aa teknoloji

Black Duck

Yazılım Yaşam Döngüsü Boyunca Otomatik Güvenlik Analizi

Black Duck, yazılım geliştirme süreçlerindeki güvenlik kontrollerini otomatik hale getiren bir uygulama güvenliği çözümüdür. Kaynak kodu statik testlerle (SAST), çalışan uygulamaları dinamik (DAST) ve etkileşimli (IAST) testlerle, açık kaynak ve üçüncü taraf bileşenleri ise yazılım bileşeni analiziyle (SCA) değerlendirir. Tek başına kullanılabildiği gibi mevcut DevSecOps süreçlerine de entegre edilebilir.

Modern Güvenlik Zorlukları

Yazılım projelerinde kaynak kod, çalışan uygulamalar ve üçüncü taraf bileşenler farklı güvenlik riskleri barındırır. Güvenlik kontrollerinin geliştirme süreçlerine entegre edilmemesi, zafiyetlerin geç tespit edilmesine ve düzeltme maliyetlerinin artmasına neden olabilir. Artan bulgu sayısı da ekiplerin kritik riskleri önceliklendirmesini zorlaştırır.

Hangi Ekiplere Hitap Eder?

- Güvenlik açıklarını tespit etmek isteyen yazılım ekiplerine
- Güvenlik testlerini CI/CD süreçlerine entegre etmek isteyen DevSecOps ekiplerine
- Güvenlik bulgularını önceliklendirmek ve takip etmek isteyen siber güvenlik ekiplerine
- Yazılım güvenliğini geliştirme süreçlerine entegre etmek isteyen kurumlara

Temel İlkeler

Güvenlik
Yazılım açıklarını ve riskli bağımlılıkları tespit etme

Otomasyon
Güvenlik analizlerini CI/CD süreçlerine entegre etme

Önceliklendirme
Kritik güvenlik bulgularına odaklanma

Sürdürülebilirlik
Yazılım yaşam döngüsü boyunca güvenliği destekleme

Teknik Özellikler

Analiz Kapsamı
- Statik uygulama güvenliği testi (SAST)
- Dinamik uygulama güvenliği testi (DAST)
- Yazılım bileşeni analizi (SCA)
- Etkileşimli uygulama güvenliği testi (IAST)

Tespit Yetenekleri
- Bilinen bileşen zafiyetlerinin tespiti
- Açık kaynak lisans risklerinin analizi
- Yazılım bileşenlerinin güvenlik risklerine göre değerlendirilmesi
- Yazılım kaynak kodundaki güvenlik açıklarının etki analizinin yapılması

Entegrasyonlar
- GitLab ve GitHub gibi kaynak kod yönetim platformları
- Jenkins ve GitLab CI/CD gibi otomasyon araçları
- IDE ve geliştirici araçlarıyla entegrasyon
- SIEM/SOAR entegrasyonu

Uyumluluk ve Raporlama
- Açık kaynak lisans yükümlülüklerinin takibi
- Yazılım bileşen envanteri (SBOM) oluşturma ve yönetimi
- Güvenlik bulgularının merkezi takibi
- Risk ve lisans uyumluluğu raporlaması

Black Duck Nasıl Çalışır?

Black Duck, kaynak kodu, çalışan uygulamaları ve yazılım bileşenlerini güvenlik açısından analiz ederek zafiyetlerin ve lisans risklerinin tespit edilmesine yardımcı olur. SAST, DAST, IAST ve SCA süreçlerini destekleyen yaklaşımı, güvenlik kontrollerinin yazılım geliştirme yaşam döngüsüne entegre edilmesini ve kritik bulguların önceliklendirilmesini sağlar.

Çalışma Akışı

1. Yazılımın Analiz Edilmesi
- Kaynak kod, çalışan uygulamalar ve yazılım bileşenleri analiz edilir.
- SAST, DAST, IAST ve SCA kontrolleri uygulanır.
- Güvenlik açıkları ve riskli bağımlılıklar belirlenir.
- Lisans uyumluluğu riskleri değerlendirilir.

→

2. Güvenlik Bulgularının Değerlendirilmesi
- Tespit edilen güvenlik açıkları merkezi olarak değerlendirilir.
- Bulgular önem ve risk seviyelerine göre önceliklendirilir.
- Kritik güvenlik riskleri belirlenir.
- Düzeltme gerektiren bulgular ilgili ekiplere yönlendirilir.

→

3. Düzeltme ve Süreçlere Entegrasyon
- Geliştiricilere güvenlik bulgularını gidermeye yönelik bilgiler sunulur.
- Güvenlik kontrolleri CI/CD süreçlerine entegre edilir.
- Kritik bulgulara bağlı olarak pipeline veya release süreçleri otomatik olarak engellenebilir.
- Yeni analizlerle düzeltmelerin durumu takip edilir.

Neden AA Teknoloji?

Black Duck'ın kurulumunu, mevcut CI/CD ve kaynak kod yönetimi altyapınızla entegrasyonunu ve ekiplerinize yönelik ürün eğitimini AA Teknoloji olarak üstleniyoruz. Kurulum sonrasında 7/24 Türkçe teknik destek sağlıyoruz.

Avantajlar

Kapsamlı Güvenlik Analizi
Kaynak kodu, çalışan uygulamaları ve yazılım bileşenlerini analiz ederek güvenlik açıklarını ve lisans risklerini belirlemeye yardımcı olur.

Erken Zafiyet Tespiti
Güvenlik açıklarının geliştirme ve test aşamalarında belirlenmesine yardımcı olarak düzeltme maliyetlerini azaltır.

Risk Odaklı Önceliklendirme
Güvenlik bulgularının önem derecesine göre değerlendirilmesini ve kritik risklere odaklanılmasını sağlar.

DevSecOps Entegrasyonu
Güvenlik kontrollerinin CI/CD süreçlerine entegre edilmesini ve yazılım geliştirme yaşam döngüsü boyunca uygulanmasını destekler.

aa teknoloji

AA Teknoloji, Anadolu Ajansı iştiraki olarak medya teknolojileri, siber güvenlik ve açık kaynak çözümleri alanlarında hizmet sunan bir teknoloji şirketidir. SOC hizmetleri, sızma testi, SIEM/EDR, tehdit istihbaratı ve medya altyapısı çözümlerini kurulum, entegrasyon ve 7/24 yerel teknik destekle birlikte sunar.

Daha fazla bilgi için, aateknoloji.tr'yi ziyaret edin veya @aateknoloji LinkedIn hesabını takip edin.