RULES IN OKENA STORMWATCH

This is a list of all the RULE types we provide and within each rule type, the customizations/settings. These rules can be adjusted to the needs of the corporate environment and then combined into POLICIES, which can then be added to GROUPS. The HOSTS (your Agents) can be associated with these GROUPS, which will then protect the Agents/hosts at the level that is appropriate.

Out of the box, Okena's StormWatch version 2.1 provides 124 pre-configured rules that can be modified, copied, or used as is. The number designation of the rules is simply an ID tag for the purposes of organization. For example, the first rule you create out of the box will be assigned number 125 because that is the 125th rule that has been created for the system.

TYPE OF RULES AND THEIR BASIC SETTINGS:

1. Application Access Control
    a. User selectable High Priority Deny, Allow, Query User (Default Allow), Query User (Default Deny), Deny.
    b. Any application OF YOUR CHOICE
    c. Attempt to run.
2. COM Component Access Control
    a. User selectable High Priority Deny, Allow, Query User (Default Allow), Query User (Default Deny), Deny.
    b. Any application OF YOUR CHOICE
    c. Attempt to access a COM component of YOUR CHOICE.
3. File Access Control
    a. User selectable High Priority Deny, Allow, Query User (Default Allow), Query User (Default Deny), Deny.
    b. Any application OF YOUR CHOICE
    c. Attempt to Read only or read and write
    d. To any files of YOUR CHOICE.
4. File Version Control
    a. User selectable High Priority Deny, Allow, Query User (Default Allow), Query User (Default Deny), Deny.
    b. When an execution of the following (user defined file)
    c. File version of your particular file.

    d. This is useful to only allow certain versions of applications to run. For example, only allow Word 2000 to run.
5. Network Access Control
    a. User selectable High Priority Deny, Allow, Query User (Default Allow), Query User (Default Deny), Deny.
    b. Any application OF YOUR CHOICE.
    c. Attempt to act as a server OR client (user definable)
    d. For a user-chosen network service (i.e. TCP, UDP, FTP, etc)
    e. Communicating with host addresses (user-definable IP address or range of addresses).
6. Registry Access Control
    a. User selectable High Priority Deny, Allow, Query User (Default Allow), Query User (Default Deny), Deny.
    b. Any application OF YOUR CHOICE.
    c. Attempt to write any of these registry entries (user-definable).
    d. This feature is used to protect the registry.
7. File Monitor
    a. Any application OF YOUR CHOICE
    b. Attempt to Read only or read and write
    c. Any files of YOUR CHOICE.
    d. This feature allows the administrator to see how often a file or files are accessed for auditing purposes.
8. Network Worm Protection
    a. This option can be turned either "on" of "off." Our heuristics finds possible network worm behavior and gives user option to terminate the worm propagation (recent worms: ILOVEYOU, Anna Kournikova).
9. NT Event Log
    a. One can write ANYTHING from the NT Event log into the StormWatch Management Console.
    b. One can place parameters on what one wants written to the StormWatch Management Console (i.e. security events only).
    c. One can choose severity of the NT event (i.e. information, warning, or error)
    d. One can choose Event Code of the NT Event Log
    e. This is useful so one does not have to check multiple logs or to see who has logged into the target machine.
10. Portscan Detection
    a. Port scanning is a common method for finding weaknesses at a site by determining what network services are being run. An attacker attempts to connect to port after port on a target system, mapping ports to identify network services and machine type vulnerabilities. Using portscan detection in a policy causes the intelligent agent on a protected system to log an event (one per minute) when an attempt is made to scan the system for an open port. The intelligent agent also gathers information on the number of different source IP addresses perpetrating the scan and it reveals the source address of the latest scan attempt. If you select the

Correlate network scans checkbox in the Global Event Correlation page when scans are detected across several machines, StormWatch correlates these events and generates an additional event to warn of this correlation.

11. Service Restart
    a. Use the Service restart rule to have the StormWatch Agent restart Windows NT services that have gone down on a system or are simply not responding to service requests.
    b. This is useful if, for example, your IIS services went down and no one was around to restart them manually.
12. Sniffer and Protocol Detection
    a. Use the StormWatch Sniffer and protocol detection rule to cause an event to be logged when non-IP protocols and packet sniffer programs are detected running on systems.
    b. Non-IP protocols, such as IPX, AppleTalk, and NetBEUI, are used to provide distributed computing workgroup functions between server and clients and/or sharing between peer clients.
    c. A packet sniffer (also controlled by this rule type) is a program that monitors and analyzes network traffic. Using this information, a network manager can troubleshoot network problems. A sniffer can also be used illegitimately to capture data being transmitted on a network. Sensitive information such as login names and passwords can be extracted from this data and used to break into systems.
    d. The StormWatch Sniffer and protocol detection rule is a monitoring tool. By adding this rule to a policy, you are causing an event to be logged when any non-IP protocols and packet sniffer programs are detected running on systems that receive this rule.
13. Syn Flood Protection
    a. One can either turn Syn flood protection “on” or “off.” SYN flooding is a type of denial of service attack. It occurs when a TCP/IP connection request is received from a return address that is not in use (i.e. a non-existent host for a spoofed address) resulting in a half open connection. Using SYN flood protection in a policy prevents this attack from succeeding.
14. Trojan Detection
    a. A Trojan is a form of malicious programming code that is installed on a system by an unsuspecting user either thinking that he or she is running some other type of program, or as a result of some other activity such as reading an attachment to an email message. Once installed, Trojans may allow others to access and virtually take over a system across the network. Other Trojans may be set up to automatically send mail messages or other types of network traffic (including system passwords) while the system owner is unaware of what is occurring. The following are the types of Trojan Protection Okena StormWatch provides:
    b. Trapping of keystrokes by network applications.
    c. Injecting Code into other applications.
    d. Accessing Memory Owned by Other Applications.

e. Stealing Local Passwords.
f. Downloading and Invoking Executable Files.
g. Downloading and Invoking ActiveX Controls.
h. Accessing System Functions from Code Executing in Data or Stack Space.
i. All of these functions can be excluded for certain applications that exhibit Trojan-like behavior (i.e. Yahoo Instant Messenger).

Okena StormWatch provides excellent protections right out of the box but also allows the user to tailor the system to fit the needs of the corporate environment. There are many other features, such as reporting, auditing, simple customization for application and file sets, and easy administration that make this system ideal for the corporate environment.

Please be reminded that this documents explains in a general way the 14 core rules that ship with our product and not all of the features of StormWatch.

If you have further questions please email:

support@okena.com

Or call:

(781) 209-3225