binalyze!

INVESTIGATION & RESPONSE AUTOMATION

TURN SIGNALS INTO ANSWERS

INVESTIGATE FASTER | HUNT PROACTIVELY | RESPOND WITH CERTAINTY

Security teams face signals from alerts, threat intelligence, and SOC tools every day, but without forensically sound data, true understanding remains out of reach. Binalyze AIR turns signals into investigative momentum, giving all defenders in the SOC—analysts, threat hunters, detection engineers, and responders—the clarity and confidence to act decisively.

By combining deep visibility with scalable investigation-ready capabilities, AIR enables rapid, proactive and reactive investigations, so teams can move from uncertainty to answers in minutes.

OVERCOME KEY INVESTIGATION CHALLENGES

- Investigate with forensic depth, quickly and at scale
- Collect and understand evidence across endpoints, cloud, and applications
- Eliminate manual workflows and reduce investigation dwell time
- Empower analysts with automation and expert-level AI assistance
- Integrate seamlessly into your existing security stack
- Enable consistent, collaborative investigations across teams

THE SOC'S MISSING SUPERPOWER

AIR disrupts traditional investigation workflows and completes the SOC stack where detection-led solutions stop. Not simply a connector of telemetry, AIR introduces a new layer of forensic clarity, making deep investigation accessible at the speed and scale required to keep pace with modern threats, working alongside existing tools to enhance their value. Teams turn signals into understanding early, shifting investigations left and enabling forensic-grade insight without slowing decisions.

SEE WITH CLARITY. ACT WITH PRECISION.

AIR delivers a forensically sound data layer that closes visibility gaps detection tools can't. It rapidly collects and processes forensic data — memory, disk, and historical artifacts — from assets across major and specialised OSs, cloud workloads, and enterprise applications. AIR then integrates everything into a unified, actionable view that transforms raw data into understanding.

- **Collect evidence at speed** with profile-based, full-disk, or offline acquisition options tailored to the needs of each investigation
- **Analyze and prioritize** using severity-driven multi-engine findings, MITRE ATT&CK mapping, and collaborative timelines
- **Trust the data** with encryption, compression, and timestamping, ensuring all evidence remains raw, verifiable, and usable by human and AI operators, like Binalyze Fleet*.

POWER TO THE ANALYST

AIR reduces manual effort, cuts through noise, and puts analysts back in control. From initial triage to in-depth threat hunting, standardised workflows and expert AI-assistance give every analyst the ability to investigate effectively. AIR is designed to support defenders and to ensure investigations are consistent, precise, and scalable across the SOC.

- **Automate** repetitive investigation tasks with scheduled and event-driven workflows, while giving analysts on-demand control to pursue leads quickly.
- **Pair AIR with Fleet,** an AI-operator that works alongside human investigators to perform complex, expert-level investigation workflows
- **Accelerate triage, compromise assessments and hunting** using YARA, Sigma, osquery scans, automated asset tagging and full-text search at scale for precise, efficient investigations.

ANSWERS IN MINUTES.

AIR accelerates investigations across your entire SOC by delivering investigation-ready capabilities directly within your existing security stack. Seamlessly integrating with SIEM, EDR, XDR, SOAR, CTI and ticketing systems, becoming a critical part of the SOC stack, removing traditional investigation friction and enabling teams to act confidently and decisively in minutes rather than days.

- **Automate workflows and trigger investigations instantly** with AIR's API and webhook framework for fast, frictionless execution
- **Scale investigations, response actions and hunt** across your entire environment with on-the-edge data processing and analysis, and super remote shell capabilities
- **Accelerate detection-to-response** with enriched context, centralised case management and oversight, and ready-to-use investigation data

WHY BINALYZE AIR?

Binalyze AIR completes your SOC, transforming traditional detection-led workflows into investigation-ready operations. Built on a forensic-grade visibility layer, AIR delivers clarity at speed and scale, turning signals into actionable answers. It ensures SOC teams are able to investigate faster, hunt proactively, and respond with certainty.

* Binalyze Fleet is the agentic SOC workspace that performs investigation workflows tackled by L3 analysts, including reverse malware engineering, network capture analysis, detection rule generation (currently in private preview).