Emerging Topics

Engineering Session

NIST

Emerging Topics

- CEE
- Taxonomies
- CAPEC
- MAEC
- TNC/IF-MAP

CEE

- CEE – Common Event Expression
  - It's alive!! A proposed architecture was released
  - Work on use cases, and design are ongoing (not released yet, but should be coming)
  - Community around CEE is growing
- What CEE brings
  - Data Dictionary which helps us approach taxonomy
  - Recommendations which help us define what to log
  - Syntax and Transport

CEE

- CEE is still being developed
  - There are not final publications to work from
  - There are likely some future changes to work through
- From an EMAP perspective…
  - Since EMAP accounts for a transition period for CEE, this is not high risk
  - OEEL allows EMAP to work with CEE, other standards, as well as proprietary formats

Taxonomy

- Classifying “events” is not a simple task
  - There are many similar event types with nuanced differences
  - Naming conventions do not currently exist
  - Where would agreement on naming, meaning, etc…come from?
- To really see the value of EMAP, taxonomies must exist
  - Provide meaning to events
  - Enhance correlation

Taxonomy

- Some combination of community, industry and government must work together on event taxonomies
  - Log producers know their “source” log data better than anyone
  - Log consumers frequently know the meaning of these events in a given context (systems management vs. SIEM)
  - Often, guidance comes from the community and finds its way into industry
  - Enabling this interplay is critical
  - Standards for expression may allow “crowd-sourcing” to work

CAPEC

- CAPEC – Common Attack Pattern Enumeration and Classification
  - There is a very rich dictionary of attack patterns here
  - Maps well to other specifications and efforts
  - The data isn't for the operations folks, but could be useful as enrichment
  - Correlation or analysis can help to automate the injection of this content
  - Waiting for the observables schema (more later)

MAEC

- MAEC – Malware Attribute Enumerization and Characterization
  - High fidelity information about malware
  - Describes high, medium, and low level characteristics
  - Observables are coming
    - Observables will give us the ability to correlate logs and events with known malware
    - Forensics and analysis will enhance the observables
    - True automation from dynamic malware analysis to event correlation becomes possible in a standardized way

TNC and IF-MAP

- Work from Trusted Computing Group/Trusted Network Connect
  - IF-MAP – Interface for Metadata Access Points
    - Acts as a database for network information
    - Information can include system health (SCAP has been tested)
    - AND, events…This was tested at an Interop
  - What if we can disseminate CERE rules via IF-MAP?
    - Dynamic defense?
    - Dynamic signature generation

TNC and IF-MAP

- Malicious activity could trigger automated response
- Well thought out response actions may take simple actions (single system quarantine, and remediation) to net speeds
- Requires trusting the technology and the policies
- Great promise here in sensor information sharing
- Signatures and rules passed around through MAP to raise sensor awareness vertically and horizontally
- With good taxonomy, meaningful information can be discovered, correlated, and shared…

– This will take considerable planning and thought

- If we get it right…