Event Management Automation Protocol (EMAP) 2011 Developer Days

August 29-30, 2011

Portrait Room
The National Institute of Standards and Technology
Gaithersburg, MD

AGENDA

Monday, August 29, 2011

8:45 - 9:50 **Welcome and EMAP Program Overview** Paul Cichonski, NIST

Introduce the Event Management Automation Protocol (EMAP) from a program perspective. Discuss the high level goals, components, and use cases of EMAP. Also discuss ideas relating to the low-level activities necessary to standardize the collection, parsing, filtering, correlation, and aggregation of event data to produce meaningful results; this will set the context for the discussion throughout the rest of the developer days.

9:50 - 10:00 **Morning Break**

10:00 - 12:00 **Common Event Expression (CEE)** Bill Heinbockel, MITRE

Introduce the Common Event Expression (CEE) specifications being developed to create a standardized event data model and set of transport syntaxes for event data. Introduce the different specifications that make up CEE, focusing on how they interact to provide both standardized syntax and semantics for event expression. Discuss open questions within the CEE community; these questions will cover a variety of areas across all of the CEE specifications.

12:00 - 1:00 **Lunch** NIST Cafeteria

1:00 - 2:50 **Common Event Expression (CEE)** Bill Heinbockel, MITRE

A continuation of the briefing/discussion from the morning CEE talk.

2:50 - 3:00 **Afternoon Break**

3:00 - 5:00 **The Open Group Distributed Audit Services (XDAS) v2** David Corlette, Novell

Introduce The Open Group XDAS v2 initiative and discuss the similarities, differences and collaboration opportunities between EMAP and XDAS v2. Discuss components and use cases relating to XDAS v2 including the need for standardizing the compliance mechanism between event management systems.

Tuesday, August 30, 2011

8:30 - 10:50 **Standardizing Event Parsing and Translation** Paul Cichonski, NIST & George Saylor, G2

Discuss the issues relating to leveraging standardized event data models within legacy environments, focusing on the need to transform legacy log formats into new formats adhering to standardized data models. Introduce and discuss initial ideas for methods of standardizing the expression of event parsing and translation logic for achieving legacy-to-standardized log transformation. Discuss real-world strategies for using this type of logic and the performance implications associated with different methods of modeling the solution.

10:50 - 11:00 **Morning Break**

11:00 - 12:00 **Standardizing Event Rule Languages** Paul Cichonski, NIST & George Saylor, G2

The creation of a standardized event data model provides the foundation for building a standardized rule language for expressing complex sets of rules modeling things such as malicious incidents or complex attacks. The benefit expressing these rule sets in standardized ways is that it allows organizations, such as CSIRTs, to share rules that model ongoing cross-organizational incidents. Discuss issues relating to the standardization of event management filtering, correlation and aggregation rule languages. Discuss different strategies of standardization including the creation of a new brand new rule language versus the adoption of one or more legacy languages for use with a standardized event data model.

12:00 - 1:00 **Lunch** NIST Cafeteria

1:00 - 2:00 **Standardizing Event Rule Languages** Paul Cichonski, NIST & George Saylor, G2

A continuation of the briefing/discussion from the morning talk.

2:00 - 3:00 **Cyber Observables and Integration with EMAP** Sean Barnum, MITRE

Introduce an ongoing effort at MITRE to develop a cyber observables schema (CYBOX) to model observable indicators on an IT system. Introduce the details of the CYBOX strategy and data model and discuss potential ways for connecting this work with the EMAP initiatives.

3:00 - 3:10 **Afternoon Break**

3:10 - 4:15 **Integrating Event Management and Continuous Monitoring** Dave Waltermire, NIST

Introduce an ongoing effort at NIST to develop architecture models for implementing continuous monitoring capabilities. Discuss the basics of the approach and concepts relating to the different tiers of the architecture. Also discuss the potential ways in which an EMAP-compliant event management system may integrate with a standardized continuous monitoring architecture to satisfy such goals as alerting, incident reporting, and data collection.

4:15 - 4:45 **Wrap-up**

Wrap up the event, discuss the path forward and make any announcements.