DER FÜHRENDE ANBIETER FÜR PROAKTIVE SICHERHEITSVERWALTUNG

FOKUS

Große, komplexe Netzwerke mit hochmodernen Sicherheits- und Netzwerktechnologien bringen große Herausforderungen in Bezug auf Sicherheitsinformationen mit sich. Anhaltende externe und interne Bedrohungen, ständig wachsende Compliance-Anforderungen und ein konstanter Einsatzdruck müssen täglich bewältigt werden – normalerweise von mehreren Teams an unterschiedlichen Standorten innerhalb der verschiedenen funktionalen Organisationen.

Diese Komplexität beeinträchtigt die Effektivität des Risiko-, Richtlinien-, Konfigurations- und Änderungsmanagements und der Audit-Prozesse, die den Netzwerkzugriff bei gleichzeitiger Gewährleistung der Sicherheit sicherstellen sollen. FireMon liefert wichtige Daten zur bestehenden Netzwerksicherheitsinfrastruktur und sorgt so für eine Reduzierung der Komplexität und Automatisierung der Betriebsabläufe. Dies ermöglicht die Verbesserung der Sicherheit und eine kontinuierliche Kostensenkung.

KUNDEN

Wir stellen hochmoderne Produkte und Dienstleistungen für zahlreiche Fortune 500-Unternehmen bereit, die weltweit in den Finanz-, Gesundheitsfürsorge-, Produktions-, Transport-, Unterhaltungs-, Energie- und Einzelhandelsbranchen tätig sind.

Viele der weltweit größten und besten MSSPs verlassen sich auf die Distributed-Data-Collection-Architektur von FireMon, die flexible Bereitstellungsoptionen und hohe Skalierbarkeit bietet. Auf diese Weise können sie Tausende Geräte verwalten und hochwertige, verwaltete Sicherheitsdienstleistungen für ihre umfangreichen Kundenstämme bereitstellen.

Einige Beispielkunden:

- CSC, ein weltweit führender Anbieter von technologiebasierten Geschäftslösungen und Dienstleistungen, bindet FireMon als ein Schlüsselelement seines Managed Firewall Ruleset Assurance-Dienstes ein.
- Accor North America, ein Geschäftszweig eines weltweit agierenden Gastgewerbeunternehmens, nutzt FireMon zur Überarbeitung seiner gesamten grundlegenden Sicherheitsregeln und zur Erfassung von Konfigurationsänderungen in einem zentralen System.
- Raymond James Financial – ein diversifiziertes Finanzdienstleistungsunternehmen – überwacht mit FireMon die Einhaltung von Firewall-Richtlinien gemäß der wichtigsten Regierungs- und Branchenstandards wie FISMA, SOX und PCI DSS in einer Multi-Vendor-Firewallstruktur.

PARTNER

FireMon hat weltweit mehr als 150 aktive Partner, darunter Unternehmensberater, Einzelhändler, Distributoren, Systemintegratoren und branchenführende Technologieunternehmen.

HOMELAND SECURITY TODAY

FireMon unter den „Rising 10 of 2013“ für „Continuous Monitoring“

Unsere Lösungen unterstützen die Automatisierung der Defense Information Systems Agency (DISA), des Security Technical Implementation Guide (STIG) sowie Audits im Rahmen des Federal Information Security Management Act (FISMA). Dabei wird der betriebs- und Compliance-bezogene Arbeitsaufwand zur Bewertung von Netzwerkrisiken und zur Vereinfachung der Firewall-Richtlinienverwaltung reduziert.

FIREMON

Folgen Sie uns auf Twitter @FireMon

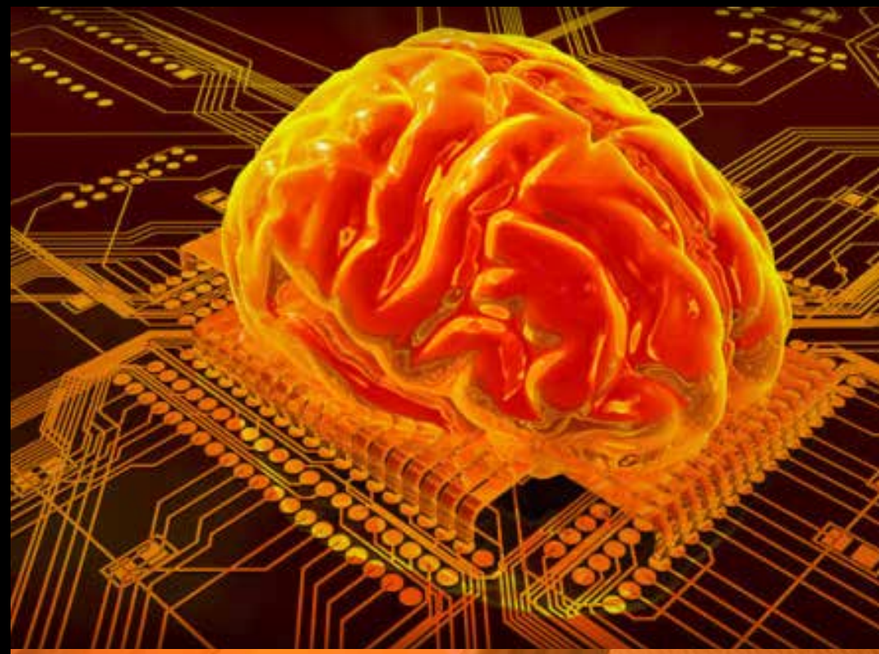
Folgen Sie uns auf Facebook:www.facebook.com/firemon

8400 W. 110th Street, Suite 400 · Overland Park, KS 66210 USA · Tel.: +1 913 948 9570 ·
E-Mail: info@firemon.com · www.firemon.de

rev121714

FIREMON

Proaktive Sicherheitsverwaltung



UNTERNEHMENSPROFIL

Unternehmen und MSSPs begehen bei der Verwaltung ihrer Netzwerksicherheitsinfrastrukturen häufig elementare Fehler. Wir haben FireMon, einen Anbieter von proaktiven Sicherheitsverwaltungslösungen gegründet, um genau diese Fehler zu beseitigen. Durch die Analyse des Sicherheitsstatus von Unternehmens- und MSSP-Netzwerken können wir IT-Sicherheitsteams bei der Erkennung, Behebung und Vermeidung von Lücken in ihrer Netzwerk-Sicherheitsinfrastruktur unterstützen.

Der Status der Unternehmensnetzwerksicherheit

IT-Sicherheitsteams haben Millionen von Dollar in ihre Sicherheitsinfrastrukturen investiert und weitere Millionen in Mitarbeiter und Subunternehmer, die diese Infrastrukturen betreiben. Und dennoch ist ein Großteil von ihnen nicht in der Lage, die grundlegenden Fragen zu ihrer eigenen Risikolage zu beantworten:

- Können riesige Regelsätze für bestehende Firewalls auf sichere Weise verringert werden?
- Welche angreifbaren Hosts sind für ausländische Regierungen erreichbar?
- Welche Zugriffsbeschränkungen sind nicht länger im Einsatz und sollten aufgehoben werden?
- Erhöht die von mir zu genehmigende Konfigurationsänderung mein Risiko?

Proaktive Sicherheitsverwaltung

FireMon bietet hochgradig skalierbare, leistungsstarke Lösungen zur Überwachung der Netzwerksicherheit, mit denen Unternehmen und MSSPs proaktiv handeln können. Durch Bereitstellung erheblicher Verbesserungen in Bezug auf Transparenz, Messung und Bewertung hilft FireMon Unternehmen, Schwachstellen zu erkennen, und gibt ihnen Empfehlungen für priorisierte Korrekturmaßnahmen, bevor interne Akteure oder externe Widersacher diese Schwachstellen ausnutzen können.

Das Risiko steht im Mittelpunkt unseres Ansatzes für die proaktive Sicherheitsverwaltung: An ihm wird das empfindliche Gleichgewicht zwischen Zugriff und Sicherheit gemessen. Die patentierte Überwachungs-Engine von FireMon simuliert Angriffspfade innerhalb des Netzwerks und misst das Bedrohungspotenzial. FireMon stellt erweiterte Funktionen für die kontinuierliche Evaluierung bereit, die bei der Automatisierung von gängigen manuellen Prozessen helfen. Dadurch werden Sicherheitsteams entlastet, sodass sie sich auf proaktive Programme zur Vermeidung von Sicherheitsverletzungen konzentrieren können.

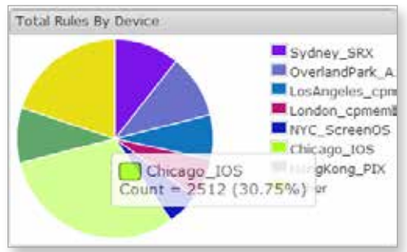
FireMon Security Intelligence Platform

FIREMON-LÖSUNGEN

SECURITY MANAGER

Der Security Manager sorgt für eine effektivere Verwaltung von Firewalls, Routern, Switches und Load Balancern, indem er sämtliche Änderungen an Firewall-Richtlinien erkennt und meldet sowie die durch Änderungen anfallenden Kosten verringert. Er zeigt, wie Traffic durch die einzelnen Regeln fließt und welche Regeln nicht genutzt werden, damit unnötige Zugriffe bereinigt werden können. Zudem ermöglicht der Security Manager die kontinuierliche Überwachung von Richtlinien für gesetzliche Vorschriften wie DICAP, FISMA, NSA-Richtlinien, PCI DSS, HIPAA, SOX und NERC-CIP, um Compliance zu gewährleisten. Zu den einzigartigen Leistungsmerkmalen gehören:

- Eine Zugriffspfadanalyse zeigt den genauen Pfad, den die Datenpakete durch das Netzwerk nehmen, einschließlich aller Schnittstellen, Routen, Sicherheitsregeln und Übersetzungsregeln, die ein potenzielles Risiko bergen. SecOps kann den Datenverkehr nun problemlos umleiten, um Assets zu umgehen, die vermutete oder bekannte Schwachstellen aufweisen.
- FireMon Insight ist ein Echtzeit-Dashboard, das Anwendern eine vollständige Übersicht aller wichtigen Leistungskennzahlen Ihrer Sicherheitskonfiguration anzeigt und REST-APIs für das Exportieren in andere Systeme bereitstellt.



Firewall-übergreifende Echtzeitanalyse aller Sicherheitsmetriken

POLICY PLANNER

Der Policy Planner ist eine intelligente Firewall-Workflow-Lösung, die den Änderungsprozess automatisiert und Firewall-Administratoren die notwendigen Werkzeuge bereitstellt, um präzise Änderungen an den Regelgrundlagen vorzunehmen. Dieses webbasierte System erfasst Zugriffsanfragen, empfiehlt Regeländerungen, stellt eine detaillierte Risikoanalyse und Bewertung der Compliance-Auswirkungen für die geforderten Änderungen bereit und ermöglicht eine vollständige Prüfung und Verifizierung aller Änderungen.

- Lässt sich nahtlos in bestehende Automatisierungs-Tools für Geschäftsprozesse einbinden und unterstützt BPMN 2.0-konforme Systeme.
- Dokumentiert und automatisiert den Workflow-Prozess für Änderungen, ganz gleich, ob Sie eine intelligente Lösung für Business Process Software oder hauseigene Tools für die Änderungsverwaltung einsetzen.

Designänderungen, die Risiken minimieren und für Compliance sorgen

POLICY OPTIMIZER

Der Policy Optimizer ist eine intelligente Firewall-Workflow-Lösung, die den Risiko- und Compliance-Teams bei der Evaluierung und Entfernung unnötiger Firewall-Regeln hilft. Dazu wird der Neubestätigungsprozess automatisiert und Firewall-Administratoren die notwendigen detaillierten Informationen zur Verfügung gestellt, die für eine fortlaufende Anpassung des Netzwerkzugriffs erforderlich sind.

- Verbindet Sicherheitsteams mit Richtlinienverfassern, um isolierte Verwaltungsbereiche zusammenzuführen, die nicht regelmäßig miteinander kommunizieren.
- Bestätigt und dokumentiert umfassend die Begründung von Regeln und quantifiziert das Risiko angeforderter Änderungen zwecks kontinuierlicher Überwachung und Überprüfung.

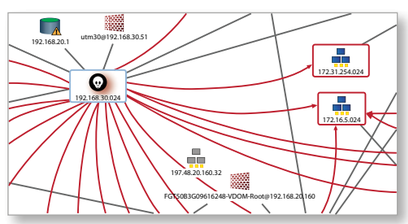
Automatische Regelprüfung auf Grundlage spezifischer Details

RISK ANALYZER

Der Risk Analyzer bietet eine neue Vorgehensweise zur Risikobemessung anhand hypothetischer Angriffsszenarien. Die Agentur definiert die Angriffsszenarien, bestehend aus einer Bedrohungsquelle und den von dieser Bedrohung gefährdeten Assets:

- Partner, die eine VPN-Verbindung für den Zugriff auf Bestellsysteme nutzen
- Geopolitische Bedrohungen, die das Ausschleusen von militärischen und technologischen Geheimnissen zum Ziel haben
- Interne Benutzer, die direkten Zugang zu geheimen Daten erhalten

Der Risk Analyzer misst die Gefährdung jedes dieser Assets in wenigen Minuten statt in Stunden. Ein aufschlussreiches Dashboard zeigt eine detaillierte Übersicht für jedes Szenario, identifiziert erreichbare Assets mit ausnutzbaren Schwachstellen und präsentiert einen visuellen Angriffsverlauf, der darstellt, wie der Angreifer die Netzwerksicherheitsmechanismen durchbrechen und einen tiefergehenden Zugang erhalten könnte.



Echtzeit-Visualisierung von Risiken für das Unternehmensnetzwerk