proofpoint.

PROOFPOINT THREAT RESPONSE

VERHINDERN SIE, DASS AUS WARNUNGEN UND ZWISCHENFÄLLEN AUSGEWACHSENE SICHERHEITSVERLETZUNGEN WERDEN

VORTEILE VON THREAT RESPONSE

- Automatisierte Erfassung forensischer Daten von potenziell kompromittierten Systemen
- Geringerer Zeitaufwand für die Bestätigung von Infektionen dank Vergleich der PC-Systemdaten mit forensischen Erkennungsdaten
- Weniger manuelle Datenerfassung von externen Geräten, Datenquellen usw.
- Zentraler Überblick über alle Vorgänge – dank Grafikoberfläche zur Überwachung von Zwischenfällen und verarbeiteten Bedrohungen
- Schnellere Reaktionsentscheidungen dank integrierter Übersichten über Bedrohungsaktivitäten
- Schneller Schutz durch Isolierung und Eindämmung von Bedrohungen – automatisch oder per Tastendruck
- Automatische Verwaltung von Benutzern, E-Mails, Hosts, IP-Adressen und URLs auf Erzwingungssystemen während aller Angriffsphasen, um Mitarbeiter für andere Aufgaben zu entlasten
- Auditfähige Verlaufsübersicht über Reaktionsmaßnahmen zur Steigerung der Rendite vorhandener Infrastrukturen
- Größere Unabhängigkeit von individualisierter Software
- Automatische Erstellung, Nachverfolgung und Verwaltung von Datensätzen zu Zwischenfällen für weniger manuelle Benutzereingriffe
- Laufende Informationen zu böswilligen Aktivitäten mit minutenaktuellen Berichten zu angegriffenen Benutzern, Systemen, Gruppen und Abteilungen

Proofpoint Threat Response™ verstärkt die Sicherheitsprozesse und koordiniert sowie automatisiert die Reaktion auf Zwischenfälle. Die Plattform ergänzt Sicherheitswarnungen mit umfangreichen Kontextdaten, um Sicherheitsteams bei Priorisierungs- und Reaktionsmaßnahmen zu unterstützen. Dabei erfasst und analysiert sie nicht nur die Kontextdaten von Sicherheitsereignissen und Untersuchungen, sondern sammelt auch forensische Endgerätedaten, mit deren Hilfe Systeminfektionen bestätigt und nutzbare Vorfallprofile erstellt werden können. Dank dieser umfangreichen Kontextdaten ermöglicht die Plattform außerdem Erzwingungs- sowie Isolierungsmaßnahmen, die automatisch oder per Tastendruck ausgelöst werden und die vorhandene Infrastruktur nutzen.

MANUELLE REAKTIONSMASSNAHMEN SIND NICHT SKALIERBAR

In vielen Unternehmen ist die Reaktion auf Sicherheitsvorfälle ein sehr langsamer und arbeitsintensiver Prozess mit verschiedenen zeitaufwändigen Schritten, die die regulären Abläufe enorm behindern. Beispiele hierfür sind:

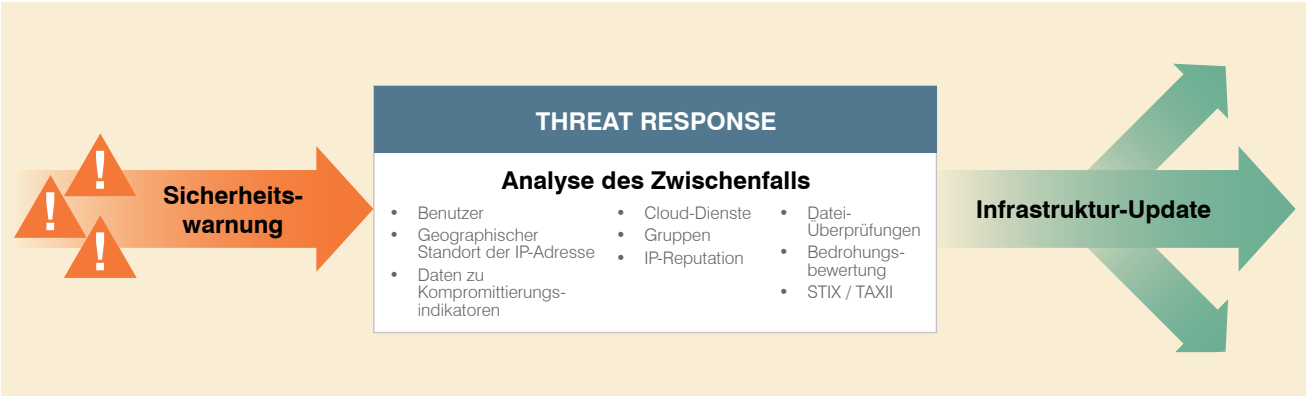
- Identifizierung wertvoller Ziele, um Bedrohungen zu priorisieren
- Identifizierung schwerwiegender Bedrohungen, die möglicherweise zu größeren Kampagnen oder Botnets gehören
- Erfassung und Vergleich forensischer Endgerätedaten, um Anzeichen einer Infektion aufzudecken
- Verwaltung von Untersuchungen, die mehrere Ziele und Warnungen umfassen
- Herstellung eines Gleichgewichts zwischen Sicherheitsmaßnahmen und Infrastruktur, inkl. Zeitaufwand für die Umsetzung

Wenn diese Aufgaben für jeden Zwischenfall wiederholt werden müssen, könnten ohnehin schon stark ausgelastete Sicherheitsteams an ihre Grenzen stoßen und Schritte überspringen oder abkürzen.

Der Nachteil zeitaufwändiger Vorfalluntersuchungen

Zur Untersuchung von Zwischenfällen werden Informationen aus mehreren isolierten Quellen herangezogen, wobei jeder weitere Datenpunkt einem Puzzleteil ähnelt. Je mehr einzelne Teile hinzugefügt, angeordnet und analysiert werden, desto klarer wird das Bild über Ausmaß, Schweregrad und Priorität des Zwischenfalls.

In der Regel kann die Kompromittierung eines Systems nur mithilfe einer Reihe manueller, zeitaufwändiger Schritte bestätigt werden. Wenn sich die Angreifer während dieser Untersuchungsphase ungehindert durch das Netzwerk bewegen, könnten in dieser Zeit wertvolle Daten von infizierten Systemen gestohlen werden, sodass eine vollständige Untersuchung häufig die Daten gefährden würde.



ZEITGEMÄSSE REAKTION AUF ZWISCHENFÄLLE DANK THREAT RESPONSE

Erfassung und Untersuchung der Quelle einer Bedrohungswarnung

Bei der Reaktion auf Zwischenfälle gibt es vier Hauptschwerpunkte:

- Untersuchung der Angriffe (Wer, Was, Wo), einschließlich angegriffene Benutzer, Systeme und Kampagnen
- Abgleich der forensischen Daten angegriffener Systeme mit forensischen Sandbox-Berichten
- Stoppen von anhaltenden Datenlecks und Verlust geistigen Eigentums durch Isolierungs- und Eindämmungsmaßnahmen
- Nachverfolgung der Leistungsindikatoren von Reaktionsmaßnahmen, damit Zwischenfälle nicht unbemerkt bleiben oder in Vergessenheit geraten

Mithilfe dieser Schwerpunkte können neben den betroffenen Benutzern auch der Schweregrad und die Dringlichkeit einer Bedrohung ermittelt werden. Außerdem werden False Positives vermieden, Infektionen an der Ausbreitung gehindert und die Exfiltration von Daten aufgehalten.

Untersuchung des „Wer, Was und Wo" mit Threat Response

Sie müssen unverzüglich ermitteln, welche internen Benutzer, Abteilungen und Gruppen betroffen sind. Wenn Sie Informationen über das „Wer" haben, können Sie kritischen Zielen wie dem Finanzvorstand, den Führungskräften und Finanzsystemen Priorität über der Poststelle oder nachrangigen Zielen zuweisen.

Neben internen Kontextdaten und Informationen können auch externe Faktoren Hinweise auf verdächtige IP-Adressen oder Domänen in Sicherheitswarnungen liefern. Diese Faktoren sind bereits in Threat Response integriert und ermöglichen den Import sowie die Nutzung von Drittanbieterdaten (z. B. STIX/TAXII-Feeds), um die Analyse weiter zu automatisieren.

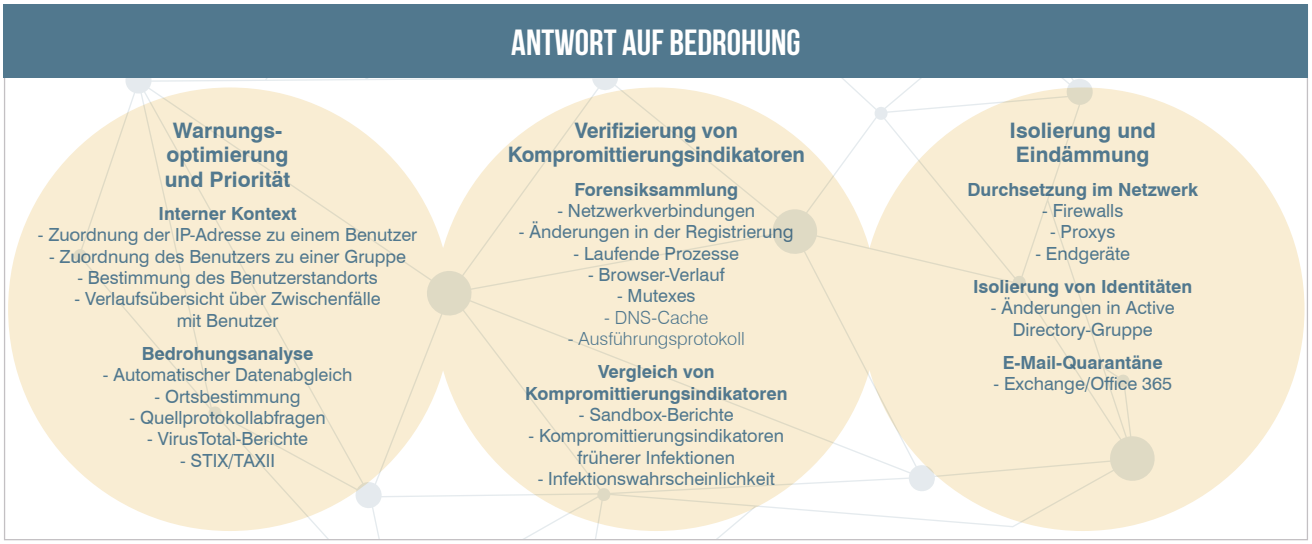
Zu den wichtigen externen Faktoren gehören:

- Aktualität der Domäne bzw. Registrierungsdauer
- Blacklist-Eintrag der Domäne
- Reputation der IP-Adresse und URL (Kategorie und Verlauf)
- Geographischer Standort der IP-Adresse
- Zugehörige Kampagnen
- Zielbranchen für Kundenkategorien

Bestätigung der Infektion dank automatischer Verifizierung von Kompromittierungsindikatoren

Threat Response erfasst und analysiert forensische Endgerätedaten auf Zielsystemen, um ein umfassendes Bild der Kompromittierungsindikatoren zu erhalten. Zu den Kompromittierungsindikatoren gehören folgende Daten:

- Änderungen in der Registrierung
- Datei-Änderungen
- Ereignisse in Protokollen zuletzt ausgeführter Dateien
- Mutexes
- Netzwerkverbindungen
- Ereignisse in Protokollen zu gelöschten Dateien
- Laufende Prozesse
- Browser-Verlauf
- DNS-Cache



Diese Informationen werden mit Änderungen verglichen, die von Malware-Analysetools und anderen Systemen gemeldet wurden. Als Ergebnis erhalten Sie einen Überblick über den Integritätsstatus des Mitarbeiters. Zudem können von Benutzern entwickelte Powershell-Skripts für die Erfassung benutzerdefinierter Daten oder für andere Aktivitäten auf Endgeräte verteilt werden.

Als weitere wichtige Funktion wird überprüft, ob die angegriffenen Systeme in der Vergangenheit schon einmal infiziert wurden. Threat Response sucht bei der On-Demand-Endgeräteerfassung also nicht nur nach Kompromittierungsindikatoren zum aktuellen Angriff, sondern auch zu früheren Infektionen in Ihrer Umgebung. Dadurch lässt sich schnell und effizient feststellen, ob sich frühere Infektionen auf das aktuell betroffene System ausgebreitet haben.

Standardmäßige Integration mit Premiumdaten und Drittanbietertools

Threat Response überprüft jede Domäne und IP-Adresse, die in Sicherheitswarnungen sowie Sandbox-Berichten aufgeführt wird, anhand integrierter Premiumdaten-Feeds wie Emerging Threats Intelligence. Durch diesen Schritt sparen Sie sich viele Stunden langwieriger Arbeit sowie einzelne und manuelle Suchläufe in Analysediensten, um die in Angriffen bekannt böswilliger Seiten verwendeten IP-Adressen sowie Hosts zu finden.

Threat Response ist in der Lage, Bedrohungsdaten von Drittanbietern automatisch oder manuell über STIX und TAXII zu importieren, sodass Sicherheitsteams von Anfang an Daten importieren und automatisch mit Bedrohungs-Feeds verschiedener ISACs (Information Sharing and Analysis Centers) abgleichen können. Darüber hinaus unterstützt die Lösung das BYOI-Konzept (Bring Your Own Intelligence), bei dem Sie Ihre eigenen Datensätze hochladen oder Daten manuell hinzufügen können.

Dank integrierter VirusTotal-Integration können Dateien nicht nur einmal, sondern fortlaufend überprüft werden. Es wird angezeigt, wie viele der mehr als 50 Virenschutzmodule böswillige Signaturen oder Eigenschaften in Dateien erkennen, die während einer potenziellen Infektion abgelegt, heruntergeladen oder entpackt wurden. Als weitere Funktionen sind unter anderem WHOIS-Suchläufe, Ortsbestimmung und Active Directory-Konnektoren standardmäßig integriert.

Isolierung und Eindämmung

Basierend auf den vom System erfassten und analysierten Kontext- und Forensikdaten liefert Threat Response eine umfassende Übersicht über die Bedrohung. Diese Übersicht ermöglicht es Analysten, Reaktionsmaßnahmen per Tastendruck durchzuführen, eingehender zu untersuchende Bereiche zu ermitteln oder automatisierte Reaktionen zu aktivieren. Zu diesen automatischen Reaktionen gehören zum Beispiel das Entfernen bereits zugestellter E-Mails aus den Postfächern von Benutzern, das Hinzufügen von Benutzern zu Gruppen mit weniger Berechtigungen oder das Aktualisieren der Sperrlisten von Firewalls und Webfiltern.

Verwaltung von Zwischenfällen

Eines der verborgenen Risiken beim Umgang mit Zwischenfällen besteht darin, dass Sie aufgrund der Vielzahl an Systemkonsolen und Browserfenstern als auch durch das Kopieren und Einfügen von Informationen zwischen diesen Systemen den Überblick über die Kontextdaten verlieren können. Deshalb umfasst Threat Response neben den Kernfunktionen auch wichtige Funktionen zur Zwischenfallverwaltung, sodass Benutzer und Teams Zwischenfälle untersuchen können, ohne die Kontextdaten beim Wechsel zwischen den Systemen aus den Augen zu verlieren. Zusätzlich zur einfachen Zuweisung und deren Nachverfolgung umfasst Threat Response folgende Funktionen:

- Verwaltung einer Verlaufsübersicht sowie eines Datensatzes für jeden Zwischenfall und alle ergriffenen Maßnahmen
- Nachverfolgung der Zwischenfall-Zuweisungen auf Mitarbeiter- und Teamebene
- Kombination von Zwischenfällen von verschiedenen Untersuchungen
- Möglichkeit für Benutzer oder Teammitglieder, mit unterschiedlichen Berechtigungen zu arbeiten
- Versand von Workflow-Benachrichtigungen, wenn sich Zwischenfälle ausbreiten und den Status ändern
- Berücksichtigung von Rollen und Berechtigungen bei Isolierungen, sodass nur die richtigen Mitarbeiter zur richtigen Zeit Maßnahmen ergreifen können
- Benachrichtigung von Benutzern oder Teams bei Veränderungen im Zusammenhang mit Zwischenfällen, z. B. wenn Bedrohungsfaktoren einen bestimmten Grenzwert übersteigen oder wenn eine Isolierungsmaßnahme abgeschlossen ist

VORTEILE

Der Einsatz von Threat Response und die Automatisierung der Isolierungs- und Eindämmungsmaßnahmen bieten unter anderem folgende Vorteile:

- Möglichkeit zum Hinzufügen von Datenbankadministratoren zu einem Isolationsbereich mit eingeschränkten Berechtigungen, um während eines Zwischenfalls den Zugang zu vertraulichen Informationen zu blockieren
- Zurückholen bereits zugestellter E-Mails, damit Benutzer nicht erneut auf böswillige URLs oder Anhänge klicken können
- Blockieren der Kommunikation aller Mitarbeiter zu CNC-Standorten, um die Kontrollkette zu durchbrechen
- Begrenzen der Möglichkeit für Malware-Infektionen, sich auf andere Systeme zu verteilen
- Reduzieren redundanter oder doppelter Analysearbeiten durch Erkenntnisse aus umfangreichen Untersuchungen zu Kampagnen, die Ihr Unternehmen angreifen
- Visualisieren der Leistungsindikatoren zu langsamen oder noch nicht verarbeiteten Zwischenfällen, zur Handhabung von Zwischenfällen sowie zu gezielten Angriffen auf Abteilungen oder Berechtigungsgruppen
- Installieren und Einrichten der Lösung innerhalb weniger Stunden für bessere Sicherheits- und Reaktionsergebnisse sowie schnellere Rendite

ZUSAMMENFASSUNG

Threat Response verbessert erheblich die Reaktion auf Zwischenfälle, indem Sicherheitsmaßnahmen standardmäßig koordiniert und automatisiert werden. Dazu werden zur Verifizierung von Infektionen, für Isolierungs- und Eindämmungsfunktionen sowie für die Zwischenfallverwaltung Kontextdaten, Forensiksammlungen und Kompromittierungsindikatoren hinzugezogen.

STANDARDMÄSSIGE INTEGRATIONEN

WARNUNGSQUELLEN

- Cisco FirePOWER NGIPS
- FireEye EX-Reihe
- FireEye NX-Reihe
- HP ArcSight ESM
- IBM QRadar
- JSON „Ereignisquelle“
- Juniper Secure Analytics
- Palo Alto Networks WildFire
- Proofpoint TAP
- Splunk Enterprise
- Suricata

BENUTZERDEFINIERTE REAKTION

- JSON-API für benutzerdefinierte Reaktion

EIDR

- Tanium
- Carbon Black

E-MAIL-QUARANTÄNE

- Microsoft Exchange

ERZWINGUNGSGERÄTE

- Check Point
- Cisco ASA
- Cisco IOS
- Cisco OpenDNS
- CyberArk Enterprise Vault
- Fortinet FortiGate
- Imperva SecureSphere
- Juniper SRX (JUNOS)
- Palo Alto Networks NGFW
- Palo Alto Networks Panorama

ZUSÄTZLICHE INFORMATIONEN

- Emerging Threats
- MaxMind
- Microsoft Active Directory
- Proofpoint Threat Graph
- Soltra
- Splunk Enterprise
- VirusTotal
- WHOIS

IDENTITÄTS- UND ZUGANGSVERWALTUNG

- Centrify
- Microsoft Azure SSO
- Okta
- OneLogin
- Ping Identity

PROXY, DYNAMIC BLOCK LISTS

- Blue Coat ProxySG
- Palo Alto Networks NGFW

TICKET-SYSTEME

- BMC Remedy Ticketing System
- JIRA

LÖSUNGEN FÜR ZWEI-FAKTOR-AUTHENTIFIZIERUNGEN

- Duo Security
- RSA Securid
- SafeNet
- Symantec 2FA

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) ist ein Cybersicherheitsunternehmen der nächsten Generation, das Unternehmen dabei unterstützt, die Arbeitsabläufe ihrer Mitarbeiter vor hochentwickelten Bedrohungen und Compliance-Risiken zu schützen. Dank Proofpoint können Cybersicherheitsexperten ihre Benutzer vor raffinierten und zielgerichteten Angriffen (per E-Mail, Mobilgeräte-Apps und Social Media) schützen, wichtige Informationen absichern und ihre Sicherheitsteams mit den notwendigen Bedrohungsdaten sowie Tools ausstatten, um bei Zwischenfällen schnell zu reagieren. Führende Unternehmen aller Größen, darunter mehr als 50 Prozent der Fortune 100, nutzen Proofpoint-Lösungen. Diese wurden für moderne IT-Umgebungen mit Mobilgeräten und Social Media konzipiert und nutzen die Möglichkeiten der Cloud sowie eine Big-Data-Analyseplattform zur Abwehr aktueller raffinierter Bedrohungen.