Dropzone AI

How a Leading European MSSP Scaled Alert Investigations Without Scaling the SOC

Executive Summary

A leading European managed security service provider (MSSP) was facing a challenge shared by many modern SOCs. Alert volumes were increasing across endpoint, cloud, identity, and network controls, while customer expectations continued to rise. Every alert needed to be investigated, explained, and resolved. Despite operating a mature SOC with strong tooling, strict SLAs, and experienced analysts, manual Tier 1 investigations had become the limiting factor.

The MSSP evaluated Dropzone to address this gap. The goal was not to replace analysts or detection technologies, but to scale investigation capacity without scaling headcount. Any solution needed to integrate into existing SOAR and case management workflows, investigate alerts at the case level, remain explainable and auditable, and respect strict customer separation and data residency requirements.

A rigorous proof of concept was designed to test Dropzone under real operational conditions. Using development tenants, historical data, and live alerts from Microsoft Defender and Sentinel, Dropzone was evaluated on investigation accuracy, multi-source enrichment, SLA alignment, and evidence quality. Investigations were triggered directly from SOAR workflows to validate day-to-day fit.

During the POC, investigations were consistently completed in minutes rather than hours, with reports that matched or exceeded human Tier 1 quality. Investigation accuracy reached approximately 90 to 95 percent, false positives were consistently eliminated, and multi-alert cases were investigated as a single unit. Analysts trusted the conclusions enough to act on them without redoing the work, marking a shift from evaluation to reliance.

Following adoption, the MSSP increased alert coverage, reduced analyst load, and improved consistency across Tier 1 investigations. The change also altered the economics of the SOC, enabling the MSSP to onboard more customers without a proportional increase in staffing and to improve margins amid growing alert volumes. Dropzone's roadmap alignment, including support for multi-tenancy and regional data hosting, reinforced confidence in long-term scalability.

For this MSSP, Dropzone did not change what the SOC did. It changed what was possible at scale, transforming alert investigation from a bottleneck into a sustainable, scalable capability.

The Problem Before the Tool

Despite operating a mature, well-run SOC, this European MSSP found itself under growing pressure. The team had invested heavily in its security operations over the years, building a sophisticated environment supported by multiple security platforms, a SOAR-driven workflow, and clearly defined SLAs. Customers trusted the service. Expectations were high. Response times mattered, and every alert carried weight.

The challenge was not a lack of tooling or expertise. It was scale. Alert volumes were rising steadily across endpoint, cloud, identity, and network controls, driven by broader attack surfaces and increasingly noisy detections. At the same time, customer expectations were shifting. Investigating only high-severity alerts was no longer enough. Customers wanted assurance that every alert gets reviewed, explained, and either acted on or confidently dismissed. That expectation collided head-on with reality. Tier 1 investigations remained largely manual, analysts were costly to hire and retain, and adding headcount did not scale linearly with demand.

What emerged was a structural gap. The SOC could detect threats effectively, but its investigative capacity lagged behind the growth in alerts. Analysts spent disproportionate time triaging benign activity, duplicating effort across tools, and writing up investigations that rarely justified the time invested. The bottleneck was no longer detection or response. It was the human effort required to investigate alerts at volume. And without a change in approach, that gap was only going to widen.

90% – 95%

Approximate investigation accuracy during POC

The Breaking Point: Why the Existing Model Didn't Scale

Over time, the pressure became impossible to ignore. What started as a manageable increase in alert volume began to expose deeper cracks in the operating model. Alert investigation was drifting toward commoditization. Customers were seeing better detection rates from their tools and questioning why investigations required so much human effort. Some even began to assume that modern security platforms alone could replace large parts of an MSSP's value.

That shift had real consequences. Margins tightened as repetitive triage consumed analyst time. Investigating only the "most important" alerts became a necessity, not a choice. Lower-severity alerts piled up, creating blind spots that were hard to justify to customers who expected full coverage. Meanwhile, the quality of investigations depended heavily on individual analysts. Context lived in people's heads. Experience, intuition, and memory influenced decisions, not consistently captured systems. When analysts changed roles or left, that knowledge went with them.

This was not a conversation about cutting staff or automating people out of the SOC. The MSSP valued its analysts and depended on their expertise. The problem was structural. Coverage was constrained by human capacity. Consistency varied by shift and experience level. Economics no longer worked when every alert demanded manual effort. SLAs became harder to guarantee as volume increased.

The breaking point was clear. The question was not how to investigate alerts faster. It was about investigating all alerts reliably and at scale without breaking the SOC.

What the MSSP Was Looking For

Before evaluating any new technology, the MSSP was clear about what success needed to look like. This was not an open-ended search for automation, nor was it a reaction to a single pain point. The requirements were shaped by years of operating a complex SOC under real customer constraints.

At the core was the need to automate Tier 1 investigations without falling back on brittle playbooks. Static rules could not keep up with the variety of environments, tools, and alert types the SOC handled every day. Any solution had to reason through investigations the way an experienced analyst would, while still fitting cleanly into the existing SOAR and case management model. To make this all work, the new tool needed to fit into the SOC without requiring the SOC to be rebuilt around it.

Flexibility mattered as much as depth. The MSSP supported customers with very different security stacks, and any approach had to work across endpoint, cloud, identity, and network tools without assuming a single vendor or data model. Investigations also needed to operate at the case level. Isolated alerts rarely told the full story. What mattered was understanding how related activities fit together and presenting that context clearly.

Transparency was non-negotiable. Investigations had to be explainable, evidence-backed, and auditable, with clear reasoning that analysts could trust and defend to customers. Just as important was strict customer separation and data residency. Operating in regulated European environments left no room for ambiguity around where data lived or how it was handled.

Above all, the MSSP needed to increase investigation capacity without increasing headcount. The goal was to absorb growing alert volumes while protecting SLAs and margins, not to trade one scaling problem for another.

There were also clear non-goals. This was not a search for another SIEM, a black-box scoring engine, or a system meant to replace analysts. It needed to produce actual results, not just serve as a training tool. For the MSSP, the right solution would extend its analysts' reach, standardize investigations, and make full alert coverage possible at scale.

Introducing Dropzone

Against that backdrop, Dropzone entered the conversation not as another security tool, but as a different way to approach investigation itself. Instead of promising better detection or more alerts, Dropzone positioned itself as an AI SOC Analyst, designed to take on the investigative work that was straining the SOC.

Dropzone investigates alerts autonomously using the same investigative framework human analysts follow. When an alert arrives, it does not score it or dismiss it based on static rules. It gathers context, queries connected systems, correlates related activity, and evaluates evidence step by step. The process mirrors how an experienced Tier 1 analyst would approach the problem, but without the constraints of time, shift changes, or alert volume.

Crucially, Dropzone works with the tools already in place. It pulls evidence directly from existing platforms across endpoint, cloud, identity, and network controls. There is no requirement to centralize data in a new system or reconfigure detections. The output is a clear, decision-ready investigation report that explains what happened, why it matters, and whether action is recommended. Analysts can review the findings, agree or override them, and move forward without redoing the work.

Just as important was Dropzone's operational fit. It integrates into the SOC's existing SOAR and case management workflows rather than sitting beside them as a separate console. Investigations are triggered as part of normal operations, and results flow back into established processes.

There were also clear boundaries. Dropzone does not generate alerts, and it does not replace detection technologies. It does not attempt to decide risk through opaque scoring models. Its role is narrowly focused and intentional. It investigates what already exists at the point where human effort has become the limiting factor.

The Evaluation: A POC Designed to Break the System

Given what was at stake, the MSSP approached evaluation with deliberate rigor. This was not a marketing demo or a guided proof point. The goal of the proof-of-concept was to determine whether Dropzone could withstand real operational pressure.

The POC began in development tenants rather than controlled demo environments. Dropzone was connected to Microsoft Defender and Sentinel and fed real alerts and historical data, including noise, edge cases, and inconsistencies found in production systems. There was no attempt to curate inputs or simplify scenarios. If the system worked here, it would work anywhere.

Equally important was how Dropzone performed operationally. Investigations were triggered from within existing SOAR workflows, not manually from a standalone interface. The SOC needed to understand whether Dropzone could operate within daily operations without forcing analysts to change their workflows or introducing new process risks at scale.

That operational impact was precisely why executive leadership was involved early. The evaluation's outcome would influence staffing models, service coverage, and customer commitments. This was not a tactical tool test. It was a decision with long-term implications for how the SOC would operate and grow.

The evaluation criteria were clear and uncompromising. Investigation accuracy mattered, but so did the way the solution arrived at its conclusions. The team scrutinized case-level reasoning to confirm that related alerts were investigated together rather than in isolation. They examined how Dropzone enriched investigations across multiple data sources and how it handled customer-specific context that often determines whether an alert is benign or actionable.

Just as critically, the MSSP assessed SLA alignment. Investigations needed to be completed quickly enough to support strict response commitments without sacrificing depth or accuracy. Every conclusion had to be explainable, backed by concrete evidence, and defensible to both analysts and customers. Anything that failed under real conditions needed to fail during the POC, not after deployment.

What the MSSP Learned During the POC

As the POC progressed, the focus shifted from validation to confidence. Early skepticism gave way to something more meaningful as Dropzone was exposed to day-to-day conditions and real investigative pressure. Investigations that once took analysts hours were consistently completed in minutes. That speed did not come at the expense of quality. In many cases, the reports matched or exceeded the SOC's expectations for a Tier 1 analyst, with clear reasoning, structured findings, and concrete next steps.

What made the difference was transparency. Every conclusion was supported by traceable evidence drawn directly from the underlying tools. Analysts could see exactly which data sources were queried, what was found, and how those findings informed the outcome. This was not a black box producing a verdict. It was a visible investigative process that analysts could follow, challenge, and ultimately trust.

Over time, a pattern emerged. False positives were consistently identified and closed with confidence. Related alerts were investigated together as a single case rather than treated as isolated events. That context reduced duplication and helped analysts understand the full scope of activity more quickly. As confidence grew, analysts began acting on Dropzone's conclusions without redoing the investigation themselves.

The numbers reinforced what the team was seeing. Investigation accuracy reached approximately 90 to 95 percent. SLA acknowledgment improved immediately as investigations were completed faster and more predictably. The turning point was not a single metric, but a shift in behavior. Dropzone stopped being something the SOC was testing and became something the SOC relied on.

> Analysts trusted the conclusions enough to act on them without redoing the work.

Fitting Into Reality: SOAR, Cases, and Customer Separation

What ultimately determined whether Dropzone could move beyond evaluation was not raw performance, but how cleanly it fit into the reality of day-to-day operations. The SOC did not want another system that analysts had to check, learn, or manage. SOAR triggered Dropzone as part of existing workflows, not launched manually or treated as a separate destination. Investigations started where analysts already worked and ended in the same systems they used to make decisions.

Just as important was what happened after an investigation was completed. Dropzone returned structured results directly into existing case management and automation pipelines. There was no requirement to adopt a new UI or change how cases were tracked and closed. Analysts reviewed the findings, agreed or overrode conclusions, and retained full control over response actions. Dropzone handled the investigation, not the authority.

As an MSSP, customer separation was a major requirement to ensure privacy. Each investigation operated within strict tenant boundaries, ensuring that data, context, and history never crossed between customers. This preserved the MSSP's operating model and met regulatory and contractual obligations without exception.

These details mattered because they removed friction where it mattered most. There was no disruption to customer contracts, no retraining of analysts, and no new compliance risk introduced by adoption. Dropzone worked because it respected how the SOC already operated and strengthened it from within, rather than asking it to adapt around a new tool.

From Validation to Trust: Iteration and Feedback

As Dropzone became part of daily operations, the POC shifted from proving capability to refining behavior. Real-world use surfaced edge cases that no controlled test could predict. Context assumptions were challenged. Certain alerts behaved differently in specific customer environments. Integration details that looked simple on paper revealed friction once exposed to production data and live workflows.

What mattered was how those moments were handled. Feedback moved quickly between the SOC and Dropzone's team. Misclassifications were reviewed, investigation logic was adjusted, and improvements were shipped, all while the POC was still underway. Rather than undermining confidence, this iteration reinforced it. The system did not stagnate. It adapted.

Analysts began to see their feedback reflected in subsequent investigations. Context became sharper. Conclusions aligned more closely with how the SOC operated in practice. The AI improved not through abstract tuning, but through direct exposure to the MSSP's reality.

By the end of the POC, the relationship had changed. Dropzone was no longer viewed as a static product being evaluated, but as a partner invested in getting investigations right. Trust grew because progress was visible, responsiveness was consistent, and the system evolved alongside the people using it.

The Bigger Question: Can This Scale?

With confidence in day-to-day operations established, the conversation widened. The question was no longer whether Dropzone worked inside a single SOC workflow, but whether it could support the MSSP's broader business model. Leadership began evaluating the platform through a different lens, one focused on scale, regulation, and long-term economics.

Several concerns surfaced quickly. Any solution had to work across more than a hundred customer environments without introducing operational sprawl. Data residency mattered, particularly in regulated European markets where expansion depended on where investigations were processed and stored. The MSSP also needed to avoid a one-tenant-per-customer model that would recreate the very scaling problems they were trying to solve. And underpinning all of it was margin. Full alert coverage only made sense if the cost per investigation could be reduced without eroding service quality.

This is where Dropzone's impact extended beyond the SOC. By supporting one-to-many customer models, the platform allowed investigations to scale without a proportional increase in operational overhead. The cost of investigating an alert dropped dramatically, shifting the economics of coverage. What had once been financially impractical became viable. Investigating every alert was no longer a theoretical goal, but a sustainable operating model.

At the executive level, that shift mattered. Dropzone reframed the investigation from a cost center constrained by human effort into a scalable capability that could grow alongside the MSSP's customer base.

> The ability to investigate every alert without scaling headcount fundamentally changed the SOC's cost structure.

The Decision: From POC to Expansion

With the open questions resolved, the decision came into focus. The proof of concept had done its job. Technical validation was complete, and investigation quality was no longer in doubt. Dropzone had proven it could reason through alerts with the depth and consistency the SOC expected, while fitting cleanly into existing workflows. Analysts trusted the output. Operations did not need to change. SLAs held.

Just as importantly, the economics worked. The ability to investigate every alert without scaling headcount fundamentally changed the SOC's cost structure. What had once been a constraint became a lever. At the same time, Dropzone's roadmap aligned with where the MSSP was headed. Support for data residency, multi-tenancy, and large-scale operations was not an afterthought. It was a priority.

The outcome was clear.

- ☑ Expansion was approved.
- ☑ Swiss hosting was prioritized to support regulatory requirements and unlock additional customers.
- ☑ Multi-tenancy was enabled to avoid operational sprawl and support growth.

Dropzone moved from an evaluated solution to a core SOC platform, positioned to support the MSSP's next phase of scale with confidence.

Results After Adoption

Following adoption, the impact was felt first in day-to-day operations. Investigation capacity increased without changing the SOC's operations. Alerts that previously would have been deprioritized or queued were now investigated consistently, allowing the team to move closer to full alert coverage. Investigation cycles shortened as Dropzone completed Tier 1 analysis autonomously, returning structured findings in minutes rather than hours. Analysts spent less time on repetitive triage and more time reviewing conclusions, handling escalations, and focusing on complex cases. Just as importantly, the output became more consistent. Tier 1 investigations followed the same reasoning framework every time, regardless of shift, customer, or alert source.

Those operational gains translated directly into business outcomes. With investigation no longer the primary bottleneck, the MSSP was able to support more customers without a corresponding increase in analyst headcount. That shift improved the underlying economics of the SOC and reduced pressure on margins that had been tightening under manual investigation models. At the same time, the ability to confidently investigate all alerts became a point of differentiation in a crowded MSSP market, where many providers still relied on selective triage or opaque automation.

Perhaps most significantly, adoption created a foundation for what came next. By standardizing and scaling investigation, the MSSP positioned itself to evolve beyond reactive services. Dropzone became an enabling layer for new, AI-driven offerings that could build on consistent investigations, shared context, and predictable workflows. The value was no longer limited to doing the same work faster. It opened the door to doing more, with confidence, at scale.

Why This Matters

What made this journey meaningful was not the adoption of a new tool, but a shift in what the SOC could realistically achieve. The core mission did not change. Alerts still needed to be investigated, evidence still needed to be gathered, and decisions still required human judgment. What changed was the ceiling. AI did not redefine the SOC's work. It removed the constraints that had quietly shaped it.

At scale, that distinction matters. When investigation is limited by human capacity, teams are forced to choose what to ignore. Coverage becomes selective, consistency suffers, and risk accumulates in the gaps. By automating investigation in a way that mirrors how analysts actually work, the MSSP reframed success. The most meaningful progress was no longer measured only by response time or closure rates, but by how much noise could be confidently eliminated without human effort.

This case illustrates a broader shift facing modern SOCs. AI is not about replacing people or accelerating individual tasks. It is about making full coverage, consistency, and accountability possible at volumes that were previously unsustainable. For organizations facing the same pressures, the lesson is clear. The value of AI is not in changing what security teams do, but in expanding what they can do without breaking under scale.

Looking Ahead

Looking ahead, the impact of this decision is less about any single capability and more about the space it creates. By removing investigation as a constant source of friction, the MSSP gained the space to operate deliberately rather than reactively. Analysts are no longer defined by alert volume alone. They have the capacity to focus on judgment, escalation, and improvement instead of repetitive triage.

The platform continues to evolve alongside the SOC, shaped by real operational feedback and long-term planning rather than short-term automation goals. As customer environments grow more complex and expectations continue to rise, the MSSP is positioned to adapt without reshaping its organization around every new challenge.

For this MSSP, Dropzone did not replace analysts. It gave them room to operate, scale, and evolve.

Dropzone did not replace analysts. It gave them room to operate, scale, and evolve.

Key Takeaways

01 Review how long alerts sit between detection and the first action. Break down the data by severity, source, and time of day to identify patterns in delays.

02 Automating investigations allowed the MSSP to expand alert coverage without increasing analyst headcount, improving the economics of the SOC.

03 Dropzone fit into existing SOAR and case management workflows without forcing process changes or removing analyst control.

04 Analyst trust was built through explainable investigations, traceable evidence, and visible improvements made during the POC.

05 By making investigations scalable, the MSSP gained the ability to support more customers, stabilize margins, and plan for future AI-driven services.

About Dropzone AI

Dropzone AI weaponizes LLMs for cyber defenders, delivering the Agentic SOC: AI agents that collaborate 24/7 so they can beat attackers. Dropzone integrates into your existing SOC stack on Day 1 (SIEM, EDR, ticketing, and threat intelligence) and agents immediately start to investigate alerts, respond to emerging threats, and proactively hunt attackers. Dropzone works with enterprises and MSSPs including ECS, Avalara, UiPath, and Zapier, and is actively protecting over 300 companies. Learn more by visiting www.dropzone.ai.

Request a Demo