OTD BİLİŞİM
GLOBAL VAD

Outpost24

Penetrasyon Testi ve Red Team Operasyonları

Kapsamlı Penetrasyon Testi ve Güvenlik Değerlendirmesi

Güvenlik seviyeniz hakkında kapsamlı bir görünürlük elde etmek karmaşık ve zaman alıcı olabilir. Outpost24 Offensive Security ekibi; uygulamalar, ağlar, mobil platformlar ve diğer kritik sistemler için kapsamlı penetrasyon testleri gerçekleştirerek gizli güvenlik risklerini ortaya çıkarır. Uzman analizleri sayesinde mevcut güvenlik duruşunuzu değerlendirir, savunma mekanizmalarınızı güçlendirmek için uygulanabilir öneriler sunar. Yüksek yetkinliğe sahip sertifikalı etik hackerlardan oluşan ekibimiz, farklı sektörlerde edindiği deneyimle güvenlik açıklarını gerçek saldırgan teknikleri ve güncel saldırı senaryolarını kullanarak tespit eder ve doğrular. Penetrasyon testleri ve Red Team değerlendirmeleri, Continuous Threat Exposure Management (CTEM) yaklaşımının bir parçası olarak ağlarınız, uygulamalarınız ve sistemlerinizde istismar edilebilir zafiyetleri ortaya çıkararak güvenlik kontrollerinizi güçlendirmenize, ihlal riskini azaltmanıza ve siber dayanıklılığınızı artırmanıza yardımcı olur.

Hizmetlerimiz:

Uygulama Güvenliği

Web Uygulamaları ve API'ler: Web uygulamaları ve API'lerdeki güvenlik açıklarını belirlemek amacıyla tek seferlik kapsamlı güvenlik değerlendirmeleri gerçekleştirilir. Gerçek dünya saldırı senaryoları simüle edilerek kötü niyetli aktörler tarafından istismar edilebilecek potansiyel zafiyetler ortaya çıkarılır.

Mobil Uygulamalar: iOS ve Android platformlarında çalışan mobil uygulamalar, mobil ortamlara özgü güvenlik açıkları ve zafiyetleri tespit etmek amacıyla kapsamlı şekilde değerlendirilir.

Ağ ve Bulut Güvenliği

Bulut Altyapısı: Azure, AWS ve Google Cloud gibi platformlarda barındırılan API'ler, web uygulamaları ve veritabanları dahil olmak üzere bulut altyapınız detaylı şekilde analiz edilerek gizli güvenlik riskleri ortaya çıkarılır.s Azure, AWS and Google Cloud to uncover hidden risks.

Ağ Güvenliği: Ağ altyapısı ve kritik sistemler, otomatik, manuel ve özel geliştirilmiş güvenlik araçları kullanılarak kapsamlı şekilde değerlendirilir. Böylece istismar edilebilir güvenlik açıkları ve risk maruziyetleri tespit edilir.

Red Team ve Risk Değerlendirmesi

Assumed Breach (İhlal Varsayımı Değerlendirmesi): İç ağınız ve sistemleriniz, bir saldırganın ağ içinde yetki yükseltme yapabileceği güvenlik açıklarını, riskli kullanıcıları ve olası saldırı yollarını belirlemek amacıyla değerlendirilir.

Phishing Simülasyonları: Çalışanların sosyal mühendislik saldırılarına karşı farkındalığını ve dayanıklılığını ölçmek amacıyla phishing kampanyaları gerçekleştirilir. Böylece saldırganların hassas verilere erişme veya kurum ortamını ele geçirme riskleri değerlendirilir.

Red Teaming: Gerçek tehdit aktörlerinin kullandığı araçlar, taktikler ve prosedürler (TTP'ler) temel alınarak senaryo odaklı saldırı simülasyonları gerçekleştirilir. Önceden belirlenen kritik varlıklar (Crown Jewels) hedef alınarak olası saldırı yolları ortaya çıkarılır ve kuruluşun tespit ile müdahale yetenekleri kapsamlı şekilde doğrulanır.

Temel Kullanım Senaryoları

Güvenlik Kör Noktalarını Ortaya Çıkarın
Saldırgan bakış açısıyla gerçekleştirilen güvenlik değerlendirmeleri sayesinde ortamınızdaki gizli zayıflıkları ve güvenlik açıklarını tespit edin. Savunma mekanizmalarınızı güçlendirerek güvenlik boşluklarını proaktif şekilde kapatın ve olası siber ihlalleri gerçekleşmeden önce önleyin.

Uzman Liderliğinde Güvenlik İçgörüleri
Sertifikalı etik hackerlardan oluşan uzman ekibimiz, en güncel saldırı tekniklerini ve metodolojilerini kullanarak ortamınızı kapsamlı şekilde değerlendirir.

Güvenlik Doğrulaması
Mevcut güvenlik kontrollerinizin gerçek dünya saldırı senaryolarına karşı etkinliğini değerlendirerek güvenlik açıklarını doğrularız.

Kapsamlı Raporlama
Detaylı raporlarımız, tespit edilen güvenlik açıkları, istismar edilebilir zafiyetler ve bunların olası etkileri hakkında net görünürlük sunar. Önceliklendirilmiş iyileştirme önerileri sayesinde güvenlik ekipleriniz kritik risklere daha hızlı müdahale edebilir.

"Kapsamlı değerlendirmemiz sonucunda Outpost24'ü tercih ettik. Sunduğu çözüm ve hizmet kalitesinden son derece etkilendik."

BT Güvenlik Yöneticisi
Landsbankinn

Outpost24

Red Team Assessment

Kuruluşunuzun güvenlik duruşunu, gerçek dünya saldırı senaryolarını simüle eden Red Team Assessment hizmetimizle güçlendirin. Alanında uzman güvenlik ekibimiz, black-box yaklaşımıyla ön bilgiye ihtiyaç duymadan sistemlerinizi gerçek bir tehdit aktörü gibi değerlendirir. Bu sayede savunma yetenekleriniz kapsamlı şekilde test edilir, kritik varlıklarınız (Crown Jewels) korunur ve güvenlik yatırımlarınızdan maksimum verim elde etmeniz sağlanır. Siber, insan ve fiziksel güvenlik boyutlarını kapsayan değerlendirmelerimiz; phishing kampanyalarından fiziksel sızma testlerine ve ağ istismar senaryolarına kadar geniş bir yelpazede gizli güvenlik açıklarını ortaya çıkararak kuruluşunuzun siber dayanıklılığını artırır.

Temel Hizmetler:

Dijital Ayak İzi Değerlendirmesi

İnternete açık sistemleri, sızdırılmış bilgileri ve istismar edilebilir güvenlik açıklarını tespit ederek olası saldırı yollarını ortaya çıkarırız. Detaylı analizler ve kapsamlı raporlarımız sayesinde dijital varlıklarınızı koruyabilirsiniz.

İstihbarat Toplama

Uzman ekibimiz, kuruluşunuza ve hedef varlıklarınıza ilişkin açık kaynaklardan erişilebilen internet verilerini toplayıp analiz ederek kapsamlı bir risk değerlendirmesi oluşturur.

Saldırı Senaryoları

Gerçek tehdit aktörlerinin kullanabileceği yöntemleri temel alarak gerçekçi saldırı senaryoları tasarlarız. Toplanan istihbarat doğrultusunda en kritik tehditleri ve en uygun saldırı senaryolarını belirleyerek hedef odaklı güvenlik değerlendirmeleri gerçekleştiririz.

Fiziksel Sızma Testi

Siber güvenlik kontrolleri güçlü olsa bile saldırganlar fiziksel erişim sağlayarak ağınıza sızabilir. Uzman ekibimiz, kontrollü Red Team senaryoları kapsamında tesislerinize yönelik fiziksel sızma testleri gerçekleştirerek fiziksel güvenlik zafiyetlerini, erişim kontrollerini ve olası saldırı yollarını değerlendirir.

Medya Baiting ve Phishing Simülasyonları

Kuruluşunuzdaki güvenlik farkındalığını ölçmek amacıyla özel olarak hazırlanan USB bellekler, phishing kampanyaları ve kontrollü zararlı içerikler kullanılarak gerçek saldırı senaryoları simüle edilir.

Ağ İstismarı

İç ve dış ağlarınızda gerçekleştirilen kapsamlı güvenlik değerlendirmeleriyle istismar edilebilir güvenlik açıklarını tespit eder, tespit ve müdahale yeteneklerinizin etkinliğini ölçeriz.

CTEM Programınızı Başlatıyor veya Yeniden Canlandırıyor musunuz?

Bu çözüm, Sürekli Tehdit Maruziyeti Yönetimi (CTEM - Continuous Threat Exposure Management) programının Doğrulama (Validation) aşamasını destekler.

Gartner'a göre, 2026 yılına kadar yatırımlarını CTEM programına göre önceliklendiren kuruluşların siber güvenlik ihlali yaşama olasılığı 3 kat daha düşük olacaktır.