Dropzone AI

SANS Research Program

Product Briefing

SOC with Dropzone AI:

Insights from the 2024 SANS Institute Survey

July 2024

The job of the SOC gets bigger every day. The budget often does not. Attracting and retaining experienced staff is the eternal struggle for SOC managers, while analysts strive to build their knowledge and protect organizational assets. Fortunately, powerful tools are available to help bridge the gap between what you have and what you need.

Dropzone AI

What if you could trust AI? That's the concept behind Dropzone AI, a SOC tool that emulates the work of a Tier 1 analyst, performing preliminary investigations autonomously. Created by founding engineers from top tech companies, Dropzone AI helps under-resourced security operations teams reduce their mean time to disposition (MTTD) and generate prioritized reports for human analysts.

The technology gives SOCs a tool to automate and orchestrate incident triage and reporting—just the sort of thing respondents to the SANS SOC Survey say is one of their biggest challenges. Dropzone AI delivers findings and recommends mitigation steps, but doesn't take action on its own, because human review still matters. SOC Survey respondents said they are struggling with inadequate staffing, and Dropzone AI eases the load on analysts with dependable, pretrained AI, using a patented large language model. Dropzone AI's systems is pretrained on security, with guardrails to prevent alerts based on false information. It knows what steps a human analyst would take, and consolidates inputs from various information sources in various formats to create actionable reporting.

Key Findings

The survey highlighted that the lack of automation and orchestration is the biggest barrier in SOCs, with 71 responses out of 388 noting this issue. Dropzone AI's autonomous SOC analyst directly addresses this challenge by automating repetitive and time-consuming SOC tasks. This not only reduces the need for high staffing levels but also helps bridge the gap caused by a lack of skilled staff. By handling routine tasks, Dropzone AI allows your team to focus on more complex and strategic issues, enhancing overall SOC efficiency.

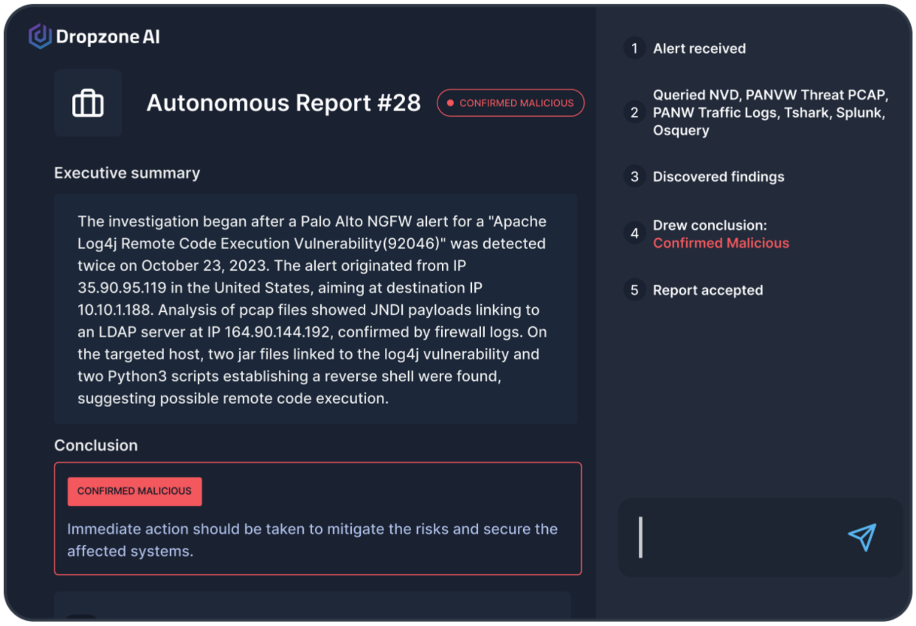
AI/ML technologies received lower satisfaction scores, with "Analysis: AI or machine learning" GPA dropping from 2.17 to 1.99 from 2023 to 2024. While there is general dissatisfaction with AI/ML technologies because they simply don't work, Dropzone AI disrupts current technologies. This is because our approach focuses on practical, real-world applications that directly improve SOC operations. Dropzone AI's autonomous SOC analyst is designed to deliver tangible improvements in efficiency and effectiveness, addressing the pain points highlighted by the survey.

High staffing requirements and a lack of skilled staff are significant barriers, with combined responses indicating this as the top issue. By automating routine SOC tasks, Dropzone AI helps reduce the manual workload, easing staffing pressures. This allows your team to focus on higher-value tasks, which can lead to increased job satisfaction and better retention rates. The job of the SOC gets bigger every day. The budget often does not. Attracting and retaining experienced staff is the eternal struggle for SOC managers, while analysts strive to build their knowledge and protect organizational assets. Fortunately, powerful tools are available to help bridge the gap between what you have and what you need.

Dropzone AI is easy to integrate, and takes less than an hour to adapt itself to your Environment—SIEM, EDR, firewalls, and so forth, as well as other security products that may be deployed. No need to write custom code, generate configurations, or create playbooks. It tests connections so it knows where to get data, then begins programmatically investigating everything it finds in the environment. The system also eliminates false positives by detecting whether a given piece of evidence actually poses a threat to the environment. For example, if nothing in your environment uses the log4j logging library, then the log4j vulnerability doesn't need to take up your analysts' time. See Figure1.

Investigation reports from Dropzone AI are easy to scan and understand, prioritized by severity, with an executive summary and recommended mitigation steps. Because many organizations are making do with less experienced analysts, and because everyone benefits when analysts learn, Dropzone AI also has a natural language chatbot. See Figure 2.

Analysts can ask questions in ordinary language and receive reliable answers, with links to further resources to create deeper understanding. Dropzone AI learns as well, from the feedback and context it gains as it spends time monitoring your environment. The longer you use it, the more time it saves your SOC.



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

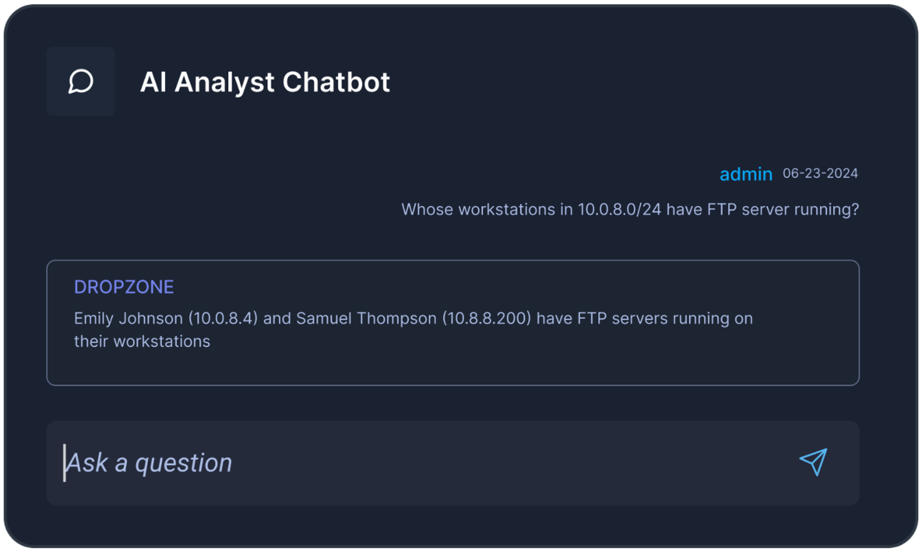
2 Queried NVD, PANVW Threat PCAP, PANW Traffic Logs, Tshark, Splunk, Osquery

3 Discovered findings

4 Drew conclusion: Confirmed Malicious

5 Report accepted

Figure 1. Example of Investigation Report Summary



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

Ask a question

Figure 2. Dropzone's Natural Language Chatbot

If you're looking for a system to help you manage staffing challenges in the SOC, visit **https://www.dropzone.ai**

Note that SANS Product Briefings do not represent a SANS endorsement of a sponsor or its products, but rather an overview of its offerings and their capabilities.