aa teknoloji

Web Application Security Platform (WAASP)

It is a platform for attack prediction, detection, and response for web apps. Powered by AI and ML, it is a solution that increases visibility, performs security analysis, and makes the whole process manageable.

Challenges of Cyber Attack Analysis for Web Applications

Growing Web App Threats: In the fast-evolving digital era, threats to web apps and services are becoming more complex and hard to prevent. Legacy security solutions fall short against modern attacks, limiting the capacity to protect critical data.
Expanding Attack Surfaces: The use of microservices and API-based systems in web apps expands the attack surface, increasing the areas attackers can exploit.
Operational Efficiency: Managing different security products like WAF, SIEM, SAST, DAST, and EDR separately complicates attack detection and response, reducing efficiency.

✓ Innovative Aspects

- It detects advanced attacks with AI and ML-powered analysis in addition to signature-based rules.
- Provides centralized and faster analysis by offering different modules like OWASP, IP Reputation, Geolocation, DDoS, ML, AI, and action management in a single integrated architecture.
- Adapts to different security products and in-house systems via API-based integrations, speeding up analysis and action processes.
- Complies with KVKK and similar regulations by processing data within the organization.
- Processes large volumes of logs and traffic effectively thanks to its modern infrastructure architecture.

Core Principles

Integrated Security Platform
Centralized management and fast analysis

Speed
Advanced attack detection mechanism

Data Security
Compliance with KVKK and regulations

Easy Integration
Integration with security products and systems

Technical Specifications

Central Visibility
- Monitoring and managing all web apps via a single platform

Real-Time Processing
- Instant analysis of web traffic

ML & AI-Powered Anomaly Detection Module
- Security layer detecting attacks like SQL Injection, XSS, Directory Traversal, Command Injection with high accuracy

OWASP Module
- Security layer providing audits in compliance with OWASP standards

Geolocation Module:
- Security layer analyzing country and city info of IP addresses in incoming requests

DDoS Attack Detection Module
- Security layer distinguishing unusual activities and DDoS attacks by baselining web app traffic

IP Reputation Module
- Security layer analyzing reputation scores of IP addresses in incoming requests

Action Management Module
- Security layer enabling blocking of requests identified as malicious via API integration with other security products.

How WAASP Works?

WAASP increases web app visibility, performs security analyses, and makes these processes manageable. Thanks to ML & AI-powered anomaly detection, IP Reputation, OWASP, Geolocation, DDoS Attack, and Action Management modules, it lets you manage all security analysis from a single hub.

Workflow

1. Data Collection
- Collecting data from different log sources.
- Organizing data within a specific rule framework.
- Forwarding processed data to relevant modules.

→

2. Data Processing
- Data from sources is processed and analyzed via ML&AI-Powered Anomaly Detection, IP Reputation, OWASP, Geolocation, and DDoS Attack Modules.
- Security analysis outputs are displayed via the user interface.
- Requests identified with high attack scores are examined.

→

3. Visualization
- Security analysis outputs are displayed via the user interface.
- Requests identified with high attack scores are examined.

4. Approval/Workflow Process
- Blocking actions are applied on FW, LB, DDoS devices, etc., with security analyst approval.
- Actions are managed with approval/workflow processes.
- Action advice is offered based on risk score.
- Rollback support is provided for applied actions.
- Actions are centrally managed and monitored.

Continuous Improvement
Regular updates and continuous improvement of the ML & AI Anomaly Detection Module to adapt to changing attack methods.

Advantages

Fast Deployment & Cloud Native Architecture
Offers easy setup, cloud integration, stateless operation, and scalability thanks to its Docker-based cloud-native structure.

High Scalability
Effectively processes high volumes of logs and traffic via its modern infrastructure architecture.

Cost Advantage
Offers a more affordable, flexible, and scalable licensing model compared to high license costs of commercial products.

Operational Efficiency
It reduces the operational workload of security analysts through centralized management and action processes.

aa teknoloji

AA Teknoloji is an AI-powered media technologies platform developed for modern newsrooms. Our integrated solutions, ranging from news workflow systems to digital archive solutions, real-time broadcasting infrastructure to multi-channel content management, accelerate the digital transformation processes of media organizations and offer scalable broadcasting operations.

For more information, visit aateknoloji.tr or follow the @aateknoloji LinkedIn account.