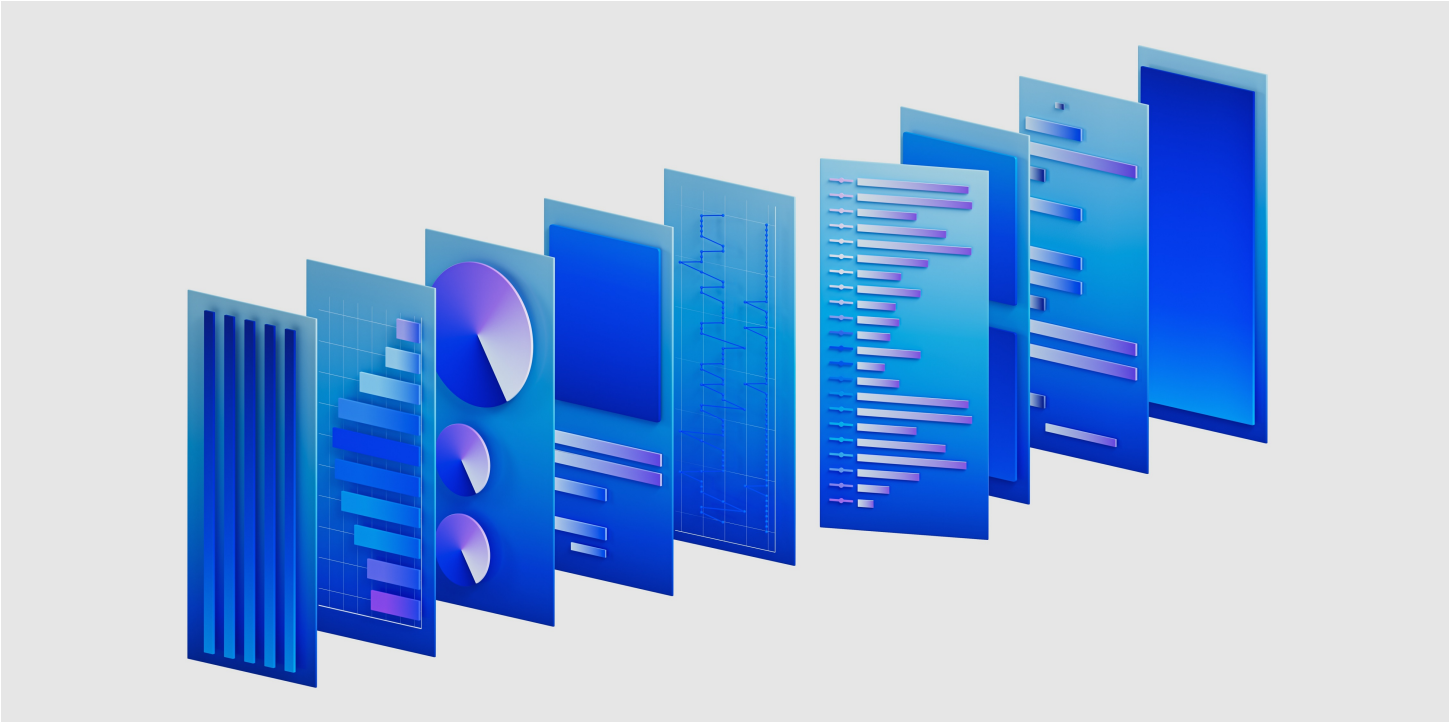
IBM DACH Newsroom

IBM stellt neue QRadar Security Suite vor, um Bedrohungen schneller zu erkennen und die Reaktion zu beschleunigen

Modernisierte, einheitliche Schnittstelle optimiert die Reaktion von Analysten während des gesamten Angriffslebenszyklus

Fortgeschrittene KI- und Automatisierungsfunktionen beschleunigen die Triage von Alerts durchschnittlich um 55 Prozent (1)



ARMONK, New York – 24. April 2023 – IBM (NYSE: IBM) hat heute seine neue Sicherheitssuite vorgestellt, die die Arbeit von Sicherheitsanalysten über den gesamten Incident-Lebenszyklus hinweg vereinheitlichen und beschleunigen soll. Die IBM Security QRadar Suite stellt eine bedeutende Weiterentwicklung und Erweiterung der Marke QRadar dar, die alle zentralen Technologien zur Erkennung, Untersuchung und Reaktion auf Sicherheitsbedrohungen umfasst. Über das gesamte Portfolio sind erhebliche Investitionen in Innovationen geflossen.

Die als Service angebotene IBM Security QRadar Suite basiert auf offenen Standardsund wurde speziell für die Anforderungen der Hybrid Cloud entwickelt. Sie bietet eine einheitliche, modernisierte Benutzeroberfläche über alle Produkte hinweg und Integrationen mit innovativer KI und Automatisierung. So können Analysten schneller, effizienter und präziser mit ihren Toolsets arbeiten.

Der digitale Fußabdruck, auch über Hybrid-Cloud-Umgebungen hinweg, wächst immer schneller und erhöht damit die Komplexität und Herausforderung für die heutigen Teams in Security Operation Centern (SOC), um mit den zunehmenden Angriffsgeschwindigkeiten Schritt zu halten. Diese Teams können durch arbeitsintensive Untersuchungen von Vorfällen und den jeweiligen Reaktionsprozessen ausgebremst werden, indem sie Erkenntnisse manuell zusammenfügen und zwischen nicht integrierten Daten, Tools und Schnittstellen wechseln. Laut einer aktuellen Umfrage sagen SOC-Experten, dass sie rund ein Drittel ihres Tages damit verbringen, Vorfälle zu untersuchen und zu validieren, die sich als keine tatsächlichen Bedrohungen erweisen.[2]

IBM hat basierend auf der bestehenden Leadership in 12 Kategorien für Sicherheitstechnologien[3] sein marktführendes Portfolio für die Erkennung und Reaktion auf Sicherheitsbedrohungen neu konzipiert, um Geschwindigkeit und Effizienz zu maximieren und den speziellen Anforderungen der Sicherheitsanalysten von heute gerecht zu werden. Die neue IBM Security QRadar Suite umfasst EDR/XDR, SIEM, SOAR und eine neue cloudnative Log Management Funktion, die auf einer gemeinsamen Benutzerschnittstelle, gemeinsamen Erkenntnissen sowie verbundenen Workflows basiert und die folgenden zentralen Gestaltungselemente umfasst:

- **Umfassende Analystenerfahrung:** Die Suite wurde in Zusammenarbeit mit Hunderten von Benutzern aus der Praxis optimiert und bietet eine einheitliche, modernisierte Benutzerschnittstelle für alle Produkte: Sie wurde entwickelt, um die Geschwindigkeit der Analysen und Effizienz über die gesamte Angriffskette hinweg drastisch zu steigern. Sie ist mit auf Unternehmen abgestimmten KI- und Automatisierungsfunktionen ausgestattet, die die Triage und Untersuchung von Alerts im ersten Jahr nachweislich um durchschnittlich 55 % beschleunigen.[1]
- **Bereitstellung in der Cloud, Geschwindigkeit & Skalierung:** Bereitgestellt als Service auf Amazon Web Services (AWS) ermöglicht die QRadar Suite eine vereinfachte Bereitstellung, Transparenz und Integration in Cloudumgebungen und Datenquellen. Die Suite enthält außerdem eine neue, cloudnative Log Management Funktion, die für eine hocheffiziente Datenverarbeitung, schnelle Suche und Analysen in hohem Maßstab optimiert ist.
- **Offene Standards, vorgefertigte Integrationen:** Die Suite vereint die Kerntechnologien, die für die Erkennung, Untersuchung und Reaktion auf Sicherheitsbedrohungen erforderlich sind – basierend auf offenen Schnittstellen, einem umfassenden Partnernetzwerk und mehr als 900 vorgefertigten Integrationen, die eine starke Interoperabilität zwischen IBM und Toolsets anderer Anbieter bieten.

„Angesichts der zunehmenden Angriffsoberfläche und der immer kürzeren Angriffszeiten sind Geschwindigkeit und Effizienz von grundlegender Bedeutung für den Erfolg ressourcenbeschränkter Sicherheitsteams“, sagte Mary O'Brien, General Manager bei IBM Security. „IBM hat die neue QRadar Suite um eine einheitliche, modernisierte Benutzeroberfläche herum entwickelt, die mit ausgefeilter KI und Automatisierung ausgestattet ist, um die Produktivität von Sicherheitsanalysten zu maximieren und ihre Reaktion in jedem Schritt der Angriffskette zu beschleunigen.“

Gemeinsame Weiterentwicklung von praxisnahen Anforderungen im Sicherheitsbereich

Die QRadar Suite ist der Höhepunkt jahrelanger IBM Investitionen, Akquisitionen und Innovationen in der Erkennung und Reaktion auf Sicherheitsbedrohungen. Die Lösung bietet dutzende ausgereifter KI- und Automatisierungsfunktionen, die im Laufe der Zeit durch reale Benutzer und Daten optimiert wurden, darunter IBM Managed Security Service-Projekte mit mehr als 400 Kunden. Dazu gehören auch Innovationen, die in Zusammenarbeit mit IBM Research und der Open-Source-Sicherheitscommunity entwickelt wurden.

Diese KI-basierten Funktionen haben gezeigt, dass sie die Geschwindigkeit und Genauigkeit von SOC Vorgängen deutlich verbessern: So konnten IBM Managed Security Services beispielsweise mehr als 70 % der Untersuchungen von Alerts[4] automatisieren und die Zeit für Alert-Triage durchschnittlich um 55 %[1] im ersten Jahr der Implementierung reduzieren.

Die QRadar Suite vereint diese Funktionen in einer einheitlichen Analystenumgebung. Sie stellt Alerts automatisch in einen Kontext und priorisiert sie, zeigt Daten im visuellen Format für eine schnelle Nutzung an und bietet gemeinsame Einblicke und automatisierte Workflows zwischen Produkten. Dieser Ansatz kann die Anzahl der Schritte, die erforderlich sind, um Bedrohungen zu untersuchen und darauf zu reagieren, drastisch reduzieren. Beispiele dafür:

- **KI-gestützte Alert-Triage:** Automatische Priorisierung oder Schließung von Alerts auf der Grundlage von KI-gestützter Risikoanalyse mithilfe von KI-Modellen, die auf Basis von früheren Reaktionsmustern von Analysten trainiert wurden, zusammen mit externen Bedrohungsdaten von IBM X-Force und umfassenderen, kontextbezogenen Erkenntnissen aus verschiedenen Erkennungstools.
- **Automatisierte Untersuchung von Sicherheitsbedrohungen:** Identifiziert Vorfälle mit hoher Priorität, die einer genaueren Untersuchung bedürfen und leitet automatisch eine Untersuchung ein, indem es die zugehörigen Informationen abruft und mittels Data-Mining in verschiedenen Umgebungen weitere Indikationen sammelt. Das System verwendet diese Ergebnisse, um zeitliche Abhängigkeiten und eine graphische Visualisierung des Vorfalls auf der Basis des MITRE ATT&CK-Frameworks zu generieren und empfiehlt Maßnahmen zur Beschleunigung der Reaktion.
- **Beschleunigtes Threat Hunting:** Verwendet die Open-Source-Grundlagen für Threat Hunting und die föderierte Suche, um Analysten dabei zu unterstützen, verdeckte Angriffe und Indicators of Compromise in ihren Umgebungen zu erkennen, ohne Daten aus den ursprünglichen Quellen zu verändern.

Indem QRadar Technologien den Analysten helfen, schneller und effizienter zu reagieren, können sie auch die Produktivität der Sicherheitsteams verbessern und den Analysten Zeit für höherwertige Aufgaben verschaffen.

Offene, vernetzte und modernisierte Security Suite

Die QRadar Suite nutzt offene Technologien und Standards im gesamten Portfolio sowie hunderte von vorgefertigten Integrationen mit IBM Security-Partnern. Diese Vorgehensweise ermöglicht tiefere gemeinsame Erkenntnisse und automatisierte Aktionen über Cloud Umgebungen von Drittanbietern, -Produkte und Data-Lakes hinweg, was die Bereitstellungs- und Integrationszeiten von Monaten auf Tage oder Wochen reduzieren kann.

Die IBM QRadar Suite enthält die folgenden Produkte, die zunächst als SaaS bereitgestellt und mit der neuen, einheitlichen Analystenfunktion aktualisiert wurden:

- **QRadar Log Insights:** Eine neue, cloudnative Lösung für das Log Management und Sicherheitsüberwachung, die eine vereinfachte Datenverarbeitung, sekundenschnelle Suche und rasche Analysen ermöglicht. Diese Lösung nutzt einen Elastic Security-Data Lake, der für die Erfassung, Speicherung und Durchführung von Analysen für Terabyte an Daten mit höherer Geschwindigkeit und Effizienz optimiert und für eine kosteneffiziente Verwaltung von Sicherheitsprotokollen sowie für die föderierte Suche und Untersuchung konzipiert ist.
- **QRadar EDR und XDR**: Unterstützt Unternehmen dabei, ihre Endpunkte vor bisher unbekannten Zero-Day-Bedrohungen zu schützen – mithilfe von Automatisierung und Hunderten von Modellen für maschinelles Lernen und Verhaltensmodellen, um Verhaltensanomalien zu erkennen und nahezu in Echtzeit auf Angriffe zu reagieren. Es nutzt einen einzigartigen Ansatz, der Betriebssysteme von außen überwacht und hilft, Manipulationen oder Störungen durch Angreifer zu vermeiden. Für Unternehmen, die ihre Erkennungs- und Reaktionsfunktionen über den Endpunkt hinaus erweitern möchten, bietet IBM auch XDR mit Alertkorrelation, automatisierter Untersuchung und empfohlenen Reaktionen über Netz, Cloud, E-Mail und mehr, sowie Managed Detection and Response (MDR) an.
- **QRadar SOAR:** Der jüngste Gewinner des Red Dot Design Award für Benutzeroberfläche und Benutzererfahrung hilft Unternehmen bei der Automatisierung und Orchestrierung von Workflows zur Reaktion auf Vorfälle und stellt sicher, dass ihre spezifischen Prozesse konsistent, optimiert und messbar verfolgt werden. Es umfasst 300 vorgefertigte Integrationen und bietet sofort einsatzfähige Playbooks für die Reaktion auf mehr als 180 globale Datenschutzbestimmungen.
- **QRadar SIEM:** IBMs marktführendes QRadar SIEM wurde um die neue, einheitliche Analystenschnittstelle erweitert, die gemeinsame Einblicke und Arbeitsabläufe mit umfassenderen Toolsets für den Sicherheitsbetrieb bereitstellt. Die Lösung bietet Echtzeiterkennung, die KI-, Netz- und Benutzerverhaltensanalyse sowie reale Bedrohungsdaten nutzt, um Analysten

genauere, kontextbezogene und priorisierte Alerts bereitzustellen. IBM plant außerdem, QRadar SIEM bis Ende des zweiten Quartals 2023 als Service auf AWS zur Verfügung zu stellen.

Die IBM Security QRadar Suite ist heute verfügbar über individuelle SaaS-Angebote. Weitere Informationen finden Sie unter: https://www.ibm.com/qradar

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 schützt die weltweit größten Unternehmen und Behörden mit einem integrierten Portfolio von Sicherheitsprodukten und -services, 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. Tausende von Unternehmen vertrauen IBM als Partner bei der Bewertung, Strategie, Implementierung und Verwaltung von Sicherheitstransformationen. 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 Unternehmenskommunikation

barbara.jax@at.ibm.com

---

[1] Basierend auf der internen Analyse von IBM von zusammengefassten Leistungsdaten, die bei Projekten des Managed Security Service mit mehr als 400 Kunden von 2018 – 2019 beobachtet wurden. Dies ergab, dass die durchschnittliche Zeitachse der Alerttriage im ersten Jahr um 55 % reduziert wurde, mithilfe von KI und Automatisierungsfunktionen, die jetzt Teil von QRadar sind. Die tatsächlichen Ergebnisse hängen von den Kundenkonfigurationen und -bedingungen ab, so dass keine allgemein erwarteten Ergebnisse angegeben werden können.

[2] Weltweite Ergebnisse einer Security Operations Center Studie, durchgeführt von Morning Consult und in Auftrag gegeben von IBM, März 2023. Basierend auf den Antworten von 1.000 befragten Security Operation Center-Experten aus einer Stichprobe von 1.000 SOC-Teammitgliedern aus 10 Ländern.

[3] Basierend auf Bewertungen von Sicherheitsprodukten durch externe Analystenfirmen wie Gartner, IDC, Forrester, KuppingerCole und Omdia, die IBM in 12 Kategorien für Sicherheitsprodukte als Leader einstufen: SIEM, SOAR, Fraud Reduction Intelligence Platform, Risk Based Authentication, Identity Governance und Administration, Access Management, Identity und Access Management as a Service, Access Governance & Intelligence und Identity Governance, Authentication, Customer Identity und Access Management, Data Security, Unified Endpoint Management.

[4] Bericht des IBM Institute for Business Value, "AI and automation for cybersecurity", 2022. Die Ergebnisse basieren auf einer IBM-Analyse der aggregierten jährlichen Leistungsdaten von Hunderten von Kunden weltweit, die KI- und Automatisierungsfunktionen nutzen, die jetzt Teil der QRadar Suite sind. Die tatsächlichen Ergebnisse können je nach Kundenkonfiguration und -bedingungen variieren, daher können keine allgemein erwarteten Ergebnisse angegeben werden.

Additional assets available online: Photos

https://de.newsroom.ibm.com/2023-04-24-IBM-stellt-neue-QRadar-Security-Suite-vor,-um-Bedrohungen-schneller-zu-erkennen-und-die-Reaktion-zu-beschleunigen