aa teknoloji

# Imperum

A SOAR platform that centrally manages cybersecurity, system, and network operations; analyzes incidents and converts them into automated actions.

## Challenges of Modern Security Operations

In organizations, SIEM, EDR, firewall, and other security systems usually operate independently from each other. This leads to delays in incident response processes, manual processing workloads, and operational inefficiency.
Security teams are forced to manually analyze, correlate, and take action on alarms coming from different systems. This process both increases the risk of error and results in delayed responses to critical threats.
An expanding attack surface, high alarm volumes, and the necessity of 24/7 monitoring have become unsustainable with traditional methods.

⚠ Who can benefit?

- For organizations experiencing a lack of integration between security systems
- For SOC teams manually analyzing high volumes of alarms
- For organizations wishing to shorten incident response times
- For organizations aiming to build standardized and automated security processes

### Core Principles

**Automation**
Automates repetitive security tasks.

**Speed**
Supports real-time response to incidents.

**Continuity**
Provides 24/7 uninterrupted security operations.

**Centralized Management**
Gathers all systems onto a single platform.

## How Does Imperum Work?

Imperum centrally manages the entire lifecycle of security incidents. Thanks to playbook-based automation, incidents are analyzed, decision mechanisms are executed, and necessary actions are deployed automatically. Data from different security systems are gathered onto a single platform and given context through correlation. Automated or approved action scenarios are triggered depending on critical conditions.

### Technical Specifications

**Centralized Security Management**
- SIEM, EDR, Firewall integration
- Incident correlation and analysis
- Centralized dashboard and monitoring
- Management of alarms and events from a single panel

**Automation and Playbook**
- Playbook / workflow-based architecture
- Automated action triggering
- Manual approval mechanisms
- Condition-based decision and action flows

**Incident Response**
- IP, user and endpoint isolation
- Quarantine in email threats
- Security product rule management
- Malicious hash and IOC blocking operations

**Reporting and Monitoring**
- Real-time incident reporting
- Alarm history and action log tracking
- Dashboard-based security visibility
- Multi-channel notification system

**Artificial Intelligence**
- AI-powered incident analysis
- Alarm prioritization and risk scoring
- Anomaly and threat behavior detection
- AI-powered playbook generation

### Workflow

**1. Incident Collection**
- Alarm and log data are received from SIEM, EDR, firewall, and other systems.
- Data is normalized and transferred to the centralized platform.

**2. Analysis and Decision**
- Incidents are analyzed with correlation rules.
- Playbooks are triggered according to the risk level.
- Automated or manual approval mechanisms step in.

**3. Action and Response**
- IP blocking, user locking, endpoint isolation are applied.
- Rules are generated automatically in firewall and other systems.
- Notification and reporting processes are initiated.

**Continuous Improvement**
Supports security operations to remain continuously up-to-date and effective against changing threats.

## Advantages

**Playbook AI**
Enables the generation of dynamic action scenarios according to incident types and the smart optimization of processes thanks to AI-powered playbook production.

**Centralized Orchestration**
Provides centralized visibility and management by combining data coming from SIEM, EDR, Firewall, and other security systems onto a single platform.

**Real-Time Action**
Deploys actions such as IP blocking, user isolation, and alarm triggering instantly by analyzing threats in real time.

**Integration Capability**
Integrates easily with existing corporate systems thanks to its OpenAPI / REST API support, Connector / App-based modular design, and scalable architecture.

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.