AI Threat Intel Analyst and AI Threat Hunter

Autonomous response to emerging threats with federated threat hunts

Security teams have always wanted to hunt proactively. But thorough threat intel analysis and hunting demands time, expertise, and cross-tool investigation that most teams can't sustain alongside their daily workload. Until now, continuous hunting was a luxury only the largest, best-resourced SOCs could afford.

Dropzone AI's Agentic SOC makes proactive threat hunting possible for every organization. The AI Threat Intel Analyst monitors threat intel sources, extracts TTPs and IOCs, and creates hunt packs that The AI Threat Hunter executes autonomously, 24/7. Hunt reports also surface non-attack insights—misconfigurations, shadow IT, and vulnerabilities—even when no active attacker is found.

Benefits

Search at scale

Federated search across all your tools casts a wide net for every data source the hunt requires—SIEM, EDR, cloud, identity—simultaneously. A single search can return up to half a million rows of telemetry.

Filter at scale

AI Threat Hunter slices that data in thousands of ways in parallel using data science and LLMs, boiling results down to the anomalies that matter. This is computing doing what computing does best—processing data at a scale no human analysis workflow can match.

Investigate at scale

Each lead typically takes 10-20 minutes of manual analyst time. AI Threat Hunter pursues dozens of deep-dive investigations in parallel to confirm whether anomalies represent real threats.

Hunt Categories

Emerging Threats

Hunting for indicators of compromise from just-released intelligence before they become widespread attacks.

Threat Actors

Intelligence-driven hunts that map your logs against the known behaviors of groups like Scattered Spider and Lazarus.

Vulnerabilities

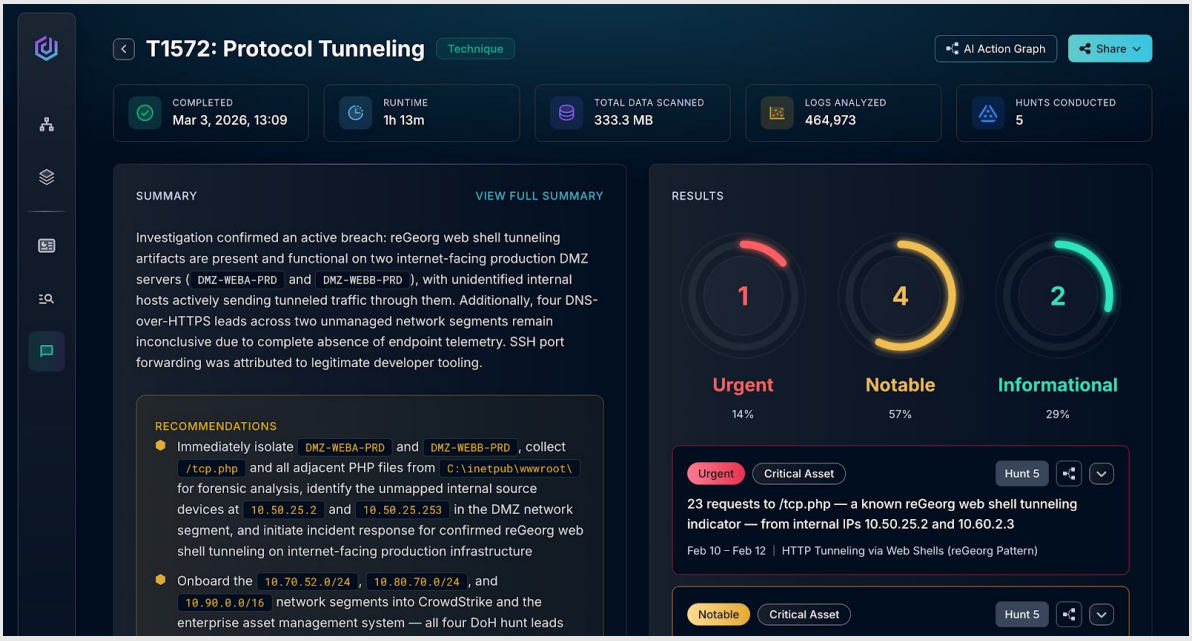
Going beyond scanning to hunt for evidence of active exploitation of critical CVEs within your environment.

ATT&CK Techniques

Lateral movement, persistence, living-off-the-land—the techniques that live below the detection threshold.

Operational Anomalies

Detecting abuse of legitimate business logic, from MFA fatigue attacks to unusual administrative overrides.



RUN HYPOTHESIS-DRIVEN, FEDERATED HUNTS ACROSS YOUR ENVIRONMENT

How It Works

Threat Landscape Monitoring
Continuously scan 2,500+ threat intel sources: NVD, GitHub Advisory Database, security blogs, social media feeds, and more. Filters for intelligence relevant to your industry and technology stack.

Threat Intel Operationalization
Extracts indicators of compromise (IOCs) and behavioral techniques (TTPs) and assesses relevance to your environment. Creates hunt packs with hypotheses and queries ready for autonomous federated hunts across your SIEM, EDR, and cloud environments.

Every Hunt Is a Glass Box You Can Audit
Every hypothesis, query, and finding is logged and visible. No black-box decisions. When coaching directives influence a hunt, the system attributes them explicitly.

Vendor-Agnostic Hunts Across Your Entire Stack
AI Threat Hunter queries your SIEM, EDR, cloud, and identity tools via API—the same way your analysts do. Federated hunts across 90+ integrations mean every hunt draws from your full security context, not just one vendor's ecosystem.

Part of the Agentic SOC, Not Standalone Agents
Intelligence triggers hunting. Hunting triggers investigation. Works autonomously without requiring human prompting. AI Threat Hunter operates in a closed loop with AI Threat Intel Analyst and AI SOC Analyst. Agents collaborating at machine speed, 24/7.

About Dropzone AI

Dropzone AI weaponizes LLMs for cyber defenders, delivering the Agentic SOC: AI agents that collaborate 24/7 to overmatch attackers. Dropzone is ready to go on Day 1 and integrates into your existing tools. AI agents start work immediately to investigate alerts, respond to emerging threats, and proactively hunt attackers. Dropzone works with enterprises and MSSPs including ECS, Avalara, UiPath, and Zapier, and is actively protecting over 300 companies. Learn more at www.dropzone.ai