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 BAKIŞ AÇISIYLA DEĞERLENDİRİN

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, veri tabanlarından veya şifreli ortamlardan veri elde etme.

ELDE EDİLEN BİLGİ TÜRÜ

- Kurumsal ve devlet veri tabanları
- 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.

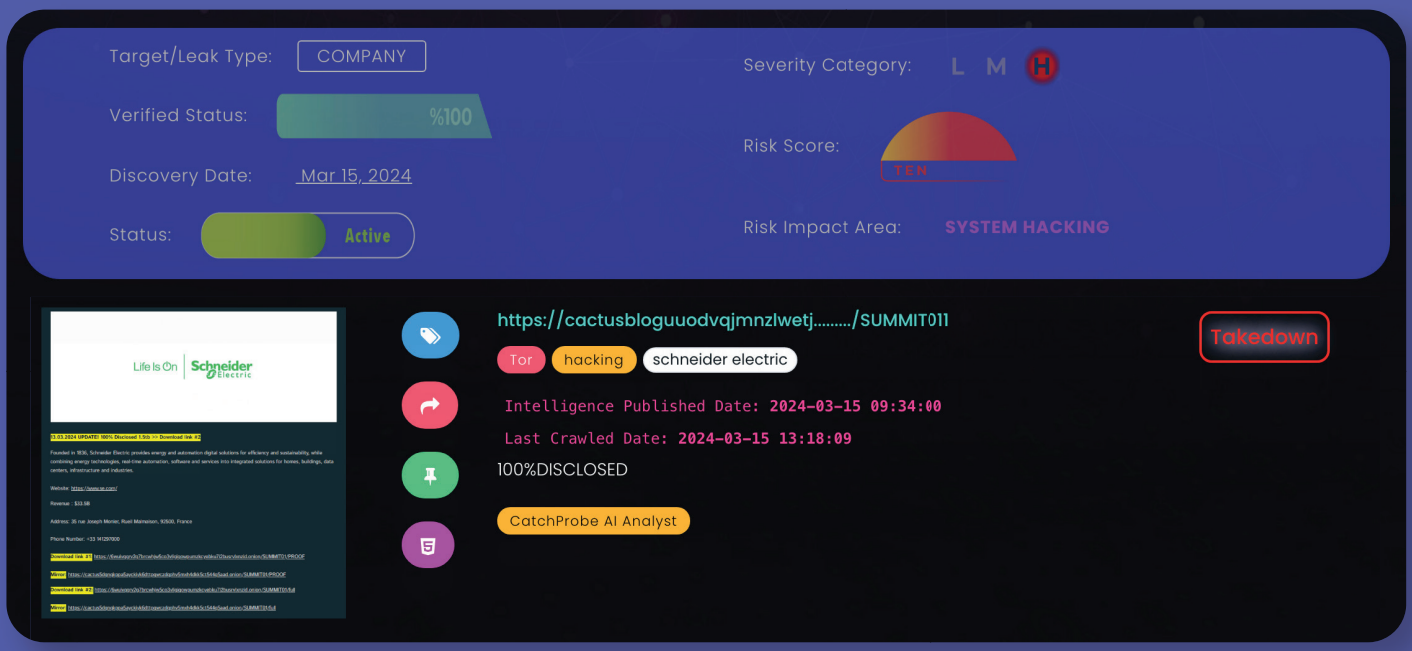
DARKMAP: Yapay Zekâ ve Yeni Nesil Yeteneklerle Web İstihbaratını Yeniden Tanımlama

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

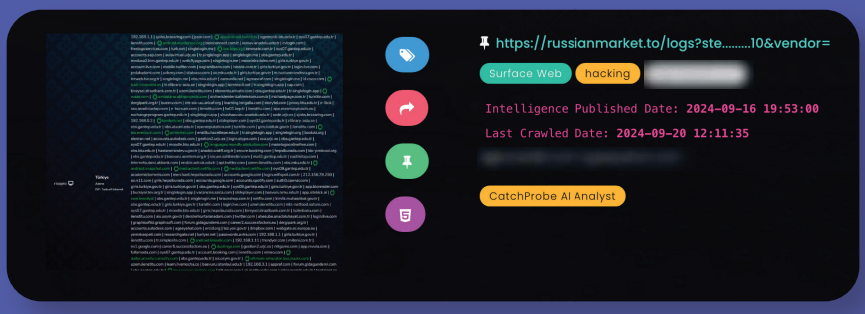
Yapay Zekâ Tabanlı Değerlendirme:

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:

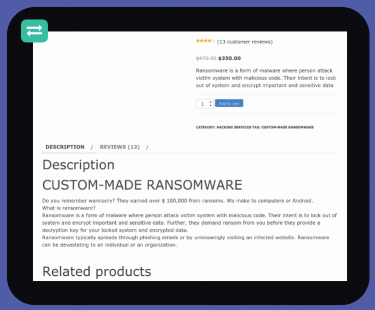
Üyelik gerektiren veya erişimi kısıtlı platformları yönetebilme kabiliyeti sayesinde, DarkMAP web'in tüm katmanlarında tam veri erişimi sağlar.



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

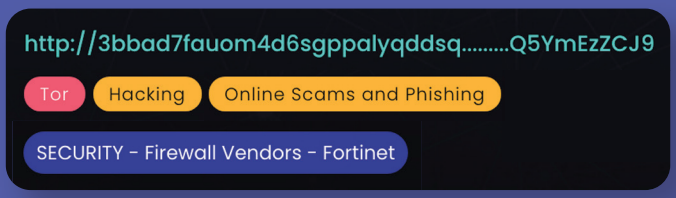
DarkMAP

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.



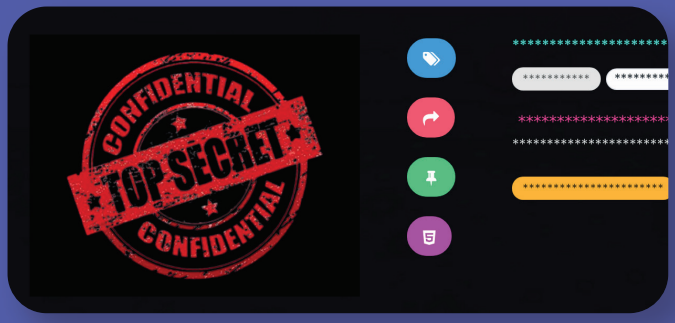
Otomatik ve Manuel Raporlama

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