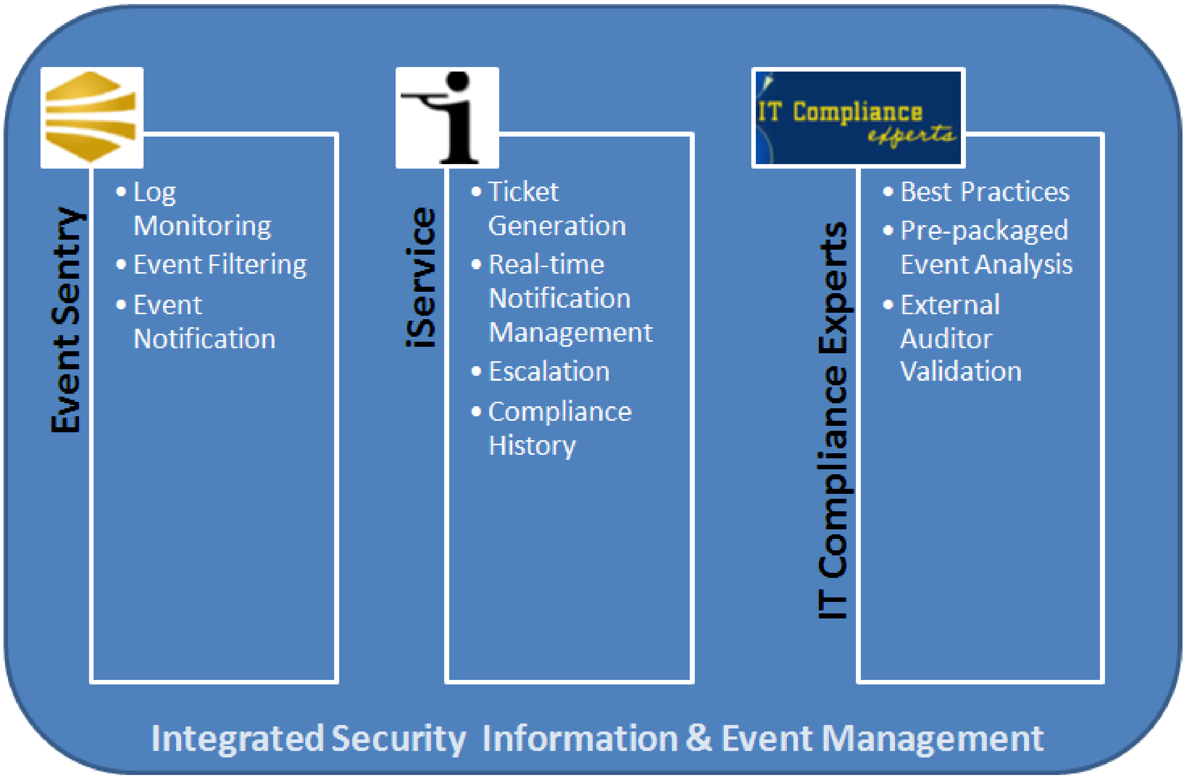
Security Information & Event Management – A Best Practices Approach

Implementing a best-of-class IT compliance framework using iService® help desk and EventSentry monitoring software



Event Sentry

- Log Monitoring
- Event Filtering
- Event Notification

iService

- Ticket Generation
- Real-time Notification Management
- Escalation
- Compliance History

IT Compliance Experts

- Best Practices
- Pre-packaged Event Analysis
- External Auditor Validation

Integrated Security Information & Event Management

A white paper written by Scott E. Whitsitt based on real-world experience.

Table of Contents

Overview

Compliance with the many requirements of Sarbanes-Oxley, HIPAA, PCI and other regulations is a daunting task for most IT organizations. IT Compliance Experts has undertaken a project in connection with two leading software products, iService and EventSentry, to greatly simplify the process for companies subject to these regulations, or any organization interested in improving security and uptime.

The importance of event logs and monitoring

Your critical information systems leave a bread crumb trail in the form of logs that provide insight into how your systems are being used. These logs can tell you if someone is attempting to gain unauthorized access, a new user has been added to your network, and a variety of other critical events. Reviewing these logs is an important part of most organization's IT compliance strategy, but a manual review process is not feasible because of the overwhelming amount of data produced.

Event monitoring solutions, like EventSentry, have been developed to streamline and automate this important task. These solutions provide the ability to monitor event logs, syslogs, services, system performance, and network devices in real-time. They provide the ability to notify your security and network team so they can take the appropriate action, and archive information for future use.

Going beyond monitoring solutions

An effective compliance framework must go beyond event and system monitoring. It requires fine tuning the types of events monitored and documenting the actions taken. Many organizations utilize the notification processes provided by log monitoring software, but discover during their first audit that they don't have evidence of how the events were resolved.

> “Many organizations utilize the notification processes provided by log monitoring software, but discover during their first IT compliance audit that they don't have evidence of how the events were resolved. “

IT Compliance Experts has partnered with a leading monitoring solution (EventSentry) and a leading help desk system (iService®), to provide a truly integrated solution for this monitoring and compliance dilemma. When required, important events automatically create support tickets within iService for immediate review. Less urgent events are archived in a database for reporting and future reference.

An out of the box solution

Windows event logs contain hundreds of event types and can be difficult to analyze. We've identified the key events and determined whether they need real-time notification and documented follow-up, periodic reporting, or can be archived for future use. Notifications include plain English descriptions of what happened along with the action that should be taken. We've even prewritten the responses your auditors will expect for many of the most common events, and they can be accessed by your IT staff with a single click in the iService system.

The result is a solution that can be quickly deployed, makes your IT organization more responsive and efficient, and helps ensure compliance with key regulations at reduced effort. And, it's available at an affordable price and is easily implemented.

Aligning events with processes

One of the most important aspects of implementing a monitoring solution is ensuring that it's properly aligned with your security strategy and business processes. Focusing on the highest risk processes will help ensure the success of your solution. There are several steps that you should follow to achieve this alignment and ensure a risk-based approach is followed.

Identify key control procedures and processes

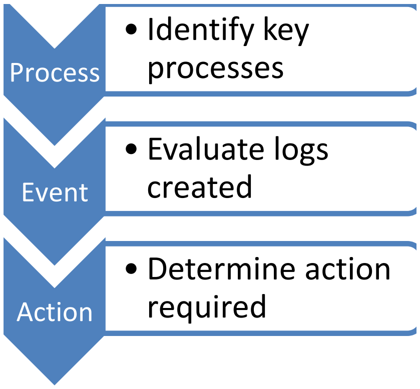
The number of events generated by Windows servers, firewalls, and other devices can be staggering. As a result, one of the most common questions we hear is "What events should we be monitoring?" Only a subset of control procedures end up generating Windows event logs. So your first step is to identify your key control procedures and processes that are directly related to Windows or other system events.

While there are many events that can be monitored and provide interesting insight, it's critical to limit notifications to those that are mission-critical. Limiting your focus to those control procedures considered "key" will help ensure you are focused on the highest risk areas.

Map processes to events

After years of designing and evaluating control environments, we've identified a subset of events that directly support the most common control procedures followed by IT organizations. These events tend to align very well with the processes and procedures used to manage changes to systems, logical access to systems, and operational activities such as system backups.

For example, your IT organization likely has a control to ensure that all new user accounts are authorized. When you add a new user to your Windows domain, an event is written to the Windows security log documenting this action. To align your monitoring with these processes, you need to analyze the business processes that are key and map them back to the events that are logged.



Analyze events

After you have identified your key control procedures and processes and identified the various Windows events available, you will need to do some detailed analysis. For example, you need to identify those events that require real-time notification and then find a way to document the action for each of these events. If you already have a robust help desk solution in place, you might consider integrating it with your log monitoring system. You will also need to filter on various details within the events themselves.

This type of analysis can be very time-consuming, and requires staff that have detailed knowledge of Windows event logs and IT control processes. But, it is critical to the overall effectiveness of your solution.

The IT Compliance Experts solution

A packaged but adaptable solution

Based upon years of experience with the EventSentry monitoring software and iService help desk system, we've developed a prepackaged solution that is adaptable to nearly any enterprise. Our framework was created by identifying common control procedures and activities that generate system events. Then, the corresponding events were analyzed to determine the exact specification for the EventSentry monitoring solution.

These events were further divided into those that require documented action, versus those that simply need to be retained for forensic purposes. For example, you might generate an iService ticket for investigation when a new account is created, but only log account deletions to the EventSentry database without generating a help desk ticket.

Map your procedures to our framework

Our framework includes a set of expected key controls that can be easily mapped to your existing control methodology or procedure documents. After a simple mapping of your procedures to our matrix, you'll find a set of events and filter definitions ready to use within the EventSentry and iService applications.

This saves you many hours of required analysis and helps ensure that you are monitoring the highest value events. The preconfigured EventSentry monitoring package and iService configuration ensure you will have an effective process from day one.

Generate actionable real-time notifications

Monitoring your network is only one small part of your IT governance requirements. When important events are identified, you need to ensure the right people now about it, and produce evidence that corrective action was taken. EventSentry includes an HTTP action that streamlines this process by creating tickets directly within iService over an https encrypted connection to iService web services. This is very important for multi-location environments, because sending user login details and other event notices via email can compromise your security.

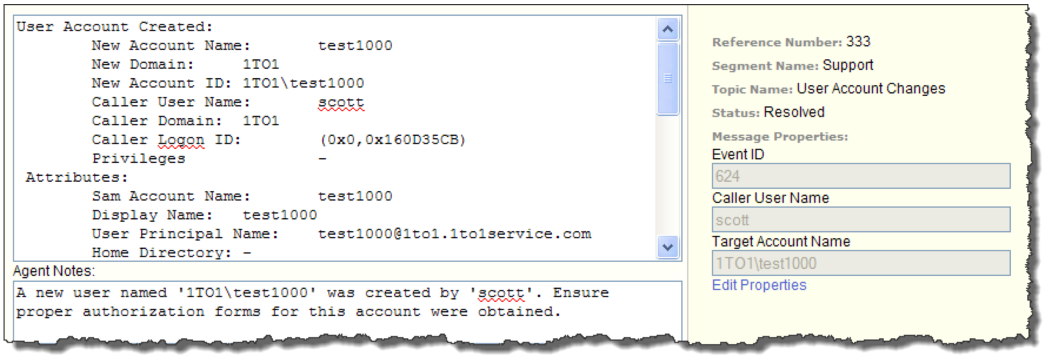
> “EventSentry includes an HTTP action that creates tickets directly within iService populated with key information such as the server or workstation that generated the notification.“

iService tickets are populated with key information such as the server or workstation that generated the notification, the user that initiated the action, and even descriptive notes telling the recipient of the ticket in plain English what needs to be done. Your IT staff can receive email notifications from iService when events occur, and management can be alerted via escalation rules if events are unresolved after a predetermined service level.

An Example – New Account Created

For example, most IT organizations have a control procedure that states “All new Windows user accounts are authorized.” This control will align with EventSentry filters and actions for Windows event 624 (Windows 2003), which is generated each time you create a new account within Microsoft Active Directory.

EventSentry selects these events as they occur, and a predefined action generates tickets within the iService system. As show below, the result is a user-friendly notification that any of your help desk representatives will understand.



```
User Account Created:
        New Account Name:       test1000
        New Domain:     1TO1
        New Account ID: 1TO1\test1000
        Caller User Name:       scott
        Caller Domain:  1TO1
        Caller Logon ID:        (0x0,0x160D35CB)
        Privileges              -
 Attributes:
        Sam Account Name:       test1000
        Display Name:   test1000
        User Principal Name:    test1000@1to1.1to1service.com
        Home Directory: -
```

Agent Notes:

```
A new user named '1TO1\test1000' was created by 'scott'. Ensure
proper authorization forms for this account were obtained.
```

Reference Number: 333

Segment Name: Support

Topic Name: User Account Changes

Status: Resolved

Message Properties:

Event ID: 624

Caller User Name: scott

Target Account Name: 1TO1\test1000

When the ticket is created, the appropriate members of your team can be notified and prompted to ensure proper authorization was obtained. To close out the ticket, a pre-written response can be used to document the investigation with a single mouse click.

Reduce noise and false positives

Some actions, such as creating a new account in Microsoft Active Directory, create multiple events in the Windows security log. Some of these events contain no useful information and end up being false positives that can be ignored. However, in order to identify these events you must evaluate various aspects of the event details.

In order to identify this event log noise, you need to understand how Windows events are built. Each event is based on a predefined template that is made up of different string values. These string values define various aspects of the action that took place, such as the user that initiated the action or the account that was affected.

By analyzing the details of these events we can identify those that do not require any action. In collaboration with EventSentry and iService, we performed this analysis and developed prepackaged filters that will save you a significant amount of time.

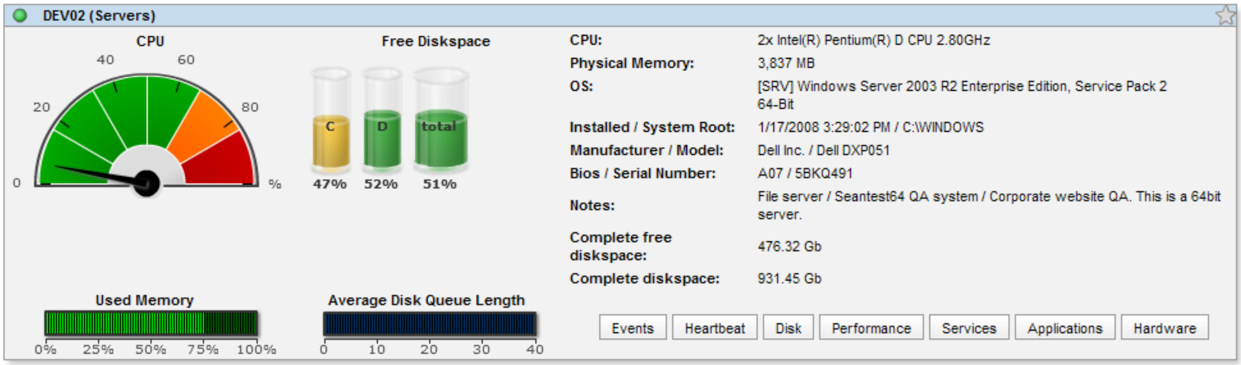
An event mapping sample for key controls

The table below includes a few of the more important control procedures and related Windows events.

Business Event	Business process that can be managed within iService	Windows event IDs (W2003 / W2008)	Suggested action (All events are archived)
Login occurs with an account that has privileged access and should only be used in conjunction with an approved project.	An iService help desk request should be logged documenting the permission to use the account.	528 / 4624	Real-time notification via a ticket in iService that can be matched to the approved permission request.
Rights are added to an existing account, such as adding an account to the administrators groups.	An iService help desk request should be logged documenting approval for the new access rights.	632 / 4728 (Global) 636 / 4732 (Local) 660 / 4756 (Universal)	Real-time notification via a ticket in iService that can be matched to the approved access request.
A new account is created on the Windows network.	An iService help desk request should be logged documenting approval for the new account.	624 / 4720	Real-time notification via a ticket in iService that can be matched to the approved access request.
An account is deleted from Windows Active Directory.	These are usually accounts that have been dormant and previously disabled, or are related to a user termination. An iService ticket should be created to document the account deletion.	630 / 4726	No need for real-time notification. Just archive to the EventSentry database for use during your audit.
A Windows account is disabled.	An iService help desk request should be logged for all user terminations with a requested date for removing access.	629 / 4725	No need for real-time notification. Just archive to the EventSentry database for use during your audit.
An account is locked out because of failed logon attempts.	There is no routine process associated with account lockouts.	644 / 4740	If the account has privileged access, real-time notification is justified. Otherwise, a daily report summarizing activity may be sufficient.
A Windows account that was disabled is re-enabled.	This is similar to a new account being created, and should be accompanied by an authorized user request in iService.	The body of 642 / 4738 must be filtered to identify disabled versus enabled accounts.	Real-time notification via a ticket in iService that can be matched to the approved access request for re-enabled accounts.

Incorporating operational issues

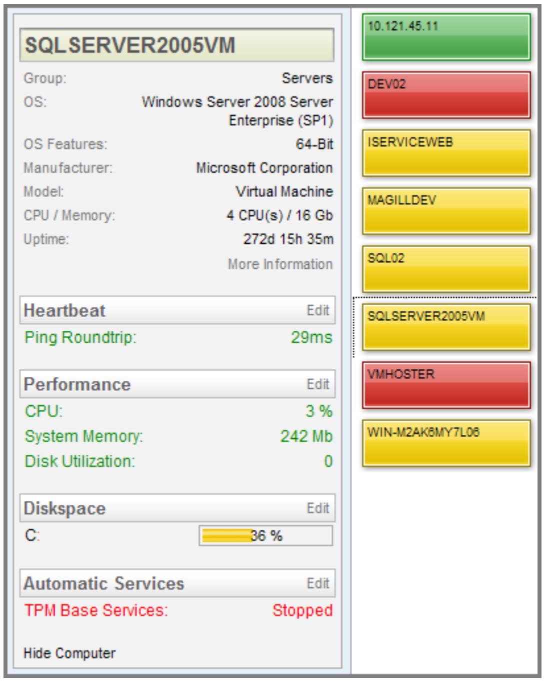
In addition to monitoring for security and IT compliance, most organizations leverage their monitoring solution to track important aspects of key servers and network devices. EventSentry includes the ability to monitor disk space, CPU and memory utilization, Windows services, files, applications, network devices, and most aspects of your IT environment.



DEV02 (Servers)

CPU:	2x Intel(R) Pentium(R) D CPU 2.80GHz
Physical Memory:	3,837 MB
OS:	[SRV] Windows Server 2003 R2 Enterprise Edition, Service Pack 2 64-Bit
Installed / System Root:	1/17/2008 3:29:02 PM / C:\WINDOWS
Manufacturer / Model:	Dell Inc. / Dell DXP051
Bios / Serial Number:	A07 / 5BKQ491
Notes:	File server / Seantest64 QA system / Corporate website QA. This is a 64bit server.
Complete free diskspace:	476.32 Gb
Complete diskspace:	931.45 Gb

Similar to the examples shown for security events, EventSentry can generate tickets directly within the iService help desk that contain important details about operational issues. For example, if the free disk space on a key server falls below a specified threshold EventSentry can generate a ticket in iService for immediate investigation.



SQLSERVER2005VM

Group:	Servers
OS:	Windows Server 2008 Server Enterprise (SP1)
OS Features:	64-Bit
Manufacturer:	Microsoft Corporation
Model:	Virtual Machine
CPU / Memory:	4 CPU(s) / 16 Gb
Uptime:	272d 15h 35m

Heartbeat

Ping Roundtrip:	29ms

Performance

CPU:	3 %
System Memory:	242 Mb
Disk Utilization:	0

Diskspace

C:	36 %

Automatic Services

TPM Base Services:	Stopped

The iService help desk system accepts input via HTTPS, which greatly simplifies integration with EventSentry. You can generate tickets for any operational issue and capture important information such as the computer affected, service that stopped, and other descriptive information. iService manages the real-time notifications to staff and can route the ticket to the appropriate member of your IT team based upon server, application, type of issue, or any aspect associated with the event.

About The Author

About the Author

Scott E. Whitsitt, founder of IT Compliance Experts, has over 25 years of experience with all aspects of IT governance. He has worked with executive management of numerous public companies to implement the requirements of Sarbanes-Oxley and HIPAA. IT Compliance Experts was formed to help organizations achieve a balance that ensures IT compliance while improving operating performance. Our goals as a service organization are:

- to provide people that understand the trade-off between a highly structured control environment and the realities of doing business; and
- to help clients continuously improve the effectiveness of their compliance projects and IT operations.

IT Compliance Experts is a division of One-to-One Service.com, Inc. You can learn more about the organization at www.ITComplianceExperts.com.

About iService and One-to-One Service.com, Inc.

One-to-One Service.com is a leading provider of web-based email management and workflow software (iService®) that is easy to implement and enhances each customer interaction. iService routes and manages customer inquiries, provides a powerful self-help web site, and captures a complete history of every customer interaction whether online or offline. iService is available as an on-demand or on-premise solution and is easily customizable to integrate with other applications.

Formed in 1997, One-to-One Service.com is a veteran in the email response management and eCRM industry. Located in Champaign, Illinois, One-to-One Service.com can be reached at 217.398.MAIL (6245) or on the Web at www.1to1service.com.

About EventSentry and Netikus.net, Ltd.

NETIKUS.NET is a privately held, growing software company located in the Chicago loop (US), which was founded in 2002. We develop commercial software, freeware software, and provide our customers with free tutorials and free online services such as myeventlog.com and our blog eventlogblog.com.

Our feature software product, EventSentry, originally released in 2001 under the name EventwatchNT, is a comprehensive and affordable event log and system monitoring solution that can be integrated into Unix networks. We are the only company that offers a true freeware event log monitoring solution with EventSentry Light, a stripped-down version of EventSentry. You can learn more about EventSentry at www.EventSentry.com.