proofpoint.

FICHE TECHNIQUE

Proofpoint Account Takeover Protection

Détectez, analysez et neutralisez les prises de contrôle de comptes en plusieurs phases

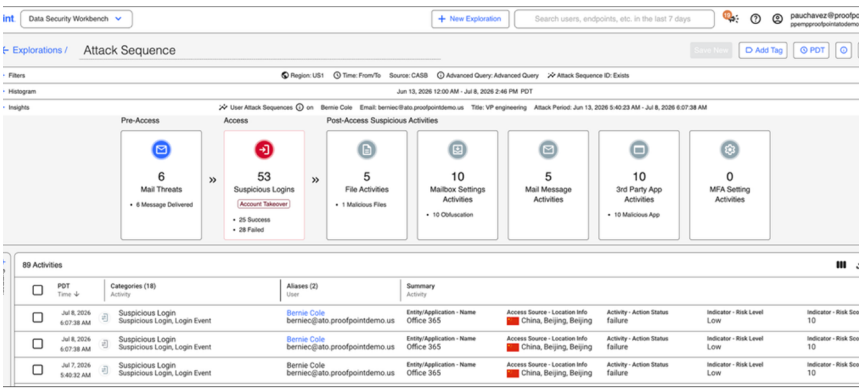
Principaux atouts

- **Détection des compromissions de compte en plusieurs phases avec une grande précision**
- **Accélération des investigations grâce à une visibilité unifiée tout au long du cycle de vie des attaques**
- **Réduction de la durée d'implantation des cybercriminels grâce à une réponse et à une correction automatisées**
- **Prévention de la fraude, des fuites de données et des perturbations des activités liées aux comptes compromis**
- **Renforcement de la défense en profondeur avec Proofpoint Collaboration Security Prime**

Proofpoint Account Takeover Protection aide les entreprises à détecter, à analyser et à contenir les comptes utilisateur compromis tout au long du cycle de vie des prises de contrôle de comptes (ATO) – des indicateurs de pré-accès et de la compromission réussie aux activités cybercriminelles post-accès.

Optimisé par Proofpoint Nexus® AI et la threat intelligence, Proofpoint Account Takeover Protection permet une détection extrêmement fiable des compromissions de compte confirmées tout en offrant une visibilité complète sur le comportement des cybercriminels. Les équipes de sécurité peuvent rapidement comprendre la portée d'un incident, accélérer les investigations et contenir les menaces avant qu'elles ne dégénèrent en piratage de la messagerie en entreprise (BEC, Business Email Compromise), vol de données, déplacement latéral ou autres attaques ayant un impact sur les activités.

Dans le cadre de Proofpoint Collaboration Security Prime, Proofpoint Account Takeover Protection s'intègre à Threat Protection Workbench et à la Threat Interaction Map pour étendre les investigations au-delà d'un seul compte compromis. En établissant une corrélation entre les compromissions d'identité et les menaces par email, les interactions avec les utilisateurs et les activités des cybercriminels, il aide les équipes de sécurité à mieux comprendre la campagne d'attaque. Cela permet d'accélérer les investigations, de mieux informer les décisions de réponse et de renforcer la correction.



1. Figure 1. Bénéficiez d'une visibilité complète sur l'ensemble du cycle de vie des attaques ATO, des activités pré-accès aux activités post-accès.

Détection extrêmement fiable des attaques ATO

Optimisé par Proofpoint Nexus AI, Proofpoint Account Takeover Protection permet une détection extrêmement fiable des compromissions de compte confirmées touchant Microsoft 365, Google Workspace et Okta.

En analysant en permanence les activités des utilisateurs tout au long du cycle de vie des prises de contrôle de comptes (des indicateurs de pré-accès au comportement des cybercriminels post-accès), Proofpoint Account Takeover Protection identifie les compromissions confirmées avec un degré élevé de confiance et hiérarchise les détections en fonction de la gravité du risque (critique, élevé ou modéré). Chaque détection comporte les indicateurs comportementaux et les éléments de preuve ayant contribué à l'identification, ce qui aide les analystes à comprendre rapidement pourquoi un compte a été identifié comme compromis, à hiérarchiser les actions de réponse et à intervenir en toute confiance.

Visibilité complète sur l'attaque

Une fois la compromission du compte confirmée, Proofpoint Account Takeover Protection offre une visibilité complète sur la séquence d'attaque, ce qui permet aux équipes de sécurité de comprendre comment l'attaque s'est déroulée et ce que le cybercriminel a fait après avoir obtenu un accès.

Des analyses forensiques complètes révèlent les activités post-accès, notamment la manipulation des boîtes email, les règles de boîte de réception malveillantes, l'exploitation d'OAuth, les modifications des privilèges, le phishing interne, les activités email suspectes et les techniques de persistance. Cela aide les analystes à déterminer rapidement la portée, le niveau de sophistication et l'ampleur de l'attaque. En reconstituant la séquence d'attaque et en mettant en évidence les utilisateurs et les ressources touchés, Proofpoint Account Takeover Protection contribue à accélérer les investigations, soutient des décisions de réponse plus éclairées et améliore la correction.

Réponse automatisée aux menaces

Proofpoint Account Takeover Protection aide les entreprises à contenir rapidement les menaces actives grâce à des actions de correction automatisées qui perturbent l'accès des cybercriminels et accélèrent la récupération. Parmi les actions de réponse : forcer les changements de mot de passe, réinitialiser les mots de passe utilisateur, révoquer les sessions actives, supprimer les règles de boîte email malveillantes, révoquer les applications OAuth tierces non autorisées et autres mesures de correction conçues pour éliminer la persistance des cybercriminels et restaurer l'intégrité des comptes.

En automatisant les actions de confinement critiques, les équipes de sécurité peuvent réduire la durée d'implantation des cybercriminels, limiter les déplacements latéraux, minimiser les perturbations des activités et accélérer la récupération après une compromission de compte.

Défense en profondeur avec Proofpoint Collaboration Security Prime

Dans le cadre de Proofpoint Collaboration Security Prime, Proofpoint Account Takeover Protection s'étend au-delà des compromissions de compte pour offrir une protection coordonnée sur l'ensemble du cycle de vie des attaques humaines. Tandis que Proofpoint Account Takeover Protection détecte, analyse et contient les comptes compromis, Proofpoint Prime renforce la protection en bloquant les menaces avant la compromission, en corrélant les attaques sur les canaux de messagerie et de collaboration, en améliorant le comportement des utilisateurs grâce à une formation adaptative et en fournissant des investigations et une réponse unifiées via Threat Protection Workbench et la Threat Interaction Map.

Ensemble, ces fonctionnalités soutiennent une stratégie de défense en profondeur qui aide les entreprises à prévenir les attaques, à atténuer les menaces actives, à renforcer la résilience des utilisateurs et à améliorer continuellement leur niveau de sécurité grâce à une plate-forme intégrée.

Visitez le site **proofpoint.com/fr** pour en savoir plus