Attendees:

Sarah

Trey

Chris Ricard

Bret Jordan

John Wunder

Mark Davidson

Nathan Reller

Rich Struse

Christian Hunt

Dave lemire

Ivan

Jmg

Rich Piazza

Sean Barnum

Terry MacDonald

Paul Patrick

Bill Chu

Jeff

TOPIC: IEP

John: IEP is intended to supplement TLP, it’s a set of policy statements. IEP 1 is released already, working on IEP 2. They have gotten feedback (some from CTI-TC) regarding the spec. IEP would be added as a data marking, to tag content in STIX with IEP polices. The proposal is in the playground, with a reference to IEP document itself. It’s pretty straightforward to add into STIX text, but that could hide complexity into what it could MEAN to ingest IEP. What does a tool do with it? What does it mean for conformance and interoperability?

What does it mean to “support” IEP policy statements? How does a tool accomplish this (rather than a person)? What about policies that don’t make sense for that specific tool? The issues aren’t specific to IEP, TLP has some of the same failings.

Should we implement it if we can’t validate that the tools can comply it?

Option 1: Add a statement saying IEP or other markings don’t attempt to define behavior and are more informational than conformance requirements. (this is how TLP works now)

* Doesn’t insure interoperability of policy statements in the language,
* Doesn’t insure automation
* May cause people to blame STIX or products if IEP doesn’t work right

Option 2: Defer adding IEP for now, work with FIRST SIG to make it more automatable.

* Ensures we get an automatable, interoperable policy
* Avoids giving our stamp of approval to something that may not be fully baked

Terry: I’m one of the FIRST IP SIG co-chairs. We view it as TLP with more details. Producers felt they weren’t able to convey what they wanted people to be able to do with the data they provided (looking at it from a legal entity to entity level). It wasn’t designed to be machine to machine, more from an informational level of use. It would be up to the people running the software to make sure they were compliant (not the software).

Chris Ricard: This may be a slight modification to option 1, STIX 2.x requires TLP support. It seems like all STIX communication will include TLP, if we went with option 1, STIX content may include IEP. The TLP marking within IEP doesn’t have to be the same as the TLP marking within the TLP marking. If it has both, and you ignore the IEP rules, maybe you can use just TLP, and you could consider it TLP: RED?

John: IEP also contains TLP, so you could have both.

Terry: They could be different TLPs. The extra controls IEP provides could allow you to relax other controls, (like lower the TLP) within IEP.

Chris: Suggests if you ignore IEP you should have a blanket TLP (ie: RED) that you HAVE to adhere to.

Sean: Data markings are informative, and are separate from STIX. STIX provides a mechanism for marking data, so that you can convey it, but the meaning of the markings is out of band. He things that this is option 1 and that this is the best way. IEP can be used outside of STIX, and therefore the rest of the questions about how to do it within STIX, should not be dealt with at STIX, but rather larger group outside of STIX.

Mark: Option 3: Modify markings could have a MAY understand and MUST understand. Option #1 seems like a MAY understand. A way for the producer to convey whether the consumer is required to understand the marking in order to be able to process. Concept lifted from SOAP.

Bret: Given the complexity of IEP, how do you process it in a tool? Everything would need to be bubbled up to a user, which would slow stuff down, or drop it on the floor. Worry that people will just drop all IEP marked data on the floor if they can’t process it. What do we need to do for interop? If you’re a producer, how do you know if the consumer CAN handle this? Out of band? Should they be able to auto-negotiate?

Rich: Organizations will have to sign legal agreements, and there are understandings on them. If the producer wants to levy requirements, they can do that in those documents. If consumers can’t comply, there will be a negotiation at that level. Just because a tool can’t interpret it, that doesn’t mean we shouldn’t support it.

Terry: With IEP v2, we made changes to allow references to remotely accessible policies you can reference. They’ll create the most common ones that anyone can use. Eventually the idea is to normalize on a small set of policies, and only when new policies come up would they need to bubble up to the user.

Mark: If you put it in as optional, it’s going to be a hard conversation with customers when it doesn’t get followed.

Terry: That’s already happening. It was dealt with at the trust group level.

Bret: Products may or may not know about it, and then the end user may not realize content is getting dropped on the floor.

Terry: It depends on restrictions in STIX about sending through unrecognized data, it should pass it, not drop it on the floor (if it’s not enforced)

John: Maybe different definition of drop it on the floor. Not display the IEP, or don’t display the data?

Rich: We should define what is correct behavior for data marked with some markings. We should not allow rewrite of data without original markings. Markings you find inconvenient, you can remove the data from the stream, but you can’t rewrite objects. It’s up to the trust circle to define those expectations.

Bret: The product might be able to consume and store it, but not parse it. IT doesn’t know what to do with it, no UI element, no actions, like it’s not there. Or it could be treated as custom property and your tool might not know how to parse it. So it may drop the custom properties, since they aren’t part of STIX, and the tool doesn’t have the ability to handle it.

Trey: There are plenty of external standards referenced, so just because it’s outside stix doesn’t mean it won’t be handled properly.

Bret: The others don’t have properties we have to parse, consume, store. The consumer may not know they’re missing stuff, and the producer may not know the consumer isn’t getting it.

Mark: Option #1 is basically we’re defining IEP as informational. Consumers are not required to do these things.

John: From STIX, that’s correct.

Mark: Still have questions about implementability. My concerns would be alleviated with must\_understand.

John: Would people actually use a may\_understand? If it’s must understand and they don’t, there should be defined behavior.

Sean: We all agree something like IEP is needed. TLP is inadequate. If we don’t deal with it, either everyone who wants to is going to create their own IEP in STIX, or the IEP group is going to publish STIX wrapper, or no one will use it. So, if we don’t do it, someone else will. All we would be defining in STIX is a wrapper. Option 1 makes more sense.

Chris: on may/must understand, it could already be addressed, with TLP = must, IEP = MAY. It would allow IEP to coexist with TLP without every system having to understand IEP.

Terry: we could do the MUST Markings at the TAXII channel level, that would have some sort of member criterion (legal agreement, etc).

Bret: I could get on board with option 1 with caveats. It says it’s informational and it’s crystal clear, clear conformance language, no interop requirements, add something to TAXII collections/channels that does auto negotiation/advertising.

John: I like the TAXII channel idea. It goes along well with #1, also solves #3, but instead of doing it in STIX, we do it in TAXII.

Mark: If you wanted to troubleshoot what happened and why, the taxi info would be long gone. It may be a safeguard. TAXII is about efficiency of interchange. Don’t feel this solves it.

Trey: Auto negotiation in TAXII seems to fly in the face of TAXII being decoupled from STIX. Does negotiation work with that?

John: IEP is also not limited to STIX.

Terry: Us keep TAXII so separate from STIX is restricting us.

Jeff: I’m a fan of putting this in TAXII. By the time you have it in STIX, it’s too late to control.

John: I’m hearing support for option 1/5.

Rich: 5 seems reasonable, though the enforcement will likely happen at the legal level

Sean: I’m less concerned if it gets rolled into TAXII. More concerned about it being in STIX.

Chris: I’d be comfortable with 1 with possibly option 5 later on.