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.

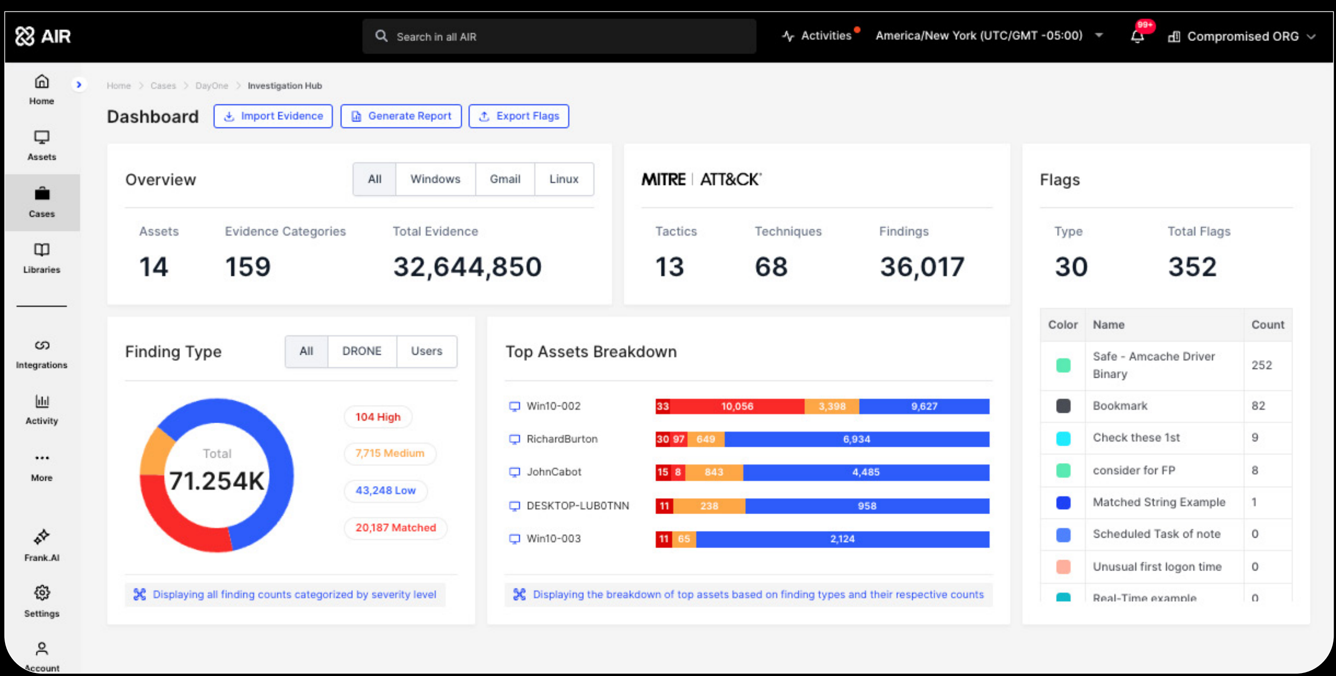
Solution:
Consolidated, integrated investigations

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 platform.

The Investigation Hub sits at the heart of the AIR (Automated Investigation and Response) platform, integrating deep forensic visibility and efficiency-driving capabilities in one unified, 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 automated analysis and prioritized intelligence-led findings



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 advanced filtering capabilities and global search helps you quickly review and focus your investigation on relevant details without relying on external tools. Avoid constant tool switching, siloed workflows 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

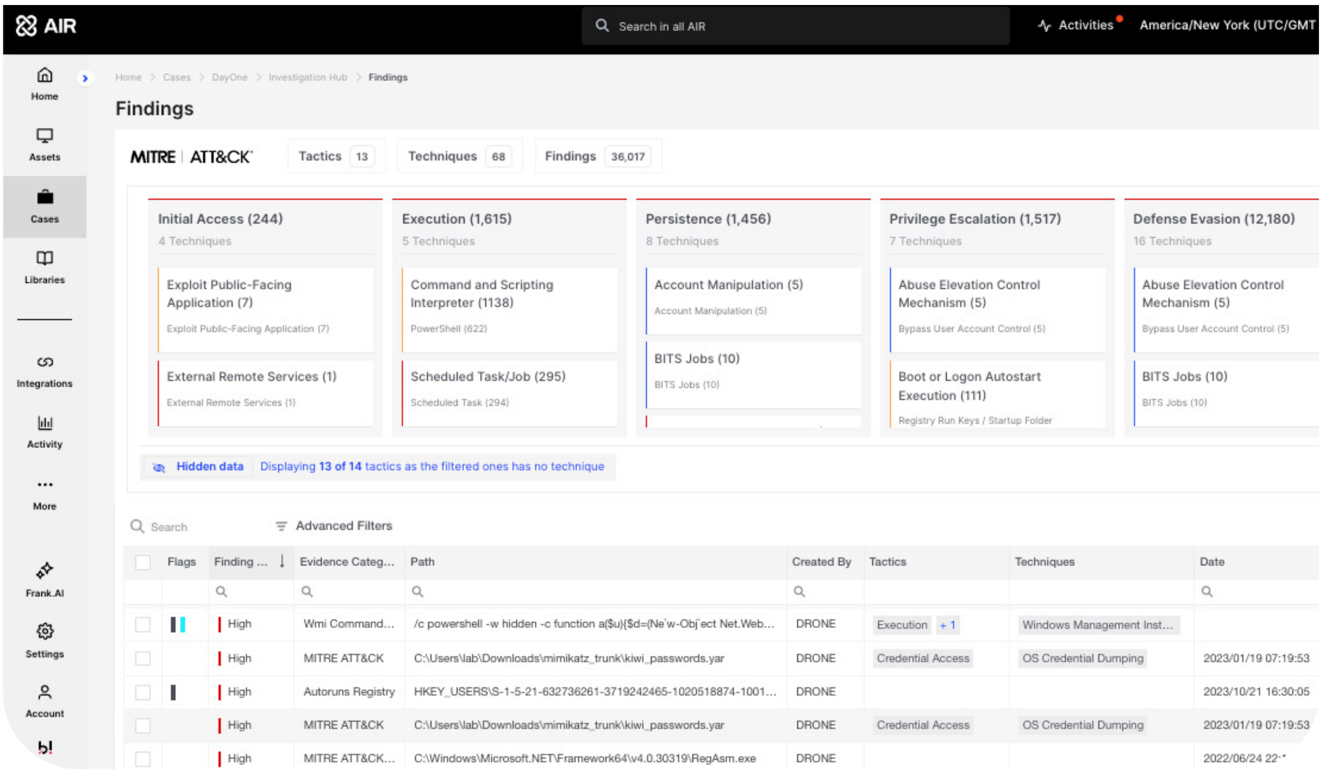
The Investigation Hub includes prioritized findings, to help you start your investigations where it matters most. DRONE's proprietary analyzers use pre-built YARA, Sigma and osquery rules to scan assets and evidence. You can uncover compromised assets concurrently across hundreds of assets to get to the insights that help prioritize the next steps in your investigation and target critical areas more quickly.

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

AIR

DRONE

AIR's built-in compromise assessment capability, DRONE, supports Windows, macOS, and Linux. DRONE's automated analyzers are continuously updated and improved by our dedicated DFIR Lab team of cybersecurity researchers, threat hunters and malware analysts to deliver peace of mind and confidence that you are integrating the latest real-world intelligence on threat actor TTPs.



Efficiency-driving collaboration

Empower teams and enable collaboration with a cloud-native 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 Activity Feed features enables team collaboration and transparency by logging all actions taken by team members working together in an investigation.

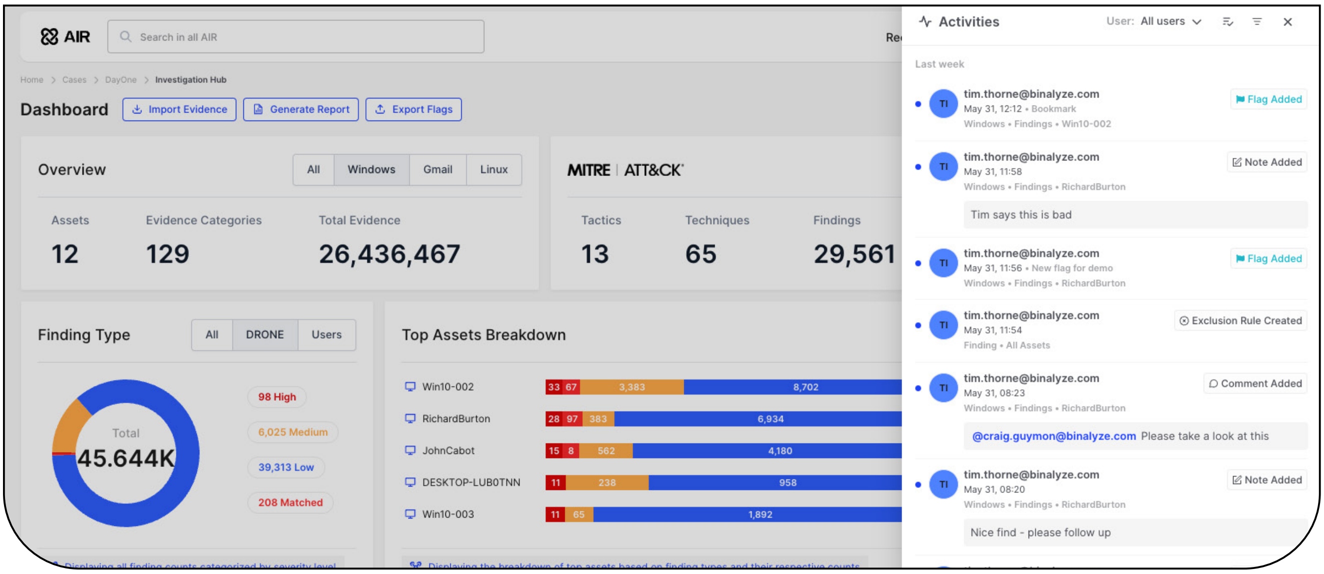
In addition, the Investigation Hub's custom flagging, notes and commenting capabilities enhance collaboration between analysts and responders working on a case by marking evidence and pointing team members to useful information, insights, and findings. The ability to save and share filters ensures everyone can benefit from useful investigation methodologies and processes.

The vision

Binalyze AIR offers a comprehensive Automated Investigation and Response platform. AIR provides MSSPs, Incident Response Service Providers, and Enterprise SOCs the capabilities to quickly, seamlessly, and confidently move from evidence collection into thorough analysis and investigation.

"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?

Speed and accuracy meets simplicity

Forensic data collection and analysis capabilities provide incident responders and analysts with fast and accurate insights in just a few clicks. AIR enables teams to collect and analyze evidence concurrently across platforms like Windows, Linux, macOS, ChromeOS, and ESXi within minutes.

Streamline investigations with intelligent automation

Accelerate critical and manual investigation processes, allowing teams to cut through the noise of overwhelming data. Seamlessly integrate with SIEM, EDR, XDR and/or SOAR and empower investigators to rapidly uncover critical insights for fast, confident decision making.

Unified workflows for fast incident resolution

Integrate workflows seamlessly with existing SOC detection and monitoring tools, uniting teams across the SOC with a single, unified view. This collaborative approach ensures full visibility, breaking down silos and accelerating investigation times.

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

Binalyze is the developer of AIR, an innovative Automated Investigation and Response platform powered by forensic-level visibility. Binalyze empowers incident response and SOC teams with rapid, accurate, and unified insights at unmatched speed and scale, delivering faster investigations, stronger security outcomes, and boosting cyber resilience.

With features like remote evidence acquisition, automated analysis, precision hunting, and an intuitive, collaborative interface that provides a consolidated view of context-rich, effective forensic insights, AIR drastically reduces investigation times and simplifies the entire investigation workflow.

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