MILE Working Group
Internet-Draft
Intended status: Informational
Expires: October 28, 2013

P. Kampanakis
Cisco Systems
April 26, 2013

IODEF Usage Guidance
draft-ietf-mile-iodef-guidance-00.txt

Abstract

The Incident Object Description Exchange Format [RFC5070] defines a data representation that provides a framework for sharing information commonly exchanged by Computer Security Incident Response Teams (CSIRTs) about computer security incidents. Since the IODEF model includes a wealth of available options that can be used to describe a security incident or issue, it can be challenging for implementers to develop tools that can Leverage IODEF for incident sharing. This document provides guidelines for IODEF users and implementers. It will also address how common security indicators can be represented in IODEF. The goal of this document is to make IODEF's adoption by vendors easier and encourage faster and wider adoption of the model by Computer Security Incident Response Teams (CSIRTs) around the world.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

The Incident Object Description Exchange Format in [RFC5070] defines a data representation that provides a framework for sharing information commonly exchanged by Computer Security Incident Response Teams (CSIRTs) about computer security incidents. The IODEF data model consists of multiple classes and data types that are used in the IODEF XML schema.

The IODEF schema was designed to be able to describe all the possible fields that would be needed in a security incident exchange. Thus, IODEF contains plenty data constructs that could potentially make it harder for IODEF users and implementers to decide which are the most important ones. Additionally, in the IODEF schema, there exist multiple fields and classes which do not necessarily need to be used in every possible data exchange. Moreover, there are fields that are useful only in data exchanges of non-traditional security events. This document tries to address the issues above. It will also address how common security indicators can be represented in IODEF. It will point out the most important IODEF classes for an implementer and describe other ones that are not as important. Also, it addresses some common challenges for IODEF implementers and how they should be addressed. The end=goal of this document is to make IODEF's adoption by vendors easier and encourage faster and wider adoption of the model by Computer Security Incident Response Teams (CSIRTs) around the world.

Section 3 discusses the recommended classes and how an IODEF implementer should chose the classes to implement. Section 4 presents common considerations and implementer will come across and how to address them. Section 5 goes over some basic security concepts and how they can be expressed in IODEF.

2. Terminology

The terminology used in this document follows the one defined in RFC 5070 [RFC5070] and I-D.draft-ietf-mile-sci [I-D.ietf-mile-sci].

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

3. Implementation Strategy

It is important for IODEF implementers to be able to distinguish how the IODEF classes will be used for incident information exchanges.

It is critical for an implementer to follow a strategy according to which he will chose to implement various IODEF classes. It is also important to know what the most common classes that will be used to describe common security incident or indicators. Thus, this section will describe the most important classes and factors an IODEF implementer should take into consideration before designing the implementation or tool.

3.1. Recommended classes to implement

This section explains the mandatory to implement IODEF classes that are required more than once and also are useful.

[...More to be added...]

3.2. Decide what IODEF will be used for

This section describes that there is no need to implement all fields of IODEF, the ones that are necessary for your use-cases. The implementer should look into the schema and decide classes to implement (or not) Also it explains that other external schemata might be needed to describe incidents or indicators, based on SCI draft extensions.

[...More to be added...]

4. IODEF considerations and how to address them

4.1. Logic for Multi-Indicator use-cases

This section describes how multiple indicators can be combined in an IODEF document. An example is the Watchlist-source element of how to do AND / OR (watchlist means or). [We want to make sure the logic was consistent throughout the schema and set in guidance. For Node information, a watchlist of Systems means that the information is ORed with the other information in the Flow section and an AND with rest of the content in the EventData grouping. As such, we need to replicate this pattern elsewhere, which is easy to do in the current format. For HashInformation type, A watchlist type was added for each value. In the Key class, a type was added with watchlist as an option. If the watchlist is used, the data provided is just that, a watchlist of separate values. Like the Node class, if information is grouped together, it represents the same thing. With this pattern, if you set the type value for HashInformation to file_hash, the list provided are just alternate representations for the same hash (sha256, sha1, md5, etc.). For the Key information, it's a little different as the grouping without it would just be part of a joined

event as opposed to alternate ways to represent the same value. To keep the pattern consistent. It would make sense to have the different Keys provided have the tags at the higher level (WindowsRegistryKeyModified tag included), but have them all represented within the same EventData instance. The included examples are following this logic pattern if examples are helpful to weigh in on this. If agreed on the pattern for logic.] "

[...More to be removed and added...]

4.2. Unnecessary Fields

This section talks about fields that do not always play in important role like Assessment, Impact

[...More to be added...]

4.3. Restrictions in IODEF

This section describes how Restriction can pose challenges

[...More to be added...]

4.4. Enumerations

This section explains how enumerators have been expanded to include multiple indicators. And also how external ones can be defines.

[...More to be added...]

4.5. Extensions

This section explains how to describe things IODEF can't describe (SCI draft), or extensions not yet known, or implemented, when do you use another xml schema encapsulated in iodef

[...More to be added...]

4.6. External References

draft draft-montville-mile-enum-reference-format "This format allows the <Version> to be associated with the id rather than the id_type. By requiring that a specific type and version be associated with the identifier, an implementer can look up the type in an IANA table to understand exactly what the identifier in ReferenceName is and how s/he may expect that identifier to be structured."

[...More to be added...]

4.7. Groupings

This section describes set-id, indicator-id

[...More to be added...]

5. Common Security Concepts and how to describe them in IODEF

5.1. Sinkholes and C&C, Bots

Describes how Bots and their C&C can be presented using the updated IODEF schema

[...More to be added...]

5.2. Domain Data

Describes how DNS data (A record, PTR records) can be described using the new IODEF schema

[...More to be added...]

5.3. Malware

Describes how a piece of malware can be descrivbed using the updated IODEF schema.

[...More to be added...]

5.4. Email Abuse - Phishing

Using ARF and/or http://ietf.org/rfc/rfc5901.txt

[...More to be added...]

5.5. DoS

Describes how a common DDoS attack can be described using IODEF

[...More to be added...]

6. Security Considerations

7. Acknowledgements

8. Security Considerations

9. Normative References

[I-D.ietf-mile-sci]
Takahashi, T., Landfield, K., Millar, T., and Y. Kadobayashi, "IODEF-extension to support structured cybersecurity information", draft-ietf-mile-sci-06 (work in progress), February 2013.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC5070] Danyliw, R., Meijer, J., and Y. Demchenko, "The Incident Object Description Exchange Format", RFC 5070, December 2007.

Author's Address

Panos Kampanakis
Cisco Systems
170 West Tasman Dr.
San Jose, CA 95134
US