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.

AÇIĞA ÇIKMIŞ KİMLİK BİLGİLERİNİ BUL

İSTİHBARAT TOPLA

KİMLİK BİLGİSİ DOLDURMA SALDIRILARINI ÖNLE

İHLALLERİ TAKİP ET

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.

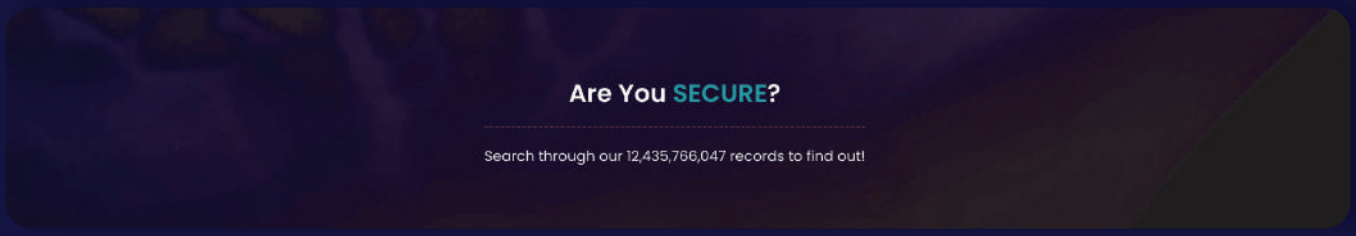
LEAKMAP: Veri İhlallerini Titizlikle Yönetmek

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

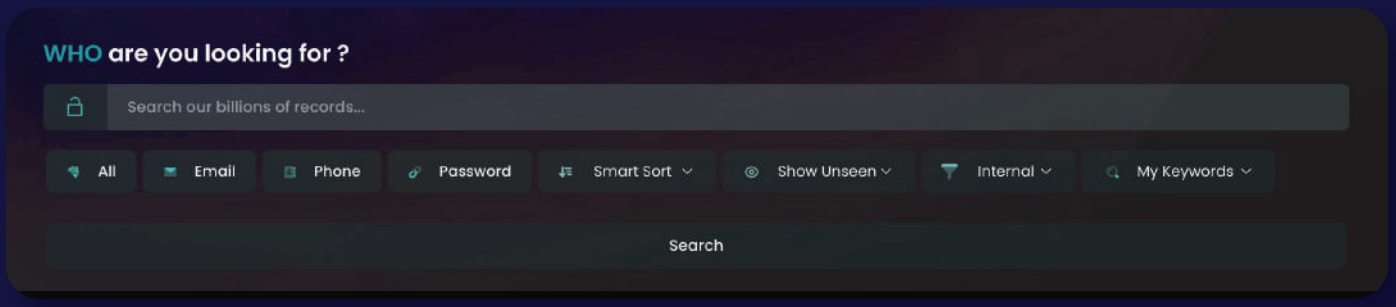
LeakMAP

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.