Boost cyber resilience with proactive and rapid investigation and response

Binalyze AIR is a next-generation automated investigation and response platform that streamlines incident response workflows, enhancing cyber resilience. Unlike traditional, complex forensic solutions, AIR makes forensics accessible by simplifying the process, offering forensic-level visibility at unprecedented speed and scale. With features like remote evidence acquisition, automated analysis, and intelligent triage, AIR integrates seamlessly with existing detection tools, boosting root cause analysis and proactive response efficiency.

Supercharge investigations with next-gen automation

Binalyze AIR redefines traditional incident investigations with cutting-edge automation, equipping your team with the tools to identify compromise and suspicious anomalies, investigate, and respond more effectively.

Overcome key investigation challenges

- Empower investigation teams to quickly gain full visibility across compromised assets, enabling investigations at scale and speed.
- Eliminate manual effort and accelerate time to contextualized insights with automated analysis that reduces response times.
- Enable streamlined, integrated workflows that provide a consistent framework for investigation and remediation.
- Address common gaps such as incomplete incident visibility, limited remote acquisition, and increasing cloud infrastructure risks.
- Minimize alert fatigue by filtering critical insights and prioritizing actionable data.
- Strengthen collaboration across teams with a single platform that consolidates evidence and analysis into one unified view.

Speed and accuracy meets simplicity

Binalyze AIR's forensic data collection and analysis capabilities provide incident responders and analysts with fast, and accurate insights in just a few clicks. AIR's cloud-native platform enables teams to collect and analyze evidence concurrently across platforms like Windows, Linux, macOS, ChromeOS, and ESXi within minutes, ensuring:

- **Evidence-based insights across** hundreds of evidence types.
- **Full evidence encryption** compression, and timestamping, maintaining data integrity.
- **Effortless case management** through an integrated single-pane-of-glass interface.

Unified workflows for faster incident resolution

Binalyze AIR offers a complete, integrated workflow that works seamlessly with SOC tools, uniting teams across the SOC and beyond with a single, unified view. This collaborative approach ensures full visibility for every stakeholder, breaking down silos and accelerating investigation times. With aggregated evidence and MITRE ATT&CK mapping, AIR empowers teams to:

- **Focus investigations** with prioritized, intelligence-driven insights, ensuring critical threats are addressed first.
- **Maintain a unified view** of events with comprehensive timelines, enabling quicker decision-making.
- **Leverage powerful filters and search** to efficiently query large datasets, streamlining analysis and reducing time to resolution.

Streamline investigations with intelligent automation

Binalyze AIR automates and accelerates critical and manual investigation processes, allowing teams to cut through the noise of overwhelming cybersecurity data, while seamless SIEM, EDR, XDR and SOAR integrations ensure continuous 24/7 task automation across environments. Binalyze AIR empowers analysts and responders to rapidly uncover critical insights and hidden threats to enable fast and confident decision making. Key capabilities include:

- **Webhooks and API** support for custom workflows and integrations.
- **Advanced Triage and DRONE features** leverage proprietary analyzers; YARA, Sigma, and osquery rules for precise detection.
- **Automated auto-asset tagging and baseline comparisons** eliminate manual tasks and enable proactive hunting and assessments.
- **Granular access control**, ensuring secure and efficient investigations.

Why Binalyze AIR?

Binalyze AIR revolutionizes investigation and response processes by blending forensic-level visibility with intelligent automation. It empowers incident response teams and SOCs with proactive, rapid, accurate, and collaborative insights, resulting in faster investigations and stronger security outcomes.

With features like remote evidence acquisition, automation-driven analysis, and an intuitive, collaborative interface, AIR drastically reduces investigation times and simplifies the entire process. Let Binalyze AIR help your team work smarter—not harder—for faster, more effective threat resolution.

Visit us at: binalyze.com

𝕏 @binalyze

in company/binalyze