Privia SECURITY

# Sızma (Penetrasyon) Testi

## Profesyonel Offensive Security Hizmetleri

"Zafiyetleri Tespit Edin, Riskleri Yönetin!"



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

+90 (216) 514 72 14

www.priviasecurity.com

*“Gerçek zamanlı testlerle, zayıf noktalarınızı belirleyip bu alanlardaki kaslarınızı güçlendiriyoruz.”*

Pentest hizmeti olarak da bilinen sızma testi, bilişim sistemlerindeki sorun, hata ve zafiyetleri ortaya çıkararak herhangi bir güvenlik zafiyetini önlemek ve sistemleri daha güvenli hale getirmek amacı ile alanında uzman kişiler tarafından gerçekleştirilen özel bir siber güvenlik danışmanlık hizmetidir.

Kurumların siber saldırılara karşı güvenlik seviyelerini değerlendirmeyi ve tespit edilen riskleri yönetmeyi amaçlayan sızma testleri, zafiyetleri tespit etmenin ötesinde tespit edilen zafiyetleri kullanarak ilgili sistemde yetkili erişimlerin nasıl elde edilebileceğini ve nelerle sonuçlanabileceğini gösterir. Ayrıca sistemin güçlü yönlerini de göstererek tam bir risk değerlendirmesi yapılmasını sağlar.

Her bir varlık türüne göre önceden belirlenen senaryolar dahilinde uygulanan sızma testi, gerek ulusal gerekse de uluslararası metodolojik yaklaşımlar temel alınarak gerçekleştirilir. Gerçekleştirilen test sonrasında uzman ekibimiz tarafından hazırlanan raporla daha hedeflenmiş ve etkili bir güvenlik değerlendirmesi sağlanır.

# Hizmete Ait Bileşenler

### Test Metodolojisi ve Yaklaşım Belirleme

Sızma testlerinin başarısı, uygulanan metodolojinin doğruluğuna bağlıdır. Black Box (kara kutu), White Box (beyaz kutu) ve Grey Box (gri kutu) yaklaşımları, sistemlerin farklı açılardan test edilmesini sağlar. OWASP ve NIST gibi uluslararası standartlara uygun olarak, testlerin kapsamı belirlenir. Her test metodu, sistemin iç ve dış tehditlere karşı nasıl performans gösterdiğini anlamaya yardımcı olur. Bu yaklaşım, hem tehdit modellemesi yaparak zafiyetleri önceden görmeyi hem de saldırı simülasyonları ile savunmanın zayıf noktalarını tespit etmeyi sağlar.

### Bilgi Toplama ve Zafiyet Analizi

Bilgi toplama aşamasında, sistem hakkında pasif ve aktif araştırmalar yapılarak potansiyel saldırı yüzeyi belirlenir. DNS taramaları, port taramaları ve sosyal mühendislik gibi yöntemler kullanılır. Zafiyet analizinde otomatik tarama araçlarının yanı sıra manuel testlerle derinlemesine analizler gerçekleştirilir. Bu süreçte elde edilen bilgiler, olası saldırı yüzeyini daraltmak ve riskleri önceden görmek için kritik öneme sahiptir. Amaç, tüm güvenlik açıklarını önceden belirleyerek önlem almaktır.

### Kimlik Doğrulama ve Erişim Yönetimi Testleri

Sistemlerin kimlik doğrulama ve erişim yetkileri, siber güvenlik açısından kritik bileşenlerdir. Bu aşamada, çok faktörlü kimlik doğrulama (MFA) ve oturum yönetimi gibi mekanizmalar test edilir. Erişim kontrollerinde zafiyet olup olmadığı tespit edilerek yetkisiz erişimlerin önüne geçilir. Rol tabanlı erişim kontrolü (RBAC) gibi modellerin doğru şekilde uygulandığı doğrulanır. Gerçekleştirilen testler, sistemin güvenlik politikalarının ne kadar güçlü olduğunu ortaya koyar.

### Ağ Güvenliği ve Şifreleme Analizi

Ağ güvenliği testlerinde, sistemler arası veri trafiği ve şifreleme protokolleri detaylı bir şekilde incelenir. HTTPS, TLS gibi güvenli iletişim protokollerinin etkinliği doğrulanır. Yanlış yapılandırılmış ağlar ve zayıf şifreleme algoritmaları tespit edilerek raporlanır. Ağ segmentasyonu ve güvenlik duvarı politikalarının etkinliği de değerlendirilir.

### Sızma ve Hak-Yetki Yükseltme

Bu evrede, tespit edilen zafiyetler üzerinden sistemlere sızma girişimleri gerçekleştirilir. Saldırgan perspektifiyle yapılan testler, zafiyetlerin gerçek dünyada nasıl kullanılabileceğini gösterir. Hak yükseltme adımlarıyla, yetkili erişim elde edilip sistemde daha yetkili seviyelere (Örn, AD, FW, KVM vb.) ulaşılması sağlanır. Hedef, saldırganların gerçekleştirebileceği her türlü hareketi önceden simüle etmektir.

### Raporlama ve Çözüm Önerileri

Testlerin sonunda, tespit edilen zafiyetlerin ve risklerin detaylı bir raporu hazırlanır. Raporlar, her zafiyetin önem derecesini belirterek önceliklendirme yapar. Ayrıca, her bir zafiyet için teknik çözüm önerileri sunulur ve iyileştirme yolları açıklanır. Yönetim seviyesinde sunulan özet raporlarla karar vericilere hızlı aksiyon alma imkanı sağlanır.

### Sürekli Güvenlik ve Uyumluluk Denetimi

Güvenlik tehditlerinin sürekli değişen doğası, sistemlerin düzenli olarak izlenmesini ve test edilmesini zorunlu kılar. Periyodik sızma testleri ve otomatik zafiyet taramalarıyla, yeni ortaya çıkan tehditlere karşı proaktif savunma sağlanır. PCI DSS, GDPR, ISO 27001, BDDK, TSE, EPDK, SPK ve SGT gibi standartlara uyumluluk denetimleri gerçekleştirilerek, yasal düzenlemelere tam uyum garanti altına alınır. Sürekli izleme ve iyileştirme süreçleriyle güvenlik açıklarının zamanında tespit edilmesi ve kapatılması sağlanır.

### Denetim ve Kapanış

Testlerin tamamlanmasının ardından, doğrulama denetimi gerçekleştirilir ve bulguların kapatıldığı kontrol edilir. Kapanış toplantısında, gerçekleştirilen testlerin sonuçları ve alınan aksiyonlar detaylandırılır. Elde edilen sonuçlara göre kalan riskler belirlenir ve çözüm önerileri sunulur. Nihai raporla birlikte, gelecekteki güvenlik adımlarını planlamak için stratejik öneriler sunulur. Test sürecinin bütüncül bir şekilde tamamlanmasını ve sistemlerin güvenli hale getirilmesini sağlar.

# Sık Sorulan Sorular

**Sızma testi nedir?**

Sızma testi, bir organizasyonun ağ, uygulama veya sistem güvenliğini değerlendirmek amacıyla gerçekleştirilen kontrollü siber saldırılardır. Testler ile, sistemdeki güvenlik zayıflıklarını belirlemek için saldırganların yöntemlerini simüle eder.

**Neden sızma testi yaptırmalıyım?**

Sızma testleri, organizasyonların veri güvenliğini sağlamak için kritik bir araçtır. Potansiyel zafiyetleri tespit ederek, bu zayıflıkları kapatmanıza ve olası siber saldırılara karşı proaktif bir savunma oluşturmanıza yardımcı olur. Ayrıca, yasal düzenlemelere uyum sağlamak ve müşteri güvenini artırmak da bu testlerin önemli faydalarındandır.

**Sızma testi ile otomatik zafiyet taraması arasındaki fark nedir?**

Otomatik zafiyet taramaları, bilinen güvenlik açıklarını tespit eden araçlardır, ancak sızma testleri daha derinlemesine bir analiz sunar. Sızma testleri, gerçek saldırı senaryolarını simüle ederek daha kapsamlı bir güvenlik değerlendirmesi yapar.

**Sızma testi süreci nasıl işler?**

Sızma testi süreci, uluslararası standartlara uygun olarak planlama, bilgi toplama, zafiyet analizi, exloitation, raporlama ve kapanış aşamalarından oluşur. İlk olarak, testin kapsamı ve hedefleri belirlenir, ardından pasif ve aktif bilgi toplama teknikleri kullanılarak sistem hakkında veri toplanır. Bu aşamada, güvenlik zafiyetleri tespit edilir ve otomatik araçlar ile manuel analizler yapılır. Sonraki aşamada, zafiyetler kullanılarak sistemlere sızma girişimleri gerçekleştirilir, bu da zayıf noktaların ne kadar etkili olduğunu gösterir. Test sonuçları, tespit edilen zafiyetlerin önceliklendirilmesi ve kapatılması için önerilerle birlikte detaylı bir raporla sunulur.

**Sızma testleri ne sıklıkla yapılmalıdır?**

Sızma testlerinin, genellikle altı ayda bir defa yapılması önerilmektedir. Ancak önemli sistem değişiklikleri veya yeni uygulama dağıtımı gibi durumlarda daha sık yapılması tavsiye edilir. Düzenli testler, yeni zafiyetlerin ortaya çıkmasını önlemek için gereklidir.

**Sızma testi sırasında sistemlerim etkilenir mi?**

İyi planlanmış bir sızma testi, sistemler üzerinde minimum etki bırakarak gerçekleştirilir. Ancak, her testin potansiyel bir etkisi olabileceğinden, önceden doğru iletişim kurulması ve dikkatli bir planlama yapılması önemlidir.

**Sızma testi sonrası ne tür raporlar alırım?**

Test tamamlandığında, tespit edilen zafiyetler ve önerilerle birlikte kapsamlı bir rapor sunulur. Bu rapor, teknik detayların yanı sıra yönetsel özetler içerir; böylece güvenlik iyileştirmeleri için gereken adımlar net bir şekilde ortaya konur.

**Sızma testi yasal bir zorunluluk mudur?**

Birçok sektörde yasal düzenlemeler, sızma testlerinin belirli aralıklarla yapılmasını zorunlu kılar. Özellikle enerji, finans, havacılık ve sağlık sektörleri gibi hassas veri barındıran alanlarda, bu testler yasal uyumluluğun sağlanması açısından kritik önem taşır.

**Sızma testinden sonra ne yapılmalıdır?**

Test sonuçlarına göre, tespit edilen zafiyetlerin önceliklendirilmesi ve giderilmesi gerekmektedir. Bu süreç, organizasyonun güvenlik duruşunu güçlendirmek ve potansiyel tehditleri en aza indirmek için sürekli bir iyileştirme sürecinin parçası olmalıdır.

## 1. Sızma testi evreleri nelerdir?

Privia Security, güvenlik açıklarını tespit etmek ve önlemek için kapsamlı bir analiz süreci izlediği sızma testlerinde, aşağıda belirlenen 13 evreden oluşan süreci işler.

- **Zafiyet Seviyelendirmesi:** Sızma testi sürecinde tespit edilen zafiyetler, sistemin güvenliğini tehdit ediş boyutları göz önünde bulundurularak seviyelendirilir.
- **Bilgi Toplama:** Kapsamlı bir sızma testi yapabilmek için hedef hakkında olası tüm bilgiler toplanır.
- **Pasif Bilgi Toplama:** Bilgi toplama evresinde hedef sistemler ile birebir iletişime geçilmeden, arama motorları aracılığıyla bilgi toplanır.
- **Aktif Bilgi Toplama:** Bilgi toplama evresinde hedef sistemler ile birebir iletişime geçilerek sistemler hakkında bilgi toplanır.
- **Port Tarama:** Bilgi toplama evresinin ardından hedefle ilgili tüm olası bilgiler elde edildiğinde, hedef network ve kaynaklarını analiz etmek için daha teknik bir yaklaşım uygulanır.
- **Zafiyet Tarama:** Hedef sisteme ait bilgi toplama, port tarama ve servis tespitinin ardından, elde edilen bilgiler değerlendirilerek zafiyet taraması gerçekleştirilir.
- **Enumeration:** Açık olduğu tespit edilen portları hangi servislerin kullandığı, bu servislerin hangi üreticiye ait servisler olduğu ve versiyonları gibi bilgiler öğrenilir.
- **Exploitation:** Zafiyet tarama ve enumeration evrelerinin ardından tespit edilen zafiyetler istismar edilmeye çalışılarak hedef sistem ve güvenliği üzerinde denemeler gerçekleştirilir.
- **Hak ve Yetki Yükseltme:** Tespit edilen zafiyetler istismar edilerek hedef sistem üzerinde erişim elde edilmeye çalışılır.
- **Post Exploitation:** İstismar sonrası evrede, ele geçirilen sistemin değerinin belirlenmesi ve sistemin daha sonra kullanmak üzere denetiminin sürdürülmesi gerçekleştirilir.
- **Yapılan İşlemleri Geri Alma:** Bu evrede, test bitirilmeden önce sistemler üzerinde yapılan tüm değişiklerin geriye alınır.
- **Raporlama:** Müşteri tarafından yazılı olarak istenmesi durumunda raporun matbu hali üzerine "Gizli" ibaresi vurularak kapalı bir zarf içerisinde teslim edilir.

- **Sunum:** Raporların tesliminden sonra istenmesi halinde kurum personeline, gerçekleştirilen sızma testine ilişkin özet mahiyetinde bir sunum yapılır. Bu sayede kurum personeli, sızma testini gerçekleştiren uzmanlarımızla test ile ilgili görüş alışverişinde bulunabilme imkânı kazanır.

## 2. Test sürecinde kullanılan araç ve metodolojiler nelerdir?

Sızma testlerimiz, hem ulusal hem de uluslararası metodolojik yaklaşımlar temel alınarak gerçekleştirilir ve güvenlik zafiyetlerini ortaya çıkarmak için hem dışarıdan (Internet) hem de içeriden (Internal) sızma testleri uygulanır. Bu yaklaşım, mevcut güvenlik açıklarını belirleyerek etkili bir risk analizi sağlar.

Testi ekibimiz otomatik zafiyet tarama uygulamalarına güvenmez. Gizli ve karmaşık güvenlik açıklarını tespit etmek için saldırı yüzeyi haritalama, ağ ve varlık keşfi gibi görevleri manuel olarak gerçekleştirmek için bir dizi açık kaynaklı ve ticari penetrasyon testi aracından yararlanır.

Yapmış olduğumuz testler, hedef sistemin aktif, dinamik ve statik analizini içeren OWASP (Open Web Application Security Project), PTES (Penetration Testing Execution Standard), OSSTM (Open Source Security Testing Methodology Manual), NIST ve ISSAF (Information Applications Security Assessment Framework) gibi güvenlik normlarına, metodolojilerine ve standartlarına dayanır.

Uyguladığımız sızma testi metodolojileri, iletişim ve kaynak optimizasyonu için standartlaştırılmış bir çerçeve sağlayarak gelişen siber tehditlere karşı savunmanın güçlendirilmesinde hayati bir rol oynar.

**OWASP:** Yaygın olarak bilinen bu standart, en son siber tehditlere ayak uyduran bir topluluk tarafından geliştirilir ve güncellenir. Uygulama açıklarının yanı sıra süreçlerdeki mantık hatalarını da hesaba katar.

**PTES:** Bilgi güvenliği uzmanlarından oluşan bir ekip tarafından tasarlanan bir pentest metodolojisidir. PTES'in amacı, sızma testleri için kapsamlı ve güncel bir standart oluşturmanın yanı sıra işletmeler arasında bir sızma testinden ne bekleneceği konusunda farkındalık yaratmaktır.

**OSSTMM:** En yaygın kullanılan ve tanınan sızma testi standartlarından biridir. Test uzmanları için uyarlanabilir kılavuzlar içeren sızma testine yönelik bilimsel bir yaklaşıma dayanır.

**NIST:** Testin doğruluğunu artırmaya yardımcı olmak için test ekibine çok özel sızma testi yönergeleri sunar. Çeşitli sektörlerdeki hem büyük hem de küçük şirketler, sızma testi için bu çerçeveden yararlanabilir.
**ISSAF:** Open Information Systems Security Group tarafından desteklenen bir pentesting kılavuzudur. Bu metodoloji artık güncellenmemektedir,bununla birlikte, kapsamlı doğası nedeniyle hala kullanılmaktadır.

## 4. Hangi sektörlerde sızma testi gereklidir?

Sağlık kuruluşları, kamu kurumları, Ar-Ge ağırlıklı şirketler, finans kurumları ve e-ticaret işletmeleri gibi hassas verileri işleyen veya siber saldırı riski yüksek olan şirketlerin en az üç ayda bir olmak üzere sızma testi yaptırmasını öneriyoruz.

Bu tür kuruluşlar, katı uyumluluk gereksinimleri ve verilerin tehlikeye girmesi durumunda daha yüksek risklerle karşılaşabilecekleri için düzenli olarak yapılan sızma testleri ile yasal uyumluluğu sağlarken veri ihlallerine karşı etkili bir savunma mekanizması geliştirebilir.

## 6. Sızma testinden sonra alınması gereken önlemler nelerdir?

Penetrasyon testi sonrasında şirketinize sunduğumuz raporu aldıktan sonra güvenlik açıklarını önceliklendirmek, düzeltme planı oluşturmak ve gerekli güvenlik önlemlerini hızla devreye sokmak için aşağıda sunduğumuz önerileri uygulayabilirsiniz:

**Güvenlik açıklarına öncelik verin:** Raporda belirttiğimiz güvenlik açıklarını, risk seviyelerine ve etkilerine göre önceliklendirin ve hangilerini önce ele alacağınıza karar verin.

**Sorumlulukları atayın:** Güvenlik açıklarını düzeltme sorumluluklarını geliştiriciler, BT personeli veya üçüncü taraf satıcılar gibi ilgili taraflara atayın. Düzeltmenin hedeflerini, kapsamını, zaman çizelgesini, beklenen sonuçlarını ve her bir tarafın rol ve sorumluluklarını iletin.

**Önerileri uygulayın:** Güvenlik açıklarını gidermek için penetrasyon testi raporumuzda bulunan önerileri uygulayın, herhangi bir sorunuz veya şüpheniz varsa bizimle iletişime geçin.

**Düzeltmeyi doğrulayın ve onaylayın:** Düzeltmenin başarılı olduğunu ve güvenlik açıklarının giderildiğini onaylayın. Ayrıca, belge ve kayıtlarınızı sistemin mevcut durumunu yansıtacak şekilde güncelleyin.

## 7. Sızma testi, sistemlerinizi nasıl etkiler?

Sızma testinin süresi; hedeflere, yaklaşıma ve test edilecek ortamın (saldırı yüzeyi) büyüklüğüne ve karmaşıklığına bağlıdır. Bir uygulama veya KOBİ (SMB) için yapılan sızma testi birkaç günde tamamlanabilir, ancak büyük ve karmaşık bir ortam daha uzun sürebilir. Test edilecek sistemlerin yapısı ve karmaşıklığı nedeniyle test süreci uzayabilir.

Tüm bu süreçte Privia Security, sızma testini en katı yasal ve teknik etik standartlara uygun olarak gerçekleştirilir. Testler, iş operasyonlarını aksatma riskini en aza indirirken çoğu durumda testin devam ettiğini bile anlaşılmadan operasyonel süreklilik devam eder. Kullanılabilirliği etkileyebilecek bir sistemi test etmemiz gerektiğinde, bu durum şirketinize bildirilir ve ihtiyaçlarınıza göre hareket edilir.

## 8. Sızma testi sonuçları ne kadar sürede raporlanır?

Privia Security tarafından yapılan bir sızma testinin tamamlanıp raporlanması ortalama 2 ila 4 hafta sürer. Fakat potansiyel saldırı yüzeyinin boyutu ve mevcut siber güvenlik savunmalarının kapsamı gibi faktörler bu süreyi etkileyerek sürecin artmasına neden olabilir.

Raporumuz öncelikle bir yönetici özeti ile başlar, güvenlik açıklarını ve bunların iş üzerindeki etkilerini özetler ve açıkları düzeltmek için önerilerde bulunur.

## 9. Sızma testini kimler gerçekleştiriyor?

Privia Security sızma testi, ulusal ve uluslararası (TSE, OSCP gibi) geçerlilikte sertifikasyonlara sahip personellerimiz tarafından gerçekleştirilmektedir.

Uzman ekibimiz çeşitli işletim sistemleri, ağlar ve uygulamalar hakkında güçlü bir anlayışa, güvenlik açıkları ve istismarları hakkında derin bir bilgiye, çeşitli güvenlik test araçları ve tekniklerinde yetkinliğe sahiptir.

## 10. Sızma testi sırasında elde edilen veriler nasıl korunur?

Privia Security tarafından yapılan bir sızma testinde, verilerin korunması için hem ulusal hem de uluslararası standartlara uygun güvenlik protokolleri uygulanır. Ayrıca, müşterilerimizle imzaladığımız Gizlilik Sözleşmesi (NDA) kapsamında, bu veriler kesinlikle üçüncü kişilerle paylaşılmaz. Test sürecinde elde edilen bilgiler yalnızca müşterinin güvenlik duruşunu iyileştirmek amacıyla kullanılır. Hazırlanan rapor iletildikten sona güvenli veri silme yönetmleriyle sistemlerden silinir.

## 12. Sızma testi, uyumluluk (compliance) gereksinimlerimizi karşılamaya nasıl yardımcı olur?

Privia Security tarafından yapılan bir sızma testinden sonra test ekibimiz bir pentest raporu hazırlar. Bu raporda, güvenlik açıkları ve düzeltme adımları belgeler halinde şirketinize sunulur. Güvenlik açıkları giderildikten sonra tüm boşlukların giderildiğini ve sisteminizin korunduğunu doğrulamak için yeniden tarama yapılır.

Bu tür bir test, şirketinizin belirli yerel ve küresel güvenlik uyumluluklarını sağlamak amacıyla çeşitli endüstrilerde zorunlu kılınmıştır. PCI, SOC 2, HIPAA, GDPR vb. penetrasyon testi gerektiren birçok endüstri standardı vardır.

- Sağlık kuruluşları için HIPAA
- Ödeme işleyen şirketler için PCI-DSS, TSE
- Bankalar ve bankacılık dışı finans kuruluşları için RBI-ISMS, BDDK, SPK, TSE
- Sivil Havacılık şirketleri için SGT, TSE
- Hizmet kuruluşları için SOC 2
- Bilgi güvenliği etrafında iş yapmaya istekli herhangi bir kuruluş için ISO 27001

Düzenleyici gereksinimlere uyum sağlamak için sızma testinin sonuçları denetçiler tarafından kullanılabilir. Bu tür bir test, işletmenizin güvenlik önlemlerinin etkinliğini göstermek ve potansiyel riskleri yönetmek için önemli bir kanıt sağlar.

## 15. Sızma testi sonuçları ne kadar süreyle saklanır?

Doğrulama testi tamamlandıktan sonra müşteriye sunulan rapor güvenli veri silme yöntemleri ile sistemimizden kalıcı olarak imha edilir ve tutanak altına alınır.

**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