Vectra Security AI-driven Attack Signal Intelligence™

Seit Jahrzehnten ging es in der Cyber-Sicherheit immer nur um das, was zu Bedrohungen bekannt ist. Die Methoden, um Cyber-Angreifer zu erkennen und daran zu hindern, Unternehmen zu infiltrieren und Daten zu stehlen, beruhten vornehmlich auf der Verwendung von Signaturen, Anomalien und Regeln. Dieser Ansatz funktioniert nicht mehr.

Da Unternehmen zunehmend zu Hybrid-Cloud- und Multi-Cloud-Umgebungen wechseln und digitale Identitäten, digitale Lieferketten und Ökosysteme einführen, wächst die Belastung der Sicherheits- und Compliance-Verantwortlichen durch:

- Mehr Angriffsflächen
- Mehr Angreifer, die hochentwickelte Umgehungstaktiken einsetzen
- Mehr Tools und zu analysierende Daten
- Mehr Signaturen, Anomalien, Regeln
- Mehr Warnungen, Triage, False Positives
- Mehr Arbeit, Überlastung und Fluktuation für Analysten

Trotz einer wachsenden Zahl an Tools, Daten, Signaturen, Richtlinien, Regeln, Warnungen und Mitarbeitern bleibt das Kernproblem das gleiche:

„Wir wissen *im Moment* nicht, wo sich unsere Schwachstellen befinden."

Angreifer haben durch unbekannte Bedrohungen einen Vorteil

- Umgehung von Präventionsmaßnahmen
- Umgehung von Erkennungsregeln für Signaturen und Anomalien
- Infiltration, laterale Bewegung
- Datendiebstahl

Vectra Security AI-driven Attack Signal Intelligence beseitigt unbekannte Bedrohungen

Vectra Security AI-driven Attack Signal Intelligence verfolgt einen risikobasierten Ansatz für Cyber-Angriffe und verringert gleichzeitig die Zahl manueller Aufgaben, Warnungen und die Überlastung von Analysten. Attack Signal Intelligence unterstützt Security-Analysten bei folgenden Aufgaben:

Denkweise der Angreifer annehmen

KI-gestützte Erkennungen nutzen nicht nur Signaturen und Anomalien, um Angreiferverhalten zu verstehen und den vollständigen Verlauf eines Angriffs offenzulegen.

Konzentration auf Schadaktivitäten

KI-gestützte Triage verringert die Zahl unnötiger Warnungen, denn sie unterscheidet schädliche Aktivitäten von scheinbaren Bedrohungen, sodass schädliche True Positives identifiziert und harmlose Aktivitäten lediglich protokolliert werden.

Erkennen, was kritisch ist

KI-gestützte Priorisierung verringert die Zahl unnötiger Warnungen, automatisiert die Triage-Prüfung von Warnungen und bietet eine um 85 % effektivere Priorisierung von Bedrohungen, die die größte Gefahr für ein Unternehmen darstellen.

Priorisierung realer Bedrohungen statt ungewöhnlicher Ereignisse

Attack Signal Intelligence basiert auf Sicherheitsforschung und Datenwissenschaft und nutzt daher mehr als nur einfache Anomalie-Erkennung, um reale Angriffe und Aktivitäten in allen Phasen der Kill Chain zu erkennen.

KI-gestützte Erkennung

- Identifizierung von TTPs, die für Angriffe genutzt werden
- Zuverlässige Erkennung von Angreifer-TTPs durch verhaltensbasierte Modelle
- Nutzung des optimalen ML-Ansatzes zur korrekten Erkennung

KI-gestützte Triage

- Kontinuierliche Untersuchung aller aktiven Erkennungen auf Gemeinsamkeiten
- Intuitives Design zur Unterscheidung zwischen schädlichen und harmlosen Aktivitäten
- Automatisierte Aufdeckung schädlicher Aktivitäten und Protokollierung harmloser Aktivitäten

KI-gestützte Priorisierung

- Domain-übergreifende korrelierte Erkennungen von Angreifer-TTPs
- Umfassender Überblick über den vollständigen Angriffsverlauf
- Einheitliche Ansicht priorisierter Bedrohungen nach Schweregrad und Auswirkung

VECTRA
SECURITY THAT THINKS®

KI-gestützte Erkennung

Nimmt die Denkweise der Angreifer an
Geht über einfache Anomalie-Erkennung hinaus

- Aufdeckung von Angreifer-TTPs
- Verhaltensbasierte TTP-Erkennung
- Nutzt das optimale ML-Modell

KI-gestützte Triage

Erkennt schädliche Aktivitäten
Reduziert Fehlalarme

- Führt kontinuierliche Analysen durch
- Intuitive Bedienung
- Deckt schädliche Aktivitäten auf

KI-gestützte Priorisierung

Konzentriert sich auf kritische Bereiche
Für schnellere Untersuchungen und Response

- Korreliert TTP-Erkennungen
- Umfassende Transparenz
- Einheitliche priorisierte Ansicht

Stoppen Sie Angreifer mit KI-gestützten Abläufen

Unterstützung für Sicherheitsverantwortliche, Architekten und Analysten, um modernen Cyber-Angriffen einen Schritt voraus zu sein.

Integrierte Untersuchungen liefern Analysten umgehend Antworten.

- Fokus auf kritische Bedrohungen, geordnet nach Schweregrad und Auswirkung
- Threat Hunting über die gesamte Angriffsfläche
- Untersuchungen mithilfe von Kontext und Forensik über eine zentrale Benutzeroberfläche

Automatisierte Workflows verringern Komplexität und Kosten durch die Automatisierung manueller Aufgaben.

- Konsolidierung der Arbeitsabläufe von Analysten in einer einzigen Oberfläche
- Vereinfachte SIEM-Daten-Feeds, Dashboards und Berichte
- Individuelle Integrationen in vorhandene Ticketing- und Bericht-Workflows

Gezielte Reaktionsmaßnahmen geben Menschen die Kontrolle über die Response durch Analysten-gesteuerte Durchsetzung.

- Flexible Reaktionsmaßnahmen (z. B. Kontosperrungen) werden automatisch oder manuell ausgelöst, um Endgeräte zu isolieren oder ein SOAR- bzw. ITSM-Playbook auszulösen
- Standardmäßige Integrationen der besten EDR- und SOAR-Anbieter
- Nutzung von Vectra MDR-Services im Rahmen der Managed Response

Im Gegensatz zu anderen Ansätzen, die einfache Anomalie-Erkennung nutzen und manuell optimiert und gewartet werden müssen, automatisiert Vectra Security AI-driven Attack Signal Intelligence die Bedrohungserkennung, Triage und Priorisierung ohne menschliches Eingreifen. Dank dieser Technologie können Security-Teams unbekannte Bedrohungen beseitigen, Angreifer stoppen und die Welt sicherer machen.

Über Vectra

Vectra® ist ein weltweit führendes Unternehmen im Bereich der Detection & Response in der Hybrid Cloud. Die patentierte Vectra-Lösung Attack Signal Intelligence™ erkennt und priorisiert Bedrohungen in der Public Cloud, in SaaS-Anwendungen, Identitäten und Netzwerken mit einer einzigen Plattform. Vectra Attack Signal Intelligence geht über einfache Anomalie-Erkennung hinaus, um das Verhalten von Angreifern zu analysieren und nachzuvollziehen. Das daraus entstehende zuverlässige Bedrohungssignal und der umfangreiche Kontext ermöglichen Security-Operations-Teams, auf Bedrohungen früher zu reagieren und laufende Cyber-Angriffe schneller zu stoppen. Weltweit verwenden Unternehmen die Vectra-Plattform und MDR-Services, um sich vor aktuellen Cyber-Angriffen zu schützen.

Weitere Informationen:
E-Mail: info@vectra.ai | vectra.ai