LUCY BEYAZ BÜLTEN

LUCY NEDİR?

Çalışanlarınızı test edin, eğitin ve katılımlarını sağlayın

LUCY, kurum ve kuruluşların bir siber saldırgan rolüne bürünerek hem teknik hem de çalışan bilgi düzeylerinde mevcut zafiyetleri ortaya çıkarmaları ve kapsamlı e-öğrenme programı ile bunları ortadan kaldırmalarını sağlar.

ÇALIŞAN TESTLERİ
Saldırı Simülasyonları (oltalama, vb.)

ALTYAPI TESTİ
Kötü Amaçlı Yazılım Simülasyonu ve Taraması

ÇALIŞAN EĞİTİMİ
Entegre Öğrenme Yönetim Sistemi (LMS)

İLERLEME ÖLÇÜMLERİ
Risk ve Öğrenme Analizi

ÇALIŞAN ENTEGRASYONU
Raporlama Sistemi (E-posta Oltalama Butonu, vb.)

All Rights Reserved 2019

LUCY BEYAZ BÜLTEN

IÇINDEKILER

GENEL ÖZELLİKLER

- Hatırlatmalar
- Yanıt saptaması
- Tam teçhizatlı e-posta iletişim istemcisi
- Zamanlama Randomizasyonu
- Performans araçları
- Çok dilli panel arayüzü
- Sertifika (SSL)
- Rol bazlı erişim denetimleri
- Çok katmanlı kullanıcı grupları
- Çoklu istemci destekler
- Kampanya şablonları
- Risk bazlı kılavuz ile kurulum sihirbazı
- Kampanya denetimleri
- Onaylama İş Akışı
- DNS API

SALDIRI SİMÜLASYONU

- Taşınabilir ortam saldırıları
- SMiShing
- Veri girişi saldırıları
- Köprü bağlantısı saldırıları
- Güçlü URL yönlendirme yazılımı
- Karma saldırılar
- Dosya bazlı saldırılar
- Çifte saldırıları
- Java bazlı saldırılar
- PDF bazlı saldırılar
- Fidye yazılım simülasyon saldırıları
- Veri girişi doğrulama yazılımı
- Çok Dilli Saldırı Şablonu Kitaplığı
- Sektör ve bölüme özel şablonlar
- Eşzamanlı saldırı şablonu kullanımı
- Saldırı URL'si varyasyonları
- URL Kısaltma
- Pentest kiti
- Web sitesi klonlayıcı
- Seviye bazlı saldırılar
- Spear (hedefli) oltalama simülasyonu
- Oltalama E-postaları için DKIM / S / MIME Desteği
- E-posta tarayıcı
- Özel ana sayfa oluşturma

ALTYAPI TESTLERİ

- Kötü Amaçlı Yazılım Test Kiti
- Posta ve Web Filtreleme Testi
- Aktif ve Pasif İstemci Zafiyetinin Saptanması
- Spoofing Testi

TEKNİK TESTLER

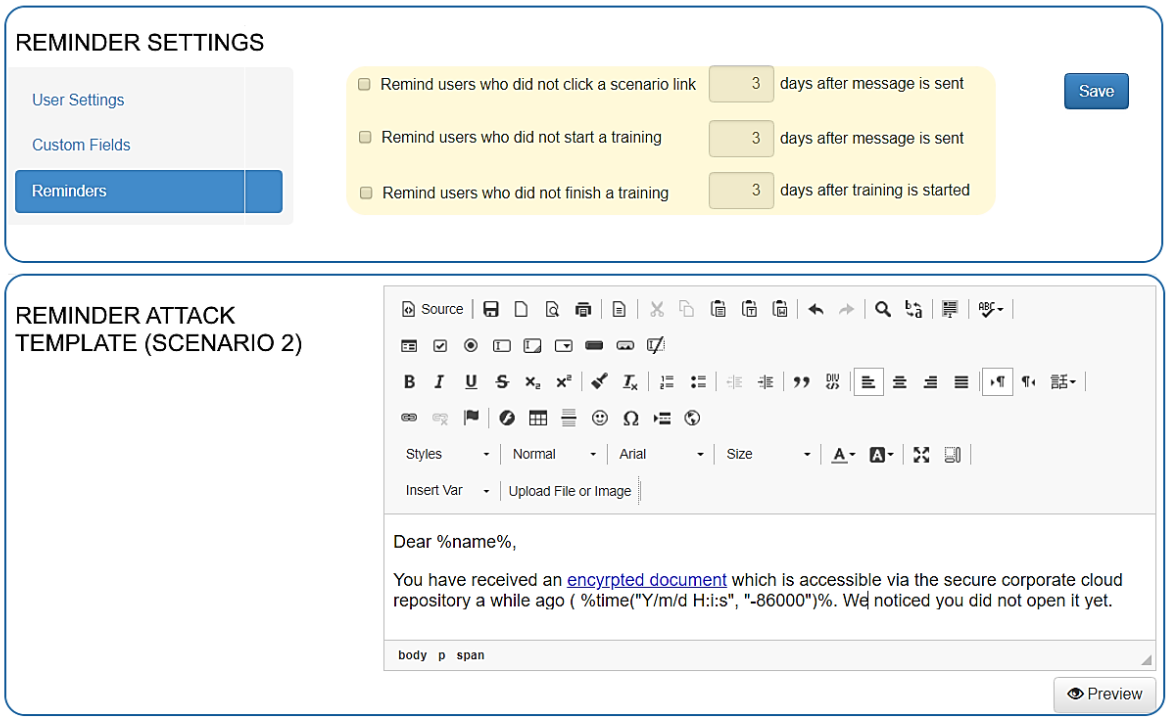
- İtibar Bazlı e-Öğrenme
- Son Kullanıcı Eğitim Portalı
- Farkındalık Eğitimi Diploması
- e-Öğrenme Yazarlık Kiti
- Zengin Ortam Farkındalığı Eğitimi
- Eğitim Kitaplığı
- Statik Eğitim Desteği
- Çevrimdışı Eğitim Desteği
- Mikro Öğrenme Modülleri
- Video Kişiselleştirme
- Mobil Destekleyen Format
- Video İçe / Dışa Aktarma
- Dinamik Eğitim İpuçları

ÇALIŞANLARINIZIN KATILIMINI SAĞLAYIN

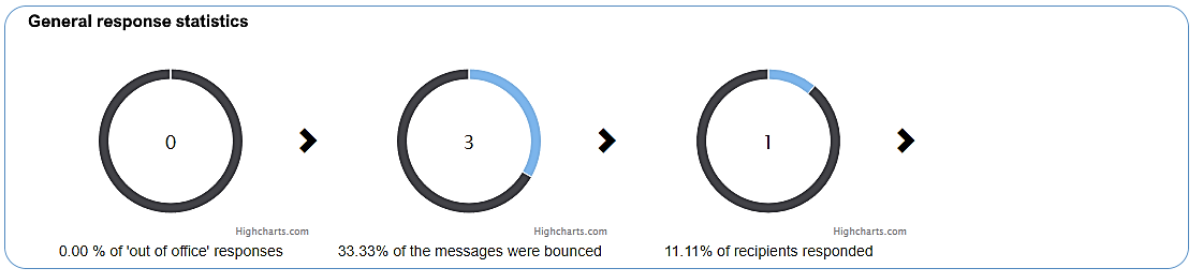
- Tek tıkla E-posta rapor etme
- Olumlu Davranışın Pekiştirilmesi
- Derinlemesine teftiş talebi
- Otomatik Olay Analizi
- Olay Otomatik Geribildirimi
- Tehdit Azaltma
- Özel kural bazlı analiz
- Eklenti kişiselleştirme seçenekleri
- Üçüncü taraf entegrasyonu
- Ortak noktalara sahip saldırıları belirleme
- Olay kullanıcı itibar profilleri
- Saldırı simülasyonları ile entegrasyon
- Kolay Kurulum

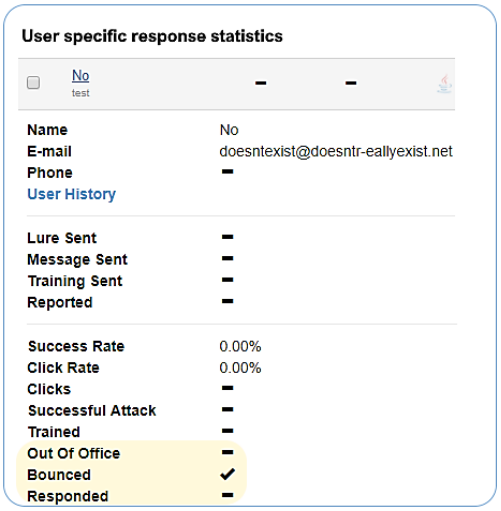
GENEL ÖZELLİKLER

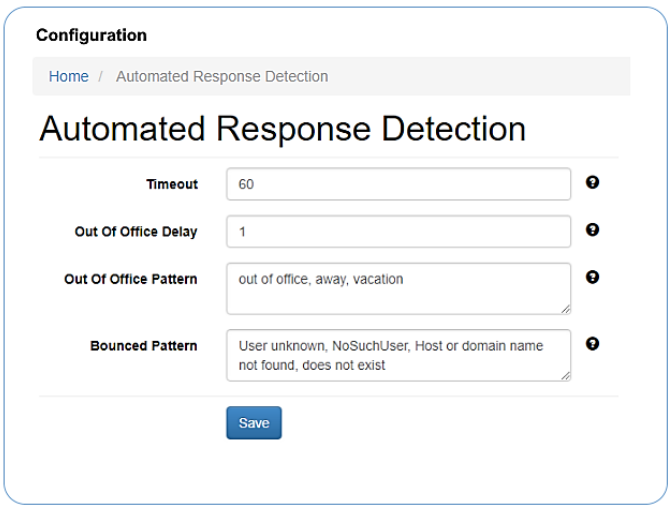
- **Hatırlatmalar:** Bir saldırı bağlantısına veya bir eğitim kursuna belirli bir süre sonrasında tıklamamış olan kullanıcılara otomatik olarak yeniden göndermek için hatırlatma şablonları kullanılabilir.



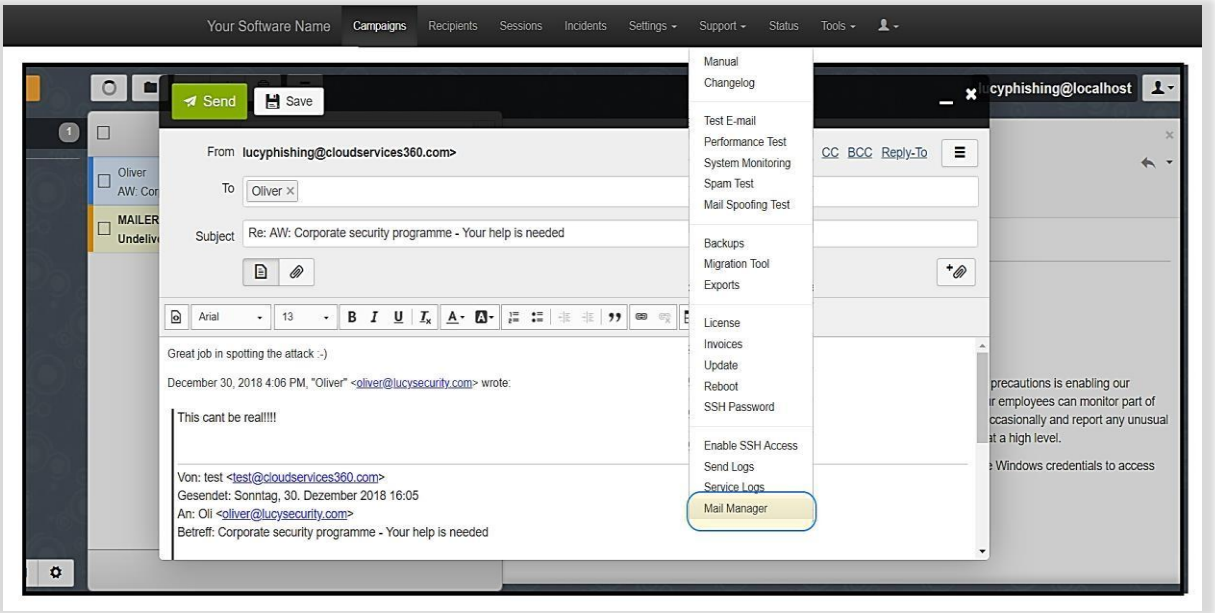
- **Yanıt saptaması:** Otomatik yanıt saptaması ile otomatik e-posta yanıtlarının (ofis dışındayım, vb.) yanı sıra kampanya dahilindeki e-posta gönderme hatalarının (bilinmeyen kullanıcı, vb.) belirlenmesi ve analiz edilmesi mümkün hale gelir.



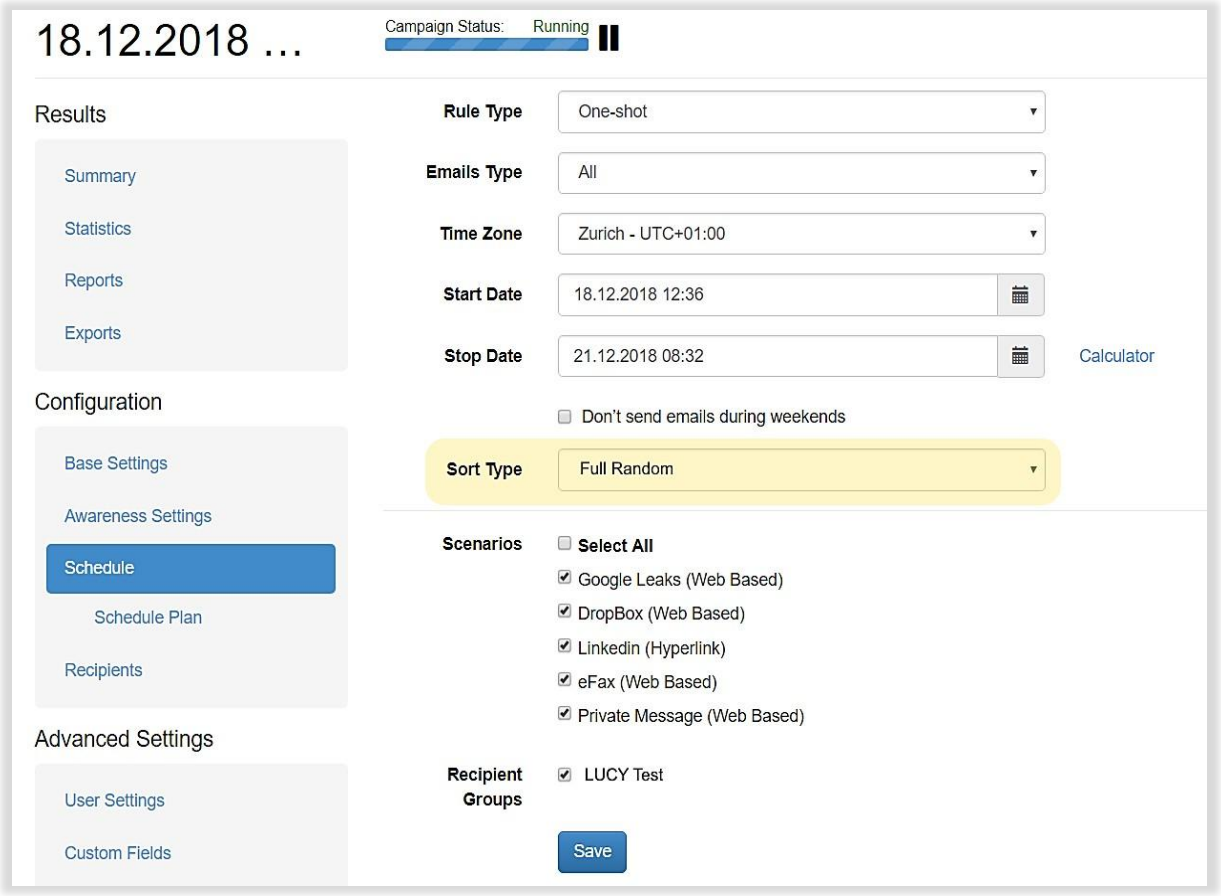




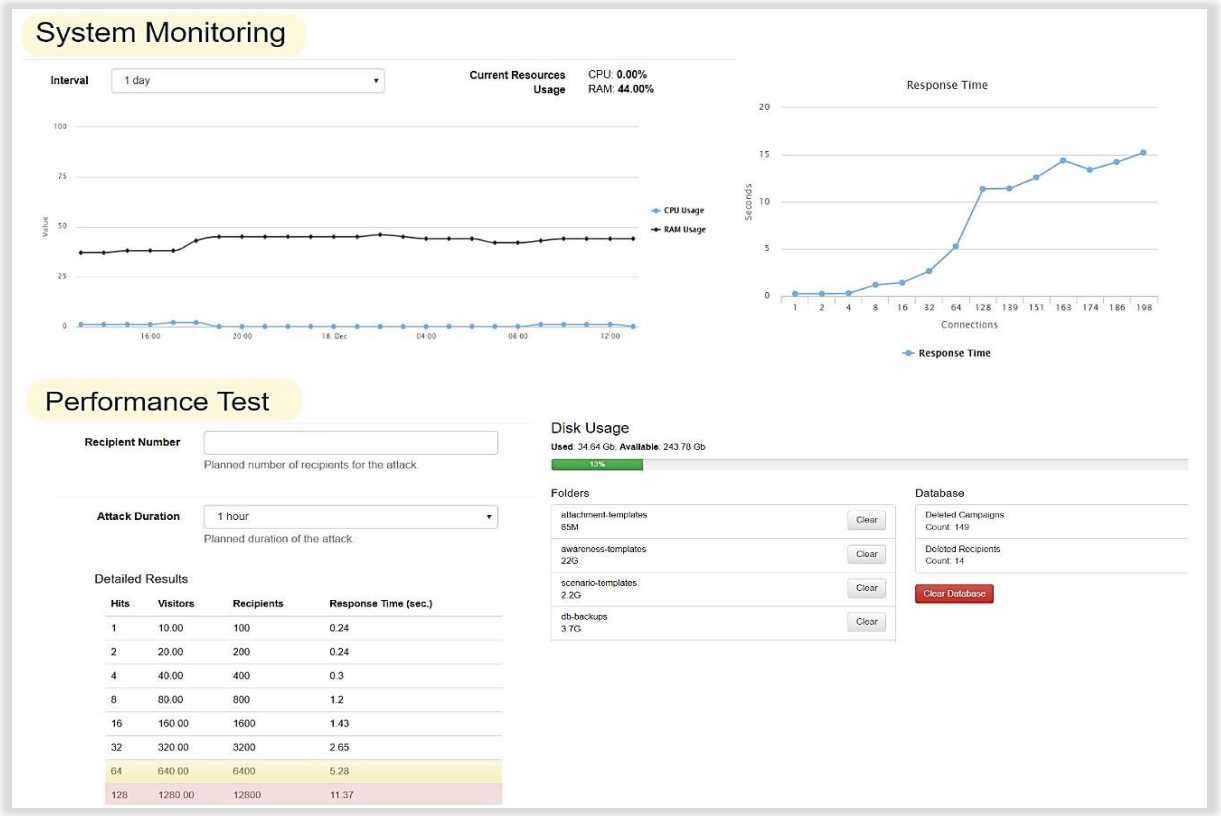
- **Tam teçhizatlı e-posta iletişim istemcisi:** Entegre mesajlaşma platformu sayesinde LUCY yöneticisi, LUCY kampanyaları içinde ve dışındaki alıcılar ile interaktif bir şekilde iletişim kurabilir. Tüm e-postalar arşivlenir ve gözden geçirilebilir.



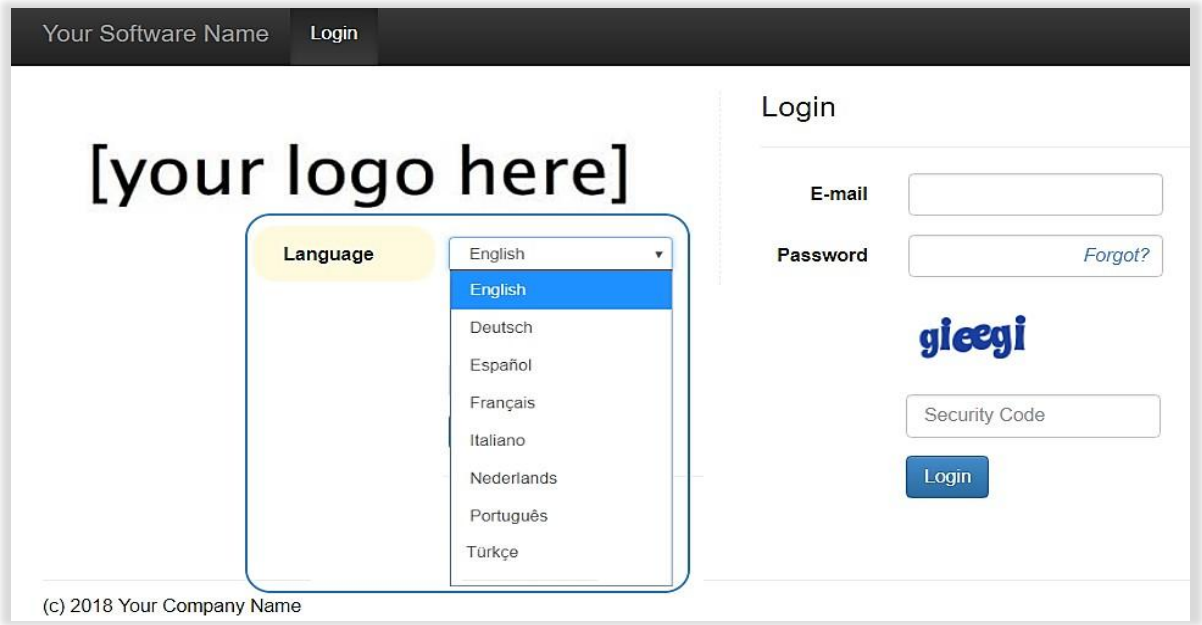
- **Zamanlama Randomizasyonu:** Çalışan farkındalığını randomize olarak artırmak, kurum içinde etkili ve sürdürülebilir farkındalığın başlıca faktörüdür. Birçok eşzamanlı kampanyayı rastgele olarak göndermek çalışanları eğitmenin en iyi yollarından biridir..



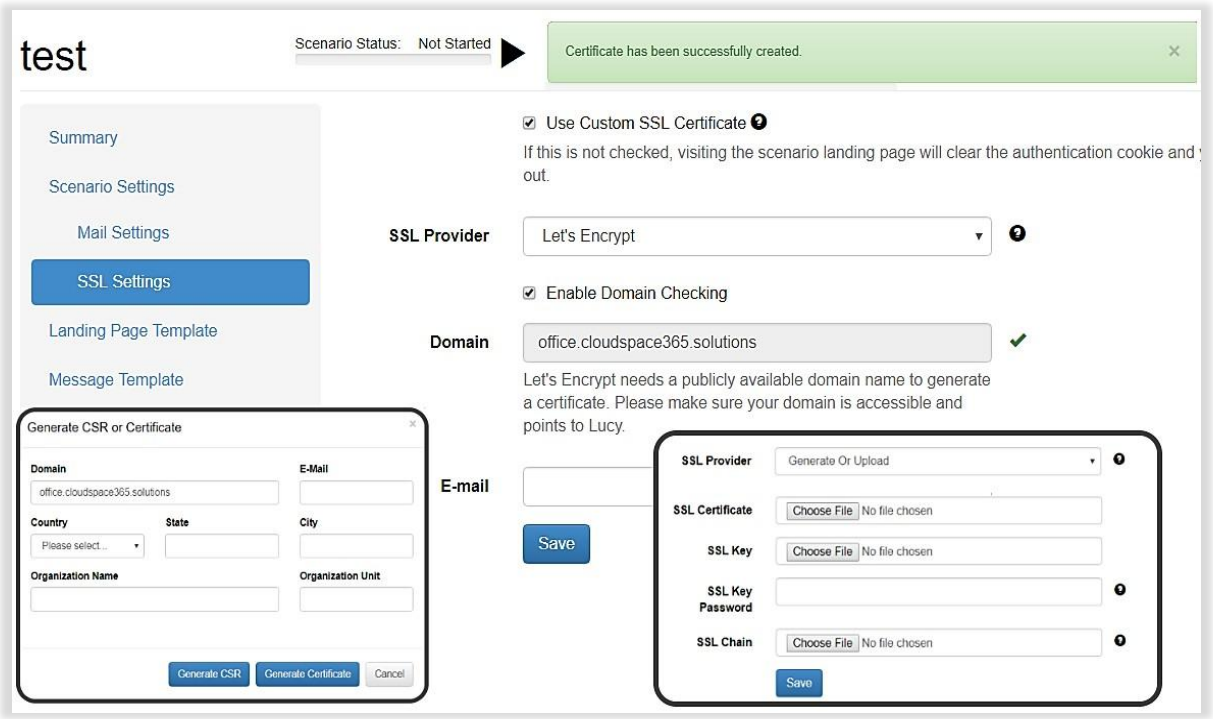
- **Performans araçları:** LUCY akıllı rutinleri, sunucu kurulumunu belirlenen kaynaklara adapte eder. Uygulamalar Sunucusu, DBMS Ölçekleme, Bellek ve CPU kullanımları kurulum veya işletim sırasında hesaplanır. Tek bir bulut tabanlı LUCY kurulumunu 400 binden fazla kullanıcı için ölçekleyebilirsiniz.



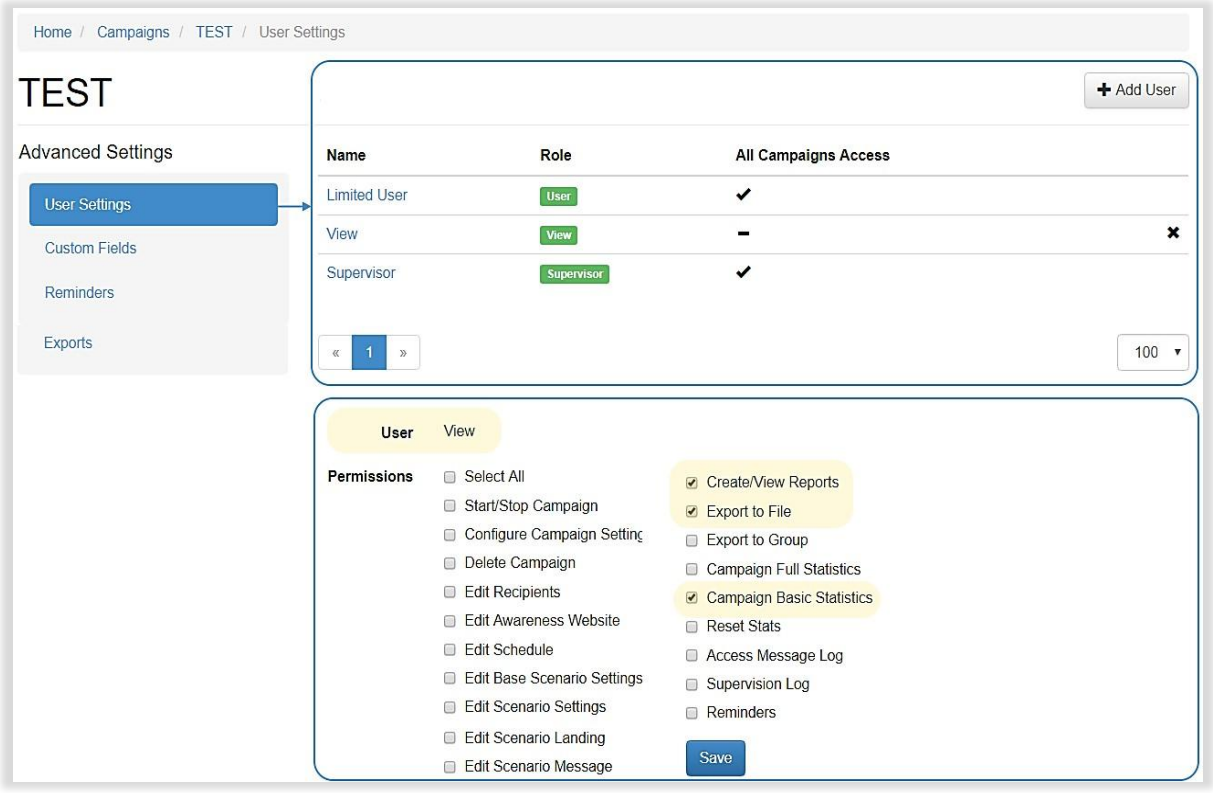
- **Çok dilli panel arayüzü:** LUCY kullanıcı paneli arayüzü farklı dillerde hizmet vermektedir ve talep üzerine diğer dillere çevrilebilir.



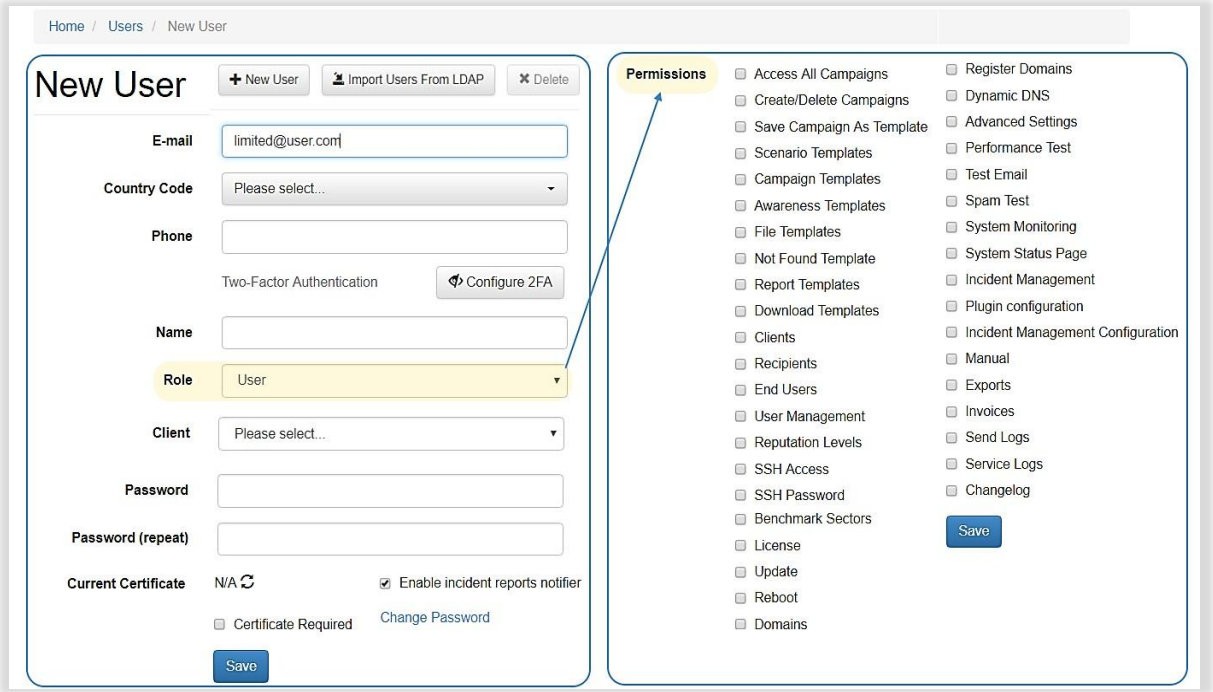
- **Sertifika (SSL):** Yönetici, backend ve kampanyalar için resmi ve güvenilir sertifikalar oluşturulmasına imkan tanır. LUCY sertifika oluşturmak için otomatik olarak sistemde tanımlanmış olan alan adını kullanacaktır. Kampanya için SSL kullanmayı tercih ederseniz özel bir sertifika veya bir CSR (Sertifika İmzalama Talebi) oluşturabilirsiniz. Ayrıca resmi güvenilir sertifikaları içe aktarabilirsiniz.



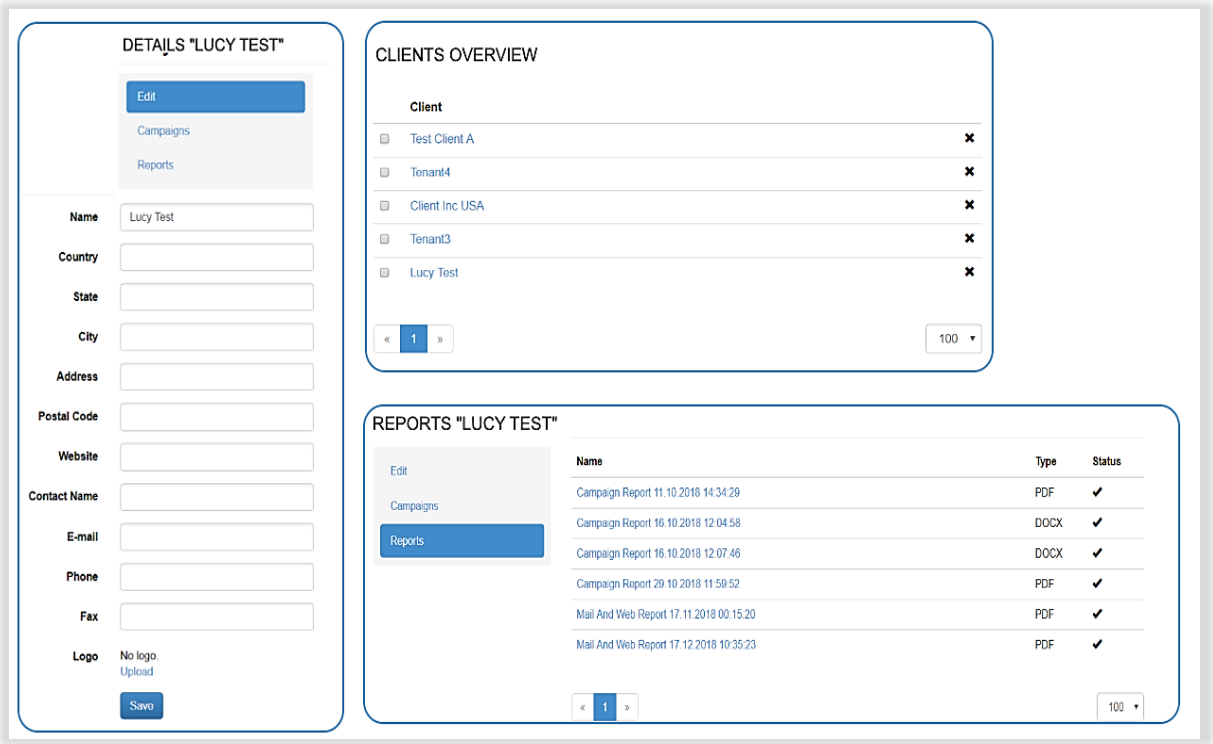
- **Rol bazlı erişim denetimleri:** LUCY, sisteme erişimi yalnızca yetkili kullanıcılar ile sınırlandıran bir rol bazlı erişim denetimi (RBAC) sunar. Belirli işlemleri gerçekleştirme izinleri, kullanıcı ayarları içerisindeki belirli rollere atanır. Üyeler veya çalışanlara (veya diğer sistem kullanıcıları) belirli LUCY işlevlerini gerçekleştirmek için gerekli bilgisayar izinlerini almalarını sağlayan belirli roller atanır.



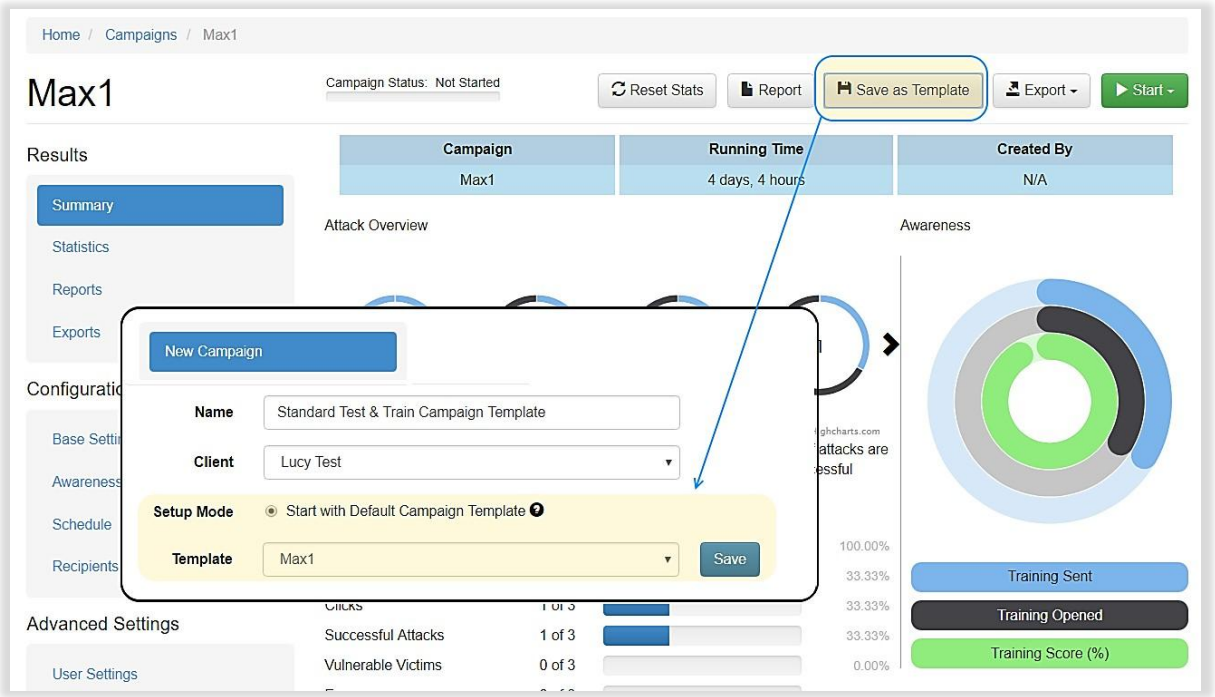
- **Çok katmanlı kullanıcı grupları:** Bir CSV, LDAP veya metin dosyası ile kullanıcılar toplu olarak hızla yükleyin. Departman, bölüm, unvan, vb. altında düzenlenmiş farklı gruplar oluşturun. Devam eden bir kampanyada kullanıcıları güncelleyin. Oltalama kampanyası sonuçlarına göre dinamik kullanıcı grupları oluşturun.



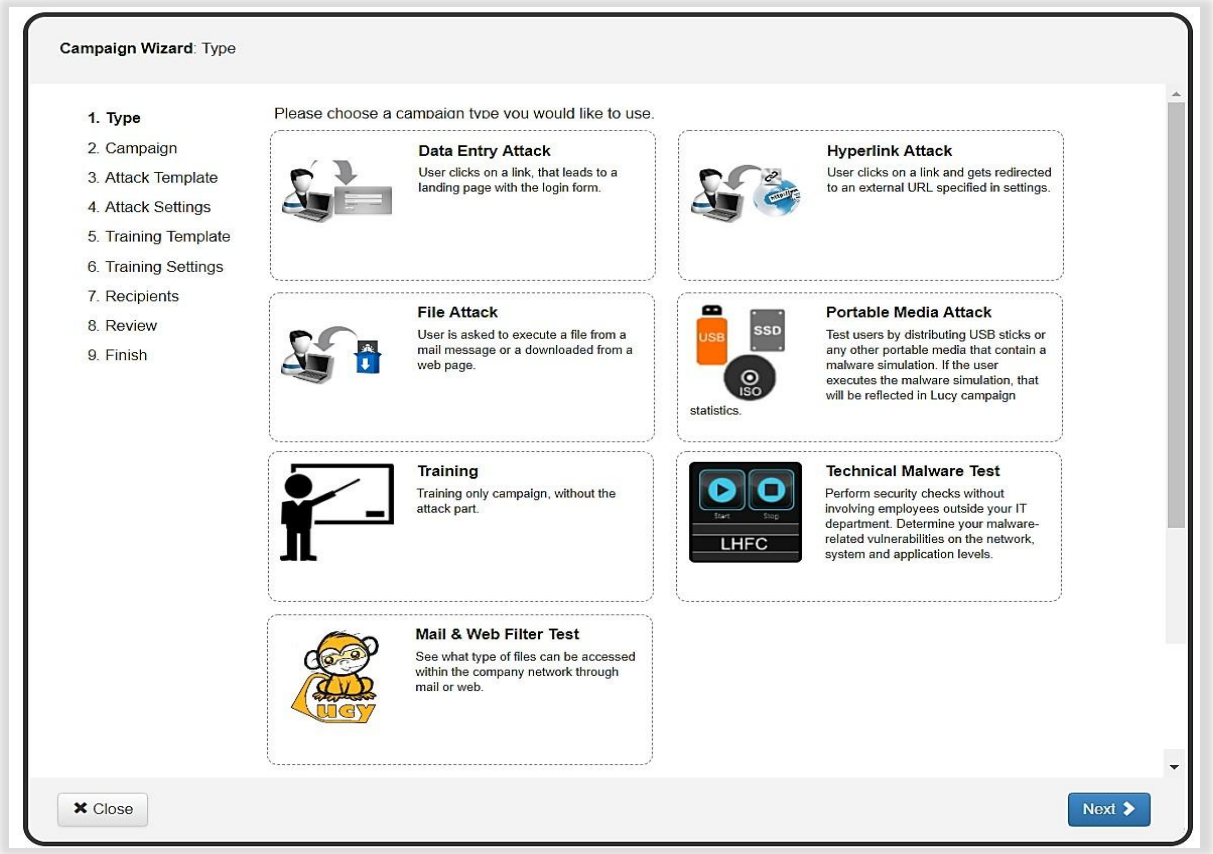
- **Çoklu istemci destekler:** "İstemci" terimi LUCY içerisinde ilgili bir kampanyaya sahip farklı şirketler, departmanlar veya grupları ifade eder. Bu istemciler örneğin kampanyaya özel erişim izni vermek veya müşteriye özel analizler oluşturmak için kullanılabilir.



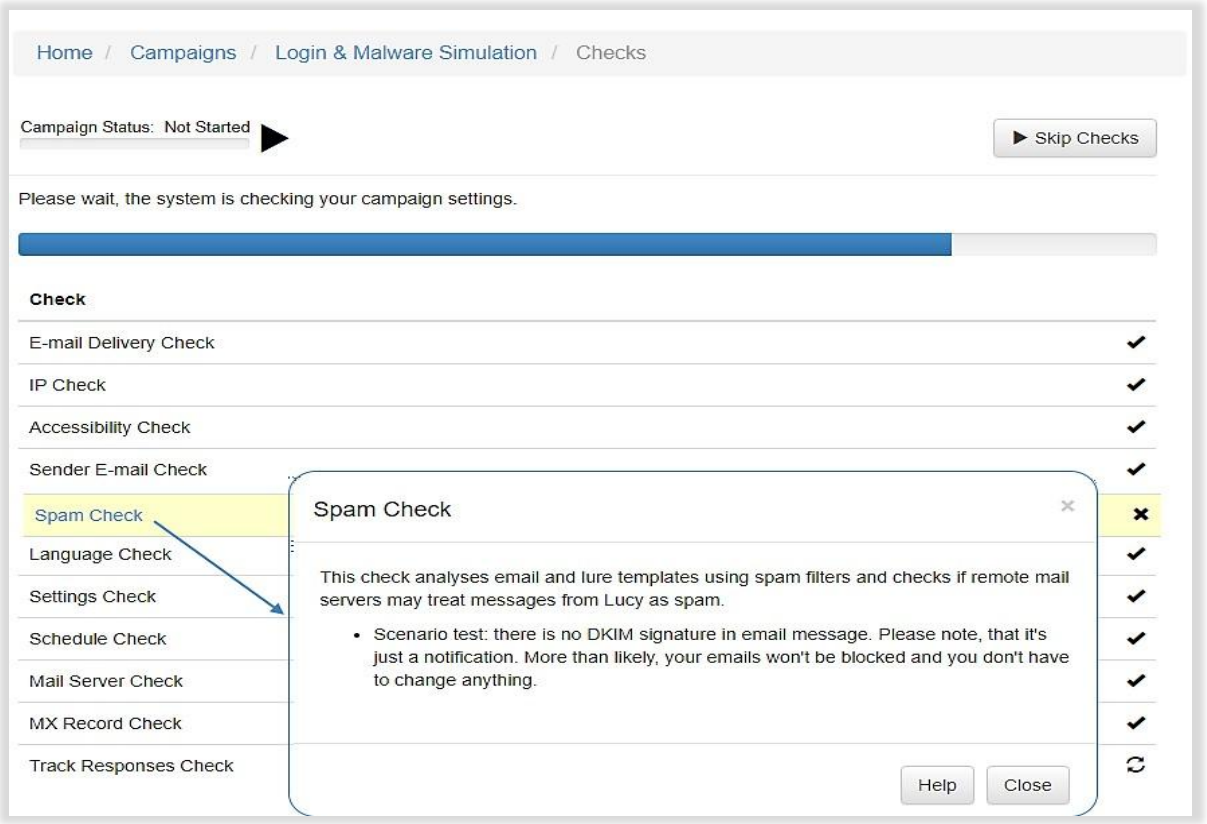
- **Kampanya şablonları:** Benzer kampanyaları yeniden kullanmak istemeniz halinde saldırı şablonları ile bir kampanyanın tamamını ve e-Öğrenme içeriklerini bir kampanya şablonu kaydedebilirsiniz. Bu özellik sayesinde benzer konfigürasyonları tekrar tekrar yinelemek zorunda kalmazsınız.



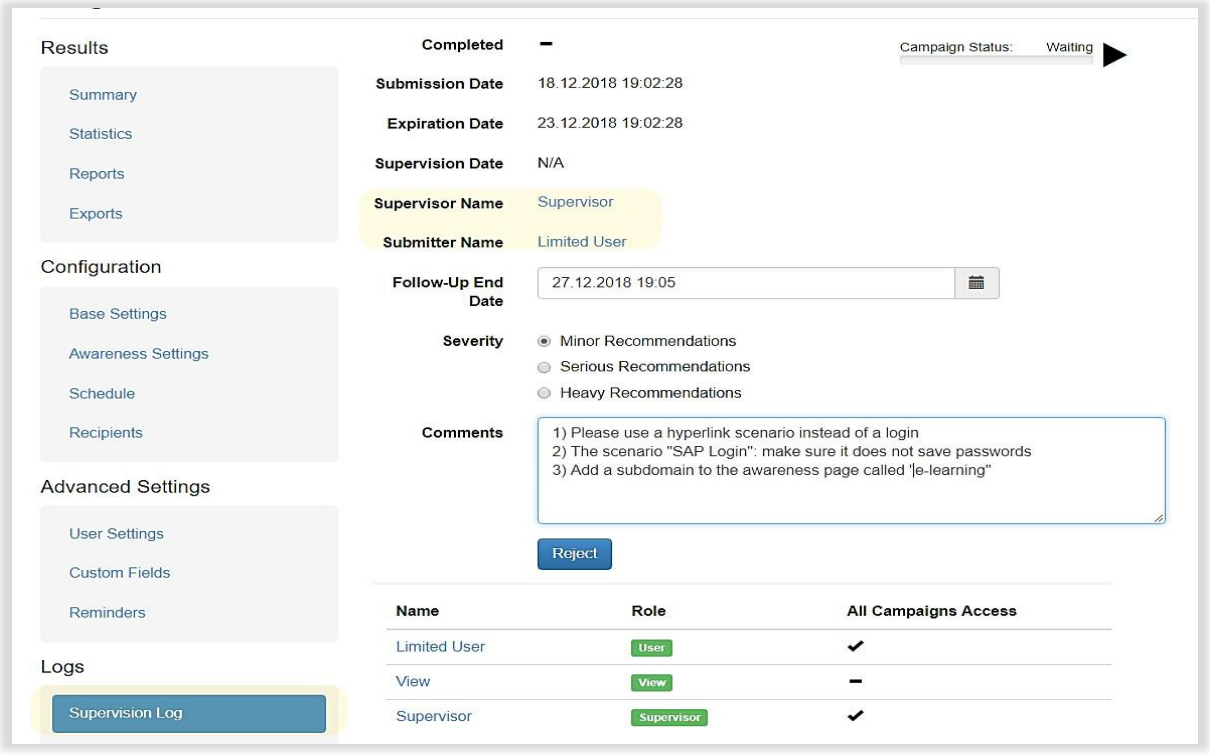
- **Risk bazlı kılavuz ile kurulum sihirbazı:** LUCY çeşitli Kurulum Araçları sunmaktadır. Öntanımlı kampanya şablonlarını kullanarak 3 dakikadan kısa sürede kampanyanızı tamamlayın veya Kurulum Sihirbazı'nın size konfigürasyonda kılavuzluk etmesine izin verin. Opsiyonel olarak, şirketinizin boyutu be sektörünüze bağlı olarak siber saldırı ve farkındalık şablonları seçimi için belirli önerilerde bulunan risk bazlı kurulum modu da mevcuttur.



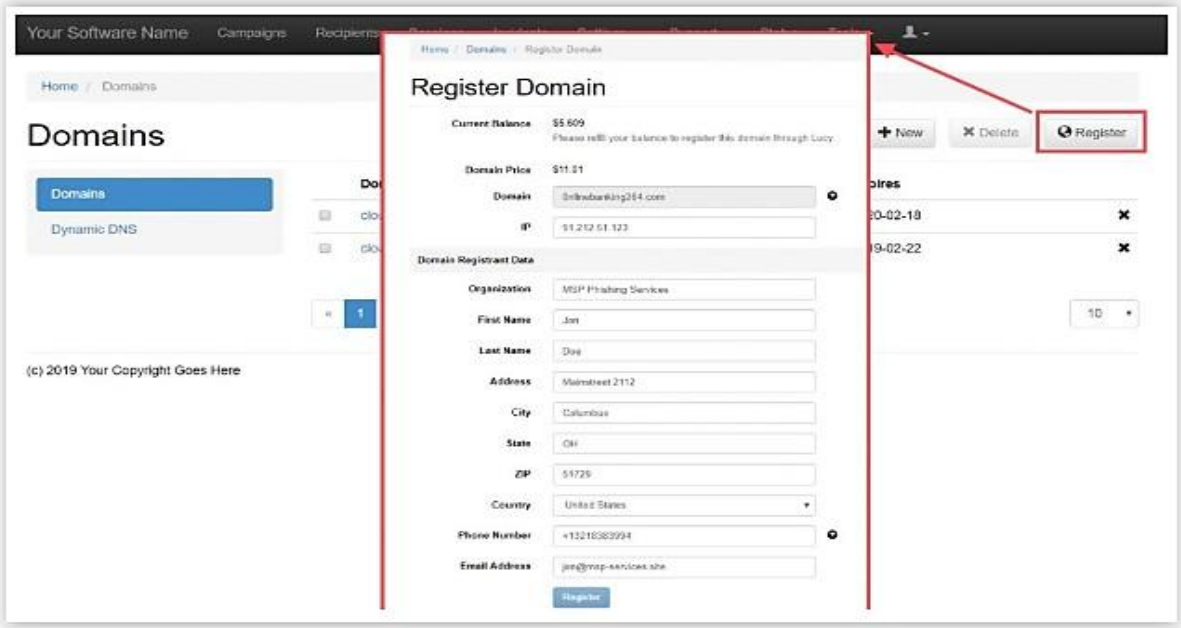
- **Kampanya denetimleri:** Bir LUCY kampanyasını başlatmadan önce ön denetimler: E-Posta Gönderim Denetimi, MX Kayıt Denetimi, Zamanlama Denetimi, Spam Denetimi ve diğerleri.



- **Onaylama İş Akışı:** Bir kampanya onaylanması için LUCY içerisinde bir süpervizöre gönderilebilir.

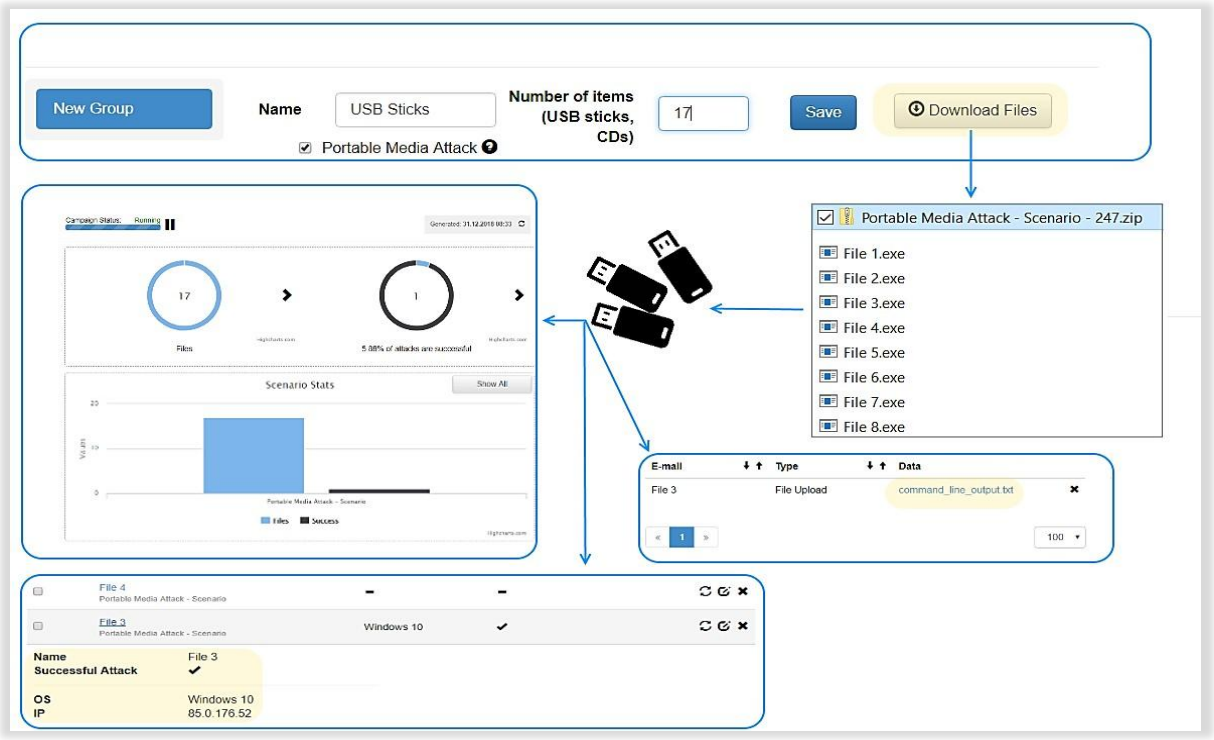


- **DNS API:** DNS API, yöneticinin saniyeler içerisinde LUCY üzerinde herhangi bir alan adını oluşturmasına imkan tanır. Siber saldırganlar müşteri alan adında benzer imla hatalarını sıklıkla kullandıkları için (buna Typosquatting adı verilir) bu risk de LUCY'de temsil edilebilir. Müşterinin orijinal alan adı örneğin "onlinebanking.com" ise "0nlinebanking.com", "onl1nebanking.com" veya "onlinebanking.services" gibi alan adlarını ayırtmak ve bunları daha sonra bir kampanyaya atamak için DNS sihirbazı kullanılabilir. LUCY daha sonra otomatik olarak LUCY'nin üzerinde kurulu olduğu IP için ilgili DNS girişlerini (MX, SPF, Whois Koruması, vb.) oluşturur. Elbette, yönetici LUCY'de alan adlarına sahip olmak için kendi sağlayıcısını kullanmayı da seçebilir.

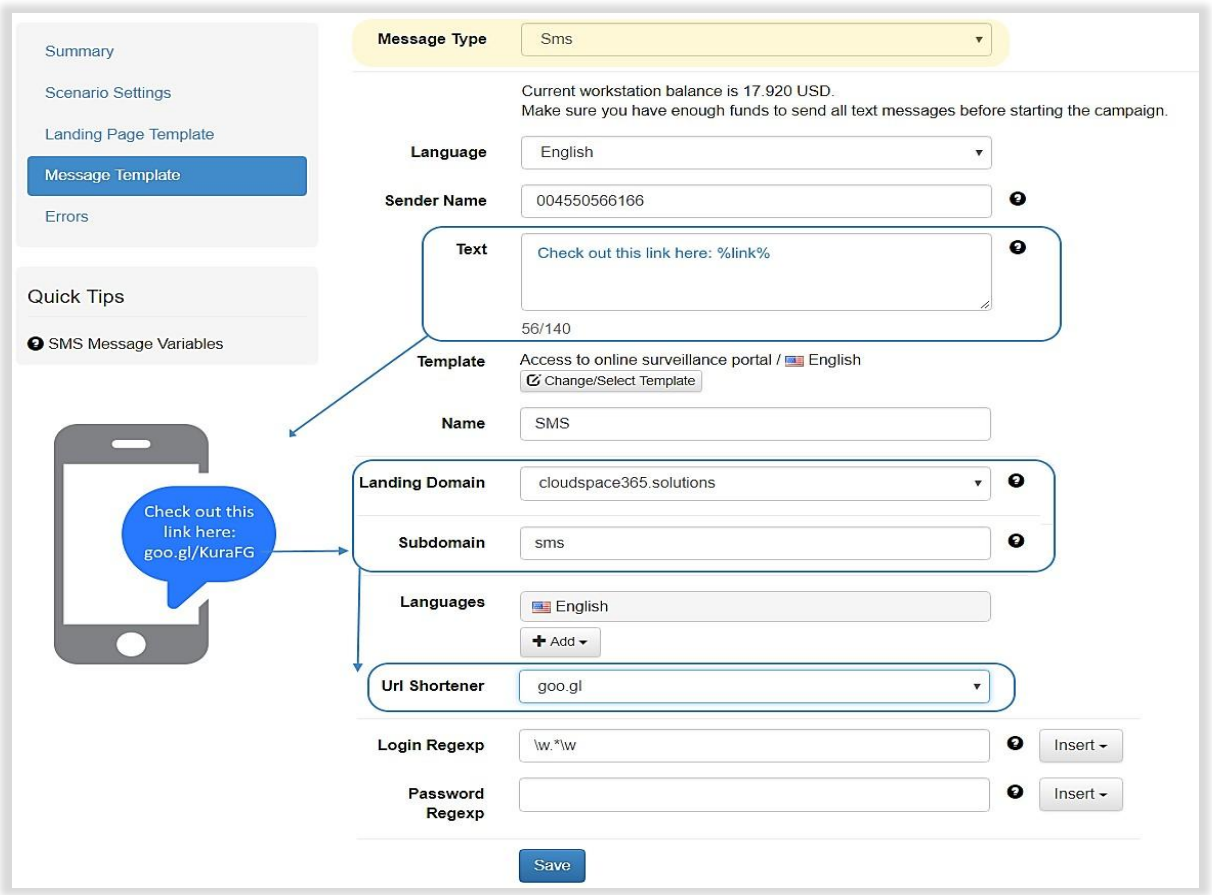


SALDIRI SİMÜLASYONU

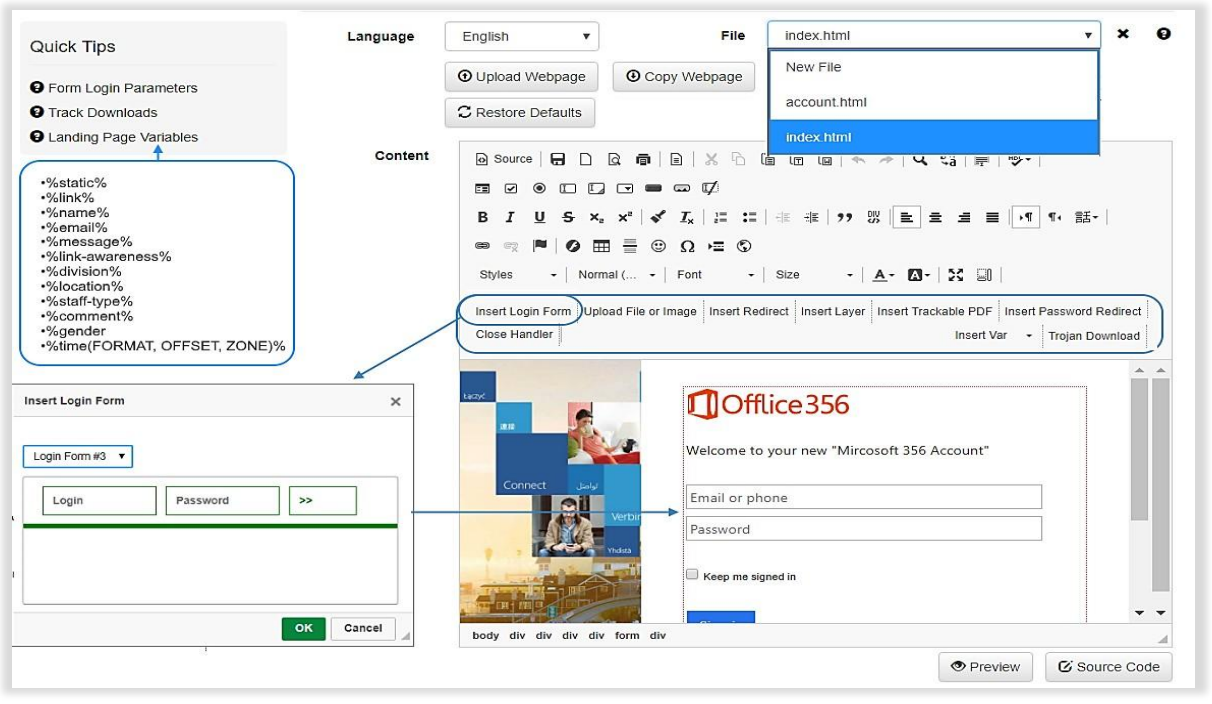
- **Taşınabilir ortam saldırıları:** Bilgisayar korsanları, bir bilgisayar veya ağda bulunan hassas bilgilere erişim sağlamak için taşınabilir ortam sürücüleri kullanabilir. LUCY, bir dosya şablonunun (çalıştırılabilir, arşiv, makrolar içeren ofis belgesi, vb.) USB, SD kart veya CD gibi bir taşınabilir ortam cihazına kaydedilebileceği taşınabilir ortam saldırıları gerçekleştirme seçeneğini sunmaktadır. Bu dosyaların aktivasyonu (çalıştırılması) LUCY içerisinde takip edilebilir.



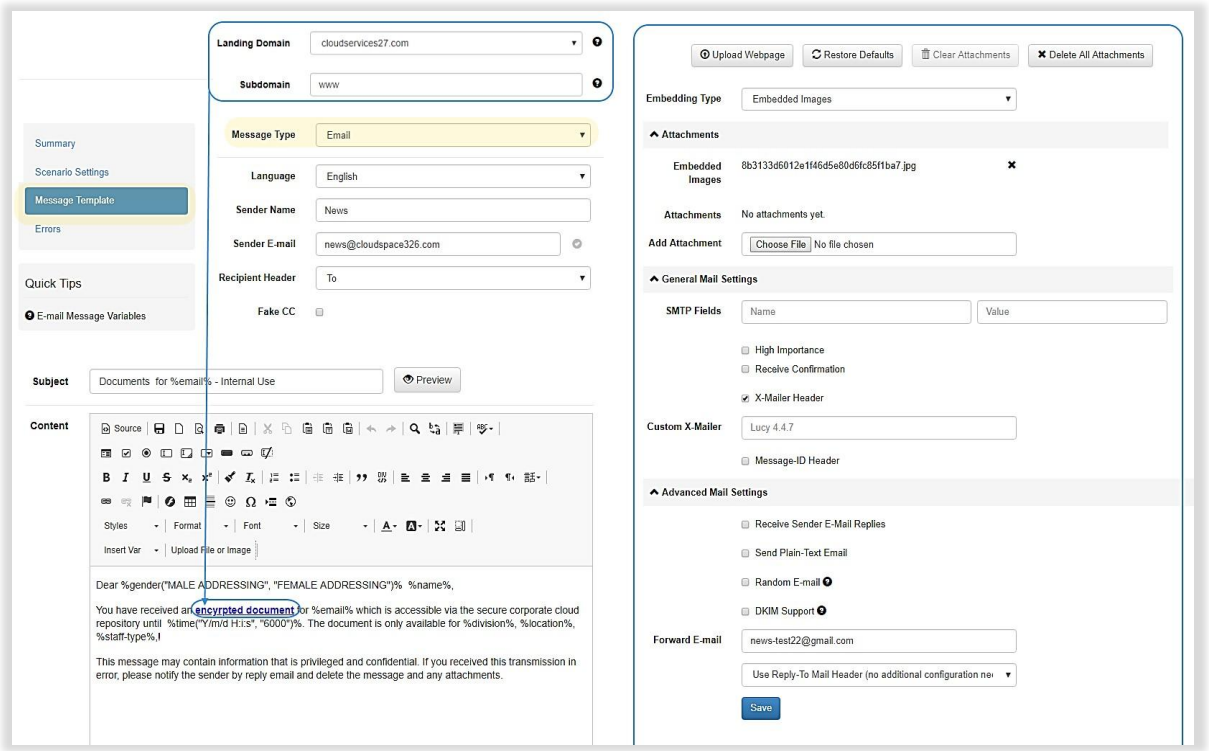
- **SMiShing:** Smishing, "SMS oltalama" saldırısıdır. Siber suçlular "oltalama" yaptıkları zaman, alıcıyı kötü amaçlı yazılım yüklü bir eklentiyi açmaya veya kötü amaçlı bir bağlantıya tıklamaya ikna etmeye çalışan düzmece e-postalar gönderirler. Smishing ise e-postalar yerine SMS mesajlarını kullanır.



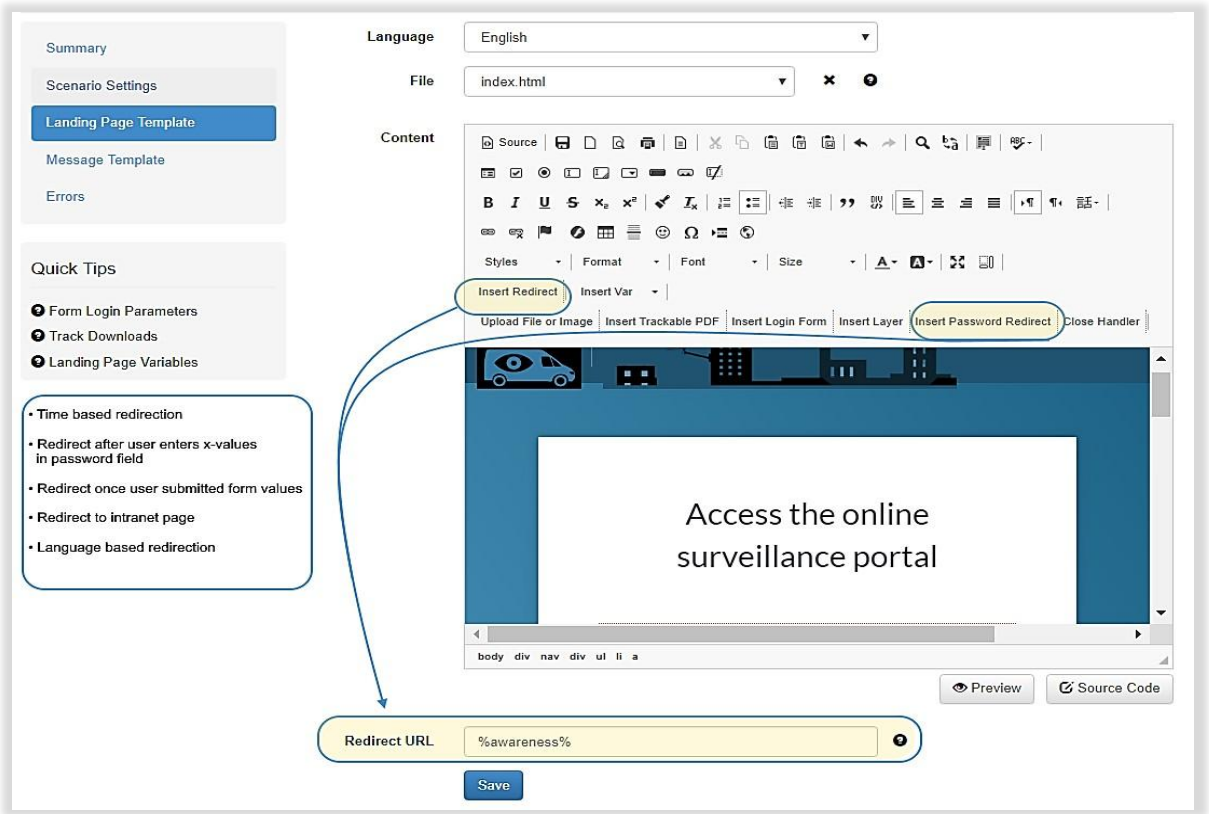
- **Veri girişi saldırıları:** Veri girişi saldırıları kapsamında hassas bilgi girişinin önünü kesen bir ya da daha fazla internet sayfası olabilir. Mevcut internet sayfaları LUCY web editörü ile kolaylıkla özelleştirilebilir. İlave düzenleme araçları sayesinde oturum açma formları, indirme alanları, vb. işlevleri HTML bilginiz olmaksızın hızla oluşturabilirsiniz.



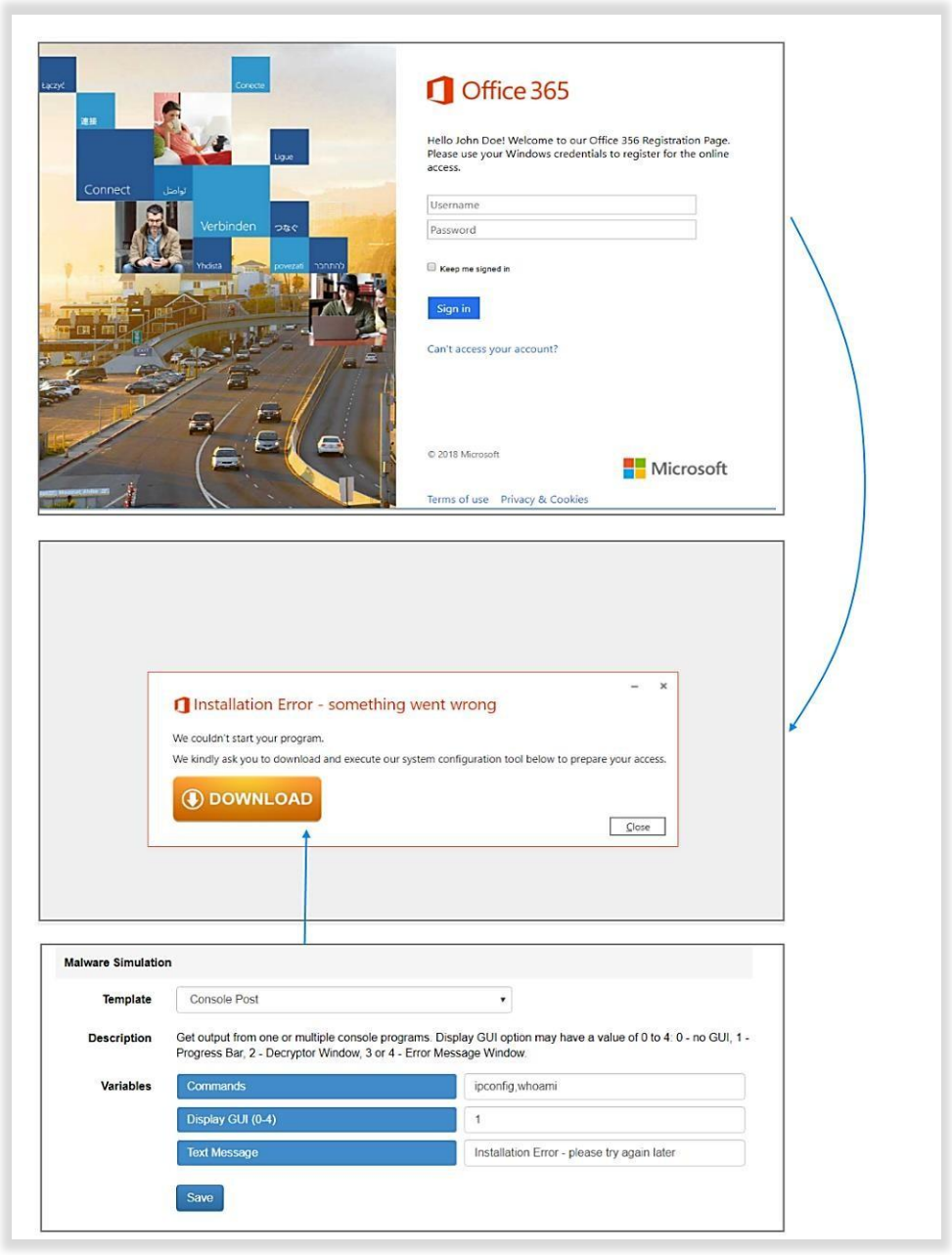
- **Köprü bağlantısı saldırıları:** Köprü bağlantısı bazlı bir kampanya, kullanıcılara rastgele bir izleme URL'si içeren bir e-posta gönderir.



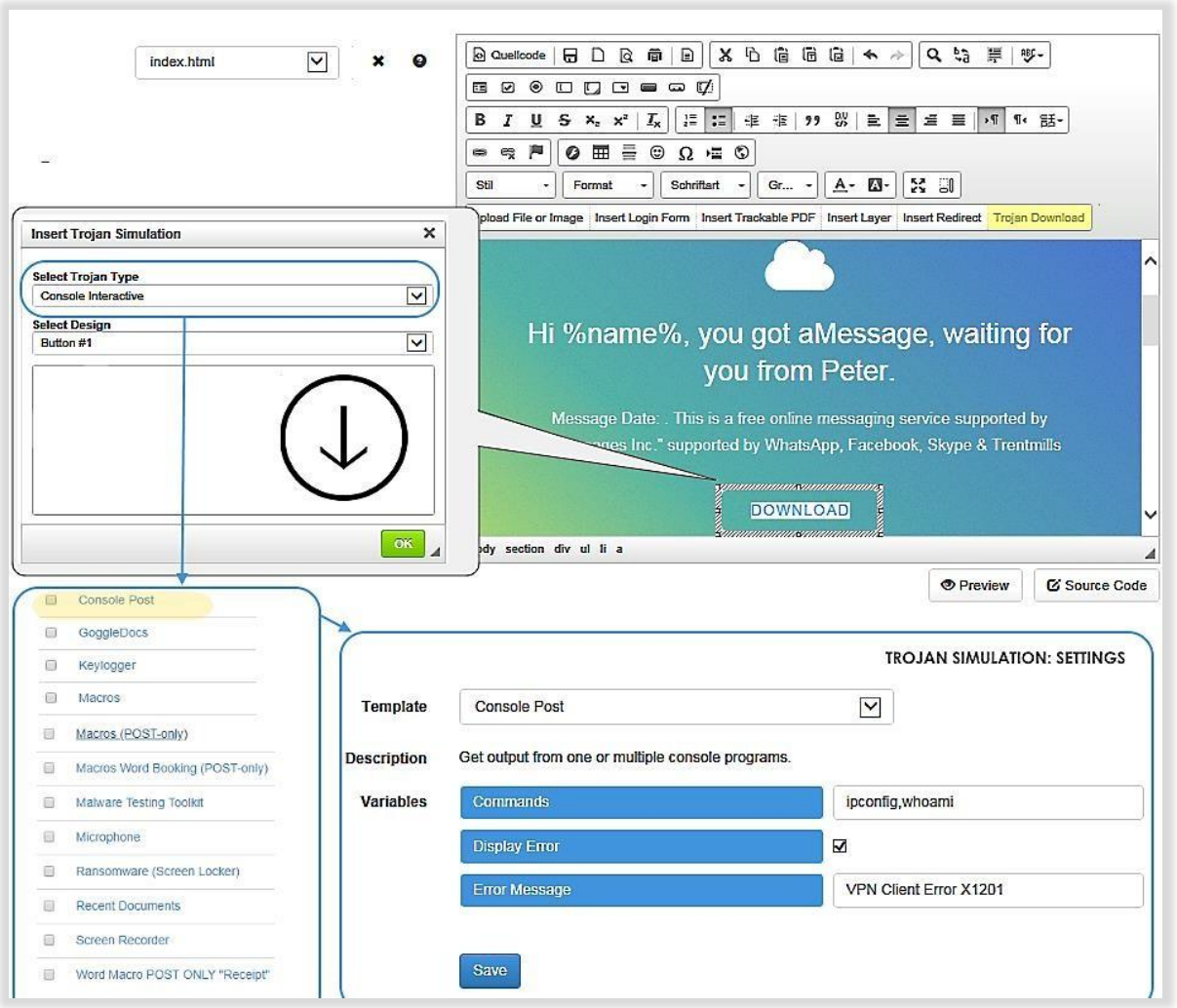
- **Güçlü URL yönlendirme yazılımı:** LUCY'nin esnek yönlendirme işlevleri, kullanıcının saldırı simülasyonu veya eğitimin istenen alanlarına doğru anda yönlendirilmesini sağlar. Örneğin, bir oltalama simülasyonuna bir şifrenin ilk 3 karakteri girildikten sonra kullanıcı şifre koruma hakkında özel bir eğitim sayfasına yönlendirilir.



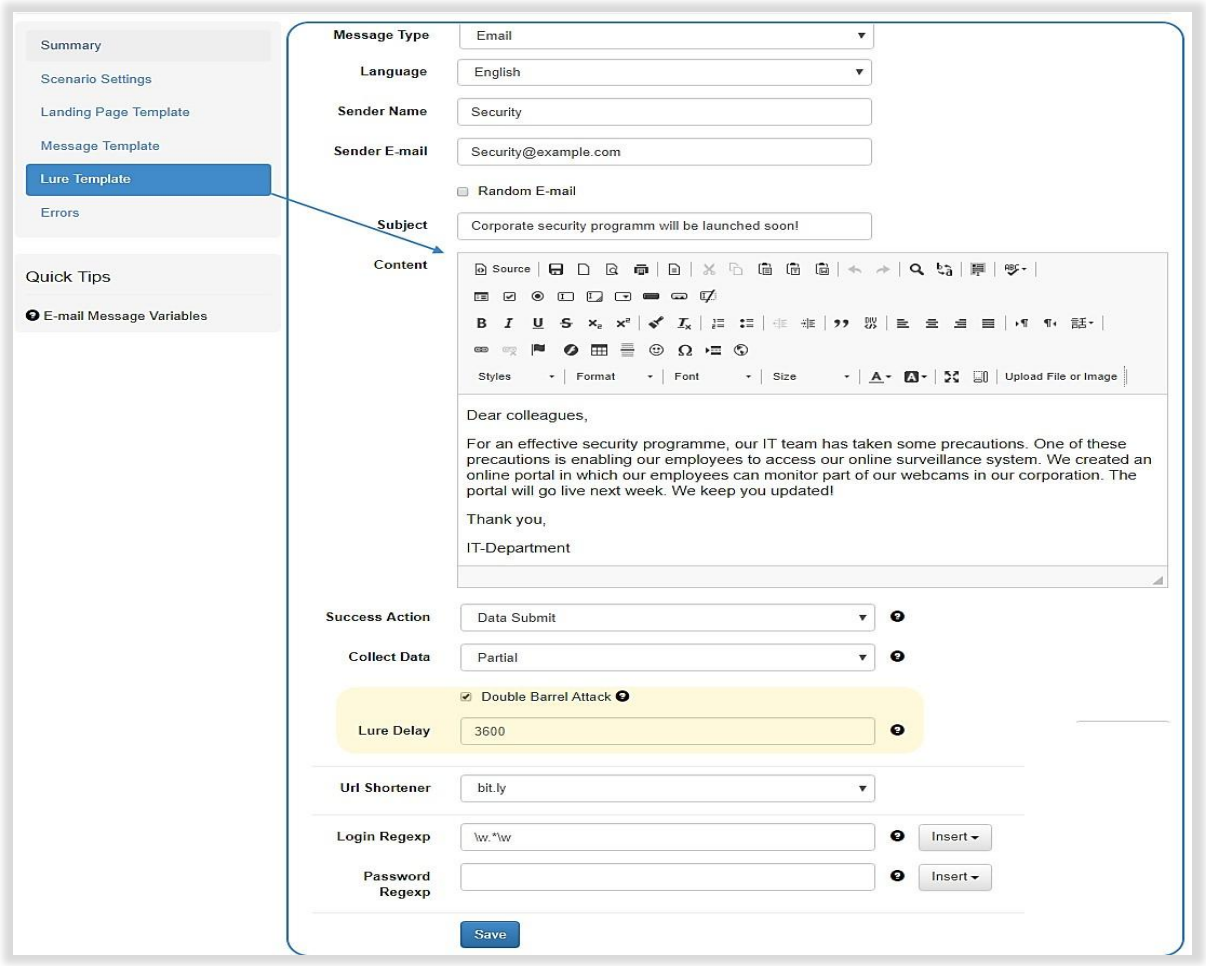
- **Karma saldırılar:** Karma saldırılar, aynı kampanya içerisinde birden fazla senaryo tipinin (dosya bazlı, veri girişi, vb.) bir kombinasyonunun kullanılmasına imkan tanır.



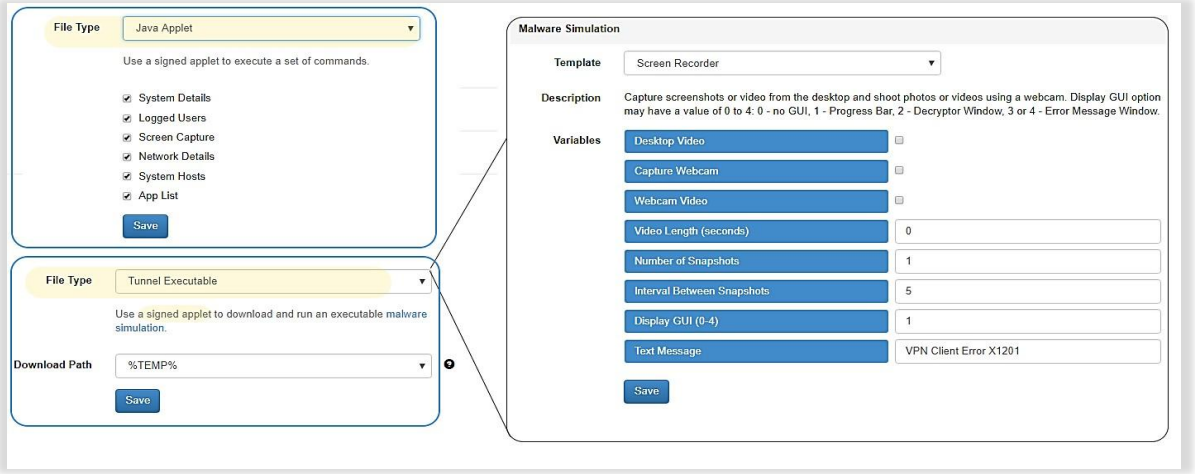
- **Dosya bazlı saldırılar:** Dosya bazlı saldırılar LUCY yöneticisinin farklı dosya tiplerini (makrolar içeren ofis belgeleri, PDF'ler, çalıştırılabilir dosyalar, MP3'ler, vb.) LUCY üzerinde oluşturulan e-posta eklentilerine veya web sitelerine entegre etmesini ve bunların indirilme veya çalıştırılma oranlarını ölçmesini sağlar.



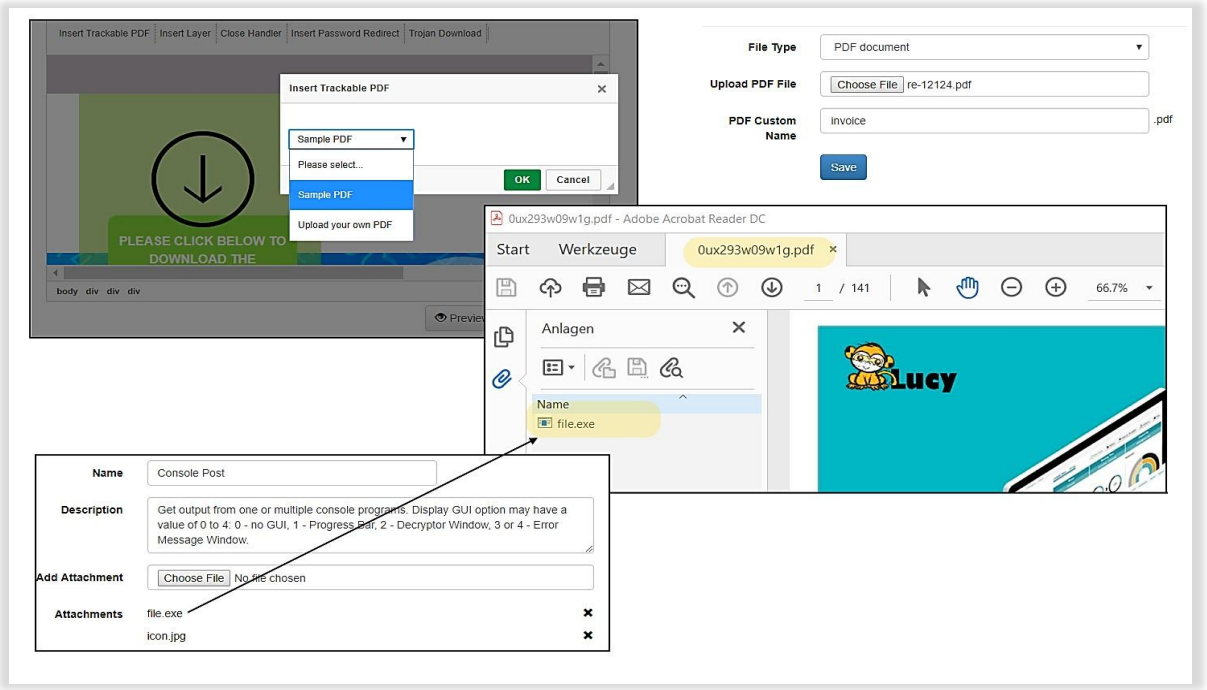
- **Çifte saldırıları:** Bu özellik sayesinde her bir kampanyada, ilki hiçbir kötü niyetli içeriği olmayan ve alıcıdan bir yanıt istemeyen tehlikesiz bir e-posta (yem) olmak üzere birden fazla oltalama e-postaları göndermek mümkündür.



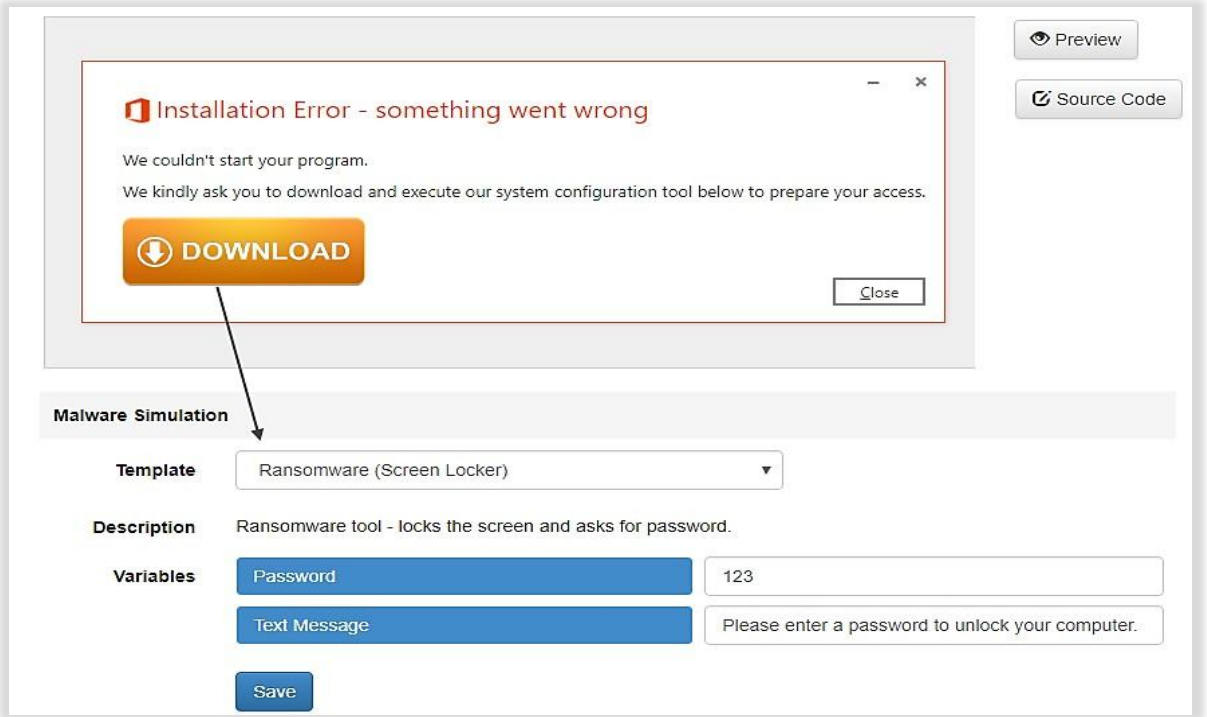
- **Java bazlı saldırılar:** Java bazlı saldırılar ile LUCY yöneticisi, LUCY içerisinde bulunan dosya bazlı veya karma saldırı şablonlarına güvenilir bir uygulama entegre edebilir ve bunun kullanıcı tarafından çalıştırılmasını ölçümleyebilir.



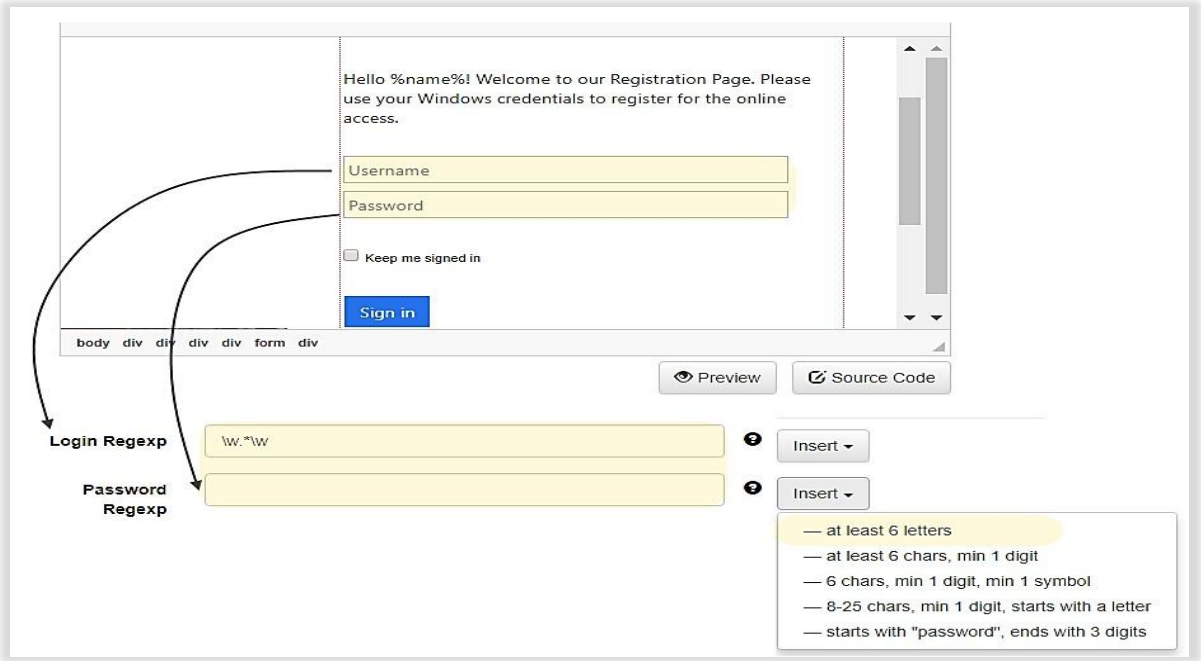
- **PDF bazlı saldırılar:** PDF bazlı oltalama saldırıları bu modül ile simüle edilebilir. LUCY, çalıştırılabilir dosyaların PDF eklentiler olarak "gizlenmesine" ve bunların çalıştırılma oranlarının ölçümlenmesine olanak tanır. Dahası, PDF'ler içerisinde dinamik oltalama bağlantıları da oluşturulabilir.



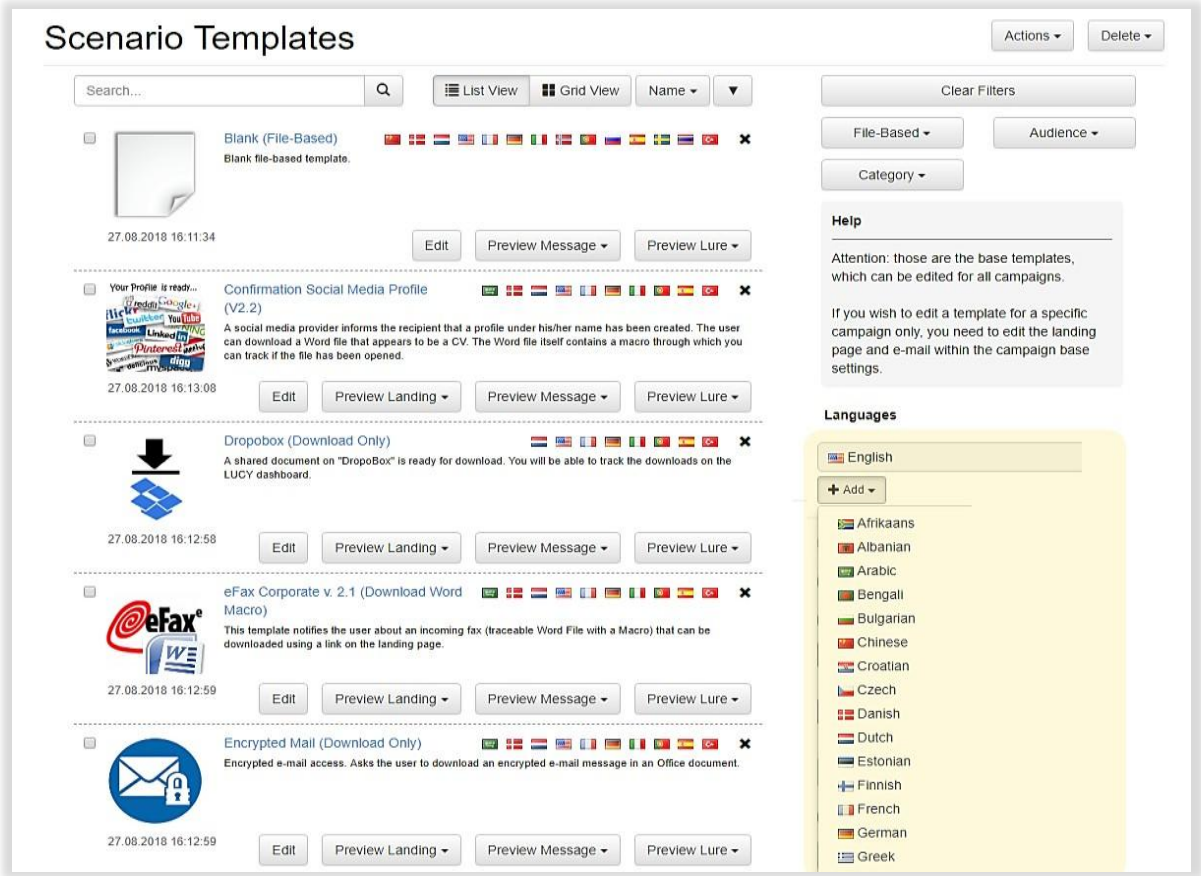
- **Fidye yazılım simülasyon saldırıları:** LUCY, biri çalışanları test eden ve diğeri de altyapıyı test eden iki farklı fidye yazılım simülasyonuna sahiptir.



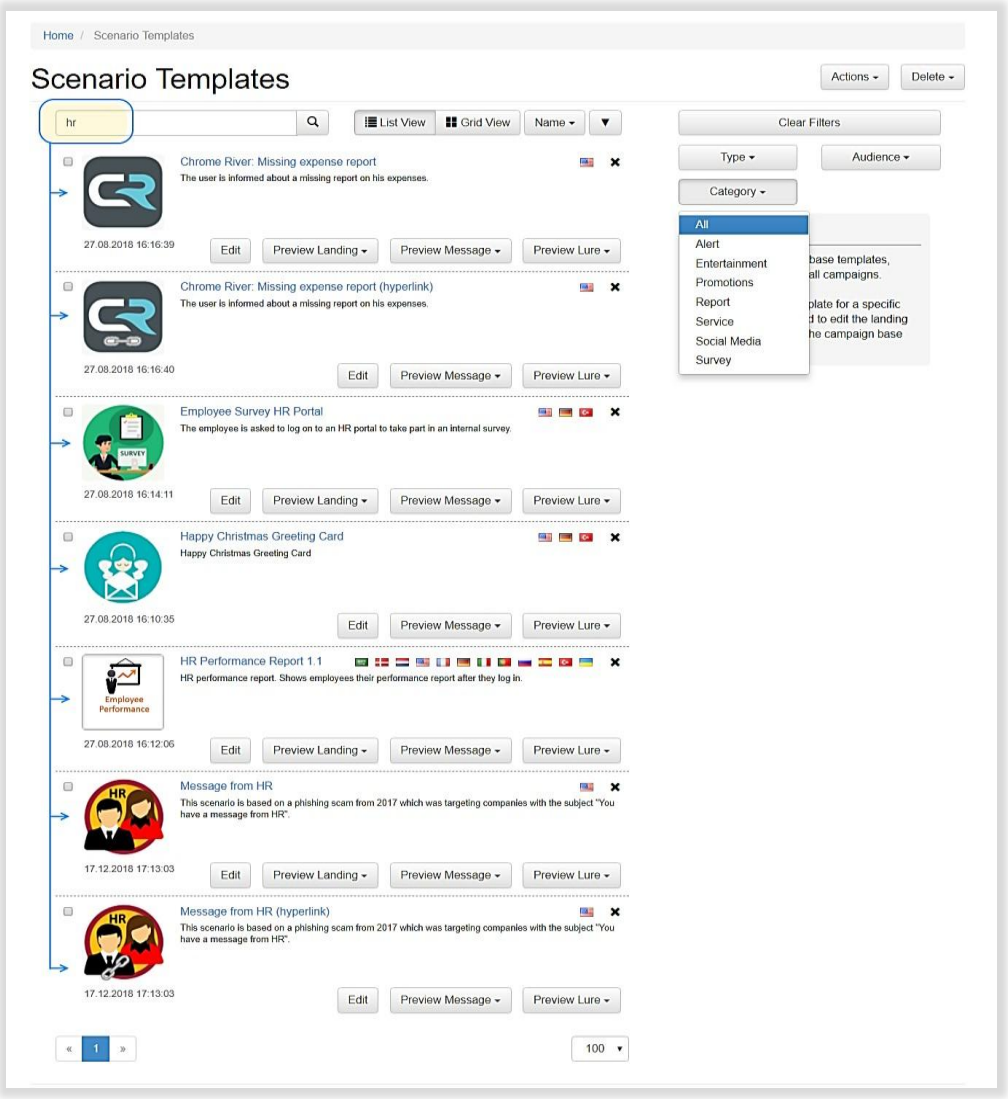
- **Veri girişi doğrulama yazılımı:** Oltalama simülasyonlarında, kullanıcı bilgi alanlarına girilen sahte pozitiflerden (geçersiz bir söz dizisi ile oturum açma gibi) kaçınılmalıdır. Şirket ilkeleri şifreler gibi hassas verilerin iletilmesini yasaklayabilmektedir. Bu amaç doğrultusunda LUCY, her gereksinime uygun bir çözüm sunan esnek bir girdi filtreleme motoru sağlamaktadır.



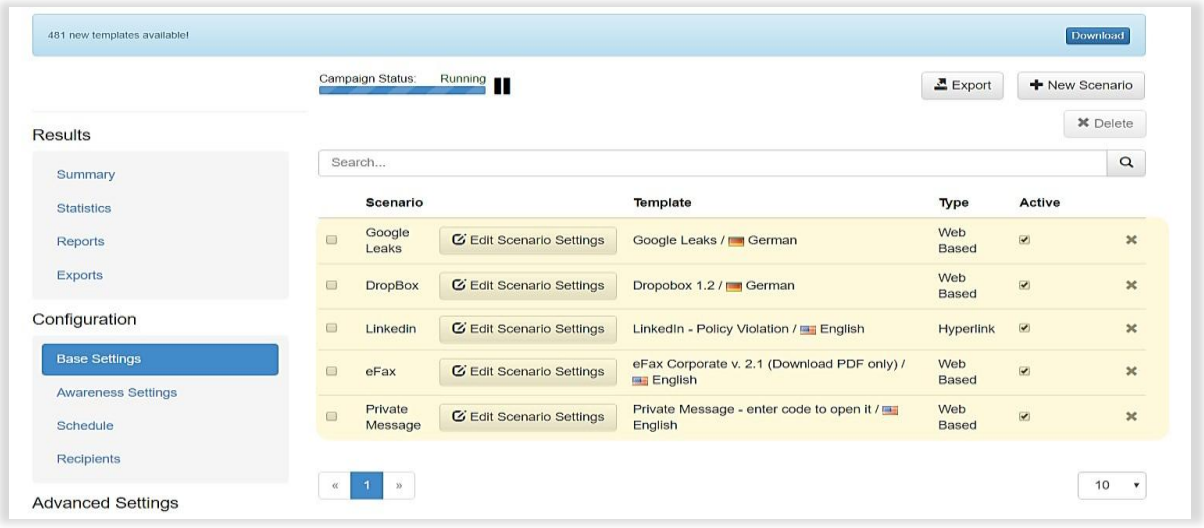
- **Çok Dilli Saldırı Şablonu Kitaplığı:** LUCY, veri girişi (web siteli şablonlar), dosya bazlı (dosya indirmeli e-posta veya web sitesi), köprü bağlantısı (bağlantı içeren e-postalar), karma (veri girişi ve indirmenin kombinasyonu) ve taşınabilir ortam kategorilerinde 30 dilde yüzlerce öntanımlı saldırı şablonu hazır olarak sunulmaktadır.



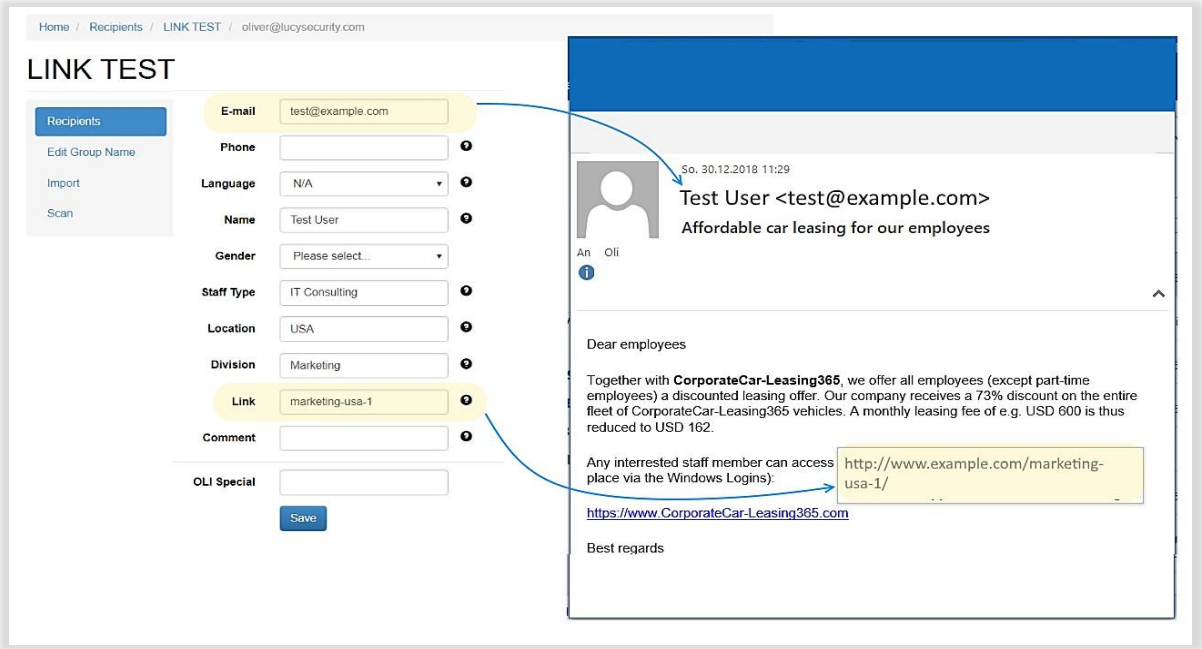
- **Sektör ve bölüme özel şablonlar:** Belirli sektörler veya bölümler için tasarlanmış saldırı şablonları.



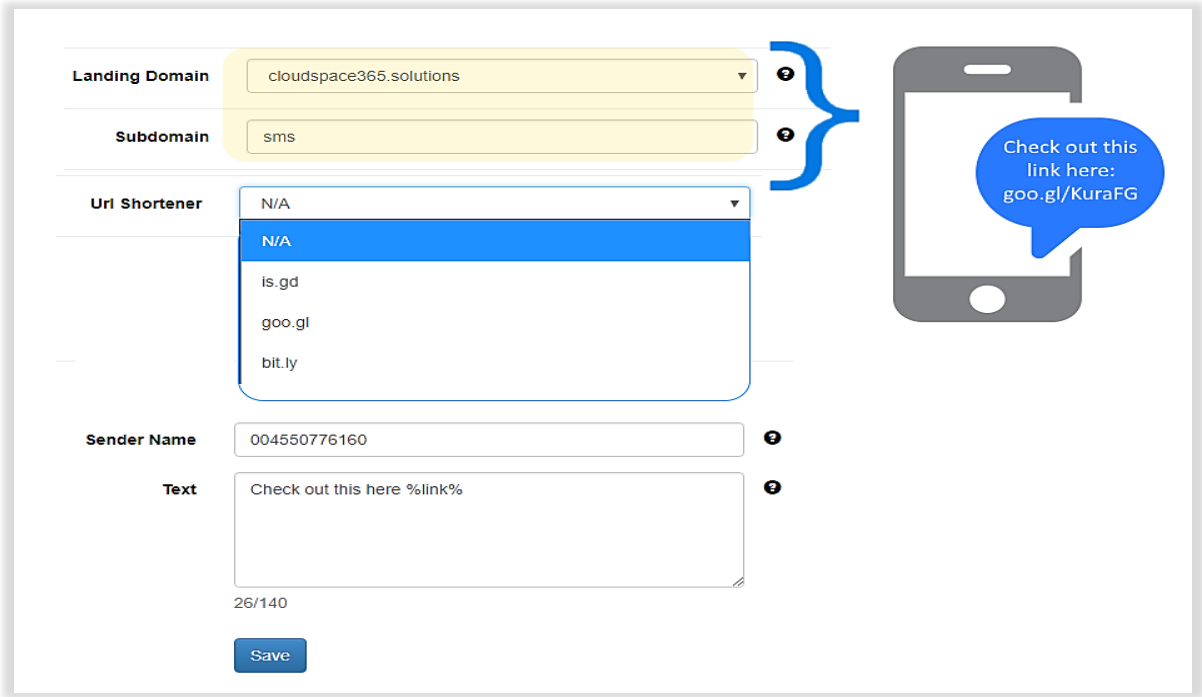
- **Eşzamanlı saldırı şablonu kullanımı:** LUCY size tek bir kampanyada birden fazla saldırı simülasyonu şablonu kullanma seçeneğini sunmaktadır. Farklı tipleri (köprü bağlantısı, dosya bazlı, vb.) farklı saldırı temalarıyla birleştirerek mümkün olan en yüksek risk kapsamına ulaşın ve çalışanlarınızın zafiyetlerini daha iyi anlayın. Zamanlama randomizasyonu aracımız ile birlikte kompleks saldırı modelleri daha uzun bir süre zarfında gerçekleştirilebilir.



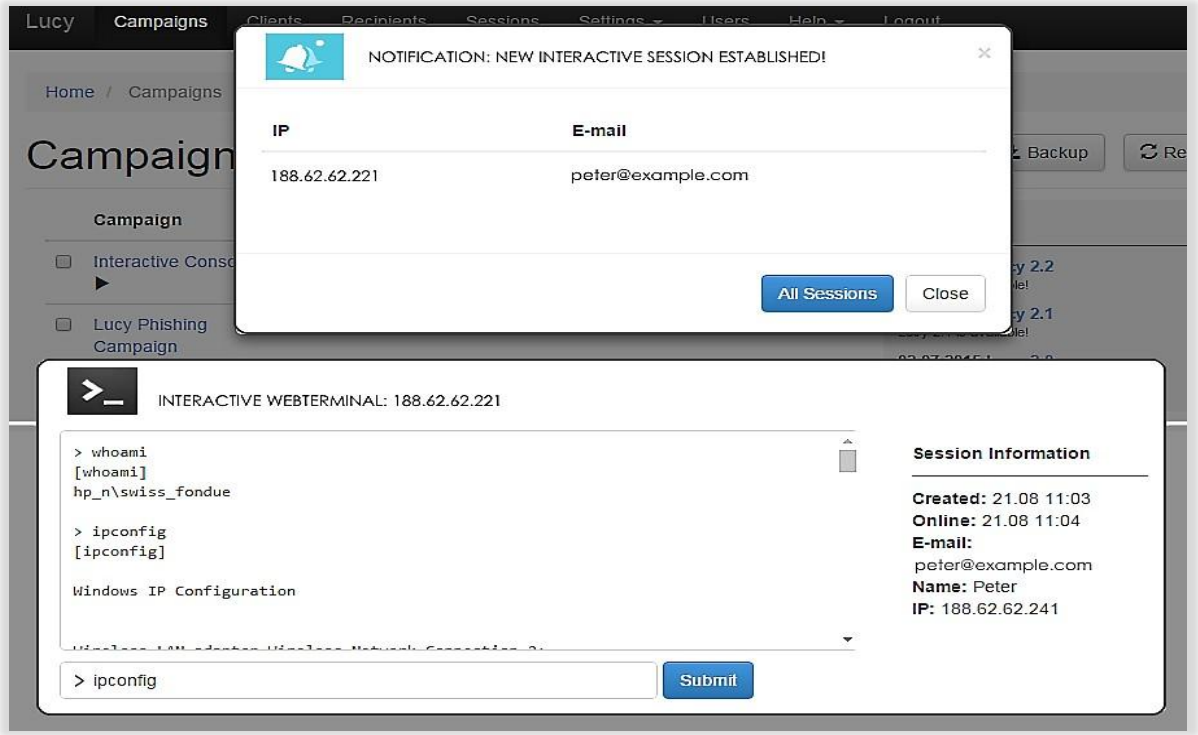
- **Saldırı URL'si varyasyonları:** Alıcıları belirlemek için oluşturulan URL'lerin kontrolünü elinize alın. Otomatik kısa (< 5 karakter) veya uzun URL dizileri kullanın ya da her bir kullanıcı için ayrı URL'ler belirleyin. Manüel URL oluşturma ile bir kullanıcının kolaylıkla hatırlayabileceği bağlantılar oluşturabilirsiniz. Bağlantıya tıklama özelliğinin e-postalarda devre dışı bırakılmış olduğu ortamlarda bu bir zorunluluktur.



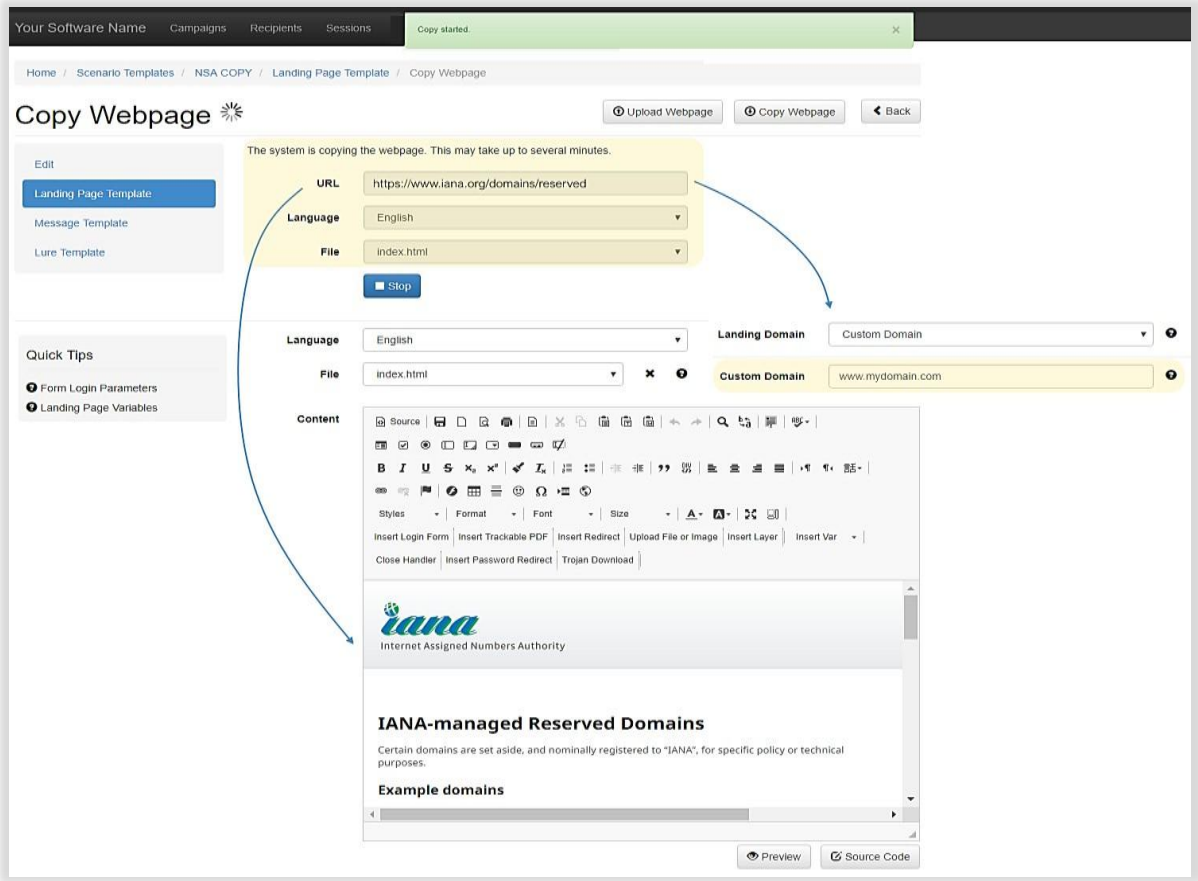
- **URL Kısaltma:** URL kısaltma, yeni sayılabilecek bir İnternet hizmetidir. Birçok online sosyal hizmet karakter sınırlamaları getirmiş (Twitter gibi) olduğu için bu URL'ler son derece pratiktir. Ancak URL kısaltma siber suçlular tarafından bir bağlantının gerçek hedefini, yani oltalama veya virüs sitelerini gizlemek için kullanılabilir. Bu nedenle de LUCY, bir e-posta veya SMS oltalama kampanyasına farklı kısaltma hizmetlerini dahil etme imkanını sunar.



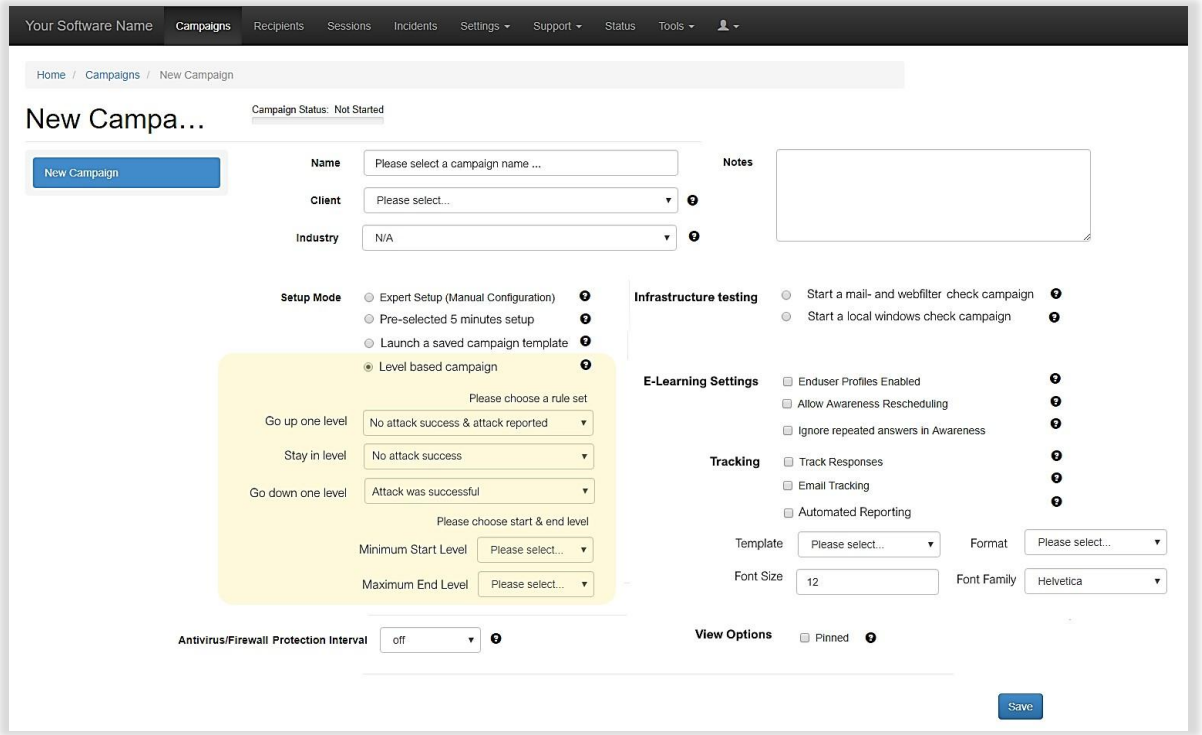
- **Pentest kiti:** Pentest kiti, kötü amaçlı yazılım simülasyon yazılımının bir alt modülüdür ve "İnteraktif Oturumlar" adı ile geçmektedir. Tersine http/s bağlantıları kullanarak güvenlik duvarları ardındaki bir istemci bilgisayarı ile interaktif olarak iletişim kurmanıza olanak tanır.



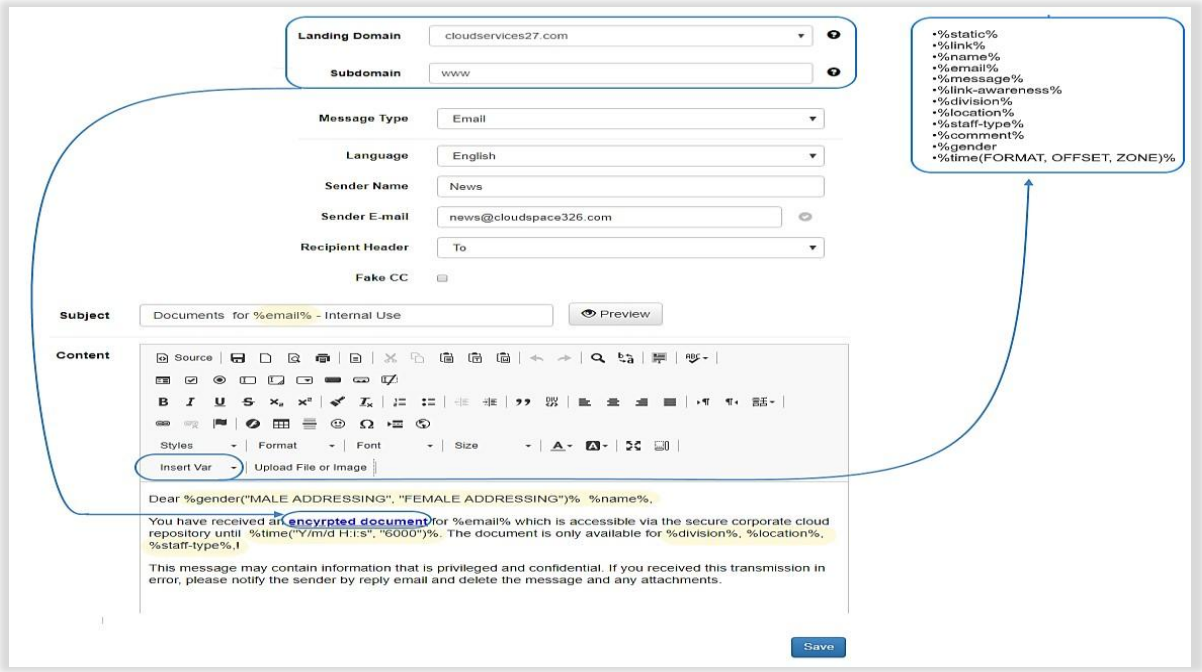
- **Web sitesi klonlayıcı:** Kampanyalarınız için hızla son derece profesyonel görünümlü giriş sayfaları oluşturun. Mevcut web sitelerini klonlayın ve veri giriş alanları, indirilebilir dosyalar, vb. ile bunlara ilave katmanlar ekleyin.



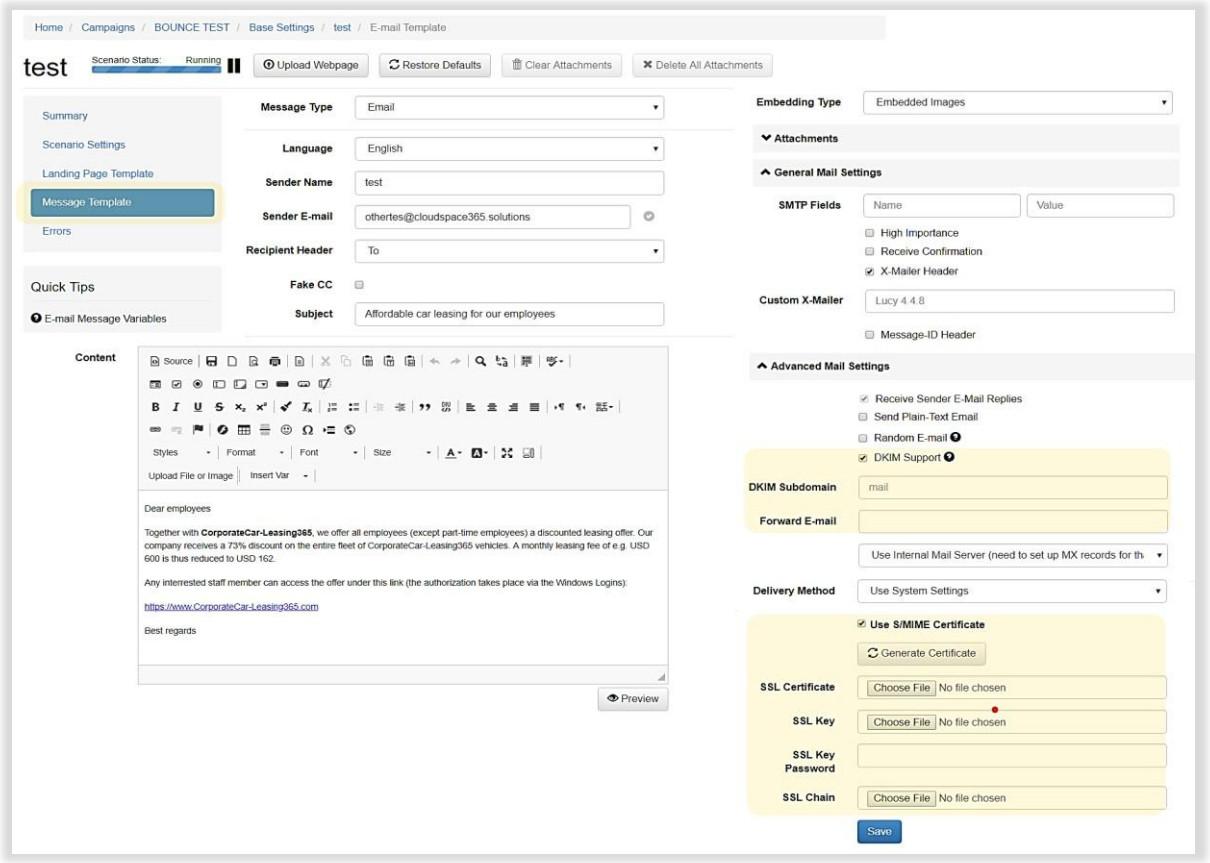
- **Seviye bazlı saldırılar:** Çalışanlar için seviye bazlı oltalama eğitimi, sosyal hacklenme riskinin ölçeklenebilir olmasına hizmet etmektedir. Bireysel eğitim içeriklerinin otomatik olarak sağlanabilmesi için bilimsel analizlerin en önemli risk faktörlerini belirlemesi gerekir.



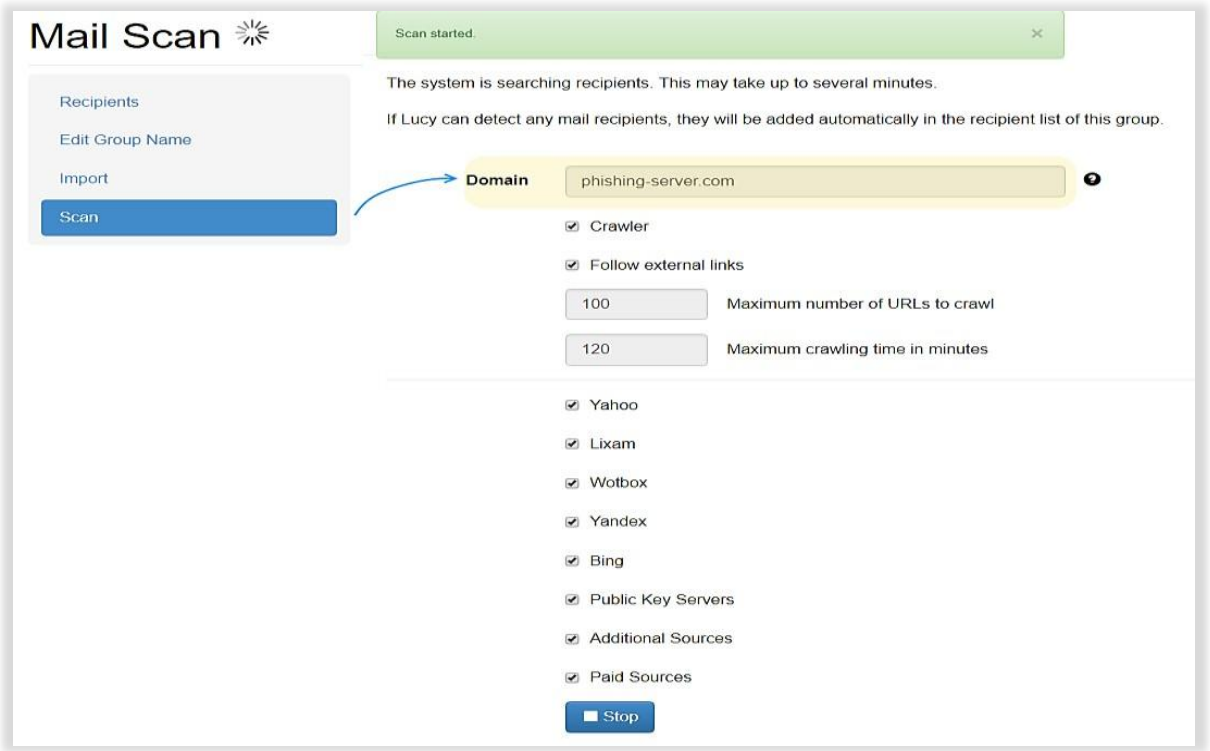
- **Spear (hedefli) oltalama simülasyonu:** Spear Phish Uyarlaması, giriş sayfası ve mesaj şablonlarında kullanabileceğiniz dinamik değişkenler (cinsiyet, saat, isim, e-posta, bağlantılar, mesajlar, bölüm, ülke, vb.) ile çalışır.



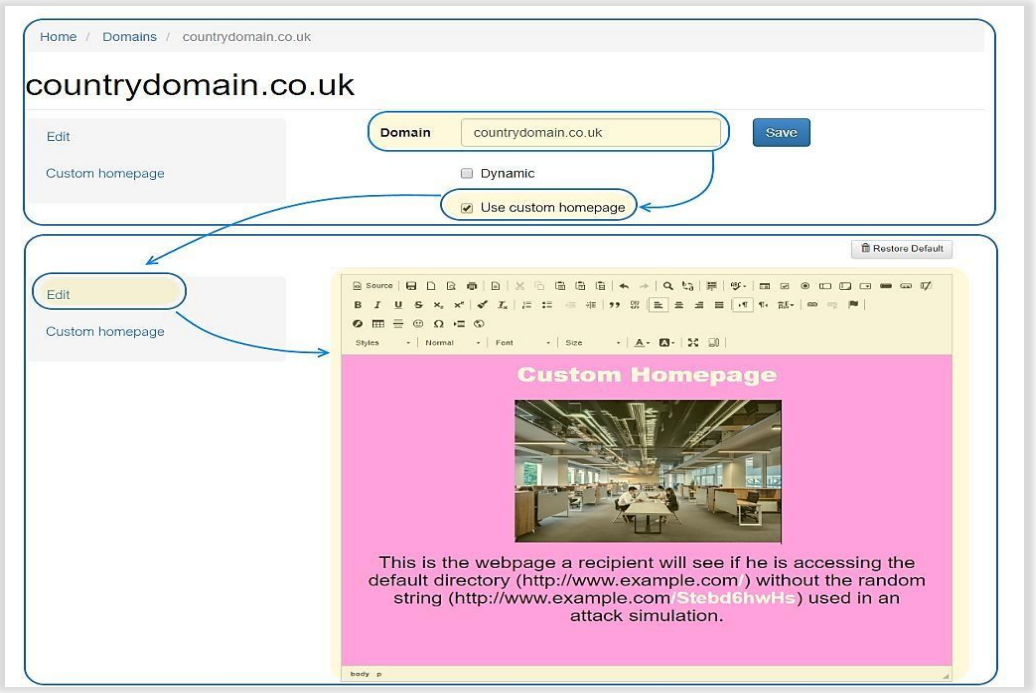
- **Oltalama E-postaları için DKIM / S / MIME Desteği:** E-postalar için dijital imzalar: İmzalanmış simülasyon postaları (s/mime) gönderin. Daha iyi bir gönderici skoru almak için DKIM kullanın.



- **E-posta tarayıcı:** Kurumunuzun hangi e-posta adreslerinin internette bulunabileceğini merak mı ediyorsunuz? LUCY'nin e-posta tarayıcısını kullanın ve bir bilgisayar korsanının şirketiniz hakkında zaten neler bildiğini öğrenin.

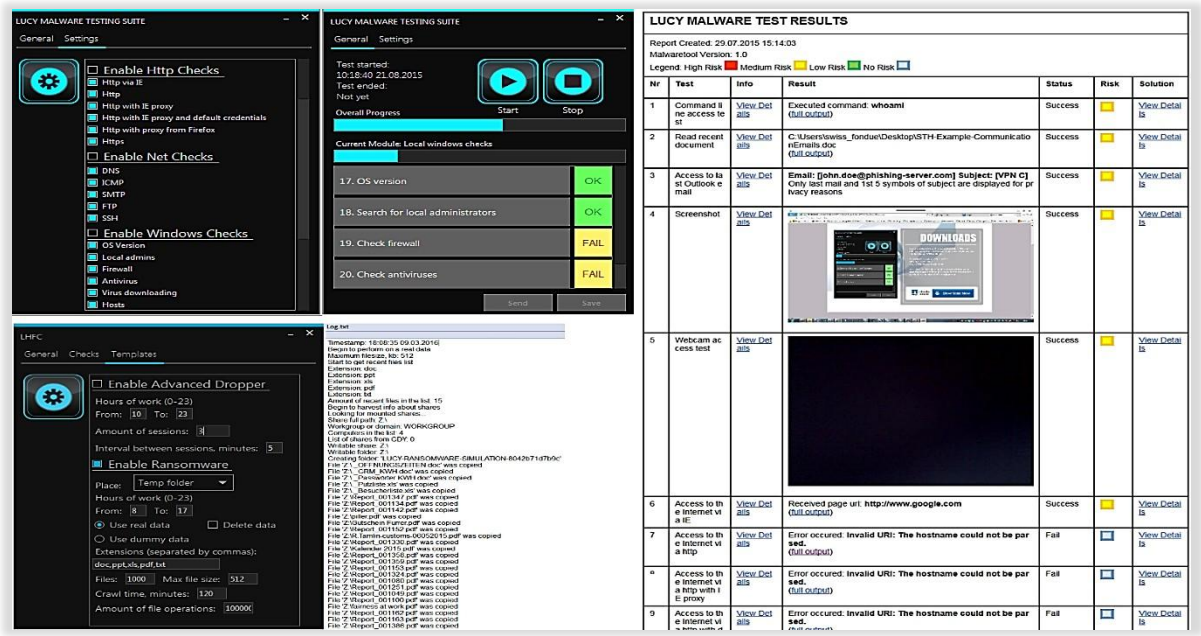


- **Özel ana sayfa oluşturma:** Teknik bilgileri daha iyi olan alıcılar, rastgele oluşturulmuş olan oltalama bağlantısı ile ilişkilendirilmiş alan adı veya IP adresini aratmak için tarayıcılarını kullanabilirler. Hata mesajlarının görüntülenmesini ya da son kullanıcının yönetici panelinin giriş ekranına ulaşmasını önlemek amacıyla, oltalama simülasyonunda kullanılan alan adları için LUCY içerisinde standart "ana sayfalar" oluşturabilirsiniz.

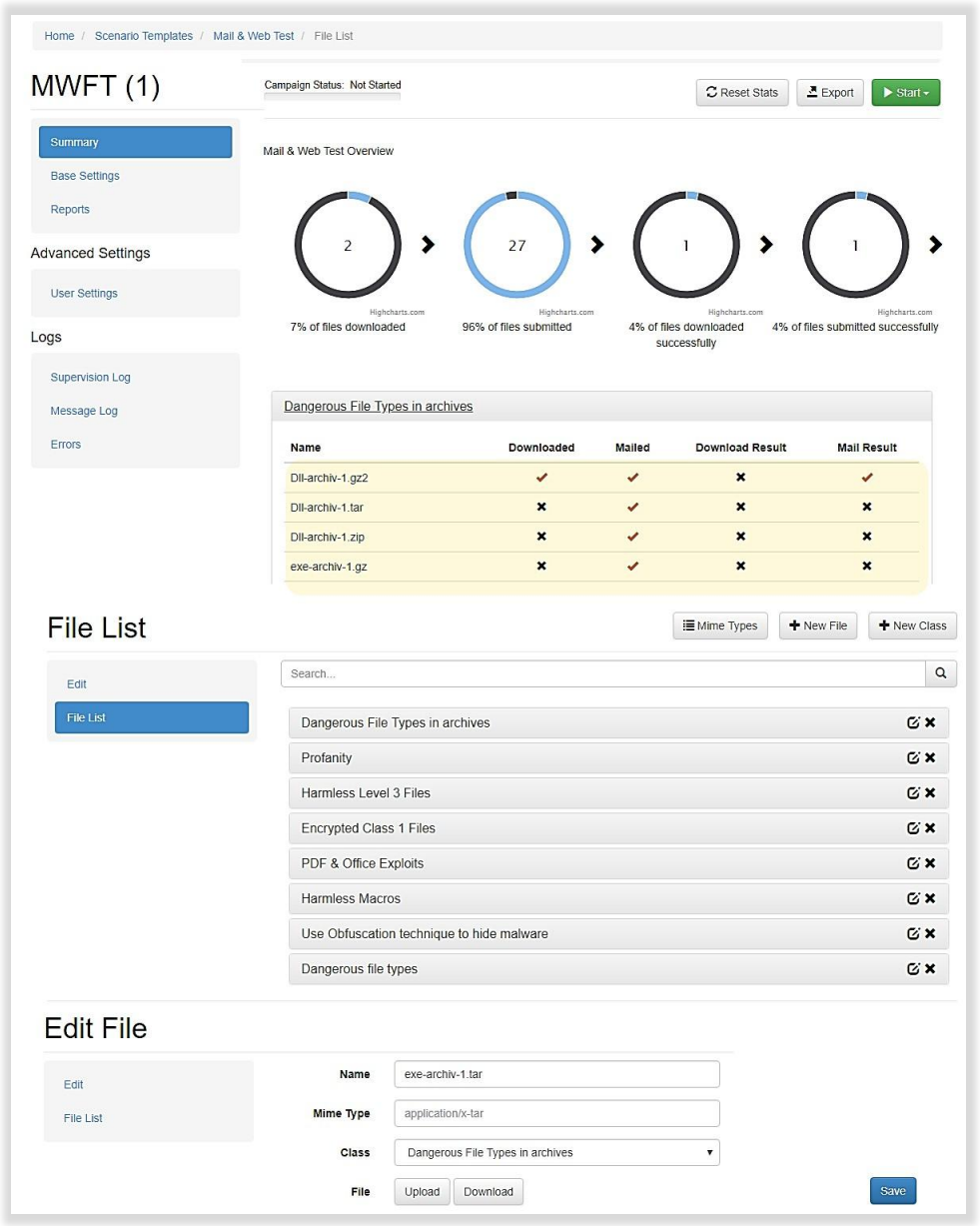


ALTYAPI TESTLERİ

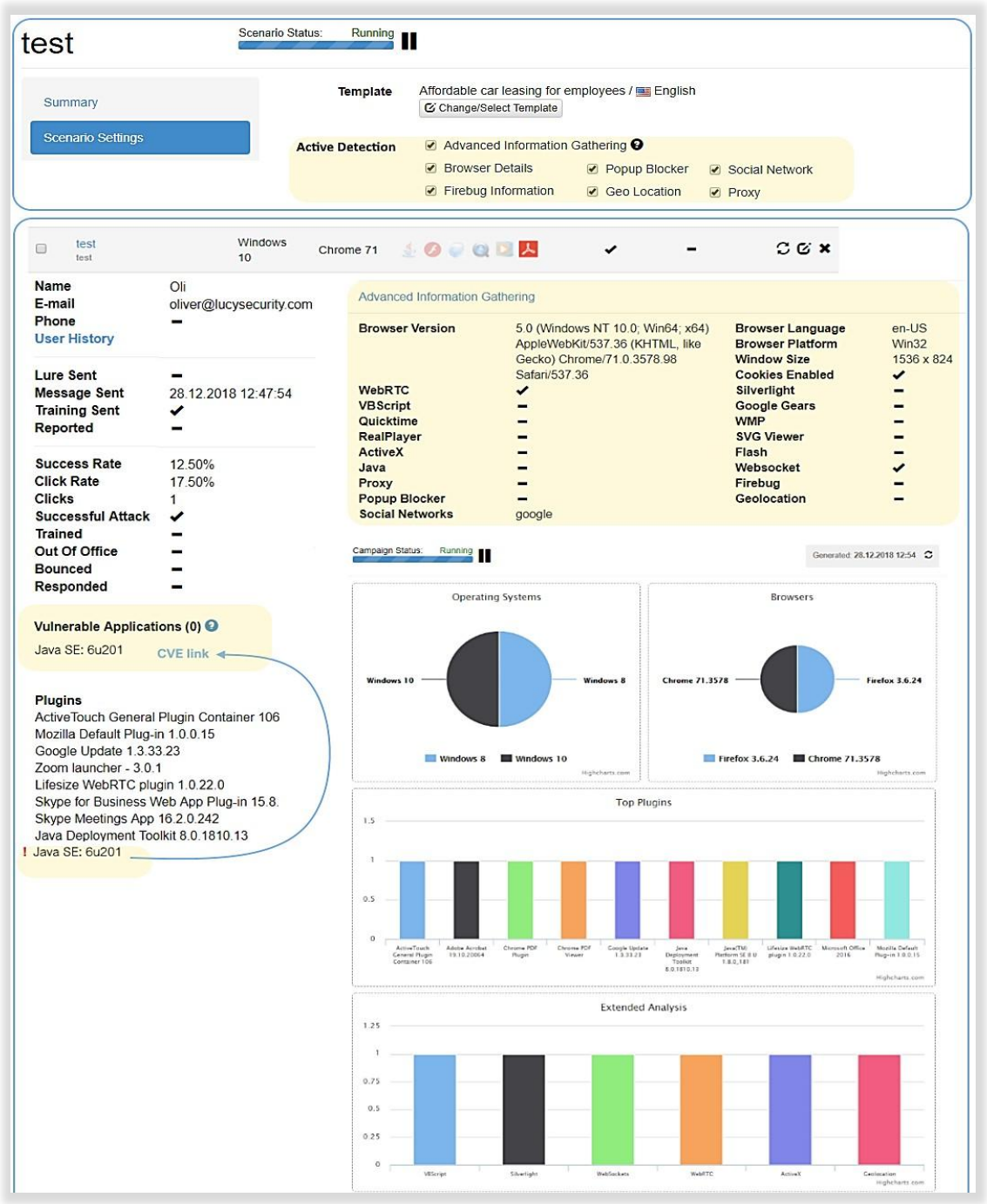
- **Kötü Amaçlı Yazılım Test Kiti:** Kötü Amaçlı Yazılım Simülasyon Kiti, çeşitli tehditleri taklit etme yeteneğine sahip gelişmiş bir kötü amaçlı yazılım simülasyonudur. Bir denetçinin, siber suçlular tarafından kullanılan araçların birçoğuna denk, gelişmiş bir dizi özelliğe erişimine imkan tanır. Dolayısıyla da bu araç, LUCY yöneticisinin BT departmanı dışındaki çalışanları dahil etmeksizin güvenlik kontrolleri gerçekleştirmelerine imkan tanır.



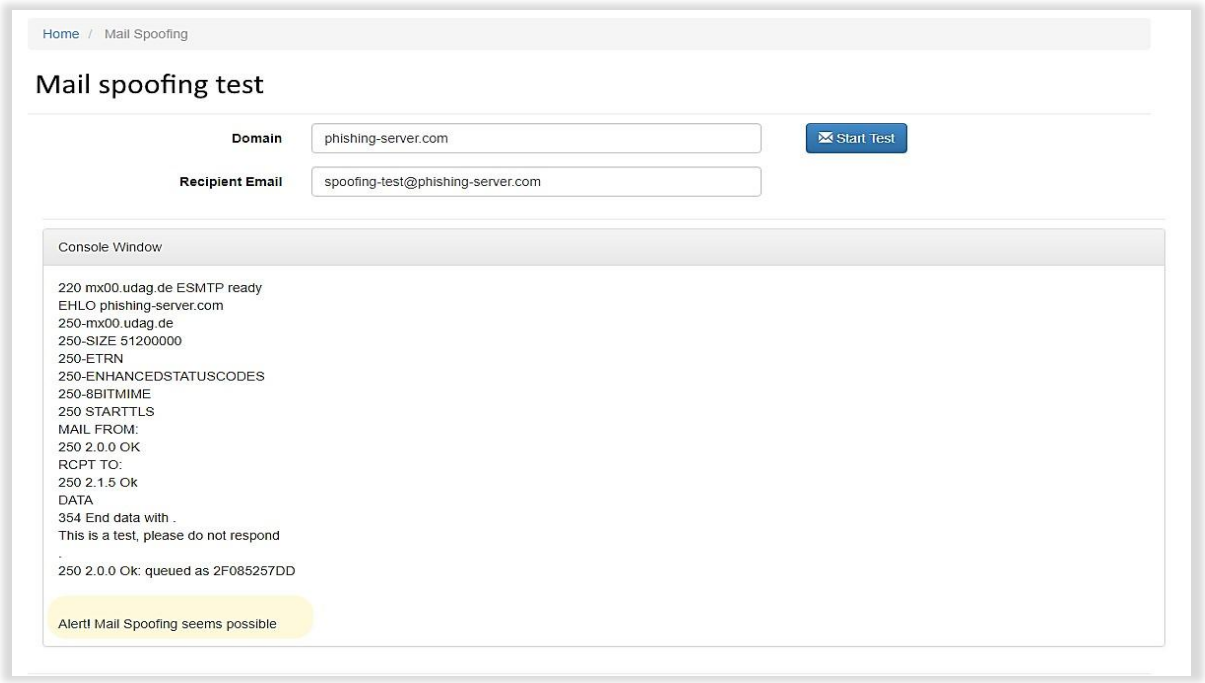
- **Posta ve Web Filtreleme Testi:** Bu işlev, internet ve posta trafiğini güvenli hale getirmekte mevcut en önemli sorulardan birini yanıtlamaktadır: Hangi dosya tipleri internetten indirilebiliyor ve hangi e-posta eklentileri filtreleniyor ya da filtrelenmiyor?



- **Aktif ve Pasif İstemci Zafiyetinin Saptanması:** Bu özellik, istemci tarayıcısının yerel olarak test edilmesi ve olası zafiyetlerin özel JavaScript kitaplıkları ve tarayıcı kullanıcı aracı sunucusu verilerine dayalı olarak saptanmasına imkan tanır. Bulunan eklentiler otomatik olarak zafiyet veritabanları (CVE) ile karşılaştırılarak korumasız cihazlar belirlenebilir.

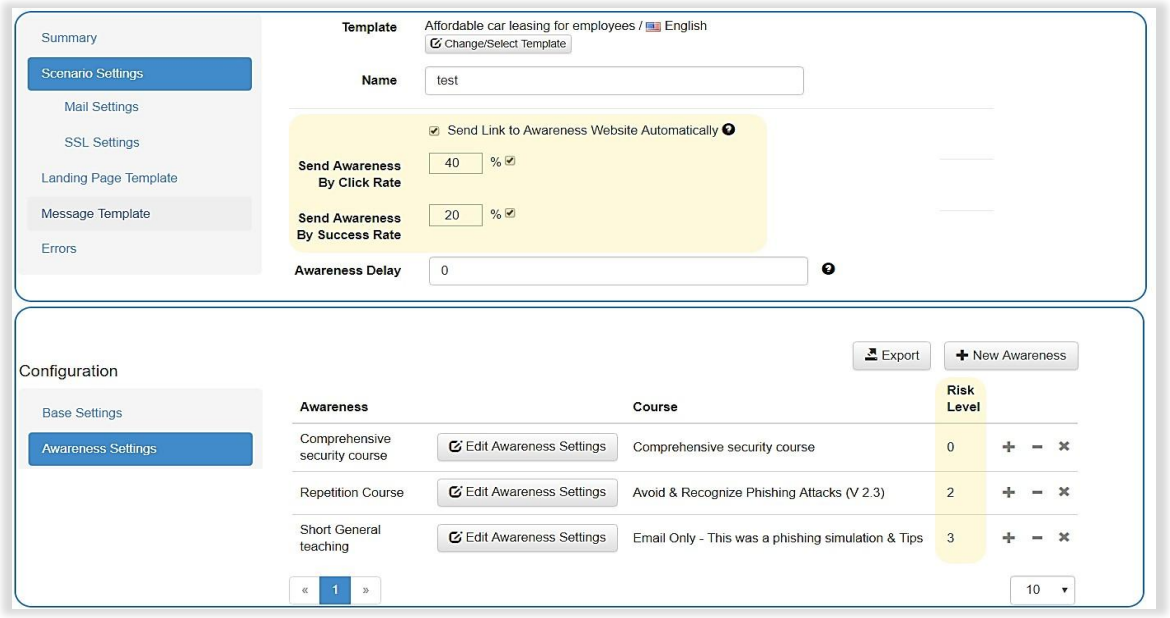


- **Spoofing Testi:** Kendi altyapınızı e-posta spoofing zafiyetlerine karşı test edin.

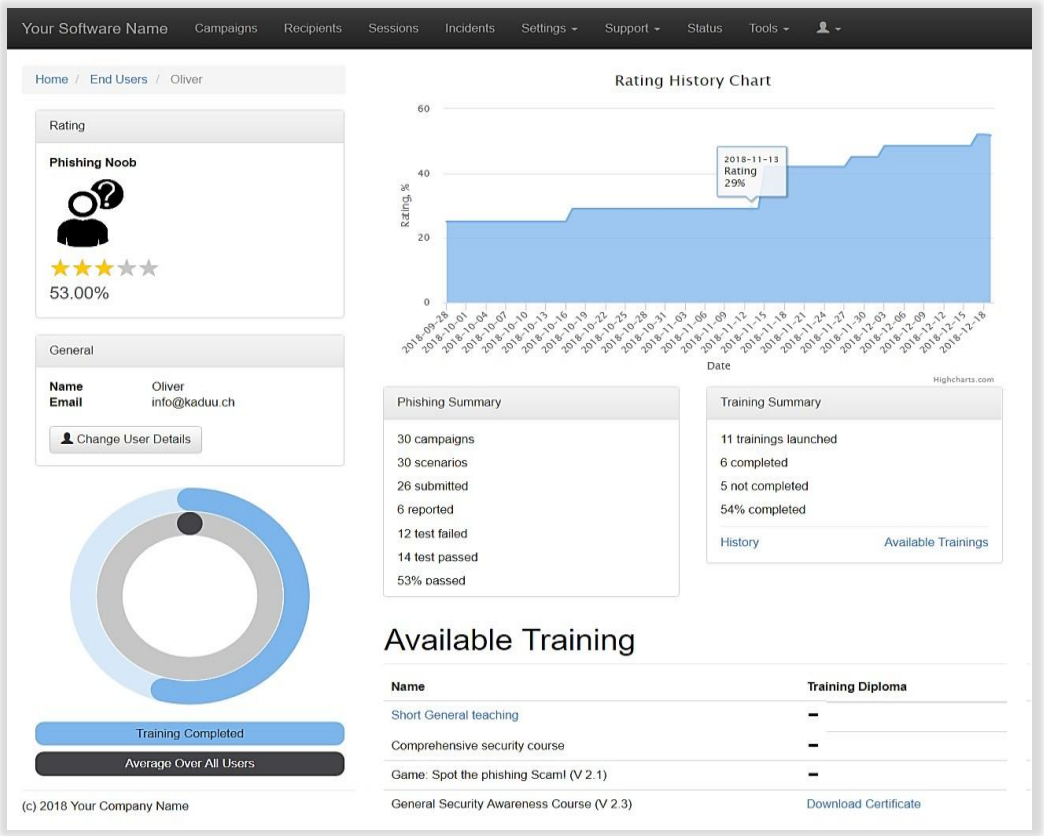


TEKNİK TESTLER

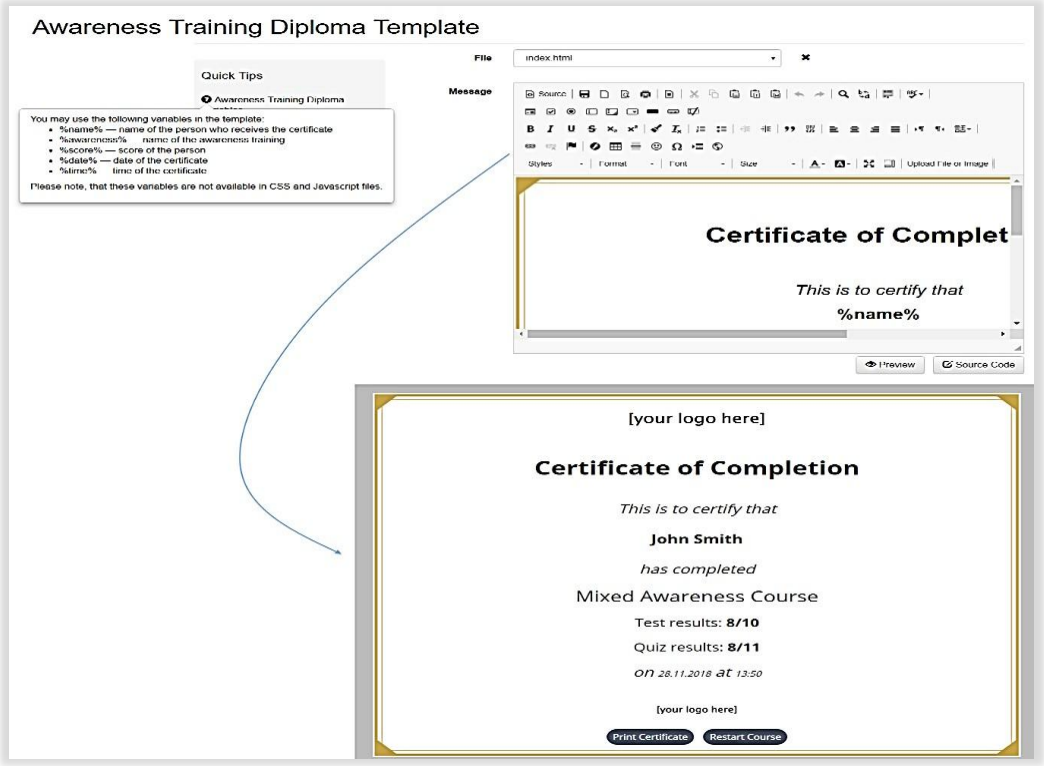
- **İtibar Bazlı e-Öğrenme:** Çalışanlarınızı kendilerinden beklenen becerilere uygun olarak eğitin. Çalışanların yeteneklerini ölçün ve iş arkadaşları arasında dostça rekabet olanağı (oyunlaştırma) sağlayın.
Sistem, her bir kullanıcının itibar profillerine bağlı olarak otomatikman birden fazla eğitim seansı sunacaktır. İtibar profilleri, diğer faktörlere ek olarak kullanıcının oltalama simülasyonlarındaki davranışlarına dayanmaktadır. Bu da tekrarlayan hatalar yapan kullanıcıların, bir saldırı simülasyonuna ilk kez tıklayanlardan farklı eğitim içerikleri almalarını sağlar.



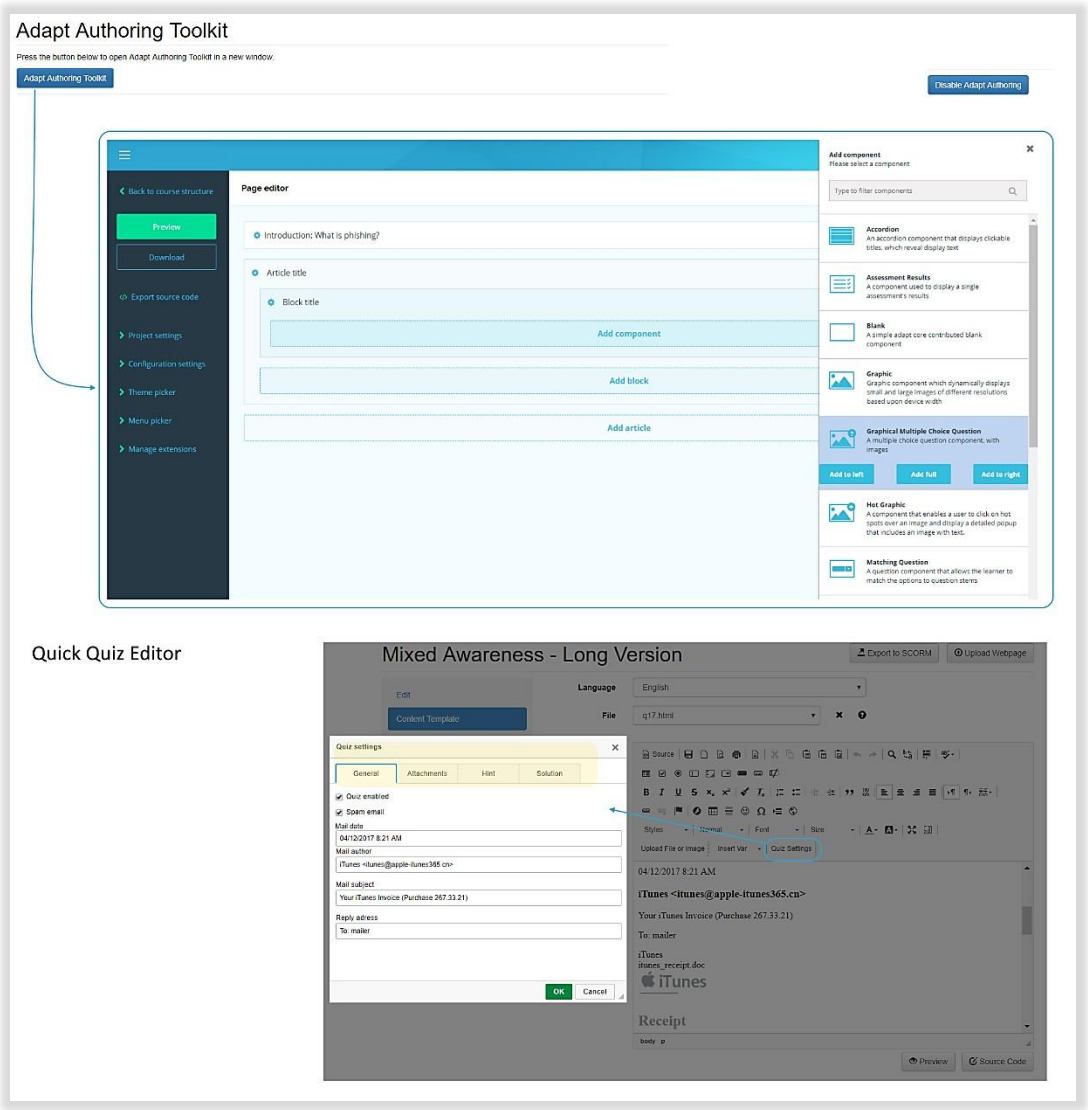
- **Son Kullanıcı Eğitim Portalı:** Öğrenme Yönetim Sistemi (LMS) işlevi: Her çalışana, kendileri için özel hazırlanmış kendi kurslarınızı içeren kişiselleştirilmiş eğitim ana sayfasına erişim sunar. Bu ana sayfa üzerinde kendi performans istatistiklerini görüntüleyebilir, eğitime devam edebilir veya tekrarlayabilir, kurs sertifikaları oluşturabilir ve aldıkları sonuçları diğer departmanlar veya gruplar ile karşılaştırabilirler.



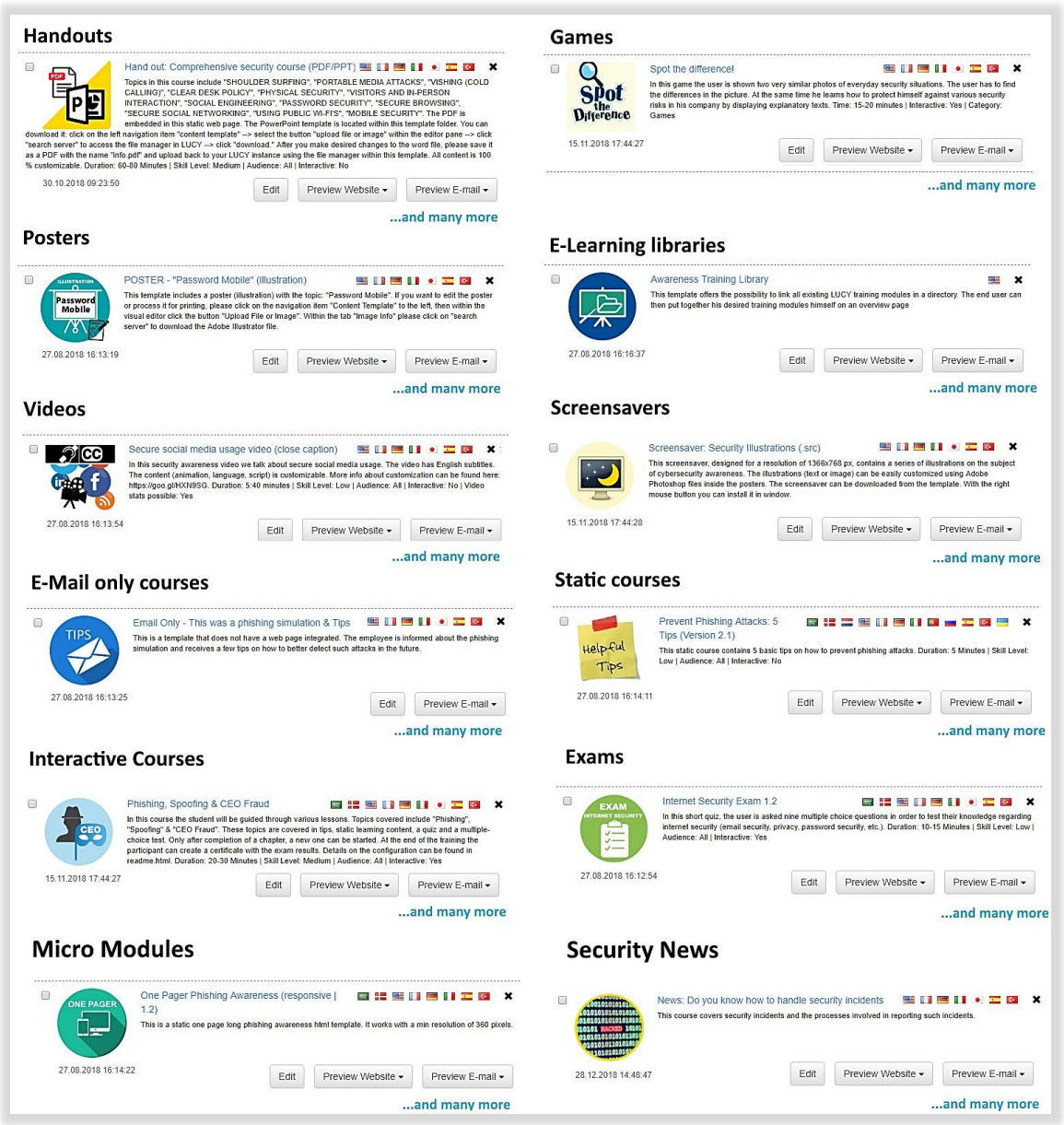
- **Farkındalık Eğitimi Diploması:** e-Öğrenme sertifikaları alıcı tarafından eğitim içerisinden doğrudan ya da LMS portalı içerisinden oluşturulabilir ve yazdırılabilir.



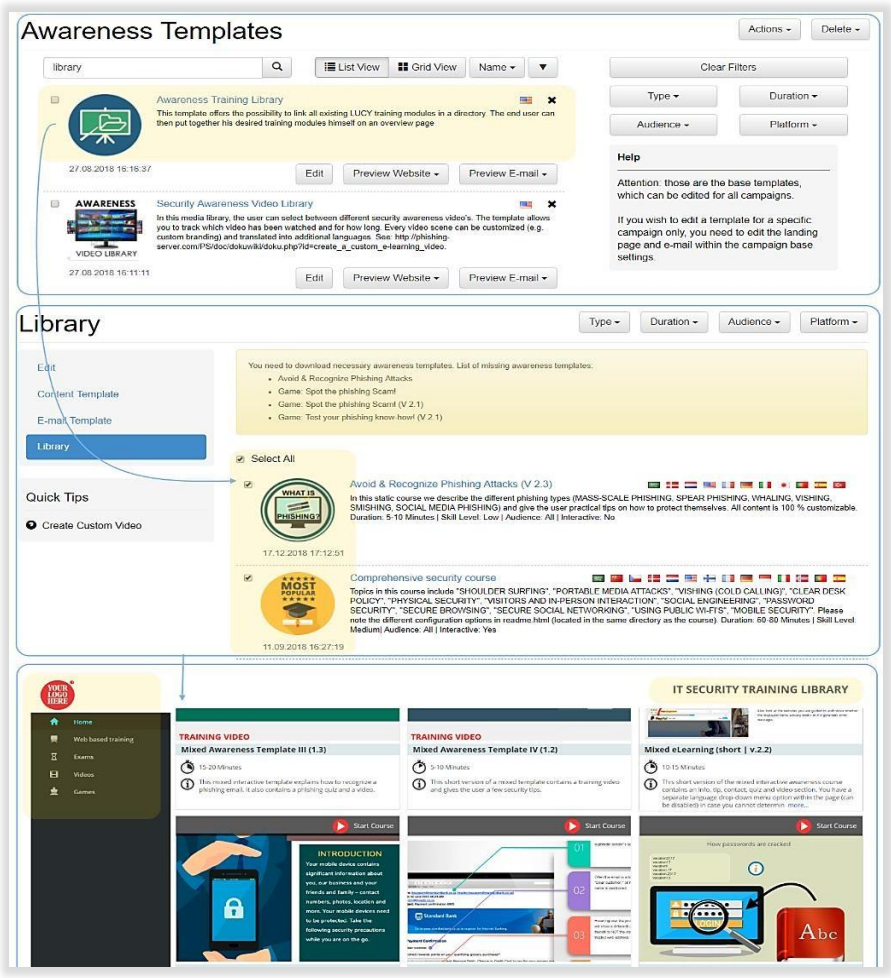
- **e-Öğrenme Yazarlık Kiti:** e-Öğrenme Yazarlık Kiti (Adapt) ile kişiselleştirilmiş eğitim içerikleri oluşturmak mümkündür. Videolar veya diğer herhangi zengin ortam biçimini sürükleyin ve bırak, öntanımlı menülerden sınavlar ekleyin, interaktif e-öğrenme içeriklerini sıfırdan kısa sürede oluşturun.



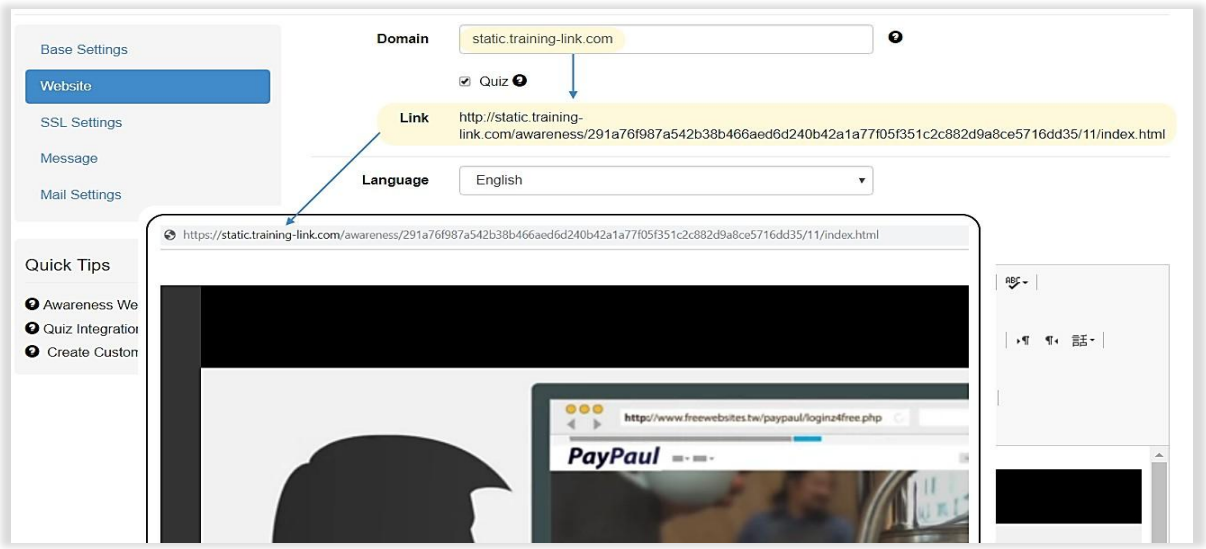
- **Zengin Ortam Farkındalığı Eğitimi:** Zengin ortamı (video, ses dosyası veya izleyicilerin içerik ile etkileşimi ve katılımını teşvik eden diğer unsurlar) farkındalık eğitimlerinize entegre edin. Mevcut eğitsel videoları kullanın, onları uyarlayın veya kendi zengin ortamınızı ekleyin.



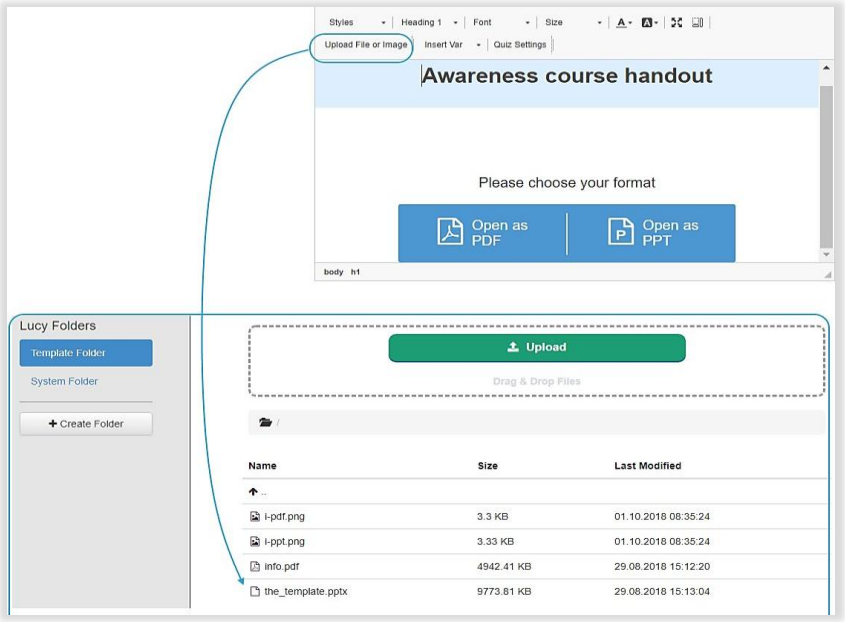
- **Eğitim Kitaplığı:** Çalışanlarınız kurumunuzun eğitim içeriklerine "eğitim kitaplığı" adı verilen bir genel bakış sayfasından erişebilirler. Bu sayfa LUCY'nin standart, girdi işlevi gören e-öğrenme şablonlarından geniş bir seçki içerir. Genel bakış sayfası belirli başlıklara (video, ara test, test, vb.) göre sıralanabilir.



- **Statik Eğitim Desteği:** Eğitim içerikleri ayrıca LUCY veya intranet içerisindeki statik sayfalarda da yayınlanabilir ve kullanıcıya olası saldırı simülasyonlarından bağımsız olarak eğitim içeriklerine erişim sunar.

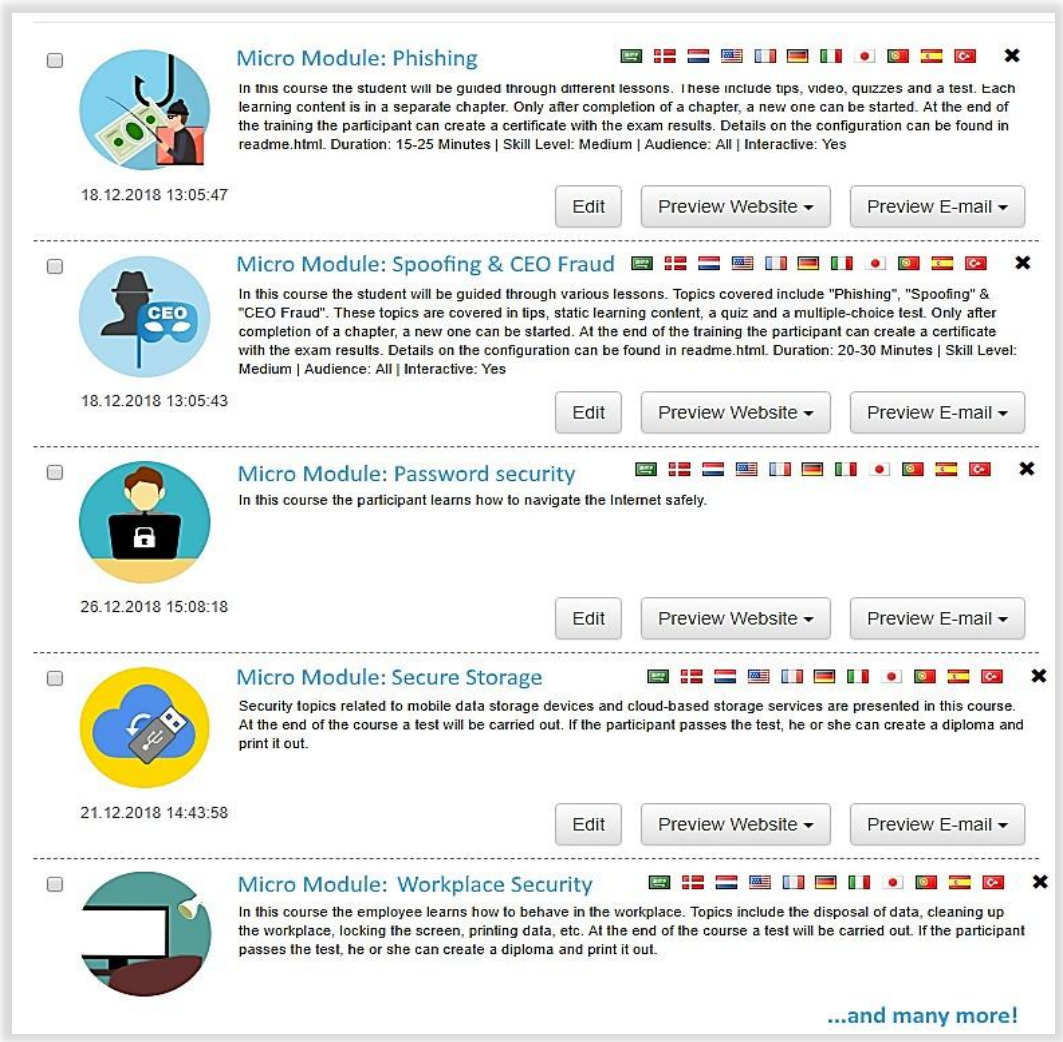


- **Çevrimdışı Eğitim Desteği:** LUCY farkındalık eğitimi için posterler, ekran koruyucular, el ilanları, vb. bir dizi düzenlenebilir şablon (Adobe Photoshop veya Illustrator dosyaları) ile donatılmıştır.

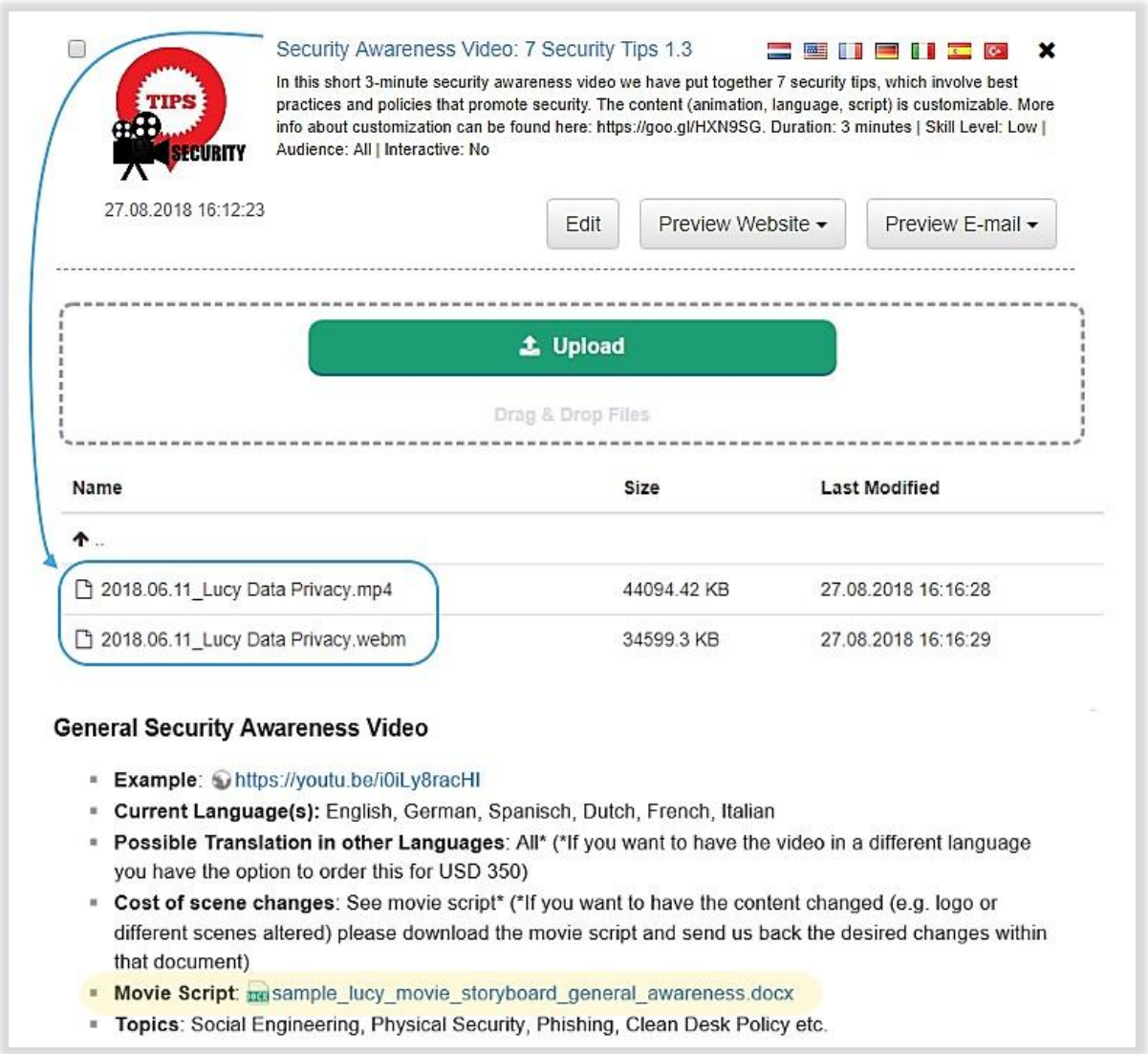


.

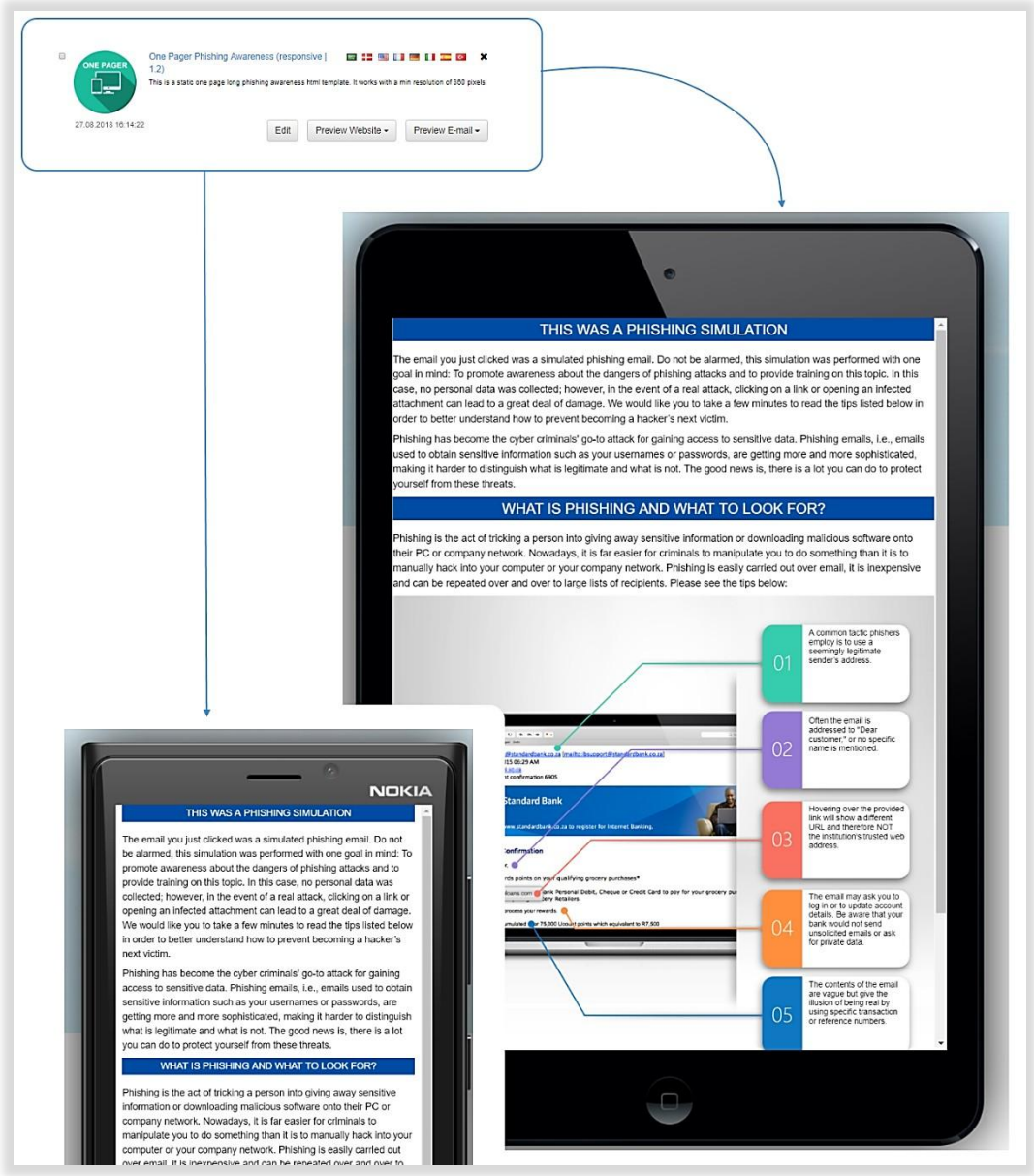
- **Mikro Öğrenme Modülleri:** Kurumunuzun marka ve politika ihtiyaçlarına göre değiştirilebilen mikro öğrenme eğitim modülleri (örneğin, 1 dakikalık videolar veya 1 sayfalık farkındalık yazıları) tasarlamış bulunuyoruz.



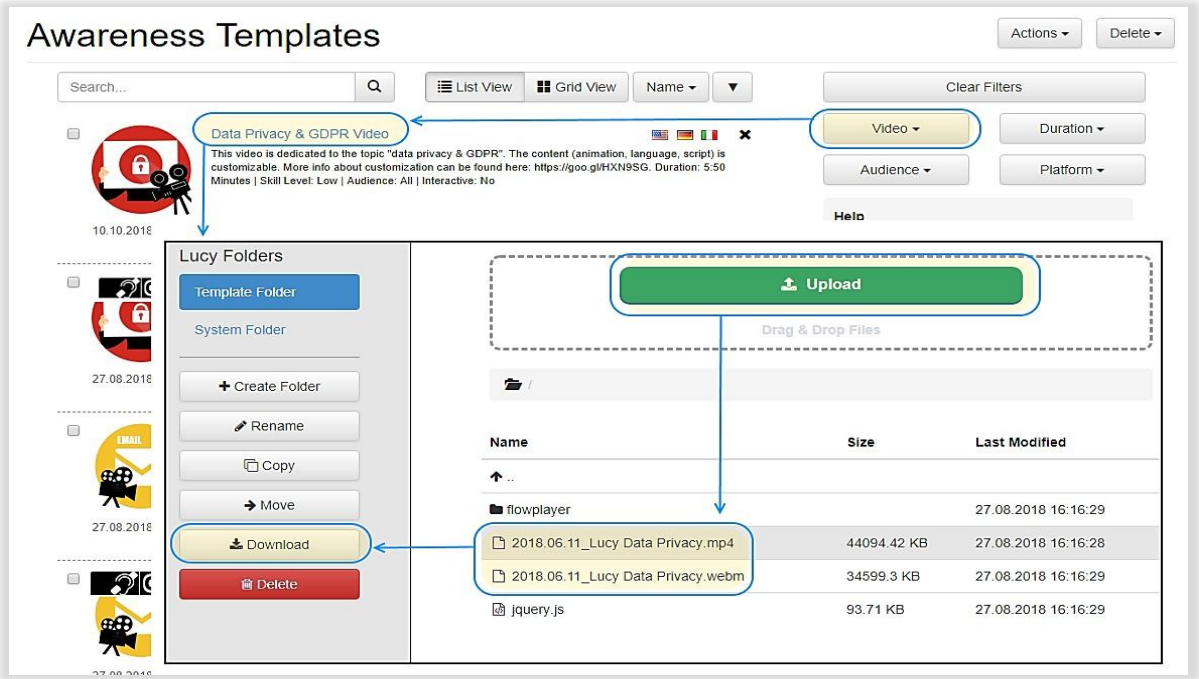
- **Video Kişiselleştirme:** Bize şirketinizin logosunu gönderin ve bizde onu eğitim videolarına dahil edelim. Başka bir dil mi istiyorsunuz? Hiç sorun değil. Videoyu tercih ettiğiniz dilde oynatacak şekilde ayarlayacağız. Farklı bir arka plan mı istiyorsunuz? Video metinlerini indirmeniz ve istediğiniz değişiklikleri işaretlemeniz yeterli.



- **Mobil Destekleyen Format:** LUCY'nin çoğu entegre modülü, kullanıcılara herhangi internete bağlı cihazdan eğitim alabilme esnekliğini sunan mobil destekleyen formatta mevcuttur.



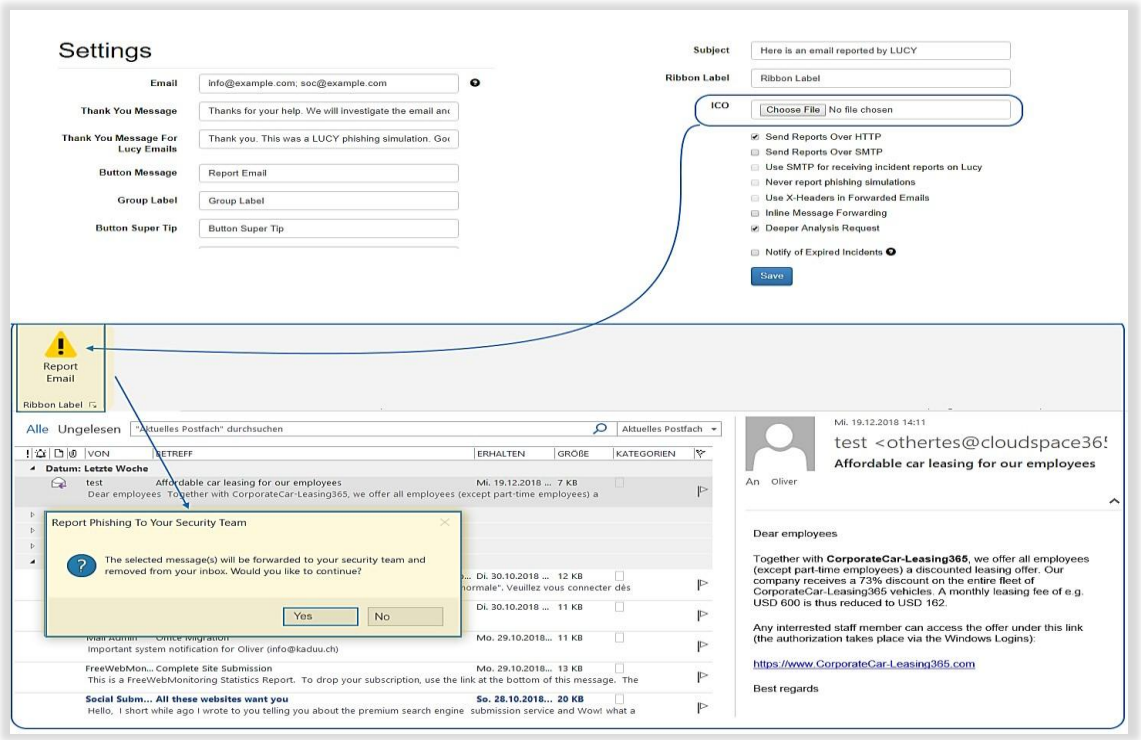
- **Video İçe / Dışa Aktarma:** LUCY videolarını kendi sisteminize dışa aktarmanın yanı sıra kendi videolarınızı da LUCY içine aktarabilirsiniz.



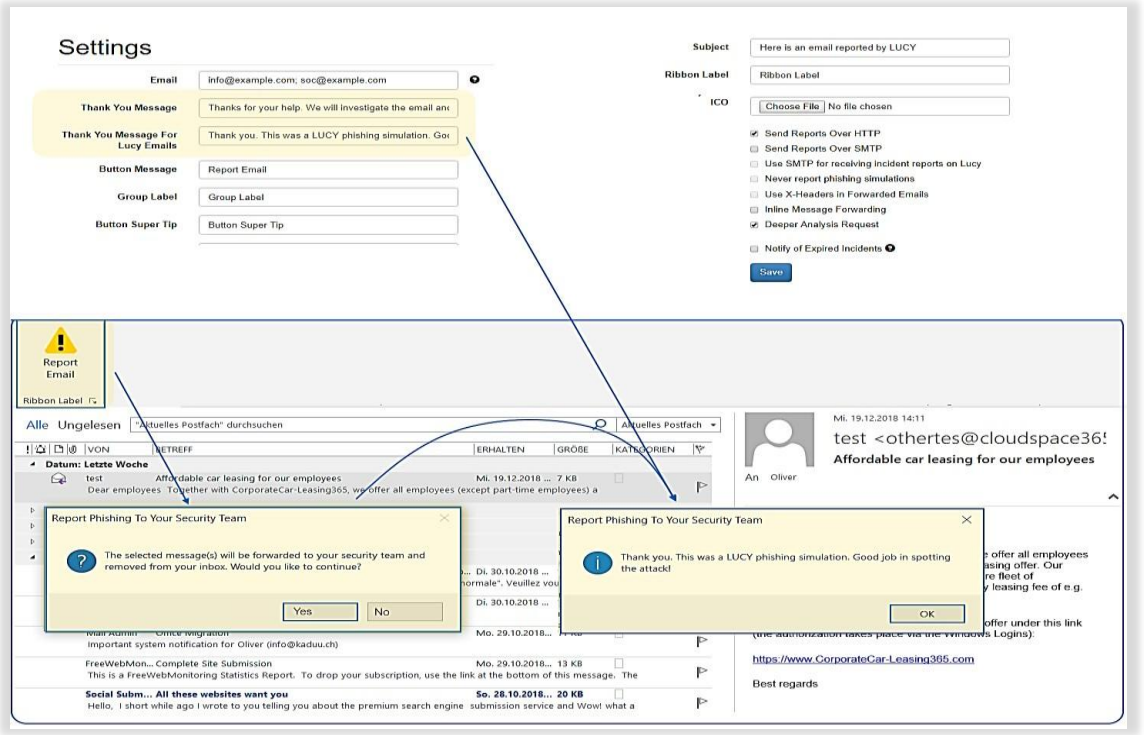
- **Dinamik Eğitim İpuçları:** Uygulanan dinamik ipuçları, yöneticinizin saldırı şablonları üzerinde işaretlemeler yaparak çalışanlarınızın e-öğrenme içerikleri içerisinde oltalama saldırısının nerede tespit edilebileceğini belirtmesine imkan tanır.

ÇALIŞANLARINIZIN KATILIMINI SAĞLAYIN

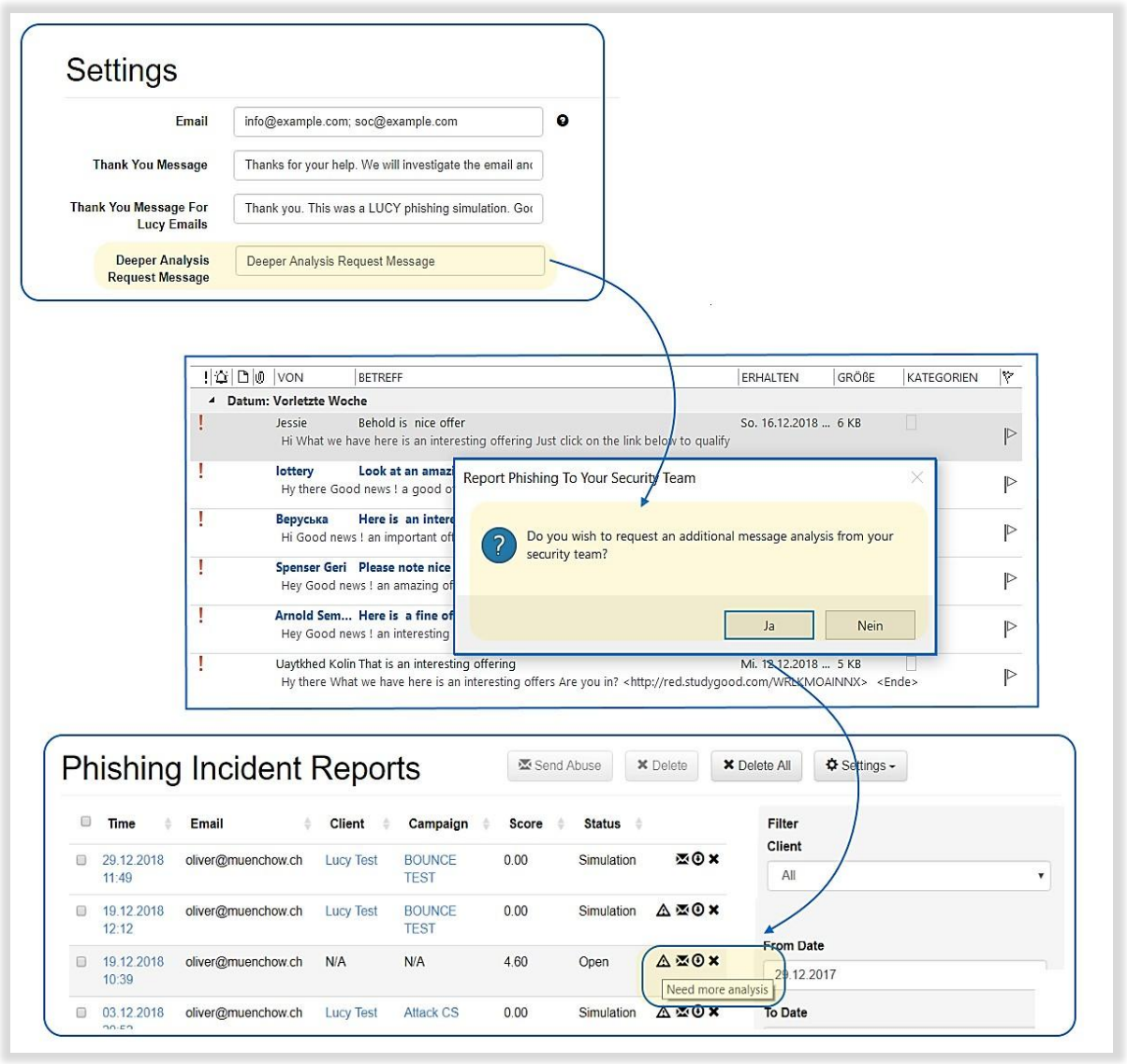
- **Tek tıkla E-posta rapor etme:** Kullanıcılar, şüpheli e-postaları tek tıkla bir ya da daha fazla e-posta hesabına rapor edebilir ve bunların LUCY olay analizi konsoluna yönlendirilmesini sağlayabilirler.



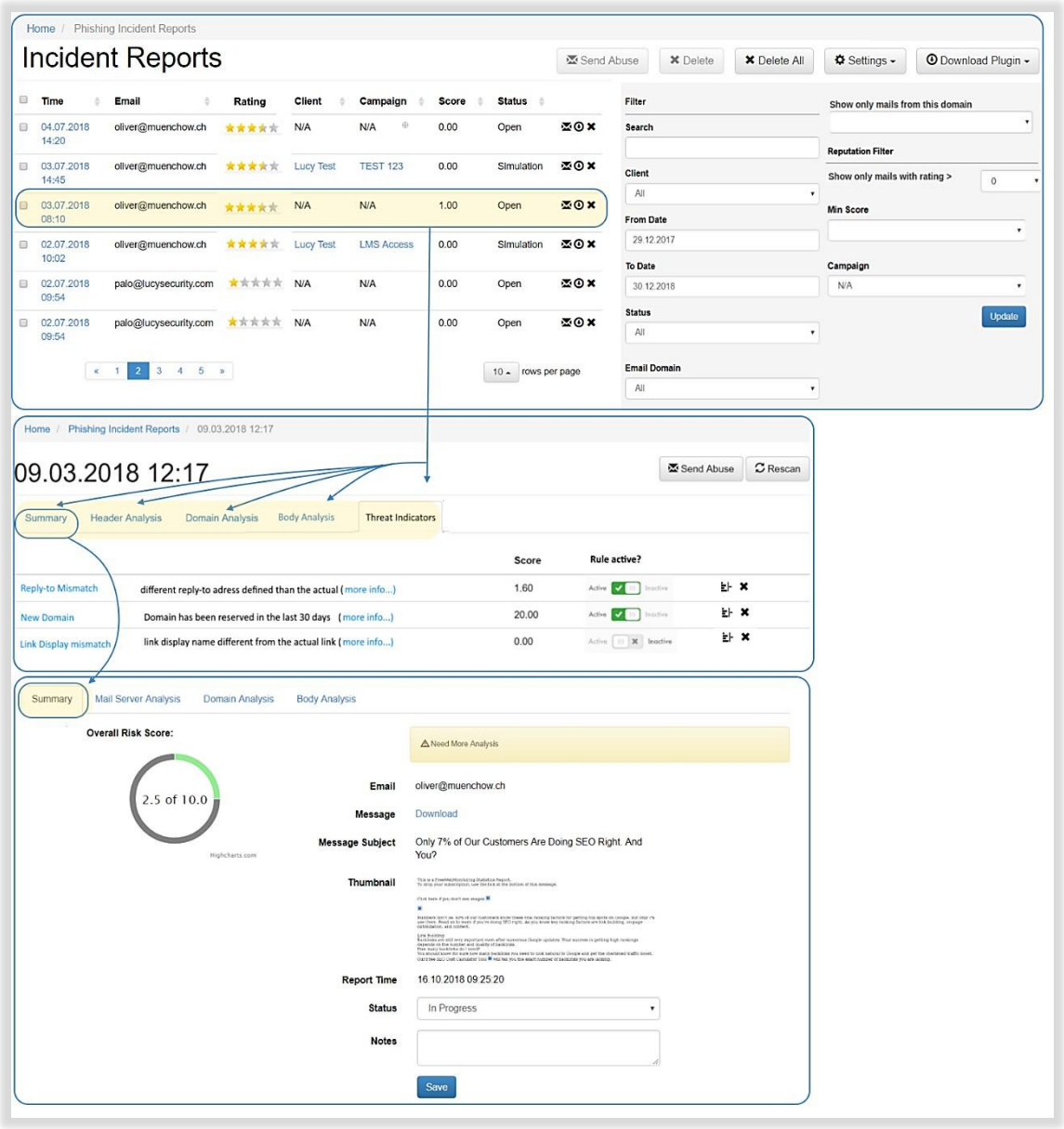
- **Olumlu Davranışın Pekiştirilmesi:** Eklentimiz, kurumunuz tarafından tanımlanmış kişiselleştirilmiş bir mesaj ile minnettarlık göstererek otomatik olarak olumlu davranışı pekiştirir.



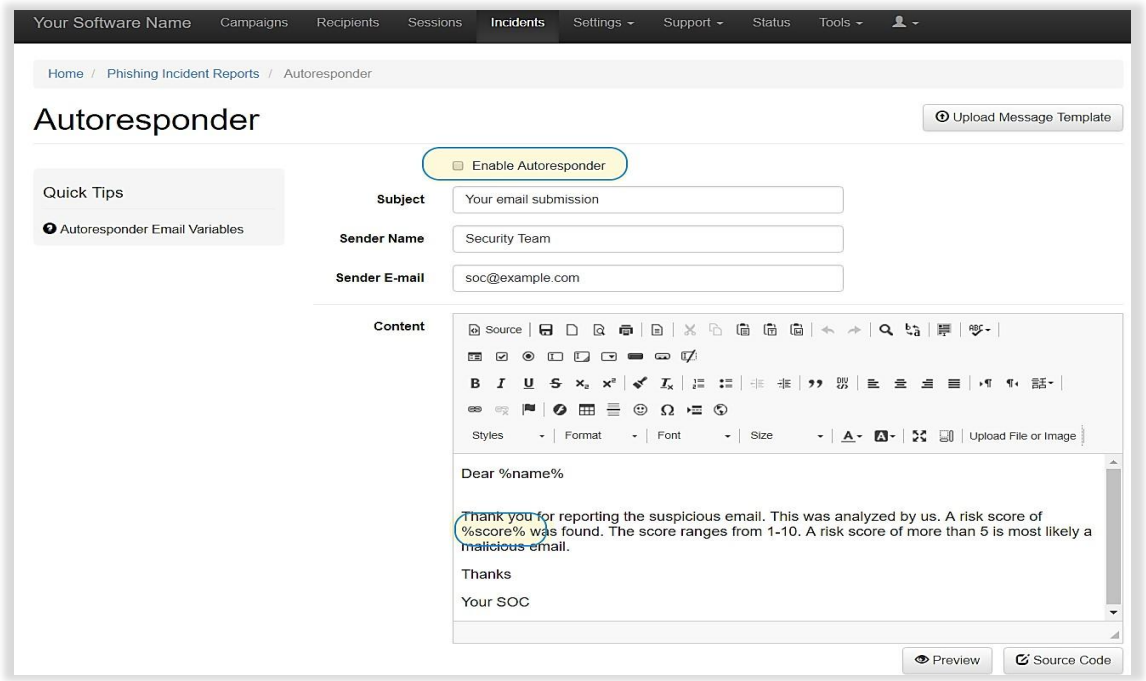
- **Derinlemesine teftiş talebi:** Kullanıcılar bazen aldıkları e-postanın güvenle açılıp açılamayacağını bilmek isterler. Kullanıcı opsiyonel olarak, güvenlik ekibine rapor edilen e-posta hakkında değerlendirme almak istediğini yerel eklenti içerisindeki "derinlemesine teftiş talebi" ögesini kullanabilir.



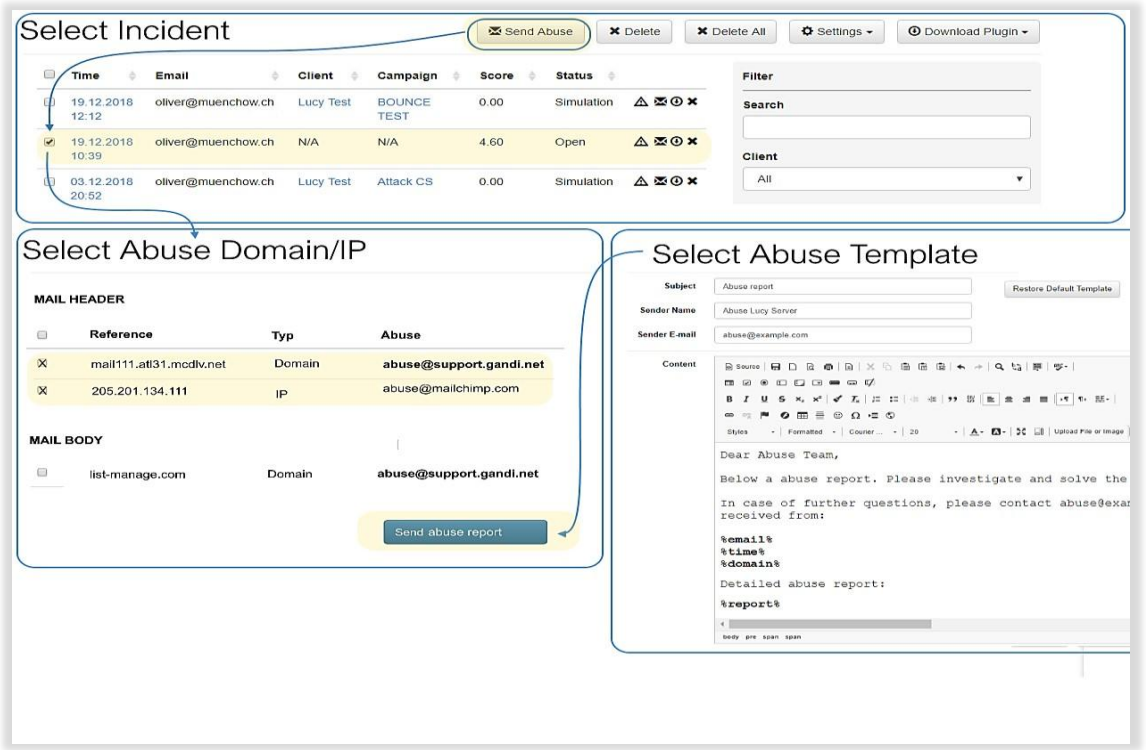
- **Otomatik Olay Analizi:** Merkezi yönetim konsolunu kullanarak rapor edilen şüpheli e-postaları yönetim ve bunlara yanıt verin: LUCY analizör işlevi, rapor edilen mesajların (üstveri ve gövde) otomatik teftişine imkan tanır. Analizöre, rapor edilen e-postaların gerçek zamanlı sıralamasını veren bir bağımsız risk puanı dahildir. Tehdit Analizörü, güvenlik ekibinin iş yükünü fark edilir şekilde azaltır.



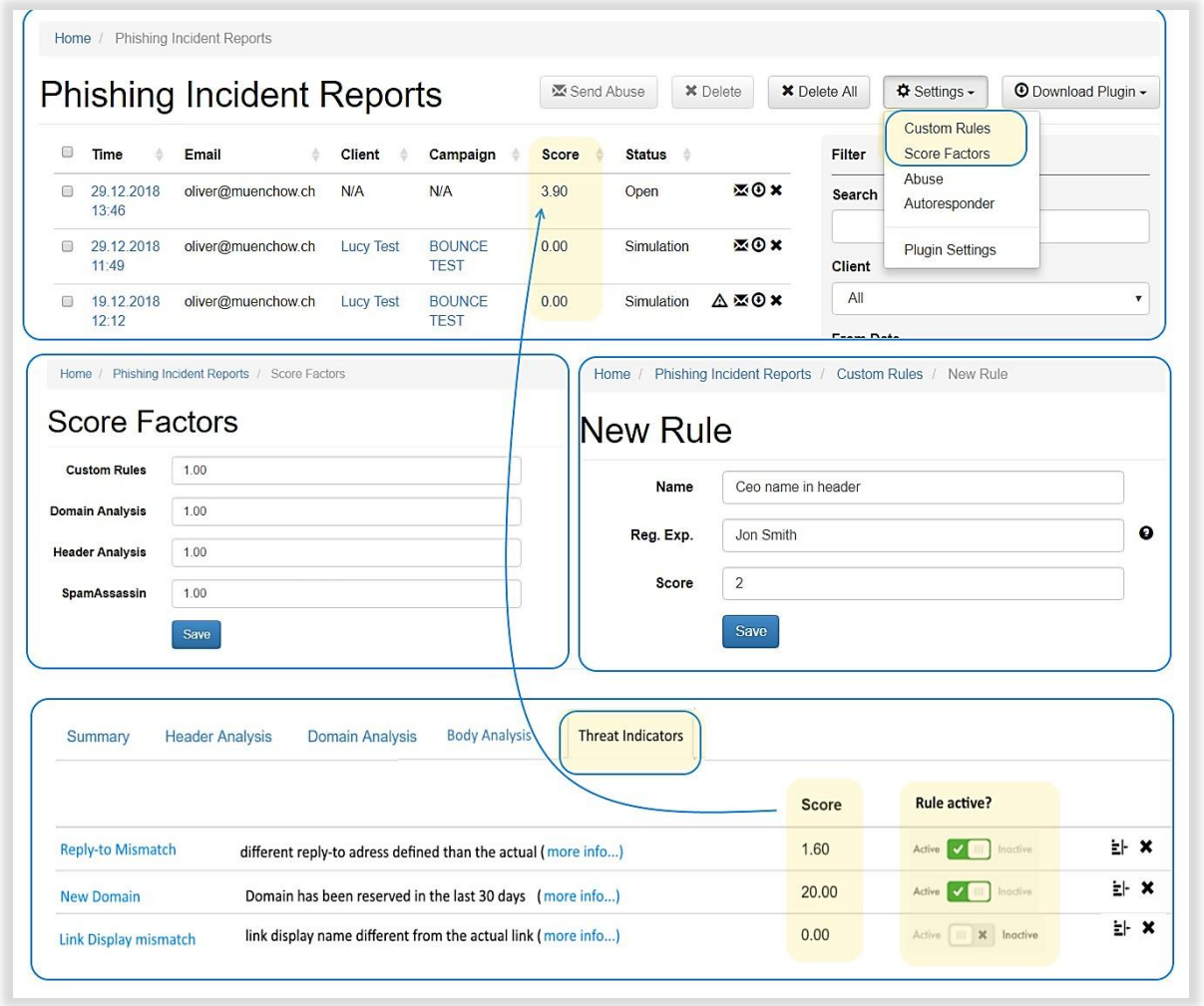
- **Olay Otomatik Geribildirimi:** Olay Otomatik Yanıtlayıcısı, e-posta tehdit analizinin sonuçlarını içeren bir otomatik bildirimin kullanıcıya gönderilmesini mümkün hale getirir. Mesaj metni istendiği gibi değiştirilebilir ve gerekmesi halinde LUCY E-posta Risk Puanı da buna dahil edilebilir.



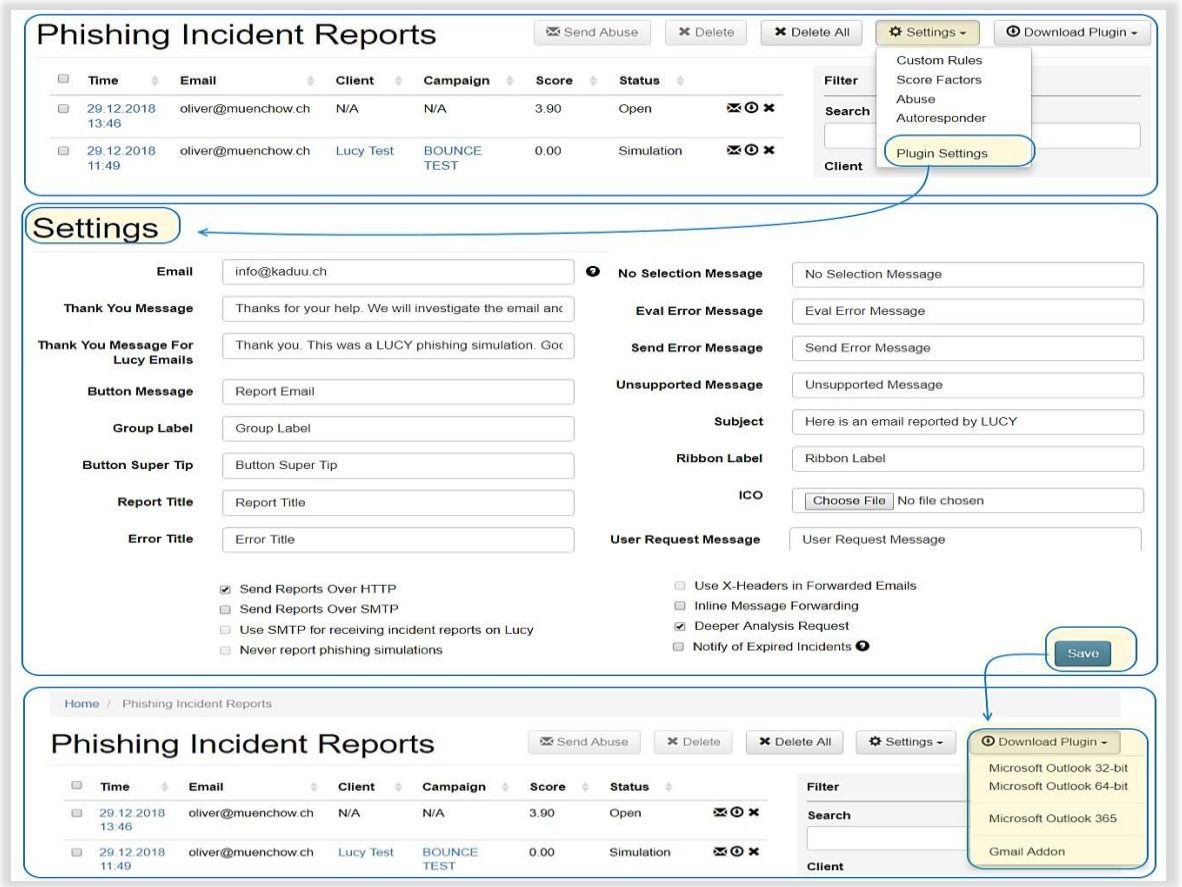
- **Tehdit Azaltma:** Davranışsal tehdit azaltma işlevi, e-postaya ilişkin riskleri ortadan kaldırmak için devrim niteliğinde bir yaklaşım getirmektedir. Saldırıyı durdurmakta güvenlik yöneticisine destek sağlayacaktır (saldırı ile ilgilenen belirli bir suistimal ekibine otomatik olarak rapor göndermek gibi).



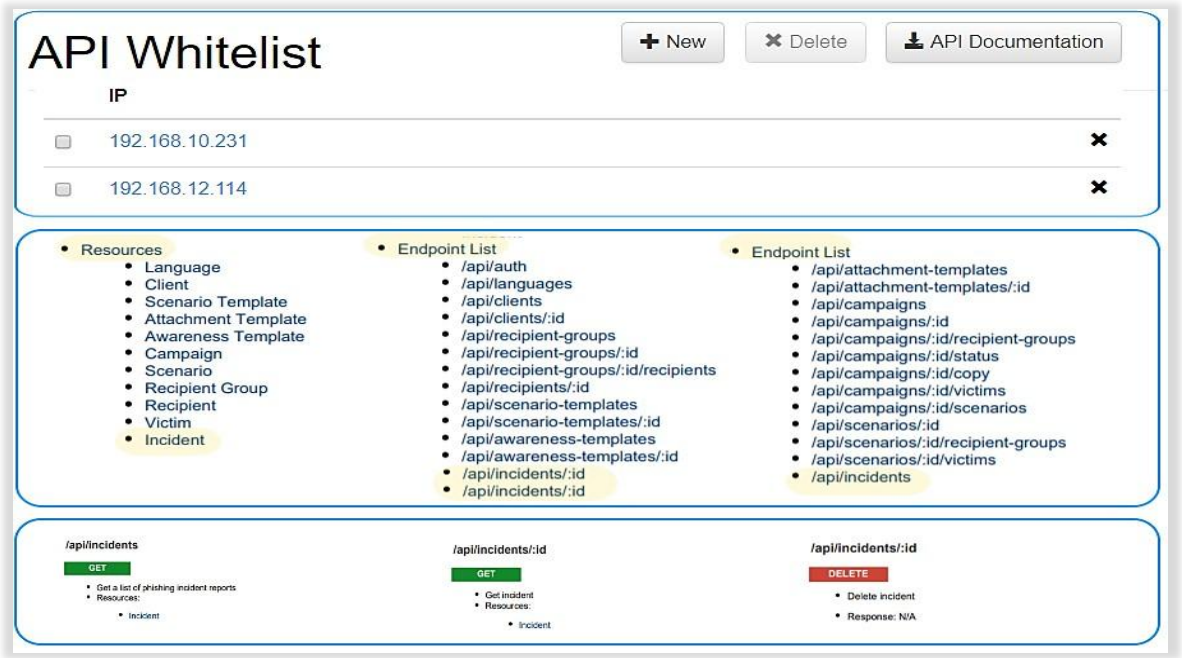
- **Özel kural bazlı analiz:** E-posta analizi ve risk hesaplamaları için kendi kurallarınızı tanımlayın.



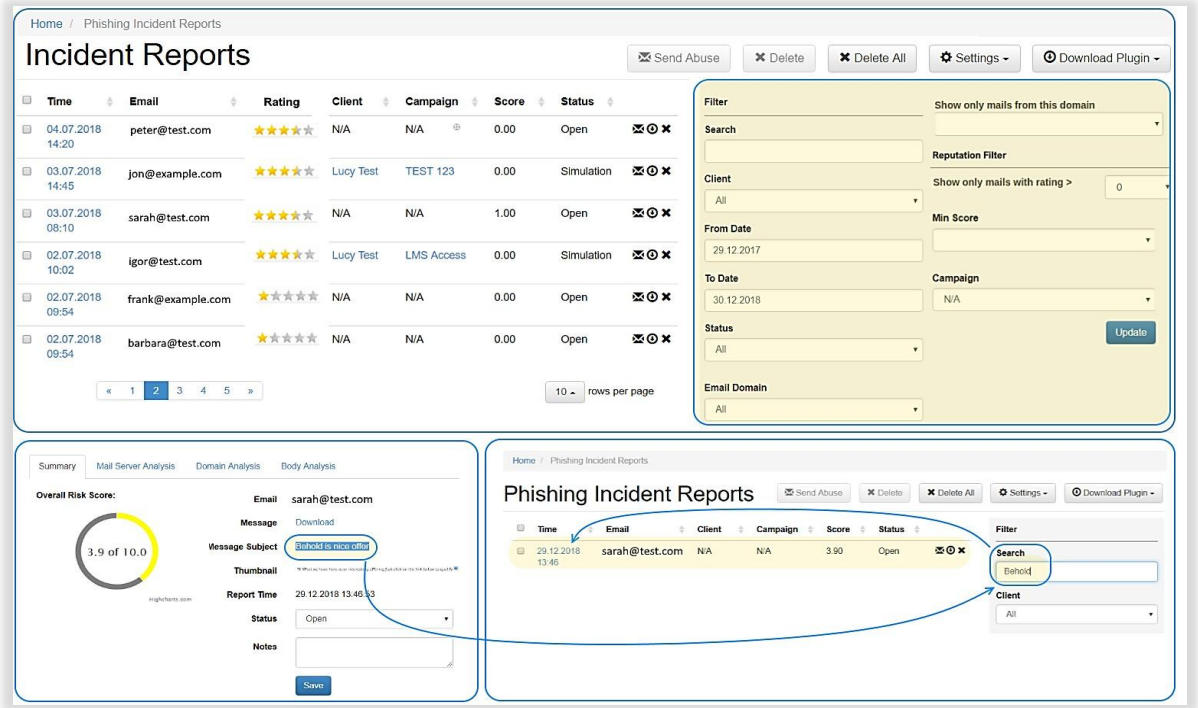
- **Eklenti kişiselleştirme seçenekleri:** LUCY, çeşitli eklenti işlevlerinin (görüntülenen simge, geribildirim mesajları, etiket, iletim protokolü, gönderilen üst veri, vb.) kolay kişiselleştirmesi ve tamamen boş etiketli olmasına izin verir.



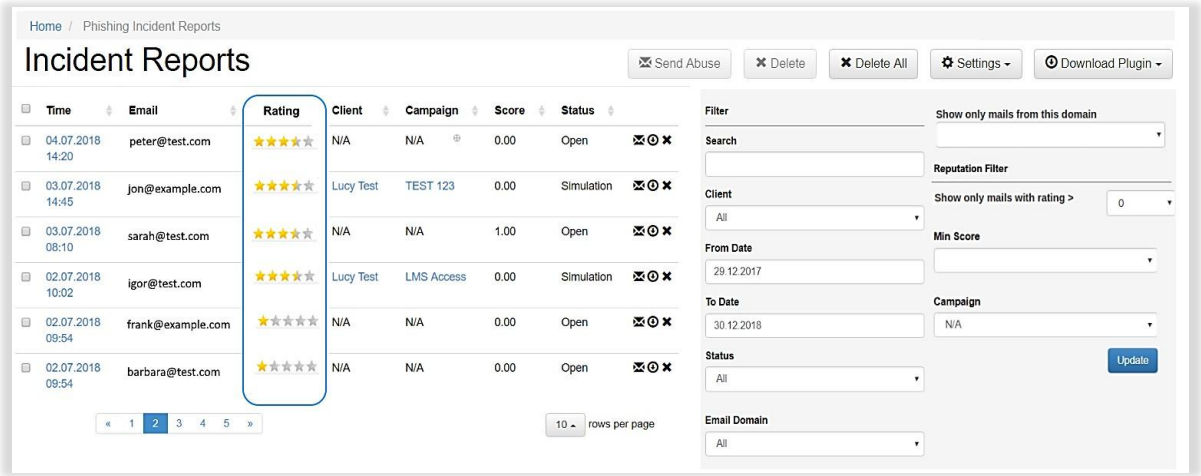
- **Üçüncü taraf entegrasyonu:** LUCY'nin olay REST API otomasyonunu kullanarak rapor edilen e-postaları işleme alabilir ve güvenlik ekibinize aktif oltalama saldırılarını daha gerçekleşirken durdurmakta yardımcı olabiliriz.



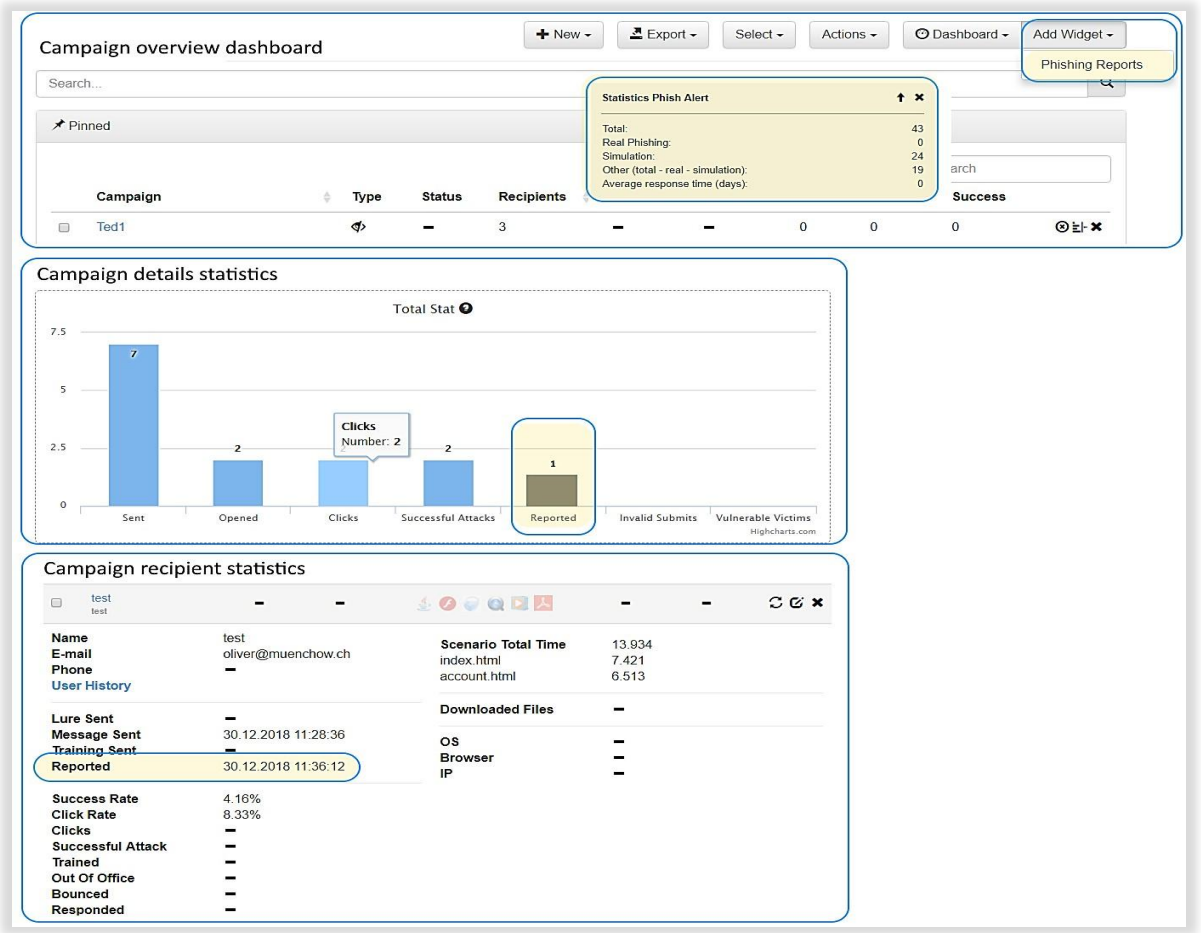
- **Ortak noktalara sahip saldırıları belirleme:** Kurumunuzda sıkça rastlanan saldırı vektörlerini saptamak için LUCY'nin kullanıcı paneli filtrelerini uygulayın. Benzer zayıf noktaların göstergelerini görmek için rapor edilen tüm e-postalar içerisinde arama yapın.



- **Olay kullanıcı itibar profilleri:** Kullanıcıları bir olay itibar skoru ile sınıflandırın..



- **Saldırı simülasyonları ile entegrasyon:** Oltalama simülasyonları ile kusursuz raporlama ve kullanıcı paneli entegrasyonu: bir oltalama simülasyonunda örnek davranış ortaya koyan kullanıcıları belirleyin.



- **Kolay Kurulum:** Outlook, Gmail, Office365 için Oltalama Olay Eklentisini kurun.