Automated XML Content Data Exchange and Management

draft-waltermire-content-repository-00

http://datatracker.ietf.org/doc/draft-waltermire-content-repository/

David Waltermire (david.waltermire@nist.gov)

Current State

- Work has started to standardize the expression of content used to drive security processes
  - Assessment methods (e.g. OVAL)
  - Configuration policies (e.g. XCCDF)
  - Reporting format descriptions (e.g. ASR)
  - Record-based data feeds (e.g. vulnerability info)
- Standardization in content enables multiple tools to use the same content
- Content is broadly distributed using largely ad-hoc methods (e.g. HTTP, sneaker-net, product-bundled)

Content Distribution Issues

- Lack of interoperability between existing content-based solutions
- Content is often duplicated during distribution
  - Poor reuse model: copy-and-paste propagates defects
  - Complicates tracking/responding to bugfixes and other necessary updates
- Content is not often reused, even when usage rights allow reuse
  - Causes duplication of effort
  - Unnecessary drift in the approach defined within the content
- Content is packaged/bundled in many different ways, complicating data access (e.g. compression, packaging, composition)
- Verifying the validity of content can be challenging
  - Integrity mechanisms are non-standardized
- Management of dependencies are often handled using ad-hoc methods

Content Repository Requirements

- Vendor-neutral content access
- Support for multiple document encoding formats (e.g. XML, JSON)
  - Support for validation of content conformity when possible
- Utilize existing transport protocols if possible
- Retrieval of content by identifier (as a resource?)
- Support for requesting content revisions
- Content references should be dereferenceable
- Provide standardized mechanism(s) for access control
  - Security authenticating the user at minimum
- Support mechanism(s) for caching
  - May limit use of secure transport in some use cases (e.g. TLS)

How does this relate to the IETF?

Security Automation and Continuous Monitoring (SACM)

Use Case 1: System State Assessment (draft-waltermire-sacm-use-cases-02)

- Data Collection (4.1.2)
  - Enables data collection methods defined as automation content to be distributed and used by assessment tools
- Assessment Result Analysis (4.1.3)
  - Content records can contain scoring/weighting information and expected state
- Content management (4.1.4)
  - Supports the standardized retrieval of various types of content

How does it relate to the IETF? (Cont'd)

Security Automation and Continuous Monitoring (SACM)

Use Case 3: Security Control Verification and Monitoring (draft-waltermire-sacm-use-cases-02)

- Tasking and Scheduling (4.3.1)
  - Enables the identification (and eventual retrieval) of any content needed to perform assessments
- Data Aggregation and Reporting (4.3.2)
  - Provide supporting information based on content references that enhance reported data
  - Use referenced metadata to support data aggregation

How does it relate to the IETF? (Cont'd)

Managed Incident Lightweight Exchange (MILE WG)

IODEF-extension to support structured cybersecurity information (SCI) (draft-ietf-mile-sci-05)

- Enables SCI to be included by reference instead of being embedded

Different in scope and possibly in concept from draft-field-mile-rolie-00

- This effort is focused on assessment content and supporting metadata used for reporting (broad)
- Rolie is focused on the lightweight exchange of indicator and incident related information (specific)

Future Work / How you can help?

- Help define a protocol draft describing how content is retrieved

- Help to refine the requirements
- Comment on the draft
- Volunteer to be a co-editor