



How UiPath Extended Its Agentic SOC with AI SOC Analysts



Company Profile

UiPath operates a globally distributed, AI-forward security organization built on an automation-native model. Its security team integrates detection and response, engineering, threat intelligence, governance, and automation into a unified system designed for scale.

Powered by its Maestro™ agentic platform, UiPath executes system-driven security workflows that reduce reliance on manual processes. This approach enables consistent investigations, structured triage, and measurable outcomes—while allowing analysts to focus on higher-value work like detection strategy and workflow optimization.

Within this model, adopting an AI SOC analyst was a natural extension of UiPath’s broader effort to continuously improve how security operations are executed.

Dropzone fit naturally into our agentic SOC strategy. It brings structured reasoning to the front of the funnel, so our analysts can stay focused on the work that actually advances our security posture.

Michael Viton
Senior Director of Information Security

Challenges

UiPath’s SOC was already highly automated and mature. The challenge was not replacing manual work, but optimizing how intelligence flows through an agentic system:

Signal-to-Noise Management in Cloud Environments

Even with advanced detection engineering and automation, complex cloud environments generated high alert volumes. A consistent, scalable way to triage and investigate lower-priority alerts was required.

Maintaining Investigative Rigor at Speed

UiPath needed faster decision-making on the front lines, but without sacrificing reasoning quality, consistency, or defensibility.

Protecting High-Value Analyst Workflows

Low-priority alerts risked consuming attention that should be directed toward advanced investigations, detection engineering, and system improvements.

Ensuring System-Wide Continuity

Any solution needed to integrate cleanly into UiPath’s Agentic SOC platform, preserving context across escalation workflows and avoiding rework.

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



Dropzone gives us fast, structured triage decisions without sacrificing analytical rigor. That's critical in a high-volume cloud environment.

Dropzone contributes to a continuous learning loop. What gets escalated, resolved, and fed back improves the entire system—not just a single workflow.



Michael Viton, Senior Director of Information Security

Selection & Implementation

UiPath sought an AI SOC Analyst product that aligned with its broader agentic security architecture.

Specifically, the team was looking for a solution that could expertly use its existing SIEM, EDR, and cloud tools to deliver structured, defensible triage decisions as part of the larger UiPath Agentic SOC platform.

Dropzone AI was deployed as the frontline reasoning layer for alert triage and investigation for UiPath:

- 1 Alerts enter UiPath's security pipeline
- 2 Dropzone AI uses existing security tools deployed at UiPath to perform autonomous investigation and triage
- 3 Lower-complexity alerts are resolved with structured reasoning
- 4 Higher-risk cases are escalated into the UiPath Agentic SOC platform
- 5 Full investigative context is preserved during escalation
- 6 Outcomes from advanced investigations are fed back into Dropzone AI

This creates a closed-loop system, where AI components continuously reinforce each other and improve over time.

Key Performance Indicators (KPIs) and Results:

86% reduction in false positive alerts

700+ analyst hours saved over six months

More than 2,000 pieces of context memory added over six months to improve investigation accuracy

A System-Level Approach to AI in the SOC

For UiPath, Dropzone plays a critical role in a continuously improving agentic system. Dropzone's AI SOC analyst ensures that frontline signal is handled cleanly, decisions are made consistently, and human investigative workflows remain focused where they deliver the most value.



Dropzone protects our analysts' time. It handles the work that should be automated so humans can focus where judgment really matters.

Michael Viton, Senior Director of Information Security



Benefits Realized with Dropzone AI



Structured, High-Confidence Triage at Scale

Dropzone delivers consistent, defensible decisions at the front of the funnel, improving both speed and analytical rigor.



Cleaner Signal Handling Across the SOC

By resolving lower-complexity alerts early, Dropzone reduces noise and ensures that downstream workflows focus on meaningful threats.



Preserved Context Across Investigations

Escalated cases retain full investigative context, enabling UiPath's Agentic SOC platform to operate without duplication or rework.



Continuous Learning Across Systems

Feedback loops between Dropzone and UiPath's platform strengthen decision-making over time, contributing to a continuously improving security system.



Improved Allocation of Human Expertise

Analysts spend less time on repetitive triage and more time on detection strategy, workflow optimization, and high-value investigations.

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