SANS | Research Program

Dropzone AI Can Make Internal SOC Teams More Effective

SPONSORED BY

Dropzone AI

A SANS First Look

Written by **Mark W. Jeanmougin** | June 2025

Introduction

Today's organizations are fighting global adversaries that are constantly launching attacks, increasingly using AI for greater scale and effectiveness. Executives demand around-the-clock incident detection capabilities, challenging SOC teams to become increasingly efficient at performing Tier 1 alert triage. A managed security service provider (MSSP) can ease the burden on resource-limited teams—but it's not always the best option for an organization. Although working with an MSSP can bring significant benefits, it also comes with potential hurdles, including:

- Limited visibility into the internal environment
- Rigid MSSP processes or playbooks
- Communication gaps

These issues can lead to detection gaps that are exploited by adversaries, all at a higher cost than relying on the current SOC team.

Organizations that prefer not to outsource this critical function need a strategy that both is cost effective and eases the burden on their internal SOC teams. In this SANS First Look, we examine Dropzone AI, an AI system that can watch your alerts, perform Tier 1 triage at a constant rate, and escalate to personnel with full investigation reports including findings and evidence.

A Look at Dropzone AI

Dropzone AI connects to endpoint, cloud, network, identity, email, and other sources that produce security alerts. It also produces metrics showing when the detection event fired, when it hit the investigation queue, and the time the AI system took to investigate the alert. Most Dropzone AI investigations are completed in less than 10 minutes.

Each investigation from Dropzone AI includes a summary of malicious, suspicious, or benign activity. The findings include detailed evidence and a one-line summary, allowing analysts to "check the work" of the AI, even learning from the queries it makes to various systems (see Figures 1 and 2).

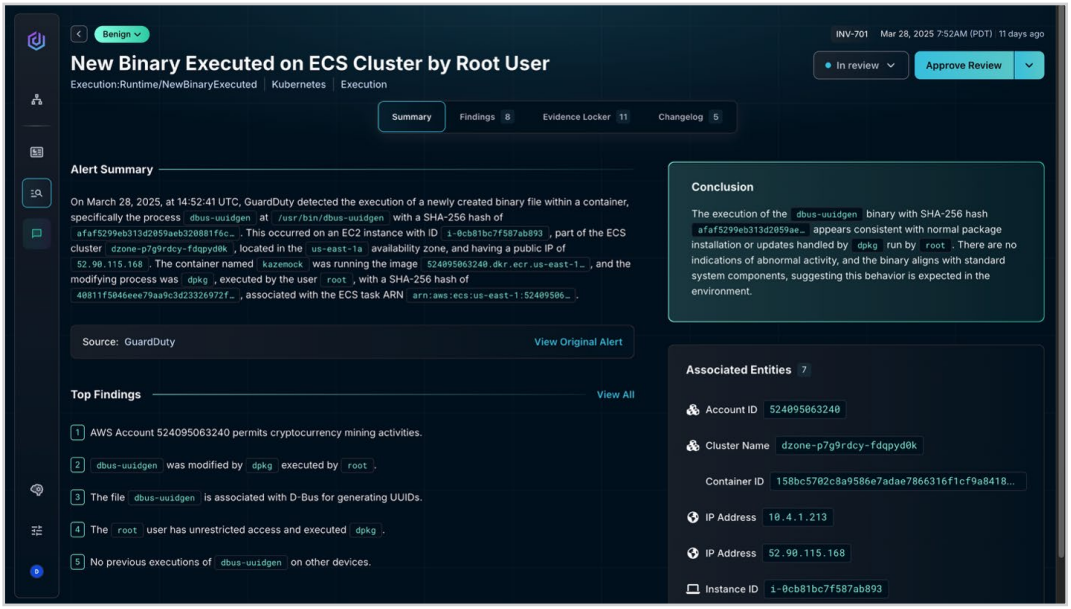

Figure 1. Dropzone AI Investigation Summary

Dropzone AI doesn't replace your existing incident management system. Instead, it will send investigation findings to Jira, ServiceNow, PagerDuty, and Twilio.

A key Dropzone AI feature is context memory that learns details from investigations and uses them to improve the accuracy of future investigations. Users also can add details to context memory, such as the function of specific servers, which VPN services are approved, or a range of IPs used by your test environment.

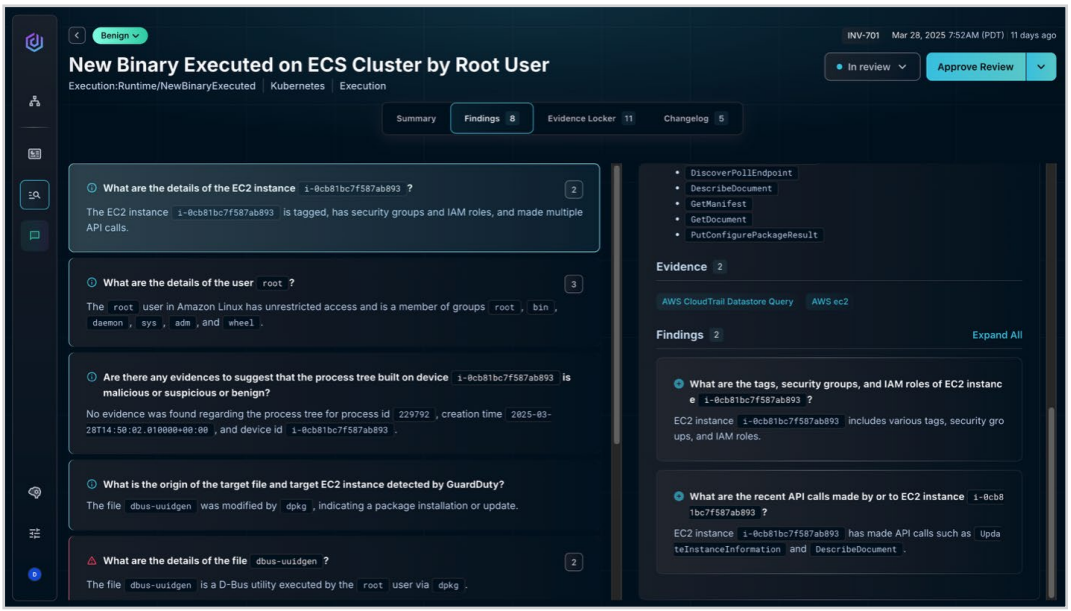

Figure 2. Dropzone AI Investigation Findings

Another interesting feature is the AI interviewer, which can run user interviews in Slack or Microsoft Teams to gather details needed for the investigation, such as checking whether they added permissions for another user or if users are working from a new location.

In-House 24/7 Incident Detection

Dropzone AI learns about what's normal (and abnormal) for your environment. It isn't simply triaging alerts based on some predefined playbook. You get real escalations for real incidents from AI that uses tools and follows an investigative methodology.

Dropzone AI can receive alerts from the tools you've already deployed and configured in your security stack. Everything from your network firewalls, OS and endpoint controls, and cloud sources, up to application-level visibility. Of course, it also integrates with the market's leading SIEMs.

With Dropzone AI, data stays where it currently is. There's no need to move gigabytes or terabytes of data across the network into another tool for analysis. This aligns with the philosophy that Dropzone AI is acting like one of your SOC analysts. You don't send all your logs to each of your analysts, so why would you send them to Dropzone AI?

Resource-constrained organizations that want to run a SOC internally will find Dropzone AI particularly useful. Auditors and customers will like knowing that their data is protected 24/7, and your SOC team is getting notified at all hours of the day when adversaries are taking steps to go after the data they have been entrusted with.

Augmenting Your Human Analysts with AI

Dropzone AI isn't going to replace your existing staff. It is going to make each analyst more effective, like a teammate who can take over the routine triage and investigation work—and do it well.

Dropzone AI helps each analyst focus on the work that's most important and the most rewarding, such as preventive security projects or threat hunting. Rather than being stuck dealing with false positives and repetitive tasks, teams are instead augmented with AI. SOC teams always start with full investigative reports, complete with findings and evidence, so they can dismiss false positives and spend time examining more serious incidents. This can mean improvements to your enterprise detection blueprint and other engaging work that leads to employee retention.

Looking under the hood, each Dropzone AI investigation gives you a readable summary plus the top few details (called "findings") on how it came to that conclusion. The modern SOC has so many different log sources that each analyst ends up with an individual specialty, which can make it difficult to understand what every event means. Dropzone AI will interact with your existing security tools, pulling relevant log events, and running queries to gather additional contextual data. Dropzone AI can derive useful information from those events, then explain them with a "human-readable" description.

Dropzone AI pulls in data from sources you might not think of at first. It also leaves in data that runs counter to the conclusion, which is a benefit because incident detection sometimes means dealing with contradictory data. As analysts work with that data, they can support or contradict Dropzone AI's conclusions. They'll also learn more about the data sources in the environment and what can be helpful in working incidents.

If an alert requires follow-up with a user, the Dropzone AI Interviewer tool reaches out via Slack. It can interpret the result to understand if the user was authorized to carry out the event. Then, all that information is added to the ticket and closed out.

Analysts also can use Dropzone AI's chatbot function to investigate incidents further. The chatbot generates queries to tools as appropriate, saving analysts time and empowering staff members who are not expert in a particular tool.

The preferred Dropzone AI implementation rollout starts by putting the "trust but verify" responsibility in the hands of your current analysts. As you get more comfortable with Dropzone AI, you can set up more automated response actions based on investigation conclusions. This feature allows you to make use of your existing automation and to easily integrate with your current tools and workflows. Dropzone AI requires less setup time than SOAR automation because it requires only read-only user accounts to your systems and does not use playbooks or require coding. It uses AI reasoning to help teams work each alert faster, providing a suggested conclusion and the data to understand why it came to that conclusion.

Faster Onboarding of New Hires

Attracting, hiring, and retaining SOC analysts and engineers is a challenge. Once you get them in the door, you want to quickly ramp up without being a draw on your existing staff. Dropzone AI enables new analysts to not just learn some basics of incident detection, but also to get up to speed on how to make the most of your existing tools. They can learn on their own before seeking insight from more experienced analysts.

Junior analysts get a personal, patient coach to teach them. Dropzone AI's investigation reports show the appropriate level of detail to include in their reports. Reading the alert investigation reports shows which data sources to include and how to interpret the data, providing a valuable source of training for junior analysts. In addition, junior analysts can ask questions about investigations using the chatbot function.

A junior analyst is likely to come up with a theory of what an adversary is doing. Then, they search for events across all the sensors, looking for data to support their hypothesis. However, if they never search for data that contradicts their hypothesis, then they'll never discover a better hypothesis. What makes Dropzone AI special is that it will show events that don't *exactly* support the conclusion. This helps a new analyst understand that their first idea isn't always the best one.

Dropzone AI pulls information from your organization's existing security controls. This means that your analysts are learning about how you've deployed and configured your various security tools rather than seeing idealized configurations in a training class. The downside is that you're learning that some of your deployments could be a whole lot better. The upside is that the Dropzone AI users have time to implement those fixes because they're free from repetitive work due to poorly configured alerts.

Dropzone has given back to the community, releasing COACH,[1] a free Chrome web browser extension to guide junior analysts through security investigations.

Final Thoughts

Wouldn't it be great if you had a tool that understood logs from Linux servers, Windows laptops, Kubernetes managed containers, Google Cloud Platform, identity and AWS, access management (IAM) providers, and more? You would normally need to find multiple analysts to get that kind of breadth over such a wide range of sources. But, to really understand an adversary's activity, you need to be able to track them utilizing all those services. You need one source of information that understands each of those tools, to correlate adversary activity. Ideally, it should also have dark mode. Dropzone AI can do this and more.

Dropzone AI serves as a force multiplier. It builds on your existing security tools and staff to make them better. It can make your team more efficient, freeing up time to better configure those tools, implement defensive controls, or tend to other tasks. Dropzone AI enables cost-effective, 24/7 alert coverage for lean SOC teams while obviating the need for outsourcing Tier 1 triage. It augments human analysts by delivering transparent, detailed investigations that save time while allowing full trust and verification. Dropzone AI's comprehensive reports also serve as a training tool, helping junior SOC analysts learn investigation best practices and strengthening an organization's talent pipeline. Reach out at **https://dropzone.ai** to learn more.

[1] "Meet COACH," www.dropzone.ai/coach