IBM Security QRadar SIEM

Steigert den Schutz vor Bedrohungen und die Einhaltung der Compliance mit einer integrierten und anpassbaren Berichterstattung

Highlights

- Verknüpfung von Log Management und Technologien zur Abwehr von Netzwerkbedrohungen in einer zentralen Datenbank und einer gemeinsamen Dashboard-Benutzeroberfläche
- Reduktion von Tausenden von Sicherheitsereignissen zu einer überschaubaren Liste möglicher Angriffe
- Erkennung und Verfolgung schädigender Aktivitäten über längere Zeiträume, um hochentwickelte Bedrohungen aufzudekken, die von anderen Sicherheitslösungen häufig übersehen werden
- Erkennen von Insiderbetrug dank innovativer Funktionalität
- Unterstützung der Einhaltung von Auflagen und von Compliance-Anforderungen

Moderne Netzwerk sind größer und komplexer als je zuvor und der Schutz dieser Netzwerke vor schädigenden Aktivitäten ist eine nicht enden wollende Aufgabe. Unternehmen, die ihr geistiges Eigentum und die Identität ihrer Kunden schützen und Unterbrechungen ihrer geschäftlichen Abläufe vermeiden wollen, müssen mehr tun, als Protokolle und Netzwerkübertragungsdaten zu überwachen. Sie müssen modernste Tools einsetzen, um diese Aktivitäten in einer aussagekräftigen Form offenzulegen. IBM® Security QRadar Security Information and Event Management (SIEM) kann als „Ankerlösung“ in der Sicherheitszentrale eines Unternehmens dienen durch Security-Intelligence. Sie sammelt, normalisiert und korrelliert verfügbare Netzwerkdaten basierend auf langjährigen kontextbezogenen Erkenntnissen. Das Ergebnis heißt *Security-Intelligence*.

Den Kern dieses Produkts bildet ein hoch skalierbare Datenbank, die Echtzeit-Protokollereignisdaten und Netzwerkübertragungsdaten erfasst, um die Spuren potenzieller Angreifer offenzulegen. QRadar SIEM ist eine Unternehmenslösung, die Protokollquellen-Ereignisdaten von Tausenden im Netzwerk verteilten Einheiten zusammenführt. Jede Aktivität wird in ihrer ursprünglichen Form dokumentiert und dann mit anderen Ereignissen verknüpft, um Zusammenhänge zu ermitteln und auf diese Weise echte Bedrohungen von falsch positiven Ergebnissen zu trennen. Darüber hinaus werden mittels Deep Packet Inspection-Technologie Layer 4-Netzwerkübertragungsdaten in Echtzeit und – was die Lösung besonders auszeichnet – Layer 7-Anwendungsnutzdaten erfasst.

Über eine intuitive Benutzeroberfläche, die allen Komponenten der QRadar-Produktfamilie gemeinsam ist, kann die IT Netzwerkangriffe schnell identifizieren und nach Priorität beseitigen, indem Hunderte Benachrichtigungen und Muster ungewöhnlicher Aktivitäten zu einer deutlich reduzierten Anzahl von *Angriffen* verdichtet werden, bei denen weitere Untersuchungen gerechtfertigt sind.

Transparenz in Echtzeit für die Abwehr und Priorisierung von Bedrohungen

QRadar SIEM ermöglicht die kontextbezogene und verlässliche Überwachung der gesamten IT-Infrastruktur und unterstützt Unternehmen auf diese Weise dabei, Bedrohungen zu erkennen und zu beseitigen, die von anderen Sicherheitslösungen häufig übersehen werden. Bei diesen Bedrohungen kann es sich um die nicht sachgerechte Nutzung von Anwendungen, Insiderbetrug oder auch hochentwickelte, schwer auffindbare und über einen langen Zeitraum bestehenden Bedrohungen handeln, die angesichts der Vielzahl an Ereignissen sehr schnell übersehen werden.

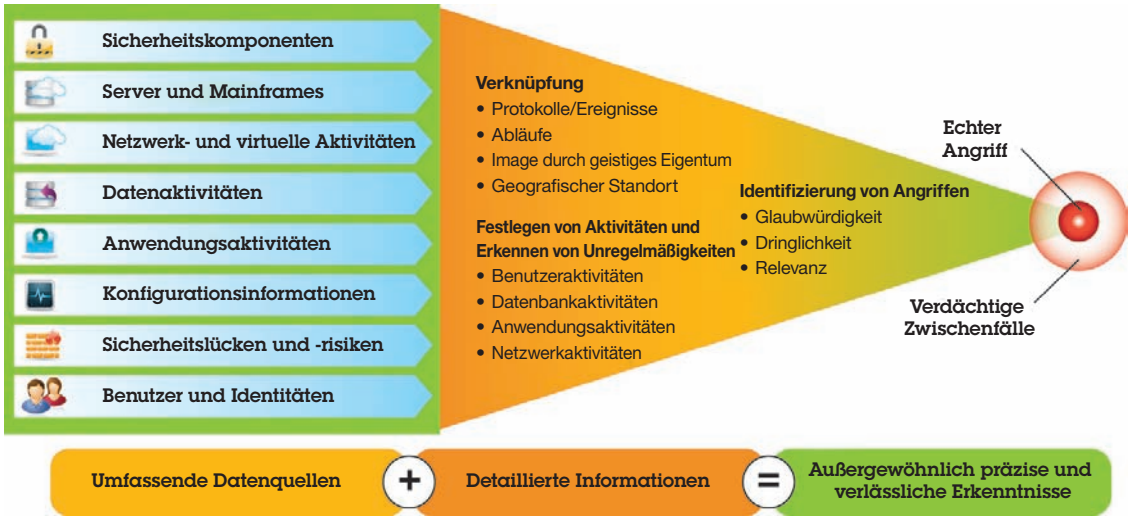
Zu den von QRadar SIEM erfassten Informationen zählen:

- **Sicherheitsereignisse:** Ereignisse von Firewalls, virtuellen privaten Netzwerken (VPNs), Systemen zur Erkennung von unbefugten Zugriffen und anderen
- **Netzwerkereignisse:** Ereignisse von Switches, Routern, Servern, Hosts und mehr
- **Netzwerkaktivitätskontext:** Layer 7 Application-Kontext von Netzwerk- und Anwendungsdatenverkehr
- **Benutzer- oder Assetkontext:** Kontextbezogene Daten von Identitäts- und Zugriffsmanagementprodukten und Software zur Schwachstellensuche
- **Betriebssysteminformationen:** Herstellernamen- und Versionsnummerdetails für Netzwerkassets
- **Anwendungsprotokolle:** Enterprise-Resource-Planning (ERP), Workflow, Anwendungsdatenbanken, Managementplattformen und mehr

Reduktion und Gewichtung von Benachrichtigungen zur gezielten Weiterverfolgung von Angriffen

In vielen Unternehmen werden täglich Millionen – oder sogar Milliarden – von Ereignissen generiert und die Reduktion dieser Daten zu einer übersichtlichen Liste der schwerwiegendsten Angriffe kann eine enorme Aufgabe sein. QRadar SIEM erkennt automatisch die meisten Netzwerkprotokollquellen und untersucht Netzwerkübertragungsdaten, um gültige Hosts und Server (Assets) im Netzwerk zu finden und zu klassifizieren, indem die verwendeten Anwendungen, Protokolle, Services und Ports verfolgt werden. Diese Daten werden erfasst, gespeichert, analysiert und in Echtzeit zueinander in Beziehung gesetzt, um mögliche Zusammenhänge zu erkennen und die Ergebnisse im Rahmen der Bedrohungserkennung und der Compliance-Berichterstellung und -Prüfung zu verwenden. Milliarden von Ereignissen und Datenflüssen lassen sich auf diese Weise zu einer Handvoll von weiterzuverfolgenden Angriffen reduzieren und gemäß ihrer Auswirkungen auf das Unternehmen gewichten.

Sicherheitsspezialisten können daher in der Regel bereits schon nach Tagen und nicht erst nach Wochen von einer QRadar SIEM-Installation profitieren. Zudem lassen sich Implementierungen auch ohne eine kleine Armee teurer Berater durchführen. Dank der Funktionen für die automatische Erkennung sowie der standardmäßig enthaltenen Vorlagen und Filter müssen Sie das System nicht über Monate auf ihre Umgebung „trainieren“, wie es bei Universaltools für den IT-Betrieb notwendig ist. Die Architektur nutzt verschiedene Modelle von Event-Processor-Appliances, Event-Collector-Appliances, Flow-Processor-Appliances und eine zentrale Konsole, die alle in Form hardwarbasierter, ausschließlich softwarebasierter oder virtueller Software-Appliances verfügbar sind. Kleinere Installationen können mit einer einzigen Komplettlösung beginnen, die problemlos zu einer Konsolenbereitstellung aktualisiert werden kann, indem nach Bedarf Event- und Flow-Processor-Appliances hinzugefügt werden.



QRadar SIEM erfasst Daten aus einer breiten Palette unterschiedlicher Quellen und reduziert sie anhand vordefinierter und benutzerdefinierter Regeln auf eine überschaubare Liste von Angriffen.

Schlüsselfragen für eine effektivere Bedrohungsabwehr

Durch die Beantwortung einiger Schlüsselfragen können Sicherheitsteams ihre Bedrohungen deutlicher und im gesamten Umfang erkennen. Wer ist der Angreifer? Was ist das Ziel des Angriffs? Welche geschäftlichen Auswirkungen hat der Angriff? Wo muss ich nachforschen? QRadar SIEM verfolgt signifikante Vorfälle und Bedrohungen, indem ein Protokoll aus unterstützenden Daten und relevanten Informationen zusammengestellt wird. Details wie Ziele eines Angriffs, Zeitpunkt, Assetwert, Status der Schwachstelle, Identitäten der verantwortlichen Benutzer, Angreiferprofile, aktive Bedrohungen und Aufzeichnungen früherer Angriffe versorgen das Sicherheitsteam mit dem nötigen Know-how, um auf Vorfälle und Risiken reagieren zu können.

Durch echtzeit-, standort- oder verlaufsbasierte Suchen in Ereignis- und Datenflussdaten zu Analyse- und Untersuchungszwecken lassen sich Aktivitäten leichter bewerten und Vorfälle schneller beheben. Dank benutzerfreundlicher Dashboards, Zeitreihenansichten, Drilldown-Suchen, Inhaltstransparenz bis auf Paketebene und einer großen Anzahl vordefinierter Suchen ist es Benutzern problemlos möglich, Daten zu aggregieren, um Unregelmäßigkeiten und die wichtigsten Faktoren im Hinblick auf bestimmte Aktivitäten zusammenzufassen und zu identifizieren. Darüber hinaus können übergreifende Suchen in großen, geografisch verteilten Umgebungen durchgeführt werden.

Anwendungstransparenz und Erkennung von Anomalien

QRadar SIEM unterstützt eine Vielzahl an Funktionen zur Anomalieerkennung, um Verhaltensänderungen zu identifizieren, die sich auf Anwendungen, Hosts, Server und Bereiche im Netzwerk auswirken. So kann QRadar SIEM beispielsweise die außerplanmäßige oder exzessive Nutzung einer Anwendung oder eines cloudbasierten Service oder auch Netzwerkaktivitätsmuster erkennen, die nicht mit Langzeitprofilen, die auf dem gleitenden Durchschnitt basieren, und saisonabhängigen Nutzungsmustern übereinstimmen. QRadar SIEM lernt, diese täglichen und wöchentlichen Nutzungsprofile zu erkennen, und unterstützt die IT-Mitarbeiter auf diese Weise bei der schnellen Erkennung signifikanter Abweichungen.

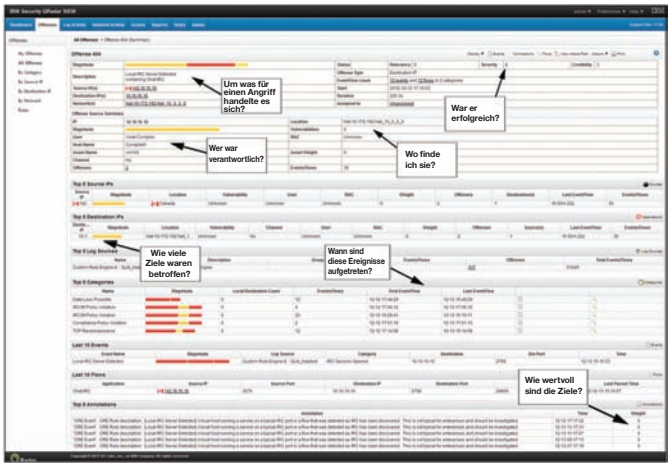
In der zentralen Datenbank von QRadar SIEM werden sowohl Protokollquellenereignisse als auch Netzwerkübertragungen gespeichert, sodass separate Ereignisse mit bidirektionalen Netzwerkübertragungsaktivitäten verknüpft werden können, die von der gleichen IP-Quelle ausgehen. Darüber hinaus können Netzwerkübertragungen gruppiert und Aktionen, die innerhalb eines engen Zeitfensters auftreten, in Form eines einzigen Datenbankeintrags aufgezeichnet werden, um die Speicherbelegung zu reduzieren und sparsam mit erforderlichen Lizenzen umzugehen.

Dank der Fähigkeit, Layer 7-Anwendungsdatenverkehr zu erkennen, kann QRadar SIEM präzise Analysen und Erkenntnisse zu einem Unternehmensnetzwerk bereitstellen, die im Rahmen der Überwachung von Richtlinien, Bedrohungen und der allgemeinen Netzwerkaktivität Verwendung finden. Mit den neuen IBM Security QRadar QFlow- und VFlow-Collector-Appliances kann QRadar SIEM die Nutzung von Anwendungen wie ERP, Datenbanken, Skype, Voice over IP (VoIP) und soziale Medien in einem Netzwerk überwachen. Dies umfasst Informationen darüber, wer welche Anwendungen nutzt, Analysen und Benachrichtigungen zu Inhaltsübertragungen sowie die Verknüpfung mit anderen Netzwerk- und Protokollaktivitäten, um unangemessene Datenübertragungen und Muster, die eine übermäßige Nutzung aufzeigen, aufzudecken. Zusätzlich zu den zahlreichen im Lieferumfang QRadar SIEM enthaltenen Regeln für die Erkennung von Unregelmäßigkeiten und Verhaltensmustern können Sicherheitsteams auch eigene Regeln erstellen, indem sie Filterfunktionen nutzen, mit deren Hilfe die Anomalieerkennung auf Zeitreihendaten angewendet werden kann.

Steuerung über eine zentrale intuitive Sicherheitslösung

QRadar SIEM bietet ein solides Fundament für die Sicherheitszentrale eines Unternehmens, indem es eine zentrale Benutzerschnittstelle bereitstellt, die den rollenbasierten Zugriff nach Aufgabenbereich und eine globale Ansicht unterstützt, um den Zugriff auf Echtzeitanalysen, Vorfallmanagement und Berichtswesen zu ermöglichen. Über diese Benutzerschnittstelle sind fünf Standarddashboards zu den Bereichen Sicherheit, Netzwerkaktivität, Anwendungsaktivität, Systemüberwachung und Compliance verfügbar. Darüber hinaus können Benutzer eigene Arbeitsbereiche erstellen und anpassen.

Mithilfe dieser Dashboards können Spitzen in der Benachrichtigungsaktivität, die auf den Beginn eines Angriffs hindeuten können, leicht identifiziert werden. Durch Klicken auf ein Diagramm wird eine Drilldownfunktion aktiviert, über die ein Sicherheitsteam die hervorgehobenen Ereignisse oder Netzwerkübertragungen, die mit einem möglichen Angriff verbunden sind, in kürzester Zeit weiter untersuchen kann. Darüber hinaus stehen zahlreiche Vorlagen für bestimmte Rollen, Einheiten, Compliance-Vorschriften und vertikale Branchen zur Verfügung, um die Berichterstellung zu beschleunigen.



QRadar SIEM bietet eine Fülle an aufschlussreichen Details zu jedem möglichen Angriff sowie die Möglichkeit, vorhandene Regeln zu optimieren oder neue Regeln hinzuzufügen, um die Anzahl der falsch positiven Ergebnisse zu reduzieren.

Ausweitung der Bedrohungsabwehr auf virtuelle Umgebungen

Da virtuelle Server mindestens genauso anfällig für Sicherheitslücken sind wie physische Server, muss eine umfassende Security-Intelligence-Lösung auch geeignete Mechanismen bereitstellen, die den Schutz von Anwendungen und Daten innerhalb eines virtuellen Rechenzentrums unterstützen. Mit den VFlow-Collector-Appliances von QRadar können sich IT-Spezialisten ein besseres Bild von den vielfältigen Geschäftsanwendungsaktivitäten innerhalb der virtuellen Netzwerke des Unternehmens machen und diese Anwendungen im Rahmen der Sicherheitsüberwachung, der Analyse der Verhaltens auf Anwendungsebene und der Anomalieerkennung leichter identifizieren Operatoren können zudem den Anwendungsinhalt erfassen, um genauere Sicherheits- und Richtlinienanalysen vorzunehmen.

Ausführliche Datenzugriffs- und Benutzeraktivitätsberichte für das Compliance-Management

QRadar SIEM bietet die Transparenz, Zurechenbarkeit und Messbarkeit, die nötig ist, wenn ein Unternehmen die Einhaltung von Bestimmungen und Auflagen sicherstellen und aussagekräftige Compliance-Berichte erstellen will. Da die Lösung Überwachungsquellen korrelieren und verknüpfen kann, stehen umfassendere Kennzahlen zur Beschreibung von IT-Risiken zur Verfügung. Darüber hinaus enthält sie eine große Anzahl an Berichten und Regelvorlagen, um branchenspezifischen Compliance-Anforderungen Rechnung zu tragen.

Dank der Erweiterbarkeit von QRadar SIEM, die es ermöglicht, neue Definitionen, Vorschriften und Best Practices über automatische Updates einzubinden, kann ein Unternehmen effizient auf compliance-bezogene Anforderungen bei der IT-Sicherheit reagieren. Zudem können Profile aller Netzwerkassets nach Geschäftsfunktion gruppiert werden, beispielsweise Server, deren Konformität mit dem Health Insurance Portability and Accountability Act (HIPAA) geprüft wird.

Die vordefinierten Dashboards, Berichte und Regelvorlagen der Lösung sind für die folgenden gesetzlichen Bestimmungen und Kontrollrahmen konzipiert: CobiT, SOX, GLBA, NERC/FERC, FISMA, PCI DSS, HIPAA, UK GSi/GCSx, GPG und weitere.

Zusätzliche Funktionen für High-Availability und Disaster-Recovery

Um High-Availability und Disaster-Recovery zu unterstützen, können alle Komponenten der QRadar-Appliancefamilie in Verbindung mit identischen Sekundärsystemen verwendet werden. Von Event-Processor-Appliances über Flow-Processor-Appliances bis hin zu Komplett- und Konsolen-SIEM-Appliances lassen sich Stabilität und Schutz nach Bedarf weiter ausbauen, um zur Aufrechterhaltung des fortlaufenden Betriebs beizutragen.

Unternehmen, für die das Thema Ausfallsicherheit von großer Bedeutung ist, bieten QRadar High-Availability-Lösungen integrierten, automatischen Failover und die vollständige Datenträgersynchronisation zwischen Systemen. Dank der architektonisch eleganten Plug-and-Play-Appliances ist die Implementierung dieser Lösung ganz einfach und zusätzliche Fremdanbieterprodukte für Fehlermanagement sind nicht erforderlich.

Unternehmen, für die die Themen Datensicherheit und -wiederherstellung von großer Bedeutung sind, bieten QRadar Disaster-Recovery-Lösungen Funktionalität, um Livedaten (beispielsweise Datenflüsse und Ereignisse) von einem primären QRadar-System an ein sekundäres Parallelsystem weiterzuleiten, das sich in einer separaten Einrichtung befindet.

Erstellung von Risikoprofilen

IBM Security QRadar Risk Manager stellt eine ideale Ergänzung zu QRadar SIEM dar, da mit dieser Lösung die anfälligsten Assets in einem Netzwerk identifiziert werden können. Es wird gleich eine Nachricht erzeugt, sobald eines dieser Systeme an Aktivitäten beteiligt ist, die es gefährden könnte. So ist es beispielsweise möglich, Unternehmensnetzwerke nach nicht gepatchten Anwendungen, Einheiten und Systemen zu durchsuchen, die Anwendungen, Einheiten und Systeme zu bestimmen, die eine Verbindung zum Internet herstellen, und Korrekturmaßnahmen auf der Basis des Risikoprofils der verschiedenen Anwendungen zu priorisieren. Weitere Informationen finden Sie im Datenblatt zu QRadar Risk Manager.

Umfassende Unterstützung von Einheiten, um Netzwerkereignisse und Datenflüsse erfassen zu können

Dank der Unterstützung von mehr als 450 in Unternehmensnetzwerken eingesetzten Produkten praktisch aller führenden Anbieter ermöglicht QRadar SIEM die Erfassung, Analyse und Verknüpfung der Daten von einer großen Palette an Systemen, u. a. Netzwerklösungen, Sicherheitslösungen, Server, Hosts, Betriebssysteme und Anwendungen. Darüber hinaus kann die Unterstützung von QRadar SIEM problemlos auf proprietäre Anwendungen und neue Systeme von IBM und vielen anderen Anbietern ausgeweitet werden.

Warum IBM?

IBM betreibt eine der weltweit größten Einrichtungen für die Erforschung, Entwicklung und Bereitstellung von Sicherheitstechnologien. IBM Lösungen versetzen Unternehmen in die Lage, Sicherheitslücken zu reduzieren und sich mehr auf den Erfolg strategischer Initiativen zu konzentrieren.

Weitere Informationen

Weitere Informationen dazu, wie IBM Security QRadar SIEM Ihnen helfen kann, die mit Bedrohungsabwehr und Compliance verbundenen Aufgaben zu bewältigen, erhalten Sie von Ihrem IBM Ansprechpartner oder IBM Business Partner oder auf folgender Website: **ibm.com**/security.

Informationen zu IBM Security-Lösungen

IBM Security bietet eines der innovativsten und am besten aufeinander abgestimmten Portfolios mit Sicherheitsprodukten und -services für Unternehmen. Das Portfolio, das durch die weithin bekannte Forschungs- und Entwicklungsgruppe IBM X-Force unterstützt wird, bietet die notwendige Security-Intelligence, um Unternehmen beim umfassenden Schutz von Personen, Infrastrukturen, Daten und Anwendungen zu unterstützen. Erreicht wird dies durch die Bereitstellung von Lösungen für Identitäts- und Zugriffsmanagement, Datenbanksicherheit, Anwendungsentwicklung, Risikomanagement, Endpunktmanagement, Netzwerksicherheit und vieles mehr. Diese Lösungen unterstützen Unternehmen beim erfolgreichen Risikomanagement und bei der Implementierung integrierter Sicherheit für mobile, Cloud-, Social Media- und andere Geschäftsarchitekturen. IBM betreibt eine der weltweit größten Einrichtungen für die Erforschung, Entwicklung und Bereitstellung von Sicherheitstechnologien, überwacht täglich ca. 13 Milliarden Sicherheitsereignisse in mehr als 130 Ländern und besitzt mehr als 3.000 Patente im Bereich Sicherheitstechnologie.

Mithilfe von IBM Global Financing (IGF) können Sie die Software, die Ihr Unternehmen benötigt, kosteneffizient erwerben. Wir bieten Kunden individuelle Finanzierungslösungen, die auf ihre geschäftlichen Zielsetzungen abgestimmt sind und ihnen helfen, ihren Cashflow zu verbessern und die Gesamtkosten zu senken. Finanzieren Sie wichtige IT-Anschaffungen mit IGF und verschaffen Sie Ihrem Unternehmen einen Vorsprung. Weitere Informationen finden Sie im Internet unter: **ibm.com**/financing/de

IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
ibm.com/de

IBM Österreich
Obere Donaustrasse 95
1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Die IBM Homepage finden Sie unter: **ibm.com**/de

WGD03021-DEDE-00