SCAP Methods – Present and Future

A brief overview of the “Positive Assertion Model” as it applies to Security Content Automation Protocol (SCAP) and the Federal Desktop Core Configuration (FDCC)

Sol Cates – Sept 20th 2007

Specification and Methods under SCAP

SignaCert

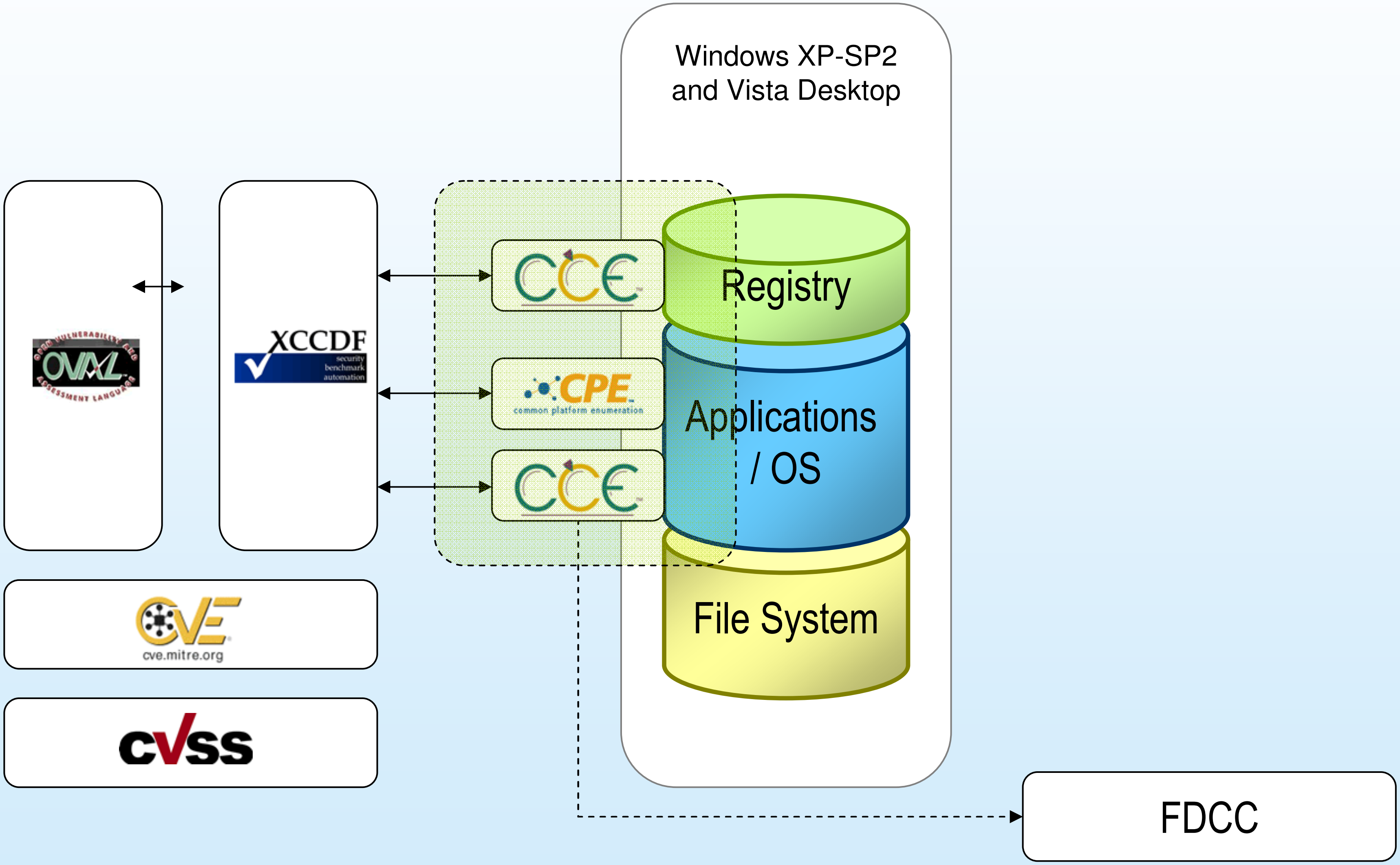
MITRE	CVE cve.mitre.org	**CVE**	Common Vulnerabilities and Exposures	Standard nomenclature and dictionary of security related software flaws
MITRE	CCE	**CCE**	Common Configuration Enumeration	Standard nomenclature and dictionary of software misconfigurations
MITRE	CPE common platform enumeration	**CPE**	Common Platform Enumeration	Standard nomenclature and dictionary for product naming
National Security Agency United States of America	XCCDF security benchmark automation	**XCCDF**	eXtensible Checklist Configuration Description Format	Standard XML for specifying checklists and for reporting results of checklist evaluation
MITRE	Open Vulnerability and Assessment Language OVAL	**OVAL**	Open Vulnerability Assessment Language	Standard XML for testing procedures
FIRST Improving Security Together	CVSS	**CVSS**	Common Vulnerability Scoring System	Standard for measuring the impact of vulnerabilities

Overview

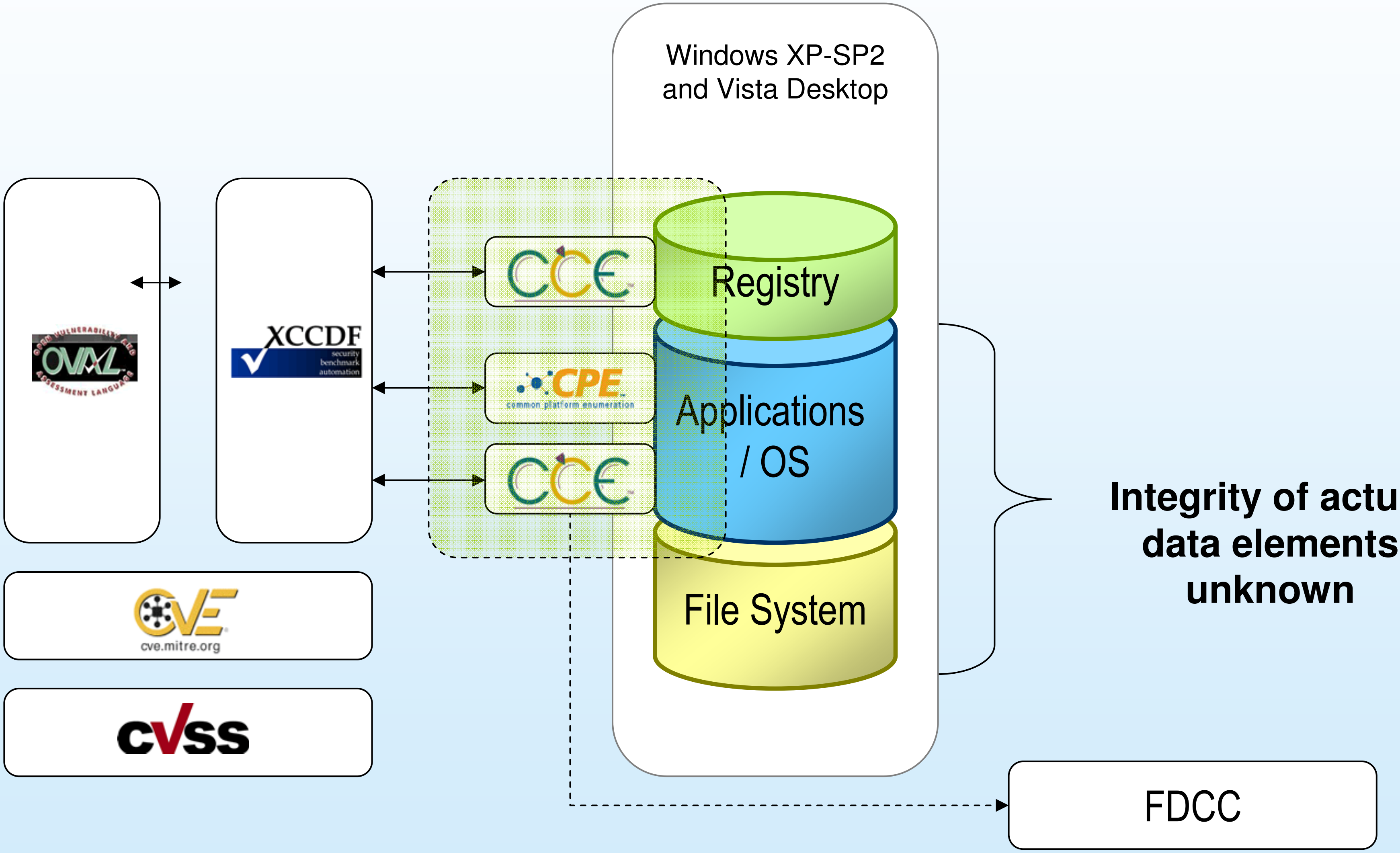
SignaCert

- The current SCAP and FDCC methods focus on the verification and validation of the CONTROL and CONFIGURATION elements themselves, such as:
  - Testing the registry for approved configuration settings and patch levels.
  - Scanning application settings for secure and approved configurations.
  - Querying NTFS for file version information of application files.
- These "second order" methods leave an integrity gap
  - "Configuration" verification should incorporate the components of the platform as well – binaries, libraries, images, etc…

Mapping the Specs to the Desktop

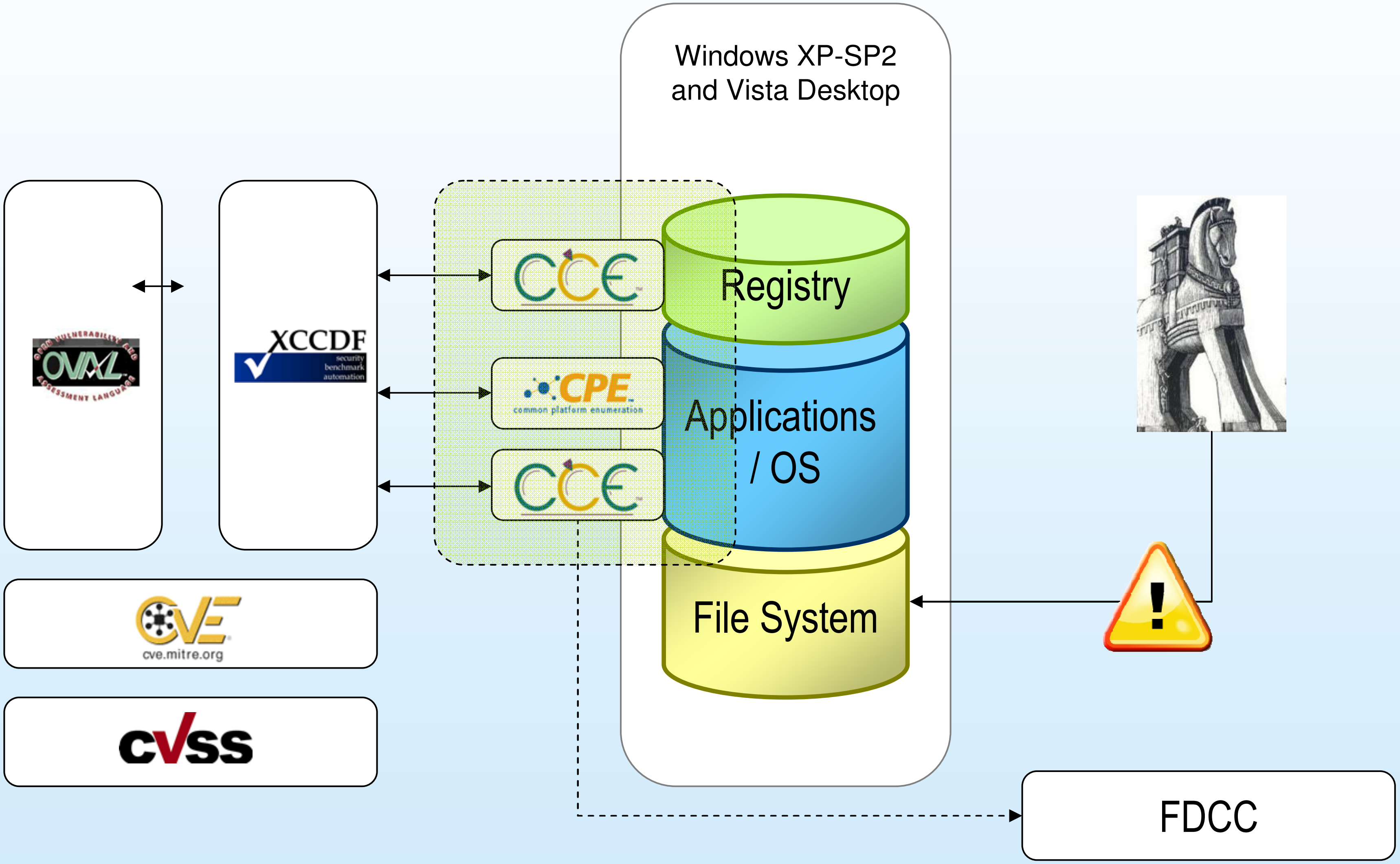


Coverage Gaps

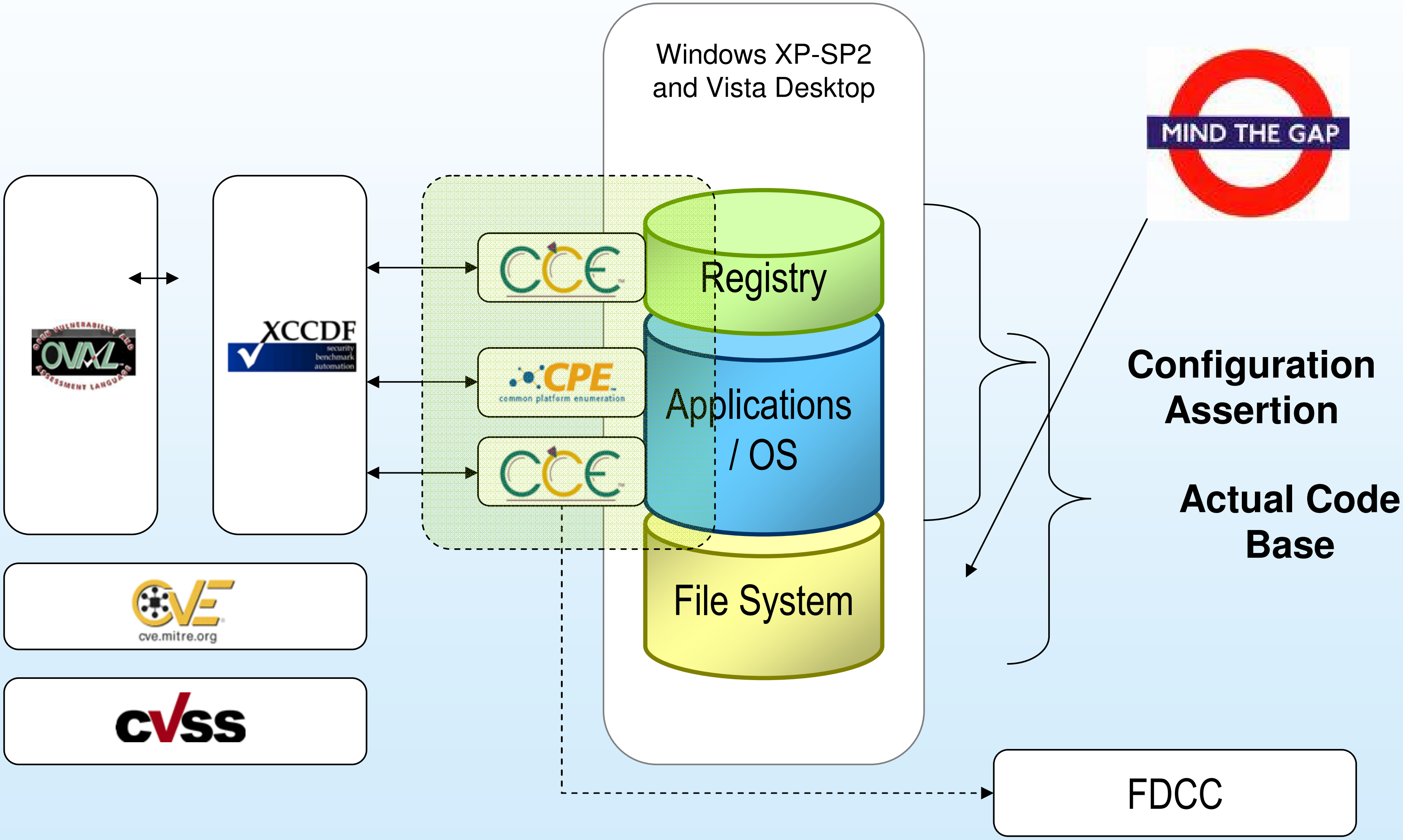


Integrity of actual data elements unknown

Mapping the Specs to the Desktop



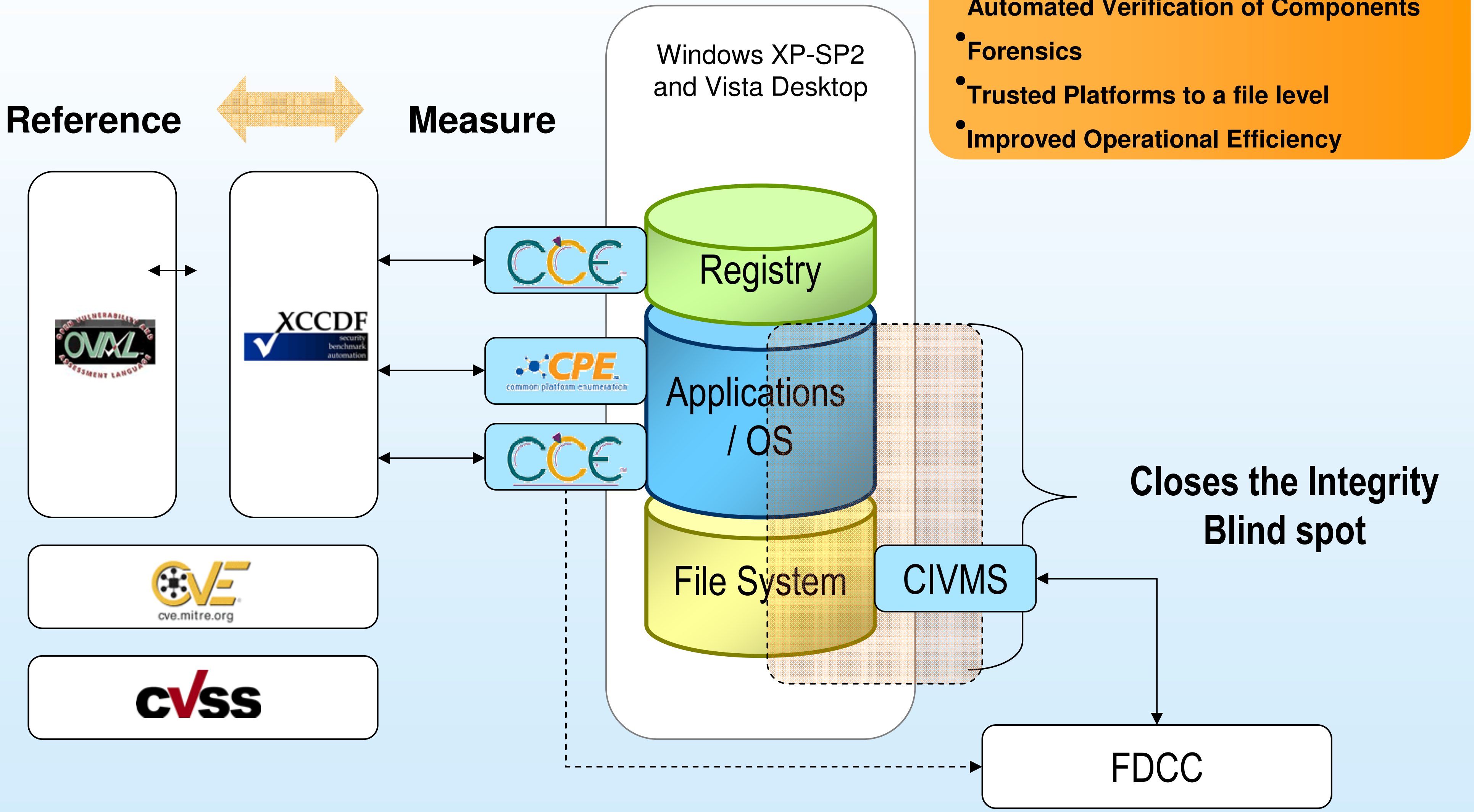
Coverage Gaps



SCAP + CIVMS – Positive Assertion Model

SignaCert

- Automated Verification of Components
- Forensics
- Trusted Platforms to a file level
- Improved Operational Efficiency


Reference
Measure
OVAL
XCCDF
security benchmark automation
CVE
cve.mitre.org
CVSS
CCE
CPE
common platform enumeration
CCE
Windows XP-SP2 and Vista Desktop
Registry
Applications / OS
File System
CIVMS
FDCC
Closes the Integrity Blind spot

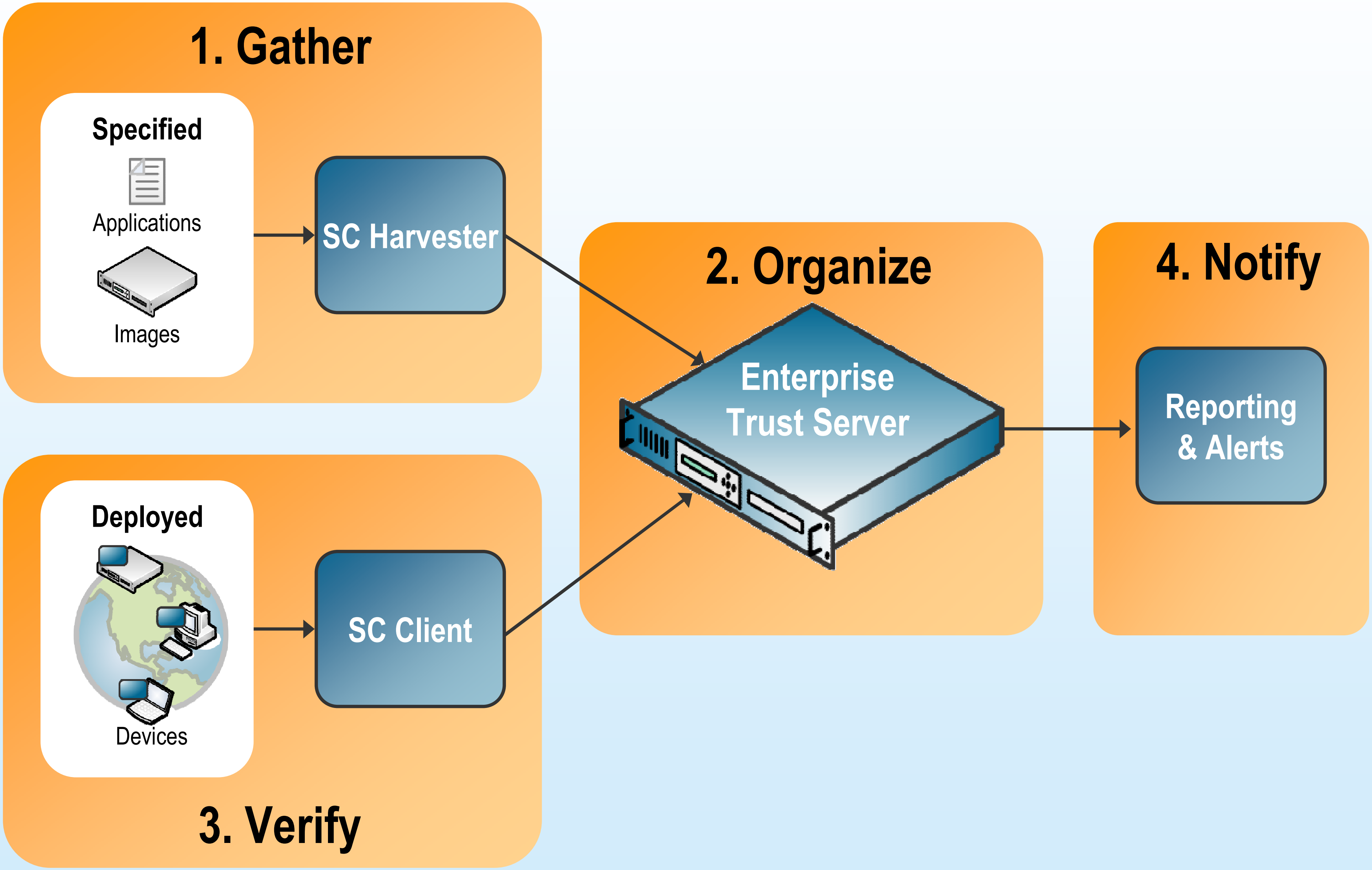
An Additional Standard and Method?

SignaCert

MITRE	CVE cve.mitre.org	**CVE**	Common Vulnerabilities and Exposures	Standard nomenclature and dictionary of security related software flaws
MITRE	CCE	**CCE**	Common Configuration Enumeration	Standard nomenclature and dictionary of software misconfigurations
MITRE	CPE common platform enumeration	**CPE**	Common Platform Enumeration	Standard nomenclature and dictionary for product naming
NATIONAL SECURITY AGENCY UNITED STATES OF AMERICA	XCCDF security benchmark automation	**XCCDF**	extensible Checklist Configuration Description Format	Standard XML for specifying checklists and for reporting results of checklist evaluation
MITRE	OPEN VULNERABILITY AND OVAL ASSESSMENT LANGUAGE	**OVAL**	Open Vulnerability Assessment Language	Standard XML for testing procedures
FIRST Improving Security Together	CVSS	**CVSS**	Common Vulnerability Scoring System	Standard for measuring the impact of vulnerabilities
NIST / NSA?	NATIONAL SECURITY AGENCY UNITED STATES OF AMERICA NIST	**CIVMS**	Common Integrity Verification Measurement System	Standard for measuring the integrity of software/firmware images.

Platform Measurement

SignaCert



1. Gather

Specified

Applications

Images

SC Harvester

2. Organize

Enterprise Trust Server

4. Notify

Reporting & Alerts

Deployed

Devices

SC Client

3. Verify

Summary

- Full Configuration Standardization
  - SCAP can be extended with Positive Measurement Methods to a component level, to ensure full platform configuration attestation.
- FDCC and STIG's could use the Positive Assertion of platform compliance down to file level
- Now is the opportunity to prove that, what we compute with is what we expected.

Thank you

Sol Cates

sol@signacert.com