FIREMON

PROACTIVE SECURITY INTELLIGENCE

www.firemon.de

POLICY PLANNER

Verbesserung des Firewall-Betriebs durch Änderungsautomatisierung

Mit der steigenden Komplexität von Unternehmensnetzwerken und Gerätekonfigurationen gestaltet sich auch die Verwaltung und Implementierung von Änderungen immer schwieriger. Die manuelle Instandhaltung der sich ständig verändernden Netzwerkzugriffs- und Sicherheitsanforderungen ist beinahe unmöglich. Diese Vorgehensweise ist nicht nur zeitraubend, sondern ist auch fehleranfällig.

Der Policy Planner für den FireMon Security Manager automatisiert den Änderungs-Workflow, empfiehlt Regeländerungen, analysiert die Auswirkungen der geplanten Änderungen und dokumentiert den Zweck und die Zuständigkeit der Regeln.

WAS IST DER POLICY PLANNER?

Der FireMon Policy Planner ist eine Lösung für den Änderungs-Workflow, die den Änderungsprozess automatisiert und Firewall-Administratoren die notwendigen Werkzeuge für eine kontinuierliche Anpassung der Richtlinien und Schutzmechanismen bereitstellt. Dieses webbasierte Modul erfasst Benutzeranforderungen, empfiehlt Regeländerungen, stellt eine detaillierte Risikobewertung der angeforderten Änderungen bereit und unterstützt vollständige Systemprüfungen und -verifizierungen. Der Policy Planner kann zusammen mit vorhandenen Automatisierungstools für Geschäftsprozesse eingesetzt werden und ermöglicht die Kommunikation während des Änderungsprozesses.

Task	Resolution	Date/Time	Notes
Verify Solution	Verify	Wednesday 11:44AM	
Implement Change	Complete	Wednesday 12:03AM	done with install.... Tested successfully
Approve Design	Approve	Tuesday 4:32PM	it's good to go
Design Solution	Complete	Tuesday 12:20PM	Hey, please do this tonight
Provide More Info	Complete	Tuesday 9:37AM	
Design Solution	Need More Info	Monday 4:15PM	These destinations and services do not seem accurate. Please update
Request Ticket	Submitted	Monday 3:03PM	

Prüfen Sie schnell, ob die Änderungen den richtigen Validierungs- und Verifikationsverfahren entsprechen.

Der FireMon Policy Planner verbessert den Workflow für Änderungen an der Netzwerksicherheit mithilfe von Firewall-spezifischen Funktionen, die:

- gerätespezifische Compliance-Richtlinien definieren und gewährleisten, dass die geplanten Änderungen diese Standards nicht verletzen, bevor sie implementiert werden
- Firewall-Felder wie Quelle, Ziel, Dienst und Begründung erfassen
- die Erstellung von Anforderungen eliminieren, die bereits durch Firewall-Richtlinien erfüllt wurden
- technische Empfehlungen für alle notwendigen Firewall-Änderungen bereitstellt
- die das Risikopotenzial für neue Zugriffsanfragen vor der Implementierung bewertet
- die Regeländerungen im FireMon Security Manager dokumentiert

VORTEILE DES POLICY PLANNER

Stellen Sie sicher, dass die richtigen Firewall-Änderungen zur richtigen Zeit unter möglichst geringem Ressourcenaufwand erfolgen.

DER POLICY PLANNER BIETET FOLGENDE MÖGLICHKEITEN:

- Prüfung der Risiken des angeforderten Zugriffs
- Proaktive Prüfung der geplanten Änderungen auf die Richtlinien-Compliance
- Senkung der Kosten für die Compliance-Dokumentation
- Steigerung der Effizienz Ihrer Firewall-Administratoren
- Ermöglichung von Prüfungen für geschäfts-, technik- und Compliance-bezogene Änderungen

FUNKTIONEN:

- Verbesserung des IT-Änderungs-Workflows
- Integration mit bereits vorhandenen Geschäftssystemen
- Verhinderung risikoreicher Zugriffsanfragen
- Dokumentation von Genehmigungen

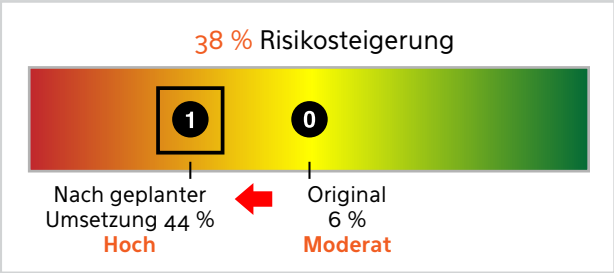
FORDERN SIE EINE KOSTENLOSE TESTVERSION DES **POLICY PLANNER** AN UNTER: WWW.FIREMON.DE

MERKMALE DER LÖSUNG

RASCHE RISIKOBEWERTUNG

Bewerten und kommunizieren Sie die Risiken neuer Zugriffsanfragen, und halten Sie mit den Änderungen und der Komplexität Schritt, denen Ihr Netzwerk unterliegt.

- Erkennen Sie, wenn ein neuer Zugriff ein verwundbares System aufdeckt.
- Schätzen Sie die Auswirkungen der geplanten Änderungen vor der Implementierung ein.
- Optimieren Sie die Genehmigung für Zugriffe, die das Risikoprofil nicht beeinflussen.
- Sorgen Sie für die Analysen und die Transparenz, die zur Verhinderung der Einführung von problematischen Einstellungen nötig sind.



Machen Sie die Auswirkungen der angeforderten Änderungen sichtbar, bevor diese implementiert werden.

ERWEITERTE GESCHÄFTSPROZESSINTEGRATION

Integrieren Sie den Policy Planner in bestehende Prozessverwaltungslösungen unter Einhaltung der Best Practices gemäß dem „Business Process Model and Notation (BPMN)"-Standard. Dieser Standard erlaubt mehreren Teams, einschließlich geschäftlichen und technischen Anwendern, die Workflows, warteschlangenspezifischen Vorlagen und Abläufe des Ticketing-Systems ihrer Anfrage entsprechend anzupassen.

Neben der Volltextsuche lassen sich im Policy Planner Ad-hoc-Anfragen auf Grundlage aller Felder in Bezug auf Ticketing-Anforderungen erstellen. Benutzer können offene Tickets über Dashboard-Widgets überwachen oder Engineering-Ressourcen mithilfe einer Liste verwalten, die Informationen zu offenen Tickets, zugewiesenen Benutzern und der Zeit in der Warteschlange enthält.

REGELEMPFEHLUNG

Die Regelempfehlung des FireMon Policy Planner analysiert das aktuelle Verhalten von Regelsätzen und bestimmt umgehend alle notwendigen Änderungen. Er hilft zudem bei den folgenden gängigen Szenarien:

- **Keine Änderungen notwendig** – Der Policy Planner erkennt, wenn eine neue Anforderung einen Zugriff dupliziert, der bereits in der Standard-Firewall-Richtlinie bekannt ist, bevor der angewiesene Techniker mit der Implementierung fortfährt.
- **Es existieren gleichartige Zugriffe** – Der Policy Planner macht Regeln ausfindig, die einen ähnlichen Zugriff auf eine neue Anfrage erlauben, um die Erstellung von überflüssigen Regeln und die damit einhergehende Komplexität zu verhindern.

Detaillierte Regelempfehlungen

PROAKTIVE COMPLIANCE-PRÜFUNG

Stellen Sie schon während der Regelplanungsphase sicher, dass neu hinzugefügte Regel- oder Konfigurationsänderungen den bestehenden Compliance-Richtlinien und Best Practices entsprechen. Es können verschiedene Prüfungen für verschiedene Gerätegruppen konfiguriert werden. Zum Beispiel können unternehmensweite Geräteprüfungen allen Geräten zugeteilt werden und PCI-Prüfungen nur solchen Geräten, die sich in einer PCI-Datenumgebung befinden. Die Prüfungsergebnisse werden angezeigt, bevor die Regeländerungen genehmigt werden, und zeigen, ob die Richtlinien in ihrer jetzigen Form implementiert werden sollten oder nicht.

Ermitteln Sie geplante Regeln, die die bestehenden Compliance-Richtlinien verletzen.

FIREMON

8400 W. 110th Street, Suite 500
Overland Park, KS 66210 USA
Tel.: +1 913 948 9570 E-Mail: info@firemon.com

Erfahren Sie mehr über unsere Lösungen:
www.firemon.de

REV 041415