SentinelOne

Verbesserte Sicherheits-prozesse mit Daten und KI

Die Vorteile eines einheitlichen Cybersecurity-Ansatzes

E-Book

Inhaltsverzeichnis

Generative KI erweckt Daten zum Leben und erweitert die Kompetenzen von Sicherheitsexperten

Wenn Ihre Sicherheitsdaten sprechen könnten, was würden sie sagen? Bei generativer KI (GenAI) ist diese Frage nicht nur rein rhetorisch. Während KI nach und nach alle Branchen erreicht, wird ihr transformatives Potenzial vor allem im Sicherheitsbereich deutlich sichtbar.

Im Cybersecurity-Bereich muss generative KI mehr sein als nur ein Chatbot. Dank der Kombination der analytischen Fähigkeiten von herkömmlicher KI mit der Fähigkeit, zu lernen und Inhalte zu erstellen, können Sicherheitsteams **mit generativer KI Bedrohungen schneller und effektiver erkennen, abwehren und beheben**, ohne zusätzliche Ressourcen zu benötigen. Forscher des Ponemon Institute haben festgestellt, dass hochentwickelte GenAI-Modelle hervorragend in der Lage sind, komplexe Systeme wie Netzwerkinfrastrukturen oder Softwareanwendungen zu analysieren, um Schwachstellen zu identifizieren, neue Bedrohungen aufzudecken und Risiken zu reduzieren.[1]

Generative KI wird Cybersicherheitsteams nicht ersetzen, sondern deren Möglichkeiten verbessern. Sie verändert die Arbeitsweise von Teams, indem sie zeitaufwändige Schritte übernimmt und wichtige Prozesse beschleunigt, sodass sich Ihre Experten auf die Aufgaben konzentrieren können, die sich nur von Menschen erledigen lassen. **Benutzer können mit der KI über eine einfache Benutzeroberfläche in natürlicher Sprache kommunizieren, so als würden sie sich mit einem Sicherheitsanalysten austauschen, der ihnen gegenüber sitzt.** Dadurch können sowohl neue Mitarbeiter als auch erfahrene Sicherheitsexperten fast in Echtzeit die wichtigen Erkenntnisse gewinnen, die sie für ihre Arbeit benötigen. Die KI durchsucht dazu enorme Datenmengen und erkennt Muster sowie Bedrohungen mit Maschinengeschwindigkeit. Gleichzeitig lernt die Technologie im Laufe der Zeit dazu.

Daher liegen die vielversprechendsten Anwendungsbereiche derzeit in der Identifizierung und Untersuchung von Bedrohungen. Generative KI kann zum Beispiel erheblich dazu beitragen, die Warnmeldungsmüdigkeit zu reduzieren. Laut einer Untersuchung ist KI in der Lage, im Durchschnitt 51 % aller Warnmeldungen ganz ohne menschliche Überwachung zu verarbeiten. Ähnliches gilt für die Suche nach Bedrohungen: Diese für menschliches Personal meist sehr zeitaufwändige Aufgabe wird mit generativer KI erheblich beschleunigt. KI kann Benutzer durch Untersuchungen führen und dabei natürliche Sprache in komplexe Abfragen übersetzen, automatisch Zusammenfassungen zu Bedrohungen generieren, damit verwandte Abfragen vorschlagen usw. Mithilfe von KI können Teams enorme Mengen an Sicherheitsdaten aus verschiedenen Umgebungen innerhalb von Minuten statt Stunden analysieren. Damit sparen sie in Situationen, wenn jede Sekunde zählt, wertvolle Zeit.

63 % der IT-Experten sehen in der Cybersicherheit den Bereich mit dem größten Potenzial für generative KI[2]

Im Durchschnitt können **51 %** aller Sicherheitswarnungen ganz ohne menschliche Überwachung verarbeitet werden[1]

50 % der Unternehmen berichten, dass sich ihre Sicherheitslage durch die Einführung von KI für die Cybersicherheit verbessert hat[1]

Fast **69 %** der Unternehmen sind der Meinung, dass sie ohne KI nicht auf Cyberbedrohungen reagieren können[3]

[1] Ponemon Institute und MixMode: *The State of AI in Cybersecurity Report*, 2024.
[2] KPMG: *Using generative AI to strengthen cybersecurity*, 2023.
[3] ISC2: *The Real-World Impact of AI on Cybersecurity Professionals*, 2024.

In den falschen Händen kann generative KI ebenso disruptiv sein

Angreifer kennen die Möglichkeiten von generativer KI ebenfalls – und nutzen sie immer schneller und effektiver aus

Viele Arten von Cyberangriffen sind sich ähnlich, weil die erfolgreichen Strategien immer wieder die gleichen sind. Lassen Sie sich davon aber nicht täuschen: Angreifer führen ständig Neuerungen ein und **nutzen die Möglichkeiten generativer KI für die Weiterentwicklung ihrer Taktiken**. Generative KI senkt die Einstiegshürde für Cyberkriminalität so weit, dass böswillige Akteure lediglich Schwachstellen in einer Software finden müssen. Gleichzeitig ist GenAI in der Lage, das Schadenspotenzial und die Effektivität von Angriffen zu steigern sowie deren Erkennung zu erschweren. Laut dem britischen National Cyber Security Centre (NCSC) nutzen bereits alle Arten von Cyberbedrohungsakteuren KI in irgendeiner Form. Das gilt für staatlich unterstützte und auf eigene Rechnung handelnde sowie für erfahrene und unerfahrene Angreifer gleichermaßen.[1]

Nehmen wir einen Phishing-Angriff, bei dem die Hacker mithilfe von WormGPT (einem böswilligen Zwilling von OpenAI ChatGPT) überzeugendere Phishing-Nachrichten erstellen, die keine verräterischen Grammatikfehler enthalten und daher Benutzer schneller dazu verleiten, sensible Informationen weiterzugeben.[2] Böswillige Akteure verwenden generative KI auch, um Schadcode zu generieren, der Schwachstellen in Sicherheitssystemen ausnutzen kann, sodass sie auf sensible Daten zugreifen und über einen längeren Zeitraum unerkannt bleiben können. Leider sind diese Szenarien nur die Spitze des Eisbergs. Nach dem Aufkommen von Ransomware-as-a-Service (RaaS)[3] ist ein Schwarzmarkt entstanden, auf dem hochentwickelte KI-gestützte Tools im großen Maßstab verkauft werden. Dies hat die Einstiegshürden für böswillige Akteure gesenkt und die Tür für Weiterentwicklungen und noch größere Schäden in der Zukunft geöffnet. Das gilt zumindest dann, wenn den Angreifern freie Hand gelassen wird.

Angreifer lassen sich am besten mit ihren eigenen Waffen schlagen

Auch wenn die Gefahr von KI in den falschen Händen real ist, zeigen aktuelle Trends einen Vorteil bei den Sicherheitsexperten. Laut dem NCSC wird die Nutzung von KI für Cyberbedrohungen durch eine stärkere Resilienz ausgeglichen, weil KI die Erkennung und die standardmäßigen Cybersicherheitsfunktionen verbessert.[1] Generative KI kann relevante Erkenntnisse zur Priorisierung von Bedrohungen liefern, indem sie Schwachstellen identifiziert und die Auswirkungen potenzieller Bedrohungen bewertet – ähnlich wie bei böswilligen Akteuren, allerdings für einen guten Zweck.

[1] National Cyber Security Centre: *The Impact of AI on Cyberthreats*, 2024.
[2] SlashNext,com: *WormGPT – The Generative AI Tool Cybercriminals Are Using to...*, 2023.
[3] SentinelOne: *Das Gute, das Schlechte und das Hässliche in der Cybersicherheit, Woche 15*, 2024.

Daten sind die Grundlage für leistungsstarke KI-gestützte Sicherheitsprozesse

KI-Nutzung für Cybersicherheit beginnt mit Daten

GenAI-Modelle benötigen Daten, um Bedrohungen effektiv abwehren zu können.

Ohne ausreichend nutzbare, hochwertige Daten fehlt den KI-Algorithmen möglicherweise die Datenbasis für fundierte Empfehlungen und entscheidungsrelevante Erkenntnisse. Schlimmer noch: Ohne eine solide Datenbasis können die Ergebnisse ungenau oder einseitig sein, was die Effektivität reduziert und negative Folgen haben kann.

KI-fähige Sicherheitsprozesse erfordern eine neue Datenstrategie und einheitliche Daten

Damit Unternehmen Modelle für generative und herkömmliche KI nutzen können, die die erforderliche Genauigkeit und Leistung bieten, benötigen sie eine einheitliche Basis für hochwertige, standardisierte Daten. Der Aufbau dieser Datenbasis kann jedoch aus verschiedenen Gründen schwierig sein:

- Unternehmen verfügen häufig über **mehrere Data Lakes**, die unterschiedliche Schemata, Datenformate, Daten-Governance-Richtlinien usw. nutzen.
- Unternehmen speichern unter Umständen **enorme Datenmengen**, die sich nur mit erheblichen Investitionen zusammenführen lassen.
- Unternehmen nutzen **verschiedene Tools oder Lösungen, die sich nicht integrieren lassen**, sodass Daten, Produkte und Workflows isoliert bleiben.
- Unternehmen fehlen die personellen oder finanziellen **Ressourcen**, um Daten zu vereinheitlichen.

Kurz gesagt: Unternehmen benötigen einen ganzheitlichen Ansatz für Daten und KI, der alle Aspekte berücksichtigt, einschließlich Datenquellen, KI-Modelle und die Prozesse zur Bereitstellung der Erkenntnisse für das Sicherheitsteam. Gleichzeitig müssen die Kosten überschaubar bleiben. Das ist nur möglich, wenn Unternehmen den isolierten Ansatz für Daten, Lösungen und Workflows hinter sich lassen.

Regulatorischer Druck erschwert Vereinheitlichung von Daten

Da jedes Jahr neue Sicherheits- und Compliance-Vorschriften eingeführt werden, steigt der regulatorische Druck. Die US-amerikanische Börsenaufsichtsbehörde SEC (Securities and Exchange Commission) hat allein im Jahr 2023 **mehr als 50 Durchsetzungsmaßnahmen im Bereich Cybersicherheit** veranlasst.

Das Befolgen all dieser Anforderungen ist eine Herausforderung und wird immer kostenintensiver und aufwändiger. Denn Unternehmen archivieren Daten zu Compliance-Zwecken und schaffen damit immer mehr Datensilos, was die Erstellung vereinheitlichter Daten weiter erschwert.

[1] Newfront: *Newfront Cyber Update: New Cyber Rules Coming into Force in 2024*, 2024.

Ein einheitlicher Plattformansatz ist zur vollständigen Nutzung von Daten und KI und zur Reduzierung von Risiken unverzichtbar

Maximieren des Datenwertes und Beginn eines Zeitalters der KI

Wie binden Sie also Sicherheitsdaten ein, damit generative KI mit deren Hilfe die Sicherheitsprozesse verbessern kann? Die Antwort ist eine einheitliche Cybersecurity-Plattform, die eine grundlegende Infrastruktur für die effektive Verwaltung, Analyse und Nutzung von Unternehmensdaten bereitstellt. Doch ein einheitlicher Ansatz führt nicht nur zu organisierten Daten, sondern ermöglicht zudem verbesserte sowie umfassende Transparenz für den Bedrohungsdaten-Lebenszyklus – von der Erkennung und Untersuchung bis zur Reaktion und darüber hinaus. Eine einheitliche Plattform ermöglicht die Konsolidierung von Tools und Prozessen und vereinfacht die Automatisierung von Aufgaben mit KI sowie die Gewinnung relevanter Erkenntnisse für Sicherheitsteams. Dadurch sinken die Kosten und der Aufwand, während gleichzeitig die allgemeine Sicherheit des Unternehmens gesteigert und das Risiko reduziert wird.

Nicht nur das Offensichtliche: Die Elemente einer einheitlichen Cybersecurity-Plattform

Doch was genau macht einen „einheitlichen Plattform-Ansatz“ aus? Ganz einfach ausgedrückt, bezieht sich ein einheitlicher Ansatz auf eine umfassende und vollständig integrierte Plattform, die Sicherheitslösungen in eine **einzige Backend-Datenumgebung mit einer Benutzeroberfläche** konsolidiert. Die Plattform **entwickelt sich dabei ständig weiter**, um mit neuen Bedrohungen Schritt zu halten, und sie ist erweiterbar, um innovative Schutzansätze einbinden zu können. Ein einheitlicher Ansatz bietet folgende Vorteile:

- Verbesserter Zugriff auf Informationen, da es einfacher und schneller möglich ist, Erkenntnisse aus einer **einheitlichen Datenbasis** zu gewinnen, die alle Unternehmensdaten umfasst
- Optimierte Benutzererlebnisse, da funktionsübergreifende **koordinierte Sicherheits-Workflows** unterstützt werden, sodass Sicherheitsteams schneller und effizienter arbeiten können
- Umfasst eine integrierte **Ebene für Analysen und KI**, die Sicherheitsteams unterstützt und zukünftige Innovationen ermöglicht

Sehen wir uns diese Vorteile und das Potenzial bei Sicherheitsprozessen genau an, beginnend mit einer einheitlichen Datenbasis.

Verbesserte Sicherheitsprozesse mit leicht abrufbaren, hochwertigen Daten

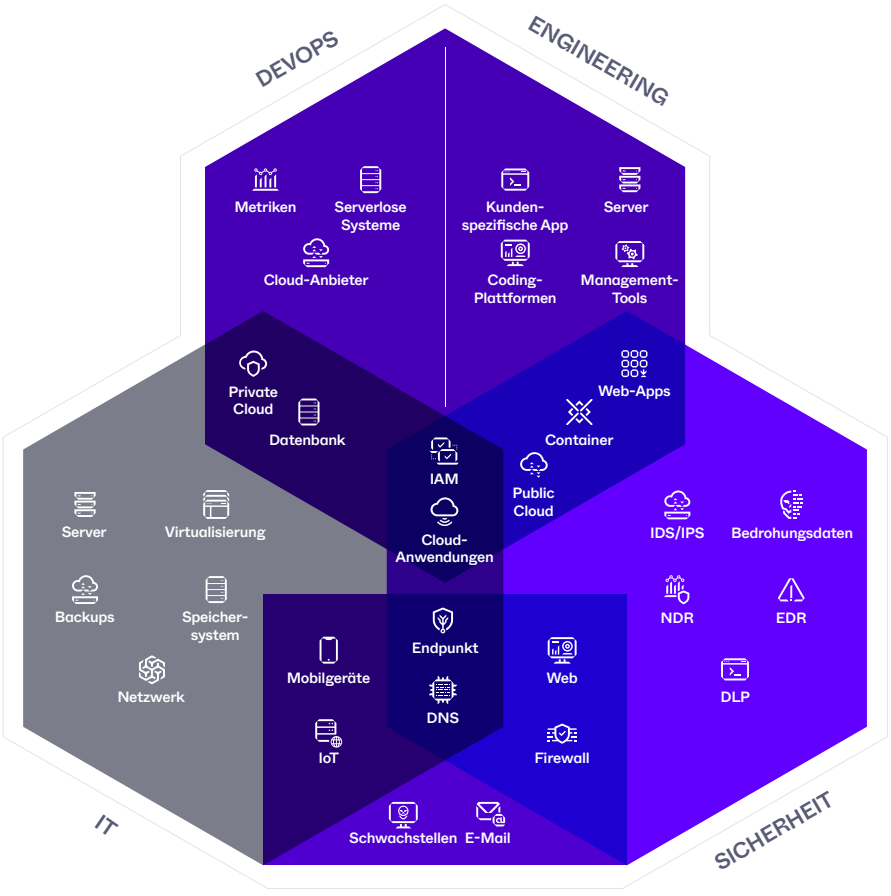
Mit einem einheitlichen Data Lake können Anwendungen native und externe Daten kontextualisieren und weitergeben

Bei vielen vorgeblich „einheitlichen Plattformen“ handelt es sich um getrennte Lösungen, die über eine Benutzeroberfläche verbunden sind, oder um Produkt-Suites, die jeweils eigene Data Lakes nutzen. In beiden Fällen bieten diese „Plattformen“ lediglich eine zentralisierte Benutzeroberfläche. **Damit Anwendungen wirklich effektiv zusammenarbeiten können, müssen sie sich auch die Daten und den Kontext im Backend teilen.** Deshalb ist ein einheitlicher Data Lake unverzichtbar.

Bei einem **einheitlichen Data Lake** erhalten umgebungsübergreifende Oberflächen ein zentrales Repository für den Abruf und die Speicherung von Daten. Das Markenzeichen eines starken **Data Lakes ist die Erfassung**, Speicherung und Verwaltung von nativen und externen Daten, einschließlich aller Protokolle und Forensikdaten. Gleichzeitig lässt sich ein solcher Data Lake leicht verwalten und bleibt dabei kostengünstig.

Durch die Zentralisierung von Daten an einem einzigen Ort können Teams alle erfassten Daten durchsuchen, um schneller Erkenntnisse zu gewinnen und die mittlere Zeit bis zur Erkennung und Reaktion (MTTD/MTTR) zu reduzieren. Ein einheitlicher Data Lake verringert zudem die Speicherkosten, die bei mehreren Data Lakes erforderlich sind.

Zudem gilt bei generativer KI ganz besonders: Wenn Sie einen einheitlichen Data Lake verwenden, können erheblich umfangreichere Daten aus mehr Bereichen abgefragt werden. Bei einem größeren Pool an Informationen können Modelle ihre Entscheidungsfindung verbessern und genauere sowie relevantere Antworten geben.



Eine starke Datenstrategie beschränkt sich nicht auf Datensammlung

Optimierung des Zugriffs mit offenen Cybersecurity-Datenstandards und Datenportabilität

Ein einheitlicher Data Lake bietet nicht nur Datenaggregation, sondern umfasst auch **Konnektoren und Parser, die Daten aus Anwendungen in einem gemeinsamen Framework normalisieren und kontextualisieren**, um Redundanz zu vermeiden und die Speicherkosten zu senken. Im Idealfall basiert dieses Framework auf offenen Standards wie OCSF (Open Cybersecurity Schema Framework), um die Interoperabilität jetzt und in Zukunft zu verbessern. Offene Standards beschleunigen die Bedrohungserkennung, Analyse sowie Reaktion und reduzieren den Aufwand für Cybersicherheitsteams. Dadurch müssen die Teams nicht mehr wertvolle Arbeitszeit für das Zusammenstellen und Standardisieren von Daten verschwenden, sondern können sich auf die proaktive Implementierung von Sicherheitsverbesserungen konzentrieren. Offene Standards ermöglichen auch **Datenportabilität**, sodass Unternehmen bei Bedarf mehr Sicherheitstools nutzen und dank nahtloser Datenmigration den störungsfreien Geschäftsbetrieb sicherstellen können.

Einfachere Datenabfragen und -abrufe bei geringeren Speicherkosten

Wirklich einheitliche Data Lakes unterstützen eine **einheitliche Abfragesprache**, um die systemübergreifende Interoperabilität zu verbessern und den Datenzugriff für Anwender zu vereinfachen. Bei einer einheitlichen Abfragesprache müssen die Analysten nicht mehr aufwändig mehrere Syntax-Formen für verschiedene Datenquellen und Systeme lernen und nutzen. Dadurch sparen sie nicht nur Zeit, auch die Fehlerwahrscheinlichkeit wird verringert. Wenn eine einheitliche Abfragesprache mit KI-Modellen kombiniert wird, die offene Standards wie OCSF unterstützen, wachsen dadurch die Möglichkeiten von KI. So verbessert KI durch die normalisierte Abfrage, Nutzung und Analyse nativer und externer Daten beispielsweise die Geschwindigkeit und Effizienz von Sicherheitsprozessen.

Und nicht zuletzt erlaubt ein einheitlicher Data Lake auch effiziente Datenabrufe und damit schnellere Incident Response und optimierte Untersuchungen. Möglich ist das durch die **Integration und Kommunikation zwischen unterschiedlichen Datenquellen** sowie durch die spaltenbasierte Speicherung, bei der die Daten jeder Spalte separat gespeichert und Abrufe und Abfragen erheblich beschleunigt werden. In Verbindung **mit einer Cloud-nativen Architektur sowie einem mehrmandantenfähigen Aufbau** lässt sich dieser Ansatz leicht mit dem Wachstum des Unternehmens skalieren.

Wussten Sie schon? Offene Standards sind im Aufschwung

Offene Standards wie OCSF gewinnen weltweit an Fahrt[1] – und dafür gibt es einen guten Grund. Viele Unternehmen nutzen immer mehr Sicherheitstools, um mit den Bedrohungen Schritt zu halten. Damit diese Tools miteinander kommunizieren und maximalen Nutzen entfalten können, sind jedoch offene Standards erforderlich.

Die derzeit gebräuchlichen anbieterspezifischen Standards führen dazu, dass Anwendungen in Datensilos isoliert sind. Das bedeutet für Sicherheitsteams nicht nur mehr Aufwand für die Integration von Tools, sondern beeinträchtigt auch die Effizienz von Sicherheitslösungen, weil wichtige Erkenntnisse fehlen.

OCSF ermöglicht die Integration dieser Systeme, ohne deren Vertraulichkeit und Integrität zu beeinträchtigen, sodass Unternehmen schnell auf neue Bedrohungen reagieren und sicherstellen können, dass auch weitere Tools – unabhängig vom Anbieter – reibungslos integriert werden können. Sicherheitsteams sparen dadurch erheblich Zeit, da sie nicht mehr Daten aus mehreren Einträgen zusammenstellen und standardisieren müssen, um nützliche Erkenntnisse zu gewinnen. Offene Standards bieten noch viele weitere Vorteile. So können Entwickler auf der Arbeit ihrer Kollegen aufbauen und gemeinsam den Weg für branchenweite Innovationen bahnen.

[1] Linux Foundation: *The 2023 State of Open Standards*, 2023.

Verbesserte Abläufe für Analysten durch koordinierte Sicherheits-Workflows und Echtzeit-Analysen

Nicht vernetzte Workflows sind ein Sicherheitsproblem

Im Idealfall verbringen Sicherheitsteams ihre Zeit mit der Beseitigung von Risiken und mit proaktiven Maßnahmen gegen Bedrohungen. Tatsächlich führen komplexe Workflows jedoch zu Ineffizienzen. Aktuelle Cybersecurity-Workflows sind häufig nicht vernetzt, da die Unternehmen verschiedene isolierte Tools und Prozesse nutzen, z. B. für Bedrohungserkennung, Incident Response und Schwachstellenverwaltung. Das kann zu Transparenz- und Koordinationslücken führen, was auf jeden Fall die Reaktionszeit verlängert und Ressourcen verschwendet. Schlimmstensfalls bedeutet es jedoch eine kostspielige Sicherheitsverletzung, die schwerwiegende Folgen für das Unternehmen haben kann.

Eine zentrale Konsole macht häufige Wechsel zwischen Sicherheitstools überflüssig

Da die Teams über eine einzige Oberfläche auf ihre Tools zugreifen können, **verbessern sich Transparenz und Benutzerfreundlichkeit** erheblich. Bei einer zentralen Verwaltungs- und Steuerungskonsole müssen Sicherheitsteams weniger Zeit mit dem Wechsel zwischen mehreren Tools und Prozessen verbringen. Diese Konsole dient als Zentrale für die Verwaltung von Richtlinien, Überwachen von Ereignissen und Koordinierung von Incident-Response-Aktivitäten, sodass die Sicherheitsverantwortlichen einen besseren Überblick über ihre gesamte Umgebung erhalten. Wenn zudem das richtige Maß an Anpassbarkeit gegeben ist, können Analysten genau so arbeiten, wie es für sie optimal ist.

Verbesserte grundlegende Funktionen mit zukunftsorientierter Ausrichtung der Sicherheitsprozesse

Einer der wichtigsten Vorteile einer einheitlichen Plattform ist die **Geschwindigkeitssteigerung ohne Einbußen bei der Effizienz**. Die Nutzung von Funktionen wie XDR über eine einzige Benutzeroberfläche ist erheblich einfacher und effektiver, sodass Sicherheitsteams die benötigten Informationen schnell abrufen können. Eine einheitliche Plattform hilft Benutzern mit integrierten KI- und Analysefunktionen und beim Untersuchen von Threat Intelligence-Feeds aus verschiedenen Quellen sowie beim Anreichern von Sicherheitstelemetrie mit Kontextinformationen über bekannte Bedrohungen. Dabei wendet die KI Erkennungslogik und Analysen für alle Daten im Unternehmen an und ist dabei schneller, als das menschenmöglich wäre. Dadurch sparen die Sicherheitsteams viel Zeit und können größere Bereiche als bisher abdecken.

Nicht zuletzt schafft ein einheitlicher Ansatz eine **erweiterbare Basis, die fit für die Zukunft ist**. Diese Erweiterbarkeit gibt Unternehmen die Möglichkeit, neue eigene und externe Lösungen unkompliziert zu integrieren, zu skalieren und neue Bedrohungen abzuwehren, selbst wenn sie ansonsten Legacy-Systeme nutzen. Dadurch können die neuesten Cybersecurity-Innovationen integriert werden, während gleichzeitig die Interoperabilität und Kompatibilität mit vorhandenen Tools und Prozessen gewährleistet bleibt.

Risikominimierung durch eine GenAI-Ebene, die Sicherheitsprozesse für das gesamte Team beschleunigt

Worin bestehen die Unterschiede? Erklärung typischer KI-Begriffe

Künstliche Intelligenz (KI)
Systeme, die mit hochentwickelten Analysen und Logik intelligentes Verhalten imitieren, einschließlich Verstehen von Artefakten/Texten, Produzieren neuer Artefakte/Texte und Toking- oder Automatisierungs-Aktionen.

Machine Learning (ML)
Klasse von Algorithmen, deren Verhalten sich abhängig von den erhaltenen Daten verändert.

Generative KI
Kategorie stark skalierter ML-Modelle, die von einer Artefakt-Darstellung lernen und nach Aufforderung neue darauf bezogene Artefakte generieren kann.

Large Language Models (LLMs)
Kategorie von GenAI-Modellen, die mit großen Textmengen trainiert wurden, um Texteingaben zu verstehen und menschlich klingende Textausgaben zu generieren.

Generative KI gibt Analysten Echtzeit-Informationen und automatisierte Funktionen in die Hand

Konventionelle Cybersecurity-Ansätze zur Datenanalyse führen oft zu Verarbeitungsverzögerungen von mehreren Stunden – oder noch länger. Dadurch sind sie der Geschwindigkeit komplexer Bedrohungen nicht gewachsen. **Die Integration von GenAI-Lösungen in eine einheitliche Plattform schließt die Reaktionslücke, minimiert die Verarbeitungszeit und ermöglicht Datenanalysen nahezu in Echtzeit.** Das verbessert nicht nur die Effizienz von Cybersicherheitsmaßnahmen, sondern liefert auch eine umfassende Übersicht über die Sicherheitslage des Unternehmens.

Eine KI- und Analyseebene macht Datenbestände lebendig – und zum festen Bestandteil des Sicherheitsteams

Der Vorteil von generativer KI und Analysen liegt darin, dass damit Daten lebendig werden und Sicherheitsteams mit der KI in **natürlicher Sprache** wie mit einem zusätzlichen Experten im Team interagieren können. Das bietet für alle Benutzer enorme Vorteile: Bei Nachwuchsanalysten erweitert das ihre Möglichkeiten, weil sie nicht mehr zeitaufwändig Abfragen in einer bestimmten Sprache lernen und optimieren müssen, sondern stattdessen Daten wie bei einem Gespräch abfragen können. Gleichzeitig können erfahrene Analysten der generativen KI das Schreiben der Abfragen überlassen, was ihnen Zeit für Aufgaben gibt, die nur sie beherrschen.

Generative KI **optimiert die Bedrohungserkennung und -untersuchung**, indem sie Erkennungslogik und Datenanalysen anwendet und als „Wächter“ über mehrere Angriffsflächen hinweg Echtzeit-Erkenntnisse generiert, z. B. bei Spitzen in der Netzwerkaktivität. Sie **minimiert die Warnmeldungsmüdigkeit**, weil sie die Teams mit geführten Empfehlungen darüber informiert, welche Bedrohungen sie priorisieren sollen. KI kann auch die Behebung von Warnungen beschleunigen, indem sie (z. B. über Integrationen mit Ticket-Systemen) automatisierte Workflows auslöst. Sie ist stets wachsam und führt automatisch Untersuchungen im Hintergrund durch, um den Überwachungsaufwand für alle Teams nachhaltig zu reduzieren.

Nicht zuletzt ist KI ein leistungsstarkes **Tool zur Bedrohungsabwehr**. Beim Anwenden von Richtlinien ermöglicht generative KI Ein-Klick-Migrationsaktionen und Orchestrierungsintegrationen für angepasste, automatisierte Playbook-Reaktionen. Nachdem eine Bedrohung behoben wurde, liefert die KI zudem automatische Zusammenfassungen, sodass Benutzer ihre Zeit nicht mit dem Dokumentieren ihrer Ergebnisse verschwenden müssen.

Einheitliche Plattformen ermöglichen nützliche GenAI-Nutzungsszenarien und erleichtern Sicherheitsteams die Skalierung

Eine einheitliche GenAI-gestützte Plattform verringert nicht nur die Zahl der Workloads, ohne den Schutz zu beeinträchtigen – sie definiert die Möglichkeiten in der Cybersecurity neu

Wir sehen zahlreiche transformative Nutzungsszenarien, die von einer einheitlichen GenAI-gestützten Plattform möglich gemacht werden. Da die künstliche Intelligenz im Laufe der Zeit nur noch weiter verbessert wird, ist noch mehr zu erwarten. Zu den aktuell wichtigsten Nutzungsszenarien gehören:

KI-gestützte Anomalie-Erkennung in Drittanbieter-Protokollen

KI bietet umfangreiche Erkennungsmöglichkeiten, die in eingebundenen Protokollen automatisch Anomalien in Ereignissen finden. Wenn ein Unternehmen Drittanbieter-Protokolle einbindet, die dann im einheitlichen Data Lake erfasst werden, kann KI potenzielle Sicherheitsbedrohungen identifizieren. Dazu gehören potenziell gekaperte Konten, die in Ereignissen mit verdächtigen geografischen Standorten auftauchen.

Automatisierte Triage von Warnmeldungen und globale Ähnlichkeitsanalysen

KI automatisiert das Triagieren von Warnmeldungen, indem sie weltweit Milliarden anonymisierte Datensignale analysiert, um ähnliche Warnungen zu identifizieren und zu verstehen, wie Analysten darauf reagiert haben. Wenn Analysten eine Warnung erhalten, sehen sie zum Beispiel, dass „93 % der ähnlichen Warnungen“ als True Positive gekennzeichnet wurden (sodass die KI diese Warnung ebenfalls als relevant eingestuft hat). Da die Analysten außerdem erfahren, dass „32 ähnliche Warnungen in ihrer Umgebung offen“ sind, können sie für die optimale Reaktion effiziente und evidenzbasierte Entscheidungen treffen. Die KI lernt anschließend aus den Reaktionen der Analysten, um ihre Ähnlichkeitsanalyse und die Empfehlungen kontinuierlich zu verbessern.

KI-gestützte Reaktionen und hyperautomatisierte Empfehlungen, die vollautomatische Reaktionen ermöglichen

Die KI empfiehlt intelligente Behebungsmaßnahmen, um die mittlere Reaktionszeit (MTTR) zu verkürzen und den Schutz erheblich zu skalieren. Dazu wird Analysten für jede Warnmeldung eine Empfehlung angezeigt, die auf typischen Reaktionen bei ähnlichen Warnungen basiert. Diese Aktion lässt sich auf alle ähnlichen offenen Warnmeldungen in ihrer Umgebung anwenden. Möglich ist aber auch die Erstellung einer Hyperautomatisierungsregel, die bei jeder neuen und vergleichbaren Warnung automatisch reagiert.

Automatisch rund um die Uhr ablaufende Untersuchungen unterstützen Sicherheitsverantwortliche

Wenn nach der automatischen Triagierung einer Warnmeldung weitere Untersuchungen ausgelöst werden, geht die KI automatisch alle Untersuchungsschritte durch, überprüft die Protokolle und sammelt Nachweise. All diese Schritte werden in einer leicht verständlichen Oberfläche dargestellt. Durch diese automatischen Untersuchungen ersparen sich Sicherheitsteams aufwändige Arbeitsschritte und können sich stattdessen auf die Überprüfung der Ergebnisse konzentrieren, die von der KI zu bereits abgeschlossenen Untersuchungen geliefert wurden.

Vorsprung vor aktuellen und zukünftigen Bedrohungen dank vertrauenswürdiger Cybersecurity-Partner

Technologie steht nicht immer an erster Stelle

Bei der Implementierung von Cybersecurity-Strategien in Unternehmen spielen erfahrene Partner eine zentrale Rolle. Die besten Partner haben sowohl eine klare Zukunftsvision für die Cybersicherheit als auch die Möglichkeiten, dieses Versprechen umzusetzen. Ein starker Partner, der Sie beim Implementieren einer einheitlichen Plattform mit KI-Funktionen unterstützt, sollte Folgendes bieten:

- Eine klare **Cybersecurity-Vision**, die an den wichtigsten Strategien und Prioritäten Ihres Unternehmens ausgerichtet ist
- Das Fachwissen für die Bereitstellung von **Managed Detection and Response sowie proaktiven Planungsservices**
- **Cloud-native SaaS-Verwaltung** für stark skalierte Umgebungen
- **Flexible, lokale Verwaltung**, die konkreten und individuellen Anforderungen von Kunden Rechnung trägt
- **Unterstützung für Kunden beim Erstellen der Konnektoren**, die sie für die Implementierung der Plattform benötigen
- Engagierte Umsetzung **neuer Vorschriften**, die z. B. KI oder Datenschutz abdecken, damit die bereitgestellten Tools alle Compliance-Anforderungen erfüllen
- Einhaltung von **Datenschutzvorschriften**; nicht alle Anbieter, die ihre Lösungen mit Kundendaten (z. B. Sicherheitsinformationen, Prozesse und Erkenntnisse) trainieren, halten hohe Datenschutzstandards ein

SentinelOne öffnet die Tür zum Zeitalter von Daten und KI-gestützter Cybersecurity

Mehr Funktionen. Weniger Komplexität. Das ist SentinelOne.

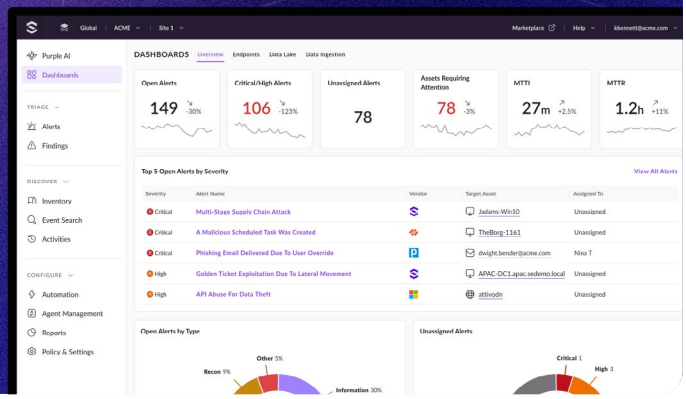
Mit der führenden KI-Sicherheitsplattform ist SentinelOne optimal aufgestellt, um Unternehmen bei der Nutzung von Daten und KI für reibungslosen Schutz zu unterstützen. In den folgenden Ressourcen lernen Sie unseren einheitlichen Ansatz kennen.

- Besuchen Sie SentinelOne.com und erfahren Sie, wie wir die Zukunft der Cybersecurity definieren.
- Unsere Webseite zur Singularity-Plattform bietet viele Details zur weltweit fortschrittlichsten Cybersicherheitsplattform.
- Erfahren Sie, wie der Singularity Data Lake Ihre Daten zentralisieren und transformieren kann, um nahezu in Echtzeit Bedohungsdaten zu liefern.
- Lernen Sie die leistungsstarken Funktionen von Purple AI kennen, der weltweit fortschrittlichsten KI für Sicherheitsanalysen.

Haben Sie Interesse an einer Demo?

Weitere Informationen dazu finden Sie auf der SentinelOne-Website oder kontaktieren Sie uns unter +1-855-868-3733.

de.sentinelone.com



Innovativ. Vertrauenswürdig. Anerkannt.

Gartner

Führender Anbieter im 2023 Magic Quadrant™ für Endpoint Protection-Plattformen

MITRE ENGENUITY

Rekordergebnis bei der ATTACK-Bewertung

+ 100 % Schutz. 100 % Erkennung
+ Höchste analytische Abdeckung, 3 Jahre in Folge
+ 100 % Echtzeit und keinerlei Verzögerungen

Gartner Peer Insights

96 % BEI GARTNER PEER INSIGHTS™

EDR-Analysten empfehlen SentinelOne Singularity

FedRAMP · TEVORA PCI DSS Attestation HIPAA Attestation · AICPA SOC · STAR LEVEL ONE · 100 VIRUS · SE Labs BEST Innovator WINNER 2021 · AAA · Trusted Cloud Provider CSA

Kontaktieren Sie uns

sales@sentinelone.com
+1-855-868-3733

de.sentinelone.com

Informationen zu SentinelOne

SentinelOne (NYSE:S) ist ein Vorreiter auf dem Gebiet der autonomen Cybersicherheit und verhindert, erkennt und stoppt Cyberangriffe schneller und genauer als je zuvor. Unsere Singularity XDR-Plattform schützt und stärkt weltweit führende Unternehmen mit einem Echtzeitüberblick über Angriffsflächen sowie mit plattformübergreifender Korrelation und KI-gestützten Reaktionen. Nutzen Sie mehr Optionen mit geringerer Komplexität.

Strengthening_Security_Operations_with_Data_and_AI_v2_de_01232025