proofpoint

# PROOFPOINT THREAT RESPONSE

## EVITE QUE LAS ALERTAS Y LOS INCIDENTES DE SEGURIDAD SE INTENSIFIQUEN HASTA CONVERTIRSE EN BRECHAS COMPLETAS

Proofpoint Threat Response™ es la primera plataforma de administración de amenazas que automatiza la respuesta a incidentes mediante el suministro de datos contextuales abundantes a las alertas de seguridad con el objeto de crear inteligencia procesable, confirmar las infecciones de los sistemas y aplicar las protecciones automáticamente o con solo pulsar un botón. Al recopilar y analizar el contexto, los datos forenses y la inteligencia de los eventos de seguridad, y al convertirlos en una respuesta automática o de pulsación de botón, la plataforma acorta la distancia entre la detección y la protección, mediante la confinación de las amenazas y la detención de la propagación de infecciones.

### VENTAJAS QUE OFRECE THREAT RESPONSE

- Recopilación automatizada de datos forenses de los sistemas sospechosos que ahorra tiempo
- Confirmación de la infección que ahorra incontables horas al comparar los datos de PC de sistemas con los datos forenses de detección
- Reducción de la recopilación manual de datos de dispositivos externos, fuentes de inteligencia y mucho más
- Monitorización visual de incidentes y amenazas procesadas
- Coherencia en el análisis significa coherencia en la respuesta
- Aceleración de decisiones con vistas integradas
- Cuarentena y confinamiento automáticos y con pulsación de botón para brindar protección rápida
- Administración automatizada del ciclo de vida de usuarios, hosts, direcciones IP y direcciones URL en los dispositivos de aplicación de políticas
- Rastro de auditoría de las acciones de respuesta para aumentar el retorno de la inversión de la infraestructura actual
- Reducción de la dependencia de los módulos de software con código personalizado
- Creación automática de incidentes y seguimiento de la administración de incidentes para reducir los requisitos de ingreso de datos manual
- Informes actualizados de usuarios, sistemas, grupos y departamentos atacados


### LAS RESPUESTAS MANUALES NO SE INTENSIFICAN

En muchas organizaciones, la respuesta a los incidentes de seguridad es un proceso lento y laborioso que puede tomar días o semanas, dependiendo del personal disponible. Las tareas que consumen tiempo se convierten en cuellos de botella que no pueden evitarse:

- Identificación de los objetivos de alto valor para priorizar las amenazas
- Identificación de las amenazas de alto valor que puedan formar parte de campañas o botnets más grandes
- Recopilación y análisis de datos forenses de extremos en busca de señales de infección
- Negociaciones laboriosas entre la seguridad y la infraestructura con tiempo de implementación para la aplicación de políticas

La repetición de esas tareas con cada uno de los incidentes se puede traducir en más tiempo que el que tiene disponible el grupo de seguridad, ocasionando que se omitan pasos y se tomen atajos.

**La penalización del tiempo de investigación de respuesta a incidentes**
La investigación de la respuesta a incidentes requiere de la recopilación de información en varias fuentes desconectadas, la organización de los datos y el análisis de estos, así como una serie de pasos manuales para confirmar que se han afectado uno o más sistemas. Durante la fase de investigación, los datos valiosos podrían robarse de los sistemas infectados y los atacantes podrían propagarse de forma lateral en toda la red. Para realizar una investigación completa, en ocasiones se tiene que poner en riesgo la propiedad intelectual.

### MODERNICE LA RESPUESTA A INCIDENTES CON THREAT RESPONSE

**Recopilación e investigación manual de amenazas**
La respuesta a incidentes tiene cuatro principales áreas de enfoque:

1. Investigar quién, qué y dónde, incluyendo los usuarios y los sistemas atacados
2. Verificar los datos forenses de los sistemas atacados con los informes forenses en espacios aislados
3. Detener el sangrado y la pérdida de direcciones IP con medidas de cuarentena y confinamiento
4. Seguir los indicadores clave de rendimiento (KPI) de respuesta a incidentes para asegurarse de que los incidentes no se excluyan, se olviden o se pasen por alto

Estas áreas de enfoque ayudan a identificar qué usuarios se han infectado y la gravedad y urgencia de las amenazas, a eliminar los falsos positivos y a detener la propagación de la infección y de la exfiltración de datos.

**Quién, qué y dónde con Threat Response**
Determine de inmediato qué usuarios, departamentos y grupos internos han sido afectados en la red. El hecho de saber "quién" significa que podrá priorizar los objetivos de alto valor, tales como el director financiero, el personal ejecutivo y los sistemas de finanzas, por encima del departamento de correspondencia.

Además del contexto y la inteligencia internos, los factores externos pueden brindar claves en cuanto a direcciones IP o dominios sospechosos en las alertas de seguridad. Estos factores se integran previamente en Threat Response para ofrecer otro nivel de análisis automatizado a los grupos de seguridad.

Algunos factores externos clave que se pueden analizar son:

- Antigüedad o registro reciente del dominio
- Lista negra de dominios
- Reputación de direcciones IP y URL
- Ubicación geográfica de direcciones IP

**Confirmación de la infección mediante la verificación automática de indicadores de compromiso (IOC)**
Threat Response recopila y analiza los datos forenses de los sistemas atacados para brindar una instantánea abundante de los IOC. Los datos de IOC incluyen una lista reciente de cambios en el sistema (registro y archivos modificados), de procesos activos y de conexiones de red abiertas. Esta información se compara con los cambios informados por los sistemas de análisis de malware y otros eventos que hayan sido recibidos en el sistema, a fin de brindar perspectivas en cuanto a la integridad del cliente.

Otra funcionalidad clave consiste en buscar infecciones pasadas en los sistemas atacados. Cada vez que Threat Response realiza una recopilación de extremos a petición, no solamente verifica los IOC del ataque actual, sino que busca IOC de infecciones pasadas que Threat Response haya visto en ese sitio. Eso se traduce en un método rápido y eficaz para verificar que las infecciones pasadas no se hayan perpetrado y propagado en el sistema atacado actualmente.

**Integración instantánea con inteligencia superior y herramientas de terceros**
Por medio de la integración de VirusTotal, los archivos se pueden verificar no solamente una vez, sino a lo largo del tiempo, con el fin de detectar cuántos de los más de 50 motores antivirus detectan firmas o propiedades malintencionadas en los archivos colocados, descargados o descomprimidos durante una potencial infección.

Las fuentes de inteligencia superior incorporadas en Threat Response se verifican automáticamente con cada uno de los dominios y las direcciones IP proporcionados en cada alerta de seguridad e informe de espacio aislado. La verificación automática elimina las horas de trabajo tedioso y de búsqueda manual en cada uno de los servicios de inteligencia para encontrar las direcciones IP y los hosts atacantes que saquen provecho de los sitios malintencionados conocidos.

El análisis brinda inteligencia procesable que permite la priorización, lo cual pone a Threat Response en acción.

**Confine la amenaza**
Para detener el sangrado, ciertos cambios en la red pueden brindar protección inmediata:

- Evitar que las infecciones se propaguen de un sistema a otro
- Evitar que las señales de control lleguen al malware
- Evitar que los datos confidenciales lleguen a los sitios externos

Threat Response automatiza el confinamiento mediante el uso de los dispositivos de aplicación de políticas actuales con el fin de acortar la distancia entre la detección de la amenaza y la protección en tiempo real.

**"Proofpoint acorta la distancia entre la detección de amenazas y la respuesta rápida al brindar a nuestro grupo datos contextuales detallados de cada incidente, así como compatibilidad con una variedad de opciones de aplicación de políticas en la red. Es nuestro analista de respuesta a incidentes en una caja".**

Kevin Moore, director de tecnología de la información de Fenwick & West, LLP

## ESPECIFICACIONES

**Fuentes de eventos:**

- Proofpoint Targeted Attack Protection
- FireEye MPS
- Palo Alto Networks WildFire
- HP ArcSight
- QRadar/Juniper STRM
- Splunk
- Cisco FirePOWER NGIPS
- Suricata

**Dispositivos de aplicación de políticas:**

- Cisco ASA
- Palo Alto Networks
- Check Point
- Cisco IOS
- Juniper SRX (JUNOS)
- Fortinet FortiGate
- Blue Coat
- Microsoft Exchange/O365
- OpenDNS

**ACERCA DE PROOFPOINT**
Proofpoint, Inc. (NASDAQ:PFPT) es una empresa de ciberseguridad de siguiente generación que permite que las organizaciones protejan la manera en que la gente trabaja en la actualidad de las amenazas avanzadas y los riesgos de cumplimiento. Proofpoint ayuda a los profesionales de ciberseguridad a proteger a sus usuarios de los ataques avanzados que se dirigen a ellos (por medio de correo electrónico, aplicaciones móviles y redes sociales), a proteger la información crítica que la gente crea y a equipar a sus grupos con la inteligencia y las herramientas adecuadas para que respondan rápidamente cuando algo vaya mal. Las organizaciones líderes de todos los tamaños, incluyendo más del 50 por ciento de las empresas Fortune 100, confían en las soluciones de Proofpoint, las cuales se han diseñado para los entornos de TI móviles y habilitados para las redes sociales de hoy, y aprovechan tanto la potencia de la nube como una plataforma de análisis centrado en macrodatos para combatir las amenazas avanzadas modernas.