



EchoCTI Siber Tehdit İstihbaratı

Dijital dünyada karşılaşılabilecek riskleri önceden haber veren, hızlı ve doğruluk payı yüksek yerli siber tehdit istihbarat ürünü EchoCTI

"Gerçek zafer, savaşmadan kazanılan zaferdir. Gerçek önder savaşmadan kazanan önderdir."
Sun Tzu (MÖ 500)

Siber tehdit istihbaratı, bir kuruluşun bilinçli bir karar vermesi için gerekli olan bilgileri sağlamakla ilgilidir. Yeni bir alan olmayıp, zekayı çevreleyen binlerce yıllık birikmiş bilgeliğin üzerine inşa edilen bir alandır. Öyle ki Sun Tzu'nun 2500 yıl önce askeri istihbarat hakkında söylediği şeylerin çoğu hala hem geleneksel istihbarat teşkilatlarında hem de siber istihbarat teşkilatlarında geçerlidir.

Siber tehdit istihbaratı, günlük güvenlik izleme kullanımının ötesinde bir role hizmet eder.

Saldırganlar taktiklerini sürekli olarak değiştirdikçe hızla gelişen ve büyüyen siber tehdit ortamı için tehdit istihbaratı, BT ekiplerinin saldırganların amaçlarını ve davranışlarını anlamasını sağlar. Bu öngörü sayesinde de BT ekipleri, tehdit istihbaratını olası tehditleri izleme ve azaltma konusunda karar verme süreçlerini destekleyici nitelikte kullanır.

Günümüzde veri akışı önemli ölçüde artarken dijitalleşme de bir taraftan çığ gibi büyümekte; Organizasyonların sağlam ve sürdürülebilir ekonomik ve politik ilişkiler kurabilmesi açısından siber tehdit istihbaratını stratejik ve güvenlik planlarına dahil etmeleri her geçen gün bir zorunluluk haline gelmektedir.

Karşı karşıya oldukları tüm tehdit aktörlerini tespit etmek isteyen kuruluşların gerekli korumayı sağlayabilmeleri için ilk olarak "tehditi anlaması" gerekir. Bunun için de siber tehdit istihbaratı şarttır. İş operasyonları destekleyen siber tehdit istihbaratı olası tehditlere karşı bağımsız bir bakış açısı sunarken, mevcut bilgi akışına, varlıklara ve sistemlere de yeni bir bakış açısı kazandırır. Bu sayede, potansiyel tehdit alanları etkili bir şekilde belirlenir.

ECHO

CYBER THREAT INTELLIGENCE

EchoCTI proaktif bir şekilde tehditlerin takip edilmesini, verilerinin toplanmasını ve aksiyon alınabilir şekilde çözümler üretebilmesini sağlayan bir siber tehdit istihbaratı hizmetidir. Müşterilerimizin marka değerlerini ve alt yapılarını tehlikeye sokan tehdit unsurları için uyarılar ve çözümler üretir.

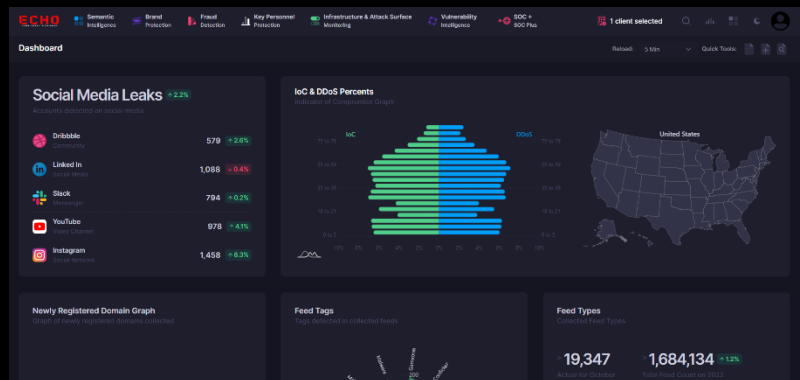
EchoCTI sayesinde doğru hedeflendirilen tehditlere bildirim sağlayarak, kurumlara bu tehditlere karşı hızlı bir şekilde aksiyon alma imkanı sunuyoruz.

EchoCTI çözümü, organizasyonların iş akışlarına zarar verebilecek her seviyedeki tehdidi güçlü sensörler sayesinde önceden ortaya çıkartabilir ve olası tehditlerin saldırıya dönüşüp organizasyona zarar vermesini engelleyecek "erken önlem" alabilmesini sağlayarak olası kaybın önüne geçebilir.

EchoCTI içerisinde ayrıca;

- Dijital Risk Koruma modülünde veri sızıntıları, ortalama aktiviteleri, sosyal medya takibi ve kaynak kod takibi vb.
 - Tehdit İstihbaratı ve Tehdit Beslemeleri
 - Marka Koruma
 - Dolandırıcılık Tespiti ve Bilgilendirme
 - Atak Yüzeyi Takibi ve Analizi
 - Kilit Personel Tespiti ve Bilgilendirme
 - Zafiyet İstihbaratı
 - SIEM Kuralları
- gibi modüller bulunmaktadır.

Tüm sektörleri olumsuz yönde etkileyen, sayısı ve niteliği bakımından hızla artış gösteren siber tehditleri önceden belirlemeniz amacı ile siber güvenliğinizi etkili bir şekilde sağlamanız için size EchoCTI ürünü ve hizmeti sunuyoruz.



"En büyük farkımız, büyük veriyi hızlı işliyor, uzmanlarımız ile sonuçları değerlendiriyor ve müşterilerimize gerçek zamanlı olarak bilgilendirme sağlayarak doğru aksiyonları alabilmeleri için tavsiyelerde bulunuyoruz.

Doğruluk ve gerçek zamanlılık en önemli farkımız.

Aynı zamanda bölgesel ve sektörel kategorizasyon da gerçekleştirmekteyiz. Böylece yalnızca belirli bir sektör grubunda yaşanan saldırı tiplerini veya belirli altyapılara yönelik saldırıları tespit edip, müşterilerimizi önceden uyarabiliyoruz. "

Bir siber tehdit istihbaratı yeteneği tanımlarken ve oluştururken, şu önemli soruları sormanız her zaman gereklidir:

- Neden yapıyorsun? (İş hedefi)
- Ne yapman gerek? (İş hedefini destekleyen faaliyetler)
- Nasıl uygulayacaksınız? (Mimari, operasyonel model vb.)
- Kim inşa edecek? Kim işletecek? (Beceriler ve kaynak bulma seçenekleri)

The dashboard displays several security modules: Brand Protection, Fraud Detection, Key Personnel Protection, Infrastructure & Attack Surface Monitoring, Vulnerability Intelligence, and SOC + SOC Plus. It also features a 'More Dashboards' section with options for Fraud Detection, Key Personnel Protection, Infrastructure & Attack Surface Monitoring, Vulnerability Intelligence, and SOC + SOC Plus. Below this, there are sections for Miss Configurations, Phishings, Social Media, Botnet Leaks, Company Employee Leaks, Source Code Leaks, and Combolist. A 'More Dashboards' section also includes Credit Card Leaks, Identity Leaks, and Config File Detections.

The dashboard also shows a 'Key Personnel Protection' section with Identity Leaks, Company E-Mail Leaks, Personal E-Mail Leaks, and Others. Another 'More Dashboards' section includes IoT Search Engines, Vulnerability Management, Domain Tracking, Port Tracking, Security Certificate Tracking, and Blacklist.

The bottom section is a table of vulnerabilities with columns for Title, Categories, Client, State, Takedown Status, Assignee, Badge, On, and Date. The table lists several vulnerabilities, including 'Orecek E-Business Süre ve SugarCRM güvenlik Açılan Saldırı altında', 'Cisco Ix ve FS B9-IP Ürünlerine Yeni Yüksek Derecede Güvenile Açılan Keşfedildi', 'Microsoft, KPS (Kritik) Sorunları İçin Güncelleme Yayınadı', 'SHIMMER İşlemleri, Kuruluş Tarafından Yönetilen Chromebook'lar İçin Tehdit Oluşturuyor', and 'QMAP Yayınlandı: Güncelleme ile NAS Üzerinde Bulunan Kritik Zafiyetleri Kapatıldı'. The table also includes a 'SOC +' section with various security rules and alerts, such as 'LockBit_Green Yara Rule', 'Titan Stealer Detection Rule', 'MyBB <= 1.8.31 Remote Code Execution', 'ALPHM/BlackCat Yara Rule', 'ALPHV Ransomware Grubu', 'Webshell Creation in Microsoft Exchange Directories (ProxyNotCheck)', and '(CVE-2022-30190) Microsoft Office Code Execution PoC'la Vulnerabilite'.