Enhancing SCAP:
Whitelist-based Image Management

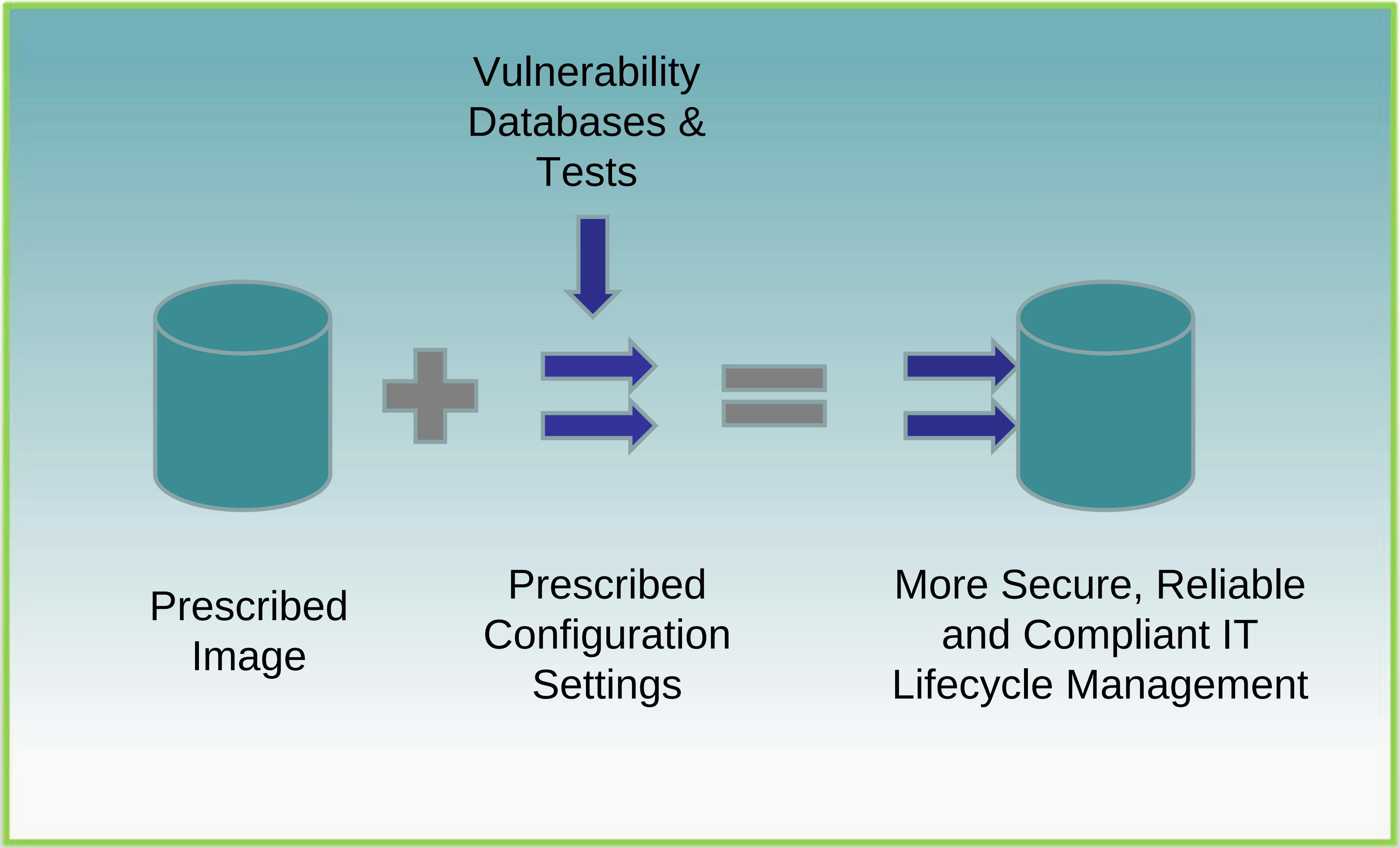
W. Wyatt Starnes

SignaCert, Inc. - Founder and CEO

ITSA Conference – October 2009

Enhancing SCAP:

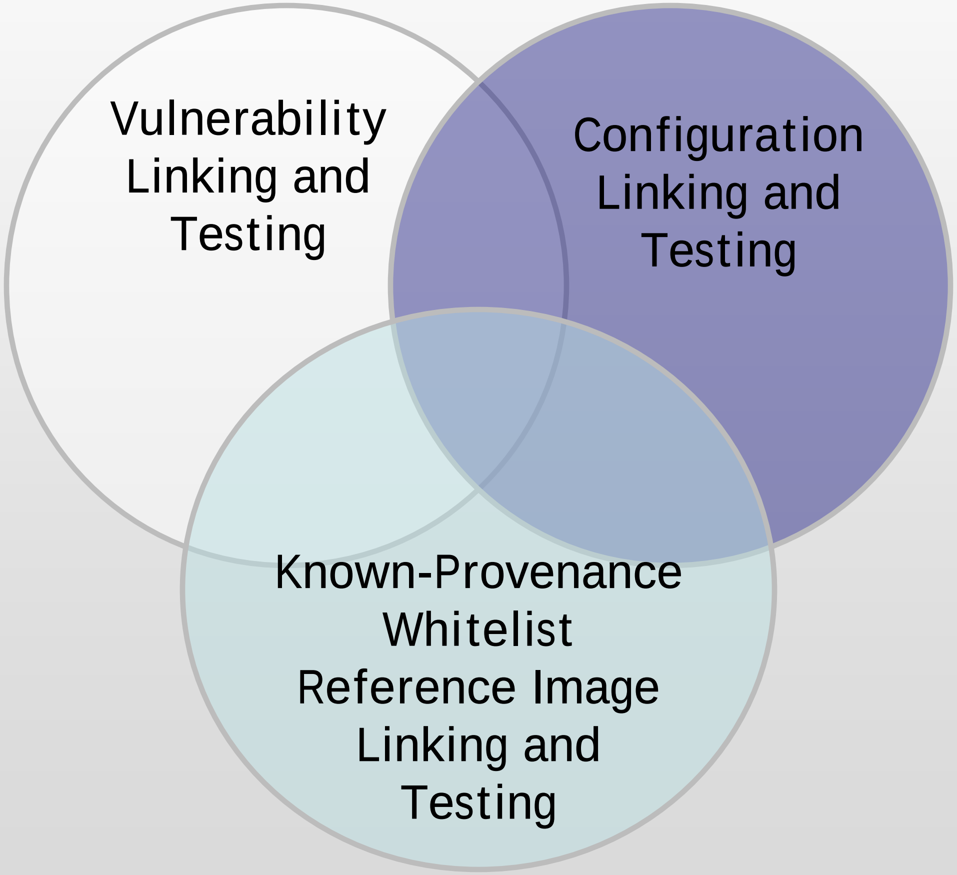
Whitelist, Configuration and Vulnerability Management



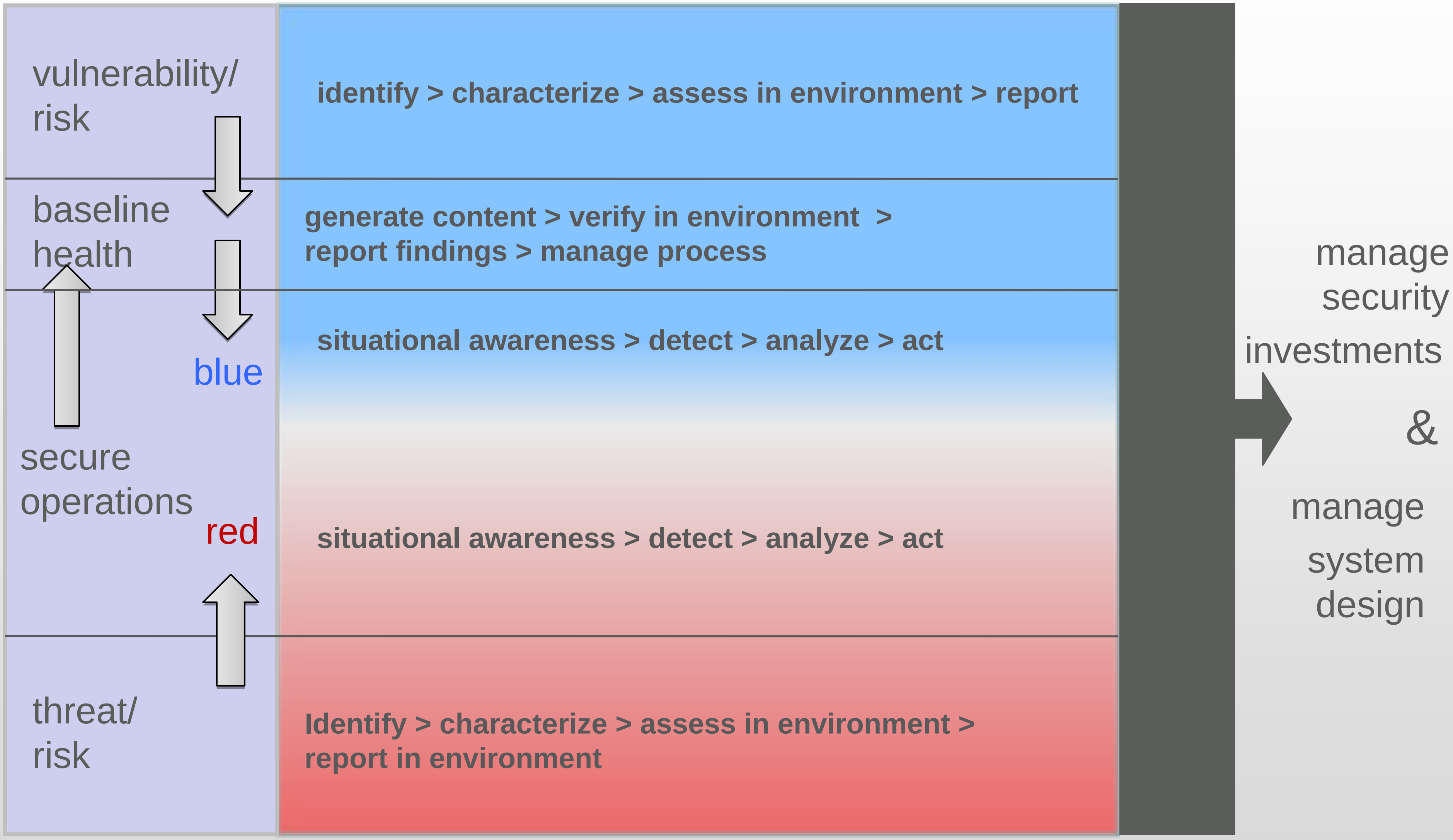
Vulnerability Databases & Tests
Prescribed Image
Prescribed Configuration Settings
More Secure, Reliable and Compliant IT Lifecycle Management

Enhancing SCAP with Whitelisting

A Leapfrog in Methods


Vulnerability Linking and Testing
Configuration Linking and Testing
Known-Provenance Whitelist Reference Image Linking and Testing

Bringing it All Together



vulnerability/ risk

identify > characterize > assess in environment > report

baseline health

generate content > verify in environment > report findings > manage process

situational awareness > detect > analyze > act

blue

secure operations

red

situational awareness > detect > analyze > act

threat/ risk

Identify > characterize > assess in environment > report in environment

manage security investments

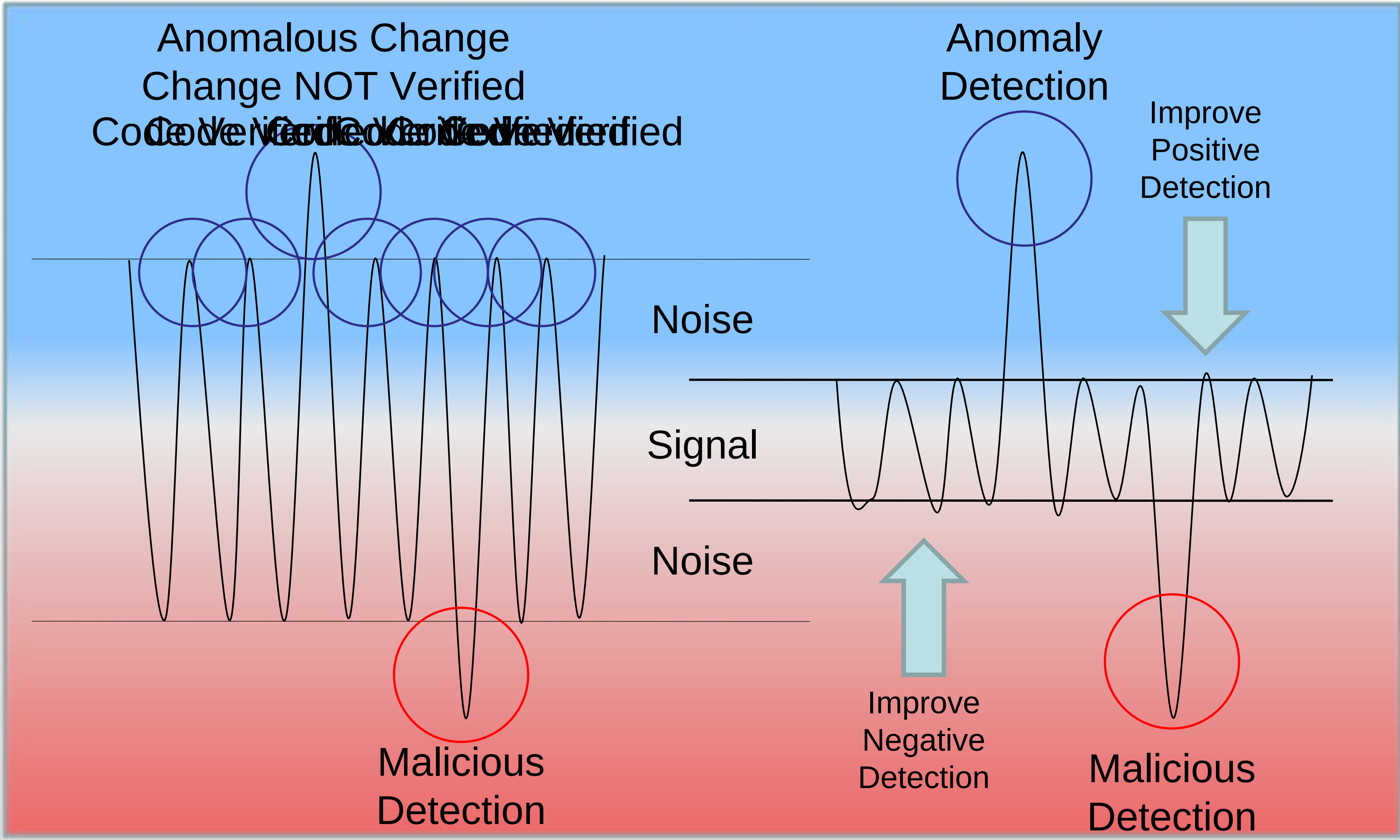
&

manage system design

Closing the Blind Spot:

Adding the Positive, Whitelist Attestation View

Whitelist View



Anomalous Change

Change NOT Verified

Code Verified

Noise

Signal

Noise

Malicious Detection

Anomaly Detection

Improve Positive Detection

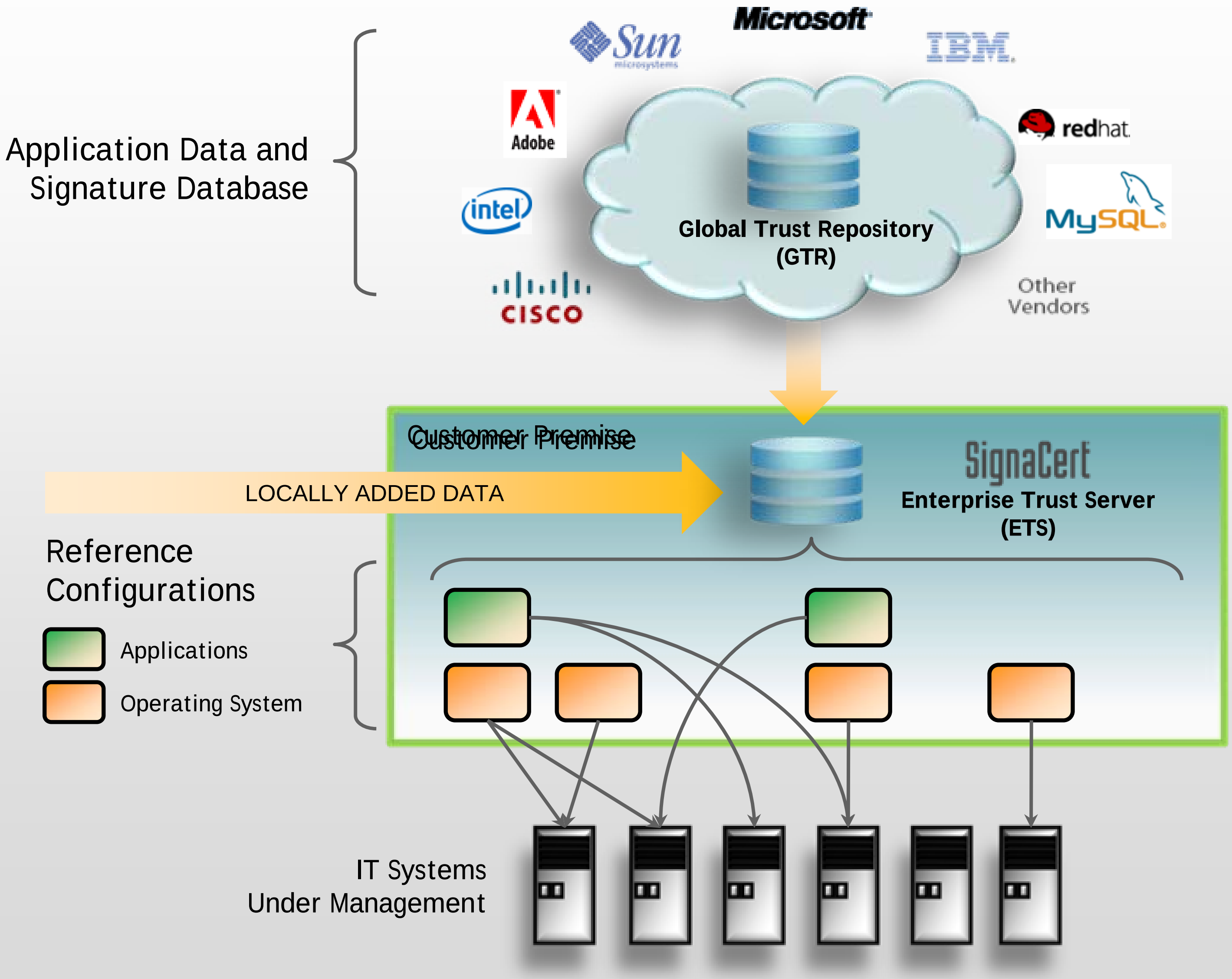
Improve Negative Detection

Malicious Detection

Blacklist View

Enhanced SCAP:

An Architecture for Immediate Delivery



Application Data and Signature Database

Global Trust Repository (GTR)

Customer Premise

Customer Premise

LOCALLY ADDED DATA

SignaCert Enterprise Trust Server (ETS)

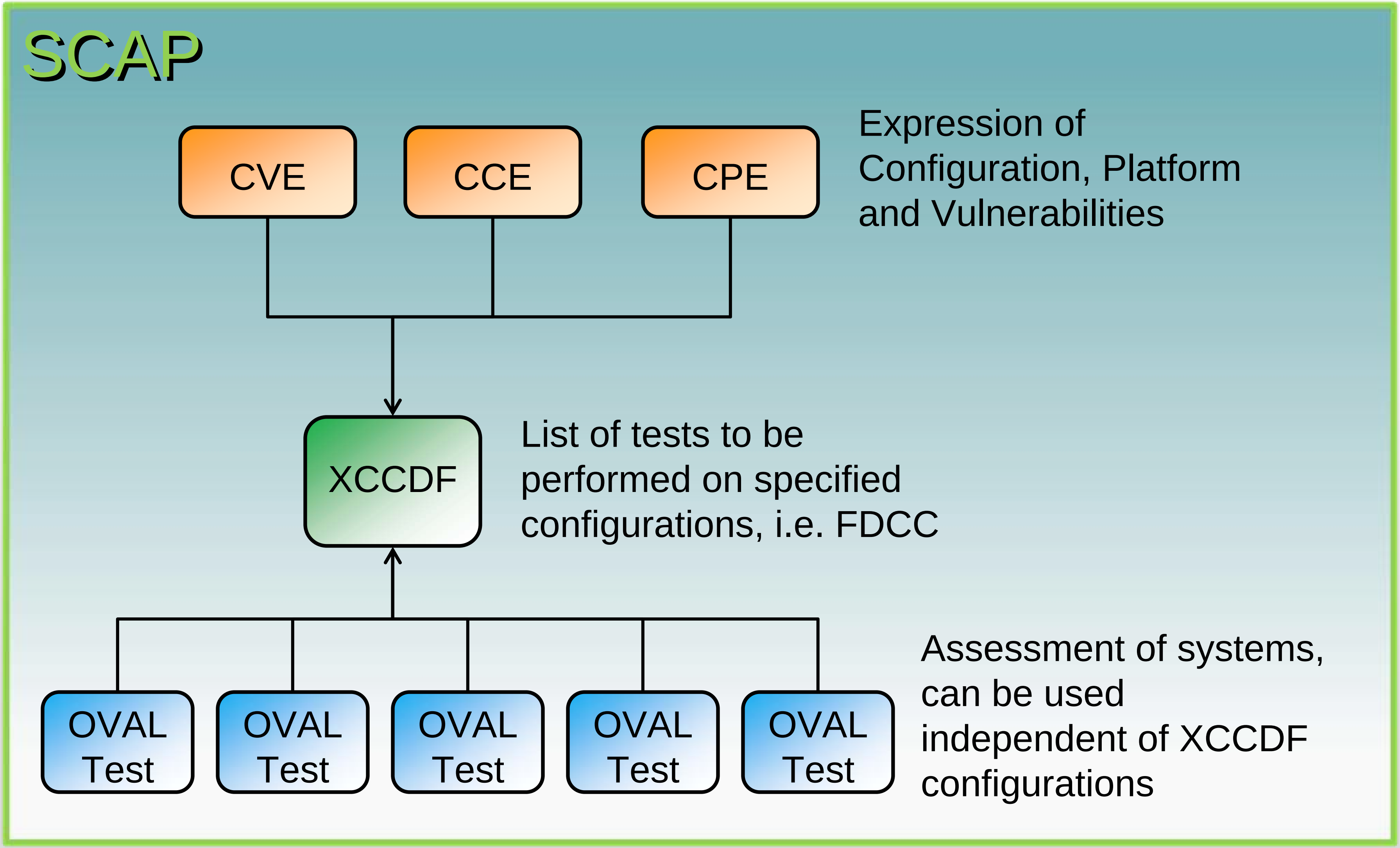
Reference Configurations

🟩 Applications

🟧 Operating System

IT Systems Under Management

SCAP Today



SCAP

CVE

CCE

CPE

Expression of Configuration, Platform and Vulnerabilities

XCCDF

List of tests to be performed on specified configurations, i.e. FDCC

OVAL Test

OVAL Test

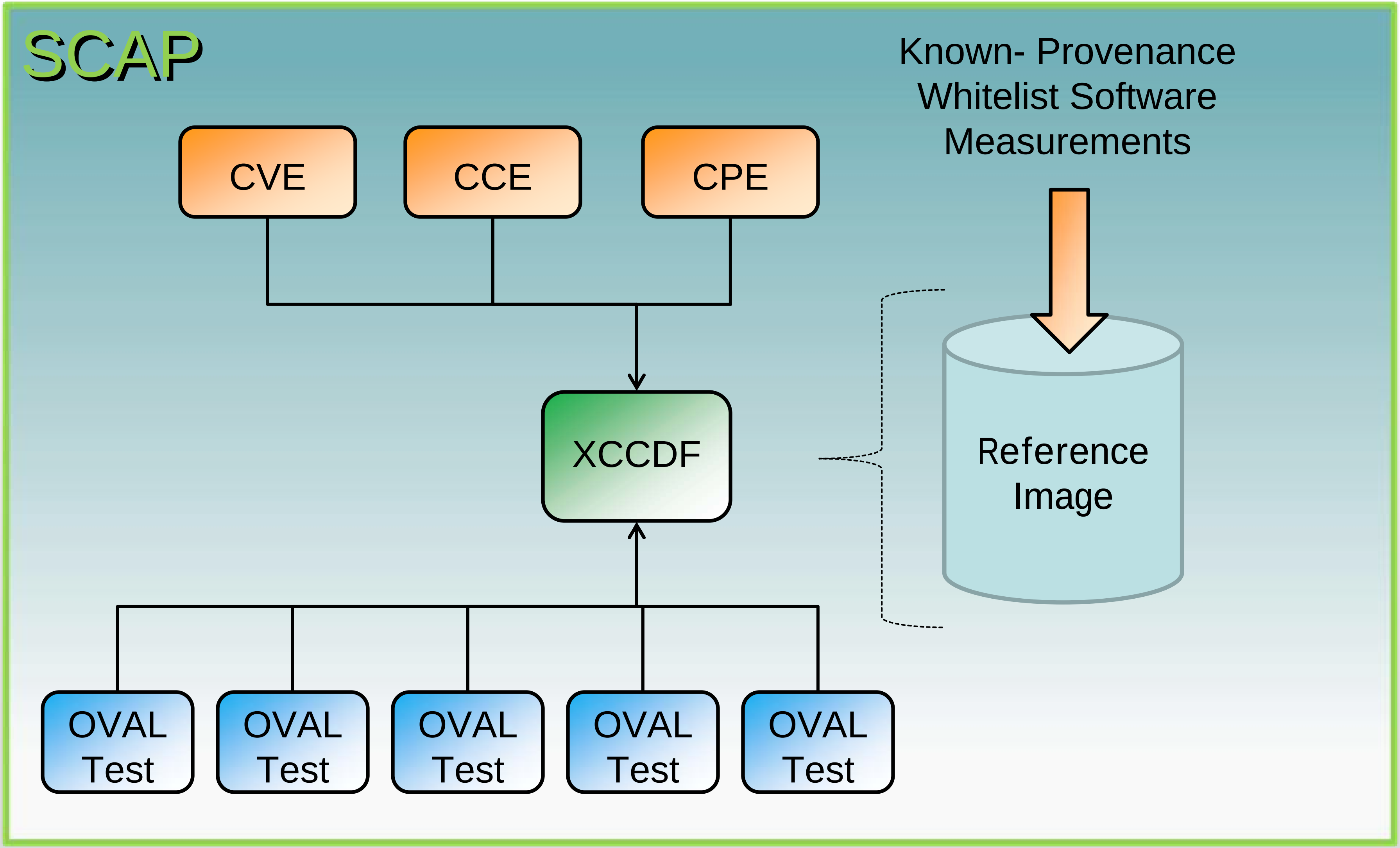
OVAL Test

OVAL Test

OVAL Test

Assessment of systems, can be used independent of XCCDF configurations

Enhanced SCAP with Image Referencing



Total SCAP:

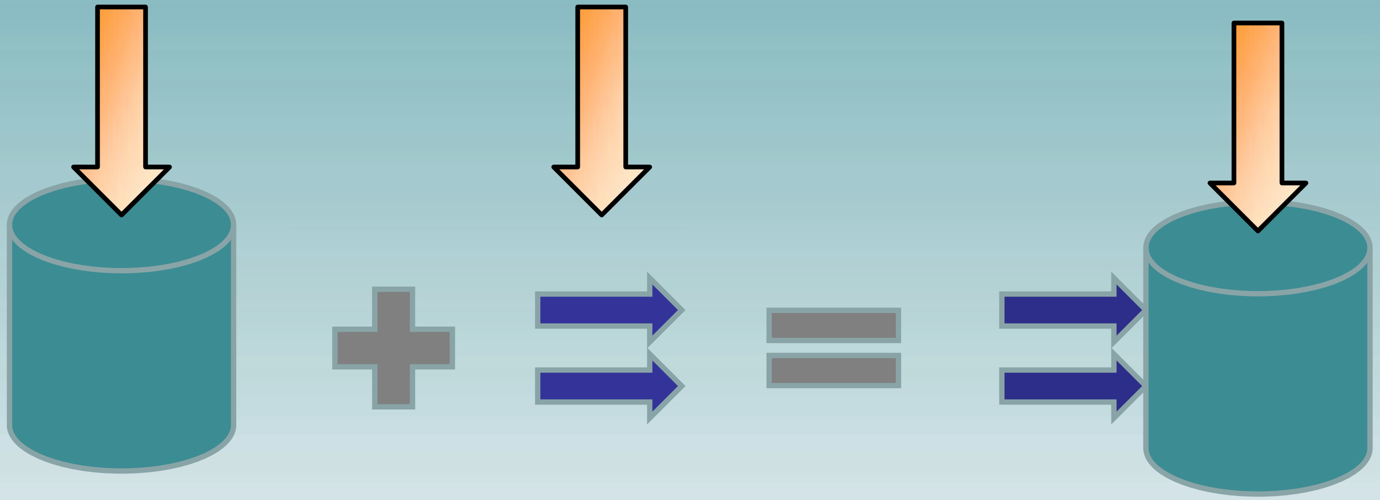
Whitelist, Configuration and Vulnerability Management

SignaCert

Known-Provence Whitelist Software Measurements

SCAP-derived Configuration Settings

SCAP-derived Vulnerability Checking



Pre-established Reference Image

Defined and Verified Configuration Settings

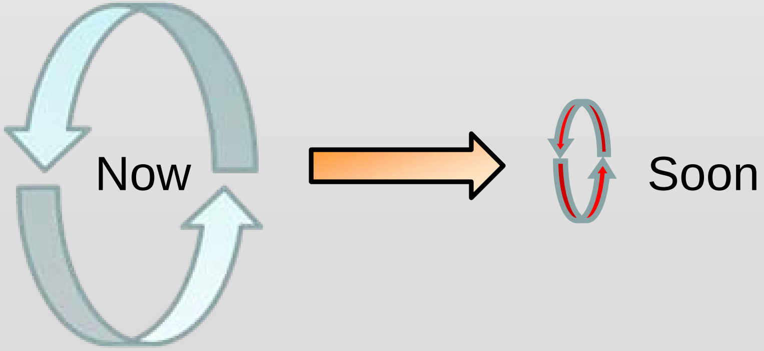
More Secure, Reliable and Compliant Continuous Monitoring = ***Operational Readiness***

Moving from C&A to Continuous Monitoring:

Assuring Operational Readiness

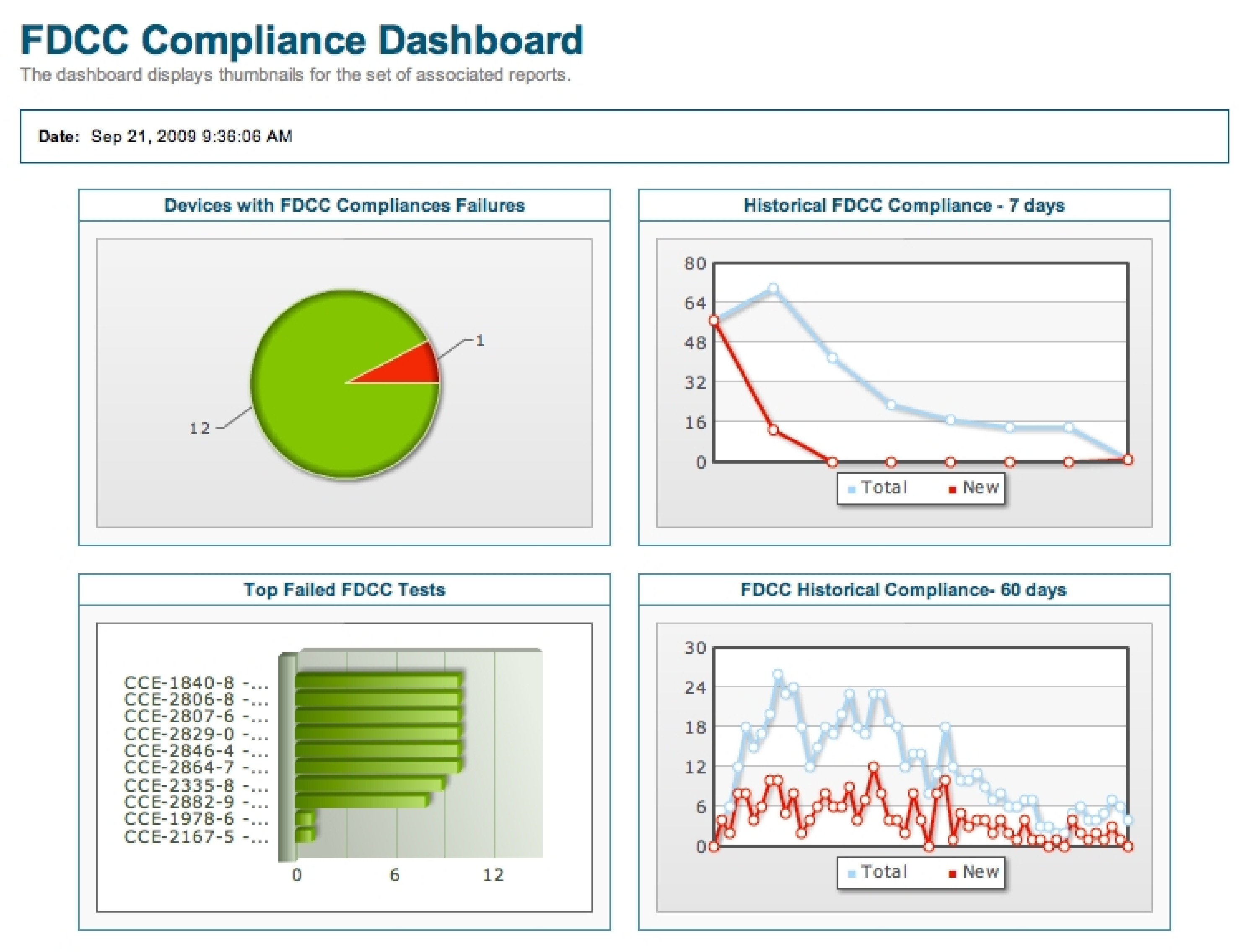
- Certification and Accreditation
  - Slow
  - Expense
  - Out-of-date before completion
  - Financial and human capital resource drain
  - Results in:

- Continuous Monitoring
  - Faster OODA[1] cycle (goal is near real time for critical systems)
  - Broader sensor view (whitelist plus blacklist)
  - Higher fidelity change detection improves availability and uptime while reducing OpEx



[1] OODA: Observe, Orient, Decide, Act

SCAP – FDCC Dashboard



FDCC Compliance Dashboard

The dashboard displays thumbnails for the set of associated reports.

Date: Sep 21, 2009 9:36:06 AM

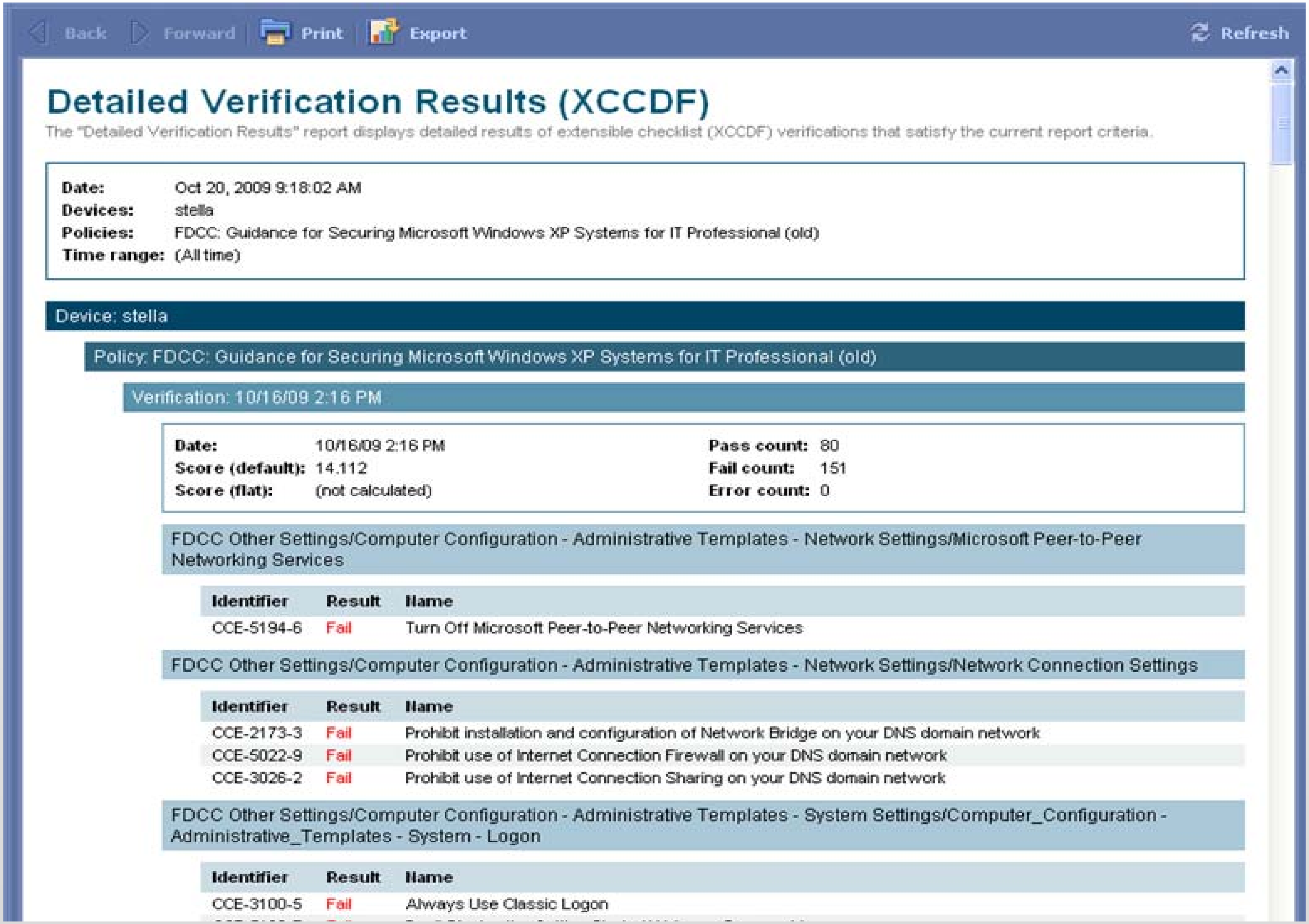
Devices with FDCC Compliances Failures

Historical FDCC Compliance - 7 days

Top Failed FDCC Tests

FDCC Historical Compliance- 60 days

Detailed XCCDF Results for FDCC



Detailed Verification Results (XCCDF)

The "Detailed Verification Results" report displays detailed results of extensible checklist (XCCDF) verifications that satisfy the current report criteria.

Date:	Oct 20, 2009 9:18:02 AM
Devices:	stella
Policies:	FDCC: Guidance for Securing Microsoft Windows XP Systems for IT Professional (old)
Time range:	(All time)

Device: stella

Policy: FDCC: Guidance for Securing Microsoft Windows XP Systems for IT Professional (old)

Verification: 10/16/09 2:16 PM

Date:	10/16/09 2:16 PM	**Pass count:**	80
Score (default):	14.112	**Fail count:**	151
Score (flat):	(not calculated)	**Error count:**	0

FDCC Other Settings/Computer Configuration - Administrative Templates - Network Settings/Microsoft Peer-to-Peer Networking Services

Identifier	Result	Name
CCE-5194-6	Fail	Turn Off Microsoft Peer-to-Peer Networking Services

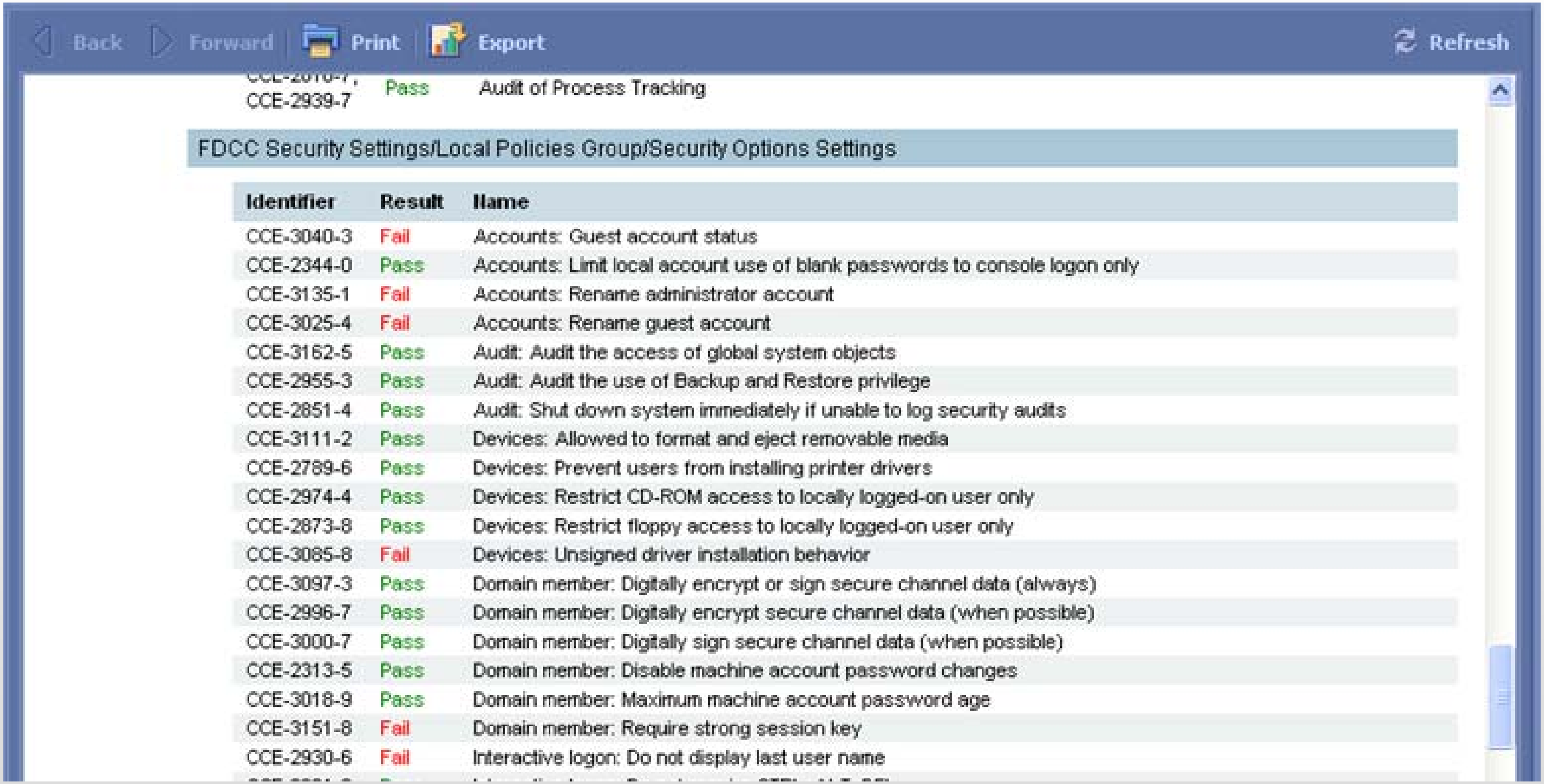
FDCC Other Settings/Computer Configuration - Administrative Templates - Network Settings/Network Connection Settings

Identifier	Result	Name
CCE-2173-3	Fail	Prohibit installation and configuration of Network Bridge on your DNS domain network
CCE-5022-9	Fail	Prohibit use of Internet Connection Firewall on your DNS domain network
CCE-3026-2	Fail	Prohibit use of Internet Connection Sharing on your DNS domain network

FDCC Other Settings/Computer Configuration - Administrative Templates - System Settings/Computer_Configuration - Administrative_Templates - System - Logon

Identifier	Result	Name
CCE-3100-5	Fail	Always Use Classic Logon

FDCC Cont. - Security Settings

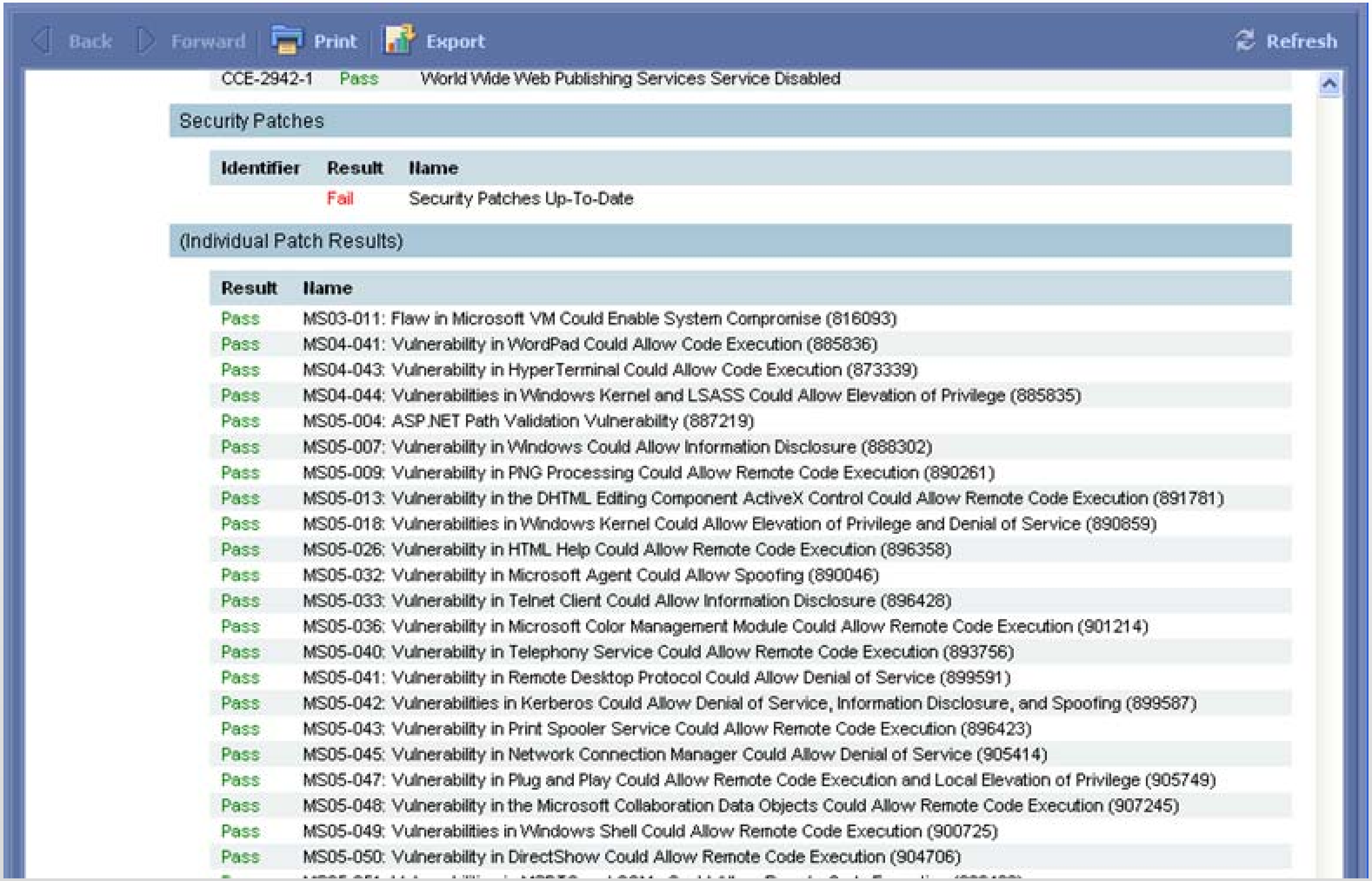


[illegible], CCE-2939-7	Pass	Audit of Process Tracking

FDCC Security Settings/Local Policies Group/Security Options Settings

Identifier	Result	Name
CCE-3040-3	Fail	Accounts: Guest account status
CCE-2344-0	Pass	Accounts: Limit local account use of blank passwords to console logon only
CCE-3135-1	Fail	Accounts: Rename administrator account
CCE-3025-4	Fail	Accounts: Rename guest account
CCE-3162-5	Pass	Audit: Audit the access of global system objects
CCE-2955-3	Pass	Audit: Audit the use of Backup and Restore privilege
CCE-2851-4	Pass	Audit: Shut down system immediately if unable to log security audits
CCE-3111-2	Pass	Devices: Allowed to format and eject removable media
CCE-2789-6	Pass	Devices: Prevent users from installing printer drivers
CCE-2974-4	Pass	Devices: Restrict CD-ROM access to locally logged-on user only
CCE-2873-8	Pass	Devices: Restrict floppy access to locally logged-on user only
CCE-3085-8	Fail	Devices: Unsigned driver installation behavior
CCE-3097-3	Pass	Domain member: Digitally encrypt or sign secure channel data (always)
CCE-2996-7	Pass	Domain member: Digitally encrypt secure channel data (when possible)
CCE-3000-7	Pass	Domain member: Digitally sign secure channel data (when possible)
CCE-2313-5	Pass	Domain member: Disable machine account password changes
CCE-3018-9	Pass	Domain member: Maximum machine account password age
CCE-3151-8	Fail	Domain member: Require strong session key
CCE-2930-6	Fail	Interactive logon: Do not display last user name

FDCC Cont. - Patches



CCE-2942-1	Pass	World Wide Web Publishing Services Service Disabled

Security Patches

Identifier	Result	Name
	Fail	Security Patches Up-To-Date

(Individual Patch Results)

Result	Name
Pass	MS03-011: Flaw in Microsoft VM Could Enable System Compromise (816093)
Pass	MS04-041: Vulnerability in WordPad Could Allow Code Execution (885836)
Pass	MS04-043: Vulnerability in HyperTerminal Could Allow Code Execution (873339)
Pass	MS04-044: Vulnerabilities in Windows Kernel and LSASS Could Allow Elevation of Privilege (885835)
Pass	MS05-004: ASP.NET Path Validation Vulnerability (887219)
Pass	MS05-007: Vulnerability in Windows Could Allow Information Disclosure (888302)
Pass	MS05-009: Vulnerability in PNG Processing Could Allow Remote Code Execution (890261)
Pass	MS05-013: Vulnerability in the DHTML Editing Component ActiveX Control Could Allow Remote Code Execution (891781)
Pass	MS05-018: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege and Denial of Service (890859)
Pass	MS05-026: Vulnerability in HTML Help Could Allow Remote Code Execution (896358)
Pass	MS05-032: Vulnerability in Microsoft Agent Could Allow Spoofing (890046)
Pass	MS05-033: Vulnerability in Telnet Client Could Allow Information Disclosure (896428)
Pass	MS05-036: Vulnerability in Microsoft Color Management Module Could Allow Remote Code Execution (901214)
Pass	MS05-040: Vulnerability in Telephony Service Could Allow Remote Code Execution (893756)
Pass	MS05-041: Vulnerability in Remote Desktop Protocol Could Allow Denial of Service (899591)
Pass	MS05-042: Vulnerabilities in Kerberos Could Allow Denial of Service, Information Disclosure, and Spoofing (899587)
Pass	MS05-043: Vulnerability in Print Spooler Service Could Allow Remote Code Execution (896423)
Pass	MS05-045: Vulnerability in Network Connection Manager Could Allow Denial of Service (905414)
Pass	MS05-047: Vulnerability in Plug and Play Could Allow Remote Code Execution and Local Elevation of Privilege (905749)
Pass	MS05-048: Vulnerability in the Microsoft Collaboration Data Objects Could Allow Remote Code Execution (907245)
Pass	MS05-049: Vulnerabilities in Windows Shell Could Allow Remote Code Execution (900725)
Pass	MS05-050: Vulnerability in DirectShow Could Allow Remote Code Execution (904706)

The Benefits of Enhanced SCAP Delivery

- One Operational SCAP platform to Define and Manage:
  - Domain-specific reference images
  - Prescribed Configuration Settings
  - Threat, Risk and Vulnerably Feeds (Active and Automated)
- Deploying Command and Control infrastructure to support:
  - Initial Device Build & Deployment
  - Ongoing IT Device System Maintenance
  - Closed-Loop IT Operational Lifecycle Management
- Dimensional reporting supports different mission objectives:
  - Security
  - Compliance
  - Improved Availability
  - Reduced Operational Cost
- Moving from C&A to **Continuous Monitoring**

SignaCert 3.6 Product Release

SCAP enabled product release

- Native XCCDF and OVAL in and out
- All platform and device types supported
- Ability to support “live” threat and vulnerability feeds
- Ability to accept risk/vulnerability/thread intelligence and map precisely where that risk may exist in the domain (enabled by high-resolution image intelligence)
- Is an highly-scalable “Continuous Monitoring” solution designed from the ground up for data center operations

See us at booth ITSA Booth 125

SignaCert 3.6 Product Release

SCAP enabled product release - Continued

- No additional cost or "add-on modules" for FDCC auditing – included in the SignaCert ETS platform
- Known-provenance reference image management included standard as part of the FDCC offering allowing customers to cover the "blind spot" in image management
- Partner-friendly solution provides simplified integration with endpoint, enterprise management solutions and issue tracking/trouble ticket solutions

See us at booth ITSA Booth 125