



Recommended Security Watch Settings

MonitorIT provides various 'Watch' types for monitoring a variety of security related activities on all your servers, workstations, and network devices. These various 'Watch' types and the variety of security related Events, Processes, Services, Files, Counters, and Traps that can be monitored are:

1. EventLogWatch for Windows Events.

- Suspicious activity filter.
- Failed logons.
- Security Audit failures.
- Application errors and warnings.
- Audit policy changed.
- Security log cleared.
- New user account created.
- User account changed.
- Member added to group.
- Global group changed.
- Privileged service called.
- New computer(s) added to domain.
- Account lockouts.
- After-hours logons.
- Entry to user workstations through network logons.
- Successful or failed file access (including access to specific filenames).

2. ProcessWatch for Windows Processes.

- Processes that should be running (`Lsass.exe`).
- Processes that should not be running.
 - Sasser worm: check for "`avserve.exe`".
 - Blaster worm: check for "`msblast.exe`".
 - Welchia worm: check for "`dllhost.exe`".
 - Welchia worm: check for "`svchost.exe`".
 - Beagle worm: check for "`au.exe`".
 - Mydoom worm: check for "`taskmon.exe`".
 - Netsky.B worm: check for "`services.exe`".
 - Gator or GAIN Adware: check for "`bundle.exe`".

MonitorIT®

3. WinServicesWatch for Windows Services.

- Virus protection service.
- Event Log service.
- IPSec Policy Agent service.
- Kerberos Key Distribution Center service.
- Net Logon service.

4. CustomWatch with a Windows Executable.

- Retina® Network Security Scanner.
- Security Administrator Tool for Analyzing Networks (SATAN).
- Port scanners like `Nmap`.
- Snort™.
- ISS Internet Scanner®.
- Tripwire.

5. FileWatch for Windows Files.

- Hackers like to delete log files to cover their tracks.
- Are virus definition files being updated in timely manner?
- Monitor log files created by various security related tools you execute periodically with CustomWatch.

6. CounterWatch for Windows Counters.

- Memory: % Committed Bytes In Use, Available, Page Faults/sec.
- Processor: % Processor Time
- Web Service: Current Connections, Total Locked Errors, Total Not Found Errors.

7. SNMPWatch for SNMP Traps / SYSLOGWatch for SYSLOG Messages.

- Real-time monitoring of select Trap & SYSLOG messages from your network devices indicating suspicious, unauthorized, or performance related activities.
- Real-time, proactive SNMP Query monitoring of select SNMP Counter variables from your network devices indicating suspicious, unauthorized, or performance-related activities.