Siber Tehdit İstihbaratı (CTI)

Günümüz dijital çağında, kurumlar kritik verilerinin dark web gibi görünmez alanlarda izinsiz dolaşması tehdidiyle karşı karşıyadır. Şirketlerin domain adreslerine, çalışan bilgilerine veya müşteri verilerine yönelik sızıntılar, ciddi güvenlik riskleri oluşturarak finansal kayıplara, itibar zedelenmelerine ve yasal sorunlara yol açabilir. Proaktif bir yaklaşımla bu tehditleri bertaraf etmek, dijital varlıklarınızın korunması için hayati öneme sahiptir.

Hizmetimiz Neleri Kapsar?

Siber Tehdit İstihbaratı hizmetimiz, verilerinizin güvenliğini sağlamak adına kapsamlı bir yaklaşım sunar:

- Sürekli Tarama: Telegram grupları, özel hacker forumları, dark web siteleri ve sızıntı platformları gibi riskli kaynaklarda 7/24 kesintisiz tarama yapıyoruz.
- Anında Tespit: Şirketinizin domain adresine, çalışan kullanıcı bilgilerine veya hassas müşteri verilerine yönelik olası sızıntıları anında tespit ederek erken uyarı mekanizması sağlıyoruz.
- Detaylı Raporlama: Tespit edilen her bir tehdit için detaylı ve anlaşılır raporlar hazırlıyor, bulguları risk seviyesine göre sınıflandırarak kurumunuza özel aksiyon önerileri sunuyoruz.

VERİ SIZINTILARINI ÖNCEDEN GÖRÜN

Çalınan veriler büyümeden ve geniş kitlelere yayılmadan önce tespit edildiğinde, kurumlar hızlı ve etkili bir şekilde müdahale edebilir, potansiyel zararları minimize edebilirler. Bu sayede veri güvenliği stratejiniz önemli ölçüde güçlenir ve kurumunuzun dijital itibarı korunur.

Domain Adresi Bildirimi

Müşterimiz, korunmasını istediği domain adreslerini bize bildirir.

Kapsamlı Tarama

Belirtilen varlıklar için dark web, sızıntı forumları ve diğer ilgili kaynaklarda derinlemesine veri sızıntısı taraması başlatılır.

Bulguların Raporlanması

Tespit edilen veri sızıntıları kapsamlı bir şekilde analiz edilip raporlanır ve müşteriye sunulur