securonix

DATENBLATT

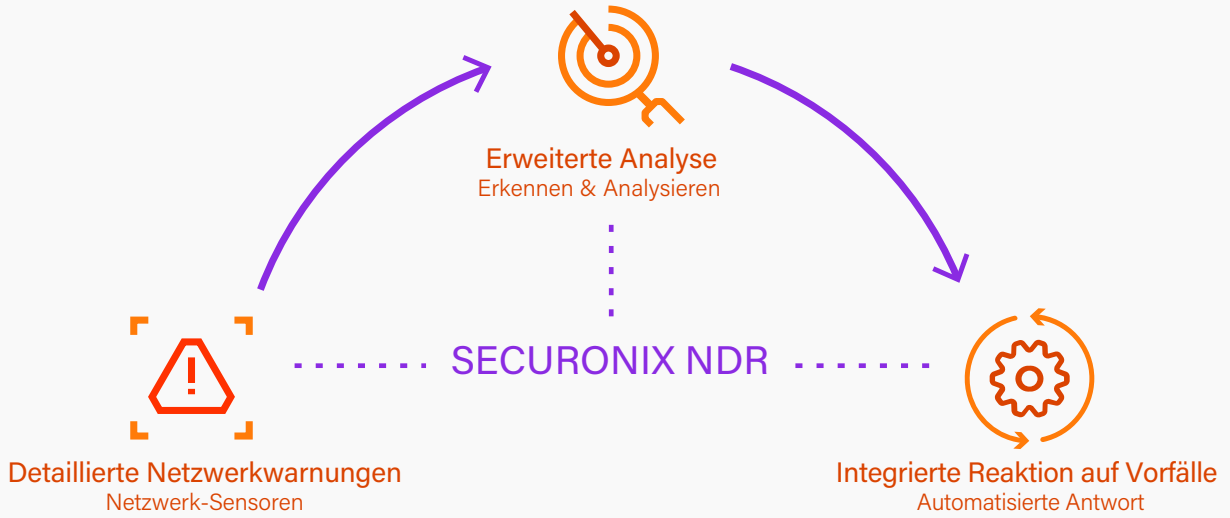
Network Detection and Response

Robuste, skalierbare Netzwerk-Forensik

Argumente für Securonix

Bedrohungen aus dem Netzwerk sind schwer zu erkennen, und herkömmliche Netzwerkschutz-Tools und Firewalls liefern nicht immer einen vollständigen Überblick. Securonix Network Detection and Response (NDR) bewältigt diese Herausforderung, indem es Sicherheitsvorfälle in Ihrer gesamten IT-Umgebung mit Netzwerkaktivitäten zusammenführt und Ihr Team zusammen mit unserem Next-Gen SIEM auf Anomalien aufmerksam macht.

Securonix NDR erleichtert es Sicherheitsteams, das Unternehmen durch bessere Transparenz des Netzwerks und des Kontextes vor Cyberbedrohungen zu schützen – alles über eine einzige Konsole.



Vorteile der Netzwerktransparenz für Erkennung und Reaktion

Maximierung Ihrer SIEM-Investition

Identifizieren Sie erweiterte Bedrohungen, die von eigenständigen NDR- oder SIEM-Lösungen nicht erkannt werden können. Wenn sich alle Netzwerk- und Sicherheitsdaten an einem Ort befinden, kann Ihr Sicherheitsteam Erkenntnisse gewinnen, die den nötigen Kontext zur Erkennung von und Reaktion auf komplexe Bedrohungen liefern.

Blinde Flecken beseitigen

NDR erkennt blinde Flecken, indem es Netzwerkaktivitäten erfasst und mit dem Rest Ihrer IT-Umgebung zusammenführt. Zusammen mit Securonix Next-Gen SIEM verfolgt die Lösung das Verhalten von Benutzern, Konten und Systemen im Netzwerk, an Endpunkten und darüber hinaus, um Bedrohungen in Echtzeit zu erkennen und darauf zu reagieren.

Ausgeklügelte Bedrohungen erkennen

Moderne Cyberangriffe erfolgen oft in mehreren Schritten über längere Zeit und sind daher schwer zu erkennen. Securonix setzt maschinelles Lernen und leistungsstarke Analysen ein, um unterschiedliche IOCs zu einem vollständigen Bild zusammenzufügen. Unsere Lösung fasst komplexe Bedrohungen mit mehreren Warnmeldungen zu verwertbaren Erkenntnissen zusammen und reduziert gleichzeitig die Fehlalarme für Ihr SOC.

Vernetztes Ökosystem

Netzwerk-Sensoren: Erfassen Sie Netzwerkdaten und reichern Sie diese mit Sicherheitsinformationen an. Kombinieren Sie Daten der Netzwerksensoren von Drittanbietern mit anderen Sicherheitsdaten, so dass Ihr SIEM eine zusätzliche Erkenntnisebene erhält. Wir unterstützen die Integration mit allen wichtigen Netzwerksensoren, einschließlich strategischer Partnerschaften mit Corelight, Verizon Protectwise und Gigamon.

Suche nach Netzwerkbedrohungen: Öffnen Sie für die Suche nach Bedrohungen einen 360-Grad-Einblick in Protokoll-, Endpunkt- und Netzwerkdaten. Wenn Sie die Suche auf Netzwerkbedrohungen ausweiten, können Sie Punkte schneller verbinden und die Zeit bis zur Erkennung und Reaktion verkürzen.

Securonix NDR – Transparenz, Erkennung und erweiterte Analysen

Verwertbare Analysen

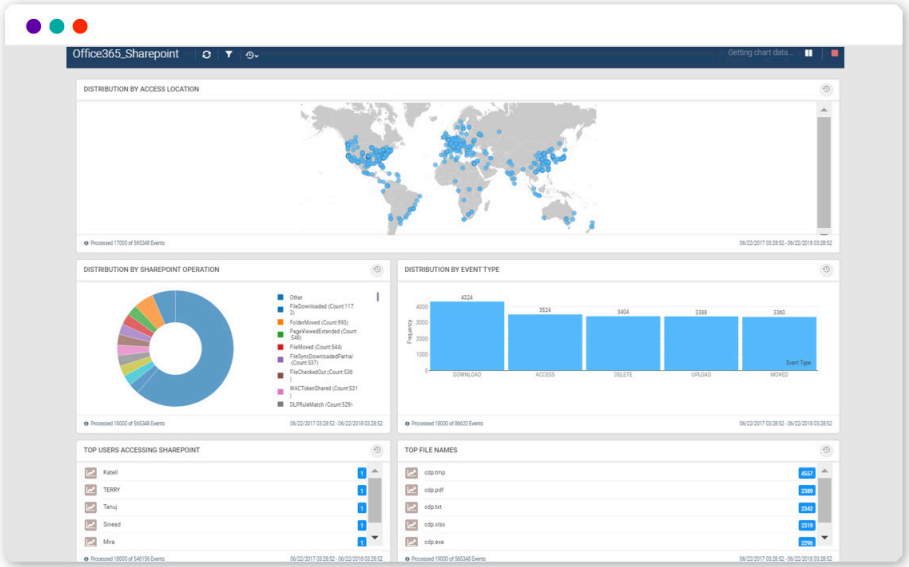
Threats Chains: Reduzieren Sie die Zahl der Warnmeldungen mit Hilfe von Threat Models, die sowohl die Anforderungen des MITRE ATT&CK- als auch des US-CERT-Framework erfüllen. Unsere Analyse der Threat Chain nutzt den Identitätskontext und erleichtert die Erkennung niedrigschwelliger und sich langsam aufbauender Bedrohungen in Netzwerk- und Sicherheitsereignissen.

Erweiterte Analyse: Nutzen Sie erweiterte Analysen mit maschinellem Lernen, um zu erkennen, wann das Netzwerkverhalten von den festgelegten Grundregeln abweicht. Dies ist in dem heutigen komplexen Umfeld von entscheidender Bedeutung, da ein regelbasierter Ansatz zu einer Fülle von Fehlalarmen führen würde.

Ganzheitliche Datentransparenz

Einzelplattform: Reduzieren Sie die betriebliche Komplexität durch eine einzige, vollständig integrierte Backend-Architektur. Da Sie keine Infrastruktur verwalten müssen, kann sich Ihr SOC auf die Erkennung von Bedrohungen konzentrieren, bevor sie eskalieren.

Robuste Berichte: Nutzen Sie die Einblicke in Netzwerkdaten, einschließlich der Berichte zum Netzwerkverkehr, und integrierte, gemeinsam nutzbare Dashboards, um datengestützte Entscheidungen zu treffen. Unsere konsolidierte Plattform ermöglicht Ihrem Team die Zusammenarbeit und Optimierung der Bedrohungssuche.



Integrierte Reaktion auf Vorfälle

Integrierte SOAR-Funktionen helfen Ihnen, Ihre Reaktionszeiten auf Vorfälle zu verbessern. Mit unserer Lösung erhält Ihr Team eine intelligente Automatisierung und Vorschläge für Playbook-Aktionen, welche die Analysten bei der Problembeseitigung unterstützen.

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