securonix

DATENBLATT

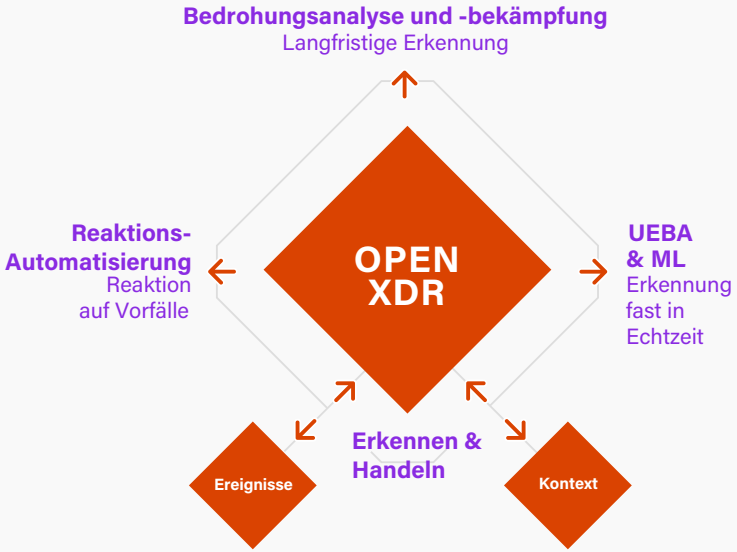
Open XDR

Umfassende Fabric zur Erkennung von und Reaktion auf Bedrohungen

Schnellere Erkennung von und Reaktion auf Bedrohungen mit Ihrem SOC

Viele Unternehmen nutzen heute hybride und Cloud-Umgebungen, bei denen blinde Flecken in der Cybersicherheit entstehen und sie anfälliger für komplexe und ausgeklügelte Cyberangriffe machen. Heute können Bedrohungen aus mehreren Datenquellen innerhalb Ihrer Cloud stammen. Mit Securonix Open XDR (eXtended Detection and Response) werden Bedrohungen und Bedrohungskontexte sichtbar, so dass versteckte Bedrohungen schnell erkannt und eingedämmt werden können. Sicherheitsteams können dann schnell weitere Auswirkungen beseitigen sowie Schweregrad und Ausmaß des Angriffs verringern.

Zur Vereinfachung der Benutzererfahrung kombiniert Securonix Open XDR Verhaltensanalyse, Bedrohungssuche und Reaktion in einer einzigen Lösung.



Vorteile von Open XDR

Umfassende Lösung zur Erweiterung der Analyse

Open XDR erweitert die modernen Analyse- und Erkennungsfunktionen auf Endpunktdaten und darüber hinaus. Nutzen Sie Analyse- und Automatisierungsfunktionen zur Erfassung von Daten sowie zur Erkennung von Bedrohungen in Ihrer gesamten IT-Umgebung. Unsere Open XDR-Lösung macht den Weg frei für alle, die ihre Fähigkeiten zur Erkennung von und Reaktion auf Bedrohungen schnell ausbauen möchten. Wir bieten zudem einen reibungslosen Upgrade-Pfad, damit Sie in Zukunft problemlos auf ein vollständiges SIEM erweitern können.

Erweiterte und Insider-Bedrohungen mit größerer Präzision erkennen

Ihre Angriffsfläche wird immer größer. Sie müssen unbedingt wissen, ob es in Ihrer Umgebung unentdeckte Bedrohungen gibt.

Securonix Open XDR kombiniert mehrere Telemetriequellen mit moderner Verhaltensanalyse, um komplexe Bedrohungen mit minimalen Fehlalarmen aufzuspüren, selbst solche, die derzeit unerkannt in Ihrer Umgebung lauern. Unsere Lösung nutzt vordefinierte Analysen, UEBA und maschinelles Lernen (ML), um Anomalien und andere verdächtige Aktivitäten mit Identitäten zu verbinden.

Schnellere Reaktion auf Vorfälle

Manuelle Untersuchungen und Reaktionen sind zeitaufwändig. Securonix Open XDR ermöglicht mit vordefinierten Playbook-Aktionen für die häufigsten Anwendungsfälle eine automatisierte Reaktion auf Vorfälle. Dank dieser geringeren Komplexität können Sie Produktivität und Effizienz Ihres SOC steigern.

Produktmerkmale

Transparenz und Analysen erweitern

Bei Endpunktlösungen fehlen oft erweiterte Analysen, um ausgeklügelte Bedrohungen zusammenzuführen und zu erkennen. Securonix Open XDR ermöglicht erweiterte Analysen der Daten in Ihrer Cloud, im LAN und von Endpunkten zur besseren Erkennung von und Reaktion auf Bedrohungen.

ML-gestützte Verhaltensanalyse: Aktivieren Sie Verhaltensanalysen für Protokolle, die von Endgeräten, Netzwerken, aus der Cloud und anderen Quellen gesammelt wurden. Securonix Open XDR unterstützt die Erkennung von anomalem Verhalten mit maschinellem Lernen (ML) und Algorithmen zur Risikobewertung. Nutzen Sie eine Bibliothek mit integrierten Bedrohungsinformationen, um Bedrohungen für bestimmte Anwendungsfälle zu erkennen. Unsere XDR-Lösung wertet einzelne Ereignisse und Aktivitätsdaten aus, verbindet die Daten und analysiert diese dann, um ausgeklügelte, unbekannte und Insider-Bedrohungen zu erkennen.

Erweiterte Sichtbarkeit mit der Connector Library: Verkürzen Sie die Wertschöpfungszeit mit sofort einsatzbereiten Integrationen und Konnektoren, die Technologien wie Endpunkte, Netzwerke, Clouds, Geschäftsanwendungen usw. abdecken. Diese Integrationen erleichtern die Übernahme von Daten, die Anreicherung von Kontext, die Suche nach Bedrohungen, die Erkennung und automatische Reaktion. Nutzen Sie Ihre bestehenden Sicherheitsinvestitionen besser – durch eine einzige, vereinheitlichte Ansicht für das SOC.

Erweiterte Erkennung von Bedrohungen

Unsere Lösung, deren Kernstück erweiterte Analysen sind, umfasst die kontextbezogene Anreicherung und benutzerabhängige Risikobewertung, damit Sie komplexe Bedrohungen mit minimalen Fehlalarmen aufdecken können.

Integrierte Analyse des Benutzer- und Entitätsverhaltens: Die identitätsorientierte Verhaltensanalyse bietet Transparenz, die über reine Endpunktaktivität hinausgeht. MITRE ATT&CK-Threat Chain kombinieren einzelne Alarme zu Bedrohungsmustern, um Bedrohungen mit hohem Risiko zu priorisieren.

Risikobewertung: Dank umfassender Identitäts- und Risikoprofile für jeden Benutzer und jede Einrichtung wissen Sie, wann Sie handeln müssen.

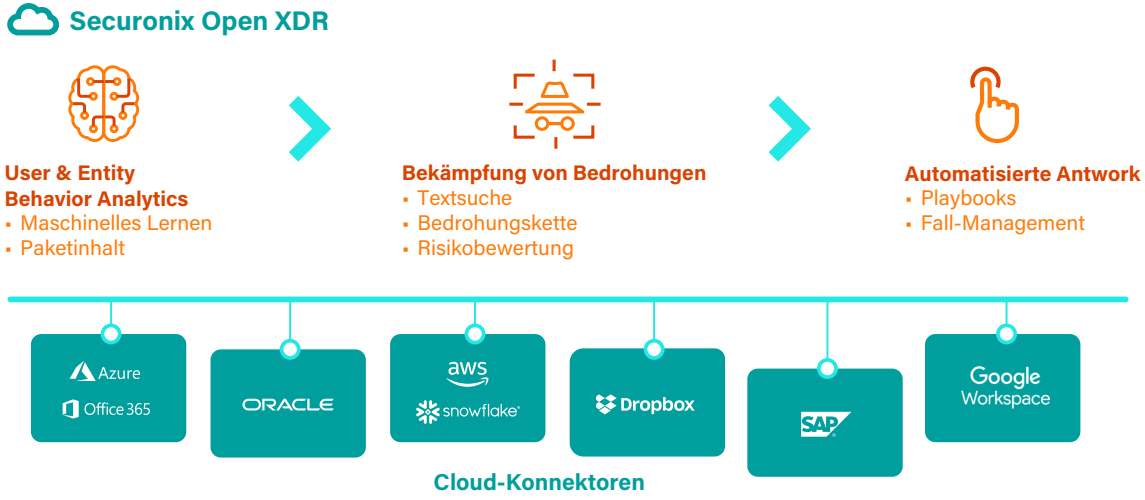
Bedrohungskette: Reduzieren Sie die Zahl der Warnmeldungen mit Threat Models, die sowohl dem MITRE ATT&CK- als auch dem US-CERT-Framework entsprechen.

Security Orchestration, Automation, and Response (SOAR)

Sicherheitsvorfälle, auf die nicht schnell reagiert wird, können einem Unternehmen schnell Schaden zufügen. Eine automatisierte Reaktion auf Vorfälle kann dazu beitragen, das Risiko durch schnelle Reaktion zu mindern. Security Orchestration, Automation and Response steigern die Produktivität und Effizienz Ihres SOC-Teams.

Integrierte Playbook-Aktionen: Securonix Open XDR erleichtert den Analysten durch vordefinierte oder vollständig anpassbare Playbook-Aktionen die Arbeit. Analysten können damit Antwortaktionen für häufige Anwendungsfälle automatisieren.

Management von Vorfällen: Integrierte Funktionen zum Management von Vorfällen ermöglichen eine effiziente Verfolgung und Meldung der Reaktionen auf Vorfälle. Dieser Ablauf beginnt in dem Moment, in dem ein Analyst mit der Untersuchung eines möglichen Ereignisses beginnt, und endet, wenn eine identifizierte Bedrohung entschärft wurde.



Weitere Informationen zu Securonix Open XDR finden Sie unter: www.securonix.com/request-a-demo.

securonix