BAIT CYBER TECHNOLOGY

“Yapay Zeka Temelli Oltalama Simülasyonu”



BAIT CYBER TECHNOLOGY

❖ 14 Aralık 2024 – Kuruluş

2024 Aralık’ta kurulan BAITCyberTechnology; ismini, ‘yem’(bait) ve yapay zekânın (AI) birleşiminden almıştır.

❖ Teknopark Onayı

2025 şubat ayında Boğaziçi Ünv. Teknopark’a kabul edildik.

B.AI.T CYBER SECURITY

DÜNYADA VE TÜRKİYE'DE PHISHING SALDIRILARI

Microsoft Phishing Saldırısı (2021)

• Saldırganlar, Microsoft çalışanlarına **kurumsal destekten geliyor gibi görünen** e-postalar gönderdi. • E-postalardaki sahte **SharePoint** bağlantısına tıklayanlar, gerçek görünümlü bir giriş ekranına yönlendirildi. • Giriş yapanların kimlik bilgileri saldırganların eline geçti. **Bu hesaplar, başka kurumlara da phishing amaçlı e-posta göndermek için kullanıldı.**

Milford Entities Phishing Saldırısı

- Temmuz 2025'te, dolandırıcılar BPCA'dan geliyormuş gibi görünen **sahte e-postalar** ve **"spoofing"** yöntemiyle şirketi sahte bir banka hesabına ödeme yapmaya yönlendirdi.
- Toplamda **19 milyon dolar** dolandırıcılara aktarıldı.
- Olay, Milford Entities'in yönettiği **yüzlerce lüks konutun kira ve vergi ödemelerini etkiledi; şirketin itibarında ciddi zedelenme yarattı.**

HMRC Phishing Saldırısı (Mart–Haziran 2025)

- Birleşik Krallık vergi kurumu HMRC, tarihinde yaşanmış en büyük oltalama (phishing) saldırılarından birine uğradı.
- Siber saldırganlar, HMRC'nin online vergi sistemini kullanan bireysel vergi mükelleflerini klasik e-posta phishing yöntemiyle kimlik bilgilerini ele geçirdi.
- Yaklaşık 100.000 vatandaşın hesabı bu saldırıdan etkilendi.
- £47 milyon zarar oluştu.

Turkcell, Vakıf Katılım Phishing Saldırısı

- RedBeard grubu, **Turkcell ve Vakıf Katılım** çalışanlarına phishing e- postaları göndererek sahte Word dosyalarıyla sistemlere sızmaya çalıştı. Amaç finansal kazanç değil, **kritik bilgilerin çalınması ve uzun vadeli erişim sağlamaktı**. Resmî kayıp açıklanmadı; en büyük risk **veri sızıntısı operasyonel riskler, ve itibar kaybı** oldu.

B.AI.T CYBER SECURITY

DÜNYA GENELİ PHISHING ZARAR MALİYETİ

250 Milyar $

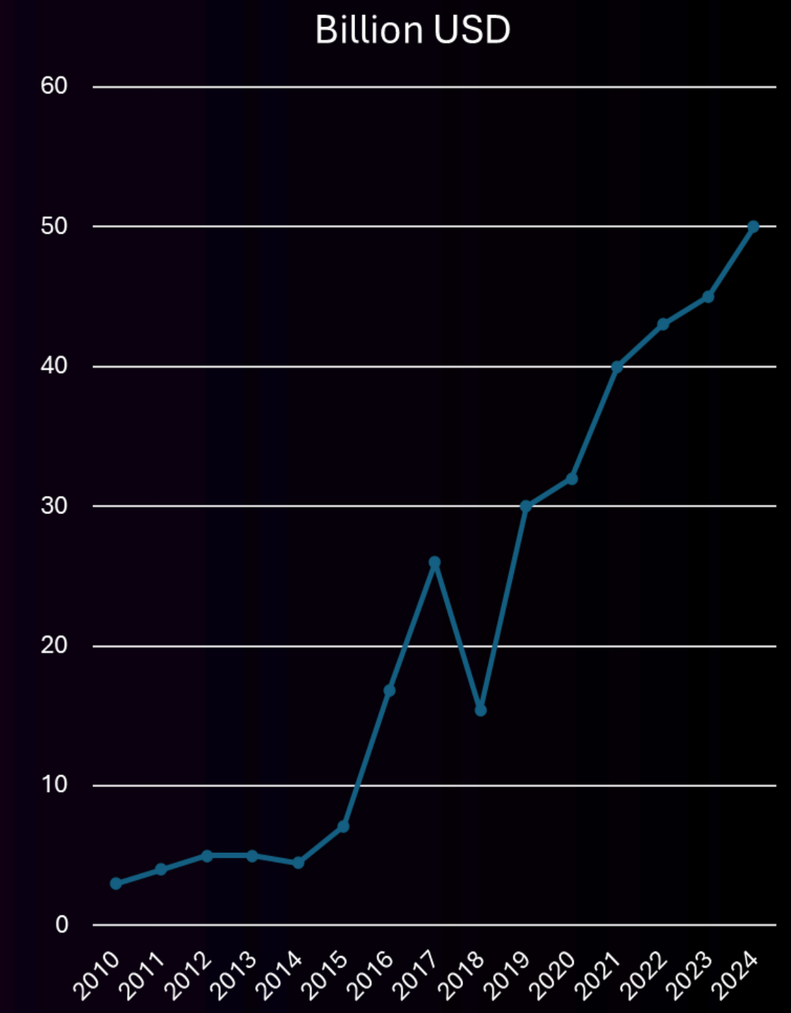
2024'te phishing saldırılarının küresel maliyeti.

%91

Başarılı siber saldırıların %91'i bir phishing e-postası ile başlamaktadır.

%36

Phishing saldırıları, siber güvenlik ihlallerinin yaklaşık %36'sını oluşturmaktadır.



Dünya genelinde şirketler, phishing saldırıları nedeniyle trilyonlarca dolarlık mali kayıp yaşamaktadır.

B.AI.T CYBER SECURITY

HAKKIMIZDA

Biz, dijital dünyada insanların bir tehdit değil, güvenliğin kalbi olabileceğine inanıyoruz.

BAIT, bu inançla doğdu. Siber saldırıların %90'ı insan hatasından kaynaklanıyor.

Biz bu istatistiği değiştirmek için varız.



B.AI.T
CYBER SECURITY

BAIT KULLANIRSANIZ...

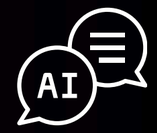
Maddi ve İtibari Kayıpları Önleme	Kurumsal Güvenlik Kültürü Oluşturma	Regülasyonlara Uyum	Farkındalık Artışı
Phishing saldırılarının ortalama zararı milyonlarca doları bulur. Simülasyonlar, veri kaybı, müşteri güveni ve marka itibarındaki riskleri önemli ölçüde azaltır.	Güvenlik, tüm çalışanların ortak sorumluluğudur. Düzenli simülasyonlarla farkındalık pekişir, tüm seviyelerde güvenlik bilinci yerleşir.	Phishing testleri uyumluluk için güçlü bir kanıttır. Denetimlerde avantaj sağlar.	Çalışanlar sahte e-postaları tanımayı öğrenir, gerçek saldırılara karşı hızlı tepki verme becerisi kazanır. “Eğitim yerine deneyim” yaklaşımı uygulanır.

B.AI.T CYBER SECURITY

ÜRÜN MODELLERİ

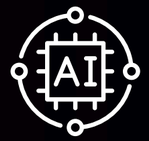
AI PHISING

En tehlikeli oltalama, kişiye özel ve ikna edici sahte iletilerle zafiyetleri suistimal eden sosyal mühendisliktir. Bait Cyber, yapay zekâ destekli simülasyon ürünüyle bu saldırı modelini test eder ve kurumlara güçlü çözümler sunar.



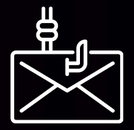
AI VISHING

Gerçekçi sesli arama simülasyonlarıyla çalışanların sosyal mühendislik zafiyetlerini test eder, kurumların savunma direncini güçlendiririz.



Campaing PHISING

Güvenilir görünen sahte e-postalar aracılığıyla kurumları hedef alır ve bilgi güvenliğini tehlikeye atmayı hedefler.



ÜRÜN MODELLERİ

AWARENESS EĞİTİM

Kullanıcının kişisel güvenlik skoru ve tespit edilen zaafiyetlerine göre, ihtiyaca özel siber güvenlik eğitimleri gerçekleştirilir.



BAIT GAME

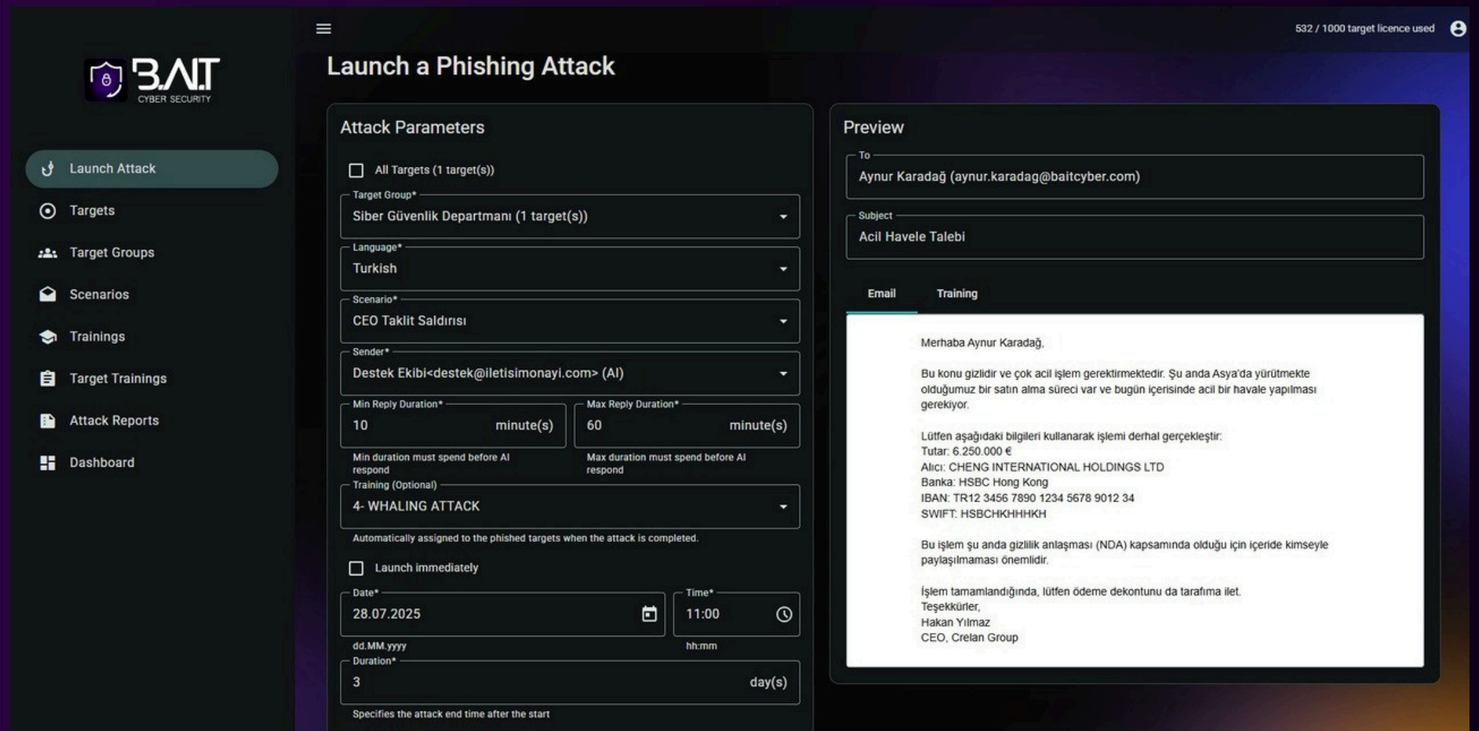
Kullanıcıları gerçek hayata yakın senaryolar içinde karar almaya yönlendiren oyunlaştırılmış bir eğitimdir. Sınav yaklaşımı yerine, davranış ve refleksleri ölçerek zafiyet seviyesini ortaya koyar.



YÖNETİM PANELİ

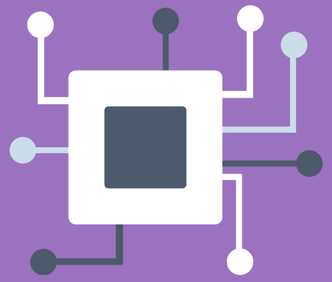
Departman bazında gelişimi izleyin, KPI’lara dayalı kararlar alın.





B.AI.T CYBER SECURITY

SOSYAL MÜHENDİSLİKLE GERÇEKÇİ SİMÜLASYONLAR



Geleneksel Testler

- ✕ Statik ve öngörülebilir içerik
- ✕ Tek seferlik iletişim
- ✕ Gerçeklikten uzak senaryolar



BAIT Simülasyonları

- ✓ Dinamik ve gerçekçi içerik
- ✓ Çok adımlı ikna süreci
- ✓ Yapay zeka tabanlı etkileşim

B.AI.T CYBER SECURITY

AI PHISHING

Merhaba Aynur Karadağ,

Şu anda Asya’da yürütmekte olduğumuz bir satın alma süreci var ve bugün içerisinde acil bir havale yapılması gerekiyor. Lütfen aşağıdaki bilgileri kullanarak işlemi derhal gerçekleştir:
Tutar: 6.250.000 €
Alıcı: CHENG INTERNATIONAL HOLDINGS
Banka: HSBC Hong Kong IBAN: TR12 3456 7890 1234 5678 9012 SWIFT: HSBCHKHHHKH
Bu işlem şu anda gizlilik anlaşması (NDA) kapsamında olduğu için içeride kimseyle paylaşılmaması önemlidir. İşlem tamamlandığında, lütfen ödeme dekontunu da tarafıma ilet. Teşekkürler,
Hakan Yılmaz
CEO, Crelan Group



Merhaba Hakan Bey,

Belirttiğiniz havale işlemiyle ilgili hazırlıkları yaptım. Ancak işlem tutarının büyüklüğü ve alıcının daha önceki işlemlerimiz arasında yer almaması nedeniyle, ilgili departman prosedürlerini gözden geçirerek ilerlemem gerekiyor.

Söz konusu transferin detaylarını içeren bir onay belgesi ya da önceki yazışmalara ait doküman varsa paylaşmanız mümkün müdür?

İşlemi tamamlamak için teyidinizi bekliyorum.

Saygılarımla,
Aynur Karadağ
Finans Uzmanı

Merhaba Aynur Hanım,

Hızlı dönüşünüz için teşekkür ederim. Anlayışınız için minnettarım. Bu işlem gerçekten önemli ve zamanında tamamlanması gerekiyor. Gizlilik anlaşması (NDA) kapsamında olduğumuz için, bu konuyla ilgili daha önceki yazışmaların paylaşılması mümkün değil. Ancak, bu işlemin şirketin stratejik bir kararı olduğunu ve üst yönetim tarafından onaylandığını belirtmek isterim

Herhangi bir başka belgeye erişimimiz olmamakla birlikte, işlemi hızlandırmak adına elimizden geleni yapıyoruz. Sizin bu süreci hızlandırmanız büyük önem taşıyor. Eğer başka bir sorunuz veya endişeniz varsa, lütfen bana bildirin.

Teşekkürler,iyi çalışmalar,

Hakan Yılmaz

B.AI.T CYBER SECURITY

STRATEJİK İŞ ORTAKLIKLARI

vodafone

TRAI

TÜRKİYE SİBER GÜVENLİK KÜMELENMESİ

BOĞAZİÇİ ÜNİVERSİTESİ TEKNOPARK

B.A.I.T CYBER SECURITY

TEŞEKKÜRLER



B.AI.T
CYBER SECURITY