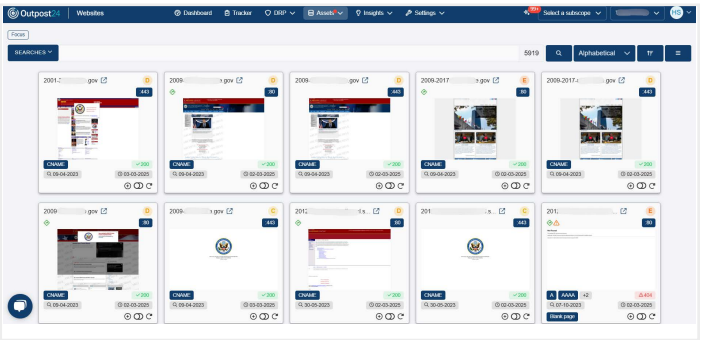
OTD BİLİŞİM
GLOBAL VAD

Outpost24

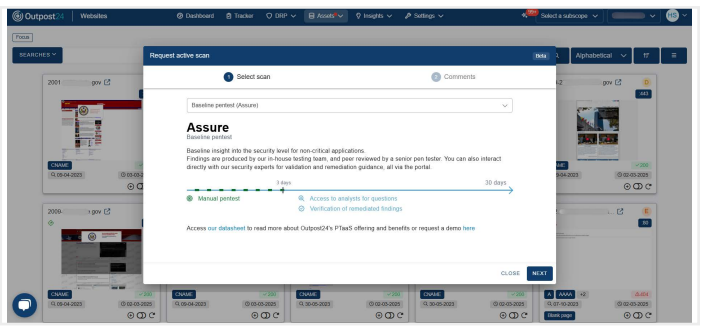
CyberFlex

Gelişen Saldırı Yüzeyine Karşı Kapsamlı Bir Uygulama Güvenliği Stratejisi

Uygulama saldırı yüzeyi büyüdükçe, birçok kuruluş saldırı yüzeyi verilerini penetrasyon testi planlamalarıyla verimli bir şekilde ilişkilendirmekte zorlanmaktadır. Uygulama envanteri hakkında görünürlük ve farkındalık eksikliği, hem bilinen hem de bilinmeyen uygulamaların yeni güvenlik açıkları ve riskler oluşturması nedeniyle yanlış bir güvenlik algısına yol açabilir. Etkili iyileştirme süreçleri yürütmek ve veri ihlali riskini azaltmak için anlamlı ve aksiyona dönüştürülebilir içgörülere erişim kritik önem taşır. Outpost24 CyberFlex ile uygulama güvenliği stratejinizin hayata geçirilmesini desteklemede, yetkisiz erişimleri önlemede ve uygulamalarınızın bütünlüğünü ile erişilebilirliğini korumada önemli bir rol üstleniyoruz. Kapsamlı uygulama güvenliği önlemlerini hayata geçirerek riskleri azaltabilir, marka itibarınızı koruyabilir ve müşterileriniz ile paydaşlarınızın güvenini sürdürebilirsiniz. Kapsamlı Attack Surface Management ve isteğe bağlı Penetration Testing as a Service (PTaaS) çözümümüz ile uygulama güvenliği stratejinizi güçlendirin. Hizmetimiz, saldırı yüzeyinizi analiz ederek daha ayrıntılı değerlendirme gerektiren en yüksek riskli uygulamaları belirler ve güvenlik ekibinizin en kritik alanlara odaklanmasını sağlar. Ölçeklenebilir ve esnek çözümümüz, yıllık penetrasyon testi çalışmalarınız boyunca bütçenizi en verimli şekilde kullanmanıza yardımcı olurken iş süreçlerinizi yavaşlatmaz. CyberFlex ile güvenlik çalışmalarınızı optimize etmek ve riskleri azaltmak için ihtiyaç duyduğunuz araçlara, uzman rehberliğine ve stratejik içgörülere tek bir platform üzerinden erişebilirsiniz.



Uygulama Envanteri



Uygulama Penetrasyon Testi Hizmeti (PTaaS)

Temel Kullanım Senaryoları

Sürekli Uygulama Keşfi ve İzleme

Bilinen ve bilinmeyen uygulama envanterinizi analiz ederek güvenlik açıklarına ilişkin kapsamlı görünürlük sağlar, riskleri bağlamsal olarak değerlendirir ve potansiyel etki seviyelerine göre önceliklendirilmiş öneriler sunar.

Saldırı Yüzeyi Puanlama ve Risk Önceliklendirmesi

Uygulamalarınızı ve maruziyet seviyelerini analiz ederek saldırı yüzeyinizi risk bazlı puanlandırır. Güvenlik açıklarına ilişkin kapsamlı içgörüler sunar.

Kapsamlı Risk Değerlendirmesi

Kullanım, sahiplik ve konum gibi kritik faktörleri dikkate alarak ayrıntılı risk sınıflandırması ve güvenlik derecelendirmesi sunar. Birleşik PTaaS değerlendirmesi sayesinde uygulama risklerini daha etkin yönetmenize, güvenlik önceliklerinizi belirlemenize ve iyileştirme süreçlerinizi optimize etmenize yardımcı olur.

İyileştirme ve Uyumluluk

Tam görünürlük sağlayarak yamalanmamış yazılımları tespit edin, kullanılmayan saldırı giriş noktalarını ortadan kaldırın ve saldırı yüzeyinizi azaltın. Kuruluşunuz büyüdükçe iyileştirme süreçlerini hızlandırarak sürekli uyumluluğu koruyun ve güvenlik duruşunuzu güçlendirin.

Saldırı Yüzeyi Yönetimi ve Penetrasyon Testlerinde Uzman Rehberliği

- Hangi bilinen ve bilinmeyen uygulamalarım şu anda internete açık durumda?
- Sahip olduğum uygulamalar arasında en yüksek riski hangileri taşıyor?
- İhlal riskini azaltmak için hangi uygulama güvenlik açıklarına öncelik vermeliyim?
- Penetrasyon testi süreçlerim ne kadar etkili?
- Saldırı yüzeyine eklenen yeni uygulamaları nasıl sürekli izleyebilirim?
- Daha kapsamlı güvenlik testlerini hızlandırmak için tüm riskli uygulamaları tespit edebilir miyim?
- Shadow IT varlıklarını nasıl tespit edip etkin şekilde yönetebilirim?
- Penetrasyon testi yatırımlarımdan nasıl maksimum değer elde edebilirim?
- Yeni düzenlemelere ve uyumluluk gereksinimlerine sürekli olarak uyum sağlayacağımdan nasıl emin olabilirim?

Kapsamlı Uygulama Güvenliği Stratejisi

SecOps

Tüm dijital varlıklarınız ve uygulama güvenliği duruşunuz hakkında kapsamlı görünürlük elde ederek güvenliği ön planda tutun. Derinlemesine analizlerimiz, geliştirme ekiplerinizi güçlendirir ve Application Security programlarınızı destekleyerek iş açısından kritik uygulamaların güvenlik açıklarından arındırılmış şekilde yayınlanmasına yardımcı olur. Böylece marka itibarınızı korurken güvenlikten ödün vermeden büyümenizi desteklersiniz. Esnek kullanım bazlı fiyatlandırma modeli ve entegre platform yapısı sayesinde daha ileri testler gerektiren tüm riskleri kolayca belirleyebilir, güvenlik yatırımlarınızdan maksimum verim (ROI) elde edebilir ve uyumluluk gereksinimlerini güvenle karşılayabilirsiniz.

DevSecOps

Application Security uzmanlarımız, sürekli geri bildirim ve detaylı güvenlik önerileri sunarak geliştiricilerin kritik güvenlik açıklarını bir sonraki geliştirme aşamasına geçmeden önce proaktif şekilde gidermesine yardımcı olur. Kapsamlı bir uygulama envanteri oluşturarak ve ek penetrasyon testleri için öneriler sunarak güvenlik açıklarının erken aşamada tespit edilmesini sağlar. Ayrıca, kritik riskleri önceliklendiren aksiyona dönüştürülebilir bir iyileştirme listesi oluşturarak geliştirme ekiplerinin en önemli güvenlik açıklarına öncelik vermesine, daha bilinçli kararlar almasına ve güvenlik yatırımlarından daha yüksek verim elde etmesine destek olur.

M&A

Birleşme ve satın alma (M&A) süreçlerinde, yeni edinilen kuruluşun uygulama ekosistemini anlamak, ilişkili güvenlik risklerini değerlendirmek ve sonraki adımlara yönelik doğru kararlar almak kritik önem taşır. Tüm uygulamaları manuel olarak tespit etmek ve test etmek zaman alıcı olmasının yanı sıra güvenlik açıklarının gözden kaçmasına neden olabilir. Outpost24, otomatik keşif yetenekleri, kapsamlı görünürlük ve detaylı risk raporları sunarak eksiksiz bir uygulama güvenliği değerlendirmesi sağlar. Böylece kuruluşlar stratejik kararlarını güvenle alabilir, potansiyel siber tehditleri proaktif olarak yönetebilir ve M&A süreçlerinde güvenlik risklerini en aza indirebilir.

Temel Ürün Özellikleri

7/24 Sürekli İzleme

Saldırı yüzeyinizi ve uygulama risklerinizi 7/24 sürekli izleyerek potansiyel tehditleri erken aşamada tespit edin. Sürekli risk sınıflandırması sayesinde uygulamalarınızı saldırganlar istismar etmeden önce koruyun ve proaktif bir güvenlik yaklaşımı benimseyin.

Kapsamlı Keşif

İnternete açık uygulamalarınızı otomatik olarak keşfeder, haritalandırır ve analiz eder. Bilinen uygulamaların yanı sıra görünmeyen veya farkında olmadığınız varlıkları da tespit ederek saldırı yüzeyiniz üzerinde tam görünürlük sağlar.

Etkileşimli Gösterge Paneli

Uygulama saldırı yüzeyinize ilişkin kapsamlı analizler ve detaylı güvenlik önerileri sunan etkileşimli gösterge paneli sayesinde riskleri derinlemesine inceleyin,

Aksiyona Dönüştürülebilir Sonuçlar

Application Security uzmanlarımız uygulama risklerinizi detaylı şekilde analiz ederek doğrulanmış bulgular ve uygulanabilir güvenlik önerileri sunar.

Özelleştirilebilir Uyarılar ve Raporlama

İhtiyaçlarınıza göre tamamen özelleştirilebilen uyarı ve raporlama özellikleriyle kritik güvenlik olaylarını anında takip edin. Esnek yapı sayesinde güvenlik süreçlerinizi daha etkin yönetin.

Esnek Kullanım Bazlı Lisanslama

Kullanım bazlı esnek fiyatlandırma modeli sayesinde güvenlik bütçenizi en yüksek risk taşıyan uygulamalara yönlendirin.