Proofpoint Threat Response

Enhance SOC Efficiency. Respond Faster to Incidents.

KEY BENEFITS

- Consume alerts from any source and correlate them into one incident
- Leverage threat intelligence from Proofpoint and third parties to automatically enrich alerts
- Quarantine and contain threats automatically or at a push of a button for fast protection
- Manage users, emails, hosts, IPs and URLs automatically on enforcement systems throughout the attack to free up staff

Your security team faces many challenges when they respond to threats that target your people. Qualified talent is hard to come by these days. There is an overwhelming number of alerts. And it's a struggle to reduce the time it takes to respond and remediate threats. Proofpoint Threat Response is a leading security orchestration, automation and response (SOAR) solution that helps your security team respond faster and more efficiently to the dynamic threat landscape.

AUTOMATE SECURITY ALERT ENRICHMENT

Threat Response collects alerts from a variety of sources and automatically enriches and groups them into incidents in seconds. Your security team receives rich, relevant context by leveraging threat intelligence from Proofpoint and third parties, such as STIX/TAXII feeds, WHOIS, VirusTotal, Soltra and MaxMind. This data helps your team understand the "who, what and where" of attacks. As a result, they can quickly triage and prioritize incoming events.

RESPOND TO INCIDENTS MORE EFFECTIVELY

Threat Response provides a context-rich view of threats based on the forensics collected and analyzed. Your analysts can take action by simply pushing a button. They can identify areas for additional investigations or turn on automated responses. These include: retract delivered email from users' mailboxes, add users to low permission groups, update block lists of firewalls and web filters, and more. Your team can contain threats by blocking across Microsoft Exchange, firewalls, endpoint detection and response (EDR), web gateways, Microsoft Active Directory, network access control (NAC), and other solutions.

Immediate Out-of-the-Box Value

Threat Response comes with many out-of-the-box integrations to provide immediate value to your security team. It delivers security orchestration, automation, and response by integrating with:

- **Alert sources:** Cisco, FireEye EX and NX Series, HP ArcSight, IBM QRadar, Juniper Networks, Palo Alto Networks WildFire, Splunk and Suricata
- **Endpoint solutions:** Carbon Black and Tanium
- **Email providers:** Exchange, Microsoft Office 365, Google Gmail and IBM Domino
- **Threat intelligence providers:** Proofpoint, Emerging Threats, MaxMind, Microsoft Active Directory, Splunk, Soltra, VirusTotal and WHOIS
- **Enforcement devices:** Check Point, Cisco ASA, Cisco IOS, Cisco OpenDNS, CyberArk Enterprise Vault, Fortinet FortiGate, Imperva SecureSphere, Juniper Networks SRX, Palo Alto Networks Next-Generation Firewalls and Palo Alto Networks Panorama
- **Identity access management solutions:** Okta, OneLogin, Idaptive, Microsoft Azure AD Seamless SSO and Ping Identity
- **Two-factor authentication solutions:** Duo Security, RSA SecurID, SafeNet and Symantec 2FA

Extend and Customize Threat Response

Threat Response is designed to work in small, medium, or large IT security and security operations center (SOC) environments. It comes complete with tools that make it easy to integrate with third-party security products. Threat Response can be customized and extended to meet your specific needs through rich application programming interface (API) functionality. It supports customizations and integrations through List Management API, Incident API, Custom Response API, JSON Alert Source, Python scripting and custom PowerShell scripts.

PROTECT AGAINST THE NO. 1 THREAT VECTOR

Over 94% of successful attacks that lead to a breach or data loss arrive via email.[1] With Threat Response, messaging and security administrators can analyze emails and automatically move malicious or unwanted emails to quarantine after delivery.

Threat Response receives alerts from detecting systems when a malicious email is delivered. It then leverages Proofpoint Threat Intelligence, sandboxing analysis and other third-party threat intelligence to enrich context. Security and messaging teams have the actionable context they need to offload repetitive tasks. Messages are enriched by building associations between recipients and user identities. This helps reveal associated campaigns and surfacing IP addresses and domains in the attack. Threat Response then goes into Exchange, Office 365, Domino and Gmail to move the message into quarantine. This applies to forwarded mail and distribution list recipients and creates an activity trail that is easy to audit.

IDENTIFY AND REDUCE PHISHING RISK WITH CLEAR

Informed employees can be your last line of defense against an attack. With Closed-Loop Email Analysis and Response (CLEAR), the cycle of reporting, analyzing and remediating potentially malicious emails is reduced from days to just minutes. Enriched with our world-class threat intelligence, CLEAR stops active attacks in their tracks with just a click. And your security team can save time and effort by automatically quarantining malicious messages.

CLEAR is a complete solution that blends multiple capabilities. These include:

- PhishAlarm®, the email reporting button
- PhishAlarm Analyzer, which categorizes and prioritizes using Proofpoint Threat Intelligence
- Threat Response for message enrichment and automatic remediation of malicious messages

1 Verizon. "Data Breach Investigation Report." July 2019.

LEARN MORE

For more information, visit **proofpoint.com/us/products/threat-response**.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at **www.proofpoint.com**.

©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. **Proofpoint.com**