Denetci.org

REFERANS İLKELERİ

Güvenlik İzleme İlkeleri

Rİ-ISL-4

Sürüm 1.0 · 11.08.2026

www.denetci.org

Güvenlik İzleme İlkeleri

Güvenlik izleme, sistemlerde ve güven ilişkilerinde meydana gelen güvenlik açısından anlamlı davranışların zamanında fark edilebilmesini ve yeterli bağlamla değerlendirilebilmesini ele alır. Amaç mümkün olan en fazla veriyi veya alarmı üretmek değil; güven kaybına işaret edebilecek durumların görünür hale geldiği ve bu görünürlüğün gerçek kararları destekleyebildiği bir izleme anlayışı oluşturmaktır.

İlke 1: İzleme veri toplamaktan değil cevaplanması gereken güvenlik sorularından başlamalıdır.

Çok sayıda kayıt veya telemetri bulunması kendi başına güvenlik görünürlüğü oluşturmaz. İzleme, hangi davranışların güven açısından önemli olduğunu ve hangi değişikliklerin araştırılması gerektiğini ortaya çıkarabilecek biçimde tasarlanmalıdır.

İlke 2: İzleme kapsamı sistemin gerçek güven sınırlarını yansıtmalıdır.

Kimlikler, yönetim yolları, uygulamalar, veriler, ağlar ve dış hizmetler farklı güven alanları oluşturabilir. Yalnızca kolay izlenebilen veya merkezi sistemlerin görünür olması diğer alanların güvenilir olduğu anlamına gelmez.

İlke 3: Görünmeyen alan güvenli alan olarak yorumlanmamalıdır.

Bir sistemden veya güvenlik alanından yeterli bilgi alınamıyorsa orada olağan dışı davranış bulunmadığı sonucuna varılamaz. Görünürlük eksikliği kendi başına güven düzeyini etkileyen bir belirsizliktir.

İlke 4: İzleme sisteminin kendi sağlığı da görünür olmalıdır.

Log üretiminin, olay aktarımının veya başka izleme yeteneklerinin durması normal sessizlik gibi görünmemelidir. Bir güvenlik alanına ilişkin görünürlüğün kaybolması, o alandaki güven hakkındaki kesinliği de azaltmalıdır.

İlke 5: Güvenlik davranışı bağlamından kopuk tekil olaylara indirgenmemelidir.

Aynı işlem kullanıcıya, sisteme, zamana, kullanılan yetkiye veya iş bağlamına göre farklı anlam taşıyabilir. İzleme, yalnızca olayın gerçekleştiğini değil mümkün olduğu ölçüde hangi koşullarda gerçekleştiğini de değerlendirebilmelidir.

İlke 6: Olayın gerçek kaynağı teknik aracılar arasında kaybolmamalıdır.

Ortak hesaplar, servisler, proxy'ler ve otomasyonlar bir işlemin gerçek kaynağını görünmez hale getirebilir. Güvenlik açısından önemli davranışlar gerektiğinde ilgili kullanıcı, cihaz, hizmet veya başka sorumlu kaynakla ilişkilendirilebilmelidir.

İlke 7: Kimlik ve yetki değişimleri izleme bağlamının bir parçası olmalıdır.

Bir kullanıcı oturum açtıktan sonra başka rol kullanabilir, yetki yükseltebilir veya başka bir kimlik adına işlem yapabilir. İlk kimlik bilgisi olay anındaki gerçek güven durumunu tek başına açıklamaya yetmeyebilir.

İlke 8: Yüksek etkili faaliyetler olağan davranış içinde kaybolmamalıdır.

Ayrıcalıklı işlemler, güvenlik yapılandırması değişiklikleri ve güven sınırlarını etkileyebilen diğer davranışlar sıradan kullanım faaliyetlerinden daha geniş sonuçlar doğurabilir. İzleme bu farkı anlamlı biçimde yansıtabilmelidir.

İlke 9: Güvenlik kontrollerini değiştiren davranışlar özel önem taşımalıdır.

Loglamayı kapatmak, erişim kontrolünü değiştirmek veya başka bir güvenlik mekanizmasını etkisiz hale getirmek sonraki davranışların güvenlik anlamını değiştirebilir. Savunmanın kendisine yönelik değişiklikler görünmez sıradan yapılandırma işlemleri olmamalıdır.

İlke 10: Başarılı davranış güvenlik açısından önemsiz kabul edilmemelidir.

Ele geçirilmiş geçerli bir kimlik veya yetkili bir taraf saldırısını başarısız denemeler üretmeden gerçekleştirebilir. İzleme yalnızca reddedilen veya hatalı işlemlere dayanırsa önemli kötüye kullanımlar görünmez kalabilir.

İlke 11: Tek bir sinyal kesin saldırı kanıtı olarak görülmemelidir.

Olağan dışı bir davranış güvenlik olayına işaret edebilir; ancak meşru nedenlerle de oluşabilir. İzleme, şüphe ile doğrulanmış durum arasındaki farkı korumalıdır.

İlke 12: Birden fazla zayıf sinyal birlikte daha güçlü anlam oluşturabilmelidir.

Tek başına önemsiz görünen olaylar aynı kimlik, sistem, zaman veya işlem zinciri içinde değerlendirildiğinde anlamlı bir güvenlik davranışı ortaya çıkarabilir. İzleme yalnızca bağımsız alarm mantığına bağlı kalmamalıdır.

İlke 13: Korelasyon yapay bir kesinlik oluşturmamalıdır.

Farklı olayların benzer zaman veya kimlik bilgisine sahip olması aynı saldırının parçaları olduklarını her zaman göstermez. Birleştirilen sinyallerin hangi ilişkiye ve hangi belirsizliğe dayandığı anlaşılabilir olmalıdır.

İlke 14: Alarm üretmek ile bir olayın fark edilebilir olması aynı şey değildir.

Çok sayıda alarm gerçek güvenlik sorunlarının gürültü içinde kaybolmasına yol açabilir. İzleme yaklaşımı alarm miktarını değil, önemli davranışların uygun zamanda fark edilip değerlendirilebilmesini hedeflemelidir.

İlke 15: Öncelik olay sayısından çok olası etkiye dayanmalıdır.

Benzer teknik davranışlar farklı sistemlerde farklı sonuçlar doğurabilir. İzleme, olayın etkileyebileceği veri, kimlik, hizmet ve güven sınırlarını dikkate alabilmelidir.

İlke 16: Ağ, uç nokta, kimlik, uygulama ve veri görünürlüğü birbirinin yerine geçmemelidir.

Her katman sistem davranışının farklı bir bölümünü gösterebilir. Bir alanda güçlü görünürlük bulunması diğer alanlarda olanların eksiksiz biçimde bilindiği anlamına gelmemelidir.

İlke 17: Şifrelenmiş veya teknik olarak görünmeyen davranış güvenilir kabul edilmemelidir.

İçeriğin izlenememesi trafiğin veya işlemin meşru olduğunu göstermez. İçerik görünürlüğünün mümkün olmadığı durumlarda kimlik, hedef, hacim, zaman ve başka bağlamsal sinyaller anlam taşıyabilir.

İlke 18: İzleme verisi kendi başına korunması gereken bir güvenlik varlığıdır.

İzleme sistemleri kullanıcı davranışları, sistem yapıları, güvenlik olayları ve başka hassas bilgiler barındırabilir. Görünürlük ihtiyacı bu veriye gereksiz erişim veya sınırsız saklama hakkı doğurmamalıdır.

İlke 19: İzleme amacı sırların ve hassas içeriğin gereksiz kopyalarını oluşturmamalıdır.

Parolalar, erişim belirteçleri, anahtarlar veya olayın anlaşılması için gerekli olmayan hassas veriler izleme sistemlerine taşındığında yeni bir güven kaybı alanı oluşabilir. İzleme kanıtı sağlarken korumaya çalıştığı değerleri gereksiz biçimde çoğaltmamalıdır.

İlke 20: Algılama yaklaşımı yalnızca geçmiş saldırıların biçimine bağlı kalmamalıdır.

Bilinen saldırı göstergeleri değerlidir; ancak yeni veya farklı saldırılar aynı izleri bırakmayabilir. İzleme, belirli imzaların yanında sistemin kendi güven varsayımlarının bozulduğu davranışları da fark edebilecek bir anlayış taşımalıdır.

İlke 21: İzleme mantığı sistem değiştikçe geçerliliğini yeniden kazanmalıdır.

Yeni mimariler, kimlik modelleri, uygulama davranışları ve iş süreçleri daha önce olağan veya olağan dışı kabul edilen davranışların anlamını değiştirebilir. Eski algılama yaklaşımı değişen sistem üzerinde otomatik olarak doğru sayılmamalıdır.

İlke 22: Güvenlik izleme güvencesi gerçek tespit ve anlamlandırma kapasitesi üzerinden doğrulanabilmelidir.

Kural sayısı, alarm hacmi, izleme ürünü veya veri miktarı tek başına güvence oluşturmaz. Önemli bir güvenlik davranışının gerçekten fark edilip edilemediği, yeterli bağlamla açıklanıp açıklanamadığı ve görünürlük kaybının kendisinin anlaşılabilir olup olmadığı gerektiğinde gösterilebilmelidir.