Configuration Management

What:
“A systems engineering process for establishing and maintaining consistency of a product's performance, functional, and physical attributes with its requirements, design, and operational information throughout its life.”


In our case, with respect to cyber security
Configuration Management

How:

Provide access to a centralized repository of code
  - easier to manage and distribute from central source
  - easier to protect configuration information

Manage and track multiple versions of the same applications

Manage multiple developers

Identify when changes are made and their impact

Detect and resolve conflicting changes

Distribute and deploy the latest versions of code

Back up and preserve access to older versions of code

Manage and distribute reuse libraries
Configuration Management

Importance:
Attackers look for systems with vulnerable default settings
Attackers make changes once a system is exploited

Security Configuration Management (SCM) can
→ identify misconfigurations making the system vulnerable
→ identify “unusual” changes to the system

SCM is used to meet CIS, NIST hardening standards
https://www.cisecurity.org/
https://www.newnettechnologies.com/cis-benchmark.html?keyword=cis%20hardening%20standards&gclid=EAIaIQobChMIpdTaptDF4QIvKVx6tBh0aMw9bEAAYASAAEglHHvD_BwE
https://www.newnettechnologies.com/cis-benchmark.html?keyword=Cis%20Hardening%20Standards&gclid=EAIaIQobChMI9oyO3s3F4QIvqSCiBh1N7Qq-EAAAYASAEgJEG_D_BwE#ubuntu

SCM is used to meet HIPAA compliance standards
https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

2015 Verizon Data Breach Investigation Report:
→ 60% of incidents are due to misconfiguration
→ https://enterprise.verizon.com/resources/reports/dbir/
Configuration Management

Center for Internet Security Critical Security Controls: why? Defenders have access to a large number of
security tools, security standards & best practices
training, classes & certifications
vulnerability databases
guidance
catalogs of security controls
security checklists
benchmarks
recommendations, reports & alert services
threat sharing frameworks
risk management frameworks
compliance & regulatory mandates

Fog of More:
competing options, priorities, opinions, claims
can paralyze or distract an enterprise from vital action

Center for Information Security: https://www.cisecurity.org/
CIS Critical Security Controls: what?

CIS CSC are a prioritized, highly focused set of actions with a community support network to make them implementable, usable, scalable, and compliant with all industry and/or government security requirements

CIS CSC are the result of actual attack outcomes and analysis with input from individuals who are threat responders, threat analysts, vulnerability finders, tool makers, solution providers, defenders, policy makers, auditors from government, power, defense, finance, transportation, academia, consulting, IT

Objective: reduce attack surface via hardening device configs identify compromised machines to address long-term threats inside an organization’s network, disrupt attacker's C-C of implanted malicious code, establish an adaptive, continuous, maintainable defense and response capability

Center for Information Security: https://www.cisecurity.org/
Configuration Management

CIS Critical Security Controls: tenets

Offense informs defense:
use knowledge of actual compromising attacks to build effective, practical defenses over time – use only controls that are known to stop real attacks

Prioritization:
first: invest in feasibly implemented controls providing highest risk reduction and protection against the most dangerous actors

Metrics:
establish common metrics to provide a shared language for executives, IT specialists, auditors, security officials to determine effectiveness of security measures so adjustments can be made

Continuous diagnostics and mitigation:
test and validate the effectiveness of current security measures

Automation:
automate defenses to achieve reliable, scalable, measurement of adherence to the controls and related metrics
**Configuration Management**

**CIS Critical Security Controls:**
- Inventory of authorized and unauthorized devices
- Inventory of authorized and unauthorized software
- Secure configurations for hardware and software on mobile devices, laptops, workstations, and servers
- Continuous vulnerability assessment and remediation
- Controlled use of administrative privileges
- Maintenance, monitoring, and analysis of audit Logs
- Email and web browser protections
- Malware defenses
- Limitation and control of network ports, protocols, services
- Data recovery capability

Center for Information Security:  [https://www.cisecurity.org/](https://www.cisecurity.org/)
Configuration Management

CIS Critical Security Controls:
Secure configurations for network devices such as firewalls, routers, and switches
Boundary defense
Data protection
Controlled access based on the need to know
Wireless access control
Account monitoring and control
Security skills assessment and training to fill gaps
Application software security
Incident response and management
Penetration tests and red team exercises

Center for Information Security:  https://www.cisecurity.org/
Configuration Management

Automated Security Control:

**SCAP:** *Security Content Automation Protocol*
suite of specs that standardize format and nomenclature to support communication of software flaw and security configuration information [http://scap.nist.gov/](http://scap.nist.gov/)

**XCCDF:** *Extensible Configuration Checklist Description Format*
specification language for writing security checklists, benchmarks, and related kinds of documents
Click specification link, scroll to & click XCCDF entry

**OVAL:** *Open Vulnerability and Assessment Language*
represent configuration information of systems for testing analyze for vulnerability, configuration, patch (etc.) state report results of the assessment.
Spec: [https://oval.mitre.org/](https://oval.mitre.org/)
Ex: [https://qualysguard.qualys.com/qwebhelp/fo_portal/scans/oval_vulnerability_samples.htm](https://qualysguard.qualys.com/qwebhelp/fo_portal/scans/oval_vulnerability_samples.htm)
Configuration Management

Automated Security Control:

**CVSS:** Common Vulnerability Scoring System
framework for communicating the characteristics and impact of IT vulnerabilities  
https://nvd.nist.gov/cvss.cfm
Standard spec: http://www.first.org/cvss/v2/guide
Vector spec: https://nvd.nist.gov/CVSS/Vector-v2.aspx

**CPE:** Common Platform Enumeration
standardized method of describing and identifying classes of applications, operating systems, and hardware devices present among an enterprise's computing assets
Spec: https://cpe.mitre.org/specification/
Dictionary: https://nvd.nist.gov/cpe.cfm

**CCE:** Common Configuration Enumeration
provide unique identifiers to system configuration issues in order to facilitate fast, accurate correlation of configuration data across multiple information sources and tools
CCE & CPE are widely used to check for known vulnerabilities
Try: https://nvd.nist.gov/config/cce
Checklist: https://web.nvd.nist.gov/view/ncp/repository
Configuration Management

SCAP Interoperability:
Configuration Management

SCAP:
developed to organize, express and measure security information in standardized ways, to provide an automated approach to maintaining the security of enterprise systems

SCAP is used to maintain system security as follows:
  automatically
  → verifying the installation of patches
  → checking system security configuration settings
  → examining systems for signs of compromise

Helps organizations needing to comply with US Government Configuration Baseline (USGCB)
  https://csrc.nist.gov/Projects/United-States-Government-Configuration-Baseline

SCAP-validated scanning tools scan for compliance

SCAP tools can be used continuously, not occasionally
Configuration Management

SCAP Content:
Software flaw and security configuration standard reference data

Provided by the National Vulnerability Database (NVD), managed by NIST sponsored by the Department of Homeland Security (DHS)
# Configuration Management

## SCAP Specifications:

<table>
<thead>
<tr>
<th>Languages: Means of providing instructions and reporting results</th>
<th>eXtensible Checklist Configuration Description Format (XCCDF) 1.1.4</th>
<th>NSA and NIST</th>
<th>XML-based language for specifying checklists and reporting the results of checklist evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enumeration: Conventions for identifying and naming</td>
<td>Open Vulnerability and Assessment Language (OVAL) 5.3 and 5.4</td>
<td>MITRE</td>
<td>XML-based language for specifying test procedures to detect machine state</td>
</tr>
<tr>
<td>Metrics: Risk measurement</td>
<td>Common Vulnerabilities and Exposures (CVE)</td>
<td>MITRE</td>
<td>Nomenclature and dictionary of security-related software flaws</td>
</tr>
<tr>
<td></td>
<td>Common Configuration Enumeration (CCE) 5</td>
<td>MITRE</td>
<td>Nomenclature and dictionary of software security configuration issues</td>
</tr>
<tr>
<td></td>
<td>Common Platform Enumeration (CPE) 2.2</td>
<td>MITRE</td>
<td>Nomenclature and dictionary for product names and versions</td>
</tr>
<tr>
<td></td>
<td>Common Vulnerability Scoring System (CVSS) 2.0</td>
<td>FIRST</td>
<td>Methodology for measuring the relative severity of software flaw vulnerabilities</td>
</tr>
</tbody>
</table>

Configuration Management

SCAP Checklists:
Integrate SCAP components and content
Example: view https://web.nvd.nist.gov/view/ncp/repository
Microsoft Internet Explorer 7 – choose USGCB IE7
Click 'download prose' (human readable)
Click 'download' link at top – open spreadsheet, goto last tab
spreadsheet indexes policy setting and name with the
CCE reference, the registry setting, the description,
the Federal Desktop Configuration for each policy
Download All Platforms  https://nvd.nist.gov/config/cce
Configuration Management

SCAP Common Uses:

Security configuration verification
  compare settings in a checklist to a system’s actual configuration

verify configuration before deployment, audit/assess/monitor operational systems

map individual settings to high level security requirements that originate from mandates such as FDCC

similar process for verifying patch installation and identifying missing patches

Check systems for signs of compromise
  known characteristics of attacks, such as altered files or the presence of a malicious service
Configuration Management

SCAP Common Uses:

Standardize Security Enumerations
interoperability for security management tools, such as vulnerability scanners and patch management utilities information sharing, such as security bulletins and incident reports

Vulnerability Remediation Prioritization
use scores of relative vulnerability severity to help prioritize remediation, such as applying patches

Acquire and use SCAP-validated products
validated products list:
https://nvd.nist.gov/scapproducts.cfm
scroll to bottom of page to see accredited laboratories
Configuration Management

SCAP: how it works

Software Developers
- register and use standardized identifiers
- make security settings available through automation
- develop software with SCAP requirements in mind to avoid costly manual checks and proprietary checking mechanisms

SCAP Content Producers
- develop security checklists in SCAP format and contribute them to the National Checklist Program
- participate in developing OVAL

End-user organizations
- acquire products and services that support SCAP
- use SCAP in organization-developed software, databases, etc.
Configuration Management

SCAP Validation:
Independent laboratories test submitted products
tests defined in NIST IR 7511, SCAP Validation
Program Test Requirements

NIST validates products based on the test results, then
posts the validations
http://nvd.nist.gov/scappproducts.cfm

Federal agencies have requirements to purchase SCAP
validated products
details at http://nvd.nist.gov/scappproducts.cfm
Configuration Management

SCAP Revision Cycle:

1. Update Candidate List
2. Review Candidate SCAP Specifications +3 Months
3. Deadline for Publication of Draft SCAP SP 800-126 and DTRs (IR 7511) 0 Months
4. SCAP Beta Content Available +3 Months
5. Deadline for Publication of Final SCAP SP 800-126 and DTRs (IR 7511) +12 Months
6. SCAP Content Final +14 Months
7. Laboratory Tool Validation Period Begins (DTR Effective Date) +15 Months
8. Laboratory Tool Validation Period Ends (DTR Expiration Date) +27 Months
9. Tool Validations Expire and Mandatory Content Maintenance Period Ends +39 Months

DTR=Derived Test Requirements

Community Feedback
## Configuration Management

### SCAP Redux:

<table>
<thead>
<tr>
<th>Question</th>
<th>Tool</th>
</tr>
</thead>
<tbody>
<tr>
<td>What IT systems do I have in my enterprise?</td>
<td>CPE (Platforms)</td>
</tr>
<tr>
<td>What vulnerabilities do I need to worry about?</td>
<td>CVE (Vulnerabilities)</td>
</tr>
<tr>
<td>What vulnerabilities do I need to worry about RIGHT NOW?</td>
<td>CVSS (Scoring System)</td>
</tr>
<tr>
<td>How can I configure my systems more securely?</td>
<td>CCE (Configurations)</td>
</tr>
<tr>
<td>How do I define a policy of secure configurations?</td>
<td>XCCDF (Configuration Checklists)</td>
</tr>
<tr>
<td>How can I be sure my systems conform to policy?</td>
<td>OVAL (Assessment Language)</td>
</tr>
</tbody>
</table>
Configuration Management

SCAP Benefits:

- Automation reduces manual effort to obtain assessment results, determine corrective actions needed and provides substantial cost savings.
- SCAP mandates a common language that supports easier communication of results with other SCAP system users.
- SCAP supports easier comparison of issue sets between security organizations because vulnerabilities are described using the CVSS, CVE and CPE.
- Use of SCAP-validated products prepares organization’s FDCC/USGCB audits.
- It is possible to make and modify custom checklists.

Use of FDCC / USGCB content is required only under government mandate.
Unix Configuration Guidelines:
http://gauss.ececs.uc.edu/Courses/c6056/lectures/ubuntu-18.04-LTS.pdf
http://gauss.ececs.uc.edu/Courses/c6056/lectures/PDF/config_management.pdf