Abnormal

Abuse Mailbox Automation

Available as an Add-On to Abnormal Inbound Email Security

Automatically triage and remediate user-reported phishing emails.

Traditional approaches to managing user-reported phishing emails are highly manual, lack intelligence, and provide limited context. As a result, IT teams and security analysts waste time in a cumbersome and inefficient workflow, missing higher-impact attacks.

Abuse Mailbox Automation automates the user-reported email process.

- Automatically triages and remediates user-reported emails and marks them as malicious, spam, or safe.
- Intelligently locates and removes other unreported emails within the same phishing campaign.
- Enhances visibility into each reported email submission to see the full attack context for each campaign and email.
- Closes the communication loop by automatically sending a follow-up email to inform reporters of the submission outcome and remediation action.
- Integrates with existing end-user phishing reporting buttons, SIEM/SOAR solutions, and ticketing system workflows to enable centralized alerts for SOC analysts.

95%	Reduction in time spent reviewing user-reported emails.
5,000	SOC analyst hours saved annually.
2	Full-time employees freed from handling user-reported email.

The Abnormal Advantage at a Glance

Alleviates bottlenecks. AI-powered detection and automated triage process streamlines your entire user-reported email workflow.

Saves time. Substantially reduces the number of user-reported emails requiring analyst review.

Improves the employee experience. Swifter, personalized response to phishing reports encourages a healthy cybersecurity culture.

Provides holistic insights. Gives enhanced visibility into quantitative metrics, attack summaries, detailed email analyses, and more.

Tame Your Abuse Mailbox.
Request a Demo.

abnormalsecurity.com →