Mehrfach prämierte Lösung

Attraktives Preis-Leistungsverhältnis

Bei **Tausenden von Kunden** im Einsatz bewährt

Überwachung, Auswertung und Archivierung von Systemmeldungen leicht gemacht

Systemmeldungen, die täglich in großer Anzahl im Netzwerk anfallen, liefern wertvolle Informationen. Ihre Verarbeitung ist Teil eines effektiven Infrastruktur-Managements, das zur Zuverlässigkeit, Sicherheit und optimalen Verfügbarkeit des Netzwerks beiträgt und zudem hilft, Compliance-Verpflichtungen einzuhalten. Sicherheit und betriebliche Kontinuität lassen sich am besten gewährleisten, indem Systemmeldungen in Echtzeit überwacht werden – eine bedeutende Herausforderung angesichts des immensen Datenaufkommens.

GFI EventsManager™ entlastet Administratoren bei Erkennung, Verwaltung und Analyse von Problemen mit der IT-Infrastruktur. Seine proaktive Ereignisverwaltung in Echtzeit ermöglicht eine schnellere, zielgerichtete Lösung und erhöht die Verfügbarkeit und Sicherheit des Netzwerks. Unterstützt werden Ereignisse vielfältiger Art, ob aus W3C-Protokollen, Windows-Ereignisprotokollen sowie SQL-Server- und Oracle-Audits, oder auch Syslog-Meldungen und SNMP-Traps verschiedener Hardware.

VORTEILE VON GFI EVENTSMANAGER

- Besserer Schutz des Unternehmens dank rascher Ermittlung und Auswertung von Sicherheitsvorfällen
- Problemerkennung per Echtzeit-Alarmierung/Dashboard und höhere Netzwerk-Uptime
- Effiziente, kostensparende Überwachung und Verwaltung des gesamten Netzwerks
- Leichtere Einhaltung gesetzlicher und institutioneller Compliance-Vorgaben (SOX, PCI DSS, HIPAA u. v. m.)
- Zentrale Erfassung von Syslog-, W3C- und Windows-Events, SQL-Server-/Oracle-Audit-Daten und SNMP-Traps von Firewalls, Servern, Routern, Telefonanlagen, PCs u. v. m.
- Gebrauchsfertige Regeln zur Ereignisalarmierung sowie zur Klassifizierung und Verwaltung von Meldungen unterschiedlicher Hardware von Cisco, 3Com, HP u. v. a.

GFI EventsManager™

Überwachung, Verwaltung und Archivierung von Netzwerkereignissen

Weitere Vorteile von GFI EventsManager

- Granulare, weitreichende Datenerfassung
- Detaillierter Überblick zu Vorgängen in unterschiedlichen Umgebungen durch Auswertung einer großen Auswahl von Ereignistypen
- Nachverfolgung von Oracle- und SQL-Server-Aktivitäten mit Meldung von Änderungen an Datenbank-Tabellen, unbefugten Zugriffsversuchen u. Ä.
- Zuverlässige Datenquellen für forensische Untersuchungen

Gewährleistung der Netzwerksicherheit

Sicherheitsereignisse werden von GFI EventsManager in Echtzeit analysiert. Vorfälle lassen sich detailliert auf Ursachen überprüfen.

Überwachung des Systemzustands

Unternehmenskritische Netzwerkgeräte und Server werden proaktiv überwacht. Verhindern Sie Netzwerkausfälle, indem Sie z. B. Meldungen von Firewalls, Sensoren und Routern kontrollieren lassen oder Ereignisse, die von Microsoft ISA Server, SharePoint, Exchange Server, SQL Server und IIS ausgegeben werden. Halten Sie sich über folgende Bereiche kontinuierlich auf dem Laufenden: Status von E-Mail-Warteschlangen und SMTP-Gateways, Verfügbarkeit von MAPI, Festplattenzustand, verfügbarer Festplattenspeicher und vieles mehr.

Einhaltung von Compliance-Vorgaben

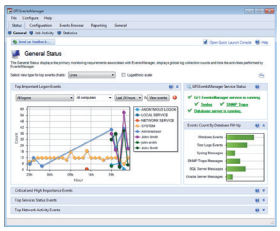
GFI EventsManager unterstützt Unternehmen bei der Umsetzung unterschiedlicher Vorgaben zur Archivierung und Analyse von Systemmeldungen, festgelegt durch Basel II, PCI DSS, SOX, Gramm-Leach-Billey Act, HIPAA, FISMA, USA Patriot Act, Turnbull Guidance 1999, UK Data Protection Act und EU DPD.

Forensische Sicherheitsanalysen

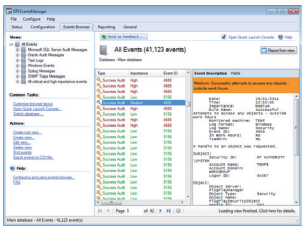
Bei der Erforschung von Problemursachen dienen Systemmeldungen als Grundlage. Sie helfen, Vorkommnisse chronologisch nachvollziehen zu können. Mit GFI EventsManager können Sie Auswertungen zeitnah, effizient und kostengünstig durchführen – unternehmensintern und ohne externe Sicherheitsberater.

Ereigniskontrolle mit höherer Granularität

Überwachen Sie eine breite Auswahl an Systemen und Hardware. Systemmeldungen unterschiedlicher Art, darunter Windows-Ereignisse, Syslog-Meldungen, W3C-Events und SNMP-Traps von Netzwerkelementen, werden zentral gesichert und analysiert. Erfassen Sie relevante Daten von Windows-Computern und anderen Geräten mit höherer Granularität, und verarbeiten Sie Informationen auch auf der Ebene erweiterter Tags. Über ein weiteres Vorgehen kann dann umgehend auf Grundlage der vorliegenden Ergebnisse entschieden werden – ohne zusätzliche Datenverwaltung.



Verwaltungskonsole



Verständlichere Ereignisprotokoll-Einträge

Analyse von Systemmeldungen (SNMP-Traps, Windows-Ereignisprotokolle, SQL-Server- und Oracle-Audit-Daten, W3C-Protokolle und Syslog)

Netzwerkadministratoren stehen regelmäßig vor der herausfordernden Aufgabe, mit zahlreichen kryptischen Einträgen überfüllte Event-Logs auszuwerten. GFI EventsManager hilft beim netzwerkweiten Kontrollieren und Analysieren von Windows-Ereignisprotokollen, W3C-Protokollen, SQL-Server- und Oracle-Audit-Daten oder Syslog-Meldungen von Netzwerkquellen. Dank Unterstützung von SNMP (Simple Network Management Protocol) können Zustand und Betriebsstatus unterschiedlicher Netzwerkelemente wie Router, Sensoren und Firewalls überwacht und gemeldet werden.

Weitere Leistungsmerkmale

- Zentrale Ereignisprotokollierung
- Echtzeit-Überwachung und Versand von Warnungen rund um die Uhr
- Hochleistungs-Scan-Engine
- Erfassung von im WAN verteilten Ereignisinformationen in einer zentralen Datenbank und/oder automatische dateibasierte Ereignisarchivierung
- Regelbasierte Verwaltung von Systemmeldungen
- Auto-Updater
- Leistungsstarkes Dashboard
- Fortschrittliche Funktionen zur Ereignisfilterung mit einfacher Erstellung von Regeln und Filtern
- Scan-Profile für Ereignisprotokolle
- Berichte zu wichtigen aktuellen Sicherheitsereignissen im Netzwerk
- Nachverfolgung von Benutzeraktivitäten unter Microsoft SharePoint
- Unterstützung bei Einhaltung des PCI DSS und ähnlicher Compliance-Vorgaben
- Unterstützung neuer Hardware (MIB-Datei-Import)
- SQL-Server-Auditing
- Oracle-Server-Auditing für Oracle 9i, 10, und 11g
- Verständliche Erklärungen zu Windows-Ereignissen
- Vielseitige Einsatzmöglichkeiten für unterschiedliche Unternehmensanforderungen
- Entfernung irrelevanter Ereigniseinträge
- Zeitgesteuerte Berichterstellung mit automatischem Versand per E-Mail
- Export von Ereignissen in individuell anpassbare HTML-Dateien
- Einsatz in virtuellen Umgebungen

Systemanforderungen

- Microsoft Windows XP, Windows Vista, Windows 7, Windows Server 2003/2008
- Microsoft .NET Framework 2.0
- Microsoft Data Access Components (MDAC) 2.8 oder später
- Zugriff auf Microsoft SQL Server 2005 (alle Editionen) oder später

Weitere Informationen und eine kostenfreie Testversion stehen zum Abruf bereit auf http://www.gfisoftware.de/eventsmanager

Microsoft Partner
Gold Independent Software Vendor (ISV)

GFI EventsManager™

Überwachung, Verwaltung und Archivierung von Netzwerkereignissen

Kontaktinformationen

Malta	GB	USA	Deutschland
Tel.: +356 2205 2000	Tel.: + 44 (0)870 770 5370	Tel.: +1 (888) 243-4329	Tel.: +49 (0) 69 22 22 73 12
Fax: +356 2138 2419	Fax: + 44 (0)870 770 5377	Fax: +1 (919) 379-3402	Fax: +49 (0) 69 2 22 22 64 78
sales@gfi.com	sales@gfi.co.uk	ussales@gfi.com	sales@gfisoftware.de

Weitere Niederlassungen von GFI finden Sie hier: http://www.gfisoftware.de/company/contact.html

GFI®
www.gfisoftware.de