aa teknoloji

Binalyze DFIR

Forensic-Powered Automated Cyber Investigation Platform

Binalyze DFIR enables SOC teams to get to the truth behind an alert within minutes, with remote evidence collection, forensic analysis, and automated investigation capabilities across endpoint, cloud, and hybrid environments. As Binalyze's authorized partner, AA Teknoloji designs the platform's integration with existing Wazuh, CrowdStrike, and SOC infrastructures, and manages the POC, deployment, training, and technical support process end-to-end.

Challenges Facing Today's SOC Teams

EDR, XDR, and SIEM systems generate alerts, but understanding an incident's root cause, affected systems, and scope of attack often requires additional evidence. In distributed environments, manually collecting this evidence from endpoints and cloud sources prolongs investigations and pulls analysts' time away from actual analysis toward data gathering.

Who can benefit?

- SOC teams that need to quickly confirm whether an alert points to a real incident
- Incident response and DFIR teams slowed down by manual evidence collection
- Analysts who want to bring endpoint and cloud evidence together under one investigation
- Organizations looking to make their investigation and reporting process more traceable

Core Principles

Visibility
Forensic-grade evidence collection from endpoints, cloud, and applications

Speed
Fast transition from alert to investigation

Integrity
Bringing evidence and findings together in one place

Analysis
Automated forensic analysis and prioritization powered by the DRONE engine

Technical Specifications

Evidence Collection Modules

- Acquisition: Targeted or full forensic evidence collection
- Hunt: Threat hunting with YARA, Sigma, and osquery
- Compare: Baseline comparison and anomaly detection
- InterACT: Real-time command execution and response

Cloud & Extended Capabilities

- Tornado: Evidence collection from Microsoft 365 and Google Workspace
- Magellan: Full-text search and eDiscovery
- Fleet AI: Natural-language generation of YARA, Sigma, and osquery rules
- Outpost: Support for remote and air-gapped environments

Platform Support

- Windows, Linux, macOS endpoint support
- ESXi virtualization environment support
- On-premise or SaaS deployment options
- Active Directory, 2FA, and LDAP support

Integrations

- Wazuh, CrowdStrike, Splunk
- Microsoft Sentinel and Cortex XSOAR
- ServiceNow, Okta, Slack
- Cisco, Sumo Logic, Elasticsearch Logstash Kibana Integration

How Does Binalyze DFIR Work?

After a security alert, Binalyze DFIR remotely collects the forensic evidence needed, analyzes it, and consolidates the findings under a single investigation so analysts can focus on understanding what actually happened and how far it spread, instead of searching for data across different tools.

Workflow

1. Evidence Collection

- Live and historical data collected from endpoints.
- Cloud evidence acquired.
- Targeted or comprehensive forensic data collection performed.
- Collected data enriched with threat intelligence and detection rules.

2. Analysis and Prioritization

- The DRONE engine automatically analyzes forensic evidence.
- Threat hunting performed with YARA, Sigma, and osquery rules.
- Abnormal changes detected through baseline comparison.
- Critical findings prioritized, noise filtered out.

3. Investigation and Reporting

- All evidence and findings consolidated in a central hub.
- Timeline and case management created.
- Investigation outputs reported.

Sample Use Case

When a suspicious alert appears in Wazuh, CrowdStrike, or another SIEM/EDR, Binalyze DFIR can be used to collect forensic evidence from the relevant system and confirm the incident. The move from alert to DFIR investigation happens within the same workflow.

Advantages

DRONE Automated Analysis
Automatically processes forensic evidence with built-in analyzers and detection rules; prioritizes critical findings and significantly shortens investigation time.

Centralized Investigation Hub
Brings evidence, findings, notes, and timelines together in one place, making team collaboration and case management easier.

Fleet AI (AI-Powered Investigation)
Converts natural-language commands into YARA, Sigma, and osquery rules, speeding up investigation workflows and letting analysts focus on critical decisions.

Works Alongside Your Existing SOC
Complements Wazuh and CrowdStrike alerts with a forensic investigation process.

aa teknoloji

AA Teknoloji is a technology company and an Anadolu Ajansı affiliate, providing media technologies, cybersecurity, and open-source solutions. It delivers SOC services, penetration testing, SIEM/EDR, threat intelligence, and media infrastructure solutions together with deployment, integration, and 24/7 local technical support.

For more information, visit aateknoloji.tr or follow @aateknoloji on LinkedIn.