

**Finans Dünyasında Görünmez  
Güç: Siber Güvenliğin Geleceğe  
Yön Veren Stratejileri**

Payten Siber Güvenlik Yöneticisi  
İsmail Orhan, CISSO, CTFI, CCII

# Giriş ve Kişisel Tanıtım

İsmail Orhan, CISO, CTFI, CCII

- Payten'de Siber Güvenlik Müdürü.
- 12 yılı aşkın siber güvenlik deneyimi.
- Güvenlik Operasyonları, Tehdit Avcılığı, Red Team Operasyonları, Adli Bilişim, Tehdit İstihbaratı ve Güvenlik Eğitimleri konularında tecrübe.
- Amerikan Silahlı Kuvvetleri – Cyber Command ve Türk Savunma Sanayi Tecrübeleri,
- CISSO, CSLO, CTFI, CCII sertifikalarına sahip, Mile2 resmi gözetmeni.



## 2. Dijital Dönüşüm ve Finans Sektörüne Etkisi

## 2. Dijital Dönüşüm ve Finans Sektörüne Etkisi

- "Dijital dönüşüm, finans sektörünü köklü bir şekilde yeniden şekillendiriyor ve yeni teknolojiler, hizmetleri ve iş modellerini dönüştürüyor."
- "Veri odaklı çözümler ve yapay zeka, finansal karar alma süreçlerinde hız ve doğruluğu artırarak sektördeki rekabeti yeniden tanımlıyor."
- "Finans kuruluşlarının dijital dönüşüme uyum sağlaması, müşteri beklentilerini karşılamak ve operasyonel verimliliği artırmak için kritik hale geldi."
- "Siber güvenlik, dijitalleşen finans dünyasında en kritik unsurlardan biri haline geldi; dijital çözümler gelişirken güvenlik riskleri de artıyor."
- "Dijital dönüşümle birlikte, finans sektörü artık sadece bankacılık hizmetlerinden ibaret değil; fintech çözümleri sektörü çok daha dinamik ve erişilebilir hale getiriyor."

### 3. Finans Dünyasında Siber Güvenliğin Stratejik Önemi

### 3. Finans Dünyasında Siber Güvenliğin Stratejik Önemi



Dijitalleşmenin  
Güvenlik Riskleri

%70 dijitalleşme oranı (her yıl %10 artış) Genişleyen saldırı yüzeyi Yıllık 3.86 milyon \$ zarar



Regülasyonlara  
Uyum

%85 uyum zorlukları GDPR, PCI DSS kritik 1.2 milyar \$ GDPR cezası (2022)



Müşteri Verilerinin  
Korunması

1 milyar müşteri kaydı sızdı (2023) Güvenlik = müşteri güveni 4.24 milyon \$ ihlal maliyeti



Siber Tehditlerin  
Artışı

Finans %30 siber saldırı hedefi (2023) Fidyeye yazılım %150 artış 1.7 milyon yeni tehdit/gün



Risk Yönetimi ve  
Strateji

%70 strateji eksikliği Proaktif yönetim = erken tespit %20 operasyonel maliyet tasarrufu

## 4. Kuantum Teknolojileri ve Finans Sektörü

## 4. Kuantum Teknolojileri ve Finans Sektörü



Kuantum Şifreleme  
ve Güvenlik

Kırılması imkansız şifreleme (QKD) Mevcut şifreleme sistemlerine tehdit , Kuantum şifreleme ile güvenlik artışı



Kuantum Dirençli  
Algoritmalar

RSA, ECC tehdit altında, NIST, kuantum dirençli algoritma yarışması, Kuantum sonrası güvenlik için hazırlık



Finansal Sistemlerde  
Kuantum  
Uygulamaları

Süper hızlı veri analizi, Portföy optimizasyonu, Daha verimli ticaret stratejileri



Kuantum  
Hesaplama ile Risk  
Yönetimi

Hızlı senaryo analizi  
Daha iyi risk tahmini  
Derin veri analizi ile stratejik kararlar



Kuantum Çağına  
Hazırlık

Kuantum yatırımları artıyor, Kuantum eğitimi ve farkındalık Erken adaptasyon rekabet avantajı



## 5. Yapay Zeka ve Otomasyonun Güvenlikteki Rolü

# 5. Yapay Zeka ve Otomasyonun Güvenlikteki Rolü



Tehdit Algılamada  
Yapay Zeka

Anomali tespiti,  
Makine öğrenimi  
ile tehdit öngörüsü,  
Gerçek zamanlı  
izleme



Olay Müdahale  
Süreçlerinde  
Otomasyon

Hızlı tepki süreleri  
SOAR çözümleri  
(Security  
Orchestration)  
Olay yönetiminde  
otomasyon



Yapay Zeka ile  
Proaktif Güvenlik

Saldırı tahmini  
Savunma  
otomasyonu, AI  
tabanlı erken uyarı  
sistemleri



Siber Tehdit  
İstihbaratında AI  
Tabanlı Çözümler

Tehdit verilerini analiz  
etme AI destekli  
tehdit avı, Küresel  
tehdit istihbaratı  
paylaşımı



Otomatikleştirilmiş  
Güvenlik  
Denetimleri

Sürekli uyumluluk  
kontrolü, Otomatik  
zafiyet tarama, Risk  
azaltma süreçlerinde  
otomasyon

## 6. Global Siber Güvenlik Trendleri

## 6. Global Siber Güvenlik Trendleri



Zero Trust Güvenlik Yaklaşımı

Kimseye güvenme, her işlemi doğru, Finansal veri erişim kontrolleri, ihlal önleme ve iç tehditlerin azaltılması



Siber İstihbaratın Önemi

Finansal tehdit tespiti, Proaktif risk yönetimi, Tehdit avcılığı ile erken uyarı



Bulut Güvenliğinin Evrimi

Hibrit bulut çözümleri, Finans sektöründe veri güvenliği endişeleri, Bulut yerel güvenlik araçları (CSPM, CWPP)



Sıfır Gün Açıkları

Finansal sistemlerde kritik riskler, Anında yama yönetimi zorunluluğu, İstismar edilen açıklarla büyük kayıplar



Siber Dayanıklılık Stratejileri

İş sürekliliği planları, Finans kuruluşlarında kriz yönetimi, Hızlı iyileşme ve tehdit adaptasyonu

## 7. Kapanış ve Gelecek Öngöröleri

## 7. Kapanış ve Gelecek Öngöruları



Kuantum  
Teknolojilerinin  
Yükselişi

Kuantum güvenlik  
çözümleri,  
Kuantum sonrası  
şifreleme, Finans  
dünyasında  
kuantum  
hazırlıkları



Yapay Zekanın  
Gelecekteki Rolü

Otonom tehdit  
tespiti, AI ile  
sürekli iyileşen  
savunmalar,  
Akıllı güvenlik  
sistemleri



Siber Güvenlikte  
Dayanıklılık  
Stratejileri

Kriz yönetimi ve hızlı  
iyileşme, Finans  
sektöründe  
dayanıklılık altyapısı,  
Sürekli adaptasyon  
ve risk azaltma



Global Güvenlik  
İşbirlikleri

Uluslararası tehdit  
paylaşımı, Finansal  
kurumlar arası  
işbirliği, Ortak siber  
güvenlik standartları



Yeni Nesil Siber  
Güvenlik Çözümleri

Yapay zeka destekli  
güvenlik, Bulut ve  
hibrit çözümler,  
Otonom güvenlik  
yazılımları

**Ortalama maliyet**  
5.72 milyon USD



**Fidye yazılım artışı: %74 arttı**



**Veri ihlali oranı:**  
%61

**Saldırı hedefi**

%17



**Siber sigorta: %84**

**Tespit süresi: 207 gün ortalama**



**Hizmet kesintisi: %45'te 4 saat**



**Fidye ödeme oranı: %33'ü ödeme yaptı**

**İç tehdit oranı: %35 iç tehdit**

## Ödüllerimiz





# Kaynaklar ve Öneriler



Gizli Siber Cephe - Kitap



Kuantum Çizgisinin Ötesinde - Kitap



MasterCard - Blog



Gartner



McKinsey & Company



National Institute of Standards and Technology (NIST)



ENISA (European Union Agency for Cybersecurity)



IBM Security



World Economic Forum (WEF) - "The Global Risks Report 2024"

Teşekkürler

# Yasal Sorumluluk

Bu sunumda sunulan içerik telif hakkı korumasına tabidir. Metinler, grafikler, fotoğraflar, sesler, animasyonlar ve videolar ile bunların sunumda dağıtımı, Telif Hakları ve ilgili haklar Kanunu kapsamında korunmaktadır. Bu belgede yer alan herhangi bir materyalin izinsiz kullanımı, telif hakkı, ticari marka veya diğer yasaların ihlali anlamına gelebilir. Bu sunumdaki materyaller, Payten yazılı olarak onay vermediği sürece, kamuya açıklanamaz, kamuya açıklanamaz, icra edilemez, dağıtılamaz veya başka herhangi bir kamusal veya ticari amaçla kullanılamaz. Bu sunumun içeriğinin üçüncü şahıslar tarafından ticari kullanımı, dağıtımı, değiştirilmesi veya içeriğinin alınması dahil olmak üzere herhangi bir amaç için kopyalanması yasaktır. Ayrıca, bu sunum üçüncü taraflara sunulan tekliflere ve hizmetlere referans içerebilir. Bu teklifler ve hizmetler için kullanım şartları bu kuruluşlar tarafından tanımlanır.

Payten, bu kuruluşların teklif ve hizmetlerinin kullanım koşullarına, içeriklerine ve etkilerine ilişkin hiçbir sorumluluk kabul etmez. Bu sunumda yer alan bilgi ve bilgiler sadece bilgi amaçlıdır. Sunum Inscale şirket ürünlerinin kullanımı ile hazırlanmıştır. Payten'in adı ve logosu tescilli ticari markalardır. Bu işaretlerin kullanılması, Payten'in önceden açık bir şekilde anlaşılmasını gerektirir.