Microsoft Windows Security

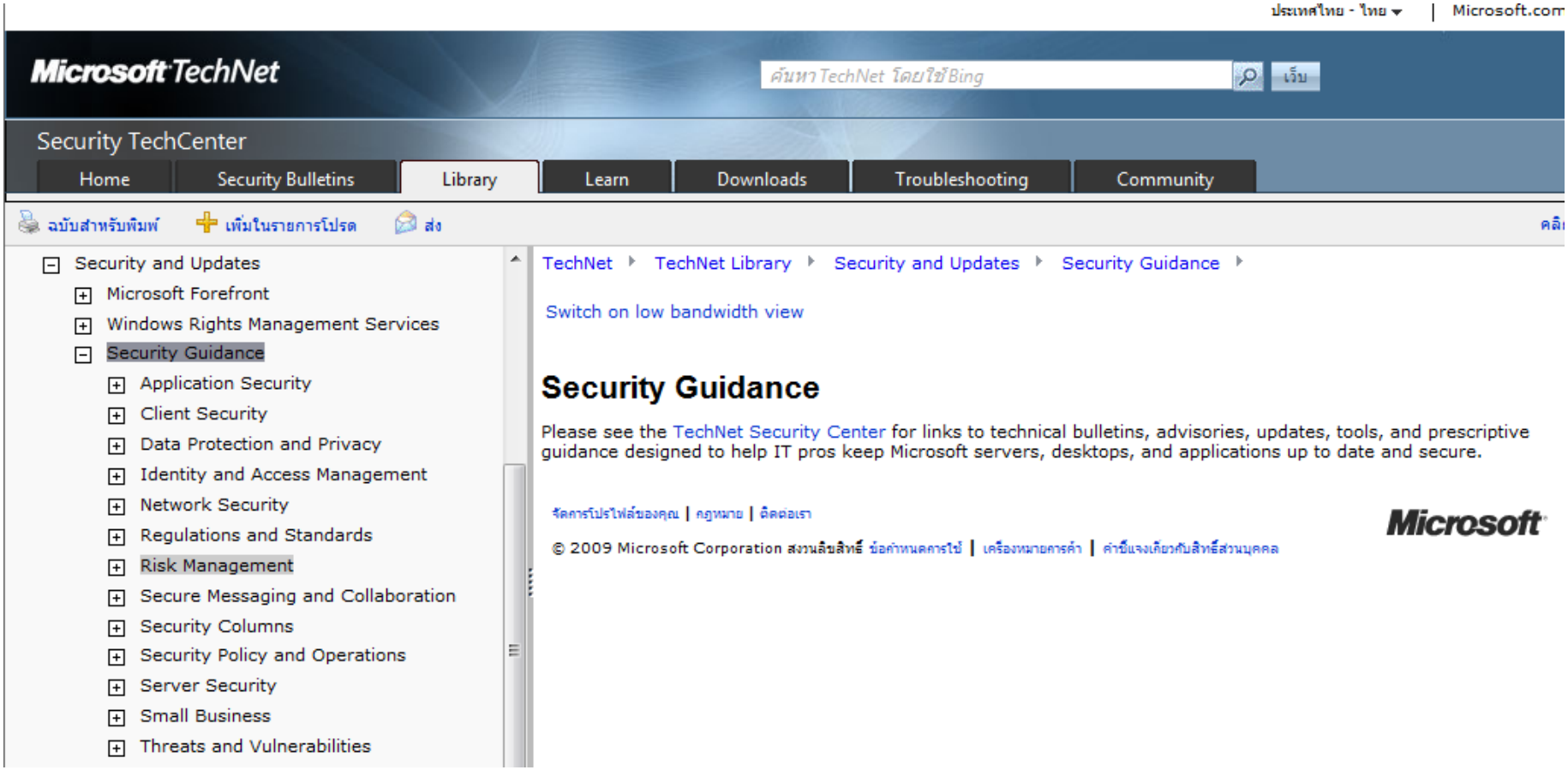
ภัคพงศ์ กฤตวัฒน์

Senior Instructor (ACIS Professional Center)

Microsoft Certified Trainer, EC-Council Certified Instructor, Certified Wireless Network Trainer

http://www.microsoft.com/security

Security Guidance



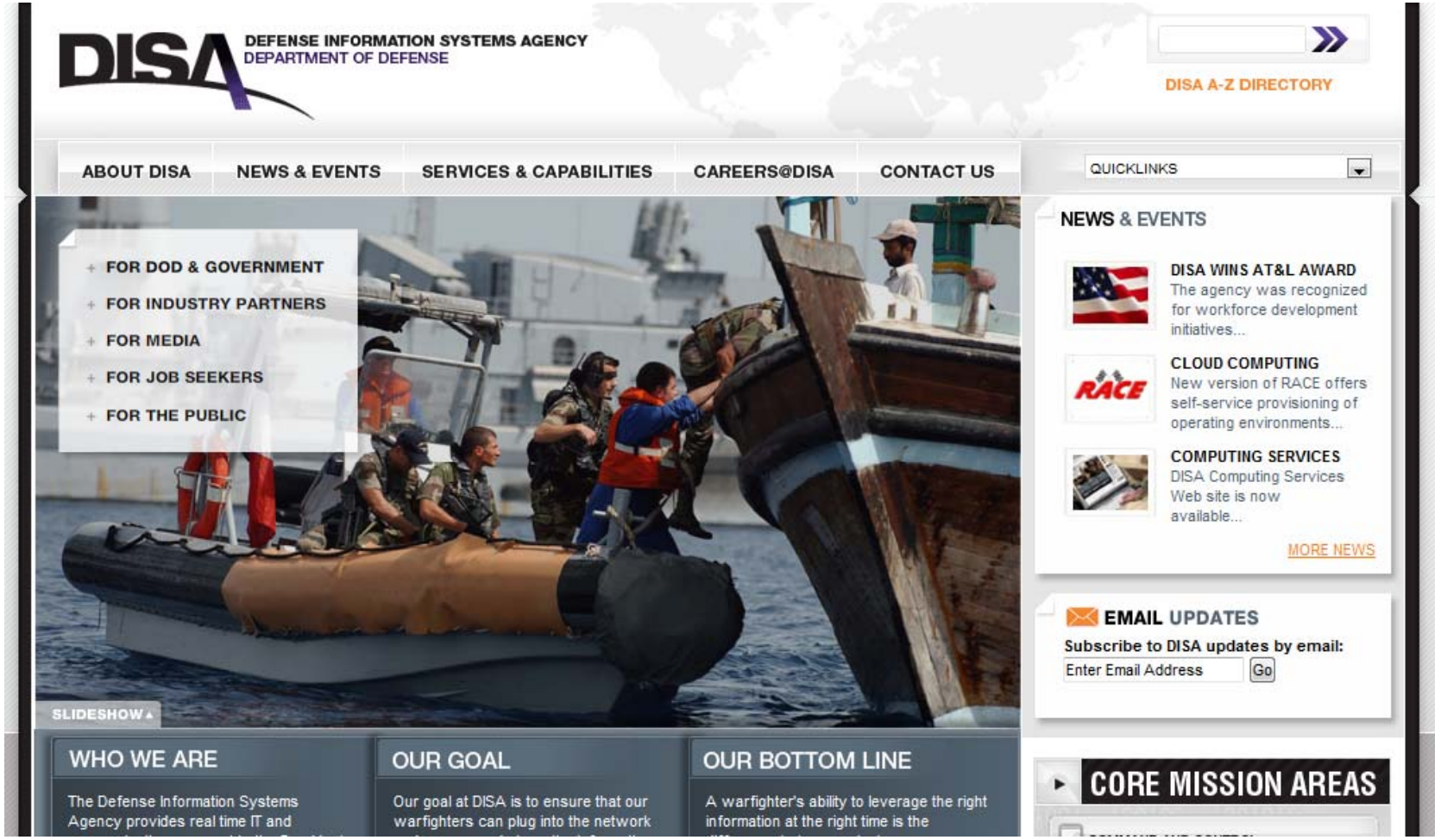
Security Compliance Management Toolkit series

- Windows Server 2008
- Windows Server 2003
- Windows Vista
- Windows XP
- Microsoft Office 2007

Other Security Guidelines

- DISA STIGs
- NSA IA Guidance
- The CIS Benchmarks

DISA (http://www.disa.mil)



DISA STIGS

- Security Checklists
- Security Readiness Review Evaluation Scripts
- Security Technical Implementation Guides

http://iase.disa.mil/stigs/

NSA (http://www.nsa.gov)

Center for Internet Security (http://www.cisecurity.org)

Hardening Concept

- Reduce Attack Surface
- Defense In Depth
- Least Privilege
- Fail to Secure Mode

Attack Surface

The "Attack Surface" is the sum of the ways in which an attacker can get at you

Smaller Attack Surface is better

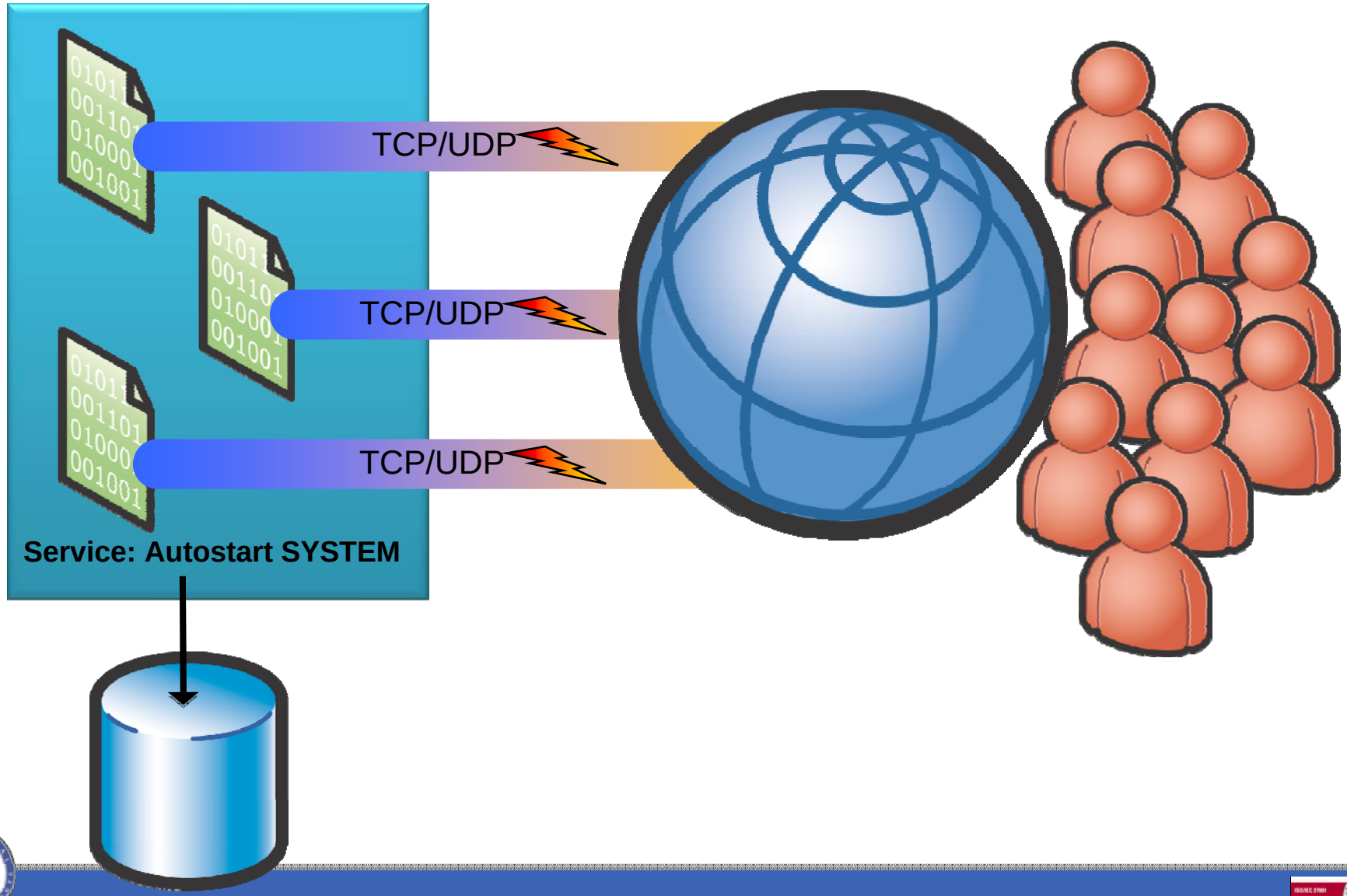
Understand Your Attack Surface

- Networking protocols that are enabled by default
- Network Endpoints
- Code that auto-starts or will execute when accessed
  - Examples: Services, daemons, ISAPI filters and applications, SOAP services, and Web roots
- Reusable components
  - ActiveX controls, COM objects, and .NET Framework assemblies, especially those marked with the AllowPartiallyTrustedCallersAttribute)
- Process identities for all the code you run
- User accounts installed

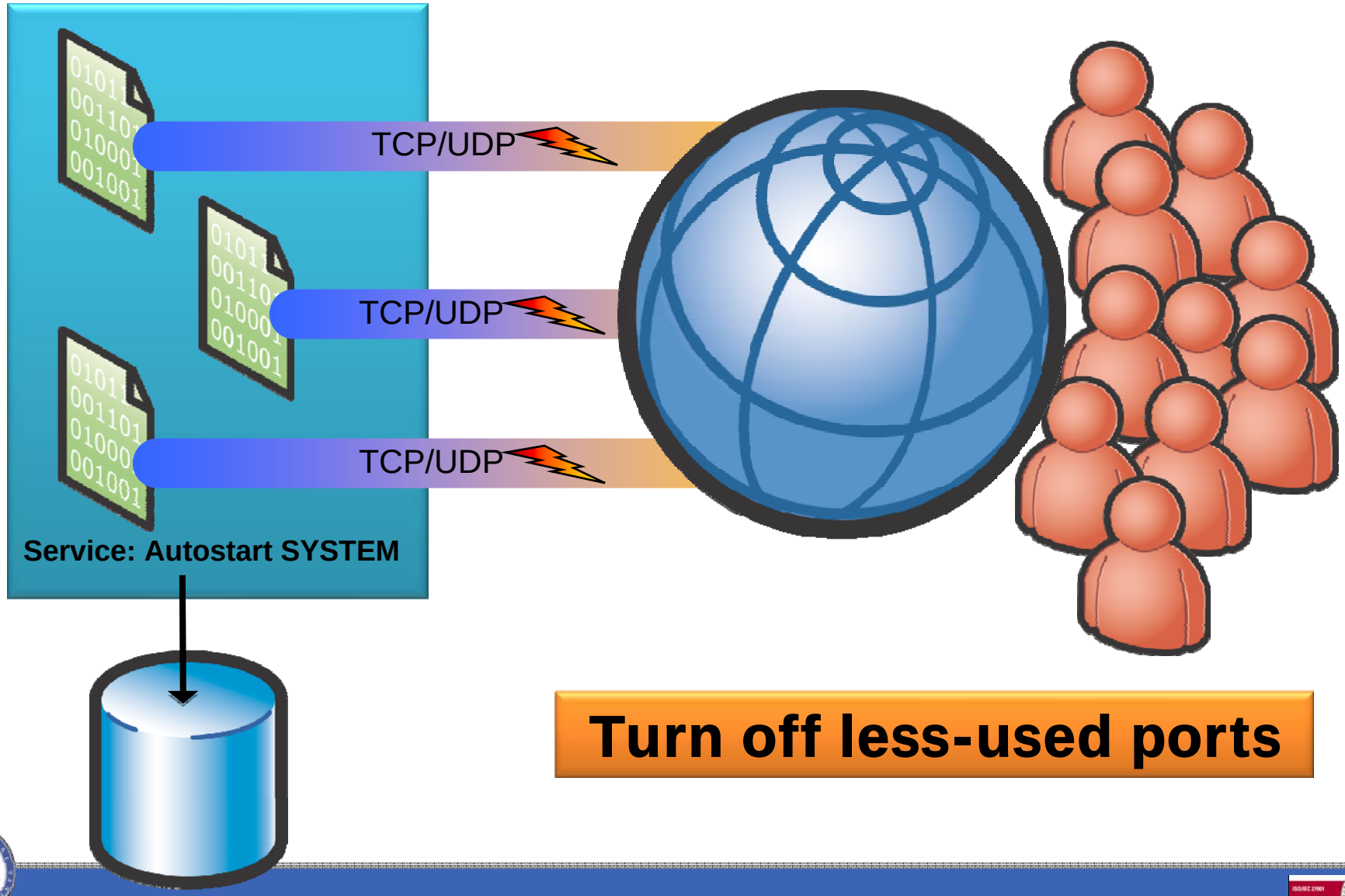
Reduce Attack Surface

HARDENING

Reducing Attack Surface

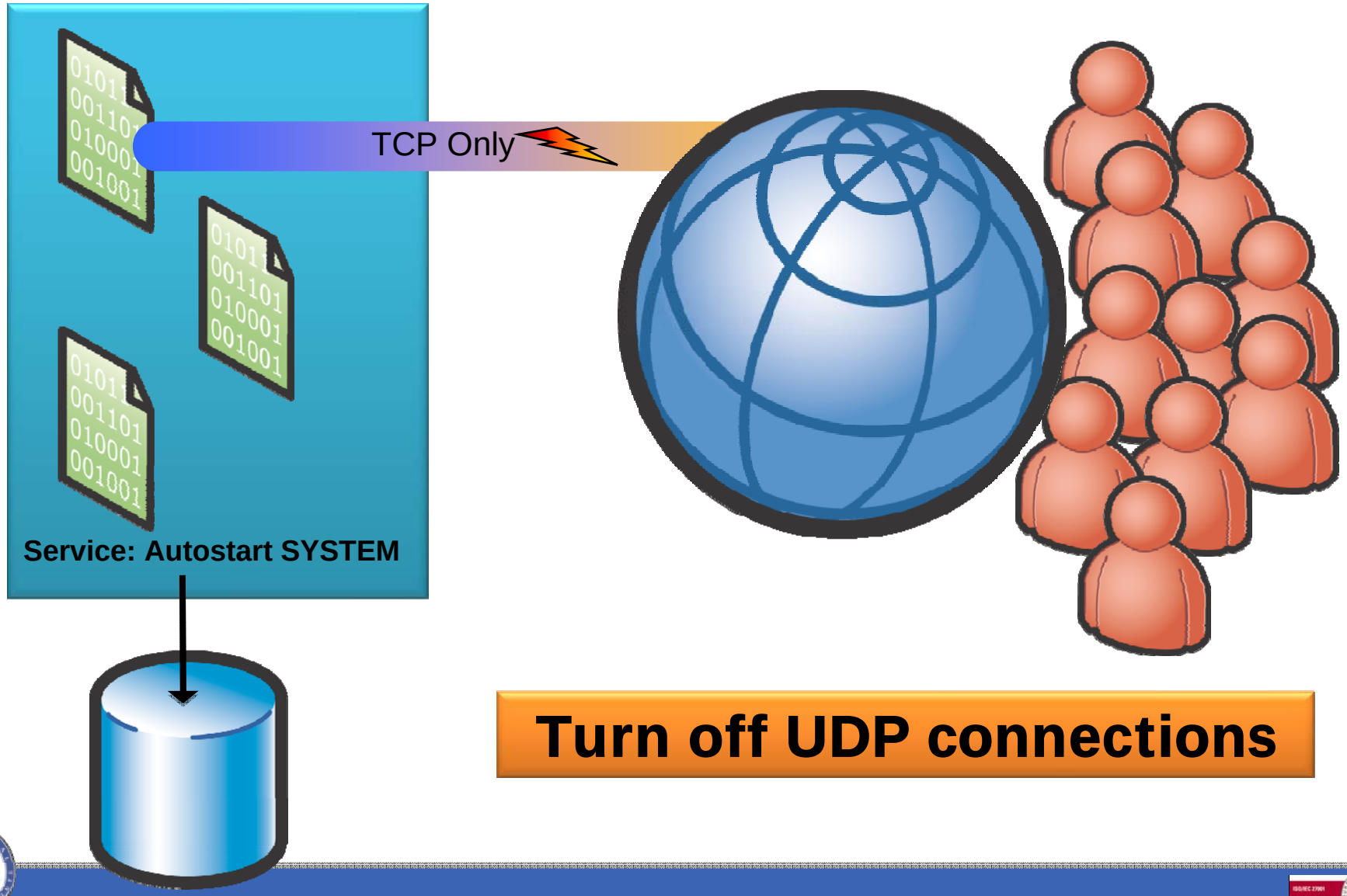


Reducing Attack Surface



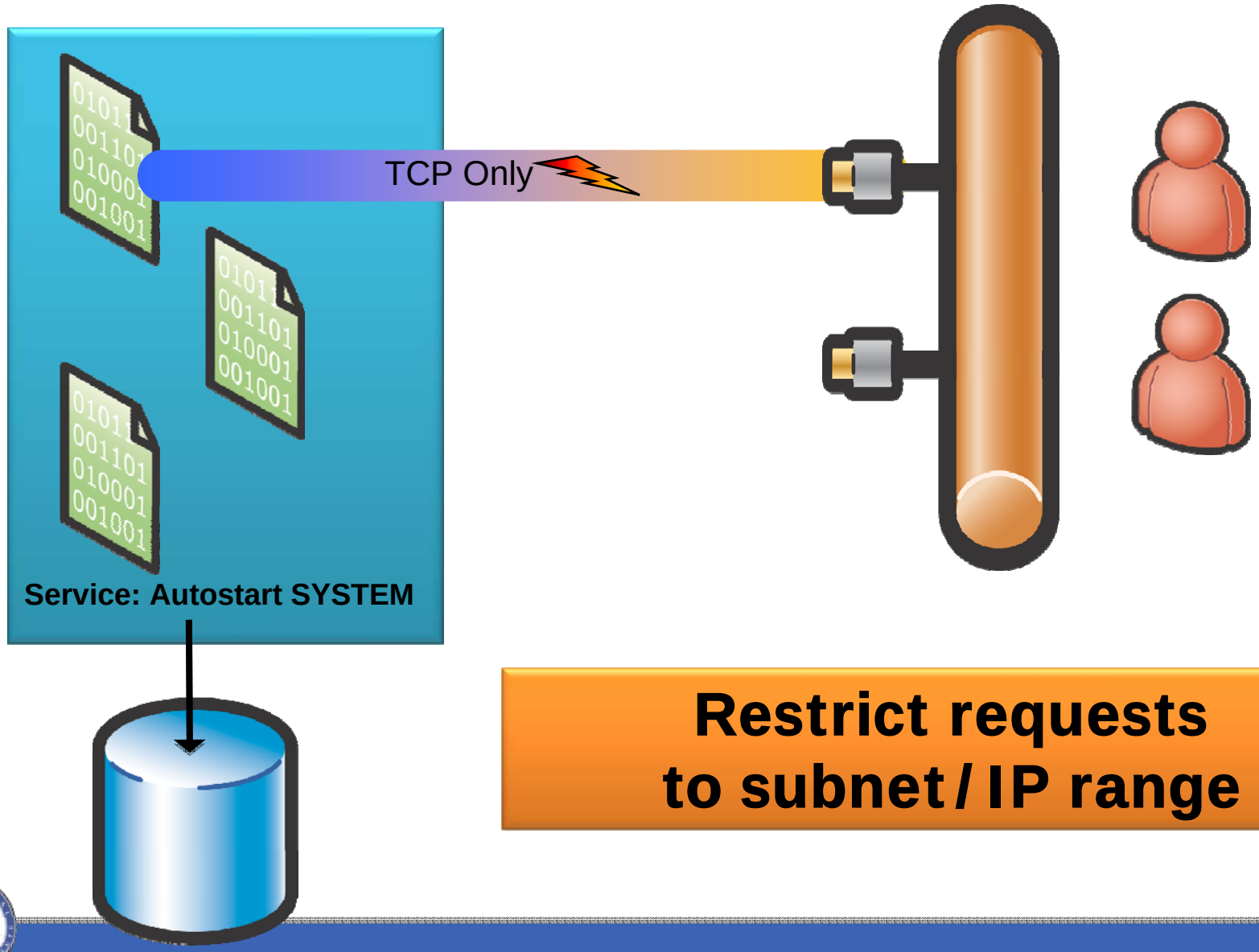
Turn off less-used ports

Reducing Attack Surface



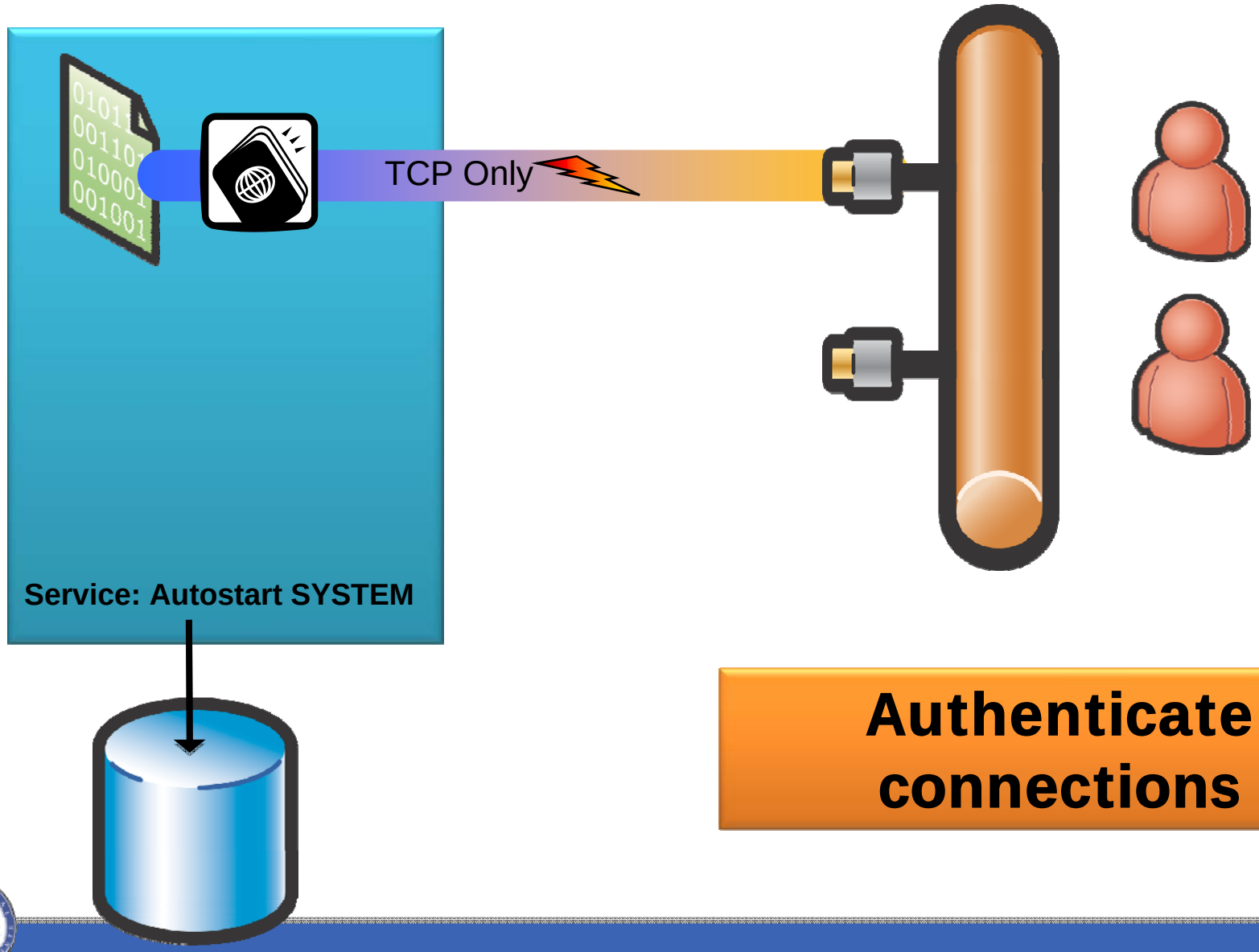
Turn off UDP connections

Reducing Attack Surface



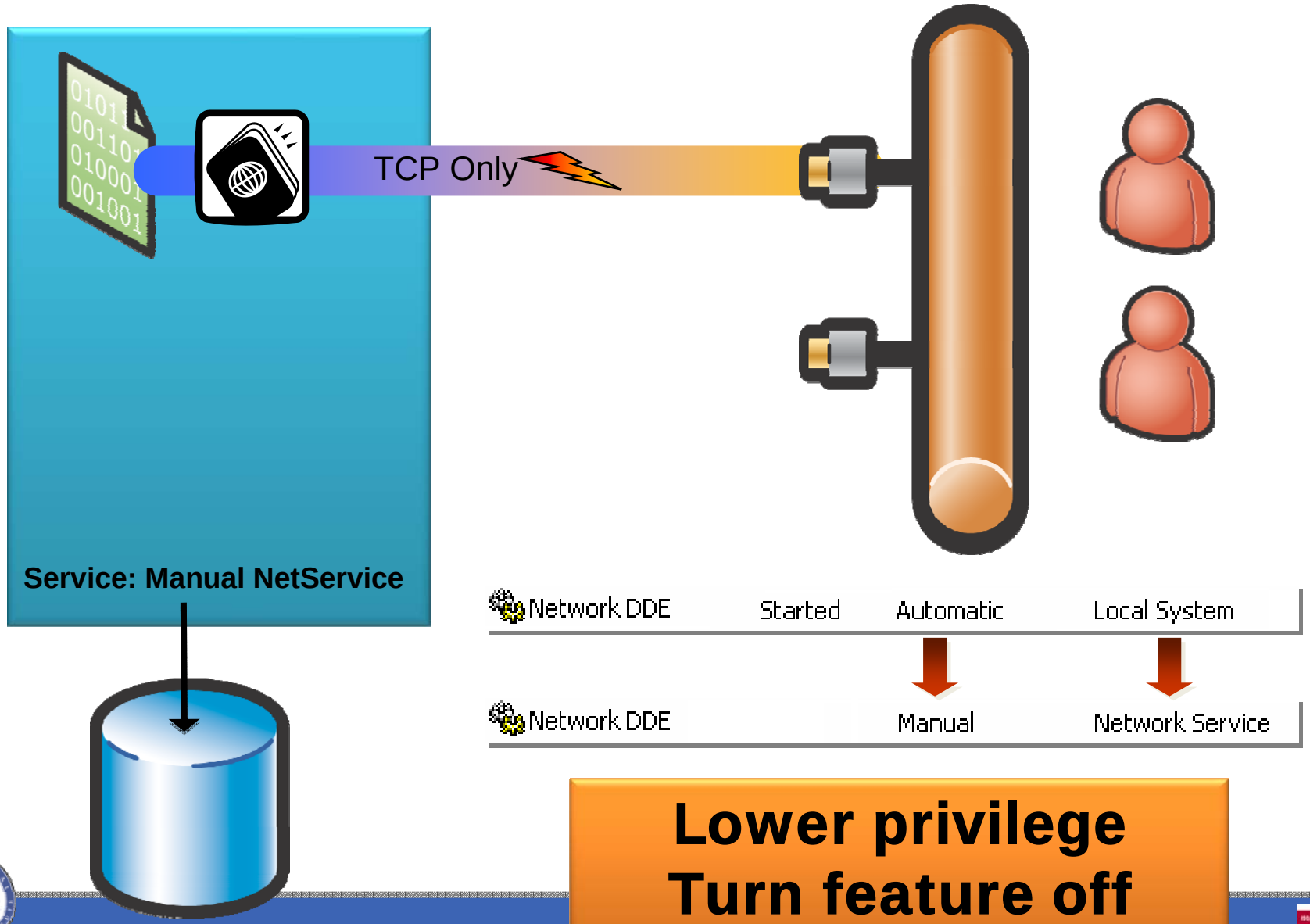
Restrict requests to subnet / IP range

Reducing Attack Surface



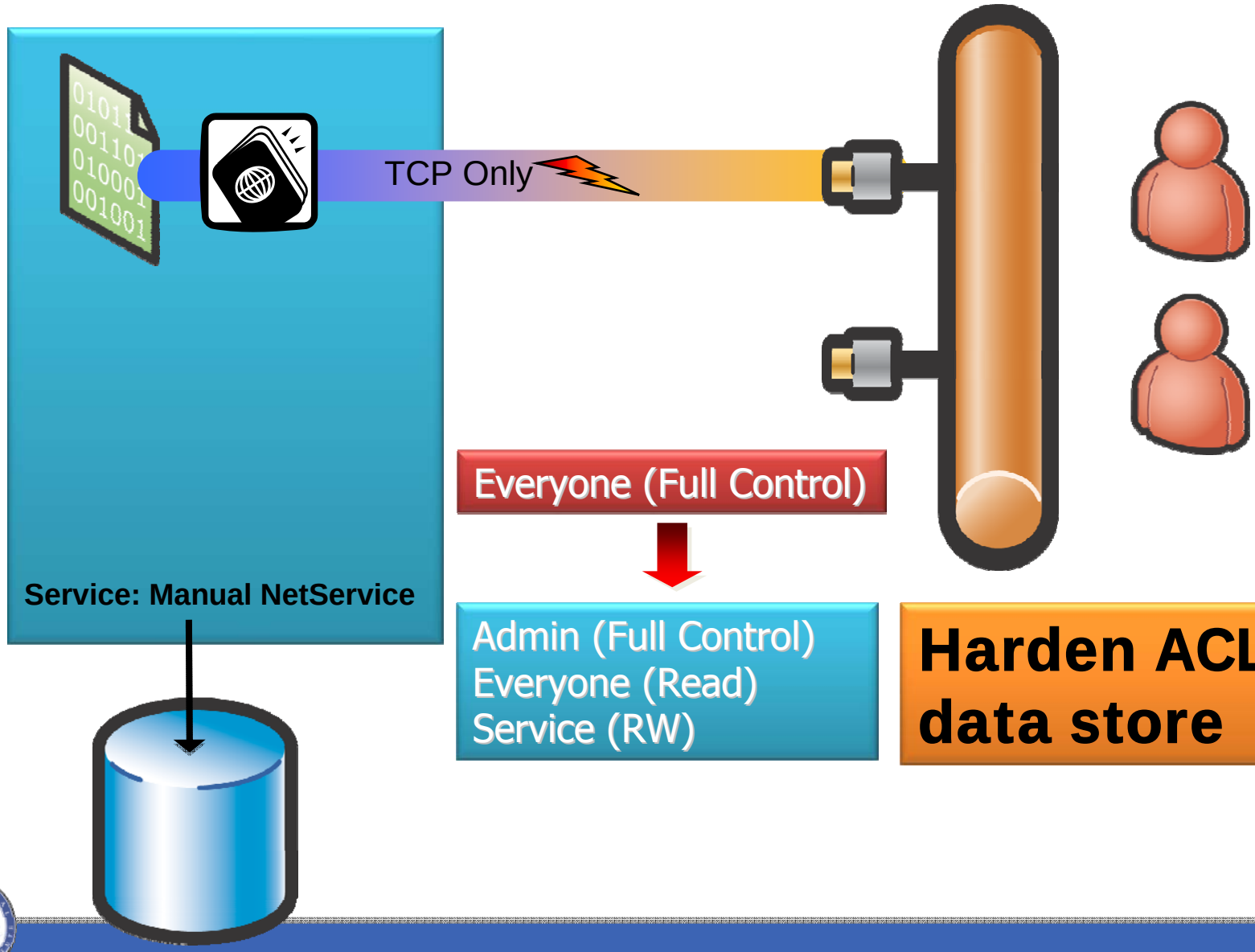
Authenticate connections

Reducing Attack Surface



Lower privilege
Turn feature off

Reducing Attack Surface



Defense in Depth

HARDENING

Defense In Depth

- Don't count on one line of defense for everything
  - What if the attacker penetrates that defense?
  - Contain the damage
- An example – Nuclear Plants
  - "Multiple redundant safety systems. Nuclear plants are designed according to a "defense in depth" philosophy that requires redundant, diverse, reliable safety systems. Two or more safety systems perform key functions independently, such that, if one fails, there is always another to back it up, providing continuous protection. "
    - - Nuclear Energy Institute

Defense in Depth (MS03-007)

Windows Server 2003 Unaffected

The underlying DLL (NTDLL.DLL) not vulnerable	Code made more conservative during Security Push
Even if it was vulnerable	IIS 6.0 not running by default on Windows Server 2003
Even if it was running	IIS 6.0 doesn't have WebDAV enabled by default
Even if it did have WebDAV enabled	Maximum URL length in IIS 6.0 is 16kb by default (>64kb needed)
Even if the buffer was large enough	Process halts rather than executes malicious code, due to buffer-overrun detection code (-GS)
Even if it there was an exploitable buffer overrun	Would have occurred in *w3wp.exe* which is now running as 'network service'

Least Privilege

HARDENING

Least Privilege

- A defense in depth measure
- Code should run with only the permissions it requires
- Attackers can only do whatever the code was already allowed to do
- Recommendations
  - Use least privilege accounts
  - Use code access security
  - Write Apps that non-admins can actually use

Fail To Secure Mode

HARDENING

Fail To Secure Mode

- Watch out for exceptions
- Never initialize variables to success results

```
Function Authenticate(UserID As String, Password As String)
    Authenticated As Boolean = True
        Dim conn As New SqlConnection(connString)
        conn.Open()
        Dim cmd As New SqlCommand("SELECT Count(*) FROM Users …")
        Dim count As Integer
        count = cmd.ExecuteScalar()
        Authenticated = (count = 1)
    Catch ex As Exception
        MessageBox.Show("Error logging in " + ex.Messag
    End Try
    Return Authenticated
End Function
```

Danger!! Assumes Success

Authenticated flag may still be true here

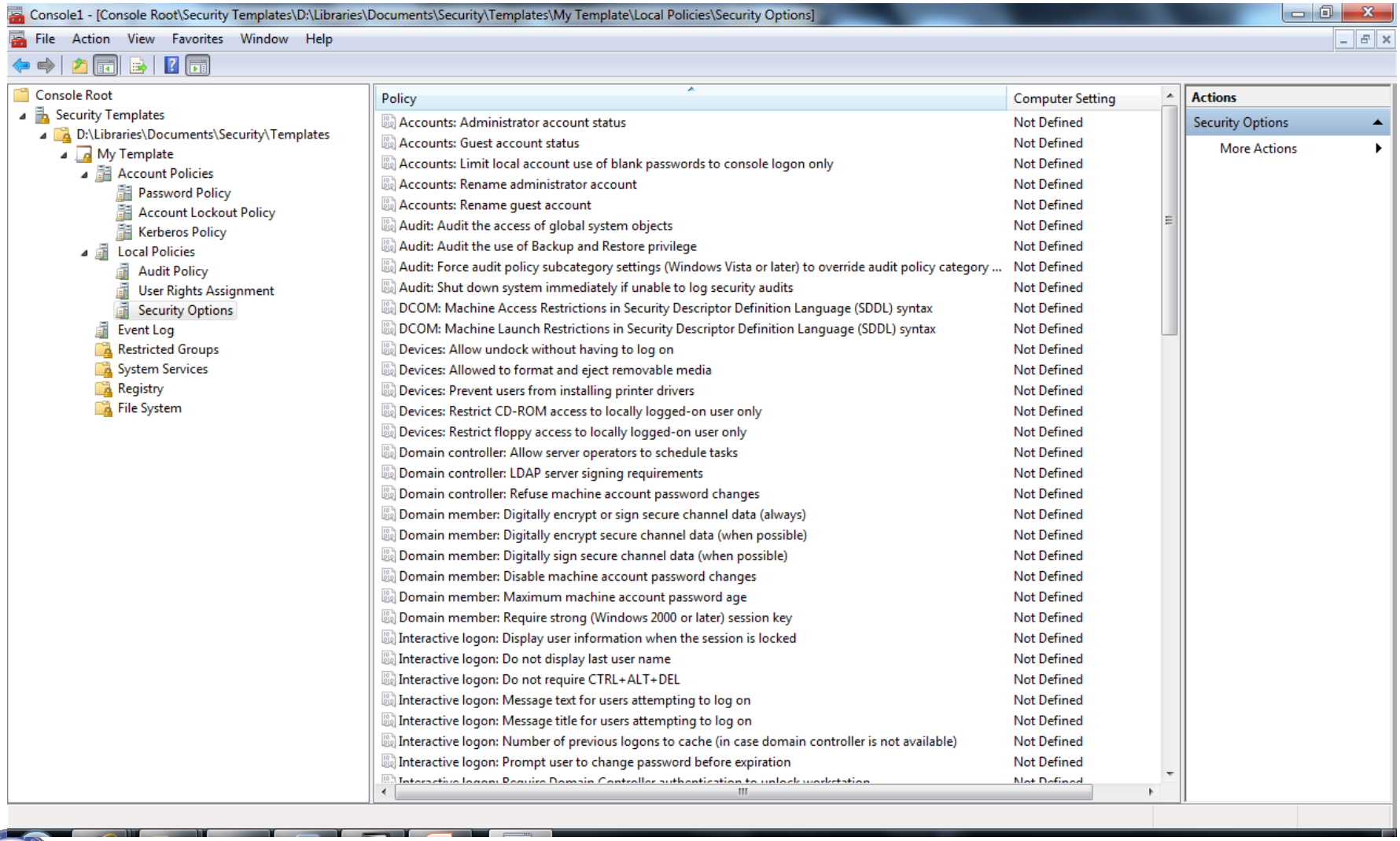
Secure baseline

- Settings for applications and services
- Operating system components
- Permissions and rights
- Administrative procedures
- Physical access

Server Hardening - Templates

- Predefined Security Templates
- Security Guide Templates
- Industrial Templates
  - SANS
  - CIAC
  - NSA
  - DoD DISA
- Custom Templates

Demo: Security Template

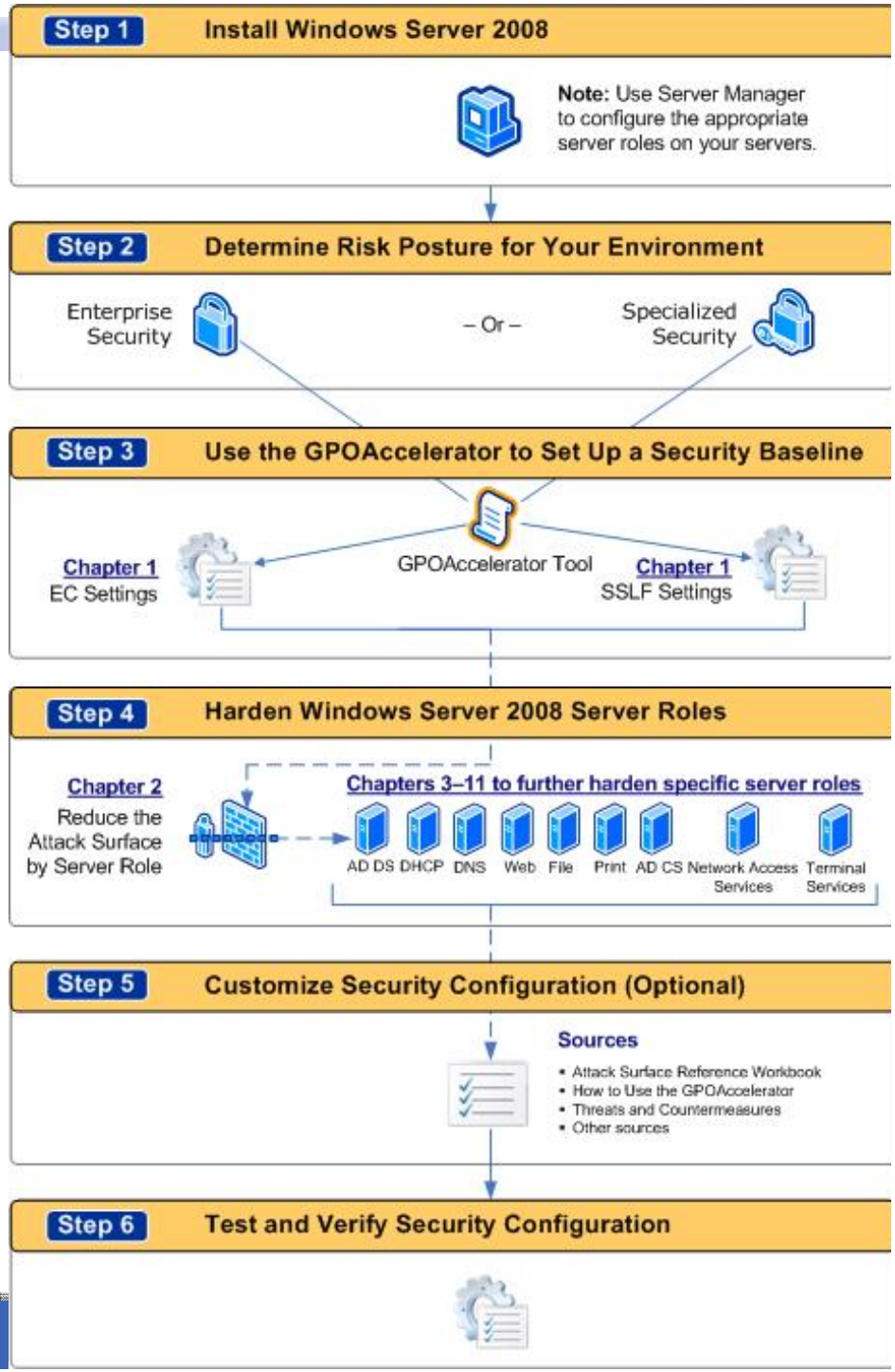


Template Deployment

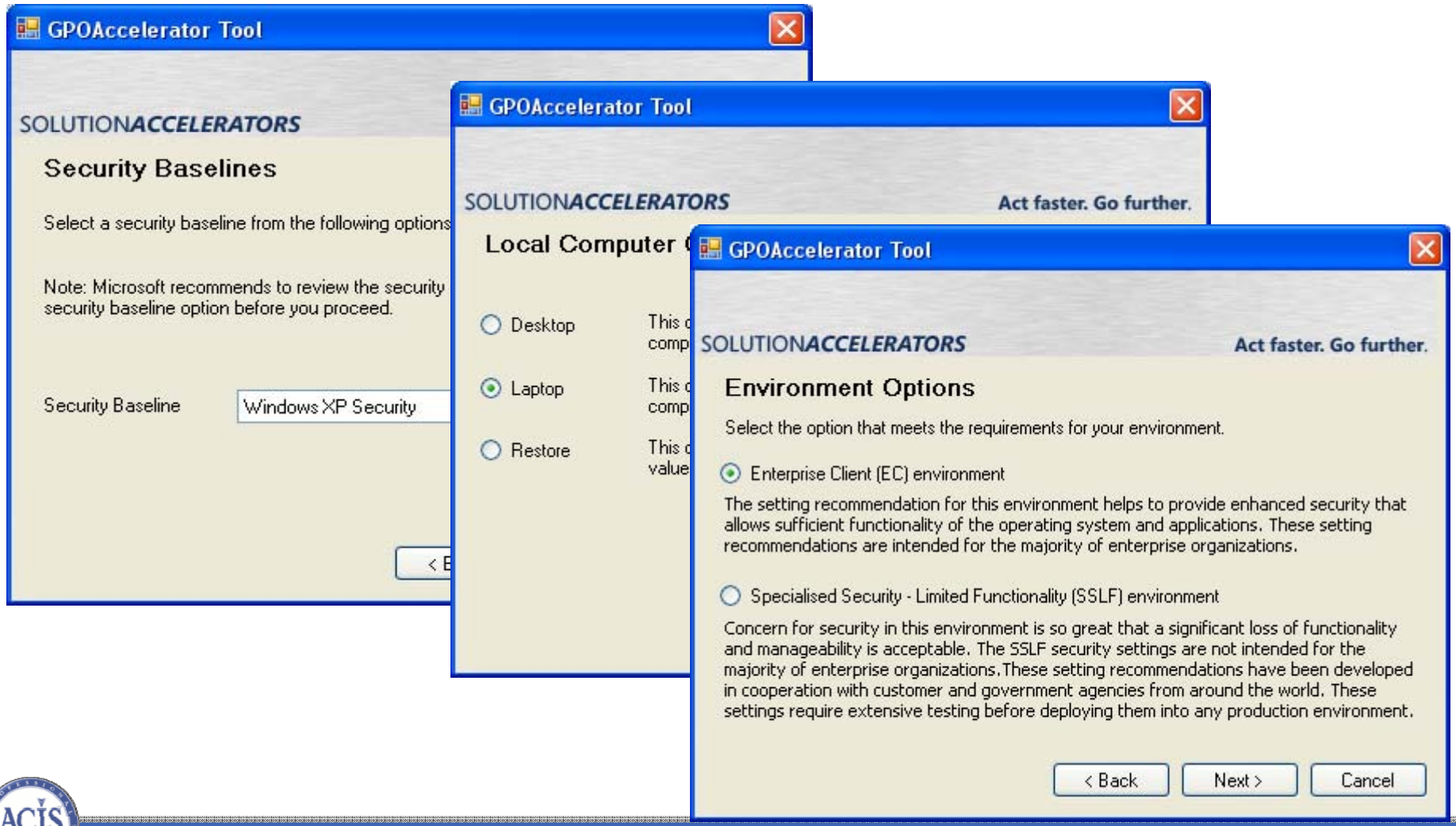
- Test before deployment
- Periodic analysis
  - Security Configuration and Analysis snap-in
  - Scripting (Secedit.exe)
- Deployment Methods
  - Group Policy (Active Directory)
  - Security Configuration and Analysis snap-in
  - Scripting (Secedit.exe)

GPOAccelerator

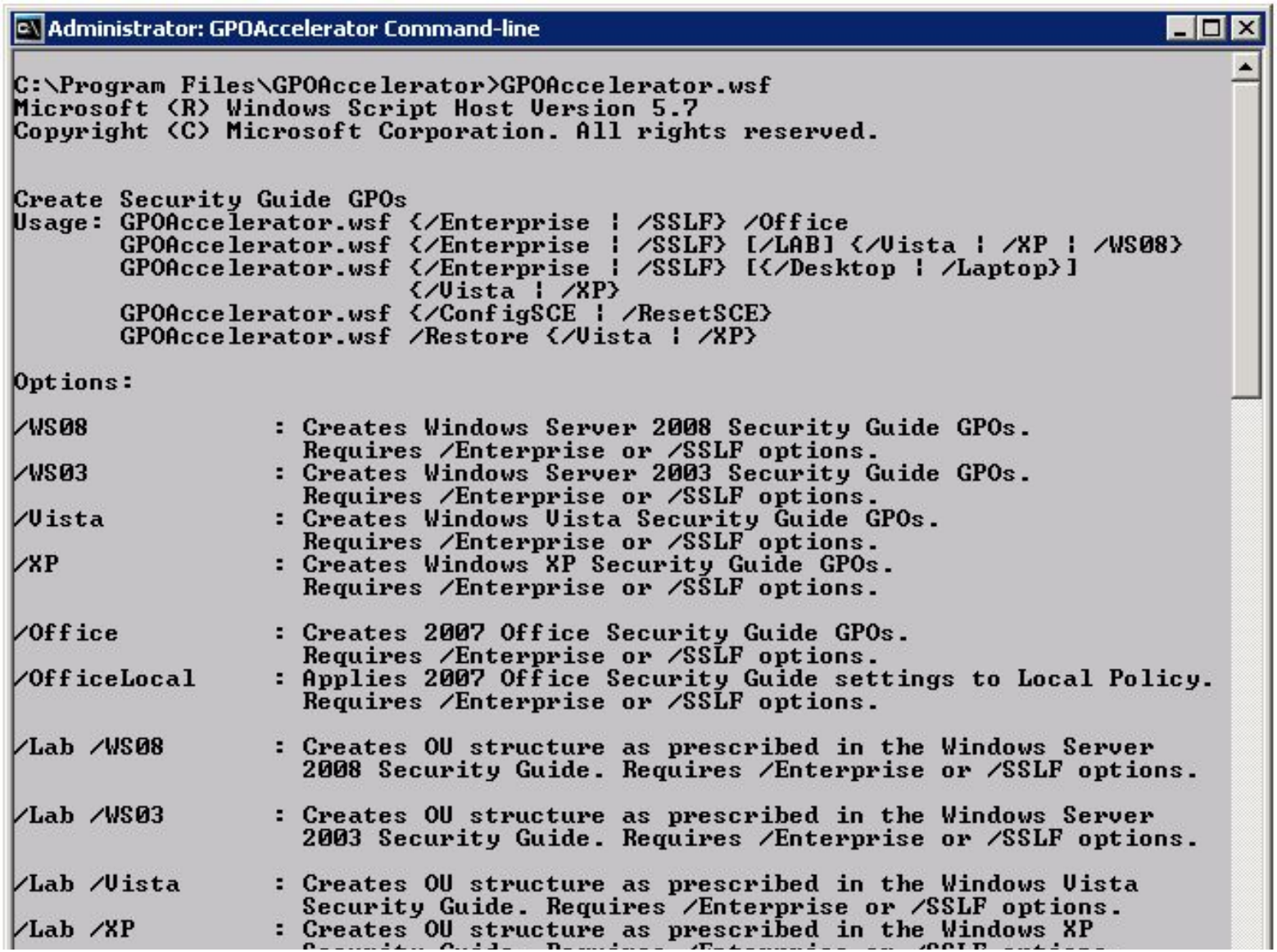
- A tool that you can use to create all the Group Policy objects (GPOs) you need to deploy your chosen security configuration.



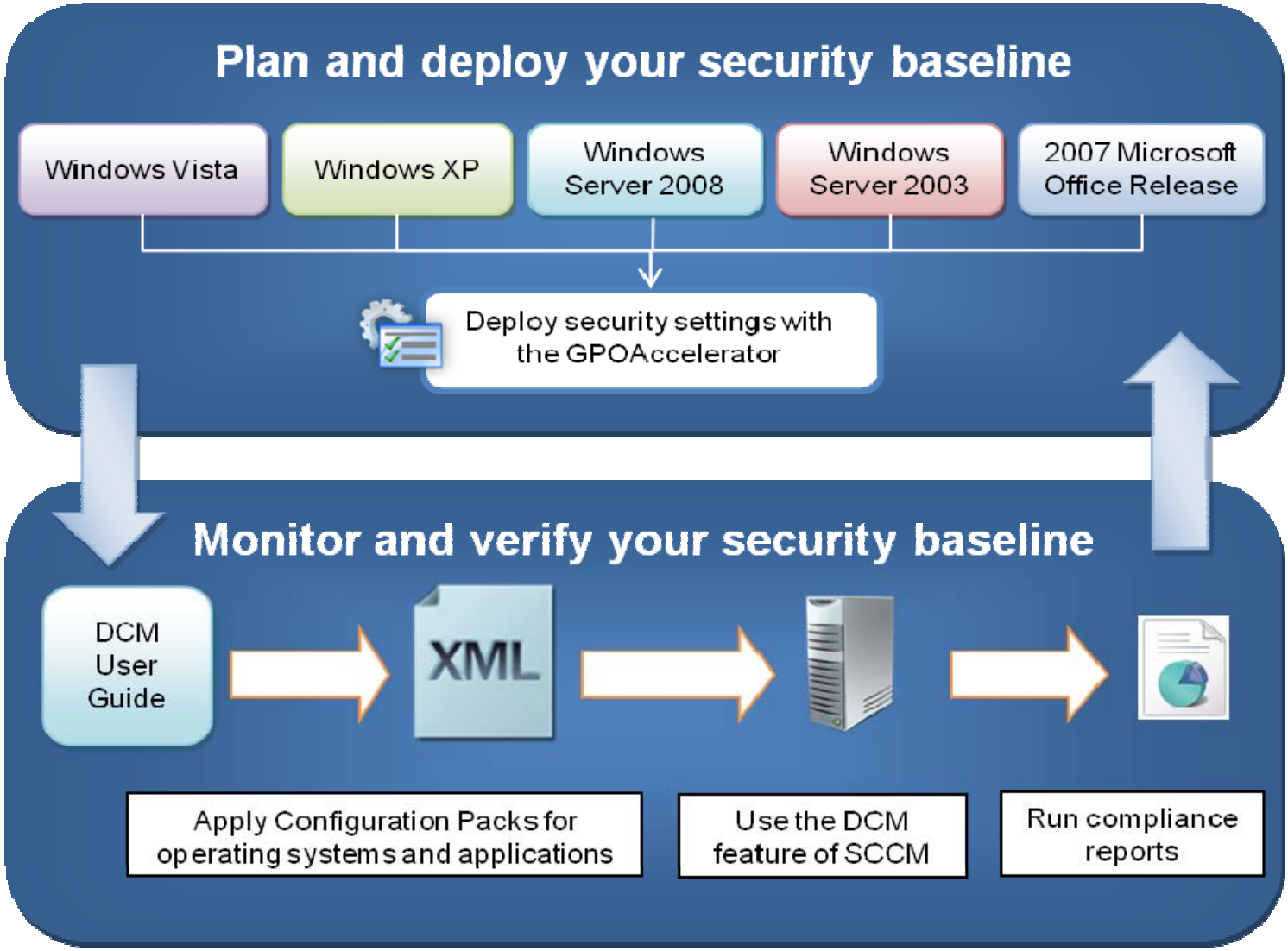
GPOAccelerator



GPOAccelerator (cont)



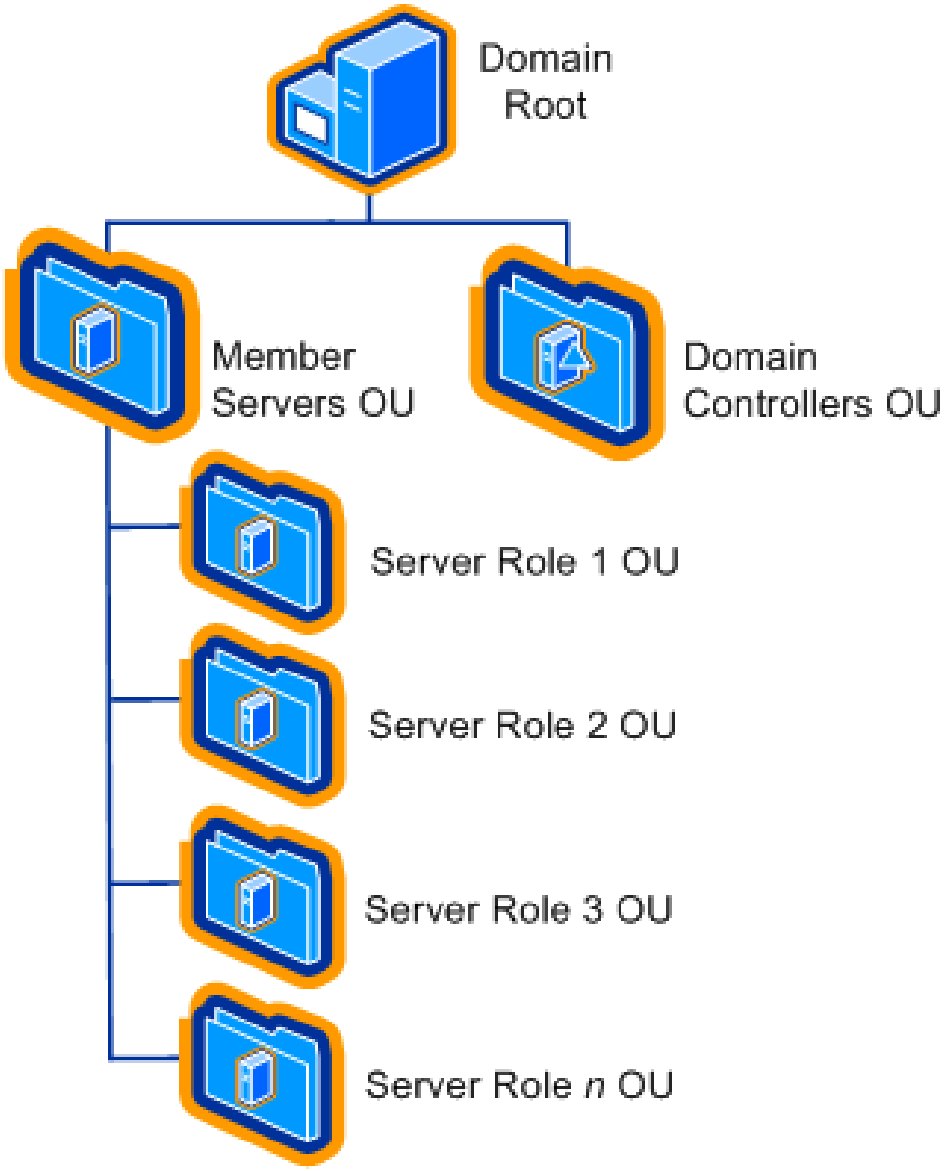
Baseline Compliance Management



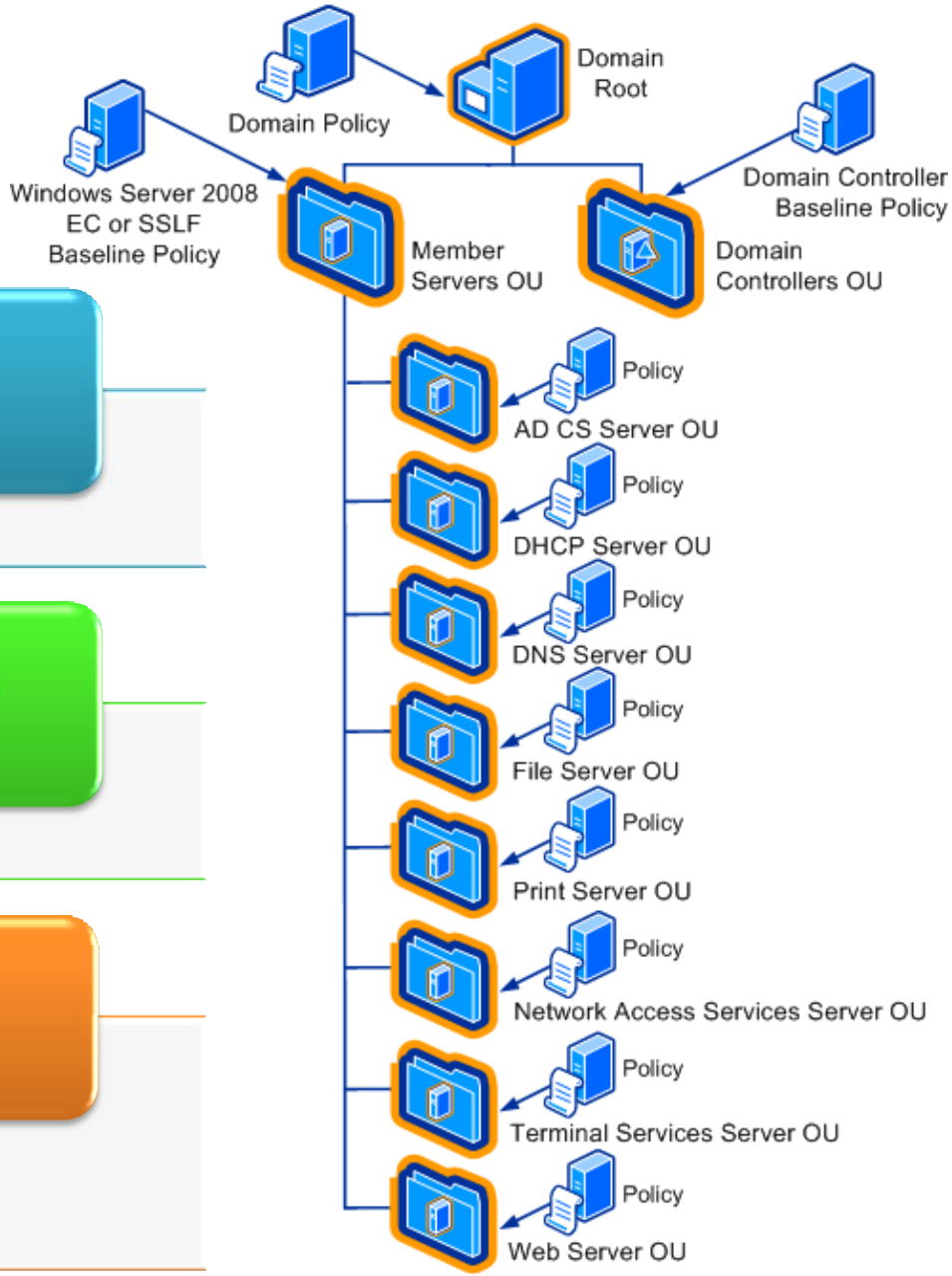
Security Baseline Environments

- The Legacy Client (LC) Environment
- The Enterprise Client (EC) Environment
- The Specialized Security – Limited Functionality (SSLF) Environment

Security Design



Example: OU Structure



Domain Root

Domain Controllers OU

Member Servers OU

- **Server Role OUs**

Example: OU Structure

Windows XP Users OU

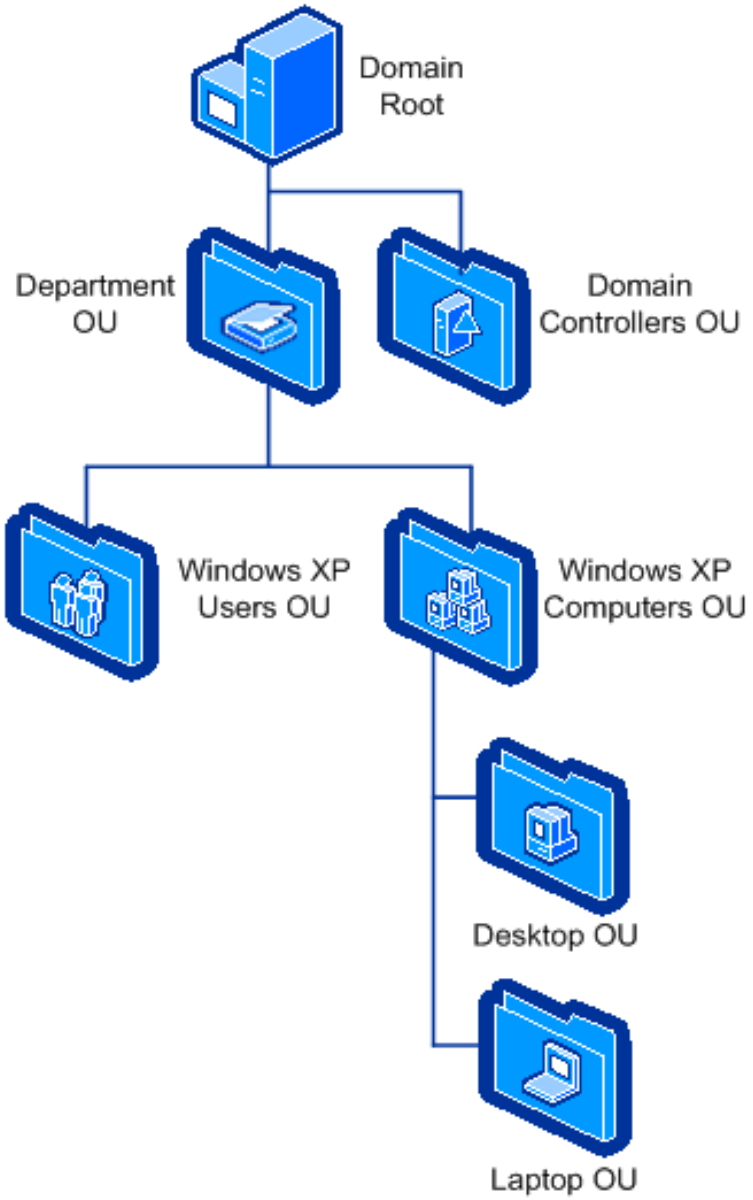
This OU contains the user accounts for the EC environment.

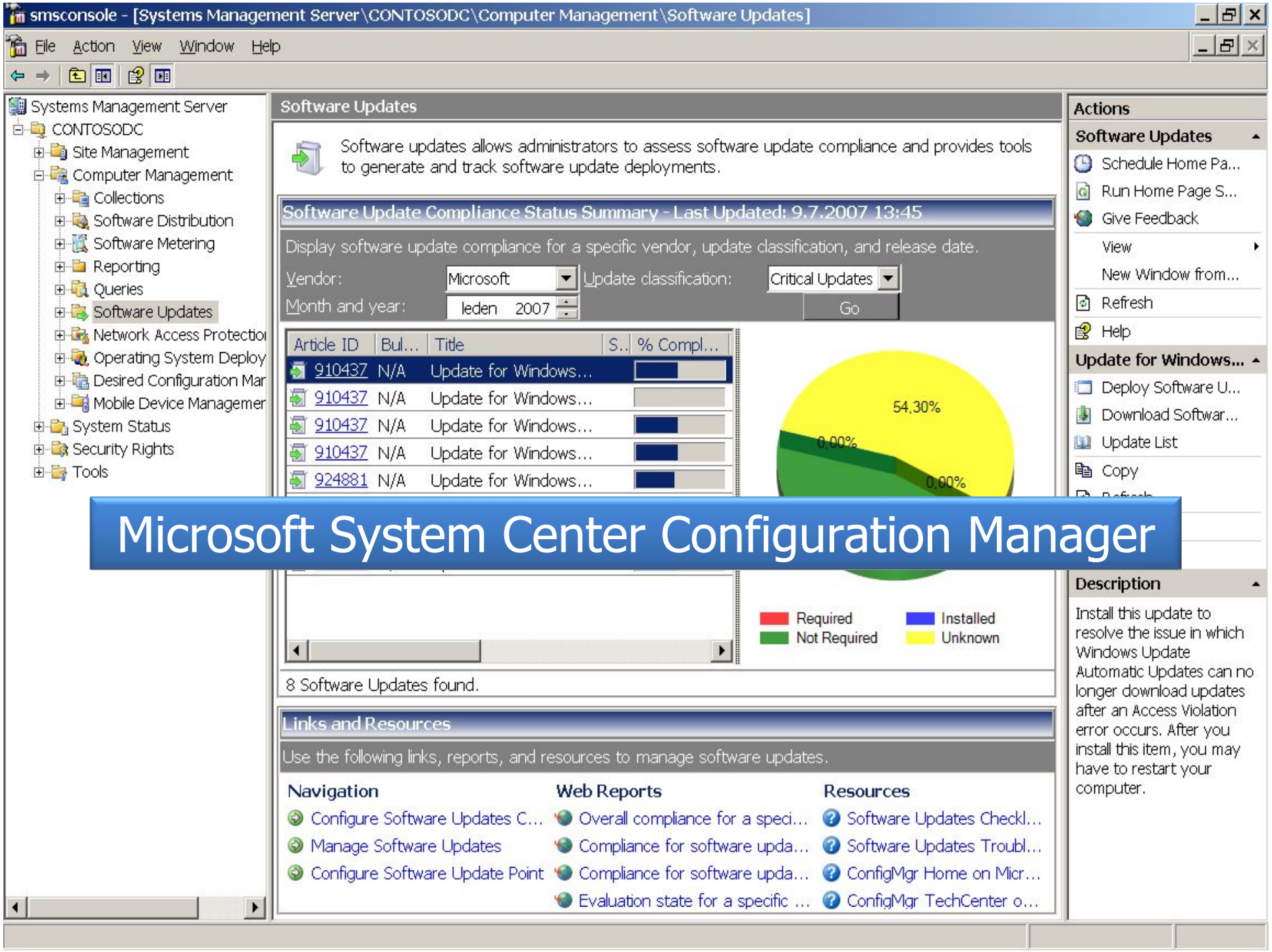
Windows XP Computers OU

This OU contains child OUs for each type of client in the EC environment.

Desktop OU. This OU contains desktop computers that constantly remain connected to the network.

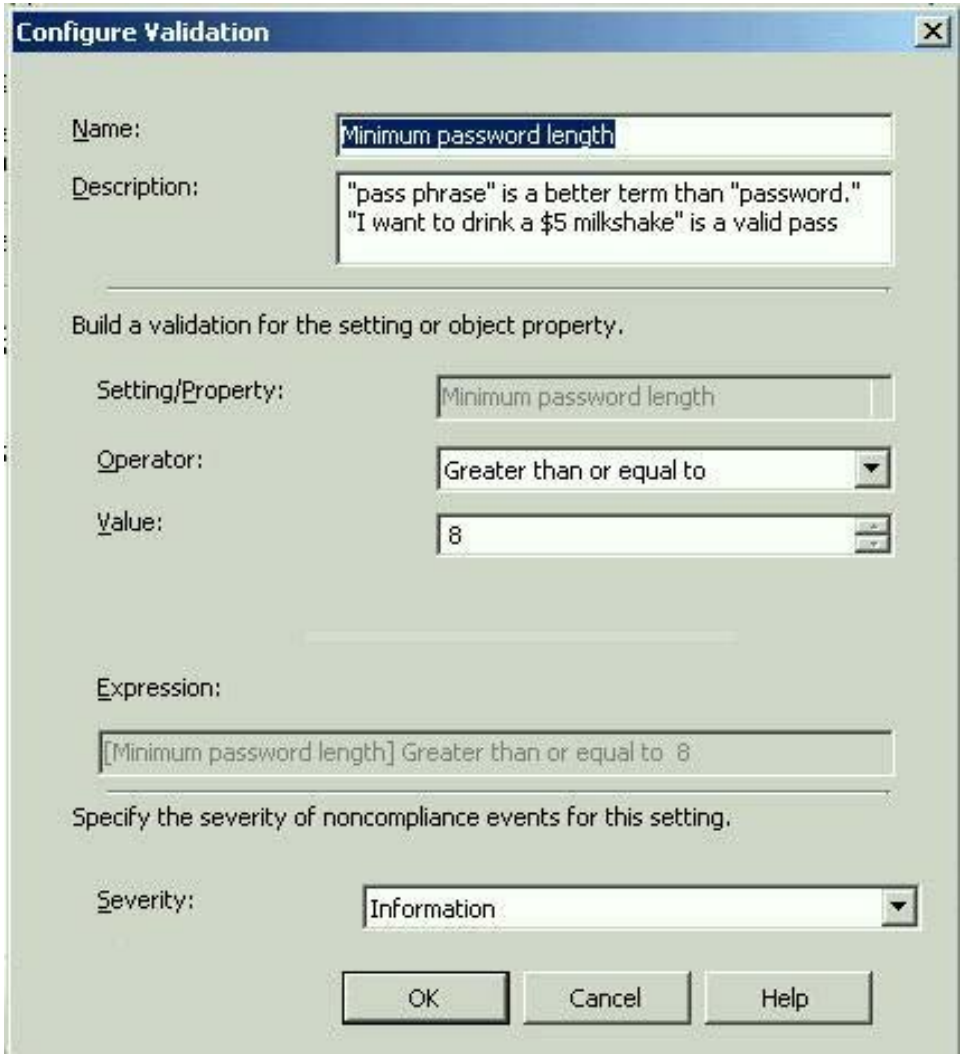
Laptop OU. This OU contains laptop computers for mobile users that are not always connected to the network.



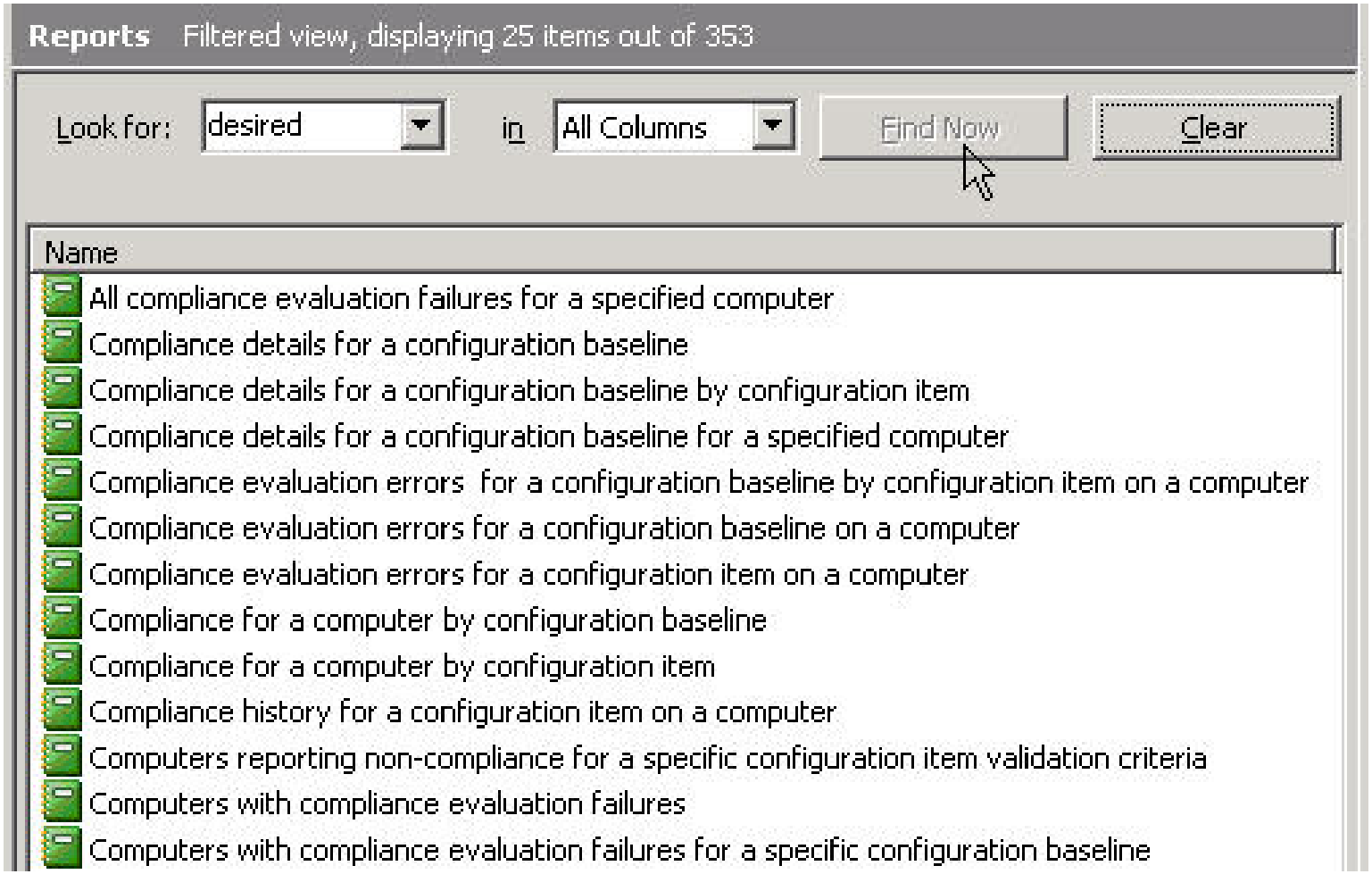


Microsoft System Center Configuration Manager

Example:
The Configure Validation dialog box



Example: Report



Ensuring Secure Computer Configurations

within the Federal Government

FDCC AND SCAP

Federal Desktop Core Configuration (FDCC)

- Standardized security configuration for Windows
- OMB and the CIO council seek to reduce federal systems vulnerability to individual and state sponsored cyber terrorism
  - "OMB Deep Dive" (Office of President initiative)
    - New government wide program (DOD, Intel, Civilian) that leverages existing components
- Deadline for deployment is February, 2008
- Scope of program requires automation

Information Security Automation Program (ISAP)

- Interagency (NIST, NSA, DISA, OSD, DHS) response to the need for consistent standards-based vulnerability management in the federal government and private industry.
- Automate the implementation of information system security controls in the IT systems through security-data sharing in standard formats.
- Security Content Automation Protocol (SCAP) is the technical implementation of ISAP

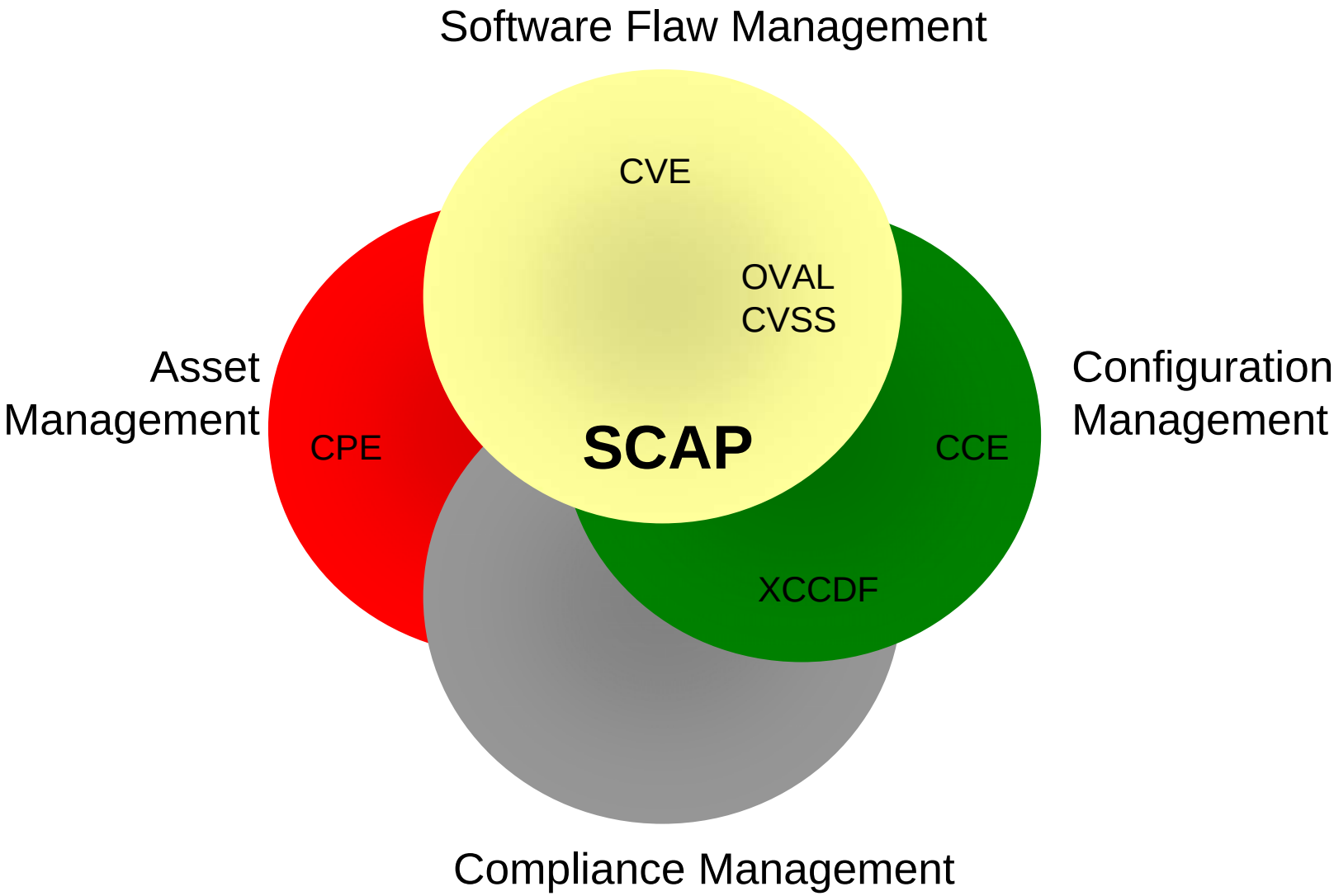
Security Content Automation Protocol (SCAP)

- Enables standardized and automated vulnerability management, measurement, and policy compliance evaluation (e.g., FISMA and DoD 8500.2/8510 compliance)
- Enumeration of vulnerabilities, misconfigurations, platforms, and impact
- Machine readable security configuration checklists

SCAP Components: Six open XML standards

Common Vulnerabilities and Exposures (CVE)	• Dictionary of security related software flaws
Common Configuration Enumeration (CCE)	• Dictionary of software misconfigurations
Common Platform Enumeration (CPE)	• Standard nomenclature and dictionary for product naming
eXtensible Checklist Configuration Description Format (XCCDF)	• Standard XML for specifying checklists
Open Vulnerability Assessment Language (OVAL)	• Standard XML for checking machine state
Common Vulnerability Scoring System (CVSS)	• Standard for scoring the impact of vulnerabilities

SCAP Interoperability



SCAP Vendors

SCCM and SCAP

SCAP Checklists

- SCAP Checklists:
  - Windows Vista (FDCC Profile)
  - Windows XP (FDCC Profile)
  - Windows Vista Firewall (FDCC Profile)
  - Windows XP Firewall (FDCC Profile)
  - Windows Server 2003
  - Red Hat Linux
  - Internet Explorer 7 (FDCC Profile)
  - Microsoft Office 2007
  - Symantec Antivirus

SCAP Compliance Program

- Ensuring security tools
  - comply to the NIST Security Content Automation Protocol (SCAP)
  - enable agencies to continuously monitor systems against OMB mandated configuration settings (results mapped to FISMA)
- Supports Multiple Initiatives:
  - OMB FDCC Secure Configuration Effort
  - NIST FISMA Implementation Phase II (also applies to NIST HIPAA work)
  - Information Security Automation Program (ISAP): OSD, DISA, NSA, DHS, NIST
  - OSD Computer Network Defense Pilot
  - NIST Checklist Program
  - NIST National Vulnerability Database