

Security and Control of Microsoft Windows Servers and Active Directory

Seminar Focus and Features:

Microsoft is a major player in both the IT infrastructure and application development arenas. Active Directory provides a significant anchoring point for all Microsoft related infrastructure. In this practical, information packed three-day seminar, you will learn a structured approach to securing and auditing Microsoft server and networking infrastructure from end-to-end and from top to bottom. You will cover all key Windows member server and domain controller control points, as well as common security risks, safeguards, and audit procedures. Key changes affecting security and audit in different versions of Windows servers will be highlighted. Forests, domains, and directory services control points and associated security and audit procedures within the Microsoft Active Directory architecture will be analyzed. In addition, you will receive a comprehensive audit checklist for each major Microsoft building block/control point. You will gain criteria for selecting and using best-of-breed bundled, freeware, and commercial security and audit tools. Sample exercises will be used to demonstrate use of commonly available audit tools to perform key Windows audit procedures. You will also focus on strengthening your organization's ability to demonstrate due diligence by emphasizing and leveraging important guidelines from Microsoft, Center for Internet Security (CIS), and National Institute of Standards and Technology (NIST), Defense Information Systems Agency (DISA), and other key sources of industry best practices.

Prerequisites: *Network Security Essentials (ASG203)*, *Auditing Networked Computers (ITG211)*, *Information Security Bootcamp (ISG291)* or equivalent knowledge in the fundamentals of operating system and network security and audit.

Learning Level: Intermediate

Bonus: You will receive the *Standard Edition of the MIS Swiss Army Knife Reference Guide* listing hundreds of valuable resources for you and your organization.

Who Should Attend

Information Security Managers, Architects, and Analysts; IT Managers, Architects, and Application Developers; IT Audit Managers and Staff; Operational Auditors

What You Will Learn

1. Microsoft Infrastructure Architecture

- Common Building Blocks and Control Points in Microsoft's server, network, and application Architecture
- Highlighting Major Features And Changes in the Microsoft Server Product Chronology:
- Windows NT, Windows 2000, Windows 2003, and Windows 2008
- Critical Threats, Vulnerabilities, and Risks Associated With Microsoft Systems
- Sources of Industry Baselines, Security Alerts, and Best Practices for Designing, Securing and Auditing Microsoft Applications

- Defining the Overall Audit Plan, Objectives, And Information-Gathering Requirement for Your Audit

2. Windows Server

- Member Server Roles and Control Points
- Windows Server Administrative Console Tools
- User Accounts: Local and Domain
- Password Management
- Groups
 - Local vs Domain
 - Built-In/Default Groups
 - Customized Groups
- Local Security Policy File
 - Account Policies: Passwords, Lockouts
 - Audit Policies
 - User Rights Assignments Security Options
 - Policy Data Extract Procedures
- User Rights and Privileged Users
- Data Protection and Access Controls
 - Data Management Architecture
 - NTFS File Security
 - Windows File Share Security
 - File Encryption: Encrypting File System (EFS) and 3rd Party Alternatives
- Microsoft TCP/IP Applications and Network Services
- Privileged Programs
- Security Event Log Management
 - Event Log Types
 - Log File Management and Security
 - Log Data Aggregation, Correlation, and Host-based Intrusion Detection
- Hypervisors and Virtualization
- Vulnerability and Patch Management for Windows Systems
- Configuration Management and Change Control
- Identifying Installed Software
- Windows Server and Network Services Management, Security and Audit Tools
 - Built-in Server Utility Software
 - Windows Workstation and Server Support Tools, Resource Kits, Admin Packs, Snap-ins, and VB Scripts
 - Useful Freeware Security and Audit Tools
 - Prominent Commercial System Management, Security and Audit Tools
- Windows Server and Network Services Audit Procedures and Checklists

3. Active Directory Architecture

- Domains, Forests, and Associated Policy and Trust Relationships
- Types of Active Directory Objects

- Categorizing Domain Controllers and Their Roles
- Windows pre-2000 Compatibility Configuration Security Issues
- Lightweight Directory Access Protocol (LDAP)
- Domain Name System (DNS)
- Dynamic Host Configuration Protocol (DHCP)
- Domain Authentication Systems: NTLM, Kerberos
- Domain Security Policy Management
 - Scope of Domain Security Policies
 - Domain Security Policy
 - Domain Controller Security Policy
 - Organizational Units and Associated Group Policies
 - Security Templates and Group Policy Management Tools
- Administrative Authority in Active Directory
- Integrating Unix and other Systems under the Active Directory Umbrella
- Domain Controller and Active Directory Management, Security, and Audit Tools
 - Built-in Server Utility Software
 - Windows Directory Services Support Tools, Resource Kits, Admin Packs, Snap-ins, and VB Scripts
 - Useful Freeware Tools for Active Directory and Domain Trust Mapping, Security and Audit
 - Prominent Commercial Active Directory Management, Security and Audit Tools
- Domain Controller and Active Directory Audit Procedures and Checklists

4. Final Thoughts

- Review of Key Control Points and Audit Sampling in a Microsoft Network
- Summarizing the most significant risks and important audit priorities associated with Microsoft Windows Server, Active Directory, and associated Microsoft application building blocks