IBM Security QRadar Log Manager

Echtzeit-Log Management zum Schutz von IT-Infrastrukturen und zur Einhaltung gesetzlicher Bestimmungen

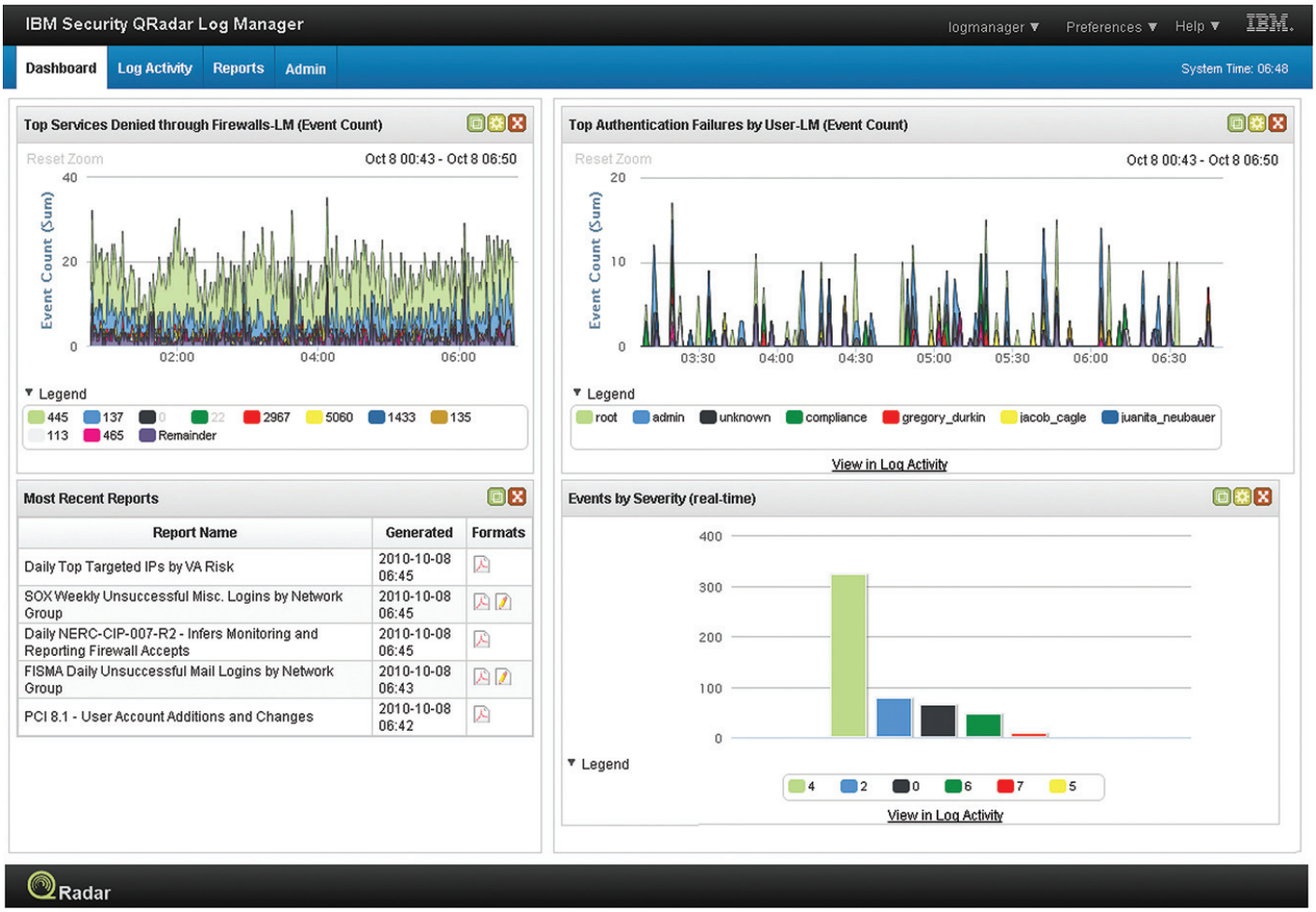
Highlights

- Generiert verlässliche IT-Analysen durch die Zusammenstellung und Verknüpfung unterschiedlicher Protokolle und Ereignisse
- Sammelt Ereignisdaten von Sicherheits- und Netzwerkeinheiten, Servern, Endpunkten und Anwendungen in einem zusammenhängenden Repository mit einer zentralen Ansicht
- Führt auf einfache Weise Untersuchungen und die Behebung von Anwendungs- und Netzwerkfehlern für normalisierte Daten durch, um Suchvorgänge zu vereinfachen
- Kann für die Verarbeitung von Hunderttausenden von Ereignissen pro Sekunde und pro System erweitert werden
- Bietet die Möglichkeit, gesetzliche Bestimmungen mithilfe umfangreicher Funktionen für Complianceberichte sogar zu übertreffen
- Schützt Investitionen durch die Möglichkeit der Einbindung der integrierten SIEM-Technologie (Security Information and Event Management)

Unternehmen, die eine Lösung brauchen, um zahlreiche Protokolle zu Netzwerk- und Sicherheitsereignissen zu sammeln, zu analysieren, zu archivieren und sicher zu speichern, benötigen ein leistungsfähiges, benutzerfreundliches und umfassendes Log Management-System. Dies ist insbesondere in der smarten Arbeitsumgebung von heute wichtig, in der instrumentierte, vernetzte und intelligente Unternehmen mehr Informationen als je zuvor generieren und speichern. IBM® Security QRadar Log Manager analysiert alle Daten von unterschiedlichen Netzwerk- und Sicherheitseinheiten, Servern, Betriebssystemen, Anwendungen und einer Vielzahl von Endpunkten. Sie erhalten dadurch nahezu in Echtzeit Erkenntnisse über aktuelle Sicherheitsbedrohungen und können dauerhafte Anforderungen bei der Complianceüberwachung einhalten.

Transparenz bei Protokolldaten für aussagekräftige IT-Analysen

Die meisten Unternehmen generieren große Mengen an Protokollen. Die manuelle Analyse dieser Protokolle kann sich allerdings als schwierig erweisen und einen unverhältnismäßig hohen Personalaufwand erfordern. Mit der flexibel verwendbaren Abfragefunktion von QRadar Log Manager werden unterschiedliche Protokolldaten zusammengeführt und in nachvollziehbaren IT-Prozessen und Sicherheitsuntersuchungen verknüpft. Sie können dadurch Muster bei Angriffen, bei Unregelmäßigkeiten, beim Zugriff und bei der Vewendung vertraulicher Daten sowie von internen Sicherheitsbedrohungen identifizieren.



Das anpassbare Dashboard in QRadar Log Manager ermöglicht den rollenbasierten Zugriff nach Funktion und die globale Anzeige von Protokollanalysen in Echtzeit, Ereignismanagement und Reporting.

Differenzierte Abfragen für effiziente Untersuchungen von Ereignissen

QRadar Log Manager ist dank einer intuitiv bedienbaren, zentralen Benutzerschnittstelle eine zuverlässige und unkomplizierte Grundlage für Sicherheits- und Netzwerkteams. Es stehen Standard-Dashboards nach Funktion zur Verfügung. Die Benutzer können eigene Arbeitsbereiche erstellen und anpassen, um bestimmte Aktivitäten zu überwachen oder Zeitreihenanzeigen zur Ermittlung langfristiger Datentrends aufzurufen. Damit können Unregelmäßigkeiten und mögliche Sicherheitsbedrohungen einfacher ermittelt werden, und die Netzwerkauslastung und -leistung können im Hinblick auf die Einhaltung von IT-Service-Level einfacher überprüft werden.

Umfassende Unterstützung aller Systeme und Geräte zur Erfassung aller Ereignisse im Netzwerk

QRadar Log Manager sammelt Daten von einer Vielzahl von Netzwerk- und Sicherheitseinheiten, z. B. Router, Switches, Firewalls, VPNs (Virtual Private Networks), IDS/IPS (Intrusion Detection/Prevention Systems), Antivirus-Anwendungen, Hosts, Server, Datenbanken, Mail- und Webanwendungen, kundenspezifische Einheiten und proprietäre Anwendungen.

Die Ereignisse werden über eine Device Support Module-Schnittstelle gesammelt, in der mithilfe einer erweiterten Normalisierungsstruktur mit zwei Ebenen ähnlichen Ereignissen, die aus unterschiedlichen Protokollquellen stammen, einheitliche Begriffe zugeordnet werden. Eine angepasste Rules Engine verarbeitet alle eingehenden Ereignisse in Echtzeit. Sie ordnet Attribute nach Dringlichkeit, Glaubwürdigkeit und Relevanz zu und leitet eine geeignete Reaktion ein – per E-Mail-Benachrichtigung, Dashboard-Eintrag oder durch Hinzufügen des Ereignisses zu einer Referenzgruppe ähnlicher Aktivitäten zur weiteren Überwachung.

Implementierung skalierbarer Systeme zur Ausweitung der Abdeckung

Die Konfigurationen für die QRadar Log Manager Appliance-Architektur reichen von einer universellen Hardware- oder Softwarelösung bis zu einer Unternehmensarchitektur – unter Verwendung einer zentralen Konsole und einer beliebigen Anzahl an verteilten Event Processor- und Event Collector-Systemen. QRadar Log Manager kann problemlos für die Verarbeitung von Hunderttausenden von Ereignissen pro Sekunde in einer einzigen, einheitlichen Datenbankstruktur erweitert werden.

Die Software hat bis zu 16 Terabyte fehlertoleranten Speicher pro System zur Archivierung von Ereignisprotokollen. Sie unterstützt umfangreiche Integritätsprüfungen von Protokolldateien, z. B. NIST Log Management Standard SHA-x (1-256) Hashing bei manipulationssicheren Protokollarchiven. Die verteilte Architektur ermöglicht Speichererweiterungen von Hunderten von Terabyte. Die integrierte spezielle Datenbank ist selbstverwaltend und zeichnet sich durch ein hohes Maß an Benutzerfreundlichkeit und niedrigere Gesamtbetriebskosten (TCO) aus.

Administratoren können Zeiträume für die Datenspeicherung auf der Grundlage differenzierter Richtlinien festlegen, um bestimmte interne Anforderungen oder Bestimmungen zu erfüllen. Eine anpassbare Funktion zur Ereignisindexierung sorgt für eine bessere Leistung, da sie die Verwendung beliebiger Datenbankfelder ermöglicht. Über Reportingfunktionen kann die Auslastung und Speicherplatzbelegung ermittelt werden. QRadar Log Manager komprimiert darüber hinaus ältere Daten und ermöglicht somit längere Zeiträume für die Datenspeicherung.

Weniger Aufwand für die Sicherheit – jetzt und in Zukunft

QRadar Log Manager beinhaltet über 2.000 direkt verwendbare Regeln und Berichte und bietet Unternehmen damit die Möglichkeit, Audit- und Reportinganforderungen zuverlässig einzuhalten. Hierzu gehören z. B. PCI (Payment Card Industry), HIPAA (Health Insurance Portability and Accountability Act) und GLBA (Gramm-Leach-Bliley Act). Automatisierte Mitteilungen an Sicherheitsteams tragen dazu bei, dass Benutzer Richtlinien in Echtzeit umsetzen können.

Mit QRadar Log Manager kann das Sicherheitsbewusstsein im Unternehmen gesteigert werden. Sie können damit außerdem verdächtige Ereignisse identifizieren, die bisher aufgrund der Vielzahl von Netzwerkaktivitäten unerkannt blieben. QRadar Log Manager ermöglicht als Teil der IBM QRadar Security Intelligence-Plattform die nahtlose Umstellung vom

Protokollmanagement auf die vollständige SIEM-Technologie über ein einfaches Lizenzupgrade. Dies vereinfacht zudem die Umstellung vom Management von Sicherheitsereignissen auf eine umfassende Security Intelligence-Lösung.

Sicherheit durch Optionen für hohe Verfügbarkeit und Disaster Recovery

Durch die Einführung von Hochverfügbarkeitslösungen von QRadar können Unternehmen von automatischen Ausfallsicherungen und der vollständigen Synchronisierung von Plattenlaufwerken zwischen Systemen profitieren. Diese Funktionalität ist üblicherweise nur bei kostspieligen, manuell implementierten Software- und Speicherlösungen verfügbar. Die Benutzer können hochverfügbaren Datenspeicher und Analysen über hochentwickelte Plug-and-Play-fähige Systeme auf einfache Weise einführen.

Die QRadar Disaster Recovery-Systeme bieten die Möglichkeit, alle gesammelten Daten aus Protokollquellen durch die Spiegelung auf ein sekundäres, identisches QRadar-Backupsystem zu schützen.

Warum IBM?

IBM betreibt eine der weltweit größten Organisationen für Forschung, Entwicklung und Bereitstellung von Sicherheitslösungen. Hierzu gehören 10 Security Operations Center, 9 IBM Research Center, 11 Software Security Development Labs und das Institute for Advanced Security mit Niederlassungen in den USA, in Europa und im asiatisch-pazifischen Raum. Mithilfe von IBM Lösungen können Unternehmen die Zahl der Sicherheitslücken verringern und sich verstärkt auf den Erfolg strategischer Initiativen konzentrieren. Die Produkte bauen auf dem Fachwissen des IBM X-Force Forschungs- und Entwicklungsteams für Informationen über Sicherheitsbedrohungen auf. Sie ermöglichen die Umsetzung eines präventiven Sicherheitskonzepts. IBM bietet als bewährter Partner im Sicherheitsbereich die nötigen Lösungen, um die gesamte Infrastruktur im Unternehmen, einschließlich der Cloud, vor aktuellen Sicherheitsrisiken zu schützen.

Weitere Informationen

Wenn Sie mehr über IBM Security QRadar Log Manager erfahren möchten, wenden Sie sich an den zuständigen IBM Vertriebsbeauftragten oder IBM Business Partner, oder besuchen Sie uns unter: **ibm.com**/security

IBM Deutschland
IBM-Allee 1
71139 Ehningen
Germany
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

WGD03020-DEDE-00