aa teknoloji

Cyber Threat Intelligence (CTI)

It is a threat intelligence service that provides early warning by continuously monitoring cyber threats, data leaks, and dark web activities targeting organizations; it offers analysis, visibility, and action support to technical teams.

Cybersecurity Challenges

Organizations are faced with risks such as continuously evolving cyber threats, data leaks, credential disclosures, and brand abuse. Failure to detect threats at an early stage can lead to operational and reputational losses.
Access credentials shared on dark web platforms, rogue domains, and phishing infrastructures can often remain active for a long time without being noticed. This situation increases the attack surface of organizations and complicates the response processes of security teams.
Evaluation of critical threats without contextual analysis can cause incorrect prioritization and delayed action processes.

⚠ Who can benefit?

- Early threat visibility for security teams
- Swift action support for SOC teams
- Data leakage visibility for organizations
- Counterfeit asset detection for brand teams

Core Principles

Proactive
Notices threats before they actually occur.

Visibility
Monitors critical threats from a central point.

Analysis
Offers contextual threat assessment.

Response
Enables technical teams to take swift action.

How Does the Cyber Threat Intelligence Service Work?

Within the scope of the service, open sources, data leak environments, dark web platforms, and threat data feeds are continuously analyzed. Detected findings are verified, prioritized, and transformed into actionable outputs for the relevant teams.

Service Features

Threat Monitoring
- Continuous monitoring of dark web platforms
- Tracking of ransomware group leaks
- Scanning based on brand and organization name
- Detection of risky access advertisements

Data Leakage
- Corporate domain leak scanning
- Username and password matching
- Leak date and source analysis
- Providing subdomain-based visibility

Reporting & Notification
- Instant notification for critical findings
- Executive-oriented summary reporting
- Detailed analysis for technical teams
- Risk prioritization outputs

Brand Protection
- Typosquatting domain detection
- Fake social media account analysis
- Monitoring of fraudulent ad contents
- Mobile application tracking and analysis

Monitoring and Analysis
- Tracking of threat sources
- Fake social media account analysis
- Priority of critical findings
- Continuously updated threat analysis

Workflow

1. Data Collection and Monitoring
- Open source threat data is gathered.
- Dark web platforms are regularly monitored.
- Domain and brand scans are performed.
- Data leakage sources are analyzed.

→

2. Analysis and Interpretation
- Findings are technically verified.
- Risk levels are prioritized.
- Organization-specific contextual analysis is made.
- Critical threats are filtered and separated.

→

3. Notification and Action
- Critical findings are forwarded instantly.
- Analysis is presented for technical teams.
- Executive reports are shared regularly.
- Recommended action plans are prepared.

Continuous Improvement
Cyber Threat Intelligence is presented in a structure that can be continuously updated according to new threat sources, data feeds, and needs. Thanks to its scalable architecture, it adapts to different organizational requirements.

Advantages

24/7 Threat Monitoring
Closed forums, data sharing platforms, and ransomware leak pages are continuously monitored to detect risky content associated with the organization.

Data Leakage Tracking
Corporate email addresses, domains, and user credentials are scanned regularly to make leakage sources and risks visible.

Brand Protection
Typosquatting domains, fake social media accounts, mobile applications, and fraudulent advertisement contents are analyzed to reduce brand risk.

Action-Oriented Reporting
Threats are prioritized and rapid response processes are supported thanks to reports prepared specifically for management and technical teams.

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.