aa teknoloji

Sangfor Athena NDR

A network detection and response platform that analyzes network traffic in real time, detects cyber threats and anomalies using AI, and provides advanced visibility, threat hunting, and automated network orchestration.

Modern Network Security Challenges

The expansion of corporate networks, cloud integrations, and the increasing volume of encrypted traffic create blind spots across the network. Traditional firewalls and signature-based systems fall short in detecting threats that have bypassed borders and remain hidden.
Lateral movements performed by attackers within the network, data exfiltration attempts, and insider threats can remain active for long periods without being noticed. This situation poses a major risk to corporate data centers and critical infrastructures.
Manually analyzing and making sense of massive traffic data coming from different network segments is impossible.
The lack of contextual analysis for security teams makes it difficult to differentiate between real threats and false alarms.

What Problems Does It Solve?

- Providing visibility into threats hidden within network traffic blind spots.
- Detecting lateral movements and data exfiltration attempts within the network.
- Overcoming the challenges of analyzing malicious activities within encrypted traffic.
- Automating threat response processes and monitoring the attack chain end-to-end.

Core Principles

Deep Visibility
Eliminates all network blind spots to ensure full control.

Intelligent Analysis
Detects suspicious behaviors and anomalies using AI.

Rapid Containment
Instantly blocks the spread of attacks across the network.

Unified Response
Transforms network and endpoint systems into an integrated defense.

How Does Sangfor Athena NDR Work?

Sangfor Athena NDR (Cyber Command) operates by collecting mirror traffic data or flow logs across the corporate network within its centralized infrastructure. Collected data is analyzed using artificial intelligence models and machine learning algorithms to identify network anomalies. When a cyber attack chain is detected, the system generates alerts and automatically isolates the threat via integrated security products.

Technical Specifications

Network Traffic Analysis (NTA)
- Real-time deep packet inspection (DPI)
- North-South and East-West traffic monitoring
- Encrypted traffic analysis (ETA) support
- NetFlow, IPFIX, and mirror traffic collection

Advanced Threat Detection
- AI-based behavioral anomaly detection
- Full alignment with MITRE ATT&CK taxonomy
- Unknown threat and zero-day detection
- Command and Control (C2) communications tracking

Attack Chain Visualization
- Graph-based cyber attack chain analysis
- Root-cause analysis of threats and incidents
- Identification of affected assets and devices
- Forensic investigations and log analysis support

Security Orchestration and Response
- Automated IP blocking via firewalls
- Endpoint quarantine with EDR integration
- REST API over external systems compatibility
- Flexible and automated response playbook framework

Consulting and Managed Services
- Topology analysis, traffic throughput profiling, and sensor placement planning
- Core switch TAP/SPAN port configuration and turnkey Cyber Command integration
- Reduction of false positive rates, alert analysis, and optimization support
- DPI, ETA, platform forensics, and technical threat hunting instruction for SOC teams

Workflow

1. Traffic Collection and Monitoring
- Mirror traffic data is received from all network segments.
- Encrypted and unencrypted traffic flows are continuously monitored.
- Communication maps of network components are generated.
- Protocol and packet analyses are transmitted to the central system.

2. AI-Based Behavior Analysis
- Movements deviating from the baseline profile and anomalies are searched.
- Malicious connections are matched with threat intelligence.
- Attack stages are correlated with the MITRE ATT&CK framework.

3. Coordination and Response
- The attacker IP is blocked via the integrated Firewall.
- The infected endpoint is isolated via the integrated EDR.
- Detailed forensic analysis and SOC reports are generated.

Continuous Improvement
The Sangfor Athena NDR infrastructure continuously learns traffic patterns in the network to optimize its machine learning models, regularly increasing detection accuracy against next-generation threat variants.

Advantages

Advanced Encrypted Traffic Analysis (ETA)
Detects hidden malicious activities with high accuracy by analyzing metadata such as packet size and timing using AI, without decrypting the encrypted network traffic.

XDDR Threat Correlation
Integrates with Sangfor Athena EPP and Firewall solutions to merge network anomaly information with endpoint transaction logs, offering an autonomous and seamless response ecosystem.

Visual Attack Chain (Kill Chain)
Transforms complex network alarms into a meaningful story. It clearly shows via a graphic interface where the attacker entered the network, which devices they hopped to, and their ultimate objective.

Proactive Threat Hunting
Provides comprehensive historical data analytics tools that allow security analysts to proactively hunt for advanced persistent threats (APTs) hidden inside systems.

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.