OKENA
71 Second Ave., 3rd Floor
Waltham, MA 02451

Phone 781 209 3200
Fax 781 209 3199

StormWatch™

Policy for Monitoring Mission Critical Systems Group

.

This document describes the policy shipped with the StormWatch Management Console which allows administrators to passively monitor and log modifications to critical system resources. Because this is only a monitoring tool, this policy can be used in combination with any other Sample policies.

Policy Name	Policy Description
Required Windows System Module	V2.1 policy module to allow critical Windows functions

Policy Description

This section contains descriptions of the rules included in the sample policies recommended for deployment on servers.

Required Windows System Module	V2.1 policy module to allow critical Windows functions

This policy allows administrators to passively monitor access to critical system resources.

NOTE: "Vulnerable applications" defined in various rules are network-aware applications. These application types are much more vulnerable than others. They are as follows:

- TCP and UDP servers and processes created by them are vulnerable because they are susceptible to buffer overflow attacks.
- Processes that read downloaded content are vulnerable because they may be interpreting and taking action based on downloaded data.
- Remote clients are applications running on another machine and are therefore vulnerable because StormWatch does not know what these applications are when they attempt to access resources.

The rules in this policy are as follows:

1. **File Access Control – Allow, All Applications, read System libraries, drivers and data files**

   This rule ensures that necessary applications can access system libraries and configuration files needed for startup purposes and other general operations.

2. **File Access Control – Ensure access to DOS command line**

   This rule ensures that the DOS prompt does not become a restricted application as a result of receiving a downloaded content designation.

3. **Network Access Control – Allow, MS Security applications, server for TCP and UDP services**

   This rule lets Microsoft's security subsystem communicate on the network, allowing for authentication and authorization services, e.g. Kerberos and LDAP.

4. **Network Access Control – Allow, All applications, server for TCP and UDP service from Local Host**

   This rule allows various applications running on the same system to talk to each other while still denying access to these services from other non-localhost applications. This improves system performance by allowing all local applications to attempt to access all needed local resources as a server.

5. **Network Access Control – Allow, MS Security applications, client for TCP and UDP services**

   This rule lets Microsoft's security subsystem communicate on the network, allowing for authentication and authorization services, e.g. Kerberos and LDAP.

6. **Network Access Control – Allow, All applications, client for basic services**

   This rule ensures that applications can perform functions such as name resolution and endpoint mapping.

7. **Network Access Control – Allow, All applications, server for basic services**

   This rule ensures that applications can act as a server for functions such as WINS and endpoint mapping.

8. **Network Access Control – Allow, All applications, client for TCP and UDP service to Local Host**

   This rule allows various applications running on the same system to talk to each other while still denying access to these services from other non-localhost applications. This improves system performance by allowing all local applications to attempt to access all needed local resources as a client.