Dropzone AI

How Shield53 Cut Alert Triage and Used That Time to Prevent the Next Breach

Shield53

Company Profile

Shield53 is a Canadian cybersecurity services firm that provides SOC-as-a-service, incident response, virtual CISO, and infrastructure security support to clients across various industries, including healthcare, finance, education, and manufacturing.

Chris Stewart founded Shield53 after leading a 130-client managed security service provider (MSSP) and responding to over 300 ransomware incidents. His key insight: most breaches weren't inevitable, they were the result of missed signals and burned-out analysts.

He built Shield53 to streamline detections and protect organizations against breaches. As his client base expanded, the team needed a way to scale investigations without hiring or falling back on brittle SOAR setups. Dropzone lets them do both.

> There's a lot of talk that it's not if you get breached, it's when. I kind of disagree with that. Breaches are preventable, and AI will help us get there.

Chris Stewart
Executive Director

Challenges

Shield53 was looking for a solution to the following challenges:

High Alert Volume Across Diverse Client Environments	Each new client brought its own infrastructure, tooling, and threat surface, yet the alert queue funneled through a small, centralized team.
Time-Intensive Triage With Fragmented Context	Determining the legitimacy of an alert required stitching together context from multiple systems: user roles, device types, subnets, authentication patterns, and threat intelligence feeds.
Analyst Fatigue and Diminishing Focus	Even with structured triage rotations, the repetitive nature of alert investigation was draining cognitive resources.
Limited Capacity for Proactive Security Work	Manual alert triage takes a lot of time—time that could be spent tuning detections, running threat hunts, or improving coverage across clients.
Inflexibility and Overhead of Traditional Automation Tools	Playbook-driven SOAR solutions were evaluated but ultimately rejected due to high implementation and maintenance overhead.

See what Shield53 gained by deploying Dropzone AI, in their own words:

> We've seen a huge reduction in repetitive work. Dropzone has offloaded about 30–50% of our alert volume. That's time we can now spend threat hunting, onboarding customers, or improving coverage.
>
> **Chris Stewart**
> Executive Director

Selection & Implementation

It took Shield53 less than 30 minutes to get Dropzone AI running. No playbooks, no scripting, just API keys and a connection to CrowdStrike, Microsoft Defender, Entra ID, and internal asset inventory.

"We had instant results. We tossed in some API keys, and Dropzone started working right away. For a small, nimble team, that kind of low-maintenance setup is a huge win," says Stewart.

Within minutes, Dropzone AI was triaging alerts with the same rigor as a Tier 1 analyst, stitching in user identity, subnet data, and threat intel, and sending results directly into JIRA.

Today, there is no need for custom playbooks or SOAR workflows. Dropzone's output includes full investigations with conclusions that analysts can act on. High-priority alert investigations are escalated via AlertOps, and conversations take place in Microsoft Teams.

Shield53 also uses Dropzone AI to automate containment tasks, such as isolating endpoints or disabling compromised accounts according to client policies and predefined use cases approved with their clients.

With Dropzone AI running triage, analysts spend just 1–4 hours per shift on alerts, reclaiming time for higher-impact security work.

Benefits Realized with Dropzone AI

Cut 15–20 Minutes from Every Alert	Before Dropzone AI, analysts had to log in to customer environments through VPNs, fetch user data from Microsoft Entra ID, correlate IP addresses, and manually check EDR telemetry. Now, each alert investigation comes preloaded with user identity, subnet, device info, and relevant IOCs ready to review and act on in JIRA.
Handled 100% of Alerts with the Same Team	Shield53 now processes 100% of incoming alerts across healthcare, financial, education, and manufacturing clients without increasing team size. Dropzone handles investigations in parallel and scales automatically, even during spikes in alert volume.
Auto-Isolated Endpoints and Disabled Accounts	Shield53 configured Dropzone to take actions like isolating noisy endpoints or disabling compromised accounts based on specific client conditions. These were previously manual and inconsistent. Now they're fast, repeatable, and logged through existing workflows.
Fits Directly Into Existing Workflows	Dropzone plugged into existing tools with no workflow disruption. Shield53 didn't need to change how they worked; everything flowed into JIRA, AlertOps, Teams, and their existing EDR stack.
Shifted Analyst Time to Threat Hunting and Tuning	With Dropzone handling triage, analysts reclaimed hours each week to tune detection logic, monitor attack surfaces, and run threat hunts tasks that reduce risk, but often got pushed aside due to alert load.

Key Performance Indicators (KPIs) and Results:

All incoming alerts triaged automatically across multiple client environments

Saved 15–20 minutes saved per alert, eliminating repetitive manual tasks.

Containment actions automated based on pre-approved policies.

Integrated with core tools in under 30 minutes, requiring no scripting or playbooks.

More time for proactive security such as tuning detections, improving coverage, and threat hunting.

Partnering to Operationalize Automation Across Clients

Shield53 works closely with Dropzone to refine deployments, adapt logic across clients, and shape shared use cases based on years of incident response knowledge.

When Shield53 needed to configure response actions, the Dropzone team helped. A tight loop of feedback, iteration, and implementation gives Shield53 confidence in both the platform and the people behind it.

> We've had people ask if a Dropzone ticket was written by a human because it's that good. Our clients appreciate the consistent high quality of Dropzone investigations.
>
> **Chris Stewart**
> Executive Director

Our AI Analysts Never Sleep, So You Can

Dropzone AI is the leading AI SOC Analyst, trusted by SOC teams to automate tedious, repetitive tasks. It autonomously investigates alerts 24/7, integrates with existing security tools, and delivers decision-ready investigation reports. Designed to eliminate alert fatigue and accelerate incident response, Dropzone AI frees SOC teams for higher-level work, enabling organizations to focus on real threats without adding headcount. No playbooks, code, or prompts required. Learn more by visiting www.dropzone.ai.

Request a Demo

Dropzone AI