STORMSHIELD

STORMSHIELD NETWORK
EVENT ANALYZER

SECURITY INTELLIGENCE TOOL

Whether you are a security professional or network manager, this solution is for you. Stormshield Network's Event Analyzer generates and automatically sends activity reports according to your role in the corporation to provide truly useful help in decision-making.

The wealth of indicators it provides helps you to stay compliant with various regulations (HIPAA, SOX, Basel II, PCI-DSS) by ensuring data integrity and confidentiality.

STAY ON TOP OF SECURITY MATTERS

Detailed periodic reports generated by Stormshield Network Event Analyzer make it possible to easily identify compliance with or deviations from the security policy. You are therefore in a position to control the effectiveness of your filter rules and define the appropriate corrective or preventive actions.

The dashboards and indicators it provides can be used as the basis of a continuous improvement process for your security policy. This approach is in line with the standards and regulations (HIPAA, SOX, Basel II, and PCI-DSS) that impose a regular review of event logs.

BOOST PRODUCTIVITY

Network administrators, you can now focus on your actual missions. Stormshield Network Event Analyzer will take care of your repetitive tasks.

Scheduling tasks allows you to create and modify actions that need to be performed daily or monthly. Reports are therefore generated and sent directly to the right recipients. Furthermore, maintenance operations on the database will be carried out automatically.

ADMINISTRATION TOOL

Advantages for the decision maker

- Time saved and better visibility
- Informed decisions based on data
- Compliance with legislation (legal archiving)

Advantages for the administrator

- Automation of tasks
- Powerful analysis tool (OLAP technology)
- Role-based access management

ABOUT

Arkoon and Netasq, fully owned subsidiaries of Airbus Defence and Space CyberSecurity, run the Stormshield brand and offer innovative end-to-end security solutions both in France and worldwide to protect networks (Stormshield Network Security), workstations (Stormshield Endpoint Security) and data (Stormshield Data Security).

WWW.STORMSHIELD.EU

Phone
+33 9 69 32 96 29

E-mail contact page

Non-contractual document. In order to improve the quality of its products, Arkoon and Netasq reserve the right to make modifications without prior notice.

All trademarks are the property of their respective companies.

OPTIMIZE DETAILED ANALYSES

Analyzing information to locate a particular event is a tricky task that may take up a lot of time.

The use of filters, sort functions and pivots with a simple drag & drop enables information to be analyzed much faster.

Stormshield Network Event Analyzer aggregates indicators in three dimensions (cube), thereby offering as many specific views of the information. Saving your view with its associated graphs allows you to reuse it with another data set in order to gauge changes.

INTUITIVE AND CUSTOMIZABLE PORTAL

The Stormshield Network Event Analyzer web portal enables you to view reports, schedule tasks and even perform detailed analyses in full simplicity. The possibility of customizing the homepage ensures that you always receive relevant information.

LOG PROCESSING & REPORTS
Full range supporting up to 360M events per day
More than 200 predefined reports
Support for syslog & flatfile formats
External syslog hub supported
Customized log processing
Report formats: html, pdf and txt
Customization of reports
Security indicator tracking

- Network activity
- Risk level (antivirus, IPS, antispam)
- Security policy tracking
- Vulnerability risk management *
- User activity (web, mail, ftp)

Report sending

- Management of automatic sending
- Sending to multiple recipients
- Selection of recipients according to report type
- Management of reports by client
- Sending of specific and/or customized reports
- RSS feed

TASK SCHEDULING
Intuitive web interface
Generation of reports
Time definition (start, frequency, duration)
Database maintenance
Customized SQL queries
Conditional actions

DETAILED LOG ANALYSIS
Representation of data in a cube (OLAP technology)
25 predefined queries
PSelection parameters of cube data
Browsing in cube views by dragging and dropping
Creation, backup and update of analyses

DATABASE
SQL engine
Optimized storage (data consolidation)
Data aggregation for different report types
Configuration of automatic purge
Verification of processes from the web interface
Scheduling of aggregation and purge processes
Verification of database status from the web interface

GRAPHICAL INTERFACE
Intuitive configuration interface
Direct access to generated reports
Customization of reports
Task scheduling
Execution of reports on demand
Detailed log analysis (OLAP)
Role-based access

ARCHIVING
Compliance with legal requirements (HIPAA, SOX, Basel II, PCI-DSS)
Integrity and confidentiality
Archiving of raw and/or aggregated formats
Verification of integrity during restoration

COMPATIBILITY
NETASQ Firewall in version 8 and 9
Stormshield Network Security Firewall
Windows server 2003 and 2008
Microsoft SQL Server 2005 and 2008
Microsoft IIS and .NET framework 3.5

** Requires the Stormshield Network VULNERABILITY MANAGER option on appliances from which logs are gathered*

Powered by Click&DECiDE