From: Smith, Pamela A.
Sent: Friday, March 20, 2015 9:00 AM
To: STIX-DISCUSSION-LIST@LISTS.MITRE.ORG
Subject: RE: [STIX] Discussion ref Requirements for the Contents of a Robust STIX Marking Extension

Building off of Bret's suggestions, for Allowed Action Restrictions, you could imagine three sub-elements (borrowing from XACML):

- Action: Defined vocabulary of actions that could be taken as a result of receiving the information
- Rule Effect: two values: permit or deny
- Scope: the organizations, type of people, a sharing group that has been certified, country, etc.

So, the STIX marking extension could permit an unlimited number of Allowed Action Restrictions:

Allowed Action Restriction 1
Action = "BLOGPOST"
Rule Effect = "deny"
Scope = "All"

Allowed Action Restriction 2
Action = "REPOSTFORPROFIT"
Rule Effect = "permit"
Scope = "AAAIndicators, Inc"

Allowed Action Restriction 3
Action = "REPOSTFORPROFIT"
Rule Effect = "deny"
Scope = "AcmeIndicators, Inc"

Etc.

Need to think about defaults (deny-unless-permit? permit-unless-deny?) if appropriate. Need to think about conflicts. Need to think about a standard way of representing Scope so it can be consistently parsed.

Pam Smith, JHU/APL

From: Jordan, Bret [mailto:bret.jordan@bluecoat.com]
Sent: Thursday, March 19, 2015 1:33 PM
To: Smith, Pamela A.
Cc: STIX-DISCUSSION-LIST@LISTS.MITRE.ORG
Subject: Re: [STIX] Discussion ref Requirements for the Contents of a Robust STIX Marking Extension

Brilliant.

On the allowed action restrictions, we need to consider the use cases of:
1) Taking content and generating reports, blog posts, marketing messages etc from it
2) Vendors using content for internal processing or analysis versus sharing with their customer base through their own proprietary methods. Keep in mind most vendors have an all or nothing approach to who gets their feeds.

Another part that is going to fit in with this, is something Joep, Jane, and I, along with a few others, have been talking about on the TAXII list. That is, certification. One of the TAXII client / server certification points needs to be wether or not you can handle data markings and if your software will actually listen to them in an automated way or does it require human processing. A group that has more sensitive data may not want to share data with certain organizations, not because of the organization, but due to the lack of their ability to handle data markings correctly. So the use case would be, I will share with you and you can share my data with others, so long as the software that is used can actually deal with X, Y, and Z.

Thanks,

Bret

Bret Jordan CISSP
Director of Security Architecture and Standards | Office of the CTO
Blue Coat Systems
PGP Fingerprint: 62A6 5999 0F7D 0D61 4C66 D59C 2DB5 111D 63BC A303
"Without cryptography vihv vivc ce xhrnrw, however, the only thing that can not be unscrambled is an egg."

On Mar 19, 2015, at 10:57 AM, Smith, Pamela A. <Pam.Smith@JHUAPL.EDU> wrote:

All,

As we move into a sharing environment where an information producer automatically shares their information with others or with some brokered sharing service(intermediary), would an information producer want to mark the information to control further sharing or use, even beyond that "first hop"? I am assuming yes, based on previous spirited discussions ref XPATH and marking.

I'm posting this to begin dialog on the requirements for what content would go into a robust STIX data marking extension (not to discuss the pros and cons of the XPATH approach to marking elements within a document).

Some proposed use cases: a robust STIX data marking structure would allow the producer to specify enough information to enable either the information consumer or an intermediary to observe and implement the following automated processing:

- Further Sharing Restrictions: Once a consumer (or the intermediary) has information
  - Who else can it be shared with based on data type and the potential-consumer's authority/training/capacity-to-handle that data type (e.g. personally identifiable information, proprietary information, protected critical infrastructure information, etc)

  - Who else can it be shared with, based on the characteristics of the consumer (i.e. is the next consumer a member of a specific organization, a country, a ISAO, part of the government, etc.?)
  - (Note: This pre-supposes an environment where certain trusted services are available that provide characteristics of potential consumers.)
- Allowed Action Restrictions: What actions can information consumers take based on this information (e.g. use in network defense actions, simply monitor but take no other action, test data only-don't use operationally, etc.).
- Retention Restrictions: How long can consumers or the intermediary keep the information before they must purge/destroy it?
- Others?

(Understanding that all of the above is only useful if the consumer or intermediary observes the markings…)

Pam Smith, Systems Engineer, JHU/APL