binalyze!

AIR

Automated Investigation and Response platform

Powered by forensic-level visibility

Boost cyber resilience with proactive and rapid investigation and response

The exponential growth in the volume and velocity of attack vectors, along with an expanding attack surface and data volume, presents an unprecedented challenge for defenders. Whether you're an enterprise with your own SOC or an MSSP defending your customers, the challenge remains the same: 100% breach prevention is no longer a realistic expectation.

100% breach prevention is no longer a realistic expectation.

As a result, there is a growing trend—and an urgent need—toward adopting a proactive, "assume breach" mindset that emphasizes strengthening investigation capabilities and ensuring rapid response. By placing accessible, scalable, and rapid forensics at the core of the security stack, organizations can make faster, more effective decisions that boost cyber resilience and ensure they are equipped to respond swiftly and confidently when a breach occurs.

Binalyze is an innovator in Investigation and Response Automation.

Contents

Lightning Fast Evidence Acquisition

Built on our proprietary engine, collecting digital forensic evidence from any asset on your network takes just a few clicks with AIR, and is completed in minutes.

Acquisitions in minutes

Evidence acquisition is typically completed in under 10 minutes, instead of hours or days using traditional tools.

Compression & encryption

Acquired evidence can be compressed to save storage resources and encrypted to AES-256, a standard approved by the National Institute of Standards and Technology (NIST) for secure data encryption.

Forensically sound

Evidence collected by AIR is forensically hashed and then time-stamped via RFC3161, ensuring immutable records for a robust chain of custody and forensic integrity.

Remote & scalable

Once deployed across your network, asset tasks and actions can be run concurrently and at scale.

Evidence repositories

Evidence can be stored on the local machine, an attached removable drive, a network location, an SFTP/FTPS server, SMB share or Cloud repository on Amazon or Azure.

Offline collector

Use our configurable offline collectors to to acquire evidence and perform triage. Allowing you to easily import results and context back into AIR to continue your investigation.

Over hundreds of different evidence types, parsed, processed, presented and organized in a single Investigation and Response Automation platform. AIR provides forensic depth and comprehensive incident response enabling capabilities.

Custom evidence types

In addition to hundreds of evidence types collected, custom content profiles (path/pattern based) can be defined for specific evidence requirements.

Custom acquisition profiles

AIR provides granular control of evidence acquisition through the creation of unlimited acquisition profiles.

MITRE | ATT&CK®

AIR's MITRE ATT&CK Analyzer scans live assets for evidence to immediately add valuable real-time visibility to potential threats.

Evidence types including

- System Evidence
- Disk Evidence
- Memory Evidence
- Browser Evidence
- NTFS Evidence
- Registry Evidence
- Network Evidence
- Event Logs Evidence
- WMI Evidence
- Process Execution Evidence
- Miscellaneous Evidence

Artifact types including

- Server Artifacts
- Microsoft App Artifacts
- Communications
- Artifacts
- Social Artifacts
- Productivity Artifacts
- Utility Artifacts
- Developer Tools Artifacts
- Cloud Artifacts

Network Capture

- Network Flow
- PCAP

Full disc imaging

- DD file image format
- Save to FTPS services
- Supports Ex01

Comprehensive coverage comes as standard with AIR

AIR's cross-platform capabilities cover the most prevalent operating systems, including Windows, macOS, and Linux - ensuring no stone is left unturned during your investigations.

AIR flawlessly integrates with major cloud platforms like AWS and Azure allowing for a swift and efficient response to cyber threats and incidents.

*Q3 2024

Best–in–class investigation capabilities across all your cloud assets and applications to unlock cloud native digital forensics and incident response.

Enumerate cloud assets

A simple, one–time cloud account configuration allows you to add your AWS and Azure accounts, enumerate virtual assets and start investigating.

Cloud log analysis*

Collect and forensically analyze cloud log data for a complete picture of your cloud environments.

SaaS applications forensics*

Extend cloud visibility into your SaaS applications including Microsoft 365 and Google Workspace for application level forensics such as business email compromise.

Low access overhead

Engineered to minimize the administrative and access rights overhead to make deployment and compliance quicker and easier.

One platform for all your assets

Comprehensive investigation capabilities, built on top of best-in-class on premise and off network forensic collection solutions, allows you to consolidate your onto a single platform for your entire estate to simplify incident response and investigation processes and save money.

*Q2 2025

Speed up Investigations with Auto Asset Tagging

Understand network topology and categorize assets in minutes with virtual responders quickly and easily deployed across your network.

Automated & on-demand
Auto Asset Tagging can be triggered automatically on AIR Responder deployment and used for ad-hoc categorization at any time afterwards.

Profile network assets
Default tag profiles for standard networks, such as domain controllers, web servers, and mail servers are included as standard.

Power of osquery
Leverage the powerful combination of osquery and Auto Asset Tagging for deeper asset searching and categorization that is lightning fast.

Shorter time to investigation
Remove unnecessary delays at the beginning of your investigations by finding the most likely targeted assets in minutes.

Bespoke tagging
Customize Auto Asset Tags using any combination of process, file, directory, host, and IP variables for powerful granularity of results.

Automated Decision Support

Find the relevant events in your digital forensic evidence faster and with fewer resources using DRONE, AIR's automated compromise assessment capability.

Automated Compromise Assessment

DRONE passes forensic evidence through a number of relevant analyzers to find the anomalies for you and flag events of interest.

Live YARA & Sigma scanners

DRONE has embedded YARA scanning capabilities and, uniquely, Sigma and osquery scanning capabilities on the live asset.

Decision Support

Proprietary algorithms label findings (high, medium, low, matched) to guide your decision making processes and significantly speed up the investigation.

MITRE ATT&CK Analyzer

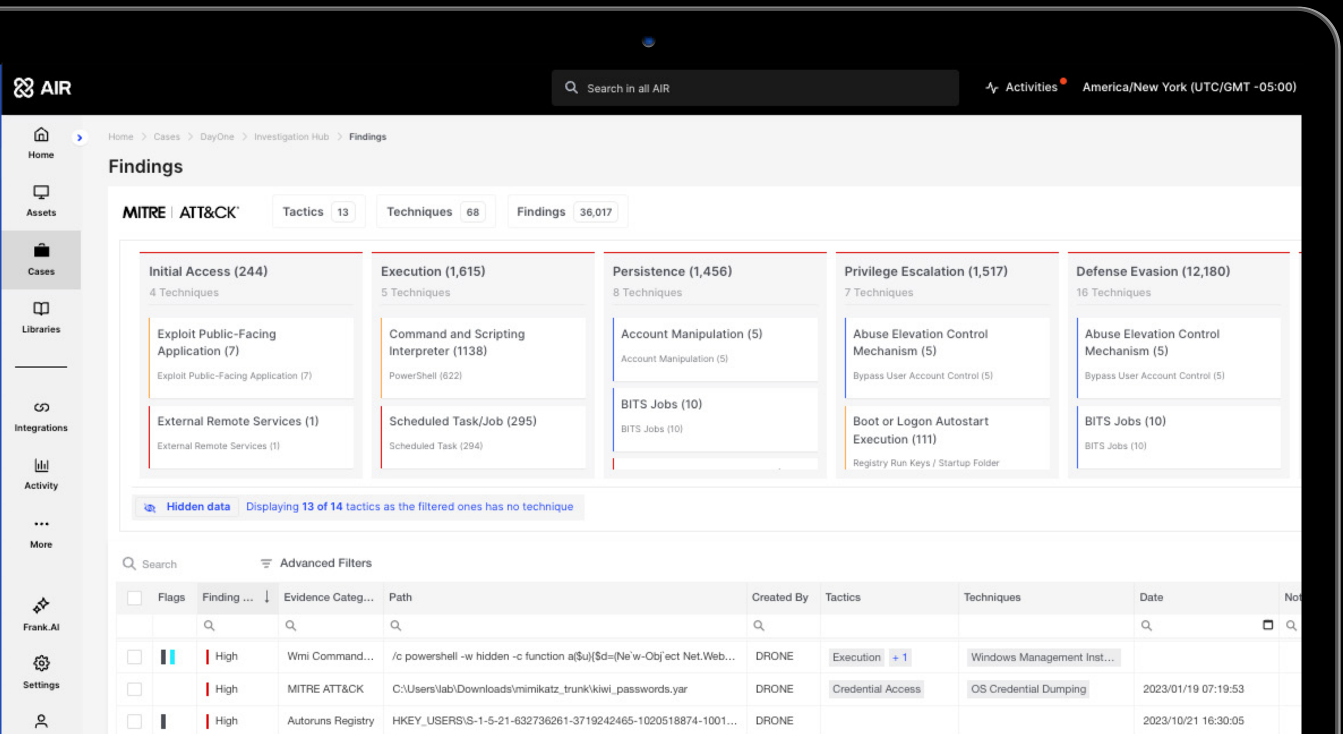
Map results to the MITRE ATT&CK framework and display results for all the evidence related to a case.

Rapid keyword searching

DRONE's flexible keyword searching capabilities provide powerful compromise assessments in just a few minutes. Search for domains, IP addresses, file names, hashes and much more.

DFIR Lab supported

DRONE's capabilities are continuously updated and improved by our dedicated DFIR Lab team of cybersecurity experts, threat hunters, and malware analysts.



Home > Cases > DayOne > Investigation Hub > Findings

Findings

MITRE | ATT&CK

Tactics 13 | Techniques 68 | Findings 36,017

Initial Access (244)
4 Techniques
- Exploit Public-Facing Application (7)
  Exploit Public-Facing Application (7)
- External Remote Services (1)
  External Remote Services (1)

Execution (1,615)
5 Techniques
- Command and Scripting Interpreter (1138)
  PowerShell (622)
- Scheduled Task/Job (295)
  Scheduled Task (294)

Persistence (1,456)
8 Techniques
- Account Manipulation (5)
  Account Manipulation (5)
- BITS Jobs (10)
  BITS Jobs (10)

Privilege Escalation (1,517)
7 Techniques
- Abuse Elevation Control Mechanism (5)
  Bypass User Account Control (5)
- Boot or Logon Autostart Execution (111)
  Registry Run Keys / Startup Folder

Defense Evasion (12,180)
16 Techniques
- Abuse Elevation Control Mechanism (5)
  Bypass User Account Control (5)
- BITS Jobs (10)
  BITS Jobs (10)

Hidden data Displaying 13 of 14 tactics as the filtered ones has no technique

Search | Advanced Filters

□	Flags	Finding ...	Evidence Categ...	Path	Created By	Tactics	Techniques	Date	Not
□		High	Wmi Command...	/c powershell -w hidden -c function a($u){$d=(Ne`w-Obj`ect Net.Web...	DRONE	Execution +1	Windows Management Inst...		
□		High	MITRE ATT&CK	C:\Users\lab\Downloads\mimikatz_trunk\kiwi_passwords.yar	DRONE	Credential Access	OS Credential Dumping	2023/01/19 07:19:53	
□		High	Autoruns Registry	HKEY_USERS\S-1-5-21-632736261-3719242465-1020518874-1001...	DRONE			2023/10/21 16:30:05	

Automated Cyber Investigations

With our flexible integration features you can automate your Investigation capabilities in minutes to deliver genuine enterprise–grade functionality.

SIEM, SOAR & EDR integrations

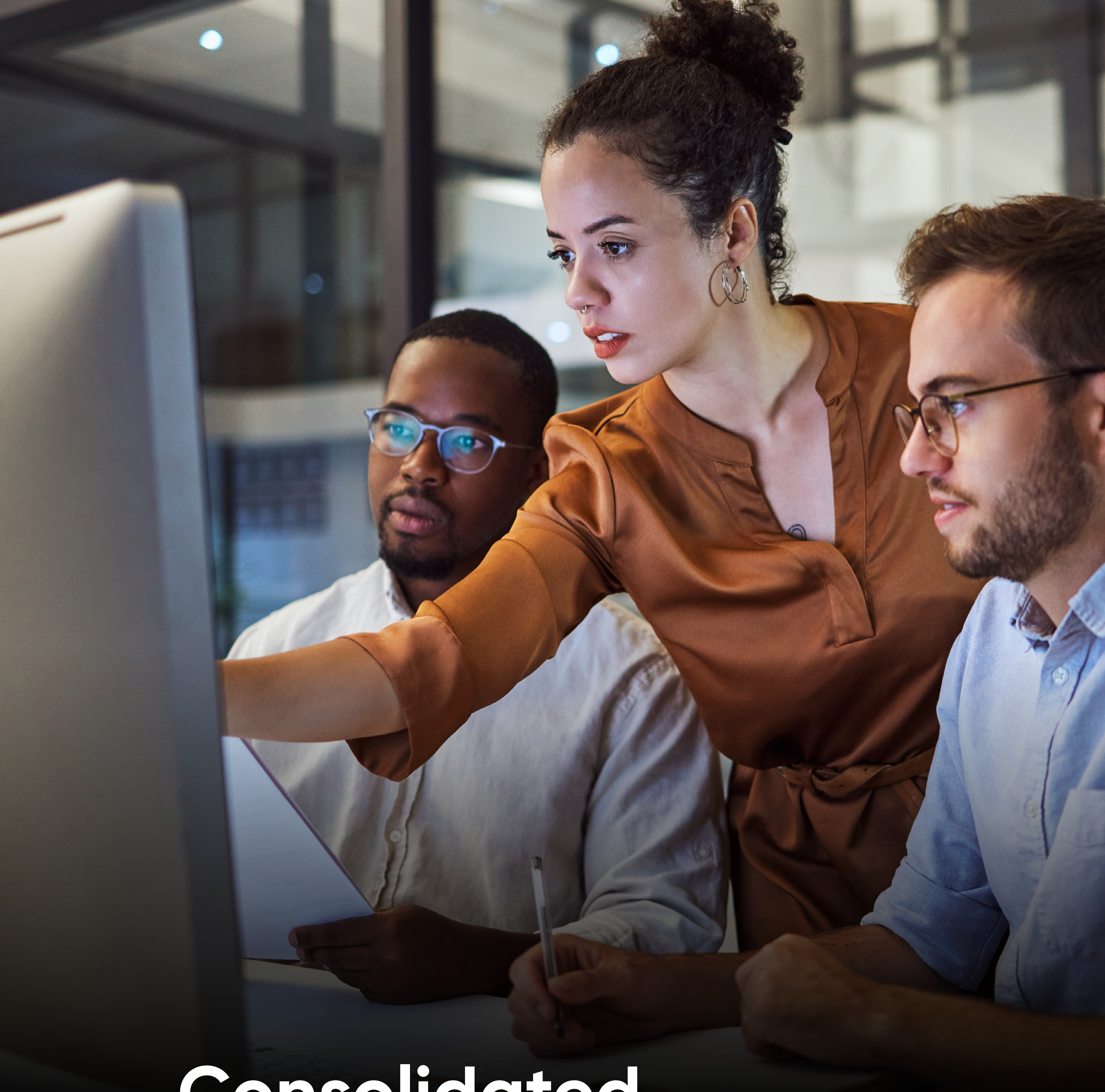
AIR supports a broad set of SIEM, SOAR, and EDR integrations out-of-the-box.

24/7 task triggering

Respond instantly to alerts and incidents from other security systems, regardless of the time of day or analysts availability, to automatically preserve forensic evidence and fast–track your investigations.

Webhooks integration

Simple and fast integration with any service that is compatible with webhooks.



Consolidated, Integrated Insights

Binalyze AIR's Investigation Hub removes the time consuming need to pivot between screens, manual tasks, and tools to enable more efficient, streamlined and collaborative investigations.

Complete Case Overview

Consolidate all evidence and findings related to a case in a unified view to quickly pivot to your investigation in one centralized place.

Intelligence-Led Prioritization

The Investigation Hub includes severity-labelled findings from AIR's automatic analyzers and triage features to help focus on the most critical information to your investigation first.

Integrated Report Generation

Use a simple wizard to populate relevant investigation information efficiently and clearly, with pre-built, customizable sections tailored to specific stakeholders and audiences.

Filtering and Global Search

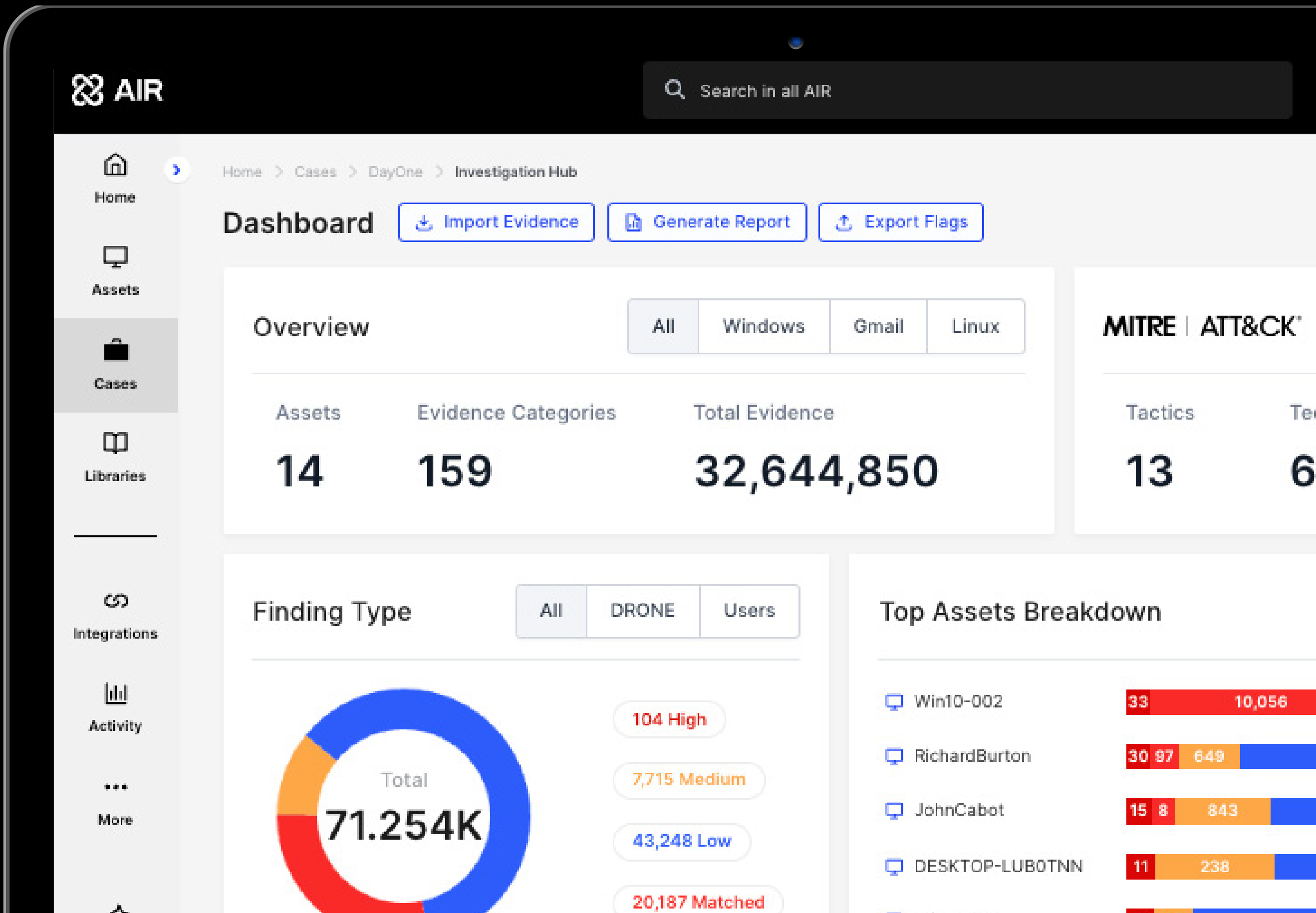
Reduce time spent trying to find and stitch insights together across hundreds of assets, and zero-in on details most relevant to your case without friction.

MITRE | ATT&CK®

With MITRE ATT&CK mapping, quickly visualize and understand what threats you are dealing with to stay ahead of next steps in an attack and pinpoint gaps in monitoring and detection capabilities.

Collaborative features

Add notes, comment, bookmark and flag evidence and findings that matter most to the investigation and point team mates to useful information in a single, shared view and activity bar.



AIR

Search in all AIR

Home > Cases > DayOne > Investigation Hub

Dashboard

Import Evidence | Generate Report | Export Flags

Overview — All | Windows | Gmail | Linux

Assets	Evidence Categories	Total Evidence
14	159	32,644,850

MITRE | ATT&CK®

Tactics	Te
13	6

Finding Type — All | DRONE | Users

Total 71.254K

104 High

7,715 Medium

43,248 Low

20,187 Matched

Top Assets Breakdown

Win10-002	33		10,056
RichardBurton	30	97	649
JohnCabot	15	8	843
DESKTOP-LUBOTNN	11		238

Remote Triage at Scale

Move seamlessly from forensic evidence acquisition findings to rapid triage across your network directly from within the AIR management console.

Search with YARA or Sigma

Create or import YARA and Sigma rules within the AIR platform and share them between analysts. Triage tasks can be sent to an endpoint in seconds to scan both memory and file system.

Fast, concurrent scanning

From the AIR management console triage can be performed remotely and at scale across multiple assets concurrently.

Leverage osquery

Utilize AIR's scalability and speed to deliver osquery triage searches to any of your assets remotely.

*Q3 2024

Collaborative 1–click Timelines

Create comprehensive event timelines with a single click and in just a few minutes. Expand the scope of your timeline as the investigation proceeds to reach the correct conclusions quicker.

Automated timelining

With a single click, AIR creates a comprehensive timeline of a single or multiple assets in minutes.

Real–time collaboration

Collaborate remotely and in real–time with other analysts directly on the AIR platform to build the investigation narrative.

Import CSV data

Use AIR's 4–step, format agnostic CSV importer to enrich your timeline with mapped data from Cloud systems, firewall logs and much more.

Event flagging

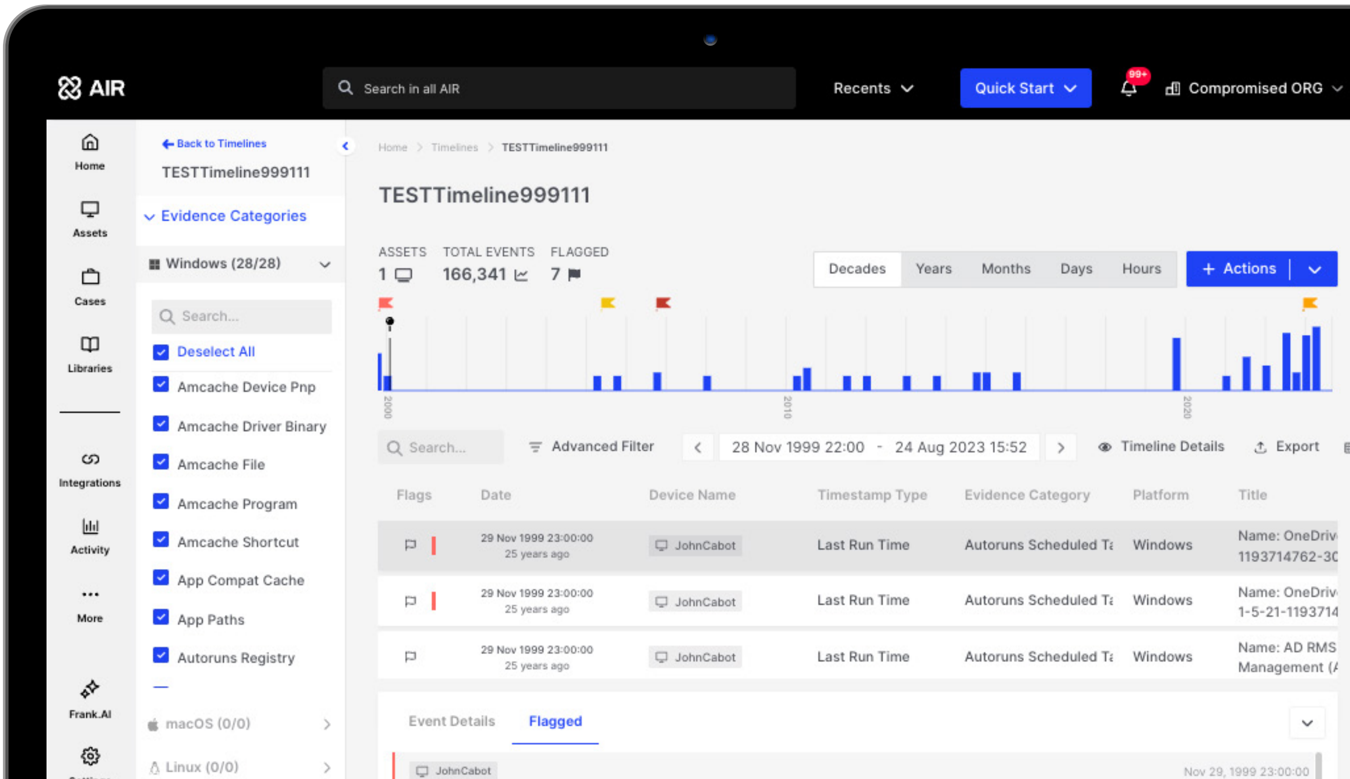
Flag events of interest with a severity level and collect flagged events for streamlined management reporting.

Enrich with milestones

Add anecdotal evidence obtained during the investigation process i.e. HR intelligence, timings of real world events etc.

Add additional endpoints

Easily add additional assets to your timelines as your investigation progresses and lateral movement is identified.



TESTTimeline999111

Evidence Categories

Windows (28/28)

☑ Deselect All
☑ Amcache Device Pnp
☑ Amcache Driver Binary
☑ Amcache File
☑ Amcache Program
☑ Amcache Shortcut
☑ App Compat Cache
☑ App Paths
☑ Autoruns Registry

macOS (0/0)

Linux (0/0)

TESTTimeline999111

ASSETS 1 TOTAL EVENTS 166,341 FLAGGED 7

28 Nov 1999 22:00 - 24 Aug 2023 15:52

Flags	Date	Device Name	Timestamp Type	Evidence Category	Platform	Title
	29 Nov 1999 23:00:00 25 years ago	JohnCabot	Last Run Time	Autoruns Scheduled Ta	Windows	Name: OneDriv 1193714762-30
	29 Nov 1999 23:00:00 25 years ago	JohnCabot	Last Run Time	Autoruns Scheduled Ta	Windows	Name: OneDriv 1-5-21-1193714
	29 Nov 1999 23:00:00 25 years ago	JohnCabot	Last Run Time	Autoruns Scheduled Ta	Windows	Name: AD RMS Management (A

JohnCabot Nov 29, 1999 23:00:00

interACT Remote Shell

Investigate, contain and remediate in a permission–based and fully audited remote shell environment that standardizes and simplifies incident response.

Cross platform

interACT standardizes and simplifies the use of remote shells with a cross–platform command set for Windows, Linux and macOS.

Script and asset library

Encourage investigative consistency across your team by managing approved scripts and assets in the interACT library.

Easily bring those assets into a shell session with a single click.

osquery compatible

Use osquery to extend interACT's native command set for deeper investigation flexibility.

Permission–based

Utilize the benefits of a remote shell while maintaining appropriate access levels for individual analysts with AIR's multiple permission levels for enumeration, read content and write/execute.

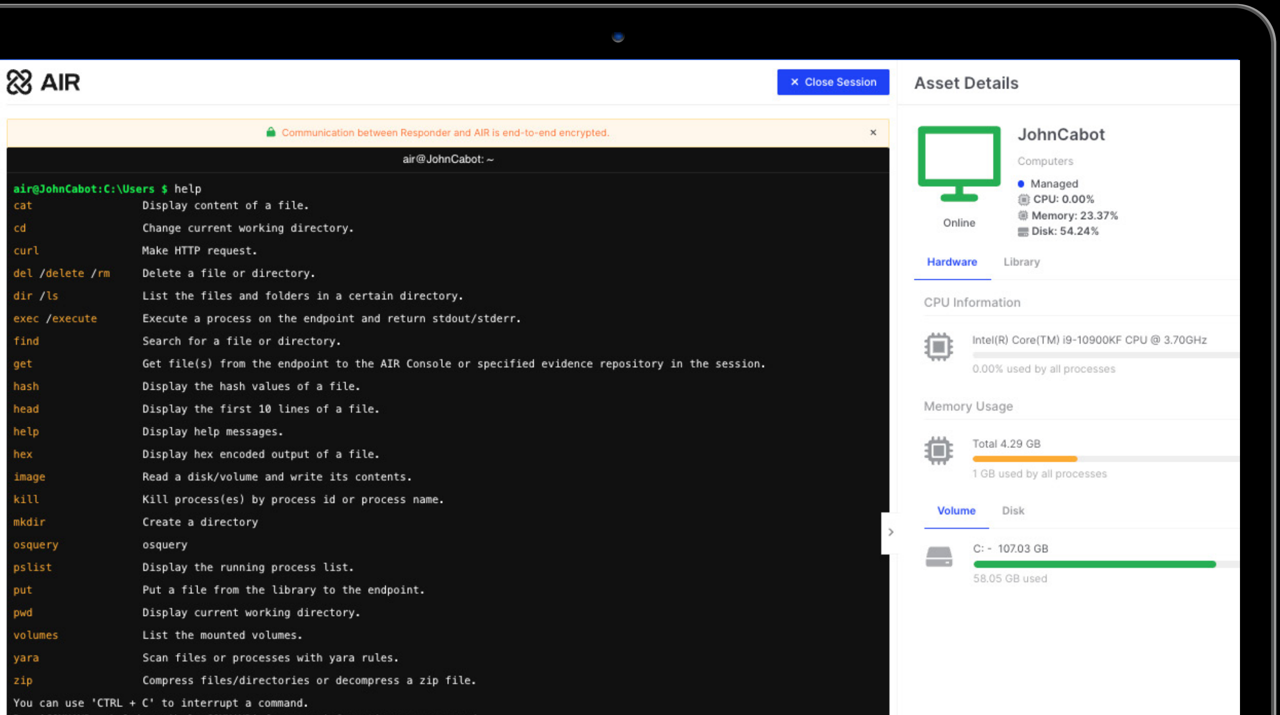
Full log & audit trail

Every command and response is logged in real–time to an interACT session report and sent to the platform–wide audit log.

Any files transferred between the asset and analyst are also logged and hashed for complete accountability.

Full disc imaging

Collect a full disk image of any device as part of a deeper investigation. Disk images are captured in the DD and Ex01 formats and can then be investigated in AIR's File Explorer.



Communication between Responder and AIR is end-to-end encrypted.

air@JohnCabot: ~

```
air@JohnCabot:C:\Users $ help
cat                 Display content of a file.
cd                  Change current working directory.
curl                Make HTTP request.
del /delete /rm     Delete a file or directory.
dir /ls             List the files and folders in a certain directory.
exec /execute       Execute a process on the endpoint and return stdout/stderr.
find                Search for a file or directory.
get                 Get file(s) from the endpoint to the AIR Console or specified evidence repository in the session.
hash                Display the hash values of a file.
head                Display the first 10 lines of a file.
help                Display help messages.
hex                 Display hex encoded output of a file.
image               Read a disk/volume and write its contents.
kill                Kill process(es) by process id or process name.
mkdir               Create a directory
osquery             osquery
pslist              Display the running process list.
put                 Put a file from the library to the endpoint.
pwd                 Display current working directory.
volumes             List the mounted volumes.
yara                Scan files or processes with yara rules.
zip                 Compress files/directories or decompress a zip file.
You can use 'CTRL + C' to interrupt a command.
```

JohnCabot

Computers

- Managed
- CPU: 0.00%
- Memory: 23.37%
- Disk: 54.24%

CPU Information

Intel(R) Core(TM) i9-10900KF CPU @ 3.70GHz

0.00% used by all processes

Memory Usage

Total 4.29 GB

1 GB used by all processes

C: - 107.03 GB

58.05 GB used

Forensic Differential Analysis

Compare is our patent–pending forensic diffing comparison feature that unlocks ultra–focused proactive investigation for more efficient, effective and threat hunting.

Quick comparisons

Compare the current forensic state of an asset with a previous point in time to identify additions, deletions and changes.

Automatic baseline acquisitions

Automatically capture baseline acquisitions (golden images) as part of the responder deployment process.

Scheduled forensic snapshots

Schedule proactive forensic snapshots on your assets on a daily, weekly or monthly cadence.

Revolutionize Investigations

Binalyze's disruptive mindset and constant innovation of AIR has enabled us to elevate investigations and unlock the power of digital forensics for incident response. Full forensic visibility, at speed, across your estate facilitates new and valuable use cases for incident response.

Identify breach persistence

Compare identifies signs of breach and breach persistence at the forensic level allowing containment to happen earlier.

Streamline Validation

Streamline alert validation and accelerates incident response, with effective forensic-visibility, enhancing SOC team efficiency and ensuring critical alerts receive timely attention.

Find 'Unknown unknowns'

Assume you will be breached. Only modern forensic data can provide the visibility for effective resilience post breach.

Enterprise–grade Cyber Resilience Platform

AIR delivers an enterprise grade solution to facilitate its management in line with your corporate policies and security requirements.

Global policies

AIR has a system of cascading policy definitions. Global policies are created as defaults to define acquisition profiles, evidence repositories, CPU usage, and more.

SSO & 2FA

Access to the AIR management console can be securely controlled using Single Sign On (SSO) and Two Factor Authentication (2FA).

Console access can also be IP restricted for additional security.

User, roles & permissions

AIR includes a highly granular roles and users definition system, with more than 105 different variables, to tightly control access permissions throughout your security team.

Custom policies

Policies at the organization, group or individual endpoint can be created where it is necessary to override the global policy.

Organizations & case management

AIR’s native Organizations feature allows for platform multi–tenancy, additional business structure definition and access management.

The Case feature provides an additional layer of investigation management and control.

Active directory

Integration with Active Directory automatically creates and maintains your organizational structure within AIR.

On premise, Offline & SaaS

AIR can be delivered on premise (inc. offline), and private cloud.

Auto backups

Configuration of backup locations and scheduling of auto–backups can all be configured in the AIR management console.

Asset isolation

AIR's asset isolation feature allows you to remotely isolate a machine from the network, in seconds, while still performing actions from the AIR management console (acquisition, triage, timeline etc).

Virtual, lightweight Responders

AIR's Responder is an extremely lightweight self contained 40mb application that replicates the skillset of a L3-L4 analyst to all your assets.

Auditing & Syslog integration

Extensive, tamper–proof audit logs are kept by the AIR platform locally and can also be integrated with your Syslog servers.

Professional Services

Our professional services complement your investment in the cyber resilience delivered by AIR to maximize your return on investment.

Assisted deployment

Our solution sales engineers can join your project team after procurement, using their experience and in–depth product knowledge to guide and inform the deployment and configuration phase.

Advanced SLA support

If you require advanced levels of support that meet a specific service level agreement, that are outside of our standard support, we can provide enhanced support services.

Accredited training

We provide a number of training programs via our Future Forensics Academy to develop the investigation capability of your security analysts on the AIR platform.

Leverage the lightning fast and comprehensive forensic visibility of AIR to power your applications and security products.

API Licensing

AIR's open API and flexible licensing unlocks world–class investigation capabilities for deeper integrations with your existing tools and security systems.

Application ecosystem

Full forensic visibility across the enterprise network facilitates exciting new opportunities for "layer 2" use cases and applications built on top of AIR's core.

Integration partners

Our expanding vendor partnerships allow automation of secondary forensic actions and the ingestion of forensic data for better customer ROI.

Binalyze is the developer of AIR, an innovative investigation and response automation platform blending forensic-level visibility with intelligent automation and efficiency driving automation.

Binalyze AIR empowers incident response and SOC teams with proactive, rapid, accurate, and collaborative insights, resulting in faster investigations and stronger security outcomes. With features like remote evidence acquisition, automation-driven, intelligence-led analysis, and an intuitive, collaborative interface, AIR drastically reduces investigation times and simplifies the entire investigation workflow.

Arrange a demonstration or sign up for a free trial today at www.binalyze.com

Binalyze OÜ
Narva mnt 5, 10117 Tallinn
Estonia

info@binalyze.com
www.binalyze.com

binalyze!