SafeBreach | OTD BİLİŞİM

SafeBreach Platform

Veri sayfası

Güvenlik Ekibinin Karşılaştığı Meydan Okumalar

İnsan kaynakları ve güvenlik ürünlerine yapılan büyük ve sürekli devam eden yatırımlara rağmen, kurumsal güvenlik ekipleri hala temel yönetim sorunlarını yanıtlamakta ve her gün karşılaştıkları meydan okumaları etkin bir şekilde çözümlemekte zorlanıyor.

- Korumam gereken işletme varlıkları için en acil riskler nelerdir?
- Savunmalarım beklendiği gibi çalışıyor mu?
- Mevcut savunmam, artan sayıda tehdide ayak uydurabilir mi?
- En iyi sonuçları alma çabalarımıza en verimli şekilde nasıl öncelik verebiliriz?

SafeBreach Platformu

SafeBreach, güvenlik ekiplerinin veriye dayalı güvenlik kanıtı sağlamasına, güvenlik kör noktalarını ve zayıflıklarını ortadan kaldırmasına ve kontrollerin beklenen şekilde çalıştığını doğrulamasına olanak tanır.

Saldırıların bir adım önünde olmak için güvenlik ekipleri, saldırganların kullandığı araç ve teknikleri kullanmalıdır. SafeBreach platformu, kanıtlanmış binlerce ihlal ve saldırı simülasyonunu otomatik, sürekli ve ölçekli olarak güvenli bir şekilde yürütür. SafeBreach, güvenliğin nerede beklendiği gibi çalıştığını belirlemek ve belirli saldırıların mevcut savunma yapılandırmalarını kıracağı alanları ortaya çıkarmak için tüm siber kill-chain'de (öldürme zincirinde) güvenli bir şekilde ihlal senaryoları gerçekleştirir.
SafeBreach aşağıdaki temel yetenekleri sunar:

- Otomatik, sürekli ve ağ çapında saldırılar.
- SafeBreach Explorer görünümü ve TTP'leri MITRE ATT&CK çerçevesine eşleyerek bir saldırının ortamınızda nasıl sonuçlanacağının resmini çizin.
- İş risklerinin gerçek zamanlı önceliklendirilmesi ve operasyonel güvenlik duruşunun etkinliği hakkında eyleme geçirilebilir istihbarat.
- Hangi güvenlik açıklarından gerçekten yararlanılabileceğine ilişkin görünürlük sağlar ve bunların önceliklerini ortamınıza göre belirler.

Kullanılabilir İçgörüler

SafeBreach Insights (İçgörüleri), binlerce sonucu otomatik olarak analiz eder ve güvenlik ekibinin güvenlik kontrollerinizdeki boşlukları veya yetersiz yapılandırmaları hızla düzeltmesi için sürekli olarak ayrıntılı rehberlik sağlar.
Bu içgörüler ve ayrıntılı eylem önerileri, ekibin iyileştirme çalışmalarına iş etkisine göre öncelik vermesine olanak tanır. Ekip, tüm yüksek riskli ve yüksek etkili öğeleri hızlı ve doğru bir şekilde çözme becerisi kazanır.
İyileştirme verileri, birçok olayın otomatik olarak düzeltilmesini sağlamak için ağ, uç nokta, bulut, SIEM ve SOAR çözümlerinden oluşan çok sayıda harici güvenlik çözümüyle paylaşılır.

Güvenlik Ekibinin Karşılaştığı Meydan Okumalar

Simülasyon

Ağınız, uç noktanız ve bulut çözümlerinizdeki savunmaları test etmek için SafeBreach Hacker's Playbook™'de (Hacker Taktik Kitabı) bulunan 15.000'den fazla saldırı yöntemiyle güvenlik kontrollerini doğrulayın.

Görselleştirme

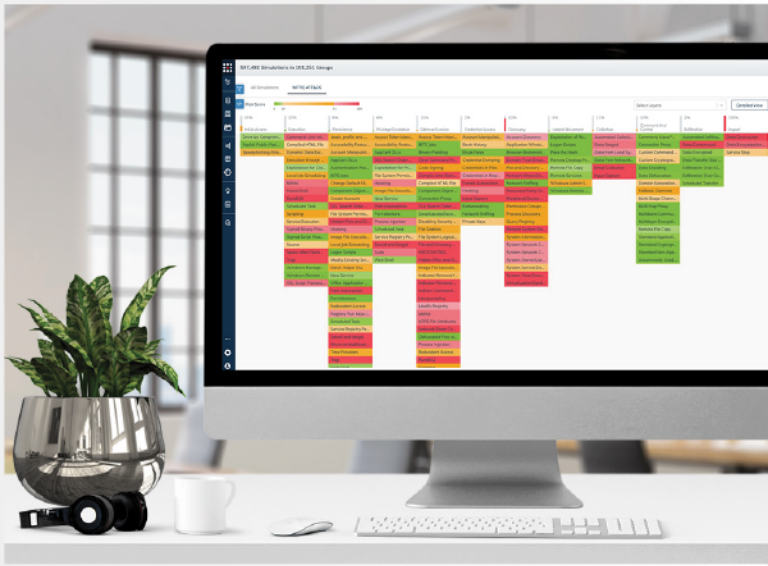
MITRE ATT&CK™ çerçevesiyle eşlenen güvenlik duruşunuzu görselleştirin. Ayrıntılı bir ağ topolojisi görünümü, siber saldırı öldürme zinciri (kill-chain) boyunca tüm riskleri gösterir..

Önceliklendirme

Güvenlik kontrollerinin düzeltilmesine öncelik vermek için veriye dayalı sonuçlar ve gerçekten yararlanılabilen sistemlerde güvenlik açığı yönetimi yama uygulaması.

Düzeltme

İş etkisine göre önceliklendirilen eyleme geçirilebilir (kullanılabilir) düzeltme verileriyle Güvenlik ve Altyapı ekipleriyle işbirliği yapar ve azaltma verilerini ağınıza, uç noktanıza, SIEM ve SOAR çözümlerinize besler.



Kapsamlı SafeBreach Platformu

Tehdit İstihbaratıyla Entegrasyon

SafeBreach ile savunmanızın nasıl önleyeceğini, tespit edip yanıt vereceğini güvenli ve hızlı bir şekilde test ederek en son tehdit istihbaratını operasyonel hale getirin. SafeBreach, tehdit beslemelerini ağınızda güvenli bir şekilde çalışacak şekilde dönüştürerek uç noktanızı, ağınızı, e-postanızı, bulut ve kapsayıcı kontrollerinizi test ederek bir bilgisayar korsanının bir saldırıya karşı savunmanızın nasıl dayanacağına dair görüşünü betimler.
Savunmanızı en son tehditlere karşı test etmek, işletmeye yönelik potansiyel riski anlamanın tek yoludur.

Risk Bazlı Güvenlik Açığı Yönetimi

Güvenlik açığı yönetiminde (VM) en büyük zorluk önceliklendirmedir. Bir kurumsal ortamda binlerce güvenlik açığı bulunabileceğinden, kuruluşların hangi güvenlik açıklarının işletme için en zararlı sonuçlara yol açabileceğini tam olarak belirlemek neredeyse imkansızdır.
VM araçlarıyla SafeBreach entegrasyonu, bilgisayar korsanlarının erişebilecekleri ve yararlanabilecekleri açısından ortamınızın gerçek durumunu netleştirir. SafeBreach, ortamınızda sürekli olarak saldırılar gerçekleştirerek hem ağ hem de ana bilgisayar saldırıları riskini hesaplar. SafeBreach içgörülerini güvenlik açığı taramalarından elde edilen sonuçlarla birleştiren VM ekipleri, iyileştirme çabalarını düşmanlar tarafından en fazla istismar riskinin bulunduğu konumlara odaklayabilir.
Savunmanızı en son tehditlere karşı test etmek, işletmeye yönelik potansiyel riski anlamanın tek yoludur.

Entegre Çözümlerle Siber Riski Değerlendirmesi

Savunmanızın hem iyi bilinen tehditlere hem de doğada görülen en son tehditlere karşı nasıl tepki vereceğini en etkili şekilde değerlendirmek için SafeBreach ile aşağıdakilerden oluşan sıkı entegrasyonlar gerekir:
• bir tehdit istihbarat sistemi
• uç nokta, ağ ve SIEM güvenlik çözümleri
• bir güvenlik açığı yönetimi çözümü
SafeBreach, güvenlik kontrollerinizin neyi tespit edip önleyeceğini doğrulamak için kuruluşunuz genelinde güvenli bir şekilde saldırılar gerçekleştirecek, verileri, istismar edilebilir olana dayalı olarak öncelikli yama yönetimiyle güvenlik açığı taramalarınızla ilişkilendirecek ve kuruluşunuzu savunmak için ayrıntılı bir iyileştirme planıyla ekiplerinizi bir araya getirecektir.

SafeBreach, bir kuruluşun siber güvenlik riskini tam olarak değerlendirmek için tehdit istihbaratı, güvenlik açığı yönetimi ve güvenlik kontrolü doğrulamasını bir araya getiren pazardaki tek çözümdür.

Temel Kullanım Vakaları

• Mevcut güvenlik kontrollerinin etkinliğini ölçümü.
• Güvenlik Aracı ROI'sini iyileştirme.
• Ortamınızda nelerin istismar edilebilir olduğunu tespit edere güvenlik açığı yaması yönetimine öncelik verme. En son tehditlere karşı güvenlik durumunuzu anlamak.
• Siber güvenlik riskinizi etkin bir şekilde ölçmek.

Entegre Ekosistem

Milyonlarca kuruluşta kurulu temel güvenlik teknolojileri ve iş platformlarıyla kapsamlı entegrasyon.

Microsoft · SentinelOne · paloalto NETWORKS · Qualys. · splunk> · CISCO

SafeBreach

OTD BİLİŞİM

Merkezi Sunnyvale, California'da bulunan Şirket, Sequoia Capital, Deutsche Telekom Capital Partners, Draper Nexus, Hewlett Packard Pathfinder, PayPal, OCV ve yatırımcı Shlomo Kramer tarafından finanse edilmektedir.

otd.salesgrp@onlineteknikdestek.com
www.onlineteknikdestek.com