Proofpoint Domain Discover

Identifizierung von und Reaktion auf betrügerische Domänen

PRODUKTFUNKTIONEN

- Erkennung
- Klassifizierung
- Untersuchung
- Benachrichtigung
- Reaktion
- Reporting

Mit Proofpoint Domain Discover können Sie betrügerische Domänen, die von Angreifern zur Täuschung Ihrer Mitarbeiter, Kunden und Partner verwendet werden, identifizieren und darauf reagieren. Domain Discover analysiert kontinuierlich neu registrierte Domänen mithilfe eines stark skalierbaren Erkennungssystems. Wenn die Lösung ein beliebiges Sicherheits-, Handelsmarken- oder sonstiges Risiko findet, gibt sie eine Warnung aus und ermöglicht eine entsprechende Reaktion.

Die Qualität unserer Daten und die Abdeckungsbreite sorgen für eine genaue Erkennung von Domänen, die ein Risiko für die Sicherheit, die Handelsmarke oder ein anderes Risiko für Ihre Marke und Ihre Kunden darstellen. Dank unseres umfangreichen Überblicks über digitale Kanäle wie E-Mails können Sie Verbindungen zwischen verdächtigen Domänen und aktiven Angriffen wie Phishing, Business Email Compromise und Malware aufdecken.

Domain Discover bietet folgende Funktionen:

Erkennung

Finden Sie Domänen, die Ihrem Unternehmen zugeordnet werden.

- Überwacht WHOIS-Datenquellen und scannt mehr als 350 Millionen URLs pro Tag
- Nutzt ein automatisiertes Erkennungssystem (das künstliche Intelligenz, Machine Learning und Verarbeitung natürlicher Sprache bietet), um Domänen kontinuierlich auf Betrug, Doppelgänger-Domänen und Typosquatting zu prüfen

Klassifizierung

Findet und kennzeichnet domänenbasierte Risiken, um den Überblick über potenzielle Bedrohungen zu vervollständigen. Domain Discover ordnet Domänen eine Risikostufe zu, damit Sie schnell Domänen mit mittlerem und hohem Risiko finden können.

Die Lösung scannt Proofpoint-Daten auf E-Mail-Aktivitäten und aktive Angriffe, um schnell Domänen aufzudecken, die für Phishing-Kampagnen oder andere Attacken genutzt werden.

- Schutzregistrierungen von Markendomänen
- Übernommenes Unternehmen
- Risikowert (hohes oder mittleres Risiko)
- Domänenstatus (aktiv, inaktiv, geparkt, unbekannt und gelöscht)
- und mehr

Untersuchung

Greifen Sie auf detaillierte Domäneninformationen zu.

Folgende Details werden bereitgestellt:

- Name und E-Mail-Adresse des Registrierenden
- Registrar
- Registrierungsdaten
- ASN
- MX-Datensätze
- Details zu Sicherheitszertifikaten
- Snapshots von Webinhalten
- und mehr

Benachrichtigung

Erhalten Sie bei der Entdeckung riskanter Domänen sofort Warnungen.

Erstellen Sie individuelle Benachrichtigungen und Empfängerlisten basierend auf folgenden Faktoren:

- Domänenklassifizierungstyp
- „Von-Status“ und „Zu-Status“ (aktiv, inaktiv, geparkt, unbekannt und gelöscht)
- Hinzugefügter MX-Datensatz
- und mehr

Reaktion

Ergreifen Sie Maßnahmen gegen schädliche Domänen mit optionalen integrierten Workflows:

Virtual Takedown-Add-on (Proofpoint-Angebot):

- Schnelles Eintragen der riskantesten Domänen auf Blocklists, um Gefahren für Mitarbeiter, Partner und Kunden zu minimieren
- Blockierung des Zugriffs über bekannte Blocklists für HTTP/HTTPS, DNS und SMTP
- Keine Intervention beim Hosting-Anbieter oder Registrar erforderlich

Herkömmliches Takedown-Add-on (über Proofpoint Partner):

- Permanente Deaktivierung und Stilllegung betrügerischer Domänen
- Intervention beim Registrar bzw. Hosting-Anbieter, um die Hosting-Infrastruktur zu deaktivieren und die Domäne permanent zu entfernen
- Start eines UDRP/URS-Prozesses bei Markenverstößen

Zusätzliche Behebungsoptionen umfassen das Exportieren von Domänenlisten, z. B. zum Blockieren am E-Mail-Gateway.

Reporting

Auswertung und detaillierte Informationen zu Domänenbedrohungen sowie Ihren Reaktionen mit leicht verständlichen Berichten.

WEITERE INFORMATIONEN

Weitere Informationen finden Sie unter **proofpoint.com/de**.