VECTRA®

Cognito Stream: Netzwerk-Metadaten mit eigener Meinung

HIGHLIGHTS

- Leitet durchsuchbare Metadaten im Zeek-Format an den Datenspeicher Ihrer Wahl weiter, unterstützt werden Kafka, syslog und Elastic
- Metadaten werden mit Sicherheits-erkenntnissen angereichert, um die Untersuchungen zu vereinfachen
- Erlaubt die Entwicklung kunden-spezifischer Werkzeuge und Modelle zur Erkennung, Untersuchung und Suche
- Nutzt alle vorhandenen Zeek-Funktionen
- Korreliert Cloud- und Netzwerk-Metadaten mit Daten von Hosts und Geräten in Ihrem Data Lake (z. B. Anwendungsprotokolle, Prozesse, Speicherzugriffe)
- Einfache Bereitstellung – keine Leistungsoptimierung oder kontinuierliche Wartung erforderlich
- Mehr als fünfmal höhere Leistung als Zeek mit einem Sensor

Cognito Stream™ von Vectra® liefert skalierbare, mit Sicherheitsdaten angereicherte Metadaten aus nativem Cloud-, Hybrid-Cloud- und Unternehmens-Traffic, die erfahrene Security-Analysten und Threat Hunter für schlüssige Untersuchungen von Vorfällen nutzen können.

Sicherheitsdaten haben heute ein Problem: NetFlow ist unvollständig und PCAPs erfordern viel Speicherplatz und Rechenleistung. Unternehmen, die sich für die Implementierung der Open-Source-Lösung Zeek entscheiden, müssen mit ressourcen- und zeitintensiven Schritten für den Aufbau und die Konfiguration der Hardware, für die Konfiguration der Software und die Integration in die vorhandenen Tools rechnen. Dieser Ansatz ist für Sicherheitsverantwortliche nicht tragbar.

Mit Cognito Stream erhalten Security-Teams den umfassenden Netzwerk-Kontext, den sie für kundenspezifische Tools sowie Feed-Modelle zur Erkennung, Untersuchung und Suche nach Bedrohungen benötigen. Da diese Sicherheitserkenntnisse im Open-Source-Format Zeek bereitgestellt werden, integrieren sie sich nahtlos in Data Lakes und SIEMs – ohne den zusätzlichen Aufwand und die Skalierungsbeschränkungen durch Zeek.

Die Metadaten aus Cognito Stream werden mit der Host-Identität angereichert, sodass die Untersuchungen statt auf den veränderlichen IP-Adressen basierend auf den Gerätenamen erfolgen können. Dadurch müssen Sie nicht mehr parallel die DHCP-Logs konsultieren, um die Veränderungen der von diesem Gerät innerhalb eines bestimmten Zeitraums genutzten IP-Adresse im Blick zu behalten. Die Suche anhand des Gerätenamens spart somit wertvolle Zeit. Durch die Kombination von Sicherheitserkenntnissen und Metadaten erhalten Threat Hunter die Intelligence, die sie für Untersuchungen und Threat Hunting benötigen.

Vorteile bei Threat Hunting und Untersuchungen von Vorfällen

- **Verwertbare Netzwerkdaten im Zeek-Format.** Cognito Stream extrahiert hunderte Metadaten-Attribute aus der Cloud und dem Unternehmensnetzwerk und präsentiert sie im kompakten, benutzerfreundlichen Zeek-Format, das alle vorhandenen Tools nutzt. Im Gegensatz zu NetFlow liefert Stream die für Analysten nötigen Details, jedoch ohne die Komplexität der vollständigen Paketerfassung.

- **Eingebettete Sicherheitserkenntnisse.** Durch maschinelles Lernen generierte Sicherheits-erkenntnisse (z. B. Beaconing-Aktivitäten, Domain-Vorkommen) sind in die Metadaten eingebettet und können von spezialisierten Threat Huntern wie Bausteine zusammengesetzt und für schnelle Schlussfolgerungen genutzt werden.

- **Untersuchungen basierend auf Hosts und nicht IP-Adressen.** Netzwerk-Metadaten werden in Cognito Stream automatisch mit anderen Attributen verknüpft, sodass Security-Analysten genaue Informationen zur Host-Identität erhalten und Hosts effizient untersuchen können – selbst dann, wenn sich die IP-Adresse ändert. Außerdem wird auf diese Weise die Untersuchung von Beziehungen zwischen Host-Gruppen ermöglicht.

- **Absolut benutzerfreundlich und ohne Wartungsaufwand.** Cognito Stream lässt sich in weniger als 30 Minuten einrichten, erfordert keine Leistungsoptimierung oder kontinuierliche Wartung und liefert eine fünfmal höhere Leistung als Zeek mit einem Sensor. Dadurch können sich Security-Teams auf die Untersuchungen konzentrieren, ohne den Verwaltungsaufwand der Open-Source-Lösung Zeek befürchten zu müssen.

Ich bin eine künstliche Intelligenz.
Die treibende Kraft hinter der
Jagd auf Cyber-Angreifer.
Ich bin Cognito.

Die Cognito-Plattform

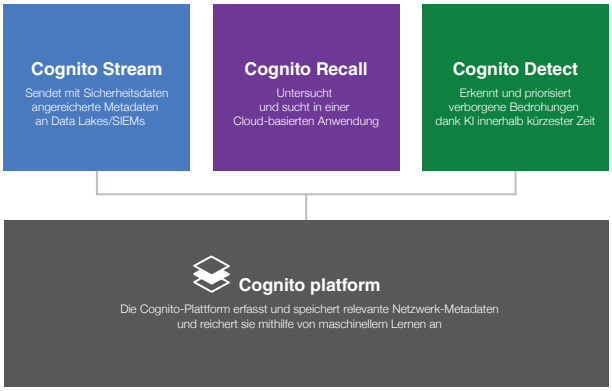
Die richtigen Daten mit dem richtigen Kontext

Vectra ist ein weltweit führendes Unternehmen im Bereich Netzwerk-Erkennung und Response. Die Cognito®-Plattform von Vectra revolutioniert die Netzwerksicherheit und ersetzt damit herkömmliche Technologien, die aktuellen Herausforderungen an Erkennung und Response nicht gewachsen sind. Dabei deckt die Cognito-Plattform Workloads in der Cloud und im Rechenzentrum ebenso wie Systeme für Endanwender und IoT-Geräte ab.

Die Cognito-Plattform beschleunigt die Erkennung und Untersuchung von Anwenderbedrohungen durch künstliche Intelligenz (KI), die dazu Netzwerk-Metadaten erfasst, speichert und mit relevanten Kontextdaten anreichert. So lassen sich bekannte und unbekannte Bedrohungen in Echtzeit erkennen und untersuchen.

Dabei lässt sich die Cognito-Plattform auch für sehr große Unternehmensnetze mit einer verteilten Architektur effizient skalieren. Dazu unterstützt die Plattform verschiedenste physische, virtuelle und Cloud-Sensoren, die einen vollständigen Einblick in Cloud-, Rechenzentrum-, Anwender- und IoT-Netzwerke liefern.

Vectra bietet für die Cognito-Plattform drei Anwendungen an, die die wichtigsten Anwendungsszenarien abdecken. Cognito Stream sendet mit Sicherheitsdaten angereicherte Metadaten an Data Lakes und SIEMs, Cognito Recall™ ist eine Cloud-basierte Anwendung zur Speicherung und Untersuchung von Bedrohungsdaten anhand angereicherter Metadaten, und Cognito Detect™ erkennt und priorisiert verborgene und unbekannte Angreifer dank KI innerhalb kürzester Zeit.



Funktionsweise von Cognito Stream

Weiterleitung angereicherter Metadaten an Data Lakes

Mit Cognito Stream erhalten Sie einen vollen Überblick über den Netzwerk-Traffic. Dazu extrahiert die Lösung Metadaten aus allen Paketen und speichert diese Daten in Ihrem Data Lake oder SIEM, damit sie dort korreliert, durchsucht und analysiert werden können. Jedes IP-fähige Gerät im Netzwerk wird identifiziert und überwacht.

Das bezieht Server, Laptops, Drucker, BYOD- und IoT-Geräte sowie Betriebssysteme und Anwendungen ein – und auch den Traffic zwischen virtuellen Workloads in Rechenzentren und in der Cloud. Die Metadaten enthalten Daten zur Konnektivität sowie weitere Details aus Protokollen, die für Threat Hunting und die Untersuchung von Bedrohungen wichtig sind.

Die erfassten Metadaten umfassen den gesamten internen Traffic, Internet-basierten Traffic sowie Traffic in der virtuellen Infrastruktur und in Cloud-Computing-Umgebungen. Cognito Stream leitet die durchsuchbaren Metadaten an Data Lakes weiter. Dabei werden Kafka, syslog und Elastic unterstützt.

Vereinfachte Bereitstellung über die Cognito-Plattform

Unternehmen können die Cognito-Plattform innerhalb von maximal 30 Minuten bereitstellen und anschließend sofort mit dem Threat Hunting oder der Untersuchung von Vorfällen beginnen, ohne sich Gedanken über zusätzlichen Verwaltungsaufwand für die Verwaltung der Sensor-Infrastruktur machen zu müssen:

- Physische und virtuelle Sensoren erfassen Metadaten aus verschiedenen Teilen des Netzwerks, z. B. Campus, Rechenzentrum und Cloud.

Die Sensoren verbinden sich mit der zentralen Entität (dem „Gehirn“), die die Datenflüsse dedupliziert, die Hosts identifiziert und die Anreicherungs-Algorithmen anwendet. Cognito Stream wird lokal als virtuelle Maschine (VM) implementiert und wandelt die Metadaten in das Zeek-Format um. Anschließend werden die Daten an Data Lakes oder SIEMs übertragen, die lokal oder in der Cloud laufen können.

Threat Hunting

Analysten finden täglich Hinweise auf Kompromittierungen (Indicators of Compromise, IoCs) im eigenen Netzwerk. Andere IoCs werden über Open-Source-Intelligence verbreitet oder durch interne Untersuchungen aufgedeckt. Analysten können angereicherte Netzwerk-Metadaten auch im Nachgang nach IoCs durchsuchen, d. h. nach IP-Adressen, Domains, URLs, Hashes und SSL-Zertifikaten, die bei Cyber-Angriffen zum Einsatz kamen. Da die Metadaten über einen langen Zeitraum gespeichert werden, ist die Suche nach hochwertigen IoCs sehr hilfreich.

Korrelation von Netzwerk- und Host-Daten

Effektives Threat Hunting erfordert umfassende Einblicke in IT-Assets, Risiken und Datenflüsse innerhalb des Unternehmensnetzwerks. Die hierfür erforderlichen Daten lassen sich in drei Kategorien aufteilen:

- Netzwerk-Metadaten zur gesamten Kommunikation zwischen Hosts mit Beschreibungen der Interaktionen zwischen Entitäten, d. h. zwischen den Anwendern, Geräten, Workloads, IP-Adressen und Domains innerhalb des Netzwerks. Mithilfe dieser Interaktionen können Threat Hunter die kriminellen Aktivitäten innerhalb des Netzwerks aufdecken.
- Host-Daten für Einblicke in Ereignisse auf den Hosts innerhalb der Umgebung, einschließlich Aktivitäten in Bezug auf Anwenderkonten sowie Systemprozesse.
- Anwendungs-Datensätze zu Ereignissen, die für die in der Umgebung laufenden Programme protokolliert werden.

Durch die Netzwerk-Metadaten erhalten Analysten einen allgemeinen Überblick über die Muster und Ereignisse im gesamten Netzwerk. Die Host- und Anwendungsdaten (in Kombination mit den Gerätedaten) liefern die Details zu Verhaltensweisen auf Host-Ebene – einschließlich Systemprozessen und Speicherzugriffen.

Durch die Kombination dieser Daten entsteht eine umfassende Karte des Unternehmens, die auf mehreren Ebenen Informationen über mögliche Vorgänge liefert. Um hochentwickelte Bedrohungen aufdecken zu können, sollten Threat Hunter die Möglichkeit erhalten, diese Datensätze parallel und in Kombination zu nutzen.

Entwicklung kundenspezifischer Werkzeuge und Modelle zur Erkennung, Untersuchung und Suche

Durch individuelle Erkennungen können Analysten Ereignisse auf beliebige Verhaltensweisen hin überwachen, zum Beispiel auf verdächtige Aktivitäten, neue Bedrohungen, Compliance-Verletzungen, internen Missbrauch oder branchenspezifische Angriffsvektoren. Die Sicherheitserkenntnisse in Cognito Stream liefern Bausteine für maschinelles Lernen, die in den Metadaten eingebettet sind und mit anderen Attributen kombiniert werden können, um leistungsstarke individuelle Modelle zur Korrelation bestimmter Hosts oder Anwenderkonten zu erstellen.

Schlüssige Untersuchungen von Vorfällen

Cognito Stream ermöglicht außergewöhnlich effiziente, weitreichende und schlüssige Untersuchungen von Vorfällen innerhalb vorhandener Data Lakes und SIEMs.

Durch die angereicherten Netzwerk-Metadaten können Security-Analysten problemlos der damit zusammenhängenden Kette von Ereignissen folgen – ganz gleich, ob der Angriff zuerst von Cognito Detect, einem Security-Produkt eines anderen Anbieters oder mithilfe durchsuchbarer, hochwertiger Threat Intelligence in historischen Netzwerk-Metadaten entdeckt wurde.

Sobald Cognito Detect oder Drittanbieter-Security-Produkte einen Vorfall melden, erhalten Security-Analysten einen vollständigen Rundumblick auf alle Workload- und Geräte-Aktivitäten.

Mit Cognito Stream können Security-Analysten außerordentlich effiziente Untersuchungen durchführen. Dazu stehen ihnen der gesamte Kontext von Vorfällen, einschließlich der Transaktionen innerhalb des Netzwerks, sowie ergänzend relevante Details zu involvierten Geräten, Konten und zur Netzwerkkommunikation zur Verfügung.

Hier können Sie eine Demo anfordern: vectra.ai/demo

VECTRA®
Security that thinks®

E-Mail info_dach@vectra.ai **Tel.** +1 408 326 2020
vectra.ai

© 2019 Vectra AI, Inc. Alle Rechte vorbehalten. Vectra, das Vectra AI Logo, Cognito und Security that thinks sind eingetragene Marken und Cognito Detect, Cognito Recall, Cognito Stream, Vectra Threat Labs und der Threat Certainty Index sind Marken von Vectra AI. Alle weiteren in diesem Dokument verwendeten oder aufgeführten Marken, Produkte und Services sind Marken oder registrierte Marken oder Servicemarken der jeweiligen Eigentümer.