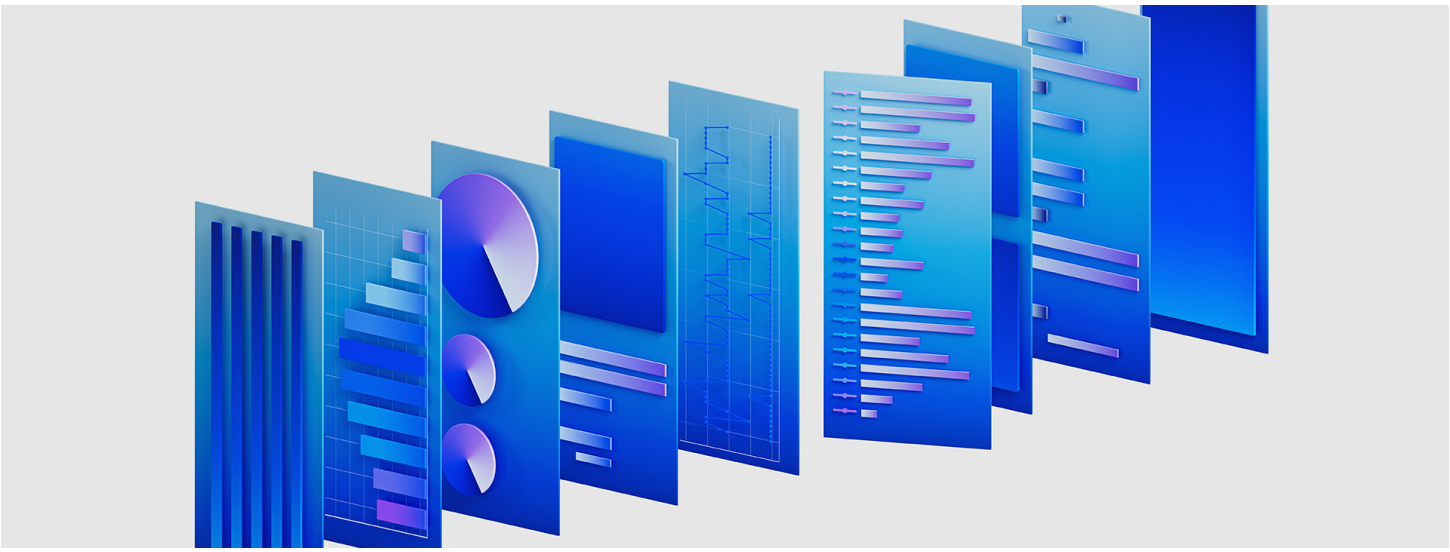
IBM DACH Newsroom

IBM stellt Cloud-natives SIEM vor, um den Ressourceneinsatz von Sicherheitsteams zu optimieren

Modernisierte Basis und neu gestaltete Benutzeroberfläche ermöglichen Sicherheitsanalysten und KI-Tools effektiver zusammenzuarbeiten



ARMONK, N.Y., 7. November 2023 – IBM kündigt heute eine bedeutende Weiterentwicklung der QRadar SIEM-Technologie an, die auf einer neuen Cloud-nativen Architektur basiert und speziell für die Skalierbarkeit, Geschwindigkeit und Flexibilität von Hybrid-Cloud-Umgebungen konzipiert wurde. Zudem stellt IBM Pläne vor, generative KI-Funktionen im Portfolio zur Erkennung und Abwehr von Sicherheitsbedrohungen zu verwenden. Die Basis bildet watsonx, die Daten- und KI-Plattform, die für den Einsatz im Unternehmen entwickelt wurde.

Heutige Hybrid-Cloud-Umgebungen entwickeln sich weiter und skalieren mit exponentieller Geschwindigkeit, wodurch eine größere und komplexere Angriffsfläche entsteht, die Unternehmen schützen müssen. Die stetig wachsende IT-Umgebung macht es für Sicherheitsteams schwieriger, ernsthafte Bedrohungen unter der Vielzahl an Meldungen zu finden. Zusätzlich werden ihre Anstregungen durch isolierte Technologien, manuelle Suchvorgänge und eine Flut von Warnmeldungen ohne klaren Kontext oder verständliche Visualisierungen erschwert. Laut einer kürzlich durchgeführten weltweiten Umfrage schaffen SOC-Fachleute an einem normalen Arbeitstag weniger als die Hälfte (49 %) der Alerts, die sie überprüfen sollen.[1]

„Unser neues Cloud-natives SIEM stellt ein Kernelement der Mission von IBM dar, die nächste Generation von Sicherheitsoperationen auf die Hybrid-Cloud- und KI-Ära auszurichten“, so Kevin Skapinetz, Vice President, Strategy and Product Management, IBM Security. „Anstatt Analysten dazu zu zwingen, mit der Komplexität von Sicherheitstechnologien umzugehen, entwerfen wir Technologien, um die Komplexität zu beseitigen – indem wir Meldungen reduzieren, das Benutzererlebnis vereinfachen und Analysten in die Lage versetzen, dringende Bedrohungen schneller und zuverlässiger anzugehen.“

Das neue Cloud-native IBM QRadar SIEM baut auf QRadars 13-jähriger Marktführerschaft und Anerkennung durch Analysten für tiefgehende Sicherheitsanalysen auf[2]. Die Cloud-native Lösung zeichnet sich durch eine neu gestaltete Architektur für die hocheffiziente Datenaufnahme, eine schnelle Suche und eine Analyse im großen Maßstab aus. Die Security-Lösung basiert auf einer offenen Grundlage und ist die neueste Ergänzung

der QRadar Suite, dem integrierten Portfolio von IBM Software zur Erkennung und Abwehr von Sicherheitsbedrohungen. QRadar wurde entwickelt, um die tägliche Arbeit von Sicherheitsanalysten zu ergänzen und aufzuwerten. KI hilft ihnen dabei, zeitaufwendige und sich wiederholende Aufgaben zu bewältigen und gibt ihnen gleichzeitig die Möglichkeit, hoch priorisierte Bedrohungen effektiver zu finden und darauf zu reagieren.

Das neue Cloud-native QRadar SIEM wird als SaaS im 4. Quartal 2023 verfügbar sein. Es ist geplant, entsprechende Software-Lösungen für die On-Premises- und Multi-Cloud-Implementierung im Jahr 2024 anzubieten.

Open at its Core: Basierend auf Red Hat OpenShift ist QRadar SIEM so konzipiert, dass es bereits auf grundlegender Ebene offen ist und damit eine tiefere Interoperabilität mit Tools und Clouds verschiedener Anbieter ermöglicht. Es nutzt Open-Source und offene Standards für Kernfunktionen wie Erkennungsregeln und Suchsprache. So können Unternehmen es über ihren umfassenderen Sicherheits- und Technologiestacks hinweg einsetzen.

Das Cloud-native SIEM

- Nutzt eine **gemeinsame Sprache für Erkennungsregeln (SIGMA)**. Damit ermöglicht es Kunden neue, von der Sicherheitscommunity bereitgestellte Erkennungsregeln („crowdsourced detections“) schnell und direkt zu importieren, während sich Bedrohungen entwickeln.
- Bietet einzigartige **Funktionen für föderierte Suche und Threat-Hunting**, die auf Open-Source-Technologien basieren und es Analysten ermöglichten, proaktiv nach Bedrohungen in Cloud- und lokal gespeicherten Datenquellen auf einheitliche Weise zu suchen, ohne Daten aus ihrer ursprünglichen Quelle zu verschieben.
- Basiert auf dem **QRadar-Ökosystem, einem der größten Partnernetzwerke** der Branche mit mehr als 700 vordefinierten Integrationen.

Verbundene Erkennung, Untersuchung & Reaktion: Als Teil der QRadar Suite bietet das neue Cloud-native SIEM Kunden Zugriff auf eine Vielzahl von integrierten Funktionen, die eine proaktivere Erkennung, Untersuchung und Reaktion über verschiedene Tools hinweg ermöglichen. Mit der QRadar Suite können Unternehmen über ASM-Funktionen (Attack Surface Management) einen Einblick in ihre gefährdeten Ressourcen gewinnen, toolübergreifend nach Bedrohungen suchen, sich mit EDR am Endpunkt schützen und eine Verbindung zu automatisierten Playbooks herstellen, um die Reaktion zu beschleunigen (SOAR). QRadar SIEM bietet Anwendern übergreifende Einblicke und automatisierte Aktionen über ihre wichtigsten Tools hinweg. Der Zugriff erfolgt direkt über die primäre Benutzeroberfläche, ohne dass zwischen den verschiedenen Tools gewechselt werden muss.

Auf Unternehmen abgestimmte KI und Automatisierung: QRadar SIEM wendet mehrere Ebenen von KI und Automatisierung an, um die Qualität von Alerts und die Effizienz von Sicherheitsanalysten zu verbessern. Diese ausgereiften KI-Funktionen wurden auf Millionen von Alerts aus dem weitreichenden IBM Kundennetz vortrainiert und nach der Implementierung weiter optimiert, um die einzigartige Umgebung jedes Kunden zu berücksichtigen. Beispiele:

- **Priorisierung von Alerts:** Verwendet KI, um auftretende Meldungen zu reduzieren und die Qualität von

Alerts zu verbessern. Automatische Depriorisierung von Alerts mit niedrigem Risikopotenzial, während Alerts mit hoher Priorität automatisch gruppiert, kontextualisiert und eskaliert werden. Dies erfolgt unter Berücksichtigung des Risikokontexts aus laufender Information zur Bedrohungslage und Antwortmustern der Analysten. Diese Funktionalität ermöglichte es IBM Consulting Cybersecurity Services 85 % des Alert-Managements für Kunden zu automatisieren[3] und die Triage von Sicherheitsbedrohungen im ersten Jahr der Nutzung um 55 % zu beschleunigen.[4]

- **Untersuchung von Sicherheitsbedrohungen:** KI-Funktionalität, die automatisch föderierte Suchen über verbundene Systeme hinweg ausführt, um eine visuelle Zeitachse für Angriffe, MITRE ATT&CK-Zuordnungen und empfohlene Aktionen zu generieren. Analysten erhalten so einen erheblichen Vorsprung bei den Untersuchungsaufgaben.
- **Adaptive Erkennung:** Die Analysen von QRadar SIEM werden kontinuierlich und automatisch mit neuen Erkennungsregeln und Bedrohungsdaten aktualisiert, um mit sich entwickelnden Bedrohungen Schritt zu halten.

Die KI-Sicherheitsfunktionen von IBM sind nativ in die Benutzeroberfläche der QRadar Suite integriert. Sie bieten Analysten kontextbezogene Einblicke und helfen ihnen, KI intuitiver in ihren regulären Workflows zu nutzen.

Generative KI zur Beschleunigung der SOC-Produktivität

IBM plant die Veröffentlichung generativer KI-Sicherheitsfunktionen für die QRadar Suite Anfang 2024 basierend auf watsonx, der KI- und Datenplattform des Unternehmens. IBM entwickelt generative KI, um Zeitaufwand und Ressourcen von Sicherheitsteams zu optimieren, indem sie bestimmte zeitintensive Aufgaben für die Analysten erledigt und es ihnen gleichzeitig erleichtert, anspruchsvollere und höherwertige Arbeiten durchzuführen. Beispiele sind:

- **Automatisierung der Berichterstellung:** Erstellung einfacher Zusammenfassungen von Sicherheitsfällen und -vorfällen, die mit einem einzigen Klick mit verschiedenen Stakeholdern geteilt werden können.
- **Beschleunigung des Threat-Huntings:** Automatische Generierung von Suchen zur Erkennung von Bedrohungen auf der Basis von Beschreibungen von Angriffsverhalten und -mustern in natürlicher Sprache. Das ermöglicht Unternehmen eine schnellere Reaktion auf neue Bedrohungskampagnen.
- **Interpretation maschinengenerierter Daten:** Unterstützung der Analysten beim schnelleren Verständnis von Sicherheitsprotokolldaten, indem einfache Erläuterungen zu Ereignissen bereitgestellt werden, die auf einem System aufgetreten sind – hierdurch werden technische Barrieren abgebaut und die Untersuchungen von Ereignissen beschleunigt.
- **Bedrohungsdaten kuratieren:** Relevante Bedrohungsdaten interpretieren und zusammenfassen, um sich auf Kampagnen zu konzentrieren, bei denen die Wahrscheinlichkeit höher ist, dass sie Kunden aufgrund ihres individuellen Risikoprofils betreffen.

IBM entwickelt außerdem vorausschauende Sicherheitsfunktionen für generative KI, die darauf trainiert werden, aktive Antworten zu erstellen, die im Laufe der Zeit optimiert werden. Beispielsweise hilft das Sicherheitsteams ähnliche Vorfälle zu finden, betroffene Systeme zu aktualisieren und anfälligen Code zu korrigieren.

Über diese Anwendungsfälle hinaus plant IBM generativer KI im gesamten Portfolio der Sicherheitssoftware und

-services einzubetten. Diese Funktionen werden die watsonx-Infrastruktur sowie watsonx-KI-Modelle nutzen. Diese wurden mit kuratierten, domänenspezifischen Datensätzen trainiert, um mehr Vertrauen, Transparenz und Genauigkeit zu bieten.

Weitere Informationen zu QRadar SIEM finden Sie unter folgender Adresse: https://www.ibm.com/products/qradar-cloud-native-siem

Weitere Informationen zum Thema KI für Sicherheit finden Sie unter: https://www.ibm.com/security/artificial-intelligence

Aussagen über die künftige Ausrichtung und Absicht von IBM können ohne Vorankündigung geändert oder zurückgezogen werden und stellen lediglich Ziele und Absichten dar.

Informationen zu IBM Security
IBM Security trägt dazu bei, die weltweit größten Unternehmen und Behörden mit einem integrierten Portfolio von Sicherheitsprodukten und -services zu schützen, das dynamische KI- und Automatisierungsfunktionen bietet. Das Portfolio, das von der weltweit bekannten IBM Security X-Force®-Forschung unterstützt wird, ermöglicht es Unternehmen, Bedrohungen vorherzusagen, Daten während der Übertragung zu schützen und schnell und präzise zu reagieren, ohne geschäftliche Innovation zu behindern. IBM wird von Tausenden von Unternehmen als Partner für die Bewertung, Strategie, Implementierung und Verwaltung von Sicherheitstransformationen vertraut. IBM betreibt eine der weltweit größten Organisationen für Sicherheitsforschung, -entwicklung und -bereitstellung, überwacht mehr als 150 Milliarden Sicherheitsereignisse pro Tag in mehr als 130 Ländern und hat weltweit mehr als 10.000 Sicherheitspatente erhalten.

Kontakt für Journalisten:

Barbara Jax

IBM Unternehmensommunikation

barbara.jax@at.ibm.com

---

[1] *Global Security Operations Center Study, 2022 von Morning Consult, gesponsert von IBM.*

[2] *QRadar wurde in mehreren Analystenberichten von Drittanbietern für die letzten 13 Jahre als Marktführer für SIEM identifiziert, darunter Berichte von Gartner, Forrester, KuppingerCole, IDC und Omdia.*

[3] *Basiert auf der internen Analyse von IBM zu aggregierten Leistungsdaten, die bei Projekten mit über 340 Kunden im Juli 2023 beobachtet wurden. Bis zu 85 % der Alerts wurden mithilfe von KI-Funktionen automatisiert, die Teil von QRadar SIEM sind. Die tatsächlichen Ergebnisse hängen von den Konfigurationen und Bedingungen des Kunden ab, weshalb keine allgemein erwarteten Ergebnisse angegeben werden können.*

[4] *Basierend auf der internen Analyse von IBM zu zusammengefassten Leistungsdaten, die bei Projekten mit mehr als 400 Kunden im Zeitraum 2018-2019 beobachtet wurden. Dies ergab, dass der durchschnittliche Triage-Zeitplan von Alerts im ersten Jahr mithilfe von KI- und Automatisierungsfunktionen, die Teil von QRadar SIEM sind, um 55 % reduziert wurde. Die tatsächlichen Ergebnisse variieren abhängig von den Clientkonfigurationen und -bedingungen. Daher können keine allgemein erwarteten Ergebnisse bereitgestellt werden.*
