# Proofpoint TAP

## Detection strategy

**April 2025**

# Product Overview

Proofpoint Targeted Attack Protection (TAP) is a cybersecurity solution that helps organizations detect, analyze, and block advanced threats targeting people through email, including malicious attachments and URLs, and offers real-time threat prevention and forensic analysis.

Expel alerts are produced from Proofpoint TAP SIEM alerts. These SIEM alerts include **Blocked Messages, Delivered Messages, Blocked Clicks, and Permitted Clicks. Blocked Click** and **Blocked Message** events are not surfaced as Expel alerts by default, but are eligible for **Did yoU Expect This (DUET)** and **Be On The Lookout (BOLO)** alerts, such as if a customer wishes to be notified when a particular threat actor has targeted their organization, or if a particular employee has been targeted, regardless of success (see ***"Allowed and Blocked Threats"*** below for details on these custom alerts).

**Delivered Message** events are surfaced as Expel Alerts when there is other correlated activity that suggests imminent risk to the organization (e.g. a confirmed click on a phishing URL, a confirmed download of a malicious attachment, suspicious activity following the receipt of a confirmed phishing email, etc.). **Permitted Click** events are always surfaced as Expel alerts as they signal that a user has already visited a suspicious/malicious URL.

If they wish, a customer can specify in their Customer Configuration to have all **Delivered Message** events auto-remediated by Expel, meaning that every **Delivered Message** event will trigger a workflow to remove that email from all impacted users' inboxes, regardless of whether or not the Expel SOC has triaged the event first. This requires the customer to have integrated their email client, such as GSuite or Microsoft 365. See the **Proofpoint TAP Onboarding Guide** for more details on setting up **Customer Configuration**.

Proofpoint TAP for MDR does not provide full-body email text to Expel SOC analysts, but rather just the alert data provided by Proofpoint TAP devices - Full-text analysis of user-submitted emails is offered via Expel's Managed Phishing service offering. When Proofpoint TAP events are promoted to Expel alerts, additional workflows are used to query Proofpoint's **Threat** and **Forensics** APIs to enrich the event with context. The **Threats** API enriches alerts by providing context surrounding a particular threat (e.g. an attachment or URL), including threat actors observed utilizing the threat, how often the threat has been observed across Proofpoint telemetry, what families of malware might be tied to the threat, and attack techniques utilized by the threat. The **Forensics** API provides details about the nature of malware or malicious URLs as observed in Proofpoint's sandbox, including file behavior within the sandbox, network activity, whether a URL has been observed as blacklisted on Proofpoint's tracked blacklists, and other data which may provide Indicators of Compromise (IoCs) to detect the follow-on effects from a phishing email. These enrichments are used to provide maximum context to Expel's SOC so that they can triage and correlate activity from a Proofpoint TAP alert.

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 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 Proofpoint TAP 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 Proofpoint TAP alert, Forensics API, and Threat API, as well as Expel-internal enrichment sources (file/IP/URL lookups) to make the best determination of a Proofpoint TAP alert.

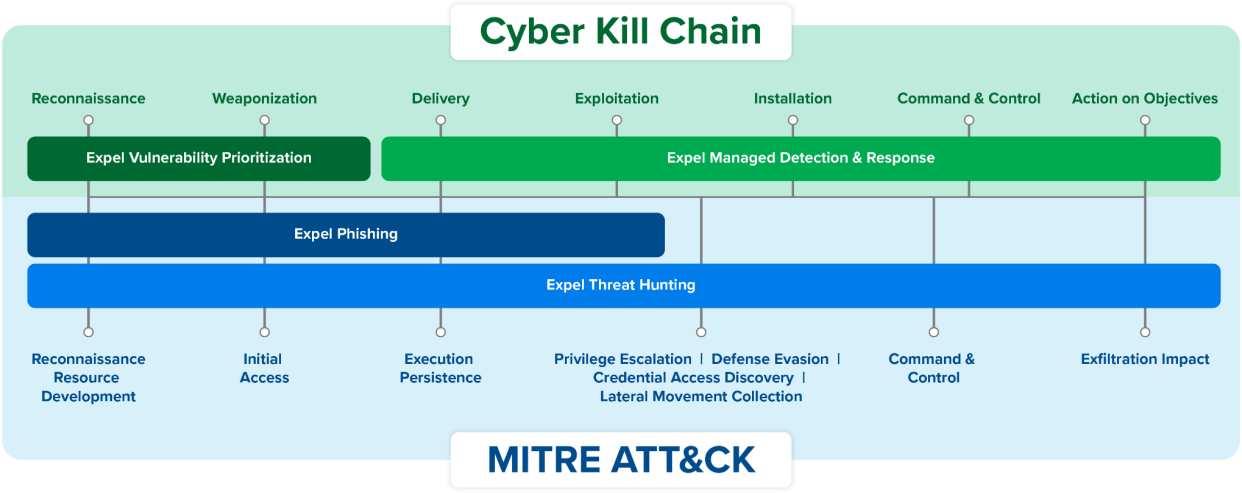
Expel integrates directly with Proofpoint TAP and uses its data in a few ways to quickly identify and investigate email and identity-based attacks:

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

## Support Quick Reference

| Supported version | Proofpoint TAP SIEM Events |
|---|---|
| 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 an attack's kill chain as possible, correlated with as much data as possible to paint a full picture of this 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.

Our messaging and productivity strategy....

- Active (meaning "not already blocked") email impersonation threats
- Active malware attachment threats
- Active malicious URL threats
- Active phishing email threats
- Suspicious authentications correlated with email threats
- Suspicious MFA activity correlated with email threats
- Suspicious file activity (attachment download/execution) correlated with email threats

## Proofpoint TAP 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 |
|---|---|---|---|

| | | | |
|---|---|---|---|
| Confirmed Delivered Phish with Confirmed Click to Malicious URL | **TA0001** - Initial Access | **T1566** - Phishing | **HIGH** |
| Confirmed Delivered Phish with Confirmed Attachment Execution | **TA0001** - Initial Access<br>**TA0002** - Execution | **T1204** - User Execution<br>**T1566** - Phishing | **HIGH** |
| Confirmed Delivered Phish with Confirmed Attachment Download | **TA0001** - Initial Access<br>**TA0002** - Execution | **T1204** - User Execution<br>**T1566** - Phishing | **HIGH** |
| Suspicious Email Delivered Followed By A Suspicious Login (by VPN/Tor/anomalous region/anomalous hours/etc.) | **TA0001** - Initial Access<br>**TA0006** - Credential Access | **T1078** - Valid Accounts<br>**T1566** - Phishing<br>**T1586** - Compromise Accounts | **MEDIUM** |
| Suspicious Email Delivered Followed Suspicious MFA Activity | **TA0001** - Initial Access<br>**TA0006** - Credential Access | **T1078** - Valid Accounts<br>**T1111** - Multi-Factor Authentication Interception<br>**T1566** - Phishing<br>**T1586** - Compromise Accounts | **MEDIUM** |
| Suspicious Email Delivered Followed By Suspicious Token Activity | **TA0001** - Initial Access<br>**TA0003** - Persistence<br>**TA0006** - Credential Access | **T1550** - Use Alternate Authentication Material<br>**T1566** - Phishing<br>**T1586** - Compromise Accounts | **MEDIUM** |
| Suspicious Email followed by New Mail Forwarding Rules | **TA0009** - Collection<br>**TA0010** - Exfiltration | **T1078** - Valid Accounts<br>**T1114** - Email Collection<br>**T1566** - Phishing<br>**T1586** - | **MEDIUM** |

| | | | |
|---|---|---|---|
| | | Compromise Accounts | |
| Suspicious Email Using Content Sharing Services (Dropbox, Sharepoint, Google Docs, etc.) | TA0001, TA0005 | T1566, T1598 | **LOW** |

## Vendor-authored detections

| Name | MITRE ATT&CK Tactic | MITRE ATT&CK Technique |
|---|---|---|
| Malware via Phish | **TA0001** - Initial Access<br>**TA0002** - Execution | **T1204** - User Execution<br>**T1566** - Phishing |
| Malicious Link | **TA0001** - Initial Access | **T1566** - Phishing |
| Spam Emails | **TA0001** - Initial Access | **T1566** - Phishing |
| Telephone-Oriented Attack Delivery | **TA0001** - Initial Access<br>**TA0043** - Social Engineering | **T1566** - Phishing<br>**T1598** - Phishing for Information |

## 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) from Specified Threat Actor(s) | Customers can provide specific Threat Actor names (using Proofpoint naming conventions) which, if observed by Expel, will be forwarded directly to the customer without SOC triage. | This use case is for customers who wish to be notified/wish to independently triage events attributed to specific threat actors, even in cases where these events are blocked, in case the knowledge of targeting by the threat actor itself is of interest |

| | | |
|---|---|---|
| | | for threat intelligence. |
| 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 Proofpoint TAP 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
- Remove email from user inbox

## Investigative actions

Expel analysts are able to take the following investigative actions via the Proofpoint TAP Expel plugin to gather data for triage and investigation of alerts:

- Query Proofpoint Threat Campaign Details
- Query Proofpoint Forensics

# Additional Details & Common Questions

## Abuse Mailbox Support

Abuse Mailbox (User Reported Emails) Support is not included as part of the Proofpoint TAP MDR integration. Support for this feature requires the Expel 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)