RSA NetWitness® Logs

Compliance und Reporting

- *Compliance-Berichte umfassen das Erstellen/Löschen/Ändern von Konten, den Administratorzugriff auf Compliance-Systeme, den Nutzerzugriff auf Compliance-Systeme, Eskalation von Berechtigungen, Firmware-Updates, Konfigurationsänderungen, den erfolgreichen Remote-Zugriff usw.*

- *Bestimmungen, die spezifische Berichte enthalten:*
  - *Basel II*
  - *Bill 198*
  - *Family Educational Rights and Privacy Act (FERPA)*
  - *Federal Financial Institutions Examination Council (FFIEC)*
  - *Federal Information Security Management Act (FISMA)*
  - *Gramm-Leach-Bliley Act (GLBA)*
  - *Good Practice Guide 13 (GPG13)*
  - *Health Insurance Portability and Accountability Act von 1996 (HIPAA)*
  - *Internationale Organisation für Normung 27002 (ISO 27002)*
  - *North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)*

- *National Industrial Security Program Operating Manual (NISPOM)*
  - *Payment Card Industry (PCI)*
  - *Sarbanes-Oxley Act von 2002 (SOX)*
  - *Statement on Standards for Attestation Engagements Nr. 16 (SSAE)*

RSA NetWitness® Logs ist ein Tool für Sicherheits-Monitoring und -forensik, das Protokolldaten aus verschiedenen Quellen erfasst, analysiert, meldet und speichert, um die Compliance von Sicherheitsrichtlinien und die Einhaltung gesetzlicher Bestimmungen zu unterstützen. Die Lösung ist modular und skalierbar und kann praktisch für jede Art von Unternehmen bereitgestellt werden. Im Gegensatz zu anderen protokollzentrierten SIEMs werden mit RSA NetWitness Logs die Protokolle zum Erfassungszeitpunkt analysiert, angereichert und indiziert. Dabei werden sitzungsbasierte Metadaten erstellt, mit denen sich Warnmeldungen und Analysen ganz erheblich beschleunigen lassen.

RSA NetWitness Logs unterstützt die Erfassung von zahlreichen Protokollen, wie z. B. Syslog, ODBC, SFTP, SCP, FTPS, SNMP, Check Point LEA und WinRM. Das Tool kann Protokolle aus über 350 Ereignisquellen verarbeiten, darunter verschiedene branchenführende Netzwerk- und Sicherheitsgeräte, gängige Anwendungen und Betriebssysteme. Zusätzlich werden Protokollrohdaten gespeichert und Metadaten extrahiert. Die Möglichkeit des zentralen Monitorings von Protokollen unabhängig von ihrer Quelle und die Bereitstellung der Erfassungskomponenten vor Ort, virtuell, in hybriden Architekturen oder gänzlich in Public Clouds wie Amazon Web Services (AWS) und Microsoft Azure sowie Anwendungen wie Microsoft Office 365 und Salesforce machen RSA NetWitness Logs zu einer vielseitigen Lösung. Die durchgängige Protokollsichtbarkeit erleichtert die Administration und Analyse von Daten in verteilten und virtuellen Umgebungen, was wiederum die Erkennung und Ermittlung sowie das Reporting und Management sämtlicher Protokolldaten beschleunigt.

Compliance

Die RSA NetWitness Logs-Lösung enthält Compliance-Anwendungsfälle und integrierte Vorlagen für SOX, PCI, HIPAA, NERC und viele weitere Bestimmungen.

Reporting

RSA NetWitness Logs bietet Ihnen die Flexibilität, Ansichten und Formatierungen für Berichte individuell anzupassen. Die vordefinierten Berichte enthalten eine oder mehrere Regeln, die Sie auch in anderen, selbst erstellten Berichten nutzen können.

Automatisierung der Protokollerkennung

Falls Sie nicht genügend Mitarbeiter haben oder mit dem Monitoring von ständig wechselnden, unterschiedlichen Umgebungen überlastet sind, kann Ihnen der Erkennungs-Workflow von RSA NetWitness Logs bei diesen Herausforderungen helfen. Im Gegensatz zu anderen Protokollerfassungen, die eine manuelle Konfiguration erfordern, verfügt RSA NetWitness Logs über eine automatisierte heuristische Analyse, damit Sicherheitsteams schnell neue Ressourcen aufnehmen können. Die neue Technologie der „dynamischen Analyse“ rendert automatisch die Rohdaten aus den meisten Protokollquellen und bietet sofortigen Zugriff auf wichtige Sicherheitsdaten in Form von nützlichen Metadaten. Die automatische Analyse neuer Protokollquellen hilft Unternehmen, mit der ständig wachsenden Anzahl an Protokollquellen Schritt zu halten.

Protokollquellen, die nicht über einen entsprechenden Parser verfügen, werden automatisch anhand von Regeln verarbeitet. Metadaten werden automatisch auf der Grundlage von Regeln extrahiert; diese Metadaten sind dann für Ergänzungen, Ermittlungen, Reporting und Warnmeldungen aus neuen Quellen verfügbar. Die Automatisierung der Protokollanalyse sorgt für sofortige Sichtbarkeit in Protokolle aus neuen, benutzerdefinierten oder nicht unterstützten Quellen.

Bei anspruchsvolleren Protokollen können Sie mit dem Parser-Tool von RSA NetWitness Logs einfach Parser für neue, nicht unterstützte oder benutzerdefinierte Ereignisquellen erstellen. Zusätzliche Unterstützung für die benutzerdefinierte Protokollanalyse ist auch über die RSA Link-Community erhältlich.

Geschwindigkeit und Flexibilität

RSA NetWitness Logs ermöglicht die Konfiguration und das selektive Aufbewahrungsmanagement von Roh- und Metadaten. Die kurzfristige Aufbewahrung ermöglicht einen extrem schnellen Zugriff auf Daten. Eine langfristige Aufbewahrung gleicht die Anforderungen für kosteneffizienten Speicher und indizierten Zugriff für Compliance-Zwecke aus.

UEBA (User And Entity Behavior Analytics)

RSA NetWitness UEBA Essentials erweitert die Bandbreite der Analysen, um erweiterte Bedrohungen zu erkennen. RSA NetWitness UEBA Essentials ist über RSA Live für alle Kunden der RSA NetWitness Platform verfügbar. Es spiegelt eine Dimension der Analysefunktionen wider, die es unseren Kunden ermöglicht, sowohl die bekannten als auch die unbekannten Bedrohungen von heute schnell zu erkennen.

Flexibles Bandbreitenmanagement

Um Herausforderungen mit der Bandbreite zu lösen, können Administratoren steuern, was aus den Satellitenbüros per Pull an die zentralen Standorte übermittelt und dort aggregiert wird. RSA NetWitness Logs bietet Optionen, um Pull-Protokolle mithilfe von voreingestellten Einschränkungen für die Anzahl und den Typ der erfassten Protokolle zu begrenzen. Das umfasst auch die Komprimierung und Verschlüsselung von Protokolldaten, die zwischen verschiedenen Komponenten in der Architektur verarbeitet und aggregiert werden.

Über die Clouds hinaus blicken

Sie können RSA NetWitness Logs in Private-, Public- oder Hybrid-Cloud-Architekturen bereitstellen. Außerdem lassen sich Office 365-Umgebungen oder Salesforce-Anwendungen problemlos überwachen. Für Sichtbarkeit in komplexen Cloud-Umgebungen können modulare Komponenten virtuell und in Public Clouds, einschließlich AWS und Amazon, bereitgestellt werden.

Endpunktsichtbarkeit

RSA NetWitness Endpoint Insights bietet wesentliche Endpunktbestandsscans (Endpoint Inventory Scans), die in Kombination mit den Weiterleitungs- und Filterfunktionen für Protokolle von Microsoft Windows die Kosten und die Komplexität bei der Bedrohungsermittlung senken. RSA NetWitness Endpoint Insights ist ein speziell entwickelter Agent, der Sichtbarkeit in Hostkonfigurationen, Prozessdetails und Nutzerkontext bietet sowie das Monitoring von Windows-Protokollen vereinfacht.

Weiterentwicklung über Protokolle hinaus

Erweitern Sie die Funktionen zur Bedrohungserkennung mit der RSA NetWitness Platform über Protokolle hinaus. RSA NetWitness Logs lässt sich nahtlos in andere modulare Komponenten der RSA NetWitness Platform integrieren, darunter RSA NetWitness Network, RSA NetWitness Endpoint und RSA NetWitness Orchestrator. Diese nahtlose Integration und eine einheitliche Plattform sorgen für mehr Sichtbarkeit und schaffen korrelierte Metadaten mit der Leistung von fortschrittlichem SIEM in Ihrem Netzwerk – mit Sichtbarkeit für Protokolle, Pakete, NetFlow und Endpunkte für eine schnellere Erkennung und Reaktion.

09/20, Datenblatt, H16876-1 W386667.