Dropzone AI

SANS | Research Program

PRODUCT BRIEFING

Elevating SOC Efficiency and Efficacy with Dropzone AI

Insights from the 2025 SANS Institute AI Survey

September 2025

Cybersecurity teams face a stark reality when implementing artificial intelligence: The technology's promise often collides with operational constraints. AI models require pre-training and context to function effectively, yet many security teams lack the resources or know-how to embed that knowledge. The opaque nature of AI algorithms creates trust barriers, leaving analysts uncertain about automated decisions that could determine their organizations' security posture. Meanwhile, cyber threats evolve rapidly, requiring AI systems that adapt in real time while avoiding the cascade of false positives that can paralyze security operations. Security leaders must navigate this tension between AI-driven automation and the irreplaceable value of human expertise and ethical oversight.

Dropzone AI: The Autonomous AI SOC Analyst

Dropzone AI purpose-built the Dropzone AI SOC Analyst to transform how security operations centers (SOCs) handle alert overload. The platform targets enterprise cybersecurity organizations that consistently face resource constraints and staffing shortages. These teams struggle with staffing and analyst fatigue, unable to adequately triage or investigate the constant stream of security notifications. Dropzone AI directly attacks the core challenge: reducing mean time to respond (MTTR) and mean time to acknowledge (MTTA) by expanding alert coverage and eliminating queue backlogs.

Dropzone AI automates the repetitive, time-consuming work that drains human resources, enabling teams to multiply their impact and shift from reactive firefighting to proactive security initiatives. The system completes investigations in three to 10 minutes—compared to the 25-minute average for human analysts—delivering dramatic improvements in speed and efficiency. More critically, it ensures comprehensive alert coverage, thoroughly investigating low- and medium-severity alerts that resource-constrained teams often ignore (see Figure 1).

Key Findings

- AI systems/agents generating many false positives, leading to alert fatigue, is a significant concern for 66% of survey respondents.
- AI struggles to identify new threats and outlier indicators due to data quality and training limitations, with 58% of respondents citing AI effectiveness as heavily dependent on data quality and relevance, and 48% noting AI's inability to fully grasp context.
- Limited adoption of AI in core incident response and investigation is evident, as only 26% of organizations use AI for responding to incidents and 33% for investigating, despite 50% generally using or planning to use AI in cybersecurity.
- Difficulty understanding and trusting AI decisions due to lack of transparency is a primary challenge, with customers appreciating human-in-the-loop review and transparent reasoning.
- Under-resourced and understaffed SOCs face alert overload and staffing challenges, highlighting the need for AI to reduce workload and enable staff to focus on strategic initiatives.

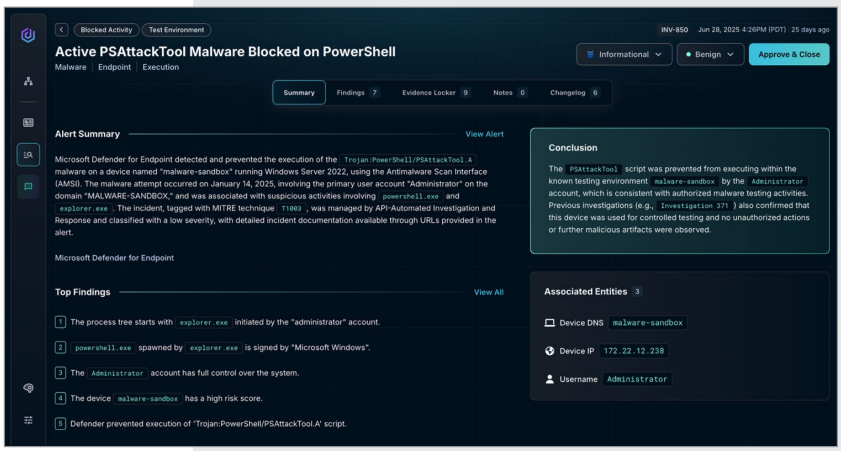

Figure 1. Dropzone AI's AI SOC Analyst: Expertly Handling Tier 1 Alert Triage and Investigation

Dropzone AI's Context Memory feature enables the AI to accumulate institutional knowledge about specific environments during alert investigations. The system stores information gathered during investigations and incorporates user feedback to continuously improve its understanding. When users modify investigation conclusions, Dropzone AI queries the reasoning and adapts accordingly. The platform also scans ticketing systems for additional context while allowing direct user input. This Context Memory operates as a retrieval-augmented generation (RAG) database, dramatically enhancing the AI's ability to deliver relevant, accurate responses during investigations.

Dropzone AI prioritizes transparency and human oversight, directly addressing skepticism around black-box AI solutions. The platform provides complete visibility into investigative reasoning, explicitly displaying all questions formulated and queries executed against systems including EDR, SIEM, Microsoft Office Exchange, Google Workspace, and JIRA. This transparency builds trust and empowers security professionals to verify AI conclusions with full confidence.

The solution features distinctive integrations that extend investigative capabilities beyond traditional security tools. Dropzone AI connects with calendaring systems like Google Calendar and Microsoft Exchange to gather contextual intelligence—such as travel schedules—that inform investigations of unusual login attempts. The platform integrates with Slack and Microsoft Teams to conduct autonomous user interviews for alerts involving phishing emails or suspicious logins, collecting real-time user input that enriches investigations.

Bridging the AI Trust Gap in Security Operations

Security leaders' hesitation to fully embrace AI reflects legitimate concerns identified in the 2025 SANS AI Survey and practical deployments:

- **Combating false positives and alert fatigue—**The Dropzone AI platform investigates and triages incoming alerts, determining threat legitimacy while providing explicit reasoning, dramatically reducing the time human analysts waste on false positives.
- **Enhancing contextual understanding and data quality—**By continuously learning environmental specifics and incorporating user feedback, Dropzone AI's Context Memory feature provides the rich context necessary for accurate analysis (see Figure 2). Its RAG database implementation directly addresses survey recommendations for enhanced AI responses.
- **Deepening AI adoption in incident response—** Dropzone AI transcends simple enrichment by functioning as a complete AI SOC analyst that actively investigates and triages incidents, pushing AI into deeper, more impactful roles where human judgment traditionally dominates.
- **Fostering transparency and trust in AI—** Dropzone AI's commitment to complete investigative transparency and human-in-the-loop review, consistently praised by customers, ensures security professionals understand and can verify AI logic, which builds essential operational trust.
- **Amplifying under-resourced SOC teams—**Through intelligent automation of repetitive tasks, Dropzone AI empowers under-resourced SOCs and small teams to redirect efforts from reactive alert analysis to proactive security measures, effectively multiplying their impact without proportional headcount increases.

Empower Your SOC. Transform Your Security Operations

Security operations constrained by alert overload and limited resources require a fundamental shift in approach. Dropzone AI transforms SOC capabilities by delivering unparalleled efficiency, transparency, and contextual understanding. To experience Dropzone AI autonomously investigating security alerts, try the self-guided demo at **www.dropzone.ai/self-guided-demo** or forward a suspicious email to **scan@try-dropzone.ai** for a tailored analysis report in minutes.

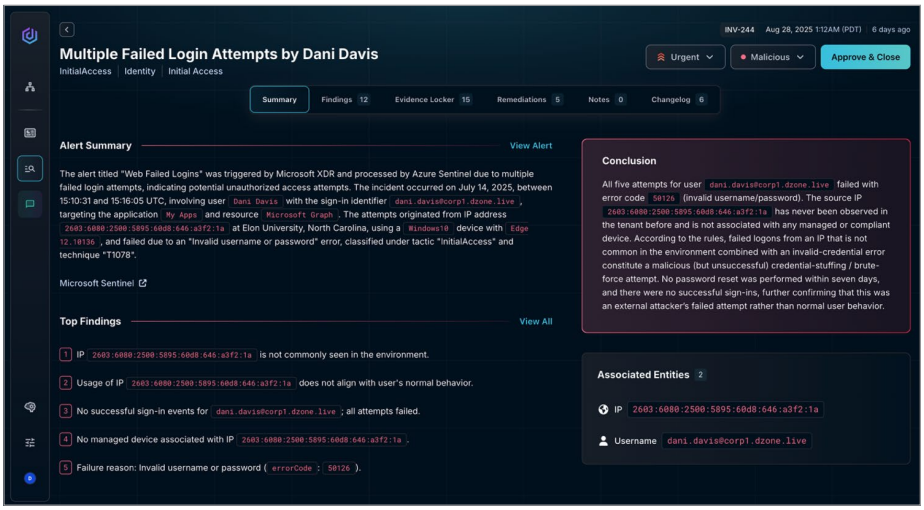

Figure 2. Accelerating Alert Resolution with Contextual Information