Dropzone AI

Cyber Defense Army (CDA) Builds Custom-Fit MDR Services with Dropzone AI

Company Profile

Cyber Defense Army (CDA) is a managed security services provider specializing in protecting small and mid-sized businesses in highly regulated industries. Encapsulating decades of experience in cybersecurity, CDA's vCISO services provide clients with the benefits of an in-house CISO at a fraction of the cost. CDA helps clients build a comprehensive security program by assessing risk, understanding security posture, developing a plan, and executing the plan with ongoing optimization.

Part of CDA's services include managed detection and response. Unlike traditional MSSPs, CDA focuses on providing customized alert triage and fast, actionable investigation outcomes for its clients.

> Humans are inconsistent. Dropzone is not. It gives you repeatable quality, day or night.

Evan Morgan
Founder, CDA

Challenges

Cyber Defense Army was looking for a solution to the following challenges:

Balancing Customization with Scale	CDA's mission is to bring the sophistication of enterprise SOCs to clients who can't afford to build one themselves. To do this, CDA needed a way to deliver deeply customized alert triage at scale.
Variability in Investigation Quality	Human analysts—especially in a 24/7 MDR setting—bring variability. Quality depends on who's on shift, how fatigued they are, and how much they know about the environment. CDA needed a way to ensure consistently high-quality alert investigations across clients.
Tool and Environment Complexity	Each client has a different tool stack. CDA needed a solution that could conduct investigations using disparate sources, including business systems like Microsoft Entra ID or Google Workspace.

Selection & Implementation

CDA realized the potential of the technology within Dropzone AI to elevate security operations teams.

"Dropzone AI equips small- and medium-sized businesses with enterprise capabilities in terms of detection and response," says Evan Morgan, Founder at Cyber Defense Army (CDA). "Extremely few organizations have the resources to staff a full in-house SOC, but with Dropzone AI every security team can now see the benefits of rapid and fast alert triage and investigation."

Key differentiators that led to CDA's selection of Dropzone AI:

01	**Supports custom alerts**	Unlike typical MSSPs, CDA delivers custom detections for each client without compromising scale. Dropzone AI investigates every alert—no matter how tailored—expertly in minutes, every time.
02	**Investigation depth**	Dropzone AI remembers environmental and business details like a seasoned in-house analyst.
03	**Context memory**	Dropzone AI went beyond the automation that traditional SOAR tools offered, reasoning through complex signals and correlating data across systems.

Benefits Realized with Dropzone AI

Customized MDR at Scale	Dropzone AI allows CDA to deliver highly customized alert triage and investigation per client—something most MSSPs sacrifice for standardization. CDA analysts can create environment-specific detections, and Dropzone automatically knows how to investigate them with precision.
Consistency and Trust	Every Dropzone AI investigation comes with a full report, complete with detailed findings and evidence. Clients and CDA analysts alike benefit from high-fidelity, audit-ready output. "Humans are inconsistent. Dropzone is not," says Morgan. "It gives you repeatable quality, day or night."
Speed and Efficiency	Dropzone AI accelerates CDA's response by automatically triaging alerts and surfacing true positives fast. CDA is authorized to contain threats, so the combination of Dropzone plus the managed service ensures response within minutes, not hours. Dropzone also serves as an ad hoc investigation assistant for CDA analysts, offering quick enrichment from multiple threat intel feeds and correlating across log sources.
Continuously Improving Accuracy with Context Memory	While Dropzone AI works out of the box, CDA invests time in training the system to maximize value. Context memory allows Dropzone to improve with each piece of feedback and details learned during investigations.

See what Cyber Defense Army gained by deploying Dropzone AI, in their own words:

> Extremely few organizations have the resources to staff a full in-house SOC, but with Dropzone AI every security team can now see the benefits of rapid and fast alert triage and investigation.

Evan Morgan
Founder, CDA

Key Performance Indicators (KPIs) and Results:

- **80% of alert triage** now fully automated
- **Consistent investigations** across all clients, regardless of analyst or shift
- **Detection to containment** in minutes, not hours
- **Reduced fatigue** for Tier 2 analysts
- **Rapid enrichment** from built-in threat intelligence feeds

Noise Eliminated

By offloading false positive triage to Dropzone AI, CDA eliminates a major time sink that can disrupt SOC operations. During alert spikes, the entire team stays focused—no need to pull in staff from other areas like vulnerability management to keep up with alert volumes.

> AI will help all defenders, but especially lift up SMBs. Dropzone AI gives smaller organizations enterprise-grade detection and response capabilities without enterprise cost.

Evan Morgan
Founder, CDA

Reinforcements have arrived

Dropzone AI's agents make SOCs fast, scalable, accurate, and proactive. With Dropzone AI autonomously handling routine Tier 1 alert triage, organizations can spend less time on reactive security and more time on proactive security. The Dropzone AI SOC Analyst replicates the techniques of elite analysts and is trusted by more than 100 enterprises and MSSPs, including CBTS, Pipe, UiPath, Zapier. Learn more at www.dropzone.ai.

Request a Demo

Dropzone AI