proofpoint.

DATENBLATT

Proofpoint Satori

Governance, Erklärbarkeit und Skalierbarkeit für autonome Sicherheitsabläufe

Wichtige Vorteile

- Eliminiert den Aufwand für das Sicherheitsteam, indem repetitive L1-Triage-Entscheidungen automatisiert werden
- Verarbeitet permanent das hohe Aufkommen an Warnmeldungen, ohne dass zusätzliches Personal benötigt wird
- Erhöht die Geschwindigkeit, Richtigkeit und Konsistenz, da für jeden Fall dieselbe Logik angewendet wird
- Kombiniert autonome Ausführung mit Leitlinien, menschlicher Aufsicht, Erklärbarkeit und Audit-Protokollen

Sicherheitsteams sind heute vielfach überlastet. Durch von Anwendern gemeldete verdächtige E-Mails, DLP-Warnungen (Datenverlustprävention) und Richtlinienverstöße werden täglich tausende repetitive Meldungen generiert, die wenig wertvolle Entscheidungen erfordern. Selbst bei starken Erkennungsfunktionen sind die SOC (Security Operations Center)- und die Datensicherheitsteams mit Triage der Stufe 1 (L1) überlastet. Dies bremst die Reaktion aus, erhöht das Burnoutrisiko und schränkt den Wert vorgelagerter Investitionen ein.

Proofpoint Satori umfasst eine Reihe von Funktionen für autonome Sicherheitsabläufe und wurde dafür konzipiert, diese Probleme zu beheben. Unterstützt von agentenbasierter KI, automatisiert die Lösung hochvolumige Sicherheitsabläufe auf sichere Weise. Dabei werden repetitive Triage-Aufgaben reduziert, während Vertrauen, Kontrolle und Rechenschaftspflicht gewahrt bleiben. Teams können Abläufe skalieren, ohne dabei die Governance zu vernachlässigen.

Autonome Automatisierung auf Basis von Missionen

Proofpoint Satori verwendet mehrstufige Arbeitsabläufe, die als „Missionen" bezeichnet werden und darauf ausgelegt sind, spezifische Sicherheitsziele zu erreichen. Missionen analysieren Proofpoints umfangreiche Telemetrie, wenden Leitlinien an, handeln dort, wo es zulässig ist, und protokollieren jede Entscheidung.

Satori basiert auf der personen- und KI-zentrierten Sicherheitsplattform von Proofpoint und kann auf First-Party-Signale sowie Kontrollpunkte zugreifen, die die von Wettbewerbern übertreffen. Dadurch erhalten Unternehmen detaillierten Kontext, sichere Automatisierungen und enge Integrationen in bestehende Arbeitsabläufe.

Governance-by-Design

Proofpoint Satori wurde entwickelt, um das Vertrauen von Unternehmen zu gewährleisten. Die integrierten Leitlinien verhindern unsichere oder riskante autonome Aktionen, sodass die Automatisierung klar definierte Grenzen hat. Wenn Analysten Verhaltensänderungen anfordern, bietet die menschliche Aufsicht eine zusätzliche Kontrollebene, die Genehmigungen, Sicherheitsabfragen und bei Bedarf auch Rücknahmen ermöglicht.

Jede von Satori getroffene Entscheidung ist erklärbar. Analysten können die Logik hinter den Ergebnissen erkennen, sodass sie sich nicht auf undurchsichtige Automatisierung verlassen müssen. Vollständige Audit-Protokolle erfassen Klassifizierungen und Interaktionen der Analysten und unterstützen die Einhaltung von Vorschriften sowie Transparenz. Verhaltensänderungen erfolgen erst nach expliziter Eskalation sowie menschlicher Überprüfung und gelten nur für zukünftige Fälle.

Satori-Missionen

Der Satori Abuse Mailbox Agent automatisiert die Bearbeitung der von Anwendern gemeldeten verdächtigen E-Mails, sodass der Aufwand für die manuelle Überprüfung von harmlosen oder risikoarmen Meldungen erheblich reduziert wird. Der Agent klassifiziert kontinuierlich große Mengen gemeldeter E-Mails und arbeitet dabei unter strengen Sicherheitsvorkehrungen, z. B. werden VIP-Schutzmaßnahmen eingehalten und Nachrichten niemals automatisch gelöscht.

Der Satori DLP Triage Agent automatisiert die Anreicherung und Priorisierung von DLP-Warnmeldungen. Durch die Reduzierung von False Positives und Überlastung durch zu viele Warnmeldungen können sich Teams besser auf die kritischsten Datenrisiken konzentrieren. Zudem wird sichergestellt, dass riskantere Ereignisse zur rechtzeitigen menschlichen Überprüfung eskaliert werden.

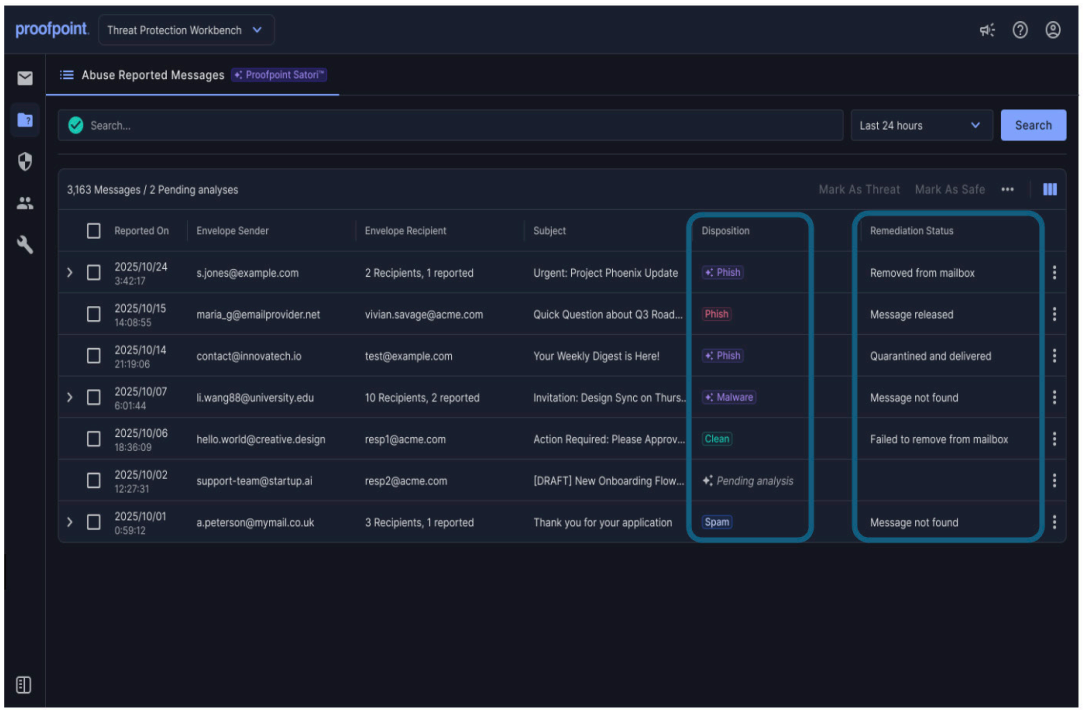

Abb. 1: Der Satori Abuse Mailbox Agent stuft E-Mails im Abuse-Postfach in Kategorien ein und löst damit verbundene Arbeitsabläufe aus.

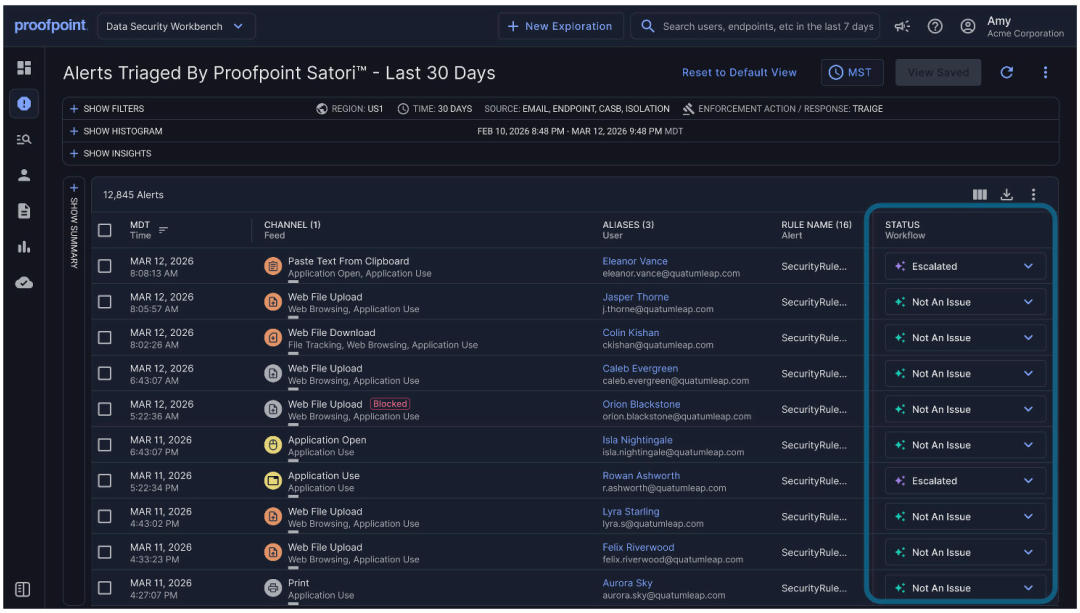

Abb. 2: Der Satori DLP Triage-Agent bewertet Warnmeldungen zu Endpunkten, Cloud und E-Mails, identifiziert False Positives und und filtert diese heraus. Analysten können eine Chat-Oberfläche nutzen, um Fragen zu stellen und Handlungsempfehlungen zu Warnmeldungen zu erhalten.

proofpoint.

Information zu Proofpoint, Inc. Proofpoint, Inc. ist ein weltweiter Marktführer bei personen- und agentenzentrierter Cybersicherheit und schützt Verbindungen zwischen Anwendern, Daten und KI-Agenten über E-Mail, Cloud und Collaboration-Tools. Proofpoint ist ein vertrauenswürdiger Partner für mehr als 80 Prozent der Fortune 100, über 10.000 große Unternehmen sowie für Millionen kleinerer Firmen und stoppt Bedrohungen, verhindert Datenverlust und sichert die Interaktionen zwischen Anwendern und KI-Workflows ab. Die Collaboration- und Datenschutzplattform von Proofpoint hilft Unternehmen jeder Größe, ihre Mitarbeiter zu schützen und zu unterstützen, damit sie KI sicher und bedenkenlos einsetzen können. Weitere Informationen unter www.proofpoint.de.

Vernetzen Sie sich mit Proofpoint: LinkedIn

LERNEN SIE DIE PROOFPOINT-PLATTFORM KENNEN →