Privia SECURITY

Offensive as a Service

Profesyonel Offensive Security Hizmetleri

“Tüm Offensive Hizmetler Bir Arada!”

Küçükbakkalköy Mah. Kocasinan Cad.
Privia Plaza No:42 Ataşehir, İstanbul

+90 (216) 514 72 14

www.priviasecurity.com

"Profesyonel Offensive Hizmetlerimiz ile siber güvenlik operasyonlarınıza kapsamlı bir yaklaşım sunuyoruz. Tüm offensive hizmet ihtiyaçlarınızı tek bir hizmet çatısı altında alın, kullandığınız kadar ödeyin."

Profesyonel Offensive Hizmetlerimiz (OaaS), organizasyonların siber güvenlik olgunluğunu geliştirmeleri ve olası tehditlere karşı hazırlıklı olmaları için hazırlanmıştır. Siber saldırı yöntemlerinin taktiklerini ve tekniklerini kullanarak sistemlerin, donanımların, ağların ve uygulamaların güvenliğini test ediyoruz. Organizasyonların siber dünyadaki saldırılara karşı daha güvenli bir altyapı oluşturmasına yardımcı oluyoruz.

Offensive as a Service Hizmetimiz, siber güvenlik ekibimizin uzmanlığıyla ağlarınız, uygulamalarınız, donanımlarınız ve sistemleriniz için kapsamlı güvenlik testleri gerçekleştirir. Saldırganların bakış açısıyla gerçekleştirilen testler, güvenlik açıklarını tespit etmenizi ve gerekli düzenleyici/önleyici faktörleri uygulamanızı sağlar.

Profesyonel offensive hizmetlerimiz, sürekli gelişen siber tehdit ortamına karşı güncel kalmanızı ve güvenlik stratejilerinizi dinamik bir şekilde yönetmenizi destekler. Hizmet kapsamında sunulan detaylı raporlar ve çözüm önerileriyle, güvenlik politikalarınızı güçlendirebilir ve risklerinizi minimize edebilirsiniz.

Hizmete Ait Bileşenler

Sızma Testleri (Penetrasyon Testleri)

Sızma testleri, sistemlerinizin ve ağlarınızın güvenlik seviyesini değerlendirmek için saldırgan yöntemleri kullanarak gerçekleştirilen kapsamlı testlerdir. Testler sırasında, siber güvenlik uzmanlarımız olası zafiyetleri tespit etmek için çeşitli araçlar ve teknikler kullanır. Sızma testleri, hem dışarıdan gelebilecek tehditlere karşı (external penetration testing) hem de içeriden gelebilecek tehditlere karşı (internal penetration testing) sistemlerinizi test eder. Testler sonucunda, tespit edilen zafiyetlerin organizasyonunuza olası etkileri analiz edilir ve önceliklendirilir.

Sosyal Mühendislik Testleri

Sosyal mühendislik testleri, insan faktörünün güvenlik üzerindeki etkisini ölçmek için tasarlanmış test yöntemidir. Sosyal Mühendislik Testleri, çalışanlarınızın güvenlik politikalarına ve prosedürlerine ne kadar uyduğunu değerlendirir. Phishing (oltalama) e-postaları, telefonla yapılan aldatıcı aramalar (Vishing) ve fiziksel erişim denemeleri gibi yöntemleri kullanabilir. Testler sonucunda, çalışanlarınızın hangi konularda daha fazla eğitime ihtiyaç duyduğu belirlenir. Sosyal mühendislik testleri, güvenlik kültürünüzü geliştirmek ve insan kaynaklı riskleri azaltmak için kritik öneme sahiptir.

Kaynak Kod Analizi

Kaynak kod analizi, uygulamalarınızın ve yazılımlarınızın güvenliğini sağlamak için gerçekleştirilen detaylı bir test türüdür. Statik kod analizi ile kodunuzun belirli kurallara ve standartlara uyumu kontrol edilir. Dinamik analiz ile uygulamalarınızın çalışma zamanındaki davranışları incelenir. Gerçekleştirilen analizler, kodlama hatalarından kaynaklanan güvenlik zafiyetlerini tespit eder. SQL injection, XSS (Cross-Site Scripting) ve güvenli olmayan veri işlemleri gibi yaygın zafiyetler tespit edilir. Kaynak kod analizi, yazılım geliştirme sürecine güvenlik önlemlerini entegre etmenize yardımcı olur.

Siber Tehdit İstihbaratı

Siber tehdit istihbaratı hizmetleri, organizasyonunuzun karşı karşıya olduğu potansiyel tehditleri önceden tespit etmenize yardımcı olur. Siber güvenlik uzmanlarımız dark web, deep web ve açık kaynaklar üzerinden organizasyonunuza yönelik tehditleri izler ve analiz eder. Olası saldırı planları, sızdırılmış veriler veya hedefli saldırı kampanyaları hakkında bilgi toplarız. Elde edilen bilgiler, güvenlik stratejilerinizi güncellemeniz ve önleyici tedbirler almanız için kullanılır.

Siber Güvenlik Danışmanlığı ve Eğitim

Profesyonel Siber Güvenlik Danışmanlığı ve eğitim hizmetlerimizle, organizasyonunuzun siber güvenlik olgunluğunu artırmayı hedefliyoruz. Siber Güvenlik Uzmanlarımız, güvenlik politikalarınızın ve prosedürlerinizin geliştirilmesi için size rehberlik eder. Risk değerlendirmeleri yaparak, güvenlik yatırımlarınızı en etkin şekilde planlamanıza yardımcı olur. Organizasyonunuzda yer alan ekiplerinizin siber güvenlik farkındalığını artırmak için özel eğitim programları oluştururuz.

Sık Sorulan Sorular

Düzenli zafiyet tarama hizmeti nedir ve neden önemlidir?

Düzenli zafiyet tarama hizmeti, bir kuruluşun bilgi teknolojileri (BT) altyapısındaki güvenlik zafiyetlerini sürekli olarak tespit etmek ve raporlamak amacıyla yapılan periyodik taramalardır. Siber tehditlerin ve saldırı yöntemlerinin sürekli evrim geçirdiği günümüzde, tek seferlik taramalar yeterli olmamakta. Düzenli taramalar, yeni ortaya çıkan zafiyetleri ve tehditlerin anında tespit edilmesine yardımcı olur. Periyodik taramalar ile güvenlik zafiyetleri siber saldırganlar tarafından istismar edilmeden önce tespit edilip giderilir.

Düzenli zafiyet taraması ile sızma testi arasındaki fark nedir?

Düzenli zafiyet taraması, otomatik araçlar kullanılarak sistemlerdeki bilinen güvenlik zafiyetlerini tespit etmeye odaklanır ve genellikle geniş kapsamlıdır. Sızma testi ise bir saldırganın bakış açısıyla sistemlere manuel olarak sızmaya çalışarak, zafiyetlerin gerçekten istismar edilip edilemeyeceğini test eder. Zafiyet taramaları hızlı ve sık yapılabilirken, sızma testleri daha derinlemesine ve daha az sıklıkla gerçekleştirilir. İkisi birlikte kullanıldığında hem yüzeysel hem de derinlemesine güvenlik değerlendirmesi yapılmış olur.

Düzenli zafiyet taramaları ne sıklıkla yapılmalıdır?

Tarama sıklığı, organizasyonunuzun büyüklüğüne, sektörüne ve risk profilinize bağlıdır. Genel olarak, aylık veya haftalık taramalar önerilir. Ancak kritik sistemlere sahip organizasyonlar için daha sık taramalar gerekebilir. Yeni sistemlerin eklenmesi, büyük güncellemeler veya güvenlik olayları sonrasında da zafiyet taraması yapılması önemlidir. Düzenli taramalar, sürekli değişen tehdit ortamına karşı güncel kalmanızı sağlar.

Hangi sistemler ve uygulamalar düzenli zafiyet tarama hizmetine dahildir?

Hizmet kapsamında ağ cihazları, sunucular, masaüstü ve dizüstü bilgisayarlar, mobil cihazlar, web uygulamaları, veritabanları ve bulut hizmetleri gibi tüm bilişim varlıkları (IT/BT) taranabilir. IoT cihazları ve endüstriyel kontrol sistemleri (EKS) gibi özel sistemler de dahil edilebilir. Özellikle OT/EKS/SCADA ağlarına yönelik oluşturulmuş, özel politikalar ile düzenli zafiyet taraması gerçekleştirilmelidir. Tarama kapsamı, organizasyonun ihtiyaçlarına ve güvenlik hedeflerine göre özelleştirilebilir.

Tarama işlemleri sırasında sistem performansı etkilenir mi?

Tarama işlemleri, sistemlerin performansını minimum düzeyde etkileyecek şekilde planlanır ve gerçekleştirilir. Tarama araçları, ağ ve sistem kaynaklarını aşırı tüketmeyecek şekilde yapılandırılır (DDoS ve Yük Testleri hariç). Tarama zamanlaması, organizasyonun yoğun olmayan saatlerine denk gelecek şekilde planlanabilir.

Tarama sonuçları nasıl raporlanır ve bu raporlar nasıl kullanılır?

Tarama sonuçları detaylı ve anlaşılır raporlar halinde sunulur. Raporlarda tespit edilen zafiyetlerin açıklamaları, risk seviyeleri, etkilenen varlıklar ve önerilen çözüm yolları yer alır. Teknik ekipler, bu raporları kullanarak zafiyetleri önceliklendirir ve giderme süreçlerini başlatır. Yöneticiler için hazırlanan özet raporlar, stratejik karar alma süreçlerinde destek sağlar.

Düzenli zafiyet tarama hizmetinin maliyeti nedir?

Hizmetin maliyeti, taranacak sistemlerin sayısı, karmaşıklığı, tarama sıklığı ve ek hizmetlere bağlı olarak değişir. Özelleştirilmiş bir teklif almak için ihtiyaçlarınızın detaylı bir şekilde değerlendirilmesi gerekir. Uzun vadede, düzenli zafiyet taramaları olası siber saldırıların ve veri ihlallerinin neden olacağı maliyetlerin önüne geçerek tasarruf sağlar.

Düzenli zafiyet tarama hizmeti yasal uyumluluğa nasıl katkı sağlar?

Düzenli zafiyet taramaları, KVKK, ISO 27001, PCI DSS gibi yasal düzenlemeler ve standartların gerektirdiği periyodik güvenlik kontrollerini karşılar. Hizmet, yasal yükümlülüklerinizi yerine getirmenize ve denetim süreçlerinde başarılı olmanıza yardımcı olur. Müşteri ve iş ortaklarınızın verilerini koruyarak güvenilirliğinizi artırır.

Düzenli zafiyet tarama hizmeti siber riskleri tamamen ortadan kaldırır mı?

Düzenli zafiyet taramaları, siber riskleri önemli ölçüde azaltır ancak tamamen ortadan kaldıramaz. Siber güvenlik, çok katmanlı bir savunma yaklaşımı gerektirir ve zafiyet taramaları bu stratejinin bir parçasıdır. Diğer güvenlik önlemleriyle (güvenlik duvarları, antivirüs yazılımları, sızma testleri, kullanıcı eğitimi vb.) birlikte işletildiğinde en etkili sonucu verir. Sürekli izleme ve iyileştirme, siber güvenlik risklerini en düşük seviyeye indirir.

Siber Güvenlikte Doğru Çözüm Ortağınız

2018 yılında siber güvenliğin geleceği için yola çıkan Privia Security, kuruluşundan bu yana, müşterilerine yüksek kaliteli hizmet sunmayı amaçlamaktadır. Güçlü ve yetenekli ekibimiz, siber güvenliğin her alanında hizmet verdiğimiz organizasyonlara en güvenilir ve kapsamlı çözümleri sunarak, organizasyonların dijital dünyadaki güvenlik ihtiyaçlarını karşılamaktadır.

Günümüzde hızla gelişen ve karmaşık hale gelen siber tehditlerle mücadele etmek giderek zorlaşıyor. Bu noktada Privia Security olarak, müşterilerimize ihtiyaç duydukları hem defansif hem de ofansif siber güvenlik stratejilerini en ileri teknolojiyle sunuyoruz. İnovatif AR-GE ürünlerimiz ve stratejik danışmanlığımız sayesinde organizasyonların siber güvenlik olgunluğunu artırmayı ve onlara proaktif çözümler sunmayı hedefliyoruz. Şu anda 300'den fazla büyük kuruluşun güvenliğini sağlamaktan gurur duyuyoruz.

Uluslararası ve Yerel Siber Güvenlik Çözümleri

Privia Security olarak, Avrupa, Asya, Ortadoğu ve Amerika dahil olmak üzere geniş bir coğrafyaya siber güvenlik hizmetleri sunmaktayız. Offensive, Defensive ve Forensic alanlarında uzmanlaşmış ekiplerimiz, kritik altyapılar, aviyonik sistemler, kurumsal ağlar ve askeri alanlar gibi farklı sektörlerde faaliyet gösteren organizasyonlara özel çözümler geliştirmektedir.

Ayrıca savunma kapasitelerini güçlendirmek isteyen ülkelere yönelik geliştirdiğimiz PriviaHub siber savaş simülasyonu ile siber savaş stratejilerinin test edilmesi, tatbikatların yürütülmesi ve uzmanların niteliklerinin ölçülmesi için kapsamlı çözümler sunuyoruz. Bu inovatif platform özel sektör, akademi ve askeri alanlarda tatbikat ihtiyaçlarını karşılamak üzere tasarlanmıştır.

İleri Teknoloji ile Güvenli Gelecek

İstanbul, Ankara, Londra ve Cumhuriyet Teknopark'taki Ar-Ge merkezimizde, müşterilerimize değer katan projeler geliştiriyoruz. Penetrasyon testleri, Red Team operasyonları, siber güvenlik eğitimleri ve kurumlara özel siber güvenlik çözümlerimizle sektörde fark yaratmaya devam ediyoruz. "Privacy For You" sloganımızla, güvenlik ve gizliliğe yenilikçi bir bakış açısı getiriyor ve müşterilerimizin dijital geleceğini güvence altına alıyoruz.

Privia
SECURITY