Security Automation Developer Days

July 9 -13, 2012

Discussion Session
Briefing Session
Demo Session

The MITRE Corporation
Bedford, MA

Agenda

Monday July 9th 2012

10:00 - 10:10 **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.

10:10 – 12:00 **CCE** David Mann, MITRE

We will cover an overview of the project, followed by a discussion of four hard problems: 1) public references in a fluid, connected world, 2) counting issues and the content decisions that face the analyst, 3) proprietary identifiers issued internally by OS and software vendors, and 4) the Linux kernel versus supported open source packages.

12:00 - 12:30 **Open Lunch**

During the open lunch break we encourage community networking.

12:30 - 1:00 **Working Lunch (SecPod SCAP Repository Demonstration)**

During the working portion of lunch, Chandra Basavanna, of SecPod, will demo an SCAP Repository Interface.

1:00 – 2:50 **CPE - SWID Tagging** Steve Klos, TagVault
Brant Cheikes, MITRE

This session will begin with an informational overview of the ISO/IEC 19770-2:2009 Software Identification Tag standard. Then we will discuss a technical proposal developed by MITRE and TagVault that defines an approach for embedded CPE-related information into Software Identification Tags.

2:50 – 3:10 **Break**

3:10 – 4:00 **CPE - SWID Integration** Steve Klos, TagVault
Brant Cheikes, MITRE

This session continues the discussion started in the previous session. During this period we will focus on potential impacts to CPE dictionary management and maintenance related to the MITRE/TagVault proposal for embedding CPE-related information in Software Identification Tags.

4:00 – 5:00 **MILE and Information Sharing** Kathleen Moriarty, EMC

The IETF MILE working group is integrating the structured cyber security related information into a valuable set of information sharing specifications. This session will describe the state of MILE and how it's associated RFCs and Internet-Drafts fit in security automation efforts.

5:00 – 5:40 **Future SCAP Releases Discussion** John Banghart, NIST

This session will discuss the frequency and issues that surround SCAP releases as well as release information for other efforts.

5:40 - 5:50 **Day 1 Wrap Up**

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

Security Automation Developer Days

July 9 -13, 2012

Discussion Session
Briefing Session
Demo Session

The MITRE Corporation
Bedford, MA

Agenda

Tuesday July 10th 2012

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

8:10 – 10:00 **Standardizing Access to Organizational SCAP Content** Dave Waltermire, NIST, Kent Landfield, McAfee
SCAP content needs to be delivered internally within an organization. Today, the SCAP vendors cannot share a single local site security policy without the site staff having to go to each of the individual products and figuring out how to inject that new or updated policy into that product's delivery mechanisms. This session will describe means to address this by creating a content repository access specification.

10:00 – 10:15 **Break**

10:15 – 12:00 **Content Repository Interface Discussions** Dave Waltermire, NIST, Adam Halbardier, Booz Allen Hamilton
This is an interactive session to discuss the content repository architecture and access approaches described in the earlier session. It is intended that an action plan and specific steps will be developed during the discussions.

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

12:30 - 1:00 **Working Lunch (gOCIL Interpreter Demonstration)**
During the working portion of lunch, David Ries of gOCIL.org will demonstrate gOCIL, a new client/server OCIL interpreter, and discuss the various challenges inherent in implementing the OCIL standard in the enterprise.

1:00 – 2:20 **Security Automation and the Int'l Community** Kent Landfield, McAfee
SCAP is gaining international appeal as other countries are recognizing its value. As such there are efforts in various international SDOs to advance security automation. This session will describe the reasoning behind the movement and how each is playing a role today. IETF, ISO, and ITU-T efforts will be discussed.

2:20 – 3:00 **CEE** John Wunder, MITRE
This session will provide an overview of CEE 1.0 Beta and future plans for CEE, with a goal of raising awareness and increasing participation within the security automation community.

3:00 - 3:15 **Break**

3:15 – 5:00 **Enterprise Asset Reporting** Adam Halbardier, Booz Allen Hamilton, Dave Waltermire, NIST
This session will present ARF & ASR concepts and discuss issues surrounding the implementation of Enterprise Roll-up Reporting. A concrete Enterprise Reporting Architectural Proposal will be presented and frame subsequent discussion. The final 30 minutes will be used for identifying next steps and action items.

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 – 7:00 **SOCIAL (Optional)**
Dinner is at Flatbread Pizza – Cost: $20, drinks not included.

Security Automation Developer Days

July 9 -13, 2012

Discussion Session
Briefing Session
Demo Session

The MITRE Corporation
Bedford, MA

Agenda

Wednesday July 11th 2012

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

8:15 – 9:00 **Continuous Monitoring (CM) History and Directions** Kent Landfield, McAfee
Continuous Monitoring means many things to many people. CM is going to be affecting and relying on Security Automation standards moving forward. This will describe the background and perceived directions of the phased approach needed to get CM effectively developed and fielded.

9:00 – 10:00 **Continuous Monitoring CAESARS-FE Overview** Dave Waltermire, NIST
This session will provide an overview of CAESARS-FE, a reference architecture for supporting CM, and will cover the overall goals, subsystem model and interface design supporting single and multi-instance CM architectures.

10:00 – 10:15 **Break**

10:15 – 12:30 **CAESARS-FE Subsystem Components** Dave Waltermire, NIST
During this session, each subsystem of the CAESARS-FE architecture will be reviewed and discussed. The purpose of this session is to develop consensus around the overall architectural approach.

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

1:00 - 1:30 **Working Lunch (Lessons/Tips of creating PowerShell Configurations for OVAL)**
During the working portion of lunch, Michael Tan, of Microsoft, will discuss lessons learned and tips from the MS baseline team's experience building PowerShell-based configurations in the SCAP 1.2 format, specifically using OVAL 5.10 with the cmdlet_test. You will learn how the MS baseline team used the cmdlet_test to support the PowerShell Config Data Model and how to drive compliance requirements into product design to create baselines more efficiently. You will also see how the MS team built custom cmdlets to support SCAP 1.2.

1:30 – 2:45 **CAESARS-FE Interfaces** David Waltermire, NIST
This session will present the four interfaces identified in CAESARS-FE. The purpose of this discussion is to develop consensus around the design of the interfaces and to identify actions required to address any gaps.

2:45 - 3:00 **Break**

3:00 – 5:00 **CM Discussions and Next Steps** Dave Waltermire, NIST
This session will be an open discussion related to issues identified in the earlier companion sessions. One hour is allotted for discussion and 30 minutes for identifying next steps and action items.

5:00 – 6:00 **Automated Checking of Windows User Configuration Settings**
Jack Vander Pol, SPAWAR
There is an automation gap in SCAP related to the ability to review Windows User Config settings. With the increasing amount of products being configured on a per user basis such as Microsoft Office, Internet Explorer, and many OS settings, SCAP, especially the OVAL language, needs to be updated to allow for this automation.

6:00 - 6:10 **Day 3 Wrap Up**
Wrap up the events of the day. Preview the next day. Make any pertinent announcements.

Security Automation Developer Days

July 9 -13, 2012

The MITRE Corporation
Bedford, MA

Discussion Session
Briefing Session
Demo Session

Agenda

Thursday July 12th 2012

8:00 - 8:10 **Welcome**

Provide an overview of the day's upcoming sessions.

8:10 – 9:40 **OVAL - Mobile Device Assessment** Chandra Basavanna, SecPod, Tim Nary - Booz Allen Hamilton

Organizations increasingly need to accommodate mobile devices on their networks. As a result, there is a need to ensure that there is a mechanism to assess the configuration of these devices in a standardized way. However, the rapid evolution of mobile devices and working within their limited resources introduces a variety of challenges. This session will begin with a discussion of a secure configuration management middleware approach that assesses mobile devices by querying a Mobile Device Management (MDM) database using OVAL. It will be followed up with a discussion on the extension of OVAL to support the assessment of Android devices. Both will drive the discussion around the needs, approaches, and challenges associated with the support of mobile devices using OVAL.

9:40 – 10:20 **OVAL for Inter-networking Devices** Luis Nunez, Apex Assurance Group, Chandra Basavanna, SecPod, David Solin, jOVAL

The OVAL specification currently supports a diverse set of platforms. We see Windows and a variety of UNIX operating systems supported of which there is only one Inter-networking platform. Inter-networking devices are routers and switches that connect the Internet. Currently Cisco is the only vendor and platform that is represented in the area of inter-networking devices. In this session, we propose a new platform to be supported by the OVAL specification. The session will cover new schema, content, and a tool (jOVALdi) associated with the new platform. The session will also compare similarities between the Cisco IOS schema and the new platform schema.

10:20 – 10:40 **Break**

10:40 – 11:20 **SCAP and the Network Configuration Protocol (NETCONF)** Luis Nunez, Apex Assurance Group, Chandra Basavanna, SecPod, David Solin, jOVAL

Further expanding the discussion on inter-networking devices (Routers and Switches) the NETCONF protocol will be discussed. NETCONF is an open standard protocol supported by major inter-networking vendors. This session looks to leveraging the NETCONF schema to retrieve the configuration files from inter-networking devices. This session will cover issues and challenges related to:

- *Security Automation and inter-networking devices.*
- *Access methods to retrieve and process device configuration settings.*

11:20 – 12:20 **OVAL - Database Vulnerability Assessment** Charlie McClain, IBM, Louis Lam, IBM

The SQL-based tests, in the OVAL Language, have been a trouble area for the community for many years whether it was due to the security concerns around storing the connection string in an OVAL Definitions document or not clearly specifying what types of SQL queries were valid with respect to the OVAL Language. This session will examine the issues and challenges regarding the existing SQL-based tests as well as present a new SQL-based test that will address these issues and challenges.

Security Automation Developer Days

July 9 -13, 2012

Discussion Session
Briefing Session
Demo Session

The MITRE Corporation
Bedford, MA

Agenda

12:20 - 12:50 **Open Lunch**

During the open lunch break we encourage community networking.

12:50 - 1:20 **Working Lunch (TAXII Adoption)**

During the working portion of lunch, Aharon Chernin, of DTCC, will discuss TAXII adoption and will demonstrate a tool created for producing and reading standards-based intelligence content.

1:20 – 3:20 **OCIL** Jim Ronayne, NSA
Shane Shaffer, G2, Inc.

This session will discuss recent proposals for OCIL, XCCDF, and CPE-language to make OCIL more usable in an enterprise environment. Other proposals to expand and clarify the OCIL specification to support better questioning will be addressed as well.

3:20 - 3:40 **Break**

3:40 – 5:40 **Reinvigorating Remediation** Jim Ronayne, NSA
Kent Landfield, McAfee

The remediation specifications have been slow to develop. The CRE specification has been released in draft form but has had little traction so far. This session will first briefly discuss a specific proposal for including CRE content in XCCDF benchmarks. A significant number of new benchmarks will be created this year and will include basic remediation content. A method for declaring remediation policy is required to make the content usable. The rest of the session will focus on the strategy for making remediation standards viable within the security automation community. Fundamental assumptions about future development and use of remediation standards will be questioned and a plan of action for specification, content, and tool development will be determined.

5:40 - 5:50 **Day 4 Wrap Up**

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

Security Automation Developer Days

July 9 -13, 2012

The MITRE Corporation
Bedford, MA

Discussion Session
Briefing Session
Demo Session

Agenda

Friday July 13th 2012

8:00 - 8:10 **Welcome**

Provide an overview of the day's upcoming sessions.

8:10 – 9:00 **TAXII / STIX** Rich Struse, DHS, Sean Barnum, MITRE

Trusted Automated eXchange of Indicator Information (TAXII) is a set of protocols and representations that enable the representation and automation-supported sharing of behavioral cyber threat indicators. Structured Threat Information eXpression (STIX) is a language for the specification, capture, characterization and communication of cyber threat information in a structured fashion to support more effective cyber threat management processes. This session will provide an overview of these efforts and describe their relationship to CybOX.

9:00 – 9:45 **High-Level CybOX** Sean Barnum, MITRE

This session will provide an overview of the Cyber Observable eXpression (CybOX) 1.0 draft, a standardized schema for the specification, capture, characterization and communication of events or stateful properties that are observable in the operational domain.

10:00 – 10:15 **Break**

10:15 – 10:45 **High Level MAEC** Penny Chase, MITRE

This session will provide an overview of Malware Attribute Enumeration and Characterization (MAEC), a standardized language for encoding and communicating high-fidelity information about malware based upon attributes such as behaviors, artifacts, and attack patterns. Particular focus will be brought upon the use cases targeted by MAEC, as well as regarding its current structure and components.

10:45 – 11:15 **MAEC Utilities** Ivan Kirillov, MITRE

A number of freely available utilities have been developed to support the creation and manipulation of MAEC content. This session will delve into the currently available suite of MAEC utilities, their use, and implementation, with emphasis on the end-to-end scenario of malware analysis to malware detection.

11:15 – 12:00 **OVAL Artifact Hunting** Charles Schmidt, MITRE

Last year, CyberESI introduced the artifact hunting use case for SCAP to the community. Specifically, this use case extended the OVAL Language to support the detection of indicators of compromise on end systems. The primary obstacle that kept this work from moving forward was the lack of an OVAL Language Sandbox where this use case could be developed and vetted. With the OVAL Language Sandbox now available, this session will revisit some of the proposals made by the CyberESI team, discuss the connection between MAEC, CybOX, openIOC, and OVAL, and discuss the challenges and issues encountered during the development of this use case.

12:00 – 12:10 **Developer Days Wrap-up**