CASE STUDY

Transforming Security Operations

How a Digital Insurance Company
Accelerated Efficiency with Dropzone AI

Dropzone AI

Company Profile

A **digital insurance company** founded in the last decade has made significant strides in the industry by offering a range of insurance products powered by AI technology. This technology enables the company to process claims and manage policies through a user-friendly app to serve almost 2 million customers. As a rapidly growing entity in the tech space, it has faced challenges in efficiently managing a high volume of security alerts without significantly expanding its team or resources.

ABOUT DROPZONE AI

Dropzone AI is building pre-trained AI analysts that work alongside human analysts in SOCs. Our technology handles the frontline work of investigating the mountain of alerts from security systems by replicating the processes and techniques of elite analysts so that human analysts can focus on only the real threats and higher-value work. It connects to your security tools and data sources, adapts to your environment, understands its context, and autonomously generates investigation reports for every alert without requiring playbooks or manual interactions. Book a demo here.

> "It's not a surprise that Dropzone is a Top 10 RSA Innovation Sandbox Finalist list, the potential for your product is great. They are further along than other GenAI cybersecurity products I have seen."

CHALLENGES

The company's initial security setup involved manual alert management, which was both time-consuming and resource-intensive. They faced numerous challenges, including:

High Volume of Security Alerts:

With the increasing number of security alerts generated by their systems, the SOC team found it challenging to keep up. The volume of alerts required constant monitoring and manual investigation, which was not sustainable as the company continued to grow.

Need for Continuous 24/7 Monitoring:

Ensuring around-the-clock monitoring was crucial for their organization due to the nature of their business and the sensitive data they handle. However, maintaining a 24/7 vigilance with a human-only team was both challenging and costly.

Time-Consuming Manual Processes:

Investigating each alert manually was a labor-intensive process that consumed significant amounts of time and effort from the SOC team. Analysts had to sift through vast amounts of data to identify potential threats, leading to delays in response times and increased chances of missing critical alerts.

Growth Capped:

Faced with a fixed budget, the company's SOC team was restricted in size, making it impractical to increase staff to match the growing demands of their workload. This situation highlighted the necessity for a scalable solution that could enhance the existing team's effectiveness without adding more personnel.

CHALLENGES

Limited Bandwidth:

SOC analysts found themselves overwhelmed by mundane, repetitive tasks that monopolized their time, diverting attention away from prioritizing significant security threats. This constant engagement with routine activities heightened the risk of burnout and diminished their overall operational efficiency.

Difficulty in Handling Complex Threats:

As security threats grew more sophisticated, the requirement for meticulous and comprehensive analysis intensified. The team faced significant challenges adapting to these complex threats, struggling to consistently identify and mitigate evolving risks effectively.

Inconsistent Analysis and Decision-Making:

The lack of a uniform method for alert investigation led to variable analysis quality, compromising the company's security posture. Such inconsistencies in handling alerts could result in overlooked vulnerabilities, undermining the organization's defenses.

High Rate of False Positives:

Manual processes often resulted in a high number of false positives, which further burdened the team. Analysts spent considerable time investigating alerts that turned out to be non-issues, reducing their ability to focus on genuine threats.

See what they have gained through working with Dropzone AI, in their own words:

> "Dropzone's investigation report summaries are extremely useful. They provide a summary analysis, broken down by detailed individual analysis sections. These thorough summaries allow me to drill down to a granular level where needed. This wouldn't happen with human analysis, there would just be a general summary with a few bullet points."

> "Dropzone's technology is a timesaver. It helps SOC analysts get through more problems at an accelerated pace. The AI SOC analyst delivers a degree of thoroughness and ultimately defensibility about a decision that would take too much effort for humans to do at scale."

SECTIONS & IMPLEMENTATIONS

The selection criteria included autonomous AI investigative capabilities, ease of integration, cost efficiency, and the ability to provide continuous monitoring while reducing the manual workload. The decision-making process was led by the CISO and involved the security team and other stakeholders.

The onboarding process was smooth and quick, with minimal configuration required. Dropzone AI seamlessly integrated with their existing systems, including AWS, Google Workspace, and Okta. The team began seeing benefits within weeks, thanks to Dropzone AI's immediate functionality.

BENEFITS REALIZED WITH DROPZONE AI

Dropzone AI brought several significant benefits to the company:

Efficiency and Time Savings:

Reduced manual workload, allowing SOC analysts to focus on higher-value tasks.

Cost Savings:

Reduced need for additional headcount and resources, leading to substantial cost savings.

Continuous Monitoring:

24/7 vigilance ensured that no alerts were missed, providing a higher degree of vigilance compared to human-only teams.

Improved Confidence:

Higher degree of confidence in alert investigations and decision-making.

> “Dropzone saves you and your team so much time from redundant tasks that no one wants to do. It gives you an accurate analysis of data sources that you would never think of looking through. It allows you to solve critical problems that you and your team don’t have the bandwidth to solve.”

KEY PERFORMANCE INDICATORS (KPIs) AND RESULTS

Detailed Investigation Reports

The detailed report summaries provided by Dropzone AI enabled a granular level of analysis, reducing the time spent on routine investigations and improving accuracy.

Reduction in False Positives

The testimonials highlight a reduction in false positives, which allowed the team to focus on genuine threats, enhancing overall efficiency.

Increased Accuracy in Threat Detection

The AI SOC analyst’s thoroughness and detailed reports contributed to more accurate threat detection and response.

CLEAR ROI REPORTING

Provided clear ROI reports tailored to real business costs, demonstrating substantial savings and efficiency.

> “The ROI reports have been particularly valuable, demonstrating substantial savings and reinforcing the importance of proactive brand protection.”

Our AI Analysts Never Sleep, So You Can