

SENTRY II

Advanced Event Log Management and System Monitoring

Security is a fundamental issue for the IT department. Sentry II is a comprehensive Security event log and performance-monitoring tool. It manages a Windows or Unix event log and interfaces to the Windows Performance Monitor. Sentry II stores important events and counters in an ODBC database and generates alerts based upon user-defined importance. In addition, it is comprised of 9 modules critical for system monitoring:

1) EVENT LOG WATCH

A real-time monitoring of Security, System, Application, Directory Service, File Replication and DNS Service Event Logs.

To get the maximum amount of security information from the event logs; focus must be placed on the Security Event Log. Proper IT security monitoring not only includes implementing proper access for user accounts but also creating audit policies in the security event logs. The security event log provides the means to manage important security processes:

Passwords changes

- Changes to access rights to shares, files, folders, etc.
- Attempts to unauthorized access to computer system resources.
- Attempts to unauthorized access to information held in application systems.
- System activity including logins, file accesses and security incidents.
- Produce and retain logs recording exceptions and security-related event
- Monitoring any attempts to unauthorized changes to IT systems.
- Monitor key system files and critical data for unauthorized changes.
- Active Directory permissions for user accounts, groups and computer accounts
- Monitor unauthorized Active Directory access permissions
- Monitor and Verify any change to users, groups, rights, and user account policies
- Notification of group policy changes

- Monitors authorized users attempts to perform unauthorized activities
- Log actions in detail and provide extensive security reporting
- Report on permission changes in Active Directory
- Monitor and log user information, access information, date and time stamp
- Monitor and notify of real-time policy modifications
- Last accessed dates for files and applications.

In addition, the native Microsoft Security Event Log offers 9 audit policies that must be turned on. The Nine Audit Policies are; Account Logon, Logon, Account Management, Policy Change, Process Tracking, Object Access, Privilege Use, System Events and Directory Service Access.

Implementing these audit polices on your network will give you important information but will also generate hundreds of records (events) in the security event logs on your enterprise servers. The easiest and best way to manage these records is to store the events in a database. SENTRY II automatically inserts all event log data into an ODBC database

The **AUTOMATIC REPORTING** tool creates the HTML reports to detail your organizations adherence to IT security policy. Schedule Sentry II Reports for automatic or periodic report generation with optional Email of the Report output, or a link to the output, to one or more recipients. You control and have complete flexibility on what is reported, for what time frame and for events related to a particular audit policy.

Sophisticated **ALERT FEATURES** notify you of potential problems, enabling you to automatically execute corrective actions when alert conditions have been met. Monitoring data can be viewed in real-time or historical data reports can be generated.

SENTRY II not only assists your staff on getting control of the event logs it adds valuable security monitoring features. It has EIGHT additional WATCH features. The WATCH DOG features of SENTRY II insure your network is secure from both internal and external security threats.

2) SERVER WATCH

Provides a GUI for availability of all servers in your network. It monitors server IP Services; HTTP, FTP, SMTP, POP3, SNMP, DNS. TCP/IP ports are watched for intrusion detection.

3) FILE WATCH

Real-time monitoring of select, key system and application files for creation, deletion, change, no change, size, and/or content. Immediately know

when important files have been altered or when key files such as 'virus definition' files are not being updated in a timely manner

4) WINDOWS COUNTER WATCH

Real-time monitoring of select, key windows system counters for exceeding selected thresholds indicative of suspicious activity, including Counters for:

- * IIS
- * Exchange
- * SQL Server
- * ISA
- * Memory
- * Processor
- * Performance Counters for system operation

5) PROCESS WATCH

Real-time monitoring of all or select running processes for key conditions:

- * Process should be running or should not be running; start process that should be running, and terminate those that should not be running
- * Watch for and terminate 'worms' and other malicious processes

6) WINSERVICES WATCH

Real-time monitoring of select, key system and application services that should be running including anti-virus and other key services. Automatically starts, restarts and stop services.

7) CUSTOM WATCH

Create your own custom intrusion-detection programs, scripts, command, or batch files:

- * They will be executed periodically on any scheduled basis you define
- * Fully integrated with alerting and reporting system.

8) SNMP TRAP & COUNTER WATCH

Real-time monitoring of select Trap messages from your network devices indicating suspicious, unauthorized, or performance related activities. Real-time, proactive SNMP Query monitoring of select SNMP Counter variables from your network devices indicating suspicious, unauthorized, or performance related activities.

9)SYSLOG WATCH

Real-time monitoring of select SYSLOG messages from your network devices and Unix/Linux systems indicating suspicious, unauthorized, or performance related activities.

All 9 Modules use the Database and Reporting features and also have complete access to Sentry II valuable enterprise wide features.

Internet explorer based Console available across entire enterprise makes SENTRY II flexible; easy to use and always available.

Generate any combination of **rules and set a precedence** on which rules are most important for notifications.

Create **Corrective action** notifications. For frequent issues or junior staff corrective action notification are created to eliminate non-productive time.

Graph and Charting Wizard lets you save and create graph templates for historical trending and analysis. Any item that SENTRY II monitors or reports on can be utilized as an input to a Chart or Graph letting you quickly view unusual activity on your Servers.

Security Options in SENTRY II provides complete control over you has access to what information. You can define authorized Users, with different security and rights to access and use the various SENTRY II features.

The easiest way to adhere to security regulations is to create automated processes for compliance. If your organization is required to comply with IT monitoring for security regulations you must implement a tool for Event Log Management and automatic Server monitoring. Engagent SENTRY II solution is easy to implement and configure.