Partenariat entre Proofpoint et CrowdStrike

CROWDSTRIKE

Protégez vos collaborateurs et leurs endpoints

LE PARTENARIAT EN BREF

- Tirez parti du partage de threat intelligence de pointe.
- Bénéficiez d'une protection multicouche contre les malwares.
- Protégez les endpoints et les données de l'entreprise contre les malwares sophistiqués et les attaques sans malware.
- Obtenez une visibilité et un contexte immédiats sur les cyberpirates et les vecteurs d'attaque.

Les entreprises ont du mal à faire face aux menaces avancées, et de nouvelles approches sont nécessaires pour en atténuer les risques. De plus, nous savons que plus de 90 % de ces menaces utilisent l'email comme vecteur. Proofpoint et CrowdStrike s'allient pour offrir à leurs clients communs un niveau de sécurité renforcé, depuis la réception des emails jusqu'aux endpoints.

Proofpoint Targeted Attack Protection (TAP) vous aide à garder une longueur d'avance sur les attaquants : son approche innovante détecte, analyse et bloque les menaces avancées avant qu'elles n'atteignent vos boîtes de réception. Cette protection couvre les ransomwares et autres menaces avancées transmises par des emails contenant des pièces jointes et des URL malveillantes. La plate-forme CrowdStrike Falcon, avec son architecture d'agent léger, exploite tout le potentiel de l'intelligence artificielle à l'échelle du cloud et offre une protection et une visibilité en temps réel dans toute l'entreprise. Cette approche innovante vous permettra de gérer efficacement les menaces. Vous disposez d'une visibilité détaillée en temps réel sur les activités des endpoints et pouvez effectuer des investigations et des corrections afin de bloquer les compromissions.

Ce partenariat technique repose sur une vision commune : la protection des personnes et de leurs endpoints contre les menaces actuelles les plus sophistiquées. Vous disposez d'une sécurité renforcée et d'une visibilité étendue, sans frais supplémentaires. De même, vous profitez des avantages d'une intégration entre ces deux solutions de pointe.

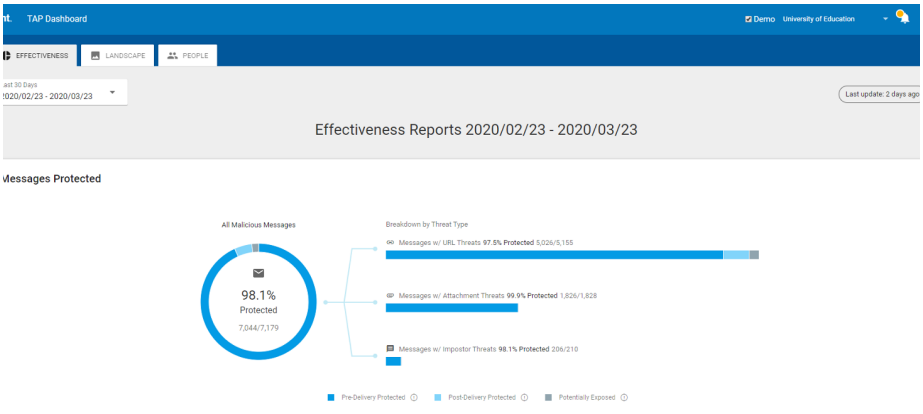
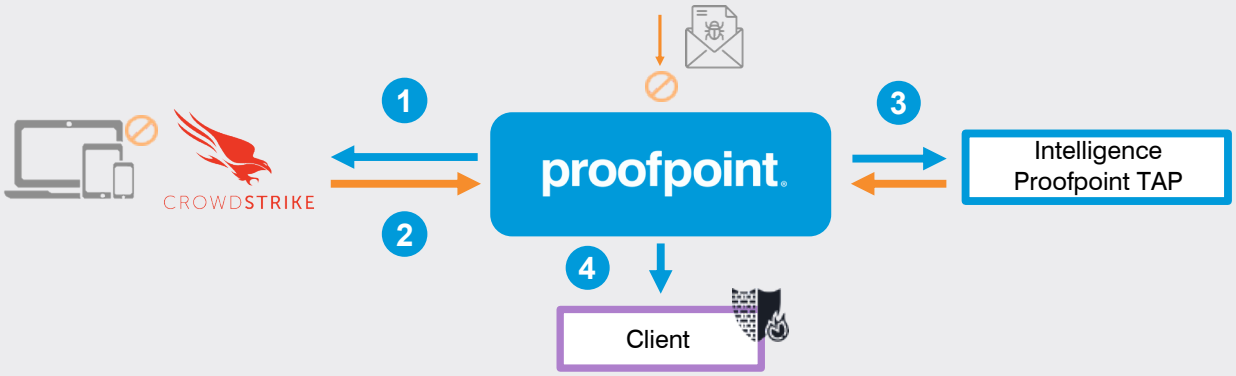


Tableau de bord Proofpoint TAP



1. Proofpoint TAP Attachment Defense inspecte le fichier et interroge l'API CrowdStrike Intelligence.
2. Si le fichier est connu de CrowdStrike comme étant malveillant, Proofpoint TAP le met en quarantaine et le message n'est pas remis au destinataire.
3. Si le fichier est inconnu de CrowdStrike, mais qu'il est jugé malveillant par Proofpoint TAP, il est mis en quarantaine et n'est pas remis au destinataire.
4. Protection renforcée pour le client grâce au partage d'informations de threat intelligence.

FONCTIONNEMENT DE L'INTÉGRATION

Threat intelligence partagée

L'intégration permet à Proofpoint TAP et à la plate-forme CrowdStrike Falcon de partager des informations de threat intelligence. Lorsqu'un email contenant un fichier est envoyé à un client, Proofpoint TAP démarre une analyse sandbox pour déterminer s'il est malveillant. Parallèlement, Proofpoint TAP interroge la plate-forme CrowdStrike Falcon X pour obtenir des informations sur la réputation du fichier. Si CrowdStrike sait que le fichier est malveillant, il en informe Proofpoint TAP. Le message et le fichier sont alors marqués comme malveillants et ne sont pas remis au destinataire. Cette threat intelligence partagée vous aide à vous défendre contre les attaques ciblées avancées en tirant parti de deux solutions de pointe.

Protection multicouche

Pour assurer une protection multicouche, Proofpoint TAP partage des informations sur les menaces avec la plate-forme CrowdStrike Falcon. Cette alliance vous garantit un niveau de sécurité renforcé pour que vous puissiez protéger efficacement vos utilisateurs, tant au niveau de la messagerie que des endpoints. Lorsque Proofpoint TAP détecte qu'un fichier malveillant a été délivré par email, il peut interroger CrowdStrike Falcon X, le module de threat intelligence, pour déterminer s'il est connu. Si ce contenu malveillant est connu, aucune action n'est entreprise puisque l'appareil est déjà protégé. En revanche, s'il n'est pas connu, les informations de hachage correspondantes sont ajoutées à la liste CrowdStrike d'indicateurs de compromission personnalisés. De plus, une alerte est générée si le contenu malveillant essaie de s'exécuter sur l'appareil. Cet indicateur de compromission personnalisé ajouté au référentiel de CrowdStrike Falcon X vous aidera à vous défendre de façon proactive contre des attaques similaires qui pourraient cibler à l'avenir d'autres endpoints de votre entreprise.

L'intégration entre Proofpoint et CrowdStrike permet de détecter, d'investiguer et de neutraliser facilement les menaces par email, offrant ainsi un niveau de protection renforcé à votre entreprise et à ses collaborateurs.

EN SAVOIR PLUS

Pour plus d'informations, visitez notre site à l'adresse : **proofpoint.com/fr**.