Blast Radius Analysis for Phishing Incidents

Dropzone AI autonomously investigates the full impact of phishing incidents

Phishing detection has improved significantly. Secure email gateways and cloud email security tools can block or flag malicious messages before they reach users. But detection alone doesn't answer the most important question: **what happened next?**

Once an email is confirmed malicious, SOC teams must determine who clicked, whether credentials were entered, if the message spread internally, and whether any systems communicated with attacker infrastructure. This blast radius analysis is critical, but often manual, time-consuming work that slows containment.

Dropzone AI investigates the downstream impact of confirmed phishing emails, replicating expert analyst techniques and delivering impact assessments in minutes.

Benefits

Accelerate containment

Quickly determine whether a malicious email led to user interaction, credential exposure, or device compromise. Reduce the time between detection and response so threats do not linger in your environment.

Give your team time back

Eliminate repetitive manual Tier 2 correlation across email, SIEM, endpoint, firewall, and identity systems. Free analysts to focus on higher-value security work.

Strengthen every phishing investigation

Ensure every confirmed malicious email triggers a consistent, comprehensive impact assessment. Remove variability from the process and increase confidence in containment decisions.

	Human-only SOC	SOC with Dropzone
Human work	Investigations require manual work	Blast radius analysis runs autonomously across tools
Time to impact assessment	Hours	Minutes
Disruption	Escalations are common	Escalations are reduced
Backlog	Phishing backlogs grow during high-volume periods	High volumes of user-reported phishing are handled at scale

How It Works

Detection	Phishing detected by email security or reported by a user.
Investigation	Dropzone AI immediately begins investigation to determine if the alert is malicious, replicating expert techniques.
Blast Radius Analysis	If deemed malicious, Dropzone AI performs blast radius analysis to determine the extent of the incident, such as if the message has spread across mailboxes or if there are signs of credential theft or infection.
Incident Response	Dropzone AI can be configured to take automated containment actions, and escalate to human analysts for further response.

Works With Your Existing Security Stack

- **Enhances detection with automated impact analysis that goes beyond just email**
- **Leverages your existing SIEM, EDR, identity, and network logs**
- **Provides deeper context for faster decision-making**
- **Can trigger automated response actions when desired**

Pricing

An annual contract includes the complete solution, including:

- ☑ Up to 4,000 full investigations per year per AI analyst
- ☑ Unlimited users
- ☑ All available security alert categories
- ☑ All pre-built integrations with your security and data tools
- ☑ Hand-picked threat intelligence and enrichment feeds
- ☑ AI chatbot for ad-hoc investigation
- ☑ Interact with engineers for support
- ☑ 8-hour customer support SLA

Built for Trust

Security
We use a single-tenant architecture and are SOC 2 Type II certified.

Transparency
We provide proof of evidence for every investigation and chat response.

Privacy
We only use your private data for your own investigations, not to train our models.

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