SafeBreach

SafeBreach Güvenlik Kontrolü Doğrulaması:

Riski En Aza İndirin, Güvenlik Yatırımlarınızın Getirisini En Üst Düzeye Çıkarın.

Çözüm Özeti

Düzinelerce güvenlik kontrolü uygulamış olabilirsiniz, ancak bu yeterli değildir. Bu kontrollerin amaçlandığı ve gerektiği şekilde çalıştığından emin olmanız gerekir.

Bunu yapmak için güvenlik denetimi doğrulaması yapmanız gerekir. Bu özet, geleneksel yaklaşımların neden yetersiz kaldığını ortaya koymakta ve SafeBreach'in etkili ve sürekli güvenlik kontrolü doğrulamasını sağlayan gelişmiş yetenekleri nasıl sunduğunu göstermektedir.

Güvenlik Kontrolü Doğrulamasının Tanıtılması

Siber saldırganların oluşturduğu tehditlerle mücadele etmek için işletmelerdeki ve devlet kurumlarındaki güvenlik ekipleri bir dizi kontrol uygulamaya ve geliştirmeye devam etmektedir. Ancak, büyük yatırımlar yapıldıktan ve araçlar dağıtıldıktan sonra bile yapılacak iş bitmemiştir. Ekiplerin güvenlik kontrollerini doğrulamaları ve gerekli savunmaları sağladıklarından emin olmaları hayati önem taşımaktadır.

SafeBreach Yönetici Panoları ile güvenlik yatırımlarını iş hedeflerinize uygun hale getirin.

- Güvenlik Kontrolü Doğrulaması
- BAS (Breach Attack Simulation)
- Tehdit Değerlendirmesi
- Bulut Güvenlik Değerlendirmesi
- Zafiyet Yönetimi

Geleneksel Güvenlik Kontrolü Doğrulama Yaklaşımlarının Sınırlamaları

Güvenlik ekipleri, güvenlik kontrolü doğrulaması yapmak için çeşitli yaklaşımlar izleyebilir. Ekipler senelerdir penetrasyon testi, kırmızı takım egzersizleri, güvenlik açığı taraması ve daha fazlasını yapmayı seçmiş olabilir. Ancak, her şey göz önüne alındığında, bu yaklaşımlar önemli sınırlamalar getirdi:

Tutarsızlık. Beyaz şapka korsanlığı ve kırmızı takım yaklaşımlarının manuel, bireysel doğası, işletmeleri en iyi ihtimalle tutarsızlığa ve öngörülemezliğe ve en kötü ihtimalle hatalara, yanlışlıklara ve ihmallere maruz bırakabilir.

Minimal içgörüler. Güvenlik açığı tarayıcıları gibi sistemlerin çıktısı, gerçek güvenlik risklerini temsil eden veya temsil etmeyen birçok sorunu ortaya çıkaran çok fazla "gürültü" olabilir. Bu sistemler, yüksek hacimli sorunlarla karşı karşıya kalarak, önceliklendirmeyi yönlendirmek için minimum iç görü sunarken gereğinden fazla çalışan güvenlik ekipleri için devasa bir görev birikimi oluşturabilir.

Yüksek maliyetler. Etkili kırmızı ekipleri çalıştırmak veya beyaz şapka korsanlığı yapmak için ihtiyaç duyulan uzman türleri yetersizdir ve yüksek ücretler talep etmektedir.

Kısıtlı frekans, kapsam. Doğru uzmanları bulmanın yüksek maliyeti ve zorluğu göz önüne alındığında, birçok kuruluş bu tür testleri yapma yeteneklerinin kapsamı, sıklığı ve süresi açısından önemli ölçüde sınırlıdır. Tipik olarak, penetrasyon testleri aralıklı olarak, genellikle yıllık olarak veya altı ayda bir yapılır; bu da, ekiplerin yalnızca belirli bir zamanda bilgi edinmesi anlamına gelir.

Safebreach'ten Güvenlik Kontrolü Doğrulamasının Tanıtılması

SafeBreach

Bugün SafeBreach, ekiplere güvenlik kontrollerini doğrulamak için etkili ve programlı bir yol sağlayan gelişmiş ihlal ve saldırı simülasyonu özellikleri sunmaktadır. Sonuç olarak platform, penetrasyon testi ve kırmızı ekip oluşturma gibi manuel, emek gerektiren yoğun faaliyetlerin sınırlamalarının üstesinden gelirken kuruluşunuzun kontrol doğrulama hedeflerini ele almanızı sağlar. Ayrıca, diğer ihlal ve saldırı simülasyon platformlarından farklı olarak SafeBreach, platformu yönetmek için özel ekipler kiralamaya gerek kalmadan ekiplerin sürekli saldırıları otomatik olarak gerçekleştirmesini sağlar.

SafeBreach platformu, güvenliğin bu tür saldırılara nerede dayanabileceğini ve nerede iyileştirilmesi gerektiğini kanıtlamak için üretim ortamlarında gerçek saldırıları güvenli bir şekilde yürütür. Platform, saldırıları güvenli ve sürekli olarak yürütebilen gelişmiş, patentli teknolojiyi kullanarak bir kuruluşun güvenlik mimarisinin test edilmesini otomatikleştirir.

Güvenlik Ekosisteminin Kapsamını Tamamlayın

SafeBreach ile insanlar, süreçler ve mevcut teknolojiler dahil olmak üzere tüm güvenlik ekosisteminizin güvenliğini değerlendirebilirsiniz. Ayrıca, tüm bu alanlarda belirli kontrolleri doğrulayabilirsiniz:

- **Veri kaybı önleme (VKÖ).** Verilerin dışarı sızmaması için VKÖ kontrollerinizin doğru şekilde yapılandırıldığından emin olun. VKÖ çözümünüzün performansını en üst düzeye çıkarmak için ihtiyaç duyduğunuz bilgileri edinin.
- **E-mail denetimleri.** E-mail denetimlerinizin doğru yapılandırıldığından emin olun, böylece bir kuruluşa sızma sinyali verdiği bilinen tüm güvenlik ihlali göstergelerini (IOC'ler) belirler.
- **Uç nokta denetimleri.** Virüsten koruma, kötü amaçlı yazılımdan koruma, uç nokta tehdit algılama ve yanıt (EDR) ve genişletilmiş tespit ve yanıt (XDR) dahil uç nokta denetimlerinin, uç noktalarınızdaki kötü amaçlı etkinlikleri önlemek veya algılamak için doğru şekilde yapılandırıldığından emin olun.
- **Ağ denetimleri.** Ağ denetimlerinizin, kötü niyetli etkinliklere karşı koruma sağlamak için en iyi şekilde yapılandırıldığından emin olun. Güvenlik duvarları, yeni nesil güvenlik duvarları, segmentasyon, izinsiz giriş önleme ve algılama sistemleri, ağ davranışı ve trafik analizi ve daha pek çok konuda kapsamlı bir şekilde doğrulama yapın.
- **Güvenlik bilgileri ve olay yönetimi denetimleri.** Saldırıları tespit eden veya önleyen kontroller

- ile başarısız olanları ayırt etmek için saldırı sonuçlarını ilişkilendirin. Her saldırı için ilgili olayları ve kuralları uygun telafi edici kontrollerle eşleştirin.
- **Dünya Çapında Ağ (Web) denetimleri.** Web ağ geçitlerinizin, Proxylerinizin ve URL filtreleme denetimlerinizin kötü amaçlı etkinlikleri önlemek veya algılamak için doğru şekilde yapılandırılıp yapılandırılmadığını belirleyin.
- **Bulut ve Container denetimleri.** Bulut geçişinizin, bulut stratejinizi en üst düzeye çıkarmak için doğru şekilde yapılandırılmış kontrol ve veri düzlemi (Data Plane) güvenlik kontrollerine sahip olduğundan emin olun.

Her doğrulamadan sonra SafeBreach çözümü kontrolünüzün etkinliğini en üst düzeye çıkarmanıza yardımcı olan ayrıntılı bir iyileştirme planı oluşturur.

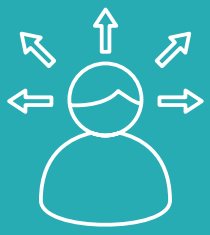
Güvenlik Kontrolü Doğrulaması: Kullanım Durumları

SafeBreach platformu, işletmenizdeki bir dizi çabaya yardımcı olabilir. Aşağıda, kuruluşunuzun bugün bu ihlal ve saldırı simülasyon platformunu kullanma yollarından sadece birkaçı verilmiştir:

- **Yetkili ve gerçeğe dayalı çözüm değerlendirmeleri yapın.** Yeni bir aracın işletmenizi rakiplere karşı ne kadar etkili bir şekilde koruyacağını tam olarak değerlendirmek ve doğrulamak zordur. SafeBreach ile, doğru yatırımı yaptığınızdan emin olmak için değerlendirme sürecinde hızla binlerce hamle gerçekleştirebilirsiniz.
- **Sıkılaştırılmış sistem görüntülerini değerlendirin.** Bir sistem görüntüsünü sıkılaştırmak için gerekli adımları attıktan sonra, değişiklikleri üretime almadan önce, değişikliklerin etkinliğini hızlı bir şekilde değerlendirmek için hamleler gerçekleştirebilirsiniz. Yerel, sanal veya bulut altyapılarında sistem görüntülerini değerlendirin ve ayrıntılı bir iyileştirme planı alın.
- **Eğitim için gerçekçi hamle senaryoları yürütün.** Saldırıları güvenli bir şekilde yürüterek ve ekiplerin saldırıları gözlemlemelerini ve olaya müdahale eğitimi almalarını sağlayarak sahte senaryoyu teorikten gerçeğe dönüştürün.
- **Uzak iş gücünü koruyun.** Güvenlik açıklarını hızla belirlemek ve gidermek için önemli saldırı yöntemlerini yürütün, böylece uzak iş gücünüzün etkinliklerini ve verilerini koruyabilirsiniz.
- **Güvenlik sağlayıcılarını sorumlu tutun.** Saldırıları önleyen ve tespit eden ve bunları tamamen kaçıran çözümleri belirlemek için tüm güvenlik ekosisteminizin güvenlik denetimlerini doğrulayın. Çözümlerinin saldırı altında gerçekte nasıl performans gösterdiğine ilişkin öngörülerden ve nesnel kanıtlardan yararlanarak tedarikçilerinizi sorumlu tutma gücü elde edin.
- **Bilgisayar sistem kaynak tüketimini en aza indirin.** Çoğu zaman, masaüstü ve dizüstü bilgisayarlar çok fazla güvenlik aracıyla aşırı yüklenir ve sistem performansını, makinenin ömrünü ve kullanıcı deneyimini düşürür. En uygun denetim kombinasyonunu belirlemek için her güvenlik aracına saldırılar gerçekleştirin, böylece cihazlarınızı ağırlaştırmadan işletmenizi savunabilirsiniz.

GÜVENLİK KONTROLÜ DOĞRULAMASI

Saldırıları Güvenle Yürüt



Veriye Dayalı Sonuçlarla Güvenlik Duruşunuzu Görselleştirin

İşletmenizi Savunmak için Bütünsel Bir Çözüm Üretin

ICT OTD PREFER EXPERIENCE ONLINE Since 2011

OTD BİLİŞİM

SafeBreach: Temel Avantajlar

Ekipleriniz, güvenlik denetimi doğrulaması yapmak için SafeBreach platformunu kullanarak bir dizi temel avantajlar elde edebilir:

- **Riski azaltın.** Siber saldırganlar bunları kötüye kullanmadan önce güvenlik açıklarını, boşlukları ve hataları belirleyin. SafeBreach ile yeni saldırı teknikleri veya kurumsal ortamınızda ortaya çıkan yeni güvenlik açıklarından kaynaklanan yeni risklerin hızlı bir şekilde belirlenmesi ve giderilmesinden emin olmak için sürekli doğrulama yapabilirsiniz.
- **Güvenliği güçlendirin.** İnsanlar, süreçler ve mevcut teknolojiler dahil olmak üzere tüm güvenlik ekosisteminin yanı sıra belirli araçların etkinliğini doğrulayın. En kritik tehditleri belirlemek için gereken objektif bilgileri edinin ve bunları ele almak için gerekli adımları atın.
- **İşletme verimliliğini artırın.** Örtüşen ve etkisiz araçları bilgili bir şekilde belirleyerek ve bunları ortadan kaldırarak yönetimi ve işlemleri düzene koyun.
- **Yeni kontrolleri akıllıca değerlendirin.** Muhtemel çözümleri doğru bir şekilde test edin, böylece satın almadan önce ortamınızda hangisinin en iyi sonucu vereceğini belirleyebilirsiniz.
- **Mevcut yatırımların getirisini en üst düzeye çıkarın.** Çeşitli araçları yerinde objektif olarak değerlendirin ve hangilerinin işe yarayıp yaramadığını belirleyin. Böylece ekipleriniz mevcut kontrollerinizden en iyi şekilde yararlanabilir ve bu sistemlerin en üst düzeyde güvenlik sağlayacak şekilde optimize edilmesini sağlayabilir.

SafeBreach

Sonuç

Kurumsal güvenlik, varsayımlara, spekülasyonlara veya hüsnükuruntulara bırakılmayacak kadar önemlidir. Güvenlik kontrolü doğrulaması, ekiplerin yeterli savunmanın mevcut olduğundan emin olmalarını sağlamak ve aksi takdirde ne yapmaları gerektiğini anlamalarını sağlamak için kesinlikle gereklidir. Ayrıca güvenlik kontrolü doğrulaması ihtiyacı, kritik öneme sahiptir, ancak bu nedenle, bu çabaların sürekli ve uygun maliyetli bir şekilde yönetme ihtiyacı da bir o kadar önemlidir. SafeBreach ile ekipleriniz, güvenlik kontrollerini doğrulamak için etkili ve programlı bir yol sağlayan gelişmiş ihlal ve saldırı simülasyon yeteneklerinden yararlanabilir. Şimdi denetimlerinizi değerlendirebilir ve güvenlik açıklarını kötü amaçlar için kullanılmadan önce ele alabilirsiniz.

IT & OT SafeBreach Platformu OTD BİLİŞİM'de!

MALTEPE OFİS
Cevizli Mah. Zuhal Cad. No: 46
Ritim İstanbul A-1 Blok D:55
34846 Maltepe - İstanbul
TÜRKİYE

HALKALI OFİS
Atatürk Mah. Güner Sok. B-1 Blok
No: 1/1B İç Kapı No: 257
34307 Küçükçekmece İstanbul
TÜRKİYE

T: +90 216 912 10 05 F: +90 216 912 10 07 otd.salesgrp@onlineteknikdestek.com

SafeBreach

Web Uygulaması Güvenliği İçin SafeBreach

Ajan kullanmadan web uygulaması güvenlik doğrulaması sayesinde tam ölüm zincirinin kilidini açın

Web uygulamaları, bilgisayar korsanlarının favori hedefidir. Siteler arası komut dosyası oluşturma, SQL enjeksiyonu ve yol geçişi gibi web uygulaması saldırılarını kullanan bilgisayar korsanları, hassas verileri çalmak veya zararlı kötü amaçlı yazılımlara sahip sistemlere bulaşmak için ağlara sızabilir ve bunları ihlal edebilir. İşletmeler, trafiği filtreleyen ve kötü amaçlı davranışlara karşı koruma sağlayan bir güvenlik katmanı sağlamak için web uygulaması güvenlik duvarları (WAF) kullanır ve yine de web uygulamaları siber saldırılar için en çok kullanılan ikinci sızma yöntemidir. Güvenlik ekipleri, web saldırılarına karşı etkili bir şekilde koruma sağlamak için web uygulaması güvenlik duvarları (WAF) ve uygulama kontrollerini nasıl optimize edebilir?

SafeBreach platformu, saldırıları sürekli ve güvenli bir şekilde yürütmenize, güvenlik denetimlerinizin etkinliğini doğrulamanıza ve optimize etmenize ve ihlaller gerçekleşmeden önce en kritik boşlukları azaltmak için iyileştirme çabalarına öncelik vermenize olanak tanıyarak kuruluşunuzun güvenlik duruşuna ilişkin bir "bilgisayar korsanı görselleştiricisi" sağlamak üzere oluşturulmuştur. Ayrıca, dağıtımı hızlı ve kolay olan aracısız web uygulaması güvenlik duvarları (WAF) doğrulaması aracılığıyla web uygulamalarınızın güvenli olmasını sağlama olanağı da sağlar.

Ajan kullanmadan Web Uygulaması Güvenliği için Neden SafeBreach'i Seçmelisiniz?

Tam ölüm zinciri doğrulaması

Belirli boğulma noktalarının bir saldırganın hedeflerine ulaşma yeteneğini nasıl etkilediğini anlamak için web uygulaması güvenlik saldırısı yüzeyini tam saldırgan ölüm zinciri bağlamında görüntüleyin.

Sektörün en büyük hamle taktikleri kitabı

SafeBreach's Hacker's Playbook™, OWASP® Foundation'ın ilk on güvenlik riskinin çoğunu test etmeye yönelik saldırılar da dahil olmak üzere en çeşitli web uygulaması saldırıları paketini sunar.

Hızlı ve kolay kurulum

Safebreach'in web uygulaması güvenlik doğrulaması, önceden kurulum gerektirmeyen ve hızlı bir şekilde yürütülebilen aracısız bir test özelliğidir.

Web uygulaması güvenlik duruşunun bağlamsallaştırılmış görünümü

Enjeksiyon saldırıları, siteler arası komut dosyası saldırıları, şifreleme hataları, güvenli olmayan uygulama tasarımı, web uygulaması güvenlik açıklarının uzaktan kullanımı, sunucu tarafı istek sahteciliği ve daha pek çok simülasyonla WAF denetimlerinizi kolayca test edin.

WAF'ınız için eyleme dönüştürülebilir Yatırım Getirisi raporlaması

Olası web uygulaması saldırılarının sonucunu anlamak, iş üzerindeki etkisini bildirmek ve WAF yatırımlarının yatırım getirisini ölçmek için özelleştirilebilir panolardan ve raporlama özelliklerinden yararlanın.