Security Automation Developer Days

July 9 -13, 2012

The MITRE Corporation
Bedford, MA

Read-Ahead Materials

Monday July 9th 2012

10:10 – 12:00	CCE
1:00 – 2:50	CPE - SWID Tagging Required Reading – *Certified SWID Tag Integration with Common Platform Enumeration names* Supplemental Reading – *Analysis of Software Identification Tools* Supplemental Reading – *Software Identification Talking Points*
3:10 – 4:00	CPE - SWID Integration
4:00 – 5:00	MILE and Information Sharing Required Reading – *IODEF-extension to support structured cybersecurity information* Supplemental Reading – *Other MILE Working Group Active Internet-Drafts and associated RFCs*
5:00 – 5:40	Future SCAP Releases Discussion Required Reading – *SP 800-126: SCAP Version 1.2* Required Reading – *Errata* Required Reading – *Guide to Adopting and Using SCAP Version 1.2*

Tuesday July 10th 2012

8:10 – 10:00	Standardizing Access to Organizational SCAP Content
10:15 – 12:00	Content Repository Interface Discussions
1:00 – 2:20	Security Automation and the Int'l Community
2:40 – 3:20	CEE Required Reading – *CEE Architecture Overview Specification v1.0a*
3:20 – 5:00	Enterprise Asset Reporting Required Reading – *NIST IR 7848: Specification for Asset Summary Reporting Format 1.0* Required Reading – *NIST IR 7693: Specification for Asset Identification 1.1* Required Reading – *NIST IR 7694: Specification for the Asset Reporting Format 1.1* Supplemental Reading – *GRC Report Exchange*

Wednesday July 11th 2012

8:15 – 9:00	Continuous Monitoring (CM) History and Directions
9:00 – 10:00	Continuous Monitoring CAESARS-FE Overview Required Reading – *Continuous Asset Evaluation, Situational Awareness, and Risk Scoring Reference Architecture Report (CAESARS)* Required Reading – *CAESARS Framework Extension: An Enterprise Continuous Monitoring Technical Reference Model* Supplemental Reading – *Continuous Monitoring Reference Model Workflow, Subsystem, and Interface Specifications* Supplemental Reading – *NIST IR 7800: Applying Continuous Monitoring Technical Reference Model to the Asset, Configuration, and Vulnerability Management Domains*
10:15 – 12:30	CAESARS-FE Subsystem Components
1:30 – 2:45	CAESARS-FE Interfaces
3:00 – 5:00	CM Discussions and Next Steps
5:00 – 6:00	Automated Checking of Windows User Configuration Settings

Thursday July 12th 2012

8:10 – 9:40	OVAL- Mobil Device Assessment Required Reading – *OVAL Read-Ahead links found here*
9:40 – 10:20	OVAL for Inter-networking Devices Required Reading – *OVAL Read-Ahead links found here*
10:40 – 11:20	SCAP and the Network Configuration Protocol (NETCONF) Required Reading – *Network Configuration Protocol (NETCONF)* Required Reading – *jOVAL Features*
11:20 – 12:20	OVAL -Database Vulnerability Assessment Required Reading – *OVAL Read-Ahead links found here*
1:20 – 3:20	OCIL Required Reading – *Recent (since May) email discussions* Supplemental Reading – *NIST IR-7692 – OCIL Specification*
3:40 – 5:40	Reinvigorating Remediation Required Reading – *NIST IR 7831: Common Remediation Enumeration (CRE) V 1.0* Required Reading – *NIST IR 7670: Proposed Open Specifications for an Enterprise Remediation Automation Framework* Required Reading – *CRE use in XCCDF (email message)* Supplemental Reading – *NIST IR-7831 – CRE Specification*

Friday July 13th 2012

8:10 – 9:00	TAXII / STIX
9:00 – 9:45	High-Level CybOX
10:15 – 10:45	High Level MAEC
10:45 – 11:15	MAEC Utilities
11:15 – 12:00	OVAL Artifact Hunting