CATCH PROBE™

OTD BİLİŞİM

GLOBAL VAD

HAKKIMIZDA

CATCHPROBE, dünyanın ilk Yapay Zekâ (AI) destekli, SaaS tabanlı, merkezi ve otonom istihbarat platformu (Intelligence Suite – sürüm: IDA Mountain) üzerinden eyleme dönüştürülebilir web istihbaratı, OSINT, aldatma (deception) sistemleri, tehdit istihbaratı ve dijital suç analitiği çözümleri sunan, uluslararası tanınırlığa sahip bir teknoloji şirketidir.

CATCHPROBE, istihbarat toplama, zenginleştirme, aldatma, profilleme, hedef belirleme, anlamsal analiz ve ilişkilendirme çözümleri için geliştirilmiş gelişmiş bir merkezi istihbarat orkestrasyon platformudur.
Potansiyel tehditleri önlemek, verilerinizi zenginleştirmek, kaynaklar arası korelasyon kurmak, raporlar oluşturmak ve elde ettiği istihbaratı kullanarak doğru analizlerle tehdit önleme süreçlerini kolaylaştırmak için gereken tüm verileri toplar.

Kamu ve özel kaynaklardan toplanan doğrulanmış tehdit istihbaratı verilerine ek olarak, Yapay Zekâ Tabanlı Otonom Aldatma Sistemleri (AI-Based Autonomous Deceptions), sızdırılmış veri tabanları (Leak DBs) ve dark/deep web kaynakları da CATCHPROBE tarafından kullanılır ve merkezi bir arayüz üzerinden erişilebilir hale getirilir.

Tüm İhtiyaçlarınız için Tek Platform

CATCHPROBE; web istihbaratı, tehdit istihbaratı, tespit, aldatma ve sızdırılmış veri profilleme hizmetleri ile yanıt (response) özelliklerini aynı platform üzerinde, hızlı ve entegre şekilde sunar. Bu bileşenler, birbirleriyle tam uyum içinde çalışarak hızlı, otomatik ve senkronize savunma süreçleri sağlar.

CatchProbe Ne Yapar

Nasıl ki evinizi bir kamera ile izliyorsanız, dijital dünyada da verilerinizi aynı şekilde korumanız gerekir.
Kamera bir hırsızlığı engelleyemez ama size kimin, ne yaptığını gösterebilir. Dijital dünyada olan her şeyi kontrol etmeniz mümkün olmasa da; farkındalık, doğru araçlar ve önleyici stratejilerle zararı engelleyebilir veya minimize edebilirsiniz. Bu nedenle CATCHPROBE, doğrulanmış istihbarata ihtiyaç duyan kurumlar, devletler ve bireyler için benzersiz bir platform sunar.

CATCHPROBE'UN SUNDUKLARI

Kesintisiz biçimde entegre edilmiş, her biri diğerinin yeteneklerini tamamlayan ve geliştiren modüllerin geliştirilmesiyle, doğrulanmış ve eyleme dönüştürülebilir istihbarat için benzersiz ve birleşik bir ekosistem oluşturduk. Bu ekosistem, diğerlerinin başaramadığını mümkün kılan kapsamlı bir yapı sunar: istihbarat ile güvenlik arasında etkili iletişim.

Yapay zekâ ile güçlendirilmiş web istihbaratı platformumuz DarkMAP, analistlere kendi operasyonlarını hedef alan siber tehditleri etkin biçimde tanımlama ve bunlara karşı koyma olanağı sağlar. 6,7 petabaytlık ham veri deposuna sahip olan DarkMAP, internetin tüm katmanlarında anahtar kelime tabanlı taramalar gerçekleştirir ve kapsamlı sonuçları 48 saat gibi kısa bir sürede sunar.

Özellikle operasyonel teknoloji ortamlarında SmartDECEPTIVE, gelişmiş aldatma sistemleri sağlayarak kritik bir rol oynar. Bu decoy'lar (yem sistemleri), tehdit aktörlerinin kimliklerinin belirlenmesini ve profillenmesini mümkün kılar, böylece kritik altyapılar olası saldırılardan korunur.

Mevcut SIEM ve Firewall (güvenlik duvarı) sistemleriyle kusursuz biçimde entegre olan ThreatWAY, olay müdahalesi sürecini otomatikleştirir, yanıt süresini azaltır ve güvenlik operasyonlarının genel verimliliğini artırır. Ayrıca ThreatWAY, son on yıla ait Indicators of Compromise (IoC) verilerine erişimi kolaylaştırır.

LeakMAP, 1 petabayttan fazla profillenmiş ve haritalanmış veri içeren geniş bir sızıntı veritabanını keşfetmek ve analiz etmek için kapsamlı bir çözümdür.

RiskROUTE, kapsamlı IP ve port taramaları gerçekleştiren, phishing saldırılarını tespit eden ve geçmiş IP güvenlik açıklarını ile potansiyel tehditleri proaktif olarak ortaya çıkaran Attack Surface Management modülümüzdür.

CATCHPROBE™

OTD BİLİŞİM
GLOBAL VAD

DarkMAP
Web Intelligence

CatchProbe DarkMAP, yalnızca istihbarat verileriyle besleyebileceğiniz basit bir platform olmanın ötesindedir. Güçlü analiz yetenekleri, veri zenginleştirme ve yapay zekâ destekli altyapısı ile sizi yeni nesil savunma teknolojilerinin ön saflarına taşır. DarkMAP'in temel amaçlarından biri, internetin tüm katmanlarında keşif ve dizinleme yapmayı mümkün kılmaktır: Sosyal Medya, DeepWeb ve DarkNet. DarkMAP, hedeflenen sayfaları eksiksiz şekilde arşivleyebilir, ayrıca otomatik içerik izleme ve keşif (discovery) süreçlerini yürütür.

DarkMAP'i diğer WEBINT (Web Intelligence) çözümlerinden ayıran bir diğer unsur, hızlı kurulumu, düşük maliyeti ve analistler ile ekipler arasında görevlerin yükseltilmesi (escalation) ve devredilmesi (delegation) yeteneğidir.

Ayrıca DarkMAP, toplanan içeriği işlevsel, sade ve kapsamlı bir biçimde sunarak, analistlerin araştırmalarını zahmetsiz ve verimli biçimde yürütmelerine olanak tanır.

Özellikler:

- Anahtar kelime analizi aracılığıyla tehdit grupları arasındaki ilişkilerin tespiti
- Yinelemeli bağlantı analizi (Recursive Link Analysis) ile Dark Web üzerindeki kör noktaların belirlenmesi
- Üyelik gerektiren platformlar (forumlar, IRC grupları, Telegram kanalları vb.) için akış yönetimi özelliği
- Çok dilli kaynakların otomatik olarak İngilizce'ye çevrilmesi
- Gerçek zamanlı tehdit değerlendirmesi
- CrimeGround entegrasyonu aracılığıyla çapraz vaka analitiği (Cross-Case Analytics) ile suç ve fail analizi
- SaaS tabanlı altyapı sayesinde düşük maliyet ve yüksek operasyonel verimlilik

Genel Değerlendirme

Tree Branch Metodolojisi	IOC ve tehdit keşfi, düzenli ifadeler kullanılarak gerçekleştirilir.
Benzersiz Teknoloji	WebIInt platformu tarafından kolaylaştırılan saldırgan analizi.
SaaS Tabanlı Platform	Analistler için olay tabanlı risk analizi.
Kullanımı Kolay	Analistler için yükseltme ve delege etme süreci.
Yeni Nesil Analiz	Departmanlar ve analistler arasında ayrıntılı yetkilendirme protokolleri.
Proaktif Savunma Yetenekleri	

HIZ VE ZAMAN KAZANIN

ELEŞTİREL BİR GÖRÜŞÜ ELEŞTİRİN

ORTAYA ÇIKAN TEHDİTLERİ BELİRLEYİN

DERİNLERİ ARAŞTIRIN

OTD BİLİŞİM
GLOBAL VAD

DARKMAP: DİJİTAL DERİNLİKLERDE YOL ALMA

SURFACE WEB

İSTİHBARAT TOPLAMA ÇABASI: MİNİMUM

Web kazıma araçları, arama motoru API'leri ve OSINT yöntemleri

ELDE EDİLEN BİLGİ TÜRÜ

Genel erişime açık tüm bilgiler

DEEP WEB

İSTİHBARAT TOPLAMA ÇABASI: ORTA

API'lerden, veritabanlarından veya şifreli ortamlardan veri elde etme.

ELDE EDİLEN BİLGİ TÜRÜ

- Kurumsal ve devlet veritabanları
- Abonelik tabanlı araştırma veya haber siteleri
- Kurum içi ağlar veya organizasyonlar

DEĞER

Özel tartışmalar gibi değerli ve ayrıcalıklı bilgiler sağlar.

DARK WEB

İSTİHBARAT TOPLAMA ÇABASI: YÜKSEK

Sosyal mühendislik, dilbilim uzmanlığı ve etik hackleme unsurlarını içerebilir.

ELDE EDİLEN BİLGİ TÜRÜ

- Çalınmış kimlik bilgileri ve kredi kartı numaraları
- Siber suç araç setleri: kötü amaçlı yazılımlar ve fidye yazılımları
- Yasa dışı pazar yerleri: uyuşturucu, silah ve sahte ürünler

DEĞER

Veri ihlalleri veya yasa dışı işlemler konusunda endişe duyan kuruluşlar için kritik öneme sahiptir. Yaklaşan siber saldırıları, satışa sunulan güvenlik açıklarını veya ortaya çıkan yeni suç eğilimlerini ortaya çıkarabilir.

ANONİM AĞLAR (TOR, I2P, YGGDRASIL)

İSTİHBARAT TOPLAMA ÇABASI: AŞIRI YÜKSEK

Belirli ağ araçlarının ileri düzeyde anlaşılmasını gerektirir. Sızma işlemi, topluluklarla güven ilişkisi kurulmasını gerektirebilir.

ELDE EDİLEN BİLGİ TÜRÜ

Yüksek düzeyde şifrelenmiş iletişim kanalları ve yasa dışı faaliyetlere hizmet eden pazar yerleri.

DEĞER

Yasa dışı faaliyetlerin takibi ve kurumsal gizli verilerin korunması için faydalıdır.

MERKEZİ OLMAYAN WEB PROJELERİ (FREENET, ZERONET)

İSTİHBARAT TOPLAMA ÇABASI: AŞIRI YÜKSEK

Özel araçlar gerektirir.
İzleme faaliyetleri sürekli katılım gerektirir.

ELDE EDİLEN BİLGİ TÜRÜ

Hassas Konuların Tartışıldığı Web Siteleri
Sansürlenmiş Bilgi veya İletişimler
Araçların Geliştirilmesi ve Paylaşımı

DEĞER

- Yasa dışı içeriğin takibi için faydalıdır.

İLETİŞİM KANALLARI (ŞİFRELİ MESAJLAŞMA UYGULAMALARI)

İSTİHBARAT TOPLAMA ÇABASI: AŞIRI YÜKSEK

Çoğu zaman sosyal mühendislik, sadece davetlilerin erişebildiği forumlara erişim veya şifreli kanalların gerçek zamanlı izlenmesi gerektirir.

ELDE EDİLEN BİLGİ TÜRÜ

- Siber saldırıların koordine edilmesi veya taktiklerine ilişkin tartışmalar
- Çalınmış verilerin veya yasa dışı içeriklerin alım-satımı
- Suç aktörleri arasındaki şifreli iletişimler

DEĞER

Gerçek zamanlı tehdit tespiti, siber güvenlik takibi ve yanlış bilgi kampanyaları ya da yasa dışı faaliyetlerin koordinasyonunun izlenmesi açısından kritik öneme sahiptir. Yaklaşan saldırılar veya dolandırıcılık girişimleriyle ilgili olarak kurumlara ya da kolluk kuvvetlerine erken uyarı sağlar.

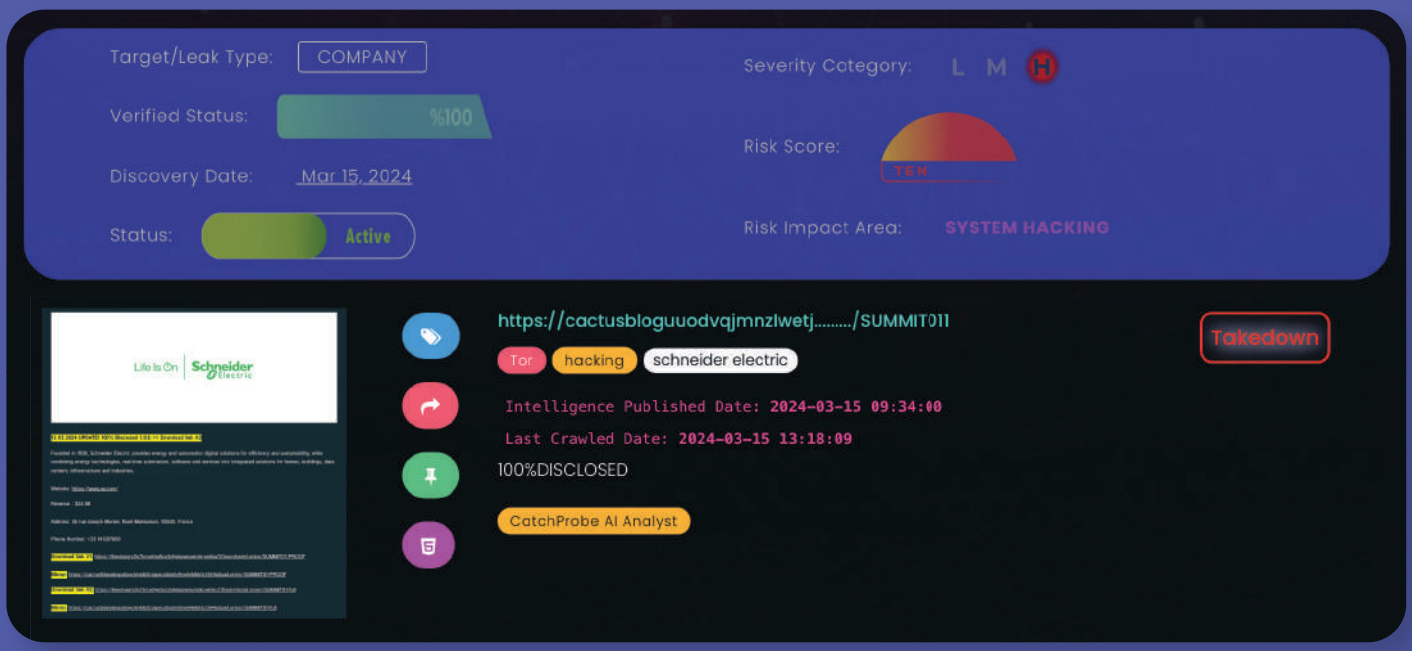
DARKMAP: Yapay Zekâ ve Yeni Nesil Yeteneklerle Web İstihbaratını Yeniden Tanımlama

CatchProbe DarkMAP modülü, internetin tüm katmanlarında hassas ve eyleme dönüştürülebilir istihbarat sunarak siber güvenlik profesyonelleri için gelişmiş tehdit tespiti, analiz ve yükseltme süreçlerini kolaylaştırır.

Temel Ayrıştırıcılar

Yapay Zekâ Tabanlı Değerlendirme:

DarkMAP'in Yapay Zeka altyapısı, gerçek zamanlı olarak değerlendirdiği bulgularla tehdit ciddiyeti hakkında kapsamlı içgörüler sunmakta, anında önceliklendirme ve harekete geçme imkanı tanımaktadır.



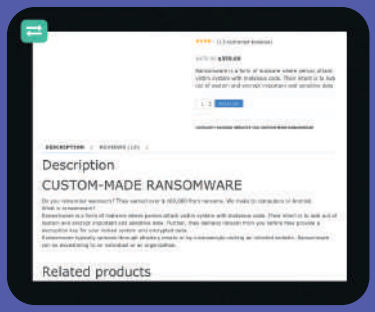
Akış Yönetimi ve Sayfa Kısıtlaması Aşımı:

Üyelik gerektiren veya erişimi kısıtlı platformları yönetebilme kabiliyeti sayesinde, DarkMAP web'in tüm katmanlarında tam veri erişimi sağlar.

Ayrıca DarkMAP, CatchProbe tarafından belirlenen ön tanımlı bütçe sınırları içinde verileri otomatik olarak toplayabilir.

İçerik Arşivleme

DarkMAP, taranan verileri ekran görüntüsü formatında arşivleyerek gelecekte kolay erişim ve geriye dönük analiz imkânı sağlar.



İlk taramadan sonra içerikte herhangi bir değişiklik tespit edilirse, kullanıcılar ekranın sol üst köşesindeki bir bildirimle otomatik olarak bilgilendirilir.

OTD BİLİŞİM
GLOBAL VAD

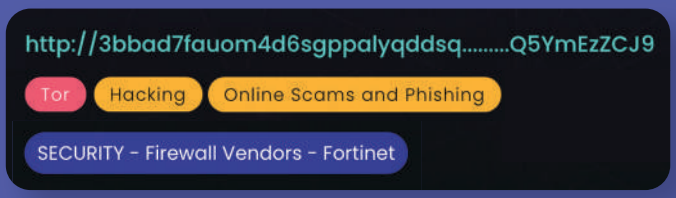
DarkMAP

Çok Dilli Çevirme

Tüm tehdit istihbaratı verileri İngilizce değildir; birçok tehdit aktörü Rusça, Korece ve diğer dilleri kullanarak faaliyet göstermektedir.
DarkMAP, bu dillerden gelen kaynakları otomatik olarak çevirerek dil engellerini ortadan kaldırır ve kapsamlı, eyleme dönüştürülebilir içgörüler sunar.

Sınırsız Satıcı İncelemesi

DarkMAP, lisans sınırlamalarına bağlı olmaksızın, güvenlik açıklarını izlemek amacıyla satıcıların sınırsız biçimde takip edilmesine olanak tanır.



Otomatik ve Manuel Raporlama

Kullanıcılar, yeni bilgiler için ne zaman, nasıl ve hangi risk puanına göre kimlerin bilgilendirilmesi gerektiğini belirleyerek PDF formatında otomatik e-posta bildirimleri oluşturabilir.
Ayrıca kullanıcılar, modül aracılığıyla doğrudan detaylı raporları manuel olarak da hazırlayabilir.

Tırmanma, Delegasyon ve Gizlilik

DarkMAP'in platform mimarisi, görevlerin ekipler ve departmanlar arasında kesintisiz bir şekilde devredilmesini sağlar; iş akışlarını optimize eder ve iş birliğini güçlendirir.

Ek olarak yöneticiler, yalnızca yetkili personelin erişimini sağlayarak, kurumla ilgili anahtar kelimeler veya hassas bilgilerin gizli tutulmasını mümkün kılar.
Gelecekte benzer içeriklerin tespit edilmesi durumunda sistem, bu verileri otomatik olarak koruma altına alır.

OTD BİLİŞİM
GLOBAL VAD

LeakMAP

Açık Kaynak İstihbarat Platformu

LeakMAP, veritabanımızda toplanan içeriğin profilini çıkararak haritalandırması ve sızdırılan içerikler arasındaki ilişkileri belirlemesi açısından diğer sızıntı veritabanı platformlarından ayrılmaktadır.

Kuruluşlar, potansiyel çalışanlar hakkında arka plan bilgisi edinmek, iş e-postalarının kötüye kullanılmasını engellemek ve olası sızıntıları kolayca tespit etmek amacıyla LeakMAP'i kullanabilir. Bu sayede, kuruluşlar bilgisayar korsanlarının karmaşık kimlik avı kampanyaları düzenlemesini, ikna edici sosyal mühendislik saldırıları gerçekleştirmesini veya daha da kötüsü, iş e-postalarını tehlikeye atmasını ve sızıntıları istismar etmesini önleyebilir.

Genel Değerlendirme

- İhlal Takibi
- Açığa Çıkmış Kurumsal Kimlik Bilgileri Takibi
- Kimlik Bilgisi Doldurma Saldırılarını Önleme
- Suç Soruşturma Süreci
- Kullanıcı Adları ve Parolalar
- Kredi Kartları
- Şirket Belgeleri
- Fotoğraflar
- Sesler
- Kimlik Kartları
- Pasaportlar
- Telefon Numaraları
- Sosyal Medya Profilleri

Özellikler:

- LeakMAP, SMARTDECEPTIVE ile mükemmel bir entegrasyon sağlar ve hedefli saldırılarla ilgili zamanında uyarılar sunar. Ayrıca, sızdırılan kaynakları otomatik olarak güçlendirmek amacıyla DARKMAP ile entegre olur.
- Korelatif İşlevsel Arama (örneğin, kimlik numarası 43 ile başlayan, kayıtlı aracının plakası AB içeren veya telefon numarası 94 ile biten kişilerin bilgilerini elde etme).
- Tam metin araması.
- GDPR uyumlu veri görüntüleme.

EPLOZED BELGELERİ BUL

ZEKA TOPLAMA

KİMLİK BİLGİSİ DOLDURMA SALDIRILARINI ENGELLEYİN

PARÇA İHLALLER

OTD BİLİŞİM
GLOBAL VAD

LEAKMAP: DARK WEB'İN SIZINTI MANZARASININ HARİTASI

SIZINTI TÜRLERİ

SIZINTI TÜRLERİ

- Kimlik Bilgileri
  E-postalar
  Kullanıcı adları
  Şifreler
- Finansal Veriler ve
  Kredi Kartı Numaraları
  Banka Bilgileri
- Kişisel Tanımlayıcı Bilgiler
  Telefon Numaraları
  Kimlik Kartları
  Sosyal Güvenlik Numaraları
- Kurumsal Belgeler
- Sözleşmeler
  Ticari Sırların
  Stratejik Planları

NEDEN ÖNEMLİDİR?

PROAKTİF KAÇAK TESPİTİ NEDEN ÖNEMLİDİR?

- Anında Tehdit Azaltma Saldırılar gerçekleşmeden önce sızdırılan bilgileri tespit etme ve yönetme
- Risk Profillemesi ve Hasar Kontrolü Sızıntının niteliğine göre savunma stratejileri geliştirme
- Kurumsal Veri Koruması Dahili ve müşteri verilerinin güvenliğini sağlama

SIZINTILAR NASIL MEYDANA GELİR?

SIZINTILAR NASIL MEYDANA GELİR?

- Kimlik Avı Saldırıları
- Zayıf Parolalar ve Yetersiz Kimlik Doğrulama Uygulamaları
- Üçüncü Taraf Tedarikçi İhlalleri
- İçeriden Gelen Tehditler
- Sosyal Mühendislik
- Kötü Amaçlı Yazılım ve Fidye Yazılımları

POTANSİYEL ETKİLER

KURULUŞLAR ÜZERİNDEKİ OLASI ETKİLER

- Mali Kayıp
  Dolandırıcılık,
  Para Cezaları,
  Hukuki Ücretler
- İtibar Zedelenmesi Müşteri Güveninin Yitirilmesi
- Uyumluluk İhlalleri
  GDPR
  HIPAA
  PCI
  DSS
- Operasyonel Kesintiler
  Veri Bozulması
  Sistem Durma Süresi
- Hedefe Yönelik Saldırılar
  Açığa Çıkan Veriler Üzerinden Gelecekteki Kullanım

ÖNLEYİCİ ÖNLEMLER

KURULUŞLAR İÇİN ÖNLEYİCİ ÖNLEMLER

- LeakMAP gibi Gelişmiş OSINT Araçlarının Kullanımı
- Hedefli Saldırıları Saptırmak İçin Sahte Sistemlerin Entegrasyonu
- Düzenli Güvenlik Denetimleri ve Güvenlik Açığı Değerlendirmeleri
- Hassas Verilerin Şifrelenmesi
- Çalışan Siber Güvenlik Eğitimi

VERİ SIZINTILARINDA GÖRÜLEN EĞİLİMLER

VERİ SIZINTILARINDA GÖRÜLEN EĞİLİMLER

- Tedarik Zinciri Saldırıları: Saldırganlar, hizmet verdikleri daha büyük kuruluşlara erişim sağlamak amacıyla giderek daha fazla üçüncü taraf satıcıları, hizmet sağlayıcıları veya yüklenicileri hedef almaktadır. Son ihlaller, tek bir satıcı ihlalinin hassas bilgilerin yaygın bir şekilde ifşa edilmesine nasıl yol açabileceğini göstererek, şirketlerin yalnızca kendi sistemlerini güvence altına almaları değil, aynı zamanda ortaklarını da izlemeleri gerektiğini vurgulamaktadır.

- Çift Gasp Saldırıları: Çift gasp saldırılarında, şirketler iki eş zamanlı tehdit ile karşı karşıya kalmaktadır: birincisi, operasyonları aksatan şifreli veriler ve ikincisi, fidye ödenmezse çalınan bilgilerin ifşa edilmesidir. Saldırganlar, ödeme baskısını artırmak için endüstrilerin kesintiye karşı savunmasızlığını kullanmaktadır.

- Kurumsal Casusluk ve İçeriden Sızıntılar: İçeriden kaynaklanan tehditler, hassas verilere erişimi olan çalışanların bilgileri kötü niyetli veya yanlışlıkla sızdırabilmesi nedeniyle kritik bir endişe kaynağı olmaya devam etmektedir. Uzaktan çalışma arttıkça, bu tehditlerin tespit edilmesi daha da zorlaşmaktadır.

- Siber Suç Çeteleri Tarafından Sızıntı Çiftçiliği: Kötü şöhretli Maze fidye yazılımı grubu gibi bazı siber suç grupları, hassas verileri toplamak ve zaman içinde yayınlamak amacıyla sistematik olarak birden fazla kuruluşu hedef almaktadır.

LEAKMAP: Veri İhlallerini Titizlikle Yönetmek

CatchProbe LeakMAP, sızdırılan verileri tespit etmek ve analiz etmek amacıyla sürekli genişleyen en büyük veritabanıdır. Kuruluşlara gerçek zamanlı içgörüler ve uyarılar sunar. Gelişmiş haritalama teknolojisi ile desteklenir ve SmartDECEPTIVE tuzaklarıyla entegre bir şekilde çalışır. Hedefli saldırılara karşı derin profilleme ve proaktif savunma imkanı sağlar.

Temel Ayrıştırıcılar

Kapsamlı Sızıntı Toplama Sistemi

Sızdırılan kimlik bilgileri, finansal veriler, kişisel olarak tanımlanabilir bilgiler (PII) ve kurumsal belgelerin en büyük ve sürekli büyüyen veritabanı. Yeni sızdırılan bilgilerin zamanında tespit edilmesini sağlamak amacıyla düzenli güncellemeler ve genişletmeler yapılmaktadır.

Derin Profil Oluşturma ve Analiz

Sızdırılan içerikleri ilişkilendirme konusundaki gelişmiş yetenek, sızıntıların ve potansiyel hedeflerin kapsamlı profillerinin oluşturulmasına olanak tanır.

Otomatik Kimlik Doğrulama

LeakMAP, sızdırılan kullanıcı adlarını ve parolaları otomatik olarak test edebilir, geçersiz veya hatalı kimlik bilgilerini tespit ederek veritabanından silebilir. Bu sayede ekibinizin doğrulama için harcadığı zaman ve emekten tasarruf ederken gerçek tehditlere odaklanma imkanı bulabilirsiniz.

ETKİSİZ / HATALI KİMLİK BİLGİSİ SIZDIRMASI

OTD BİLİŞİM
GLOBAL VAD

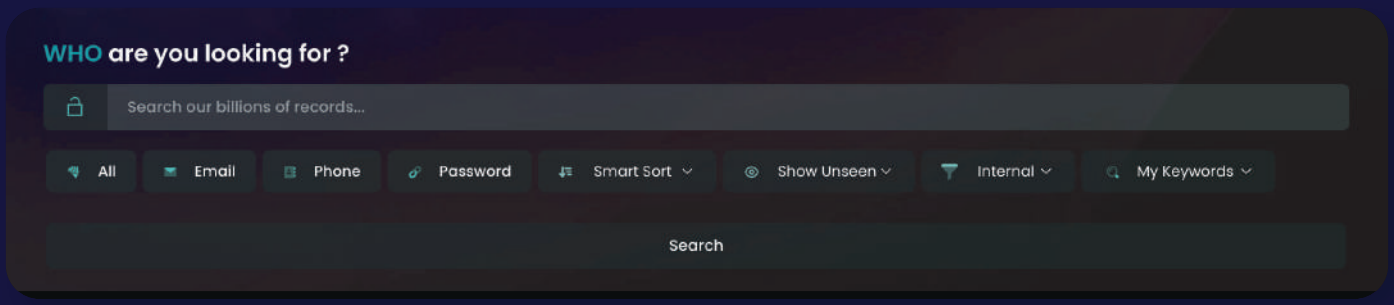
LeakMAP

Gerçek Zamanlı İkazlar ve Bildirimler

LeakMAP, gerçek zamanlı uyarıların yanı sıra, tekrarlayan veri sızıntılarını akıllıca tespit edip filtreleyerek kuruluşunuzun aynı sızıntı için birden fazla kez uyarılmasını engeller, Böylece gereksiz gürültüyü ve yanıt yorgunluğunu azaltır.

Gelişmiş filtrelerle kullanıcı dostu arayüz

Gelişmiş filtreleme seçenekleri sunan kullanıcı dostu arayüz, belirli sızdırılmış verileri hızlı bir şekilde aramanıza imkan tanır. Sonuçlar, tarihe, duruma (görülen/görülmeyen) ve alan türüne göre filtrelenebilir; bu, dışarıya bakan kurumsal varlıklar veya dahili sistemler ve kaynaklar için geçerlidir.



Gizlilik ve Gizlilik Denetimleri

Kuruluşlar, hassas veya stratejik verilere yalnızca yetkili kuruluşların veya personelin erişimini sağlamak amacıyla belirli bilgileri gizli olarak işaretlemeyi tercih edebilirler.

Hedefli Saldırı Algılama için SmartDECEPTIVE ile Entegrasyon Sağlama

Sahte veri yönetimi modülümüzle entegrasyon, sızdırılan verilerin kullanılma girişimlerinin bir uyarıyı tetiklemesini sağlayarak kuruluşlara hedefli saldırılar hakkında erken uyarı sunar.

CATCH PROBE™

INTELLIGENCE TECHNOLOGIES

SMARTDECEPTIVE

OTD BİLİŞİM

GLOBAL VAD

SMARTDECEPTIVE: SALDIRGANLARI GÖRÜNMEZ KILMAK

SMARTDECEPTIVE NASIL İŞLER?

SmartDeceptive teknolojisi, meşru ağ varlıklarını, hizmetlerini veya verilerini taklit etmek amacıyla tasarlanmış aldatma sistemlerinin ve tuzaklarının devreye alınmasını ifade eder. Bu aldatmalar, saldırganları çekmek, onları gerçek sistemlerden uzaklaştırmak ve davranışları hakkında istihbarat toplamak için stratejik bir şekilde konumlandırılır. SmartDeceptive çözümleri, gerçek ağı tehlikeye atmadan saldırganlarla aktif bir şekilde etkileşimde bulunur ve IP adresleri, saldırı yöntemleri, araçlar ve etki alanı adları gibi kritik verileri ele geçirir.

SMARTDECEPTIVE NASIL İŞLER?

• SmartDeceptive ve Tuzaklar: Bu aldatıcılar, cihazlar, sunucular, uç noktalar veya uygulamalar biçiminde ortaya çıkabilir. Gerçekten de varmış gibi görünseler de, saldırganları yanıltmak amacıyla tasarlanmışlardır.

• Saldırganları Etkileyin: Bir saldırgan bir yemle etkileşime geçtiğinde, sistem değerli veriler toplar. taktikler, teknikler ve prosedürler (TTP'ler) hakkında.

• Gerçek Zamanlı İzleme ve Uyarılar: Güvenlik ekipleri, sahte hedefler devreye girdiğinde anında uyarılar alır ve bu durum, tehditleri gerçek zamanlı olarak analiz etme imkanı sunar.

• Veri Toplama ve Analizi: Sistem, IP adresleri ve saldırı vektörleri gibi ayrıntıları yakalayıp kaydeder. ve kullanılan araçlar, kuruluşların düşman davranışlarını analiz ederek savunmalarını güçlendirmelerine olanak tanıyor.

SMARTDECEPTIVE AVANTAJLARI

• Proaktif Savunma:
SmartDeceptive, organizasyonların saldırganları saldırı yaşam döngüsünün başlangıç aşamalarında gerçek varlıklara zarar vermeden önce tespit edin.

• Doğru Tehdit İstihbaratı:
Saldırganlarla doğrudan etkileşimde bulunarak, aldatma teknoloji, tehdit istihbaratını ve müdahale çabalarını güçlendiren son derece özel veriler sunar.

• Düşük Yanlış Pozitif Oranı:
Sahte hedefler, normal ağ trafiği için tasarlanmadığından, bunlarla gerçekleştirilen etkileşimlerin büyük olasılıkla kötü niyetli olması, yanlış pozitifleri en aza indirir.

• Artan Olay Müdahale Verimliliği:
SmartDeceptive, olay müdahale platformlarıyla entegre çalışarak, güvenlik ekiplerine doğrulanmış tehditleri artırır.

NERELERDE UYGULANABİLİR?

• Dahili Ağlar:
Veritabanları gibi hayati iç varlıkları koruyun ve çalışanların kimlik bilgilerini sahte hedefler aracılığıyla ele geçirin.

• Bulut Ortamları:
Sahte hedefler belirleyerek güvenli bulut altyapıları inşa edin. Bulut tabanlı uygulamaları, kapsayıcıları ve sanal makineleri taklit eden.

• IoT Sistemleri:
Kameralar, yazıcılar veya endüstriyel kontrol sistemleri (EKS) gibi bağlı cihazları simüle eden tuzaklar dağıtarak IoT ağlarını güvence altına alın

• Operasyonel Teknoloji (OT):
Endüstriyel ortamlara özgü aldatma tekniklerini kullanarak OT sistemlerini ve kritik altyapıyı (SCADA sistemleri gibi) koruyun.

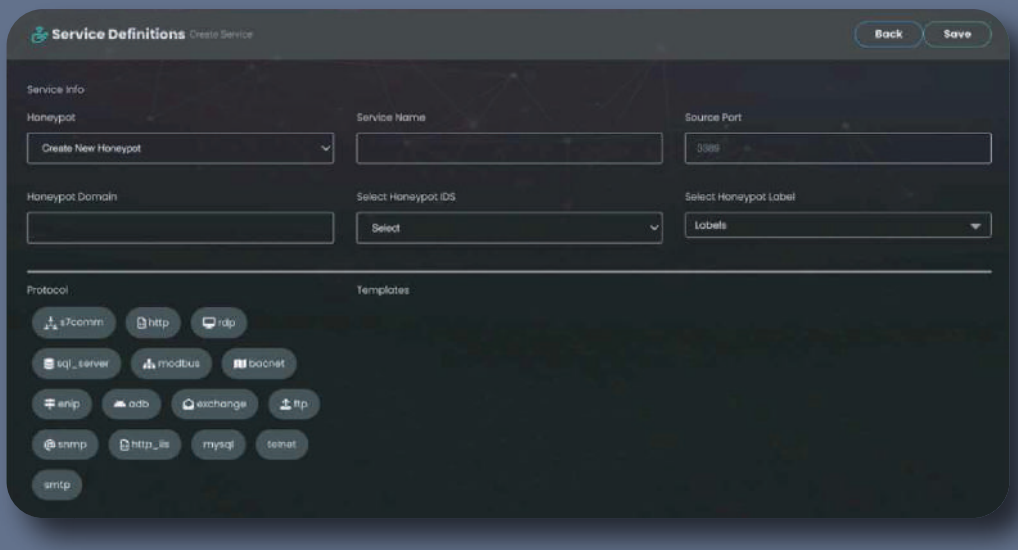
SMARTDECEPTIVE: Gerçek Zamanlı Tehdit İstihbaratı için Aldatıcı Teknoloji

CatchProbe SmartDECEPTIVE, aldatmaca tuzaklarını dağıtmak ve yönetmek, ayrıntılı siber istihbarat toplamak ve saldırgan faaliyetleri gerçek zamanlı olarak izlemek amacıyla tasarlanmış kapsamlı bir aldatma yönetim platformudur. Kuruluşları korumak için eyleme geçirilebilir içgörüler sunmak üzere ThreatWAY ve LeakMAP ile sorunsuz bir entegrasyon sağlar.

Temel Ayrıştırıcılar

Hızlı Teslimat

Dakikalar içinde konuşlandırılabilen sahte hedefler, karmaşık kurulumlar veya kapsamlı yapılandırmalar gerektirmeden hızlı bir savunma sunar.



Platformlar Arası Kurulum

SmartDECEPTIVE, geniş bir protokol ve hizmet yelpazesini desteklemektedir.

DECOY İŞLETİM SİSTEMİ TİPLERİ

Windows	Linux	Android	IoTs, Printers, Ca

UYGULAMALAR | İHTİYAÇLARINIZA GÖRE ÖZELLEŞTİRİLEBİLİR.

Microsoft

- Microsoft Exchange Server
- Microsoft IIS Server
- Microsoft SQL Server
- Microsoft RDP Server
- Microsoft Dynamics AX
- Microsoft Dynamics NAV
- Microsoft Sharepoint

Linux

- HTTP
- SMTP
- FTP
- TELNET-DNS
- SSH
- SMB
- PhpMyAdmin

ICS/SCADA

- Modbus
- S7comm
- ENIP
- BACnet

- Mobile & Android
- Elasticsearch
- SAP
- FORTINET
- CHECKPOINT
- SOLARWINDS
- PASTEBIN
- On-Demand

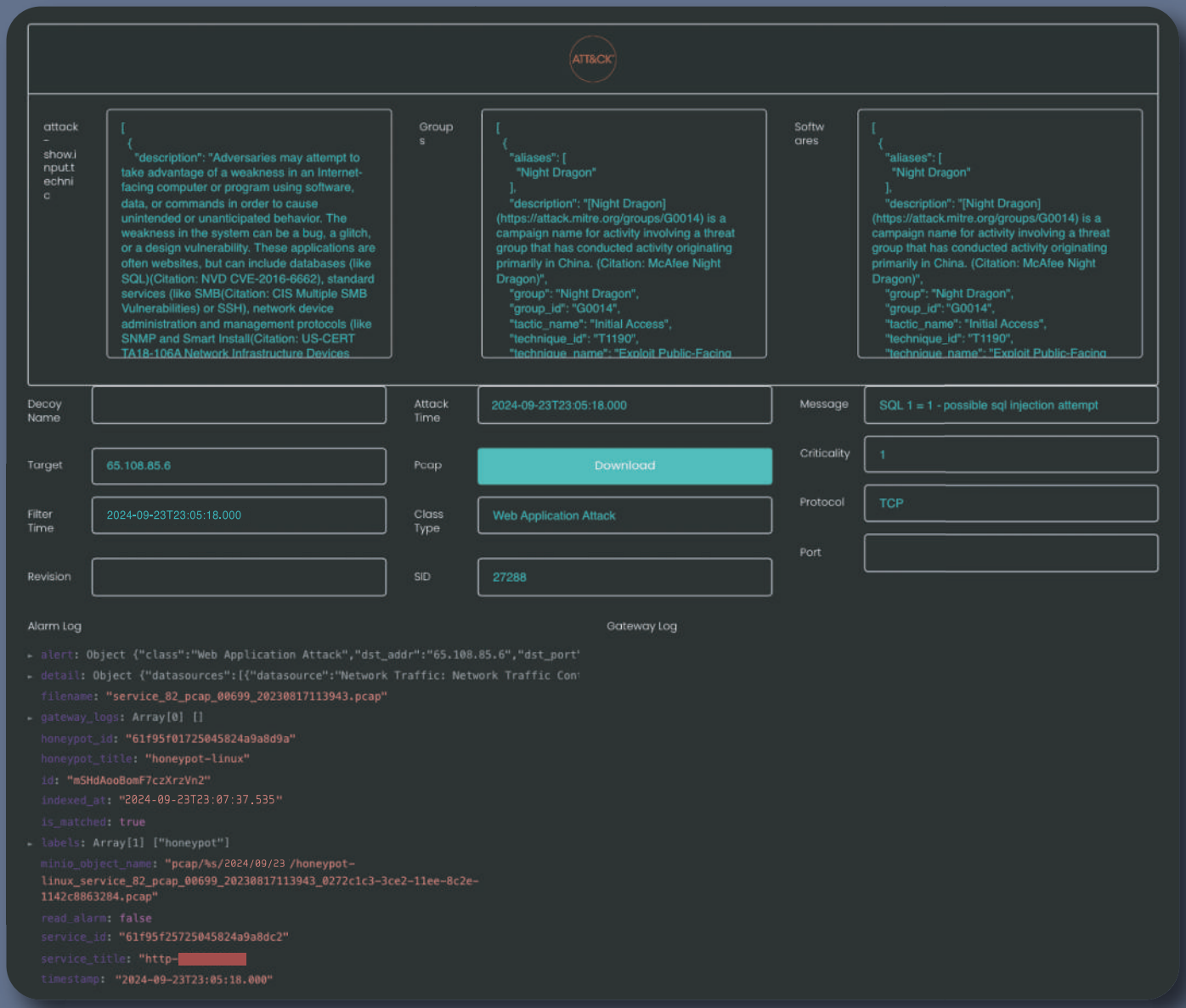
OTD BİLİŞİM
GLOBAL VAD

Maliyet Verimliliği

Ek bir lisanslama veya donanım maliyeti bulunmamaktadır; yemler, bu ortamları simüle etmek amacıyla veritabanı veya uygulama lisansları gibi ek satın alımlar gerektirmez.

Derinlemesine İnceleme

Tam paket yakalama (PCAP) yeteneği ve Mitre Att&ck entegrasyonu ile Smart DECEPTIVE, saldırgan davranışının kapsamlı bir şekilde anlaşılmasını sağlayan detaylı bir analiz sunar.

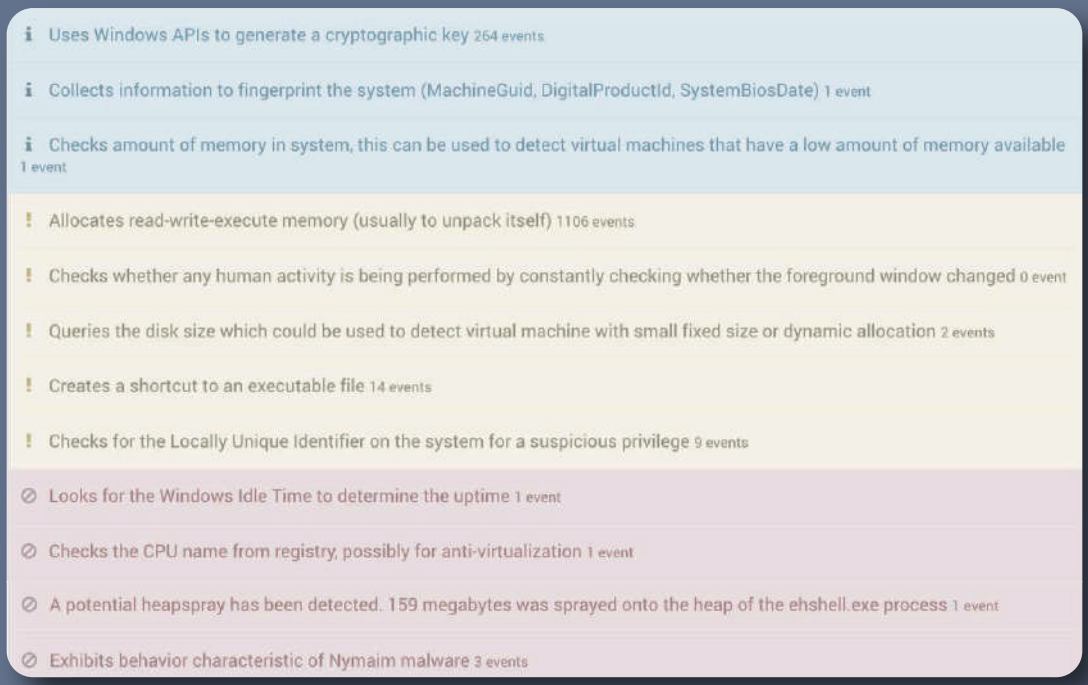


Yapay Zeka ile Hazırlanan Raporlar ve Öneriler

SmartDECEPTIVE, tespit edilen tüm saldırıları analiz eden, savunmaları güçlendirmek ve gelecekteki riskleri azaltmak amacıyla eyleme dönüştürülebilir önerilerle birlikte kapsamlı içgörüler sunan yapay zeka destekli raporlar sağlar.

Kötü Amaçlı Yazılım İncelemesi

Saldırganlar bu tuzaklara kötü niyetli yazılım yükleyerek, müşterilerin kötü niyetli yazılım hakkında kapsamlı analizler almasına olanak tanıyabilir.



Diğer Önemli Nitelikler

- Gerçek Zamanlı Durum İzleme
- Uzun Zamandır Göz Ardı Edilmiş
- Zengin ve Özel Senaryolar
- Hızlı Kurulum
- Tam PCAP Yetenek Özelliği
- Veri Zenginleştirme ve TTP Analizi
- EKS Senaryoları
- Tehdit Profillemesi ve İtibar Derecelendirmesi
- Uyarı ve Raporlama Becerileri
- SandBox'ta Otomatik Kötü Amaçlı Yazılım İncelemesi
- Sömürü, Kötü Amaçlı Yazılım ve Kabuk Kodu Tespiti

Esnek Dağıtım Sistemi

SmartDECEPTIVE tuzakları, şirket içinde veya bulut ortamında konuşlandırılabilir.

ThreatWAY LeakMAP ile Entegrasyon

SmartDECEPTIVE, otomatik olay müdahalesi için ThreatWAY ile entegre olur ve hedefli saldırıları tespit etmek ile sızdırılan verilerin kötü niyetli amaçlarla kullanılma girişimlerini belirlemek için LeakMAP ile iş birliği yapar.

SmartDECEPTIVE

CATCHPROBE™

Decoy Sistemi Nedir?

Bir aldatmaca sistemi, savunmasız sistemleri veya ağları simüle ederek potansiyel saldırganları çekmek ve tuzağa düşürmek amacıyla tasarlanmış bir siber güvenlik mekanizmasıdır. Temel hedefi, saldırganların faaliyetleri hakkında değerli içgörüler sunarak, saldırı girişimlerini tespit etmek, saptırmak veya incelemektir. Aldatma sistemleri, siber suçlulara meşru hedefler gibi görünerek onları aldatmaya teşvik ederken, güvenlik uzmanlarının eylemlerini izlemelerine ve kritik verileri toplamalarına olanak tanır.

Sistem Nasıl İşler?

Bir aldatma sistemi, saldırganları çekmek ve davranışlarını analiz etmek amacıyla savunmasız bir sistemi, ağı veya uygulama ortamını simüle ederek faaliyet gösterir. Sahte hedef, bir sunucu, uygulama, veritabanı veya ağ hizmeti gibi meşru bir hedefe benzer şekilde yapılandırılır. Kullanıcı hesapları, dosyalar veya ağ trafiği gibi gerçekçi ancak sahte verilerle doldurularak, gerçek bir sistem izlenimi yaratılır. Ağ paketleri, oturum açma girişimleri ve diğer etkileşimler dahil olmak üzere gelen ve giden tüm trafiği yakalamak için izleme araçları sahte hedefe entegre edilmiştir.

Bir saldırganın sahte hedef içinde gerçekleştirdiği her eylem, yürütülen komutlar, erişilen veya değiştirilen dosyalar ve bırakılan tüm kötü amaçlı yazılımlar dahil olmak üzere titizlikle kaydedilir. Saldırgan sahte hedefle etkileşime girdiğinde, sistem yöntemlerini ve tekniklerini kaydeder. Düşük etkileşimli sahte hedefler yalnızca temel yanıtları simüle edebilirken, yüksek etkileşimli sahte hedefler daha gerçekçi bir ortam sunar. Aldatma sisteminde tespit edilen şüpheli aktivite hakkında güvenlik personelini bilgilendirmek için gerçek zamanlı uyarılar ayarlanabilir. Toplanan istihbarat, yeni güvenlik açıklarını, kötü amaçlı yazılımları ve saldırı vektörlerini belirlemeye yardımcı olarak genel tehdit istihbaratına katkıda bulunur.

Aldatma Teknolojilerinin Kullanımının Avantajları

Bir kurumsal ağda aldatma teknolojilerini kullanmanın birçok avantajı bulunmaktadır:

Erken Tehdit Algılama: Aldatma sistemleri, kötü niyetli faaliyetleri kritik sistemlere ulaşmadan önce tespit edebilir; geleneksel güvenlik önlemlerini aşabilen sıfırıncı gün istismarları da dahil olmak üzere yeni ve ortaya çıkan tehditleri belirleyebilir.

Tehdit Analizi: Aldatma tuzakları, saldırganların taktikleri, teknikleri ve prosedürleri (TTP'ler) hakkında ayrıntılı bilgiler sunar. Bu davranışları anlamak, kuruluşların daha sağlam savunma stratejileri geliştirmesine ve genel tehdit istihbaratını artırmasına yardımcı olur.

Dikkat Dağıtma ve Aldatma: Tuzaklar, saldırganların dikkatini dağıtarak zamanlarını ve kaynaklarını boşa harcayabilir ve onları gerçek hedeflerden uzaklaştırabilir. Bu sistemler ayrıca kötü niyetli içeridekileri aldatma unsurlarıyla etkileşime girmeye teşvik ederek tespit edebilir.

Verimli Kaynak Tahsisi: Aldatma teknolojileri, güvenlik kaynaklarının daha odaklı bir şekilde tahsis edilmesini sağlayarak çabaları gerçek tehditlere yoğunlaştırır ve geniş, genelleştirilmiş savunmalara olan ihtiyacı azaltır.

Yem Çeşitleri Araştırma Yemleri:

Saldırı kalıplarını, kötü amaçlı yazılım davranışlarını ve yeni istismarları analiz etmek amacıyla kullanılır. Bu tuzaklar toplar.doğrudan savunma yerine araştırma amacıyla istihbarat.
Örnek: Botnet faaliyetlerini izlemek için oluşturulan bir tuzak ağı.
Üretim Tuzakları: Saldırıları erken tespit ederek güvenliği artırmak amacıyla devreye alınır. Gerçek tehditler için bir uyarı sistemi işlevi görürler.
Örnek: Kimlik avı girişimlerini tespit etmek için kurulan bir e-posta sunucusu tuzağı.

SmartDECEPTIVE

CATCHPROBE™

HERHANGİ BİR RİSK MEVCUT MU?

Perspektif	Geleneksel Bal Kavanozları	SmartDECEPTIVE Decoys
Saldırganlar Tarafından Belirlenme	Uzman saldırganlar tarafından tespit edilebilirler.	Son derece etkileşimli, tespit edilmesi neredeyse imkansız.
Saldırıların Artışı	İzole edilmediği takdirde tırmanma riski bulunmaktadır.	Gerçek sistemle etkileşim bulunmamaktadır, tırmanma riski mevcut değildir.
Kaynak İhtiyacı	Önemli kaynaklar talep eder.	Bulut dağıtıldı, kaynak talebi bulunmamaktadır.
Kaynak İhtiyacı	Önemli kaynaklar talep eder.	Bulut dağıtıldı, kaynak talebi bulunmamaktadır.
Yanlış Pozitifler	Yanlış pozitif, yorgunluğa neden olur.	Yapay zeka ile desteklenen saldırı analizi
Performans Problemleri	Ağ performansını etkileyebilir.	Bulut dağıtıldı, ağ performansı üzerinde herhangi bir etkisi yok.
Yanlış Yapılandırma	Yeni güvenlik açıklarının ortaya çıkma olasılığı	Yanlış yapılandırma riski bulunmamaktadır.
Aşırı Bağımlılık Durumu	Sahte hedeflere aşırı güven duyulmasına neden olabilir.	Dayanıklılık amacıyla dört modül içeren bir platformun bileşeni.

SmartDECEPTIVE

CATCHPROBE™

HACKER'IN PERSPEKTİFİNİ ANLAMAK

İlk Keşif: Sana yolumu nasıl bulduğumu göstereyim.

OSINT, SIGINT, HUMINT – hepsi klasiklerdir.

Google? O senin en yakın dostun... ve benim de.
Forumlar mı? Altın madenleridir. Resmi Cisco veya Oracle forumlarından rastgele geliştirici buluşmalarına kadar, içgörülerle doludurlar.

GitHub? Büyük ödül.
Veritabanlarını ve Pastebin'i riske atmak mı? Her ikisi de bilgi paylaşımında son derece cömerttir.

Nmap ve Shodan? Kesinlikle güvenilir dostlarım, ancak açık sistemleri keşfetme konusunda en iyi yardımcılarım.

CVE veritabanı? Her zaman faydalıdır.

Gerçek tehdit istihbaratı beslemeleri? Bazıları değerli, bazıları ise önemsizdir—ancak etkili olanlar oyunun seyrini değiştirebilir.

Bu cephanelikle (ve daha fazlasıyla), "sizin" tam bir portre oluşturmak son derece kolaydır: kim olduğunuz, nerede çalıştığınız, ne yaptığınız ve en önemlisi, bir şeye tıklamanızı veya bir sohbete katılmanızı sağlayacak unsurlar.

İlk Anlaşma: Size bu işe girmenin yollarını göstereyim.

Kimlik avı mı? Klasik bir yöntem. İkna edici bir e-posta ile gelen kutunuza sızacak ve her şeyi teslim etmenizi sağlayacağım.

Sosyal mühendislik mi? Telefonunuz, sohbetiniz veya hatta yüz yüze görüşmeniz aracılığıyla nazik bir dille size ulaşırım; inanın bana, bu oyunu nasıl oynayacağımı biliyorum.

Kimlik Bilgisi Doldurma? Şifrelerinizi tekrar mı kullanıyorsunuz? Harika. Sızdırılan kimlik bilgilerini alıp başka hangi sistemlere erişebileceğimi inceleyeceğim.

Kaba Kuvvet? Şifrelerinizi tahmin etmeye yönelik otomatik araçlarım mevcut—benim için uyku yok.

SmartDECEPTIVE

CATCHPROBE™

Sıfır Gün Saldırıları? Eğer henüz keşfedilmemiş bir güvenlik açığı varsa, bunu sizin aleyhinize kullanacak ilk kişi ben olacağım.

Truva atları mı? Meşru görünüyor, ancak içine kötü niyetli kodlar gizledim ve sizin yüklemenizi bekliyor.

Kimlik Bilgisi Doldurma? Şifrelerinizi tekrar mı kullanıyorsunuz? Harika. Sızdırılan kimlik bilgilerini alıp başka hangi sistemlere erişebileceğimi inceleyeceğim.

Kaba Kuvvet? Şifrelerinizi tahmin etmeye yönelik otomatik araçlarım mevcut—benim için uyku yok.

Fidye yazılımı mı? Dosyalarınızı kilitleyeceğim ve geri alabilmeniz için büyük bir meblağ talep edeceğim - ödemeniz sizin yararınıza olacaktır.

Aracı Adam mı? Eğer halka açık bir Wi-Fi kullanıyorsanız, farkında olmadan yaptığınız her şeyi dinleyebilirim.

SQL Enjeksiyonu nedir? O güvensiz web formları? Bunları veritabanınızın derinliklerine ulaşmak için kullanacağım.

Siteler Arası Komut Dosyası (XSS)? Bir web sayfasını yükleyeceksiniz ve kötü niyetli komut dosyaları, bilgilerinizi çalmak amacıyla yerleştirildi.

Uzaktan Kod Çalıştırma? Sisteminizde bir zafiyet mi tespit ettiniz? Harika, kötü niyetli kodumu uzaktan çalıştırarak kontrolü ele alacağım.

İstismar Kitleri? Zayıflıkları tarayıp otomatik olarak istismar etmek için hazır bir araç setim var - son derece basit.

Hadi canım, hepsini listelemem gerçekten gerekli mi?...

İçeri girdikten sonra yapacağım şey şu: İşletim sistemiymişim gibi davranarak antivirüs taleplerini engelleyeceğim, her yeni makineye bulaştığımda kodumu değiştireceğim ve gizli kalmak için kendimi yürütülebilir dosyaların içine şifreleyeceğim. Polimorfik bir motorla, her bulaşma sırasında kodumun önemli bölümlerini yeniden yazacağım ve eğer hırslı hissediyorsam, tamamen metamorfik hale gelip her hedef için kendimi tamamen yeniden yazacağım. Ardından, ağınızı tarayacak, DNS, DHCP ve sunucuları haritalayacak, ana bilgisayarlar arasındaki rotaları izleyecek ve MAC adreslerini kontrol edeceğim. Ayrıca bağlantılar için Netstat'ı ve adlar ile IP'ler için NBTStat'ı inceleyeceğim. Bunu yaptıktan sonra, tam olarak neyle karşı karşıya olduğumu görmek için DNS adlarını, NetBIOS adlarını, kullanıcı hesaplarını, MAC adreslerini, ağ bağdaştırıcılarını, paylaşımları ve hizmetleri sıralayacağım. Artık manzarayı bildiğime göre, bir sonraki hamlemi yapmak için tüm bu bilgileri kullanabilirim.

SmartDECEPTIVE

CATCHPROBE™

Uzlaşma: Bizi Durdurmak İçin Ne Yapabilirdiniz?

Güvenlik duvarları mı? Elbette, harikadırlar—tabii ki IoC'lerle aşırı yüklenmediğiniz sürece. (Hey... siz, evet siz, değerli müşterim, ThreatWAY'in alakasız IoC'leri filtrelediğini ve riskleri puanladığını bilmiyor musunuz? Böylece güvenlik duvarınız sizi bunaltmıyor!)

IDS/IPS? Baypass edildi. Alarmları devreye sokmadan nasıl geçeceğimizi biliyoruz.

DLP? Bir portu açık bıraktınız, değil mi? Verileri hemen aktaracağız. (RiskRoute'un o açık portları anında işaretleyeceğini bilselerdi!)

Derin Paket İncelemesi mi? Evet, 2012'den beri bunu atlatıyoruz.

Yamalar? Tüm satıcılarınızın güvenlik açıklarını izliyor musunuz? Sanırım bunu yapmıyorsunuz... (Şşş... DarkMAP bu konuda sizi koruyor.)

Antivirüs mü? Tebrikler, %3-7'lik etkinlik için—ah, ve zaten yarısının devre dışı bırakıldığı biliniyor.

SIEM? Yüklü mü? Harika. Ne yazık ki ekibiniz uyarılarda boğuluyor. (Evet... ThreatWAY ile değil—bunu küçük bir sır olarak saklayalım.)

Politikalar ve Prosedürler? Belki, eğer hepiniz bu konularda uzlaşabilir ve uygulama hususunda anlaşmazlık yaşamazsanız.

Gerçek şu ki, her zaman %100 kazanmanız gerekmektedir. Sadece bir kez şanslı olmamız yeterlidir.

Bu, güvenlik teknolojilerinizin güncelliğini yitirdiğini ifade etmekle ilgili değildir. Bu durum karmaşıktır, ancak çözümün yalnızca bir parçasını temsil eder. Son 20 yıldır güvenlik önlemeye odaklanılmıştır ve siber savaşı kazanmış değilsiniz. Şimdi, SaaS, IoT, BYOD, Bulut, V2V ve V2X ile çevreniz neredeyse gözenekli bir hale gelmiştir. Bu gelişen ortama uyum sağlayan akıllı ve tasarıma uygun çözümlere ihtiyacınız vardır. Tehdit modellerini ve niyetlerini tespit ederek saldırıları öngören çözümler; yemler, web istihbaratı, OSINT ve saldırganları anlamadan önce kavrayabilmek için eyleme geçirilebilir içgörüler gibi araçlar kullanır. Artık önleme tek başına yeterli olmayacaktır.

RISKROUTE: SALDIRI YÜZEYİ YÖNETİMİ

KURULUŞLARIN KARŞILAŞTIĞI TEMEL SORUNLAR

- Dinamik Tehditler: Siber suçlular, sürekli olarak açık portlar, güncel olmayan yazılımlar veya güvenli olmayan alanlar gibi göz ardı edilen giriş noktalarını hedef alırlar.
- Karmaşık Altyapı: Modern işletmeler genellikle bulut ortamlarının bir kombinasyonunu içerir ve bu durum, varlıkların yönetimini daha karmaşık hale getirir.
- Görünürlük Eksikliği: Tüm dışa dönük varlıkların izlenmesi ve anlaşılması konusundaki yetersizlik, Bilinmeyen risklere karşı savunmasız olan kuruluşlar.
- Uyumluluk ve Risk Yönetimi: Düzenleyici çerçeveler, güvenlik uyumluluğunu temin etmek amacıyla genellikle tüm varlıkların, sertifikaların ve güvenlik açıklarının titizlikle denetlenmesini zorunlu kılar.

OTD BİLİŞİM
GLOBAL VAD

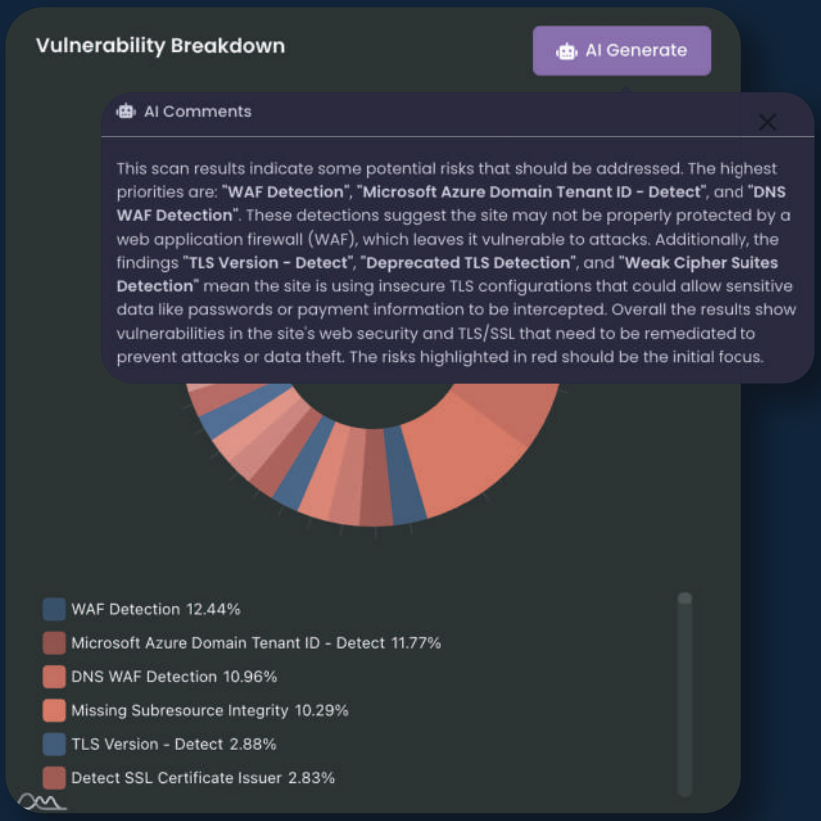
RiskROUTE: Dijital Haritanızın Her Aşaması İçin Proaktif Güvenlik

CatchProbe RiskRoute, dijital ortamınızda sürekli görünürlük ve kontrol sağlayarak kuruluşunuzun dijital varlıklarını korumak amacıyla tasarlanmış kapsamlı bir araç seti sunar. Gelişmiş yetenekleri, güvenlik ekiplerinin kritik sistemleri izlemelerini, yönetmelerini ve güvenliğini sağlamalarını, güvenlik açıklarını tespit etmelerini, varlık sağlığını izlemelerini ve olası tehditlere karşı proaktif bir şekilde savunmalarını mümkün kılarak veri ihlalleri ve siber saldırı riskini azaltır.

Temel Ayrıştırıcılar

Yapay Zeka Tabanlı Analiz ve Düzeltme Önerileri

RiskRoute, her bulguyu analiz etmek için yapay zekayı kullanarak tespitin ötesine geçer, sorunun doğası hakkında kapsamlı bilgiler sunar ve özel düzeltme adımları önerir.



Gerçek Zamanlı Tehdit Tespiti ve Yönetimi

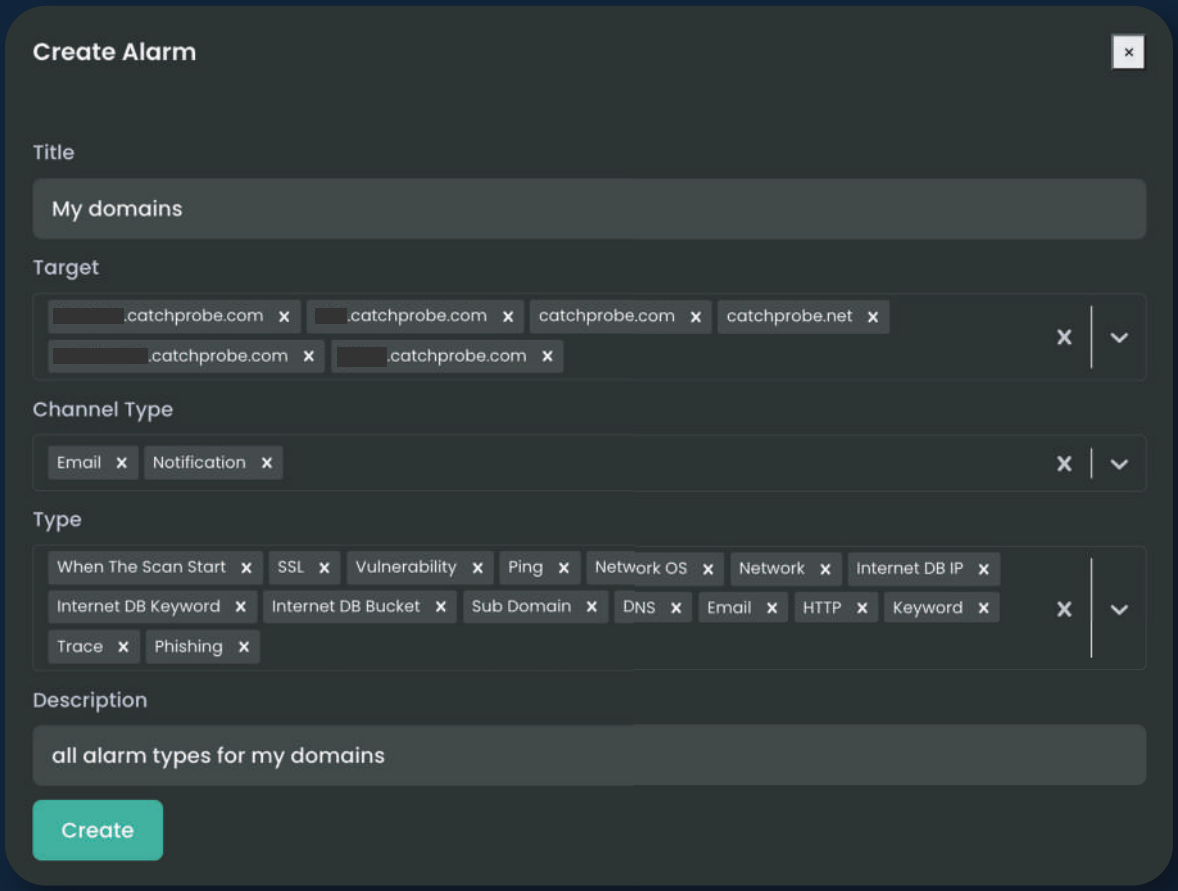
Gerçek zamanlı uyarılarla güvenlik açıklarını, sertifika bilgilerini, yanlış yapılandırmaları, kimlik avı sitelerini, HTTP bilgilerini, DNS verilerini, alt alan adı keşfini ve detaylarını, port tarayıcı sonuçlarını, işletim sistemi bilgilerini, ağ verilerini, ping sonuçlarını, traceroute detaylarını ve daha fazlasını sürekli olarak izleyin.

Kapsamlı Varlık Şeffaflığı

Portlardan ve etki alanlarından sertifikalara ve geçmiş verilere kadar dijital varlıklarınıza tam görünürlük elde edin. RiskRoute, hiçbir varlığın veya potansiyel güvenlik açığının göz ardı edilmemesini garanti eder.

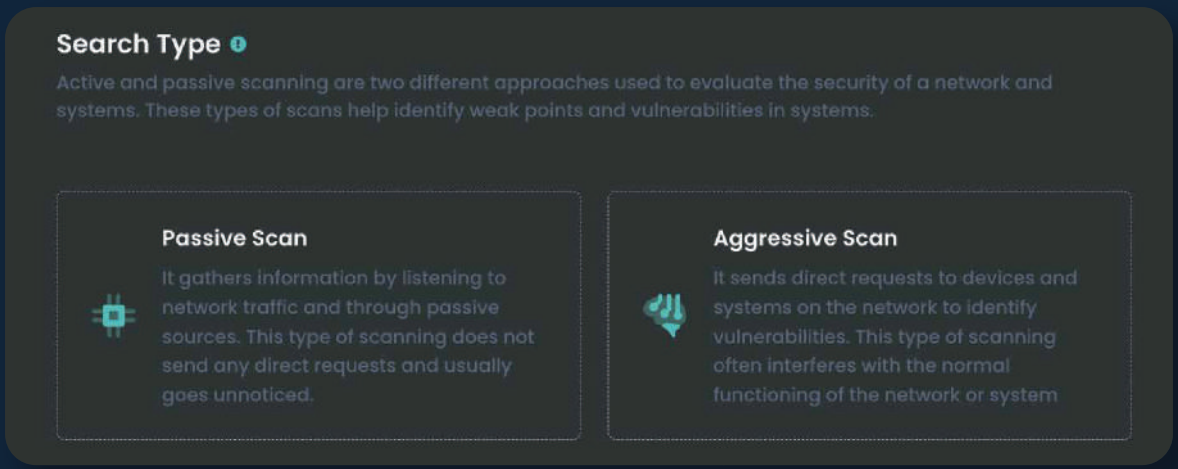
Etkin Olay Yönetimi

Güvenlik açıkları tespit edildiğinde, yanıt verme hızı o kadar önemlidir. RiskRoute, Jira, Webhook ve e-posta entegrasyonları aracılığıyla otomatik uyarılar oluşturur ve ekiplerin tehditleri hızlı bir şekilde ele almasını ve yanıt sürelerini azaltmasını sağlar.



Etkin Olay Yönetimi

Pasif tarama sistemlere doğrudan istek iletmez, bu sayede fark edilmeden devam edebilir ve düzenli ağ operasyonlarına müdahale etme riskini en aza indirir; agresif tarama ise güvenlik açıklarını tespit etmek amacıyla cihazlara ve sistemlere doğrudan istekler gönderir. Daha müdahaleci olmasına rağmen, olası zayıflıkların derinlemesine analizini sağlar.



TEHDİT YOLU; TEHDİT İSTİHBARATINI AZAMİ DÜZEYE ÇIKARMA

GELENEKSEL CTI TOPLANTISI

Çoklu Veri Kaynakları: OSINT, tescilli beslemeler, kapalı forumlar ve devlet veritabanlarından toplanmaktadır.

Yüksek Maliyetler: Kuruluşlar genellikle birden fazla besleme için ödeme yapmakta ve bu durum gereksiz masraflara yol açmaktadır.

Analiz: Yanlış pozitifleri filtrelemek ve gerçek tehditlere öncelik vermek için zaman alıcı süreçler gerekmektedir.

ALTYAPI YÖNETİMİNDEKİ ZORLUKLAR

Güvenlik Duvarı Aşırı Yüklenmesi: Büyük miktarda ham veri, güvenlik duvarlarının kapasite sınırlarına ulaşmasına ve operasyonel maliyetlerin artmasına yol açabilir.

Altyapı Zorlanması: İşlenmemiş IoC'lerin işlenmesi, kaynakları zorlayarak yavaşlamalara neden olabilir veya maliyetli yükseltmeler gerektirebilir.

Genel Tehdit Listeleri: Birçok geleneksel çözüm, alakasız uyarılara ve yorgunluğa yol açan genel IoC'ler sunmaktadır.

GELENEKSEL CTI ÇÖZÜMLERİNİN SINIRLILIKLARI

Veri Aşırı Yüklenmesi: Sistemleri alakasız veya düşük öncelikli uyarılarla doldurarak verimsizliğe yol açar.

Parçalanmış Araçlar: Farklı sistemlerin entegrasyonunu gerektirir ve veri normalizasyonunu ile paylaşımını karmaşıklaştırır.

Yavaş Olay Yanıtı: Manuel işleme, tehdit yanıtını geciktirir ve saldırıların potansiyel etkisini artırır.

OTD BİLİŞİM
GLOBAL VAD

ThreatWAY
Threat Intelligence Exchange

ThreatWAY, işletmelerin kötü amaçlı faaliyetleri proaktif bir şekilde tespit edip engellemesini sağlayan ve aynı zamanda gerçek zamanlı tehdit paylaşımını kolaylaştıran bir erken uyarı sistemi görevi görür.

Özellikler:

- Saldırıları araştırarak ve otomatik olay yanıt yeteneklerini kolaylaştırarak proaktif içgörüler sunar.
- CatchProbe'un tuzaklarından ve hem açık hem de kapalı kaynaklarla API entegrasyonundan ve tarama işlemlerinden kaynaklanan açığa çıkan saldırılardan elde edilen verileri gerçek zamanlı olarak toplar ve yayar.
- Elde edilen verileri dağıtır ve kullanıcıların bunları milisaniyeler içinde kendi kuruluşları arasında paylaşmalarını sağlar.

TEHLİKEYİ YÖNET

KORUMA ETKİNLEŞTİR

DİJİTAL ADLİ TIP

GERÇEK ZAMANLI ZEKÂ

Genel Değerlendirme

Dinamik Kanal ve Toplama Yönetimi

Binlerce honeypot'tan gelen hedefli saldırı verileri

Açık ve kapalı platformlarla API entegrasyonu

Yeni kayıtlı alan adı adreslerinin toplanması

Otomatik Veri Normalizasyonu

Gerçek Zamanlı Uyarılar: Olası tehditler hakkında gerçek zamanlı uyarılar alın

Özelleştirilebilir Veri Kaynakları: Gerektiğinde veri kaynakları ekleyin ve kaldırın.

API Desteği: Mevcut Güvenlik Duvarlarınız ve SIEM'lerinizle kolayca entegre edin.

Tehdit İstihbaratı İtibar Sıralaması

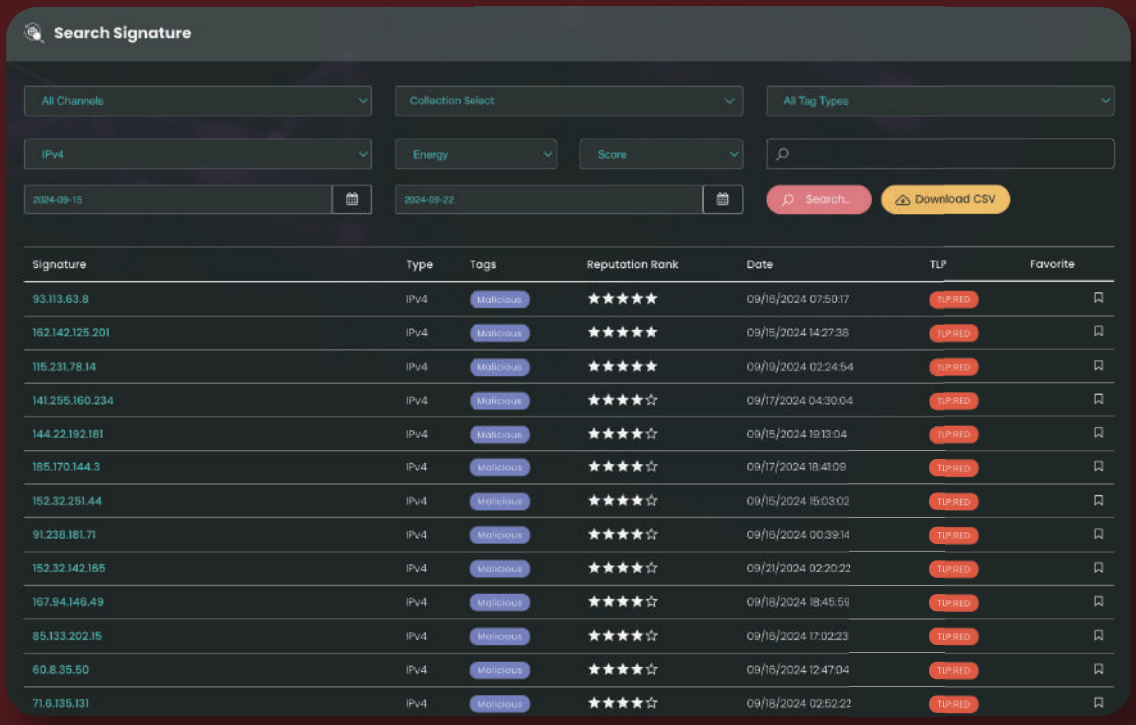
OTD BİLİŞİM
GLOBAL VAD

ThreatWAY: Gerçek Zamanlı CTI Ekosisteminize Kesintisiz Bir Şekilde Entegre Olur

Temel Ayrıştırıcılar

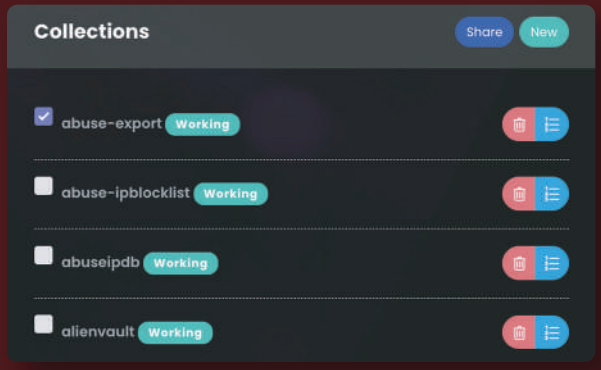
Öncelikle Kritik Tehditler: En Önemli Noktada Odaklı Koruma

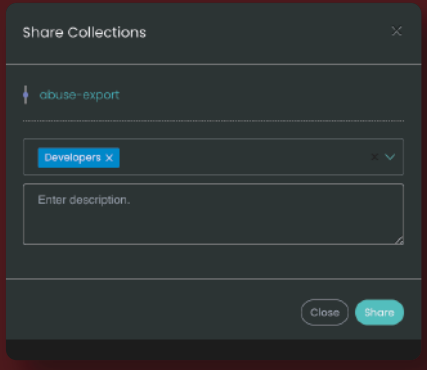
ThreatWAY, tehditleri analiz eder ve öncelik sırasına koyarak kuruluşunuzun en kritik risklere odaklanmasını sağlar. ThreatWAY, IoC'leri alaka düzeyleri ve potansiyel etkilerine göre sıralayarak, belirli ortamınız için en büyük tehlikeyi oluşturan tehditleri belirlemenize yardımcı olur, gürültüyü azaltır ve düşük riskli veya alakasız verilerden kaynaklanan dikkat dağıtıcı unsurları en aza indirir.



Otomatik Veri Toplama ve Paylaşımı

ThreatWAY'in altyapısı, işletmelerin yalnızca arama yapmalarını değil, aynı zamanda milisaniyeler içinde kurum içi ve kurumlar arası kanallarda rafine istihbarat paylaşımını da mümkün kılar.



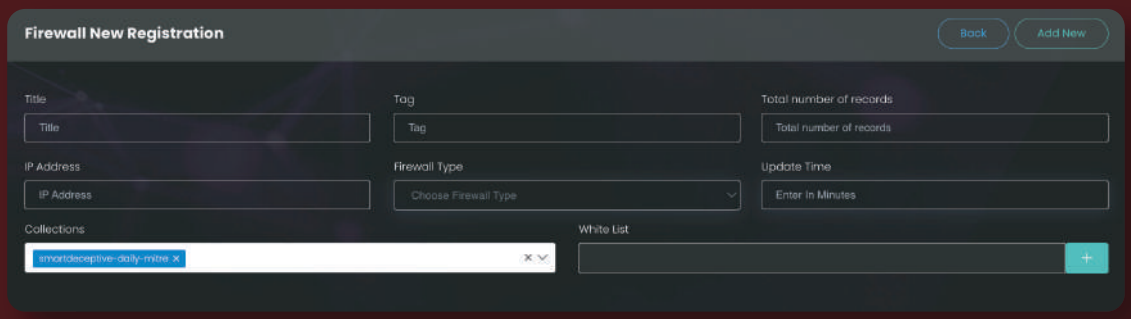


OTD BİLİŞİM
GLOBAL VAD

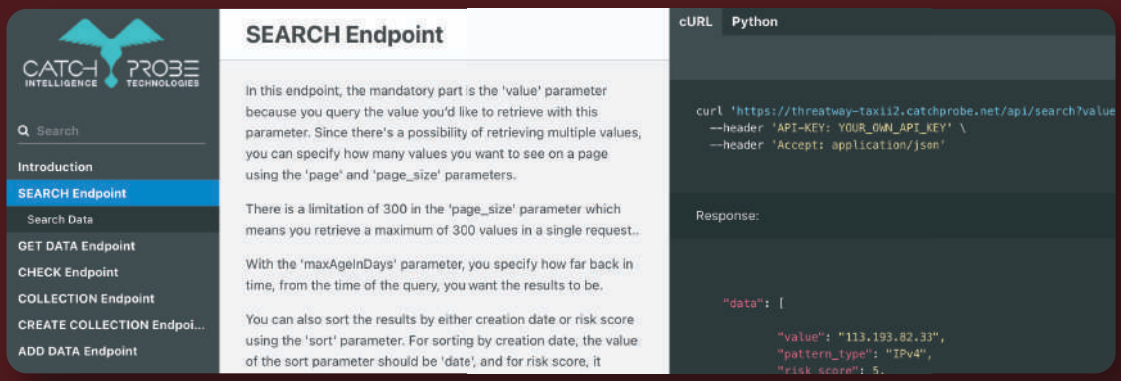
Zahmetsiz Entegrasyon, Anlık Eylem

ThreatWAY, işletmelere doğrulanmış Tehlike Göstergelerini (loC'ler) doğrudan güvenlik duvarlarına, SIEM sistemlerine ve SOAR platformlarına sorunsuz bir şekilde sunarak güç kazandırır. İster bir REST API aracılığıyla, ister özel kurallar kullanılarak doğrudan entegrasyon yoluyla olsun, ThreatWAY, tehdit istihbaratının mevcut güvenlik altyapınız içinde hızla eyleme dönüştürülebilir olmasını temin eder.

Option #1

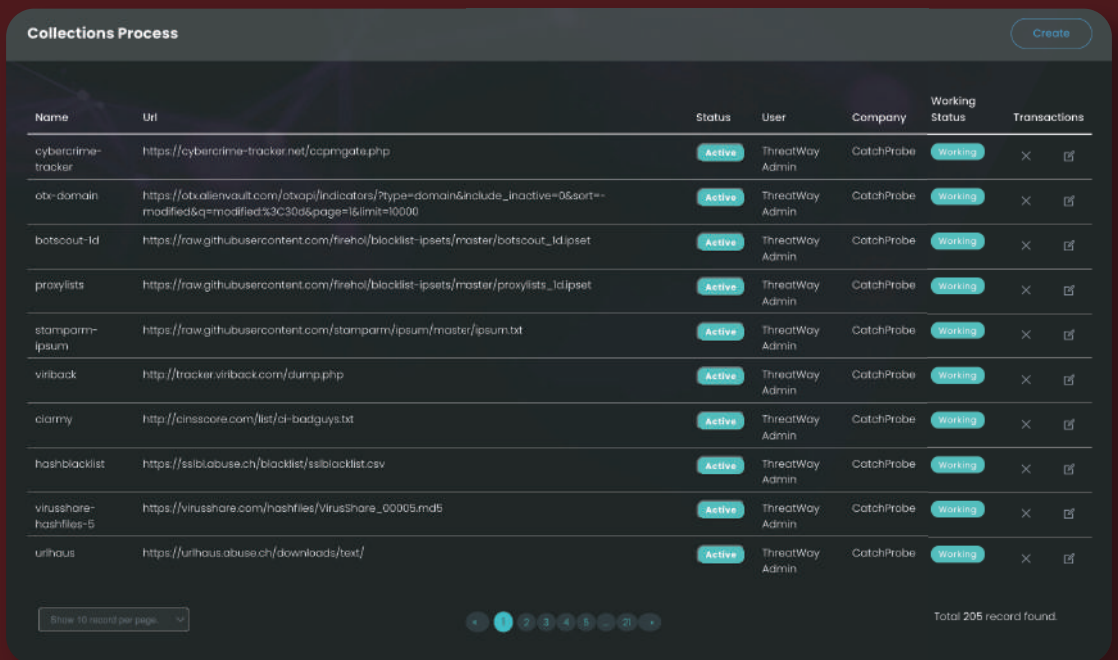


Option #2



Özelleştirilebilir Veri Kaynakları

ThreatWAY, DarkMAP'in gelişmiş tarama işlemleri ve SmartDECEPTIVE'in tuzakları ile açığa çıkan saldırılarıyla birlikte API aracılığıyla 200'den fazla platformun kusursuz entegrasyonunu sağlarken, aynı zamanda gerçek zamanlı olarak özel ihtiyaçlarınız için yalnızca en ilgili istihbaratın mevcut olmasını temin etmek amacıyla özelleştirilmiş veri kaynaklarını kolayca ekleyip kaldırmanıza olanak tanır.



OTD BİLİŞİM
GLOBAL VAD

CATCHPROBE'UN ENTEGRASYON YETENEKLERİ

Kusursuz bir şekilde entegre edilmiş modüllerin geliştirilmesiyle, eşsiz ve birleşik bir ekosistem oluşturduk. Bu, her biri diğerlerinin yeteneklerini tamamlayan ve geliştiren özel bir amaca sahip, birbiriyle bağlantılı modüllerden oluşan kapsamlı bir paket sunmamıza olanak tanır.

1 **SmartDECEPTIVE ile saldırganları yanıltın.**

SMARTDECEPTIVE, saldırganları etkili bir şekilde yanıltan özgün yanıtlar üreterek sistemlerinizi korurken, saldırganlar hakkında bilgi sağlar ve eylemlerinin güvenli bir şekilde izlenmesine olanak tanır.

SMARTDECEPTIVE
ALDATMA YÖNETİMİ VE ANALİZİ

2 **LeakMAP ile Analiz ve Profil Geliştirme**

SMARTDECEPTIVE, yapılandırılmış saldırıları tespit etmek için LeakMAP ile entegre olur. Bu, bir saldırganın sızdırılmış kimlik bilgilerini kullanarak bir sisteme erişim sağlamaya çalıştığı durumları ifade eder. Çünkü çoğu durumda, bu saldırılar belirli bir bireysel port taramasına yönelik değildir. Bu nedenle, yapılandırılmış saldırılar daha az sıklıkta gerçekleşse de, potansiyel olarak daha tehlikelidirler.

LEAKMAP

Saldırganları ThreatWAY ile durdurun.

F SMARTDECEPTIVE, yapılandırılmış saldırıları tespit etmek amacıyla LeakMAP ile entegre olmaktadır. Bu, bir saldırganın sızdırılmış kimlik bilgilerini kullanarak bir sisteme erişim sağlamaya çalıştığı durumları ifade eder. Zira çoğu durumda, bu saldırılar belirli bir bireysel port taramasına odaklanmamaktadır. Bu nedenle, yapılandırılmış saldırılar daha az sıklıkta gerçekleşse de, potansiyel olarak daha tehlikeli olma özelliği taşımaktadırlar.

THREATWAY
TEHDİT İSTİHBARATI DÖNÜŞÜM PLATFORUMU

1 **DarkMAP, loC'leri ThreatWAY'e iletir.**

ThreatWAY, SmartDECEPTIVE'in açığa çıkan saldırılarından ve açık ile kapalı kaynaklarla API entegrasyonlarından elde edilen verileri yakalamanın yanı sıra, DarkMAP'in tarama operasyonları aracılığıyla sağlanan gerçek zamanlı loC (Uzlaşma Göstergeleri) bilgilerinden de faydalanır.

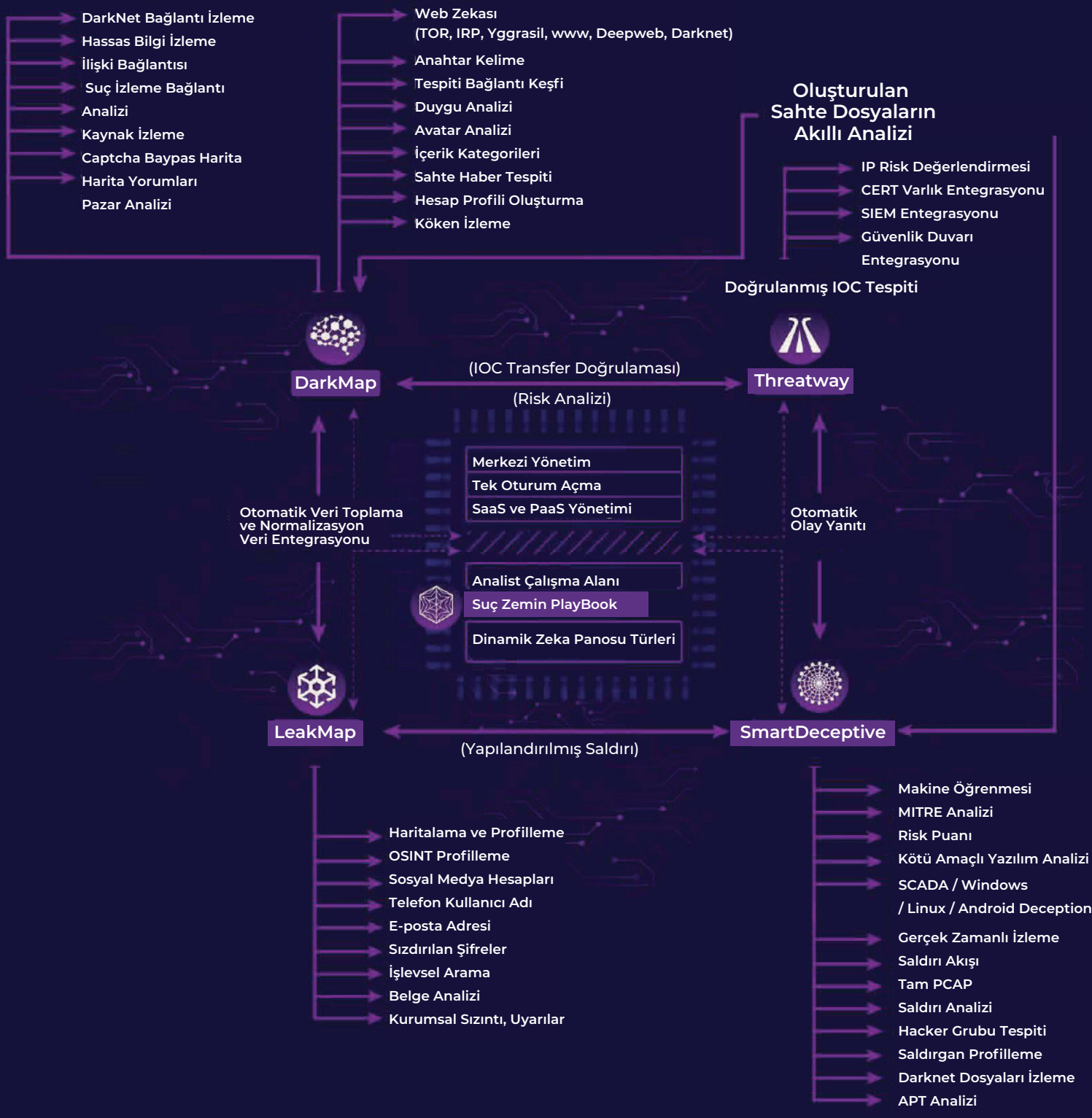
DARKMAP
WEB ZEKASI

CATCHPROBE™

OTD BİLİŞİM
GLOBAL VAD

CATCHPROBE EYLEMİ GERÇEKLEŞTİRİLEBİLİR İSTİHBARAT ORKESTRASYON MİMARİSİ

Merkezi Hepsi Bir Arada Siber ve Dijital Zeka Seti



CATCH PROBE™

OTD BİLİŞİM
GLOBAL VAD

CATCH PROBE™

OTD BİLİŞİM

GLOBAL VAD