Siber Tehdit İstihbaratı (CTI)

Siber Tehdit İstihbaratı Nedir?

Siber güvenlikte savunma alanında çalışıyorsanız, kurumunuzun gün boyunca birçok saldırıya maruz kaldığını bilirsiniz.

İstihbarat bilgisi, savaşlarda olduğu gibi siber savaşlarda da önemli bir rol oynamaktadır. İstihbarat bilgileri sayesinde saldırılar öncesinde gerekli savunma mekanizmalarını kurabilir ve saldırganlardan bir adım önde olma şansını yakalayabilirsiniz.

Başkalarını ve kendini bilirsen, yüz savaşta yenilmezsin.
Başkalarını tanımıyor ama kendini tanıyorsan, bir kazanır bir kaybedersin.
Başkalarını ve kendinizi tanımıyorsanız, her savaşta yenileceksiniz.

Sun Tzu

Siber tehdit istihbaratı, kurumunuza karşı olabilecek siber saldırıların ve siber tehdit aktörlerinin motivasyonlarını, hedeflerini ve TTP'lerini belirlemek için birçok kaynaktan veri toplayan ve gerekli filtre ve analizlerden geçen bir istihbarat türüdür.

CTI Yaşam Döngüsü

Siber tehdit istihbaratı aşağıdaki yaşam döngüsünden geçer.

1. **Planlama:** CTI'ın amaç, hedef ve gereksinimlerinin belirlenmesi
2. **Toplama** : Birçok kaynaktan veri toplama
3. **İşleme:** Toplanan verilerin işlenmesi ve analize hazır hale getirilmesi
4. **Analiz:** İşlenen verilerin analiz edilmesi, bilgilerin istihbarata dönüştürülmesi ve paylaşıma hazır hale getirilmesi
5. **Yaygınlaştırma:** Tehdit istihbaratı verilerini paylaşma
6. **Geribildirim:** Paylaşılan raporlardan geri bildirim alınarak ilerideki tehdit istihbarat operasyonları için düzenlemelerin yapılıp yapılmayacağının belirlenmesi.

Siber Tehdit İstihbaratının Faydaları

Farklı tehdit istihbarat servisleri size farklı raporlar sağlayabilir. Genel olarak, kuruluşunuz aşağıdaki şekillerde fayda sağlayabilir.

- Siber tehdit aktörleri hakkında istihbarat bilgisi sağlayarak, kuruluşunuza zarar verebilecek tehdit aktörlerini yakından izleme şansı verir.
- Siber saldırılarda elde edilen IOC bilgilerini farklı kuruluşlara karşı paylaşarak olası saldırıların üstesinden gelmenizi veya IOC bilgilerini kullanarak siber olaydan etkilenip etkilenmediğinizi kontrol etmenizi sağlar.
- Marka değerine zarar verebilecek paylaşımları tespit etmenizi sağlar.
- Dahili tehditleri tespit etmenizi sağlar.

CTI Yaşam Döngüsü

Siber tehdit istihbaratı aşağıdaki yaşam döngüsünden geçer.

1. **Planlama:** CTI'ın amaç, hedef ve gereksinimlerinin belirlenmesi
2. **Toplama** : Birçok kaynaktan veri toplama
3. **İşleme:** Toplanan verilerin işlenmesi ve analize hazır hale getirilmesi
4. **Analiz:** İşlenen verilerin analiz edilmesi, bilgilerin istihbarata dönüştürülmesi ve paylaşıma hazır hale getirilmesi
5. **Yaygınlaştırma:** Tehdit istihbaratı verilerini paylaşma
6. **Geribildirim:** Paylaşılan raporlardan geri bildirim alınarak ilerideki tehdit istihbarat operasyonları için düzenlemelerin yapılıp yapılmayacağının belirlenmesi.

Siber Tehdit İstihbarat Türleri

3 tür siber tehdit istihbaratı vardır.

1) Taktik Siber Tehdit İstihbaratı

Taktik CTI, TTP olarak da bilinen tehdit aktörlerinin taktikleri, teknikleri ve prosedürleri hakkında daha spesifik ayrıntılar sağlar.

Genellikle Taktik CTI raporları, IOC'leri (IP adresi, karma gibi veriler) içerir.

Aşağıdaki kişiler veya ürünler genellikle stratejik siber tehdit istihbaratı türünü kullanır.

- SOC Analisti
- Güvenlik Ürünleri (IPS/IDS/EDR/Güvenlik Duvarı)
- SIEM Ürünleri

2) Operasyonel Siber Tehdit İstihbaratı

Operasyonel CTI; Siber tehdit aktörünün motivasyonlarını, hedeflerini ve TTP'lerini anlamanızı sağlar.

- Tehdit Avcıları
- Olay Müdahalecileri
- Güvenlik Mühendisleri

3) Stratejik Siber Tehdit İstihbaratı

Stratejik CTI; bir siber saldırının olası sonuçlarının genel bir resmini oluşturmak için eğilimlerin ve ortaya çıkan risklerin ayrıntılı analizini sağlayan bir istihbarat türüdür.

- C Seviye Yöneticiler
- Yöneticiler

Siber Tehdit İstihbarat Toplama Yöntemleri

Tehdit istihbarat verilerinin toplanması ilk adımdır. Verileri analiz etmek ve yorumlamak için öncelikle verilerin toplanması gerekmektedir.

Siber tehdit istihbarat verileri, toplama yöntemlerine göre birkaç kategoriye ayrılmaktadır.

1. **OSINT:** Açık kaynaklardan elde edilen bir istihbarat türüdür.
2. **HUMINT:** Sahadaki bir kişiden elde edilen bir zeka türüdür.
3. **GEOINT:** Uydu ve hava fotoğrafları kullanılarak elde edilen bir istihbarat türüdür.
4. **SIGINT:** Sinyallere müdahale edilerek elde edilen bir zeka türüdür.