CATCHPROBE™

İstihbaratın Peşinde Güç Kazanmak

OTD BİLİŞİM
GLOBAL VAD

CATCHPROBE™

CatchProbe, beş yapay zekâ destekli modülü bir araya getiren, hepsi bir arada bir siber istihbarat platformudur. Bu yapı sayesinde kapsamlı ve entegre bir siber güvenlik çözümü sunar.

Platformumuz; web istihbaratı, tehdit tespiti, aldatma teknolojisi (deception technology) ve saldırı yüzeyi yönetimi (attack surface management) modüllerini hem birbirleriyle hem de müşterilerin mevcut güvenlik altyapılarıyla kusursuz biçimde entegre eder. Böylece güvenlik görünürlüğünü artırır ve eyleme dönüştürülebilir istihbarat sağlar.

OTD BİLİŞİM
GLOBAL VAD

NEDEN SİBER İSTİHBARAT

Problem

İstatistiklere göre, siber suçların küresel ekonomiye maliyeti 2026 yılına kadar 20 trilyon ABD dolarını aşacak. Bu, 2022 verilerine kıyasla 1,5 katlık bir artış anlamına geliyor (Kaynak: Statista). Geleneksel siber güvenlik önlemleri çoğunlukla tehditlere tepki verir, onları önlemek yerine saldırı gerçekleştikten sonra müdahale eder. Bu da kurumları savunmasız bırakır. Gelişen tehditlerin önünde kalabilmek için kurumların, saldırıları gerçekleşmeden önce tahmin edip etkisiz hâle getirmelerini sağlayacak gelişmiş tehdit istihbaratına ihtiyaçları vardır.

Çözüm

CatchProbe'u, ulusal güvenlik kurumlarının stratejik ihtiyaçlarıyla ve özel sektörün operasyonel gereksinimleriyle uyumlu olacak şekilde geliştirdik. Her biri belirli bir uzmanlık alanına sahip olan modüller, birbirlerinin kabiliyetlerini güçlendirerek çalışır. CatchProbe, işletmelere kapsamlı istihbarat toplama ve önleyici savunma stratejileri sunarak tehditlere karşı daima bir adım önde olmalarını sağlar.

NEDEN CATCHPROBE

Birleşik Siber İstihbarat:

Aldatma teknolojisi, karanlık web istihbaratı ve saldırı yüzeyi yönetimini yapay zekâ destekli tek bir platformda bir araya getirir.

Reaktif Güvenliğe Karşı Proaktif Güvenlik:

Tehditleri olay hâline gelmeden önce durdurarak ihlal müdahale süresini %80'in üzerinde azaltır.

Kesintisiz Ekosistem Entegrasyonu:

Güvenlik duvarları (firewall), SIEM ve SOAR platformlarıyla entegre çalışarak tehdit azaltma süreçlerini otomatikleştirir.

Kanıtlanmış Etki:

Devlet kurumları, özel sektör kuruluşları ve finansal kurumlar tarafından güvenle kullanılmaktadır.

Geleceğe Hazır Altyapı:

CatchProbe modülleri birlikte çalışarak gerçek zamanlı istihbarat paylaşımı, otomatik çözümleme (remediation) ve güvenlik ekosistemleriyle API üzerinden kesintisiz entegrasyon sağlar.

CATCHPROBE™

CATCHPROBE | HEPSİ BİR ARADA DİJİTAL İSTİHBARAT PAKETİ

DARKMAP

Web İstihbaratı (WEBINT), Marka Koruma

LEAKMAP

Açık Kaynak İstihbaratı (OSINT), İlişkilendirilmiş Veri Sızıntıları

SMARTDECEPTIVE

Sahte Sistem (Honeypot) Yönetimi

THREATWAY

Tehdit İstihbaratı Paylaşım Merkezi

RISKROUTE

Dış Saldırı Yüzeyi Yönetimi

VENSPECT

Tedarikçi Risk Değerlendirmesi

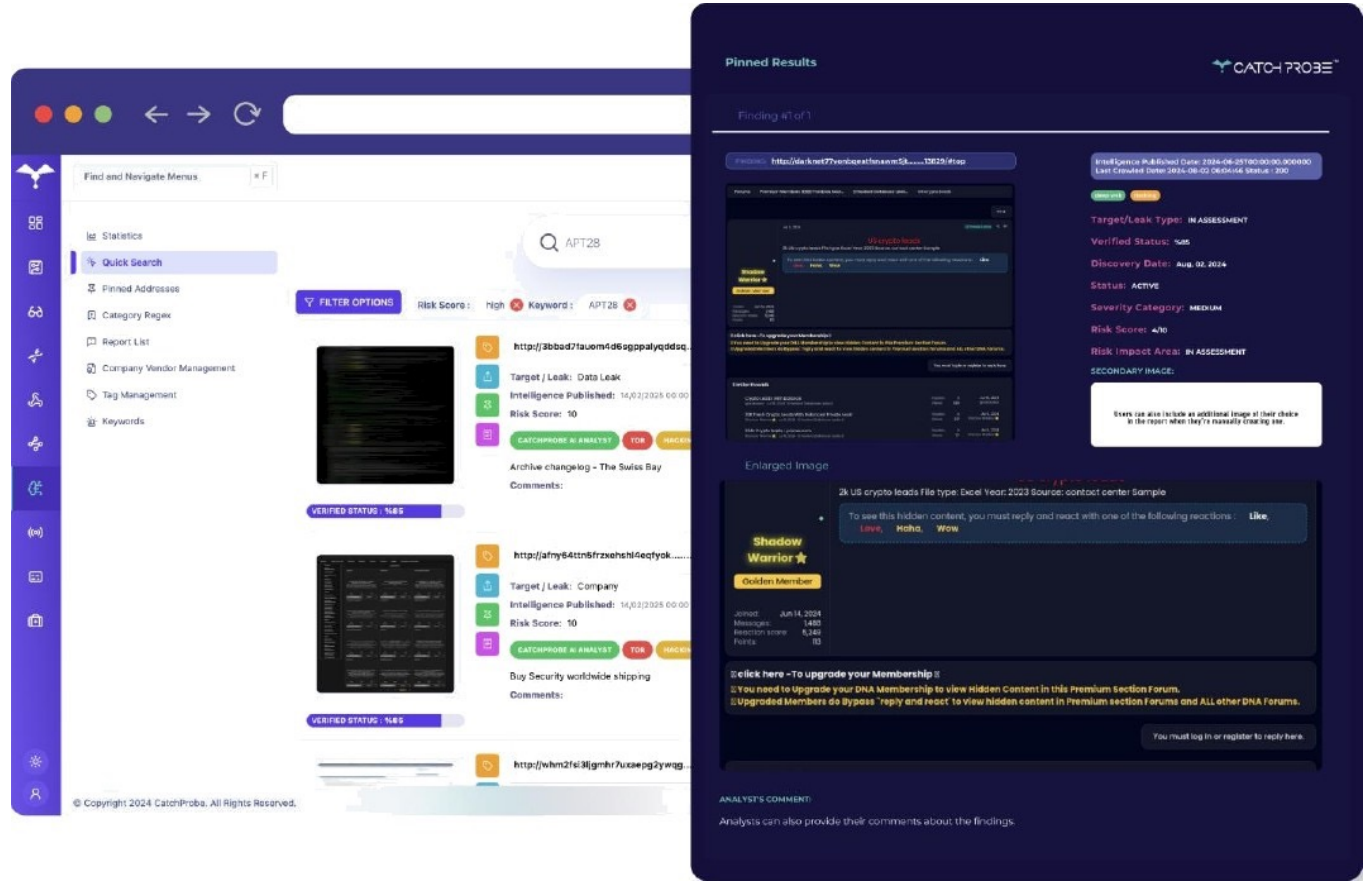
Rakipler, saldırılar gerçekleştiğinde tepki veren reaktif çözümlere odaklanır.

CatchProbe proaktif siber savunma için tasarlanmıştır.

OTD BİLİŞİM
GLOBAL VAD

DARKMAP: YAPAY ZEKÂ İLE WEB İSTİHBARATINI YENİDEN TANIMLAR

- Yeraltı forumlarını, pazar yerlerini ve gizli ağları izler.
- Kurumları; ele geçirilmiş kimlik bilgileri, sızdırılmış finansal veriler ve gizli belgeler hakkında uyarır.
- Gerçek zamanlı yapay zekâ destekli tehdit değerlendirmesi sunar.
- Kaynakları otomatik olarak İngilizce'ye çevirir, böylece dil bariyerlerini aşarak içgörü elde etmeyi sağlar.
- Tedarikçi izlemeyi sınırsız şekilde mümkün kılar; lisans kısıtlamalarına bağlı kalmadan zafiyetleri takip edebilirsiniz.
- Kullanıcılar, yeni bulgular için otomatik e-posta uyarılarını PDF formatında yapılandırabilir; ne zaman, nasıl (örneğin risk skoruna göre) ve kimlere gönderileceğini belirleyebilir.
- CatchProbe tarafından belirlenen önceden tanımlı bütçe dahilinde, sızdırılmış verileri otomatik olarak temin eder.



DARKMAP NEDEN ÖNE ÇIKIYOR?

- Analiz edilmeye hazır 9 Petabayttan fazla veri seti
- Son 20 yıla ait kritik internet sayfalarına erişim
- Dark ve deep web platformlarında gerçek zamanlı & sıcak taramalar
- Retrospektif istihbarat için tarihsel/geçmişe dönük (soğuk) taramalar
- Tüm büyük dark web altyapılarının kapsanması:

- Yggdrasil, Tor, ZeroNet, 12P, Forumlar ve Mesajlaşma Ağları

- Tespit edilen sitelerin saniyeler içinde anlık klonlanması ve indirilmesi
- Toplanan tüm verilerde regex tabanlı derin arama
- Anahtar kelime tabanlı izleme: IP'ler, alan adları, isimler vb. desteklenir
- Anahtar kelime permütasyonları ve kombinasyonları oluşturma
- Yeni ortaya çıkan anahtar kelimelere dayalı uyarılar
- Tüm dijital varlıklar üzerinde zafiyet taraması
- Hacker gruplarının ve yeraltı faaliyetlerinin canlı izlenmesi

- 83 dil kaynağı
- İlgili içerikler için otomatik indirme yeteneği
- Yapay zekâ tarafından desteklenen öngörücü istihbarat özellikleri
- Büyük veri korelasyonuyla yapay zekâ tabanlı risk analizi
- Platformlar arası kimlik eşleştirme (ör. Telegram avatarı ve forum takma adı)
- İzlenenler:

- Telegram ve WhatsApp grupları

- Kritik önceliğe göre sıralanmış şifreli ICQ ve IRC sohbetleri

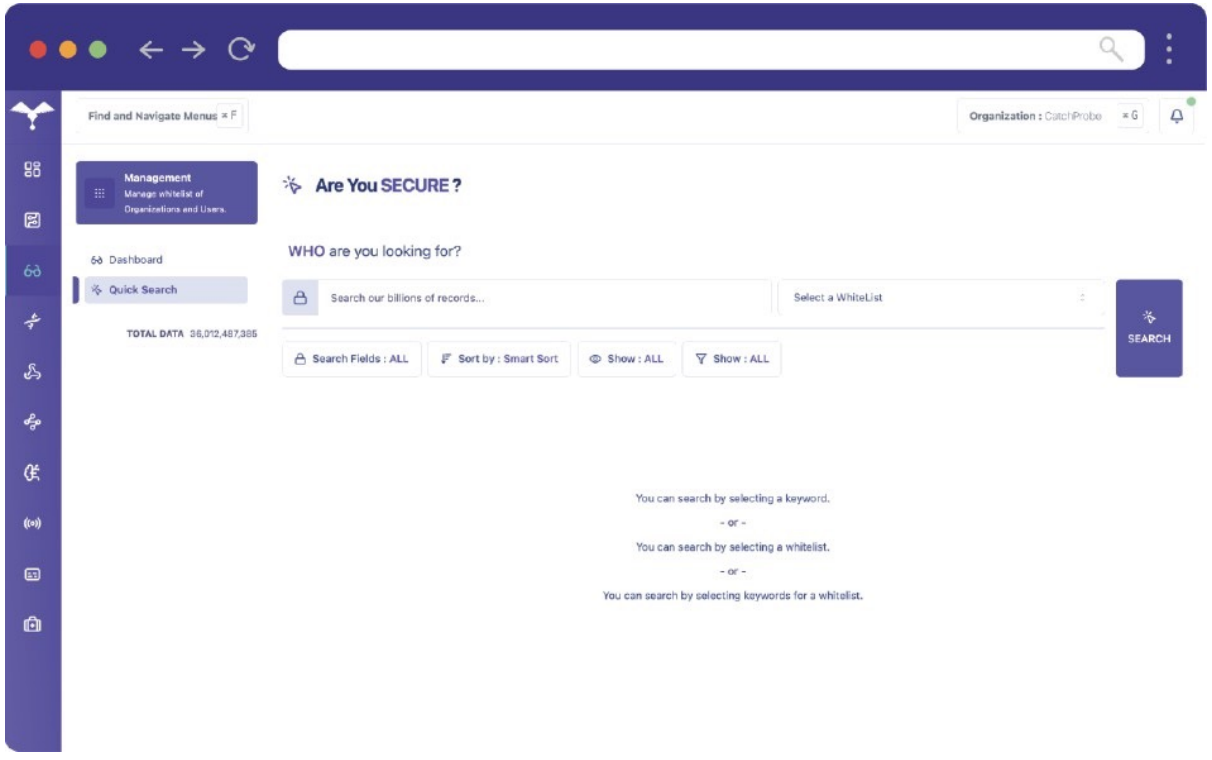
- Tüm darknet ve deepnet platformlarına anonim erişim

- Gelişmiş tehdit atıflaması için operatör davranış takibi
- CAPEX'i sıfıra indirir, OPEX'i %50'ye kadar azaltır
- Tespit ve uyarılar:

- Canlı erişim satışları (banka hesapları, telefon dinleme vb.)

LEAKMAP: VERİ İHLALLERİNİ HASSASİYETLE YÖNETMEK

CatchProbe LeakMAP, sızdırılmış verileri tanımlamak ve analiz etmek için oluşturulmuş, en büyük ve sürekli genişleyen veritabanıdır.



- Dark web kaynakları genelinde 1 petabayttan fazla sızdırılmış veriyi haritalandırır ve analiz eder.
- Sızdırılmış kimlik bilgilerini otomatik olarak doğrular, pasif veya sahte girdileri filtreler.
- Kurumları ortaya çıkan veri ihlalleri, kimlik bilgisi sızıntıları ve finansal veri maruziyetleri konusunda uyarır.
- Sızdırılmış verileri kullanmaya çalışan saldırganları tespit etmek için SmartDECEPTIVE ile entegre çalışır.

Mevcut Toplam Veri: +36 milyar.

CATCHPROBE™

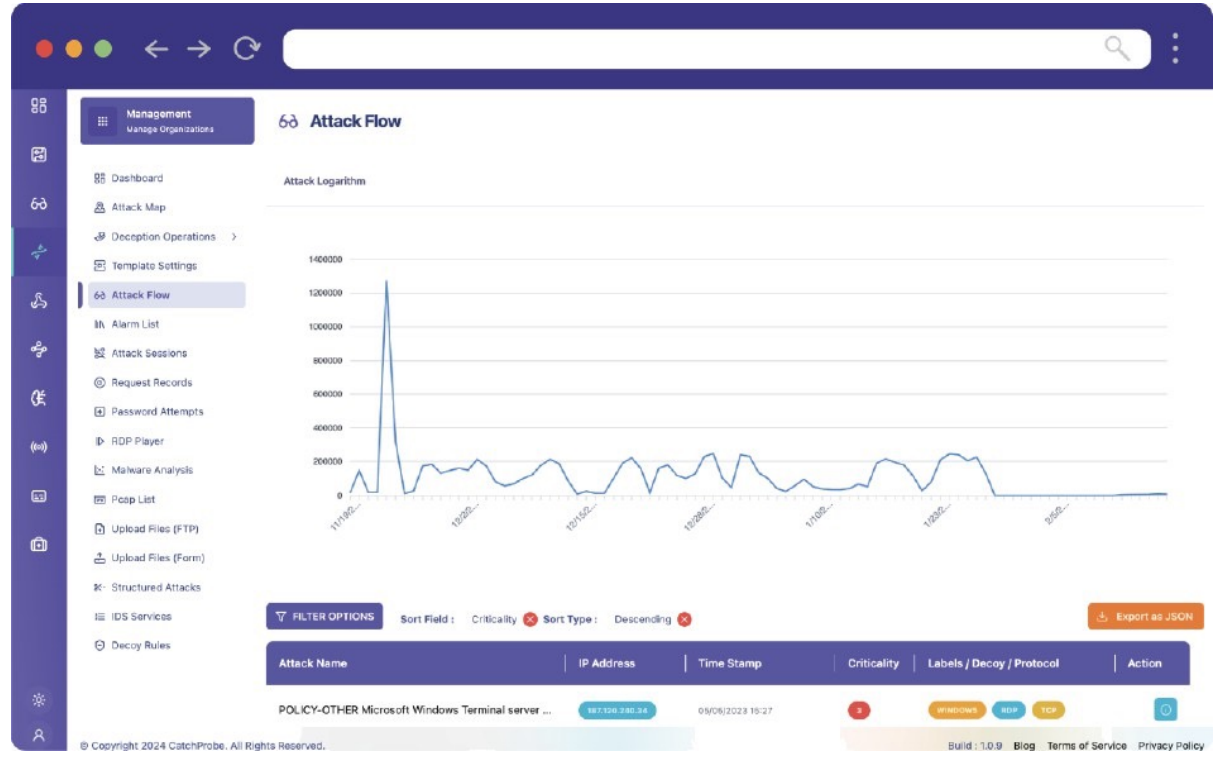
LEAKMAP NEDEN ÖNE ÇIKIYOR?

- Küresel veri setleri genelinde kapsamlı ihlal analizi
- LDAP entegrasyonu ve Active Directory güvenliği içgörüleri
- Bulguları sınıflandırmak ve önceliklendirmek için kurumsal bazlı etiketleme
- Son 20 yıla ait tüm sızdırılmış veritabanlarına erişim
- Kötü amaçlı yazılım günlüklerinin alınması ve analizi
- İnceleme amacıyla kötü amaçlı yazılım dosyalarını indirme yeteneği
- Henüz yayımlanmamış (yüzeye çıkmamış) kötü amaçlı yazılım tehditlerinin tespiti
- Toplanan tüm verilerin yapay zekâ destekli yorumlanması
- Hedefli saldırılara karşı en savunmasız çalışanların belirlenmesi
- Farklı veri türleri arasında regex tabanlı korelasyon kullanımı
- Gelişmiş veri keşfi ve analizini mümkün kılar

SMARTDECEPTIVE: SALDIRGANLARI KARANLIKTA BIRAKMAK

SmartDECEPTIVE, saldırganları cezbeden yapay zekâ destekli ve yüksek derecede özelleştirilmiş tuzaklarla (decoy) geleneksel honeypot yaklaşımını dönüştürür.

- Statik honeypot'lardan farklı olarak, CatchProbe'un aldatıcı sistemleri saldırgan davranışlarını gerçek zamanlı olarak analiz eder.
- Güvenlik duvarı (firewall) ve SIEM entegrasyonu sayesinde SmartDECEPTIVE, tehditlerin çekirdek sistemlere ulaşmadan önce çevre katmanında durdurulmasını sağlar.
- Ayrıca anında kötü amaçlı yazılım analizi yapar ve saldırganın IoC (Indicator of Compromise) verilerini açık kaynak istihbaratıyla karşılaştırarak daha derin içgörüler üretir.
- LeakMAP ile entegre çalışarak hedefli saldırıları tespit eder ve sızdırılmış verileri kötüye kullanma girişimlerini belirler.
- Tam paket yakalama (PCAP) yeteneği ve MITRE ATT&CK entegrasyonu, saldırgan davranışlarının derinlemesine anlaşılmasını sağlar.
- Bu yalnızca tespit değildir — proaktif engellemedir; saldırganların yönünü bulamadığı dijital bir mayın tarlası oluşturur.



OTD BİLİŞİM GLOBAL VAD

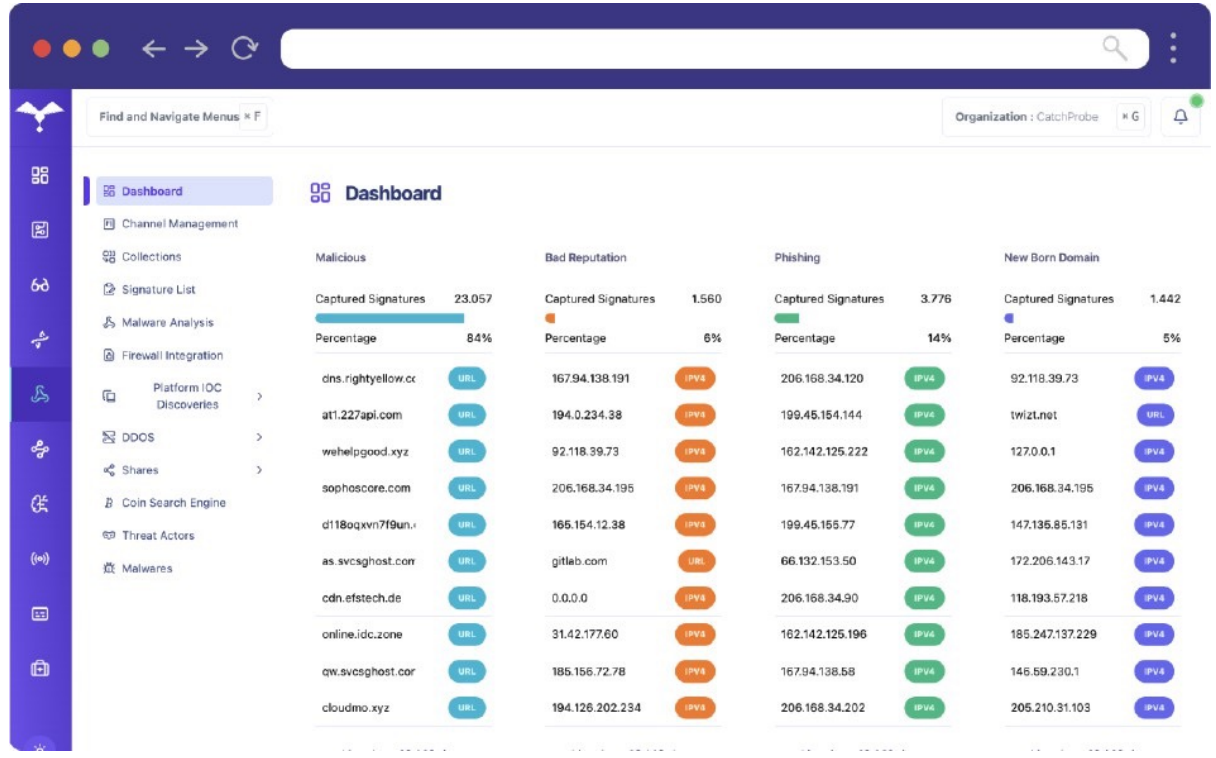
CATCHPROBE™

SMARTDECEPTIVE NEDEN ÖNE ÇIKIYOR?

- Yapay zeka destekli saldırgan profilleme ve davranış tahmini
- Tüm tuzaklar üzerinde gerçek zamanlı saldırı analizi
- Birkaç dakika içinde yüzlerce tespit edilemez tuzağı anında dağıtma
- Herhangi bir platformda aldatmaca ortamları oluşturma: Linux, Windows, SCADA, Android, Kiosk vb.
- Port ve servise göre tamamen özelleştirilebilir
- Önceden hazırlanmış geniş saldırı senaryosu şablonları kütüphanesi
- Tüm saldırı akışını (zararlı yazılım analizi dahil) saniyeler içinde çalıştırma — lisans yüklemeye veya manuel indirmeye gerek yok
- Tuzaklardan otomatik PCAP analizi
- RDP oturum izleme yeteneği
- Aynı saldırganı birden fazla IP'de tespit etme, yapay zeka ile korelasyon
- Saldırı imzalarına dayalı rekabet/karşılaştırmalı analiz imkanı
- Aldatma ortamları için özel SSL entegrasyonu
- Gelişmiş etkileşim için ters proxy desteği
- Enerji sektörü altyapıları için isteğe bağlı şirket içi (on-prem) dağıtım
- Her IDS için özel kural setleriyle sınırsız IDS örneği oluşturma
- Sermaye harcamalarını (CAPEX) sıfıra düşürme, işletme harcamalarını (OPEX) %50'ye kadar azaltma
- Esnek yanıt: otomatik izolasyon veya sadece uyarı modları

THREATWAY: EKOSİSTEMİNİZE KUSURSUZ ŞEKİLDE UYUM SAĞLAYAN GERÇEK ZAMANLI CTI

- Öncelik Kritik Tehditlerde: Korumanızı En Önemli Noktalara Odaklayın. ThreatWAY, tehditleri analiz eder ve önceliklendirir; böylece kuruluşunuz en kritik risklere odaklanır.
- İşletme içi ve kurumlar arası kanallarınız arasında işlenmiş istihbaratı milisaniyeler içinde paylaşmanıza olanak tanır.
- Kompromize Göstergelerini (IoC'leri) doğrudan güvenlik duvarlarınıza, SIEM ve SOAR sistemlerinize iletir.



ThreatWAY, API aracılığıyla 200'den fazla platformla kesintisiz entegrasyon sunar. Buna ek olarak, DarkMAP'in gelişmiş tarama (crawling) operasyonları ve SmartDECEPTIVE'in tuzakları ile ortaya çıkarılmış saldırıları sayesinde kapsamlı bir tehdit istihbaratı ekosistemi oluşturur. Ayrıca, yalnızca kuruluşunuzun ihtiyaçlarına en uygun ve anlık olarak güncel istihbaratın kullanılmasını sağlamak için özelleştirilmiş veri kaynaklarını kolayca ekleyip kaldırmanıza da olanak tanır.

CATCHPROBE™

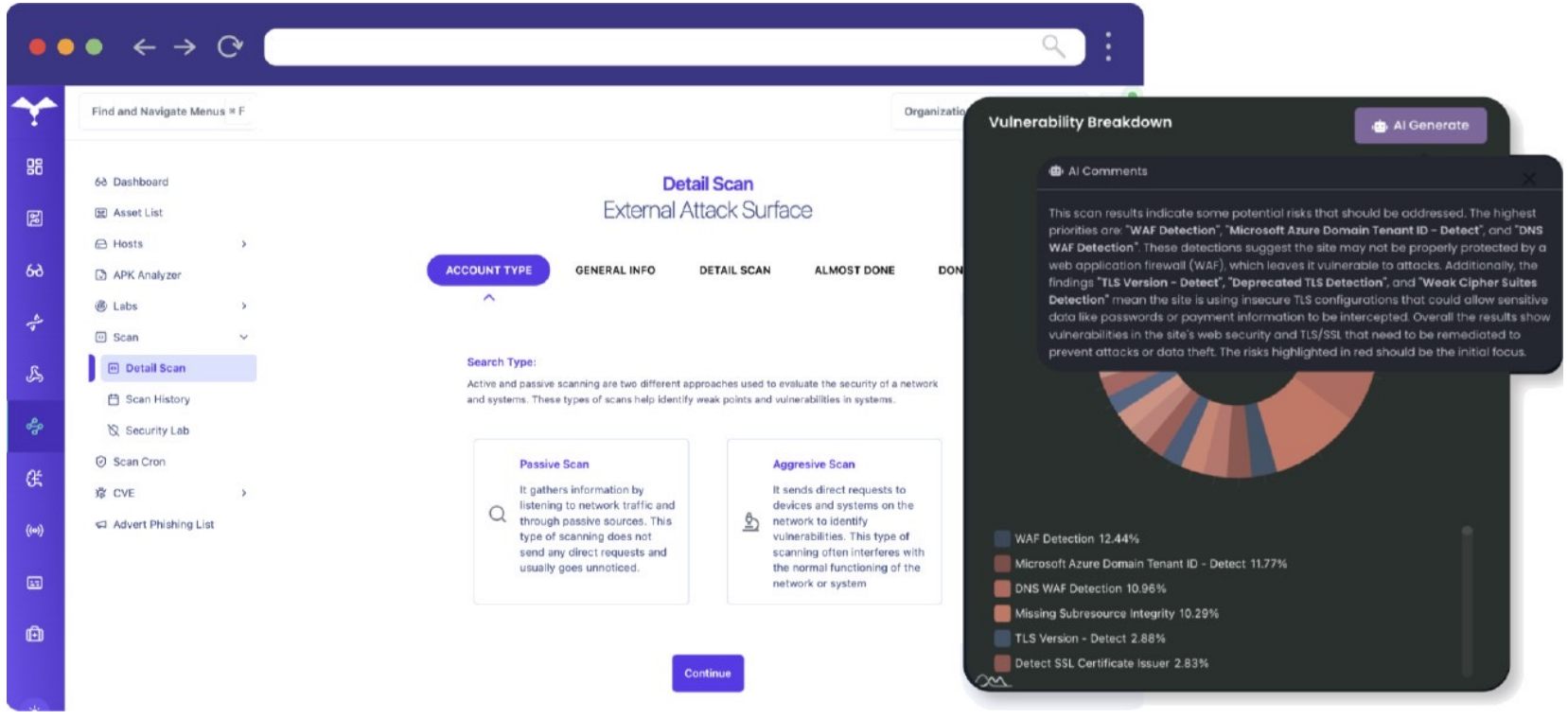
- RDP oturum izleme yeteneği
- Birden fazla IP'de aynı saldırganı tespit etme, Yapay Zeka ile korelasyon
- Saldırı imzalarına dayalı rekabet/karşılaştırmalı analiz olanağı
- Aldatmaca ortamları için özel SSL entegrasyonu
- Gelişmiş etkileşim için reverse proxy desteği
- Enerji sektörü altyapıları için isteğe bağlı şirket içi (on-prem) dağıtım
- Her IDS için özel kural setleriyle sınırsız IDS örneği oluşturma
- CAPEX'i sıfıra düşürme, OPEX'i %50'ye kadar azaltma
- Esnek yanıt: otomatik izolasyon veya yalnızca uyarı modları
- Bilgi sızıntısı tespiti
- Sosyal mühendislik göstergeleri

THREATWAY NEDEN ÖNE ÇIKIYOR ?

- Dakikalar içinde kendi CERT (Computer Emergency Response Team) ve CSIRT (Computer Security Incident Response Team) altyapınızı oluşturun
- Özel istihbarat paylaşım kanalları oluşturun
- Diğer kuruluşları tehdit paylaşım ağınıza davet edin
- İstihbarat veya uyarıları iş ortaklarınıza ya da dahili güvenlik araçlarınıza iletin
- 10 yılı aşkın süreye ait, puanlanmış ve zenginleştirilmiş kirli IP veri kümelerine erişim sağlayın
- 20'den fazla veri türünü kapsayan milyarlarca kaydı içerir
- İstihbarat içeriği şunları kapsar:
- DNS sağlık analizleri
- Yama durumu (patching status) değerlendirmeleri
- Uygulama güvenliği analizleri

RISKROUTE: KAPSAMLI SALDIRI YÜZEYİ YÖNETİMİ

CatchProbe RiskRoute, güvenlik ekiplerine kritik sistemleri izleme, yönetme ve güvence altına alma gücü kazandırır.
Zafiyetleri belirlemeye, varlıkların durumunu takip etmeye ve böylece veri ihlali ile siber saldırı risklerini azaltmaya yardımcı olur.



Yapay zekâ destekli risk analizi sunar ve duruma özel iyileştirme önerileri sağlar.

Jira, Webhook ve e-posta üzerinden entegre uyarı sistemiyle, olay müdahalesini (incident response) verimli hâle getirir ve Subresource Integrity (SRI) eksikliği gibi güvenlik olaylarına hızlı yanıt sağlar.

CATCHPROBE™

RISKROUTE NEDEN ÖNE ÇIKIYOR?

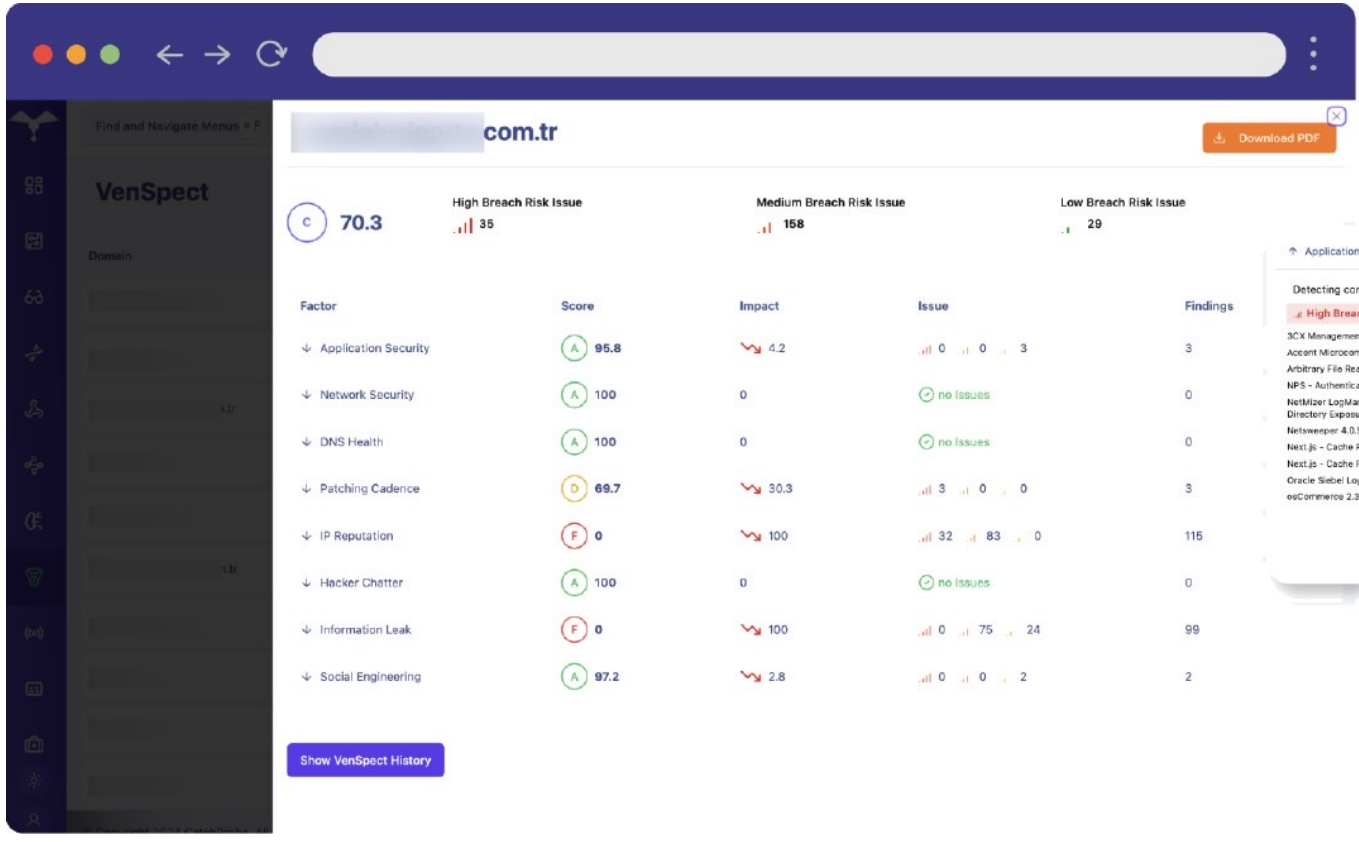
- İç ve dış varlıklar genelinde zafiyet değerlendirmesi
- Dijital altyapı için kapsamlı güvenlik hizmetleri
- Uygulama güvenliği testleri ve kod düzeyinde analiz
- Bulut ortamı güvenlik testleri
- Siber Varlık Saldırı Yüzeyi Yönetimi (CAASM)
- Entegre Dijital Risk Koruma Hizmetleri (DRPS)
- Pasif DNS taraması ile gizli iz tespiti
- Dijital platformlarda dolandırıcılık tespiti
- Sosyal medya tabanlı dolandırıcı analizi
- Reklam görselinden metin çıkarımı ile dolandırıcılık desenlerinin tespiti
- Dijital tehditlerle ilişkilendirilen sosyal medya hesaplarının keşfi
- Kuruluşunuz içindeki Shadow IT'yi tespit etme ve haritalama

OTD BİLİŞİM
GLOBAL VAD

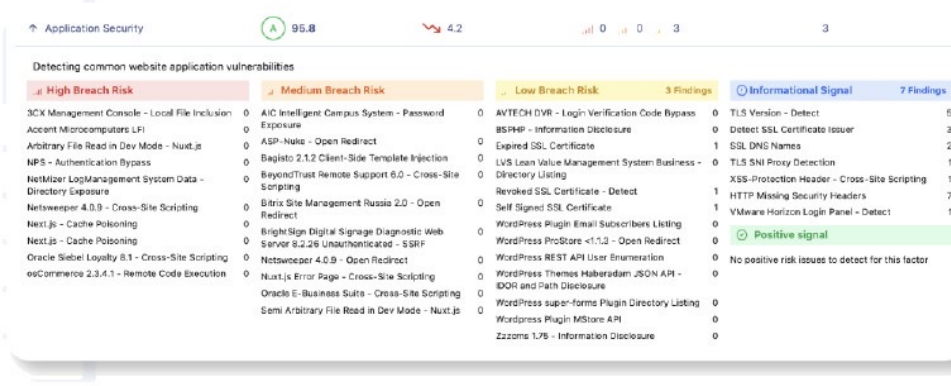
CATCHPROBE™

VENSPECT: ÜÇÜNCÜ TARAF RİSK DEĞERLENDİRMESİ

VenSPECT, üçüncü taraf tedarikçi ve hizmet sağlayıcılarınızın güvenlik duruşunu (security posture) izlemek için tasarlanmıştır. Otomatik aylık değerlendirmeler ve zaman içindeki risk puanlaması sayesinde, harici risklerin önünde kalmanızı sağlar ve manuel iş yükü olmadan bilinçli kararlar almanıza yardımcı olur.



- Gerektiğinde değerlendirmeleri manuel olarak başlatabilir, geçmiş performansı izleyebilir ve risk taşıyan iş ortaklarını hızla tespit edebilirsiniz.



- Tek tıkla, puanlar, içgörüler ve risk analizleri içeren ayrıntılı tedarikçi raporunu indirin — paylaşım, denetim veya uygunluk (due diligence) süreçleri için mükemmel bir araç.

OTD BİLİŞİM
GLOBAL VAD

CATCHPROBE™

VENSPECT NEDEN ÖNE ÇIKIYOR?

- Merkezi istihbarat orkestrasyonu: Web, dark web, aldatmaca (deception), CTI ve ASM modüllerinden gelen içgörüleri tek bir merkezde birleştirir.
- DarkMAP, LeakMAP, SmartDECEPTIVE, RiskRoute ve ThreatWAY verilerini tek bir birleşik görünümde ilişkilendirir.
- Modüller arası desen tespiti yaparak sızdırılmış veriler, altyapı zafiyetleri ve aktif tehdit aktörleri arasındaki bağlantıları ortaya çıkarır.
- Önceliklendirilmiş ve risk puanlı bulguları bağlamsal bilgilerle sunarak karar alma süreçlerini hızlandırır.
- Yapay zekâ destekli altyapı, aşağıdaki yetenekleri sağlar:
- Varlık çözümleme (entity resolution): Aynı tehdit aktörünü Telegram, forum, e-posta gibi farklı ortamlarda tanımlama
- Saldırı zinciri yeniden yapılandırma (attack chain reconstruction)
- Birden fazla saldırı vektörü arasında davranış analizi
- Ayrıca, özelleştirilebilir panolar (dashboard'lar), filtreler ve uyarı sistemleri ile analistlerin çalışma süreçlerini optimize eder.
- SOC ekipleri, tehdit avcıları (threat hunters) ve yönetici raporlamaları için ideal bir çözümdür.

CATCHPROBE™

CATCHPROBE: HEPSİ BİR ARADA DİJİTAL İSTİHBARAT PAKETİ

- **İlişkilendirilmiş Sızıntı Tespiti:**

  Birden fazla platformdaki ele geçirilmiş kimlik bilgilerini (credentials) tespit eder, farklı kaynaklardan gelen sızıntıları ilişkilendirerek kimlik doldurma (credential stuffing) saldırılarını önler.

- **Eyleme Dönüştürülebilir İstihbarat için Derin Tarama:**

  Yapay zekâ destekli tarayıcılar (scraper) kullanarak dark web pazar yerlerini, forumları ve gizli ağları analiz eder. Doğrulanmış istihbarat üretir ve her bulguya risk puanı ile sınıflandırma atar.

- **Decoy Yönetimi:**

  SmartDECEPTIVE, saldırganları cezbetmek için gerçeğe yakın tuzak sistemleri (decoy) kurar. Bu sayede kuruluşlar, gerçek altyapılarına en az riskle maruz kalarak tehdit istihbaratı toplayabilir ve saldırgan davranışlarını analiz edebilir.

- **Yapılandırılmış Saldırı Tespiti:**

  Sızdırılmış kimlik bilgilerini kullanarak tuzak sistemlere yönelik hedefli saldırıları algılar ve ThreatWAY ile entegre çalışarak otomatik olay müdahalesi (incident response) sağlar.

- **Kusursuz Entegrasyon ve Otomasyon:**

  CatchProbe modülleri, birbiriyle entegre şekilde çalışarak gerçek zamanlı istihbarat paylaşımı, otomatik iyileştirme (remediation) ve güvenlik ekosistemleriyle sorunsuz API entegrasyonları sağlar.

OTD BİLİŞİM
GLOBAL VAD