How to Structure Analysis of Competing Hypotheses (ACH) – Introducing the Hypothesis Object and Moving Beyond the STIX 2.1 Opinion Object

Author: Caitlin Huey

Contents

***Abstract**: STIX 2.1 introduces the Opinion object to allow consumers and collaborators of intelligence to express agreement and disagreement on entities and relationships. The Opinion object is a STIX 2.1 entity that is closest to being able to provide a way to represent validation of an entity or a relationship between two entities. However, the Opinion object is limited in its application and flexibility. There is a need to move beyond the Opinion object and to introduce a new entity that would allow consumers/producers of intelligence to go beyond validating entities and to apply structure to evidence-driven hypotheses. This new entity's working name is the Hypothesis object.*

Introduction to ACH

Within the intelligence community, analyst tradecraft is referred to as a method or a portfolio of known structured techniques, methods, and skills that aid an analyst in doing their job. Tradecraft can also refer to the method of analysis applied to interpret and make sense of large amounts of data. Analysis of Competing Hypotheses (ACH) is commonly cited as a method to evaluate hypotheses against a set of evidence. Intelligence vendors, producers, and consumers use ACH to evaluate a threat based on available evidence.

During the course of an investigation, analysts may need to evaluate what is consistent and inconsistent across a set of hypotheses (H1, H2, H3....). ACH improves an analyst's ability to assess and validate an issue with a tested confidence assertion.

How ACH is Currently Applied

To see this applied, on May 18, 2018 a cybersecurity intelligence provider, Digital Shadows, modeled and published a report about multiple competing hypotheses surrounding the WannaCry ransomware incident that impacted enterprise networks and organizations across the globe. Hours after WannaCry occurred, many public and private companies within the intelligence community were attempting to identify attribution (actors/groups responsible) and the motivation behind the attacks that would hopefully lead to a greater understanding of how and why the attacks took place.

Digital Shadows outlined 4 possible hypotheses about potential attribution and tested them against a set of evidence that became available during and after the incident occurred[1]:

1. A sophisticated financially-motivated cybercriminal actor – H1
2. An unsophisticated financially-motivated cybercriminal actor – H2*
3. A nation state or state-affiliated actor conducting a disruptive operation – H3
4. A nation state or state-affiliated actor aiming to discredit the National Security Agency (NSA) – H4

Evidence in this case are data points that the community learned or observed about the incident:

1. Use of Eternal Blue Equation Group exploit
2. Targeted globally diverse victims
3. Installed DOUBLEPULSAR backdoor
4. Code similarities to North Korean malware
5. No evidence of phishing vector

[1] https://www.digitalshadows.com/blog-and-research/wannacry-an-analysis-of-competing-hypotheses/

*Digital Shadows found H2 to be the highest scoring hypothesis based on the available evidence.

6. Kill switch as anti-analysis feature
7. Only three Bitcoin wallets produced

Taking Digital Shadows' plausible scenarios about WannaCry attribution, there are limitations in STIX that makes it difficult to structure the process of conducting and structuring ACH. See image below:

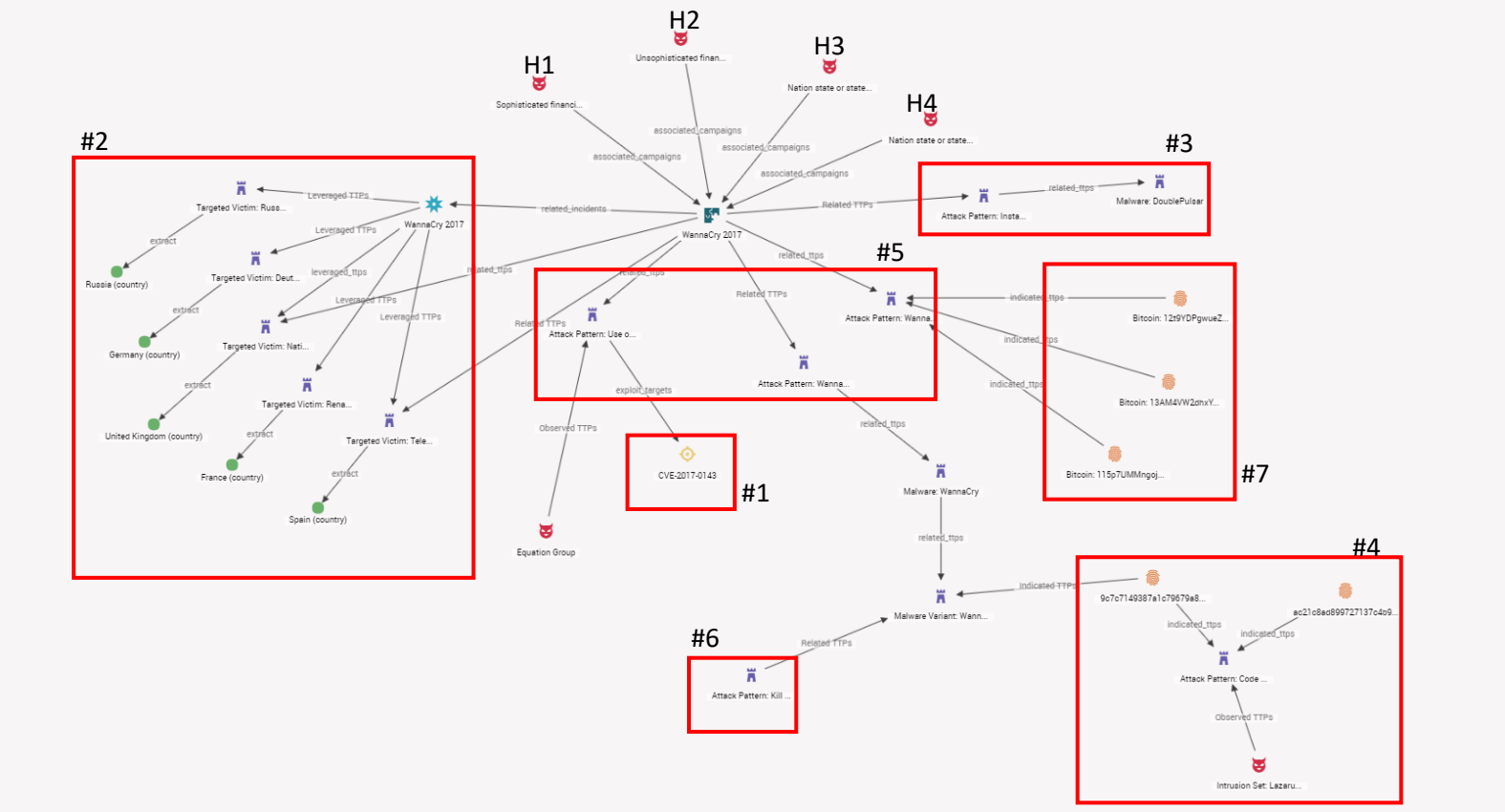

Image 1: Digital Shadows Hypothesis Testing mapped in STIX 1.X

In Image 1, one can see that there is no way in STIX for a producer/collaborator to structure and convey the results of having tested multiple hypotheses at once. In its current form, STIX allows us to see a confirmed reality (Threat Actors → Campaign; Indicators → TTPs; Incident → Targeted Victims). There is no entity that will allow us to represent an alternative view that would let us see competing hypotheses in a structured way.

At the time of Digital Shadows' analysis, they identified that H2 – an unsophisticated financially-motivated cybercriminal actor—was the strongest scoring hypothesis from the evidence that was available. After completing the process of using evidence to test a set of hypotheses, there are limits in being able to structure which hypothesis received the strongest scoring.

The Problem

There is no way to currently structure the process of testing evidence against a set of hypotheses (H1, H2, H3…). Producers of intelligence often create multiple competing-hypotheses around a given threat in order to identify the strongest hypothesis (H1) that is most supported by the evidence available. There is no way to ingest that Digital Shadows information in STIX that would allow the consumer to see all the hypotheses being tested and to see the evidence used to support each hypothesis.

The following are some limitations with STIX in being able to structure the process of conducting ACH:

- Cannot structure information from vendors who are testing competing hypotheses
- Cannot identify which hypothesis was determined to score the strongest from the set of hypotheses being tested
- Cannot separate an alternate/proposed reality from a confirmed reality

There is no ability to see whether a producer/vendor of intelligence has a higher confidence in one hypothesis (H1) over a tested set of other hypotheses (H2, H3, H4). There is a need to have an entity that would be able to structure the results of this hypothesis-testing process to see why one hypothesis was more supported/scored higher.

The need to structure this hypothesis-testing process is driven by several factors:

- To identify patterns in authors' assessments over time. (i.e. show me what the world looks like when US CERT hypotheses are true)
- To identify evidence that is consistently being used to support multiple hypotheses over time (i.e. exploiting CVE-X-X as an initial attack vector is used as evidence to support more than one hypothesis)
- To identify patterns or trends when doing threat actor attribution (i.e. show me all hypotheses that support attribution of a Russian Advanced Persistent Threat, "APT")
- To measure predictability or sophistication of a threat actor. (i.e. >80% of our hypotheses on this threat actor were correct; or <5% were correct, so clearly this threat actor changes tactics and is unpredictable)

What the Opinion Object Permits

It is clear that the STIX 2.1 Opinion object cannot be used to structure hypotheses, and that there is a need for a new object that will be able to do this. The Opinion object allows the following:

- An analyst from an organization consuming intelligence should be able to say that they "Strongly Disagree" or "Strongly Agree" with a Campaign object from a vendor, and to provide an explanation as to why
- In a more applied setting, a SOC analyst might relate an Opinion object to an Indicator with a rating of "Strongly Disagree" because it is considered to be a false positive within their environment

The current specification introduces a free-text explanation for the reason why the consumer/producer has this opinion. The object also provides properties to identify who is the `author` of this opinion, whether that be an OSINT source or a commercial, closed-source.[2]

[2] https://docs.google.com/document/d/1bkMmU1PxlwlAwjrMmyWV147rvLcRs2x62FicHbpH2gU/edit#

Table 1: STIX 2.1 Opinion Object Properties

Common Properties		
type, **spec_version**, **id**, **created_by_ref**, **created**, **modified**, **revoked**, **labels**, **confidence**, **lang**, **external_references**, **object_marking_refs**, **granular_markings**		
Opinion Specific Properties		
description, **authors**, **object_refs**, **opinion**		
Property Name	**Type**	**Description**
type (required)	`string`	The value of this property **MUST** be `opinion`
explanation (optional)	`string`	An explanation of why the producer has this Opinion. For example, if an Opinion of strongly-disagree is given, the explanation can contain an explanation of why the Opinion producer disagrees and what evidence they have for their disagreement.
authors (optional)	`list` of type `string`	The name of the author(s) of this Opinion (e.g., the analyst(s) that created it).
object_refs (required)	`list` of type `identifier`	The STIX Objects (SDOs and SROs) that the Opinion is being applied to.
opinion (required)	`enum`	The opinion that the producer has about all of the STIX Object(s) listed in the **object_refs** property. The values of this property **MUST** come from the `opinion-enum` enumeration.

Limitations of the Opinion Object

ACH does have a place in CTI (cyber threat intelligence) and is practiced by vendors and producers to help come to a more-informed conclusion about attribution, motivation of attacks, and emerging incidents on the threat landscape.

The 2.1 Opinion object is the entity that gets the closest to being something that can be used to structure hypothesis testing. The Opinion object is able to express “agreements” or “disagreements” about other STIX entities or relationships. However, it is clear that it is not meant to be expanded beyond its current form based on the below limitations.

Problem areas with this current 2.1 Opinion object:

- The current specification does not address how the community should use and apply the Opinion object. STIX is very flexible, analysts from the same team may end up modelling the same dataset or intrusion set differently
- One of the largest caveats of the Opinion object is that sharing communities are still encouraged to provide clear guidelines to their constituents regarding best practice for the use of Opinion

objects. What this means is that there is still no fundamental agreement on when and how to best use this object
- The Opinion object does not apply any additional structure beyond the free-text `explanation` as to why an author has an opinion in the first place
- There is no way to consistently track or see patterns in `explanations` for Opinions over time

Argument For a New Entity

The Opinion object focuses on validating intelligence from various sources, but only in a free-text, non-evidence-based fashion. Being able to have an entity with the sole purpose of relaying an author's thoughts and opinions about an entity or a relationship in a free-text fashion is useful. There is also a need to make that a minimum.

In addition to validating a source or commercial data, there appears to be a need to be able to structure evidence in support of a hypothesis, and to be able to structure this process of conducting ACH. Producers and consumers of CTI practice hypothesis-testing to seek attribution of a threat actor or to better understand an emerging threat. At the moment, STIX has no way to structure this thought process or the evidence that supports one hypothesis over other hypotheses. Details on what makes a new entity a more viable one for representing ACH will be discussed below.

Making Room for ACH in a New Object: The Hypothesis Object

When thinking on how to best represent ACH within an entity, we need to know what this entity would have to look like in order to be able to conduct ACH. ACH uses a variety of measures to assess how strong a given hypothesis is by using Reliability and Credibility as a way to score each hypothesis against all evidence available[3].

Some assumptions we are making:
- A Hypothesis object must consist of evidence
- A Hypothesis object must consist of a way to score Reliability of evidence
- A Hypothesis object must consist of a way to score Credibility of evidence
- A Hypothesis object can represent the process and the end-result of hypothesis testing
- Evidence within a Hypothesis object can consist of STIX entities
- Evidence within a Hypothesis object does not need to consist of only STIX entities
- The Hypothesis object 'title' can be the result of the author's strongest hypothesis that they are testing
- A Hypothesis object contains a property of `evidence type` as a way to classify what types of evidence are being used to support certain hypotheses
- A Hypothesis object has an `author`

Some things we still don't know:
- Is a Hypothesis object a standalone object?
- How will one Hypothesis object relate to the original testing group in which it was tested in?
- Is 'evidence type' a string or will it be enumerated?

[3] http://www.pherson.org/PDFFiles/ACHTutorialRevised11Mar07.pdf

- How do we expect the Hypothesis object to fit into a data model?

The Hypothesis Object: Properties

A Hypothesis object would be a way to structure the process of hypothesis-testing. To create a new object that would allow us to structure the process of having completed ACH, we need to identify properties we need this object to have.

From the assumptions that were outlined above, we can start to create properties we would like this object to contain:

Common Properties		
`type`, **`spec_version`**, **`id`**, **`created_by_ref`**, **`created`**, **`modified`**, **`revoked`**, **`labels`**, **`confidence`**, **`lang`**, **`external_references`**, **`object_marking_refs`**, **`granular_markings`**		
Hypothesis Specific Properties		
`Hypothesis_description, authors, relevancy, credibility, evidence, evidence_type`		
Property Name	**Type**	**Description**
`type` (required)	`string`	The value of this property **MUST** be `hypothesis`
`explanation` (optional)	`string`	An explanation of why the producer came to this Hypothesis. For example, if a Hypothesis was tested against several others, an explanation can contain why the Hypothesis producer supports this Hypothesis over the other hypotheses tested.
`authors` (optional)	`list` of type `string`	The name of the author(s) of this Hypothesis
`relevancy` (required)	`enum`	Relevance of the evidence to the question being analyzed, not to each individual hypothesis.
`credibility` (required)	`enum`	Credibility of the evidence provided.
`hypothesis_description`	`string`	A description of the hypothesis that is being tested.
`evidence` (required)	`string`	Evidence that is being used to test a Hypotheis.
`evidence_type` (optional)	`string`	Type of evidence (e.g. Secondary Source)
`object_refs` (required)	`list` of type `identifier`	The STIX Objects (SDOs and SROs) that the Hypothesis is being applied to.

Table 2: Proposed properties for a Hypothesis object (rough draft)

The list of above properties is only a start, as there are several assumptions we still need to work through before we identify the ideal properties to make this object work.

Opinion Object v. Hypothesis Object

One of the reasons that the Opinion object is not the best object to structure hypothesis testing is because an Opinion needs to provide a consumer/collaborator a way to interact with entities without needing any evidence. An Opinion is an expression of a varying degree of "Agree" or "Disagree" on a relationship or on an entity. It allows consumers/producers to apply a feeling about an entity without needing to supply any evidence supporting it.

Here are more applicable examples that demonstrate the need to have separate Opinion and Hypothesis objects:

1. A SOC analyst using a "Strongly Disagree" Opinion object to flag and identify false-positives within their environment
2. Opinion objects used to evaluate sources over time (i.e. how many "Strongly Disagree" Opinions has my analyst team created that relate to entities/relationships from Producer X)
3. A downstream intelligence consumer in the e-commerce sector relates a "Strongly Agree" Opinion to the relationship between Magecart Threat Actor → British Airways Campaign as a way to signal and identify Threat Actors and attribution that are important to them
4. Use Opinion objects as a way to expand an organization's threat hunting around the diamond model (i.e. to identify all the "Strong Disagree" Opinions related to Threat Actors as a way to identify what additional intelligence around attribution may be needed

Opinion objects provide a flexible way of validating intelligence as it fits within a consumer's environment. Hypothesis objects provide a way to collect what we know about the larger threat landscape and to propose and test multiple hypotheses around a given threat.

Next Steps: Proposed Hypothesis Object Specification and Properties

This section takes what we know from the sections talked about above. The core problem is that there is a current inability in STIX to structure the process of conducting ACH. The Opinion object came close, but is limited in functionality. There is a need for a new object that will allow producers/consumers/and collaborators of CTI to structure the process of doing ACH and hypothesis-testing with STIX.

We have outlined problem areas and some proposed solutions. There are still some next steps the author can focus on:

- Identify a working prototype from the assumptions we have made about what the Hypothesis object should look like
- Refine the properties and intended data model for the Hypothesis object
- Provide a specification for this new object
- Represent this in a proposed data model (using the original Digital Shadows use case)