Proofpoint TAP

Detection Strategy Guide

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 you wish to be notified when a particular threat actor has targeted your 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.

You may choose 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 you to have integrated your email client, such as GSuite or Microsoft 365. See the Proofpoint TAP onboarding guide for more details on setting up your 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 This includes 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 you 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 you do **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.

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 Proofpoint TAP

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 Proofpoint TAP, you can visit the Detections page in Workbench or ask your Sales or Support rep for the most recent download.

Supported versions	■ Proofpoint TAP SIEM Events
Proofpoint TAP detection rules support	Yes.
Detection rules written by Expel	Yes.
Auto remediations	Yes. Expel supports automatic execution of some remediation actions for this integration when you follow our setup guide to update the permissions in your vendor device, and then enable the auto remediation in Workbench. The available auto remediations for this integration include: ■ Remove Malicious Email Learn more in Proofpoint TAP for MDR Setup for Workbench.
Investigative support through Workbench	Yes. We are able to take the following investigative actions to gather data for triage and investigation of events. ■ Query Proofpoint Threat Campaign Details ■ Query Proofpoint Forensics
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 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)