Empowering Responders with Automated Investigation

SPONSORED BY binalyze!

A SANS First Look

Written by **Megan Roddie-Fonseca** | February 2025

Introduction

Digital forensics is a powerful tool when it comes to investigating security incidents. Historically, security analysts have off-loaded the acquisition and analysis of forensic data to specialized experts. Because of this, the ability for organizations to leverage forensic analysis has largely depended on their ability to have investigators with those skills on staff.

In this SANS First Look, we examine Binalyze's Automated Investigation and Response (AIR) platform to see how it is reducing the overhead of forensic investigations and providing all analysts with the ability to harness the power of forensics data even without specialized training.

From data acquisition to threat hunting to SOAR workflows, AIR provides a way for organizations to automate investigation and incident response to allow analysts to quickly and efficiently handle incidents.

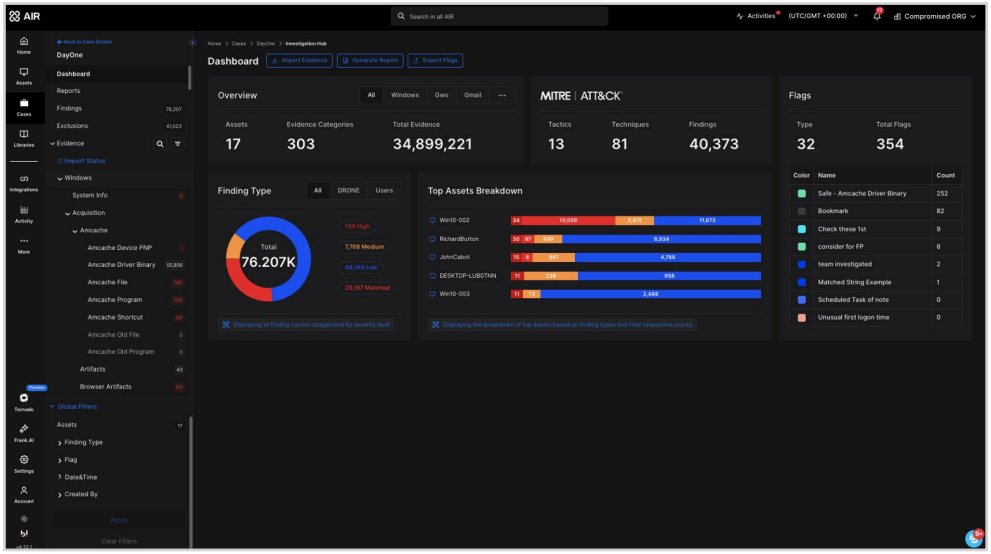

Figure 1. Investigation Hub Dashboard

The First Look

Diving into a mountain of evidence, artifacts, and findings can be a daunting task, but with the AIR Investigation Hub (see Figure 1), interpreting and navigating through that data is simplified. The Investigation Hub provides a consolidated digital forensics and incident response (DFIR) intelligence report directly within your cases. From this view, analysts are provided with a single pane-of-glass view that allows for searching, filtering, bookmarking, and investigating all case-relevant findings efficiently. It encourages collaborative investigations by allowing for comments/notes and providing an activity feed.

As a result of AIR's ability to automate the analysis of forensic artifacts, the Investigation Hub provides users with an overview of the "Finding Types." These findings are based on an automated compromise assessment module and built-in analyzers, called DRONE, which significantly reduce investigation time by providing analysts with prioritized signposting and actionable insights. Instead of spending valuable time identifying what is different, noteworthy, or unexpected in a case, analysts are automatically presented with findings that matter most to their investigation. High-severity findings flag threats that are high-fidelity risks and should be reviewed and addressed immediately, while medium- and low-severity findings bring additional artifacts of interest to the forefront that analysts can use as a starting point for investigation. "Matched" findings show results based on defined keywords, hashes, or patterns that signal recognized indicators. See Figure 2.

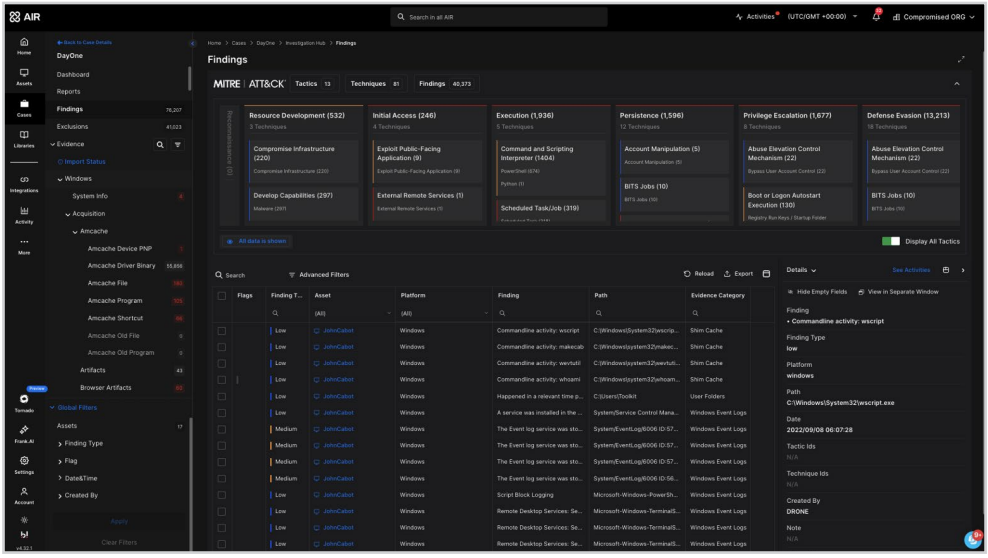

Figure 2. Findings Page in Investigation Hub

The Assets widgets in the Investigation Hub dashboard provide a breakdown on the top assets worth investigating based on the number and types of findings from each host. The Flags widget allows users to see how items have been categorized so far in the investigation, providing a quick reference during the investigation. From this dashboard, users can filter and navigate through evidence and findings with ease.

Data Acquisition

With the Binalyze AIR Responder installed, collecting forensic evidence is as simple as the click of a button (see Figure 3). Prebuilt acquisition profiles allow you to get started quickly with either a fast scan that gathers essential evidence, a full scan for all data, or a compromise assessment focused on indicators of compromise and suspicious activity (as defined by the Binalyze threat hunt team, DFIR Lab). By leveraging out-of-the-box acquisition profiles or creating custom ones, organizations can streamline acquisition to focus on specific artifacts of interest. Extensive evidence and artifacts are available to collect from Windows, Linux, macOS, and IBM AIX. With a constantly growing list that currently includes over 600 artifact types, it is beyond what can be shared in this First Look, but some examples include memory dumps, running processes, shell history, system and application logs, and browser history and cookies.

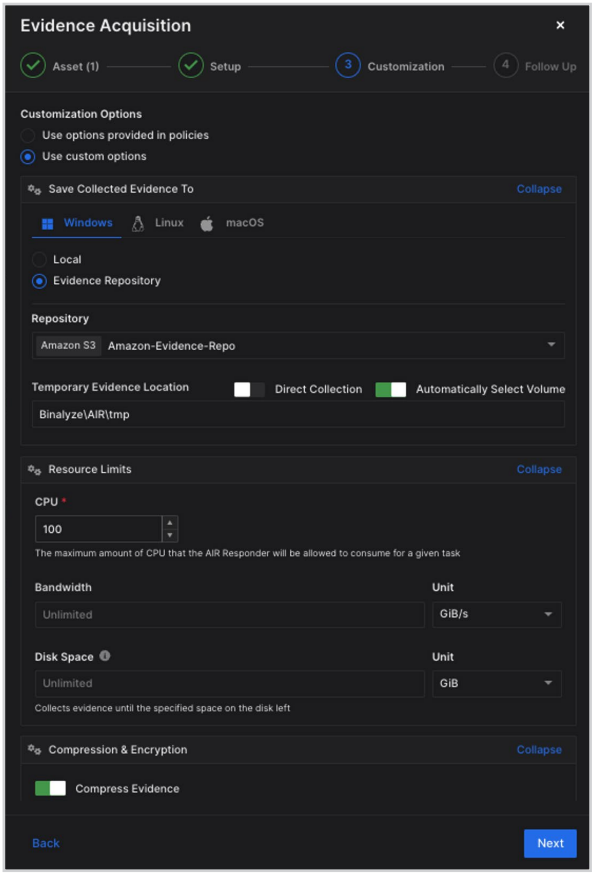

Figure 3. Evidence Acquisition

Another powerful feature that Responder provides is the ability to take a full disk image. Forensic imaging used to be a time-consuming task requiring physical access to the device, but with Responder, all it takes is the click of a button from the AIR platform. And if you're concerned about chain of custody, hashing and RFC 3161 timestamping of all collected files is built in, and all activity by users is logged for a thorough audit trail.

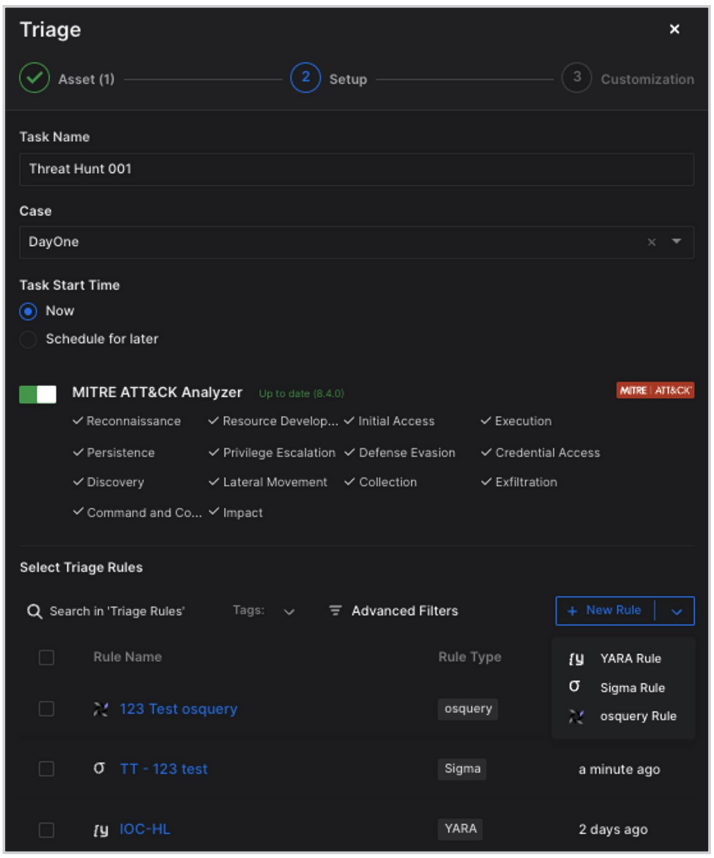

Figure 4. Triage Using YARA, Osquery, and Sigma

Triage and Precision Hunting

Whether you are triaging evidence or searching for suspicious activity, sometimes a more targeted approach is required. AIR provides analysts with the ability to perform precision threat hunting to focus on indicators of compromise (IoCs). In addition to AIR's built-in DRONE analyzers mentioned above, Binalyze AIR's Triage and precision hunting features enable investigators to hunt using YARA, Sigma, or Osquery (see Figure 4). With YARA, analysts can search for malicious binaries present on systems. Sigma provides an easy-to-write rule format that allows users to search for activity across various log sources. Osquery enables users to perform SQL-like queries against system data. With a built-in editor and library, organizations can develop, validate, and manage rules to be used to triage evidence or perform hunts on demand or on a schedule.

Integrations and API

Having all the extra forensic context available is a huge step in the right direction of automating incident response investigations, but Binalyze allows you to take it an extra step with a large library of integrations as well as a robust API (see Figure 5). With integrations for SIEMs, SOARs, and E/XDRs, building an automated analysis and response pipeline becomes a much simpler task. Whether you have Splunk, SentinelOne, or Slack as part of your security stack, Binalyze's integrations provide an easy-to-set-up connection that allows organizations to leverage the platform and its data for their own use cases. Even without a prebuilt integration, both the API and webhooks are available to build custom integrations that align with your needs.

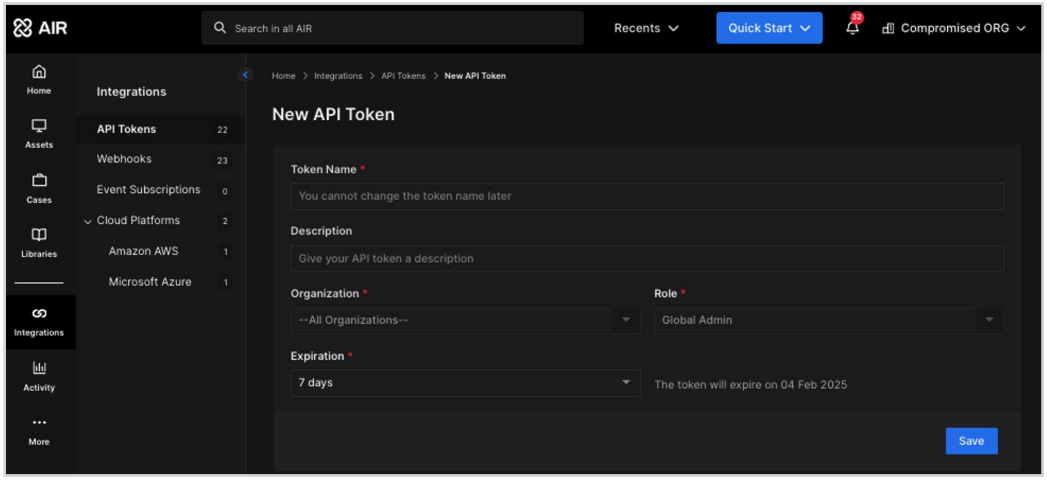

Figure 5. API Token Creation

Takeaways

Organizations leveraging Binalyze's AIR platform are equipping their security analysts with a tool set that provides extensive data, allowing for faster, more precise, and simpler response to security incidents. The platform's feature set provides organizations with:

- Simplified artifact acquisition and full disk imaging via Responder
- Automated analysis highlighting artifacts of interest via DRONE
- A consolidated, single-pane view of case data via Investigation Hub
- Threat hunting and evidence triage using YARA, Sigma, and Osquery rules
- SOAR capabilities via built-in integrations and an API interface

When an incident happens, Binalyze AIR ensures that all the data required to stop the threat as soon as possible is available, conclusive, and actionable, whether your responders are seasoned forensic investigators or recently hired security analysts.

Sponsor

SANS would like to thank this paper's sponsor:

binalyze!