Alianza entre Proofpoint y CrowdStrike

CROWDSTRIKE

Protección de sus empleados y sus dispositivos

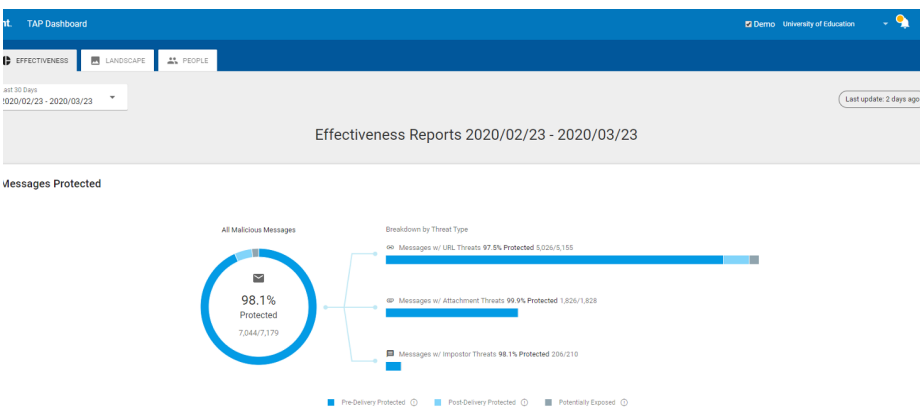
RESUMEN DE LA ALIANZA

- Aprovecha el intercambio de la mejor inteligencia sobre amenazas entre fuentes de primer nivel
- Ofrece protección frente amenazas multicapa
- Protege los dispositivos y los datos de las organizaciones frente a sofisticados ataques con y sin malware
- Proporciona contexto y visibilidad inmediata de los atacantes y los vectores de ataque

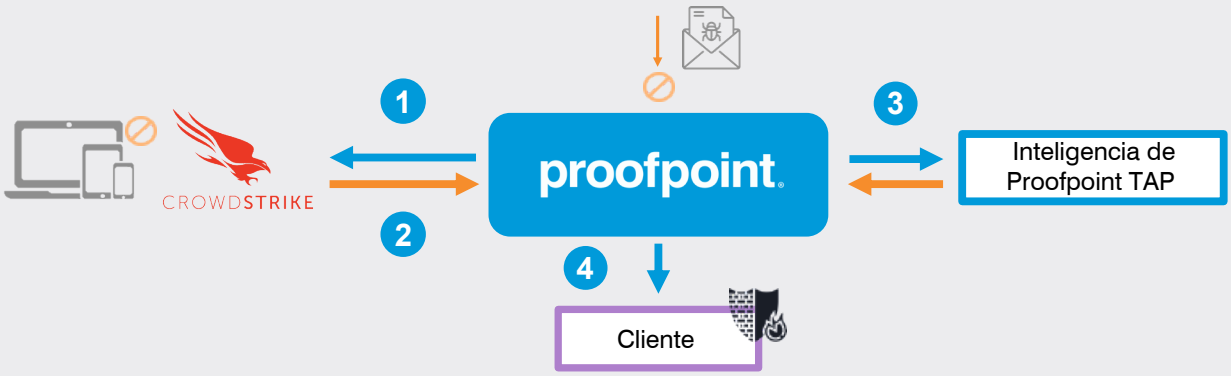
Las empresas siguen luchando contra las amenazas avanzadas que atacan a sus organizaciones y, por tanto, nuevas estrategias para mitigar el riesgo de estas amenazas dirigidas son necesarias. Sabemos que más del 90 % de las amenazas llegan a través del correo electrónico. Proofpoint y CrowdStrike se han unido para ofrecer a sus clientes comunes una estrategia mejorada de seguridad, abarcando desde el correo electrónico hasta el dispositivo final del usuario.

Proofpoint Targeted Attack Protection (TAP) le ayuda a ir siempre por delante de los agresores, gracias a su innovador enfoque que detecta, analiza y bloquea las amenazas avanzadas antes de que lleguen a su bandeja de entrada. Este tipo de amenazas incluyen el ransomware y otras que se distribuyen a través de los adjuntos y URL maliciosas que incluyen los mensajes de correo electrónico. La arquitectura de la plataforma CrowdStrike Falcon, con un único agente ligero, emplea inteligencia artificial en la nube y ofrece protección y visibilidad en tiempo real a toda la organización. Esto constituye un innovador enfoque para gestionar este tipo de amenazas. Obtendrá visibilidad a bajo nivel en tiempo real de la actividad de sus endpoints, a la vez que funciones de investigación y corrección de amenazas para detener las brechas de seguridad.

A través de esta alianza técnica, nos hemos centrado en la visión compartida de proteger a las personas y sus dispositivos frente a las más sofisticadas amenazas existentes en la actualidad. Obtendrá una seguridad adicional y mayor visbilidad, sin coste adicional, además de las ventajas que implica la integración de estas dos soluciones de primer nivel.



Panel de Proofpoint TAP



1. Proofpoint TAP Attachment Defense inspeccionará el archivo y también consultará la API de inteligencia de CrowdStrike.
2. Si CrowdStrike sabe que el archivo es malicioso, Proofpoint TAP lo pondrá en cuarentena y no se entregará al usuario.
3. Si CrowdStrike no tiene conocimiento del archivo, pero Proofpoint TAP lo considera malicioso, se pondrá en cuarentena y no se entregará al usuario.
4. Se mejora la protección del cliente mediante el intercambio de inteligencia sobre amenazas entre ambas plataformas.

CÓMO FUNCIONA LA INTEGRACIÓN

Inteligencia de amenazas compartida

Gracias a la integración, Proofpoint TAP y la plataforma CrowdStrike Falcon ahora comparten inteligencia de amenazas. Cuando un cliente recibe un mensaje de correo electrónico que contiene un archivo adjunto, Proofpoint TAP pone en marcha su entorno aislado de análisis de amenazas (Sandbox) para determinar si es malicioso. Al mismo tiempo, Proofpoint TAP consultará a CrowdStrike Falcon X sobre la reputación del archivo. Si CrowdStrike tiene identificado el archivo como malicioso, informará de vuelta a Proofpoint TAP. A partir de este punto, el mensaje y el archivo son censurados y se bloquean para impedir que lleguen al usuario final. La inteligencia compartida entre estas dos soluciones líderes en el mercado le ayudará a defenderse contra los ataques dirigidos avanzados.

Protección multicapa

Para obtener una protección multicapa, Proofpoint TAP a su vez comparte información de amenazas con la plataforma CrowdStrike Falcon. De esta forma, protegerá a su personal con mayor seguridad, tanto en el uso del correo electrónico como en sus dispositivos. Cuando TAP detecta que ha llegado un archivo malicioso a través del correo electrónico, podemos consultar a CrowdStrike Falcon X - el módulo de inteligencia de amenazas - para determinar si es conocido. Si el contenido malicioso es conocido, no se realiza ninguna acción, ya que el dispositivo estará protegido. En caso de que sea desconocido, se añade la información de identificación del archivo malicioso (hash) a la lista de indicadores de compromiso personalizados de CrowdStrike. Además, si el contenido malicioso intenta ejecutarse en el dispositivo, se crea una alerta. Esta inteligencia personalizada añadida a CrowdStrike Falcon X le ayudará en el futuro a defenderse de forma proactiva frente a ataques similares que se observen en otros endpoints en su organización.

La integración de Proofpoint y CrowdStrike facilita la detección, la investigación y la corrección de las amenazas por correo electrónico, mejorando el nivel de protección de su organización y sus empleados.

MÁS INFORMACIÓN

Para obtener más información, visite **proofpoint.com/es**.