Abnormal AI

Detection strategy

April 2025

© 2025 Expel, Inc. EXPEL PROPRIETARY—DISCLOSURE MUST BE AUTHORIZED

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 integrates directly with Abnormal AI and uses its data in two ways to quickly identify and investigate email and identity-based attacks:

- To generate Expel alerts for investigation
- To provide decision support for incident scoping and severity identification

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.

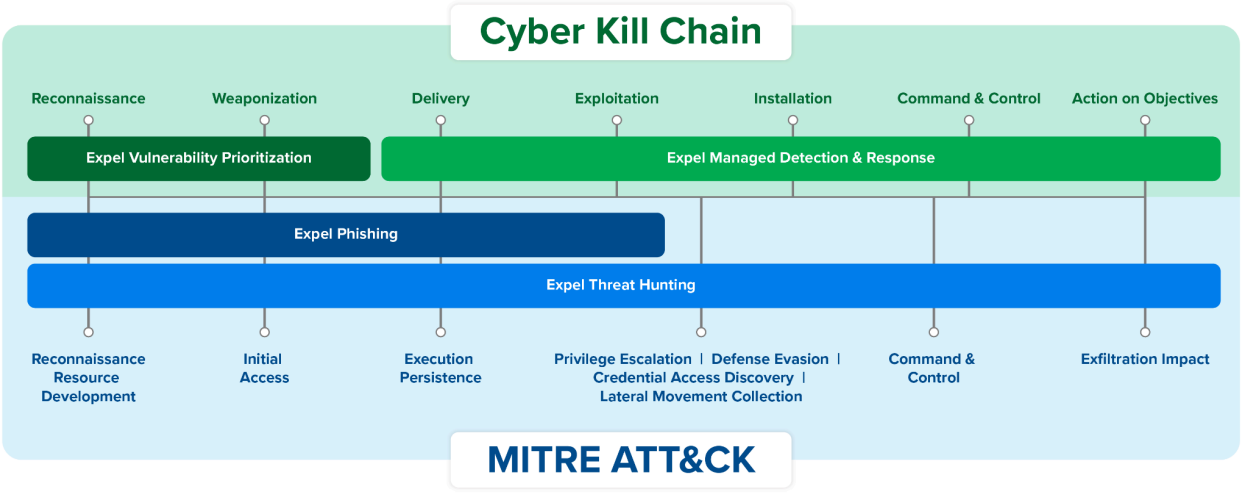
© 2025 Expel, Inc. EXPEL PROPRIETARY—DISCLOSURE MUST BE AUTHORIZED

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

Support quick reference

Supported version	■ Inbound Email Security
Detections written by Expel	Yes
Auto remediation through Workbench	Yes
Investigative support through Workbench	Yes
Hunting support	No

Detection strategy



Expel's Managed Detection and Response strategy is focused on high fidelity initial leads occurring as early in the lifecycle as possible, and correlated with as much data as possible to paint a full picture of an attack's kill chain, with an objective to take quick, decisive action against confirmed threats. Expel uses both the Cyber Kill Chain® and the MITRE ATT&CK® framework to assess lifecycle relevance. Expel's core operational mandate is to identify and respond to true positive alerts representing suspected or confirmed attacker activity and focus detection efforts on the ATT&CK for Enterprise portion of the framework. Attacker activity is an active threat when the email was not blocked/remediated by the security device or when the email was opened by the user.

© 2025 Expel, Inc. EXPEL PROPRIETARY—DISCLOSURE MUST BE AUTHORIZED

Our messaging and productivity strategy....

- Active phishing email threats
- Active email impersonation threats
- Active malware attachment threats
- Active malicious URL threats
- Internal phishing threats
- Suspicious authentications correlated with email threats
- Suspicious MFA activity correlated with email threats
- Suspicious attachment download/execution correlated with email threats

Abnormal AI detection strategy

Severity framework

Expel's detection philosophy is focused on identifying the behaviors indicative of security threats and is designed to adapt to the threat landscape as it evolves. Accordingly, Expel does not consider native vendor-assigned severity as part of detection quality or fidelity. While not a factor in detection evaluation, severity becomes a factor in response. Expel assigns detection severity by considering potential business impact, the likelihood a triggered detection represents a security incident, and our ability to adhere to response benchmarks associated with severity – determined as a function of investigative decision support relevance and availability. As those factors evolve, Expel may adjust alert severity.

Expel-authored detections

Name	MITRE ATT&CK Tactic	MITRE ATT&CK Technique	Expel severity default
Suspicious Email Internal Sender	TA0001, TA0042, TA0005, TA0008	T1199, T1566, T1586, T1656, T1534	HIGH
Suspicious Email Using Content Sharing Services	TA0001, TA0005	T1566, T1598	LOW

© 2025 Expel, Inc. EXPEL PROPRIETARY—DISCLOSURE MUST BE AUTHORIZED

Suspicious Email Received Followed By A Suspicious Login	TA0001, TA0042	T1566, T1585, T1586	MEDIUM
Suspicious Email Received Followed Suspicious MFA Activity	TA0001, TA0003, TA0042	T1566, T1585, T1586, T1098	MEDIUM
Suspicious Email Received Followed By Suspicious Token Activity	TA0001, TA0042	T1566, T1585, T1586	MEDIUM
Suspicious Email Received Correlated with Defender for ID Alert	TA0001, TA0042	T1566, T1585, T1586	MEDIUM
Suspicious Attachment Observed in EDR	TA0001, TA0008	T1566, T1598	HIGH
Suspicious Email followed by New Mail Forwarding Rules	TA0009, TA0010	T1078, T1114, T1566, T1586	MEDIUM

Vendor-authored detections

Name	MITRE ATT&CK Tactic	MITRE ATT&CK Technique
Business Email Compromise	TA0001	T1566
Credential Phishing	TA0001	T1566
Credential Vishing	TA0001	T1566.004
Extortion	TA0001	T1566
Fake Billing Scam	TA0001	T1566
Financial Services Scam	TA0001	T1566
Malware	TA0001	T1566.001, T1566.002
Vendor Email Compromise	TA0001	T1566, T1199

© 2025 Expel, Inc. EXPEL PROPRIETARY—DISCLOSURE MUST BE AUTHORIZED

DUET rules

A DUET (**d**id yo**u** exp**e**ct **t**his) rule, when enabled, will not be triaged by the SOC. They do not represent activity that identifies the behaviors indicative of security incidents and are therefore outside of Expel's detection strategy. They will instead automatically create an investigation and be sent directly to the customer via notifications. Contact your engagement manager to opt-in to receiving a DUET rule notification for any of the following.

Rule name	Description	Notes
Phishing Email (Blocked or Delivered) to High-Risk Recipients	Customers can provide a list of recipients for which they would rather bypass the Expel SOC and triage phishing events (blocked or delivered) directly.	This use case is for customers who wish to be notified/wish to independently triage events sent to individuals or distribution lists that may contain known recipients with sensitive access/VIP status.

Investigative support

Remediation actions

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 (Auto remediation available)
- Remove email from user inbox

Investigative actions

Expel analysts are able to take the following investigative actions to gather data for triage and investigation of alerts.

- Query User
- Query Domain

© 2025 Expel, Inc. EXPEL PROPRIETARY—DISCLOSURE MUST BE AUTHORIZED

- Retrieve User Login History

Additional details and common questions

Abuse Mailbox Support

Abuse Mailbox (User Reported Emails) is not supported as part of the Abnormal AI MDR integration. Support for this feature requires the Expel 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)

© 2025 Expel, Inc. EXPEL PROPRIETARY—DISCLOSURE MUST BE AUTHORIZED