BİLİŞİM YAZILIM SİSTEMLERİ

Kavi International Software Distribution

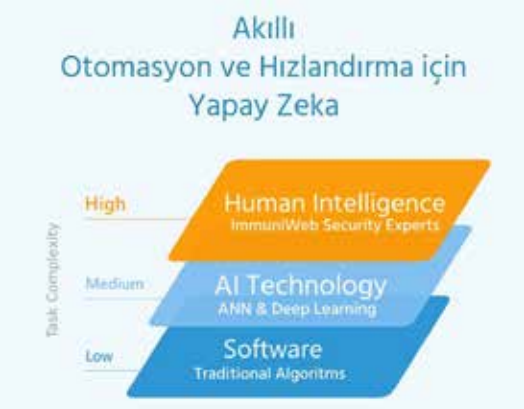
IMMUNIWEB

www.kavi.com.tr

ImmuniWeb® AI Platform Kullanım Örnekleri

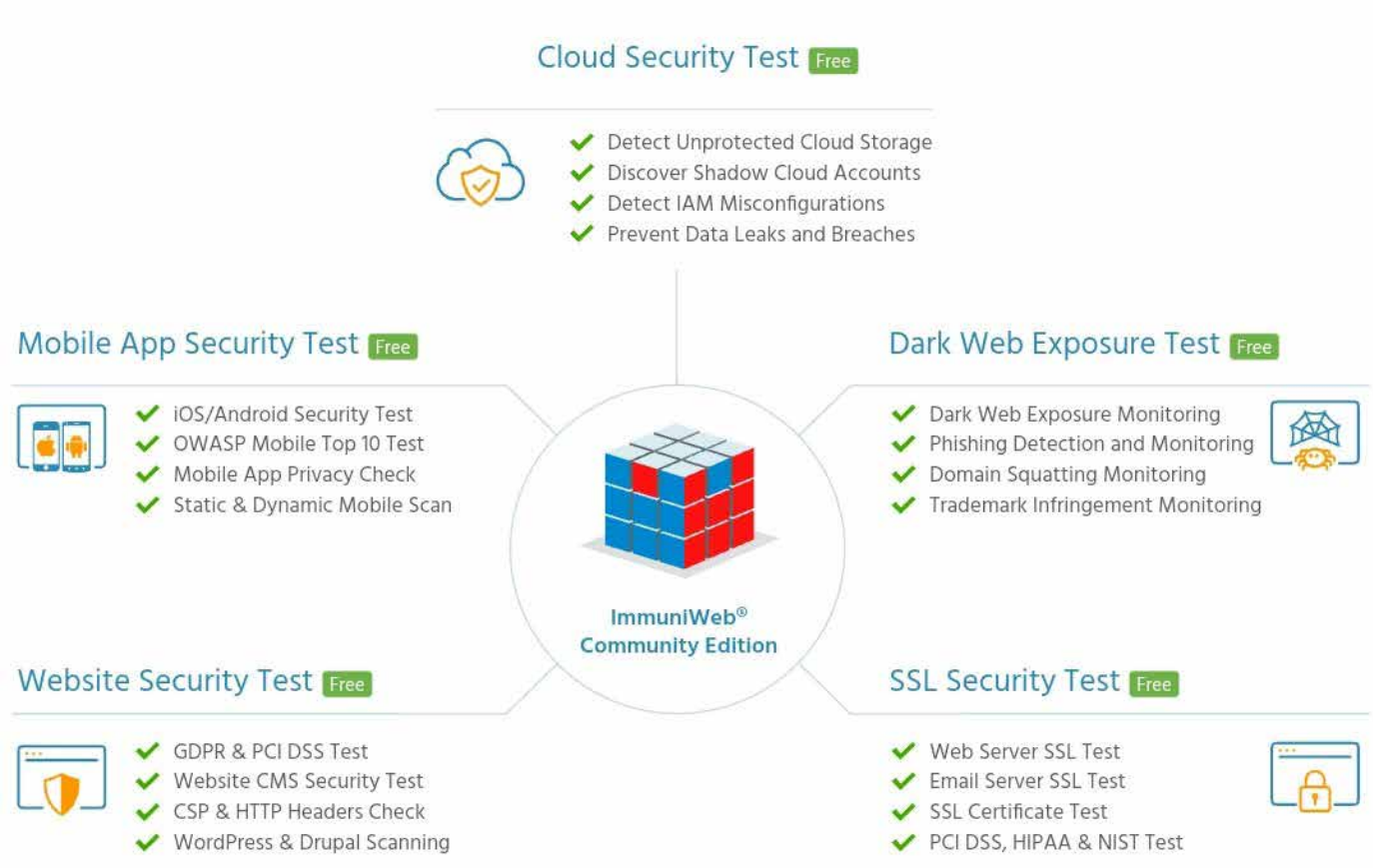
ImmuniWeb® AI Platformu, 50'den fazla ülkedeki kurumsal müşterilerin uygulamalarını, bulut altyapılarını test etmelerine, güvence altına almalarına ve korumalarına, tedarik zinciri saldırılarını azaltmalarına, veri ihlallerini önlemelerine ve uyumluluk gereksinimlerini sürdürmelerine yardımcı olur.

Akıllı Otomasyon ve Hızlandırma için Yapay Zeka



ImmuniWeb; akıllı otomasyon görev ve süreçlerin hızlandırılması için ödüllü AI (Yapay Zeka) teknolojimizden yararlanarak geleneksel hizmetlere kıyasla zamanınızdan %90'a kadar tasarruf sağlar.

Güvenlik uzmanlarımız, en karmaşık görevleri ve süreçleri ele alarak küresel pazarda en iyi kalite ve en iyi hizmet fiyatını sunar.



Bütün ihtiyaçlarınıza karşı tek platform

Web Security Scanning (Web Güvenliği Taraması)

ImmuniWeb® Discovery ile CMS, JavaScript kitaplıkları ve diğer bağımlılıklar dahil olmak üzere açık kaynaklı ve ticari web yazılımınızın kapsamlı bir envanterini alın . Saldırı yüzeyi yönetimiyle birlikte verilen web uygulaması taraması, OWASP top 10 listesinden bilinen veya kamuya açıklanmış güvenlik açıklarını belirlemek için yazılımınızın ve yüklü sürümlerin güvenilir bir şekilde parmak izini almak için gelişmiş yazılım bileşimi analizi (SCA) teknolojimizden yararlanır. Geleneksel güvenlik açığı tarayıcılarının aksine, tüm süreç üretim açısından güvenlidir ve web sitelerinizi yavaşlatmaz veya kesintiye uğratmaz.

PCI DSS, GDPR veya NIST gereksinimleri, TLS şifrelemesi, eksik WAF ve diğer yanlış yapılandırma ve zayıflıklar ile uyumluluk için sürekli testlerle geliştirilmiş, harici web uygulamalarınızın keşfini ve sürekli güvenlik izlemesini başlatmak için şirket adınızı girmeniz yeterlidir. Etkileşimli kontrol panelindeki grupları, etiketleri ve uyarıları kullanarak ekibinizdeki ilgili kişilere anında uyarılar gönderin. Bulguları PDF veya XLS'ye aktarın, verileri doğrudan SIEM, WAF veya hata izleme sistemlerinize göndermek için API'yi kullanın. Sahip olduğunuz web uygulamaları ve web sitelerinin sayısı ne olursa olsun, şirket başına sabit aylık fiyatın keyfini çıkarın.

Cloud Penetration Testing (Bulut Sızma Testi)

AWS, Azure, GCP veya diğer bulut hizmeti sağlayıcılarında barındırılan web uygulamalarınızı, bulutta yerel uygulamalarınızı, mikro hizmetlerinizi veya API'lerinizi *ImmuniWeb® On-Demand* penetrasyon testi ile test edin. OWASP top 10 ve SANS top 25 güvenlik açığının yanı sıra OWASP API top 10 zayıflığını ve buluta özgü yanlış yapılandırmaları tespit edin. Bulut ortamınızdaki aşırı erişim izinlerinden veya varsayılan Identity and Access Management (IAM) ilkelerinden yararlanarak bulut IMDS döndürme ve ayrıcalık yükseltme saldırılarıyla "privilege escalation" ataklarının neler yapılabileceğini ortaya çıkarın.

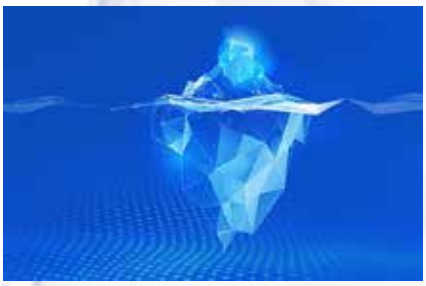
Her bulut sızma testi, sınırsız yama doğrulama değerlendirmeleriyle sağlanır, böylece bulut mühendisleriniz güvenlik kusurlarını düzeltebilir ve ardından hiçbir ek ücret ödemeden her şeyin düzgün bir şekilde düzeltildiğini doğrulayabilir. Bulut pentest raporunuzu etkileşimli kontrol panelinden PDF olarak indirin veya DevSecOps entegrasyonlarımız aracılığıyla verileri doğrudan SIEM veya WAF'nize aktarın. Rapor veya bulgular hakkında herhangi bir sorunuz olması durumunda güvenlik analistlerimize 7/24 erişimin keyfini çıkarın.

Attack Surface (Saldırı Yüzeyi Yönetimi)

Sadece şirket adınızı girerek *ImmuniWeb® Discovery* ile harici saldırı yüzeyinizi aydınlatın. Müdahalesiz keşif süreci; şirket içinde veya bir bulut ortamında bulunan BT varlıklarınızı hızla algılayacak, sınıflandıracak ve riskleri puanlayacaktır. Güvenlik açığı bulunan yazılımları, süresi dolan etki alanlarını ve SSL sertifikalarını, eski veya yanlış yapılandırılmış sistemleri ve aynalama BT altyapısını bulun. Üçüncü taraf havuzlarda bulunan korumasız kodu, kapsayıcı görüntülerini veya anlık sistem görüntülerini tespit edin. Uyumluluk amacıyla verilerinizin depolandığı coğrafi alanları ve ülkeleri görselleştirin.

Yeni keşfedilen varlıklar, yanlış yapılandırmalar, güvenlik açıkları ve güvenlik olayları için ekibinize ayrıntılı e-posta uyarıları ayarlayın. Ayrıntılı varlık izleme ve yönetimi için grupları ve etiketleri kullanın. Veri akışını doğrudan dahili güvenlik sistemlerinizle senkronize etmek veya seçilen bulguları PDF veya XLS'ye aktarmak için API'den yararlanın.

Dark Web Monitoring (Dark Web İzleme)



ImmuniWeb® Discovery ile Dark Web'deki veri sızıntılarını, çalınan kimlik bilgilerini ve gizli belgeleri keşfedin .Yeraltı pazar yerlerinin ve hack forumlarının izlenmesi, kopyalanmış web sitelerinin, sosyal ağların, IRC ve telgraf kanallarının 7/24 gözetimi ile tamamlanmaktadır. Diğer satıcıların hizmetlerinden farklı olarak, Dark Web izlememiz, herhangi bir sisteminizden, alan adlarınızdan, uygulamalarınızdan veya kullanıcılardan bahsedenleri, hepsini manuel olarak girmeye gerek kalmadan otomatik olarak algılamak için saldırı yüzeyi yönetimi ile birlikte gelir.

Devam eden kimlik avı ve alan adı hack, sahte sosyal ağ hesapları, markanızı gasp eden kötü amaçlı mobil uygulamalar ve uzlaşma göstergesini (IoC) veya bulut tabanlı BT varlıklarınızı da dikkatinize getirecek keşif ve sürekli izlemeyi başlatmak için şirket adınızı girmeniz yeterlidir. Etkileşimli kontrol panelinde sınıflandırılmış bulgulara göz atın, bulguları PDF veya XLS'ye aktarın veya verileri SIEM veya DFIR sistemlerinizle otomatik olarak senkronize etmek için API'yi kullanın.

Cloud Security Posture Management (Bulut Güvenliği Duruş Yönetimi)

ImmuniWeb® Discovery ile çoklu bulut saldırı yüzeyinizde bir kuş bakışı görünümü elde edin . Bulut güvenliği duruş yönetimi, bilgi işlem örnekleri, veri depolama, ağ geçitleri, yük dengeleyiciler, veritabanları ve AWS, Azure, GCP ve 50'den fazla diğer genel bulut hizmeti sağlayıcısındaki diğer yönetilen hizmetler dahil olmak üzere dışarıdan görülebilen bulut varlıklarınızı hızla algılar. Bulut saldırı yüzeyinizi çeşitli yanlış yapılandırmalar, aşırı erişim izinleri veya varsayılan Identity and Access Management (IAM) politikaları açısından değerlendirmenin yanı sıra, uyumluluk ve düzenleme amaçları için coğrafi veri depolamanızı da haritalıyoruz.

Diğer satıcıların aksine, bize bir bulut IAM hesabı sağlamanız gerekmez, keşif sürecini ve sürekli güvenlik izlemeyi çalıştırmak için şirket adınızı girmeniz yeterlidir. Shadow (gölge) bulut depolamayı ve yersiz bulut kullanımını tespit edin. DevOps ekibinizdeki ilgili kişilere yönelik uyarıları özelleştirin. Veri akışını mevcut SIEM sistemlerinizle senkronize etmek veya bulguları PDF veya XLS olarak dışa aktarmak için API'mizden yararlanın.

Continuous Penetration Testing (Sürekli Penetrasyon Testi)

ImmuniWeb® Continuous tarafından sağlanan 7/24 sızma testi ile geleneksel sızma testlerinden daha iyi performans gösterin . Web uygulamalarınızdaki ve API'lerinizdeki yeni kodu veya özellikleri hızla tespit eder ve ardından güvenlik açıkları, uyumluluk veya gizlilik sorunları için değişiklikleri test ederiz. Bir sorun tespit edildiğinde, e-posta, SMS veya çağrı ile hemen uyarılırsınız. Tüm müşteriler için, sözleşmeye dayalı sıfır false pozitif SLA ve tek bir false pozitif için para iade garantisi sunuyoruz.

Keşfedilen güvenlik açıklarının anında sanal olarak yamalanması için önde gelen WAF sağlayıcılarıyla entegrasyonlarımızdan yararlanın. Tek bir tıklamayla herhangi bir bulgu için yeniden test isteyin. Güvenlik analistlerimize, bulguların kötüye kullanılması veya düzeltilmesiyle ilgili sorularınızı hiçbir ek ücret ödemeden sorabilirsiniz. Bulguları içeren canlı bir gösterge panosu yaratabilir veya güvenlik açıklarını PDF olarak indirebilirsiniz. Ayrıca verileri, hata izleyicilerinize veya SIEM sistemlerinize DevSecOps entegrasyonlarımızla aktarabilirsiniz.

Cyber Threat Intelligence (Siber Tehdit İstihbaratı)

ImmuniWeb® Discovery ile siber tehdit ortamını ve güvenlik olaylarını izleyin. Devam eden kimlik avı kampanyalarını, hacklenmiş alan adlarını, sosyal ağlardaki sahte hesapları veya kimliğinizi taklit eden kötü amaçlı mobil uygulamaları tespit etmek için şirket adınızı girmeniz yeterlidir. Dark Web'de bilgisayar korsanlığı forumlarında veya yeraltı pazar yerlerinde şirketinizden veya BT varlıklarından bahsedilmesiyle ilgili anında uyarılar alın. Şirket içi veya bulut sistemlerinizde Uzlaşma Göstergesini (IoC) tespit edin. Şüpheli veya bilgisayar korsanlığı etkinlikleri için çeşitli kara listelere eklenen sistemlerinizi tespit edin ve araştırın.

Saldırı yüzeyi yönetimi ile birlikte verilen siber tehdit istihbaratı, sistemlerinizden, alan adlarınızdan, uygulamalarınızdan ve kullanıcılarınızdan herhangi birini içeren herhangi bir olayı otomatik olarak arayacaktır. Etkileşimli kontrol panelindeki grupları ve etiketleri kullanarak ekibinizdeki ilgili kişilere yeni bulgular hakkında anında uyarılar gönderin. Bulguları PDF veya XLS'ye aktarın veya API'yi kullanarak doğrudan SIEM'inize gönderin.

Mobile Penetration Testing (Mobil Sızma Testi)

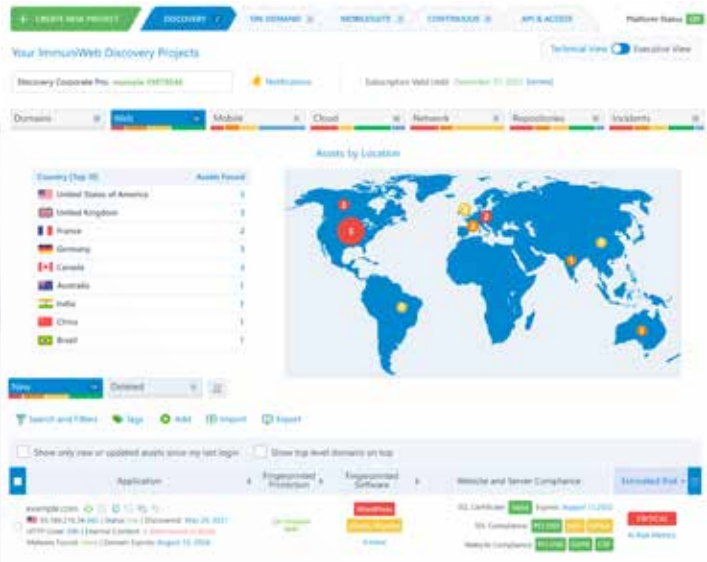
ImmuniWeb® MobileSuite ile iOS veya Android mobil uygulamanızdaki OWASP Mobile Top 10 zayıflığı tespit edin ve mobil uygulamanın uç noktalarındaki SANS top 25 güvenlik açığını keşfedin . Mobil uygulamanızın gizliliği, uyumluluğu ve şifreleme mekanizmalarının sektördeki en iyi uygulamalara uygun olup olmadığını inceleyin. Her mobil penetrasyon testi, sözleşmeye dayalı sıfır false pozitif SLA ve raporunuzda tek bir false pozitif olması durumunda para iade garantisi sağlar.

SSO, MFA veya OTP kullanarak bir Kara Kutu (black box) veya kimliği doğrulanmış test çalıştırın. İş mantığını ve kimlik doğrulamasını atlama güvenlik açıklarını tespit edin. Sızma testinden sonra sınırsız yama doğrulama değerlendirmesinden yararlanın, böylece yazılım geliştiricileriniz tüm bulguların düzgün bir şekilde yamalanıp yamalanmadığını kolayca fark edebilirsiniz. Daha hızlı düzeltme için güvenlik açığı verilerini etkileşimli panonuzdan PDF'e ve doğrudan SIEM'inize veya hata izleme sisteminize aktarın.

Digital Brand Protection (Dijital Marka Koruması)

ImmuniWeb® Discovery ile internette ticari marka ihlallerini ve kötüye kullanım durumlarını tespit edin. Saldırı yüzeyi yönetimi ile birlikte marka koruması, tüm ulusal veya küresel alan adlarının siber ve yazım hatası hacklerini (typo squating), kimlik avı kampanyalarını, sosyal ağlardaki sahte hesapları ve markanızı veya şirketinizi taklit eden kötü amaçlı mobil uygulamaları hızla dikkatinize sunar. Tasarımınızı yasa dışı amaçlarla taklit eden sahte web sitelerini tespit edin.

Sürekli izlemeyi başlatmak için şirket adınızı girin. Ekibinizdeki ilgili kişilere yönelik uyarıları özelleştirin veya doğrudan ilgili kişilere bildirim gönderin. Veri akışını dahili sistemlerinizle senkronize etmek veya bulguları PDF veya XLS olarak dışa aktarmak için API mizden yararlanın.



GDPR Penetration Testing (GDPR Sızma Testi)

GDPR ve EDBP yönergelerinin gerektirdiği şekilde kişisel verileri depolayan veya işleyen sistemlerinizin düzenli sızma testi için ImmuniWeb® On-Demand'ı kullanın . Her sızma testi, sözleşmeye dayalı false pozitif SLA ve raporunuzda tek bir false pozitif olması durumunda para iade garantisi sağlar. Web uygulamalarınızdaki ve API'lerinizdeki OWASP top 10 ve SANS top 25 güvenlik açıklarını ve yanlış yapılandırmaları tespit edin. Uyumluluk veya düzenleyici gereksinimleri ihlal edebilecek uyumluluğu ihlal edilmiş yapılandırmalar hakkında ipuçları alın.

API Penetration Testing (API Sızma Testi)

SANS Top 25 ve OWASP API Security Top 10 güvenlik açığı için mikro hizmetlerinizi ve API'lerinizi ImmuniWeb® On-Demand sızma testiyle test edin. API şemanızı Postman, Swagger, GraphQL veya başka bir biçimde yüklemeniz yeterlidir. Her sızma testi, sözleşmeye dayalı false Pozitif SLA ve raporunuzda tek bir false pozitif olması durumunda para iade garantisi ile sağlanır. Ayrıcalık yükseltme saldırılarıyla "privilege escalation" kimlik doğrulama atlama ve API iş mantığı güvenlik açıklarını tespit edin.

Her sızma testi, sınırsız yama doğrulama değerlendirmesiyle sağlanır, böylece geliştiricileriniz sorunları çözebilir ve testi hiçbir ek ücret ödemeden yeniden çalıştırabilir. Raporunuzu PDF formatında indirin veya güvenlik açığı verilerini DevSecOps entegrasyonlarımız aracılığıyla SIEM veya WAF ortamınıza aktarın. Raporla ilgili herhangi bir sorunuz olması durumunda, güvenlik analistlerimize 7/24 erişimin keyfini çıkarın.

Third-Party Risk Management (Üçüncü Taraf Risk Yönetimi)

ImmuniWeb® Discovery ile iş açısından kritik satıcı ve tedarikçilerinizin BT hijyenini, siber güvenliğini ve olay müdahalesini değerlendirin . Harici saldırı yüzeyinin, yanlış yapılandırılmış veya savunmasız sistem ve uygulamalarının, korumasız bulut depolamasının, dark web'den bahsetmenin ve veri sızıntılarının, sizi veya satıcınızı hedef alan kimlik avı veya alan işgali kampanyalarının kapsamlı bir görüntüsünü almak için bir şirket adı girin. Tüm süreç müdahaleci değildir ve üretim açısından güvenlidir, bu da onu üçüncü taraf risk yönetimi programı (TPRM) için mükemmel bir uyum haline getirir.

Satıcılarınızın ayrıntıları görmek ve sorunları hızla çözmek için bağlanabileceği etkileşimli gösterge tablosunda sınıflandırılmış risk puanlı bulguları alın. Satıcı risk yönetimi programınızı bir sonraki seviyeye taşıyarak, artan tedarik zinciri saldırılarını önleyin. Kişisel, finansal veya sağlık verilerini işleyen üçüncü taraf sistemlerini denetlemek için yasal gereklilikleri yerine getirin. BT varlıklarının sayısı, dark web'de bahsedilenler veya güvenlik olaylarının sayısı ne olursa olsun, şirket başına sabit bir fiyatın keyfini çıkarın.

Network Security Assessment (Ağ Güvenliği Değerlendirmesi)

Saldırı yüzeyi yönetimini ağ güvenliği değerlendirmesiyle bir araya getiren *ImmuniWeb® Discovery* ile dışarıdan erişilebilen ağ hizmetlerinizi keşfedin. Şirket içinde veya bulutta barındırılan sunucularınızın, ağ cihazlarınızın ve diğer BT varlıklarınızın kapsamlı bir görüntüsünü almak için şirket adınızı girmeniz yeterlidir. Her açık bağlantı noktası, size risk tabanlı bir puanlama sağlamak için çalışan hizmetin ve sürümünün parmak izini almak için dikkatlice analiz edilir. Geleneksel güvenlik açığı tarama çözümlerinin aksine, üretim için güvenli tarama teknolojimiz ağ hizmetlerinizi kesintiye uğratmaz veya yavaşlatmaz.

Kritik güvenlik açıklarına sahip gölgelenmiş, aynalanmış, terk edilmiş veya unutulmuş sunucuları ve ağ ekipmanını tespit edin. Ağ sızma testi maliyetlerini hızlandırmak ve azaltmak için ağ saldırı yüzeyinizi azaltın. Etkileşimli kontrol panelindeki grupları, etiketleri ve uyarıları kullanarak ekibinizdeki ilgili kişilere anında uyarılar gönderin. API aracılığıyla güvenlik açığı verilerini dışa aktarın veya seçilen bulguları PDF veya XLS olarak alın. Ağ varlıklarının ve hizmetlerinin sayısından bağımsız olarak şirket başına sabit aylık fiyatın keyfini çıkarın.

PCI DSS Penetration Testing (PCI DSS Sızma Testi)

PCI DSS tarafından zorunlu kılındığı şekilde ödeme kartı verilerini depolayan veya işleyen sistemlerinizin düzenli sızma testi için *ImmuniWeb® On-Demand* kullanın . Web uygulamalarınızda, mikro hizmetinizde ve API'lerinizde OWASP top 10, PCI DSS 6.5 listesi ve SANS top 25 güvenlik açıklarını ve yanlış yapılandırmaları tespit edin. Her sızma testi, sözleşmeye dayalı sıfır false pozitif SLA ve raporda tek bir false pozitif olması durumunda para iade garantisi ile sağlanır.

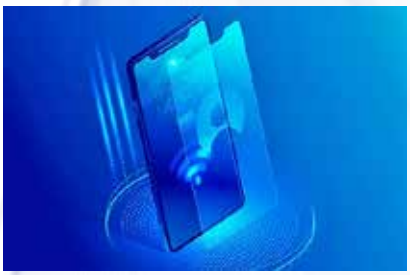
Pentestten sonra, ücretsiz olarak sınırsız güvenlik açığı doğrulama değerlendirmesi yapın, böylece yazılım mühendisleriniz, PCI DSS'nin gerektirdiği şekilde, pentest bulgularının derhal düzeltilip düzeltilmediğini kolayca kontrol edebilir. Bulguları içeren çok amaçlı bir gösterge panosu edinin, güvenlik açıklarını PDF olarak indirin, verileri doğrudan hata izleme veya SIEM sistemlerinize aktarmak için DevSecOps entegrasyonlarımızdan yararlanın. Tespit edilen güvenlik açıklarının tek tıklamayla sanal olarak yamalanması için önde gelen WAF sağlayıcılarıyla olan ortaklıklarımızdan yararlanın.

Red Teaming Exercise (Kırmızı Takım Çalışması)

Siber güvenlik stratejinize ve işletmeye özel siber tehdit ortamınıza göre uyarlanmış *ImmuniWeb® On-Demand* for Red Teaming alıştırmalarından yararlanın . Projenizi oluştururken, simüle etmek istediğiniz saldırı senaryolarını, siber tehditleri veya kötü niyetli aktörleri belirtmeniz yeterlidir. Ayrıntılı bir senaryo ekleyebilir veya web sistemlerinize karşı denememizi istediğiniz temel saldırı vektörlerini ve yöntemlerini kısaca belirtebilirsiniz. Güvenlik analistlerimiz ve sızma test uzmanlarımız, saldırı planını dikkatli bir şekilde gözden geçirecek ve nasıl genişletileceğine ilişkin soru veya önerileriniz olması durumunda size geri dönecektir.

Kırmızı Takım raporu, sızma taktiklerini, tekniklerini, prosedürlerini (TTP) ve elde edilen sonuçları tehdide duyarlı bir risk puanlamasıyla donatacaktır. Güvenlik analistlerimiz ve sızma test uzmanlarımız, Red Teaming alıştırması öncesinde, sırasında ve sonrasında hiçbir ek ücret ödemeden 7/24 hizmetinizdedir. Hizmet, sözleşmeye dayalı sıfır false pozitif SLA ve sınırsız yama doğrulama değerlendirmeleri ile sağlanır, böylece geliştiricileriniz tüm kusurların düzgün bir şekilde düzeltildiğini kontrol edebilir.

Mobile Security Scanning (Mobil Güvenlik Taraması)



ImmuniWeb® Discovery ile OWASP Mobile'ın top 10 zayıf noktasını tespit edin. Müdahalesiz, bir keşif süreci başlatmak ve Google Play veya Apple Store gibi 30'dan fazla halka açık mağazada bulunan iOS ve Android mobil uygulamalarınızın kapsamlı bir listesini almak için şirketinizin adını girmeniz yeterlidir. Otomatik SAST, DAST ve SCA testleri, OWASP Mobile top 10 güvenlik açıklarını ve zayıf noktalarını tespit etmek için keşfedilen mobil uygulamalarda otomatik olarak başlatılacaktır.

Şirketinize ait tüm mobil uygulamaları, otomatik olarak keşfedilmemesi veya genel uygulama mağazalarında bulunmaması durumunda ek ücret ödemeden yükleyebilirsiniz. Mobil güvenlik açığı taramasının yanı sıra, tehlikeli mobil uygulama izinleri, eksik veya zayıf şifreleme ve mobil uygulama harici iletişimleri gibi çeşitli gizlilik sorunlarını da göreceksiniz. Güvenlik analistlerimiz, bulgularla ilgili sorularınızı yanıtlamak için 7/24 hizmetinizdedir. Sınırsız güvenlik taraması da dahil olmak üzere tüm özellikler, sabit aylık fiyata sunulmaktadır.

WAF Security Testing (WAF Güvenlik Testi)

ImmuniWeb® On-Demand sızma testi ile WAF veya diğer güvenlik kontrollerinizin verimliliğini ve esnekliğini doğrulayın . Web uygulamalarınız, mikro hizmetleriniz ve API'lerinizdeki OWASP top 10 ve SANS top 25 güvenlik açığını keşfedin ve ardından bunların kötüye kullanılabilir olup olmadığını ve mevcut WAF yapılandırmanızın nasıl atlanabileceğini kontrol edin. WAF'nizin iş mantığı güvenlik açıklarından yararlanılmasını uygun şekilde azaltıp azaltmadığını test edin. Raporunuzda tek bir false pozitif bile olsa, sözleşmeye dayalı sıfır false pozitif SLA'mızın ve para iade garantimizin tüm avantajlarından yararlanın.

Bulguların yazılım geliştiricileriniz tarafından düzgün bir şekilde düzeltilip düzeltilmediğini defalarca kontrol etmek için pentestten sonra sınırsız yama doğrulama değerlendirmesi yapın. Etkileşimli panodaki bulguları alın, güvenlik açığı verilerini PDF veya XLS formatlarında dışa aktarın veya bulguları doğrudan hata izleme veya SIEM sistemlerinize alın. Keşfedilen tüm güvenlik açıkları için kullanıma hazır WAF kural kümeleri elde etmek için önde gelen WAF sağlayıcılarıyla teknoloji ortaklılarımızdan yararlanın.

Web Penetration Testing (Web Sızma Testi)

ImmuniWeb® On-Demand ile web uygulamalarınızdaki, RESTful API'lerinizdeki ve mikro hizmetlerinizdeki OWASP Top 25, PCI DSS 6.5 List ve SANS Top 25 güvenlik açıklarını tespit edin . Gelişmiş ayrıcalık yükseltme saldırıları "privilege escalation", kimlik doğrulama atlama ve iş mantığı güvenlik açıklarını keşfedin. Hizmet, sözleşmeye dayalı sıfır false pozitif SLA ve raporunuzda tek bir false pozitif olması durumunda para iade garantisi ile sağlanır. MFA, OTP veya SSO kullanarak kara kutuda (black box) veya kimliği doğrulanmış, çok kullanıcılı modda testi özelleştirin.

Pentestten sonra ücretsiz olarak sınırsız güvenlik açığı doğrulama değerlendirmesi yapın, böylece yazılım geliştiricileriniz pentest bulgularının düzgün bir şekilde düzeltilip düzeltilmediğini kolayca doğrulayabilir. Yapılandırılmış bulgularla çok amaçlı bir gösterge panosu edinin, güvenlik açıklarını PDF olarak indirin veya verileri doğrudan hata izleme veya SIEM sistemlerinize aktarmak için DevSecOps entegrasyonlarımızdan yararlanın. Tespit edilen güvenlik açıklarının tek tıklamayla sanal yamalanması için önde gelen WAF sağlayıcılarıyla olan bağlantılarımızdan yararlanın.

ImmuniWeb®
AI for Application Security

BİLİŞİM YAZILIM SİSTEMLERİ

1) Şirket Adını Girin

Tüm saldırı yüzeyinin açık kaynaklı istihbarat taramasını çalıştırmak için bir şirket adı girin.

2) Hackerların Gördüklerini Görün

Verilerin depolandığı veya işlendiği şirket içi sistemleri ve bulut kaynaklarını keşfedin.

3) Hackerların Ne Yaptığını Görün

Veri ihlallerini, güvenliği ihlal edilmiş hesapları veya sistemleri, çalınan verileri,kimlik avını ve markanın kötüye kullanımını tespit edin.

ImmuniWeb® Discovery

	Genişletilmiş Kurumsal	Kurumsal Profesyonel	Kurumsal	Ekspres Profesyonel
Güvenlik Analistlerine Erişim; Yapılandırma ve sorularınız için güvenlik analistlerimize 7/24 erişim.	✓	✓	✓	✓
Domain & Subdomain Keşfi Şirkete ait veya şirket tarafından işletilen alan adlarının ve alt alan adlarının kapsamlı keşfi.	✓	✓	✓	✓
Web Uygulamaları ve API Keşfi; Şirkete ait veya şirket tarafından işletilen, lokal ve bulutta barındırılan, web sitelerinin, web uygulamalarının, API'lerinin kapsamlı keşfi.	✓	✓	✓	✓
Mobil Uygulamalar ve API Keşfi; Şirketin, mobil uygulamalarının tam listesiyle (örn. API'ler ve web hizmetleri) genel olarak erişilebilir (örn. web sitesi veya genel uygulama mağazaları aracılığıyla) mobil uygulamalarının kapsamlı keşfi.	✓	✓	✓	✓
Güvenlik ve Uyumluluk İzleme; Şirkete ait veya şirket tarafından işletilen tüm harici BT varlıklarının savunmasız veya güncel olmayan web ve ağ yazılımları, güvenli olmayan yönetici arayüzleri veya konsolları, güvenli olmayan sunucu yapılandırmaları, zayıf şifreleme ve PCI,DSS,NIST ve KVKK uyumluluk arızalarının kapsamlı tespiti.	✓	✓	✓	✓
Çoklu Bulut Kaynakları Keşfi; AWS, Azure ve GCP dahil olmak üzere şirkete ait veya şirket tarafından işletilen 50'den fazla genel bulut hizmeti sağlayıcısında bulunan açık veya korumasız bulut depolama, hizmetler, API'ler ve örneklerin kapsamlı keşfi.	✓	✓	✓	
Ağ Hizmetleri Keşfi; Şirkete ait veya şirket tarafından işletilen internetten erişilebilen tüm ağ hizmetlerinin, cihazlarının ve IoT cihazlarının kapsamlı keşfi.	✓	✓	✓	
Siber Tehdit İstihbaratı; Uzlaşma Göstergeleri (IoC), tehdit istihbaratı beslemeleri, bilgisayar korsanlığı forumları, yeraltı pazarları, şirketten, yöneticilerinden veya çalışanlarından, verilerden veya BT uygulamalarından bahseden Telegram ve IRC kanallarına ilişkin tartışmalar kapsamlı olarak izlenir.	✓	✓		
Depo İzleme; Şirkete ait sızdırılmış veya açığa çıkmış kaynak kodu, sistem görüntülerini ve sabit kodlanmış sırları (örn. API anahtarları) tespit etmek için kod, sistem ve Repositories Monitoring izlenme.	✓	✓		
Dark Web İzleme; Şirketin çalınan kimlik bilgileri, belgeleri, güvenliği ihlal edilmiş sistemler, veritabanları, şirkete ait ya da şirket tarafından işletilen backdoor cihazlar ve sunucu bilgilerinin satışı için Dark Web kaynaklarının kapsamlı izlenmesi.	✓	✓		
Kimlik Avı İzleme; Şirketin yöneticilerini, çalışanlarını veya müşterilerini hedef alan kimlik avı ve çevrimiçi dolandırıcılık kampanyalarının kapsamlı izlenmesi.	✓	✓		
Marka İzleme; Şirketin markasını veya kimliğini hedef alan sosyal ağlardaki sahte hesapların kapsamlı izlenmesi, alan adının siber saldırısı ve yazım denetimi.	✓	✓		
Dark Web Analistlerine Erişim; Yeni keşfedilen izinsiz girişleri, veri ihlallerini ve diğer güvenlik olaylarını incelemek ve tartışmak için tehdit analistlerimize 7/24 erişim.	✓			
Güncellemeler; Yeni olayların, öğelerin ve varlık keşfinin sıklığı.	7/24	Her gün	Her hafta	2 Haftada Bir
Yıllık Abonelik	*$3995* Her Ay	*$1995* Her Ay	*$995* Her Ay	*$499* Her Ay

ImmuniWeb®
AI for Application Security

BİLİŞİM YAZILIM SİSTEMLERİ

1) Testinizi Yapılandırın

Web uygulamanızın URL'lerini girin, herhangi bir özel test, kapsam veya raporlama gereksinimlerini belirtin.

2) Testinizi Planlayın

Paketinizi seçin, sızma testi tarihlerini planlayın ve teslimat tarihini bildirin.

3) Raporunuzu Alın

Etkileşimli panoya göz atın, verileri PDF olarak dışa aktarın ve yama doğrulama taramasını planlayın.

ImmuniWeb® On-Demand

	Kurumsal Profesyonel	Kurumsal	Ekspres Profesyonel	Ekspres
AI-Otomatik Penetrasyon Testi Ödüllü Deep Learning AI yapay zeka destekli teknolojimiz, web uygulama güvenliğinizin genellikle insan emeği gerektiren ve karışık yapısı nedeniyle geleneksel güvenlik açığı tarayıcılar tarafından gerçekleştirilemeyen 10.000'den fazla kontrolünü hızlandırır ve otomatikleştirir.	*120 saat **	*72 saat **	*24 saat **	*12 saat**
İş Mantığının Manuel Testi CREST onaylı güvenlik uzmanlarımız, web uygulamanızın iş mantığının gelişmiş güvenlik testlerini gerçekleştirir, karışık güvenlik açıklarından yararlanır ve karmaşık yapısı nedeniyle insan zekası gerektiren diğer güvenlik ve gizlilik kontrollerini yürütür.	*3+ uzman*	*2+ uzman*	*1+ uzman*	*1 uzman*
Sıfır Yanlış Pozitif SLA Hizmet Şartlarımız, penetrasyon testi raporunuzdaki tek bir yanlış pozitif için sözleşmeye dayalı para iade garantisi sağlar.	✓	✓	✓	✓
Hızlı Teslimat SLA'sı Hizmet Şartlarımız, penetrasyon testi raporunuzun gecikmeli teslimi için sözleşmeye dayalı para iade garantisi sağlar.	✓	✓	✓	✓
WAF Sanal Yama Önde gelen WAF üreticileri ile var olan teknoloji ittifaklarımız, güvenlik açıklarını otomatik olarak azaltmak için testraporunuzla birlikte kullanıma hazır WAF kuralları üretir.	✓	✓	✓	✓
DevSecOps ve CI/CD Entegrasyonları Önde gelen SIEM ve DevOps satıcılarıyla olan teknoloji ittifaklarımız, güvenlik açığı yönetim sistemlerinize, hata izleyicilerinize tek tıklamayla güvenlik açığı verilerinin dışa aktarılmasını ve ayrıca penetrasyon testinin CI/CD pipeline entegrasyonunu sağlar.	✓	✓	✓	✓
Güvenlik Analistlerimize 7/24 Erişim Güvenlik analistlerimiz, sızma testi esnasında ve sonrasında, iyileştirme veya uygulanması hakkında herhangi bir tavsiyeye ya da ek bilgiye ihtiyacınız olduğu an hizmetinizdedir.	✓	✓	✓	✓
Sınırsız Yama Doğrulama Taraması Sızma testi raporunuzun teslim edilmesinden sonraki 100 gün boyunca, tespit edilen tüm güvenlik açıklarının yazılım geliştiricileriniz tarafından düzgün bir şekilde düzeltildiğini doğrulamak için sinirsiz yama doğrulama taraması yapılabilir.	✓	✓	✓	✓
Gizlilik Değerlendirmesi Güvenlik uzmanlarımız, web uygulamanızdaki yaygın gizlilik sorunlarını ve uyumluluk hatalarını inceler.	✓	✓	✓	
Dark Web Keşfi Güvenlik uzmanlarımız, calinti kimlik bilgileri gibi kuruluşunuzun dark Web'e maruz kalmasını araştırır ve sızma testi sırasında bu verilerden yararlanır.	✓	✓		
Kırmızı Takım Çalışması Güvenlik uzmanlarımız, talep üzerine, belirli bir siber tehdit aktörünün taktiklerini, tekniklerini ve prosedürlerini (TTP) taklit ederek tehdit ortamınıza göre uyarlanmış Kırmızı Ekip Oluşturma egzersizi gerçekleştirebilir.	✓			
Paket fiyatı (* Saat sınırlamaları yukarıda belirtilmiştir)	*$4995*	*$2995*	*$995*	*$499*

ImmuniWeb®
AI for Application Security

BİLİŞİM YAZILIM SİSTEMLERİ

1) Testinizi Yapılandırın

Mobil uygulamanızı yükleyin, herhangi bir özel test veya raporlama gereksinimini belirtin.

2) Testinizi Planlayın

Paketinizi seçin, sızma testi tarihlerini planlayın ve teslimat tarihini bildirin.

3) Raporunuzu Alın

Etkileşimli panoya göz atın, verileri PDF olarak dışa aktarın ve yama doğrulama taramasını planlayın.

ImmuniWeb® MobileSuite

	Kurumsal Profesyonel	Kurumsal	Ekspres Profesyonel	Ekspres
AI-Otomatik Penetrasyon Testi Ödüllü AI (teknolojimiz; genellikle insan emeği gerektiren ve karışık yapısı nedeniyle geleneksel güvenlik açığı tarayıcıları tarafından gerçekleştirilemeyen mobil uygulamanızın kontrolünü hızlandırır ve otomatikleştirir.	*120 saat*	*120 saat*	*72 saat*	*24 saat*
İş Mantığının Manuel Testi CREST onaylı güvenlik uzmanlarımız, mobil uygulamanızın iş mantığının gelişmiş güvenlik testlerini gerçekleştirir.	*4+ uzman*	*3+ uzman*	*2+ uzman*	*1 uzman*
Sıfır Yanlış Pozitif SLA Hizmet Şartlarımız, penetrasyon testi raporunuzdaki tek bir yanlış pozitif için sözleşmeye dayalı para iade garantisi sağlar.	✓	✓	✓	✓
Hızlı Teslimat SLA'sı Hizmet Şartlarımız, penetrasyon testi raporunuzun gecikmeli teslimi için sözleşmeye dayalı para iade garantisi sağlar.	✓	✓	✓	✓
WAF Sanal Yama Önde gelen WAF satıcılarıyla olan teknoloji ittifaklarımız, mobil uygulamanızın backend tarafında (örn. API'ler veya web hizmetleri) bulunan güvenlik açıklarını otomatik olarak azaltmak için penetrasyon testi raporunuzla birlikte kullanıma hazır WAF kural kümeleri sağlar.	✓	✓	✓	✓
DevSecOps ve CI/CD Entegrasyonları Önde gelen SIEM ve DevOps satıcılarıyla olan teknoloji ittifaklarımız, güvenlik açığı yönetim sistemlerinize, hata izleyicilerinize tek tıklamayla güvenlik açığı verilerinin dışa aktarılmasını ve ayrıca penetrasyon testinin CI/CD pipeline entegrasyonunu sağlar.	✓	✓	✓	✓
Güvenlik Analistlerimize 7/24 Erişim Güvenlik analistlerimiz, sızma testi esnasında ve sonrasında, iyileştirme veya uygulanması hakkında herhangi bir tavsiyeye ya da ek bilgiye ihtiyacınız olduğu an hizmetinizdedir.	✓	✓	✓	✓
Sınırsız Yama Doğrulama Taraması Sızma testi raporunuzun teslim edilmesinden sonraki 100 gün boyunca, tespit edilen tüm güvenlik açıklarının yazılımcılarınız tarafından düzgün ve tam düzeltildiğini doğrulamak için sınırsız yama doğrulama taraması yapılabilir.	✓	✓	✓	✓
Gizlilik Değerlendirmesi Güvenlik uzmanlarımız, mobil uygulamanızdaki yaygın gizlilik sorunlarını ve uyumluluk hatalarını inceler.	✓	✓	✓	
Platformlar Arası Uygulama Testi Kapsamlı testler için genellikle önemli ölçüde daha fazla kaynak ve zaman gerektirdiğinden, karmaşık platformlar arası uygulamalar (örn. Xamarin Çerçevesi) için kurumsal paket gereklidir.	✓	✓		
Root veya Jailbreak Algılama Bypass Mobil uygulamanızın root'lu veya jailbreak'li cihazlarda çalışmaya karşı ,koruması varsa Corporate Pro paketi gereklidir.	✓			
Emülatör Algılama Baypas Mobil uygulamanız bir emülatör üzerinde çalışmayı engelliyorsa veya gerçek bir cihazda test edilmesini gerektiriyorsa Corporate Pro paketi gereklidir.	✓			
Sertifika Sabitleme Atlaması Mobil uygulamanız SSL sertifikası sabitleme teknolojisini kullanıyorsa Corporate Pro paketi gereklidir.	✓			
Kod Gizleme Baypas Tersine mühendisliği önlemek için mobil uygulamanızın kodunun karıştırılması durumunda Corporate Pro paketi gereklidir.	✓			
Kırmızı Takım Çalışması Güvenlik uzmanlarımız, talep üzerine, belirli bir siber tehdit aktörünün taktiklerini, tekniklerini ve prosedürlerini (TTP) taklit ederek tehdit ortamınıza göre uyarlanmış Kırmızı Ekip Oluşturma egzersizi gerçekleştirebilir.	✓			
Paket fiyatı	*$9495*	*$7495*	*$3495*	*$1495*

ImmuniWeb® AI for Application Security

BİLİŞİM YAZILIM SİSTEMLERİ

1) Testinizi Yapılandırın

Uygulamanızın URL'lerini girin, herhangi bir özel test, kapsam belirleme veya raporlama gereksinimlerini belirtin

2) Testinizi Planlayın

Bir paket alın veya güvenlik analistlerimizden birini seçmek için ücretsiz danışmanlık alın

3) Raporunuzu Alın

Abonelik başlangıç tarihini seçin, kullanıcı ekleyin, uyarıları özelleştirin ve işiniz bitti!

ImmuniWeb® Continuous

	Kurumsal Profesyonel	Kurumsal	Ekspres Profesyonel	Ekspres
AI-Otomatik Penetrasyon Testi Ödüllü Deep Learning AI teknolojimiz, web uygulama güvenliğinizin genellikle insan emeği gerektiren ve karışıklık nedeniyle geleneksel güvenlik açığı tarayıcıları tarafından gerçekleştirilemeyen 10.000'den fazla kontrolünü hızlandırır ve akıllı bir şekilde otomatikleştirir.	*7/24*	*7/24*	*7/24*	*7/24*
İş Mantığının Manuel Testi CREST onaylı güvenlik uzmanlarımız, web uygulamanızın iş mantığının gelişmiş güvenlik testlerini gerçekleştirir, karışık güvenlik açıklarından yararlanır ve karışık yapısı nedeniyle insan zekası gerektiren diğer güvenlik ve gizlilik kontrollerini yürütü	*3+ uzman*	*2+ uzman*	*1+ uzman*	*1 uzman*
Sıfır Yanlış Pozitif SLA Hizmet Şartlarımız, penetrasyon testi raporunuzdaki tek bir yanlış pozitif için sözleşmeye dayalı para iade garantisi sağlar.	✓	✓	✓	✓
Hızlı Teslimat SLA'sı Hizmet Şartlarımız, penetrasyon testi raporunuzun gecikmeli teslimi için sözleşmeye dayalı para iade garantisi sağlar.	✓	✓	✓	✓
WAF Sanal Yama Önde gelen WAF üreticileri ile var olan teknoloji ittifaklarımız, güvenlik açıklarını otomatik olarak azaltmak için test raporunuzla birlikte kullanıma hazır WAF kuralları üretir.	✓	✓	✓	✓
DevSecOps ve CI/CD Entegrasyonları Önde gelen SIEM ve DevOps satıcılarıyla olan teknoloji ittifaklarımız, güvenlik açığı yönetim sistemlerinize, hata izleyicilerinize tek tıklamayla güvenlik açığı verilerinin dışa aktarılmasını ve ayrıca penetrasyon testinin CI/CD pipeline entegrasyonunu sağlar.	✓	✓	✓	✓
Güvenlik Analistlerimize 7/24 Erişim Güvenlik analistlerimiz, sızma testi esnasında ve sonrasında, iyileştirme veya uygulanması hakkında herhangi bir tavsiyeye ya da ek bilgiye ihtiyacınız olduğu an hizmetinizdedir.	✓	✓	✓	✓
Sınırsız Yama Doğrulama Taraması Sızma testi raporunuzun teslim edilmesinden sonraki 100 gün boyunca tespit edilen tüm güvenlik açıklarının yazılım geliştiricileriniz tarafından düzgün bir şekilde düzeltildiğini doğrulamak için sınırsız yama doğrulama taraması yapılabilir.	✓	✓	✓	✓
Gizlilik Değerlendirmesi Güvenlik uzmanlarımız, web uygulamanızdaki yaygın gizlilik sorunlarını ve uyumluluk hatalarını inceler.	✓	✓	✓	
Dark Web Keşfi Güvenlik uzmanlarımız, çalıntı kimlik bilgileri gibi kuruluşunuzun dark web'e maruz kalmasını araştırır ve sızma testi sırasında bu verilerden yararlanır.	✓	✓		
Kırmızı Takım Çalışması Güvenlik uzmanlarımız, talep üzerine, belirli bir siber tehdit aktörünün taktiklerini, tekniklerini ve prosedürlerini (TTP) taklit ederek tehdit ortamınıza göre uyarlanmış Kırmızı Ekip Oluşturma egzersizi gerçekleştirebilir.	✓			
Yıllık Abonelik	*$5495* Her Ay	*$3495* Her Ay	*$1495* Her Ay	*$995* Her Ay
Aylık Abonelik	*$10995* Her Ay	*$6995* Her Ay		

BİLİŞİM YAZILIM SİSTEMLERİ

Kavi International Software Distribution

Kavi Bilgisayar Sistemleri San.Tic.Ltd.Sti

Trump Tower K: 4 Ofis No: 405 Mecidiyeköy Yolu Cad. No: 12 Şişli / İstanbul

satis@kavi.com.tr 0212 356 04 04

www.kavi.com.tr