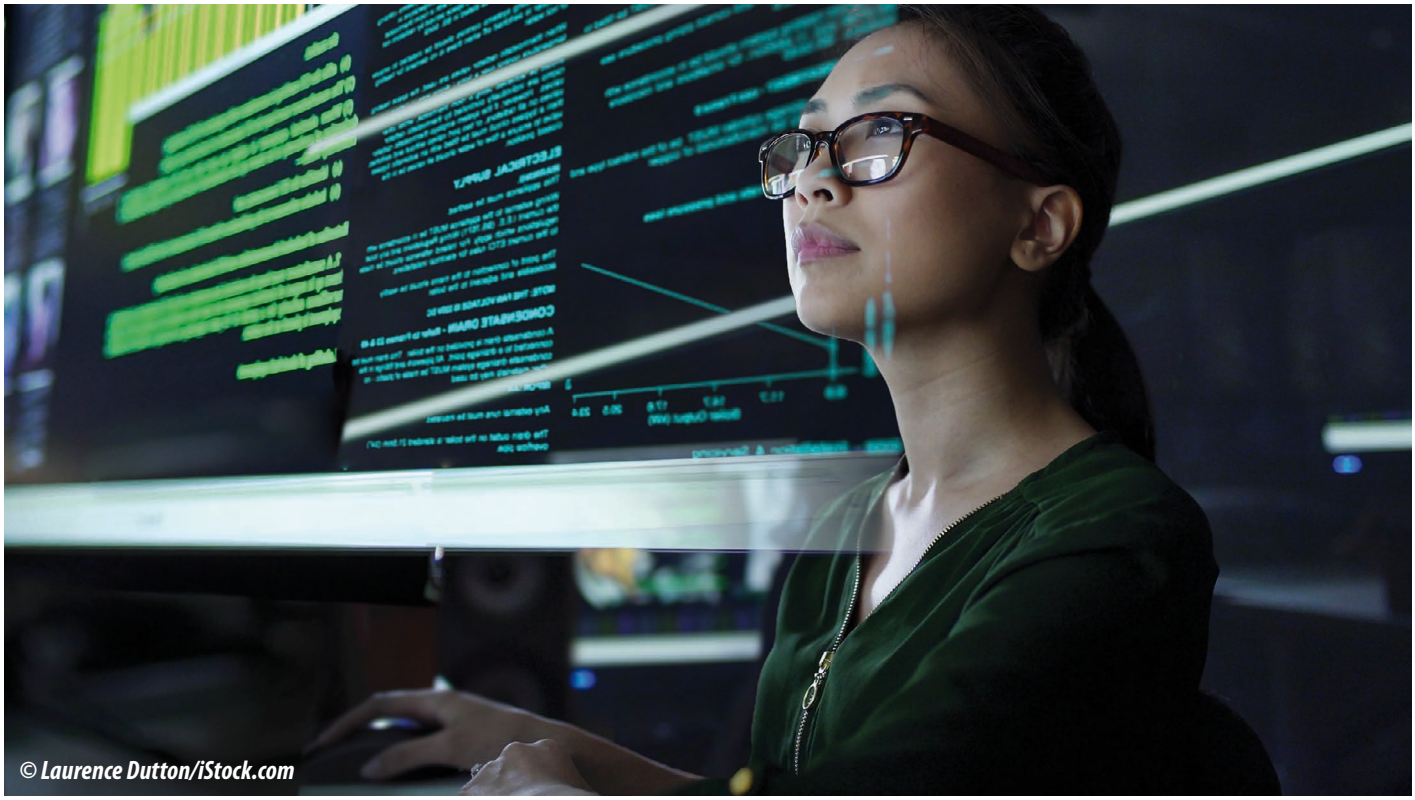
Sieben Aspekte zu Machine Learning in der Cybersicherheit



© Laurence Dutton/iStock.com

Autor:
Sergej Epp
CISO Zentraleuropa
Palo Alto Networks
www.paloaltonetworks.de

Für eine dynamische und leistungsstarke Sicherheitsplattform können Tools auf Basis von maschinellem Lernen (ML) ein wesentliches Element sein. Die Technologie lässt sich in verschiedenen Aufgabenbereichen einsetzen, zum Beispiel zur Erkennung von Malware und Netzwerkanomalien, Kategorisierung von Nutzerverhalten, Priorisierung von Schwachstellen sowie Bedrohungen, und auch zur präzisen Vorhersage zukünftiger Angriffe. Darüber hinaus kann ihr Einsatz dabei helfen, das Modellrisiko zu verbessern, die Klassifizierung von Bedrohungen zu rationalisieren – und gar unmittelbare sowie potenzielle Angriffe genau vorherzusagen. Zudem entlastet ML-basierte Automatisierung Mitarbeitende, indem sie den manuellen Aufwand minimiert.

ML birgt also sehr großes Potenzial für die Cybersicherheit – doch worauf ist bei der Implementierung im Unternehmenskontext zu achten? Die Experten von Palo Alto Networks geben einen Überblick:

1. Supervised und Unsupervised Learning

sind die Hauptkomponenten von ML. Bei der Methodik des **Supervised Learnings** („überwachtes Lernen“) werden aufbereitete Datensätze verwendet, um dem Algorithmus zu helfen, zwischen schädlichen und unschädlichen Daten zu unterscheiden. Nach Analyse der Eingangsdaten mit vorgegebener Zielvariable kann er Prognosen erstellen und präzise Empfehlungen abgeben. Es ist die wichtigste Art von ML. So kommt Supervised Learning zum Beispiel bei der Klassifizierung von Bedrohungen zum Einsatz: Eine Lösung kann potenzielle Bedrohungen eigenständig aus den Datensätzen erkennen, wenn sie ähnliche Merkmale aufweisen wie die historischen Daten.

Beim **Unsupervised Learning** („unüberwachtes Lernen“) hingegen erkundet der Algorithmus eigenständig die Struktur der Daten, ohne im Voraus bekannte Zielwerte zu erhalten. Anschließend gruppiert er diese („Clustering“). So kann Unsupervised Learning den Cybersicheheitsteams einen Überblick über normales und anormales Verhalten bieten.

Generative AI (GenAI) erweitert das Spektrum des maschinellen Lernens, indem es sowohl Supervised als auch Unsupervised Learning integriert. Diese Technik nutzt die Datenanalyse und Vorhersagefähigkeit des Supervised Learning, kombiniert mit der Mustererkennung und explorativen Natur des Unsupervised Learning. GenAI lässt sich vor allem in Bereichen wie Source Code Interpretation, Policy Analyse, Forensik oder Pentesting nutzen.

2. Daten sind der Schlüssel

Um sicherzustellen, dass ML-Algorithmen korrekt ausgeführt werden und das gewünschte Ergebnis liefern, muss eine große Menge an qualitativ hochwertigen Daten eingegeben werden. Diese Datensätze sollten

die für das jeweilige Unternehmen zu erwartenden Bedrohungen repräsentieren, damit das ML-Tool die korrekten Muster und Regeln erlernen kann. Dazu sollten sie auch auf dem neuesten Stand sein und stets erneuert werden.

Daten aus verschiedenen Quellen, die aufgrund unterschiedlicher Datentypen oder Kategorisierungen nicht gut miteinander interagieren und Lücken aufweisen, sind für eine Maschine schwer zu bewerten. Damit der Algorithmus seine volle Leistungsfähigkeit entfalten kann, sollten die Daten daher immer komplett, konsistent und korrekt sein.

3. ML ist prädiktiv, nicht deterministisch

ML befasst sich mit Wahrscheinlichkeiten und Ergebniswahrscheinlichkeiten. Das heißt, es verwendet zur Verfügung gestellte Daten und frühere Ergebnisse, um wiederum potenzielle Resultate in der Zukunft vorherzusagen. Damit ist ML prädiktiv. Obwohl die Vorhersagen nicht deterministisch sind, sind sie allerdings in der Regel sehr genau – und viel schneller verfügbar als nach einer menschlichen Analyse.

4. Regeln

Je nachdem, welche Art von Problem gelöst werden soll, gibt es verschiedene Methoden von ML wie z. B. Regression, Clustering und Assoziationsanalyse. Regression hat das Ziel, eine kontinuierliche Ausgabe oder Vorhersage zu machen. Im Bereich der Cybersicherheit lässt sie sich bei der Betrugserkennung einsetzen. Klassifikation und Clustering teilen Daten in Gruppen oder Kategorien ein, wobei Clustering speziell auf der Grundlage von Ähnlichkeiten in den Daten gruppiert. Bei der Klassifikation ordnet oder gruppiert der Algorithmus Beobachtungen in vordefinierte Kategorien, um etwa Spam von unschädlichen Daten unterscheiden zu können.

Das Lernen von Assoziationsregeln nutzt frühere Erfahrungen mit Daten, um ein bestimmtes Ergebnis wesentlich schneller zu empfehlen, als ein Mensch je in der Lage wäre. Tritt etwa ein Vorfall auf einer Website auf, lassen sich so automatisiert Lösungen bieten.

5. ML und seine Grenzen

ML-Algorithmen sind äußerst effizient bei der Mustererkennung und der Vorhersageerstellung. Allerdings erfordern sie auch viele Ressourcen und sind noch oft recht fehleranfällig, da die Datensätze in ihrem Umfang begrenzt sind – somit können auch ML-Tools an ihre Grenzen stoßen.

6. Zusammenarbeit von Mensch und Maschine

Um die Leistung von ML-basierten Algorithmen in der Cybersicherheit zu steigern, müssen Mensch und Maschine zusammenarbeiten. ML-Algorithmen können zwar die Datenanalyse durchführen, jedoch ersetzt dies nicht die Pflicht von Cybersicherheits-Teams, über die neuesten technologischen Durchbrüche und Veränderungen in der Bedrohungslandschaft auf dem Laufenden zu bleiben.

7. Nahtlose Integration und Interaktion mit anderen Tools

Neue ML-Techniken, die im Cybersicherheitsumfeld Anwendung finden, können sich erst dann entfalten, wenn diese in Prozess- und Technologie-Landschaft nahtlos integriert sind. Es bringt z. B. recht wenig Mehrwert, Gefahren noch schneller zu identifizieren, wenn diese erst nach Tagen geblockt oder behoben werden können. Daher ist es entscheidend, bei ML nicht dem Hype zu verfallen, sondern zu prüfen, in welchen Bereichen der Einsatz von ML-basierten Lösungen tatsächlich sinnvoll ist.

Fazit

„Machine Learning ist aus dem Cyberraum nicht mehr wegzudenken: ML-basierte Lösungen helfen dabei, bestehende Datensilos im Unternehmen sowie die damit verbundenen potenziellen Sicherheitslücken zu schließen und End-to-End-Security zu gewährleisten. Vor allem befähigen sie Security-Teams, proaktiv statt reaktiv zu agieren – und so der Bedrohungslage einen Schritt voraus zu sein“, so Sergej Epp, Chief Security Officer Zentraleuropa bei Palo Alto Networks.

Wer schreibt:

Palo Alto Networks ist das weltweit führende Unternehmen im Bereich der Cybersicherheit. ◄