



Modern uygulama geliştirme, inovasyon ve pazar hızı için bir yarış olsa da aynı zamanda gelir, itibar ve müşteri güvenini doğrudan tehdit eden yeni riskler de yaratmaktadır. Uygulamalar artık siber saldırıların yaklaşık %25'ini oluştururken; API'ler, açık kaynaklı bileşenler ve yapay zeka entegrasyonları, geleneksel güvenlik araçlarının nüfuz edemediği kör noktalar yaratarak saldırı yüzeyini tehlikeli bir şekilde genişletmektedir. Bu ortamda, güvenliği sonradan eklenen bir adım olarak görmek artık kabul edilemez. Güvenliği geliştirme yaşam döngüsünün her aşamasına entegre eden DevSecOps, iş sürekliliği için stratejik bir zorunluluk haline gelmiştir.

Mevcut tehdit ortamı, aşağıdaki verilerle daha net bir şekilde anlaşılabilir:

- **Büyüyen Pazar:** Küresel uygulama güvenliği pazarının büyüklüğü 2023 yılında 32,38 milyar ABD Doları olarak değerlendirilmiş olup, 2031 yılına kadar 73,59 milyar ABD Doları'na ulaşması beklenmektedir. Bu, siber güvenliğe yapılan yatırımın artan önemini göstermektedir.
- **Yazılım Tedarik Zinciri Riski:** Modern uygulamaların %97'si açık kaynaklı bileşenler içermektedir. Bu durum, tedarik zinciri saldırıları için verimli bir zemin oluşturmaktadır. Gartner, 2025 yılına kadar kuruluşların %45'inin bir yazılım tedarik zinciri saldırısı yaşayacağını öngörmektedir.
- **API Patlaması:** Şirketlerin %46'sında API güvenliği artık C-seviyesi bir öncelik haline gelmiştir. Ancak bu farkındalığa rağmen, kuruluşların sadece yaklaşık %7,5'i olgun ve kapsamlı API test programlarına sahiptir.
- **Yapay Zeka Etkisi:** Kuruluşların %61'i tehdit tespiti ve savunma için yapay zeka (AI) ve makine öğrenimi (ML) teknolojilerinden faydalanmaktadır. Diğer yandan, üretken yapay zekanın (GenAI) uygulamalara entegrasyonu, "prompt injection" gibi yeni ve karmaşık güvenlik açıkları yaratmaktadır.

Bu karmaşık tehdit ortamında kuruluşların, yenilikçilik ve pazara çıkış hızından ödün vermeden güvenlik duruşlarını güçlendirmek için proaktif, bütünleşmiş ve akıllı güvenlik çözümlerine ihtiyacı vardır.

HCL AppScan Avantajları: Neden Bizi Seçmelisiniz?

HCL AppScan'i farklı kılan, sadece teknolojik üstünlükleri değil, bu yeteneklerin günümüzün en kritik iş sorunlarını çözen stratejik farklılaştırıcılara dönüşmesidir. Platformumuz, araç karmaşasını ortadan kaldırmak, geliştirici verimliliğini artırmak, artan uyumluluk baskısını yönetmek ve nihayetinde güvenliği bir inovasyon engeli olmaktan çıkarıp bir hızlandırıcıya dönüştürmek için tasarlanmıştır.

- **Tüm Yaşam Döngüsü Koruması** AppScan, koddan buluta kadar tüm yazılım tedarik zincirini güvence altına alır. API'ler, konteynerler, açık kaynaklı bileşenler ve kod olarak altyapı (IaC) dahil olmak üzere modern uygulamaların tüm bileşenleri için ilke tabanlı ve otomatikleştirilmiş güvenlik çözümleri sunar.
- **Otomatik Mesele Korelasyonu** Platformumuz, DAST, SAST ve IAST'den gelen bulguları akıllıca birleştirerek sonuçları zenginleştirir. Bu sayede, aynı temel güvenlik açığına işaret eden farklı bulguları tek bir mesele altında gruplayarak düzeltme görevlerini azaltır ve geliştiricilerin zamanını verimli kullanmasını sağlar. Ayrıca, yapılan düzeltmelerin etkinliğini doğrular.
- **Esnek Dağıtım Modelleri** Her kuruluşun benzersiz ihtiyaçları olduğunu farkındayız. Bu nedenle AppScan, genel bulut, özel bulut, şirket içi (on-premises), dış ağ bağlantısı olmayan (air-gapped) ve hibrit ortamlar dahil olmak üzere çok çeşitli dağıtım seçenekleri sunar. Bu esneklik, veri egemenliği ve uyumluluk gereksinimlerinizi karşılamaya olanak tanır.
- **Sektör Lideri Tanınırlığı** HCL AppScan'in liderliği, sektörün en saygın analist firmaları tarafından da teyit edilmiştir. Platformumuz, Gartner Magic Quadrant'ta (2021, 2022) ve IDC MarketScape'te (2022) "Lider" olarak tanınmıştır. Ayrıca, kullanıcıların kendi deneyimlerine dayanan 2022 Gartner Peer Insights Müşterilerin Seçimi ödülünü almıştır.

Bu üstün yetenekler, HCL AppScan'in DevSecOps yaşam döngüsünün her aşamasına nasıl değer kattığını ve kuruluşunuzun güvenlik duruşunu nasıl dönüştürebileceğini göstermektedir.



DevSecOps Yaşam Döngüsünün Her Aşamasında Güvenlik

Modern yazılım geliştirmede güvenlik, geliştirme tamamlandıktan sonra uygulanan bir kontrol adımı değildir; aksine, yaşam döngüsünün her aşamasına entegre edilmesi gereken organik bir süreçtir. HCL AppScan, bu "shift-left" felsefesini temel alarak, DevSecOps döngüsünün en erken aşamalarından operasyon ve izleme süreçlerine kadar her adım için özel olarak tasarlanmış çözümler sunar. Bu sayede güvenlik, hız ve kalitenin ayrılmaz bir parçası haline gelir.

Aşağıda HCL AppScan'ın DevSecOps yaşam döngüsünün farklı aşamalarına nasıl entegre olduğu özetlemektedir:

» **Planla & Kodla:** Yazılımcıların kod yazarken güvenlik açıklarını taramasına ve düzeltmesine olanak tanır. Gerçek zamanlı geri bildirim ile güvenli kodlama alışkanlıkları oluşturur. **İlgili Ürünler:** HCL AppScan CodeSweep, HCL AppScan Source.

» **Derle & Test Et:** CI/CD süreçlerine entegre olarak statik (SAST), dinamik (DAST), interaktif (IAST) ve yazılım bileşen analizi (SCA) testlerini otomatikleştirir. Bu, güvenlik açıklarının üretime geçmeden önce yakalanmasını sağlar. **İlgili Ürünler:** HCL AppScan on Cloud, HCL AppScan 360°, HCL AppScan Enterprise.

» **Yayınla & Dağıt:** Çalışan uygulamaları ve API'leri sürekli izleyerek ve test ederek yeni veya mevcut güvenlik risklerini tespit eder. Güvenlik duruşunu sürekli olarak doğrular. **İlgili Ürünler:** HCL AppScan Standard, HCL AppScan Enterprise.

» **İşlet & İzle:** Canlı uygulamaları ve API'leri izler, otomatik mesele korelasyonu sağlar ve çalışma zamanı davranışlarına dayalı olarak bağlamsal bilgiler sunar. **İlgili Ürünler:** HCL AppScan IAST, HCL AppScan API Security.

Yaşam döngüsü boyunca bu sorunsuz entegrasyon, her biri belirli güvenlik açıklarını en uygun aşamada bulmak için özel olarak tasarlanmış, sınıfının en iyisi test teknolojilerinden oluşan temel bir paket tarafından desteklenmektedir.

Temel Güvenlik Testi Teknolojilerimiz

Kapsamlı bir uygulama güvenliği stratejisi, farklı türdeki zafiyetleri ortaya çıkarmak için birden fazla test metodolojisi gerektirir. HCL AppScan, sektörün en gelişmiş test teknolojilerini tek bir birleşik platformda bir araya getirerek, uygulamalarınızın her katmanında derinlemesine güvenlik analizi sağlar.

SAST (Statik Uygulama Güvenlik Testi)

Uygulamanın kaynak kodunu çalıştırmadan analiz eden "white-box" test yöntemidir. Geliştirme sürecinin erken aşamalarında hataları bulur.

Yetenekleri:

- Yapay zeka destekli doğruluk
- 30'dan fazla kod dili desteği
- Gizli anahtar (secrets) taraması
- Düzeltme önerileri

DAST (Dinamik Uygulama Güvenlik Testi)

Çalışan bir uygulamayı dışarıdan test eden "black-box" test yöntemidir. Bir bilgisayar korsanının yaklaşımını taklit eder.

Yetenekleri:

- Artımlı tarama ve test optimizasyonu
- Web API taraması
- OWASP Top 10 ve OWASP API Güvenliği Top 10 için %100 kapsama
- Gelişmiş XSS analizörü

IAST (İnteraktif Uygulama Güvenlik Testi)

Uygulamanın içinde çalışarak hem SAST hem de DAST'in güçlü yönlerini birleştiren hibrit bir yöntemdir. Çalışma zamanı davranışını izler.

Yetenekleri:

- Canlı uygulamaları ve API'leri izleme
- Otomatik mesele korelasyonu
- API keşfi
- Java ve .NET için patentli çözümler

SCA (Yazılım Bileşen Analizi)

Uygulamada kullanılan açık kaynaklı ve üçüncü taraf kütüphanelerdeki bilinen güvenlik açıklarını ve lisans uyumluluğu sorunlarını tespit eder.

Yetenekleri:

- Açık kaynak analizi
- Konteyner taraması
- Yazılım Malzeme Listesi (SBOM) oluşturma

İşte bu güçlü, bütünleşmiş teknoloji yığını, dünya çapında lider kuruluşların en kritik uygulamalarını güvence altına almalarını sağlar ve bu durum, kendi deneyimleriyle doğrulanmıştır.

Ertelemeyin, Harekete Geçin

Her geçen gün artan ve karmaşılaşan siber riskler karşısında beklemek, en maliyetli seçenektir. HCL AppScan'ın sunduğu yapay zeka destekli, kapsamlı ve geliştirici dostu koruma ile BBS'nin yerel uzmanlığını birleştirerek, uygulama güvenliği postürünüzü proaktif bir şekilde güçlendirebilir, risklerinizi minimize edebilirsiniz ve inovasyona güvenle odaklanabilirsiniz. Uzman ekibimizle tanışın ve işletmenize özel çözümleri birlikte tasarlayalım...