A trained and aware workforce can recognize the difference between benign email and email phish. Once a suspected email phish is identified, typical practices include forwarding the phishing email to the security team or an abuse mailbox, but often the response will be to simply delete the message or just ignore it. If a phish is ignored or deleted, the internal security teams miss a chance to identify potential campaigns or improve defenses before a larger onslaught of phish hits the company. Proofpoint Closed-Loop Email Analysis and Response (CLEAR) can reduce the productivity losses and therefore the financial impact of live attacks.

With a single click, CLEAR gives you visibility into active attacks and an automatic layer of intelligent analysis and remediation of potential phishing attacks. An integrated, first-of-its-kind solution derived from the acquisition of Wombat Security, CLEAR uses PhishAlarm, the email reporting button, PhishAlarm Analyzer, which prioritizes emails using machine learning, and Threat Response Auto-Pull (TRAP) for intelligent analysis and remediation.

**MORE POWER FROM A SINGLE BUTTON**

The PhishAlarm button gives your security team better visibility into incoming phishing emails reported by your employees.

CLEAR is a complete solution that blends the capabilities of PhishAlarm, PhishAlarm Analyzer and TRAP to make the job easier.

When PhishAlarm users receive a suspicious email, they click on the “Report Phish” button as usual. With CLEAR deployed, PhishAlarm sends the email to PhishAlarm Analyzer. PhishAlarm Analyzer provides machine-learning based
categorization and scoring on the likelihood of the email being a phishing attack. This aids in prioritization and further processing by TRAP. From there, TRAP uses security automation and orchestration to add threat context and automatically locate other instances of that malicious email across the enterprise.

**PROTECT WITH AUTOMATION**

TRAP continually checks the abuse mailbox for new emails and retracts and quarantines them after they are delivered. At the same time, PhishAlarm Analyzer processes the emails that PhishAlarm sends to the abuse mailbox. Each email is automatically broken down into:

- Header
- URL
- Sender IP
- Subject line
- Sender domain
- Body text

In seconds, TRAP analyzes these using multiple intelligence and reputation systems to verify whether any of the content is indeed malicious.

TRAP also pinpoints the geographical location of the suspect IP addresses. It automatically connects suspicious emails to recent attack campaigns for visibility into potential threats with no extra work. Armed with this insight, your team can act quickly to protect users and data.

TRAP comes pre-configured with the industry's best reputation and intelligence feeds. And it is already connected to business logic for email. That means TRAP can quickly surface and remediate emails that contain credential-phishing templates, malware links and attachments.

Other out-of-the-box capabilities include incident handling and reporting. With no need for coding or integration beyond initial setup, security teams can:

- Create an incident
- Deconstruct email headers
- Check sender IP address
- Check sending domain
- Review sender reputation
- Analyze links that lead to credential phishing or malware
- Analyze attachments for threats, malware or other active content
- Eliminate writing and maintaining YARA rules and manual scripts

TRAP scores, geolocates and connects information from emails. Analysts can quickly view a summary of the potential threat.

**REDUCE THE RISK OF MALICIOUS EMAIL**

Messaging administrators can initiate “manual” or “auto-pull” on malicious emails to pull them out of the sender’s mailbox. TRAP performs forward follow and distribution list expansion to pull forwarded messages, even those that are forwarded to distribution lists. TRAP pulls the emails out and places them in quarantine. Any malicious emails sent to the abuse mailbox are removed from your users’ inboxes, reducing risk.

No matter how many emails you might have in your abuse mailbox, you can use CLEAR to reduce your phishing risk today.

**LEARN MORE**

For more information, visit [proofpoint.com](http://proofpoint.com) or contact your Proofpoint sales representative.

*Note: PhishAlarm, PhishAlarm Analyzer and TRAP are all required for the automation described above.*

**ABOUT PROOFPOINT**

Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today’s mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.

©Proofpoint, Inc. Proofpoint is a trademark of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are property of their respective owners.