aa teknoloji

Cybersecurity Operations Service (SOC)

It is a centralized operations service that monitors, analyzes, and manages incident response processes for organizations 24/7. It ensures that CSIRT processes, threat analysis, and incident response operations are handled from a single center.

Cybersecurity Challenges for Organizations

Organizations require continuous monitoring due to advanced threats, ransomware, data leaks, and insider threats. Scattered log structures and manual analysis processes cause critical incidents to be noticed too late.
The SOC service analyzes data from different security systems centrally, prioritizes threats, and ensures that swift action is taken.

⚠ Who can benefit?

- For organizations noticing security incidents late
- For operations teams performing manual log analysis
- For SOC teams struggling with false alarm management
- For organizations requiring 24/7 monitoring and response

Technical Specifications

Log Collection and Monitoring

- SIEM analysis across different sources
- Unified log integration structure
- Active log continuity tracking
- Error and accessibility tracking

SIEM and Incident Management

- Anomaly threat analysis
- Dynamic threat correlation
- IP and user visibility
- Risk-focused alarm optimization

Threat Intelligence

- Malicious IP and hash tracking
- Up-to-date IOC integration
- Custom threat hunting for organizations
- Attack trend analysis

Reporting and Operations

- Centralized SOC incident reports
- SLA-based response tracking
- Compliance and log support
- 24/7 SOC operational support

Core Principles

Accuracy
False alarm reduction

Fast Response
Swift action on critical events

Continuous Monitoring
24/7 seamless incident tracking

Visibility
Centralized log and event visibility

How Does the SOC Service Work?

The SOC service collects logs from security products within a centralized SIEM infrastructure. Events are analyzed with correlation rules and threat intelligence; critical alarms are prioritized, and incident response processes are managed.

Workflow

1. Data Collection

- Scattered log sources are gathered centrally.
- Security system data is received centrally.
- Critical systems are monitored continuously.
- Threat intelligence is integrated.

→

2. Analysis and Correlation

- SIEM correlation rules are executed.
- Suspicious user movements are analyzed.
- Real threats are prioritized.
- False positive alarms are filtered out.

→

3. Response and Reporting

- Escalation is initiated for critical events.
- Fast incident response process is operated.
- Incident logs are kept centrally.
- SOC operational reports are prepared.

Continuous Improvement

The SOC operation is continuously updated based on new threats, attack methods, and security needs. Alarm rules, analysis processes, and response procedures are regularly optimized.

Advantages

24/7 Security Monitoring
Security incidents are monitored and evaluated 24/7 within a centralized SOC operational structure, and critical alarms are tracked instantly.

Incident Response Management
Swift response, escalation management, and incident coordination are provided for critical events within the scope of CSIRT processes.

SIEM Log Analysis
Logs coming from different security systems are correlated, analyzed, and reported within a centralized SIEM infrastructure.

Threat Intelligence
Up-to-date IOC, malicious IP, and security intelligence data are actively utilized during threat analysis 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.