KURZVORSTELLUNG

Künstliche Intelligenz für neue Cyber-Sicherheitserkenntnisse

Lösungen zur Unterstützung der Zusammenarbeit von Mensch und Maschine verwenden künstliche Intelligenz, Deep Learning und Machine Learning

Die Bedrohungslage entwickelt sich unglaublich schnell weiter. Bedrohungsdatendienste reagieren täglich auf Milliarden Bedrohungsanfragen und pflegen Datenbanken mit hunderten Millionen Schadsoftware-Varianten. Die kontinuierlich wachsende Zahl der Angriffe in Kombination mit der hohen Geschwindigkeit und Komplexität kann selbst erfahrene und effiziente menschliche Sicherheitsexperten überfordern.

Hauptvorteile

- Erweiterung der Analysefunktionen zur Suche in immer umfangreicheren und komplexeren Daten sowie Präsentation umsetzbarer Informationen
- Sofort für Sicherheitsanalysten abrufbare Angriffsanalysen, die von Maschinen generiert werden
- Anpassung und Maximierung der Abwehrmaßnahmen im Unternehmen, ohne dass zusätzliche Mitarbeiter oder Kompetenzen benötigt werden
- Erkennung von Mustern und Verhaltensweisen, die Sicherheitsverletzungen verursachen, mithilfe von Machine Learning-Algorithmen
- Verbesserung der Qualität von Bedrohungsindikatoren
- Erweiterte Malware-Verhaltensanalysen dank neuronaler Netze für Deep Learning
- Einbeziehung bestehender Investitionen, z. B. native und Drittanbieter-Kontrollfunktionen

Folgen Sie uns

Die Lösung liegt in der Kombination aus Analysen und Zusammenarbeit von Mensch und Maschine. Während Automatisierung in Sicherheitsprozessen lange Zeit nur eine Nebenrolle spielte, sind Analysetechnologien aufgrund höherer Angriffsraten und unterbesetzter Teams zu einer Kernkomponente strikter Cyber-Sicherheitspläne geworden. Durch die Kombination automatisierter Bedrohungsdaten mit menschlichen strategischen Erkenntnissen lassen sich bessere Sicherheitsergebnisse erzielen.

Durch Zusammenarbeit von Mensch und Maschine (künstliche Intelligenz, Deep Learning, Machine Learning) werden die Möglichkeiten hochentwickelter Analyse-funktionen erweitert, sodass enorme Datenmengen durchsucht und aktuelle, umsetzbare Erkenntnisse präsentiert werden können. Desweiteren können die Zusammenarbeit von Mensch und Maschine sowie ein mehrschichtiger Sicherheitsansatz dazu beitragen, einfache ebenso wie komplexe Kompromittierungen zu erkennen, abzuwehren und zu beheben. Dadurch erhalten Unternehmen die umfassende Lösung, die sie benötigen.

Die zu Bedrohungen und Angriffen gesammelten Informationen sind allein nicht in der Lage, die Cyber-Sicherheitsherausforderungen von Unternehmen zu beseitigen. Sicherheitsteams können aus den Informationen zusätzliche Erkenntnisse ziehen, mit denen sie die Abwehrmaßnahmen im Unternehmen anpassen und optimieren und so maximalen Schutz bieten können – ohne dass zusätzliche Mitarbeiter oder Kompetenzen benötigt werden. Mithilfe dieser Informationen können Sie auf Ihre Umgebung reagieren und basierend auf den Erkenntnissen Änderungen vornehmen.

Analysen mithilfe von künstlicher Intelligenz

Mit Logik zu neuen Erkenntnissen

Künstliche Intelligenz (KI) imitiert das menschliche Gehirn, indem Werte untersucht und Ergebnisse als Gut/Schlecht bzw. Richtig/Falsch eingestuft werden. Mit dem gleichen Prozess kann die Cyber-Sicherheit verbessert werden, wenn die Komplexität durch Deep Learning, vorgeschlagene Aktionen und Problemlösung erhöht wird.

- Künstliche Intelligenz verwendet Logik, um das eigene Ökosystem zu verstehen. Dazu werden verschiedene komplexe Analysen eingesetzt, z. B. Deep Learning und Sprachverarbeitung. Während Machine Learning und Deep Learning deskriptive und präskriptive Analysen umfassen können, liegt die Stärke von KI vor allem in ausgereiften prädiktiven und präskriptiven Analysen.
- KI hängt von den Daten ab, mit denen sie trainiert wurde, d. h. KI kann nur den Umgang mit solchen Situationen lernen, die im bereitgestellten Datensatz enthalten sind. Ebenso wie bei allen Sicherheits-prozessen ist es unabdingbar, Anwendungsszenarien zu identifizieren und das zu behebende Problem zu bestimmen.
- Cognitive Computing kann zusätzliche Warnmeldungen generieren und geeignete Maßnahmen zur Eindämmung von Bedrohungen einleiten.
- KI wird von Anbietern für verschiedene Zwecke eingesetzt, u. a. auch zur verbesserten Bedrohungserkennung.

Wichtige Vorteile

McAfee® MVISION EDR

- Dank der Fähigkeit von Machine Learning, kontinuierlich zu „lernen“ und immer intelligenter zu werden, verbessern sich die deskriptiven, diagnostischen, prädiktiven and präskriptiven Möglichkeiten Ihrer Abteilung.
- Ihre Sicherheitsteams werden von KI-gestützten Untersuchungen unterstützt, die relevante Risiken aufdecken sowie die bisher manuell durchgeführte Erfassung und Analyse von Beweisen automatisieren, damit Sie aktuellen Bedrohungen stets einen Schritt voraus sind.
- Falls sich verdächtige E-Mails als böswillig herausstellen, können Sie schnell feststellen, welche Geräte im Unternehmen betroffen sein können.
- Nutzen Sie KI, um Bedrohungen schnell zu klassifizieren, damit Sie Ihren schwerwiegendsten Problemen schnell die höchste Priorität zuweisen können.
- Verwenden Sie die integrierten KI-Funktionen, um die Qualität der Bedrohungsindikatoren zu verbessern.

Erweiterung der Möglichkeiten vorhandener SOC-Ressourcen

Die Informationen und Erkenntnisse aus der Zusammenarbeit von Mensch und Maschine ermöglichen effizientere und nachhaltigere Endgerätesicherheit. Sicherheitsteams allein sind nicht in der Lage, mit dem Bedrohungsaufkommen Schritt zu halten, und Maschinen können keine kreativen Reaktionen entwickeln.

- Durch erweiterte Analysen können Sie mehr Ereignisse erkennen und die Warnmeldungen besser interpretieren. KI-geführte Untersuchungen und Automatisierung zeigen selbst unerfahrenen Analysten, wie sie genauere Analysen durchführen können. Dadurch wird die Reaktionszeit verkürzt, und erfahrenen Analyseexperten steht mehr Zeit zur Verfügung, um sich auf die Suche zu konzentrieren.
- KI-geführte Untersuchungen verringern die für Untersuchungen erforderliche Expertise sowie den Aufwand und erhöhen die Geschwindigkeit und Effizienz, mit der Analysten das Risiko sowie die Ursache des Zwischenfalls ermitteln können. Dadurch kann jeder Analyst effizienter arbeiten.

Abbildung 1. Wenn verdächtige E-Mails oder Bedrohungen gefunden werden, können Analysten mit KI-geführten Untersuchungen tausende interne sowie externe Endgeräte lokalisieren und Reaktionsmaßnahmen einleiten.

Wichtige Vorteile

McAfee® MVISION Cloud

- Nutzen Sie Machine Learning, um Verhaltensmodelle zu entwickeln, die aktive Kontokompromittierung und Insider-Bedrohungen aufdecken. Mithilfe von Signaturen und Sandbox-Analysen können Sie zudem Malware in der Cloud erkennen und Bedrohungen aufhalten.
- Die UEBA-Funktion (User and Entity Behavior Analytics, Verhaltensanalyse von Benutzern und Entitäten) erstellt automatisch selbstlernende Modelle (basierend auf mehreren Heuristiken und Machine Learning), um Aktivitätsmuster zu identifizieren, die für Benutzerbedrohungen in verschiedenen Cloud-Diensten und böswilliges Verhalten (z. B. Diebstahl vertraulicher Daten) typisch sind.
- Die KI-gestützte Aktivitätszuordnung nutzt künstliche Intelligenz zur Analyse von Anwendungen und Zuordnung von Benutzeraktionen zu einem einheitlichen Satz von Aktivitäten, was standardisierte Überwachung und anwendungsübergreifende Kontrollen ermöglicht.

Bessere und schnellere Ergebnisse mit Machine Learning

Algorithmen zur Erkennung von Mustern und Verhaltensweisen

Machine Learning nutzt Automatisierung, um zu lernen und sich im Laufe der Zeit dank neuer Daten anzupassen. Machine Learning sorgt dafür, dass diagnostische und deskriptive Sicherheitsanalysen durch prädiktive und präskriptive Analysen ergänzt werden, sodass eine schnellere und zuverlässigere Erkennung von Bedrohungen möglich ist. Sicherheitsteams können mit Machine Learning-Algorithmen Muster und Verhaltensweisen, die Sicherheitsverletzungen verursachen, deutlich schneller erkennen als Menschen das könnten. So ermöglicht Machine Learning die ständige Weiterentwicklung der Endgerätesicherheit zur Abwehr neuer Angriffstaktiken.

- Machine Learning erkennt verborgene Malware. Mit der Mustererkennung wird gefährliches Verhalten erkannt, das zu bekannten sowie unbekannten Sicherheitsverletzungen führt.
- Durch Machine Learning sind Sicherheitsteams besser informiert und können somit auch bessere Entscheidungen treffen.
- Machine Learning unterstützt CSOs (Chief Security Officer) beim optimalen Einsatz der vorhandenen Mitarbeiter und Ressourcen, da erfahrene Sicherheitsanalysten von einfachen Aufgaben entlastet werden und noch unerfahrene Mitarbeiter effizienter und effektiver arbeiten können.
- Mit Machine Learning bleiben Sie bei den neuen Techniken der Kriminellen auf dem neuesten Stand. Durch die automatische Erkennung neuer Angriffstaktiken und -strategien können Sicherheitsteams mit kreativen Problemlösungen Schritt halten. Gleichzeitig erhält Ihr Sicherheitsteam die Informationen, die es für wertvolle Erkenntnisse und Reaktionen benötigt.
- Machine Learning wird mit neuen Daten immer genauer. Die Evolution in Bezug auf bessere Leistung und Kapazität führt dazu, dass Machine Learning noch schneller lernen und die Zuverlässigkeit von Cyber-Sicherheitsfunktionen steigern kann.

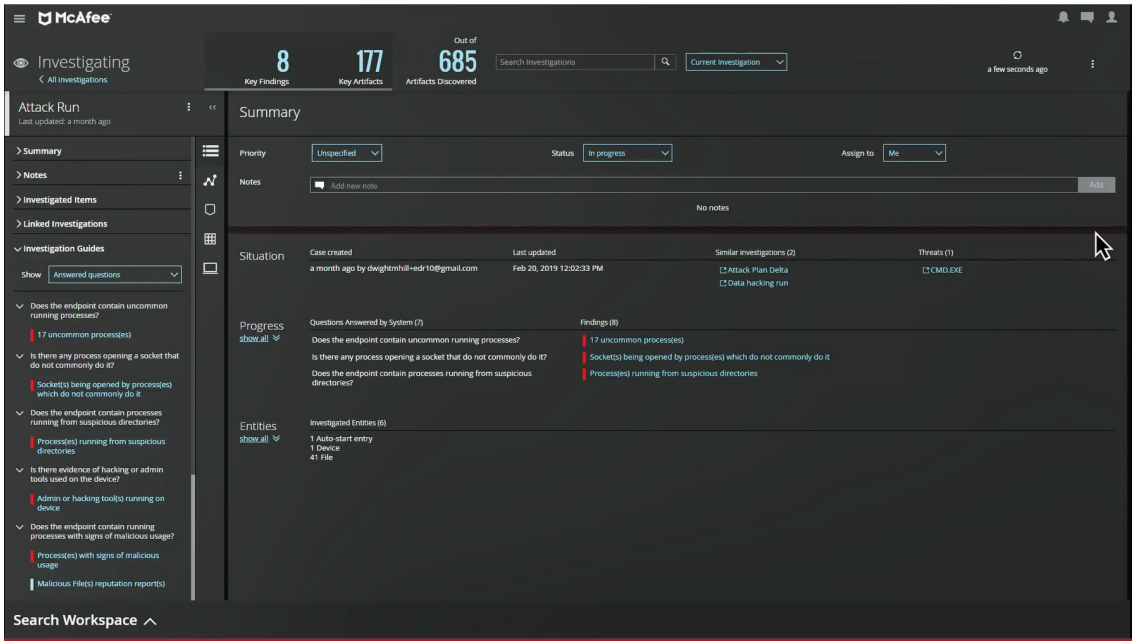

Abbildung 2. KI-geführte Untersuchungen automatisieren die Nachweiserfassung und Analyse, sodass manueller Aufwand entfällt.

- Machine Learning kann IT-Teams bei der Fehleranalyse unterstützen. Wenn Endgerätesicherheitslösungen einen Angriff und dadurch resultierende Schäden nicht verhindern können, sammelt die Machine Learning-Technologie relevante Datenelemente an einem zentralen Ort, damit Sicherheitsanalysten bei Bedarf schnell darauf zugreifen können.

Deep Learning baut auf Machine Learning auf

Durch Deep Learning erhält ein Cyber-Sicherheitssystem die Möglichkeit, automatisch anhand von Milliarden Kombinationen und Beobachtungen zu lernen, sodass menschliche Ressourcen entlastet werden. Deep Learning unterstützt Analysten bei Entscheidungen zu Abwehrmaßnahmen und setzt bei der Erkennung, Abwehr und Korrektur alter und neuer Bedrohungen auf Machine Learning. Deep Learning untersucht facettenreiches Sicherheitsverhalten mithilfe mehrerer komplexer Algorithmen und erkennt dabei Ausnahmen sowie besondere Beziehungen.

- Deep Learning ist effektiv, weil es mehr sieht und mehr weiß. Die Deep Learning-Methodik nutzt neuronale Netzalgorithmen für Schlussfolgerungen und berücksichtigt dabei vergangene Ereignisse, Logik und aktuelle sowie prädiktive Daten.
- Deep Learning-Algorithmen sind meist so komplex wie die Situation. Deep Learning kann deskriptiv, diagnostisch, prädiktiv und präskriptiv sein.
- Deep Learning-Methodiken können für komplexe Entscheidungen mit symbolischen und konzeptuellen Informationen arbeiten. Sie können – basierend auf Aktivitätsmusteranalysen – auf die Beseitigung von Bedrohungen ausgelegt werden, wobei definiert wird, welche Aktivitäten normal sind bzw. den Erwartungen entsprechen und welche als Anomalie eingestuft werden.
- Die Effektivität und Effizienz von Deep Learning-Algorithmen hängt davon ab, dass effektive Datensätze vorhanden sind.

Weitere Informationen

Weitere Informationen zu den Vorteilen von künstlicher Intelligenz, Deep Learning und Machine Learning in der Cyber-Sicherheit finden Sie in diesem McAfee-Whitepaper: Introduction to Artificial Intelligence and Machine Learning (Einführung in künstliche Intelligenz und Machine Learning)

Forrester Spotlight: Empower Security Analysts Through Guided EDR Investigation (Unterstützung der Sicherheitsanalysten durch geführte EDR-Untersuchungen) (Bericht)

SANS Institute: Nachteile herkömmlicher EDR-Lösungen und erforderliche Funktionen (Whitepaper)

SANS Institute: Nachteile herkömmlicher EDR-Lösungen und erforderliche Funktionen (Webcast)

Weitere Ressourcen

Sehen Sie sich unser Video an: AI-Guided Investigations with MVISION EDR (KI-geführte Untersuchungen mit MVISION EDR)

McAfee MVISION Cloud
Demo anfordern

McAfee Together is power.

Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 3707 0
www.mcafee.com/de