Interested in learning more about security?

# SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

## Event Logs: Defining Their Purpose in Today's Network Security Environment

The purpose of this research topic is to identify the purpose of the event log in today's network security environment. This topic came about to solve an every day business problem. Simply, there is not enough time in the day to perform all security analyst tasks and adequately monitor all network security devices. However, expectations were that monitoring all components of network security is essential. It's the way things had been done and anything short of that may render a device or component of network security a...

Copyright SANS Institute

Author Retains Full Rights

AD

**Event Logs: Defining Their Purpose in Today's Network Security Environment**
Steve Meyer
August 16, 2001

**Overview**:

Network Security has changed significantly over the past years. Because of these changes, the role of an Information Security professional has also changed. There is now more and more data to monitor and analyze in order to detect the events of an internal employee, vendor, cracker, or seasoned hacker doing something to your data or systems. As network security has evolved the event logs and their capabilities in Windows NT and Windows 2000 have remained virtually unchanged.

The purpose of this research topic is to identify the purpose of the event log in today's network security environment. This topic came about to solve an every day business problem. Simply, there is not enough time in the day to perform all security analyst tasks and adequately monitor all network security devices. However, expectations were that monitoring all components of network security is essential. It's the way things had been done and anything short of that may render a device or component of network security as 'insecure'. It was clear that something must be done.

The event log was chosen because the event log with proper auditing turned on was once the staple of detecting entry into a computer system. A failed logon attempt may indicate an attempt to gain unauthorized access. A successful logon may reveal the identity of a wrong doer in the event an unauthorized activity occurs. In addition, time was already being spent monitoring the newer technologies including the intrusion detection systems, but the event logs were no longer being reviewed. They were just put on a shelf.

This topic is also relevant because more and more companies are implementing additional network security systems such as intrusion detection systems, network monitoring tools, host based intrusion detection systems, firewalls, and the list could go on and on. We are a very security conscious corporation that incorporated network security products aggressively. If we are struggling with monitoring, other smaller and newer companies must be as well. If the result of this research helps others make sense of monitoring and put it into perspective, it has been worth it.

I would like to begin by providing a brief overview of the event log - its function and limitations. From there, I would like to discuss some of the components of network security focusing on server monitoring. Finally, I will provide discuss network security, and then end with identified issues and solutions and finally a conclusion.

**Event Log**:

The event log consists of the system log, the security log, and the application log. They are called Sys.Event.Evt, SecEvent.Evt, and AppEvent.Evt respectively. They reside in the %systemroot%\system32\config folder. The purpose of the logs is to store information about

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

problems, performance, and most importantly security as defined in the account and audit policies. In a 4/4/99 article entitled 'The Event Logs', the logs were described as follows:

"System Log: The System Log contains events pertaining to NT's services and drivers. If a service hangs upon starting, it will be recorded in this log. In a networked setting, there will often be "browser" events in this log, as the machines on the network vote on who will maintain the browse list.

Security Log: When auditing is enabled, security events will be logged to the Security Log. Auditing is enabled via User Manager, printer properties, or file/folder properties. Administrator privileges are required to view the Security Log.

Application Log: The Application Log is used for events generated by applications. This log can grow quite large when certain applications such as SQL Server or Exchange are running.

Events will always be one of five types: Error, Warning, Information, Success Audit and Failure Audit (the last two in the Security Log)" [1]

As a Security Analyst, we have been most concerned with the security events such as successful logon (event 528), logon failure (event 529), and account locked out (event 539). A cumulative list of these and other Microsoft Event Ids can be found on Microsoft's website [2].

Reviewing these event logs without a third party tool is a lengthy and cumbersome process. It entails pulling up the event viewer and manually looking through each of the three logs for each server. This becomes repeated several times or hundreds of times depending upon the number of servers in your company and also based on the frequency of reviews. In addition, the events that you want to see are scattered in amongst many other events. This requires an additional search to find the events that you want to see. It is easy to see how this process may get put aside for more rewarding tasks to be completed.

**Network Security: A focus on Server Monitoring**

Securing a network has many variables. Password authentication, physical access, logical controls, patches, anti-virus, intrusion detection, firewalls, network monitoring, social engineering, and server hardening are just a few of the elements. The rules are different depending upon if your application is internal or if it goes on the web. Each of these variables has processes and procedures to follow. It may be a change management process to follow, an operating system to administer, and undoubtedly some will produce logs that will need reviewing.

A more in-depth example of one of these variables is the process of hardening a server before it is put on a network. Once a new server is brought in, it is configured in accordance to our information security policies. It is scanned for vulnerabilities, virus software is loaded, and current patches are applied. All this before the server is ready for placement on the network. One side note is that in addition to server hardening, servers are also scanned quarterly for vulnerabilities and also includes a process to correct these vulnerabilities.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Currently, the event viewer logs are only reviewed on a very limited basis. This was because a different group of people was responsible for reviewing logs and they were not assigned this task. The lesson is that the process should be placed with the group that is going to perform the task .

I have listed some of the key systems that make up a network security system. However, it would not be effective to define each because there are so many and it is not relevant for the defined research topic of how the event logs fit into this process.

**Issues Identified / Solutions recognized:**

Research indicates that one problem with network security is that it goes about things backwards. Many companies implement all their network security components and then figure out how to perform monitoring. In the Computer Security Journal article Attacks and Countermeasures: Managed Security Monitoring, Bruce Schneir suggests:

'Traditional approaches to computer security don't work. Despite decades of research and hundreds of available products, the Internet has steadily become more dangerous. The increased complexity of the Internet and applications, the rush to put more services and people on the Internet, and the desire to interconnect everything all contribute to the increased insecurity of the digital world" [3].

He continues to argue the historical security model of threat avoidance is flawed because they either successfully repel attackers, or they fail, leading to a fragile process. His solution is active network monitoring with an emphasis on a risk-managed model meaning heavier monitoring is placed on more valuable resources or assets. He also states that security monitoring is a key component missing in most networks.

"Companies see monitoring as something to do after their security products are in place. First they develop a security policy. Then they do a vulnerability analysis. Then they install a firewall, and maybe an intrusion detection system. And finally they think about monitoring. This makes no sense." [4]

One key difference in the view presented by Bruce Schneir is he defines security monitoring as real time systems and this would be provided by his company – a third party service. He does not discuss the monitoring of historical data such as the event ids captured in the event logs by the Microsoft operating system.

The article by Bruce Schneir gave me my first solution to my business problem. It had to do with his risk-managed model.

Our company does have a security policy for auditing and capturing historical events into the security logs and we will continue to do this. This is based on compliance to our Information Security safeguards. We know which servers are high risk in relation to the other servers, but they have not been identified formally. We will continue to gather event logs for all servers in

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

case they are needed, but we will only actively monitor and formally review those for the servers that have been identified by us to need active monitoring. For example, servers will be classified as low, moderate, or high risk. Only those classified as moderate or high will receive active monitoring.

In response to his argument that monitoring is performed too late was an eye opener. His solution is to begin monitoring early. Based on monitoring, decide what additional network security components are necessary. In an industry where bottom lines are critical and IT budgets are sacred, this is essential. The concept of monitoring first before purchasing additional products is critical. By not monitoring a log from the event viewer or emails from an intrusion detection system is similar to not having the product at all and most systems are very expensive.

Another issue identified through research is the limitations of the event log reporting capabilities. Many components of the network security environment have friendly graphical user interfaces and robust reporting capabilities. This is not the case in the event logs world. According to an article by Cory L. Scott:

"While Windows 2000 promises many changes in the Windows NT architecture, Microsoft is making very few changes to the event log and event monitoring components of the operating system. Since maintaining and dealing with Windows event logs can be a frustrating experience for most conscientious system administrators, this lack of improvement is disappointing. The Event Viewer, through the standard standalone application or through the Microsoft Management Console, is often not powerful enough to display just the right view of system activity that a system administrator needs. Witness the pop-up of an entire cottage industry of event log monitoring and analysis utilities – all which attempt to overcome the shortcomings of the immature alert technology built-in to Windows NT and the ability to aggregate and analyze multiple event logs." [5].

I agree and believe the argument by Cory L. Scott is the reason many event logs are not being reviewed. In my environment, a third party tool writes all event logs to a single database. Another tool is now needed to query and report back the results of the query. In our case it is Crystal Reports, yet another application that must be learned and mastered in order too more efficiently administer this process.

In this case, learning the additional application to better manage the event logs will be worth the investment. The benefits would be that the data would be written to one location and the Crystal Reports application could query the data and significantly reduce the time commitment of the Security Analyst.

One final issue that was brought up casually in the research is that of the human element. There is a human side to all of this network security and monitoring that must be considered. With the speed at which applications are being developed for the web, some are well secured and some are not. Likewise, no two people review the contents of the same log file equally. In addition, users of computer system like to play and some people do things they shouldn't, whether intentionally or not intentionally. Finally, our tasks as security professionals are not an exact science. We must ask questions and determine what type of environment we are working in.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Depending upon the answers, we can adjust our effort towards monitoring systems accordingly. I read a Microsoft Technet article that had a list of Ten Immutable Laws of Security that bring out the personal side of this issue:

The Ten Immutable Laws of Security [6]

- Law#1 If a bad guy can persuade you to run his program on your computer, it's not your computer anymore
- Law#2 If a bad guy can alter the operating system on your computer, it's not your computer anymore
- Law#3 If a bad guy has unrestricted physical access to your computer, it's not your computer anymore
- Law#4 If you allow a bad guy to upload programs to your web site, it's not your web site anymore
- Law#5 Weak passwords trump strong security
- Law#6 A machine is only as secure as the administrator is trustworthy
- Law#7 Encrypted data is only as secure as the decryption key
- Law#8 An out of date virus scanner is only marginally better than no virus scanner at all
- Law#9 Absolute anonymity isn't practical, in real life or on the web
- Law#10 Technology is not a panacea.

If you look at these laws which are fully explained on Microsoft's website, you see the reality of what we are trying to capture and review in the event logs and as part of the monitoring process. Even if your users are good people, they can do things that will give others access to the assets that you are trying to protect. It is our job to find these events whether intentional or not.

**Conclusion:**

Prior to research, I believed that event log reviews on all servers should be part of the network security equation. Also, each new security product should be fully integrated into the existing monitoring regime. You could not pick and choose security components to monitor because the omission of one aspect may lead you to an 'insecure' environment.

The event viewer and audit log security entries have their place. Reviewing this historical data may not foil the would-be attacker attempting to gain access to your resources. However, it may help identify the individual later. I like the idea of considering a risk model by adjusting the level of monitoring to the risk. Not all devices need monitoring and that is OK with the proper analysis, justification, and documentation some devices can and should be omitted.

In my opening to this research paper, I expressed a concern that the event logs and features to monitor the event logs have not kept up with other network monitoring systems. Better and better third party tools and utilities to overcome the shortcomings of the event viewer as a stand-alone product have alleviated this concern. It doesn't mean the event viewer is outdated or no longer useful. It has its place.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Monitoring should not be viewed as a necessary evil whether it is real time monitoring or historical monitoring such as the event logs. The security world is changing fast and as security professionals, we must be efficient, flexible, and willing to adapt. This means looking at the big picture. Be aware of the resources being protected, the products that are available for use, and the policies and processes being followed. Be willing to evaluate and change any of these at any time in order to stay as close to the good guy or bad guy who attempts to do something they shouldn't whether it is intentional or not. It will be a better place for us all.

**References:**


[1] Ludens, Douglas, The Event Logs, Focus on Windows 200/NT, 04/04/99
http://www.windowsnt.about.com/library/weekly/aa040499.htm

[2] Security Event Descriptions, Microsoft Support Services, United States, 09/09/01
http://support.microsoft.com/support/kb/articles/Q174/0/74.asp

[3] Schneier, Bruce, Managed Security Monitoring: Network Security for the 21st Century, Computer Security Journal, Computer Security Institute, Volume XVII, Number 2, 2001 p.1.

[4] Schneier, Bruce, Managed Security Monitoring: Network Security for the 21st Century, Computer Security Journal, Computer Security Institute, Volume XVII, Number 2, 2001 p.8.

[5] Scott, Corey L., Dealing with Windows NT Event Logs - Part 1., April 4, 2000.
http://www.securityfocus.com/frames/?focus=microsoft&content=/focus/microsoft/nt/log1.html

[6] The Ten Immutable Laws of Security, Microsoft TechNet
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/10imlaws.asp


© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: October 10th, 2015

# Upcoming SANS Training

**Click Here for a full list of all Upcoming SANS Events by Location**

| | | | |
|---|---|---|---|
| **SANS Tysons Corner 2015** | **Tysons Corner, VAUS** | **Oct 12, 2015 - Oct 17, 2015** | **Live Event** |
| **SANS Gulf Region 2015** | **Dubai, AE** | **Oct 17, 2015 - Oct 29, 2015** | **Live Event** |
| **SANS Cyber Defense San Diego 2015** | **San Diego, CAUS** | **Oct 19, 2015 - Oct 24, 2015** | **Live Event** |
| **SANS Tokyo Autumn 2015** | **Tokyo, JP** | **Oct 19, 2015 - Oct 31, 2015** | **Live Event** |
| **SANS Sydney 2015** | **Sydney, AU** | **Nov 09, 2015 - Nov 21, 2015** | **Live Event** |
| **SANS South Florida 2015** | **Fort Lauderdale, FLUS** | **Nov 09, 2015 - Nov 14, 2015** | **Live Event** |
| **SANS London 2015** | **London, GB** | **Nov 14, 2015 - Nov 23, 2015** | **Live Event** |
| **Pen Test Hackfest Summit & Training** | **Alexandria, VAUS** | **Nov 16, 2015 - Nov 23, 2015** | **Live Event** |
| **SANS Hyderabad 2015** | **Hyderabad, IN** | **Nov 24, 2015 - Dec 04, 2015** | **Live Event** |
| **SANS Cape Town 2015** | **Cape Town, ZA** | **Nov 30, 2015 - Dec 05, 2015** | **Live Event** |
| **SANS San Francisco 2015** | **San Francisco, CAUS** | **Nov 30, 2015 - Dec 05, 2015** | **Live Event** |
| **Security Leadership Summit & Training** | **Dallas, TXUS** | **Dec 03, 2015 - Dec 10, 2015** | **Live Event** |
| **SANS Cyber Defense Initiative 2015** | **Washington, DCUS** | **Dec 12, 2015 - Dec 19, 2015** | **Live Event** |
| **SANS Las Vegas 2016** | **Las Vegas, NVUS** | **Jan 09, 2016 - Jan 14, 2016** | **Live Event** |
| **SANS Dubai 2016** | **Dubai, AE** | **Jan 09, 2016 - Jan 14, 2016** | **Live Event** |
| **SOS: SANS October Singapore 2015** | **OnlineSG** | **Oct 12, 2015 - Oct 24, 2015** | **Live Event** |
| **SANS OnDemand** | **Books & MP3s OnlyUS** | **Anytime** | **Self Paced** |