Abnormal AI

Detection Strategy Guide

April 2025

Product Overview

Identity-based attacks make up 61% of all incidents confirmed by the Expel SOC. Abnormal AI is a SaaS email security product that helps organizations defend against URL, attachment, and cloud-based threats to their inboxes. Abnormal AI stops inbound email threats by detecting and blocking BEC, phishing emails, malware, spam, and more by using threat intelligence and AI-driven technologies.

Expel alerts are produced from Abnormal AI Threats. When a Threat is ingested additional data is gathered via API to provide details and enrichment for analyst triage. This includes the Threat details and attachment details.

Threats are surfaced as Expel alerts when they indicate a potential or active compromise, or when they are correlated with additional suspicious activity that suggests imminent risk to the organization (e.g. a confirmed download of a malicious attachment, a suspicious login following the receipt of a confirmed phishing email, etc.). A potential or active compromise is determined by the status of the threat (not blocked or auto-remediated) and present suspicious indicators in the email such as malicious URLs or attachments.

Threats are not surfaced as lead alerts if they are blocked or remediated by Abnormal AI without being read by the email recipient.

Abnormal AI does not provide full-body email text to Expel SOC analysts, but rather just the alert data provided by Abnormal AI devices. Full-text analysis of user-submitted emails is offered via Expel's Managed Phishing service offering.

When Abnormal AI Threats are promoted to Expel alerts, telemetry from other integrations with Expel is used to correlate activity across the kill chain to paint a more comprehensive picture of an attack outside of just the Email threat surface. For example, if a customer has onboarded an EDR or network security device with Expel, Expel can correlate the observation of a malicious attachment in Abnormal AI with the downloading and execution of that attachment in these integrations. If a customer does not have other integrations onboarded, analysts will use the context from the Abnormal AI alert and Expel-internal enrichment sources (file/IP/URL lookups) to make the best determination of an Abnormal AI alert.

Abnormal AI Expel alerts are also enriched with data from the employee and domain API endpoints to assist with analyst triage. This includes user details, behavior analysis, login history, vendor domain analysis and interaction history.

Auto-remediations – such as removal of malicious emails from user inboxes – are available when organizations integrate Microsoft 365 or Google Workspace with Expel.

Detection Strategy for Email Integrations

Detection

Expel integrates directly with email security providers and uses their data to quickly identify and investigate email and identity-based attacks to:

- generate Expel alerts for investigation
- provide enriched context to a threat
- offer decision support for incident scoping and severity identification

Expel consumes email security provider events through a mix of raw log analysis and security alert processing, which pass through our detection engine to identify signs of post-exploitation activity. When a threat is detected, our automated response bot takes action by enriching evidence fields with first- and third-party threat intelligence. Additional bot actions query a wide span of technologies in order to directly arm analysts with key pieces of investigative information and related events.

Email security providers do not provide full-body email text to Workbench analysts, but rather the alert data provided by the email security providers' devices. Full-text analysis of user-submitted emails is offered via Expel's Managed Phishing service offering. When events are promoted to Expel alerts, additional workflows are used to query to enrich the event with context.

Response

Email alerts are useful to identify and mitigate email threats such as phishing, business email compromise (BEC), and malware. Additionally, telemetry from other integrations with Expel is used to correlate activity across the kill chain to paint a more comprehensive picture of an attack beyond the email threat surface. For example, for an onboarded EDR or network security device, Expel can correlate the observation of a malicious attachment in the email security provider with the downloading and execution of that attachment in these integrations. If no other integrations are onboarded, analysts will use the context from the alert as well as Expel-internal enrichment sources (file/IP/URL lookups) to make the best determination of an alert.

To learn more about our overall approach to detection strategy, see About Detection Strategy in the Help Center.

What We Support for Abnormal AI

To see a comprehensive list of the most up-to-date Expel detection rules, vendor detection rules, opt-in detections, and available DUETs (**d**id yo**u** **e**xpect **t**his) that we support for Abnormal AI, you can visit the Detections page in Workbench or ask your Sales or Support rep for the most recent download.

Supported versions	■ Inbound Email Security
Abnormal AI detection rules support	Yes.
Detection rules written by Expel	Yes.
Auto remediations	Expel does not support executing remediation actions through the Abnormal AI console. Expel will provide recommendations to customers about what remediation actions to take in the case of an incident. The following are examples of common remediation recommendations. ● Reset credentials ● Disable accounts ● Remove email from user inbox
Investigative support through Workbench	Yes. We are able to take the following investigative actions to gather data for triage and investigation of events. ■ Query User ■ Query Domain ■ Retrieve User Login History
Hunting support	No.

Additional Details and Common Questions

DUET

A DUET (**d**id yo**u** **e**xpect **t**his) rule flags certain events as needing an immediate verification or notification, and bypasses the normal internal event triage process. The events subject to DUET rules contain behaviors that are not typically indicative of true security incidents, as they are related to policy violations or *potential* risk.

There are a number of workflows that a DUET may follow. When enabled, the activity will be flagged for investigation and will be routed to you (rather than to us) to take a specified first action. To see the specific DUET rules currently supported for this integration, visit the Detections page in Workbench.

Abuse Mailbox Support

Abuse Mailbox (User Reported Emails) Support is not included as part of the Abnormal AI MDR integration. Support for this feature requires Expel's Managed Phishing service.

Allowed and Blocked Threats

Expel prioritizes alerts that indicate successful or potential compromise. Alerts for blocked and auto-remediated Threats that are unread by the recipient are used for context and investigative support but are not surfaced as lead alerts on their own, except through customer-requested:

Be On the Lookout Alerts (BOLOs) - Custom alerts requested by customers looking for specific threat patterns (e.g. alert any time a specific sender or threat actor is observed in the alert, even if the event is blocked)

Did yoU Expect This Alerts (DUETs) - Custom alerts requested by customers which will immediately create an incident or investigation and assign it directly to the customer, bypassing the Expel SOC's triage (e.g. wanting a certain type of email alerts to be forwarded to an internal team instead of being triaged by the Expel SOC)