aa teknoloji

# OpenCTI

OpenCTI is an open-source CTI platform developed for SOC teams, CERT structures, and security operations centers looking to centrally manage cyber threat intelligence. It correlates threat data, analyzes it, and provides operational visibility.

## Cyber Threat Intelligence Challenges

Organizations struggle to centrally manage reliable threat intelligence due to rapidly increasing threat data and a complex attack surface. Correlating, analyzing, and transferring data from different sources to operations teams creates a significant operational burden.
Manual processing of threat indicators, data mismatch across various security tools, and scattered intelligence management make it difficult for SOC teams to take swift action. This situation can lead to the late detection of threats. The lack of real-time threat visibility makes it difficult for organizations to develop a proactive security approach.

Who can benefit?

- Provides centralized threat visibility for SOC teams
- Offers fast incident correlation for CERT teams
- Provides data correlation for security analysts
- Simplifies threat sharing for corporate teams

### Core Principles

**Openness**
Open source and transparent structure

**Correlation**
Relational threat analysis

**Visibility**
Centralized threat visibility

**Automation**
Fast and continuous data flow

## How Does OpenCTI Work?

OpenCTI correlates and analyzes data collected from different threat intelligence sources on a centralized platform and provides operational visibility to security teams. It supports fast decision-making processes by establishing links between IOCs, threat actors, and attack campaigns.

### Technical Specifications

**Threat Management**
- Correlating IOC and TTP data
- Threat actor analysis support
- Campaign and attack tracking
- MITRE ATT&CK compliant structure

**Integration Support**
- MISP integration support
- Compatibility with SIEM systems
- TAXII/STIX data sharing
- API-based data transfer

**Data and Analysis**
- Centralized threat data management
- Real-time data processing
- Relational threat analysis
- Automated data enrichment

**Access and Management**
- Role-based access management
- Multi-user platform support
- Web-based management panel
- Scalable architecture support

**Automation and Workflows**
- Automated threat feed management
- Incident response process integration
- Task and process automation
- Continuous data synchronization support

### Workflow

**1. Collect Data**
- External threat sources are connected.
- IOC and STIX data are imported.
- Automated data collection processes are operated.
- Data is received from security tools.

**2. Analyze and Correlate**
- Threat actors are matched.
- Campaign relationships are created.
- IOC correlation analysis is performed.
- Risk levels are evaluated.

**3. Share and Manage**
- Data is shared between teams.
- Centralized incident management is provided.
- Report and analysis outputs are generated.
- Continuous threat tracking is performed.

**Continuous Improvement**
Thanks to its open-source nature and wide integration support, OpenCTI quickly adapts to the evolving threat landscape. It supports enterprise security operations with its scalable architecture.

## Advantages

**Centralized CTI Management**
Gathers data coming from different threat intelligence sources onto a single platform to provide centralized analysis and operations management.

**STIX/TAXII Support**
Works compatibly with standard threat intelligence formats to offer fast and secure data sharing across security tools.

**Broad Integration Structure**
Works integrated with SIEM, MISP, and other security solutions to easily adapt to the existing security ecosystem.

**Relational Threat Analysis**
Establishes links between IOCs, threat actors, and attack campaigns to provide advanced threat correlation.

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.