securonix

DATENBLATT

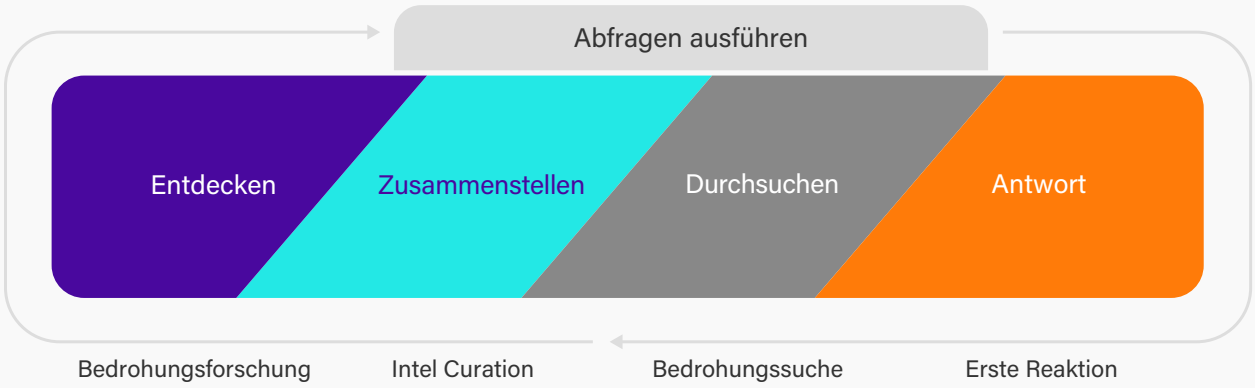
Autonomous Threat Sweeper

Schnelle Cyber-Reaktionen durch automatisierte Bedrohungsmeldungen und Post-hoc-Erkennung

Air-Cover für Ihr SOC bereitstellen

Sicherheitsteams stehen unter enormem Druck, mit dem Tempo der neuen und aufkommenden Bedrohungen Schritt zu halten. Da Cyberangriffe in Umfang und Ausmaß immer weiter zunehmen, benötigen Unternehmen autonome Lösungen, die die Gefährdung durch neue Bedrohungen kontinuierlich bewerten können.

Autonomous Threat Sweeper (ATS) nutzt die neuesten Rechercheergebnisse und Bedrohungsinformationen von Securonix Threat Labs und kodifiziert viele manuelle Aspekte der Untersuchung. Unsere Lösung fungiert als Schutzschild für Ihr Sicherheitsteam und automatisiert die Bewertung Ihrer Gefährdung und die Einleitung von Gegenreaktionen nach Angriffen.



ATS erleichtert die Erkennung unbekannter Bedrohungen in Ihrer Umgebung mit ausgewählten Bedrohungsinformationen sowie automatischer Erkennung und Untersuchung.

Vorteile von ATS

Neuen und dynamischen Bedrohungen immer einen Schritt voraus

Geben Sie Ihrem Team die Möglichkeit, Bedrohungen mit hohem Risiko mit kontinuierlich aktualisierten Bedrohungsdaten zu priorisieren. ATS funktioniert wie eine Erweiterung Ihres SOC mit rückwirkenden Suchoperationen in umfangreichen Protokollen und vergangenen Zeiträumen.

Schnelle Erkennung Ihrer Gefährdung

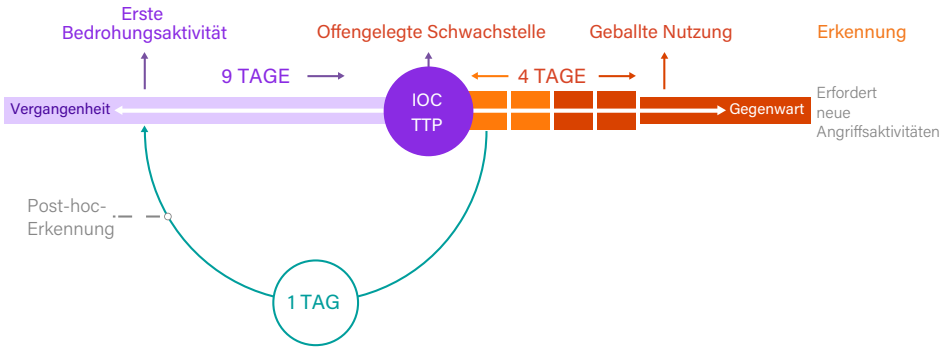
Mit der angriffszentrierten IOC- und TTP-basierten Erkennung erfahren Sie schnell, ob Sie neuen Bedrohungen ausgesetzt sind. ATS erweitert Ihr SIEM um die Fähigkeit, niedrigschwellige und sich langsam aufbauende Bedrohungen durch Post-Hoc-Erkennung von IOCs und TTPs zu erkennen, die von Securonix Threat Labs extrahiert und kodifiziert werden.

Reaktion auf Cyberangriffe beschleunigen

Beschleunigen Sie die Reaktion auf Cyberangriffe mit automatischer Berichterstattung, Alarmierung und Protokollierung. Durch die kontinuierliche Überwachung Ihrer Umgebung und die Sammlung von Informationen über neu auftretende Bedrohungen hilft ATS den Sicherheitsteams, ihre mittlere Reaktionszeit (MTTR) zu verkürzen und kritische Bedrohungen zu priorisieren.

Höhere SOC-Effizienz mit Autonomous Threat Sweeper

Dank der robusten ATS-Funktionen können Sicherheitsteams viele alltägliche Ermittlungsaufgaben auslagern und sich auf die wichtigsten Bedrohungen konzentrieren.



Ausgewählte Bedrohungsinformationen

Dank aktueller Bedrohungsinformationen und -berichte wissen Sie, wann Bedrohungen vorhanden sind.

Bedrohungsinformationen: Sichern Sie sich aktuelle Bedrohungsinformationen, die von den Experten unseres Threat Labs Teams gepflegt werden.

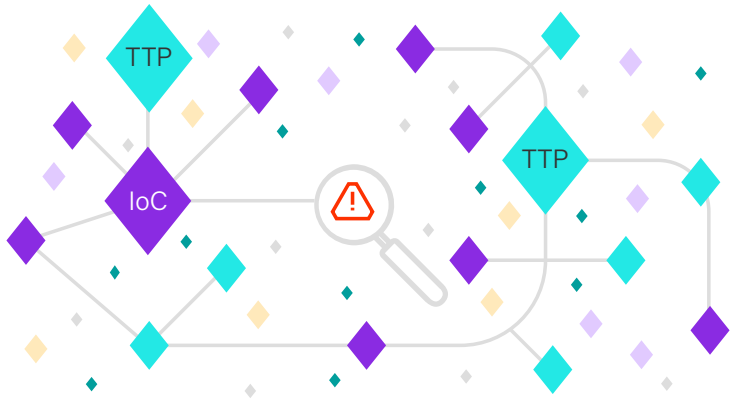
Berichte zur Sensibilisierung für Bedrohungen: Sie werden sofort benachrichtigt, wenn neue, kritische Bedrohungen in Ihrer Umgebung auftreten.

Multi-Vektor-Erkennungsmodus

Nutzen Sie mehrere Erkennungsmethoden, um sowohl „bekannte" Indikatoren einer Gefährdung als auch aus TTPs abgeleitete „bekannte/unbekannte" Aktionsindikatoren zu entdecken.

IOC-Erkennungsmodus: Extrahiert aus den Bedrohungsdaten Indikatoren für eine Gefährdung, um nach neuen Bedrohungen in Ihren langfristigen, alten Daten zu suchen.

TTP-Erkennungsmodus: Analysiert die Taktiken, Techniken und Verfahren und hilft bei der Identifizierung von Aktionsindikatoren, wenn keine IOC-Vorkenntnisse vorhanden sind.



Erweiterte Berichte und Warnmeldungen

ATS alarmiert Ihr Sicherheitsteam und bietet umfassende Berichte, praktische Handlungsanleitungen für Abhilfemaßnahmen und die automatisierte Erfassung von Vorfällen.

Automatisierung: ATS beschleunigt die Erkennung und Reaktion mit Suchvorgängen und Abfragen, die Ihre Umgebung automatisch nach Anzeichen von Gefährdungen in aktuellen und in alten Daten durchsuchen.

Praktische Handlungsanleitungen: Sie erhalten detaillierte Ergebnisse und Anleitungen zur Problembehebung, wenn IOCs und TTPs in Ihrer Umgebung entdeckt werden.

Wenn Sie weitere Informationen über Securonix ATS wünschen, vereinbaren Sie bitte einen Termin für eine Demo unter: www.securonix.com/request-a-demo

securonix