proofpoint.

HOJA DE DATOS

Proofpoint Satori

Operaciones de seguridad autónomas: gobernadas, explicables y diseñadas para evolucionar

Ventajas principales

- liminación de las tareas tediosas relacionadas con la seguridad de nivel 1 gracias a la automatización de las decisiones de clasificación repetitivas.
- Gestión coherente del volumen de alertas sin necesidad de personal adicional .
- Mejora de la rapidez, la precisión y la coherencia gracias a la aplicación de la misma lógica a cada caso.
- Ejecución autónoma combinada con medidas de protección, supervisión humana, explicabilidad y pistas de auditoría.

Los equipos de seguridad actuales están desbordados. Los correos electrónicos sospechosos denunciados por los usuarios, las alertas de prevención de la pérdida de datos (DLP) y las infracciones de las políticas generan cada día miles de decisiones repetitivas y poco útiles. Incluso cuando cuentan con sistemas de detección eficaces, los equipos de los centros de operaciones de seguridad (SOC) y de seguridad de datos siguen desbordados por la clasificación de nivel 1. Esto ralentiza los tiempos de respuesta, aumenta la sobrecarga de trabajo y limita la rentabilidad de las inversiones previas.

Proofpoint Satori resuelve estos problemas. Este conjunto de soluciones está diseñado para operaciones de seguridad autónomas. Gracias a la IA agéntica, Proofpoint Satori automatiza de forma segura los flujos de trabajo de seguridad de gran volumen. Elimina las tareas repetitivas de clasificación, al tiempo que preserva la confianza, el control y la responsabilidad. De este modo, los equipos pueden ampliar sus operaciones sin comprometer el gobierno.

Automatización autónoma y orientada a misiones

Proofpoint Satori utiliza flujos de trabajo de varias etapas, denominados "misiones", diseñados para alcanzar objetivos de seguridad específicos. Las misiones se basan en los datos telemétricos detallados de Proofpoint, implementan medidas de protección, actúan dentro de los límites autorizados y registran cada decisión.

Proofpoint Satori se basa en la plataforma de seguridad centrada en las personas y en la IA de Proofpoint. Tiene acceso a señales propios y a puntos de control que sus competidores no pueden igualar. De este modo, se beneficia de un contexto más detallado, una automatización más segura y una integración más estrecha con los flujos de trabajo existentes.

Gobierno desde el diseño

Proofpoint Satori está diseñado para ganarse la confianza de las empresas. Las medidas de protección integradas impiden cualquier acción autónoma peligrosa o arriesgada. Esto permite garantizar que los límites de la automatización estén claramente definidos. Cuando los analistas solicitan cambios en el comportamiento, la supervisión humana aporta un nivel adicional de control que permite aprobar, rechazar o anular dichos cambios según sea necesario.
Todas las decisiones que toma Proofpoint Satori son justificables. Los analistas pueden ver el razonamiento que subyace a los resultados , en lugar de tener que confiar en una automatización opaca. Las pistas de auditoría completas recogen las clasificaciones y las interacciones de los analistas, lo que garantiza el cumplimiento normativo y la transparencia. Los cambios en el comportamiento solo se aplican tras un proceso de escalado explícito y una verificación por parte de un operador humano. Además, estos cambios solo se aplican a los casos futuros.

Misiones de Satori

Proofpoint Satori Abuse Mailbox Agent automatiza la clasificación de los correos electrónicos sospechosos denunciados por los usuarios. Este enfoque reduce considerablemente el número de comprobaciones manuales de las notificaciones de menor gravedad o de bajo riesgo. Además, al clasificar constantemente grandes volúmenes de correos electrónicos marcados, el agente trabaja respetando estrictas medidas de seguridad. En particular, hay que respetar las protecciones VIP y no borrar nunca los mensajes de forma automática.
Proofpoint Satori DLP Triage Agent automatiza el enriquecimiento y la priorización de las alertas de DLP. Al reducir los falsos positivos y la sobrecarga de alertas, ayuda a los equipos a centrarse en los riesgos asociados a los datos más críticos. De este modo, los incidentes que presentan un riesgo mayor se remiten para que sean revisados por personal humano en el momento oportuno.

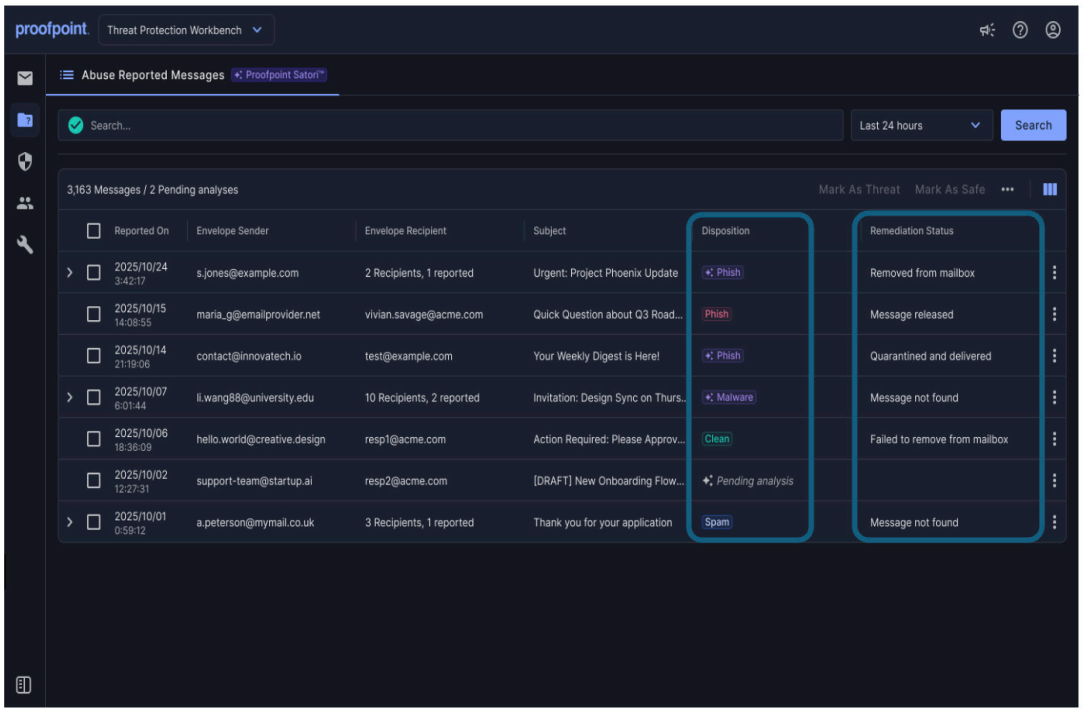

Figura 1: Proofpoint Satori Abuse Mailbox Agent asigna estados a los correos electrónicos que llegan al buzón de notificación de abusos y activa los flujos de trabajo correspondientes.

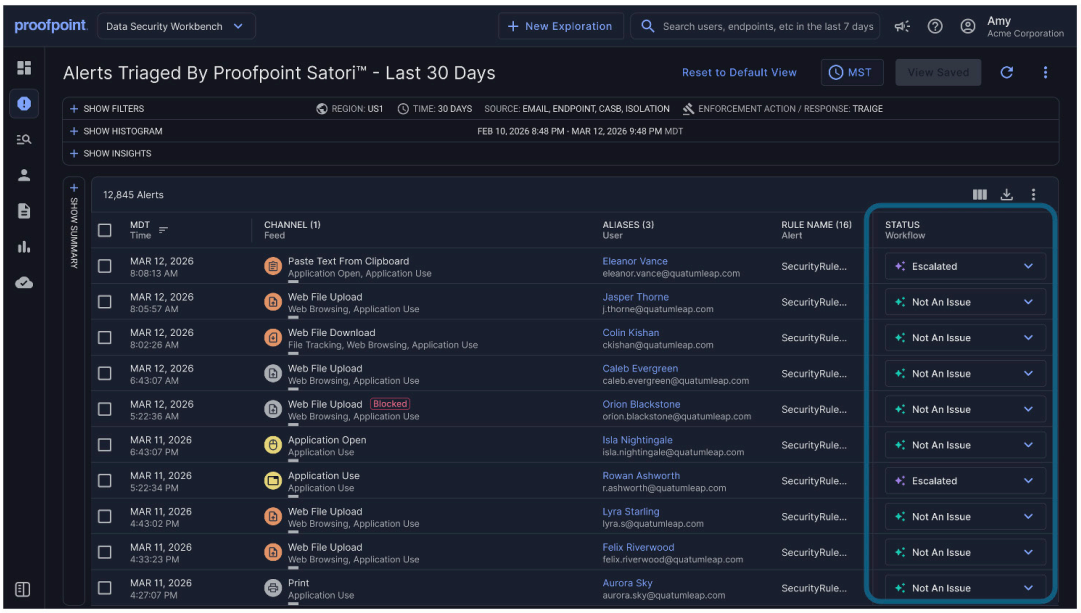

Figura 2: Proofpoint Satori DLP Triage Agent analiza las alertas procedentes de los endpoints, la nube y el correo electrónico, y a continuación identifica y filtra los falsos positivos. Los analistas pueden utilizar una interfaz de chat para plantear preguntas y obtener recomendaciones sobre cómo gestionar las alertas.

proofpoint.

Acerca de Proofpoint, Inc. Proofpoint, Inc. es un líder global en ciberseguridad centrada en las personas y en agentes, protegiendo la forma en que las personas, los datos y los agentes de IA se conectan a través del correo electrónico, la nube y las herramientas de colaboración. Proofpoint es un socio de confianza para más del 80 % de las empresas Fortune 100, más de 10 000 grandes empresas y millones de organizaciones más pequeñas, ya que ayuda a detener amenazas, prevenir la pérdida de datos y fortalecer la resiliencia en las personas y en los flujos de trabajo de IA. La plataforma de seguridad de colaboración y de datos de Proofpoint ayuda a organizaciones de todos los tamaños a proteger y empoderar a su personal mientras adoptan la IA de forma segura y con confianza. Para obtener más información, consulte www.proofpoint.com/es.
Conecta con Proofpoint: LinkedIn

DESCUBRA LA PLATAFORMA DE PROOFPOINT →