

FICHE TECHNIQUE

Proofpoint Satori

Opérations de sécurité autonomes : gouvernées, explicables et conçues pour évoluer



Principaux avantages

- Élimination des tâches fastidieuses liées à la sécurité de niveau 1 grâce à l'automatisation des décisions de tri répétitives
- Gestion cohérente des volumes d'alertes sans avoir besoin de personnel supplémentaire
- Amélioration de la rapidité, de l'exactitude et de la cohérence grâce à l'application de la même logique à chaque cas
- Exécution autonome combinée à des mesures de protection, à une supervision humaine, à l'explicabilité et à des pistes d'audit

Les équipes de sécurité modernes sont débordées. Les emails suspects signalés par les utilisateurs, les alertes de prévention des fuites de données (DLP) et les violations des règles génèrent chaque jour des milliers de décisions répétitives et peu utiles. Même lorsqu'elles disposent de systèmes de détection performants, les équipes des centres des opérations de sécurité (SOC) et de sécurité des données restent submergées par le tri de niveau 1. Celui-ci ralentit les temps de réponse, accroît le surmenage et limite la rentabilité des investissements en amont.

Proofpoint Satori résout ces problèmes. Cet ensemble de solutions est conçu pour les opérations de sécurité autonomes. Optimisé par l'IA agentique, Proofpoint Satori automatise en toute sécurité les workflows de sécurité à fort volume. Il élimine les tâches de tri répétitives tout en préservant la confiance, le contrôle et la responsabilité. Les équipes peuvent ainsi étendre les opérations sans compromettre la gouvernance.

Automatisation autonome et axée sur les missions

Proofpoint Satori utilise des workflows en plusieurs étapes, appelés « missions », conçus pour atteindre des objectifs de sécurité spécifiques. Les missions s'appuient sur les données télémétriques détaillées de Proofpoint, mettent en place des mesures de protection, agissent dans les limites autorisées et consignent chaque décision.

Proofpoint Satori s'appuie sur la plate-forme de sécurité centrée sur les personnes et l'IA de Proofpoint. Il a accès à des signaux propriétaires et à des points de contrôle que ses concurrents ne peuvent égaler. Vous bénéficiez ainsi d'un contexte plus détaillé, d'une automatisation plus sûre et d'une intégration plus étroite dans les workflows existants.

Conçu pour être gouverné dès la conception

Proofpoint Satori est conçu pour gagner la confiance des entreprises. Les mesures de protection intégrées

empêchent toute action autonome dangereuse ou risquée. Cela permet de s'assurer que les limites de l'automatisation sont clairement définies. Lorsque les analystes demandent des changements de comportement, la supervision humaine apporte une couche de contrôle supplémentaire qui permet d'approuver, de contester ou d'annuler ces changements selon les besoins.

Chaque décision prise par Proofpoint Satori est explicable. Les analystes peuvent voir le raisonnement qui sous-tend les résultats, au lieu de devoir se fier à une automatisation opaque. Les pistes d'audit complètes enregistrent les classifications et les interactions des analystes, garantissant ainsi la conformité et la transparence. Des changements de comportement sont apportés uniquement après un processus d'escalade explicite et un contrôle humain. De plus, ces changements ne s'appliquent qu'aux cas futurs.

Missions Satori

Satori Abuse Mailbox Agent automatise le triage des e-mails suspects signalés par les utilisateurs. Cela réduit fortement les vérifications manuelles des signalements bénins ou à faible risque. Tout en classant de façon homogène de grands volumes d'e-mails signalés, l'agent fonctionne aussi avec des garde-fous stricts, notamment le respect des protections VIP et l'interdiction de supprimer automatiquement des messages.

Satori DLP Triage Agent automatise l'enrichissement et la priorisation des alertes DLP. En réduisant les faux positifs et la fatigue liée aux alertes, il aide les équipes à se concentrer sur les risques de données les plus critiques. Il garantit que les événements à plus haut risque sont escaladés afin d'être examinés rapidement par un humain.

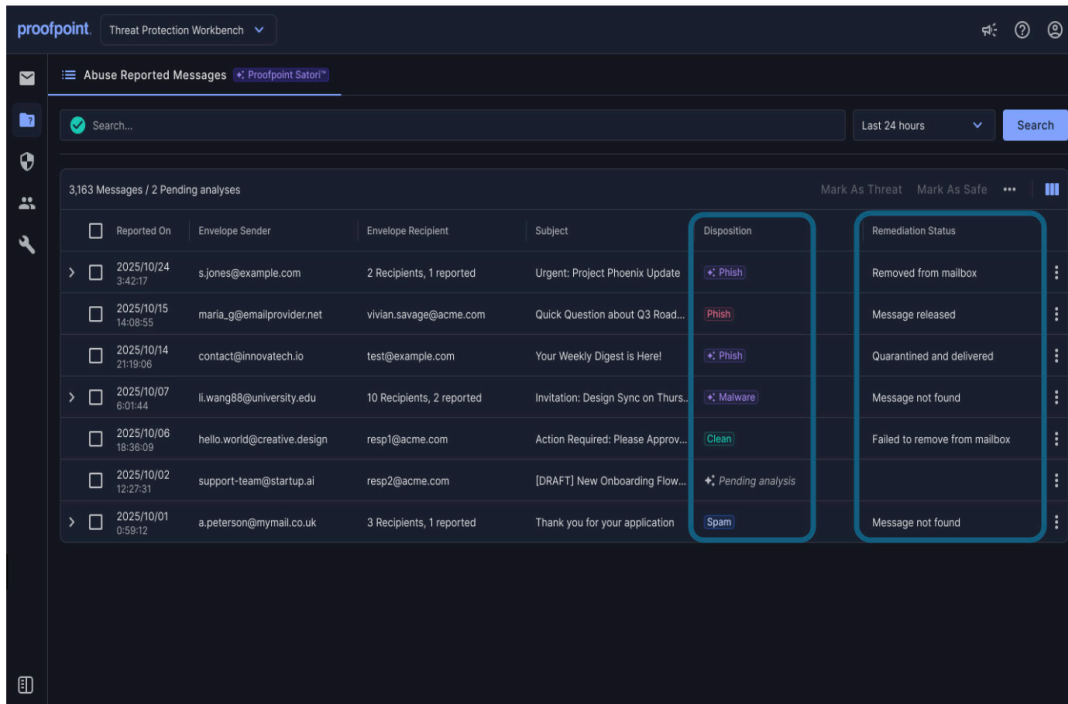


Figure 1 : L'agent Satori Abuse Mailbox attribue un statut aux e-mails de la boîte de signalement d'abus et déclenche les workflows associés.

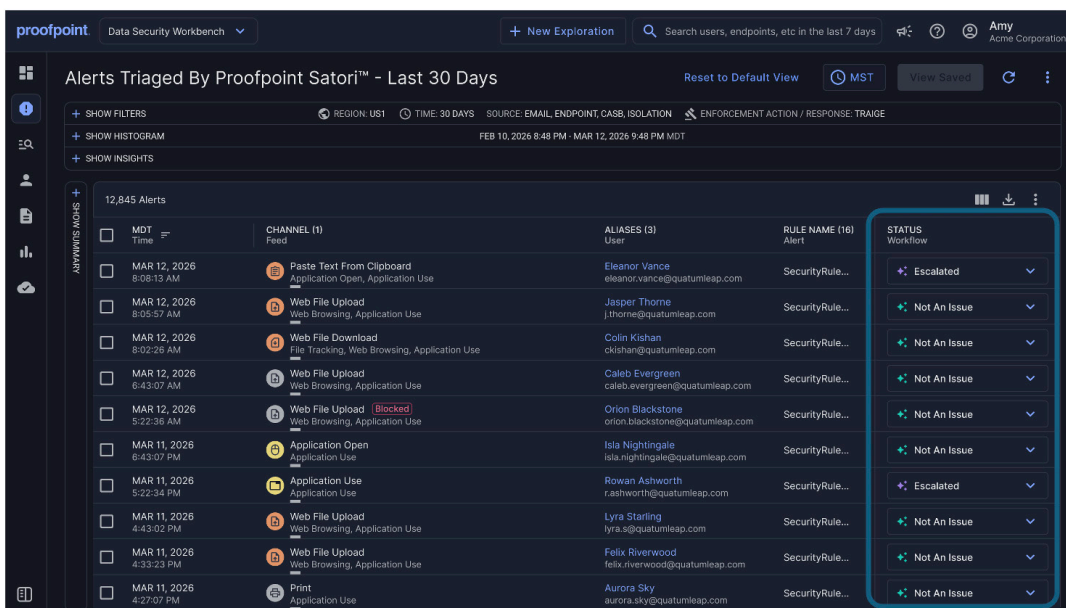


Figure 2 : L'agent de triage DLP Satori évalue les alertes sur les terminaux, le cloud et l'e-mail, puis repère et écarte les faux positifs. Les analystes peuvent utiliser une interface de chat pour poser des questions et obtenir des recommandations sur la manière de traiter les alertes.

proofpoint.

À propos de Proofpoint, Inc. Proofpoint, Inc. est un leader mondial de la cybersécurité centrée sur les personnes et les agents, qui sécurise la manière dont les personnes, les données et les agents d'IA se connectent via la messagerie électronique, le cloud et les outils de collaboration. Proofpoint est un partenaire de confiance pour plus de 80 entreprises du classement Fortune 100, plus de 10 000 grandes entreprises et des millions de petites entreprises. Il les aide à bloquer les menaces, à prévenir les fuites de données et à renforcer la résilience des personnes et des workflows d'IA. La plate-forme de collaboration et de sécurité des données de Proofpoint aide les entreprises de toutes tailles à protéger et à responsabiliser leurs collaborateurs tout en adoptant l'IA en toute sécurité et confiance. Pour en savoir plus, consultez le site www.proofpoint.com/fr.

Suivez-nous: [LinkedIn](#)

Proofpoint est une marque déposée ou un nom commercial de Proofpoint, Inc. aux États-Unis et/ou dans d'autres pays. Toutes les autres marques déposées contenues dans les présentes sont la propriété de leurs détenteurs respectifs.

DÉCOUVRIR LA PLATE-FORME PROOFPOINT →