Abnormal SOC Automation

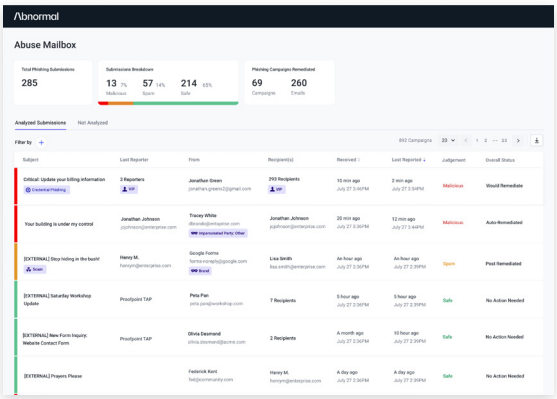
Supercharge your SOC workflows and save time with AI-assisted investigation, auto-remediation, follow-up, and reporting.

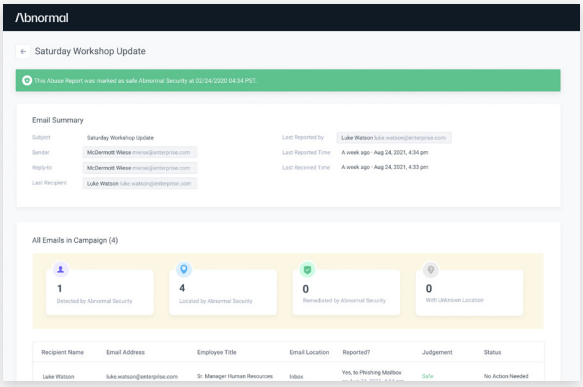
Abnormal provides a frictionless method for user-reported phishing attacks to be submitted, triaged and reviewed. The platform automatically triages phishing attacks and suspicious email submissions using behavioral AI, and then automatically investigates, remediates the entire email campaign, and notifies the reporters of the results. This automation provides security teams with up to an 80% time savings on investigation and reporting.

View All User-Reported Attacks in One Place

Abnormal Abuse Mailbox organizes all user-reported emails, including their original messages and headers, across all Microsoft Office 365 and Google Workspace tenants into a single view.

You can quickly view quantitative highlights of submissions displayed by malicious, safe, and spam messages, as well as remediated campaigns and messages.





Automatically Triage User-Reported Email Attacks

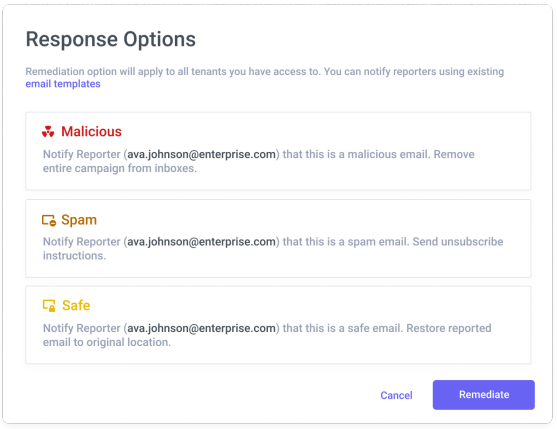
Abuse Mailbox automatically investigates submissions, and if found malicious, gathers other emails within the phishing campaign, removes them, and reports back to the submitter.

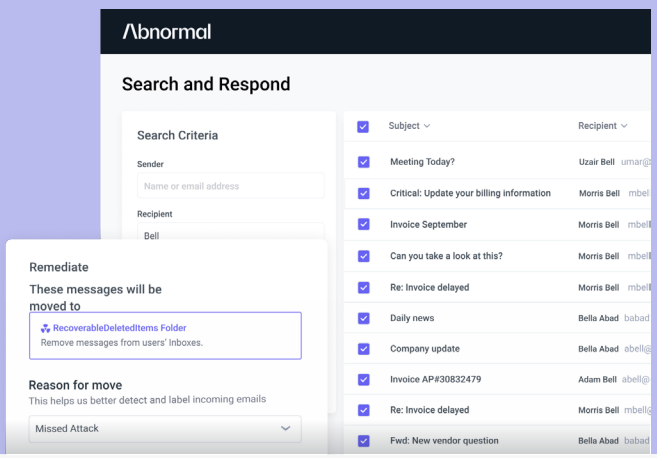
When you submit missed attacks or false positives, a dedicated team of experts investigates them to fix the incident, improve detection efficacy, and provide you with a summary of the steps taken.

Provides Intelligent and Thorough Remediation

Since Abnormal natively integrates with your cloud email service, it scans every email as it is sent, replied to, or forwarded within your email environment.

When an email is found malicious, Abuse Mailbox intelligently gathers all similar and related messages, remediates the entire campaign, and follows up with end users appropriately.





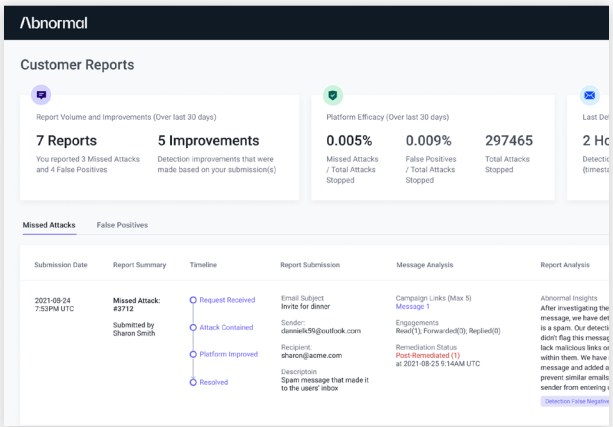
Rapidly Contain Misdirected Email

Find and remediate emails across some or all of your tenants with Abnormal Detection 360° search functionality built for rapid response.

Search for specific emails by sender, recipient, or subject, find emails sent within specific time frames, and then remediate them in bulk. Removing emails and their engagements is necessary when sensitive data is misdirected or if an attack is missed. All search activity is recorded for any audit or compliance requirements.

Track How Abnormal Gets Better Every Day

When you submit missed attacks or false positives, a dedicated team of experts investigates them to fix the incident, improve detection efficacy, and provide you with a summary of steps taken.



Abnormal SOC Automation Key Capabilities

- **Complete Abuse Mailbox Automation**
  Reduce your SOC workload by 80% or more.

- **Automated Remediation**
  Remove email campaigns that are deemed malicious post delivery.

- **Multiple Remediation Options**
  Permanently delete the email, quarantine it, or move it to another folder.

- **Frictionless Abuse Mailbox Reporting**
  Provide end users with an easy method to submit emails for further review.

- **Automated Employee Notification**
  Provide support notifications for safe and malicious email, directly to the user who reported it.

- **Collects and Categorizes**
  View the entire email attack campaign in one central location.

- **Search and Respond**
  Use global, multi-tenant email delivery search and removal to find and remediate all attacks.

- **Comprehensive Dashboards**
  View all reports and documentation within centralized dashboards.

- **Integrate with Third-Party Solutions**
  Post-remediate attacks detected by Proofpoint TAP Alerts and other solutions.

- **Seamless Integration with your Existing Security Stack**
  Integrate with ticketing systems such as ServiceNow and SIEM/SOAR tools including Splunk, LogRhythm, QRadar, Demisto, and more.

- **Platform Independent**
  Integrates with both Microsoft Office 365 and Google Workspace.

- **Detection 360°**
  Submit detection enhancements for false negatives and false positives for full feedback from Abnormal, and then view and filter these reports and their statuses.

Fully Automate Your SOC Workflows

Integrate with SIEM, SOAR, ITSM, and IAM solutions to enrich security insights and orchestrate workflows.

SIEM

Augment your SIEM with metadata and risk scores for better attack correlation.

splunk> Radar®

SOAR

Trigger playbooks when users engage with bad email or compromised accounts.

paloalto NETWORKS ANY RUN INTERACTIVE MALWARE ANALYSIS

CORTEX XSOAR BY PALO ALTO NETWORKS SWIMLANE

ITSM

Create tickets for compromised accounts or when users engage with bad emails.

servicenow

Secure Email Gateways

Trigger automated post-delivery protection when gateways send alerts on missed attacks.

proofpoint.

Phishing Training

Allow emails for training to pass inspections, and present reports on user engagement.

COFENSE KnowBe4 Human error. Conquered.

Identity Access Management

Log in to Abnormal via SSO, and to provide data to better detect account takeover attempts.

okta DUO onelogin

If Abnormal doesn't have the integration you need for your security stack, our bi-directional API-based architecture helps you set up your own custom integrations quickly and simply.

Try Abnormal SOC Automation Today

Integrate within minutes via one-click API, without any disruption to mail flow. No changes to your email configuration or custom policies required.

www.abnormalsecurity.com/risk →