nox medical

Implementing Nox Medical Product in Security Policies

Contents

Background

The purpose of this memo is to outline how Nox Medical‘s products can be implemented in security policies within organizations. Security policies are implemented within most organizations and this document will help IT to understand how Nox Medical’s products impact their policies.

It is important that an organization must take a holistic view of implementing security policies and standards. Single products cannot make organizations compliant. Instead – they should fit within the realm of organization-wide policies.

Overview

Nox Medical develops and manufactures three products where patient information is stored. This is the **Nox T3 Sleep Recorder**, **Nox A1 PSG System**, **Noxturnal Software**. Below is a discussion on each product.

Nox Recorders

The Nox T3 and the Nox A1 (Nox Recorders) store patient data on the device. When a sleep study is prepared, there is patient demographic information (name etc.) stored on the Nox Recorder. The recorder stores the data in an encrypted form.

Nox C1 Access Point

The Nox C1 is a network access point which does not store any data.

Noxturnal

Noxturnal is the analysis software needed to view and score the physiological signals recorded with the Nox recorders.

The Noxturnal software does not store any patient information. The software allows access to files which store patient information. Access and audit trail to these files is controlled through normal operating system controls, such as logins and passwords.

Configuration of Windows to Support Security Policies

Since the Noxturnal software is not a native database, users can configure Windows to know who has accessed and changed patient information. This is done through the organization‘s security policy and Windows Domain Controller. Below is an outline of how to configure the organization‘s Domain Controller to create a solution for this purpose.

General Requirements

The organization must implement a security policy. The contents of such a security policy is beyond the scope of this document but readers can easily find samples of such policies with a simple Internet search

Key elements of such a policy are:

- No shared access, logins or passwords on any computer.
- Each user must have a unique login and secret password when working on a computer belonging to the organization.

- Properly configured Domain Controller to support the Account Policy and Audit Policy of the organization. This is to know who is logged in, who accesses which files and who changes files (and when).
- Properly backed up audit logs.

Configuring Windows

Given the key requirement that each user has their own login and password and no users share access to a computer, Windows can provide an audit trail on who accesses which information and who makes changes to it. This can be achieved in two main steps:

1.) Configure Windows to capture information on who accesses what information and changes it.
2.) Generate reports to provide this information when required.

More information here: https://blogs.technet.microsoft.com/mspfe/2013/08/26/auditing-file-access-on-file-servers/

This document contains instructions for either a Server based environment and also an environment which is not connected by servers, i.e. standalone workstation environment.

Overview of Configuration for Server Environments

1.) Download and unzip the files found on Nox Medical's website under "Implementing Nox Medical Products in Security Policies", including these instructions.
2.) Import the Windows Group Policy Object (GPO) from that file collection into an empty GPO object. The GPO is in Group Policy Backup Format.
3.) Set File Auditing Access Control Lists (ACLs) on the folder file share where you keep your recordings.
4.) Schedule a task to run the PowerShell reporting script once daily.

By implementing these instructions, System Administrators will be able to collect logs for all access to sleep recordings collected by Noxturnal and also provide reports on who has accessed which file.

1. Files Included in the ZIP file "Nox Security Helper Toolkit - Servers"

These are all the files included in the package found on Nox Medical's website.

1. NoxturnalFileAccess.htm - GPO Settings Report
2. NoxturnalFileGPO.zip - GPO Backup File (for importing on DC)
3. ReportNoxturnal.ps1 - Powershell Eventlog CSV reporting script
4. CreateTask.bat - Batch file to create a scheduled task automatically

2. Creating, Importing and Linking the GPO

These steps will import the GPO.

1. Unzip the included NoxturnalFileGPO.zip file to C:\ NoxturnalFileAccess on a Domain Controller
2. Open Group Policy Management
3. Create a new GPO named „NoxturnalFileAccess“ under Group Policy Objects
4. Right click the new GPO and select „Import Settings“
5. Enter „C:\ NoxturnalFileAccess“ as the Backup folder.
6. Link the GPO to the Fileserver OU location by draging the GPO on to the OU.
7. On the Fileserver Admin Command Prompt type: „gpupdate /force“

The GPO is now deployed.

3. Assigning File Audit Permissions to the Fileshare folder of Noxturnal

This folder is where you keep your sleep recordings

1. Right Click the Noxturnal Folder on the Fileserver -> Properties -> Security Tab -> Advanced -> Auditing Tab
2. Click Edit and Add "Everyone"

Add the following ACL with checkboxes checked

• List folder / read data:	Successful and Failed
• Create files / write data:	Successful and Failed
• Create folders / append data:	Successful and Failed
• Delete subfolder and files:	Successful and Failed
• Delete:	Successful and Failed

The File Audit ACL's are now set and Security EventLog is recording all file read and write access.

4. Adjust script configuration and setup Scheduled Task

- Unzip the ReportNoxturnal.ps1 script file and CreateTask.bat to C:\ NoxturnalFileAccess folder on the File Server from the Nox Security Helper Toolkit.zip file
- Edit the C:\NoxturnalFileAccess\ReportNoxturnal.ps1 and set/unset the $server variable. If running the script on the fileserver $server should be unset.
- Choose and set the $CSVFile variable with a path and filename to the desired CSV file.

The script is now ready to process the File Access Security Events in EventLog

5. Create a Scheduled Task

- Right click the CreateTask.bat and select „Run As Administrator“. This will create a task named „Noxturnal File Auditing“ and can be modified in Task Scheduler to run at the desired hour of day.

The CSV File will now append file access data once daily for later processing with Excel or SQL database.

Overview of Configuration for Standalone Workstations

1.) Download and unzip the files found on Nox Medical‘s website under "Implementing Nox Medical Products in Security Policies”, including these instructions.
2.) Enable Advanced Policies in Local Security Settings
3.) Import the Audit Policies with a CSV settings file.
4.) Set File Auditing Access Control Lists (ACLs) on the folder file share where you keep your recordings.
5.) Schedule a task to run the PowerShell reporting script once daily.

By implementing these instructions, System Administrators will be able to collect logs for all access to sleep recordings collected by Noxturnal and also provide reports on who has accessed which file.

1. Files Included in the ZIP file “Nox Security Helper Toolkit - Workstation”

These are all the files included in the package found on Nox Medical’s website.

1. NoxturnalFileAccess.htm – Local Security Settings Report
2. NoxturnalAudit.csv – Audit Policy Backup File (for importing on a standalone workstation).
3. ImportAuditPolicy.bat – Batch file to import Audit Policies from settings file.
4. ReportNoxturnal.ps1 - Powershell Eventlog CSV reporting script
5. CreateTask.bat - Batch file to create a scheduled task automatically

2. Edit Local Security Policy and Import Audit Policy From Settings File

1. Open Control Panel → Administrative Tools → Local Security Policy.
2. In Security Options under Local Policies open the “Audit: Audit: Force audit policy subcategory settings” and select “Enabled”.
3. Extract the included NoxturnalAudit.csv and ImportAuditPolicy.bat to C:\NoxturnalFileAccess folder.
4. Right click the ImportAuditPolicy.bat file and click “Run as Administrator”.

The Audit Policies have now been applied.

3. Assigning File Audit Permissions to the Noxturnal Data Folder

This folder is where you keep your sleep recordings

1. Right Click the Noxturnal Folder on the Fileserver -> Properties -> Security Tab -> Advanced -> Auditing Tab
2. Click Edit and Add "Everyone"

Add the following ACL with checkboxes checked

• List folder / read data:	Successful and Failed
• Create files / write data:	Successful and Failed
• Create folders / append data:	Successful and Failed
• Delete subfolder and files:	Successful and Failed
• Delete:	Successful and Failed

The File Audit ACL's are now set and Security EventLog is recording all file read and write access.

4. Adjust script configuration and setup Scheduled Task

- Unzip the ReportNoxturnal.ps1 script file and CreateTask.bat to C:\ NoxturnalFileAccess folder on the Workstation from the Nox Security Helper Toolkit - Workstation.zip file
- Edit the C:\NoxturnalFileAccess\ReportNoxturnal.ps1 and set/unset the $server variable. If running the script on the fileserver $server should be unset.
- Choose and set the $CSVFile variable with a path and filename to the desired CSV file.

  The script is now ready to process the File Access Security Events in EventLog

5. Create a Scheduled Task

- Right click the CreateTask.bat and select „Run As Administrator". This will create a task named „Noxturnal File Auditing" and can be modified in Task Scheduler to run at the desired hour of day.

  The CSV File will now append file access data once daily for later processing with Excel or SQL database.

Conclusion

Following the steps explained above, institutions using Noxturnal can more easily become compliant to the requirements set forth in different security policies.

For further information please visit www.noxmedical.com or send an e-mail to support@noxmedical.com