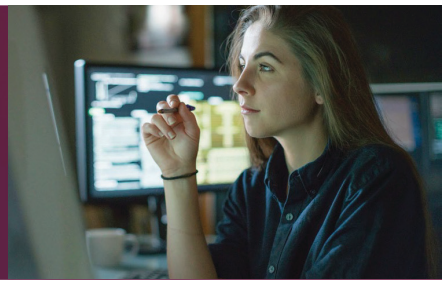
CHECK POINT

STRATEGIC CONSULTING GROUP

External Risk Management



Harici Risk ve EASM'nin Önemi

Siber güvenlik tehditleri giderek daha sofistike ve yaygın hale geldikçe, kuruluşların harici saldırı yüzeylerini yönetme konusunda dikkatli olmaları gerekir – bu yüzey, yetkisiz bir kullanıcının bir kuruluşun dijital ortamına girebileceği tüm olası giriş noktalarının veya zafiyetlerin toplamıdır. External Attack Surface Management (EASM), bu zafiyetlerin potansiyel siber saldırılara karşı belirlenmesi, analiz edilmesi ve güvence altına alınmasına odaklanır; böylece bir kuruluşun siber güvenlik stratejisinin kritik bir bileşenini oluşturur.

Yönetilen Harici Saldırı Yüzeyi Değerlendirmesi

İnternete açık dijital varlıkların çeşitliliği ve sürekli gelişen yapısı nedeniyle sürekli ve otomatik varlık keşfi ile bağlamsallaştırma kritik öneme sahiptir. Bir kuruluşun dijital ayak izine ilişkin kapsamlı görünürlük; iştiraklere ve üçüncü taraflara ait varlıklar da dahil olmak üzere, bilinmeyen veya takip edilmeyen dijital varlıkların oluşturduğu riski azaltır. Bu varlıklar, en yaygın tehdit vektörünü temsil etmektedir.

Hizmet olarak sunulan Managed EASM, gerçek zamanlı içgörüler sağlayarak ve ortaya çıkan tehditlere ölçeklenebilir, doğru ve zamanında yanıt verilmesini mümkün kılarak bu sorunları çözer; üstelik SOC kaynaklarını tüketmeden. Hizmet, Red Team bünyesinde yer alan deneyimli güvenlik analistleri tarafından sunulur ve düzenli olarak gönderilen raporlar veya kritik bir zafiyet tespit edildiğinde doğrudan iletişime geçilmesi yoluyla yürütülür. Bu yaklaşım, manuel çabayı önemli ölçüde azaltır ve daha etkili zafiyet yönetimi ile risk önceliklendirmesi sağlar.

Bir Saldırı Yüzeyi Nasıl Analiz Edilir

Saldırı yüzeyinin analizi birkaç adımdan oluşur. Süreç, sürekli güncellenen bağlamsal bilgilerle birlikte harici varlık envanterinin çıkarılmasıyla başlar. Ardından, risk tespiti gereksinimlerini karşılamak için varlık özelliklerine göre uyarlanmış payload'lar geliştirilir. Bu payload'lar, dağıtık bir test sistemi ağı aracılığıyla ilgili varlıklara gönderilir. Son olarak sonuçlar doğrulanır, derlenir ve erişilebilir arayüzler üzerinden kullanıma sunulur.

Temel Özellikler:

1. **Keşif:** Bir kuruluşun saldırı yüzeyine ilişkin kapsamlı bir küresel ağ görünümü oluşturmak ve dijital varlıkları tespit etmek için kapsamlı açık kaynak istihbaratı (OSINT) kullanır. Buna bağlı şirketlerin, bulut kaynaklarının ve diğer birbirine bağlı varlıkların belirlenmesi de dahildir.
2. **Bağlamsallaştırma:** Tespit edilen varlıkların iş bağlamına ilişkin içgörüler sunar; buna varlıkların rolü, hassasiyet düzeyi ve kuruluş için taşıdığı önem dahildir. Bu sayede varlığın önemi ve ele geçirilmesi durumunda oluşabilecek potansiyel etki daha iyi anlaşılır.
3. **Aktif Güvenlik Testi:** OWASP Top 10 gibi yaygın zafiyetlerin önemli bir kısmını kapsayan 25.000'den fazla saldırı tekniğini kullanarak varlıkların güvenliğini değerlendirir. Bu yaklaşım, keşif ve bağlamsallaştırma ile birlikte kullanıldığında, harici varlık envanterinin tamamında herhangi bir varlık kaynağına etki oluşturmadan test yapılmasını sağlar.
4. **Önceliklendirme:** Güvenlik ekiplerinin, zafiyetleri varlığın iş bağlamı, keşfedilebilirliği, saldırganlar açısından çekiciliği ve diğer kritik meta veriler temelinde belirlemesine ve önceliklendirmesine olanak tanır. Bu yaklaşım, çalışmaların en önemli risklere odaklanmasını sağlayarak verimliliği artırır.
5. **Düzeltme Sürecinin Hızlandırılması:** Sürekli ve otomatik testler aracılığıyla sorunların daha hızlı giderilmesini sağlar; kuruluşlara düzeltme çalışmalarında güven verir ve ortalama düzeltme süresini azaltır.

Değerlendirme: Girdiler, Süreç ve Çıktı

Değerlendirme, kuruluşun dijital ortamına ait verilerin sisteme girilmesiyle başlar. Süreci başlatmak için ana alan adı yeterlidir; ancak ek bilgiler (örneğin bulut ortamlarına ilişkin bilgiler) sonuçların daha da iyileştirilmesine yardımcı olabilir.

Bu veriler; keşif, varlık tespiti, bağlamsallaştırma, zafiyet analizi ve aktif güvenlik testlerini içeren adımlar aracılığıyla analiz edilir. Süreç; varlıkların otomatik olarak toplanmasını ve sınıflandırılmasını, payload oluşturulmasını, testlerin gerçekleştirilmesini ve kanıtların toplanmasını içerir. Tüm bu aşamalar, ölçeklenebilirlik ve doğruluğu artırmak amacıyla makine öğrenimi (ML) ve doğal dil işleme (NLP) teknolojileriyle desteklenir.

Sonuç olarak kuruluşun harici saldırı yüzeyine ilişkin derinlemesine ve tutarlı bir anlayış elde edilir; zafiyetler ve yanlış yapılandırmalar önceliklendirme ve giderme için açık şekilde ortaya konur. Bu sistematik yaklaşım, kuruluşun siber güvenlik duruşuna yüksek düzeyde güven sağlar; güvenlik ekiplerinin en kritik konulara odaklanmasına olanak tanır, operasyonel verimliliği artırır ve ihlal riskini önemli ölçüde azaltır.

External Attack Surface Assessment, tek seferlik bir test olarak veya hizmete yönelik sürekli yıllık abonelik şeklinde sunulabilir.

Değerlendirme Aşaması	Aktivite
1. İş Kapsamının Belirlenmesi	Kurumsal yapının ortaya çıkarılması ve haritalanması
2. Keşif / Varlık Tespiti	IP aralıklarını ve alan adlarını ortaya çıkarma Tipik kapsam IP aralıklarını tarama ve varlık envanteri oluşturma Varlıklar hakkında OSINT toplama Varlıkları sınıflandırma Varlıklara iş bağlamı ekleme Varlıklara atıf (kurumsal sahiplik) ekleme
3. Zafiyet Analizi	Yazılım sürümleri (CPE'ler) aracılığıyla CVE'lerin tespit edilmesi
4. Önceliklendirme	CVSS Varlık keşfedilebilirliği Varlık çekiciliği Tehdit istihbaratı
5. Test / Saldırı Simülasyonu	Payload tabanlı aktif testler / DAST Test edilen varlıklar (tipik) Veri hassasiyetinin sınıflandırılması Yüksek riskli istismar faaliyetleri
6. Raporlama / Öneriler	Bulgular listesi ve Yönetici özeti Düzeltme planlaması