SafeBreach

SafeBreach Propagate

Ağ Saldırı Yollarını Test Edin, İhlal Sonrası Etkiyi Anlayın

Kurumsal güvenlik ekipleri, olası güvenlik açıklarını ve saldırgan hedeflerini görebilmek için iç ağ güvenliğini düzenli olarak test etme sorumluluğuna sahiptir. Popüler araçlar olan manuel penetrasyon testleri yalnızca sınırlı ve anlık değerlendirmeler sağlar ve hızla geçerliliğini yitirir. Diğer otomatik çözümler ise ya ölçeklenebilir değildir ya da test sırasında ek sorunlara yol açma potansiyeline sahiptir.

SafeBreach Propagate, saldırganların ağ içinde nasıl hareket edeceğini simüle eden bir saldırı yolu doğrulama aracıdır. Güvenlik ekiplerinin, ihlal sonrasında oluşabilecek potansiyel etkileri daha iyi anlamasına yardımcı olur. Bu yetenek, ödüllü SafeBreach Validate aracının çevre güvenliği testlerini tamamlamak için özel olarak tasarlanmıştır. "İhlalin gerçekleştiğini varsay" yaklaşımıyla fidye yazılımlarının ve devlet destekli APT gruplarının davranışlarını taklit ederek ağ savunmalarını daha derinlemesine test eder. SafeBreach Propagate size şunları sağlar:

- Kurumsal varlıklar ve en kritik sistemlere giden yüksek riskli saldırı yollarını ortaya çıkarın.
- En kritik maruziyetlere odaklanmak için iyileştirme faaliyetlerini önceliklendirin.
- Ağ uç noktaları arasındaki ve içindeki güvenlik açıklarını ve güçlü yönleri tespit edin.
- Yerleşik raporlar ve panolar sayesinde önemli paydaşlarla iletişimi kolaylaştırın.

Propagate Faydaları

Yüksek Riskli Saldırı Yollarını Doğru Tespit Edin

Ağınızda başarılı bir ihlalin gerçek etki alanını anlamak için ileri seviye yatay hareket saldırıları çalıştırın.

Odaklanmış İyileştirme ile Zaman Kazanın

En kritik kurumsal varlıklar ve değerli sistemler için en büyük riski oluşturan zafiyetli uç noktalara göre iyileştirme faaliyetlerini önceliklendirin.

Bilgiye Dayalı Güvenlik Kararları Alın

Açık bulguları içeren yapılandırılmış raporları kullanarak güvenlik ve iş kararlarınızı bilinçli şekilde alın, kurumsal dayanıklılığınızı artırın.

BAS Yatırımınızı Güçlendirin

Önce Validate ile güvenlik açıklarını belirleyin, ardından Propagate ile saldırganın motivasyonlarını ve olası etkilerini analiz ederek riskin daha kapsamlı bir resmini elde edin.

Kullanım Senaryoları

Saldırı Yolu Haritalama

Muhtemel saldırı hedeflerini ve saldırganların test edilen ağda yatay hareket etme kabiliyetlerini anlayın ve belgeleyin.

İhlal Sonrası Kurumsal Maruziyet Değerlendirmesi

İhlal sonrası riskleri görün; kimlik ve zafiyet korumalarını optimize etme fırsatlarını ortaya koyan raporlarla içgörü kazanın.

Kurumsal Güvenlik ve Ölçeklenebilirlik

SafeBreach Propagate, kurumsal organizasyonlar için özel olarak tasarlanmıştır ve diğer güvenlik test yöntemlerinin getirebileceği risklere karşı en üst düzeyde koruma sağlar. Kurumsal güvenlik standartlarına ve politikalarına tam uyum için güvenlik önlemleri içerir. Bunlar arasında:

Kapsam Sınırlaması

Müşteriler, yayılımın kapsamını belirli bölgeler/makinelerle sınırlayabilir; IP aralıkları için “izin ver” ve “engelle” listeleri kullanabilir.

Saldırı Özelleştirme

Kullanıcılar, port taraması için izin/verme listelerini tanımla-yarak hangi portların dahil edileceğine veya hariç tutulacağına karar verebilir. Bu esneklik, hedefli ve verimli test yapılmasını sağlarken kritik servisler üzerindeki olası etkileri en aza indirir.

Kimlik Doğrulama

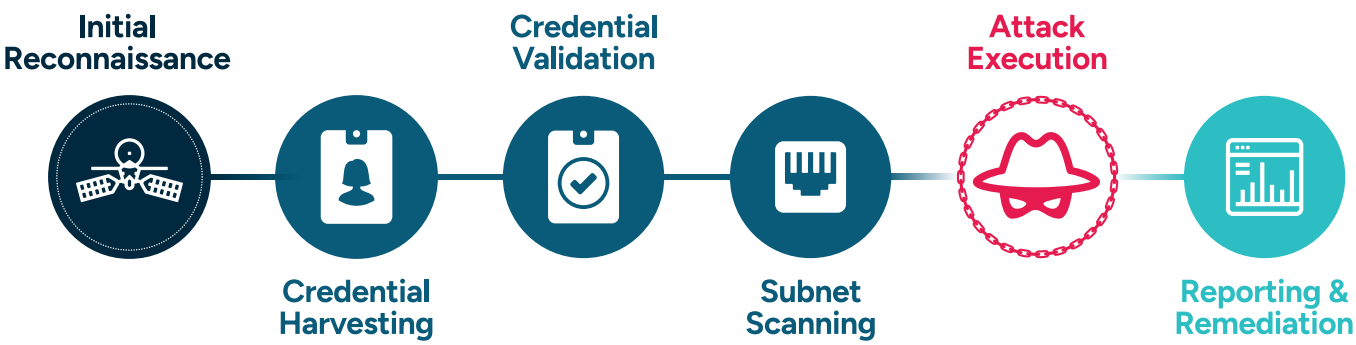
Propagate, hem çevrimdışı hem de domain tabanlı kimlik bilgilerini doğrulamaya özen gösterir. Geçersiz kimlik bilgileri lateral movement saldırılarında kullanılmaz. Bu, gereksiz saldırıları veya hesap kilitlenmelerini önlemek için ek bir güvenlik katmanı sağlar.

Gizli Veri Güvenliği

Kimlik bilgisi kurtarma mesajları HTTPS üzerinden bulut tabanlı arka uca hibrit şifreleme modeliyle güvenli şekilde iletilir. Bu kimlik bilgileri şifrelenir ve korumalı bir kasada güvenli biçimde saklanır.

Sistem Kararlılığı ve Kaynak Kullanımı

Propagate yalnızca gerekli kullanıcıları, dosyaları ve diğer kaynakları tarar. Ayrıca SafeBreach, saldırıların sistemlerin kararlılığını etkilemediğini doğrulamak için testler gerçekleştirir.



Propagate Nasıl Çalışır?

1. Ön Keşif (Initial Reconnaissance)

Mevcut bir uç nokta "hasta sıfır" olarak kullanılarak, Propagate keşif ve bilgi toplama işlemleri yapar. Hangi saldırıların hedeflere ulaşmak için başarıyla kullanılabileceğini belirler.

2. Kimlik Bilgisi Toplama (Credential Harvesting)

Kimlik bilgisi toplama saldırıları, işletim sistemi işlemlerini (örn. kayıt defteri, bellek dökümü), parola yöneticilerini ve tarayıcı depolarını hedef alarak hassas verilerin saklanabileceği zayıf noktaları ortaya çıkarır.

3. Kimlik Bilgisi Doğrulama (Credential Validation)

Toplanan kimlik bilgileri, hesap kilitleme mekanizmalarını tetikle-meden erişim sağlayıp sağlayamayacaklarını görmek için doğrulanır. Domain hash'leri ve düz metin parolaları (hem domain hem de yerel) geçerlilik açısından test edilir.

4. Alt Ağ Taraması (Subnet Scanning)

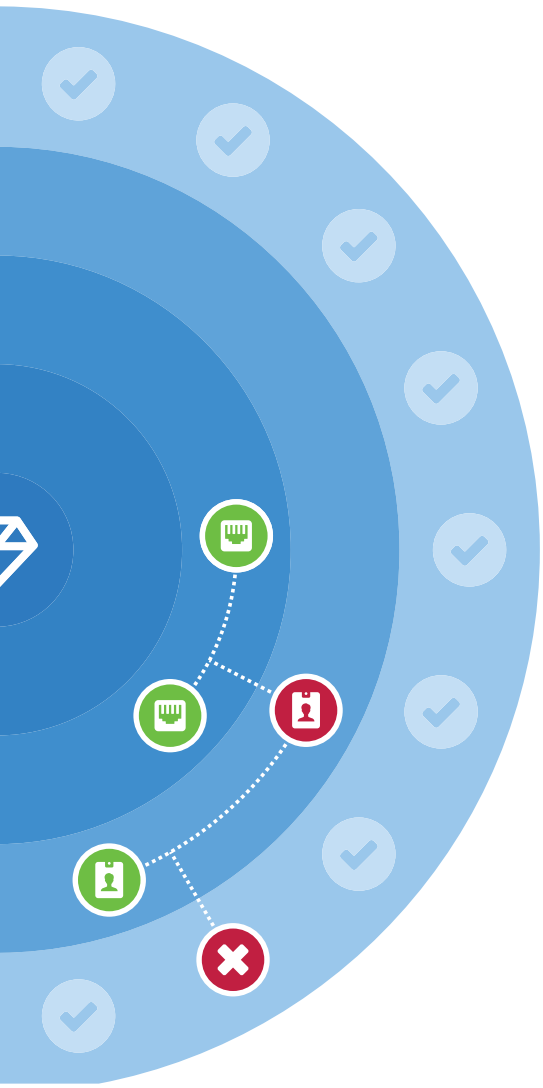
Yerel Class C alt ağı, açık portlar ve servisler için taranır. Bu sayede yatay hareket için potansiyel giriş noktaları belirlenir.

5. Saldırı Gerçekleştirme (Attack Execution)

Hedefe yatay hareket yoluyla erişim kazanmak için çeşitli saldırılar gerçekleştirilir. Bu saldırılar şunları içerir: PAExec ile Uzak Kod Yürütme (RCE) Pass the Hash, WMI lateral movement, WinRM lateral movement WinRM üzerinden Invoke Command ile RCE, RDP üzerinden RCE, PAExec ve SSPI kullanılarak RCE

5. Raporlama & İyileştirme (Reporting & Remediation)

Belirlenen güvenlik açıklarını ve uygulanabilir önerileri içeren yapılandırılmış bir rapor sunulur. Bu rapor, azaltma/iyileştirme kararlarının verilmesini kolaylaştırır.



Neden Propagate?

SafeBreach Propagate, kurumsal güvenlik ekiplerinin ihlal sonrası maruziyetleri tespit etmek ve saldırganın ağ içinde yatay hareket ederek yaratacağı olası etkiyi anlamak için zaman kazanmasını sağlar.

Propagate ile güvenlik ekipleri şunları yapabilir:

Ağ içinde tutarlı bir koruma ve görünürlük düzeyi sağlamak için sürekli saldırı yolu haritalama/doğrulama çalıştırır.

Bir saldırgan tarafından gerçekleştirilen kimlik bilgisi toplama saldırılarının etkisini hızla tespit ederek, potansiyel yönetici hesap ele geçirmeleri ve veri hırsızlığı / sızdırma risklerini belirler.

Propagate'ı Deneyimleyin

Kişiselleştirilmiş bir demo planlayın ve neden kurumsal güvenlik liderlerinin güvenlik programlarının kalitesini, etkinliğini ve değerini artırmak için SafeBreach Propagate'ı tercih ettiğini keşfedin.

SAFEBREACH HAKKINDA

SafeBreach, kurumsal ölçekte tehdit maruziyeti doğrulama alanında liderdir. Dünyanın en büyük markalarına, tehdit maruziyetini ve buna bağlı siber riskleri anlama, ölçme ve iyileştirme konusunda güvenli ve ölçeklenebilir yetenekler sunar. Ödüllü SafeBreach Exposure Validation Platformu, öncü Breach & Attack Simulation ve yenilikçi Attack Path Validation özelliklerini bir araya getirerek güvenlik ekiplerine, çevre savunmasından iç sistemlere kadar güvenlik açıklarını ölçme ve giderme imkânı sağlar. Dünyaca ünlü tehdit araştırma ekibi ve dünya standartlarında müşteri desteğiyle SafeBreach, kuruluşların güvenlik stratejilerini reaktiften proaktife dönüştürmesine yardımcı olur. Daha fazla bilgi için **www.safebreach.com**