binalyze!

INVESTIGATION AND RESPONSE AUTOMATION PLATFORM

INTRODUCTION

Your SOC is built to detect threats. But detection is only the beginning. Existing security tools generate alerts and signals, yet the questions that matter most often remain unanswered:

- What actually happened?
- Which systems are affected?
- What data is at risk?
- How far did it spread?

These are the questions that determine response, recovery, and resilience.

For many security teams, obtaining the evidence needed to answer them remains slow, fragmented, and dependent on specialist skills. As a result, critical response decisions are often made without complete clarity.

68% OF CISOS SAY THEIR TEAMS ARE FORCED TO ACT ON INCOMPLETE DATA.[1]

[1] The State of Cyber Investigations Report, 2026

Investigation should be an everyday capability of the SOC, enabling teams to move from signals to understanding whenever questions need answering. By making forensic-grade investigation part of everyday security operations, teams gain rapid access to the evidence they need to validate alerts, understand scope and impact, hunt for threats, and respond with confidence.

Binalyze AIR is the Investigation Platform that transforms alerts, signals, and findings into investigation-ready context, giving security teams the clarity to understand what happened and act with confidence.

FORENSIC VISIBILITY ACROSS YOUR ENTIRE ENVIRONMENT

AIR provides investigation-ready access across Windows, Linux, and macOS environments, extending into cloud workloads and SaaS applications. From a single Investigation Platform, security teams can collect, analyze, and respond to evidence wherever an investigation leads.

AIR collects and processes hundreds of forensic evidence types, providing the visibility needed to understand what happened, where it happened, and how activity spread across the environment. Rather than relying solely on telemetry and alerts, investigators gain direct access to the underlying evidence required to validate findings, determine scope, and drive investigations to conclusion.

Visibility across your environment

- **System & Endpoint Activity:** Processes, execution history, persistence mechanisms, system configurations, and event data across Windows, Linux, and macOS environments.
- **User & Application Behavior:** Browser history, communications, productivity applications, and user-driven activity that provide context around behavior and intent.
- **File System & Disk Evidence:** File system structures, disk artifacts, and full disk imaging across supported platforms, including NTFS and other native file systems.
- **Network & Communication Data:** Network flows, connections, and packet capture (PCAP) to support investigation of lateral movement and external communications.
- **Cloud & SaaS Environments:** Cloud workload and SaaS application evidence, including audit logs, user activity, mailbox data, and file access events.

*Discover Fleet, the Agentic Investigator

THE RESPONDER MODEL

INVESTIGATION-READY ACCESS

AIR operates as a forensic-grade investigation layer, using lightweight responders to provide investigation-ready access wherever investigations begin.

Unlike continuous monitoring tools, responders remain passive until collection, hunting, analysis, or response actions are triggered, either on-demand by an analyst or AI agent*, or automatically through integrated workflows. This enables investigations at scale without the overhead of continuous data collection.

INVESTIGATION TASKS AT SCALE

Execute acquisition, searches, hunting, analysis, and response across your entire environment simultaneously.

INVESTIGATION READINESS

Maintain continuous access to assets and evidence sources, ready to investigate whenever needed.

HYBRID ENVIRONMENT COVERAGE

Investigate on-premises, remote, and cloud environments through a single platform and consistent workflow.

LIGHTNING FAST EVIDENCE ACQUISITION

AIR enables rapid, forensic-grade evidence acquisition across endpoints, servers, cloud workloads, and SaaS environments. Investigators can collect the evidence required to validate alerts, scope incidents, and understand compromise without requiring physical access to systems.

FLEXIBLE ACQUISITION CONTROL

Whether performing rapid triage or deep analysis, AIR provides flexible collection options that balance speed, scope, and investigative requirements.

- **Profile-Based Acquisitions:** Use predefined or custom acquisition profiles to standardize investigations and collect only the evidence required for a specific case.
- **Custom Evidence Collection:** Define targeted collection criteria using paths, file patterns, and custom artifact selection to support specific investigative objectives.
- **Full Disk Imaging:** Perform full disk acquisition when complete forensic preservation is required, including support for DD and E01/Ex01 formats.

ACQUIRE FROM ANY ENVIRONMENT

Collect evidence across your environment from:

- On-prem and remote endpoints
- Offline and air-gapped systems
- Cloud virtual machines (AWS, Azure, GCP)
- Cloud and SaaS environments through Tornado*

INVESTIGATION - READY ACQUISITION

- **Automated & Integrated:** Execute acquisitions on-demand, on a schedule or automatically through integrations, event triggers and workflows.
- **Scalable & Remote:** Run acquisition tasks concurrently across large environments using lightweight responders and centralized orchestration.
- **Forensically Sound:** Evidence is hashed and timestamped to RFC 3161 standards to maintain integrity and support chain-of-custody requirements.
- **Secure Handling:** Support evidence compression, AES-256 encryption, and flexible repository options for secure storage, transfer and access.
- **Offline Collection:** Acquire and triage evidence from disconnected or air-gapped systems, then import results into AIR for continued investigation.
- **Investigation-Ready Analysis:** Built-in analyzers automatically process collected evidence and surface findings to accelerate triage and investigation.

* Acquisitions from SaaS applications is enabled via Tornado, Binalyze's application designed to collect and analyze digital evidence from cloud platforms. Integrated within AIR workflows and also available as a standalone desktop application.

AUTOMATED ANALYSIS

ACCELERATE INVESTIGATIONS WITH AUTOMATED ANALYSIS & PRIORITIZATION

POWERED BY DRONE

DRONE is AIR's automated analysis and prioritization engine, designed to analyze forensic evidence and live assets at scale.

AUTOMATED ANALYSIS & TRIAGE

Automatically process forensic evidence through built-in analyzers to surface anomalies, suspicious activity, and indicators of compromise across assets.

MITRE ATT&CK MAPPING

DRONE's MITRE ATT&CK Analyzer scans live assets for evidence, mapping activity to known techniques and providing real-time visibility into potential threats.

PRIORITIZED FINDINGS

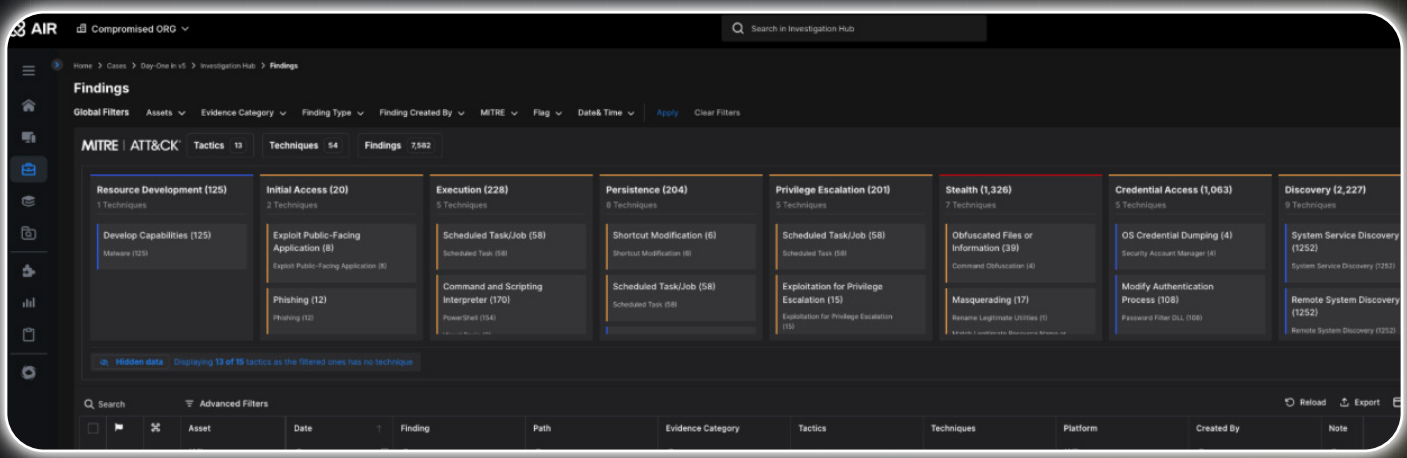
Findings are organized by severity and relevance (high, medium, low, matched), enabling investigators to focus on the most important evidence and assets first.

INVESTIGATION-WIDE ANALYSIS

Apply DRONE analysis capabilities across acquisitions, live investigations, hunting activities, and compromise assessments, as well as imported evidence.

RAPID KEYWORD SEARCHING

Perform fast, flexible searches across metadata to match domains, IP addresses, file names, hashes, and other structured artifacts.



AUTO-ASSET TAGGING

SCOPE INVESTIGATIONS WITH AUTO-ASSET TAGGING

Automatically categorize assets using system characteristics, activity, and custom criteria to rapidly identify systems relevant to an investigation.

- **Automated & on-demand:** Apply tags during deployment or run tagging activities at any time.
- **Predefined profiles:** Automatically identify common infrastructure and server roles, including domain controllers, mail servers, and web servers.
- **Custom tagging logic:** Create tailored tags using process, file, directory, host, and IP-based conditions.

INVESTIGATION TARGETING

Use tags to quickly define investigation scope across both proactive and reactive workflows.

- **Identify affected systems during active incidents**
- **Create targeted groups for threat hunting**
- **Focus exposure and vulnerability assessments**
- **Organize assets by role, behavior, or risk**

FULL-TEXT SEARCH

INVESTIGATE BEYOND METADATA WITH FULL-TEXT SEARCH

Powered by Magellan, Full-Text Search brings content-level investigation into AIR, enabling teams to search within documents, files, and artifacts directly at the source. By searching the actual contents of files rather than relying on metadata alone, investigators gain direct evidence to validate findings and answer critical investigative questions.

- **Search at the Source:** Execute searches across assets through AIR's distributed architecture, enabling efficient investigations at scale while minimizing unnecessary data movement.
- **Support proactive investigation:** Search for specific content, policy violations, or risk indicators across assets without waiting for alerts.
- **Investigate Faster:** Validate findings, uncover relationships, and answer investigative questions more quickly.

ASSET ISOLATION

CONTAIN THREATS WITH ASSET ISOLATION

Asset Isolation enables analysts to immediately contain potentially compromised assets while maintaining full investigative access through AIR.

By blocking all network communication except the connection to the AIR Console, teams can prevent attacker activity, preserve evidence, and continue investigations without interruption.

HUNT WITH PRECISION & SCALE

Execute Hunt across thousands of assets simultaneously. Hunt enables investigators to ask targeted questions across assets using live, on-demand data. Validate hypotheses, scope incidents, and proactively identify suspicious activity, exposure, and anomalous behavior without solely relying on predefined detections.

MULTI-ENGINE INVESTIGATION CAMPAIGNS

Combine multiple investigative approaches within a single workflow using built-in analyzers, MITRE ATT&CK-aligned detections, YARA, Sigma, osquery, custom logic, and targeted investigative queries.
This allows defenders to:
- Apply proven detection logic where appropriate
- Execute targeted checks across systems
- Adapt as new findings emerge

SCHEDULED & AUTOMATED INVESTIGATIONS

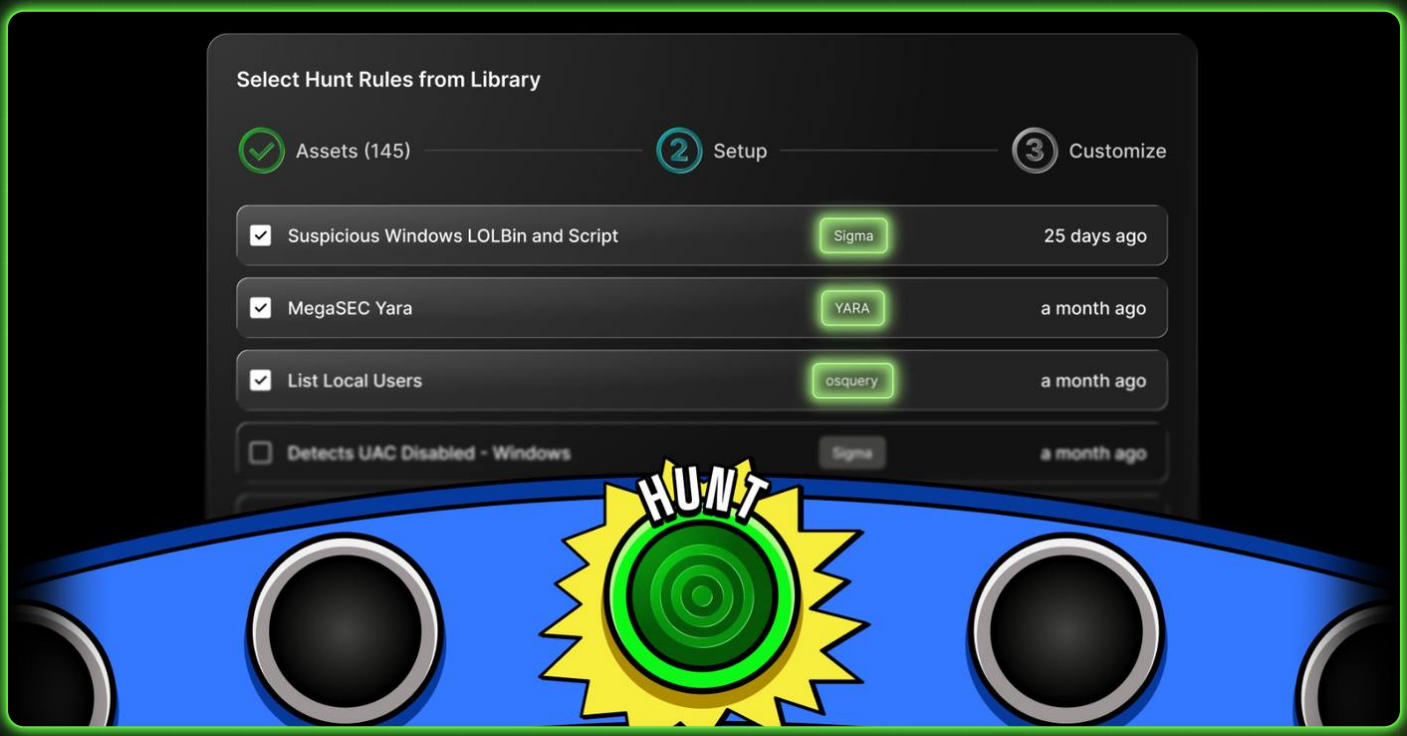
Execute hunts on-demand, on a schedule, or automatically through integrated workflows. Support continuous validation, threat exposure assessments, compromise checks, and investigation readiness activities without requiring manual execution.

BUILT FOR INVESTIGATOR CONTROL

Create, modify, and execute queries in real time using an integrated editor designed for investigative workflows. Rapidly refine searches, test hypotheses, and re-run hunts without interrupting active investigations.

TEMPLATES, LIBRARIES & GOVERNANCE

Standardize investigations through reusable templates, centrally managed rule libraries, and version-controlled content. Develop custom investigative workflows, share logic across teams, and maintain consistency through Git-based synchronization.

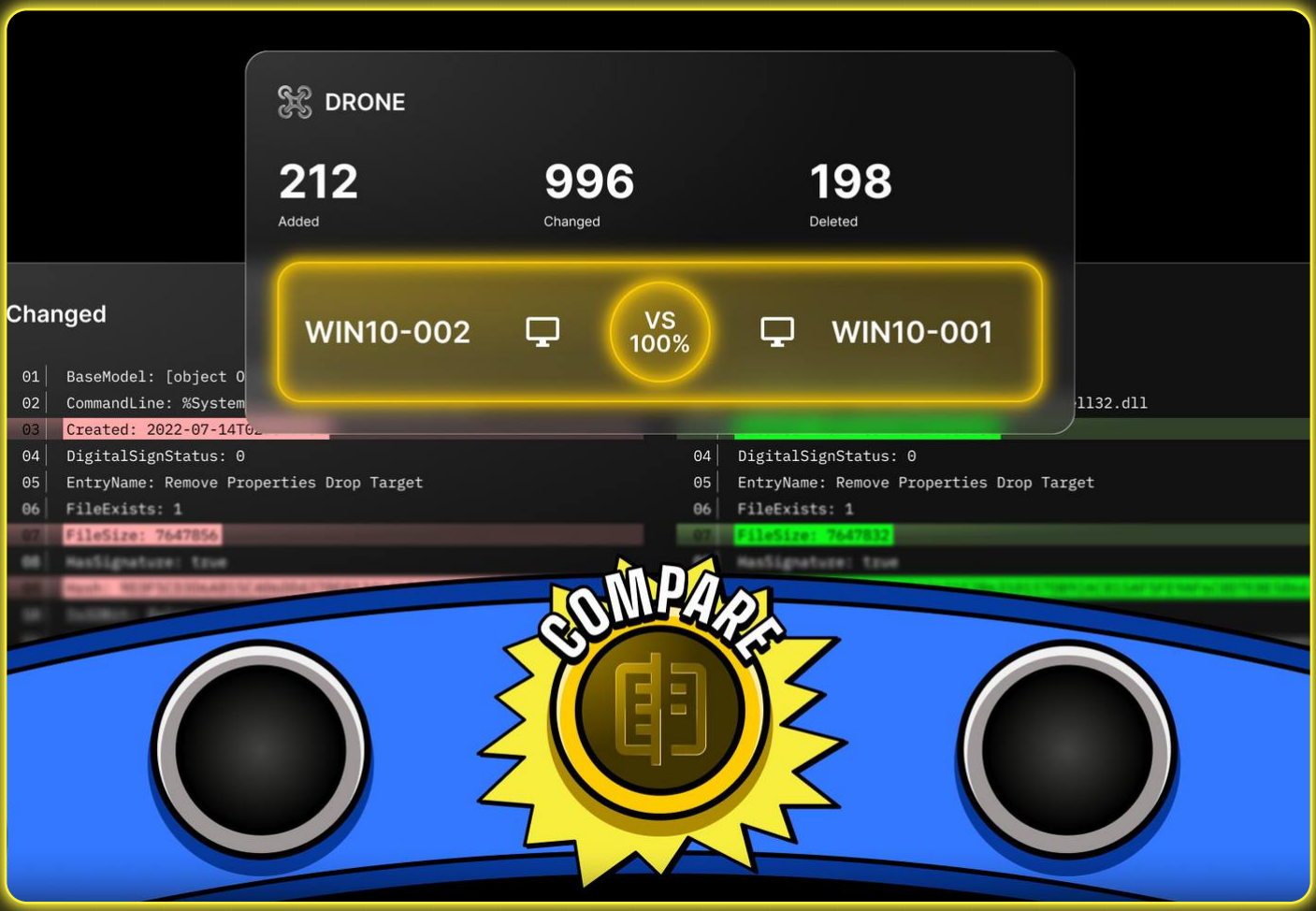


COMPARE

IDENTIFY WHAT CHANGED WITH COMPARE

Compare helps investigators identify meaningful changes across assets by highlighting additions, modifications, and deletions between forensic snapshots.

- **Proactive Baseline Analysis:** Establish trusted baselines and identify suspicious changes, unauthorized modifications, and indicators of compromise across forensic artifacts commonly abused by attackers.
- **Accelerate Investigations:** Quickly identify what changed between acquisitions without requiring access to the original asset.
- **Support Reactive & Proactive Workflows:** Use Compare during active incident response to validate findings and determine impact, or as part of ongoing investigation and assessment activities to identify unexpected change across the environment.



TAKE ACTION ACROSS YOUR ENVIRONMENT WITH INTERACT

interACT enables analysts to directly interact with assets from within AIR, supporting investigations, threat hunting, validation activities, and response workflows without requiring additional tools or remote access solutions.

Gather additional context, execute investigative tasks, validate findings, and take action within a single investigation platform.

- **Cross-platform Consistency:** Use a unified command set across Windows, Linux, and macOS, simplifying investigations and reducing the need for platform-specific expertise.
- **Multi-Asset execution:** Interact with up to 50 assets simultaneously, broadcasting commands and executing actions at scale.
- **Script and command libraries:** Use centrally managed scripts, assets, and command snippets to standardize and accelerate investigations.
- **Auditable Operations:** Operate within role-based permissions, with commands, responses, and file transfers fully logged and hashed for accountability.
- **Flexible command execution:** Extend investigations using native commands and osquery to perform targeted inspection and validation on live systems.

INVESTIGATION HUB

WORK EVERY INVESTIGATION FROM A SINGLE, UNIFIED CASE VIEW

AIR's Investigation Hub brings evidence, findings, assets, and investigation activity together within a single case-centric workspace. Investigators can review findings, validate evidence, seamlessly pivot into deeper investigations, and maintain a complete record of investigative activity without switching tools or workflows.

By bringing investigation data together within a single case, teams can collaborate more effectively, prioritize work, manage investigations, and drive cases to conclusion with confidence.

FILTERING AND GLOBAL SEARCH

Quickly locate relevant evidence, findings, and assets across complex investigations to focus on the information that matters most.

MITRE ATT&CK CONTEXT

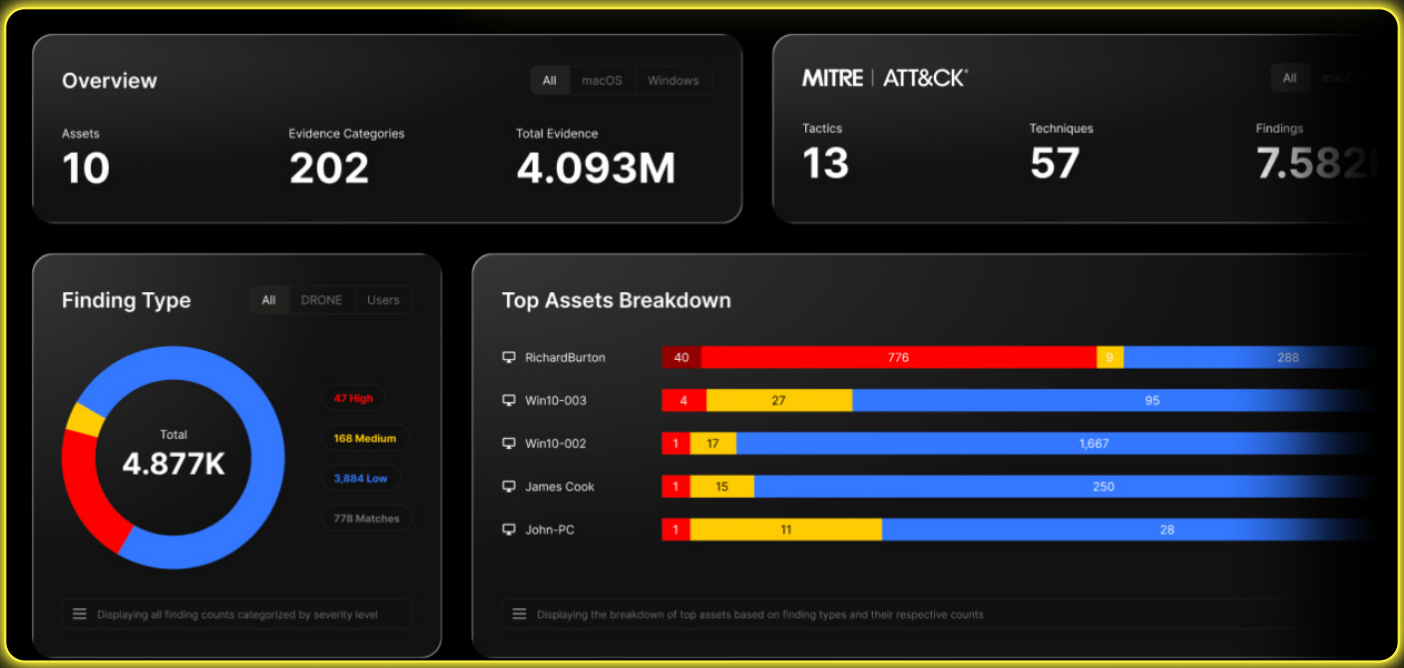
Visualize mapped ATT&CK techniques to better understand adversary behaviour, investigation scope, and potential next steps.

COLLABORATIVE FEATURES

Capture notes, comments, bookmarks, and investigation activity within a shared workspace to support collaboration and maintain investigation continuity.

INTEGRATED REPORT GENERATION

Generate investigation reports directly from cases using customizable templates tailored to different stakeholders and reporting requirements.



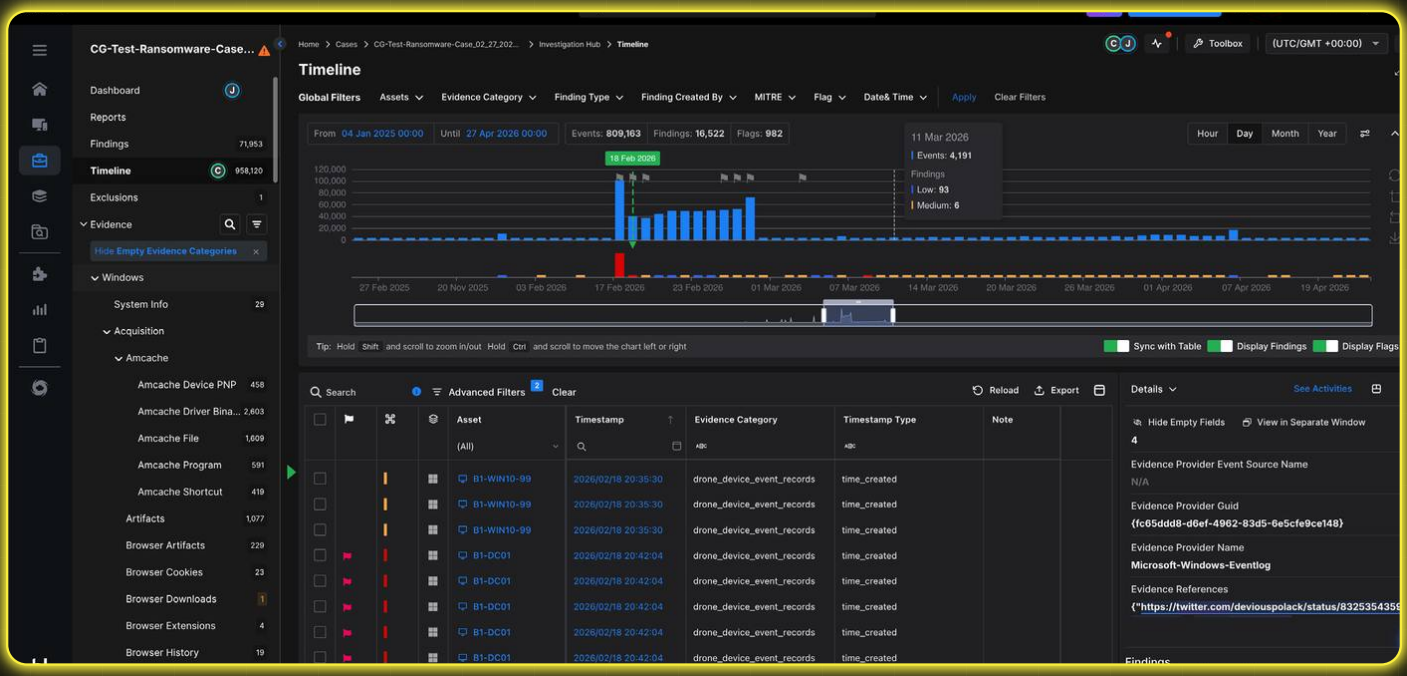
CASE MANAGEMENT & PRIORITIZATION

Assign ownership, track tasks, manage priorities, and organize investigations using tags, categories, and visual workflows. Maintain visibility across active cases while supporting consistent investigation progression and team coordination.

RECONSTRUCT EVENTS WITH INTEGRATED TIMELINES

Integrated within Investigation Hub, Timeline provides a chronological view of investigation activity, helping analysts understand context and event relationships.

- **Automated Event Correlation:** Automatically build timelines from timestamped evidence across the investigation.
- **Advanced Filtering & Exploration:** Filter, search, and pivot through events to identify patterns and relationships.
- **Collaborative Investigation:** Flag, annotate, and enrich events with additional context.



INTEGRATIONS & AUTOMATION

AIR integrates with existing security tools and workflows, providing the forensic evidence and investigation context needed to transform alerts, signals, and findings into understanding and action.

COMPLETE THE SECURITY STACK

Integrate with SIEM, XDR, EDR, SOAR, ticketing, CTI, and collaboration platforms to launch investigations and response workflows from existing tools.

FROM SIGNAL TO INVESTIGATION

Automatically trigger evidence collection and investigation workflows from alerts, detections, API calls, and event-driven integrations.

OPEN & EXTENSIBLE

Leverage AIR's REST API, webhooks, and event subscriptions to embed investigation into existing security architectures and custom workflows.

BUILT FOR OPERATIONAL SCALE & CONTROL

AIR is designed to support enterprise and multi-tenanted security operations, enabling teams to investigate, collaborate, and govern investigations consistently across distributed environments.

- **Enterprise Governance —** Role-based access controls, auditing, and policy-driven workflows help ensure investigations remain secure, accountable, and aligned with organizational requirements.
- **Operational Scale —** Support large and distributed environments through centralized management, automation, and multi-asset investigation workflows.
- **Multi-Team Collaboration —** Enable security operations teams to collaborate within a shared platform while maintaining appropriate separation and visibility.
- **Investigation Coordination —** Manage investigation ownership, tasks, priorities, and workflows directly within AIR using integrated case management capabilities.

PROFESSIONAL SERVICES

EXPERT SERVICES FOR INVESTIGATION READINESS

AIR is designed to help teams investigate with confidence every day, not just during major incidents. Our Support and Professional Services help you deploy faster, operationalize proactive investigations, and continually strengthen your investigation capability.

Whether you're building investigation readiness across your environment or responding to your most critical incidents, Binalyze's expert cyber investigators, security architects and engineers work alongside your team to help you get the most from AIR.

Explore our services:

- **Essentials Support:** Guided onboarding, expert support, and best-practice guidance included with every AIR subscription.
- **Signature Support:** Enterprise-grade 24×7 support, dedicated Customer Success, proactive health checks, and strategic guidance.
- **Professional Services:** Advanced implementation, investigator training, DFIR assistance, and expert consulting for complex environments and investigations.

Explore Binalyze Support & Services

WHY BINALYZE

DETECTION CREATES SIGNALS.
INVESTIGATION CREATES UNDERSTANDING.

Binalyze AIR is the Investigation Platform that completes the SOC, working alongside SIEM, XDR, SOAR, and threat intelligence tools to provide the forensic evidence and investigation context needed to understand what happened, validate findings, and determine the right course of action.

Making investigation an everyday capability of the SOC, AIR helps security teams move from signals to understanding, and from understanding to confident action.

ARRANGE A DEMONSTRATION OR SIGN UP FOR A FREE TRIAL TODAY AT WWW.BINALYZE.AI

binalyze!