Security Automation Developer Days

June 14 -17, 2011

The MITRE Corporation
Bedford, MA

Agenda

Tuesday June 14th 2011

8:00 - 8:15 **Welcome**

Introduce the organizers of the event and the major players; describe MITRE's role for the event; and describe the goals for this event.

8:15 - 10:00 **XCCDF 1.2 Community Review** Charles Schmidt, MITRE

The XCCDF community has been working on XCCDF 1.2 for a number of years now. A complete draft of the proposed XCCDF 1.2 is now available for feedback. This meeting is will provide the community with an opportunity to comment on the proposed draft and raise issues before it is submitted as an official Draft NIST Interagency Report.

10:00 - 10:15 **Break**

10:15 - 12:00 **OCIL** Gerry McGuire, MITRE

This session will highlight community involvement since the last developer days and review in detail OCIL Version 2.0 schema changes. An overview of changes made to the reference interpreter and a look at 3rd party tools will be presented, We will then conclude by continuing current dialog from recent calls regarding the suitability of the existing use case and expanding the development of additional enterprise level use cases.

12:00 - 1:00 **Lunch**

During the lunch break we encourage community networking.

1:00 - 1:45 **Situational Awareness and Incident Response (SAIR) Tier III** TBD

DHS/FNS & GSA will discuss SAIR Tier III's acquisition approach, the focus of blanket purchase agreement (BPA), the estimated size, and the schedule for an industry day.

1:45 - 5:00 **Content Management** George Moore, DoS, and David Waltermire, NIST

This discussion will be focused on concepts, requirements, and data models related to providing basic content management capabilities for security automation content. Emphasis will be placed on approaches that enable rapid prototyping and that will provide significant short-term value.

5:00 - 5:10 **Day 1 Wrap Up**

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

Security Automation Developer Days

June 14 -17, 2011

The MITRE Corporation
Bedford, MA

Agenda

Wednesday June 15th 2011

7:50 - 8:00 **Welcome**

Provide an overview of the day's sessions.

8:00 – 12:00 **SCAP 1.2** Karen Scarfone, Adam Halbardier, NIST

This session will cover the proposed changes to the 800-126 for revision 2. These changes include the addition of OVAL 5.10, XCCDF 1.2, CPE 2.3, a source and results format, and digital trust, among other things. There will be time to present and gather feedback about the various proposals.

12:00 - 1:00 **Lunch**

During the lunch break we encourage community networking.

1:00 - 2:50 **Asset Reporting** Mark Davidson, MITRE/ Adam Halbardier, NIST

This session, presented by the Asset Reporting Working Group, is intended to solicit feedback on two emerging areas for new specifications: summary reporting and tasking. For both topics, the working group is hoping to discuss proposed use cases, requirements, and specifications. The DoD versions of ASR and PLARR, along with modifications and new proposals suggested by the working group, will serve as the base for discussion.

2:50 - 3:10 **Break**

3:10 - 5:00 **Content Development Best Practices** Shane Shaffer, G2

This session will focus on identifying and discussing specific best practices based on the areas discussed at the Developer Days – Spring 2011 conference.

5:00 - 5:10 **Day 2 Wrap Up**

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

5:30 – 7:30 S O C I A L

Security Automation Developer Days

June 14 -17, 2011

The MITRE Corporation
Bedford, MA

Agenda

Thursday June 16th 2011

7:50 - 8:00 **Welcome**

Provide an overview of the day's sessions.

8:00 - 12:00 **OVAL** Various Discussion Leads

This session will first briefly review the status of the version 5.10 release and then quickly shift focus to considering a series of open topics for the release. There will be a brief overview of the OVAL Language specification to introduce to the community the approach taken in developing the document and begin the community review process. This session will be broken up into several sub sections around the following topics:

- *OVAL Language Specification Review – Danny Haynes from MITRE*
- *PowerShell cmdlet support in OVAL – Kelly Hengesteg, Michael Tan, & Jeffery Snover from Microsoft*
- *Implementing the sql_test – Rob Hollis from ThreatGuard*
- *Version 5.10 Selected Issues – Matt Hansbury from MITRE*

12:00 - 1:00 **Lunch**

During the lunch break we encourage community networking.

1:00 - 2:50 **Remediation** Gerry McGuire, MITRE

The Remediation Standards session will focus on continuing the ongoing community development of the standards. The discussion topics will concern the Common Remediation Enumeration (CRE) and Extended Remediation Information (ERI) standards and specifically how CRE Parameters are used in Remediation Policy and Tasking. The session will begin with a summary of the progress made since the last developer days, launch directly into specific technical issues, and will conclude with an invitation for expanded participation from the community.

2:50 - 3:10 **Break**

3:10 - 5:00 **CPE** Brant Cheikes, MITRE

The Common Platform Enumeration (CPE) specification suite version 2.3 is approaching its final draft. During this session we will review and discuss the key changes implemented in v2.3. This session will help attendees understand the new drafts and provide them an opportunity to offer feedback and recommend revisions before the specifications become final.

5:00 - 5:10 **Day 3 Wrap Up**

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

Security Automation Developer Days

June 14 -17, 2011

The MITRE Corporation
Bedford, MA

Agenda

Friday June 17th 2011

7:50 - 8:00 **Welcome**

Provide an overview of the day's sessions.

8:00 - 9:50 **OVAL for Artifact Hunting** Joseph Drissel, CyberESI

This talk will highlight recent work to leverage SCAP and more specifically OVAL for the purpose of detecting indicators of compromise on end systems. In developing an SCAP benchmark for detecting indicators of compromise, the CyberESI team has offered to share their experience with the community and has developed several changed proposals for OVAL including both requests for new OVAL Tests and other modifications to existing capabilities. These proposal and the use cases that drive them will be discussed and reviewed.

9:50 - 10:10 **Break**

10:10 - 12:00 **CCE** Joe Sain, MITRE

This session will begin with a brief overview and background of CCE, followed by a discussion of the most pressing issues affecting sponsors, Security and OS vendors, and end users. We plan to use this session to drive consensus on two important CCE issues; CCE IDs for Bundled Sub-Components, and Publicly Available References for CCEs. We will conclude with a discussion of the steps that are being taken to streamline the CCE development process and to provide content development assistance to sponsors and the community.

12:00 - 12:15 **Developer Days Wrap-up**

MITRE will announce action items that have been determined during the week and next steps will be determined.