Global Information Assurance Certification Paper

Event Management
Keeping Servers Secure with NetIQ's Security Manager

Matt Hrynkow

SANS Security Essential (GSEC) Practical Assignment
Version 1.4b
Option 1
March 22, 2004

Table of Contents

Introduction

One of the largest problems facing the security community today is event management. Companies face internal and external threats from a multitude of directions – viruses, denial-of-service attacks, unauthorized access, network penetrations, and badly configured devices are just scratching the surface. The high volume of events from devices/products designed to detect these kinds of conditions make it difficult for the security professional to effectively identify and respond to them in a timely manner. This situation creates an unsecure environment where security violations go unnoticed until it is too late or damage has been done.

NetIQ's Security Manager is a product designed to assist in managing the massive amounts of data and help make sense of it all. The features, architecture, user interfaces, reporting, and some practical examples are some of the topics to follow.

The Need for Event Management

Event management can be a daunting task. For a small network with 10 hosts, events can be generated at rates of thousands per hour. For a small company, this can mean the difference between having a small staff utilizing a product like Security Manager and employing a larger staff going over these logs and events inefficiently. A possible third option is not managing these important events at all thus having little idea as to possible intrusions or bad security practices. Obviously a choice needs to be made, either consciously, or by inaction.

Today's Internet is a global community. To do daily business, and often to retain employees, companies must be connected in some way to this network. Doing so exposes them to obvious interaction with systems outside of their control. This opens the door to viruses, hackers, loss of data, and downtime. There are also security issues that originate from "inside" the managed environment. According to the 2003 CSI/FBI report on Computer Crime and Security Survey, unauthorized insider security breaches and policy violations has continued to be a huge problem[1]. Clearly "looking the other way" when it comes to event monitoring is not a realistic answer.

NetIQ's Security Manager Overview

Security Manger assists in the management of logged events from multiple security products and devices. It provides real-time monitoring, event correlation,

[1] Richardson, Robert. "2003 CSI/FBI Computer Crime and Security Survey". 2003. URL: http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2003.pdf (Feb 27, 2004). 6-7.

automated reactions to events, and reporting through a central console. The product provides central log consolidation from multiple vendors, host-intrusion detection capabilities, firewall monitoring, IDS monitoring, anti-virus monitoring, and many popular vulnerability scanners (ISS and Nessus).

Security Manager Features[2]

Security Manager provides the following functions:

- Centralizes events and management of multiple products and vendors.
- Real-time monitoring of events.
- Provides reliable, secure transfer of events from the device, to the central repository.
- Provides a built-in set of rules that can be used to jump-start security for many types of equipment.
- Ensures audit reporting and ability to provide reports to outside auditors.
- Enables complete reporting of all security related events.

Security Manager Plug-ins

- Log Manager – Real-time monitoring of specific event in any log on a device.
- Host Intrusion Detector – Real-time monitoring of potential security breaches or violations of company policy.
- Firewall Monitor – Real-time analysis of many major vendors' firewall product logs.
- IDS Monitor - Real-time analysis of many major vendors' IDS product logs.
- ISS RealSecure – Bring in events from ISS to provide correlative analysis.
- Antivirus Monitor – Real-time analysis of leading anti-virus products' virus detections logs.
- Nessus/Security Analyzer – Log filter to go through Nessus logs and Security Manager logs for security problems or violations of company policy related to network devices.
- Tripwire for Windows 2000
- Secure Computing's Sidewinder

Security Manager Architecture

Security Managers architecture is designed to be configurable and scalable. The four major components are the **Agent**, **Consolidator**, **Database Access Server**, and the **Database** (Figure 1[3]).

[2] NetIQ Corporation. "Catalog of Modules". URL: http://www.netiq.com/products/sm/packs.asp (Feb 26, 2004).

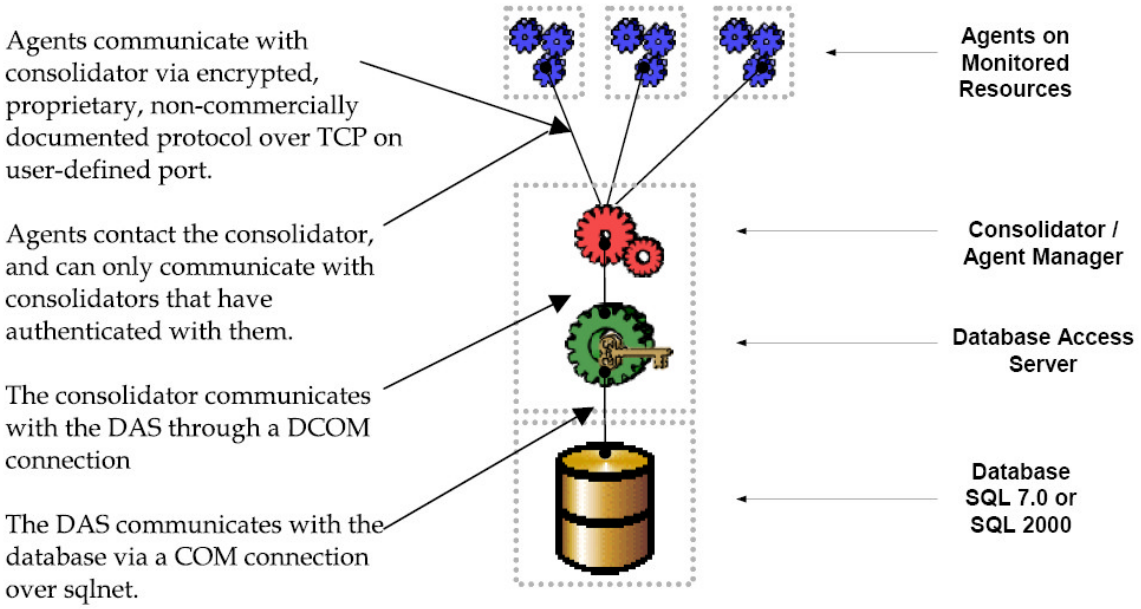


Figure 1

The agent runs on any Microsoft Windows computer running on the Intel platform. The service (OnePoint) contains a copy of the current rules, and is responsible for determining whether a new event matches any rules. New events come from a variety of methods, including flat files, NT event logs, SNMP traps, and SYSLOG messages. If an event matches a rule, then an alert is generated, and both items are sent to the consolidator. Events that do not match alerts are stored on the agent, combined with other events and sent up to the consolidator at configurable times.

The consolidator's primary job is receiving new events from the agents, and making sure the agents have the most recent copy of the rules. The consolidator is also responsible for installing/uninstalling agents and running self-maintenance/monitoring jobs as well.

The database access server (DAS), which is built on the Microsoft Transaction Server (MTS), is a shim between the consolidator, and the actual database. It also handles security for the Security Manager product via security groups on the local server.

The database can be any Microsoft SQL server higher than version 7.0. The database can handle millions of event a day, or hundreds of transactions a

[3] NetIQ Corporation. "Securing the Enterprise with NetIQ Security Manager". URL: http://download.netiq.com/CMS/Securing_the_Enterprise_with_NetIQ_Security_Manager.pdf (March 18, 2004).

second depending on the hardware. The product provides self-maintenance jobs to groom old data out and perform reindexing of the data.

Agents are deployed automatically via a rule set of managed computers. Rules can be very generic, or can be very explicit as in an individual domain and machine name.

Some minor active directory configurations need to happen as well. Since the agent collects information from the event logs, it is prudent that auditing of all the appropriate events is enabled, generally for both successes and failures. This action is usually configured in the **default domain controller policy**, and the **default domain policy** in your active directory. The following are excellent resources for configuring your policies correctly:

- Enable and Apply Security Auditing in Windows 2000 - http://support.microsoft.com/default.aspx?scid=kb;EN-US;300549
- Enabling Local Auditing Policies on Windows 2000 - http://support.microsoft.com/default.aspx?scid=kb;EN-US;252412
- Securing a Windows 2000 Domain Using Group Policies and The Security Configuration and Analysis MMC Snap-In - http://www.giac.org/practical/perry_Pierce_GCNT.doc

Auditing successes also assists with "recreating" an event, ensuring that all the appropriate information is available. All domain controllers need to be managed computers. It is through these "gatekeepers" that the majority of events will be generated. All domain level access goes through a domain controller at one time or another.

Starting with version 4.5 of Security Manager, communication between the agent and the consolidator can be configured to require encryption. These transmissions are encrypted via a 1024-bit key pair. All consolidators share a private key, so agents can talk effectively with more than one consolidator using one public key. Agents also have a private key that the public key is stored for in the database, usually shared by all consolidators.

Utilizing this communication, all events and alerts are transmitted in real-time (or close to it) from the agent to the consolidator. Even before logs can be cleared, events and alerts have already been sent away from the local machine providing an untainted account of events for later analysis offline.

Security Manager Consoles

A single console rolls all the events into a customizable screen, or one of two different MMC based consoles. There is also a highly adaptable web interface for monitoring events, data, and reports. This allows the security professional to

cross reference events across different systems and devices. One example of this is an attack to gain access to a list of servers. The servers all are configured with a Security Manager agent on it, and has the default rule set enabled. A cursory scan of the server will trip a Security Event 529 in the Windows Security log unless a good userID/password combination is used. Generally when a connection is made, the current logged in account credentials are used. A person attempting to gain unauthorized access generally will not have a valid account and will be using a brute force attack on local/domain accounts, or be attempting various common combinations or userID/passwords.

The agent will see this new event and immediately send (securely) it to the consolidator where various alerting is set up to alert the appropriate parties. In this way a security professional can see attempts made on a number of machines or multiple login attempts simultaneously in the Security Manager console. One such even looks like this:

The details look like this:

```
Configuration: COMPANYCONFIG1
Database:      DATABASESERVER1

Alert ID:      {C95C9C40-779B-426D-A21B-60813A1197A0}
Severity:      Security Breach
State:         New
Source:        Security Detect Multiple Logon Violations
Name:          Security: Logon: Failure (all): Alert on
Security Detect Multiple Logon Violations Script Event 5002
Description:    More than 8 violations from the same
workstation: CLIENTMACHINE1 within 5 minutes
 More than 8 violations from the same user: genericuserID
within 5 minutes

Domain:        DOMAIN1
Computer:      SERVER1
Time:          2/2/2004 7:50:01 PM
Owner:
Repeat Count:  0

Events

Type:          Warning
Time:          2/2/2004 7:50:00 PM
Computer:      NETIQSERVER
Provider Name: Script-generated Data
```

```
Source:         Security Detect Multiple Logon Violations
Event ID:       5002
Description:     More than 8 violations from the same
workstation: CLIENTMACHINE1 within 5 minutes
```

This event describes a user, genericuserID, logging in from a machine called CLIENTMACHINE1 multiple times (8) in the last five minutes. There are similar events generated depending on the severity of the user account. If this had been an administrator account on SERVER1, then on the first attempt (configurable) an alert would have been generated and the appropriate people could have reacted in an appropriate and timely manner.

There are four main consoles in the Security Manager product: the **Development Console**, **Monitor Console**, **Web Console** and the **Incident Management Console (IMC)**.

The Development Console is primarily used for system configuration, managing rules, managing computer groups, notification groups, and configuring the many information providers that the Security Manager product supports.

The Monitor Console allows access to the vast amount of information gathered in predefined views. There are views for Anti-Virus, Firewalls, Intrusion Detection Systems, Host Intrusion Detectors, Log Managers, and a view for monitoring the product itself. It is easy to create custom views via a wizard. An example view is a screen to see all logins for a specific person, or possibly from a specific machine. These new custom views can be done quickly and effectively.

The Web Console is a highly modular view of various events and charts. It is blocked out into ten panes that different information can be loaded into. Login violations can be located in one pane, attacks detected from your PIX on another, on the third domain controller events, and a fourth can display a list of computer health statistics. It is possible to access previously run reports in HTML format, old events, alerts, performance data, and the knowledge base.

The Incident Management Console (IMC) is generally used to update specific events with a new status, new information for the built in knowledge base (kept up to date for specific events/incidents), or assigning to personnel. The same views in the Monitor Console are available in the IMC as well, but cannot be configured there. To create new views, the view must first be set up in the Monitor Console, it will then display in the IMC.

Most of the time, security personnel will make use of either the Incident Management Console or the Monitor Console. Administrative staff will spend the majority of their time in the Development Console.

Security Manager Rules and Reports

Many different products do what Security Manager's base product does, consolidate events. The real benefit for the security personnel is the extensive rules and knowledge base built into the log managers.

There are currently over 1,400 rules that can be imported, or exist in the base product. These rules govern the behavior of the event as it goes through the system. Based on these rules, an event can trigger a script, an electronic page, or simply an alert on the central console screen. Examples of scripts that can be triggered include the following:

- Clear an event log.
- Disable a user account.
- Force a reboot.
- Force a logout.
- Restart a service.

Many of these scripts can be used to effectively secure, and enforce company policies.

For instance, assume that accounts that start with an "!" are classified as service accounts. These accounts are never to be logged in interactively by a user, and only to be used in running a service on a server. There is an out-of-the-box rule that watches the Windows security log for events from a source of Security, with an event ID of 528[4]. It must also be interactive so line 4 of the event must be logon type 2[5]. If these conditions are met, then the service runs a script to simply log the user out. Of course this happens within a fraction of a second, and the user simply cannot login with an account of this type. An alert is also generated giving the appropriate information from the event so action can be taken if the circumstances dictate. This rule is easily modified for other naming conventions that an organization might already have in place.

Other out-of-the-box rules are:

- Local administrators logging in.
- High sustained CPU utilization detected (possible DOS attack).
- Insecure settings for SNMP community strings.
- User logon attempt outside of authorized logon times.
- Failed Administrator account logon.
- User account lockouts.
- Unauthorized or harmful processes running (example, password hacking tools).

---

[4] Microsoft Knowledge Base. "Security Event for Associating Service Account Logon Events". October 2001. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;274176 (Feb 26, 2004).
[5] Microsoft Knowledge Base. "Distinguishing Windows NT Audit Event Records". May 2003. URL: http://support.microsoft.com:80/support/kb/articles/Q140/7/14.asp (Feb 26, 2004).

- Common backdoor port detected open on machine (For instance, NetBus uses TCP 12345)
- Clearing of event logs.

There are also a multitude of reports available via an MS Access front end. Some examples include:

- User logon/logoffs.
- Logon violations in 24 hours.
- Changes to security groups.
- New computer/user accounts.
- Most common events.
- Most common alerts.

New reports can be generated using a simple wizard or using general Microsoft Access knowledge.

Practical Examples

VPN Monitoring

Consider a company named Widget International (WI) that has a VPN setup that uses RADIUS to authenticate users. WI has a significant existing active directory that holds all their employee data and they would like to leverage. A simple security groups is created that authorized VPN users are added to. They decide to use Microsoft's Internet Authentication Service (IAS) since it integrates seamlessly with their existing infrastructure. The IAS server is configured to look for membership in this particular security group.

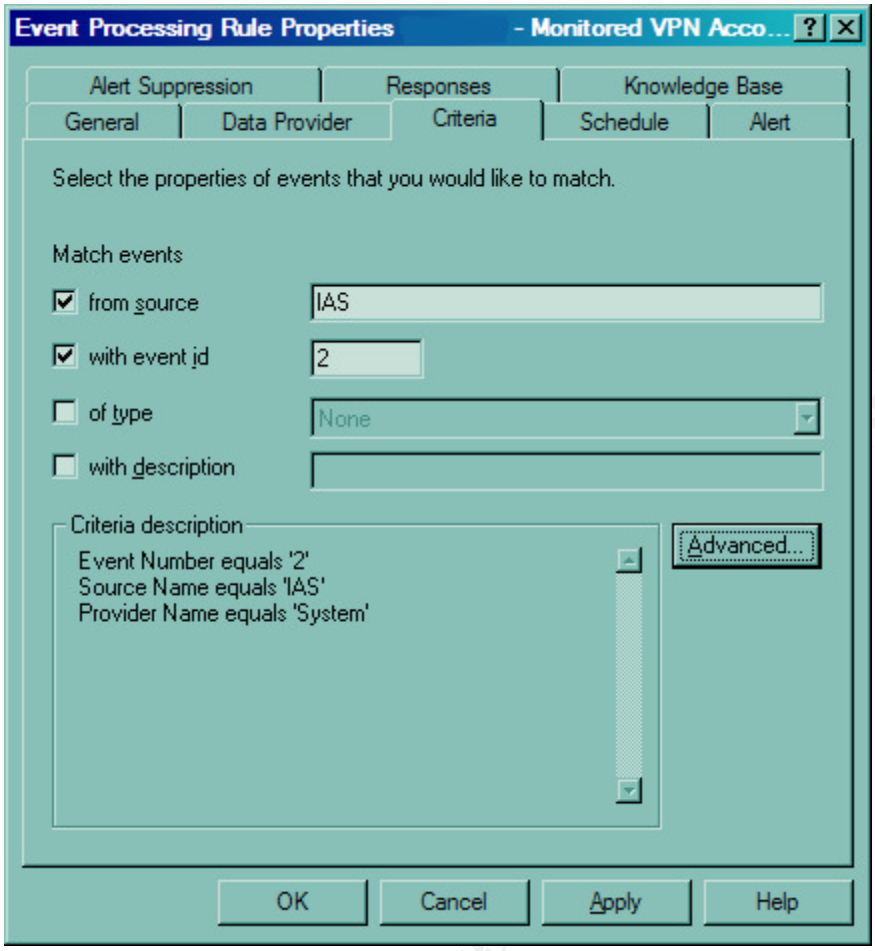
To audit this process, Security Manager can watch the logs of IAS for failures and successes. These events are all written to the windows system event log. Below is an example[6]:

```
Event Type: Warning
Event Source: IAS
Event Category: None
Event ID: 2
Date:  8/23/2001
Time:  11:30:39 AM
User:  N/A
Computer: PERLE-NLHM5IKIP
Description:
User cyung was denied access.
```

[6] Perle Corporation. "Windows Internet Authentication Service". 12/3/2003 1:00:22 PM. URL: http://www.help.perle.com/index.asp?a=4&q=23 (Feb 27, 2004).

```
 Fully-Qualified-User-Name = W2K\cyung
 NAS-IP-Address =
 NAS-Identifier = PTAC 833AS
 Called-Station-Identifier =
 Calling-Station-Identifier =
 Client-Friendly-Name = 833AS
 Client-IP-Address = 172.1.1.1
 NAS-Port-Type = Async
 NAS-Port = 23
 Policy-Name =
 Authentication-Type =
 EAP-Type =
 Reason-Code = 19
 Reason = The user could not be authenticated using
Challenge Handshake Authentication Protocol (CHAP). A
reversibly encrypted password does not exist for this user
account.
```

This event was generated by a user, *cyung*, being denied access. This event is generated when a bad password is entered, the user does not exist, the user ID is locked out, or the user is not in the "authorized" security group. All these condition cause the IAS server to deny access, and thus not allowing the user into the VPN. A similar event with an Event ID: 1 is logged for a successful authentication. Both of these events can be captured for review and archived via a simple Security Manager rule. Below is a sample rule that will match all denies logged from IAS.



Alerts can be generated when this rule is matched that are useful for identifying everything from simple user problems, to a brute force attack against the VPN concentrator. Reports can also be created charting failures against time.

Obviously, this is a very configurable application in the hands of a security professional.

Built in Active Directory Group Monitoring

Suppose management wants to be alerted whenever someone is added, or removed from some of the various built-in groups in the company's active directory. These events are generally logged (again, given audit policies are in place) on the domain controller where the action took place.

A sample event looks like this from the security log on **domaincontroller1**:

```
Event Type:    Success Audit
Event Source:  Security
Event Category:     Account Management
Event ID: 636
```

```
Date:           3/3/2004
Time:           1:01:10 PM
User:           domainname\actionUserID
Computer: domaincontroller1
Description:
Security Enabled Local Group Member Added:
     Member Name:
CN=userID,OU=Users,DC=subdomain,DC=domainname,DC=com
     Member ID:     domainname\userID
     Target Account Name:     Account Operators
     Target Domain: Builtin
     Target Account ID:  BUILTIN\Account Operators
     Caller User Name:   actionUserID
     Caller Domain: domainname
     Caller Logon ID:    (0x0,0x167CE5E8)
     Privileges:    -
```

From this sample event, it is possible to set up an easy rule to scrub for it. The rule would simply look through the security logs for event ID 636 where the event type is **SuccessAudit** and parameter for **Target Domain** is **Builtin**.

In this way, Security Manager can watch all the logs on the domain controllers simultaneously. If the organization has many DCs, then this is a huge time saver.

This same procedure also works for local groups on any machine. If a person is added or removed from any local group, for instance, Administrators, then alerts can be generated to alert appropriate people.

Conclusion

This paper has just provided a taste of what NetIQ's Security Manager is capable of accomplishing. Other functions such as event correlation and forensics, given the time to correctly setup, can be a huge time-saver for reports and investigations. The product is flexible, scalable, and can be modified to meet multiple goals depending on the desired output. Security manager focuses on allowing the user to efficiently detect and prevent security attacks and makes a superior platform for event management.

More complete documentation, white papers, trials, and product tours can be found at http://www.netiq.com/products/sm[7].

[7] NetIQ. "Security Manager". http://www.netiq.com/products/sm (Feb 24, 2004).

References

Microsoft Knowledge Base. "Security Event for Associating Service Account Logon Events". October 2001. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;274176 (Feb 26, 2004).

Microsoft Knowledge Base. "Distinguishing Windows NT Audit Event Records". May 2003. URL: http://support.microsoft.com:80/support/kb/articles/Q140/7/14.asp (Feb 26, 2004).

NetIQ. "Security Manager". http://www.netiq.com/products/sm (Feb 24, 2004).

NetIQ Corporation. "Securing the Enterprise with NetIQ Security Manager". URL: http://download.netiq.com/CMS/Securing_the_Enterprise_with_NetIQ_Security_Manager.pdf (March 18, 2004).

Perle Corporation. "Windows Internet Authentication Service". 12/3/2003 1:00:22 PM. URL: http://www.help.perle.com/index.asp?a=4&q=23 (Feb 27, 2004).

Richardson, Robert. "2003 CSI/FBI Computer Crime and Security Survey". 2003. URL: http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2003.pdf (Feb 27, 2004).

Microsoft Knowledge Base. "HOWTO: Enabling Local Auditing Policies on Windows 2000". November 2003. URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;252412 (Feb 29, 2004).

Microsoft Knowledge Base. "HOW TO: Enable and Apply Security Auditing in Windows 2000". November 2003. URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;300549 (Feb 29, 2004).

Pierce, Perry L. "Securing a Windows 2000 Domain Using Group Policies and The Security Configuration and Analysis MMC Snap-In". No date known. URL: http://www.giac.org/practical/perry_Pierce_GCNT.doc (Feb 29, 2004).

NetIQ Corporation. "Catalog of Modules". URL: http://www.netiq.com/products/sm/packs.asp (Feb 26, 2004).