

Abnormal SOC Automation

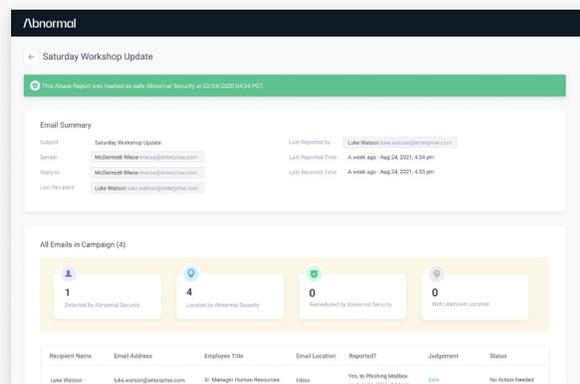
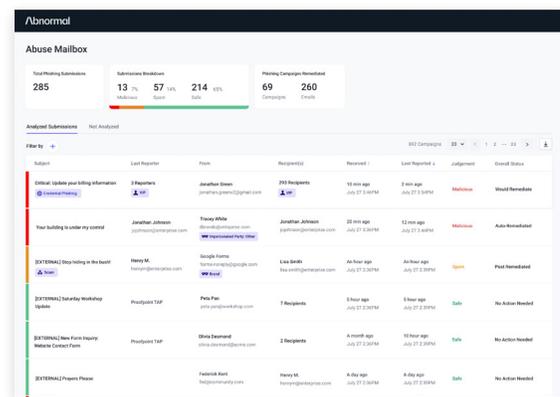
Supercharge your SOC workflows and save time with AI-assisted investigation, auto-remediation, follow-up, and reporting.

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.

Response Options

Remediation option will apply to all tenants you have access to. You can notify reporters using existing [email templates](#)

Malicious

Notify Reporter (ava.johnson@enterprise.com) that this is a malicious email. Remove entire campaign from inboxes.

Spam

Notify Reporter (ava.johnson@enterprise.com) that this is a spam email. Send unsubscribe instructions.

Safe

Notify Reporter (ava.johnson@enterprise.com) that this is a safe email. Restore reported email to original location.

Cancel Remediate

Abnormal

Search and Respond

Search Criteria

Sender
Name or email address

Recipient
Bell

<input checked="" type="checkbox"/>	Subject
<input checked="" type="checkbox"/>	Meeting Today?
<input checked="" type="checkbox"/>	Critical: Update your billing information
<input checked="" type="checkbox"/>	Invoice September
<input checked="" type="checkbox"/>	Can you take a look at this?
<input checked="" type="checkbox"/>	Re: Invoice delayed
<input checked="" type="checkbox"/>	Daily news
<input checked="" type="checkbox"/>	Company update
<input checked="" type="checkbox"/>	Invoice AP#30832479
<input checked="" type="checkbox"/>	Re: Invoice delayed
<input checked="" type="checkbox"/>	Fwd: New vendor question

Remediate

These messages will be moved to

Recoverable/Deleted/Items Folder

Remove messages from users' inboxes.

Reason for move

This helps us better detect and label incoming emails

Missed Attack

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

Customer Reports

7 Reports

You reported 3 Missed Attacks and 4 False Positives

5 Improvements

Detection improvements that were made based on your submission(s)

0.005%

Missed Attacks / Total Attacks Stopped

0.009%

False Positives / Total Attacks Stopped

297465

Total Attacks Stopped

2 Hc

Detectic (times)

Submission Date	Report Summary	Timeline	Report Submission	Message Analysis	Report Analysis
2021-08-24 7:53PM UTC	Missed Attack: #3712 Submitted by Sharon Smith	<ul style="list-style-type: none"> Request Received Attack Contained Platform Improved Resolved 	<p>Email Subject: Invite for dinner</p> <p>Sender: daniel@59@outlook.com</p> <p>Recipient: sharon@acme.com</p> <p>Classification: Spam message that made it to the users' inbox</p>	<p>Campaign Links (Max 5) Message 1</p> <p>Engagements: Block(1), Forwarded(3), Replyed(0)</p> <p>Remediation Status: Post-Remediated (1) at 2021-08-25 5:14AM UTC</p>	<p>Abnormal Insights: After investigating the message, we have det it is a spam. Our detect didn't flag this messag lack malicious links or w/other them. We have message and added a prevent similar emails sender from coming.</p> <p>View this report</p>



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.

<p>SIEM</p> <p>Augment your SIEM with metadata and risk scores for better attack correlation.</p> <p> </p>	<p>SOAR</p> <p>Trigger playbooks when users engage with bad email or compromised accounts.</p> <p>   </p>
<p>ITSM</p> <p>Create tickets for compromised accounts or when users engage with bad emails.</p> <p></p>	<p>Secure Email Gateways</p> <p>Trigger automated post-delivery protection when gateways send alerts on missed attacks.</p> <p></p>
<p>Phishing Training</p> <p>Allow emails for training to pass inspections, and present reports on user engagement.</p> <p> </p>	<p>Identity Access Management</p> <p>Log in to Abnormal via SSO, and to provide data to better detect account takeover attempts.</p> <p>  </p>

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 →