aa teknoloji

Web Uygulama Güveliği Platformu (WAASP)

Web uygulamalarına yönelik saldırı öngörü, tespit ve müdahale platformudur. Yapay zekâ ve makine öğrenimi desteğiyle web uygulamalarının görünürlüğünü artıran, güvenlik analizlerini gerçekleştiren ve tüm süreci yönetilebilir kılan bir çözümdür.

Web Uygulamalarına Yönelik Siber Saldırı Analizinin Zorlukları

Artan Web Uygulama Tehditleri: Dijital çağın hızla gelişen ortamında, web uygulamaları ve servislerine yönelik tehditler giderek daha karmaşık ve önlenmesi zor hale gelmektedir. Geleneksel güvenlik çözümleri, modern saldırılara karşı yetersiz kalmakta ve işletmelerin kritik verilerini koruma kapasitesini sınırlamaktadır.
Saldırı Yüzeylerinin Genişlemesi: Web uygulamalarında mikro servislerin ve API tabanlı sistemlerin kullanımı saldırı yüzeyini büyütmekte, saldırganların istismar edebileceği alanları artırmaktadır.
Operasyonel Verimlilik: WAF, SIEM, SAST, DAST ve EDR gibi farklı güvenlik ürünlerinin ayrı ayrı yönetilmesi saldırı tespiti ve müdahale süreçlerini karmaşıklaştırmakta, operasyonel verimliliği azaltmaktadır.

✓ Yenilikçi Yönleri

· İmza tabanlı kuralların yanı sıra yapay zekâ ve makine öğrenmesi destekli analiz ile gelişmiş saldırıları tespit eder.

OWASP, IP Reputation, Geolocation, DDoS, makine öğrenmesi, yapay zekâ ve aksiyon yönetimi gibi farklı modülleri tek bir bütünleşik mimaride sunarak merkezi ve daha hızlı analiz imkânı sağlar.

· API tabanlı entegrasyonlar sayesinde farklı güvenlik ürünleri ve kurum içi sistemlerle uyum sağlar, analiz ve aksiyon süreçlerini hızlandırır.

· Verilerin kurum içerisinde işlenmesi sayesinde KVKK ve benzeri regülasyonlara uyum sağlar.

· Modern altyapı mimarisi sayesinde büyük hacimli log ve trafiği etkin şekilde işler.

Temel İlkeler

Entegre Güvenlik Platformu
Merkezi yönetim ve hızlı analiz

Hız
Gelişmiş saldırı tespit mekanizması

Veri Güvenliği
KVKK ve regülasyonlara uyumluluk

Kolay Entegrasyon
Güvenlik ürünleri ve sistemlerle entegrasyon

Teknik Özellikler

Merkezi Görünürlük
- Tüm web uygulamalarını tek bir platform üzerinden izleme ve yönetme

Gerçek Zamanlı İşleme
- Web trafiğinin anlık olarak analiz edilmesi

ML & AI Destekli Anomali Tespit Modülü
- SQL Injection, XSS, Directory Traversal, Command Injection gibi saldırıları yüksek doğrulukla tespit eden güvenlik katmanı

OWASP Modülü
- OWASP standartlarına uygun denetim sağlayan güvenlik katmanı

Geolocation Modülü
- Gelen isteklerdeki IP adreslerinin ülke ve şehir bilgilerini analiz eden güvenlik katmanı

DDoS Atak Tespit Modülü
- Web uygulamalarının baseline trafik profilini çıkararak olağan dışı aktiviteleri ve DDoS saldırılarını ayırt eden güvenlik katmanı

IP Reputation Modülü
- Gelen isteklerdeki IP adreslerinin itibar skorlarını analiz eden güvenlik katmanı

Aksiyon Yönetim Modülü
- Zararlı olarak belirlenen isteklerin diğer güvenlik ürünleri ile API entegrasyonu sayesinde engellenmesini sağlayan güvenlik katmanı.

WAASP Nasıl Çalışır?

WAASP; web uygulamalarının görünürlüğünü artırarak çeşitli güvenlik analizleri gerçekleştirir ve bu süreçleri yönetilebilir hale getirir. ML & AI destekli anomali tespiti, IP Reputation, OWASP, Geolocation, DDoS Atak ve Aksiyon Yönetimi modülleri sayesinde tüm güvenlik analizlerini tek bir merkezden yönetmenizi sağlar.

Çalışma Akışı

1. Veri Toplama
- Farklı log kaynaklarından verilerin toplanır.
- Veriler belirli bir kural çerçevesinde düzenlenir.
- İşlenen veriler ilgili modüllere iletilir.

→

2. Veri İşleme
- Kaynaklardan gelen veriler ML&AI Destekli Anomali Tespiti Modülü, IP Reputation Modülü, OWASP Modülü, Geolocation Modülü, DDoS Atak Modülleri ile işlenerek analiz edilir.
- Güvenlik analiz çıktılarına göre veriler ayrıştırılır ve puanlanır.

→

3. Görselleştirme
- Güvenlik analiz çıktıları kullanıcı arayüzü üzerinden görüntülenir.
- Saldırı skoru yüksek olarak belirlenen isteklerin incelenir.

4. Onay/Workflow süreci
- Güvenlik analisti onayıyla FW, LB, DDoS cihazları ve benzeri sistemlerde engelleme aksiyonları uygulanır.
- Onay/workflow süreci ile aksiyonlar yönetilir.
- Risk skoruna göre aksiyon önerisi sunulur.
- Uygulanan aksiyonlar için rollback (geri alma) desteği verilir.
- Aksiyonlar merkezi olarak yönetilir ve izlenir.

Sürekli İyileştirme
ML & AI Anomali Tespit Modülünün, saldırı yöntemlerindeki değişimlere uyum sağlayacak şekilde düzenli olarak güncellenmesi ve sürekli iyileştirilmesi sağlanır.

Avantajlar

Hızlı Kurulum ve Cloud-Native Mimari
Docker tabanlı cloud-native yapısı sayesinde kolay kurulabilme, bulut sistemlere entegre olabilme, stateless çalışma ve ölçeklenebilirlik imkanı sunar.

Yüksek Ölçeklenebilirlik
Modern altyapı mimarisi sayesinde yüksek hacimli log ve trafiğin etkin şekilde işlenmektedir.

Maliyet Avantajı
Ticari ürünlerin yüksek lisams maliyetlerine kıyasla daha uygun maliyetli, esnek ve ölçeklenebilir lisanslama modeline sahiptir.

Operasyonel Verimlilik
Merkezi yönetim ve aksiyon işlemleri sayesinde güvenlik analistlerinin operasyonel iş yükünün azaltılmasını sağlar.

aa teknoloji

AA Teknoloji, modern haber merkezleri için geliştirilen yapay zekâ destekli medya teknolojileri platformudur. Haber akış sistemlerinden dijital arşiv çözümlerine, gerçek zamanlı yayın altyapılarından çok kanallı içerik yönetimine kadar uzanan entegre çözümlerimiz; medya kuruluşlarının dijital dönüşüm süreçlerini hızlandırır ve ölçeklenebilir yayın operasyonları sunar.

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