Security Automation Developer Days Winter 2010 Conference
Preliminary High Level Agenda

Dates: Monday, February 22, 2010 thru Wednesday, February 24, 2010

Location: NIST, Gaithersburg Campus, Building 101, NIST Lunch Club Room
100 Bureau Drive
Gaithersburg, MD 20899

Purpose: The Security Automation Developer Days Winter 2010 conference is a free three-day conference that is sponsored by the Department of Defense (DoD), hosted by the National Institute of Standards and Technology (NIST), and facilitated by the MITRE Corporation.

This conference will be a series of workshops that focus on engaging the security automation community in the development of key SCAP-related security automation initiatives, including the Common Platform Enumeration (CPE), the eXtensible Configuration Checklist Description Format (XCCDF), Remediation and Digital Trust.

Program:

Day 1: Monday, February 22, 2010

Time: 9:00 a.m. – 5 p.m. EST
Common Platform Enumeration (CPE) Developer Days Workshop

Day 2: Tuesday, February 23, 2010

Time: 9:00 a.m. – 5 p.m. EST
eXtensible Configuration Checklist Description Format (XCCDF) Developer Days Workshop

Day 3: Wednesday, February 24, 2010

Time: 9:00 a.m. – 12:30 p.m. EST
Remediation Developer Days Workshop

Time: 1:30 p.m. – 5:00 p.m. EST
Digital Trust Developer Days Workshop

Day 1: Monday, February 22, 2010

Common Platform Enumeration (CPE) Developer Days Workshop

Time: 9:00 a.m. – 5 p.m. EST

The CPE Developer Days Workshop is sponsored by the DoD, hosted by the National Institute of Standards and Technology (NIST), and facilitated by the MITRE Corporation. The purpose of the workshop is to elicit stakeholder-defined requirements and identify the near term mission-critical target capabilities that CPE must support in order to be successful. Success will be measured by CPE's ability to:

- achieve significant and growing vendor support;
- stimulate increasing volumes of product data contributed by the community to the CPE Dictionary;
- be acceptable to NIST for inclusion in a future release of SCAP;
- be deployed in product offerings to foster inter-vendor tool interoperability;
- be manageable across time and scale for large deployments.

Agenda:

Morning:

- Introduction and overview
- Constraints and ground rules
- Review survey results
- List user roles and tasks
- Describe user needs based on role and task. Identify and describe near-term target capabilities that the CPE specification and content management processes must support

Working Lunch: Identify and prioritize potential changes to the CPE specification and content maintenance process in order to support the target capabilities.

Afternoon:

- For each need from highest to lowest priority, describe the end state of the CPE dictionary and content maintenance process in order to support each target capability.
- Develop specific changes to the CPE specification (additions, deletions, documented implementation guidance) that must be taken in the near term to revitalize CPE adoption
- Determine next steps that the CPE specification moderators and the user community need to take to in order to achieve the target capabilities, including holding additional CPE workshops in the future.
- Develop an action plan for next steps. Identify and assign responsibility for supplemental efforts necessary to enable and ensure CPE adoption

Time permitting:

- Develop general plans for a CPE version 3.0 specification to address shortfalls in 2.x CPE

Day 2: Tuesday, February 23, 2010

eXtensible Configuration Checklist Description Format (XCCDF) Developer Days Workshop

Time: 9:00 a.m. – 5 p.m. EST

The XCCDF Developer Days Workshop is a one-day event that is sponsored by the DoD, hosted by the National Institute of Standards and Technology (NIST), and facilitated by the MITRE Corporation. The purpose of the workshop is to discuss and plan responses to the outstanding issues identified by the community.

Agenda:

Morning:

- Introduction and overview
- Alternate scoring models
- Content categorization and organization (beyond Groups)
- Updating metadata field and other metadata

Lunch

Afternoon:

- Clarify use of selected vs. role="unchecked" vs. UNCHECKED rule result
- Clarify the processing model for group selection and requires capabilities
- Clarify the behavior of the "multiple" attribute

Time permitting:
Review of error corrections and text clarifications

Day 3: Wednesday, February 24, 2010

Remediation Developer Days Workshop

Time: 9:00 a.m. – 12:30 p.m. EST

The Remediation Developer Days Workshop is a ½ day event that is sponsored and hosted by the National Institute of Standards and Technology (NIST), and facilitated by the MITRE Corporation. The purpose of the workshop is to engage the security automation community in establishing enterprise remediation standards, with a focus on common identifiers and extended metadata for remediation methods.

Agenda:

Morning:
1 hr General Discussion

- 20 minutes: Overview of existing work, broad remediation space
- 40 minutes: Explain/discuss how outreach and decision making will be performed (surveys, votes, conference calls, etc)

2.5 hr Current Issues

- 20 minutes: Common Remediation Enumeration(CRE)/Extended Remediation Data(ERD) introduction (scope, use cases, relationship to one another)
- 40 minutes: Method/effect

- 30 minutes: Scope of a single remediation/relation to indicators or other CREs (can CREs compose other CREs? can a CRE address multiple CVEs? etc.)
- 30 minutes: Remediation type/level (is remediation vs. mitigation vs. workaround vs. other part of CRE, ERD, and/or the policy language).
- 30 minutes: Parameters (when to parameterize, how to parameterize, parameter types, where do parameters fit in CRE/ERD)

Day 3: Wednesday, February 24, 2010 (Continued)

Digital Trust Developer Days Workshop

Time: 1:30 p.m. – 5:00 p.m. EST

The purpose of this workshop is to engage the community in issues relating to establishing a digital form of trust for SCAP Content.

Agenda:

Afternoon:

- Introduction and Overview
- XMLDSig Overview
- Other signing alternatives
- Enveloped versus Embedded
- Traceability
- Algorithms and parameters
- Reporting