AI SOLUTIONS GUIDE

10X SOC Team Multiplier

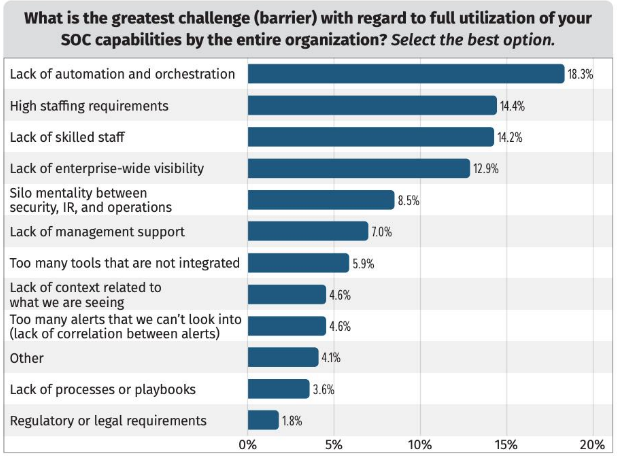
Dropzone AI

Facing SOC Challenges

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.

Lack of automation and orchestration

Automation and orchestration streamlines the integration of various security tools and processes, enabling SOCs to respond swiftly and effectively to threats. Without these capabilities, SOCs often face increased manual workloads, leading to slower response times, higher rates of human error, and a general inefficiency in managing security alerts. This deficiency not only burdens the existing staff but also magnifies the impact of the ongoing skills shortage in cybersecurity by increasing the demand for highly skilled professionals to perform tasks that could otherwise be automated.



Source: SANS 2024 SOC Survey: Facing Top Challenges in Security Operations

Our AI SOC Analyst Never Sleeps — So You Can.

High staffing requirements

The demand for skilled cybersecurity professionals outstrips supply. SOCs require a continuous and robust presence to monitor, analyze, and respond to threats effectively, leading to high staffing demands. This requirement can strain resources as recruiting and retaining qualified personnel becomes both competitive and costly.

High staffing levels are often necessary to handle the volume and complexity of security alerts that require human intervention, especially in organizations lacking sufficient automation and orchestration tools. The need for extensive staffing impacts operational budgets and puts pressure on existing staff, potentially leading to burnout and reduced efficacy.

Lack of skilled staff

This shortage is exacerbated by the rapidly evolving landscape of cyber threats, which demands a high level of expertise and continual learning from cybersecurity professionals. The need for more adequately trained and experienced personnel leads to vulnerabilities in security posture as SOCs struggle to detect, analyze, and respond to sophisticated threats effectively.

Additionally, the shortage puts undue stress on existing staff, often resulting in burnout and high turnover rates, which further degrades the operational capability of SOCs.

> **Organizations today face a daunting challenge: With an overwhelming number of security alerts and insufficient budgets, they lack the automation necessary to investigate each incident thoroughly, making it impractical to hire enough analysts to manage the load effectively.**

How it Works

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.

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**

Alert Investigation

Dropzone AI revolutionizes how SOCs handle alerts by streamlining the ingestion, deduplication, and investigation processes without relying on traditional playbooks. When Dropzone ingests alerts from various security tools, it automatically filters and deduplicates them to ensure that analysts are only notified of unique and actionable threats, reducing the noise and clutter often associated with alert overload.

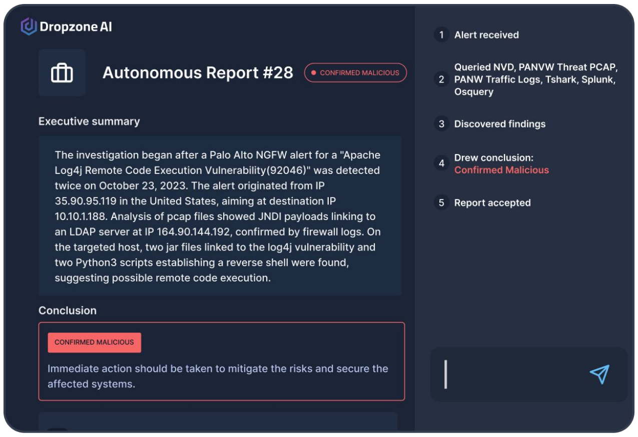
This system leverages advanced AI algorithms to analyze and prioritize alerts based on their severity and potential impact on the organization. Unlike traditional SOCs that depend on predefined playbooks, Dropzone AI autonomously investigates each alert, drawing on its deep learning capabilities to understand the context and nuances of the threat without human-scripted guidance. This approach accelerates response times and enhances the accuracy and efficiency of threat detection and mitigation, enabling SOCs to operate more effectively with fewer resources.

Dropzone AI

AI SOLUTIONS GUIDE

Dropzone in Action

Dropzone AI streamlines security operations by automating alert investigations, significantly reducing the time and manual effort required to manage threats effectively.



Dropzone AI

Autonomous Report #28 · CONFIRMED MALICIOUS

Executive summary

The investigation began after a Palo Alto NGFW alert for a "Apache Log4j Remote Code Execution Vulnerability(92046)" was detected twice on October 23, 2023. The alert originated from IP 35.90.95.119 in the United States, aiming at destination IP 10.10.1.188. Analysis of pcap files showed JNDI payloads linking to an LDAP server at IP 164.90.144.192, confirmed by firewall logs. On the targeted host, two jar files linked to the log4j vulnerability and two Python3 scripts establishing a reverse shell were found, suggesting possible remote code execution.

Conclusion

CONFIRMED MALICIOUS

Immediate action should be taken to mitigate the risks and secure the affected systems.

1 Alert received

2 Queried NVD, PANVW Threat PCAP, PANW Traffic Logs, Tshark, Splunk, Osquery

3 Discovered findings

4 Drew conclusion: Confirmed Malicious

5 Report accepted

Decision-ready investigation

Dropzone AI generates decision-ready investigation reports that streamline the response process. Utilizing advanced AI, Dropzone autonomously investigates alerts and compiles comprehensive reports that summarize the findings in a clear and actionable manner. These reports include an executive summary, a detailed threat analysis, and recommended mitigation steps, all prioritized by severity to aid in quick decision-making.

This capability allows analysts to immediately grasp the essence of the threat without sifting through raw data or performing manual analyses.

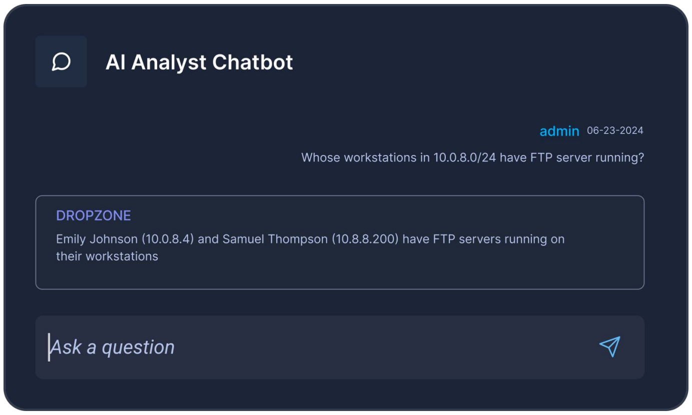
By providing ready-to-act information, Dropzone AI ensures that SOC teams can respond to threats more swiftly and effectively, minimizing potential damages and enhancing overall security posture.

Reliable Answers

Dropzone AI incorporates a sophisticated natural language chatbot that significantly enhances the user experience for security analysts within Security Operations Centers (SOCs). This chatbot utilizes advanced natural language processing (NLP) technologies to interpret and respond to queries in plain language, making it accessible even to less experienced analysts.

Users can ask the chatbot detailed questions about specific threats, investigation steps, or security protocols and receive instant, accurate responses based on metadata across different products in the existing security stack.

This feature speeds up the investigation process by providing immediate access to crucial information and serves as an educational tool, helping analysts understand complex security situations through interactive learning. The chatbot's ability to digest and straightforwardly explain intricate security data makes it an invaluable resource for enhancing situational awareness and decision-making in real time.



AI Analyst Chatbot

admin 06-23-2024

Whose workstations in 10.0.8.0/24 have FTP server running?

DROPZONE

Emily Johnson (10.0.8.4) and Samuel Thompson (10.8.8.200) have FTP servers running on their workstations

10x the brainpower in the security team and get 24/7 alert investigation coverage for 100% of your alerts

Get a Demo

Dropzone AI

Dropzone.AI

/DropzoneAI

@DropzoneAI