Dropzone AI

How ECS Broke the SOC Scalability Ceiling with AI SOC Agents

ECS

Company Profile

ECS, a $1.2B provider of advanced technology solutions in data and AI, cybersecurity, and enterprise transformation, ranked second on CyberRisk Alliance and MSSP Alert's Top 250 Managed Security Service Providers (MSSPs) list for 2024. The organization's enterprise arm operates a 24/7, multi-tenant SOC that supports clients across North America. The team analyzes billions of events each year, delivering high-quality security outcomes at scale.

As ECS's MSSP scaled, they recognized that the traditional SOC model—adding headcount to meet demand—was structurally unstable. Alert volume was rising faster than staffing capacity, forcing skilled analysts to expend disproportionate effort on benign alerts rather than adversary-driven risk.

> Matching alert growth with linear headcount simply isn't viable. We can't add alerts and add full-time employees one-for-one. Dropzone allowed us to scale our analysts' impact without replacing the people who make our SOC effective.
>
> **Dave Howard**
> Senior Director of Cybersecurity Operations, ECS

Challenges

Scaling Without Linear Headcount	As ECS's MSSP business expanded, alert volume growth outpaced the team's ability to scale proportionally. The SOC was processing roughly 30,000 alerts per month, making a hire-to-keep-up model operationally and economically unsustainable.
Alert Overload and Analyst Fatigue	Most alerts were benign, yet they consumed a disproportionate share of analyst time. High-volume, low-value triage displaced focus from genuine threats, leading to fatigue and operational inefficiency.
Inconsistent Manual Triage	Human-driven triage produced variable outcomes. ECS required triage to be executed in a standardized, repeatable, and auditable manner to ensure consistency at scale.
Limits of Existing Automation	ECS had maximized the practical limits of its security orchestration, automation, and response (SOAR) technology. While effective for enrichment and response actions, SOAR lacked the ability to reason through investigations or safely auto-close benign alerts.

What ECS gained by deploying Dropzone AI, in their own words:

> We were surprised by the depth of the investigations. Dropzone was pulling in context and evidence that our analysts wouldn't normally gather during initial triage.
>
> **Jesse Mainor**
> SOC Manager, ECS

Selection & Implementation

The ECS team recognized that AI applications for security operations were advancing but had not seen a solution that could handle the scale and complexity of their operations.

Most of the tools ECS evaluated fell short of actual investigative work that they needed to automate. That changed when Dave Howard, Senior Director of Cybersecurity Operations at ECS, came across Dropzone AI.

ECS was not attempting to replace analysts, but to give them leverage. With alert volume rising faster than headcount, the team needed a mechanism to absorb noise and enforce consistent investigations, allowing analysts to concentrate on genuine, high-impact threats.

ECS ran a structured proof of value using real production alerts, benchmarking Dropzone's investigations against existing tools and human triage. Dropzone compared very favorably in the evaluations.

What stood out was not just speed but also the consistency and depth of analysis, including context and evidence that analysts would not typically gather during initial triage.

ECS integrated Dropzone directly into its existing workflow. Alerts move from detection systems through SOAR, into Dropzone for autonomous investigation, with outcomes fed back into ServiceNow for centralized case management and auditability.

Benefits Realized with Dropzone AI

Scaled the SOC Without Adding Headcount	Dropzone allowed ECS to scale past the 30,000 alerts-per-month ceiling with their current headcount. The SOC is now able to support more clients and higher volume while providing high-quality service.
Accelerated Triage and Threat Identification	Alerts are investigated immediately instead of waiting in a queue. This reduced acknowledgment lag, accelerated mean time to triage, and helped ECS identify real threats sooner.
Eliminated Alert Noise at Tier 1	By safely auto-closing the majority of benign alerts, Dropzone removed the persistent background noise that consumed Tier 1 capacity. Analysts were able to redirect effort toward high-risk activity rather than repetitive, low-value triage.
Delivered Consistent, Defensible Investigations	Dropzone standardized how alerts are investigated across shifts and experience levels. Each alert arrives with clear conclusions, supporting evidence, and rich context, improving trust and decision quality.
Improved Analyst Effectiveness and Retention	With queues cleared and workloads more manageable, analysts experienced less burnout and greater job satisfaction. Senior staff were able to focus on higher-value work like threat hunting, detection engineering, and improving the SOC overall.

Key Performance Indicators (KPIs) and Results:

70% of Tier 1 Alerts Automatically Closed.
Dropzone safely identified and resolved the majority of benign alerts without analyst involvement.

100% of Alerts Investigated Immediately.
Every alert is investigated as soon as it is created, eliminating acknowledgment delays and speeding triage.

Tier 1 Queues Fully Cleared Across Client Base.
Dropzone eliminated triage backlogs, stabilizing day-to-day SOC operations and reducing analyst strain.

Broke the SOC Scalability Ceiling (~30,000 Alerts/ Month).
Dropzone enabled ECS to scale alert handling beyond previous limits without adding headcount.

A True Design Partner

ECS saw Dropzone as a true design partner. By rapidly building critical capabilities like an Elastic integration and acting on feedback in real time, Dropzone earned ECS' trust as a partner capable of evolving alongside their SOC.

> From the onset, Dropzone was responsive and welcomed us into a design partnership. Working with them has been one of the best vendor experiences of my career.
>
> **Dave Howard**
> Senior Director of Cybersecurity Operations, ECS

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