zenith infotech inc.

Designing Software that works

Security Solution

White Paper

Zenith Infotech Inc. 39675 Cedar Blvd, Suite # 240 A & B, Newark, California-94560

EXECUTIVE SUMMARY

Information is shared as never before, making security as the biggest challenge for the Organization from the hackers as well as yellow collars working in the organization. Organization data & infrastructure has to be highly guarded or else, breaking into networks, distributing viruses, and downing servers & damaging data would become very easy. Providing an enterprise wide security is a big challenge where all security vulnerabilities, breaches, attacks are dealt in a proactive manner. The administrator today needs is an enterprise-wide secure systems & networks which automatically detects all security related issues & provide real time monitoring & reporting analysis to address all security related issues.

Most of the security tools have a very limited scope and are not designed to scale for ever growing needs of Organization. There is concern for day to day updates & patch managements for new security threats, real time synchronizations, monitoring, alerts & notifications.

Zenith Security Solution with its unique architecture and approach is a highly scalable, flexible, comprehensive and robust securing enterprise systems & networks by automatically detecting latest security vulnerabilities, breaches, attacks, providing extensive monitoring & reporting analysis to address them all. It incorporates a potent integrated vulnerability assessment and real-time incident management solution for Windows-centric networks by automated data collection & consolidation, correlating & managing security events form single console.

It enhances security by easily highlighting security related configuration parameters that are tough to determine. It incorporates the Best Security Practices that catapults the manageability of the IT system. Administrators are notified instantaneously on any security violations, possible security loop holes, functionality alerts on application specific logs. It provides report/logs for complete Enterprise wide security of Groups, Audit Policy, Account Policy, Security Policy, Share Permission, User Rights thus

- Prevents security breaches & vulnerabilities
- Conveys true picture of security conditions
- Consolidates and correlates security events
- Enforces Policy Standardization for Security Compliance
- Identifies Security Loopholes & Enhances Network Security
- Increases System Uptime & Reduces Support Response time
- Enhances Control of Critical System / Application
- Complete Security Event Analysis for Fast Diagnosis

OVERVIEW

The Security solution offering is categorized into three main subsystems, which are independent & is managed proactively using remote admin screen

- Vulnerability Tests & Loophole Analysis System
- Proactive Management of Security System with Logged information and Errors
- Patch Management

Vulnerability tests and loophole analysis system

It discovers, tracks, monitors various vulnerability and identifies fixes, by providing more than 1000 tests for Microsoft Windows 9x, Windows NT, Windows 2000. Generate comparative reports, recommend security fixes, prioritize responses, provides comprehensive security analysis in the area of intrusion detection.

Complete analysis are performed on application, operating systems (Windows family) & networks

- Some of the tests carried out are as follow:

Operating System :: All

Test Name
NetBus backdoor
NetBus Pro backdoor server active
FTP Serv-U version 2.5 susceptible to buffer overflows
Anonymous FTP
Anonymous FTP write
FTP service enabled
UDP Port Scan
TCP/IP Port Scan
OS Detection Phase
Vulnerable Bison FTP 3.5 server
Quake2 server
Hexen2 server
Quake server
Quake3 server
Unidentified UDP ports
Unidentified TCP ports
POP3 service enabled
SMTP service enabled
Seattle Labs SL Mail buffer overflow 1

Operating System :: Windows2000

Test Name
Check if Windows 2000 SP1 is not installed
Check if Windows 2000 SP1 is installed
Check for Windows 2000 ServicePack
Running on Windows NT 5
IIS5 Test
Microsoft Exchange 2000 User Account
Internet Information Server (IIS) 5.0 FTP parameters
ActiveX Parameter Validation
Check if Windows 2000 SP2 is not installed
Malformed Request to Domain Controller can Cause Denial of Service
Mixed Object Access
Require CTRL+ALT+DEL at logon
Malformed RPC Packet
Local Security Policy Corruption
LDAP over SSL could enable passwords to be changed
Invalid RDP Data
Network DDE Agent Request
Simplified Chinese IME State

Operating System :: WindowsNT

Test Name
Microsoft Office 8.0 - Excel macro virus protection
Office 2000 Excel security settings lockdown
Microsoft Office 2000 - PowerPoint trusts all installed add-ins and templates
Office 2000 PowerPoint security settings lock down
Office 2000 Word security settings lock down
Office 2000 Outlook security settings lock down
Microsoft Office 2000 - Excel trusts all installed add-ins and templates
Microsoft Office 2000 - Security settings in Word
Office 2000 Trusted Sources security registry permission
Microsoft Office 2000 - Security settings in Excel
IIS Malformed Extension Data in URL
SQL Server 7.0 Service Pack Password Vulnerability
DTS Password Vulnerability
NetMeeting Desktop Sharing
Microsoft Office VBA shell/Text-ISAM patch
L0phtCrack packet driver
Microsoft Office 2000 - Word trusts all installed add-ins and templates
HackerShield service account

CommuniGatePro Buffer Overflow Test

FrontPage hit counter buffer overflow

Cold Fusion documentation and examples

Operating System :: Windows

Test Name
Detect Windows Shares
Check Wrapster installation
Microsoft Office 2000 global security through HKEY_LOCAL_MACHINE
Microsoft Office 2000 - Security settings in Excel under lockdown
Microsoft Office 2000 - Security setting in Access under lockdown
WebXRay Sniffer
Web Client NTLM Authentication
HyperTerminal Buffer Overflow
Visual Studio VB-TSQL Object Contains Unchecked Buffer
RemoteDB Gateway server
PowerPoint 2000 File Parsing
Windows Media Player Skins File Download
Excel CALL
Sniffer Basic (NetXRay)
Windows Media Player 6.4/7.0: .ASX Processor Contains Unchecked Buffer
Office 2000 installed
Windows Media Player 6.4/7.0: ASX Buffer Overrun and WMS Script Execution
Windows Media Player .NSC Processor Contains Unchecked Buffer
OCX Attachment
Clip Art Buffer Overrun

Recognition

Protected Store Key Length

Secure Channel: Digitally encrypt or sign secure channel data(always)

Shutdown system without being logged on

Operating System :: WindowsNT4

Test Name
Check for NT Service Pack 4
IIS4 Test
Microsoft Proxy Server Found
Windows IGMP patch
Site Server - Site Wizard Input Validation
Microsoft Exchange 5.5: Malform MIME Header
Windows NT profile users directory permissions
\\WINNT\\Profiles Directory Permissions
Internet Information Server (IIS) 2.0/3.0 FTP parameters
Internet Information Server 2.0/3.0 (IIS) anonymous FTP
Internet Information Server (IIS) 4.0 FTP logging
Internet Information Server (IIS) 4.0 FTP Anonymous user
Internet Information server (IIS) 4.0 FTP authentication
IIS4 FTP SRV logfile directory permission
Internet Information Server 2.0/3.0 (IIS) FTP logging
IIS PASV FTP
Internet Information Server 3.0 (IIS) FTP Authenticated Access Enabled
Internet Information Server 2.0/3.0 (IIS) FTP bounce attack
Internet Information Server 2.0/3.0 (IIS) FTP Guest access
RPC spoof

password

Stored Procedure Permissions

OS2 subsystem

Multiple LPC and LPC Ports Vulnerabilities

Welcome.exe checksum

Security for shared objects

TCP/IP Security not enabled

Clear pagefile at shutdown

NT/2000 ResetBrowser and HostAnnouncement Flooding

Lan Manager authentication

DCOM default launch permissions

PASSFILT.DLL checksum

Unchecked Buffer in Index Server ISAPI Extension

MSV1_0.DLL checksum

MSGINA.DLL checksum

FPNWCLNT.DLL checksum

DCOM default access value

SLMail Users registry permission

Insecure CMail 2.3 registry permissions

Exchange SMTP and NNTP denial of service

CMAIL 2.3 - User access to user.db file

CMAIL webmail interface

IMAIL 4.06 IMAP4 server active

User with Profile system performance permissions

User with Increase scheduling priority permissions

User with Load and unload device driver permissions

Proactive Management of Security System with Logged Information & Errors

It centrally collects Security event and Security log data across enterprise window systems and applications enabling multidimensional event data analysis giving insight on Event Statistics, Invalid and Successful Logons, and Object Access attempts, It incorporates reporting, monitoring & archiving of security data, application, cross referencing of various events between different logs, tracking & preventing vulnerability, increasing insight & enhancing security, thus simplifying security event management for windows systems & networks

Administrators are notified instantaneously on any security violations, any possible security loopholes & functionality alerts on application specific logs. It provides an administrator more the 55 analytics which helps him/her to proactively manage the WINDOWS subsystem giving complete Enterprise wide security Analysis of

- Groups,
- Audit Policy,
- Account Policy,
- Security Policy,
- Share Permission,
- User Rights
- And more

Some of the reports and analysis generated are:

• Account Logon Failed by Date	• Invalid Logons with Embedded Username (all reasons) (chart)
• Account Logon Success by Date	• Invalid Logons with Embedded Username by Date (all reasons)
• Activity During Non-Business Hours (chart)	• Logon Auditing Turned Off Events by Computer (chart)
• Activity of New Users (chart)	• Logon Auditing Turned Off Events by User (chart)
• Audit Log Cleared Events by Computer (chart)	• Mean Time Between 'EventLog Is Full' Events
• Audit Log Cleared Events by User (chart)	• Objects Access by Application Sessions
• Audit Log Cleared Events by User	• Objects Access by Applications
• Audit Policy History	• Objects Scanning Detection
• Current Audit Policies	• Pre-Authentication Failed by Date
• Daily Reboot Statistics	• Recommended Audit Policy

• Domain Trusts Management by Initiator	• Security Principal Added to Active Directory Group
• Domain Trusts Management by Trusted Domain	• Successful Authentication Ticket Granted by Client IP
• Domain Trusts Management by Trusting Domain	• Successful Authentication Ticket Granted by Date
• Failed File Access by File (chart)	• Successful Authentication Ticket Granted by Server
• Failed File Access by File	• Successful Authentication Ticket Granted by User
• Failed File Access by User (chart)	• Successful File Access by File
• Failed File Access by User	• Successful File Access by User
• Failed Object Access (chart)	• Successful Interactive Logons by Server
• Group Management	• Successful Logons by Date
• Invalid Interactive Logons by Server	• Successful Logons by Server
• Invalid Logons by Date (all reasons)	• Successful Logons by User
• Invalid Logons by Date	• Successful Logons by Workstation
• Invalid Logons by Server (all reasons)	• Successful Logons during None-Business Hours (chart)
• Invalid Logons by Server	• Successful Logons during None-Business Hours by Server
• Invalid Logons by User (all reasons)	• Successful Logons during None-Business Hours
• Invalid Logons by User	• Successful Object Access by User (chart)
• Invalid Logons by Workstation (all reasons)	• Successful Services Ticket Granted by Date
• Invalid Logons by Workstation	• User Activity (chart)
• User Rights Management by Initiator	• User Rights Management by User

Patch Management

Patch Management' is a software solution for Windows NT4/2000/XP and many mission critical applications. It identifies which software updates are needed for servers & workstation. 'Patch Management' remotely installs, validates and defines policies about these updates empowering administrators to control the software updating process.

Patch Management' provides the most comprehensive software updates research, query, distribution and validation solution giving administrators the decision-making and policy management solution that they need for managing the process of updating service packs, hot fixes and other self installing software patches.

It Analyses missing patches from remote machines and shows its reports on the Patch Management Console. It checks required fields from the client machine and updates administrator with all details & upgrade information. It provides regular upgrades & patches that is downloaded & updates SQL tables in the client machine which is later on deployed & run across different workstation for Patch /Upgrades and Hotfixes.

It assist administrator by providing in-depth details on

- Updates/Hotfix (research)
- Query any systems (inventory)
- Install remotely any combination of Updates/Hotfix (deployment) for the following software solutions
    - Windows NT4/2000/XP
    - IIS
    - SQL Server
    - Exchange Server
    - Internet Explorer
    - Media Player
    - Windows Media Services
    - Net Meeting
    - Office 2000
    - Office XP
    - Outlook 2000, Outlook 2002
- Verify installations (validation)

KEY FEATURES & BENEFITS

Analyzing, Reporting, Monitoring & Archiving

Security Event Data are amalgamated & analyzed, which assists in faster decision making, enhancing security & performance. It provides an exhaustive list of reports/analytics through multidimensional security event data analysis collected & consolidated across diverse platform. It correlates security events conveying true picture of security conditions thus reducing support response time & helping administrator to take informed decision.

Policy-based Approach & Enterprise Compliance

It enables Enterprises to incorporate & enforce policy & rule based approach, automatically enforcing compliance, generates alerts on their violation. Security & Compliance reports/logs generated enables administrator to take informed decision & help in maintaining standards across the Enterprise and enhances security. Thus *Enforces Policy Standardization for Security Compliance & Prevents security breaches and vulnerabilities*

Scalability & Superior Execution Methodology

It has a strong / scalable data repository design and management system that enhances the manageability of Security logs & Data by using a very methodical & meticulous process for event extraction without introducing performance overhead on the managed system.

Provides automated scheduling for data collection & consolidation with other options for efficient & effective system management, that would optimized event gathering and consolidation operations *Thus enhancing system availability & reduces down time.*

Support Windows NT/2000/XP Networks

It is fully Windows 2000/NT compatible and also supports mixed Windows 2000 and Windows NT environments.

Security Enhancement

It provides you with in-depth analysis on possible breaches, violation; giving greater insight on day–to–day security configuration enabling to locate possible security loop holes, incorporating best security practices.

Friendly GUI

Provides a rich and easy to understand GUI that puts administrator get going

Auto Documentation

Incorporates automated documentation that enhances & streamlines the reports/logs documentation process for the IT infrastructure, enables faster knowledge transfer across enterprise, generate comprehensive documentation covering

REQUIREMENTS

System Requirements

- Platform : Intel x86 (P III Recommended 1GHz)
- Operating system :Windows NT 4.0 (SP5 or higher) or Windows 2000
- Memory : 256 Mbytes (512 Mbytes recommended)
- Hard disk space : 100 Mbytes (Minimum)
- Microsoft Data Access Components 2.6 (or higher)
- Microsoft SQL Server: 2000
- Microsoft IIS Installed 5.0
- Microsoft Data Access: 2.6 (or higher)
- Microsoft Internet Explorer 5.0 or higher