Dropzone AI

DATA SHEET

Investigate every alert, like having a 10x SOC team that never sleeps

Autonomous AI SOC Analysts: 24/7 Alert Investigations, 10X your SOC team

The Challenge

A typical SOC has dozens of security tools generating thousands of alerts daily. Each alert requires 5 to 40 minutes of manual analysis, overwhelming analysts.

Security tools make up the foundation of security programs, driving alerts from numerous sensors to security analysts for triage. As the number of devices, applications, and digital interactions surges, so does the volume of security alerts generated by various systems.

These alerts, which could signal potential cyber threats, require prompt and thorough investigation to determine their legitimacy and potential impact.

However, the sheer magnitude of these alerts poses a significant challenge.

Organizations find their security teams inundated with more alerts than they can feasibly assess and resolve promptly.

Today, only 10% of alerts are investigated. This bottleneck strains resources and increases the risk of genuine threats being overlooked or addressed too late.

The problem is further intensified by the continuously evolving nature of cyber threats, requiring constant vigilance and adaptation. Consequently, this situation leaves organizations vulnerable to cyber attacks, data breaches, and other security incidents, resulting in significant financial losses, damage to reputation, and legal repercussions.

Another challenge is limited budget and a shortage of talent. Many organizations struggle to allocate sufficient resources to their cybersecurity efforts, making it difficult to invest in advanced tools and hire skilled professionals.

AI SOC Analyst that Never Sleeps. So You Can

Executive Summary

Market: Security Operations Automation

Description

Organizations do not have sufficient automation and budget to investigate 100% of security alerts today

Challenge

SOCs face an overwhelming workload due to the high volume of alerts, time-consuming investigations, and limited resources, leaving them exposed to breaches and unable to effectively prioritize threats.

Result

Dropzone AI’s specialized AI agent autonomously performs end-to-end investigations, covering 100% of your alerts. Freeing your analysts to focus on critical projects.

Dropzone AI

DATA SHEET

The Solution

Dropzone AI offers AI SOC analysts that autonomously perform thorough investigations of 100% of your security alerts 24/7.

Dropzone AI solves the pressing issue of alert overload in cybersecurity operations. Their innovative approach harnesses the power of advanced Artificial Intelligence, specifically Large Language Models, to autonomously investigate and analyze the multitude of security alerts. This AI-driven system is designed to replicate human security analysts' expertise and decision-making processes.

By doing so, Dropzone AI significantly streamlines the alert Investigation process, by automating traditional manual tier-1 analysis using software This enables organizations to quickly identify and respond to the most critical security issues, enhancing their cyber defense.

Integrating Dropzone AI into existing security operations promises a more agile, effective, and scalable approach to process the ever-growing influx of security alerts, ultimately bolstering an organization's cybersecurity posture.

Key Benefits

Dropzone AI significantly enhances threat detection and response, quickly identifying genuine threats with remarkable accuracy. Automating routine alert analysis dramatically reduces the workload on security teams, thereby minimizing alert fatigue and improving threat detection precision. This refined approach leads to fewer false alarms and a more concentrated effort on critical threats.

Scalable and adaptable, Dropzone AI effortlessly manages varying volumes of alerts, making it suitable for organizations of any size. Its focus on cost-effectiveness and ease of integration means it streamlines security operations efficiently. The AI system saves time and evolves continuously, learning from ongoing activities to enhance its effectiveness. This results in a marked improvement in cyber resilience, transforming how organizations approach and handle cybersecurity challenges and ensuring a robust and agile defense against evolving digital threats.

Features

- Autonomous Alert Investigation
- SOC analyst chatbot
- Organizational context adaption
- Patented Large Language Model-based reasoning system
- Replication of Human Expert Techniques
- 30 min deployment
- Out-of-the-box automation with no playbook, code, prompt required

Benefits

- 24/7 Autonomous Alert Investigations
- Enhanced Threat Detection and Response
- Reduction in Mean Time to Resolution (MTTR)
- Reduced Alert Fatigue
- Improved Accuracy
- Continuous Learning and Adaptation

Dropzone AI's Autonomous AI SOC Analysts thoroughly investigate every alert 24/7, empowering your SOC to operate like a 10x larger team.

Test Drive Dropzone AI Today