Lösungen für Security Information and Event Management
Zur Unterstützung Ihrer Geschäftsziele

Tivoli® software

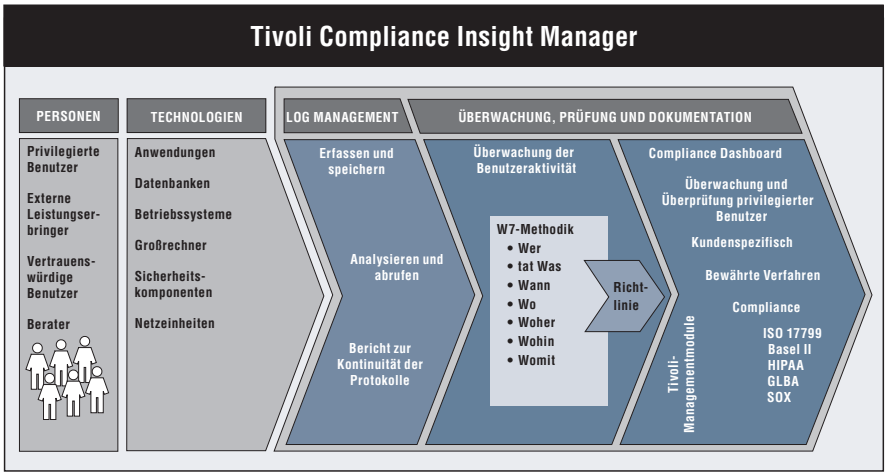
Überwachung und Überprüfung privilegierter Benutzer mit IBM Tivoli Compliance Insight Manager

Unbefugte Aktivitäten privilegierter Benutzer können ein großes Risiko für die Sicherheit Ihres Unternehmens und Ihre Bemühungen zur Einhaltung von Vorschriften darstellen. Die Festlegung der richtigen Sicherheitsrichtlinie ist aber nur ein Teil der Lösung. Wie können Sie Kontrollmechanismen implementieren, die nicht mit den Zuständigkeiten Ihrer Administratoren für die Betriebssysteme, Datenbanken, Anwendungen und Geräte Ihres Unternehmens in Konflikt geraten?

Administratoren mit unbeschränktem Zugriff auf Anwendungen und Plattformen können unabsichtlich oder in böswilliger Absicht Aktionen durchführen, die Unternehmensrichtlinien verletzen und zu Vorfällen von Identitätsdiebstahl führen. Viele Complianceanforderungen, Prüfer und Kontrollstrukturen wie CObIT (Control Objectives for Information and related Technology) und ISO (International Standards Organization) 17799 haben ein besonderes Augenmerk auf die durch privilegierte Benutzer entstehenden Risiken. Deshalb benötigt Ihr Unternehmen oft Funktionen zur Überwachung und Prüfung privilegierter Benutzer (Privileged-User Monitoring and Audit, PUMA), um die Aktionen von Administratoren überwachen, dokumentieren und analysieren zu können.

IBM Tivoli Compliance Insight Manager bietet verlässliche Informationen zum Verhalten privilegierter Benutzer, mit deren Hilfe Sie wichtige Datenbestände Ihres Unternehmens schützen und Prüfern und dem Management gegenüber die Wirksamkeit Ihrer Kontrollmechanismen nachweisen können. Durch Automatisierung der Überwachung, Dokumentation und Analyse des Benutzerverhaltens kann Ihr Unternehmen die Wirksamkeit Ihrer internen Kontrollmechanismen dokumentieren, implementieren und maximieren – in der Regel ohne die wirtschaftliche Produktivität der Administratoren zu beeinträchtigen.

Tivoli Compliance Insight Manager realisiert eine in sich geschlossene Struktur zur Überwachung und Dokumentation von Datenbanken, Betriebssystemen, Großrechnern, Anwendungen, Sicherheitskomponenten und Netzeinheiten und integriert auf diese Weise das PUMA-Konzept in Ihr unternehmensweites System zur Einhaltung von Vorschriften.



Beantwortung der Fragen von Prüfern und anderen

Complianceanforderungen, Standards und Prüfer fordern von Ihnen ein aktives Management der Risiken und Kosten, die mit dem notwendigen Zugriff privilegierter Benutzer auf sensible oder vertrauliche Datenbestände verbunden sind. Tivoli Compliance Insight Manager unterstützt Sie bei der Beantwortung der Fragen rund um den Zugriff privilegierter Benutzer in Ihrem Unternehmen, zum Beispiel:

Was tun Administratoren, Datenbankadministratoren (DBAs) und Rootbenutzer im System?

Welche Änderungen wurden am System vorgenommen?

Wurde ein privilegierter Zugriff dazu genutzt, das Prinzip der getrennten Zuständigkeiten zu verletzen?

Hat ein unzufriedener Administrator versucht, eine fremde Identität zu stehlen?

Haben Administratoren vertrauliche oder sensible Daten eingesehen?

Durch eine plattformunabhängige Überwachung im gesamten Unternehmen und die Möglichkeit, entsprechende Berichte zu erstellen, unterstützt Sie Tivoli Compliance Insight Manager bei der Beantwortung dieser und vieler weiterer Fragen. So können Sie in systemeigenen Logdaten Informationen über den privilegierten und nicht privilegierten Zugriff erfassen. Die Protokollierung ist äußerst effizient, sicher und zuverlässig und läuft im Hintergrund ab, so dass privilegierte Benutzer Schlüsselfunktionen ohne unnötige Einschränkungen ausführen können.

Für die anschließende Interpretation der Daten müssen diese zuerst normalisiert werden. Erst dann kann das Verhalten der einzelnen Benutzer nachvollzogen werden. Da die Logs durch die zum Patent angemeldete W7-Methodik in eine einfache, leicht verständliche Sprache umgesetzt werden, können Sie schnell ermitteln, Wer, Was, Wann, Wo, Woher, Wohin und Womit getan hat. Dies vereinfacht den Vergleich der Benutzeraktivitäten mit Ihren Richtlinien, so dass sich stark technisch orientierte Fachleute wie Programmierer und DBAs auf geschäftskritische Aktivitäten konzentrieren können. Wird ein ungewöhnliches Verhalten – ob von normalen oder privilegierten Benutzern – festgestellt, können Sie mit Hilfe einer Gesamtübersicht zur Richtlinieneinhaltung, von Benachrichtigungsfunktionen und eines umfassenden Berichtswesens Maßnahmen zur Fehlerbehebung ergreifen.

Berichte zur Überwachung privilegierter Benutzer als Nachweis Ihrer Kontrollmechanismen gegenüber Prüfern

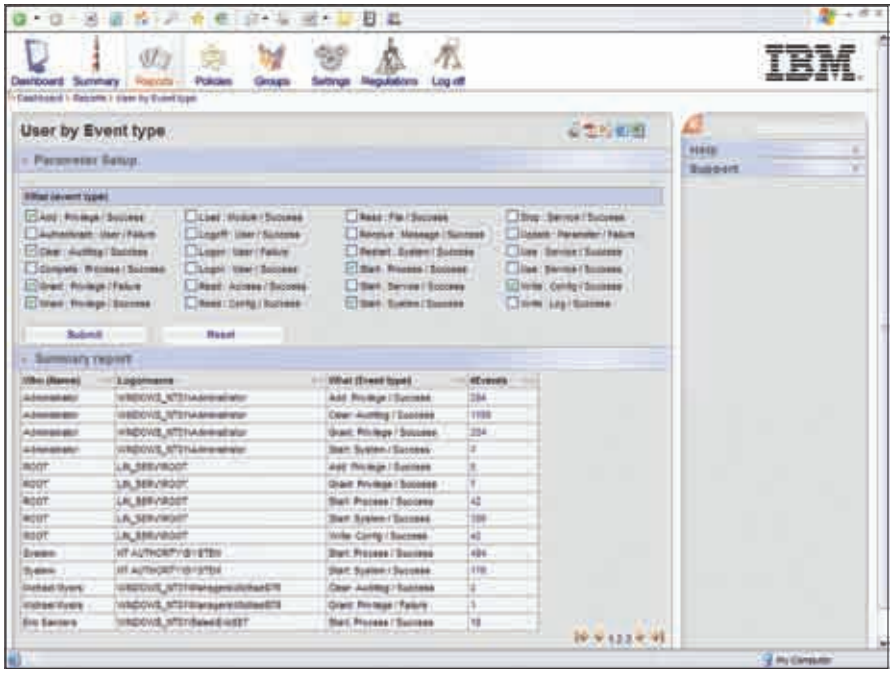
Tivoli Compliance Insight Manager unterstützt Sie nicht nur bei der Erfassung und Interpretation der Logdaten, sondern stellt auch eine leistungsfähige Statusübersicht und Best-Practice-Berichte für die Kommunikation mit Prüfern und Personen innerhalb Ihres Unternehmens bereit. Unter den hunderten von Berichten, über die Tivoli Compliance Insight Manager verfügt, sind folgende für PUMA besonders hilfreich:

Unternehmensweite Statusübersicht für die Prüfung

Diese richtlinienorientierte Statusübersicht ermöglicht einen allgemeinen Überblick über die Aktivitäten im System, wobei Problembereiche an Größe und Farbe zu erkennen sind. Zum Beispiel können Sie schnell feststellen, wenn ein Manager Aktionen mit einem Prüfprotokoll durchführt oder in Verletzung geltender Nutzungsrichtlinien auf Finanzdaten zugreift. In den anpassungsfähigen Ansichten der Statusübersicht werden die für den jeweiligen Benutzer interessanten Informationen angezeigt. Drilldown-Funktionen ermöglichen einen schnellen Zugriff auf die zugrundeliegenden Ereignisse.

Bericht „User by Event type“

Mit diesem Bericht können Sie feststellen, wer plattformübergreifend – und im gesamten Unternehmen – administrative Aktionen ausgeführt hat. Der Bericht zeigt neben der Person, die die Aktivität ausgeführt hat, auch den jeweiligen Aktivitätstyp. Durch einfachen Klick auf die Ereignisse erhalten Sie genauere Informationen. Mit diesem Bericht können Sie feststellen, ob Administratoren nicht-administrative Aktivitäten ausgeführt haben und ob Benutzer ohne Administratorrechte privilegierte Änderungen am System vorgenommen haben. Genau diese Fälle gehören zu den Situationen, von denen Ihre Prüfer und das Management wissen möchten, ob Sie sie überwachen.



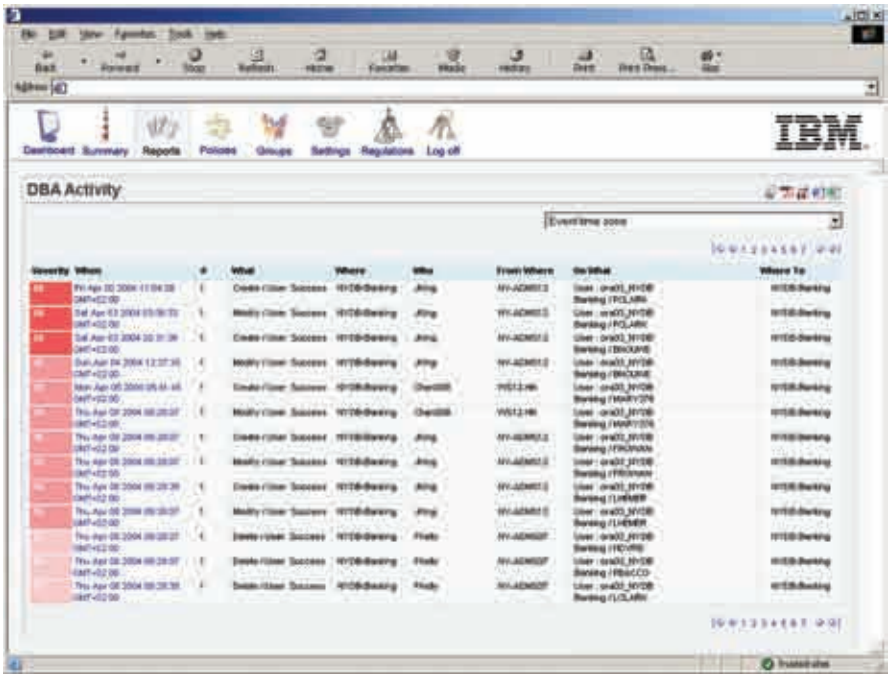
Mit dem Bericht „User by Event type“ erhalten Sie eine Übersicht über die administrativen Aktivitäten im gesamten Unternehmen als Hilfestellung für die Vorbereitung auf Audits. Neben der Anzahl und dem Typ der Ereignisse werden auch die Anmeldedaten angezeigt.

Erweiterung von PUMA durch Services

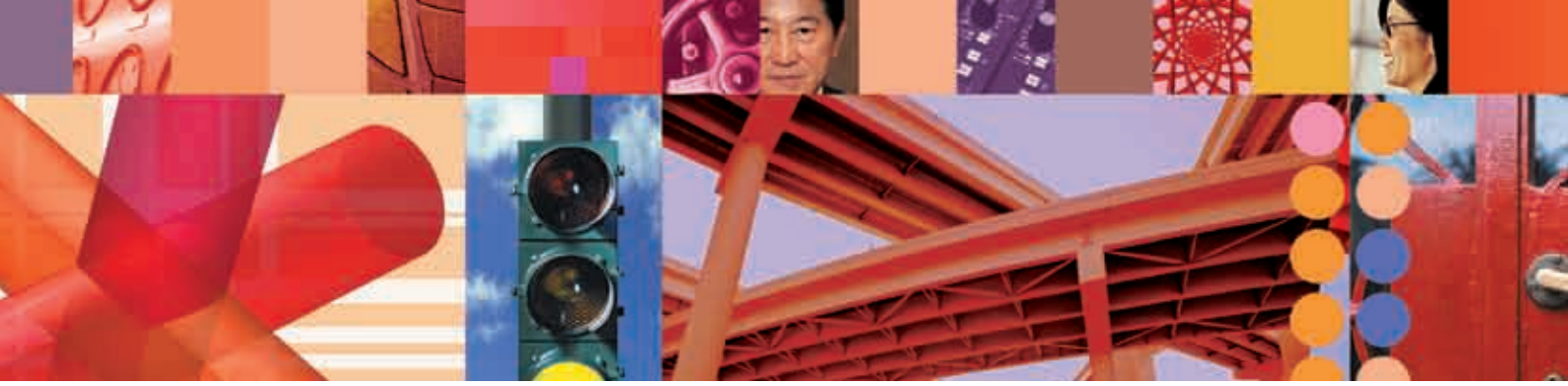
Mit Tivoli Compliance Insight Manager können Sie ohne Vorbereitungs- oder Anpassungsaufwand das Verhalten privilegierter Benutzer überwachen. Mit Hilfe professioneller Services für die Implementierung und Vor-Ort-Schulung können Sie die Gesamtlösung weiter optimieren und noch besser an die Erfordernisse Ihres Unternehmens anpassen. IBM Fachleute, die bereits an zahlreichen Implementierungen beteiligt waren, können Ihnen den Einstieg erleichtern, indem sie Berichte so definieren und optimieren, dass Aktivitäten in den verschiedensten Subsystemen erfasst und die Anforderungen an Complianceberichte und Berichte für die Unternehmensführung erfüllt werden. Zusätzlich bieten sie individuelle Vor-Ort-Schulungen an, um Ihr Team bei der Verwaltung und Nutzung der Lösung zu unterstützen.

Weitere Berichte

Tivoli Compliance Insight Manager beinhaltet auch Berichte, die einen Überblick über die Aktivitäten ausgewählter Benutzer (wie Administratoren oder DBAs) bieten, alle Unternehmensereignisse nach ihrem Typ aufführen, genaue Angaben für die Analyse von Ereignissen liefern, den Zugriff auf sensible Daten identifizieren, operative Änderungen überwachen und vieles mehr. Darüber hinaus können Sie mit der benutzerfreundlichen und dennoch äußerst leistungsfähigen Funktion zum Schreiben angepasster Berichte Ihre Berichte auf spezielle Unternehmensanforderungen zuschneiden.



Der Bericht zu den DBA-Aktivitäten zeigt die Datenbankzugriffe an, deren Quelle außerhalb der Anwendungsschicht liegt. Einige Aktivitäten sind routinemäßige DBA-Ereignisse. Für andere Aktivitäten wird eine hohe Prioritätsstufe angegeben; diese können dann mit den Drilldown-Funktionen von Tivoli Compliance Insight Manager genauer betrachtet werden.



Weitere Informationen

Auf der Basis über zwanzigjähriger Erfahrung in den Bereichen Security Audit- und Compliancemanagement bietet Tivoli Compliance Insight Manager eine führende Lösung für die Logdatenerfassung und -analyse, die Überwachung privilegierter Benutzer und die Erstellung von Audit- und Complianceberichten im gesamten Unternehmen – von Betriebssystemen und Großrechnern über Datenbanken und Anwendungen bis hin zu Netzeinheiten und Sicherheitskomponenten.

Wenn Sie mehr darüber erfahren möchten, wie Tivoli Compliance Insight Manager Ihr Unternehmen dabei unterstützt, die Aktivitäten privilegierter Benutzer zu überwachen und die Maßnahmen zur Einhaltung von Richtlinien zu integrieren, wenden Sie sich an Ihren IBM Ansprechpartner oder IBM Business Partner, oder besuchen Sie uns unter:

ibm.com/tivoli

Tivoli-Software von IBM

Tivoli-Software stellt ein umfassendes Paket von Angeboten und Funktionen zur Unterstützung von IBM Service Management zur Verfügung – ein skalierbares, modulares Verfahren, das Ihrem Unternehmen effizientere und effektivere Services bereitstellt. Tivoli erfüllt die Ansprüche von Unternehmen jeder Größe und ermöglicht es Ihnen, durch Integration und Automatisierung von Prozessen, Arbeitsabläufen und Aufgaben hervorragende Services für die Unterstützung Ihrer Geschäftsziele bereitzustellen. Die sichere, auf offenen Standards basierende Service-Management-Plattform Tivoli wird ergänzt durch proaktive Lösungen für operatives Management mit durchgängiger Transparenz und Kontrolle. Sie wird außerdem gestützt durch den hervorragenden IBM Kundendienst, die IBM Unterstützungsfunktion und ein aktives Geschäftsumfeld von IBM Business Partnern. Des weiteren können Tivoli-Kunden und -Geschäftspartner gegenseitig ihre bewährten Verfahren nutzen, indem sie an unabhängigen IBM Tivoli Benutzergruppen auf der ganzen Welt teilnehmen. Besuchen Sie:

www.tivoli-ug.org

IBM Deutschland GmbH
70548 Stuttgart
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

Gedruckt in den USA
06-07

TAKE BACK CONTROL WITH Tivoli®

TIB10406-DEDE-00