Dropzone AI

A Fighting Chance for the SOC: How Assala Energy Scaled Security Operations with AI

ASSALA ENERGY

Company Profile

Assala Energy is an oil exploration and production company focused on safely increasing production for mature oil and gas assets in Africa. With core operations in Gabon, Assala is headquartered in London, UK, where a lean global IT Security team protects the company's diverse and extended network.

Assala Energy's information security team is tasked with protecting this network from a variety of threats—cyber criminals, hacktivists, nation-state actors—that could impair operations. The problem was that threats were growing faster than the ability of the lean team to keep up.

"We need to know quickly when there's a security issue because the risk to the business is real," says Kevin Turnbull, Global IT Director at Assala Energy. "We're always on the lookout for a smarter way to sift through noise, find the signal faster, and help our analysts—especially new hires—spend time on the alerts that matter."

> Simply adding more people to the team is not a scalable solution; using augmented AI to enhance your team's capabilities is the way forward.
>
> **Kevin Turnbull**
> Global IT Director

Challenges

Assala Energy's security team was looking for a solution to the following challenges:

Scalability of the Team	The security team at Assala Energy recognized an opportunity to enhance their operational efficiency. Knowing their lean team faced a high volume of daily alerts, they sought a significant step forward in their triage capabilities to keep pace and maintain robust security.
Identification of True Positives	Assala Energy's security team wanted a way to reduce the time spent triage false positives and allow them to focus their efforts on true positives.
Low Risk Tolerance	As the company's operations rely on the availability of IT systems, the security team at Assala Energy needs a detection and response posture that minimizes the risk of downtime.
Onboarding New Hires	Assala Energy's security team needed a way to streamline the onboarding process for new analysts while ensuring a consistently high standard across investigations.
Alert Enrichment	When faced with a high volume of daily alerts, manually researching every entity to confirm or deny malicious activity consumed a lot of the team's time. A tool that automates this investigation element would allow analysts to make quicker, informed decisions and dedicate their efforts to more crucial aspects of an incident.

See what Assala Energy gained by deploying Dropzone AI, in their own words:

> Dropzone's investigations truly surprised us —
> the AI consistently took proactive steps to enrich alerts.

> With Dropzone, we don't get "This is a problem," we get "This is a problem and here's why."

Kevin Turnbull
Global IT Director

Selection & Implementation

At an industry event, Global IT Director Kevin Turnbull was captivated by the Dropzone AI team. He recalls, "When I discovered Dropzone's AI SOC analyst, it immediately struck me as a game-changer that could provide my SOC with a decisive edge," says Turnbull. "Simply adding more people to the team is not a scalable solution; using augmented AI to enhance your team's capabilities is the way forward."

Assala Energy's pilot of Dropzone AI quickly demonstrated its value, offering immediate and clear benefits in terms of time saved and operational efficiency through the AI SOC analyst.

Assala Energy benchmarked Dropzone AI's investigations with the analysis from their existing toolset and was impressed with the consistency and depth of the analysis. "We were surprised at the Dropzone investigations—extra steps that we necessarily wouldn't have taken, the AI took."

Assala Energy's information security team spends their time in Microsoft Sentinel, where they collect security alerts for analysis. Dropzone AI connected with Sentinel, augmenting their existing workflow.

Benefits Realized with Dropzone AI

Efficiency of Alert Triage

Assala Energy's vital human SOC team now boasts **enhanced efficiency in alert triage** thanks to AI augmentation. Dropzone AI empowers their lead SOC team to effectively handle and prioritize thousands of daily alerts.

24/7 SOC Coverage

Dropzone AI works round-the-clock and never tires or takes a lunch break, providing Assala Energy with uninterrupted vigilance. The AI SOC analyst can also investigate multiple alerts in parallel and so can help the SOC keep up with spikes in workload.

5x Faster MTTR

Dropzone AI's investigations help analysts know about real threats faster and give them a tremendous head start on response. "With Dropzone, we don't get 'This is a problem,' we get 'This is a problem and here's why," says Turnbull.

More Value From Existing Security Tools

Assala Energy uses many different security tools for cloud, endpoint, network, and identity. While these alerts are sent to Microsoft Sentinel for correlation, Dropzone AI takes the analysis much further by autonomously investigating them. Each alert from these tools is thus given a full report with conclusion, findings, and evidence.

Key Performance Indicators (KPIs) and Results:

- **100%** of incoming alerts investigated
- **Reduced false positives** flagged for manual review by 70%
- **Cut triage time per alert** from ~25 minutes to under 5 minutes for common scenarios
- **Quick integration** with Microsoft Sentinel and existing security tools
- **Faster onboarding** of new security analysts

Responsive Vendor Team

Equally as important as the technology itself is the close partnership that Assala Energy has with the Dropzone AI team. Dropzone was able to prioritize an integration with Palo Alto Networks Next-Generation Firewall to meet Assala Energy's requirements.

> The Dropzone AI team won our trust in terms of responsiveness and their planned roadmap. We are looking for partners and feel that Dropzone fits that role.
>
> **Kevin Turnbull**
> Global IT Director

Rapid Pace of Product Enhancement

The Assala Energy security team has been impressed with the rapid progress of the Dropzone AI product. For example, a recent AI Interviewer feature reaches out to users to confirm details needed to complete investigations.

"The pace of development of the product is phenomenal, and we are excited about the AI agent having the ability to reach out to our users, checking on security alerts like 'impossible travel,'" says Turnbull.

Our AI Analysts Never Sleep, So You Can

Dropzone AI is the leading AI SOC Analyst, trusted by SOC teams to automate tedious, repetitive tasks. It autonomously investigates alerts 24/7, integrates with existing security tools, and delivers decision-ready investigation reports. Designed to eliminate alert fatigue and accelerate incident response, Dropzone AI frees SOC teams for higher-level work, enabling organizations to focus on real threats without adding headcount. No playbooks, code, or prompts required. Learn more by visiting www.dropzone.ai.

Request a Demo

Dropzone AI