OTD BİLİŞİM
GLOBAL VAD

Outpost24

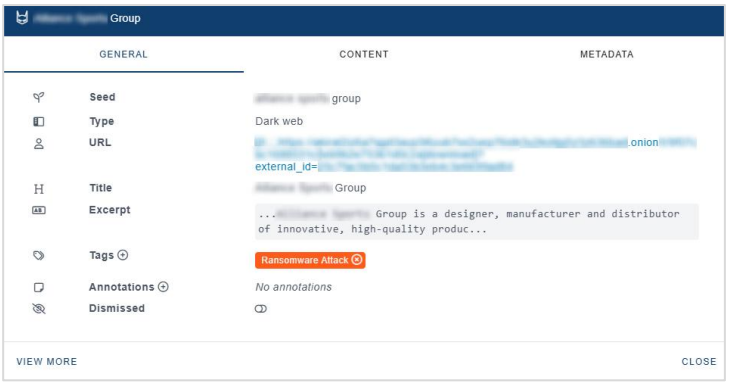
Digital Risk Protection

Dijital varlıklarınızı korumak ve saldırganların planlarını harekete geçmeden önce anlamak için gelişmiş Siber Tehdit İstihbaratından yararlanın.

Günümüzün siber tehdit ortamı her geçen gün daha karmaşık ve öngörülemez hale geliyor. Tehdit aktörleri, kuruluşları hedef almak için giderek daha gelişmiş saldırı teknikleri kullanırken, çevrimiçi faaliyet gösteren her kurum; finansal verilerden müşteri kişisel bilgilerine (PII), kurumsal varlıklardan fikri mülkiyete kadar değerli dijital varlıklarını korumak zorundadır. Bu kritik varlıklara yönelik başarılı bir saldırı; veri ihlalleri, operasyonel kesintiler, itibar kaybı ve uyumluluk yaptırımları gibi ciddi sonuçlara yol açabilir.

Outpost24 Digital Risk Protection (DRP), işletmenizi hedef alan dış tehditleri proaktif olarak tespit etmenize ve önlemenize yardımcı olur. Piyasadaki en geniş dijital risk kapsamını sunan çözüm, olay müdahale süreçlerini güçlendiren aksiyona dönüştürülebilir tehdit istihbaratı sağlar. Bulut tabanlı platformu sayesinde hızlı kurulum ve anlık görünürlük sunarken, güvenlik ekiplerine otomatik, operasyonel, taktiksel ve stratejik tehdit istihbaratını tek merkezden yönetebilecekleri kapsamlı bir kontrol noktası kazandırır.

Sızdırılmış Kimlik Bilgileri



Dark Web'de Tespit Edilen Ransomware Bulguları

Temel Ürün Özellikleri

- 13 yılı aşkın geçmişe sahip tehdit verisi arşivi
- Açık, kapalı ve özel kaynaklardan kapsamlı tehdit verisi toplama
- Doğrulanmış terabaytlarca tehdit verisi sağlayan kurum içi Siber Tehdit İstihbaratı araştırma ekibi
- Bağlamsal analiz ve detaylı içgörüler sunan büyük veri analitiği
- SIEM, SOAR ve TIP platformları için hazır entegrasyon eklentileri
- MSSP programları dahil farklı iş ortaklığı modellerini destekleyen esnek lisanslama yapısı
- Cyber Threat Alliance (CTA) ile devam eden stratejik iş birliği

Siber Tehdit Ortamında Size Rehberlik Ediyoruz

- Kuruluşunuzu kimler hedef alıyor ve bu tehditler nereden kaynaklanıyor?
- Dark Web'deki dijital görünürlüğünüzün farkında mısınız?
- Kurumsal ağınız hangi yöntemlerle ihlal edilmiş olabilir?
- Markanızı veya üst düzey yöneticilerinizi (VIP) kimler taklit ediyor?
- Hassas verileriniz sızdırıldı mı?
- Kimlik bilgileriniz ele geçirildi mi ve dolandırıcılık amacıyla kullanılıyor mu?
- Bir veri ihlali yaşanması durumunda karşılaşabileceğiniz uyumluluk ve yasal yükümlülükleri biliyor musunuz?

Dijital Risk Koruması Hakkında

Dark Web

Siber tehdit ekosisteminde yaşanan gelişmeleri yakından takip edin, kuruluşunuzu hedef alan kötü niyetli faaliyetleri gerçek zamanlı olarak izleyin ve gelecekteki saldırıları proaktif şekilde önleyin. Tehdit aktörleri hakkında daha kapsamlı bilgi edinerek güvenlik ekiplerinize stratejik bir avantaj kazandırın. Potansiyel saldırıları önceden öngörün, etkili karşı önlemler geliştirin ve kuruluşunuzun siber dayanıklılığını güçlendirin.

Sızdırılmış Kimlik Bilgileri

Sızdırılmış, çalınmış veya satışa sunulmuş kimlik bilgilerine ilişkin aksiyona dönüştürülebilir tehdit istihbaratı elde edin. Outpost24, açık web, derin web ve Dark Web kaynaklarını gerçek zamanlı olarak izleyerek ele geçirilmiş kimlik bilgilerini ve bunların çalınmasında kullanılan ilgili zararlı yazılımları tespit eder. Sinkhole, Honeypot, web tarayıcıları (Crawlers) ve gelişmiş sensörlerden oluşan küresel tehdit istihbaratı altyapısı sayesinde veri sızıntıları, yeraltı forumları ve hedefli zararlı yazılım faaliyetleri sürekli izlenir.

Veri Sızıntıları

Kuruluşunuza ait hassas belgelerin, kaynak kodlarının ve kritik verilerin açık web, derin web, Dark Web veya P2P ağlarında istemli ya da istemsiz şekilde sızdırılıp sızdırılmadığını tespit edin. Yetersiz güvenlik önlemlerine sahip dosya paylaşım platformları üzerinden paylaşılan kurum içi belgeler dahil olmak üzere veri sızıntılarını sürekli izleyerek hassas bilgilerin yetkisiz erişime maruz kalmasını önlemeye ve veri ihlali risklerini proaktif olarak azaltmaya yardımcı olun.

Sosyal Medya İzleme

Kuruluşunuzun dijital ayak izini bloglar, forumlar, web siteleri ve sosyal medya platformları dahil olmak üzere Web 2.0 kaynaklarında sürekli izleyin. Markanızı, logolarınızı ve dijital varlıklarınızı yetkisiz şekilde kullanan, sahte iş ortaklığı iddialarında bulunan veya marka itibarınızı riske atan platformları tespit ederek bu tehditlere karşı hızlı ve proaktif aksiyon almanızı sağlayın.

KrakenLabs Tehdit İstihbaratı Ekibi

KrakenLabs Tehdit İstihbaratı Ekibi, kuruluşunuza özel olarak hazırlanan kapsamlı tehdit analizleri ve raporları sunar. Hizmetlerimiz; kuruluşunuzu hedef alan tehdit aktörleri, Göstergeler (IoC), güvenlik açıkları ve Taktik, Teknik ve Prosedürler (TTP) hakkında kolay anlaşılır, aksiyona dönüştürülebilir tehdit istihbaratı sağlayarak güvenlik ekiplerinizin daha hızlı ve doğru kararlar almasına yardımcı olur.

Ayrıca Dark Web kaynaklı tehditler, veri ihlali analizleri ve Açık Kaynak İstihbaratı (OSINT) değerlendirmeleri dahil olmak üzere kuruluşunuzun proaktif güvenlik stratejisini destekleyen uzman danışmanlık hizmetleri sunar. Bu sayede siber tehditleri önceden tespit edebilir, riskleri etkin şekilde yönetebilir ve tehdit aktörlerinin bir adım önünde olabilirsiniz.

KrakenLabs Tehdit İstihbaratı hizmeti, DORA (Digital Operational Resilience Act) kapsamında yer alan risk yönetimi ve tehdit istihbaratı gereksinimlerini destekleyerek kuruluşların uyumluluk süreçlerini güçlendirmesine de katkı sağlar.