

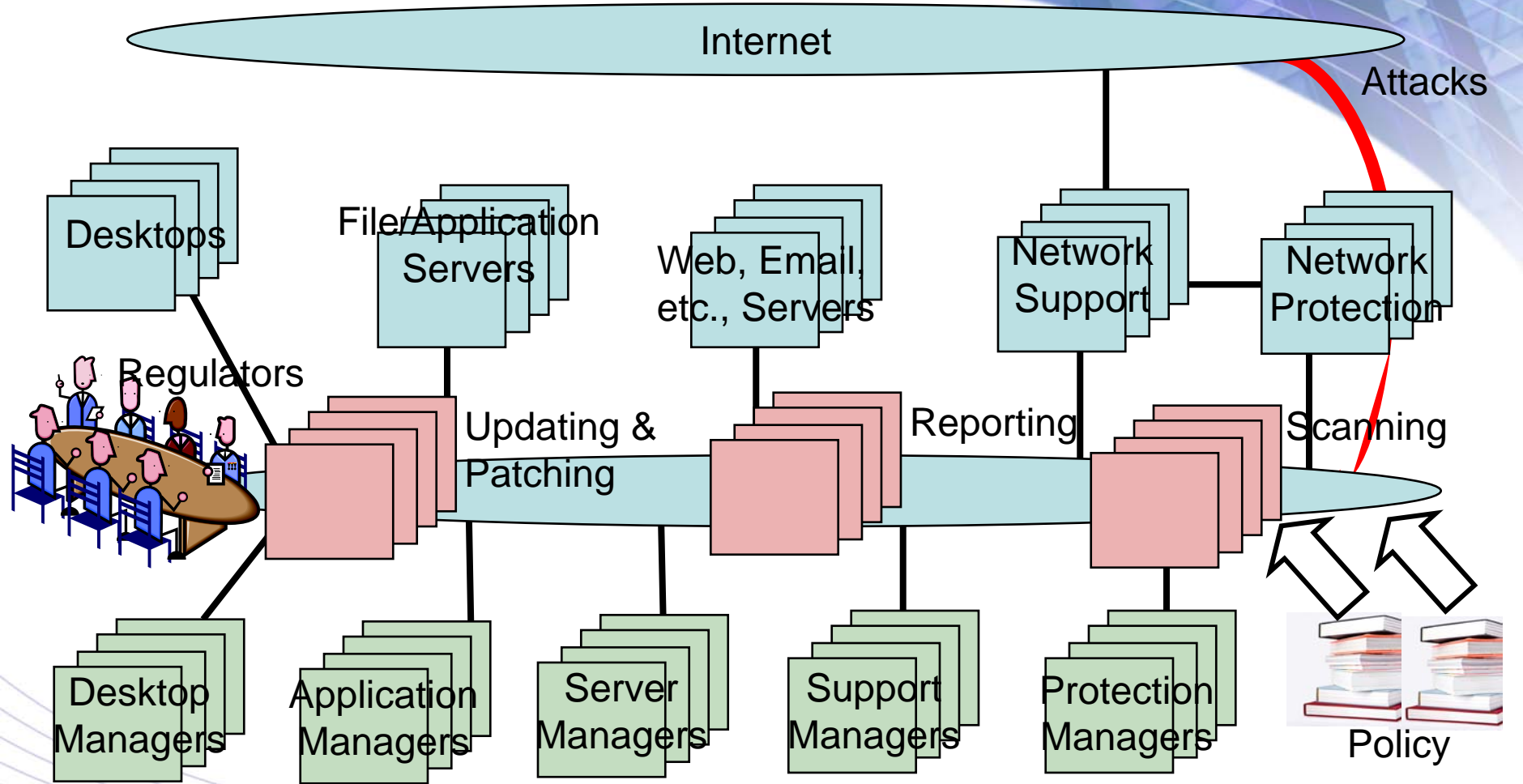
Leveraging Automation Protocols in CC Evaluated Products

Dawn Adams and Erin Connor
EWA-Canada
28 September 2011

Your Trusted Partner

- **Enterprise Network Evolution**
- **Why Automation and What to Automate?**
- **Security Content Automation Protocol (SCAP) Overview**
- **CC & Automation Protocols**
- **National Checklist Program**
- **Over the Automation Horizon**
- **References & Resources**
- **Questions**

Enterprise Network Evolution



Your Trusted Partner

Why Automation?

- **Proprietary information and formats across products**
- **Incompatible information across technologies**
- **Information collection is costly and error prone**
- **Inefficient use of resources managing configurations, vulnerabilities and patches**
- **Same or similar problems when systems connected into networks and events start happening**
- **Doesn't scale well as networks grow and the number of desirable and undesirable events multiply**

Your Trusted Partner

What to Automate?

- **Standard Language**
 - Using the same name for the same object in all instances
 - Lends itself to the use of automated tools, reducing manual requirements
 - increases accuracy in reporting and subsequent response
- **Tools using a common language and reporting in a “single” place**
- **Valuable human resources can be tasked to more difficult problems**
- **Benefits:**
 - Reduce/re-assign support staff
 - Increase the ratio of operations to support

Your Trusted Partner

Security Content Automation Protocol (SCAP) Overview

- **Security Content Automation Protocol (SCAP) is an initiative of NIST, DHS, NSA, DoD/DISA to address the problem of ensuring secure configurations for products connected to networks and provide better means to exercise control over them**
- **Purpose of SCAP is to provide a common language to specify automated scanning of products to:**
 - Verify correct configuration settings
 - Identify patches applied
 - Determine vulnerabilities not yet addressed
 - Report findings in human readable form
- **Validation Program to test and verify that scanning tools properly implement and understand the language defined by the six underlying automation standards, and can properly execute SCAP content**

Your Trusted Partner

Security Content Automation Protocol (SCAP) Overview

SCAP “Common” Language Elements:

- **Common Platform Enumeration (CPE™)**
 - defines a structured naming scheme for information technology systems, platforms, and packages
- **Common Configuration Enumeration (CCE™)**
 - defines unique identifiers for system configuration issues in order to facilitate fast and accurate correlation of configuration data across multiple information sources and tools
- **Common Vulnerabilities and Exposures (CVE®)**
 - comprises a dictionary of publicly known information security vulnerabilities and exposures (configuration/patch issues)

Security Content Automation Protocol (SCAP) Overview

SCAP “Operational” Elements :

- **eXtensible Configuration Checklist Description Format (XCCDF)**
 - defines a specification language for writing security checklists, benchmarks, and related kinds of documents representing a structured collection of security configuration rules for some set of target systems
- **Open Vulnerability Assessment Language (OVAL)**
 - an information security community effort to standardize how to assess and report upon the machine state of computer systems, i.e., how to query configuration, vulnerability, etc., status of a target
- **Common Vulnerability Scoring System (CVSS)**
 - provides an industry standard for assessing the severity of computer system security vulnerabilities thereby allowing comparison and prioritization of response
- **Open Checklist Interactive Language (OCIL)**
 - defines a framework for expressing a set of questions to be presented to a user and corresponding procedures to interpret responses to these questions, i.e., non-automated manual checks

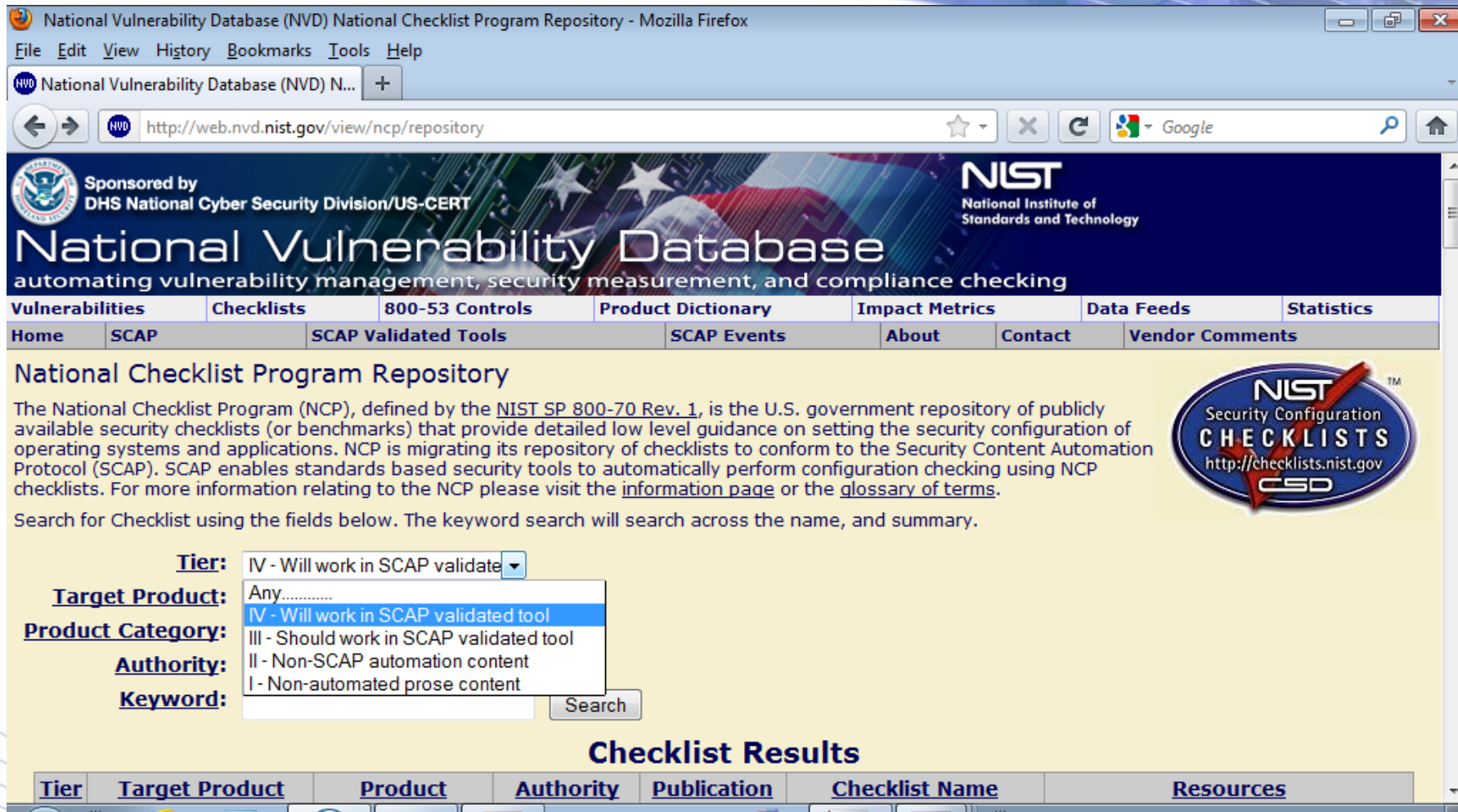
Your Trusted Partner

CC & Automation Protocols

- **IT security evaluation and testing programs, such as CC, look at a product at a point in time and in a specific (set of) configuration(s)**
 - **Automation protocols and content to confirm deployment of Certified products in an Evaluated Configuration**
- **After deployment, bugs and vulnerabilities will be found, and patches will be developed to address them**
 - **Automation protocols and content to confirm application of approved patches**
- **Users will make changes to configuration settings that will allow them to “better perform” their jobs**
 - **Automation protocols and content to confirm configuration of products in accordance with policy**

Your Trusted Partner

- **Automation protocols need to be able to gain access to products to collect status information (configuration settings and patches)**
 - PPs and STs include SFRs relating to interfaces necessary to collect needed platform, configuration and patch information
 - Review OVAL to ensure it defines appropriate tests that will provide scanning access to these interfaces
- **Automation Tools need (SCAP) content in order to carry out scanning and other future activities**
 - Define CPE and CCE content to identify product platforms and configuration settings/parameters
 - Monitoring and submission of issues to CVE
 - Create checklists from simple prose all the way to validated XCCDF content that validated tools can use to automate checks
- **Users/Administrators may also need specific guidance for manual operations they need to carry out/confirm**
 - Create OCIL “content” for these (hopefully few) manual tasks



National Vulnerability Database (NVD) National Checklist Program Repository - Mozilla Firefox

File Edit View History Bookmarks Tools Help

NVD National Vulnerability Database (NVD) N... +

http://web.nvd.nist.gov/view/ncp/repository

Sponsored by
DHS National Cyber Security Division/US-CERT

NIST
National Institute of
Standards and Technology

National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

Vulnerabilities | Checklists | 800-53 Controls | Product Dictionary | Impact Metrics | Data Feeds | Statistics

Home | SCAP | SCAP Validated Tools | SCAP Events | About | Contact | Vendor Comments

National Checklist Program Repository

The National Checklist Program (NCP), defined by the [NIST SP 800-70 Rev. 1](#), is the U.S. government repository of publicly available security checklists (or benchmarks) that provide detailed low level guidance on setting the security configuration of operating systems and applications. NCP is migrating its repository of checklists to conform to the Security Content Automation Protocol (SCAP). SCAP enables standards based security tools to automatically perform configuration checking using NCP checklists. For more information relating to the NCP please visit the [information page](#) or the [glossary of terms](#).

Search for Checklist using the fields below. The keyword search will search across the name, and summary.

Tier: IV - Will work in SCAP validate

Target Product: Any.....

Product Category: IV - Will work in SCAP validated tool

Authority: III - Should work in SCAP validated tool

Keyword: II - Non-SCAP automation content

I - Non-automated prose content

Search

Checklist Results

Tier	Target Product	Product	Authority	Publication	Checklist Name	Resources
------	----------------	---------	-----------	-------------	----------------	-----------



Your Trusted Partner

- **National Checklist Program (NCP) repository for checklists created at web.nvd.nist.gov/view/ncp/repository**
- **Four “tiers” defined into which the checklist for a product can fall:**
 - 1. Prose description only for manual configuration (97)
 - 2. Security settings available in machine-readable but non-standard (non-SCAP) format (62)
 - 3. Settings available in “SCAP expressed” form that should be able to be used by SCAP-validated tools (28)
 - 4. Tier 3 plus the SCAP-content has been validated by NIST (8)

NCP Tier 4 Content (Validated)

National Vulnerability Database (NVD) National Checklist Program Repository - Mozilla Firefox

File Edit View History Bookmarks Tools Help

NVD National Vulnerability Database (NVD) N... +

http://web.nvd.nist.gov/view/ncp/repository?tier=4&product=&category=&authority=&keyword=

National Checklist Program Repository

The National Checklist Program (NCP), defined by the [NIST SP 800-126 Rev. 1](#), is the U.S. government repository of publicly available security checklists (or benchmarks) that provide detailed low level guidance on setting the security configuration of operating systems and applications. NCP is migrating its repository of checklists to conform to the Security Content Automation Protocol (SCAP). SCAP enables standards based security tools to automatically perform configuration checking using NCP checklists. For more information relating to the NCP please visit the [information page](#) or the [privacy notice](#).

Search for Checklist using the fields below. The keyword search will search across the name, and summary.

Tier: Any
 Target Product: Any
 Product Category: Any
 Authority: Any
 Keyword:

Search

Checklist Results

Tier	Target Product	Product Category	Authority	Publication Date	Checklist Name (Version)	Resources
IV	• Microsoft Internet Explorer 7	• Web Browser	• OMB	06/19/2008	FDCC Internet Explorer 7 (1.2)	<ul style="list-style-type: none"> • GPOs - FDCC Windows Vista Firewall GPOs • Prose - This is the human readable version of the FDCC settings. • SCAP 1.0 Content - FDCC Internet Explorer 7 SCAP Content using OVAL version 5.3 • SCAP 1.0 Content - FDCC Microsoft Internet Explorer 7 SCAP content using OVAL version 5.3
IV	• Microsoft Internet Explorer 8	• Web Browser	• NIST, Computer Security Division	09/24/2010	USGCB Internet Explorer 8 (1.1.0.0)	<ul style="list-style-type: none"> • GPOs - USGCB Windows IE8 GPOs • Prose - USGCB 1.1.x.0 Settings • SCAP 1.0 Content - USGCB Internet Explorer 8 OVAL 5.3 • SCAP 1.0 Content - USGCB Internet Explorer 8 OVAL 5.4
IV	• Microsoft Windows 7 • Microsoft Windows 7 32-bit • Microsoft Windows 7 64-bit	• Operating System	• NIST, Computer Security Division	09/24/2010	USGCB Windows 7 (1.1.0.0)	<ul style="list-style-type: none"> • GPOs - USGCB Windows 7 GPOs • Prose - USGCB 1.1.x.0 Settings • SCAP 1.0 Content - Windows 7 OVAL 5.3 • SCAP 1.0 Content - Windows 7 OVAL 5.4
IV	• Microsoft Windows 7 • Microsoft Windows 7 32-bit • Microsoft Windows 7 64-bit	• Operating System	• NIST, Computer Security Division	09/24/2010	USGCB Windows 7 Firewall (1.1.x.0)	<ul style="list-style-type: none"> • SCAP 1.0 Content - Windows 7 Firewall OVAL 5.3 • SCAP 1.0 Content - Windows 7 Firewall OVAL 5.4 • Prose - USGCB 1.1.x.0 Settings • GPOs - USGCB Windows 7 Firewall GPOs
IV	• Microsoft Windows Vista	• Operating System	• OMB	06/19/2008	FDCC Windows Vista (1.2)	<ul style="list-style-type: none"> • GPOs - FDCC Windows Vista Firewall GPOs • Prose - This is the human readable version of the FDCC settings. • SCAP 1.0 Content - FDCC Windows Vista using OVAL version 5.3 • SCAP 1.0 Content - FDCC Windows Vista using OVAL version 5.4
IV	• Microsoft Windows Vista	• Operating System	• OMB	06/19/2008	FDCC Windows Vista Firewall (1.2)	<ul style="list-style-type: none"> • SCAP 1.0 Content - FDCC Windows Vista Firewall using OVAL version 5.3 • SCAP 1.0 Content - FDCC Windows Vista Firewall using OVAL version 5.4 • Prose - This is the human readable version of the FDCC settings.
IV	• Microsoft Windows XP Pro SP2 • Microsoft Windows XP Pro SP3	• Operating System	• OMB	06/19/2008	FDCC Windows XP Firewall (1.2)	<ul style="list-style-type: none"> • SCAP 1.0 Content - FDCC Windows XP Firewall SCAP content using OVAL version 5.3 • SCAP 1.0 Content - FDCC Windows XP Firewall SCAP content using OVAL version 5.4 • GPOs - FDCC Windows Vista Firewall GPOs • Prose - This is the human readable version of the FDCC settings.
IV	• Microsoft Windows XP Pro SP2 • Microsoft Windows XP Service Pack 3	• Operating System	• OMB	06/19/2008	FDCC Windows XP (1.2)	<ul style="list-style-type: none"> • GPOs - FDCC Windows Vista Firewall GPOs • Prose - This is the human readable version of the FDCC settings. • SCAP 1.0 Content - FDCC Windows XP using OVAL version 5.3 • SCAP 1.0 Content - FDCC Windows XP using OVAL version 5.4

* This checklist is still undergoing review for inclusion into the NCP at this tier ranking. There are 8 matching records. Displaying matches 1 through 8.

Your Trusted Partner

Automation Protocol initiatives underway or proposed, including:

- **Enterprise Remediation Automation Protocol**
- **Enterprise System Information Protocol**
- **Enterprise Compliance Automation Protocol**
- **Threat Analysis Automation Protocol**
- **Software Assurance Automation Protocol**
- **Incident Management Automation Protocol**

Potential to get to the point where network managers can respond to events in real time by changing policies and configurations from a central management point using automation protocols

Your Trusted Partner

Selected Standards:

- Security Content Automation Protocol (SCAP) <http://scap.nist.gov/>
- Common Platform Enumeration (CPE) <http://cpe.mitre.org/>
- Common Configuration Enumeration (CCE) <http://cce.mitre.org/>
- Common Vulnerabilities & Exposures (CVE) <http://cve.mitre.org/>
- eXtensible Configuration Checklist Description Format (XCCDF)
<http://scap.nist.gov/specifications/xccdf/>
- Open Vulnerability Assessment Language (OVAL) <http://oval.mitre.org/>
- Common Vulnerability Scoring System (CVSS) <http://www.first.org/cvss/>
- Open Checklist Interactive Language (OCIL)
<http://scap.nist.gov/specifications/ocil/>
- CWE <http://cwe.mitre.org/>
- Common Attack Pattern Enumeration and Classification (CAPEC)
<http://capec.mitre.org/>
- Malware Attribute Enumeration and Characterization (MAEC)
<http://maec.mitre.org/>
- Asset Reporting Format (ARF) <http://scap.nist.gov/specifications/arf/>
- Common Event Expression (CEE) <http://cee.mitre.org/>

Your Trusted Partner

Automation Content

- Federal Desktop Core Configuration <http://nvd.nist.gov/fdcc/index.cfm>
- United States Government Configuration Baseline (USGCB)
<http://usgcb.nist.gov/>

Conferences

- 7th Annual IT Security Automation Conference (31 Oct – 2 Nov 2011)
<http://www.nist.gov/itl/csd/7th-annual-scap-conference.cfm>
- Software Assurance Forum – semi-annual Spring and Autumn forums
<https://buildsecurityin.us-cert.gov/swa/forums.html>

National Vulnerability Database (NVD) <http://nvd.nist.gov/>

Questions



Erin Connor
Director
+1-613-230-6067 x1214
econnor@ewa-canada.com

Your Trusted Partner