Resource-Oriented Lightweight Indicator Exchange
draft-ietf-mile-rolie-01

IETF 95
Buenos Aires, Argentina
2016-04-05

John P. Field <jfield@pivotal.io>
David Waltermire <david.Waltermire@nist.gov>
Relevance to the SACM Charter

The working group will define:

2. A set of standards for interacting with repositories of content related to assessment of endpoint posture.

Repository protocols are needed to store, update, and retrieve configuration checks and other types of content required for posture assessment (see step 2 above). A content repository is expected to house specific versions of checklists (i.e. benchmarks), may be required to satisfy different use cases (i.e. asset inventory, configuration settings, or vulnerabilities). In addition, content repositories are expected to store up-to-date dictionary of specific enumerations, such as those used for configuration element identifiers, asset classifications, vulnerability identifiers, and so on.
Applicability to SACM Use Cases

RFC7632 defines use cases for:

• Section 2.1.1: Define, Publish, Query, and Retrieve Security Automation Data
  • Provides a mechanism to organize vulnerability alerts, OVAL definitions, SWID tags, XCCDF checklists, configuration scripts, etc.
  • Supports federation of repositories
  • Discovery of a given organizations “guidance” collections
  • Cross referencing between data sources
  • Persistent, resource identifiers based on URLs
Applicability to SACM Use Cases (Continued)

RFC7632 defines usage scenarios for:

• Section 2.2.1: Definition and Publication of Automatable Configuration Checklists
  • ATOMPub provides a RESTful interface for publication

• Section 2.2.6: Identification and Retrieval of Guidance
  • ATOMPub provides a RESTful interface for discovering, querying, and retrieving resource collections

• Section 2.2.7: Guidance Change Detection
  • Temporal metadata in ATOM format allows for changes to resources to be identified
Issue: ROLIE is very CSIRT focused

• CSIRTS are described as the primary user
  • IODEF as MTI
  • Normative text references CSIRTs.

For example:
  A CSIRT implementing this specification MUST implement server-authenticated TLS.

  At least one collection MUST provide a feed of incident information for which the content model for the entries uses the IODEF schema.
Issue: Anonymous access is not allowed

• Some types of guidance may be publicly available
  • Configuration checklists
  • Vulnerability reports (e.g., vendor, National Vulnerability Database, Japanese Vulnerability Notes)
  • SWID tags

• Section 5.4: “Servers MUST require user authentication.”

• Authentication and access controls might be more applicable as collection-specific configurations
Issue: ROLIE server discovery

• Section 5.8:
  The service document SHOULD be discoverable via the CSIRT organization's Web home page or another well-known public resource.

• We should consider a method to enable discovery of a security automation ROLIE service.
  • DNS SRV records
  • Standard URL path for ATOM service document
  • Focus on MUST requirements
Issue: Feed categories based on Expectation and Impact Classes

• Recommended in section 5.3
• Used to support triage of incident investigation and response activities based upon current threat environment or resource limitations

• Applies to only some classes of information (e.g., incident), but not others

• Need to consider categories specific to each information class?
Next Steps

• Drive mailing list discussion about open issues
• Produce an updated -02 draft addressing issues