Privia SECURITY

Red Team Hizmeti

Profesyonel Offensive Security Hizmetleri

“Gerçek Saldırılara Hazırlıklı Olun!”

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

+90 (216) 514 72 14

www.priviasecurity.com

"Red Team hizmetimiz, siber tehditlere karşı hazırlığınızı artırmak için derinlemesine analiz ve simülasyonlar sunar. Zayıf noktalarınızı tespit ederek etkili savunma stratejileri geliştirebilirsiniz."

Red Team hizmetimiz, organizasyonlarınıza yönelik potansiyel siber tehditleri keşfetmek amacıyla tasarlanmış kapsamlı bir güvenlik testidir. Red Team hizmeti, gerçek dünya saldırı senaryolarını simüle ederek, güvenlik açıklarınızı ortaya çıkarmaya ve bunları gidermeye yönelik stratejiler geliştirmeye yardımcı olur. Saldırganların bakış açısıyla hareket ederek, zayıf noktalarınızı belirleyip, bu alanlarda alınması gereken önlemleri raporlar.

Red Team Hizmeti, MITRE ATT&CK çerçevesini temel alarak, gelişmiş saldırı tekniklerini ve taktiklerini kullanır. Organizasyonunun savunma altyapısının ne ölçüde etkin olduğunu değerlendirme fırsatı sağlar. Her bir test, özel olarak tasarlanmış senaryolarla yürütülerek, belirli tehdit gruplarının hedef alabileceği alanları belirler.

Red Team testleri, güvenlik ekibinizin becerilerini test etmekle kalmaz, aynı zamanda siber olay müdahale planlarınızı da gözden geçirmenizi sağlar. Zayıf noktaları ortaya çıkararak savunma stratejilerinizi güçlendirir ve gelecekteki saldırılara karşı hazırlıklı olmanızı sağlar. Sonuç olarak, organizasyonunuzun siber güvenlik olgunluğunu artırarak, potansiyel riskleri en aza indirir.

Sonuçların analiz edilmesi ve raporlanması aşamasında, her bir güvenlik açığı detaylı bir şekilde ele alınır ve uygulanabilir çözüm önerileri sunulur. Güvenlik ekibinizin önceliklendirilmesi gereken alanları belirlemesi kolaylaşır. Red Team hizmetimiz, siber güvenlikte proaktif bir yaklaşım benimsemek isteyen tüm organizasyonlar için kritik bir hamle sunar.

Hizmete Ait Bileşenler

Tehdit Modelleme

Tehdit modelleme, organizasyonunuzun karşılaşabileceği potansiyel siber saldırıların kapsamlı bir analizini sağlar. Saldırganların kullandığı taktikler, teknikler ve prosedürler (TTP'ler) incelenir, böylece savunma stratejilerinizi bu tehditlere göre uyarlamak mümkün hale gelir. Sonuç olarak, en büyük risklerinizi belirleyerek güvenlik önlemlerinizi daha etkili bir şekilde planlayabilirsiniz.

Gerçekçi Saldırı Senaryoları

Red Team hizmeti, organizasyonunuza özgü, gerçekçi saldırı senaryoları oluşturarak güvenlik zafiyetlerinizi test eder. Saldırganların davranışlarını simüle ederek, güvenlik sistemlerinizin ne kadar dayanıklı olduğunu ölçer. Her senaryo, sistemlerinizi hedef alan olası saldırıları keşfetmek için tasarlanmıştır ve sonuçları, güvenlik önlemlerinizi güçlendirmek için kullanılabilir.

Sızma Testleri

Sızma testleri, organizasyonunuzun güvenlik duvarlarını aşmaya çalışan siber saldırganların perspektifinden sistemlerinizi değerlendirmeyi amaçlar. Yetkilendirilmemiş erişim ve veri sızıntısı gibi tehditleri önlemek için kritik bir öneme sahiptir. Sızma testleri sonucunda elde edilen bulgular, güvenlik zafiyetlerinizi kapatmak için gerekli adımları belirlemenize yardımcı olur.

Kapsamlı Analiz ve İyileştirme Önerileri

Red Team hizmetinin bir parçası olarak, gerçekleştirilen tüm testlerin ardından kapsamlı bir analiz süreci başlar. Tespit edilen zayıf noktalar detaylı bir şekilde ele alınarak, hangi alanlarda iyileştirmelerin gerektiği belirlenir. Elde edilen bilgi, belge ve bulgular doğrultusunda önerilen stratejiler, organizasyonun güvenlik altyapısının daha da güçlenmesine katkı sağlar.

Raporlama ve Analiz

Red Team çalışmaları sonrasında, ayrıntılı bir raporlama süreci başlar. Raporlar testlerin bulgularını, analizlerini ve önerilen iyileştirme stratejilerini içerir. Raporlama, yöneticilere ve güvenlik ekiplerine net bir bakış açısı sunarak, hangi alanlarda gelişme kaydedilmesi gerektiğinin belirlenmesine yardımcı olur.

Sürekli Eğitim ve Farkındalık Programları

Red Team hizmetinin etkili olabilmesi için, çalışanların siber güvenlik konusundaki farkındalıklarını artırmak da kritik bir bileşendir. Önerilen programlar, sosyal mühendislik testleri ve simülasyonlar aracılığıyla, çalışanların potansiyel tehditlere karşı ne kadar bilinçli olduğunu değerlendirir. Sürekli eğitimler, güvenlik kültürünün güçlendirilmesine ve çalışanların tehditlere karşı daha hazırlıklı olmalarına yardımcı olur.

Sosyal Mühendislik Testleri

Sosyal mühendislik testleri, çalışanlarınızın siber tehditlere karşı bilinçli olmasını sağlamak için kritik bir bileşendir. Sosyal mühendislik testleri, çalışanların bilgi güvenliği konusunda ne kadar bilgi sahibi olduğunu ve sosyal mühendislik saldırılarına karşı ne kadar dirençli olduklarını değerlendirir. Elde edilen veriler, güvenlik farkındalığını artırmaya yönelik eğitim ve iyileştirme stratejileri geliştirmek için kullanılabilir.

Fiziksel Güvenlik Testleri

Fiziksel güvenlik testleri, organizasyonunuzun fiziksel alanlarının güvenliğini değerlendirir ve bu alanlara yönelik olası tehditleri simüle eder. Fiziksel testler, binaların, veri merkezlerinin ve diğer kritik alanların fiziksel güvenlik önlemlerinin ne kadar etkili olduğunu ölçer. Ayrıca, çalışanların fiziksel güvenlik protokollerine uyumunu değerlendirmek ve zayıf noktaları tespit etmek için de önemli bir bileşendir.

Sık Sorulan Sorular

Red Team hizmeti nedir ve ne işe yarar?

Red Team, bir organizasyonun siber güvenlik sistemlerinin zayıflıklarını belirlemek için saldırgan perspektifinden testler gerçekleştiren bir hizmettir. Red Team Hizmeti, siber tehditleri simüle eder ve potansiyel saldırı senaryolarını uygulayarak sistemlerin durumunu değerlendirir. Organizasyonların güvenlik açıklarını tespit etmesine ve iyileştirme yapmasına olanak tanır.

Red Team hizmetinin faydaları nelerdir?

Red Team hizmeti, organizasyonların güvenlik zafiyetlerini tespit etmeye ve zayıf noktaları belirlemeye yardımcı olur. Gerçekçi saldırı senaryoları uygulayarak, potansiyel tehditleri ve zafiyetleri önceden tanımlamak için değerli bilgiler sağlar.

Red Team ile Blue Team arasındaki farklar nelerdir?

Red Team, siber saldırganların perspektifinden organizasyonun savunma sistemlerini test ederken, Blue Team, savunma sistemlerini koruma ve iyileştirme görevini üstlenir. Red Team, saldırı simülasyonları gerçekleştirirken, Blue Team, bu saldırılara karşı nasıl bir yanıt verileceğini planlar ve uygular. İki ekip arasındaki iş birliği, organizasyonun genel siber güvenlik stratejilerini güçlendirir.

Red Team simülasyonları nasıl gerçekleştirilir?

Red Team simülasyonları, öncelikle tehdit modelleme ve senaryo geliştirme ile başlar. Ardından bu senaryolar doğrultusunda sistemlere saldırılar gerçekleştirilir. Simülasyonlar, organizasyonun güvenlik sistemlerinin etkinliğini test ederek zayıf noktaları ortaya çıkarır. Testlerin sonunda elde edilen bilgi, belge ve bulgular, analiz edilerek raporlanır ve iyileştirme önerileri sunulur.

Red Team hizmeti almak için hangi metodolojiler kullanılır?

Red Team hizmetleri, MITRE ATT&CK çerçevesi gibi çeşitli metodolojik yaklaşımları kullanarak güvenlik zafiyetlerini belirler. Hizmet kapsamında kullanılan çerçeveler (Framework), sistematik bir değerlendirme yaparak, zayıf noktaların tespit edilmesini ve güvenlik önlemlerinin optimize edilmesini sağlar. Metodolojiler, organizasyonun ihtiyaçlarına göre özelleştirilebilir.

Siber güvenlikte Red Team neden önemlidir?

Red Team, organizasyonların güvenlik açıklarını gerçekçi senaryolarla test ederek, siber tehditlere karşı hazırlıklı olmalarını sağlar. Red Team hizmeti, zayıf noktaların keşfedilmesi ve zayıflıkları tespit edilen alanların güçlendirilmesi yoluyla potansiyel siber saldırıların önlenmesine yardımcı olur.

Red Team testleri hangi aşamalardan oluşur?

Red Team testleri genellikle planlama, keşif, yürütme ve analiz aşamalarını içerir. İlk aşamada, testin kapsamı belirlenir. Keşif aşamasında, hedef sistemler hakkında bilgi toplanır. Yürütme aşamasında saldırılar simüle edilir ve son olarak, analiz aşamasında elde edilen bulgular raporlanarak iyileştirme önerileri sunulur.

Red Team hizmeti ile düzenlemelere uyum nasıl sağlanır?

Red Team hizmetleri, organizasyonun siber güvenlik protokollerini mevcut yasal ve endüstri düzenlemelerine uyumlu hale getirmek için kullanılır. Test sürecinde, tespit edilen güvenlik açıkları ve riskler, düzenlemelere uygun şekilde raporlanır ve düzeltme adımları önerilir. Organizasyonlar yasal yükümlülüklerini yerine getirirken aynı zamanda güvenlik seviyelerini de artırmış olurlar.

Red Team çalışmaları sonuçları nasıl raporlanır?

Red Team çalışmaları sonrasında, elde edilen bilgi, belge ve bulgular kapsamlı bir rapor halinde sunulur. İlgili rapor, tespit edilen güvenlik zafiyetlerini, zayıf noktaları, zararlı yazılım kodlarını, senaryo dahilinde üretilen saldırı amaçlı donanımları ve bu alanlarda yapılması gereken iyileştirmeleri içerir. Rapor, yöneticilere ve güvenlik ekiplerine, uzun vadeli stratejik kararlar almak için gerekli bilgileri sağlar.

Sızma testi ile Red Team hizmeti arasındaki farklar nelerdir?

Sızma testleri, genellikle belirli bir sistem veya uygulamanın güvenliğini değerlendirmek için yapılan sınırlı testlerdir. Red Team hizmeti ise daha geniş kapsamlı ve gerçekçi saldırı senaryoları içerir. Red Team, siber saldırganın perspektifinden organizasyonun genel güvenlik durumunu değerlendirirken, sızma testleri belirli bir hedef üzerinde yoğunlaşır. Her iki hizmet de organizasyonun güvenlik seviyesini artırmak için kritik öneme sahiptir, ancak farklı yaklaşımlar ve kapsamlar içerirler.

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