Dropzone AI

How Mysten Labs Eliminated Toil and Scaled Security With Dropzone AI

MystenLabs

Company Profile

Mysten Labs is a web3 infrastructure company with a lean, highly senior team; every engineer is staff-level or higher, averaging 15+ years of experience. This small group is responsible for building web3 infrastructure that is secure, reliable and ready for mass adoption.

Paul Padilla, Head of Software and Infrastructure Security, approaches the challenge like an engineer: security operations shouldn't mimic a 40-year-old SOC model, but instead mimic the discipline of site-reliability engineering (SRE) so that only the right people are involved in fixing the problem.

That philosophy led Mysten Labs to Dropzone AI.

> I want security operations to look like site-reliability engineering: low toil, high automation, and engineers focused on building, not swatting flies.
>
> **Paul Padilla**
> Head of Software and Infrastructure Security

Challenges

Mysten Labs operates with a very low risk tolerance and a SOCless model. Instead of security analysts, security alerts flow directly to IT and application engineers that intimately know the systems they operate. They set out to solve the following challenges:

Protect Against Advanced Adversaries	The web3 ecosystem that Mysten Labs operates in is targeted by nation-states that use sophisticated techniques. Mysten's security operations team needs to be able to respond extremely fast to even subtle threats.
Protecting Engineers' Time	Every engineer is staff-level or higher, with 15 or more years of experience. Their time is better spent building, rather than triaging alerts that turn out to be false positives.
High Alert Volume, Low Signal	Mysten's security tooling generates thousands of alerts per month, overwhelming engineers with noise and obscuring a handful of genuine issues.
Need for Observability Without Toil	Mysten's security team builds detections the same way site-reliability engineers (SREs) build observability. Without Dropzone, those detections created noise that stole valuable time from engineers.

Selection & Implementation

Head of Software and Infrastructure Security Paul Padilla wanted a way to protect his senior engineers' time while still maintaining a very low risk tolerance. He saw SOAR as insufficient to the challenge, and started to investigate how AI could automate alert triage. Dropzone AI stood out.

"What struck me about Dropzone was that it is actually replicating the techniques of security analysts," says Padilla.

Deploying Dropzone AI was simple and finished in a day. Mysten sends all types of security alerts to Dropzone: endpoint, identity, cloud, email, and network alerts.

"It was a lot of fun to watch it start using tools and completing alert investigations," recalls Padilla.

Once connected to their SIEM and business systems, the team customized their Dropzone implementation. "We use custom strategies in the Dropzone to tune the system, basically providing guidance to the system about what's irrelevant and what's important," says Padilla.

Today, Dropzone investigation results are pushed back into Mysten's SIEM and on-call engineers are paged for serious events. The result is a SOCless, low-toil security operations model where important alerts are surfaced and resolved efficiently.

99% Reduction in Triage Workload

Mysten Labs reduced thousands of monthly alerts needing human review to fewer than 20 per month. Instead of being overwhelmed by false positives, engineers now spend their time on only the handful of events that matter.

>90% Faster Investigations

Before Dropzone, engineers could spend 30–60 minutes investigating a single alert. With Dropzone, that time has dropped to roughly a minute now that engineers have thorough context for each event.

"Without context, a lot of alerts look scary," says Padilla. "Dropzone gathers and analyzes content so you can see that the IP in an alert actually does have endpoint protection enabled, for example."

Trust Under Constant Attack

Mysten faces persistent campaigns from state-sponsored adversaries, including DPRK operators using subtle "Living off the Land" techniques. Dropzone surfaces true threats with speed and context, improving Mysten's security posture.

Fine-Tuning the Fire Hose

Mysten's team customized Dropzone to understand its policies and escalate only investigations that humans needed to review.

Scalable, Low-Toil Security Model

Dropzone enables Mysten to efficiently operate a SOCless model where alerts flow directly to highly senior engineers who can quickly identify anomalous behavior. This model scales better than a traditional SOC and delivers better results.

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

> We went from a fire hose where it feels like you're reading the matrix to receiving only a few things a week, and each of those things matters.
>
> With Dropzone, I have the context I need to make my investigation a one-minute exercise, not a 30-minute one.

Paul Padilla
Head of Software and Infrastructure Security

Key Performance Indicators (KPIs) and Results:

99% reduction in alert volume, with thousands of monthly alerts reduced to fewer than 20.	**>90% faster** investigations from 30–60 minutes to roughly one minute.	Deployment in **under a day**, fully integrated with SIEM and core services.	Engineers are only engaged on critical alerts, a **SOCless model that protects valuable engineering time.**	**More time for proactive security**, reclaimed hours for threat modeling, detection engineering, and observability improvements.

Scaling Security Operations by Eliminating Toil

For Mysten Labs, scaling security is an engineering challenge. "We need to re-think security operations. What's needed to thrive in the future? I think scalability is the biggest problem, but you can never hire enough skilled people. You must eliminate toil, and Dropzone is the best solution I've seen that helps you do that," says Padilla.

> You can't hire your way out of alert overload. The only way to scale is to eliminate toil, and Dropzone makes that possible.

Paul Padilla
Head of Software and Infrastructure Security

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