proofpoint.

FICHE SOLUTION

Proofpoint Active Exploits Protection

Bloquez les exploits au tout début — avant qu'ils ne s'exécutent

Principaux avantages

- Bénéficiez d'une protection de premier ordre contre les exploits en identifiant et en bloquant l'activité d'exploitation à la porte d'entrée de la boîte email — avant l'exécution de la charge virale ou la compromission de l'endpoint.
- Priorisez les vulnérabilités en fonction des exploits actifs observés dans la nature.
- Réduisez l'exposition avant le déploiement des correctifs, tout en vous protégeant contre les malwares basés sur des exploits et les activités de commande et de contrôle.
- Accélérez les investigations grâce à des données contextuelles sur les menaces actuelles et anciennes ainsi qu'à des renseignements en matière de détection continuellement mis à jour.
- Préparez-vous pour les workflows de sécurité pilotés par l'IA et les agents.

Présentation

La vitesse et l'ampleur des exploitations ne cessent d'augmenter. Outre le fait que le nombre de nouvelles vulnérabilités divulguées atteint des niveaux record, les cybercriminels les transforment en armes plus rapidement que jamais. Les solutions traditionnelles de gestion des vulnérabilités et de gestion de l'exposition définissent souvent les priorités en fonction des scores de gravité et des risques théoriques — mais manquent de visibilité sur les failles que les cybercriminels tentent activement d'exploiter.

Proofpoint Active Exploits Protection change la donne.

Grâce à la visibilité dès le départ qu'il offre sur la distribution des exploits via les emails et le trafic réseau, Proofpoint aide les entreprises à identifier les activités malveillantes avant que la charge virale ne s'exécute. La solution combine renseignements sur les exploits actifs, priorisation tenant compte des cybercriminels et fonctionnalités de protection instantanée pour aider les équipes de sécurité à se concentrer sur ce qui compte le plus et à réduire l'exposition plus rapidement. Le résultat ? Une approche plus proactive de la protection contre les exploits, basée sur la prévention des attaques à un stade plus précoce de la chaîne d'attaque.

La solution : des renseignements sur les exploits dès le départ et une protection instantanée

Proofpoint Active Exploits Protection transforme les renseignements sur les exploits actifs en protection exploitable et en réponse priorisée. La solution combine renseignements sur les exploits tenant compte des cybercriminels, détection des menaces basée sur les emails et le réseau et intégrations opérationnelles pour aider les entreprises à identifier et à bloquer les activités d'exploitation avant leur exécution.

Grâce à une visibilité de premier ordre sur les exploits dérivée des emails, qui sont le point de départ de nombreuses attaques modernes, Proofpoint peut identifier les tentatives de distribution d'exploits et le comportement réel des cybercriminels dès la première phase de la chaîne d'attaque, avant l'exécution de la charge virale, la compromission des endpoints ou le déplacement latéral.

Proofpoint Active Exploits Protection tire parti de ces renseignements uniques sur les vulnérabilités et de la large couverture des menaces basées sur le réseau et les exploits pour aider les entreprises à prioriser les vulnérabilités en fonction de leur exploitation active, à réduire leur exposition en attendant l'application des correctifs, et à accélérer les investigations grâce à une threat intelligence exploitable.

Donnez la priorité aux exploits actifs plutôt qu'aux risques théoriques

Concentrez les efforts de remédiation sur les vulnérabilités associées à une exploitation active — et pas seulement sur les scores CVSS élevés.

Proofpoint Active Exploits Protection met en corrélation les renseignements sur les exploits et le comportement des cybercriminels observé à travers des sources de télémétrie mondiales pour aider les entreprises à identifier rapidement les vulnérabilités qui présentent un risque opérationnel immédiat.

Cette approche axée sur les cybercriminels aide les équipes de sécurité à réduire les informations parasites, à mieux établir les priorités et à concentrer les ressources sur les expositions les plus susceptibles d'être exploitées.

Les principales fonctionnalités sont les suivantes :

- Priorisation de l'application des correctifs en fonction des CVE activement exploitées
- Distinction entre les menaces urgentes et les risques de moindre priorité
- Priorisation des correctifs guidée par un contexte clair et exploitable sur les menaces, y compris des flux de réputation des adresses IP et des domaines en temps réel
- Alignement des priorités sur l'activité réelle des cybercriminels pour un meilleur ciblage opérationnel

Bénéficiez d'une protection instantanée en attendant l'application des correctifs

L'application de correctifs prend du temps. Proofpoint Active Exploits Protection aide les entreprises à réduire leur exposition durant cette période en fournissant des renseignements constamment mis à jour sur les exploits et en offrant une protection instantanée des emails et du trafic réseau.

Il fournit une logique de détection fiable et en temps opportun pour les menaces avancées, y compris :

- Distribution de malwares
- Communications de commande et contrôle
- Kits d'exploitation
- Phishing d'identifiants de connexion
- Propagation de l'attaque
- Ransomwares, botnets
- Anomalies des protocoles et des applications
- Minage de cryptomonnaie
- Attaques par déni de service distribué (DDoS)
- Attaques contre les systèmes de contrôle et d'acquisition de données (SCADA)

Les principales fonctionnalités sont les suivantes :

- Renseignements sur les exploits constamment mis à jour et conçus pour améliorer la protection à un stade plus précoce de la chaîne d'attaque
- Règles de détection basées sur le réseau pour les systèmes IDS, IPS et NGFW et contrôles de sécurité associés
- Signatures fiables pour les callbacks de malware, les injecteurs, les communications de commande et contrôle, l'obfuscation, les menaces liées aux kits d'exploitation et l'exfiltration
- Mises à jour quotidiennes des règles pour suivre l'évolution du paysage des menaces
- Couverture des principales familles de malwares, des campagnes d'attaque et des vecteurs de menaces basés sur le réseau
- Prise en charge des formats IDS et IPS largement utilisés, y compris des déploiements compatibles avec Suricata et Snort

Enrichissez les outils de sécurité avec une threat intelligence mondiale

Proofpoint Active Exploits Protection fournit des renseignements exploitables qui s'intègrent à un large éventail d'outils de sécurité, y compris les pare-feux, les solutions IDS, IPS, NGFW, UTM et SIEM, les systèmes d'authentification, les plates-formes de traque des menaces, les workflows de réponse aux incidents et les outils de sécurité personnalisés.

La solution fournit des renseignements sur la réputation et les menaces concernant les adresses IP, les domaines, les malwares, les signatures et les campagnes suspects et malveillants, ainsi que les activités d'attaque associées.

Les principales fonctionnalités sont les suivantes :

- Threat intelligence actuelle et historique pour les adresses IP, les domaines, les hachages de malware, les signatures et le contenu des messages
- Flux de réputation des adresses IP et des domaines organisés par catégorie de menaces et score de confiance
- Mises à jour fréquentes des flux avec vieillissement accéléré pour refléter l'activité actuelle
- Base de données mondiale consultable sur les menaces permettant la navigation, l'exploration en profondeur et les investigations
- Prise en charge de multiples formats de flux à des fins d'intégration opérationnelle, y compris les formats TXT, CSV, JSON, IDS et compressés
- Enrichissement basé sur API pour les outils SIEM, TIP, de réponse aux incidents et internes

Renforcez la précision de la détection et réduisez le bruit

Proofpoint Active Exploits Protection s'appuie sur les observations de menaces réelles, les analyses des malwares, le feedback de capteurs mondiaux et les recherches consacrées aux menaces. Cette approche contribue à une détection extrêmement fiable, tout en réduisant les faux positifs dans les outils de sécurité réseau existants.

Les principales fonctionnalités sont les suivantes :

- Contenu des détections piloté par les recherches et fondé sur les menaces observées
- Analyse des malwares en sandbox afin de capturer le comportement réseau après exécution
- Feedback en provenance de capteurs mondiaux afin d'accroître la précision de la détection
- Descriptions de signatures, références et documentation pour soutenir les workflows des analystes
- Application des règles basée sur des catégories et alignée sur les priorités de l'entreprise

Évoluez avec des workflows pilotés par l'IA

Proofpoint Active Exploits Protection est conçu pour prendre en charge les opérations de sécurité modernes axées sur la threat intelligence. Les capacités futures devraient permettre l'accès à la threat intelligence via le protocole MCP et des workflows basés sur des agents, facilitant des cas d'utilisation pilotés par des API et l'IA.

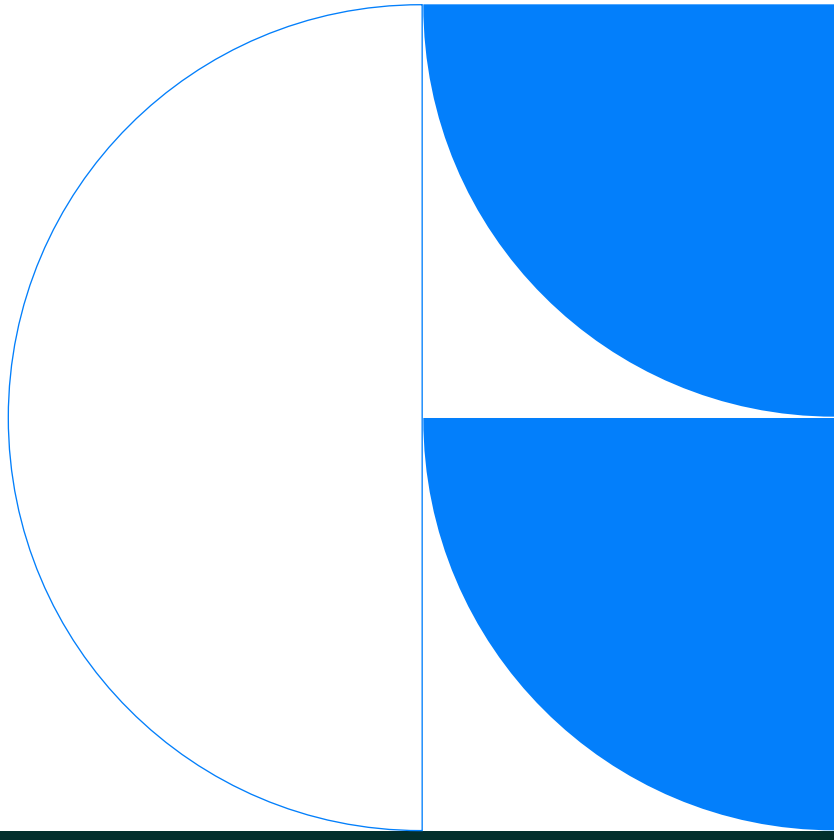
Ces workflows visent à aider les équipes à intégrer directement la threat intelligence priorisée dans des opérations de sécurité automatisées, à accélérer la prise de décisions et à réduire le tri manuel.

Résumé

Proofpoint Active Exploits Protection aide les entreprises à prévenir les attaques basées sur des exploits avant toute compromission en combinant visibilité de premier ordre sur les exploits dérivée des emails, renseignements sur les exploits tenant compte des cybercriminels et fonctionnalités de protection instantanée.

Plutôt que de se fier uniquement à des scores de gravité des vulnérabilités ou à des modèles d'exposition théoriques, Proofpoint Active Exploits Protection permet aux équipes de sécurité d'établir les priorités en fonction des cibles réelles des cybercriminels.

En unifiant l'établissement des priorités, la protection et l'investigation, Proofpoint Active Exploits Protection aide les équipes de sécurité à se concentrer sur ce qui compte, à offrir une protection instantanée et à enquêter plus rapidement.



proofpoint.