Denetci.org

REFERANS İLKELERİ

Tehdit İstihbaratı İlkeleri

Rİ-ISL-5

Sürüm 1.0 · 11.08.2026

www.denetci.org

Tehdit İstihbaratı İlkeleri

Tehdit istihbaratı, kuruluşun karşılaşabileceği tehditler hakkında elde edilen bilgilerin güvenlik kararlarını geliştirecek biçimde anlamlandırılmasını ele alır. Amaç mümkün olan en fazla göstergeyi, raporu veya tehdit akışını toplamak değil; hangi tehdit bilgisinin kuruluş için anlam taşıdığını, bu bilgiye ne ölçüde güvenilebileceğini ve mevcut güvenlik varsayımlarını nasıl değiştirdiğini ortaya koymaktır.

İlke 1: Tehdit istihbaratı bilgi toplamakla değil karar ihtiyacıyla başlamalıdır.

Bir kuruluş çok sayıda rapor ve göstergeye sahipken tehditleri hakkında yine de anlamlı bir görüşe sahip olmayabilir. İstihbarat, hangi güvenlik kararının daha iyi verilmesini sağlayacağıyla ilişkilendirilebilmelidir.

İlke 2: Tehdit bilgisinin önemi kuruluşun gerçek bağlamından türemelidir.

Kullanılan teknolojiler, sunulan hizmetler, tutulan veriler, coğrafi faaliyetler ve mevcut güven sınırları hangi tehdidin anlam taşıdığını belirler. Genel tehdit gündemi kuruluşun kendi maruziyetinin yerine geçmemelidir.

İlke 3: Bir tehdidin görünürlüğü önemiyle eşit kabul edilmemelidir.

Çok konuşulan saldırılar kuruluş açısından ilgisiz olabilirken daha az görünür bir tehdit mevcut mimariye doğrudan uyabilir. Öncelik popülerlikten çok gerçek temas ve etki ihtimaline dayanmalıdır.

İlke 4: Dış istihbarat kuruluşun kendi gözlemlerinin yerine geçmemelidir.

Kuruluşun karşılaştığı saldırı girişimleri, olaylar ve olağan dışı davranışlar kendi tehdit ortamı hakkında doğrudan kanıt sağlar. İç ve dış bilgi birbirini tamamlayan bağlamlar olarak kullanılmalıdır.

İlke 5: Kaynağa duyulan güven ile belirli bilginin doğruluğu ayrı değerlendirilmelidir.

Geçmişte güvenilir olmuş bir kaynak hatalı bilgi verebilir; yeni bir kaynak da doğru bir gözlem sunabilir. Kaynak itibarı, her iddianın otomatik doğrulaması olmamalıdır.

İlke 6: Tek bir kaynaktan gelen bilgi gereksiz kesinliğe dönüştürülmemelidir.

Bazı bilgiler yalnızca tek bir kaynaktan elde edilebilir ve yine de kullanılabilir. Ancak bağımsız destek bulunmadığında bu sınır karar vericiden gizlenmemelidir.

İlke 7: Olgu, değerlendirme ve varsayım birbirinden ayırt edilebilir olmalıdır.

Gözlemlenmiş bir olay ile analistin o olaydan çıkardığı sonuç aynı güven düzeyinde değildir. İstihbarat, yorumun kanıtın kendisi gibi görünmesine yol açmamalıdır.

İlke 8: Belirsizlik istihbaratın kusuru olarak gizlenmemelidir.

Tehdit ortamı eksik ve çelişkili bilgiler içerir. Bir değerlendirmenin ne ölçüde kesin olduğu ve hangi önemli bilinmeyenlere dayandığı, kararın doğru yorumlanabilmesi için görünür kalmalıdır.

İlke 9: Göstergeler taşıdıkları bağlamdan koparılmamalıdır.

Bir adres, alan adı, dosya özeti veya başka teknik özellik belirli bir zaman ve saldırı bağlamında anlam taşıyabilir. Göstergenin kendisi süresiz ve evrensel kötü niyet kanıtına dönüştürülmemelidir.

İlke 10: Tehdit göstergelerinin değeri zaman içinde değişebilir.

Saldırgan altyapıları ve teknik özellikler hızla değişebilir veya daha sonra meşru kullanıma geçebilir. Geçmişte doğru olan bilgi sınırsız süreyle engelleme veya alarm gerekçesi olarak kullanılmamalıdır.

İlke 11: İstihbarat yalnızca kolay değiştirilebilen göstergelere dayanmamalıdır.

Adresler ve dosya değerleri saldırgan tarafından hızla değiştirilebilir. Daha kalıcı davranışlar, teknikler ve güven ilişkilerini kötüye kullanma biçimleri de tehdit anlayışının parçası olmalıdır.

İlke 12: Saldırı tekniği ile saldırgan kimliği birbirine bağlanmamalıdır.

Aynı yöntem farklı aktörler tarafından kullanılabilir ve saldırganlar başka grupların izlerini taklit edebilir. Savunma, belirli bir aktör adının doğruluğuna gereksiz biçimde bağımlı olmamalıdır.

İlke 13: Tehdit aktörü atfı mevcut kanıtın izin verdiğinden daha kesin olmamalıdır.

Atıf bazı kararlar için önemli olabilir; ancak çoğu savunma kararında saldırının davranışı ve oluşturabileceği etki daha doğrudan değer taşır. Aktörü adlandırma ihtiyacı koruma ihtiyacının önüne geçmemelidir.

İlke 14: Teknik tehdit bilgisi kuruluş üzerindeki olası etkisiyle ilişkilendirilebilmelidir.

Bir saldırı yönteminin nasıl çalıştığını bilmek tek başına hangi kararın alınması gerektiğini açıklamaz. Bilgi mümkün olduğunda hangi varlık, hizmet veya güven sınırının etkilenebileceğini gösterebilmelidir.

İlke 15: İstihbarat hedef kitlenin vereceği karara uygun anlam düzeyine sahip olmalıdır.

Yönetim için gerekli olan tehdit eğilimleri ile teknik savunma ekibinin ihtiyaç duyduğu gözlemlenebilir özellikler aynı ayrıntı seviyesinde olmayabilir. Fazla teknik veya fazla soyut bilgi karar vermeyi zorlaştırmamalıdır.

İlke 16: İstihbaratın eyleme dönüşmesi yalnızca anlık teknik engelleme anlamına gelmemelidir.

Tehdit bilgisi izleme, güvenlik açığı önceliği, mimari karar, tedarik tercihi veya uzun vadeli risk yaklaşımını değiştirebilir. Değer, yalnızca otomatik kural üretme kapasitesiyle ölçülmemelidir.

İlke 17: Yeni tehdit bilgisi mevcut güvenlik varsayımlarını değiştirebilmelidir.

Geçmişte makul kabul edilmiş bir saldırgan yeteneği veya risk modeli yeni kanıtlarla geçerliliğini yitirebilir. İstihbarat yalnızca mevcut görüşü doğrulayan bilgi üretmekle sınırlı kalmamalıdır.

İlke 18: Otomasyon belirsiz istihbaratı kesin güvenlik kararına dönüştürmemelidir.

Makine tarafından işlenen tehdit bilgisi hızlı tepki sağlayabilir; ancak hatalı veya eskimiş bilgi geniş engelleme ve hizmet etkisi oluşturabilir. Otomatik kararın etkisi kullanılan bilginin güven düzeyiyle uyumlu olmalıdır.

İlke 19: Birden fazla kaynak görünürde çeşitlilik sağlarken gerçekte aynı kaynağı tekrar ediyor olabilir.

Aynı ilk gözlem birçok rapor veya hizmet tarafından yeniden yayımlanabilir. Kaynak sayısının artması bağımsız doğrulama bulunduğu varsayımını otomatik olarak oluşturmamalıdır.

İlke 20: Tehdit bilgisinin paylaşımı kendi güvenlik ve etik sınırlarına sahip olmalıdır.

Yararlı paylaşım; hassas kaynakları, kişisel veriyi veya kuruluşun kendi zayıflıklarını gereksiz biçimde açığa çıkarmamalıdır. Bir bilginin edinilebilmesi veya paylaşılabilmesi onun sınırsız biçimde kullanılmasını haklı çıkarmaz.

İlke 21: Tehdit istihbaratının güvencesi gerçek güvenlik kararlarına etkisi üzerinden doğrulanabilmelidir.

Kaynak sayısı, gösterge hacmi veya yayımlanan rapor miktarı tek başına olgunluk kanıtı değildir. İstihbaratın kuruluş için önemli tehditleri daha doğru anlamaya, yanlış varsayımları değiştirmeye ve gerçek güvenlik kararlarını iyileştirmeye katkısı gösterilebilmelidir.