Developer Days 2013

July 22 - 24, 2013

Discussion Session
Briefing Session
Demo Session

Agenda

Monday July 22nd 2013

10:00 - 10:10 Welcome
Introduce the organizers and notable participants. Describe MITRE's role and the goals for this event.

10:10 - 10:30   Remediation - Status Update & Session Objectives   Luis Nunez, MITRE
The status of the Remediation work currently being undertaken by the MITRE team will be briefed.

10:30 - 11:30   Remediation - XCCDF Remediation discussions   Luis Nunez, MITRE
This session will cover current and future XCCDF remediation capabilities. Some topics for this session include fix tag, scripts and ideas on enhancements to enable automated remediations.

11:30 - 12:30   Remediation - Lessons Learned   Shawn Wells, Red Hat
The Red Hat team will lead a discussion on the Red Hat SCAP Security Guide project to produce RHEL 6 STIG content with automated remediation capabilities.

12:30 - 1:00   Open Lunch
During the open lunch break we encourage community networking.

1:00 - 1:30   Working Lunch (SCM Demo)   Ryan Garvey L-3 Communications
The open source remediation system was designed to test the current XCCDF concepts using the fix tag. The system is a collection of open source tools that are integrated together to create a reference implementation. OpenSCAP is used to perform scanning and remediation functions on assets. Puppet is used as a command and control infrastructure to manipulate the OpenSCAP tool and collect reports on a central server. The demonstration shows how the system enables administrators to perform remediation actions on managed assets using XCCDF.

1:30 - 2:30   Remediation - OVRL   Richard Kelly, SPAWAR
The Open Vulnerability Remediation Language (OVRL) is the next step in automated Secure Configuration Management (SCM). This session will focus on the OVRL path forward and schema design approach so it can be utilized within existing SCAP standards.

2:30 - 2:50   OVAL - Status Update & Session Objectives   Matt Hansbury, MITRE
The OVAL team will give a brief status update to include the status of OVAL 5.11, the OVAL Interpreter and the OVAL Repository as well as the high level goals for the OVAL sessions during the event.

2:50 - 3:20   OVAL - The OVAL Sandbox Process   Matt Hansbury, MITRE
The OVAL Sandbox has been in place for over a year now and many contributions have been made towards this experimental environment. This session will be a discussion of how to improve the process and ensure contributions get ushered through the Sandbox process correctly and effectively.

3:20 - 4:00   OVAL - License and System-Metric Tests   David Solin, jOVAL
David Solin of jOVAL will lead a discussion of the proposed new Windows license and system-metric tests, with the goal of generating consensus on the inclusion of these proposed updates in the 5.11 version of the OVAL Language.

Developer Days 2013

July 22 - 24, 2013

The MITRE Corporation
McLean, VA

Agenda

4:00 - 4:30   **OVAL - Bitwise Functions**   David Rothenberg, MITRE

This topic will further introduce the newly proposed bitwise functions (AND, OR, XOR, NOT) for OVAL. A detailed look at the available usage options will help clarify its usefulness and applicability to the Language.

4:30 - 5:30   **OVAL - NT User Test**   Jack Vander Pol, SPAWAR

Jack Vander Pol of SPAWAR will lead a discussion of the proposed NT User test, with the goal of generating consensus on the inclusion of this proposed test in the 5.11 version of the OVAL Language.

5:30 - 5:45   **Day 1 Wrap Up**

Wrap up the events of the day. Preview the next day. Make any pertinent announcements.

Developer Days 2013

July 22 - 24, 2013

The MITRE Corporation
McLean, VA

Agenda

Tuesday July 23rd 2013

8:00 - 8:10   Welcome
Provide an overview of the day's upcoming sessions.

8:10 - 9:00   OVAL - Cisco Schema Updates   Omar Santos, Cisco
Omar Santos of Cisco will provide an overview of the proposed updates to the Cisco platform extensions, with the goal of generating consensus on the inclusion of these proposed updates in OVAL 5.11. This includes updates for Cisco IOS and newly added support for Cisco ASA and IOS-XE. He will also lead the discussion on future new schemata for other networking devices and software such as Unified Communications, NX-OS, and IOS-XR.

9:00 - 9:45   OVAL - Checking Packages on Mac OSX   Jasen Jacobsen, MITRE
Mac OS X uses "packages" similar to other UNIX operating systems. This session will discuss a proposed addition to the OVAL Language to access the package receipt database.

9:45 - 10:00   Break

10:00 - 11:00   OVAL - Solaris Schema Updates   Warren Belfer, Oracle & Dan Haynes, MITRE
A discussion of the proposed updates to the Solaris platform extensions will be held, with the goal of generating consensus on the inclusion of these proposed updates in the 5.11 version of the OVAL Language. This will primarily focus on adding support for the Image Packaging System, introduced in Solaris 11.

11:00 - 12:00   OVAL - Apple Platform Discussion   Shawn Geddis & Josh Wisenbaker, Apple
During this session, several topics related to Apple platforms will be discussed. Primarily, this will focus on Apple MacOS plist configuration files and profiles.

12:00 - 12:30   Open Lunch
During the open lunch break we encourage community networking.

12:30 - 1:00   Working Lunch (OVAL - Adoption Conversation)   Omar Santos, Cisco
During the working portion of lunch, Omar Santos of Cisco will lead a conversation about OVAL adoption.

1:00 - 1:45   OVAL - 10th Anniversary Presentation   Gary Gagnon & Jon Baker, MITRE
OVAL is 10 years old. Join us for a small presentation to celebrate this significant milestone.

1:45 - 2:45   OVAL - Juniper JunOS Recap   David Solin, jOVAL
David Solin of jOVAL will lead a recap of the Juniper JunOS experimental schema with the goal of generating consensus on the inclusion of this proposed test in the 5.11 version of the OVAL Language.

2:45 - 3:00   Break

3:00 - 4:00   OVAL - Mobile Platform Discussion   Mike Peck, MITRE
The OVAL team will discuss and solicit community feedback on the current status and future plans for OVAL support for the Android and iOS mobile operating systems.

Developer Days 2013

July 22 - 24, 2013

The MITRE Corporation
McLean, VA

Discussion Session
Briefing Session
Demo Session

Agenda

4:00 - 4:45   **OVAL - INI Test**   William Munyan, Center for Internet Security

William Munyan of CIS will lead a discussion of the proposed INI test, with the goal of generating consensus on the inclusion of this proposed test in the 5.11 version of the OVAL Language.

4:45 - 5:00   **Day 2 Wrap Up**

Wrap up the events of the day. Preview the next day. Make any pertinent announcements.

5:30 - 7:00   **Social Event (Optional)**   Sponsored by Red Hat

Join us at Gordon Biersch at the Tysons Corner Mall for our Social Event.

Gordon Biersch is located 1.5 miles away in the nearby Tysons Corner Mall. The official address is 7861 Tysons Corner Center, McLean, VA 22102. To get there from MITRE, begin by taking Colshire Drive back towards Dolley Madison Blvd. Take a left onto Dolley Madison Blvd and continue under 495, at which point the street becomes Chain Bridge Road. From the leftmost lane, you can turn onto Shoptysons Blvd, and continue around the mall to the left. Gordon Biersch is located at the back of this left wing.

We encourage you to organize your own carpool transportation prior to this event.

Developer Days 2013

July 22 - 24, 2013

The MITRE Corporation
McLean, VA

Agenda

Wednesday July 24th 2013

8:00 - 8:15   **Welcome**
Provide an overview of the day's upcoming sessions.

8:15 - 9:15   **OVAL - XCCDF Evaluation Reference Architecture**   David Ries, jOVAL
David Ries of jOVAL will lead a discussion around the challenges of evaluating XCCDF checks containing both automated and manual checks (e.g., OVAL & OCIL), including the introduction of a reference architecture created by the jOVAL/gOCIL team as a starting point.

9:15 - 10:15   **CMRS - Problem Space Overview**   Joe Wolfkiel, DISA
Joe Wolfkiel of DISA will introduce the problem space for the CMRS project.

10:15 - 10:30   **Break**

10:30 - 12:30   **CMRS - Interoperability Requirements**   Joe Wolfkiel, DISA
Interoperability Requirements to Enable Federated Dashboard correlation, analysis, and visualization
- Establishing and maintaining standard taxonomies and ontologies to enable federated correlation, rollup, drilldown, and access control
- Implementation challenges and potential solutions to labeling data to provide centralized situational awareness in a federated environment
- XML languages and tools in use by the DoD

12:30 - 1:30   **Lunch**

1:30 - 3:30   **CMRS - Common Risk Scoring**   Joe Wolfkiel, DISA
Common Risk Scoring Algorithms for IT Security Risk Status Sharing
- Department of State scoring methodology review
- Commonly deployed security controls that can be continuously collected and reported
- Generalization strategies to allow for direct comparison between different vendor tools
- Establishment of processes to maintain common scoring logic and algorithms

3:30 - 5:30   **CMRS - Data Collection Requirements**   Joe Wolfkiel, DISA
Data Collection Requirements for IT Security Risk Scoring
- Review of data required from "DoD CMRS Data Ingest" paper
- Discussion of NIST ARF/ASR as alternatives
- Discussion of other alternatives

5:30 - 5:40   **Developer Days Wrap-up**