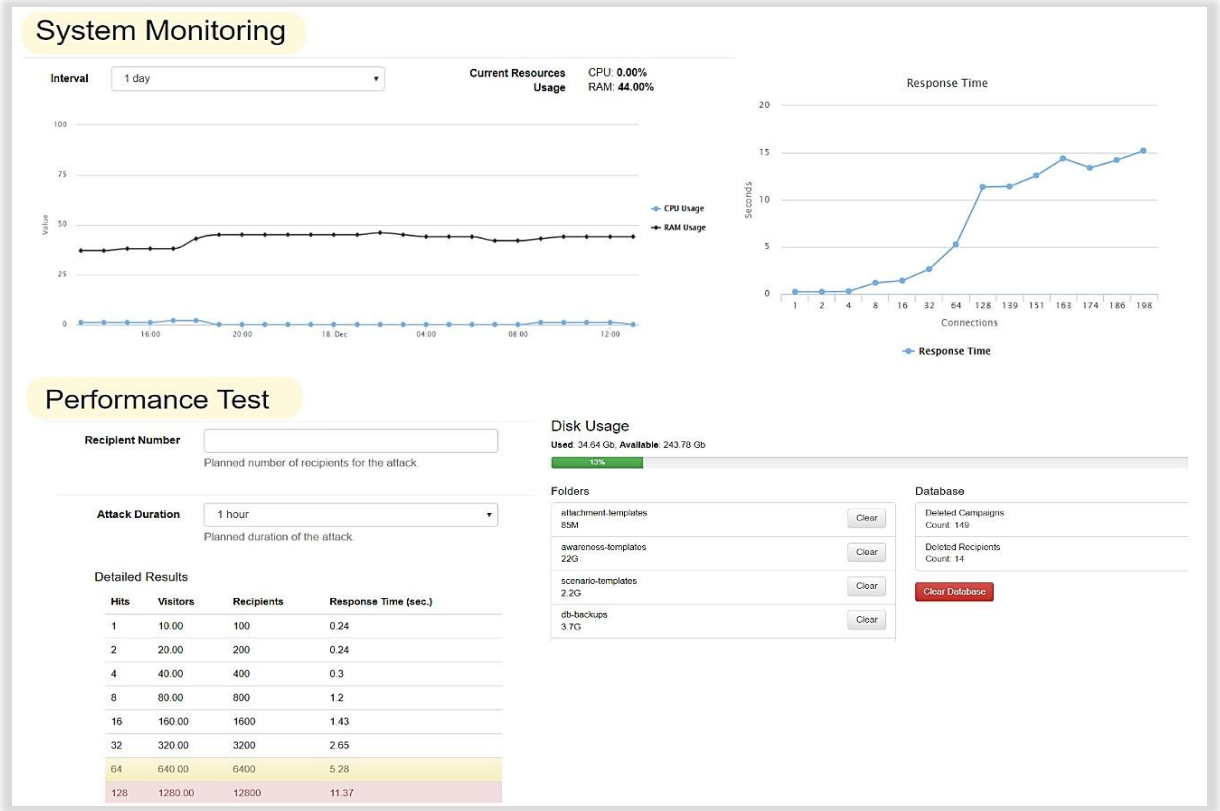
- **CLIENTE DE COMUNICAÇÃO INTEGRAL:** Uma plataforma de mensagens incorporada permite que o administrador do LUCY comunique interativamente com os destinatários dentro ou fora das campanhas LUCY. Todos os e-mails são arquivados e podem ser avaliados.



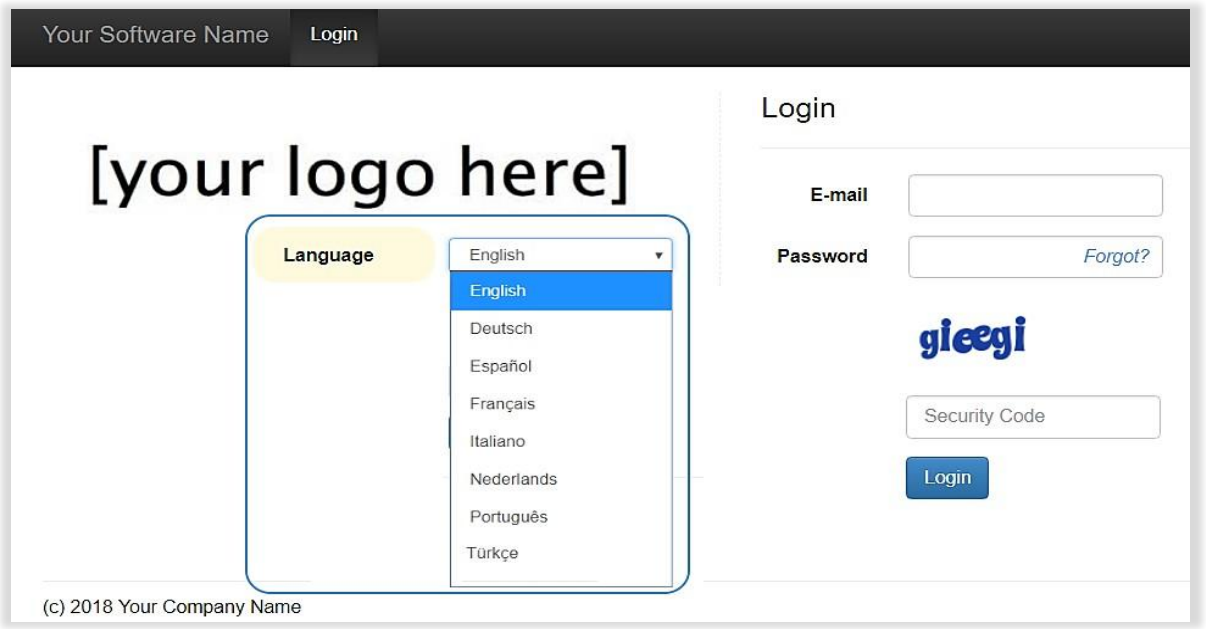
- **Aleatorização do agendamento:** Aumentar a conscienciali zação dos colaboradores aleatoriamente é o fator chave para a conscienciali zação efetiva e sustentável dentro da organização. O envio aleatório de muitas campanhas em simultâneo é um dos melhores meios de formação dos colaboradores.



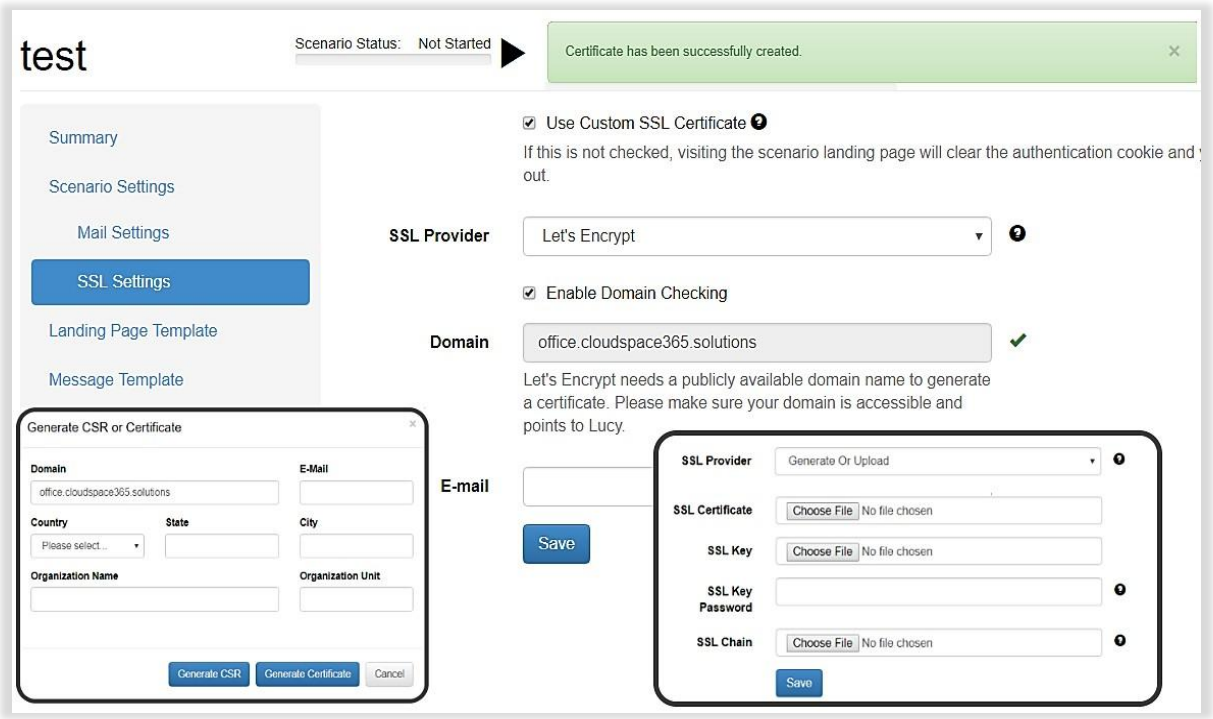
- **Ferramentas de desempenho:** as rotinas inteligentes do LUCY adaptam a instalação do servidor aos recursos indicados. O servidor de aplicações, o dimensionamento de SGBD, as utilizações da memória e do CPU são calculados durante a instalação ou durante as operações. Pode escalar uma única instalação LUCY baseada na nuvem para mais de 400 000 utilizadores.



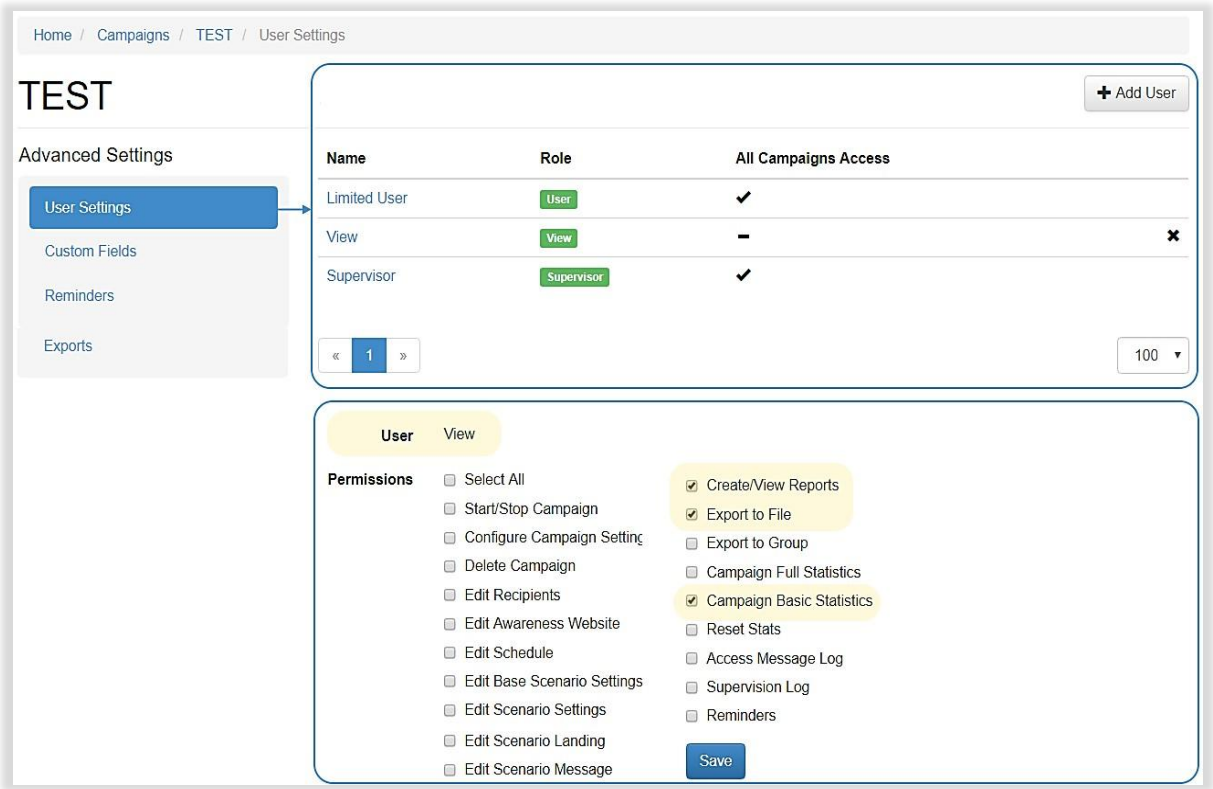
- **Interface de administração multilingue** A interface de administração LUCY está disponível em diferentes idiomas e pode ser traduzida noutras línguas mediante pedido.



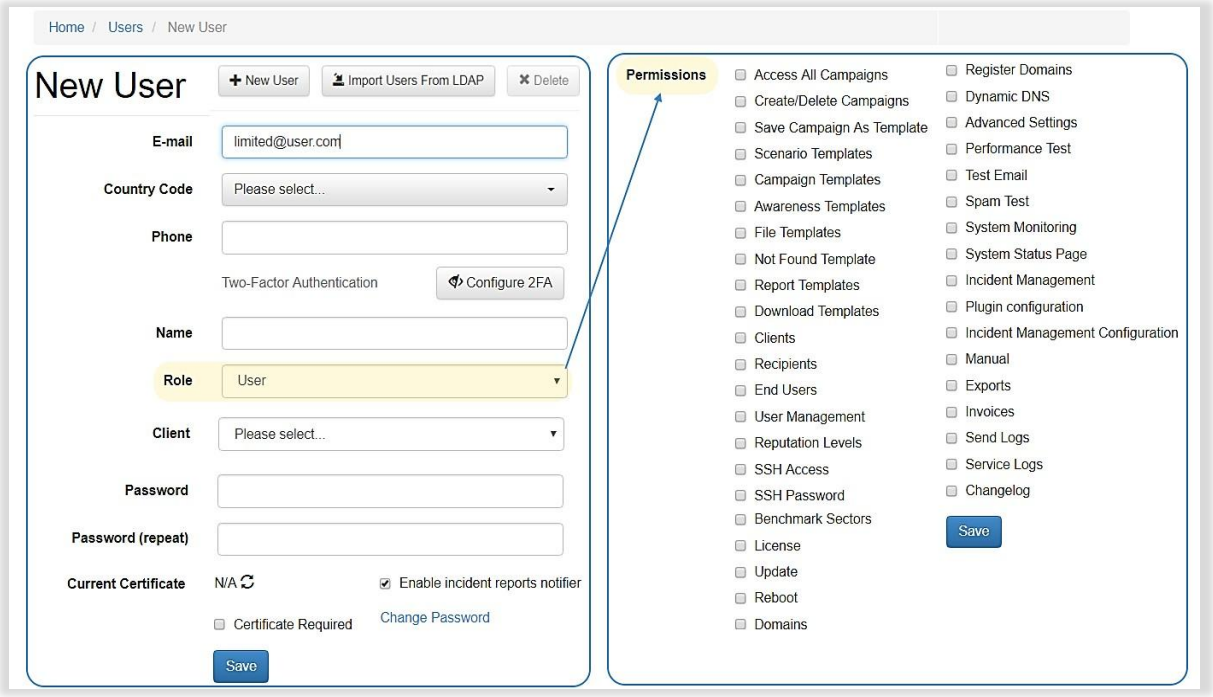
- **Certificado (SSL):** Permite a criação automática de certificados oficiais e fiáveis para a administração, backend e para as campanhas. O LUCY irá usar automaticamente o domínio configurado no sistema para gerar o certificado. Se decidir usar SSL para a campanha, pode gerar um certificado personalizado ou uma RAS (Requisição de Assinatura de Certificado). Também pode importar certificados oficiais de confiança.



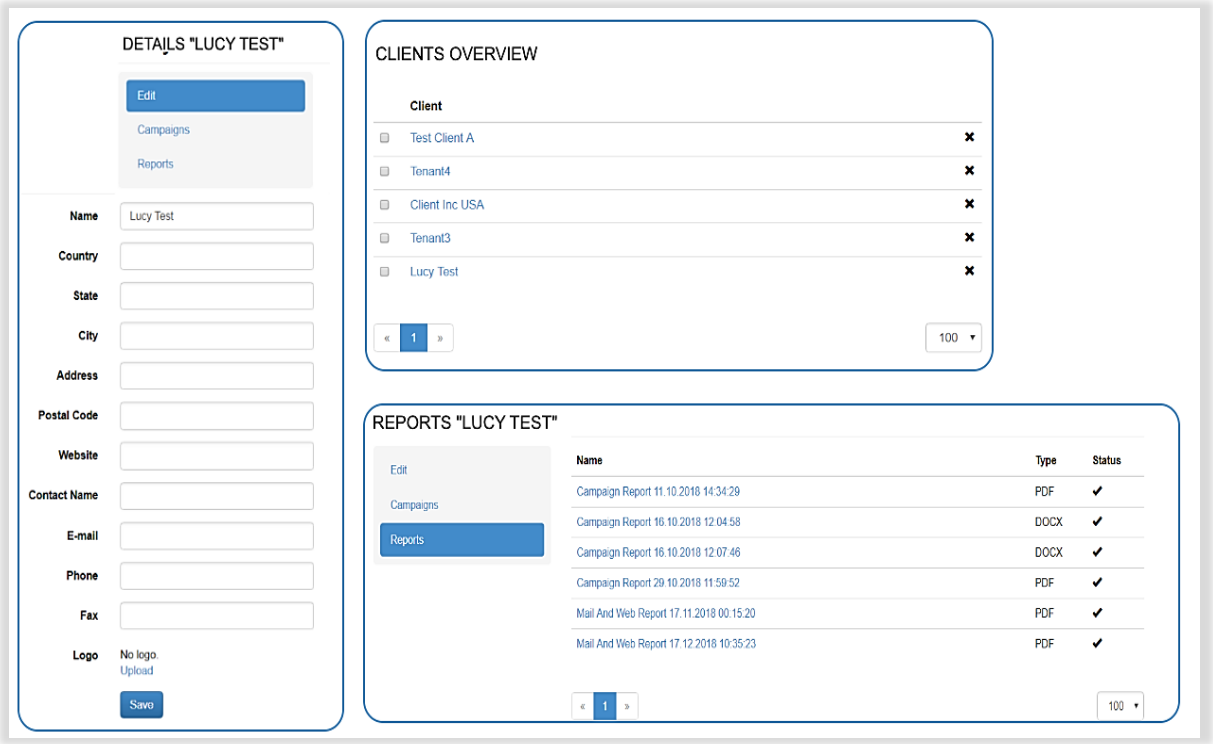
- **Controlos de acesso baseados em funções:** O LUCY oferece um controlo de acesso baseado nas funções (RBAC), que restringe o acesso ao sistema apenas aos utilizadores autorizados. As permissões para realizar certas operações são atribuídas a funções específicas, no âmbito das configuração do utilizador. São atribuídas funções específicas aos membros ou funcionários (ou a outros utilizadores do sistema), através das quais adquirem as permissões de computador necessárias para desempenhar determinadas funções LUCY.



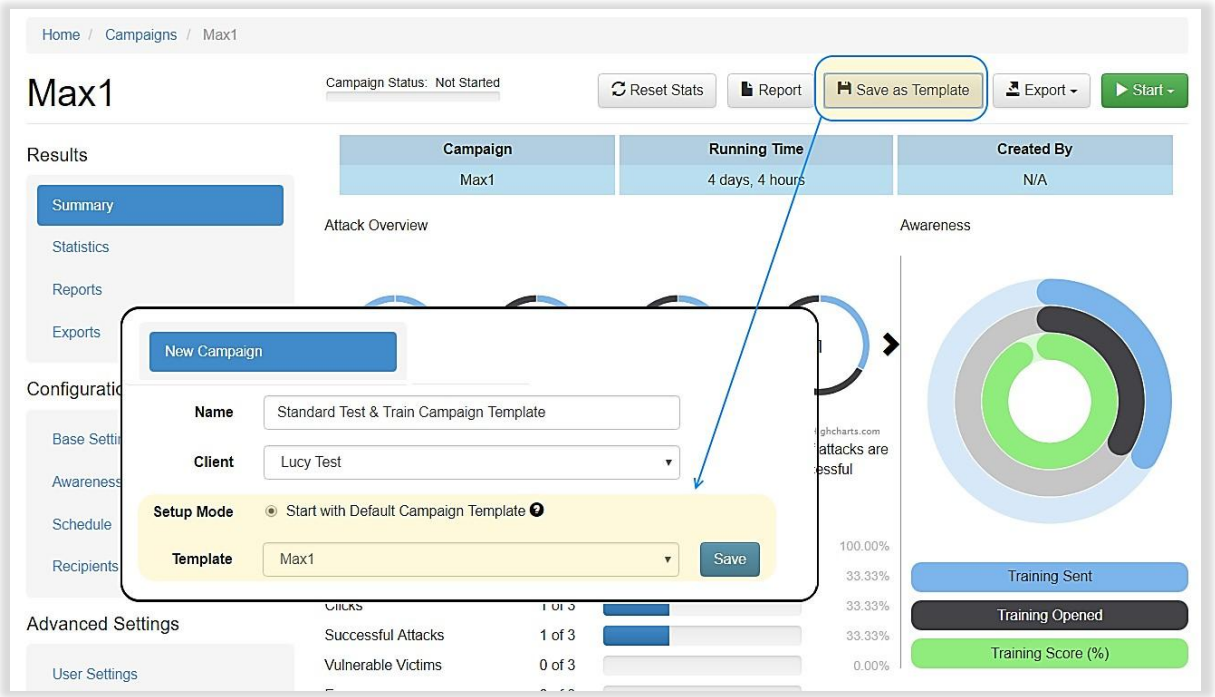
- **Grupos de utilizadores multicamada**: Faz rapidamente o upload em massa de ficheiros CSV, LDAP ou de texto. Cria grupos diferentes, organizados por departamento, divisão, título, etc. Atualiza os utilizadores numa campanha em execução. Cria grupos de utilizadores dinâmicos com base nos resultados da campanha de phishing.



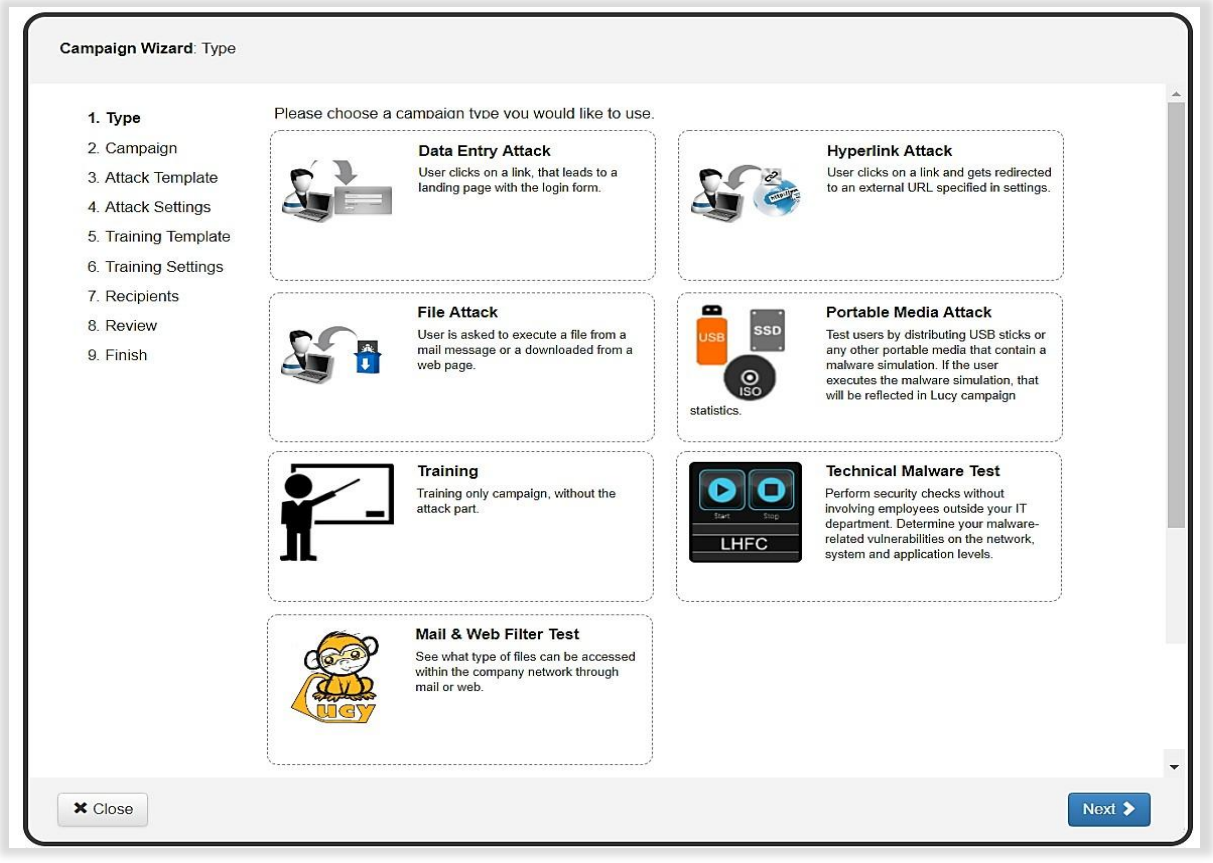
- **Compatível com multicliente:** "Clientes" pode referir-se a diferentes empresas, departamentos ou grupos que tenham uma campanha associada com o LUCY. Estes clientes podem ser utilizados, por exemplo, para permitir o acesso específico à campanha ou para criar análises específicas para o cliente.



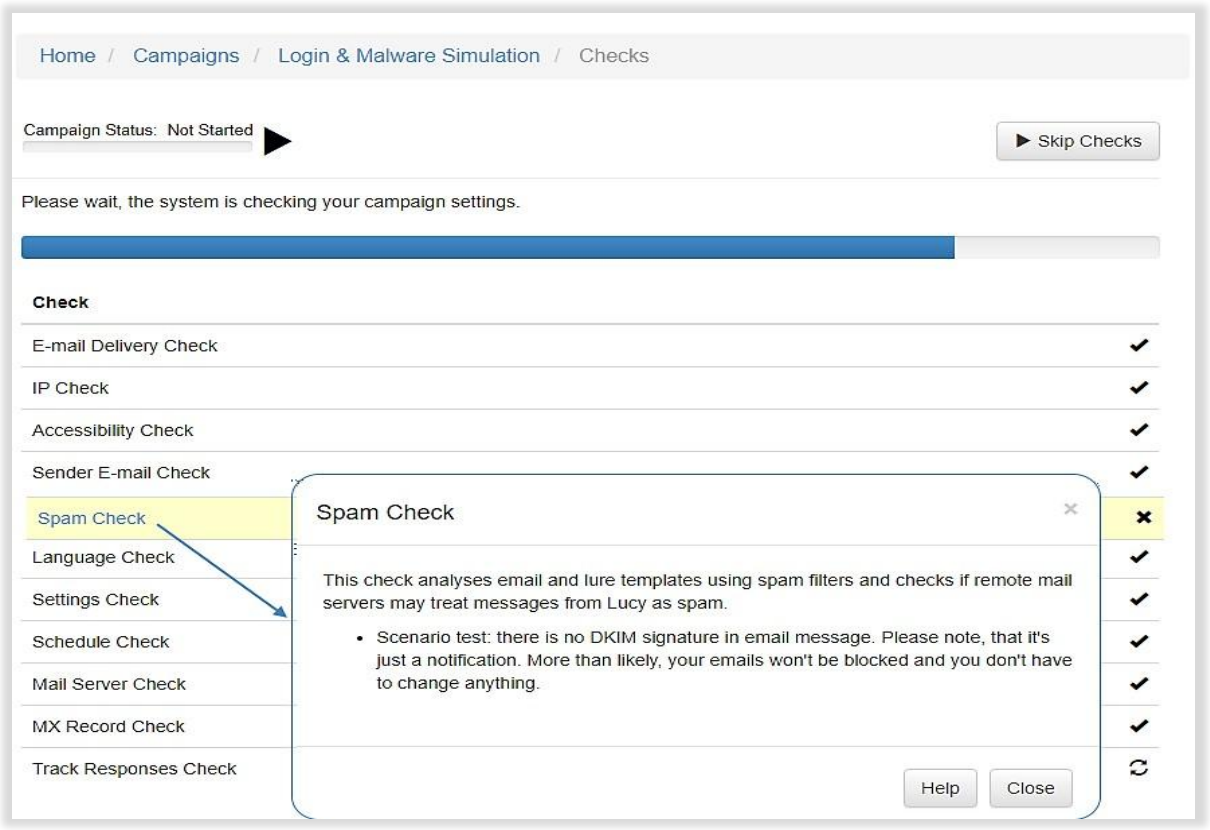
- **Modelos de campanha:** No caso de querer reutilizar campanhas semelhantes, pode guardar uma campanha completa com modelos de ataque e conteúdo de elearning como modelo de campanha. Esta funcionalidade permite-lhe evitar ter de repetir configurações semelhantes repetidamente.



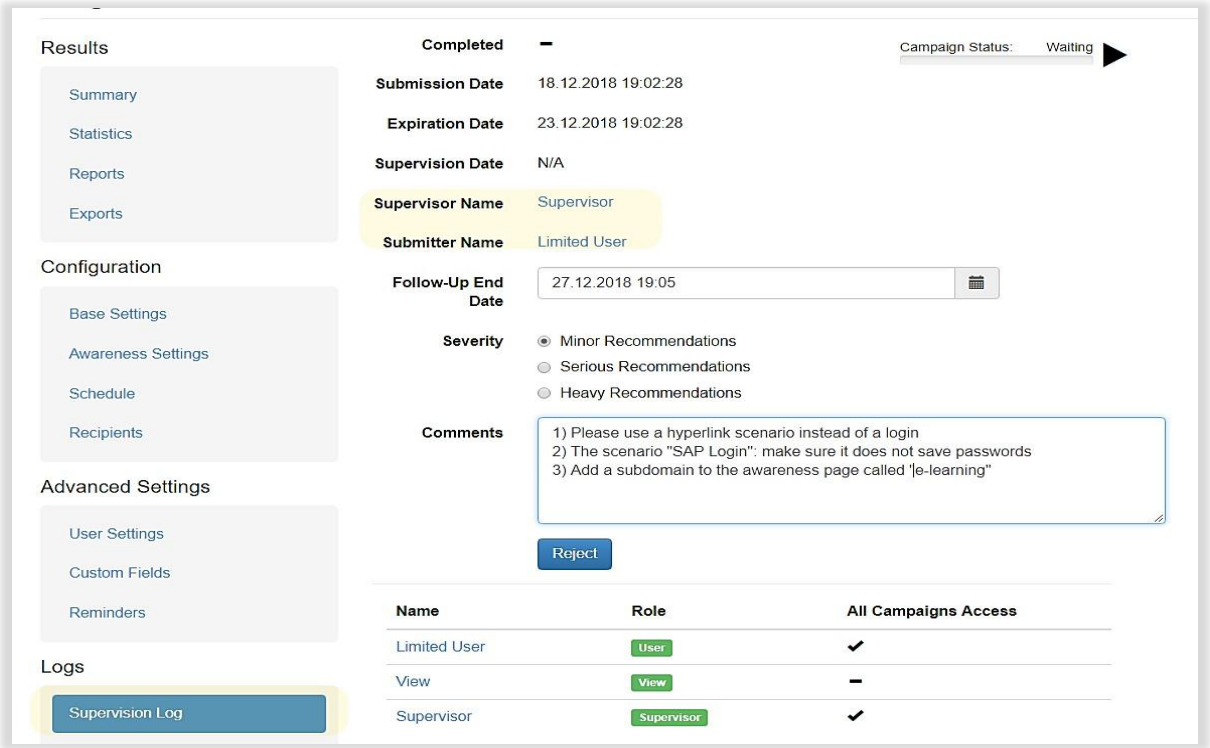
- **Assistente de configuração com orientação baseada no risco:** O LUCY disponibiliza várias ferramentas de configuração. Crie uma campanha completa em menos de 3 minutos usando os modelos predefinidos da campanha ou deixe o assistente de configuração guiá-lo no processo de configuração. Opcionalmente, está disponível um modo de configuração baseado no risco, que faz sugestões específicas para a seleção de modelos de ataque e consciencialização, com base na dimensão e setor da empresa.



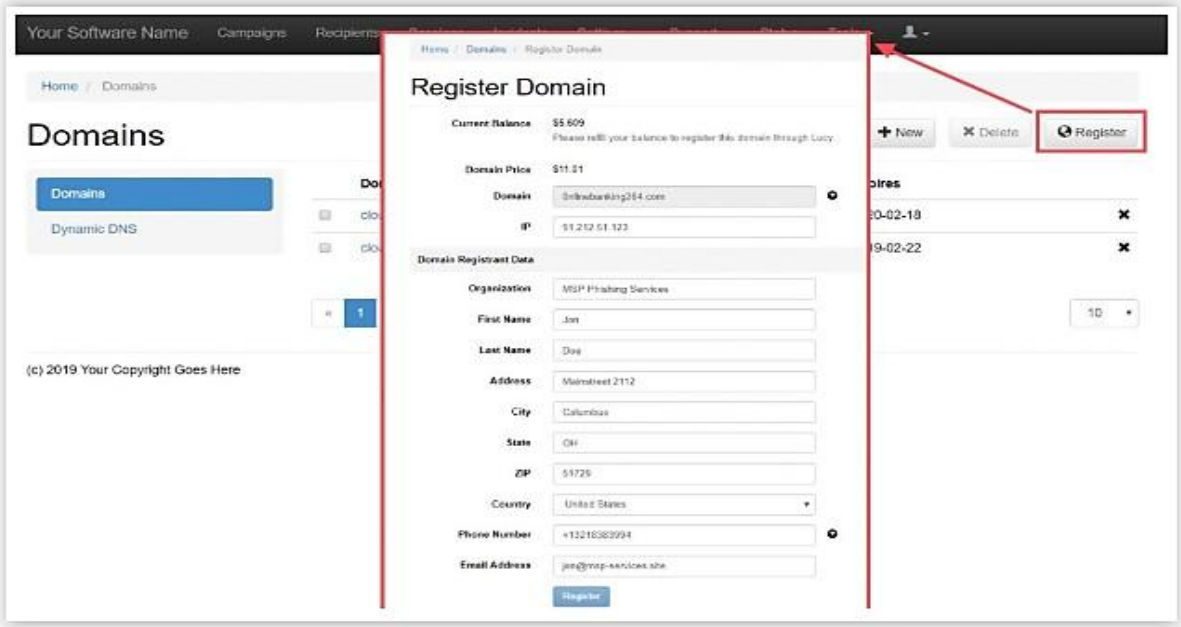
- **Verificações de campanha:** Verificações preliminares antes de iniciar uma campanha LUCY: verificação de entrega de e-mail, verificação de registo MX, verificação de agendamento, verificação de spam e outros.



- **Fluxo de trabalho de aprovação:** uma determinada campanha pode ser enviada a um supervisor no LUCY para aprovação.

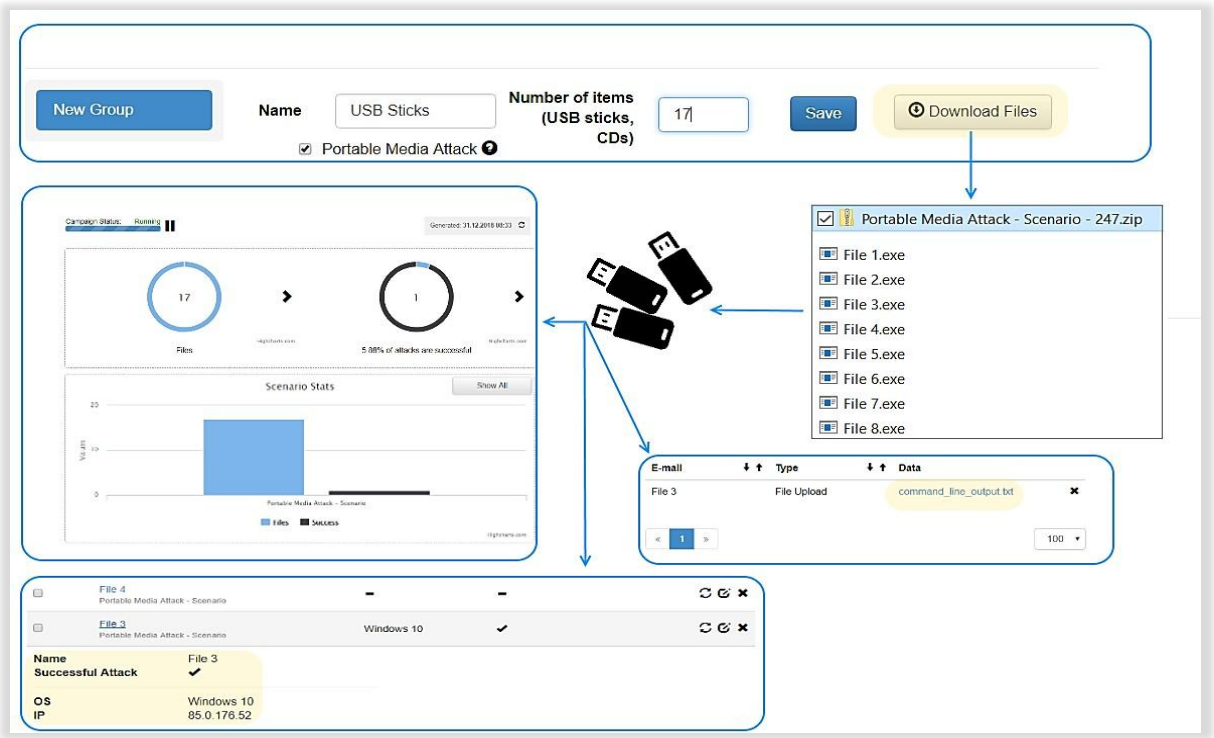


- **API de DNS:** A API de DNS permite ao administrador criar qualquer domínio no LUCY em segundos. Dado que os atacantes usam muitas vezes grafias semelhantes ao domínio de um cliente (chamado Typosquatting), este risco também pode ser apresentado no LUCY. Se o domínio original do cliente é, por exemplo, "onlinebanking.com", o assistente DNS pode ser usado para reservar domínios como "0nlinebanking.com", "onl1nebanking.com" ou " onlinebanking.services " e atribuí-lo a uma campanha posteriormente. Depois, o LUCY cria automaticamente as entradas DNS correspondentes (MX, SPF, proteção Whois, etc.) para o IP onde o LUCY está instalado. Claro que o administrador também pode usar os próprios domínios do seu provedor no LUCY.

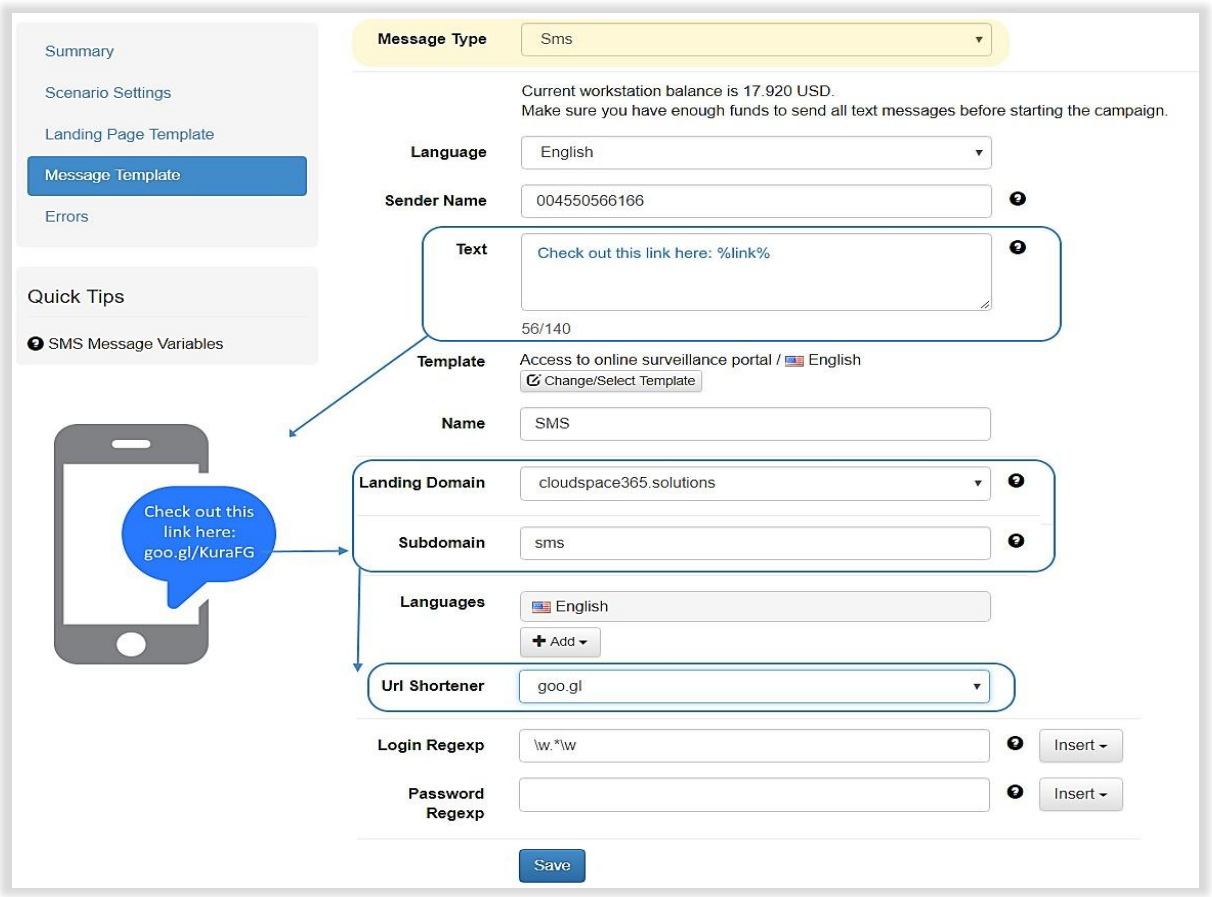


SIMULAÇÃO DE ATAQUE

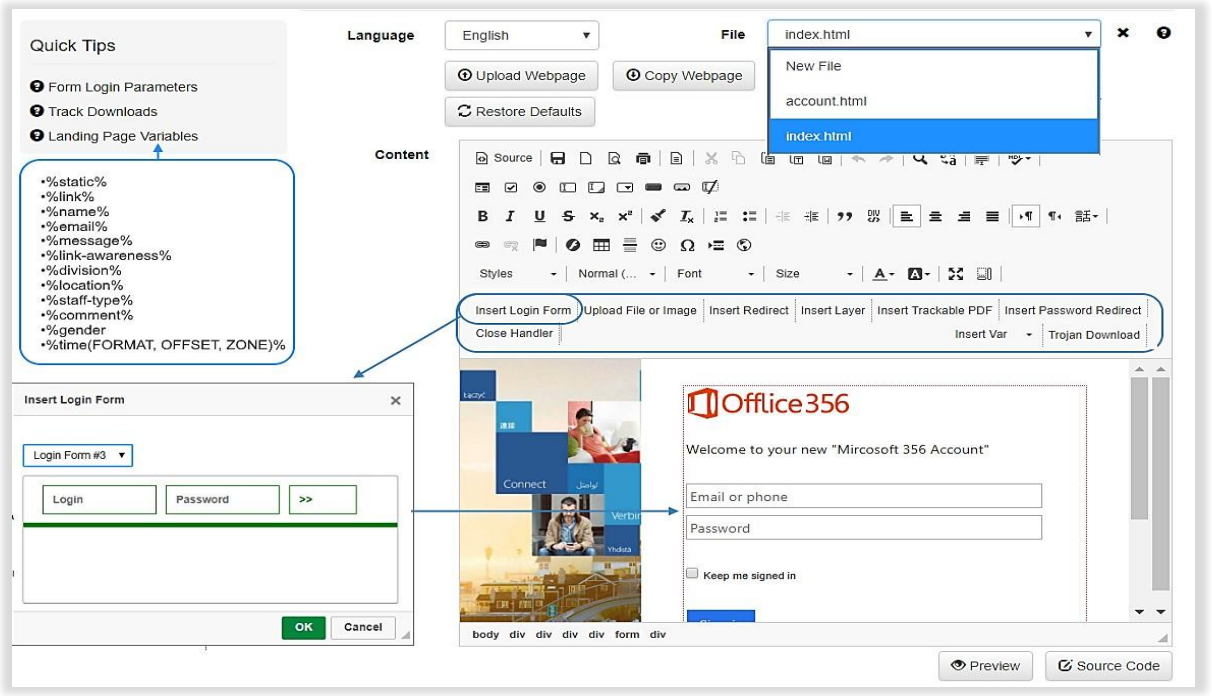
- **Ataques de média portátil:** Os hackers podem usar unidades de média portáteis para obter acesso a informações sensíveis armazenadas num computador ou rede. O LUCY oferece a opção de executar ataques de média portátil em que um modelo de ficheiro (por exemplo, executável, arquivo, documento do office com macros, etc.) pode ser armazenado num dispositivo de média portátil, tal como USB, cartão SD ou CD. A ativação (execução) destes ficheiros individuais pode ser rastreada no LUCY.



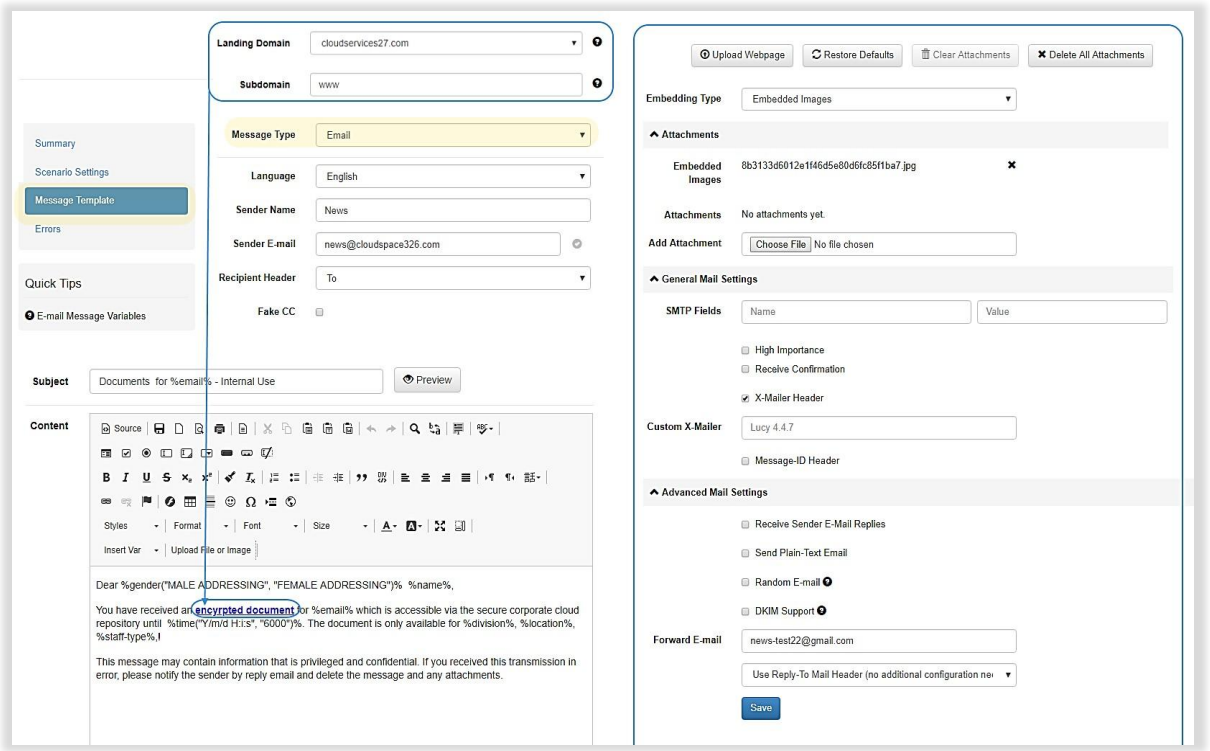
- **SMiShing:** O smishing é, em certo sentido, "phishing por SMS." Quando os cibercriminosos fazem um "phish", enviam e-mails fraudulentos que procuram enganar o destinatário, para que este abra um anexo carregado de malware ou clique num link malicioso. O smishing usa simplesmente mensagens de texto, em vez de e-mail.



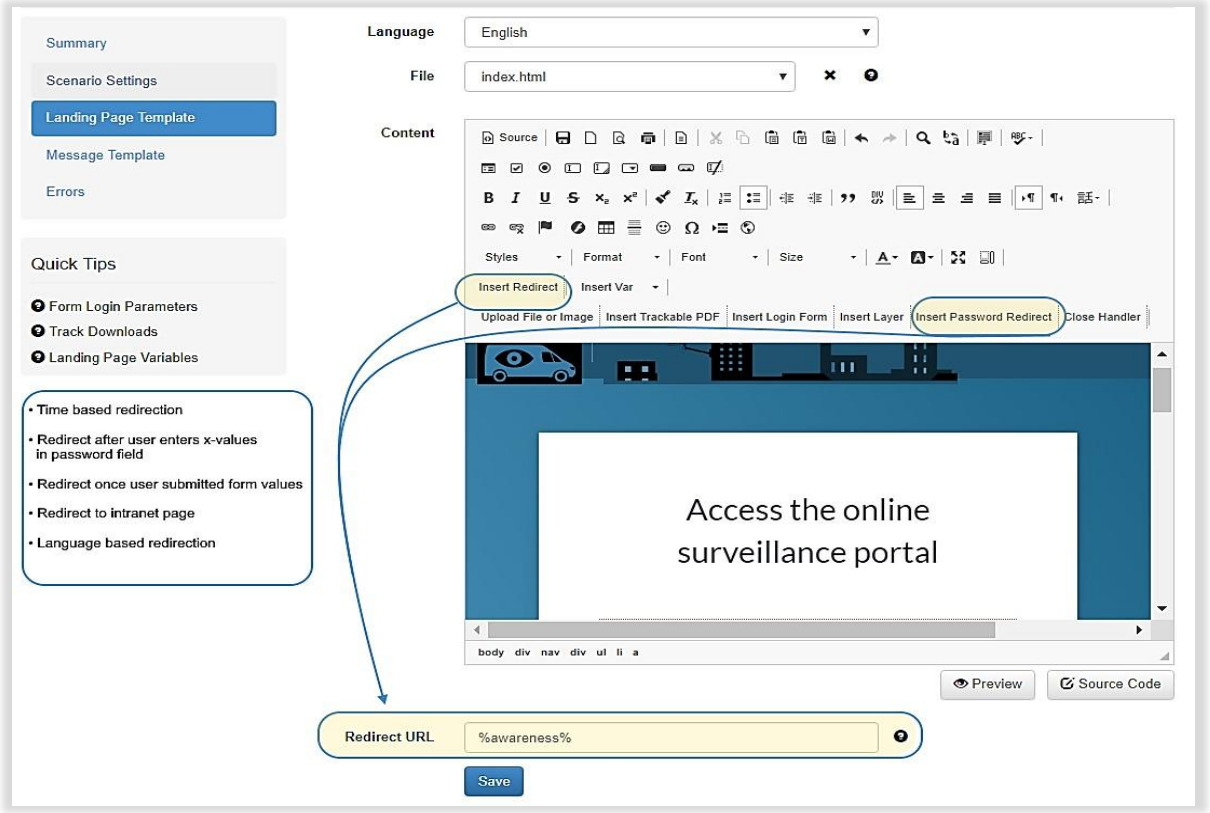
- **Ataques de introdução de dados:** Os ataques de introdução de dados podem incluir uma ou mais páginas web que intercetam a entrada de informações sensíveis. As páginas web disponíveis podem ser facilmente personalizadas com um editor web do LUCY. Ferramentas adicionais de edição permitem configurar rapidamente funções como formulários de log-in, áreas de download, etc., sem conhecimentos de HTML.



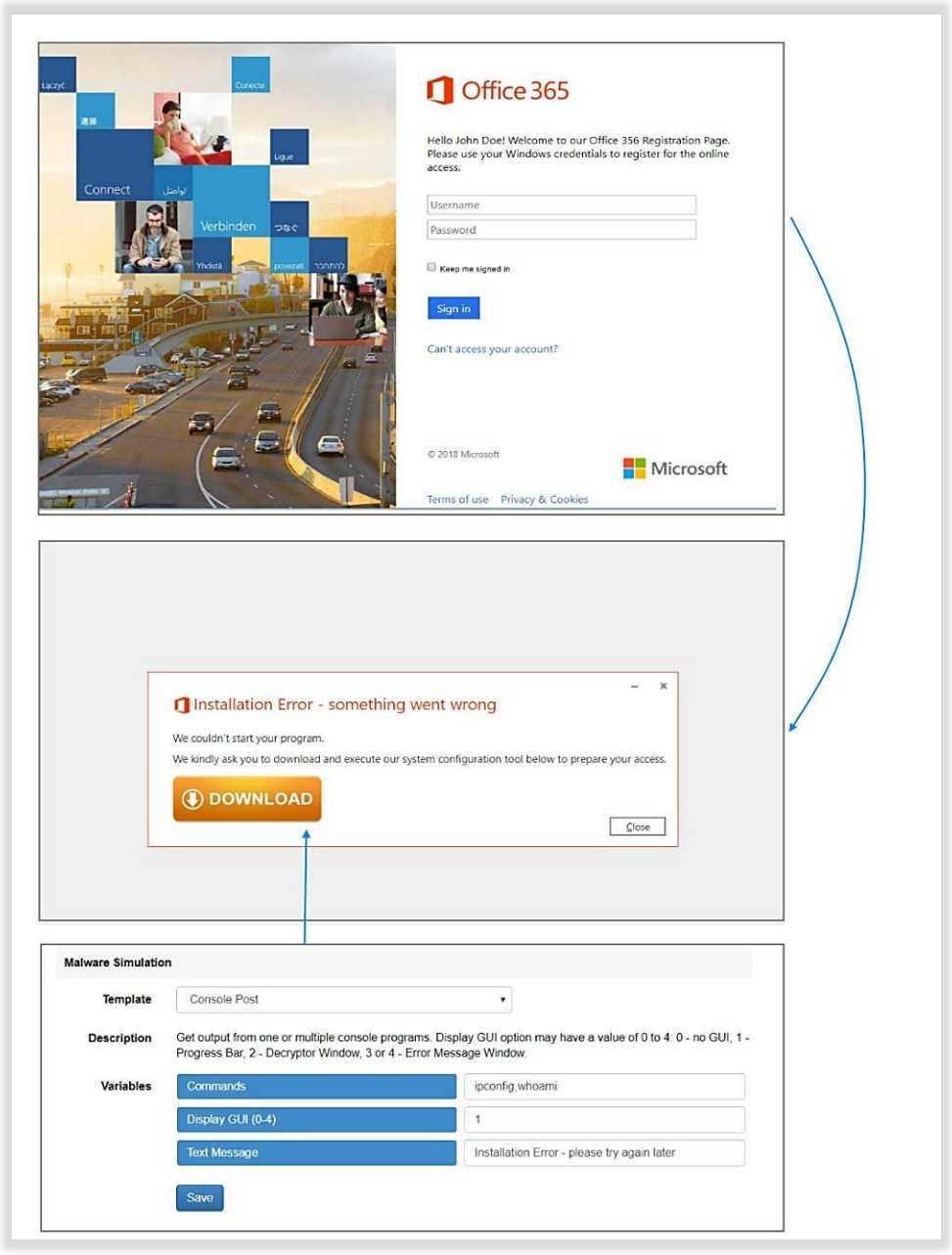
- **Ataques com hiperligações:** Uma campanha baseada em hiperligações enviará aos utilizadores um e-mail que contém um URL de rastreamento aleatório.



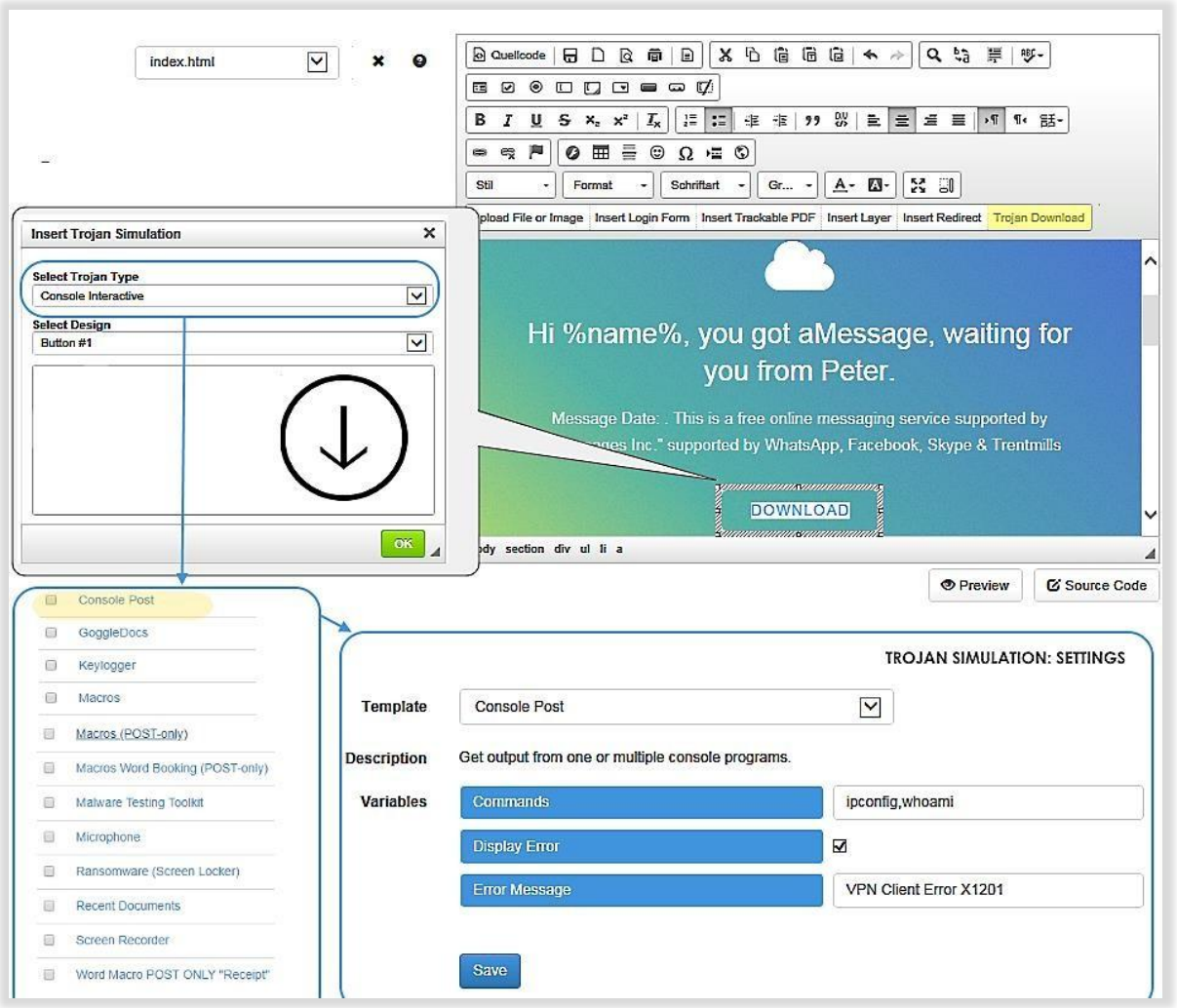
- **Ferramenta poderosa de redirecionamento de URL:** As funções de redirecionamento flexíveis do LUCY permitem que o utilizador seja guiado, no momento certo, para as áreas desejadas de simulação de ataque ou formação. Por exemplo, depois de inserir os 3 caracteres de uma palavra-passe numa simulação de phishing, o utilizador pode ser redirecionado para uma página de formação especial sobre a proteção com palavra-passe.



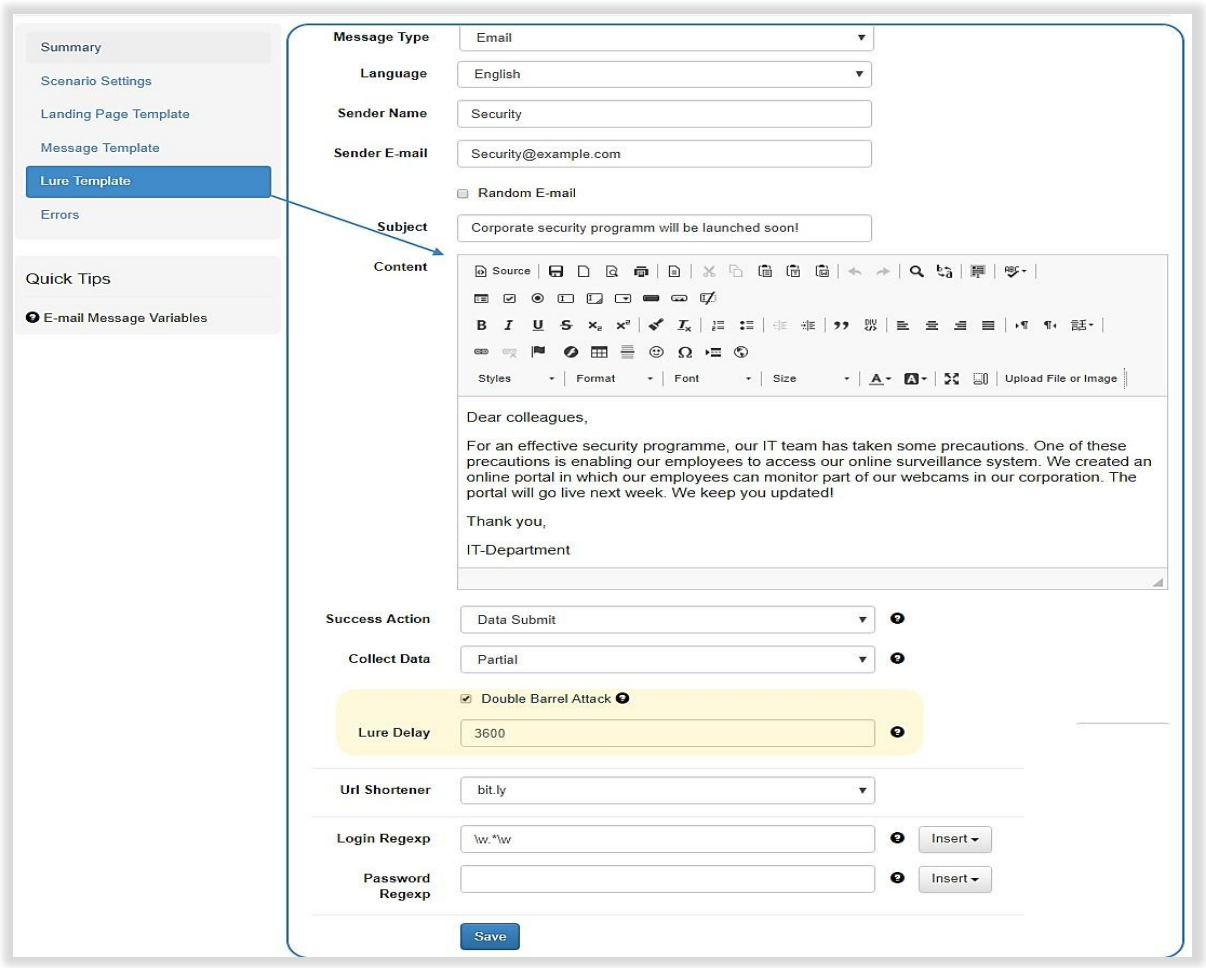
- **Ataques mistos:** Os ataques mistos permitem uma combinação de vários tipos de cenário (baseado em ficheiros, introdução de dados, etc.) na mesma campanha.



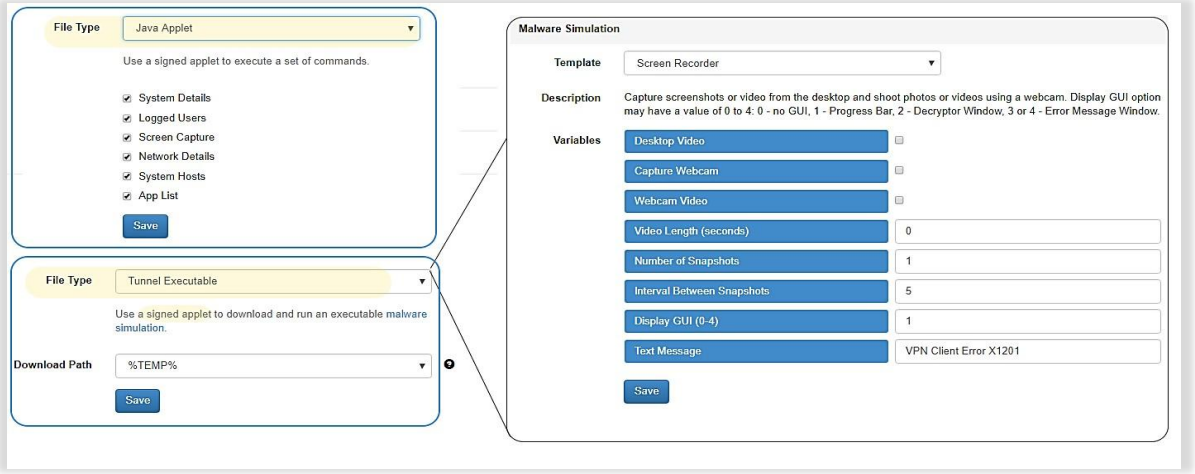
- **Ataques baseados em ficheiros:** Ataques baseados em ficheiros permitem ao administrador LUCY integrar diferentes tipos de ficheiros (documentos do office com macros, PDFs, executáveis, MP3s, etc.) em anexos de e-mail ou sites gerados no LUCY e medir a sua taxa de download ou execução.



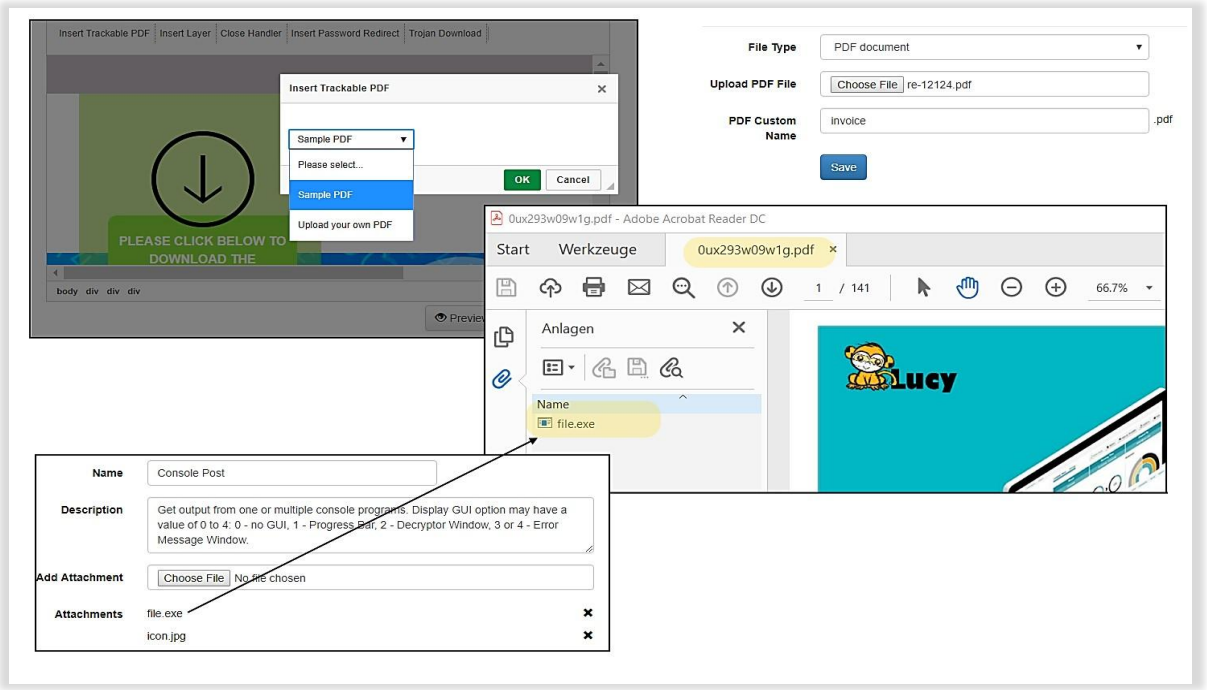
- **Ataques de cano duplo:** Esta funcionalidade possibilita o envio de vários e-mails de phishing em cada campanha, em que o primeiro e-mail benigno (o isco) não contém nada malicioso e não exige uma resposta do destinatário.



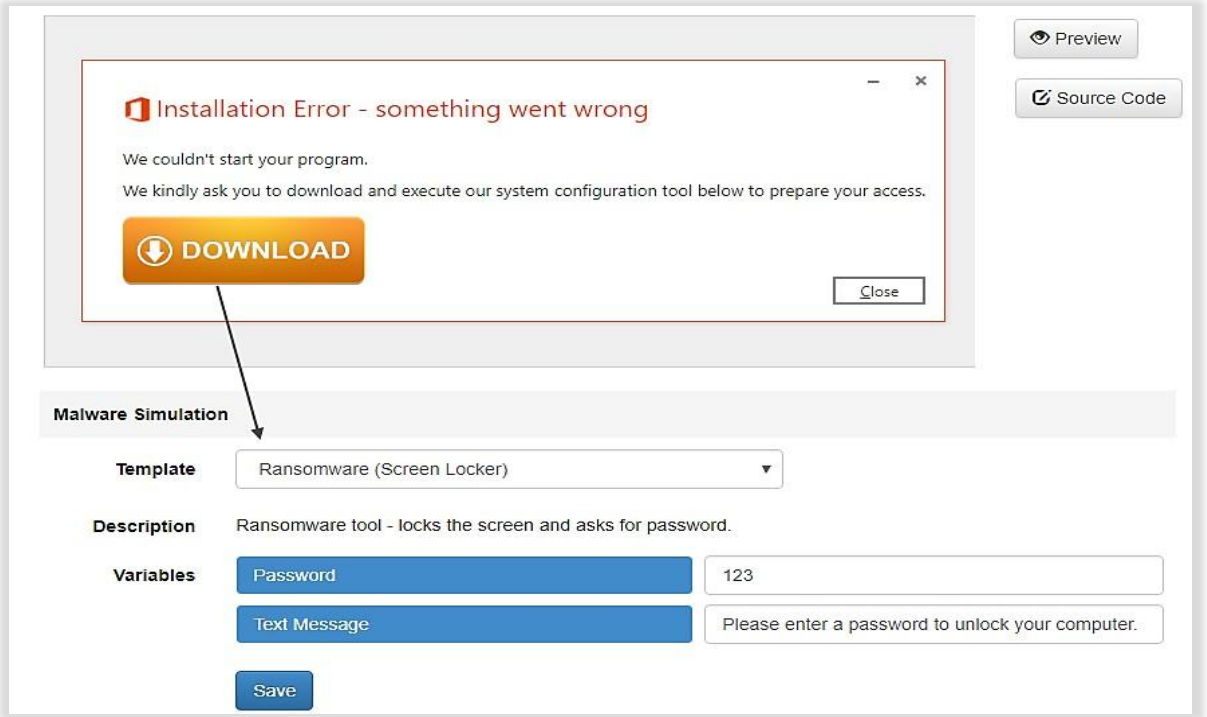
- **Ataques baseados em Java:** Ataques baseados em Java permitem que o administrador LUCY integre um applet fiável dentro dos modelos de ataque baseados em ficheiros ou mistos fornecidos pelo LUCY e meça a sua execução pelo utilizador.



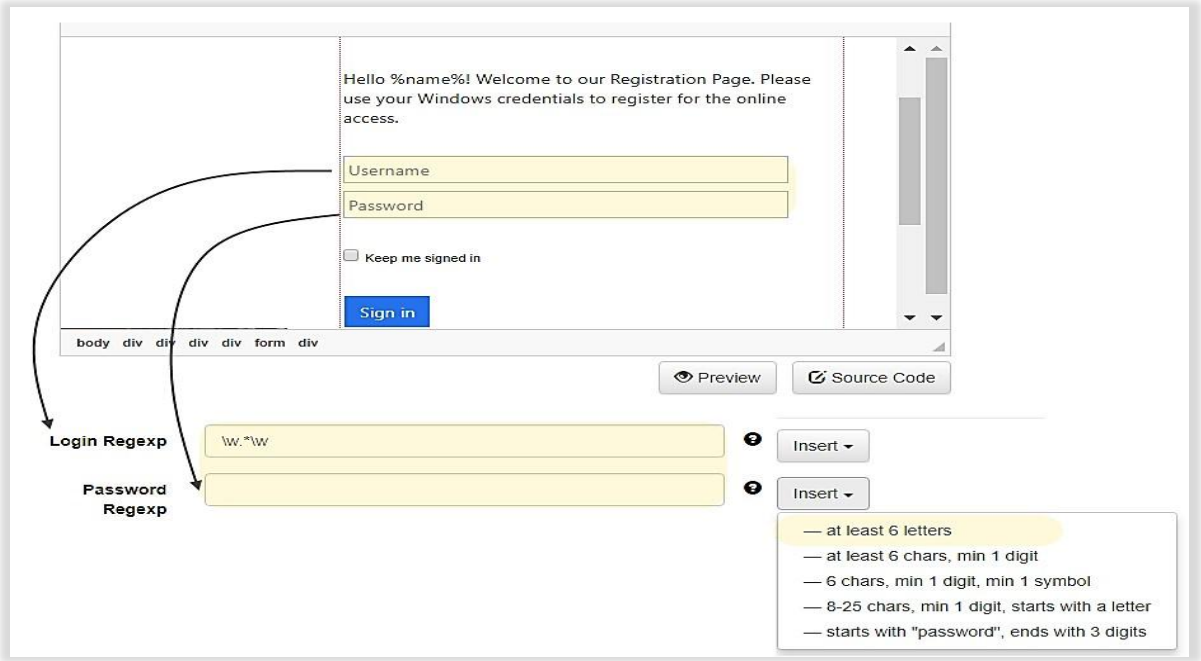
- **Ataques baseados em PDF:** Os ataques de phishing baseados em PDF podem ser simulados com este módulo. O LUCY permite "esconder" ficheiros executáveis como anexos PDF e medir a sua execução. Além disso, também podem ser geradas ligações dinâmicas de phishing dentro dos PDFs.



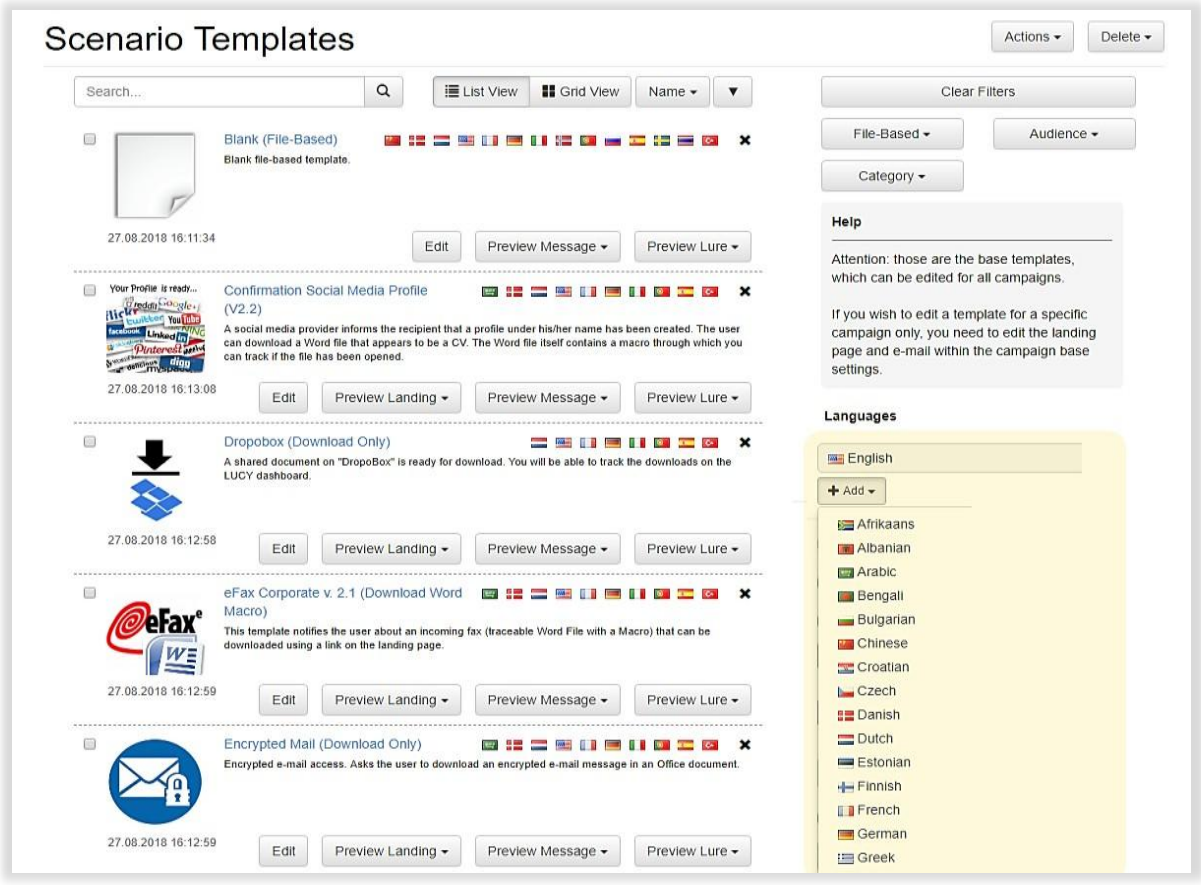
- **Ataques de simulação de ransomware:** O LUCY tem duas simulações diferentes de ransomware, uma das quais testa a equipa, e a outra, a infraestrutura.



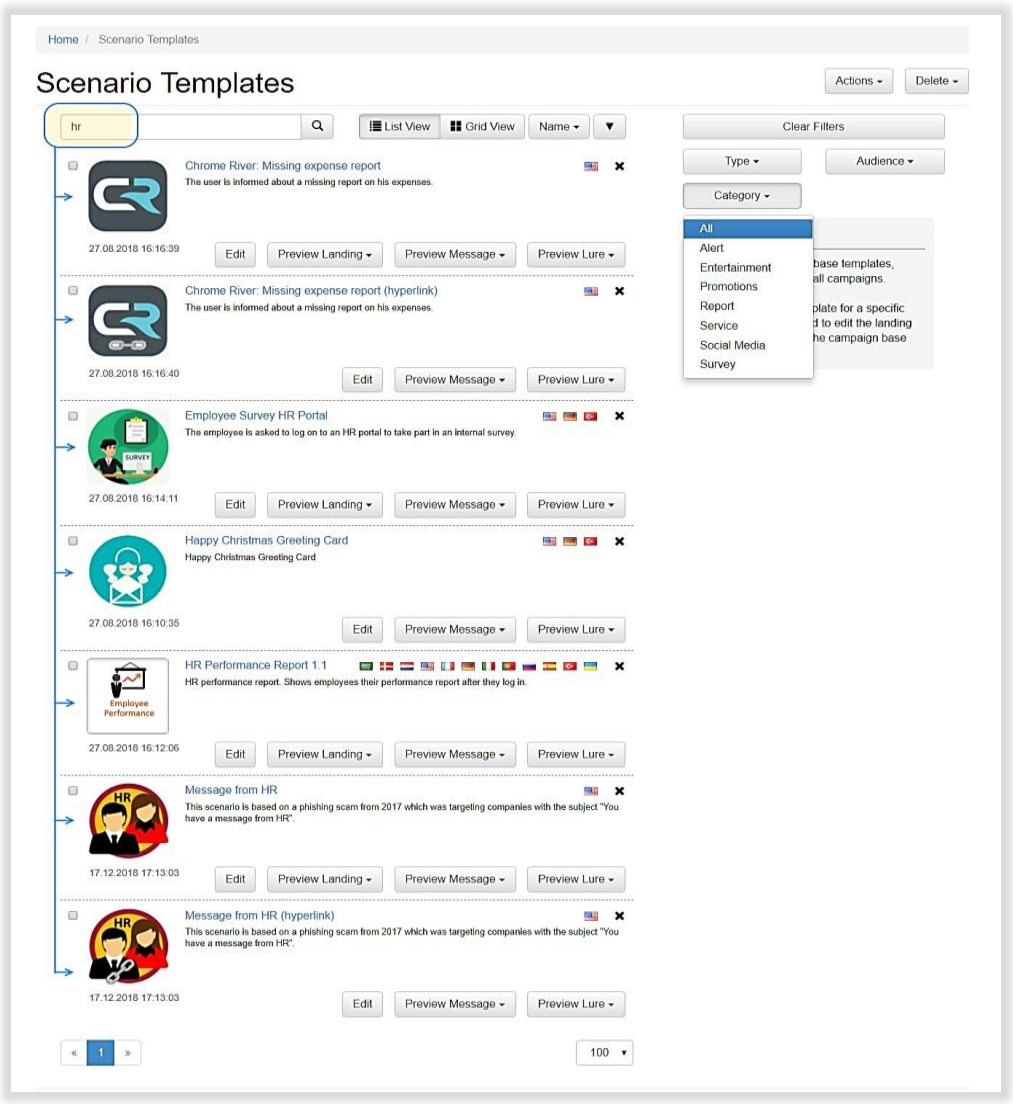
- **Ferramenta de validação de introdução de dados:** Em simulações de phishing, os falsos positivos devem ser evitados para os campos de login (por exemplo, acessos com sintaxe inválida). As diretrizes da empresa também podem proibir a transmissão de dados sensíveis, como palavras-passe. Para este fim, o LUCY fornece um motor flexível de filtragem de entrada que oferece uma solução adequada para cada requisito.



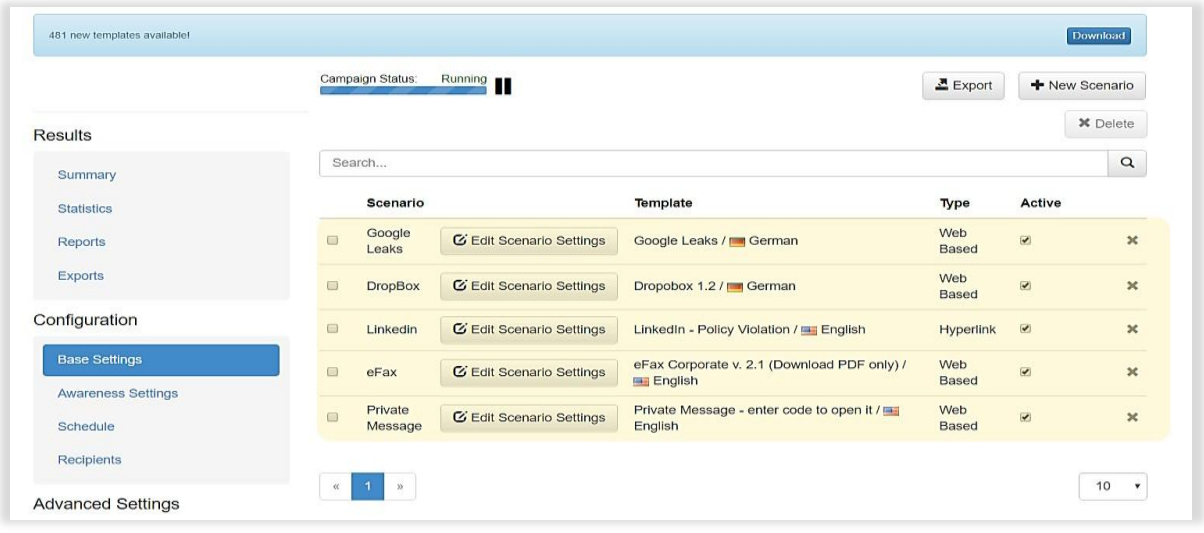
- **Biblioteca de modelos de ataque multilingue:** O LUCY vem com centenas de modelos de ataque predefinidos em mais de 30 idiomas nas categorias de introdução de dados (modelos com um site), baseados em ficheiros (e-mails ou sites com um download de ficheiro), hiperligação (e-mails com um link), mistos (combinação de introdução e download de dados), e média portátil.



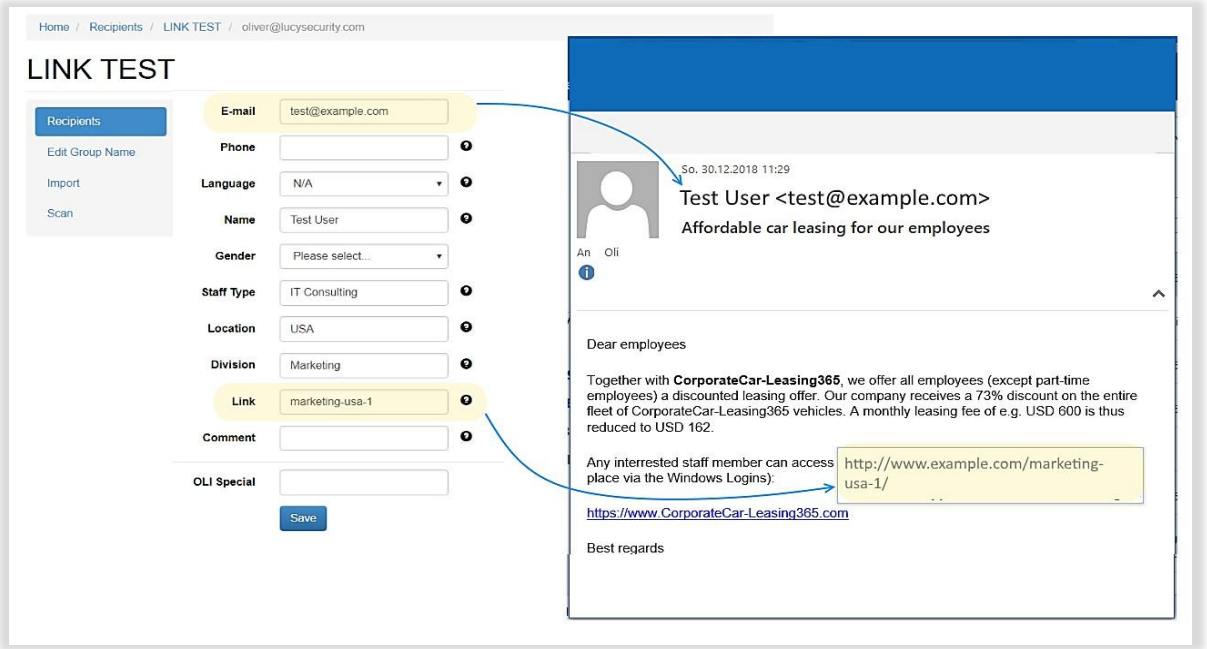
- **Modelos específicos de setor e divisão:** Estão disponíveis modelos de ataque para setores ou divisões específicas.



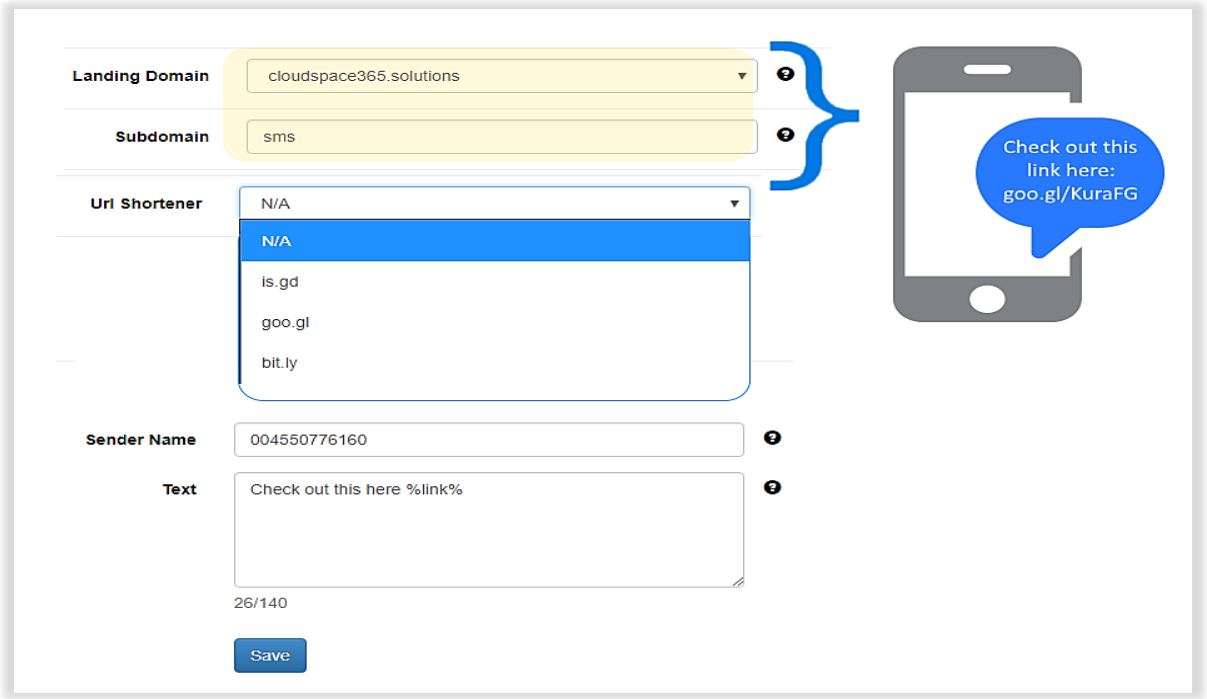
- **Utilização simultânea de modelos de ataque:** O LUCY dá-lhe a opção de usar vários modelos de ataque simulados numa única campanha. Misture os diferentes tipos (hiperligação, baseado em ficheiros, etc.) com diferentes temas de ataque para alcançar a maior cobertura de risco possível e uma melhor compreensão das vulnerabilidades dos funcionários. Em combinação com o nosso gerador aleatório de agendamento, podem ser executados padrões complexos de ataque durante um longo período de tempo.



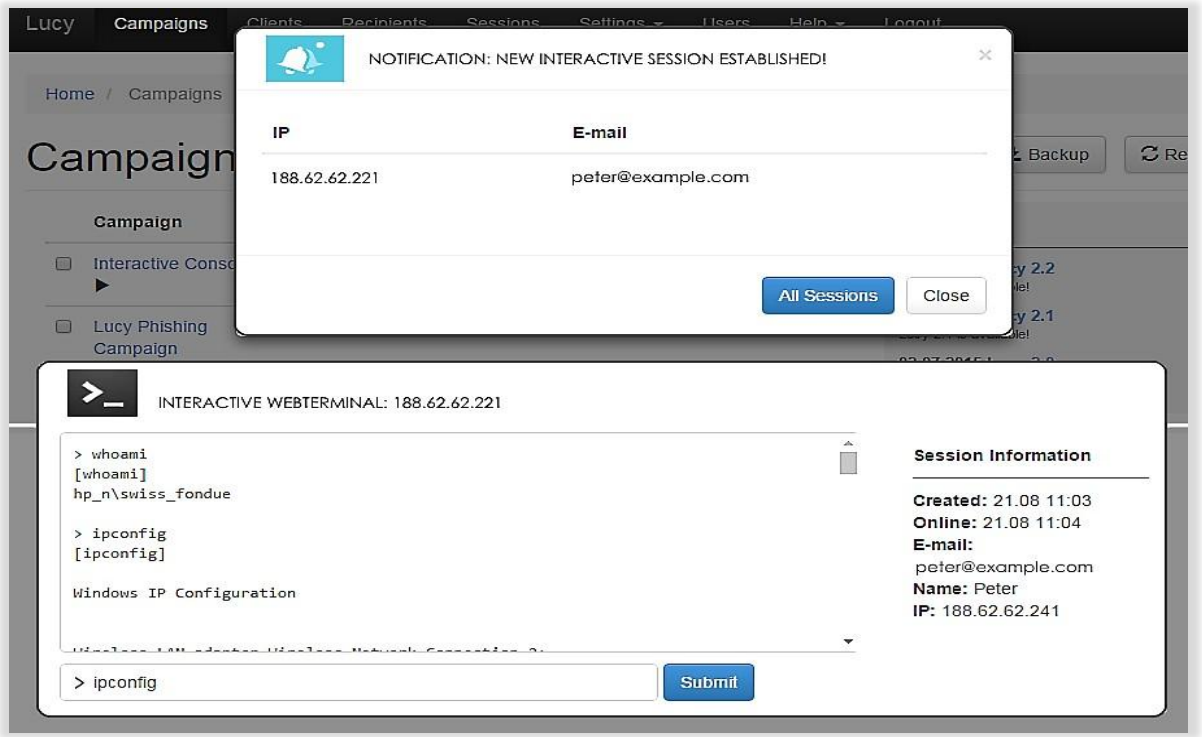
- **Variações de URL de ataque:** Assuma o controle dos URLs gerados para identificar os destinatários. Use strings de URL curtas (< 5 caracteres) ou longas automatizadas ou defina URLs individuais para cada utilizador. A criação manual de URL permite-lhe formar links que um utilizador pode memorizar facilmente. Nos ambientes em que os cliques no link são desativados nos emails, isso é obrigatório.



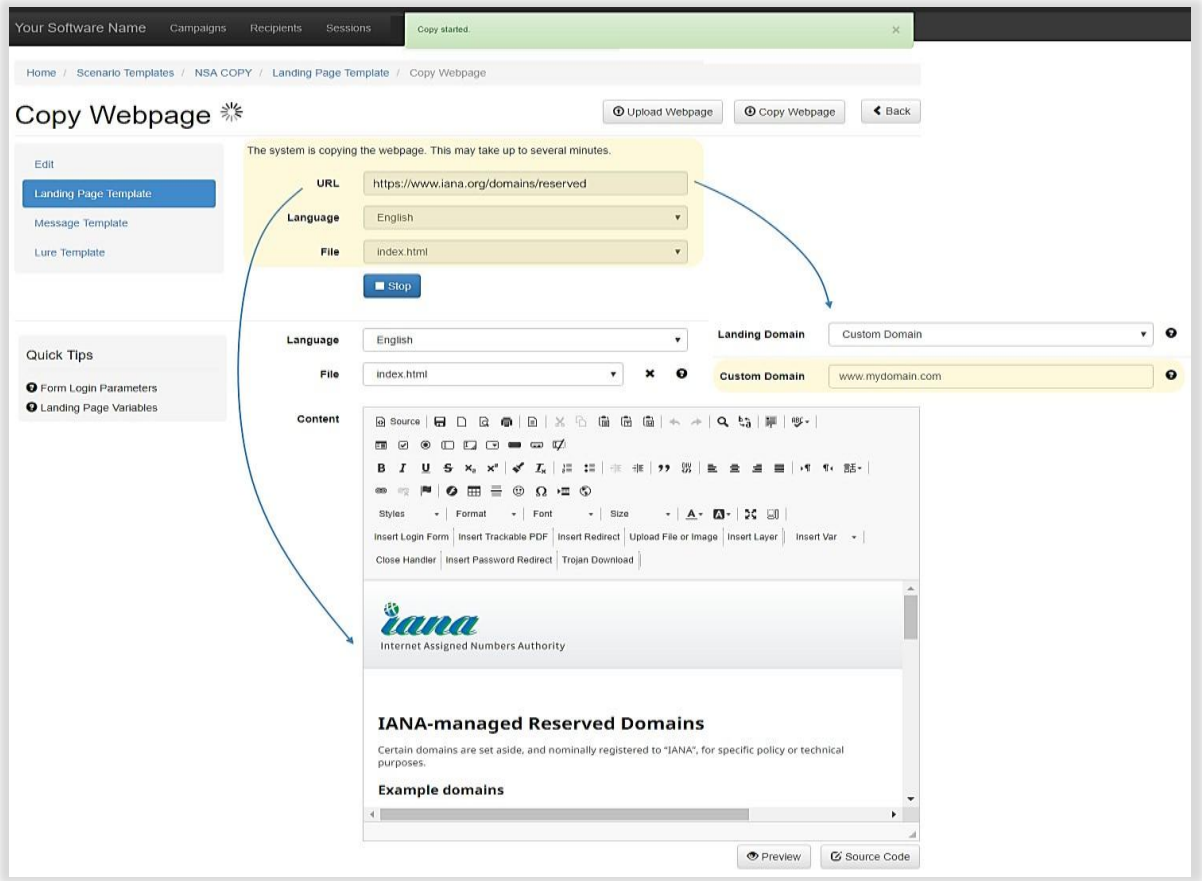
- **Encurtamento de URL:** O encurtamento de URL é um serviço de Internet relativamente novo. Como muitos serviços sociais online impõem limitações de caracteres (por exemplo, o Twitter), estes URLs são muito práticos. No entanto, o encurtamento de URL pode ser usado por cibercriminosos para esconder o alvo real de um link, tal como phishing ou site infetados. Por esta razão, o LUCY oferece a possibilidade de integrar diferentes serviços de encurtamento dentro de uma campanha de phishing ou smishing.



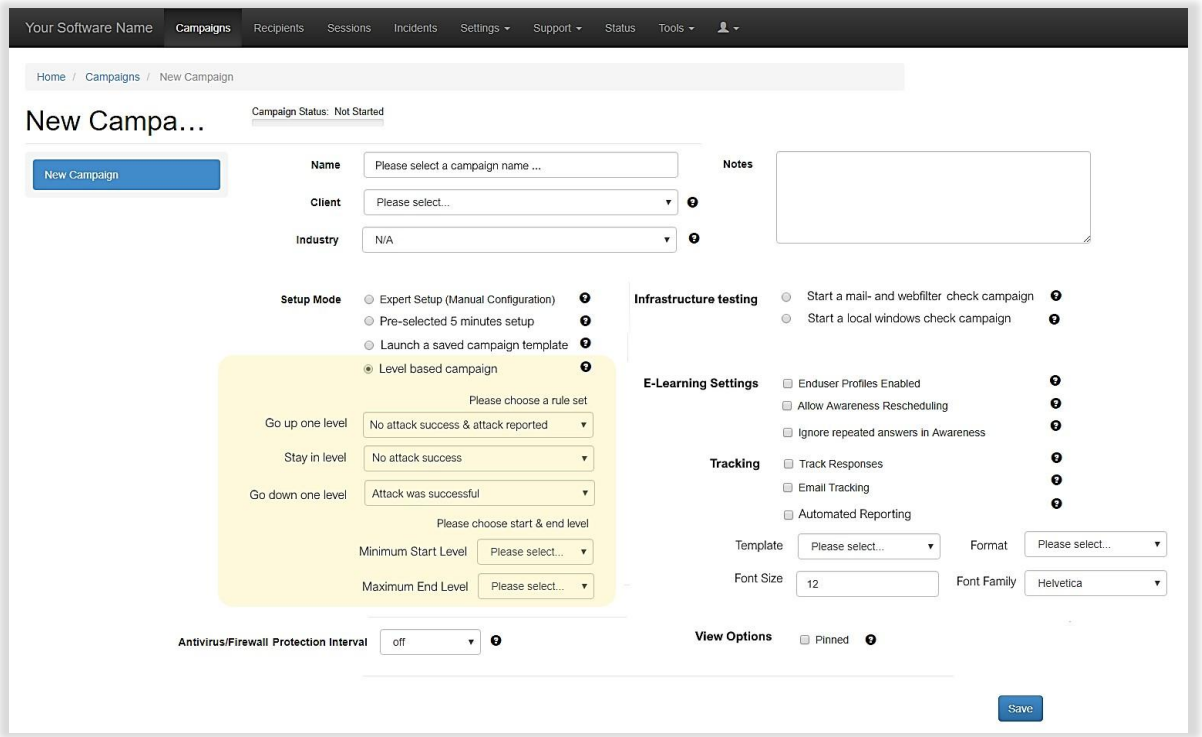
- **Kit pentest:** O kit pentest é um sub-módulo da ferramenta de simulação de malware e dá-se pelo nome de "Sessões Interativas." Ele permite-lhe comunicar interativamente com um PC cliente que esteja atrás de firewalls, usando conexões http/s inversas.



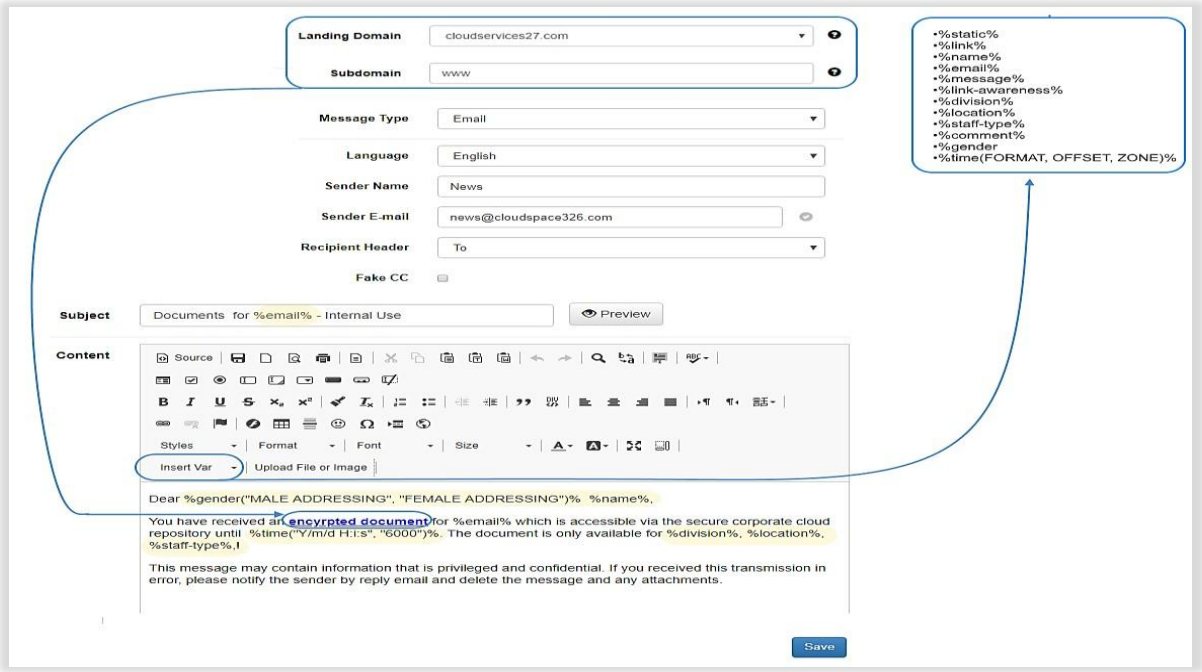
- **Clonador de site:** Crie rapidamente páginas de destino altamente profissionais para as suas campanhas. Clone sites existentes e adicione camadas adicionais com campos de introdução de dados, ficheiros para download e muito mais.



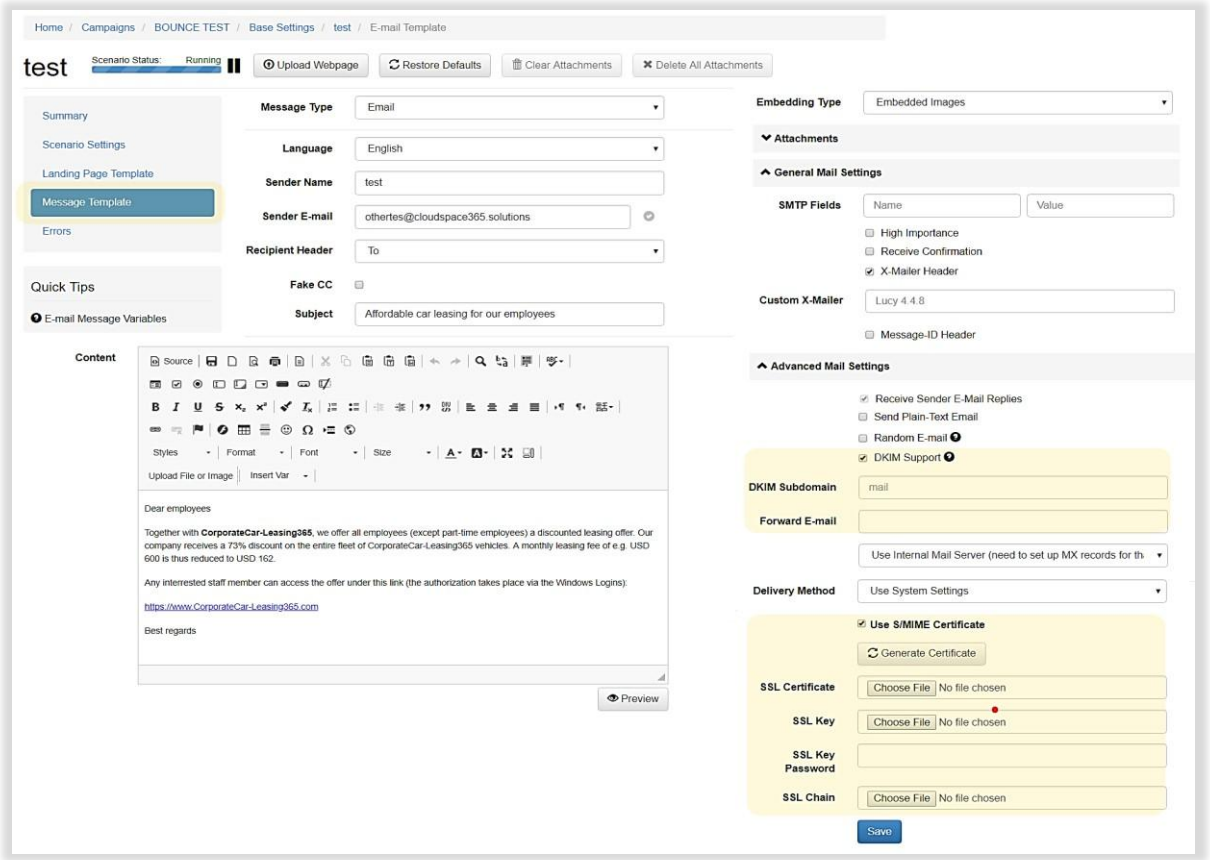
- **Ataques baseados em nível:** A formação de phishing baseado em nível para funcionários serve para tornar o risco de hacking social mensurável. A análise científica também deve identificar os fatores de risco mais importantes para que o conteúdo da formação individual possa ser disponibilizado automaticamente.



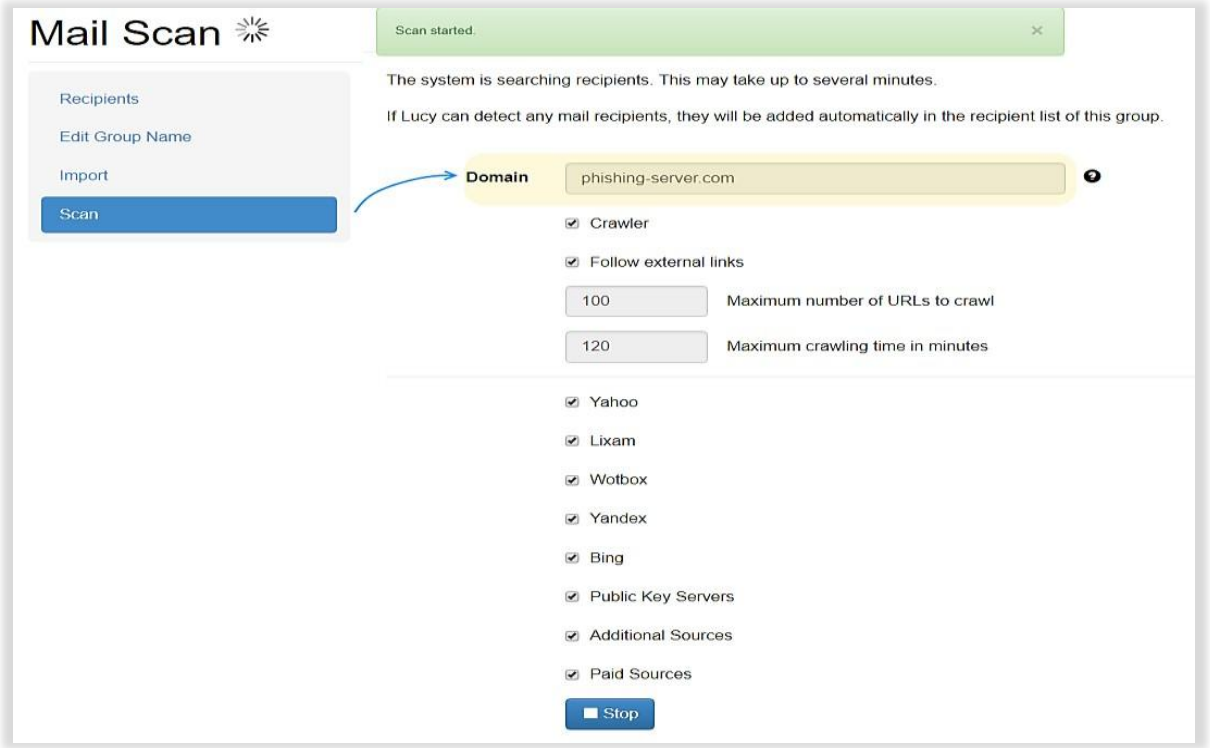
- **Simulação de spear phishing:** O Spear Phish Tailoring trabalha com variáveis dinâmicas (sexo, hora, nome, email, links, mensagens, divisão, país, etc.) que pode usar nos modelos de destino e mensagem.



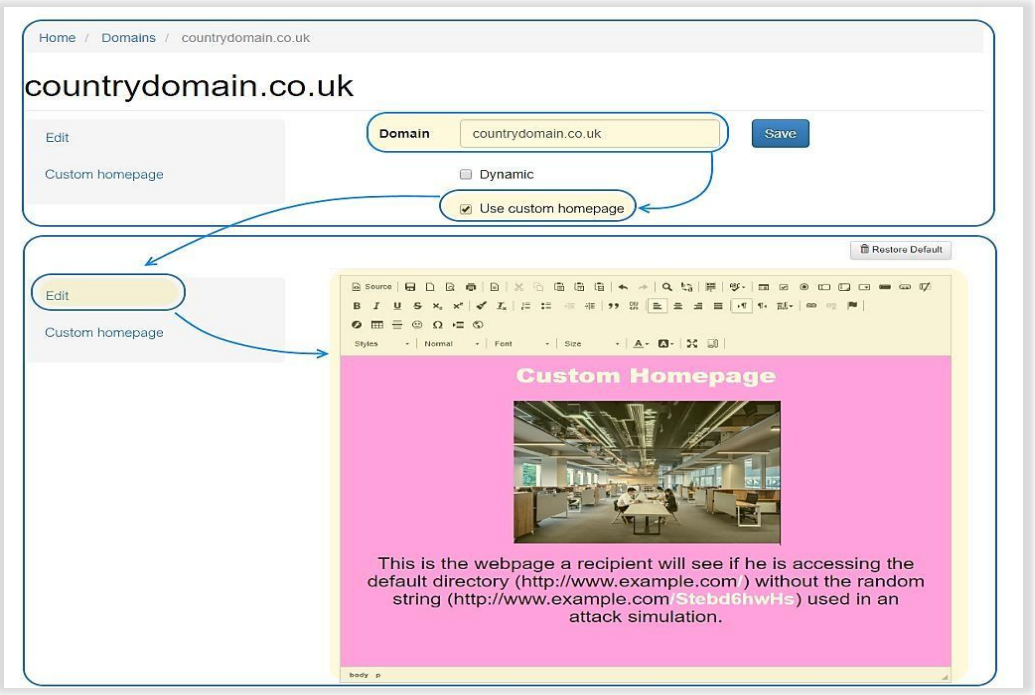
- **Suporte DKIM / S / MIME para e-mails de Phishing:** Assinaturas digitais para e-mails: enviar mensagens de simulação de phishing assinadas (s/mime). Use o DKIM para obter uma melhor pontuação de remetente.



- **Scanner de e-mail:** Curioso sobre quais são os endereços de e-mail da sua organização que podem ser encontrados na Internet? Use o scanner de correio da LUCY e descubra o que é que um hacker já sabe sobre a sua empresa.

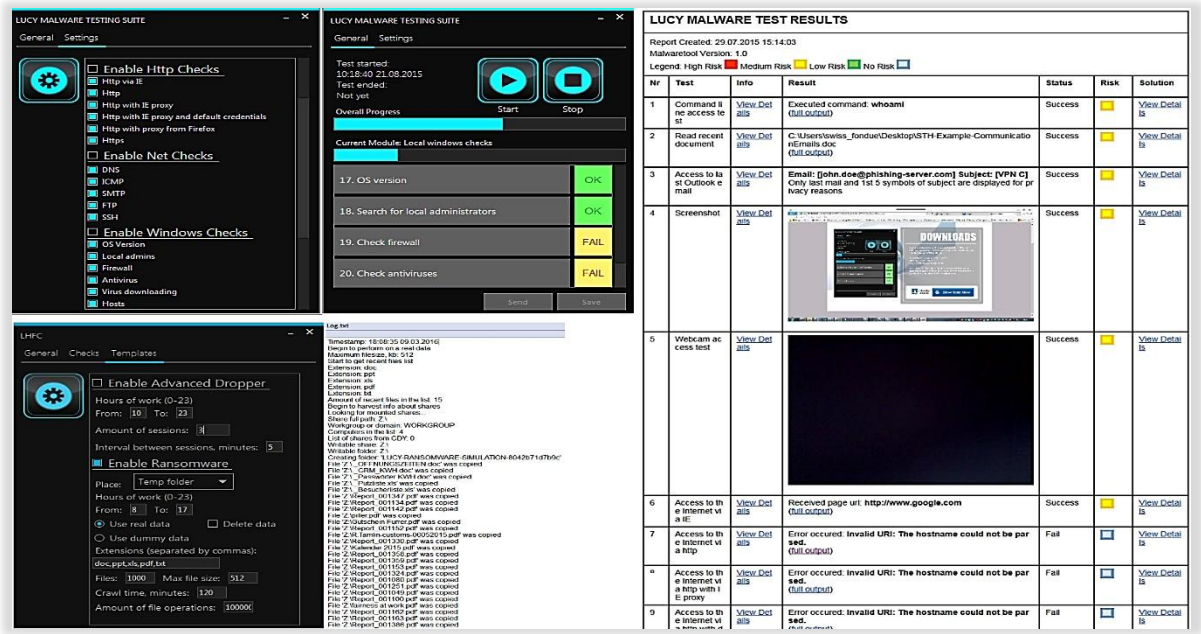


- **Criação de páginas iniciais personalizadas:** Os destinatários com um melhor entendimento técnico podem usar o navegador para chamar o domínio ou o endereço de IP associado ao link de phishing gerado aleatoriamente. Para evitar que apareçam mensagens de erro ou que o utilizador final chegue à área de autenticação da consola de administração, poderá criar "páginas iniciais" genéricas dentro do LUCY para os domínios usados na simulação de phishing.

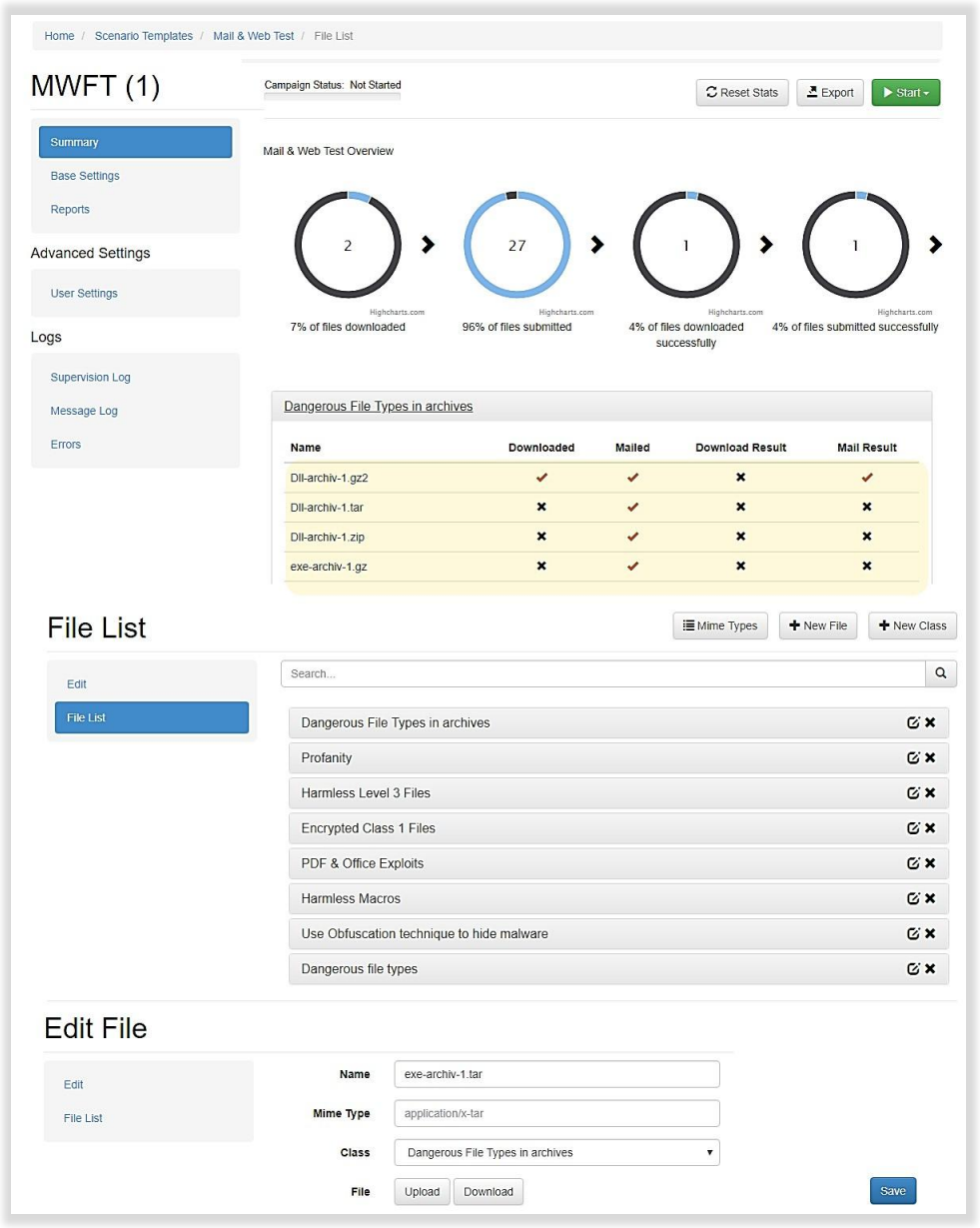


TESTE DA INFRAESTRUTURA

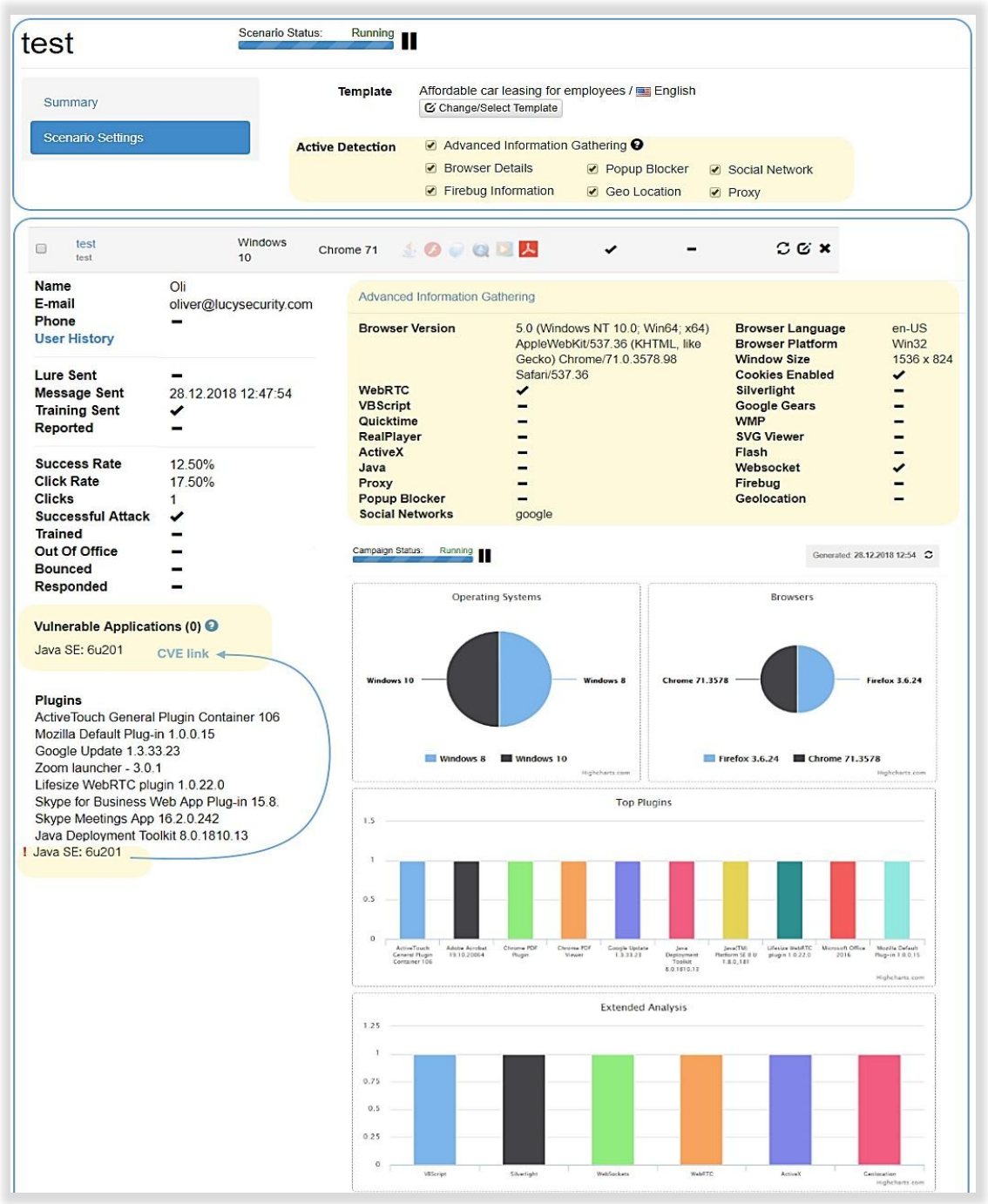
- **Ferramenta de teste de malware:** A ferramenta de simulação de malware é um pacote avançado de simulação de malware capaz de emular várias ameaças. Ela permite que um auditor aceda um conjunto avançado de recursos equivalentes a muitas das ferramentas utilizadas por cibercriminosos. Portanto, a ferramenta permite ao administrador LUCY realizar verificações de segurança sem envolver funcionários externos ao departamento de TI.



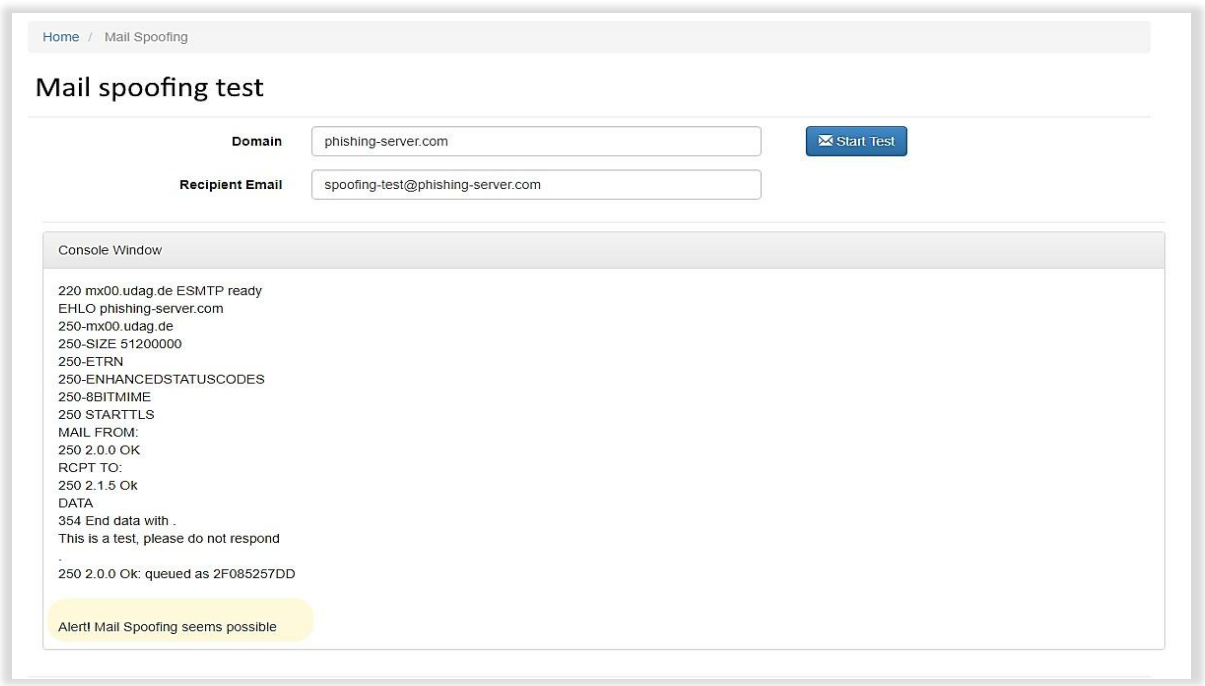
- **Teste de filtro de e-mail e web:** Esta funcionalidade dá a resposta a uma das questões mais importantes na segurança do tráfego da Internet e do e-mail: que tipos de ficheiros podem ser descarregados da Web e que anexos de e-mail são filtrados ou não?



- **Deteção de vulnerabilidade ativa e passiva do cliente:** Esta funcionalidade permite testar localmente o navegador do cliente e detetar possíveis vulnerabilidades, com base em bibliotecas personalizadas de JavaScript e nos dados do agente de utilizador do navegador. Os plugins descobertos podem ser automaticamente comparados com as bases de dados de vulnerabilidade (CVE) para identificar dispositivos vulneráveis.

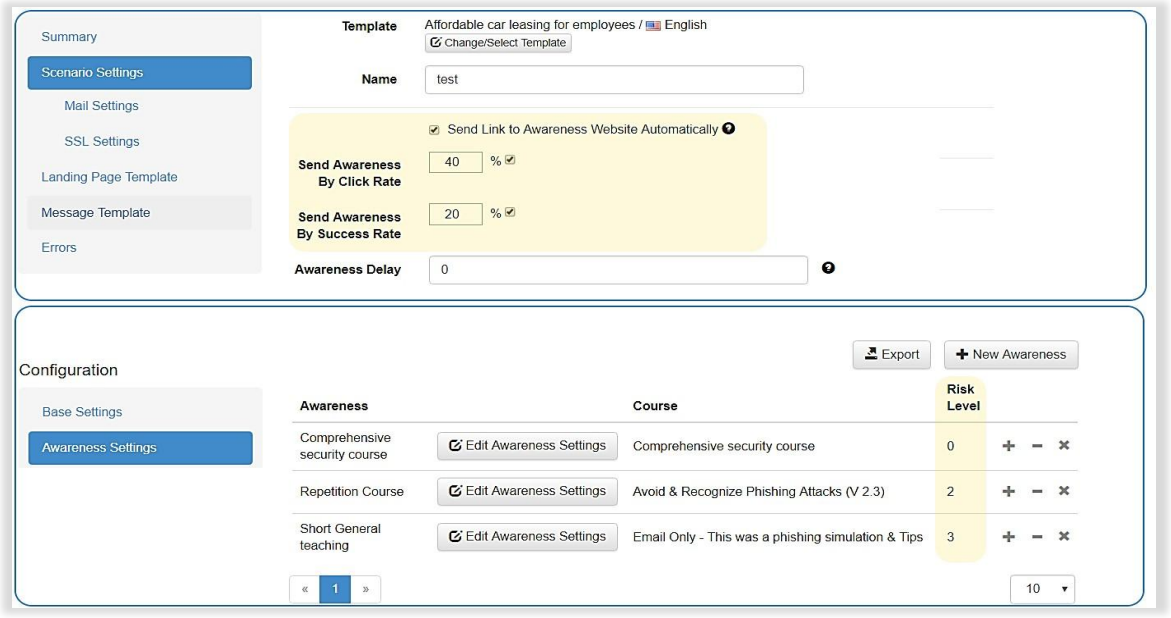


- **Teste de spoofing:** Teste a sua própria infraestrutura a vulnerabilidades de spoofing por correio.

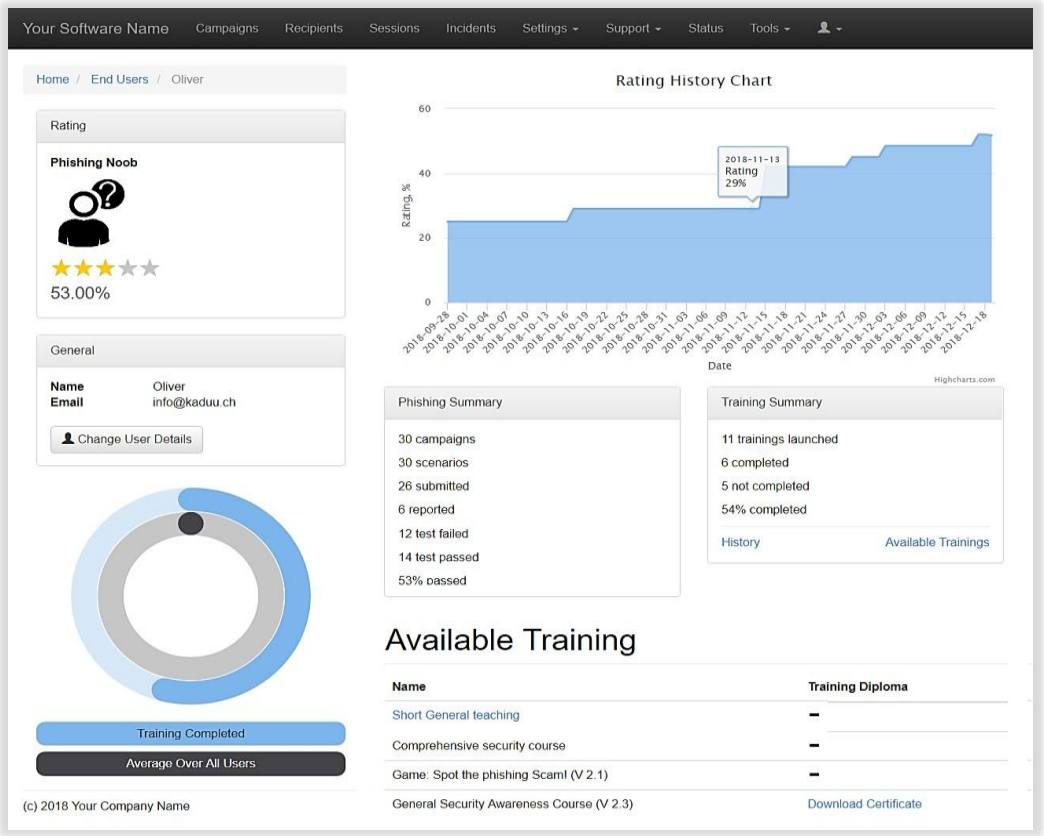


TESTES TÉCNICOS

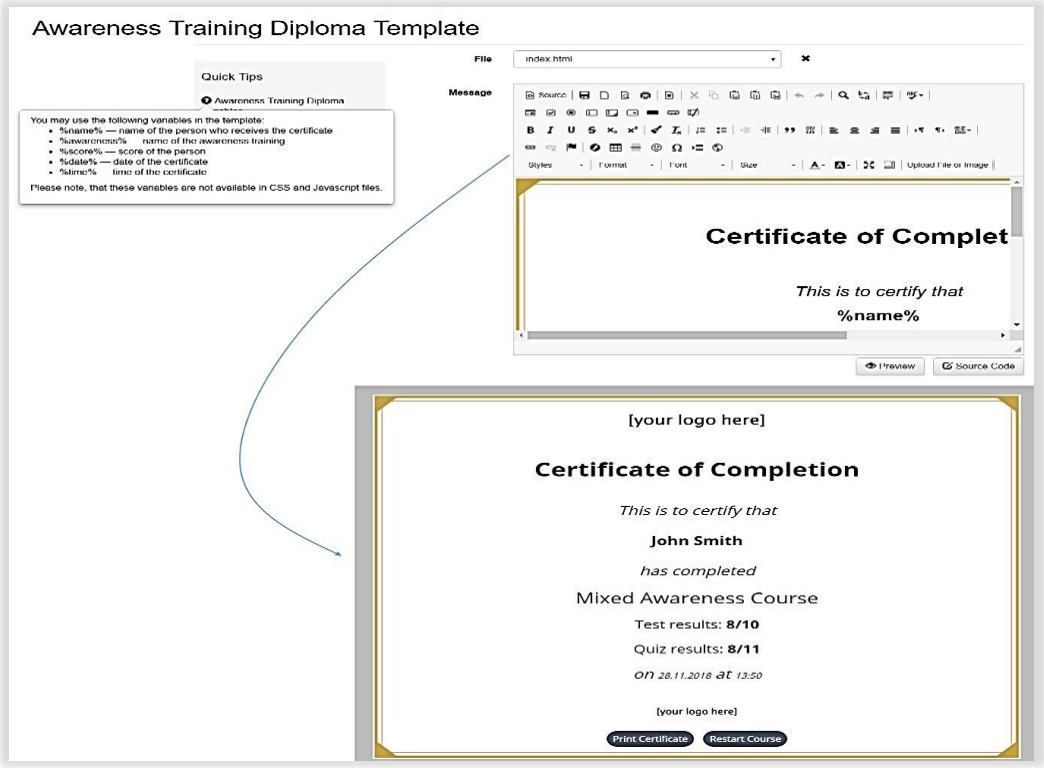
- **Elearning baseado na reputação:** Treine os seus funcionários de acordo com as suas competências de que necessitam. Meça as competências dos funcionários e facilite uma concorrência amigável entre colegas (gamificação).
  Com base nos perfis de reputação de cada utilizador final, o sistema pode fornecer-lhes automaticamente várias sessões de formação. Os perfis de reputação baseiam-se, entre outros fatores, no comportamento do utilizador em simulações de phishing. Isto garante que os utilizadores que são infratores reincidentes recebem conteúdos de formação diferentes daqueles que clicam numa simulação de ataque pela primeira vez.



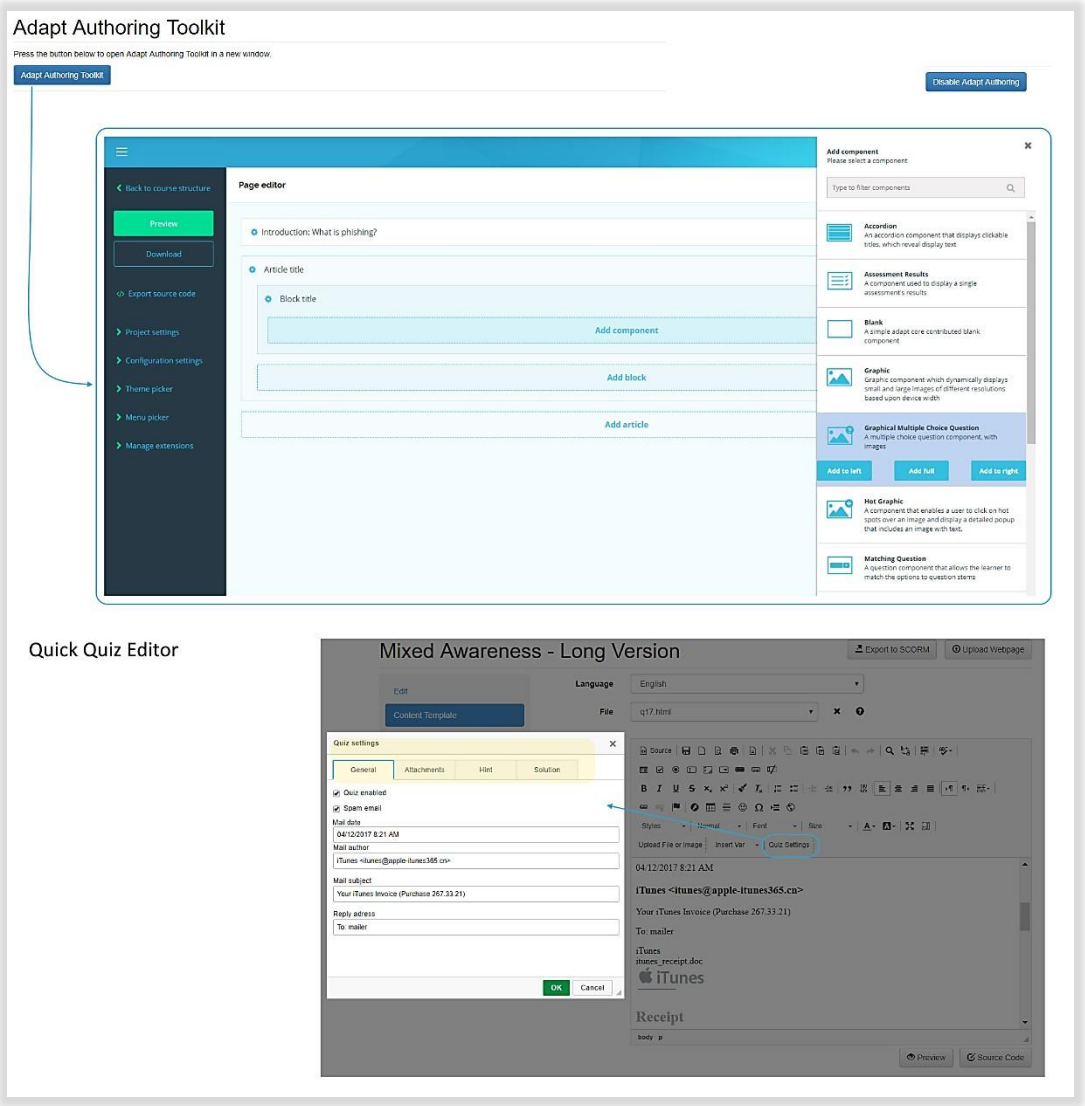
- **Portal de formação do utilizador final:** Funcionalidade do Sistema de Gestão de Aprendizagem (SGA): dá a cada funcionário acesso permanente a uma página inicial de formação personalizada que apresenta os seus próprios cursos, especificamente adaptados para eles. Nesta página inicial eles podem ver as suas estatísticas de desempenho, retomar ou repetir a formação, criar certificados de curso e comparar os seus resultados com outros departamentos ou grupos.



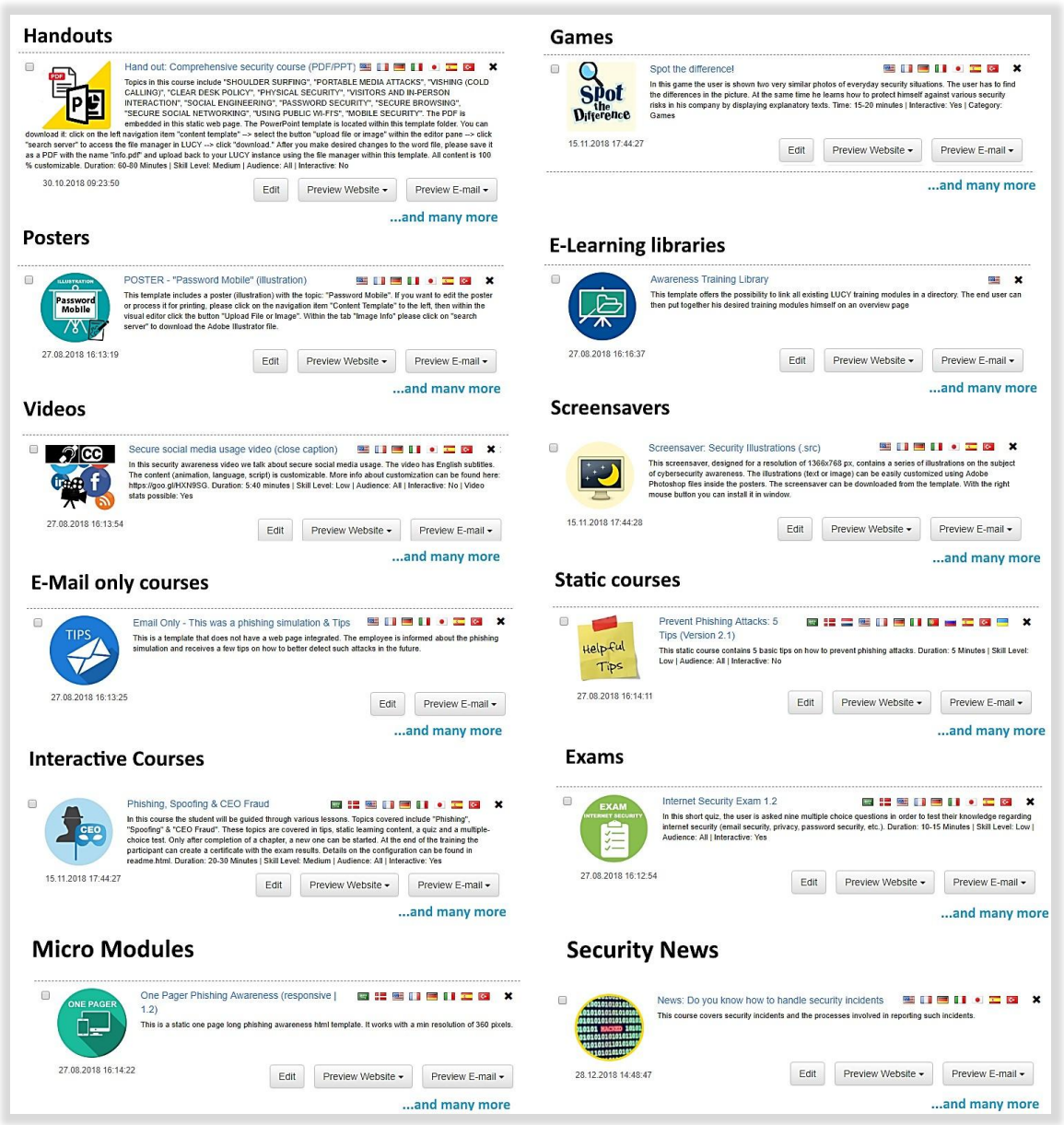
- **Diploma de educação de conscienciali**zação: Os certificados de elearning podem ser criados e impressos pelo destinatário, quer diretamente no âmbito de uma formação, quer dentro do portal SGA.



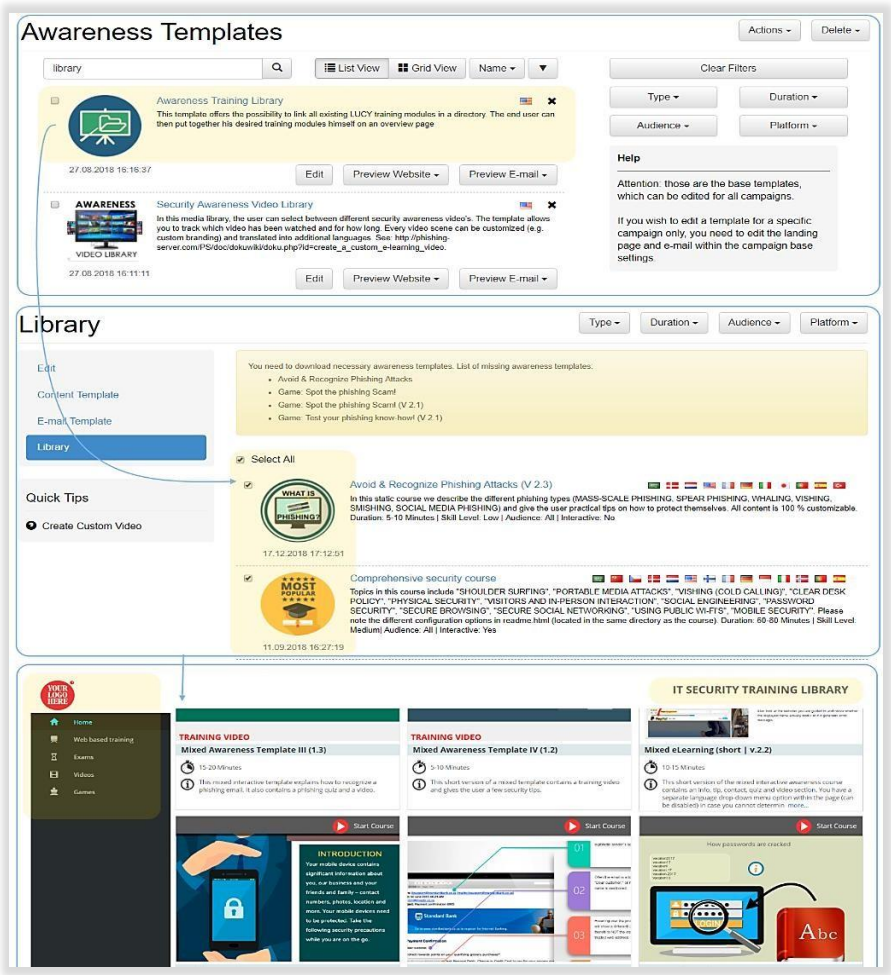
- **Ferramenta de autoria de elearning:** A ferramenta de autoria de elearning (Adapt) permite a criação de conteúdo de aprendizagem individualizado. Arrastar e largar vídeos ou qualquer outro formato de rich media, inserir exames de menus predefinidos, criar conteúdo interativo de elearning a partir do zero num curto período de tempo.



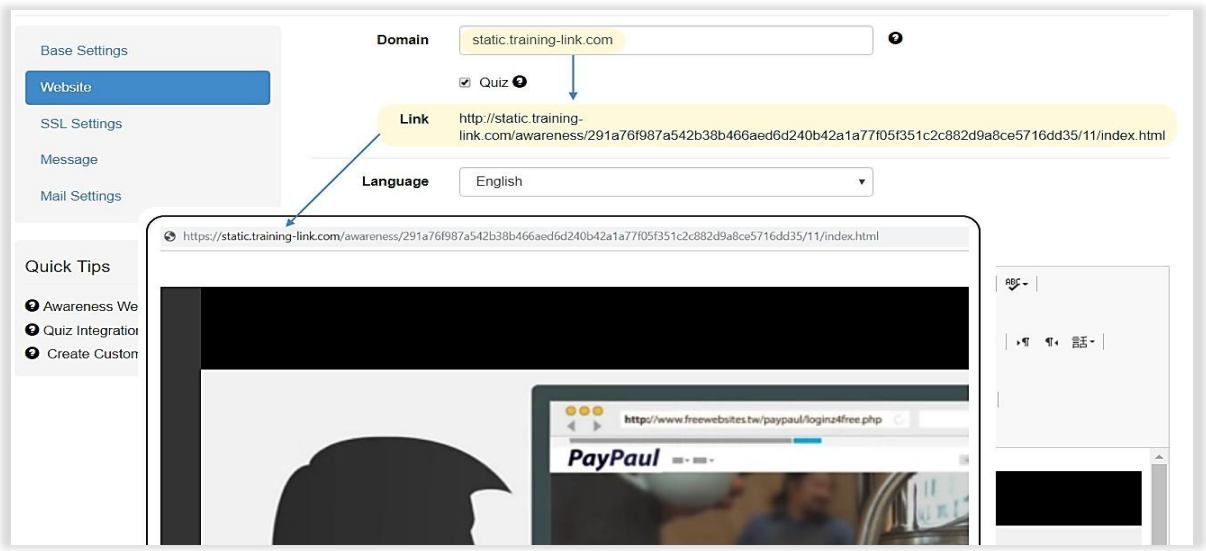
- **Formação de consciencialização rich media:** Integre rich media (vídeo, áudio ou outros elementos que incentivam os visualizadores a interagir e envolver-se com o conteúdo) nas suas formações de consciencialização. Use os vídeos educacionais existentes, adapte-os ou adicione a sua própria rich media.



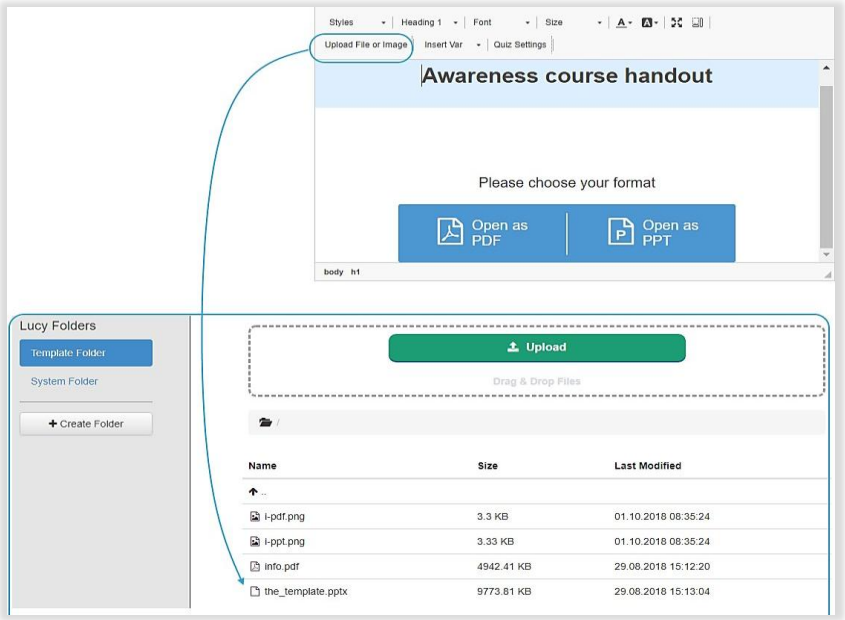
- **Biblioteca de formação:** Os seus funcionários podem aceder ao conteúdo de formação da sua organização a partir de uma página de resumo chamada "biblioteca de formação." Elá contém uma grande seleção de modelos regulares de elearning do LUCY, que servem como introdução. A página de resumo pode ser ordenada por determinados tópicos (vídeo, quiz, teste, etc.).



- **Suporte de formação estática:** O conteúdo de formação também pode ser publicado em páginas estáticas dentro do LUCY ou na intranet, dando ao utilizador acesso permanente ao conteúdo de formação, independente de possíveis simulações de ataque.

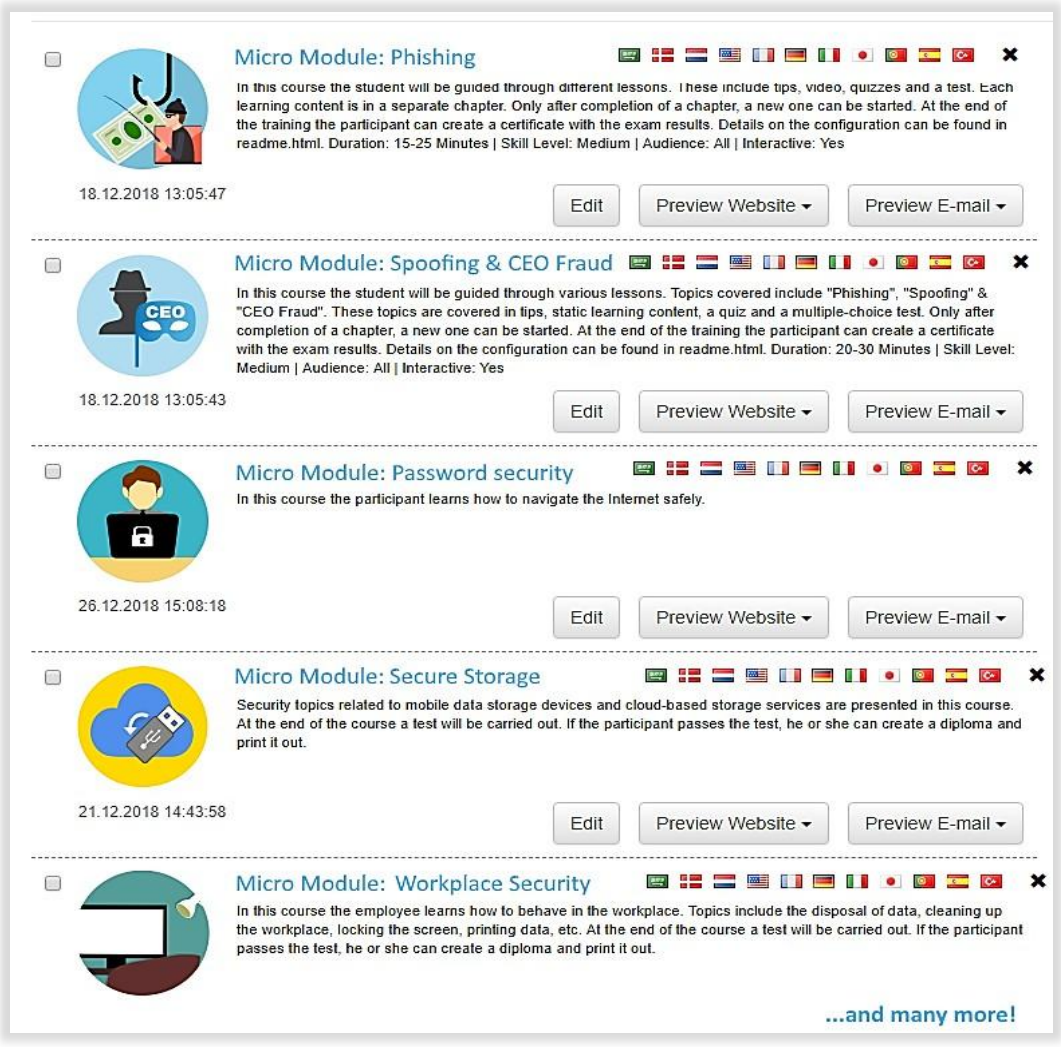


- **Suporte de formação offline:** O LUCY tem uma série de modelos editáveis (ficheiros do Adobe Photoshop ou Illustrador) para formação de consciencialização, tais como posters, protetores de ecrã, panfletos, etc.

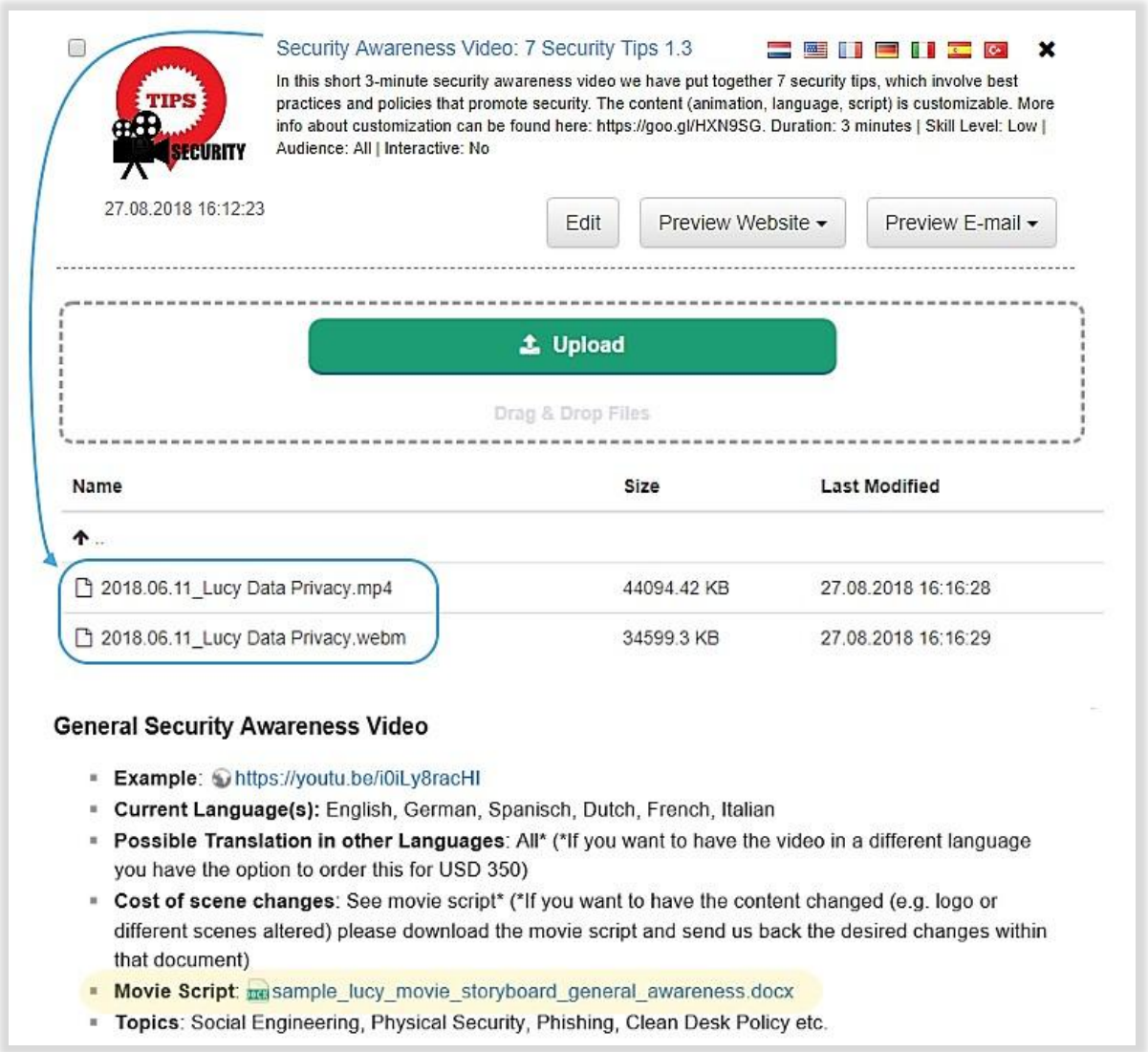


.

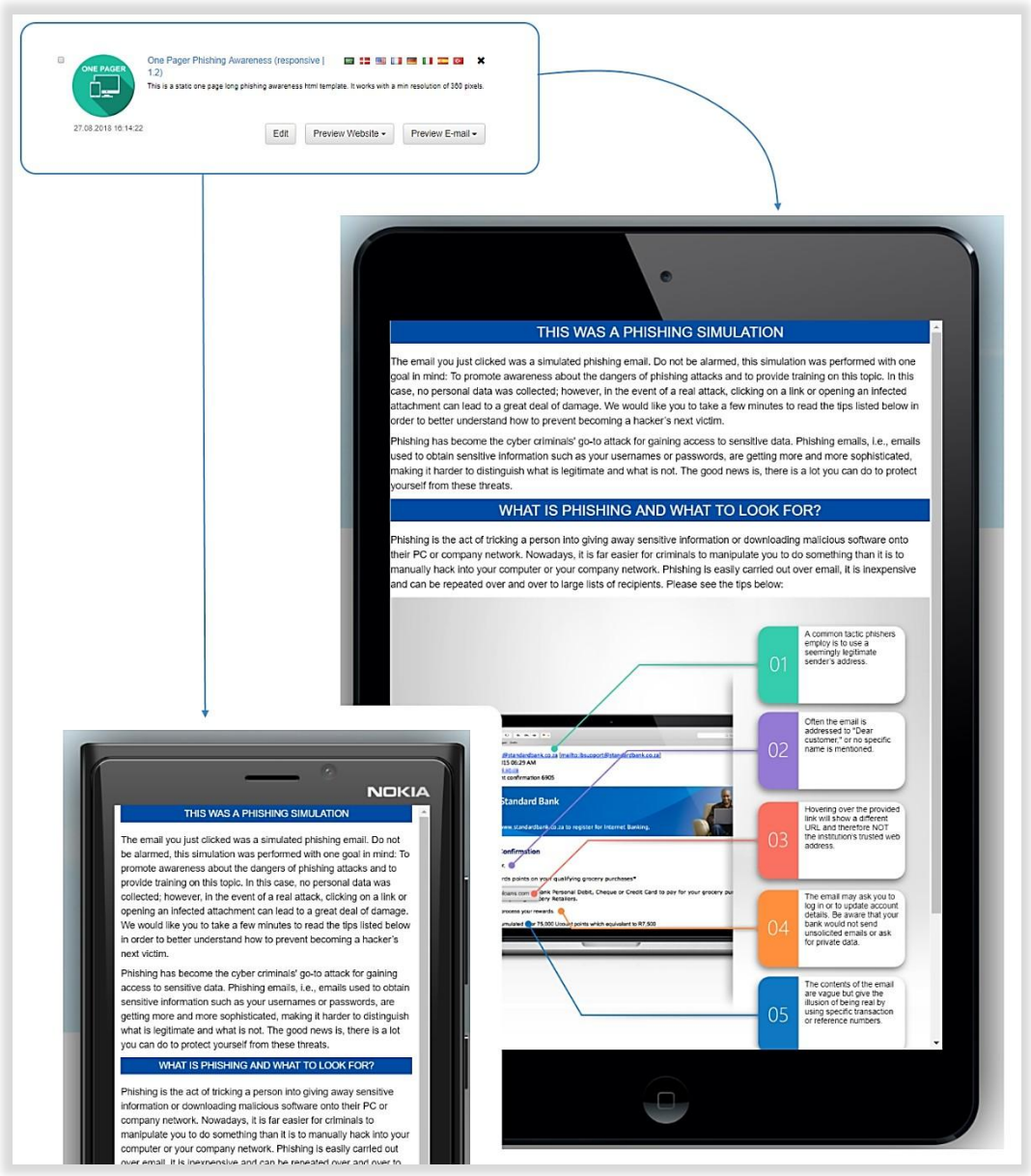
- **Módulos de microaprendizagem:** Concebemos módulos de formação de microaprendizagem (por exemplo, vídeos de 1 minuto ou documentos de uma página para consciencialização) que podem ser adaptados às necessidades da marca e às políticas da sua organização.



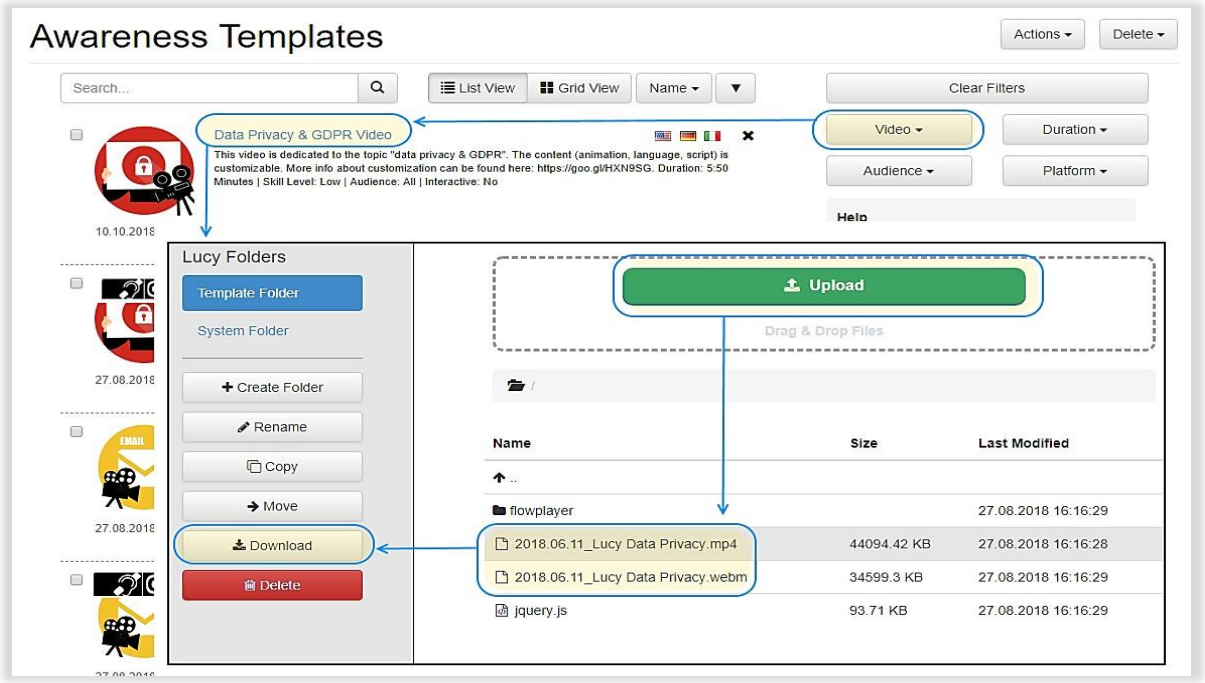
- **Personalização de vídeo:** Envie-nos o logotipo da sua empresa e incluímo-lo nos vídeos de formação. Pretende outro idioma? Não há problema. Definimos o vídeo para ser reproduzido no idioma que preferir. Quer uma cena diferente? Basta descarregar os guiões de vídeo e assinalar as mudanças desejadas.



- **Formato para dispositivos móveis:** Muitos dos módulos incorporados do LUCY estão disponíveis num formato compatível com dispositivos móveis, que dá aos seus utilizadores a flexibilidade de participar da formação em qualquer tipo de dispositivo conectado.



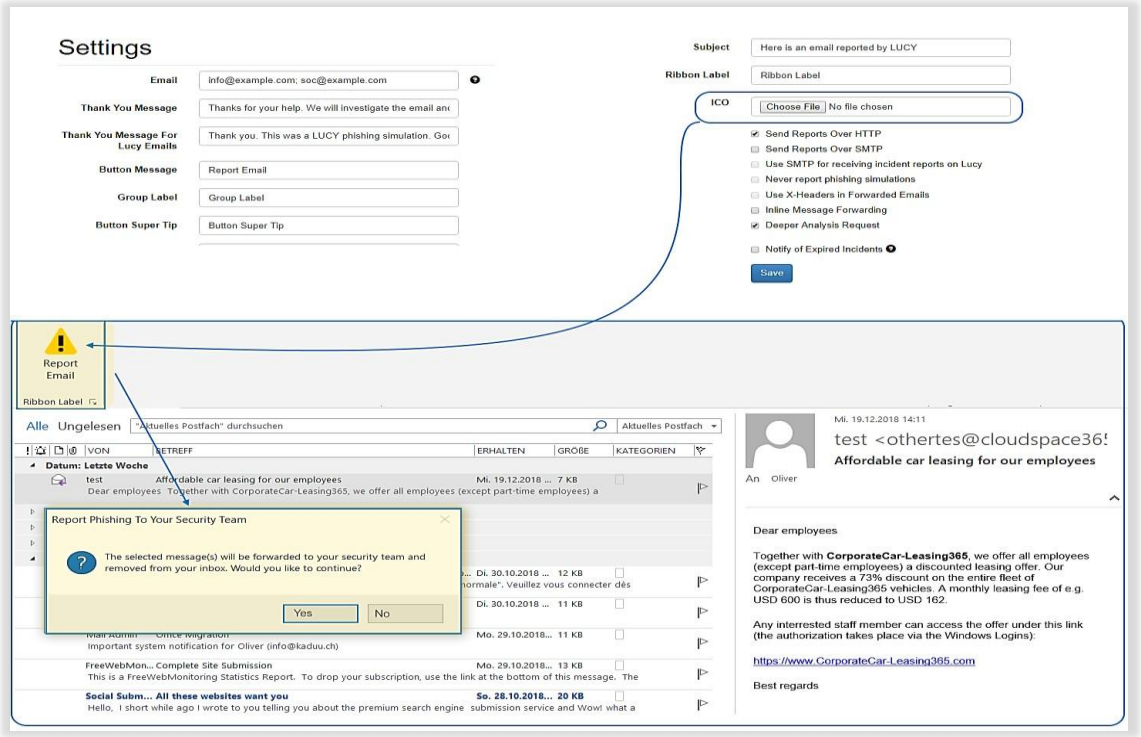
- **Importação / exportação de vídeo:** Pode exportar vídeos LUCY para o seu próprio sistema, bem como importar os seus próprios vídeos para o LUCY.



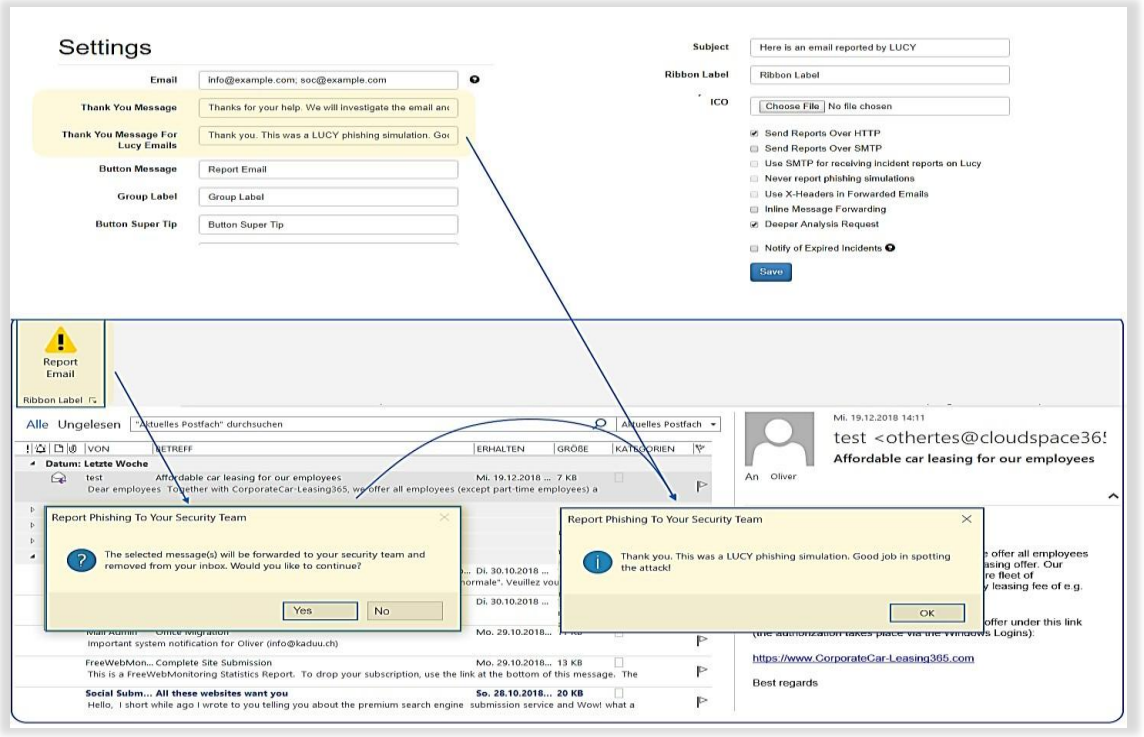
- **Dicas dinâmicas de formação:** As dicas dinâmicas implementadas permitem ao seu administrador definir marcadores nos modelos de ataque que podem indicar aos seus funcionários, dentro do material de elearning, onde é que o ataque de phishing pode ter sido detetado.

ENVOLVER OS FUNCIONÁRIOS

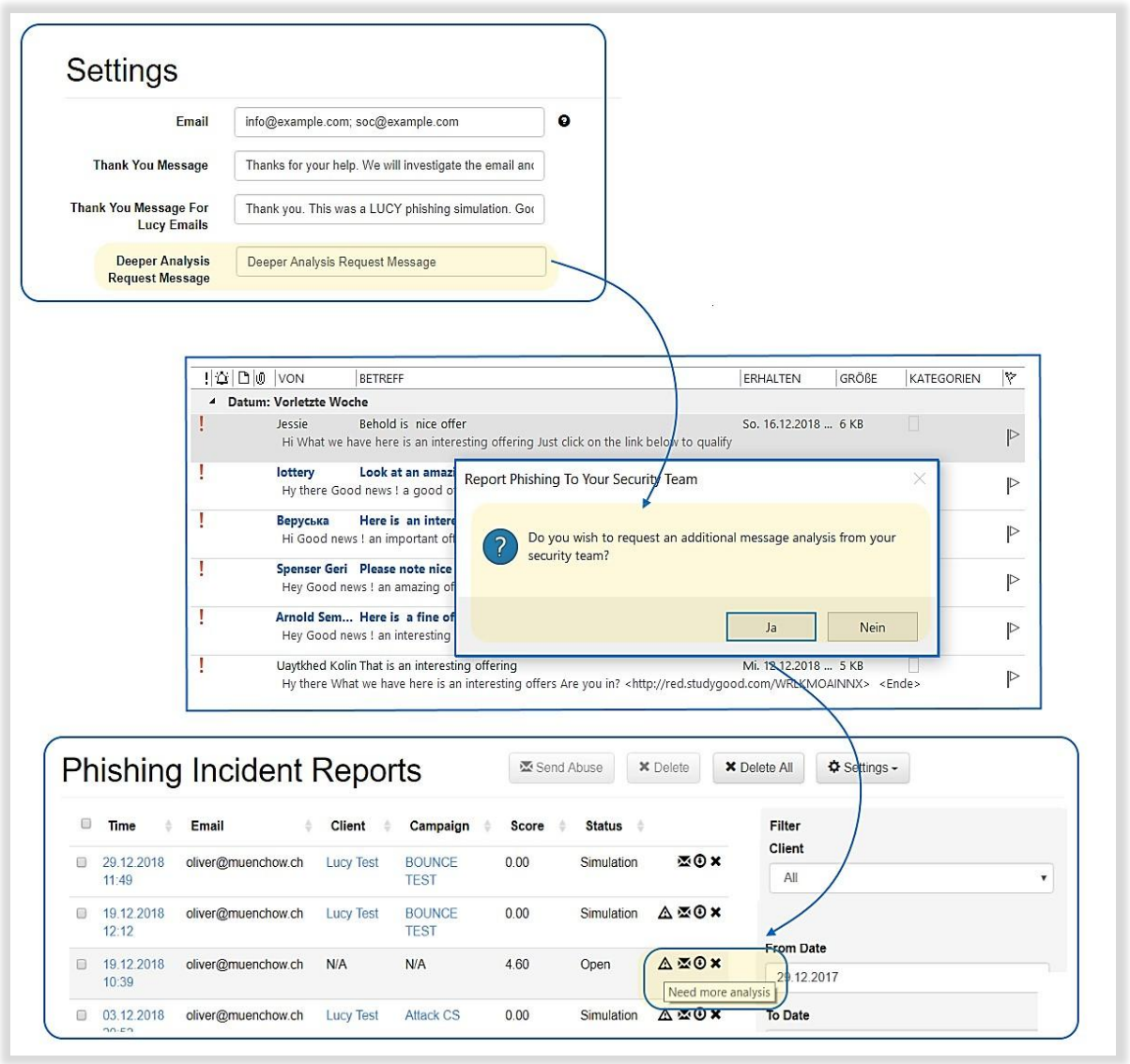
- **Denunciar e-mails com um único clique:** Os utilizadores finais podem denunciar e-mails suspeitos com um único clique em uma ou várias contas de e-mail e reencaminhá-los para a sua consola de análise de incidentes LUCY.



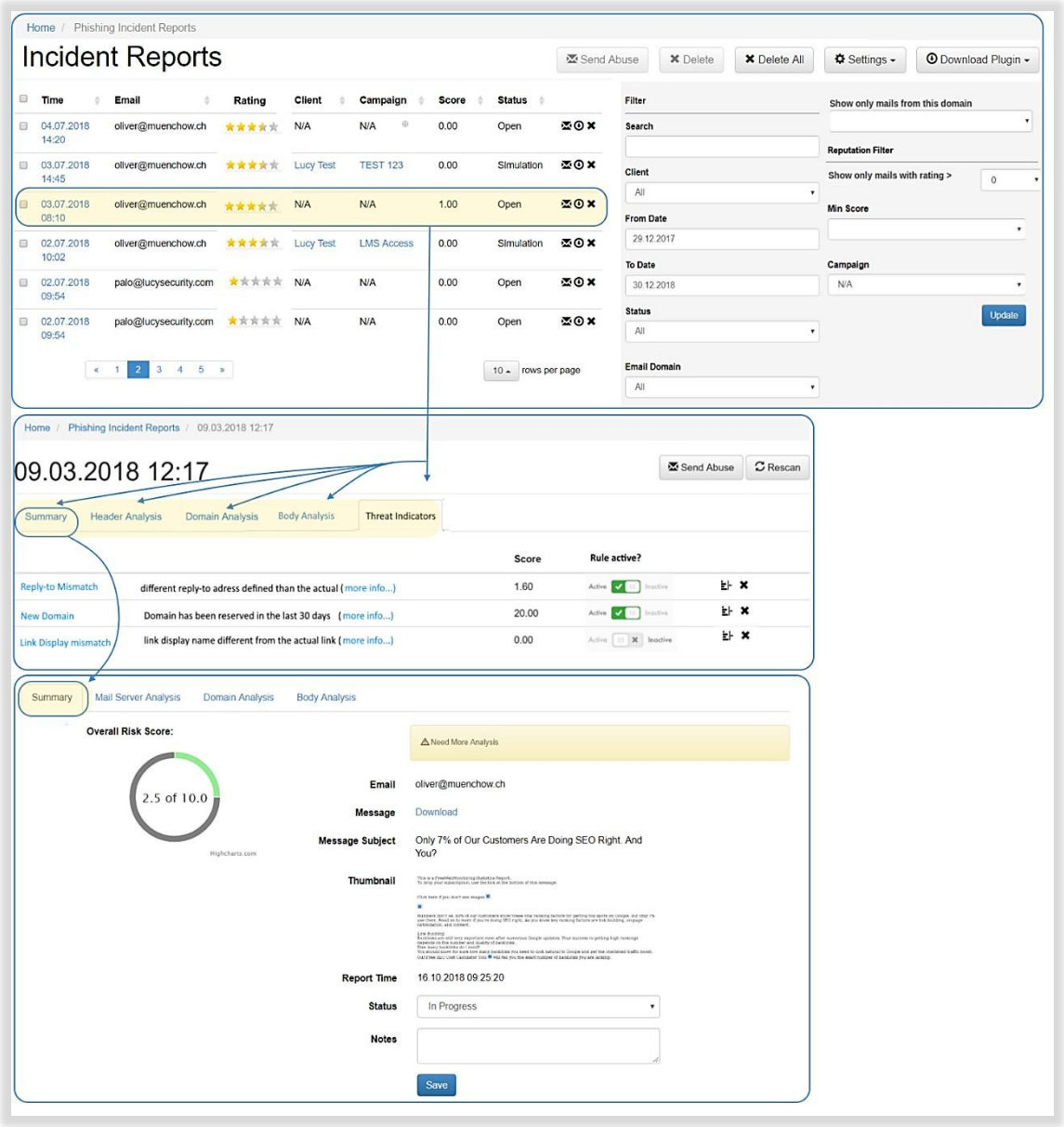
- **Reforço de comportamento positivo:** O nosso plugin fornece automaticamente reforço de comportamento positivo, manifestado gratidão aos utilizadores finais, através de uma mensagem personalizada, definida pela sua organização.



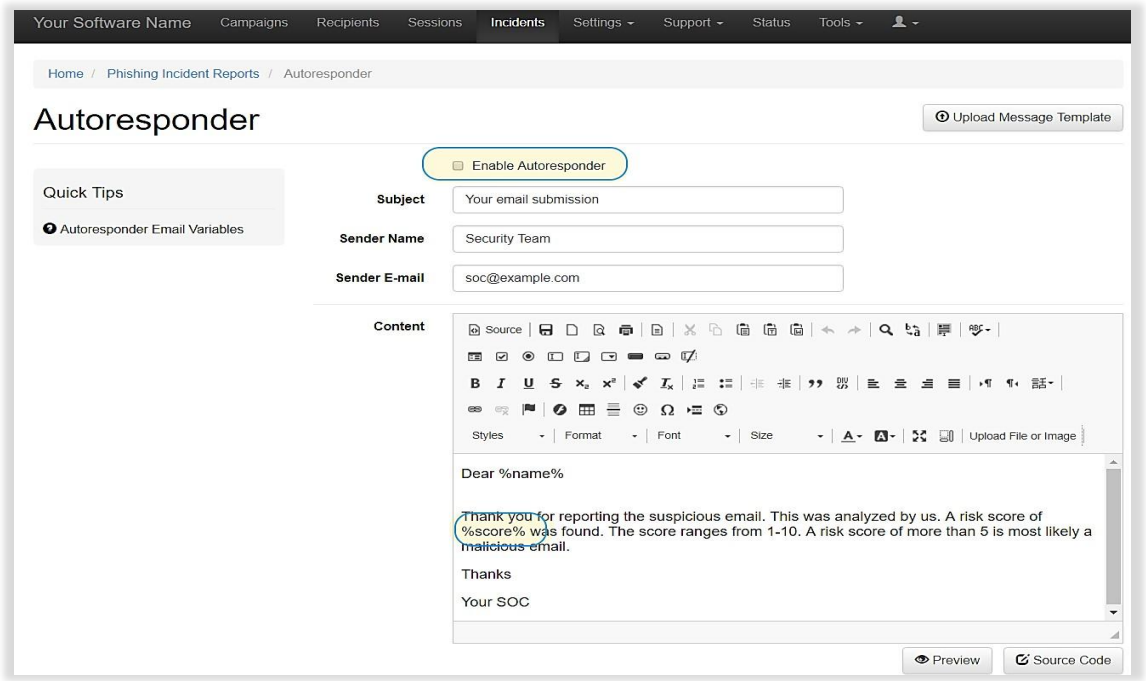
- **Pedido de inspeção aprofundada:** Por vezes, os utilizadores querem saber se o e-mail recebido pode ser aberto com segurança. Opcionalmente, o utilizador pode usar o "pedido de inspeção aprofundada" dentro do plugin local para dizer à equipa de segurança que quer um feedback sobre o e-mail comunicado.



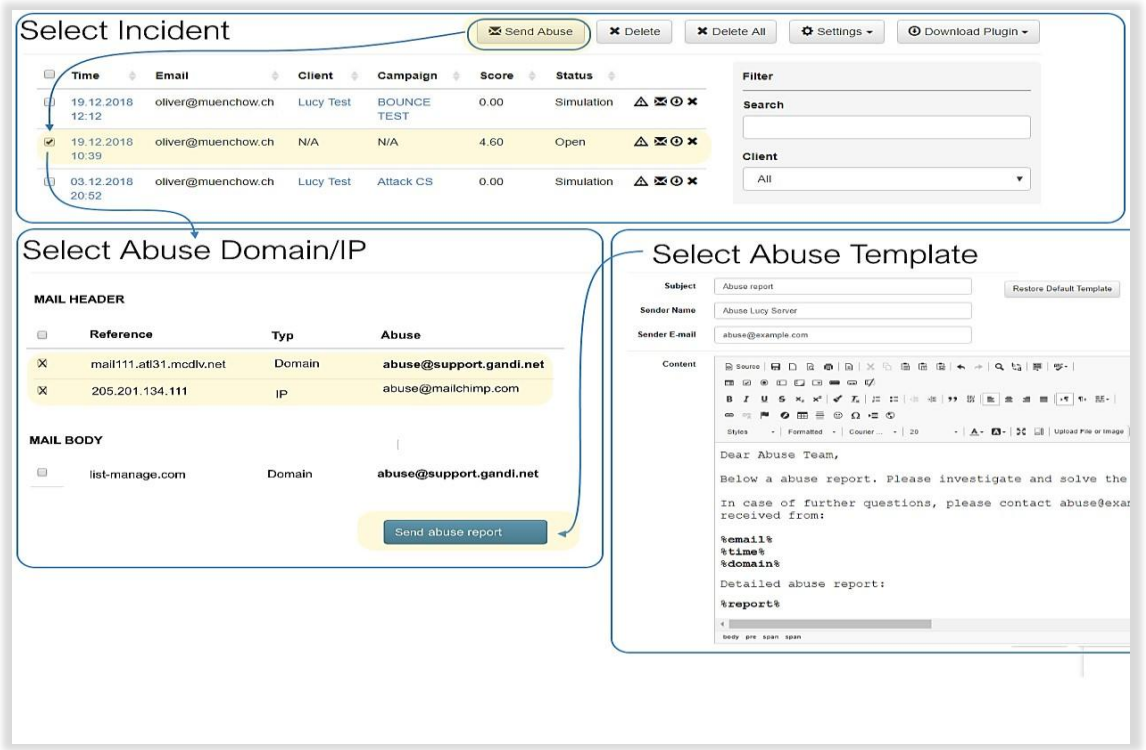
- **Análise automática de incidentes:** Gerir e responder a e-mails suspeitos denunciados por meio de uma consola de gestão centralizada: o analisador do LUCY permite fazer uma inspeção automatizada das mensagens denunciadas (cabeçalho e corpo). O analisador inclui uma pontuação de risco individual, fornecendo uma classificação em tempo real de e-mails denunciados. O analisador de ameaças representa um alívio notável da carga de trabalho da equipa de segurança.



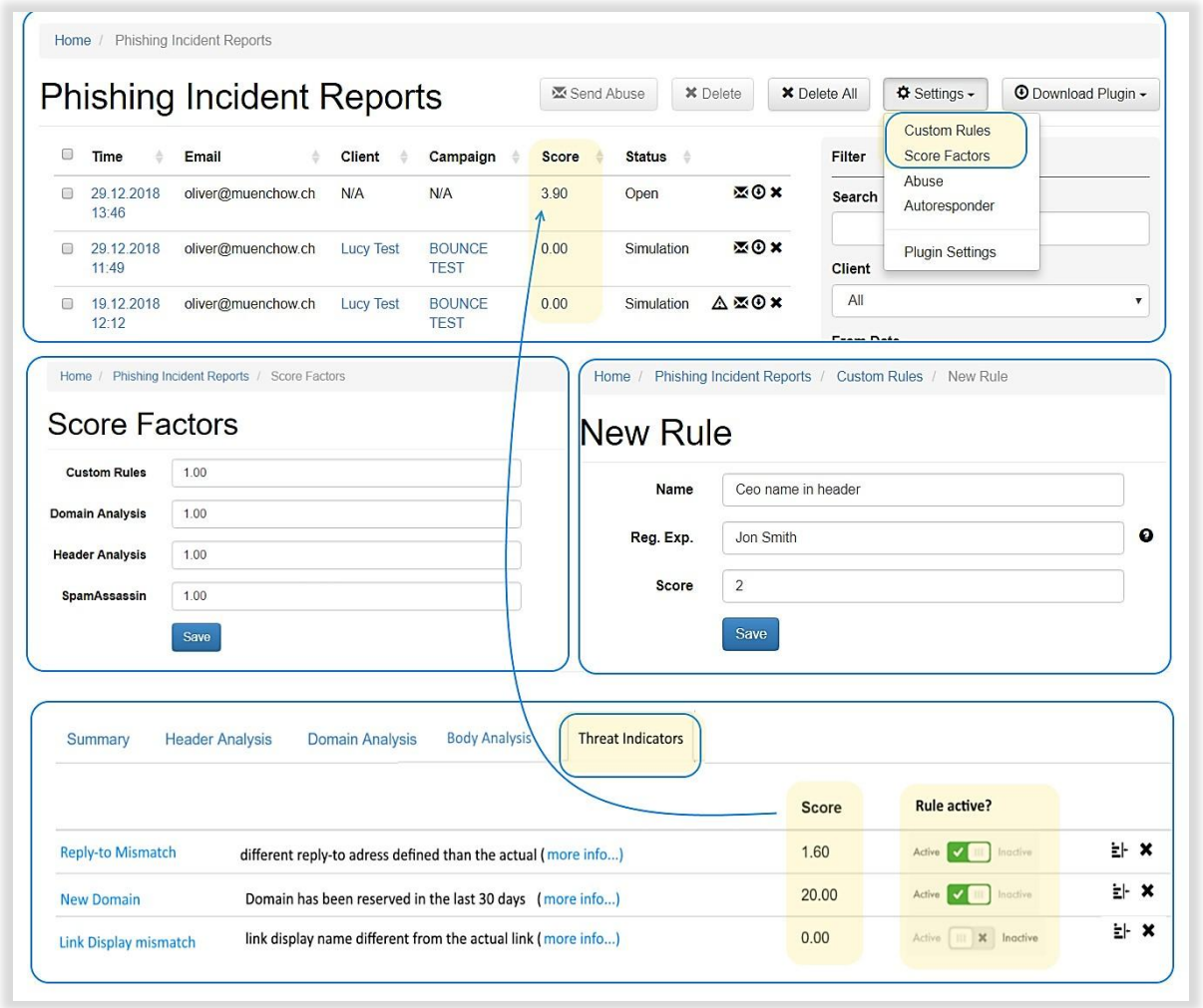
- **Feedback automático de incidentes:** A resposta automática a incidentes permite o envio de uma notificação automática para o utilizador final, fornecendo os resultados da análise de ameaças por e-mail. O texto da mensagem é livremente configurável e a pontuação de risco do e-mail dada pelo LUCY também pode ser incluída, se necessário.



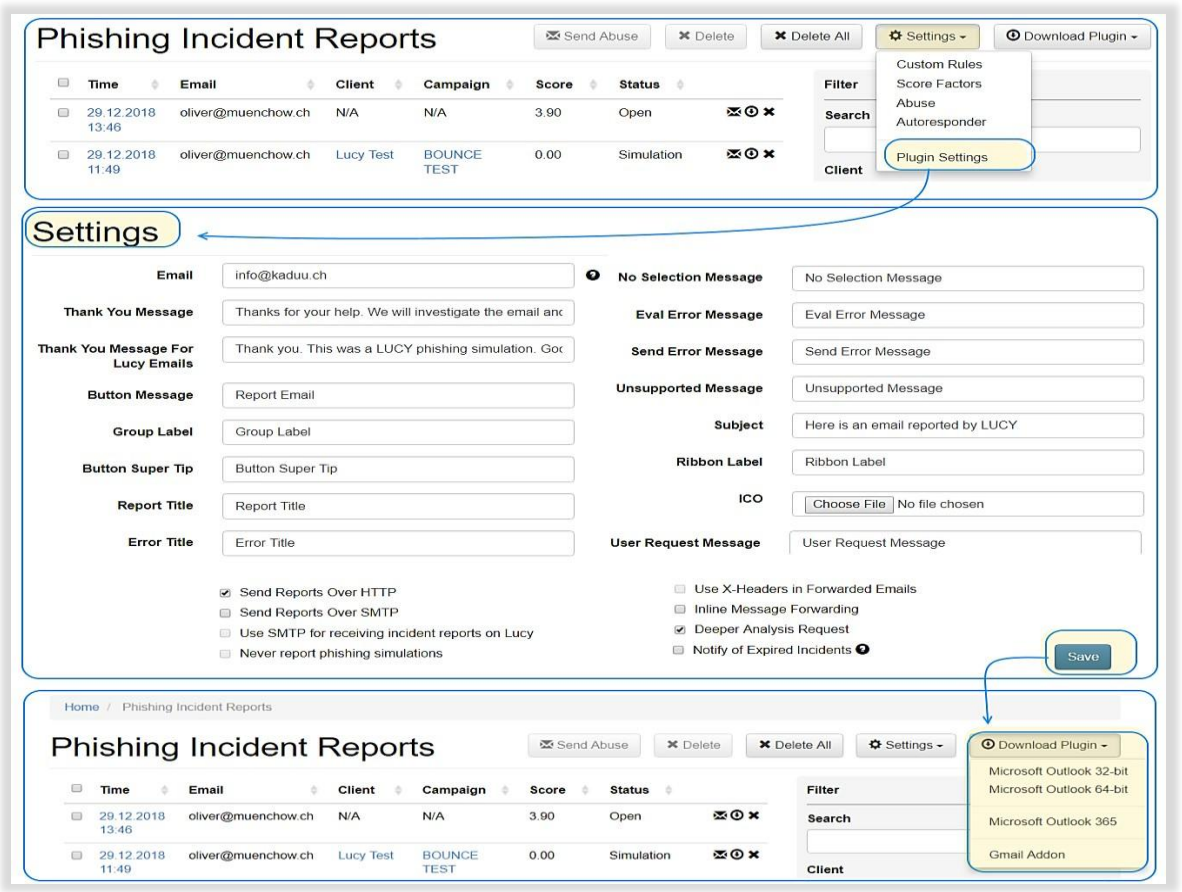
- **Mitigação de ameaças:** O mitigador de ameaças comportamentais é uma abordagem revolucionária para eliminar os riscos de e-mail. Ele apoiará o administrador de segurança na anulação do ataque (por exemplo, enviando um relatório automatizado para a equipa de fornecedores de abuso especificada envolvida no ataque).



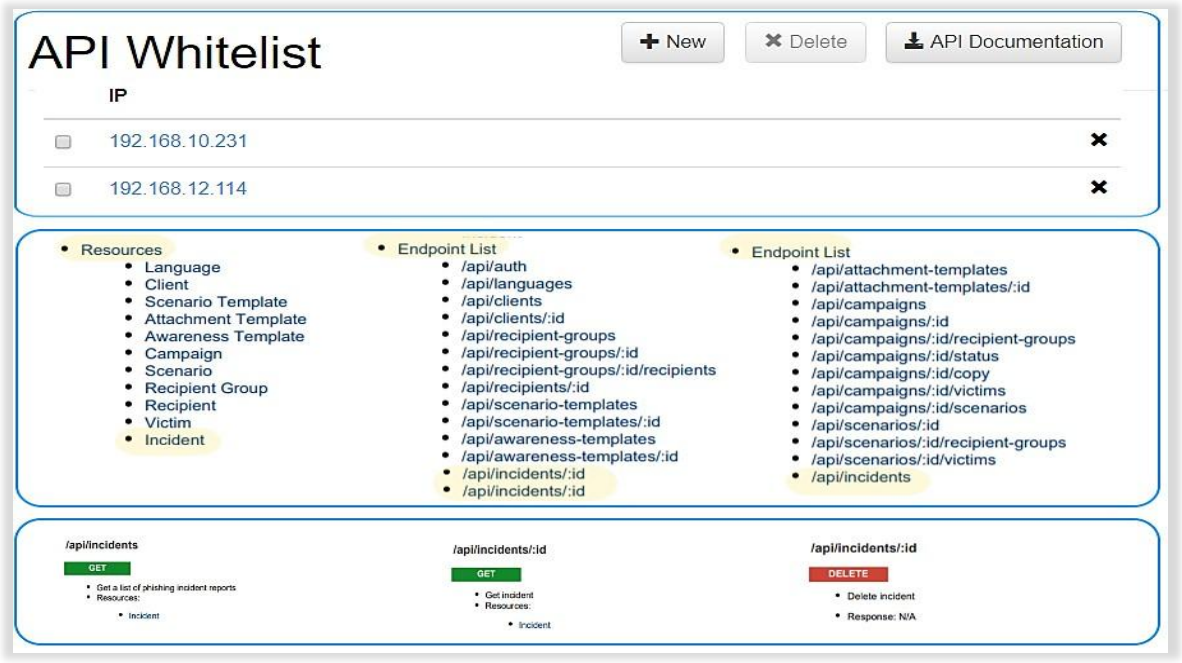
- **Análise personalizada baseada em regras:** Define as suas próprias regras para a análise de e-mail e cálculos de risco.



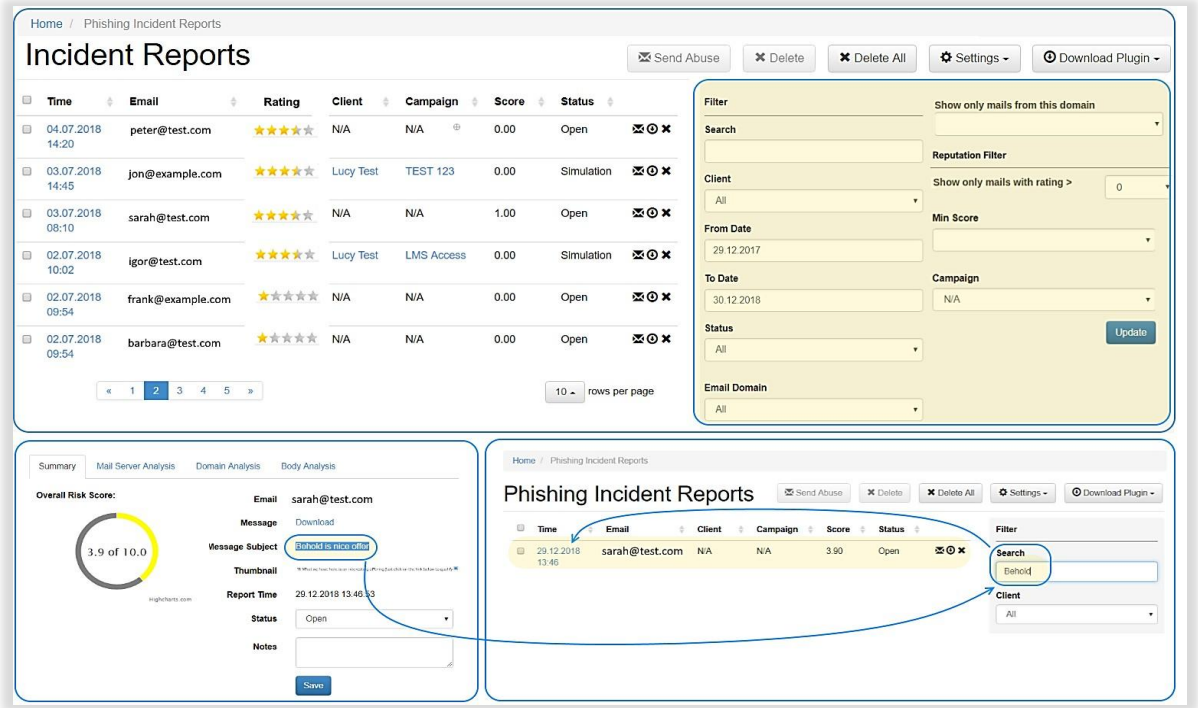
- **Opções de personalização do plugin:** O LUCY permite uma personalização fácil e uma marca branca completa de várias funções do plugin (ícone apresentado, mensagens de feedback, etiqueta da fita, protocolo de transmissão, cabeçalho enviado, etc.).



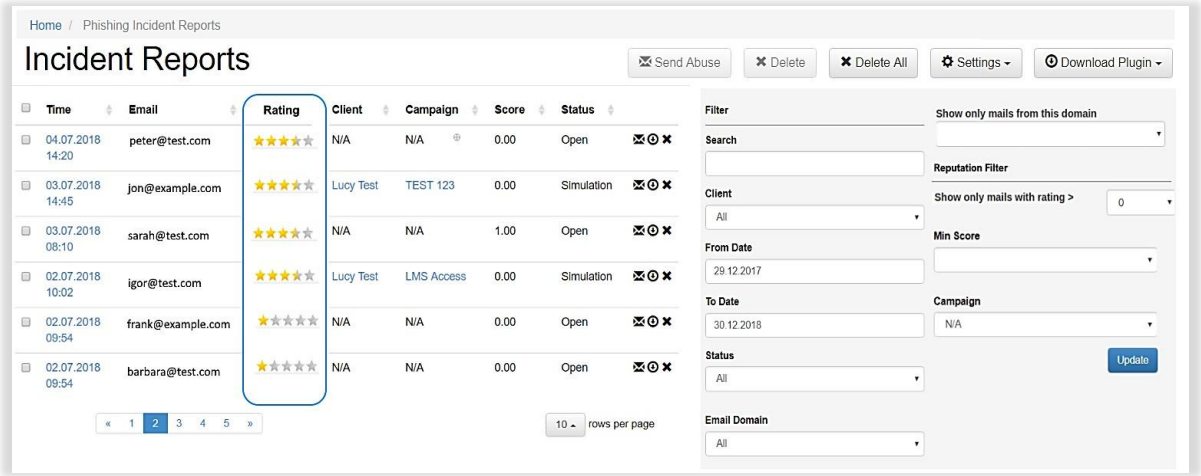
- **Integração de terceiros:** Usando a automação de API REST de incidentes do LUCY, podemos processar e-mails denunciados e ajudar a sua equipa de segurança a interromper ataques de phishing ativos enquanto estão em ação.



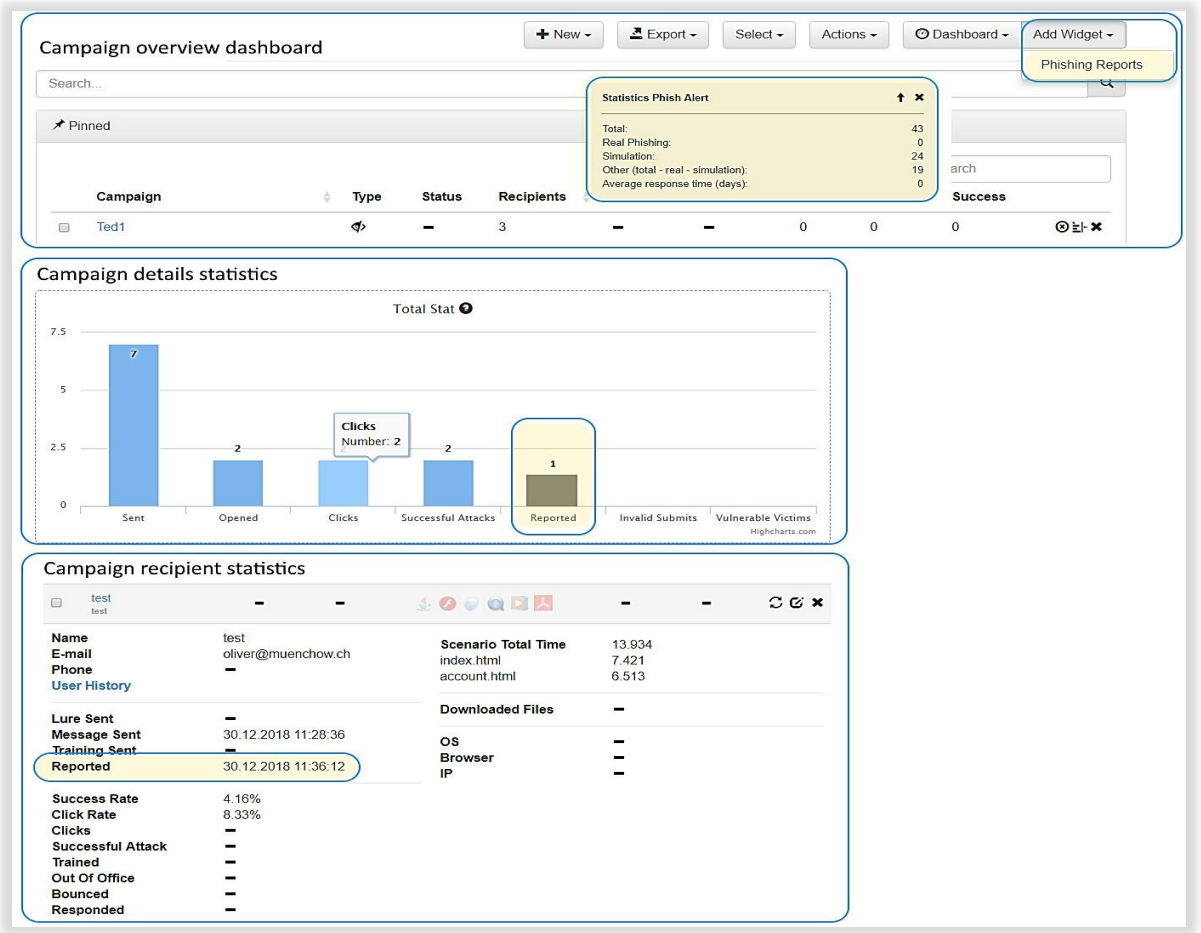
- **Identifique ataques com padrões comuns:** Aplique os filtros do painel do LUCY para detetar vetores de ataque comuns em toda a sua organização. Procura indicadores semelhantes de comprometimento em todos os e-mails denunciados.



- **Perfis de reputação de utilizador do incidente:** Classifica os utilizadores com uma pontuação de reputação do incidente.



- **Integração com simulações de ataque:** Integração contínua de relatórios e painel com simulações de phishing: identifica os utilizadores que se comportaram de maneira exemplar numa simulação de phishing.



- **Instalação fácil:** Instale o plugin de Incidente de Phishing para Outlook, Gmail, Office365.