Dropzone AI

How Zapier Cut Manual Alert Investigation by 85% With Dropzone AI

_zapier

Company Profile

Zapier is the leader in easy automation, helping businesses automate workflows and move data across nearly 8,000 apps. The company's no-code automation platform is used by over 3.4 million businesses, from startups to Fortune 100 companies.

Behind the scenes, a lean detection and response team monitored security alerts to quickly identify and stop threats. Every day, the team faced unpredictable alert volumes. Each alert investigation demanded pivots across multiple systems, draining time and pushing critical projects like detection engineering, observability, and vulnerability management further behind.

> If you're not automating away manual triage, you're not entering a modern SOC world. You're stuck back in pre-LLM days, and that's not where security is heading.
>
> **Michael Kuchera**
> Manager, Security Detection and Response

Challenges

With no option to grow headcount, Zapier's detection and response team set out to solve challenges that stretched far beyond their size:

Too Few Hands for Too Much Risk	A company of Zapier's scale was defended by a team you could count on one hand. Some days brought more alerts than could reasonably be investigated by the analyst on shift, potentially slowing response as each analyst could only perform one investigation at a time.
Alerts That Ate Entire Sprints	Triage wasn't just a daily distraction; it consumed entire sprints. The standing Jira ticket for "Alert triage" swallowed story points that should have gone into building detections or hardening systems. Projects that would mature the security program slipped, sprint after sprint. Michael Kuchera, Detection & Response Manager, recalls: "Spending time doing triage as a small team really impacts what else you can do. It meant that other programs fell behind."
Noise That Trains You to Miss the Signal	When the same noisy alerts appeared day after day, analysts fought against human nature. Making assumptions or taking shortcuts meant that a real threat might get lost in the noise. What the team needed was consistency, every alert investigated thoroughly, every time.

See what Zapier gained by deploying Dropzone AI, in their own words:

> For me, the aha moment was when I was using the Ask a Question feature and saw how Dropzone pulled data from Okta, AWS, Google Workspace, and Panther to answer a question.

Alana Kim, Sr. Security Incident Response Engineer

> When you have a smaller team that's growing and maturing, Dropzone is an awesome tool to shore up blind spots.

Kat Nestor, Security Engineer

Selection & Implementation

Zapier's security team had seen plenty of tools that promised automation, but most didn't deliver what they needed—a solution that could autonomously carry complex investigations to completion.

Kuchera explains why the team found Dropzone AI appealing: "Dropzone AI stood out because it worked like an analyst, not a rules engine. Unlike other automation tools, it isn't a black box; analysts can see every query it runs and every piece of evidence it gathers, which builds trust in the results."

Prior to deploying Dropzone, Alana Kim, Sr. Security Incident Response Engineer at Zapier, had built a service to enrich alerts but it required a lot of ongoing effort to maintain. Dropzone AI met all the requirements of that project and more.

"For me, the aha moment was when I was using the Ask a Question feature and saw how Dropzone pulled data from Okta, AWS, Google Workspace, and Panther to answer a question," says Kim. "I didn't have to go system by system; I could just ask, and Dropzone pulled it all together."

The deployment was completed in two days. Dropzone integrates with Zapier's core systems and pushes enriched investigations directly into Panther. They connected to their corporate Slack so that Dropzone can conduct AI interviews of users, when necessary.

The Zapier team appreciates Dropzone AI's ability to learn details about the environment and business. "We add details to context memory and the Dropzone AI system will take those into account during investigations," says Kim. "For example, we can flag users who are traveling and Dropzone will raise the severity of related alerts."

Key Performance Indicators (KPIs) and Results:

- **85% faster investigations**, with alert triage time reduced from 10-15 minutes to under 2 minutes
- **1-2 analyst hours saved** daily in alert investigations
- **Expanded alert investigative capacity** without hiring or outsourcing
- **Reduced risk** through more thorough and consistent alert investigations

A Lean Security Team, Finally in Control

Zapier's detection and response team is much more efficient and effective with Dropzone AI handling alert triage and investigation. The time savings have been apparent.

"The difference that Dropzone has made in terms of time reclaimed is obvious in our monthly reports and caught the attention of our executives," says Kuchera.

> Now every investigation comes with the context I need. I can finish reviewing in minutes and spend my time improving detections instead of chasing noise.

Alana Kim
Sr. Security Incident Response Engineer

Benefits Realized with Dropzone AI

From 100 Investigations a Day to a Handful That Matter	Zapier's security team once faced 50–100+ alert investigations daily, most of them turning out to be false positives. Dropzone collapsed that noise into only the handful that truly needed attention.
Minutes Instead of Afternoons	What used to take 10-15 minutes on average now takes under two minutes. Investigations arrive fully enriched and ready to act on. "Now, if an alert comes in without a Dropzone comment, then I'm reminded of all the work we used to have to do ourselves. It saves so much time," says Kim.
No More Guesswork	Dropzone conducts thorough investigations—taking steps beyond what a human would typically complete. "In one case, we had a data exfiltration alert and Dropzone went through 200 files contained in a folder to see if there might be sensitive data," says Kuchera. "The thoroughness that Dropzone adds gives us a lot of confidence that things aren't slipping through the cracks."
Engineers Building, Not Chasing Alerts	With alert triage off their plate, Zapier's engineers spend time engineering detections, expanding observability, and projects that improve the maturity of the security program.
Even Compliance Runs Smoother	The Governance, Risk, and Compliance (GRC) team self-serves through Dropzone's Ask a Question feature. Audit evidence, provisioning checks, and user investigations no longer interrupt security; they're answered instantly, without pulling analysts away from higher-value work.
Scale Security Without Adding Headcount	Dropzone acts like a 24/7 SOC analyst team, delivering consistent investigations directly into workflows, allowing Zapier to scale without hiring or outsourcing.

Reinforcements have arrived

Dropzone AI's agents make SOCs fast, scalable, accurate, and proactive. With Dropzone AI autonomously handling routine Tier 1 alert triage, organizations can spend less time on reactive security and more time on proactive security. The Dropzone AI SOC Analyst replicates the techniques of elite analysts and is trusted by more than 100 enterprises and MSSPs, including CBTS, Pipe, UiPath, Zapier. Learn more at www.dropzone.ai.

Request a Demo

Dropzone AI