b!nalyze

Binalyze AIR: **Investigation Hub**

Harness the power of consolidation, prioritization, and collaboration for efficient incident response investigations

Current challenges: Slow and fragmented investigations

Today, incident responders and security analysts rely on a combination of different tools, face increasing data volumes, and struggle with siloed analysis and investigation methodologies. These challenges lead to process inefficiencies that leave investigations prone to gaps and expensive delays. Despite having access to evidence, often collected with great effort over several days, the data is still dispersed in various formats. Thus making it challenging to consolidate for actionable outputs or insights in both reactive and proactive investigations.

Adding to these challenges are the manual and repetitive tasks associated with case management and reporting. This complexity underscores the inadequacy of traditional DFIR tools and existing security solutions, which are not equipped to handle the urgent demands of investigating both known and unknown threats.

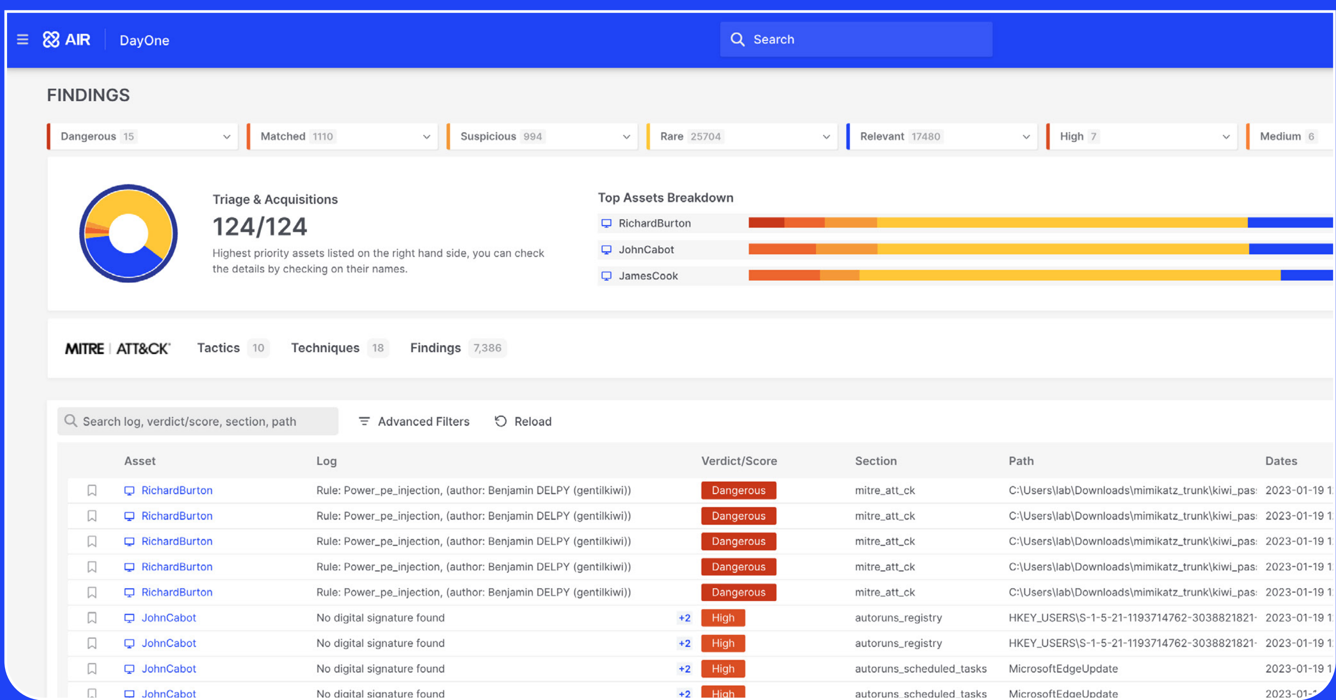
Solution: Consolidated, integrated investigations

To remove the need to move between screens, manual tasks, and tools, Binalyze AIR's Investigation Hub provides a single pane of glass that enables security analysts and incident responders to perform efficient and streamlined investigations within a single Digital Forensic and Incident Response (DFIR) platform.

The Investigation Hub sits at the heart of the AIR platform, integrating deep forensic visibility and efficiency-driving capabilities in one single, collaborative space to manage and progress an investigation from beginning to end.

Key benefits

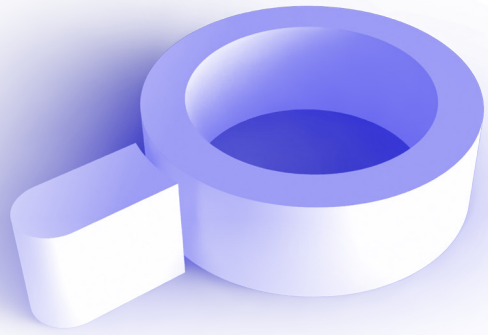
- Reduce time-consuming investigation and analysis tasks with a single, unified view of case-related insights
- Cut through large collected data sets and focus on the most important artifacts first with enriched investigation data
- Navigate through investigations and analysis intuitively
- Immediately highlight and identify the most significant assets to accelerate your investigation
- Get started on your investigation faster with prioritization through automated intelligence-driven scoring and verdicts



Unified and searchable insights

The Investigation Hub provides a single consolidated and organized view of all the assets, evidence, artifacts, and triage results associated with a case. Using filtering and global search helps you quickly review and focus your investigation on relevant details without relying on external tools. Avoid constant tool switching and time spent moving between screens and piecing data together.

Enhance and further enrich your investigations and analysis with additional sources and context with data importing capabilities.

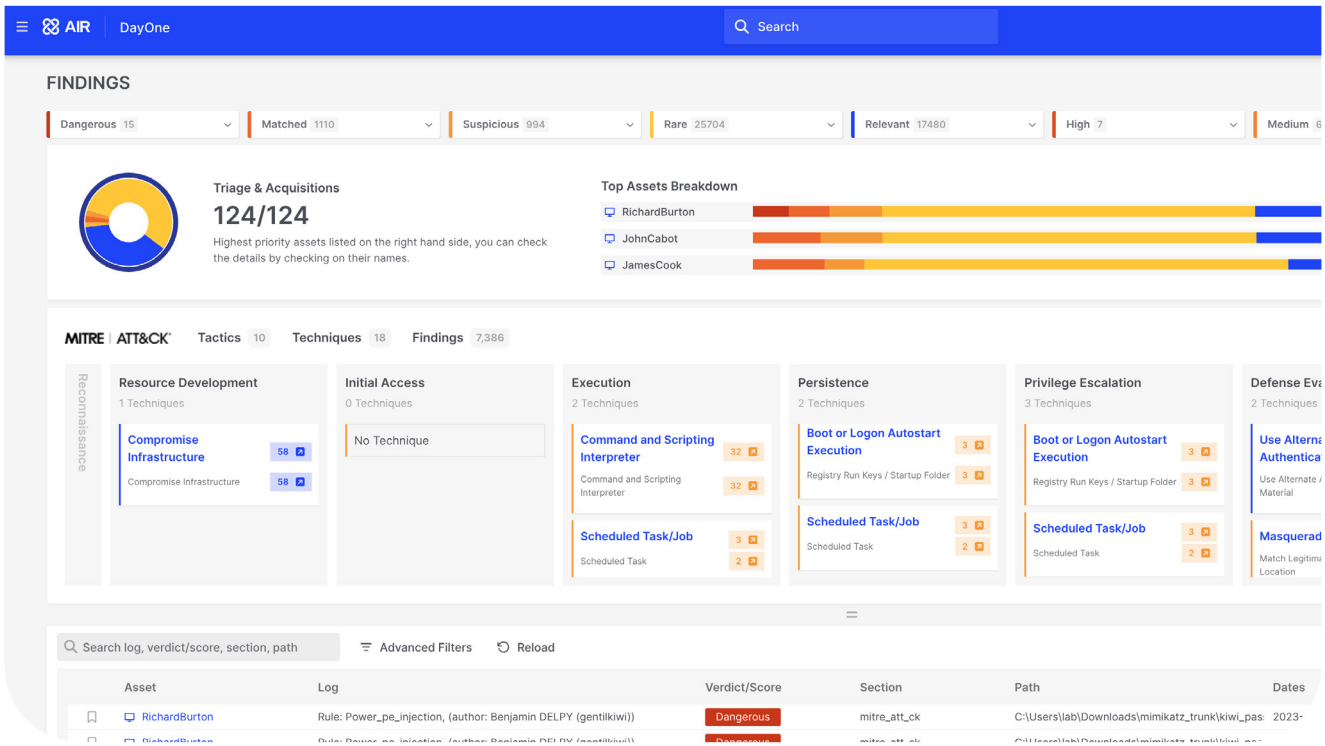


Intelligent evidence prioritization

The Investigation Hub includes findings, scores, and verdicts from Binalyze AIR's Triage and DRONE features to help you get a head start on any investigation. Using DRONE's proprietary analyzers, YARA, Sigma, and osquery can scan assets and evidence. You can uncover compromised assets to sift through evidence from hundreds of assets to get to the insights that help prioritize the next steps in your investigation and target critical areas more quickly.

AIR's automated evidence analyzer, DRONE, supports Windows, macOS, and Linux. Automated analyzers are continuously updated and improved by our dedicated DFIR Lab team of cybersecurity researchers and malware analysts to deliver peace of mind and confidence that you are integrating the latest real-world intelligence.

The integrated MITRE ATT&CK mapping adds context to understand which threats you are dealing with and stay ahead of the next steps in an attack, and identify gaps in existing monitoring and detection capabilities.



Efficiency-driving collaboration

Empower teams and enable collaboration with a web-based platform that provides a shared view accessed by global and remote team members. It doesn't matter where the skills and specialists are around the globe. The evidence and findings are available for all team members contributing to closing the case.

The Investigation Hub's bookmarking capabilities enhance collaboration between analysts and responders working on a case by marking evidence and pointing team members to the most useful information, insights, and findings. This experience will continue to evolve as the Investigation Hub is enhanced with additional collaborative features in every subsequent release.

The vision

AIR provides MSSPs, Incident Response Service Providers, and Enterprise SOCs the capabilities to quickly, seamlessly, and confidently move from evidence collection into thorough analysis, investigation, containment, and ultimately full remediation.

AIR's Investigation Hub continues to integrate advanced investigative features, including comprehensive Timeline capabilities, customizable reporting, case management, and additional collaborative features.

"We've just started using the Investigation Hub feature and we already love it.

It's dramatically improving efficiency when you need to investigate hundreds of assets at once, and having one unified view for the entire team is really helpful."

– Monti Sachdeva, DFIR Lead at CyberClan

Why Binalyze AIR?

Lightning-fast evidence acquisition

Remote collection of over 350 digital forensic evidence types. Collecting from any asset on your network across Windows, Linux, macOS, and Cloud takes a few clicks and is completed in minutes

Cut through the noise of security data

A comprehensive suite of capabilities to help you analyze, investigate, collaborate, and complete investigations and threat hunts quickly with Timeline, Triage, interACT secure remote shell capability, and AIR's automated evidence analyzers.

Automated integrated and collaborative forensics

Work smarter, not harder, with flexible integration features to automate DFIR capabilities, eliminate low-value manual tasks, and make teamwork easy and consistent.

AIR covers Windows, Linux, macOS, ChromeOS, ESXi & Cloud

Binalyze is the developer of AIR, the world's fastest, end-to-end Digital Forensics and Incident Response (DFIR) platform.

AIR offers a combination of powerful automation, advanced integration features, and a user-friendly collaborative interface. This comprehensive solution assists SOC teams and incident responders to efficiently resolve incident response cases. By doing so, it significantly shortens dwell times and enhances cyber resilience.

AIR's suite of capabilities includes remote evidence acquisition and automated intelligence-driven evidence analyzers. Its core Triage, Timeline, and interACT remote shell features speed up investigation and remediation efforts. The AIR Investigation Hub sits at the heart of the platform to provide an integrated view of case-related evidence and insights to seamlessly and consistently manage investigations.

Learn more about delivering cyber resilience with improved investigations

Download AIR Brochure