Practical Cyber Security for Cyber Security Practitioners

Prof. Sandeep Kumar Shukla

Department of Computer Science and Engineering

Indian Institute of Technology, Kanpur

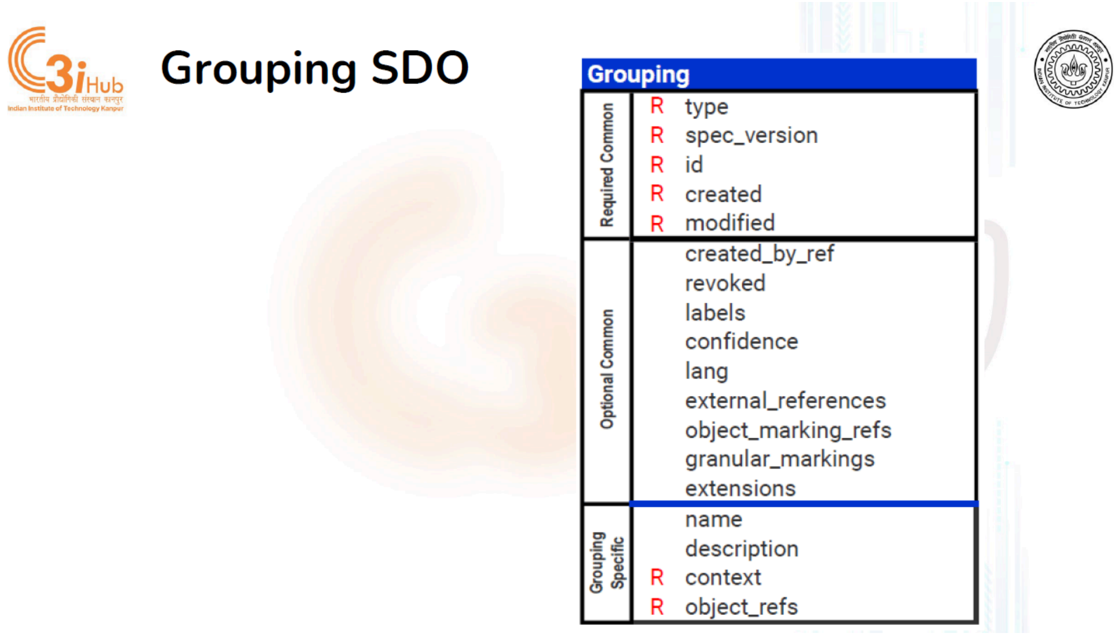
Lecture 27

So I am going to start. So the reason why we are doing this extra class is because we have this Eid on Thursday which is a holiday. Also tomorrow I have a meeting So, I cannot be in the class. So, I thought I would finish this structured threat intelligence exchange format and then we can squeeze in another topic in the next week, which is about the SCAP. which is another standard for another standard for you know automation of security tools right. So, that would be an additional thing that we can do next week if I can finish it today.

On Friday we will have class. So, we will probably start Scap on. or maybe we can we may have to finish this on Friday I am not sure it depending on how long we want to stay here today I think one and half hours would be good enough. so we were talking about this structured threat intelligence sharing format or data model and we discussed that there are three kinds of there is actually six kinds of entities in this data model Of course, the most extensive one is this STIX domain objects or SDOs and then you have STIX cyber observables or SCOs.

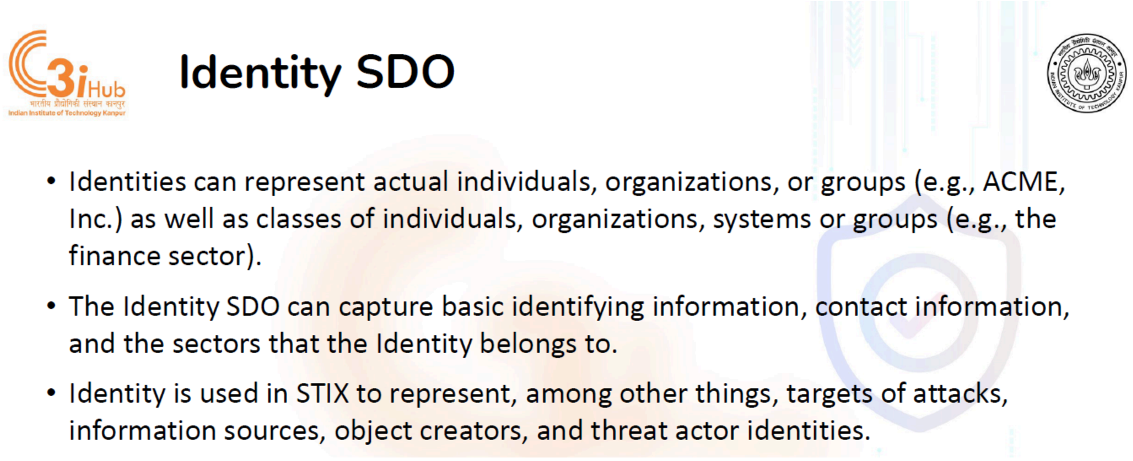
Relationship objects, SROs and then extension definition object and meta objects and the bundle and there is a patterning language which is used mostly inside these. So, that is the different types of entities in the data model. And we saw an example on the sticks viewer which is a tool that you can also use if you have a sticks file and you can find many sticks files online. So, basically you have this SDOs and SCOs which are nodes in this data model and then there are relationships objects which are edges in the graphical representation of the data model, but the graphical representation is just for you know taking a look at you know various parts of these things various components, but actually it is supposed to be parsed automatically by your security tools. So, that you can actually have threat intelligence automatically coming to you through taxi protocol and then automatically ingested by firewall and other tools and certain actions are taken some intelligence can be used for getting more information on your security visualization like seam tools and so on.

And then we talked about some SDOs. So, attack pattern SDO we talked about, we talked about campaign SDO, we talked about course of action SDO, which is actually is a kind of a stub, a place holder. Then we talked about grouping SDO for grouping certain threat intelligence objects, identity SDO for giving names or some kind of identity to entities and organizations, individuals, etcetera. And then we have incident STO which is again a stub which basically you know is part of a threat report it is a that an incident has happened and various parts of this thing. and then we came to indicator SDO when we stopped discussing.



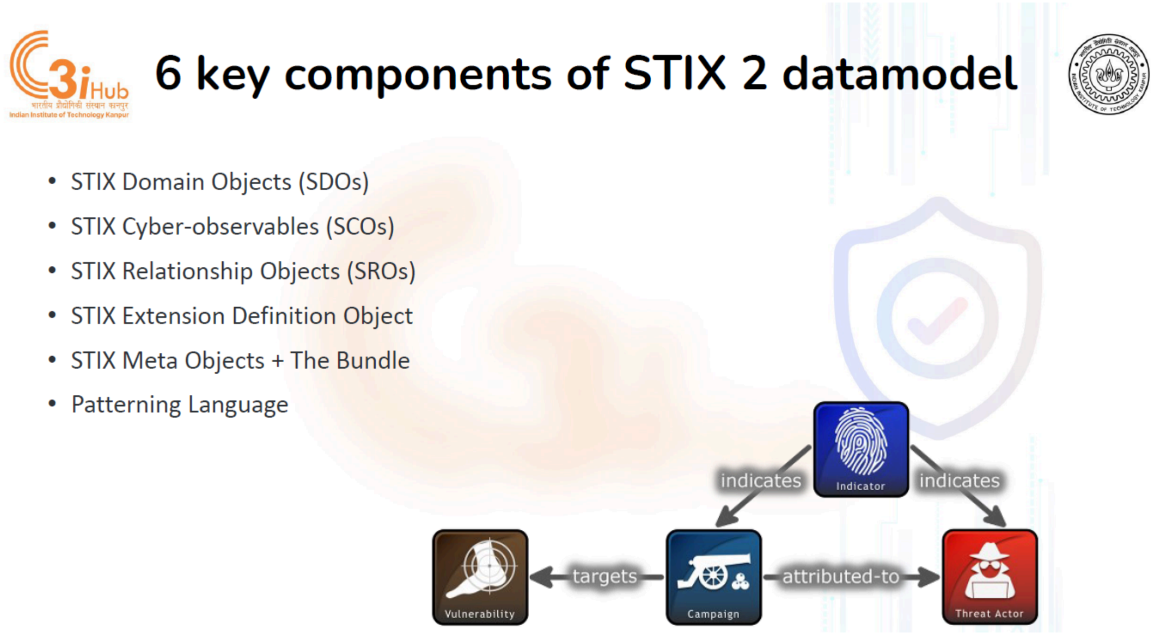
Grouping SDO

Grouping		
Required Common	R	type
	R	spec_version
	R	id
	R	created
	R	modified
Optional Common		created_by_ref
		revoked
		labels
		confidence
		lang
		external_references
		object_marking_refs
		granular_markings
		extensions
Grouping Specific		name
		description
	R	context
	R	object_refs



Identity SDO

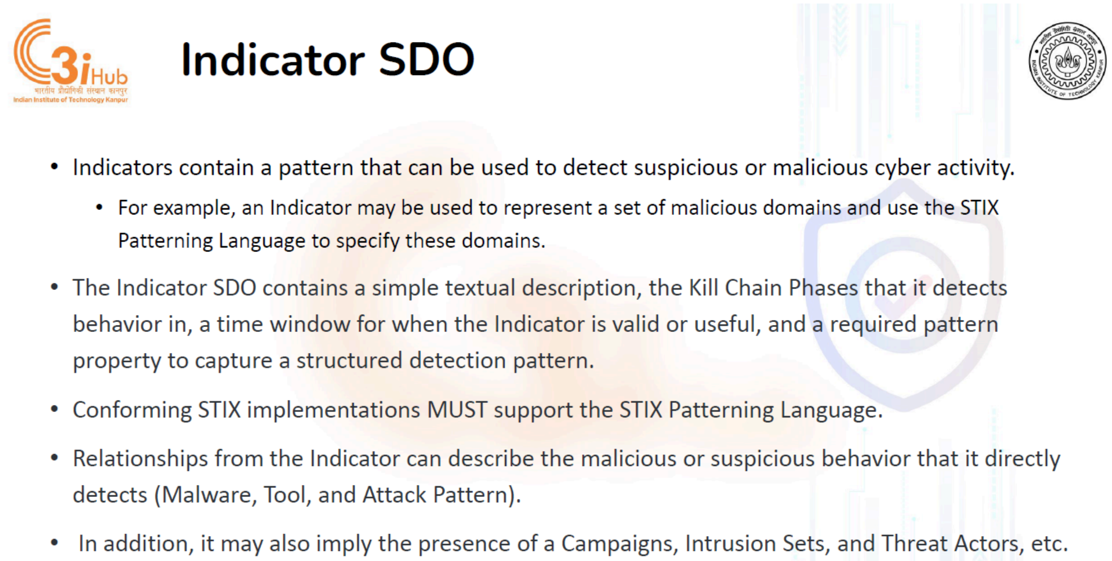
- Identities can represent actual individuals, organizations, or groups (e.g., ACME, Inc.) as well as classes of individuals, organizations, systems or groups (e.g., the finance sector).
- The Identity SDO can capture basic identifying information, contact information, and the sectors that the Identity belongs to.
- Identity is used in STIX to represent, among other things, targets of attacks, information sources, object creators, and threat actor identities.



6 key components of STIX 2 datamodel

- STIX Domain Objects (SDOs)
- STIX Cyber-observables (SCOs)
- STIX Relationship Objects (SROs)
- STIX Extension Definition Object
- STIX Meta Objects + The Bundle
- Patterning Language

Indicator
indicates
indicates
Vulnerability
targets
Campaign
attributed-to
Threat Actor



Indicator SDO

- Indicators contain a pattern that can be used to detect suspicious or malicious cyber activity.
  - For example, an Indicator may be used to represent a set of malicious domains and use the STIX Patterning Language to specify these domains.
- The Indicator SDO contains a simple textual description, the Kill Chain Phases that it detects behavior in, a time window for when the Indicator is valid or useful, and a required pattern property to capture a structured detection pattern.
- Conforming STIX implementations MUST support the STIX Patterning Language.
- Relationships from the Indicator can describe the malicious or suspicious behavior that it directly detects (Malware, Tool, and Attack Pattern).
- In addition, it may also imply the presence of a Campaigns, Intrusion Sets, and Threat Actors, etc.

So, indicator SDO is basically, so any kind of attack will leave some signature on your system right. So, and they will leave a you know file in your file system, they will probably an imprint of their the incident. It could be some IP address that they communicated on your network or URL they communicated to on your network. They could actually change some settings. So all those things we call indicators of compromise.

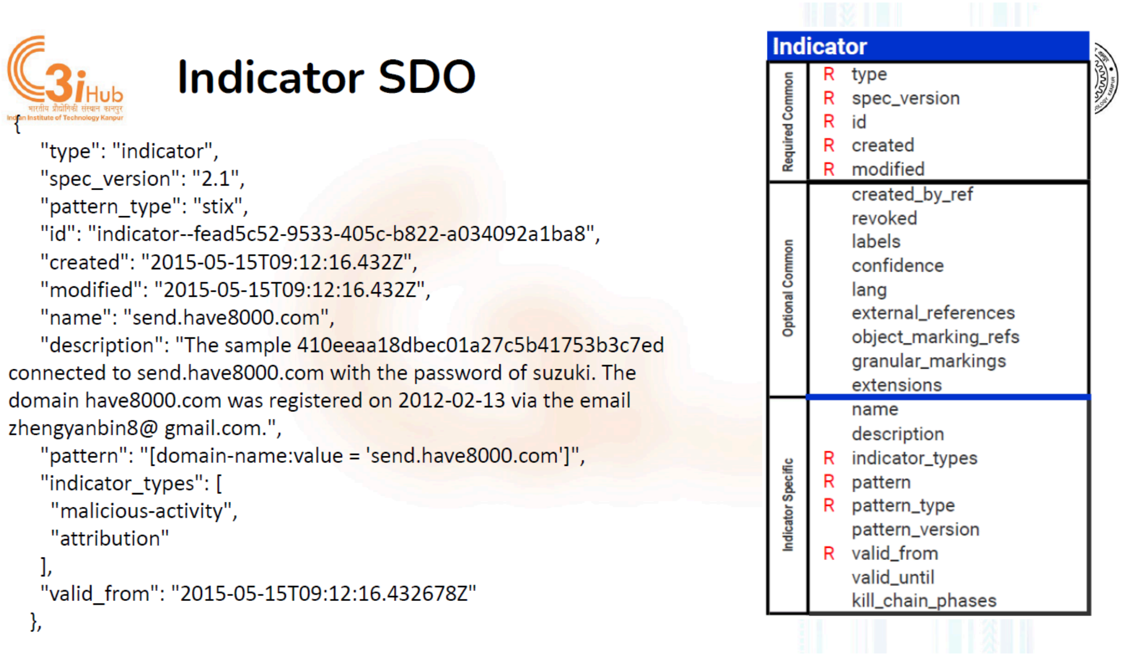
So indicators are IOCs. So IOCs are very important part of threat intelligence right because if I want to caution you that my organization got attacked by so and so threat actor with so and so malware. and I want to caution you to say that you might be the next target so what you should be looking for. So, you should be looking for a binary files which has a particular hash for example or you might be looking for traffic that goes in goes to a particular IP address or particular URL or you might be looking for some changes in the certain change in the windows registry or you might see a change in the some particular directory this kind of stuff. So, these are indicators that you want to tell the other party that these are the things you should look for so you should have the entrapment or ability to actually look for these things right if you are not looking for anything then you won't see anything right so the visibility of your endpoints visibility of your network traffic is very important, without that visibility, without checking what is going on in your DNS, what is going on in your regular traffic, routing traffic, what is going on in your new files that are coming in, new certificates that are coming in into your system, if you do not observing them, then you are not going to get the benefit of indicators of compromise.

But assuming that you have all that you know observability, then you want to see what you should try to observe. You cannot keep observing everything right. So, everything is huge amount humongous amount of data that you have to observe. So, you have to know the threat intelligence to know what to observe and that is what the indicators give you. So, indicators are the one of the most important part of any threat intelligence.

So, sometimes this indicators are also you can say which kill chain phase this indicator belongs to like is it something that you would see during command and control or are you going to see this during the initial access or whatever the indicator whatever kill chain phase, you might be in to see that indicator and seeing that indicator you would also know how far the threat actor has progressed in your system if you see command and control traffic you know already that you have been compromised with the malware right and that means initial access and then you know persistence all those things have been achieved by the threat actors so your he's deep into your system so that's the situation that you want to be knowing and then you see the how the indicator is expressed. So, they have a patterning language. So, remember like when we say that there are 6 components of stix the 6 component was a patterning language. So, this patterning language is we will see we do not have to necessarily learn the patterning language in this class, but there is a patterning language. however there are many tools for creating threat intelligence for editing threat intelligence or for creating new threat intelligence right so you can actually get some tools in which you can act they will help you with this patterning language and also you do not necessarily have to know the patterning language as good as you know they say regular expression and so on so an indicator also implies maybe it may imply that you have a malware infection or it may say that maybe some tool is being used against you or you might see an attack you might see that an attack pattern or you might see a campaign intrusion certain threat actor so more you know so an indicator for example at some point initially when you see the indicator and you are the first one to seeing that indicator.

So nobody has told you through threat intelligence that this means this URL if you see this URL it means that you are infected by Emotet right botnet right let us say the first time. So then you have to actually discover what else is going on in your system and so on and then you create the threat intelligence. So in the beginning you say I am seeing a bot So, you will associate this indicator, this particular URL or IP address with let us say a bot. Then later on somebody would say so this state intelligence is shared widely. Then another organization that says I found some more information about this particular bot and this bot is actually from Russian group APT28 let us say.

I am just giving an example hypothetical so you say so this is APT 28 so you will then additional add additional information into the indicator saying that it is associated with threat actor APT 28. And then you can say so somebody says this is part of a particular campaign so this is spaced in time specific you know like Ukraine war related campaign right. So you might say okay so this is related to a particular campaign. So you can add additional information to this indicator. So the indicator threat intelligence gets enriched over time right it does not necessarily stay the static yeah.



Indicator SDO

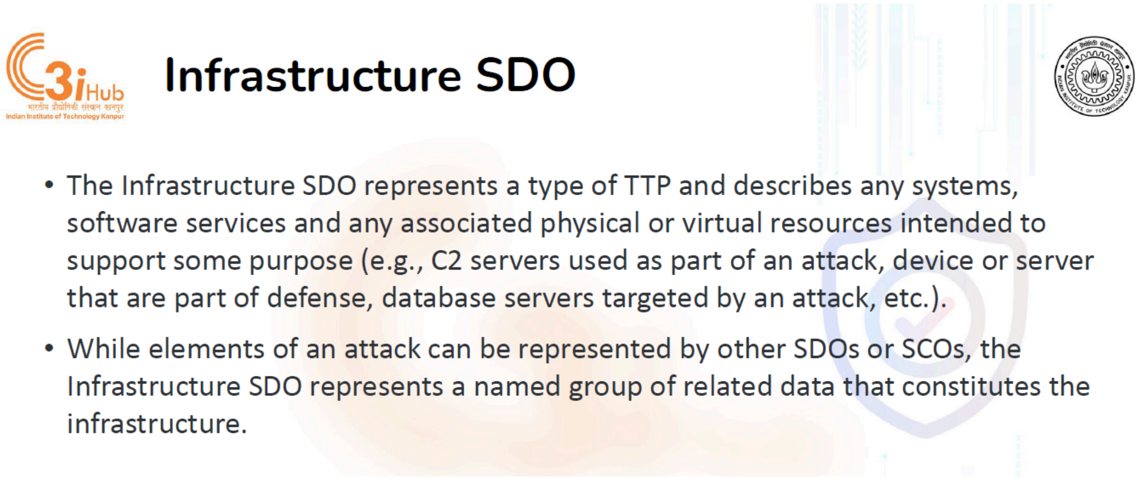
```
{
    "type": "indicator",
    "spec_version": "2.1",
    "pattern_type": "stix",
    "id": "indicator--fead5c52-9533-405c-b822-a034092a1ba8",
    "created": "2015-05-15T09:12:16.432Z",
    "modified": "2015-05-15T09:12:16.432Z",
    "name": "send.have8000.com",
    "description": "The sample 410eeaa18dbec01a27c5b41753b3c7ed
connected to send.have8000.com with the password of suzuki. The
domain have8000.com was registered on 2012-02-13 via the email
zhengyanbin8@ gmail.com.",
    "pattern": "[domain-name:value = 'send.have8000.com']",
    "indicator_types": [
     "malicious-activity",
     "attribution"
    ],
    "valid_from": "2015-05-15T09:12:16.432678Z"
  },
```

Indicator		
Required Common	R	type
	R	spec_version
	R	id
	R	created
	R	modified
Optional Common		created_by_ref
		revoked
		labels
		confidence
		lang
		external_references
		object_marking_refs
		granular_markings
		extensions
Indicator Specific		name
		description
	R	indicator_types
	R	pattern
	R	pattern_type
		pattern_version
	R	valid_from
		valid_until
		kill_chain_phases

So, I will show you example right. So, this is a pattern. So, this is if you go and look up stix pattern you will see that. So, this is the pattern in which this has to be expressed right. So, what it says is that if you are doing a pattern based search then you have to use this format.

So, that is what this is. So, we will see that there are certain you know this language is very specific to stix. no so the pattern language is part of part of the stix specification so stick specification said that this is the syntax of the pattern language this is how you write a pattern to express indicator or names right so this is what then anytime you want to say okay so this is you could see this pattern is very specific this this is a full-fledged URL right you could have had a star dot have 8000.com also so that would be more like that would mean that the this intelligence would have said that this domain every time you see it is a problem right here we are saying that this domain this particular you know domain suffix is not a problem it is just the this particular specific URL is a problem so this pattern will tell you that kind of information. and then you know when you get threat intelligence you will get you know a file or a bunch of files each in this format right then you have to do a JSON based parsing and then how you process that information is up to you.

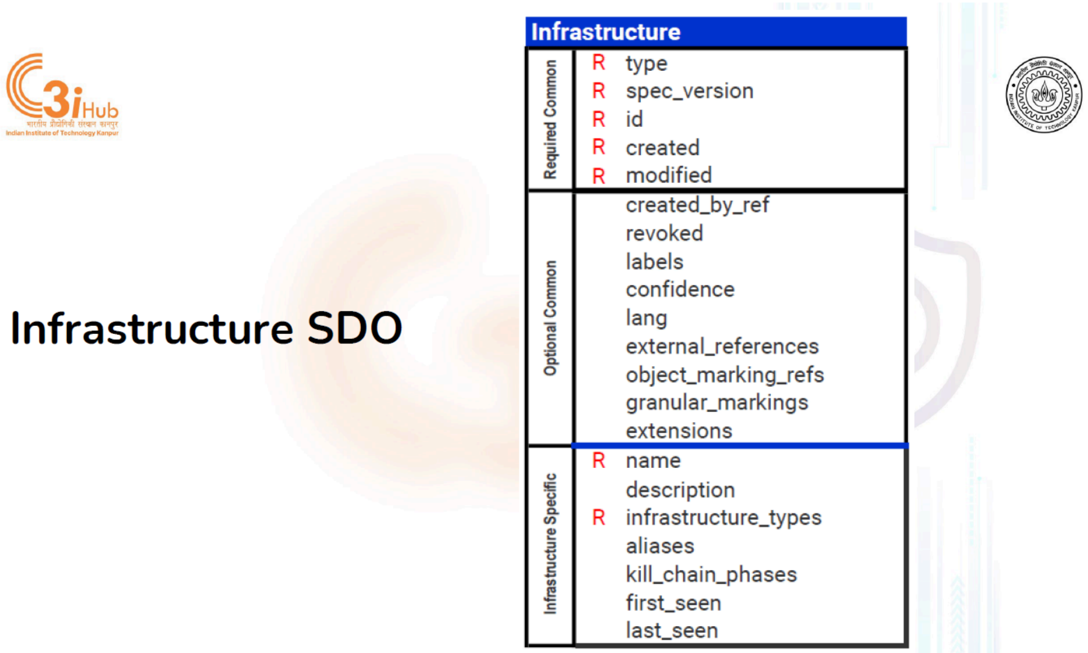
So, today's many tools will has the ability to parse it. So, when you get this you actually connect the taxi feed into those tools and the tools automatically download the latest stix files and then process them and do certain things you can, but what they do is based on what has been programmed into them. So, you might add additional programming, if there are hooks to do that, to do more intelligent stuff with it. So, this is the indicator SDO, you can see that you know it is type and this is stix 2.1 version, this is a stix patterning language used here.



Infrastructure SDO

- The Infrastructure SDO represents a type of TTP and describes any systems, software services and any associated physical or virtual resources intended to support some purpose (e.g., C2 servers used as part of an attack, device or server that are part of defense, database servers targeted by an attack, etc.).
- While elements of an attack can be represented by other SDOs or SCOs, the Infrastructure SDO represents a named group of related data that constitutes the infrastructure.

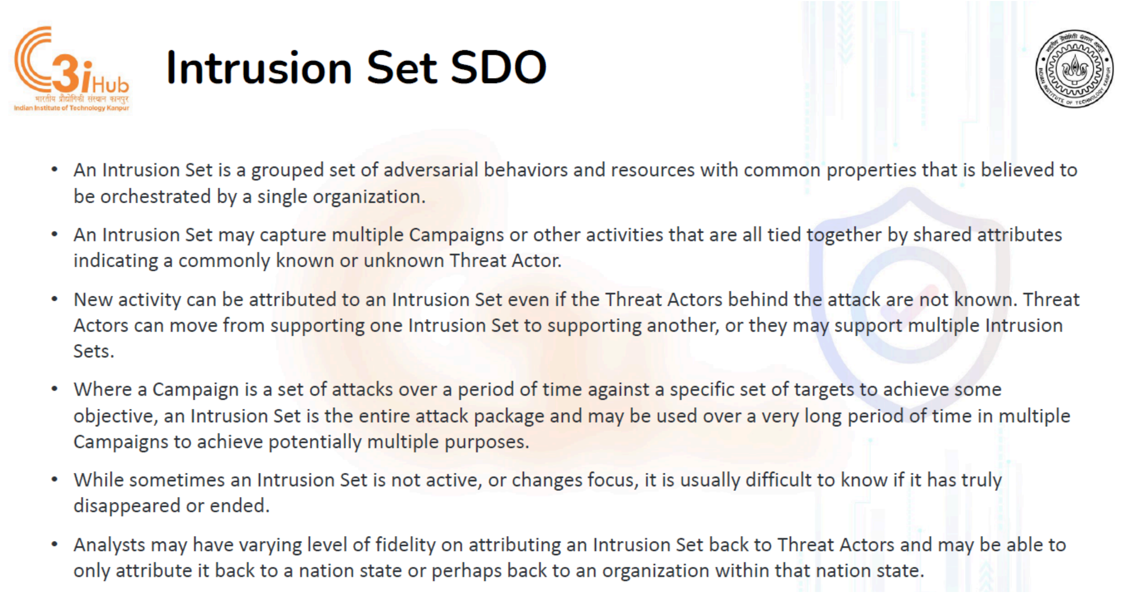
So, pattern type and pattern are usually close by, but in JSON it does not matter, this is a key value pairing, JSON language is basically key value pairing. So, the order does not matter, this is the ID which is very important it has to be unique created and modified date name they gave a name same as this thing it does not have to be the same there is a textual description and then there is indicator type and then when it is valid from. So, not every information that is required that is possible has to be there right so but there are certain the ones marked with R must be there the others are optional so more enriched your threat intelligence is better more information you will get. so then you there could be an infrastructure information you can get like for example when you know that a threat actor uses a particular c2c the command and control infrastructure right so if you know more information about that infrastructure you can actually put that in an infrastructure objects right and it may not be necessarily a c2c server It can be some device which is part of you know their infrastructure database or maybe some also what is the what targets what are being targeted that could be also part of an infrastructure. So, infrastructure you know SDO is has all this name infrastructure type description kill chain phases in which this infrastructure is used and so on.



Infrastructure SDO

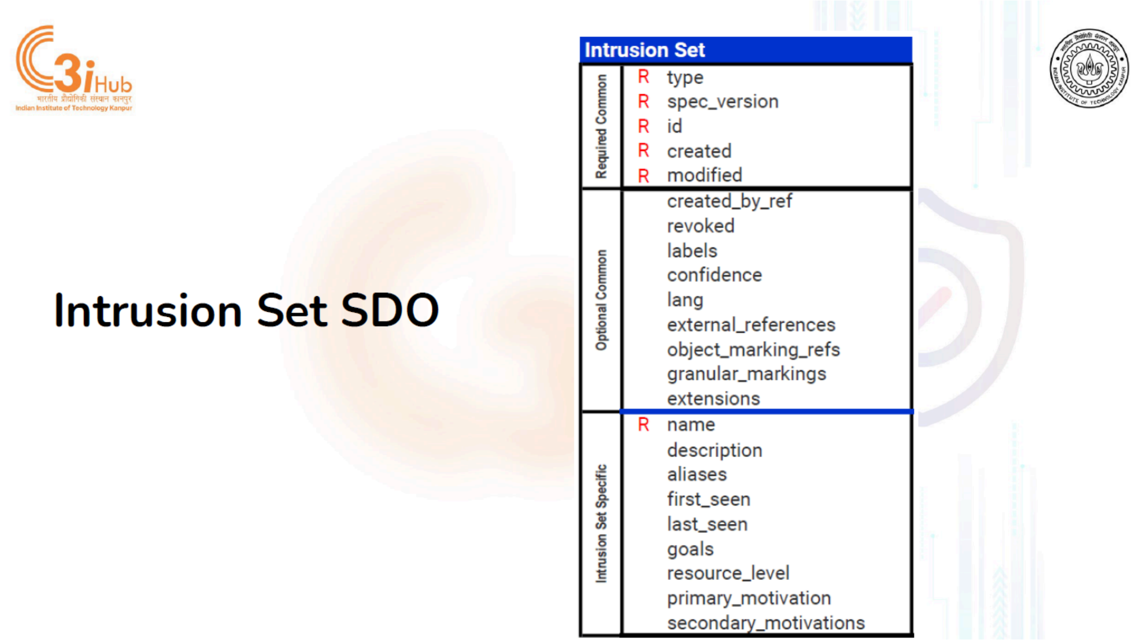
Infrastructure		
Required Common	R	type
	R	spec_version
	R	id
	R	created
	R	modified
Optional Common		created_by_ref
		revoked
		labels
		confidence
		lang
		external_references
		object_marking_refs
		granular_markings
		extensions
Infrastructure Specific	R	name
		description
	R	infrastructure_types
		aliases
		kill_chain_phases
		first_seen
		last_seen

So, that kind of information could be there. so we already said that intrusion set right so remember that we said we the first very first is do we looked at was actually the attack pattern right so attack pattern actually may become may be part of a campaign then we looked at a campaign and a campaign may be part of intrusion set right so an intrusion set may capture multiple campaigns or other activities that are tied together by a shared attribute usually that sharing is basically that they they belong to the same threat actor right so intrusion set so intrusion set is more long-living so an attack pattern is usually a pattern that is used in multiple different campaigns right so many campaigns use the same attack pattern and an intuition set may be many campaigns right so many campaigns together will form an intuition set so intuition set is do also has all this information it may have aliases first seen last seen You may also make some comment about its goals, what kind of resource level, are they very highly resourced or not so resourced, primary motivation, secondary motivation. Now, good thing about JSON is all of this information is textual. So, it is a string. Basically, every key is filled with a string.



Intrusion Set SDO

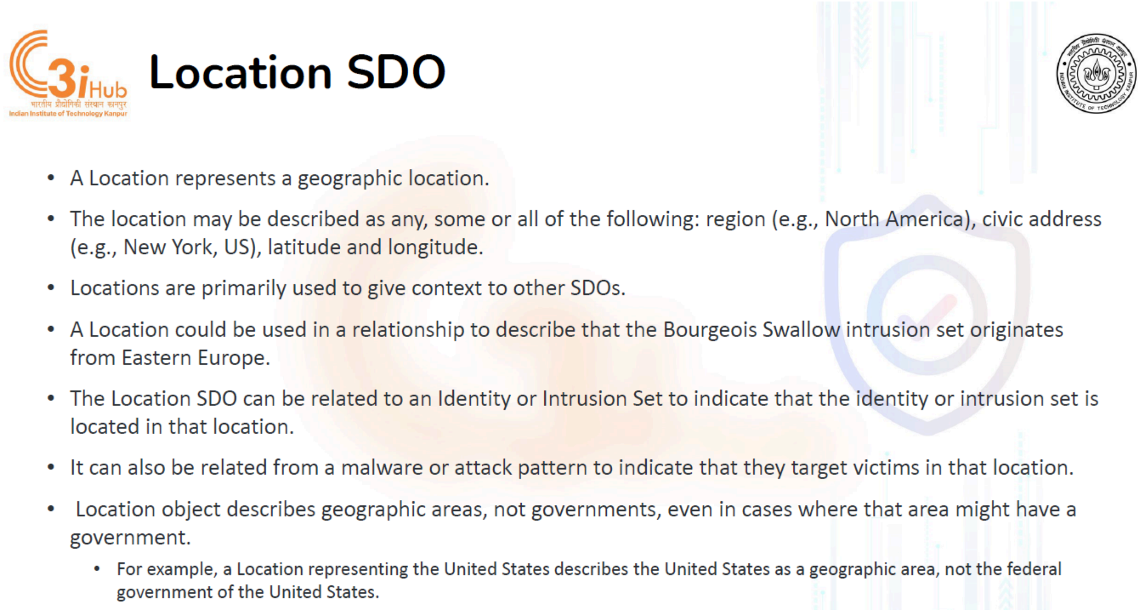
- An Intrusion Set is a grouped set of adversarial behaviors and resources with common properties that is believed to be orchestrated by a single organization.
- An Intrusion Set may capture multiple Campaigns or other activities that are all tied together by shared attributes indicating a commonly known or unknown Threat Actor.
- New activity can be attributed to an Intrusion Set even if the Threat Actors behind the attack are not known. Threat Actors can move from supporting one Intrusion Set to supporting another, or they may support multiple Intrusion Sets.
- Where a Campaign is a set of attacks over a period of time against a specific set of targets to achieve some objective, an Intrusion Set is the entire attack package and may be used over a very long period of time in multiple Campaigns to achieve potentially multiple purposes.
- While sometimes an Intrusion Set is not active, or changes focus, it is usually difficult to know if it has truly disappeared or ended.
- Analysts may have varying level of fidelity on attributing an Intrusion Set back to Threat Actors and may be able to only attribute it back to a nation state or perhaps back to an organization within that nation state.



Intrusion Set SDO

Intrusion Set		
Required Common	R	type
	R	spec_version
	R	id
	R	created
	R	modified
Optional Common		created_by_ref
		revoked
		labels
		confidence
		lang
		external_references
		object_marking_refs
		granular_markings
		extensions
Intrusion Set Specific	R	name
		description
		aliases
		first_seen
		last_seen
		goals
		resource_level
		primary_motivation
		secondary_motivations

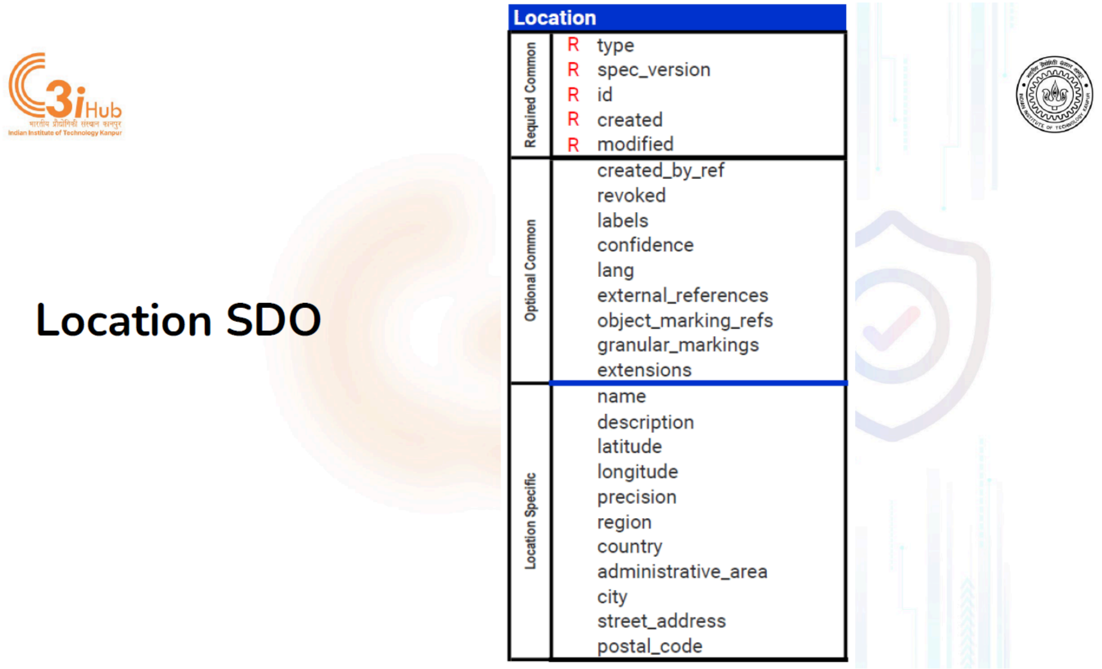
So, you can do many things with the string. One thing you can do is just display the string on your tools like on your SIM or SOC, etcetera. But the other thing you can do is use NLP natural language processing to get more information out of these to actually get more out of this information only bad thing about only problem downside of that is that these are not required fields. So, if you have written if you have created a natural language processing based processing of feeds and this most of your stix files that you are getting, They are not filling this kind of fields. then you are not going to get much out of them right so you might get very little information so you have to see how enriched is your stix provider is like your stix provider if you are paying them money they will give you a much more enriched stix than if you are getting it for free from site or other organizations right so so they will give you the minimum Location SDO is again something that represents a geographic location.



Location SDO

- A Location represents a geographic location.
- The location may be described as any, some or all of the following: region (e.g., North America), civic address (e.g., New York, US), latitude and longitude.
- Locations are primarily used to give context to other SDOs.
- A Location could be used in a relationship to describe that the Bourgeois Swallow intrusion set originates from Eastern Europe.
- The Location SDO can be related to an Identity or Intrusion Set to indicate that the identity or intrusion set is located in that location.
- It can also be related from a malware or attack pattern to indicate that they target victims in that location.
- Location object describes geographic areas, not governments, even in cases where that area might have a government.
    - For example, a Location representing the United States describes the United States as a geographic area, not the federal government of the United States.

So, why do I need that information? Sometimes that is important as to where this threat actor might be working from like we usually get that kind of threat intelligence by analyzing the time of the day they attack,for example if they are attacking at the time which seems to coincide with the work time of say Russia or China or something we kind of get some idea that is does not mean that it is a full proof way of understanding where the location is, but there are may be other things like for example, there may be strings of Russian language inside their malware or there could be some previous malware that we have determined to be belonging to some particular Russian group or Chinese group the fragments of code are common all these things are not necessarily a full-fledged proof of the fact that they belong to a particular location but you could indicate that so you could actually say. See here you see that the confidence. So you can actually indicate the confidence with which this threat intelligence is being shared. So if you are a threat intelligence analyst and you are very focused on Chinese threat groups and you say that this is Chinese, this is from Shanghai for example. and you put your confidence to be high or very high or something then the consumer of this straight intelligence will take it more seriously you can also have longitude latitude information now why do I need this because sometimes I can use this threat information to be displayed on a geographical map right so this kind of information helps there so these are all about you know how you make use of the threat intelligence.

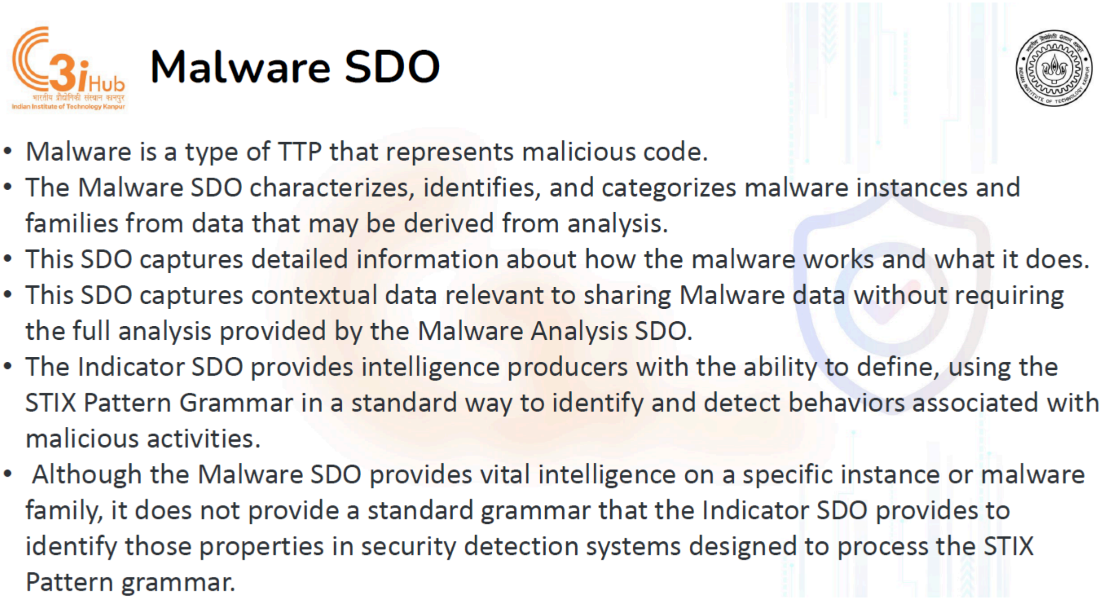


Location SDO

Location		
Required Common	R	type
	R	spec_version
	R	id
	R	created
	R	modified
Optional Common		created_by_ref
		revoked
		labels
		confidence
		lang
		external_references
		object_marking_refs
		granular_markings
		extensions
Location Specific		name
		description
		latitude
		longitude
		precision
		region
		country
		administrative_area
		city
		street_address
		postal_code

So, there is a there is a whole new field called human centered security right. So, there is so much threat information, so much vulnerability information, so much attack going on on the systems. So, now there used to be a whole field of human computer interaction HCI, you might have heard of HCI is a field of cyber security which we have a professors, professor Sruthi Raghavan who is an HCI expert. So, we also have cognitive science people who also look at HCI issues also design people in the design department which also has this. So, this is getting more and more important you will find that in the top conferences nowadays I see that lot of papers are on human centered security.

So, this how you are going to visualize this threat information and whether that visualization actually helps in combating the threat actors, are matter of research and that is but this information may actually help now if you have threat intelligence you cannot have malware information right so if you find malware being used by a threat actor you obviously want that threat intelligence to be spread like be aware of this particular malware. of course you can provide a signature of the malware like if you are a endpoint security company or if you are a antivirus company you will all provide the signature of that malware right so you will send the signature of the malware to all your clients but if you are a threat intelligence company your job is not to directly provide a signature, but you want the consumer of your threat intelligence to know that you have noticed a particular malware and you have certain data especially you have indicators. You know what indicators would indicate that a particular malware has been found or in your system if you see those indicators you can kind of assume that you are also infected by that one. So here is an example of a malware SDO so here the main thing is name here you see here they also gave a hash. although the name does not have to be a hash, but they have given a hash of this malware as a part of the name also in the description.



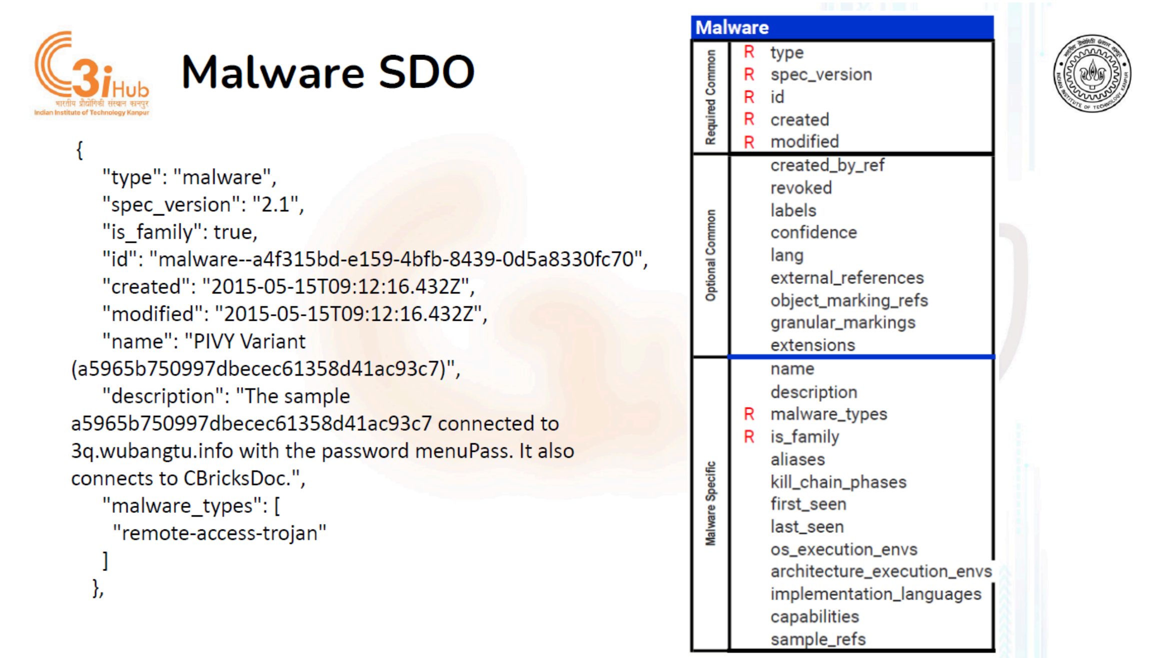
Malware SDO

- Malware is a type of TTP that represents malicious code.
- The Malware SDO characterizes, identifies, and categorizes malware instances and families from data that may be derived from analysis.
- This SDO captures detailed information about how the malware works and what it does.
- This SDO captures contextual data relevant to sharing Malware data without requiring the full analysis provided by the Malware Analysis SDO.
- The Indicator SDO provides intelligence producers with the ability to define, using the STIX Pattern Grammar in a standard way to identify and detect behaviors associated with malicious activities.
- Although the Malware SDO provides vital intelligence on a specific instance or malware family, it does not provide a standard grammar that the Indicator SDO provides to identify those properties in security detection systems designed to process the STIX Pattern grammar.

And it is connected, see in the description it has given more information that it is connected to so and so info with so and so password etcetera, it connects to some other thing. and it is a remote access Trojan. Now you could have more information like if it is a family, so it is a family of malware not just a standalone malware. It might have aliases, it may be actually used in specific kill chain phase. First scene, last scene usually this first scene information may be there, last scene is highly unlikely unless something that goes away.

OS execution environments like you know is it a Windows malware, is it a Windows 7 malware or is it a Windows 10 malware. What architecture execution environment like does it work for x86 or ARM or whatever. whether the implementation language is known whether it is written in C Python whatever capabilities it may have certain capabilities right. So like for example it might do a privilege escalation or it may attempt a literal movement and things like that and then some sample references where will you get the sample. and then you can have this thing now when we look at the relationship objects you will see that malware are usually related by two indicator objects so you may have a malware and there are a couple of indicator objects so I will relate the malware object to indicator object so that whenever I see those indicators I will assume that this malware is seen There is also an object called malware analysis.

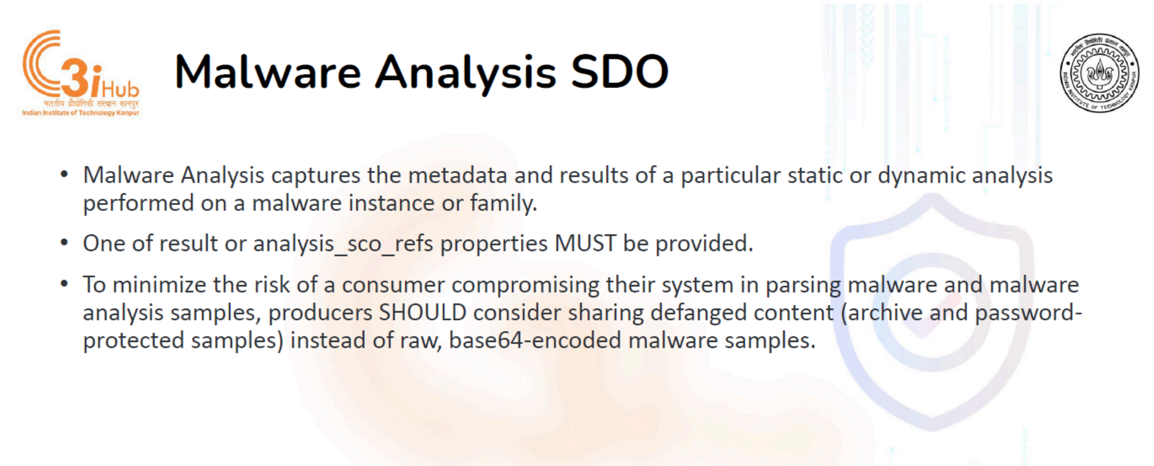
Malware analysis captures metadata and results of a particular static or dynamic analysis performed on a malware instance or family. So it should be either a result or reference these are the sticks observed fiber observable should be provided. So what have I seen right when I analyze the malware what kind of observables I have seen. So and then you should not have the actual copy of the malware in the object because that could be dangerous while you are parsing. the malware object or malware analysis object, if you are actually putting the actual sample of the malware in raw or base 64 encoded form, you might actually accidentally have your consumer compromise.



Malware SDO

```
{
    "type": "malware",
    "spec_version": "2.1",
    "is_family": true,
    "id": "malware--a4f315bd-e159-4bfb-8439-0d5a8330fc70",
    "created": "2015-05-15T09:12:16.432Z",
    "modified": "2015-05-15T09:12:16.432Z",
    "name": "PIVY Variant
(a5965b750997dbecec61358d41ac93c7)",
    "description": "The sample
a5965b750997dbecec61358d41ac93c7 connected to
3q.wubangtu.info with the password menuPass. It also
connects to CBricksDoc.",
    "malware_types": [
      "remote-access-trojan"
    ]
  },
```

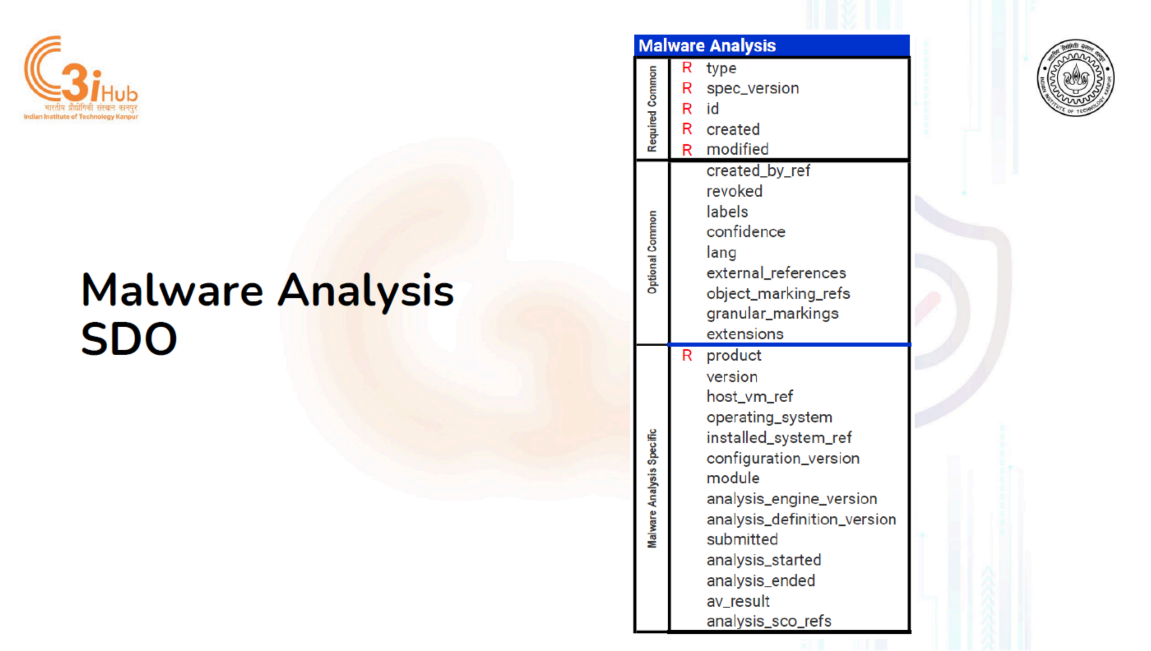
Malware		
Required Common	R	type
	R	spec_version
	R	id
	R	created
	R	modified
Optional Common		created_by_ref
		revoked
		labels
		confidence
		lang
		external_references
		object_marking_refs
		granular_markings
		extensions
Malware Specific		name
		description
	R	malware_types
	R	is_family
		aliases
		kill_chain_phases
		first_seen
		last_seen
		os_execution_envs
		architecture_execution_envs
		implementation_languages
		capabilities
		sample_refs



Malware Analysis SDO

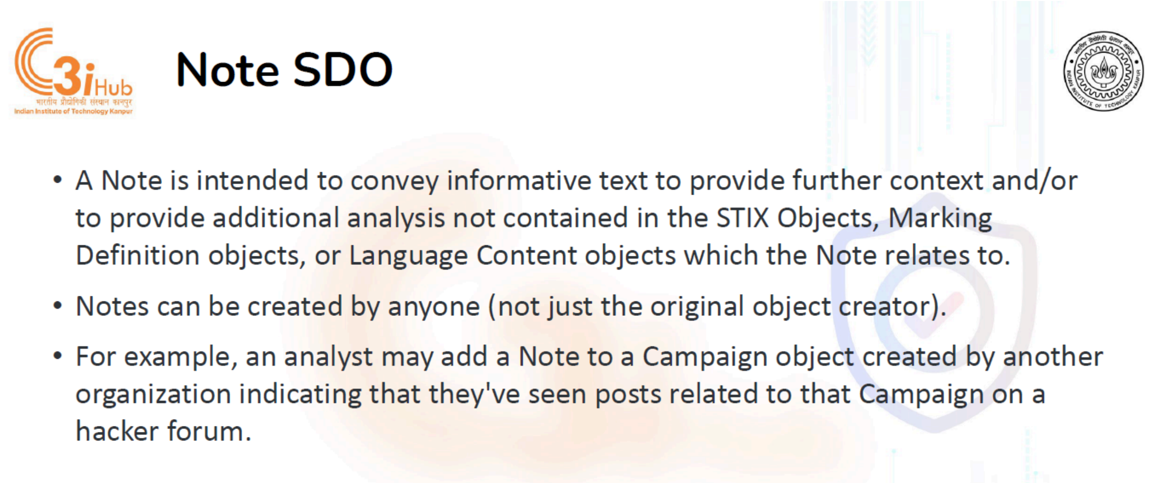
- Malware Analysis captures the metadata and results of a particular static or dynamic analysis performed on a malware instance or family.
- One of result or analysis_sco_refs properties MUST be provided.
- To minimize the risk of a consumer compromising their system in parsing malware and malware analysis samples, producers SHOULD consider sharing defanged content (archive and password-protected samples) instead of raw, base64-encoded malware samples.

So, you should have it in a defined manner that is you put it in the archive format or password protected format and so on. So, this is where this malware analysis object so what you know version host VM like where did you do the analysis virtual machine what operating system installed system configuration all this analysis related what analysis have you done on this malware. Now when you look at the relationship objects malware objects may be actually related to the analysis objects through a relationship object. This is additional information if you want to add a note to the threat information. So, informative text to provide more context or to provide additional analysis not contain in the sticks object or the marking definition object or language content objects which the note relates to.



Malware Analysis SDO

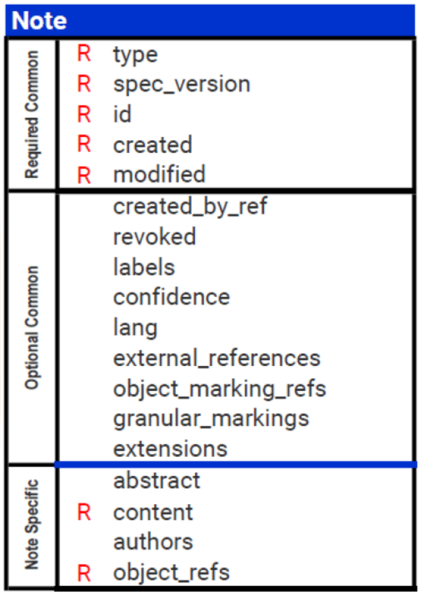
Malware Analysis		
Required Common	R	type
	R	spec_version
	R	id
	R	created
	R	modified
Optional Common		created_by_ref
		revoked
		labels
		confidence
		lang
		external_references
		object_marking_refs
		granular_markings
		extensions
Malware Analysis Specific	R	product
		version
		host_vm_ref
		operating_system
		installed_system_ref
		configuration_version
		module
		analysis_engine_version
		analysis_definition_version
		submitted
		analysis_started
		analysis_ended
		av_result
		analysis_sco_refs



Note SDO

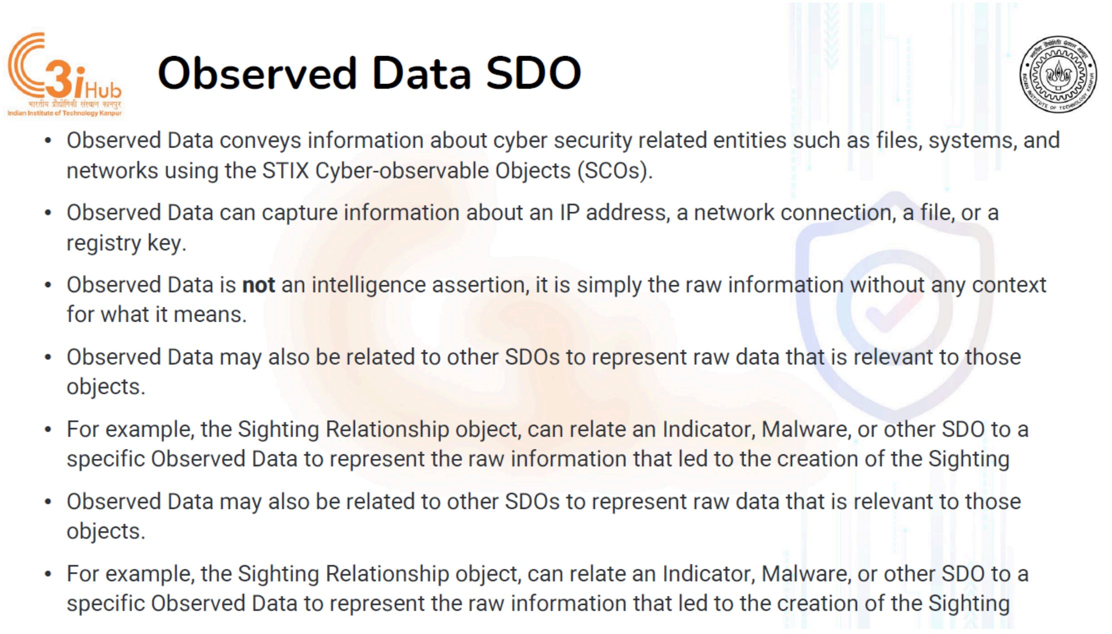
- A Note is intended to convey informative text to provide further context and/or to provide additional analysis not contained in the STIX Objects, Marking Definition objects, or Language Content objects which the Note relates to.
- Notes can be created by anyone (not just the original object creator).
- For example, an analyst may add a Note to a Campaign object created by another organization indicating that they've seen posts related to that Campaign on a hacker forum.

Note SDO



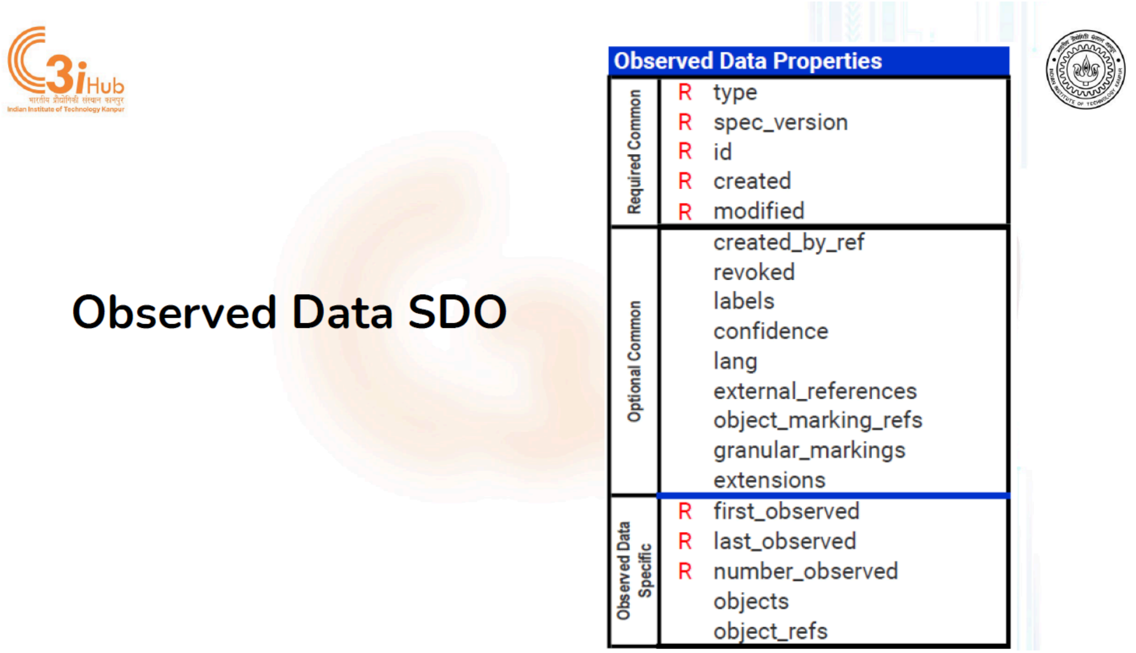
Note		
Required Common	R	type
	R	spec_version
	R	id
	R	created
	R	modified
Optional Common		created_by_ref
		revoked
		labels
		confidence
		lang
		external_references
		object_marking_refs
		granular_markings
		extensions
Note Specific		abstract
	R	content
		authors
	R	object_refs

So, this is additional meta information. So, this is not going to be actually processed as such. So, you can have like you know the note content of the note, you may also mark the author you can give some reference to additional objects or URLs and so on and confidence with which the note has been written whether the note has been revoked all this kind of information now observe data so whenever you are you are going to do some you are going to be attacked you might if you have a detection capabilities as I saying that you have to have the detection capabilities then you have to have the ability to observe certain data such as files, systems, networks and usually those are captured as stix cyber observable objects or SCOs. So, it can also capture information about IP address, a network connection, a file or a registry key etcetera. so observe data is not an intelligence assertion simply raw information without any context for what it means it has to be actually related to other objects so it can be related to other SDOs or SCOs or through the what you call a citing relationship. So, when you say this particular indicator was cited in this particular incident then you can have a citing relationship.



Observed Data SDO

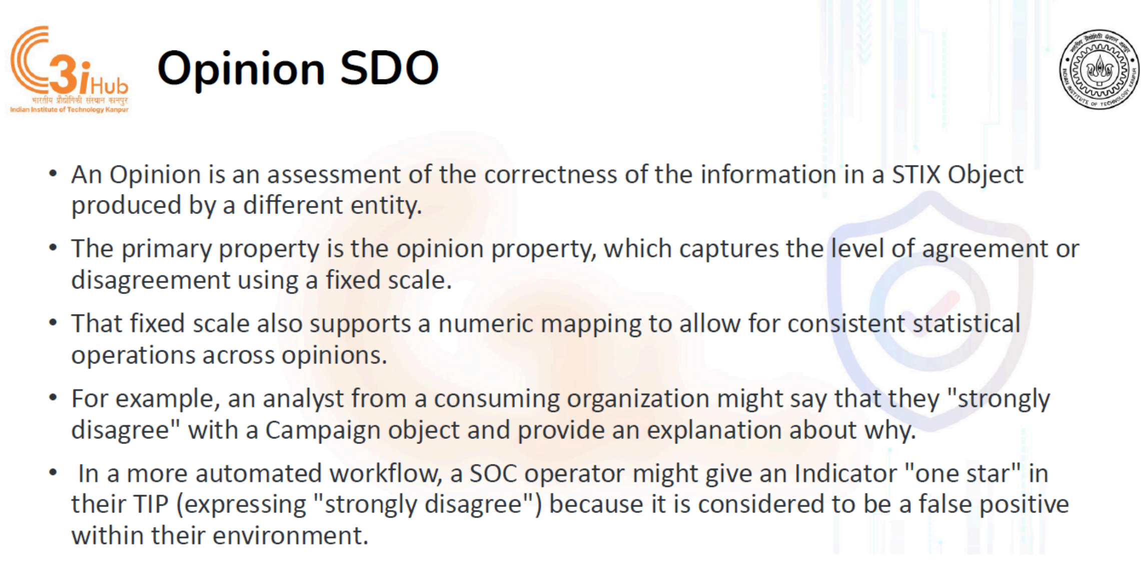
- Observed Data conveys information about cyber security related entities such as files, systems, and networks using the STIX Cyber-observable Objects (SCOs).
- Observed Data can capture information about an IP address, a network connection, a file, or a registry key.
- Observed Data is **not** an intelligence assertion, it is simply the raw information without any context for what it means.
- Observed Data may also be related to other SDOs to represent raw data that is relevant to those objects.
- For example, the Sighting Relationship object, can relate an Indicator, Malware, or other SDO to a specific Observed Data to represent the raw information that led to the creation of the Sighting
- Observed Data may also be related to other SDOs to represent raw data that is relevant to those objects.
- For example, the Sighting Relationship object, can relate an Indicator, Malware, or other SDO to a specific Observed Data to represent the raw information that led to the creation of the Sighting



Observed Data SDO

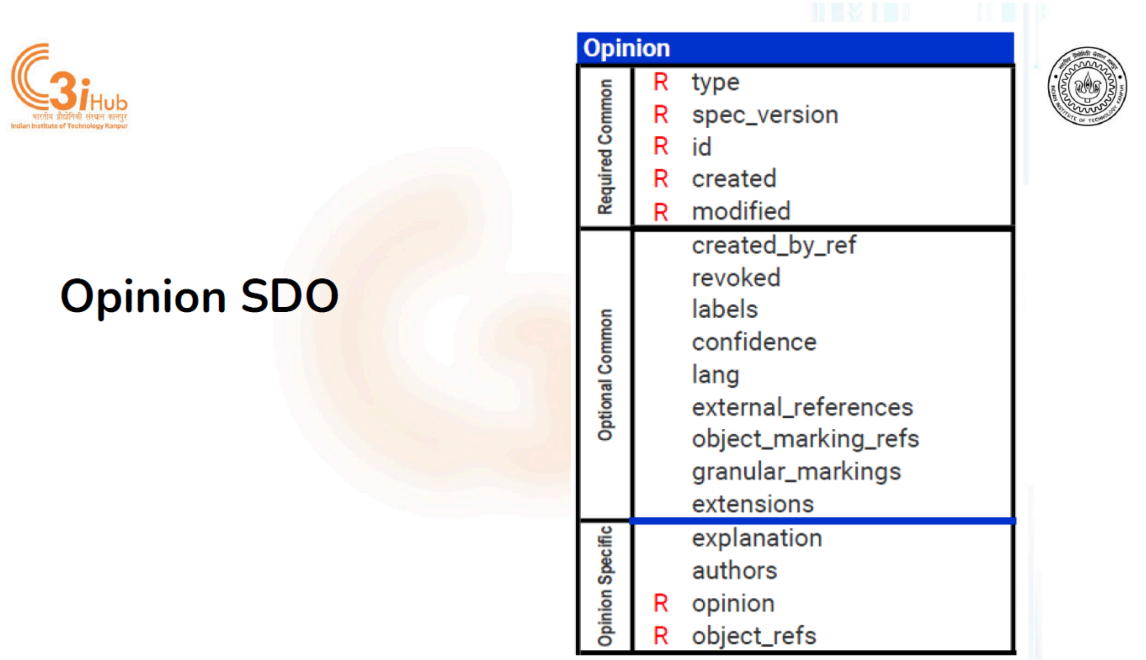
Observed Data Properties		
Required Common	R	type
	R	spec_version
	R	id
	R	created
	R	modified
Optional Common		created_by_ref
		revoked
		labels
		confidence
		lang
		external_references
		object_marking_refs
		granular_markings
		extensions
Observed Data Specific	R	first_observed
	R	last_observed
	R	number_observed
		objects
		object_refs

So, this is the observed data. So, it has this first observed, last observed, number of times it has been observed, what kind of objects have been observed, observed reference. So, usually this would actually be related to these SCOs or cyber observables . you can also have an opinion SDO which is kind of like the note but it is more about the it will it asserts something about the correctness information so usually the consumer of threat intelligence will add this opinion SDO before moving it through its organization or to another organization saying that I strongly disagree with a particular object and provide an explanation why right an SOC operator might give an indicator 1 star in their tip the threat intelligence so because it is considered a false positive within their inward right so so you can have add additional information by enhancing the file so that next person who will be using the threat intelligence will know that somebody has disagreed or somebody found it as false positive and so on. So that's the opinion one, so you can see opinion and object references, explanation, author, these are the main content.



Opinion SDO

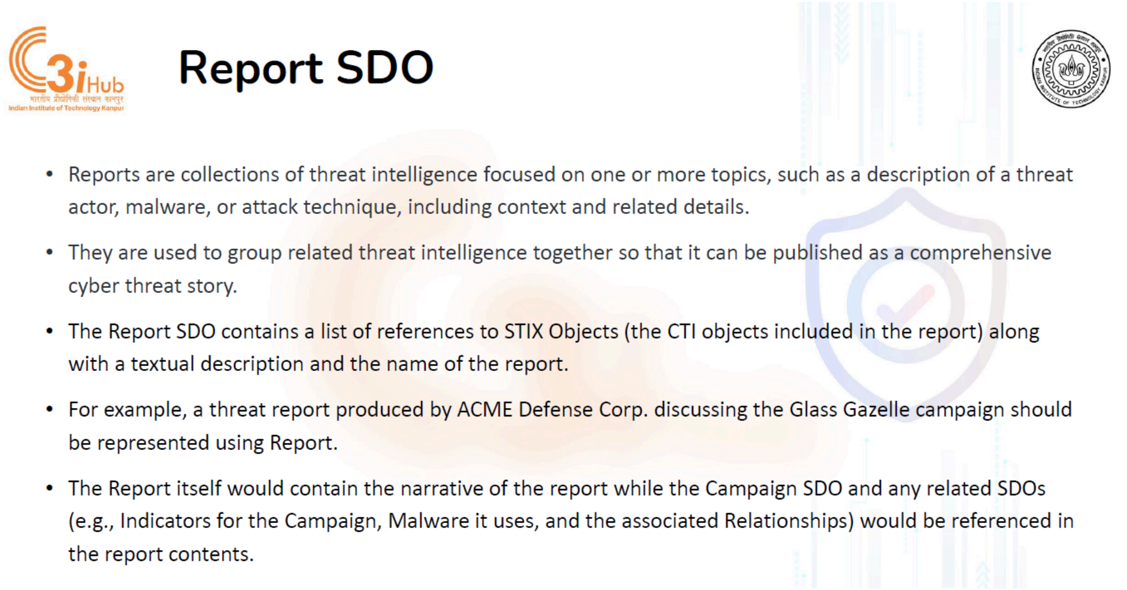
- An Opinion is an assessment of the correctness of the information in a STIX Object produced by a different entity.
- The primary property is the opinion property, which captures the level of agreement or disagreement using a fixed scale.
- That fixed scale also supports a numeric mapping to allow for consistent statistical operations across opinions.
- For example, an analyst from a consuming organization might say that they "strongly disagree" with a Campaign object and provide an explanation about why.
- In a more automated workflow, a SOC operator might give an Indicator "one star" in their TIP (expressing "strongly disagree") because it is considered to be a false positive within their environment.



Opinion SDO

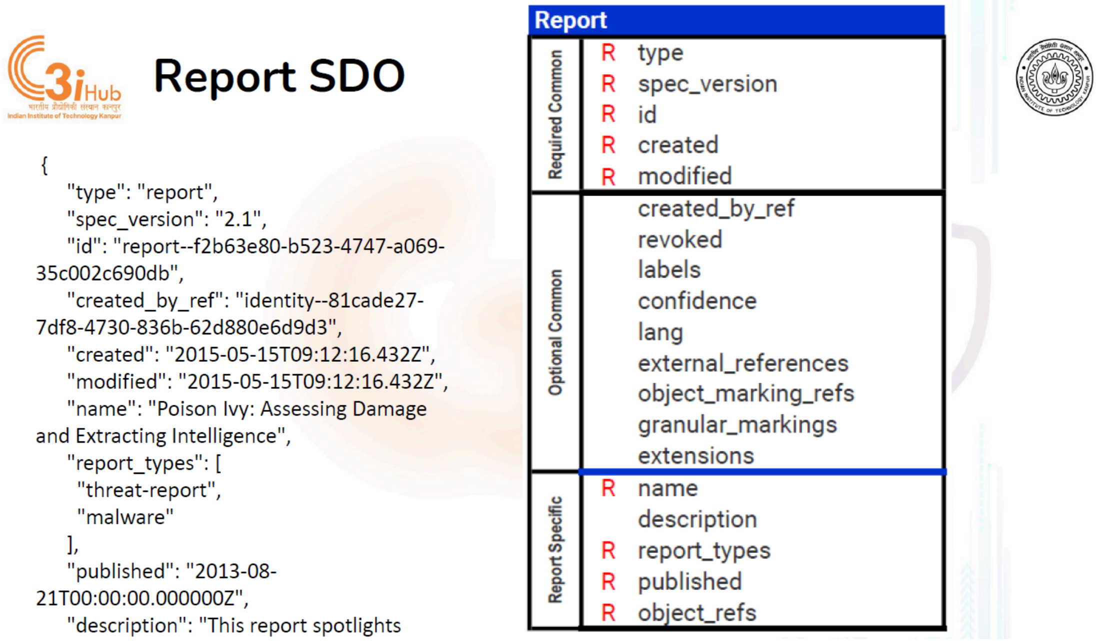
Opinion		
Required Common	R	type
	R	spec_version
	R	id
	R	created
	R	modified
Optional Common		created_by_ref
		revoked
		labels
		confidence
		lang
		external_references
		object_marking_refs
		granular_markings
		extensions
Opinion Specific		explanation
		authors
	R	opinion
	R	object_refs

Now report SDO, reports are usually the top level SDO.



Report SDO

- Reports are collections of threat intelligence focused on one or more topics, such as a description of a threat actor, malware, or attack technique, including context and related details.
- They are used to group related threat intelligence together so that it can be published as a comprehensive cyber threat story.
- The Report SDO contains a list of references to STIX Objects (the CTI objects included in the report) along with a textual description and the name of the report.
- For example, a threat report produced by ACME Defense Corp. discussing the Glass Gazelle campaign should be represented using Report.
- The Report itself would contain the narrative of the report while the Campaign SDO and any related SDOs (e.g., Indicators for the Campaign, Malware it uses, and the associated Relationships) would be referenced in the report contents.



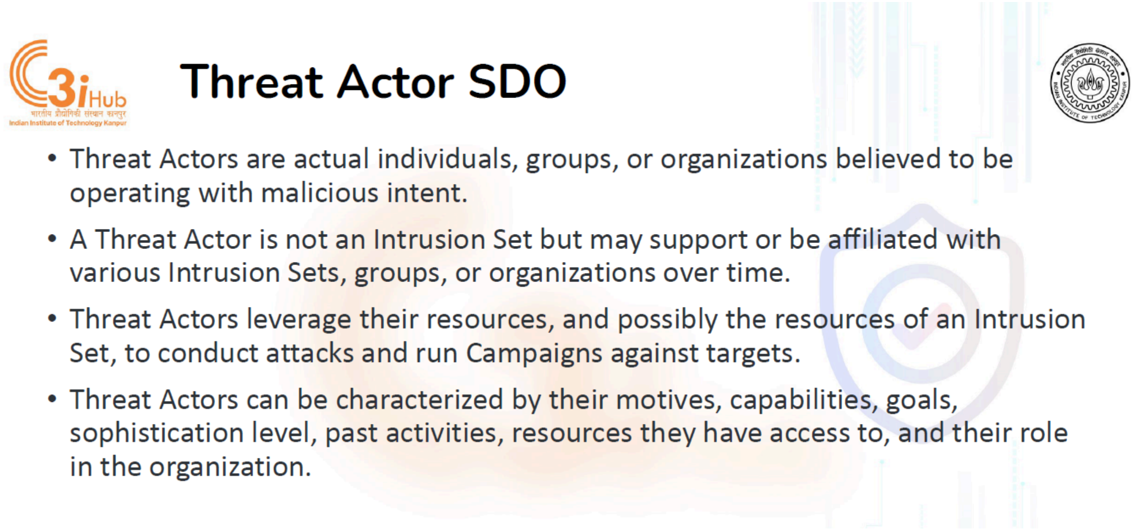
Report SDO

```
{
    "type": "report",
    "spec_version": "2.1",
    "id": "report--f2b63e80-b523-4747-a069-
35c002c690db",
    "created_by_ref": "identity--81cade27-
7df8-4730-836b-62d880e6d9d3",
    "created": "2015-05-15T09:12:16.432Z",
    "modified": "2015-05-15T09:12:16.432Z",
    "name": "Poison Ivy: Assessing Damage
and Extracting Intelligence",
    "report_types": [
      "threat-report",
      "malware"
    ],
    "published": "2013-08-
21T00:00:00.000000Z",
    "description": "This report spotlights
```

Report		
Required Common	R	type
	R	spec_version
	R	id
	R	created
	R	modified
Optional Common		created_by_ref
		revoked
		labels
		confidence
		lang
		external_references
		object_marking_refs
		granular_markings
		extensions
Report Specific	R	name
		description
	R	report_types
	R	published
	R	object_refs

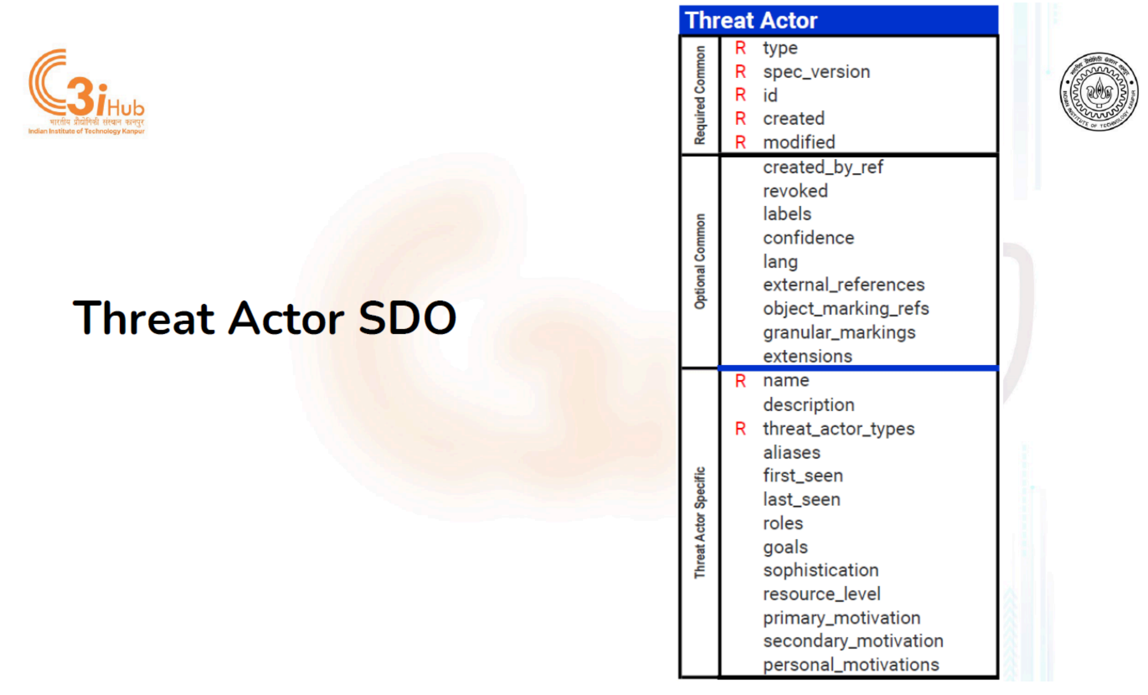
So report basically contains the entire threat intelligence. So when you are reporting, based on your some threat assessment, like say Microsoft wants to put out a report, it can put out a report in the textual form, but if it wants others to also consume the threat intelligence in automation in their security automation systems, then they can actually put this as a report by creating the SDOs and SCOs and relationship objects and then overall this whole entire thing will be an report object. So, the report object will now refer to all the other objects that are there. So, report object contains a list of references to STIX objects or the cyber threat intelligence objects included in the report along with a textual description and name of the report. So, for example, Acme Defense Corporation, that is a bank that we talked about earlier.

So, this particular campaign you know that analysis may be represented as a STIX file but it is overall the entire STIX file is represented as a report. So report itself would contain the narrative of the report while campaign SDO and other related SCOs would be referenced in the report content. So here is a report So, you say it is a type report, it has an id which we can reference created by another identity, remember an identity object. So, it may be created by let us say fire eye or it could be created by Microsoft. So, you have a identity object that you can refer to know that it what this identity is created at this date and modified at this date, you can give a name.



Threat Actor SDO

- Threat Actors are actual individuals, groups, or organizations believed to be operating with malicious intent.
- A Threat Actor is not an Intrusion Set but may support or be affiliated with various Intrusion Sets, groups, or organizations over time.
- Threat Actors leverage their resources, and possibly the resources of an Intrusion Set, to conduct attacks and run Campaigns against targets.
- Threat Actors can be characterized by their motives, capabilities, goals, sophistication level, past activities, resources they have access to, and their role in the organization.

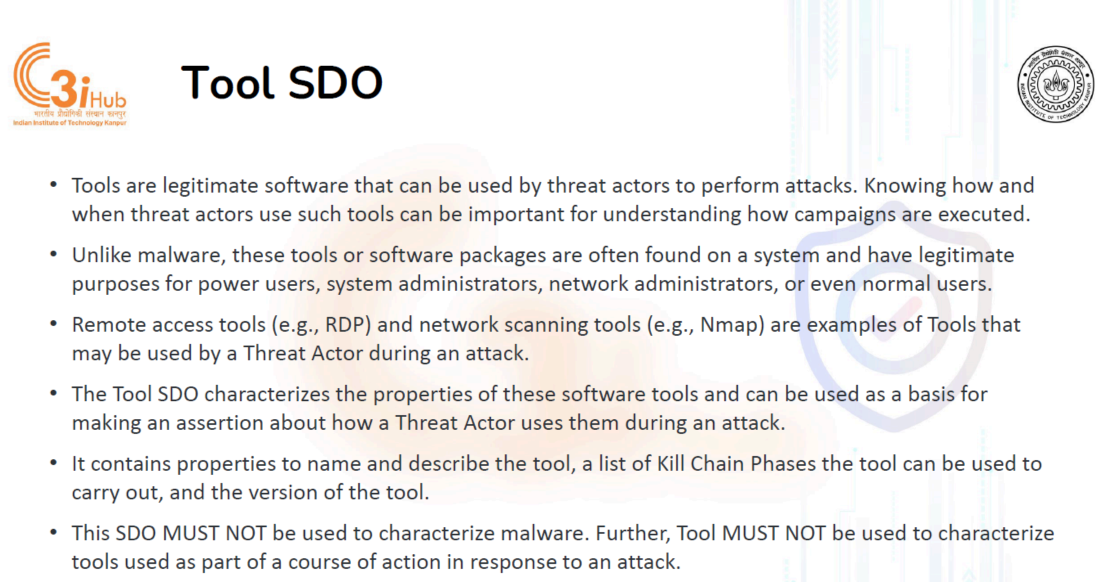


Threat Actor SDO

Threat Actor		
Required Common	R	type
	R	spec_version
	R	id
	R	created
	R	modified
Optional Common		created_by_ref
		revoked
		labels
		confidence
		lang
		external_references
		object_marking_refs
		granular_markings
		extensions
Threat Actor Specific	R	name
		description
	R	threat_actor_types
		aliases
		first_seen
		last_seen
		roles
		goals
		sophistication
		resource_level
		primary_motivation
		secondary_motivation
		personal_motivations

This is a threat report as well as a malware report it is published when description and so on. So, and this object references this is I am not showing the full file here. So, object references will now talk about a malware SDO it will talk about some indicators it will have some relationship objects all that stuff. So, in the entire intelligence about that particular case Acme case would be part of this references object references and those objects references can then be looked up to see what they are talking about.

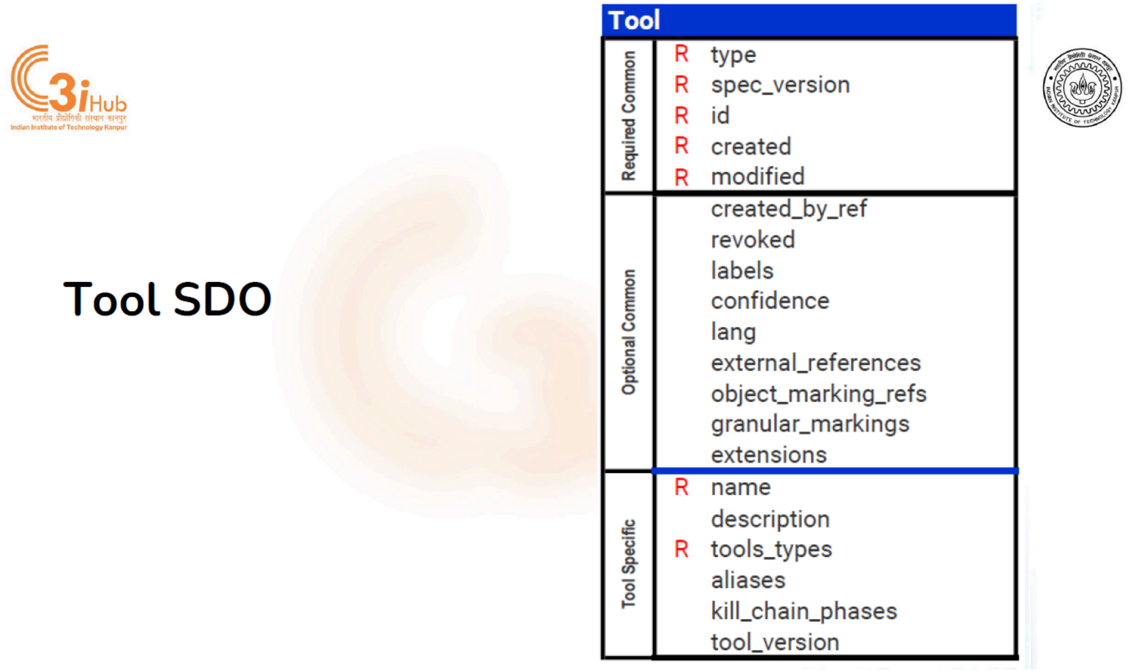
So, that is report. threat actor, threat actor, SDO are individuals, groups or organizations and they may support or be affiliated to various intrusion sets, groups and organizations. They leverage their resources and possibly the resources of intrusion set can be characterized by their motives, capabilities, goals, sophistication level, past activities, resources they have access to and their role in the organization. So, see there is a lot of information you can add here for example, what is their sophistication level, what resource level they have, you can have some data about primary motivation, secondary motivation. personal motivation and first scene, last scene, etcetera, what kind of threat actor type, name, etcetera. So, you can describe a threat actor and then that threat actor object it has an id so using that id you can relate it to a campaign or it can relate it to a intrusion set or you can relate it to an attack pattern.



Tool SDO

- Tools are legitimate software that can be used by threat actors to perform attacks. Knowing how and when threat actors use such tools can be important for understanding how campaigns are executed.
- Unlike malware, these tools or software packages are often found on a system and have legitimate purposes for power users, system administrators, network administrators, or even normal users.
- Remote access tools (e.g., RDP) and network scanning tools (e.g., Nmap) are examples of Tools that may be used by a Threat Actor during an attack.
- The Tool SDO characterizes the properties of these software tools and can be used as a basis for making an assertion about how a Threat Actor uses them during an attack.
- It contains properties to name and describe the tool, a list of Kill Chain Phases the tool can be used to carry out, and the version of the tool.
- This SDO MUST NOT be used to characterize malware. Further, Tool MUST NOT be used to characterize tools used as part of a course of action in response to an attack.

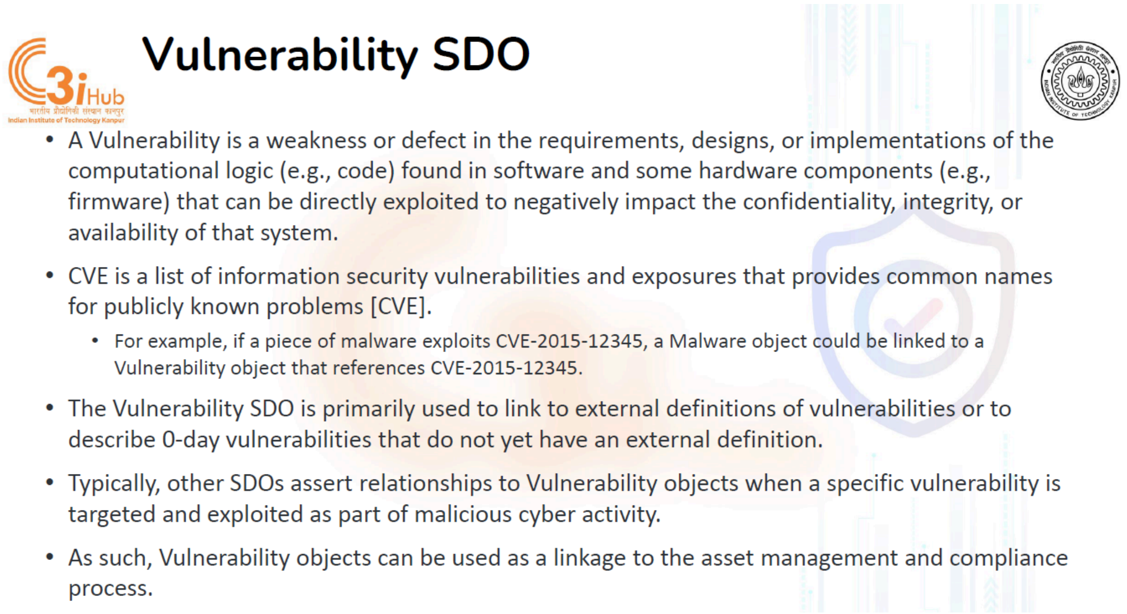
so tool another sdo is a tool as i said that there could be tools like remote access tools like rdp or network scanning tools like nmap that may be used by threat actors during an attack. So, you can describe the various tools that you noticed while analyzing the incident to tell the potential user of your threat intelligence that be careful because they are using RDP. So, if you have an RDP which is not properly protected, if you have a remote desktop port open and you have a vulnerable version of windows you might be attacked by this actor or you might be scanned by nmap by this threat actor right. So, do not answer to the nmap scan do obfuscation and so on. So, usually tool what tool types what kill chain phase it is being used what version of the tool might be used etcetera are information that you want to have there.



Tool SDO

Tool		
Required Common	R	type
	R	spec_version
	R	id
	R	created
	R	modified
Optional Common		created_by_ref
		revoked
		labels
		confidence
		lang
		external_references
		object_marking_refs
		granular_markings
		extensions
Tool Specific	R	name
		description
	R	tools_types
		aliases
		kill_chain_phases
		tool_version

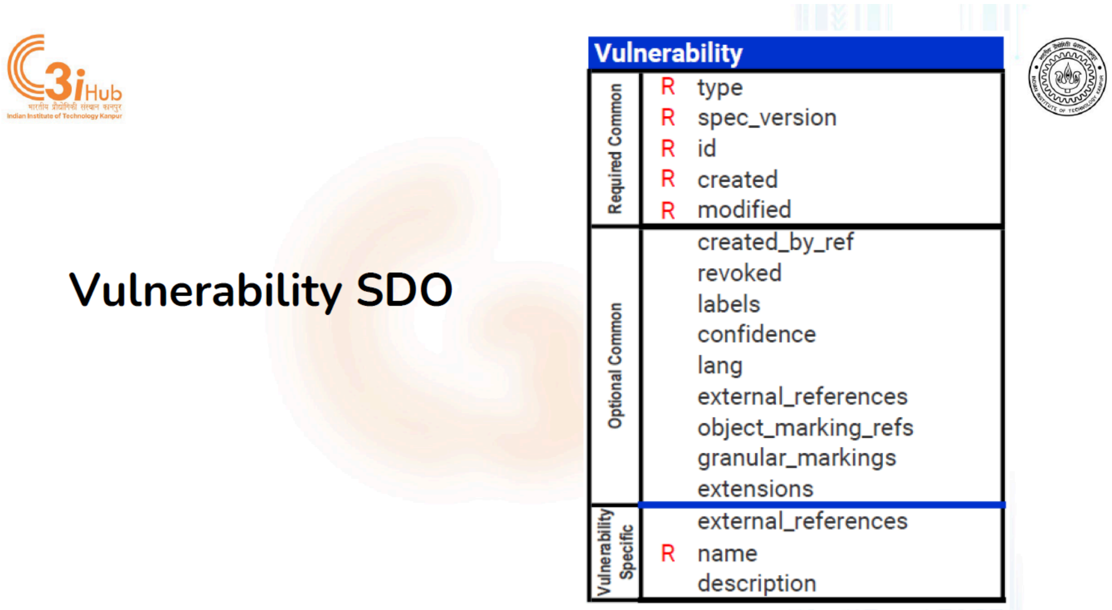
now if you are giving threat intelligence you may want to know what vulnerability the threat actor is using right because eventually to compromise your system your system should have some vulnerability .



Vulnerability SDO

- A Vulnerability is a weakness or defect in the requirements, designs, or implementations of the computational logic (e.g., code) found in software and some hardware components (e.g., firmware) that can be directly exploited to negatively impact the confidentiality, integrity, or availability of that system.
- CVE is a list of information security vulnerabilities and exposures that provides common names for publicly known problems [CVE].
  - For example, if a piece of malware exploits CVE-2015-12345, a Malware object could be linked to a Vulnerability object that references CVE-2015-12345.
- The Vulnerability SDO is primarily used to link to external definitions of vulnerabilities or to describe 0-day vulnerabilities that do not yet have an external definition.
- Typically, other SDOs assert relationships to Vulnerability objects when a specific vulnerability is targeted and exploited as part of malicious cyber activity.
- As such, Vulnerability objects can be used as a linkage to the asset management and compliance process.

Now vulnerability you know you may have unpatched system therefore you may have vulnerability and the threat intelligence would say that for example last to last week we had the XZ vulnerability Linux XZ vulnerability that had a severity of 10 right. So it had a CVE number I think CVE 2023 something. so that vulnerability was exploited by many threat actors so any threat intelligence that was produced when that was going on would reference that particular vulnerability. so there should be a way to capture individual vulnerabilities so it should have external references so this usually would be reference to the national vulnerability database or CVE database name and description and then you can have a description may you will have the CVE number etcetera.



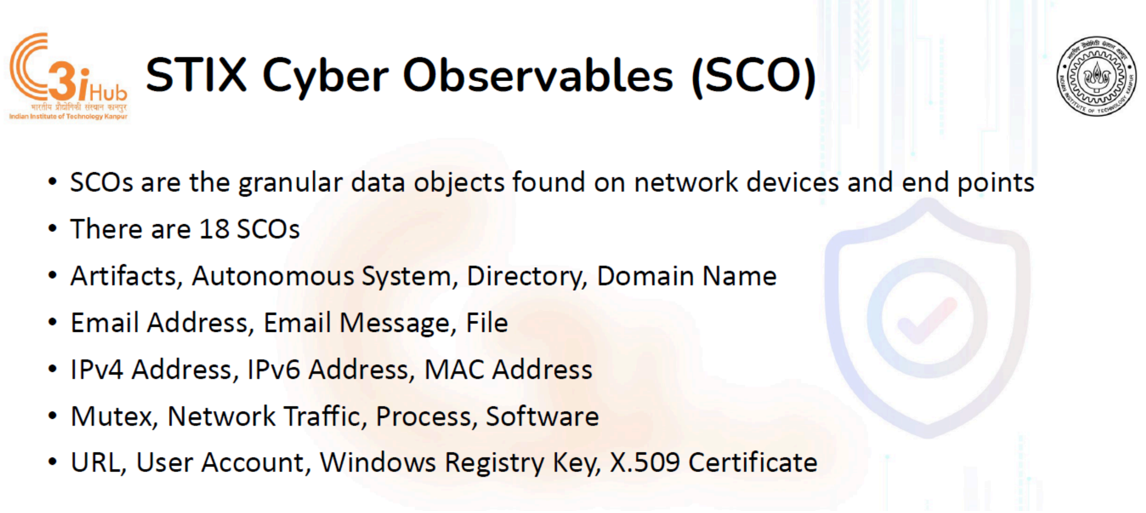
Vulnerability SDO

Vulnerability		
Required Common	R	type
	R	spec_version
	R	id
	R	created
	R	modified
Optional Common		created_by_ref
		revoked
		labels
		confidence
		lang
		external_references
		object_marking_refs
		granular_markings
		extensions
Vulnerability Specific		external_references
	R	name
		description

So, you can actually parse the description or the parse the name the name could be also CVE. So, it could be the name also. So, that was the list of all SDOs. So, these are all the SDOs there is in the STIX 2.

1 specification. Now you have the observables, observables are what you observe. So, as you saw in the SDO what you saw was more of you know the different types of data like we have attack pattern, we have campaign, we have intuition set, we have threat actor, we have malware, we have malware analysis, we have indicators, we have identities, we have location, we have notes, reports, we have opinions. So, all these things different types of objects right that are relevant to a threat intelligence information. Now what I want is that I want to describe what you know if threat intelligence is only as good if I can use it to detect the attacks or detect the presence of threat actor or detect the presence of malware.

So, there has to be some observables right. So, an observables are those that gets created because of the attack or because of some action by the threat actor and those has to be then used for detection purposes or forensic purposes. So I if I am going to give you some threat intelligence based on what I have noticed in my system happening then I should also tell you so here is an IP address from which I got nmapped or here is an IP address from which I got to which my malware was communicating or my Trojan was communicating or here is a URL that my Trojan was communicating or I could say that this particular malware creates a file inside so and so directory or it creates as this specific directory or I could say that it creates this kind of binary into DLL files or I might say that this affects the network traffic in this way that I seen flood right or I see a particular process being created or set of processes being created by this malware or I see that there is some Windows registry key being created or deleted or whatever. So, I have to be able to express those. yes? No, so indicator SDO we will see is going to be related to this.

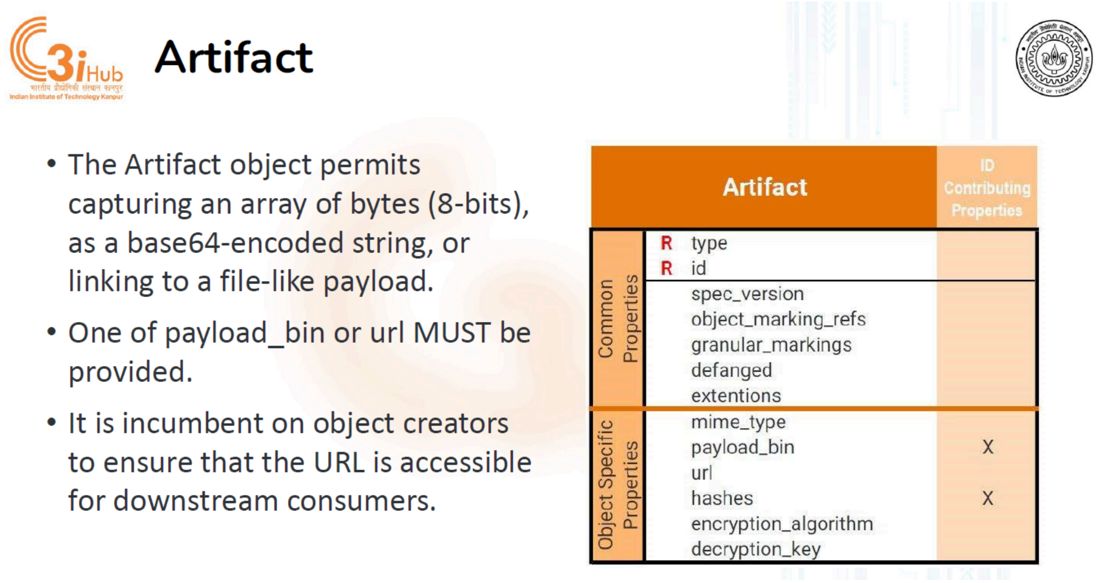


STIX Cyber Observables (SCO)

- SCOs are the granular data objects found on network devices and end points
- There are 18 SCOs
- Artifacts, Autonomous System, Directory, Domain Name
- Email Address, Email Message, File
- IPv4 Address, IPv6 Address, MAC Address
- Mutex, Network Traffic, Process, Software
- URL, User Account, Windows Registry Key, X.509 Certificate

So when I am describing let us say an IPv4 address. So indicator, if you go to the indicator, so I think I have to, let us go and see the indicator again. So, you see in indicator I am very being very generic. So, in this case I am saying the indicator type is related to malicious activity and attribution and I see this as a pattern right, but this indicator does not say that this is an URL. so eventually I have to somehow if I want to make more sense in an automated fashion as a human if I read as a human this whole thing I will know that this is they are talking about an URL indicator right but the same indicator object with the same indicator type malicious activity might as well contain an IP address or a registry key right so eventually what I want is that I also want to have more semantics of an indicator so what the SCOs are giving you are actually more semantically rich information then you can say with a relationship object that this is an indicator which indicates something right.

So, that way you have more information right. So, you can think of this as I do not know if you have taken a relational database course in a relational database I might have a relational for every type of SCO I may have a table right. So, I have a directory, I have a artifact whatever. So, I can have multiple tables and then I can have also table that like indicators right and then I will be able to have a foreign key that connects this indicator to a particular table. So, that way I can do better queries right.



Artifact

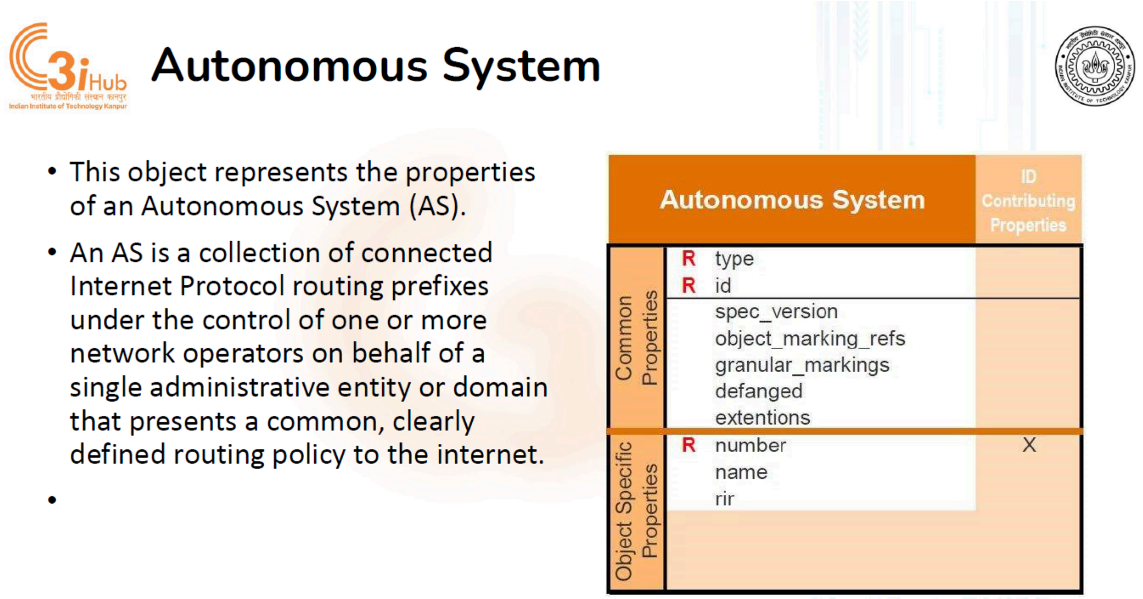
- The Artifact object permits capturing an array of bytes (8-bits), as a base64-encoded string, or linking to a file-like payload.
- One of payload_bin or url MUST be provided.
- It is incumbent on object creators to ensure that the URL is accessible for downstream consumers.

		Artifact	ID Contributing Properties
Common Properties	R	type	
	R	id	
		spec_version	
		object_marking_refs	
		granular_markings	
		defanged	
		extentions	
Object Specific Properties		mime_type	
		payload_bin	X
		url	
		hashes	X
		encryption_algorithm	
		decryption_key	

So, there are 18 such different SCOs. So, in this SCO you see that, so this is artifact object. So, artifact object is usually for capturing an array of bytes as a base 64 encoded string or linking to a file like payload. So, you see that here. I can have a either URL or file hash or I can actually have a payload bin which is base 64 encoded string right.

So and one of these has to be present. So even though it does not say R but one of them has to be present otherwise this artifact object is useless right. So if neither indicates to a file or if it does not indicate the binary right. So, now it is incumbent on the object creators to ensure that the URL is accessible to the downstream consumers, so you cannot give an URL that is you know local to you right, so it has to be resolvable right. now this does not relate, see here you see that this observer has no relationship with any malware or anything, right? it just a standalone object, right? later on with relationship I have to relate this to something otherwise this what is what good is it, right? no no these are all json. I am just saying that sometimes information is kind of given out of context.

This is context free. There is no context in this information. Relationship objects will bring context to this. That is why I was trying to explain how we design tables and stuff. So, here is an autonomous system we know the autonomous system is what like you know like for example, IIT Kanpur itself is an autonomous system right. So, it has an AS number it is your ISP any ISP you have is an autonomous system right. So, it is basically autonomous system is characterized by a set of IP prefixes right or in CIDR form right.



Autonomous System

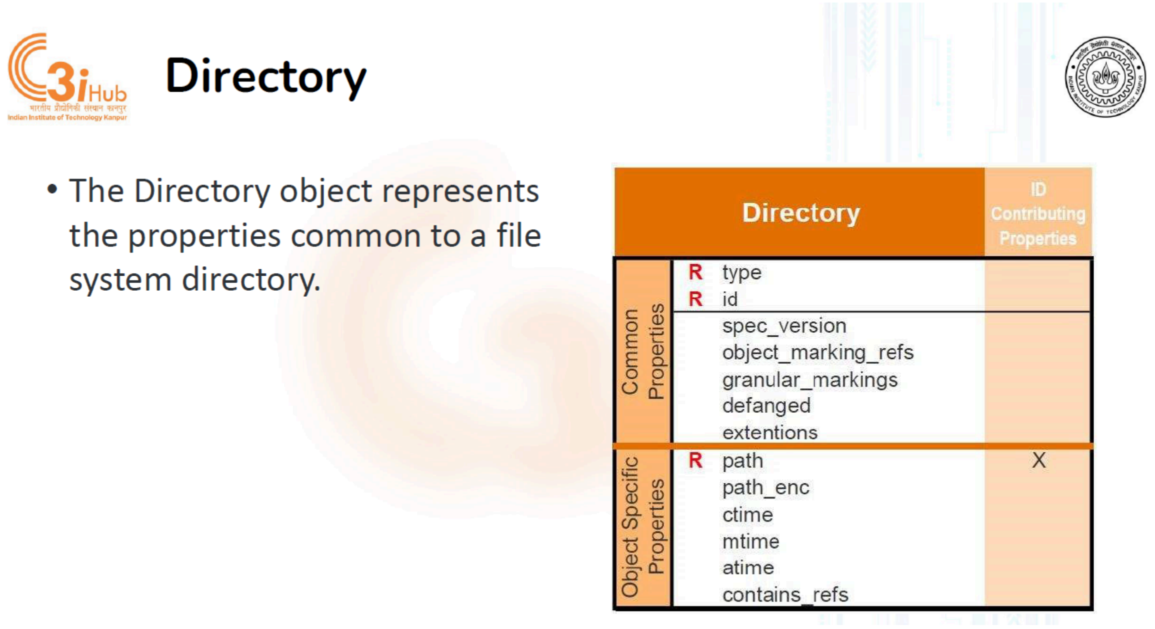
- This object represents the properties of an Autonomous System (AS).
- An AS is a collection of connected Internet Protocol routing prefixes under the control of one or more network operators on behalf of a single administrative entity or domain that presents a common, clearly defined routing policy to the internet.

	Autonomous System		ID Contributing Properties
Common Properties	R	type	
	R	id	
		spec_version	
		object_marking_refs	
		granular_markings	
		defanged	
		extentions	
Object Specific Properties	R	number	X
		name	
		rir	

So, autonomous system, so it is basically each autonomous system has a unique number throughout the world right. So, if you look at the IIT Kanpur's autonomous system, so 202.

3.77.16 I think. see our autonomous system number is 55479 right. So, that is IIT Kanpur campus network we are given an autonomous system number and this is the this thing, but in any case. So, autonomous system characterizes. So, many times when we investigate a particular cyber attack we try to figure out which autonomous system it came from if it is at all possible because or when we see an IP address we try to figure out with a who is look up or IP look up which autonomous system because then we can request that ISP if that ISP is going to listen to us for knowing more about that IP address if they are attacking us. AS number is unique yes.

So it is basically related to IP address prefix right so 202.3.77 I think slash 24 or do we have 24 bit yeah so 24 slash 24 so 202.3.77.1 slash 24 is IIT Kanpur's IP prefix on on Airtel I think right is it no it is NKN. So, this is the IIT Kanpur got long time ago from the regional internet registry and regional internet registry got it from the global internet registry.

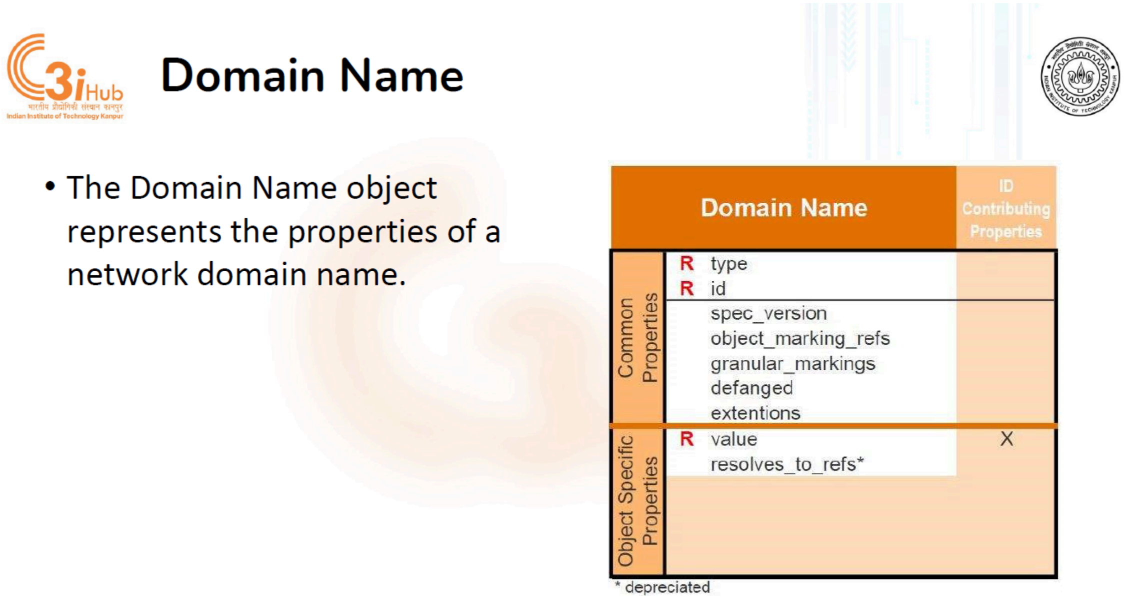


Directory

- The Directory object represents the properties common to a file system directory.

Directory			ID Contributing Properties
Common Properties	R	type	
	R	id	
		spec_version	
		object_marking_refs	
		granular_markings	
		defanged	
		extentions	
Object Specific Properties	R	path	X
		path_enc	
		ctime	
		mtime	
		atime	
		contains_refs	

So, that is the unique to IIT Kanpur. So, this chunk of IP addresses is AS5545 whatever that number is. so directory object is basically mainly it has characterized by path and so on. Domain name object .



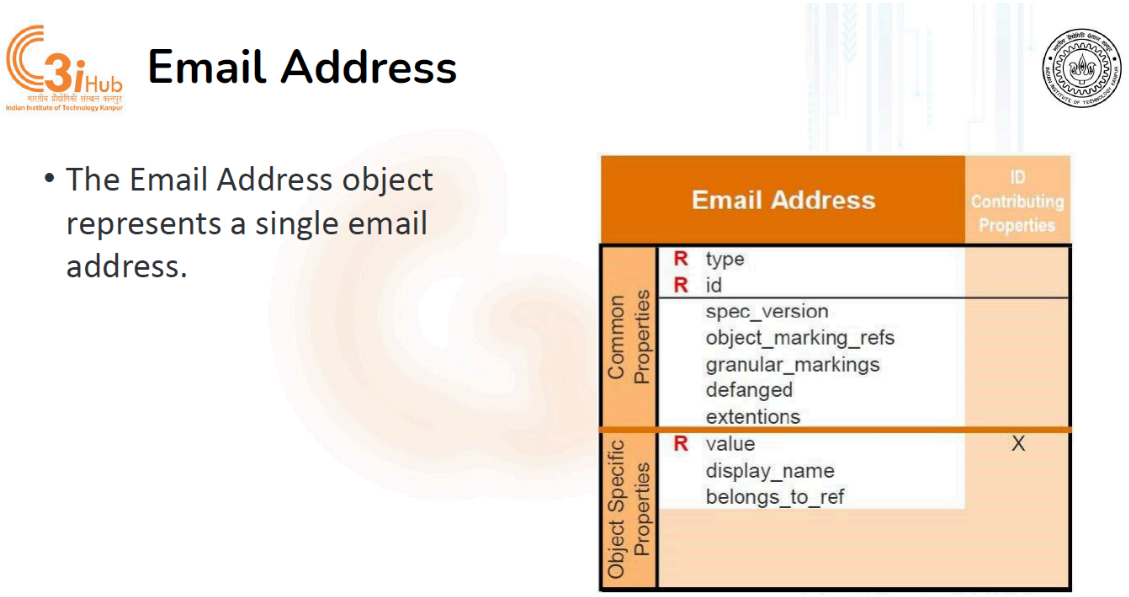
Domain Name

- The Domain Name object represents the properties of a network domain name.

Domain Name			ID Contributing Properties
Common Properties	R	type	
	R	id	
		spec_version	
		object_marking_refs	
		granular_markings	
		defanged	
		extentions	
Object Specific Properties	R	value	X
		resolves_to_refs*	

* depreciated

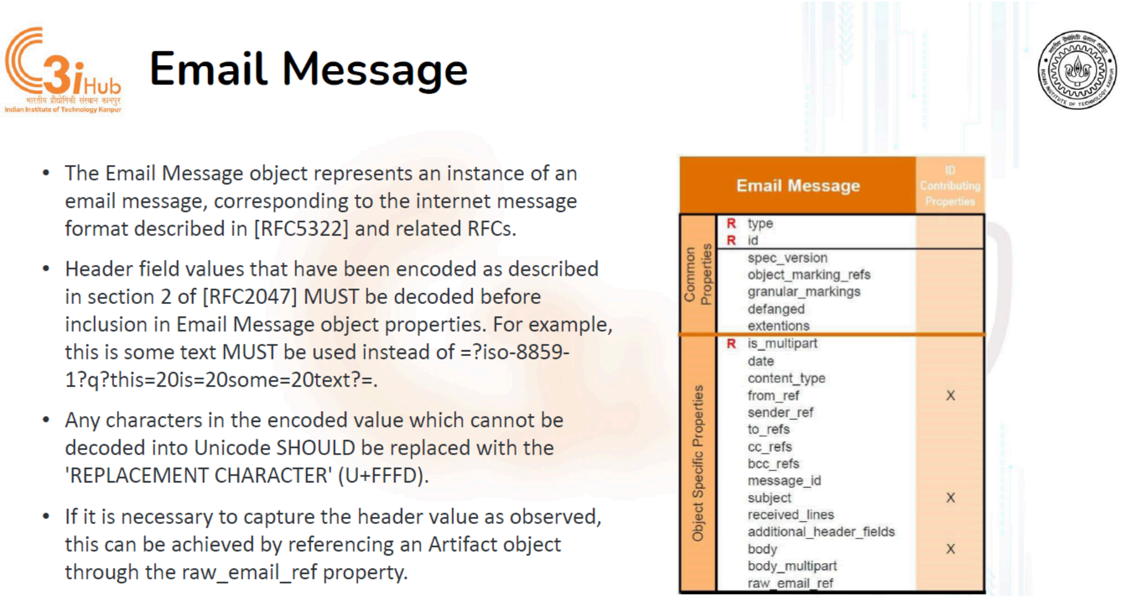
You know the value here may resolve to reference here you can actually put the IP address it resolves to email address object represents a single email address. Email message has to be decoded the header has to be decoded etcetera.



Email Address

- The Email Address object represents a single email address.

Email Address			ID Contributing Properties
Common Properties	R	type	
	R	id	
		spec_version	
		object_marking_refs	
		granular_markings	
		defanged	
		extentions	
Object Specific Properties	R	value	X
		display_name	
		belongs_to_ref	

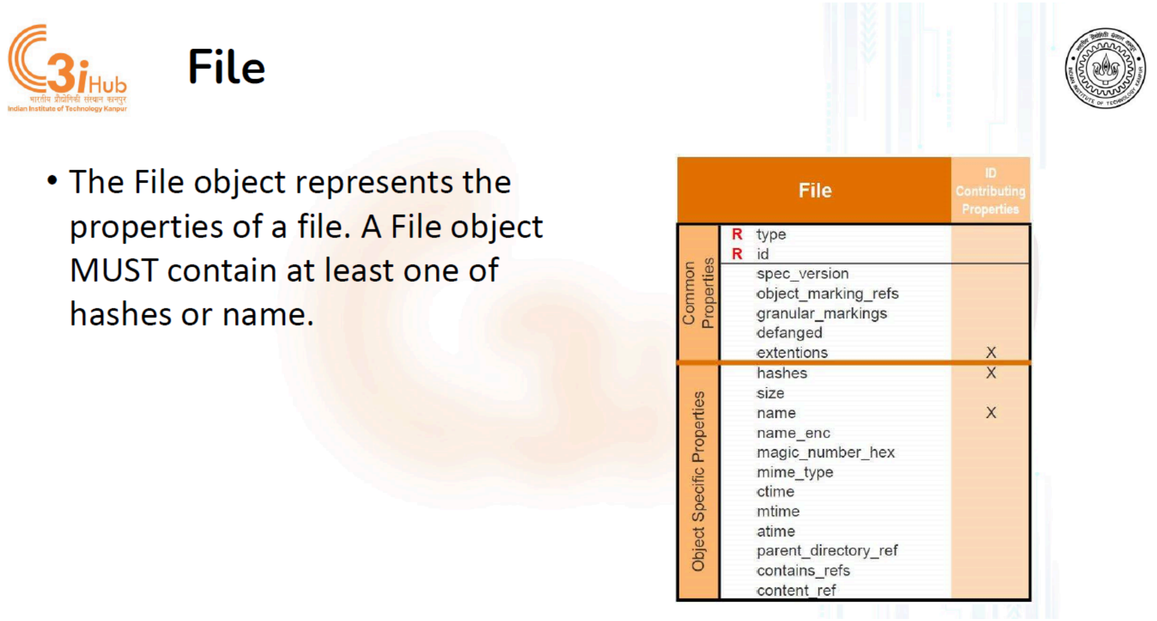


Email Message

- The Email Message object represents an instance of an email message, corresponding to the internet message format described in [RFC5322] and related RFCs.
- Header field values that have been encoded as described in section 2 of [RFC2047] MUST be decoded before inclusion in Email Message object properties. For example, this is some text MUST be used instead of =?iso-8859-1?q?this=20is=20some=20text?=.
- Any characters in the encoded value which cannot be decoded into Unicode SHOULD be replaced with the 'REPLACEMENT CHARACTER' (U+FFFD).
- If it is necessary to capture the header value as observed, this can be achieved by referencing an Artifact object through the raw_email_ref property.

Email Message			ID Contributing Properties
Common Properties	R	type	
	R	id	
		spec_version	
		object_marking_refs	
		granular_markings	
		defanged	
		extentions	
Object Specific Properties	R	is_multipart	
		date	
		content_type	
		from_ref	X
		sender_ref	
		to_refs	
		cc_refs	
		bcc_refs	
		message_id	
		subject	X
		received_lines	
		additional_header_fields	
		body	X
		body_multipart	
		raw_email_ref	

So, whether it is a multi part email and so on. You can have lot more information or this is at least the required information you can actually have this entire email message, but the problem is that because of privacy reasons if you are if you are going to produce threat intelligence, based on an attack, Let us say this is a phishing attack whose information is being produced. You may not want to give all the information that is in the email, but you may give some information that is useful. File object, of course, if a file is created or something or at least one of hash or the name of the file has to be there.



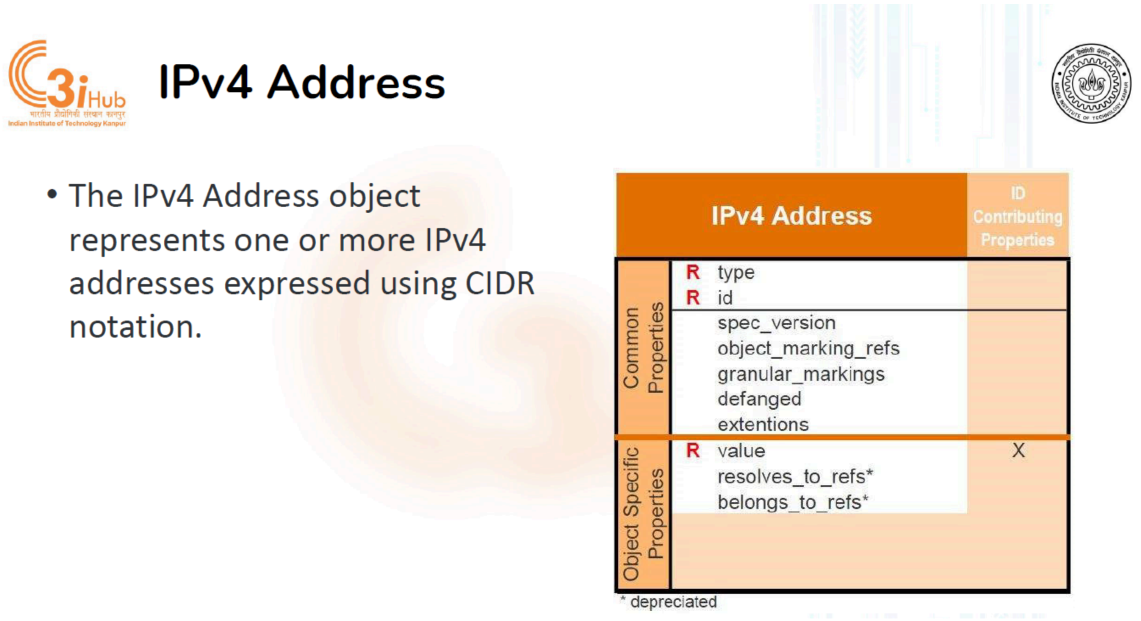
File

- The File object represents the properties of a file. A File object MUST contain at least one of hashes or name.

		File	ID Contributing Properties
Common Properties	R	type	
	R	id	
		spec_version	
		object_marking_refs	
		granular_markings	
		defanged	
		extentions	X
Object Specific Properties		hashes	X
		size	
		name	X
		name_enc	
		magic_number_hex	
		mime_type	
		ctime	
		mtime	
		atime	
		parent_directory_ref	
		contains_refs	
		content_ref	

IPv4 address, IPv6 address, MAC address, mutex object, network traffic. So, you may have arbitrary network traffic, you may give it a source and destination, source and destination addresses and ports.

and you can give the traffic in pcap file or whatever you can give reference to the pcap file.



IPv4 Address

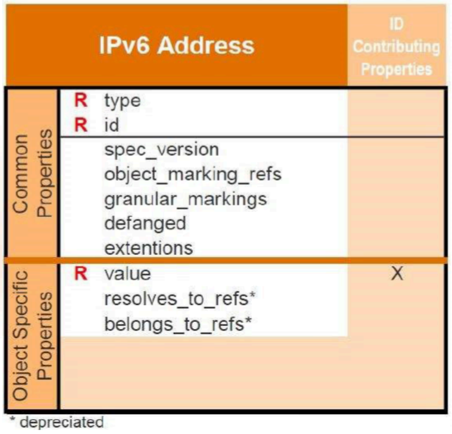
- The IPv4 Address object represents one or more IPv4 addresses expressed using CIDR notation.

		IPv4 Address	ID Contributing Properties
Common Properties	R	type	
	R	id	
		spec_version	
		object_marking_refs	
		granular_markings	
		defanged	
		extentions	
Object Specific Properties	R	value	X
		resolves_to_refs*	
		belongs_to_refs*	

* depreciated

IPv6 Address

- The IPv6 Address object represents one or more IPv6 addresses expressed using CIDR notation.

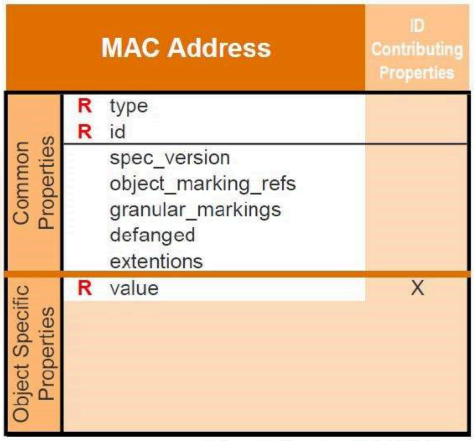


		IPv6 Address	ID Contributing Properties
Common Properties	R	type	
	R	id	
		spec_version	
		object_marking_refs	
		granular_markings	
		defanged	
		extentions	
Object Specific Properties	R	value	X
		resolves_to_refs*	
		belongs_to_refs*	

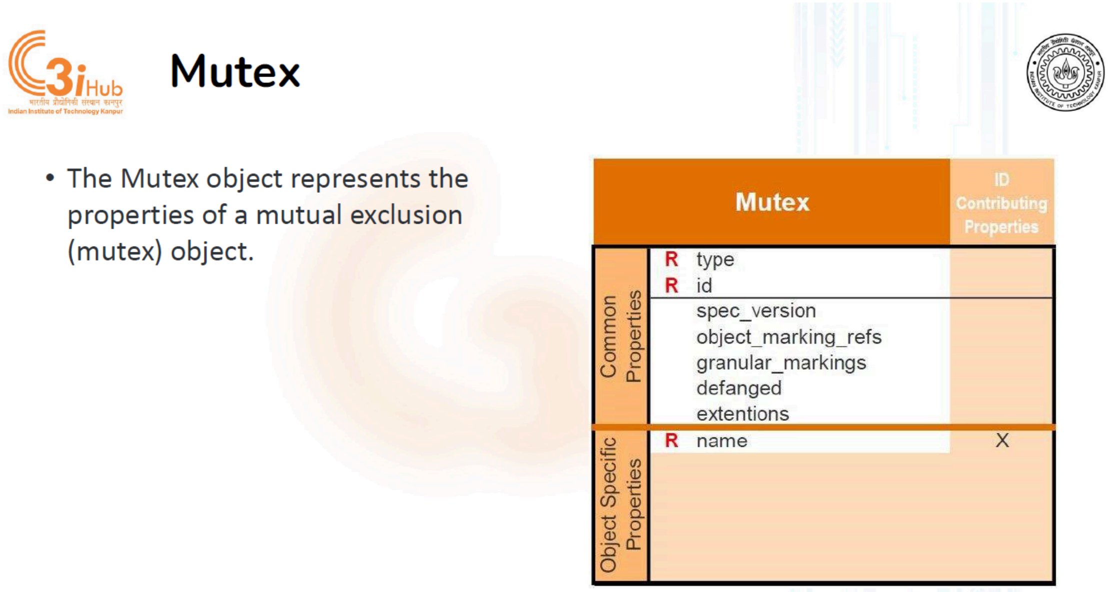
* depreciated

MAC Address

- The MAC Address object represents a single Media Access Control (MAC) address.



		MAC Address	ID Contributing Properties
Common Properties	R	type	
	R	id	
		spec_version	
		object_marking_refs	
		granular_markings	
		defanged	
		extentions	
Object Specific Properties	R	value	X



Mutex

- The Mutex object represents the properties of a mutual exclusion (mutex) object.

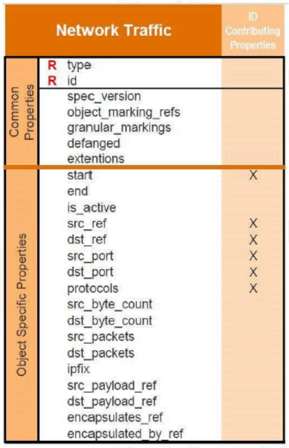
		Mutex	ID Contributing Properties
Common Properties	R	type	
	R	id	
		spec_version	
		object_marking_refs	
		granular_markings	
		defanged	
		extentions	
Object Specific Properties	R	name	X

So, you can, but you may not always share the entire information. If a process is being created, you might give at least the what process is being created by this threat actor or malware. If a software object is seen, then you can talk about this software object.

URL is seen then you can talk about the URL. You can talk about user account sometimes user accounts are created by specific names like root or admin or things like that. You can also that may be a you may actually see a user account information for a social media account which was used to phishing attack and things like that. Windows registry key, so you may have key and value here. You may see an X.509 certificate a digital you know SSL certificate that is part of threat intelligence that this particular certificate.

Network Traffic

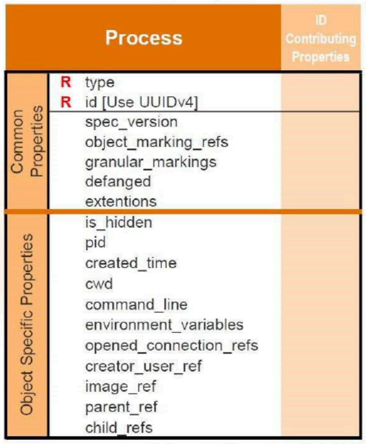
- The Network Traffic object represents arbitrary network traffic that originates from a source and is addressed to a destination. The network traffic MAY or MAY NOT constitute a valid unicast, multicast, or broadcast network connection. This MAY also include traffic that is not established, such as a SYN flood.
- To allow for use cases where a source or destination address may be sensitive and not suitable for sharing, such as addresses that are internal to an organization's network, the source and destination properties (src_ref and dst_ref, respectively) are defined as optional.



		Network Traffic	ID Contributing Properties
Common Properties	R	type	
	R	id	
		spec_version	
		object_marking_refs	
		granular_markings	
		defanged	
		extentions	
Object Specific Properties		start	X
		end	
		is_active	
		src_ref	X
		dst_ref	X
		src_port	X
		dst_port	X
		protocols	X
		src_byte_count	
		dst_byte_count	
		src_packets	
		dst_packets	
		ipfix	
		src_payload_ref	
		dst_payload_ref	
		encapsulates_ref	
		encapsulated_by_ref	

Process

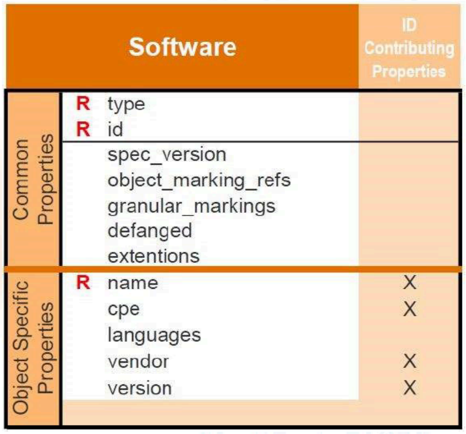
- The Process object represents common properties of an instance of a computer program as executed on an operating system. A Process object MUST contain at least one property (other than type) from this object (or one of its extensions).



		Process	ID Contributing Properties
Common Properties	R	type	
	R	id [Use UUIDv4]	
		spec_version	
		object_marking_refs	
		granular_markings	
		defanged	
		extentions	
Object Specific Properties		is_hidden	
		pid	
		created_time	
		cwd	
		command_line	
		environment_variables	
		opened_connection_refs	
		creator_user_ref	
		image_ref	
		parent_ref	
		child_refs	

Software

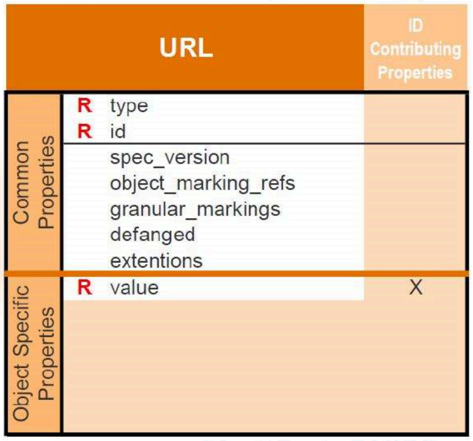
- The Software object represents high-level properties associated with software, including software products.



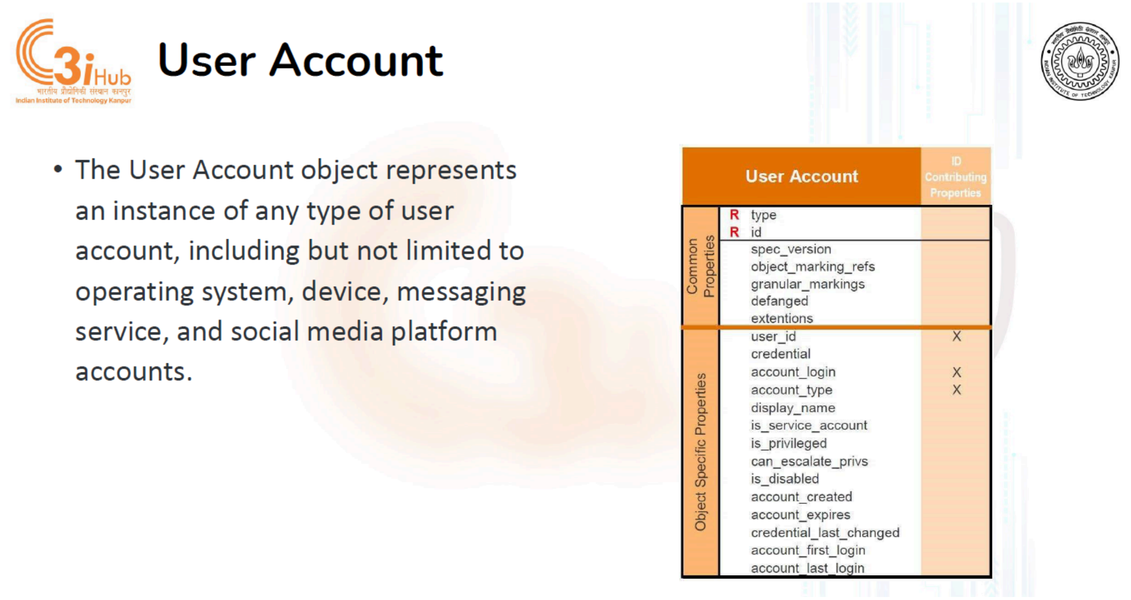
		Software	ID Contributing Properties
Common Properties	R	type	
	R	id	
		spec_version	
		object_marking_refs	
		granular_markings	
		defanged	
		extentions	
Object Specific Properties	R	name	X
		cpe	X
		languages	
		vendor	X
		version	X

URL

- The URL object represents the properties of a uniform resource locator (URL).



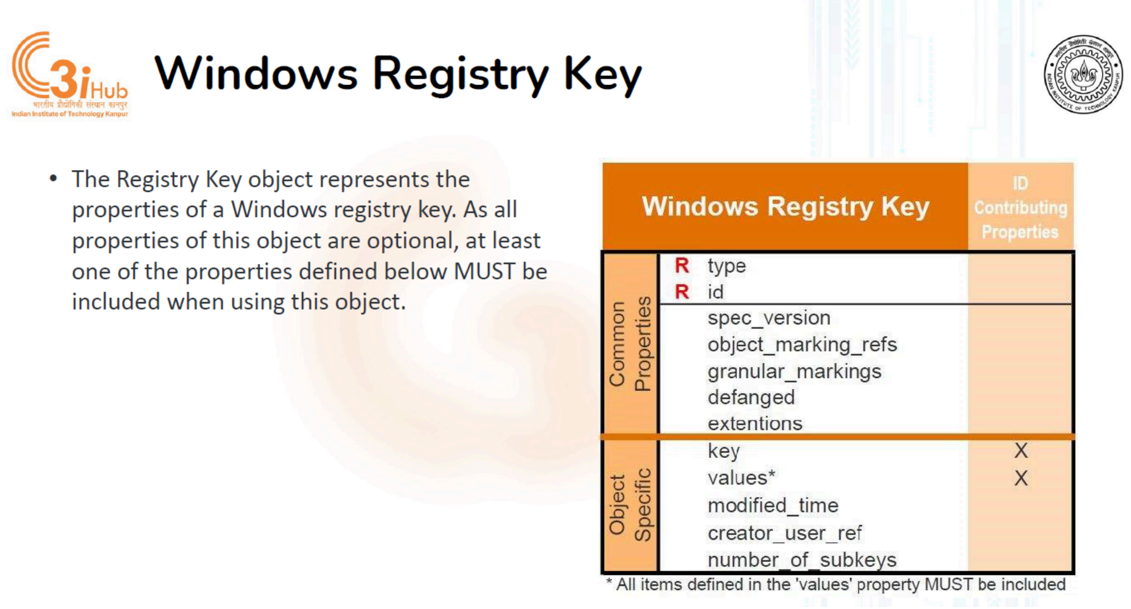
		URL	ID Contributing Properties
Common Properties	R	type	
	R	id	
		spec_version	
		object_marking_refs	
		granular_markings	
		defanged	
		extentions	
Object Specific Properties	R	value	X



User Account

- The User Account object represents an instance of any type of user account, including but not limited to operating system, device, messaging service, and social media platform accounts.

		User Account	ID Contributing Properties
Common Properties	R	type	
	R	id	
		spec_version	
		object_marking_refs	
		granular_markings	
		defanged	
		extentions	
Object Specific Properties		user_id	X
		credential	
		account_login	X
		account_type	X
		display_name	
		is_service_account	
		is_privileged	
		can_escalate_privs	
		is_disabled	
		account_created	
		account_expires	
		credential_last_changed	
		account_first_login	
		account_last_login	



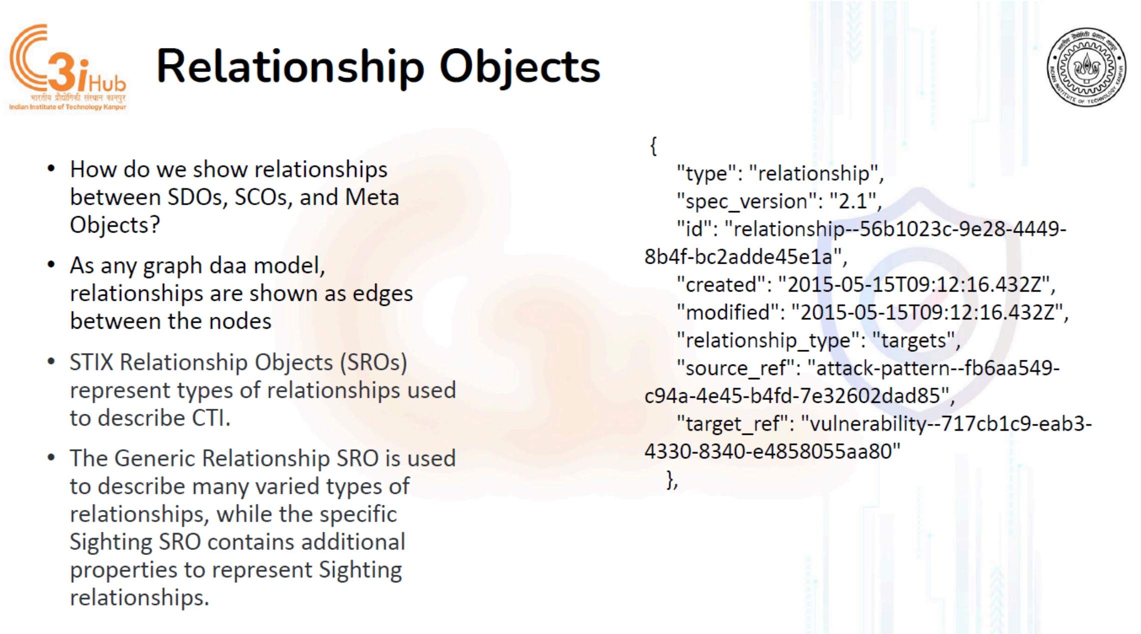
Windows Registry Key

- The Registry Key object represents the properties of a Windows registry key. As all properties of this object are optional, at least one of the properties defined below MUST be included when using this object.

		Windows Registry Key	ID Contributing Properties
Common Properties	R	type	
	R	id	
		spec_version	
		object_marking_refs	
		granular_markings	
		defanged	
		extentions	
Object Specific		key	X
		values*	X
		modified_time	
		creator_user_ref	
		number_of_subkeys	

* All items defined in the 'values' property MUST be included

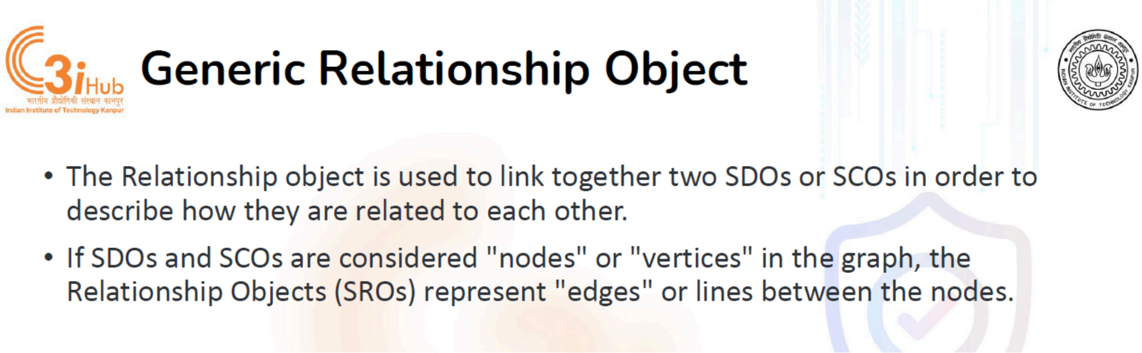
Remember like you know in Stuxnet for example, they forged digital certificates. So, there has been many attacks where digital certificates have been forged. So, forged certificate attacks may be used. Now comes the relationship object. So, we have SDOs, we have SCOs.



Relationship Objects

- How do we show relationships between SDOs, SCOs, and Meta Objects?
- As any graph daa model, relationships are shown as edges between the nodes
- STIX Relationship Objects (SROs) represent types of relationships used to describe CTI.
- The Generic Relationship SRO is used to describe many varied types of relationships, while the specific Sighting SRO contains additional properties to represent Sighting relationships.

```
{
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--56b1023c-9e28-4449-
8b4f-bc2adde45e1a",
    "created": "2015-05-15T09:12:16.432Z",
    "modified": "2015-05-15T09:12:16.432Z",
    "relationship_type": "targets",
    "source_ref": "attack-pattern--fb6aa549-
c94a-4e45-b4fd-7e32602dad85",
    "target_ref": "vulnerability--717cb1c9-eab3-
4330-8340-e4858055aa80"
   },
```



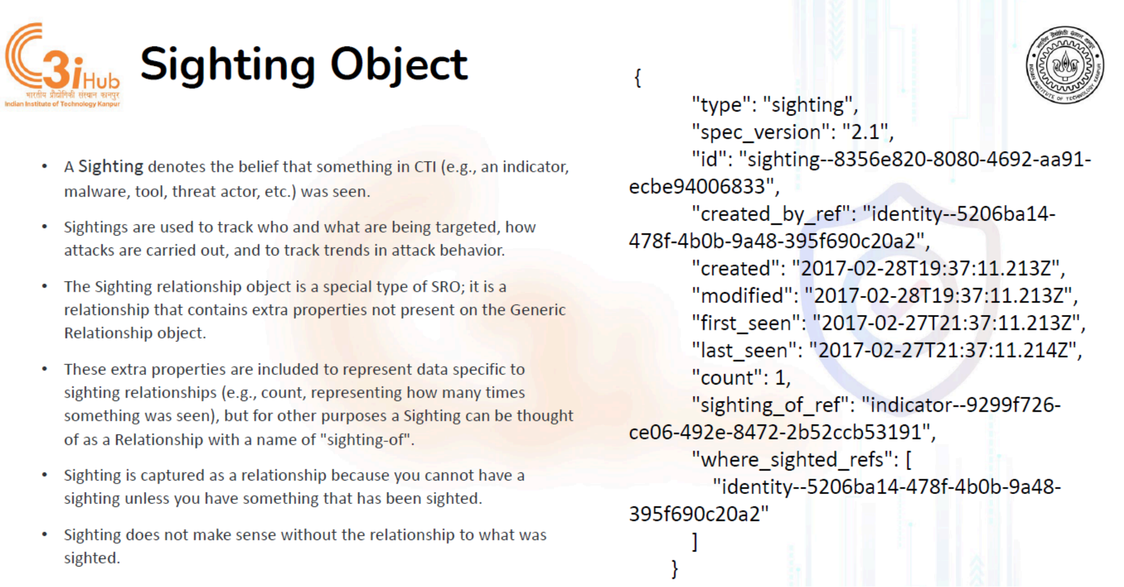
Generic Relationship Object

- The Relationship object is used to link together two SDOs or SCOs in order to describe how they are related to each other.
- If SDOs and SCOs are considered "nodes" or "vertices" in the graph, the Relationship Objects (SROs) represent "edges" or lines between the nodes.

and now we have to relate them because otherwise it makes no sense right. So, I have lots of SCOs and then I have some malware description some description of some malware I have some description of an intuition set a threat actor, but how would they all related to each other right. So, you have to have the relationship object right and relationship type will tell you what the relationship is. So, for example, maybe an attack pattern uses a particular vulnerability or targets a particular vulnerability on the target system right. So, I would say that a relationship type is targets. So, you see attack pattern now I am not describing the attack pattern because I have an already an SDO which has all the information right

So, I have to just take get go there and get that information and I have to go there and get this information this is also an SDO. and then I am relating them by targets. So, this is how I am doing the targets. So, these are called the generic relationship objects.

So, there are many such objects you can create. So, this for example, I can say that this indicator indicates So, in that case instead of targets I will say I will have an indicator ID here and a malware ID here and I will say that indicates. So, I can have a malware analysis and I can have a file SCO object here and I can say this file is created by this malware. So, this kind of relationships can be described. So these are called generic relationship objects.



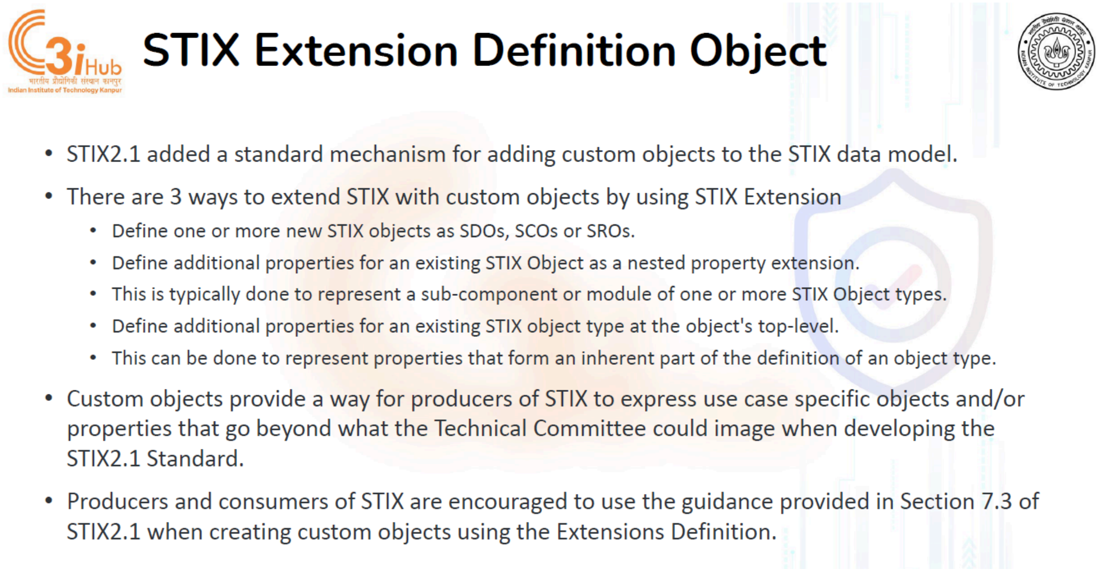
Sighting Object

- A Sighting denotes the belief that something in CTI (e.g., an indicator, malware, tool, threat actor, etc.) was seen.
- Sightings are used to track who and what are being targeted, how attacks are carried out, and to track trends in attack behavior.
- The Sighting relationship object is a special type of SRO; it is a relationship that contains extra properties not present on the Generic Relationship object.
- These extra properties are included to represent data specific to sighting relationships (e.g., count, representing how many times something was seen), but for other purposes a Sighting can be thought of as a Relationship with a name of "sighting-of".
- Sighting is captured as a relationship because you cannot have a sighting unless you have something that has been sighted.
- Sighting does not make sense without the relationship to what was sighted.

```
{
        "type": "sighting",
        "spec_version": "2.1",
        "id": "sighting--8356e820-8080-4692-aa91-
ecbe94006833",
        "created_by_ref": "identity--5206ba14-
478f-4b0b-9a48-395f690c20a2",
        "created": "2017-02-28T19:37:11.213Z",
        "modified": "2017-02-28T19:37:11.213Z",
        "first_seen": "2017-02-27T21:37:11.213Z",
        "last_seen": "2017-02-27T21:37:11.214Z",
        "count": 1,
        "sighting_of_ref": "indicator--9299f726-
ce06-492e-8472-2b52ccb53191",
        "where_sighted_refs": [
           "identity--5206ba14-478f-4b0b-9a48-
395f690c20a2"
        ]
     }
```

So SDOs and SCOs are kind of nodes or vertices in the graph. And the SROs, the relationship objects, represent edges or lines between the nodes. So that's the graphical representation. There is also another kind of relationship called sighting. So sighting, for example, I can say sighting of a particular indicator and where cited so identity so so maybe a particular indicator for example an ip address was cited in an organization so i can i can put that information here saying that this indicator so i can go and check what what that indicator was it could be a traffic network traffic it could be an url it could be a file and where it has been cited and I will say where was it first seen and last seen and all that information how many times it has been seen and so on so there is a citing type of relationship which is different from generic relationship which basically relates in many different ways also if you do not feel that you are a threat intelligence creator or you are a threat intelligence consumer and then you want to move that threat intelligence forward to somebody else.

So, you can extend this by three different ways you can create custom objects. So, here I am saying that I am saying that I can do a new SDO SCO or SRO I can define which is less likely to happen. or I can define additional properties for an existing Stix object as a nested property extension. So, typically done to represent a sub component or module of a one or more stix object types or you can define additional properties for existing stix object type at the object top level. So, either you can nest it or you can put it in the object top level.



STIX Extension Definition Object

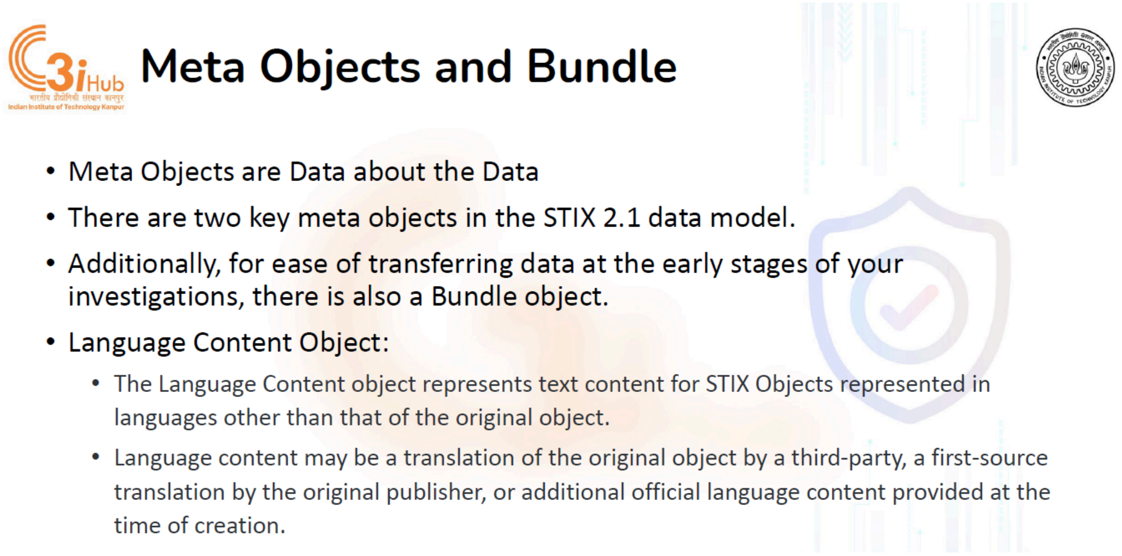
- STIX2.1 added a standard mechanism for adding custom objects to the STIX data model.
- There are 3 ways to extend STIX with custom objects by using STIX Extension
  - Define one or more new STIX objects as SDOs, SCOs or SROs.
  - Define additional properties for an existing STIX Object as a nested property extension.
  - This is typically done to represent a sub-component or module of one or more STIX Object types.
  - Define additional properties for an existing STIX object type at the object's top-level.
  - This can be done to represent properties that form an inherent part of the definition of an object type.
- Custom objects provide a way for producers of STIX to express use case specific objects and/or properties that go beyond what the Technical Committee could image when developing the STIX2.1 Standard.
- Producers and consumers of STIX are encouraged to use the guidance provided in Section 7.3 of STIX2.1 when creating custom objects using the Extensions Definition.

So, that is how you are extending. So, it is kind of like you know when you do C++ or Java you know derivation of a class a subclass then you add additional methods and additional data right. So, same thing here you do additional properties to do this you can do this as a nested or you can do this as at the top level. So, you can use this extension to express use case specific objects or properties that go beyond what the technical committee could imagine while developing this standard. So, in the next iteration of stix standard some of this may actually make it to the standard right.

So, for now the good thing about JSON is parsing JSON is easy and flexible right. So, if you are parsing then you are basically parsing key value things. So, you can actually interpret that way yeah. yeah no you do not remove right so let us say you have a malware object right and then you say that in my organization this malware had this additional certain additional attributes see malwares vary from organization to organization same malware right so I might add some additional properties I am defining what those properties are and I am doing this. Now whoever is going to parse it they will when while parsing they will see that this is not in the original stix specification so I am going to have to interpret it right. So we will say take it as key value pair right and then they might put it into a database or data structure or something and then they can do whatever they want to do.

So producers and consumers of sticks are encouraged to use guidance provided by a particular section of this stix manual for creating custom objects and extensions. So we do not have to go into that level for us. So just to know that it can be extended.

Now, so we have meta objects also.



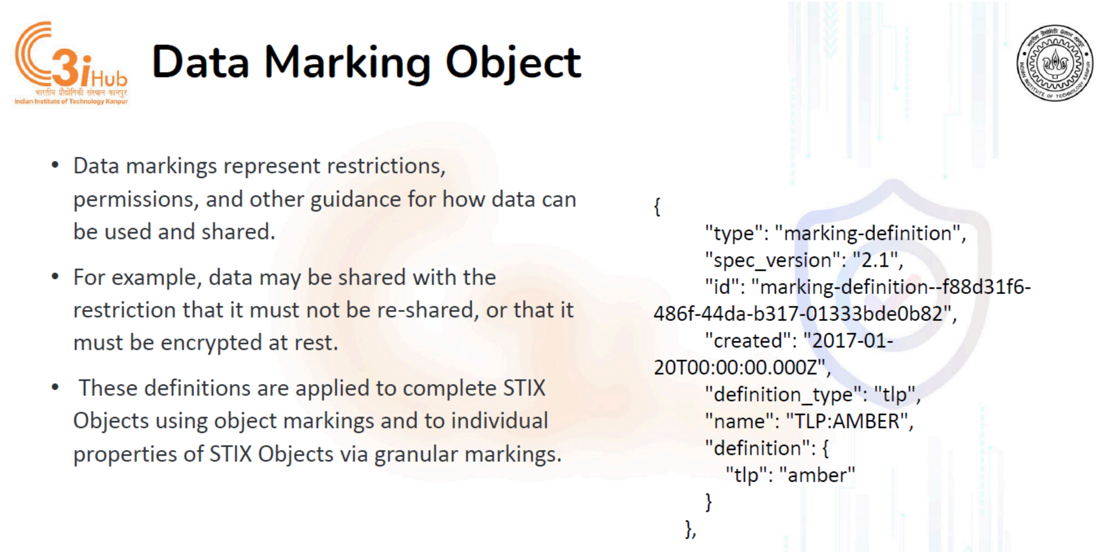
Meta Objects and Bundle

- Meta Objects are Data about the Data
- There are two key meta objects in the STIX 2.1 data model.
- Additionally, for ease of transferring data at the early stages of your investigations, there is also a Bundle object.
- Language Content Object:
  - The Language Content object represents text content for STIX Objects represented in languages other than that of the original object.
  - Language content may be a translation of the original object by a third-party, a first-source translation by the original publisher, or additional official language content provided at the time of creation.

So, for example, language content object. So, you may translate some threat intelligence and add language content. So, you might have noticed that some of the SDOs and SCOs had a language field. mostly see you see that there is a language field here right so so you can actually say in what language are you putting this information like for example in Korea or Japan all these things will be in Japanese or Korean and Japanese and stuff like that right. so so that is not very relevant to us but bigger information is that you might have also noticed that we have this in every object we had this which we did not describe so object marking reference and granular marking right so threat intelligence is often characterized by who I can share that information whether the information is copyrighted and so on right So, I may not I may say here is a stix file and I am sharing with you, but you cannot share this forward right.

So, there is this protocol called TLP right the traffic light protocol. Traffic light protocol basically if it is red then it is highly confidential you cannot forward it at all. If amber then within your organization you can forward and if it is green then you can forward to anybody outside also right. So as a creator of the threat intelligence in a source you might actually say that okay here I am usually it is used for specific things like where there is a for example identity identity SDO or location SDO or traffic you know this network traffic SDO or URL this kind of information which might lead to various issues you might want to put them with a traffic light protocol marking so and then.. Now there are two types of marking definition one is regular object level marking object marking another is called granular marking.

So, object marking basically says that the entire object entire SDO if the if there is a marking. So, see if the entire SDO is marked as let us say red then the entire object is not going to be you know forwarded but if you want to if you say this is green but you do some granular marking that you cannot for example well this one you may not want to share the name or something right so some specific property you cannot share so that will be in the granular marking now this marking information is not directly in the object but it is in the separate meta object marking called marking object data marking object.

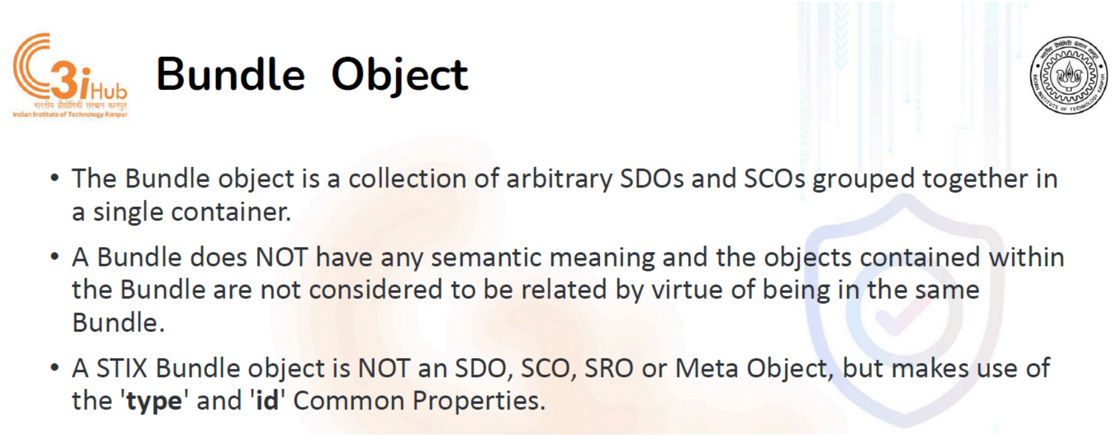


Data Marking Object

- Data markings represent restrictions, permissions, and other guidance for how data can be used and shared.
- For example, data may be shared with the restriction that it must not be re-shared, or that it must be encrypted at rest.
- These definitions are applied to complete STIX Objects using object markings and to individual properties of STIX Objects via granular markings.

```
{
      "type": "marking-definition",
      "spec_version": "2.1",
      "id": "marking-definition--f88d31f6-
486f-44da-b317-01333bde0b82",
      "created": "2017-01-
20T00:00:00.000Z",
      "definition_type": "tlp",
      "name": "TLP:AMBER",
      "definition": {
        "tlp": "amber"
      }
    },
```

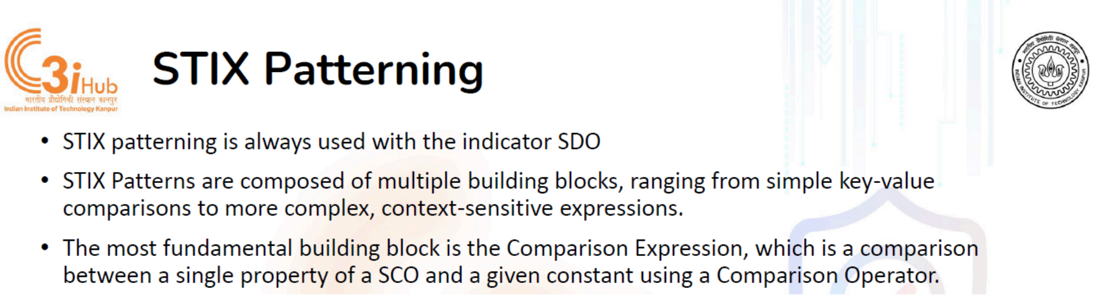
and then you will be relating this data marking object to the actual object right so you will create a data marking object like this and then you will say that this particular SDO or this particular report or this particular note has this marking so based on the marking the automated tools will then decide whether to forward it or whether to suppress it and so on. so, the last meta object is bundle object so bundle basically bundles all you know does not have any semantic meaning or context.



Bundle Object

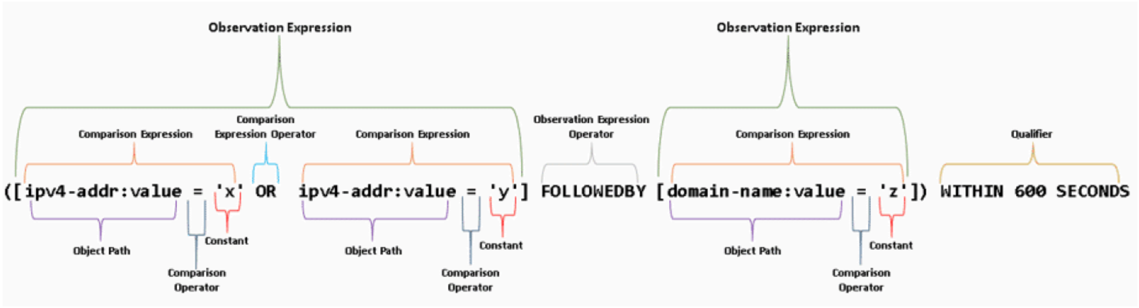
- The Bundle object is a collection of arbitrary SDOs and SCOs grouped together in a single container.
- A Bundle does NOT have any semantic meaning and the objects contained within the Bundle are not considered to be related by virtue of being in the same Bundle.
- A STIX Bundle object is NOT an SDO, SCO, SRO or Meta Object, but makes use of the '**type**' and '**id**' Common Properties.

So basically it puts together a lot of SDOs, SCOs, SROs and meta objects into a single bundle so that this entire bundle can be referenced with an ID. So usually useful for sharing information among the members of a particular group. So this is the STIX patterning language what it looks like. So, Stix patterning language is more than regular expression as you can see that it has connectives like OR, AND followed by this kind of stuff.



STIX Patterning

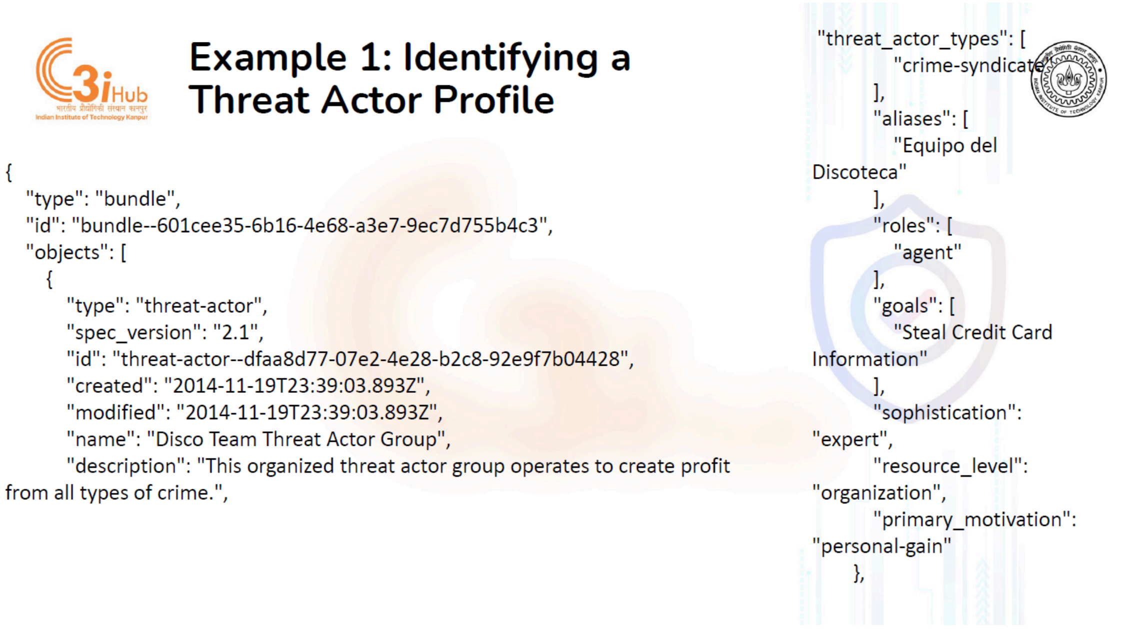
- STIX patterning is always used with the indicator SDO
- STIX Patterns are composed of multiple building blocks, ranging from simple key-value comparisons to more complex, context-sensitive expressions.
- The most fundamental building block is the Comparison Expression, which is a comparison between a single property of a SCO and a given constant using a Comparison Operator.



```
([ipv4-addr:value = 'x' OR  ipv4-addr:value = 'y'] FOLLOWEDBY [domain-name:value = 'z']) WITHIN 600 SECONDS
```

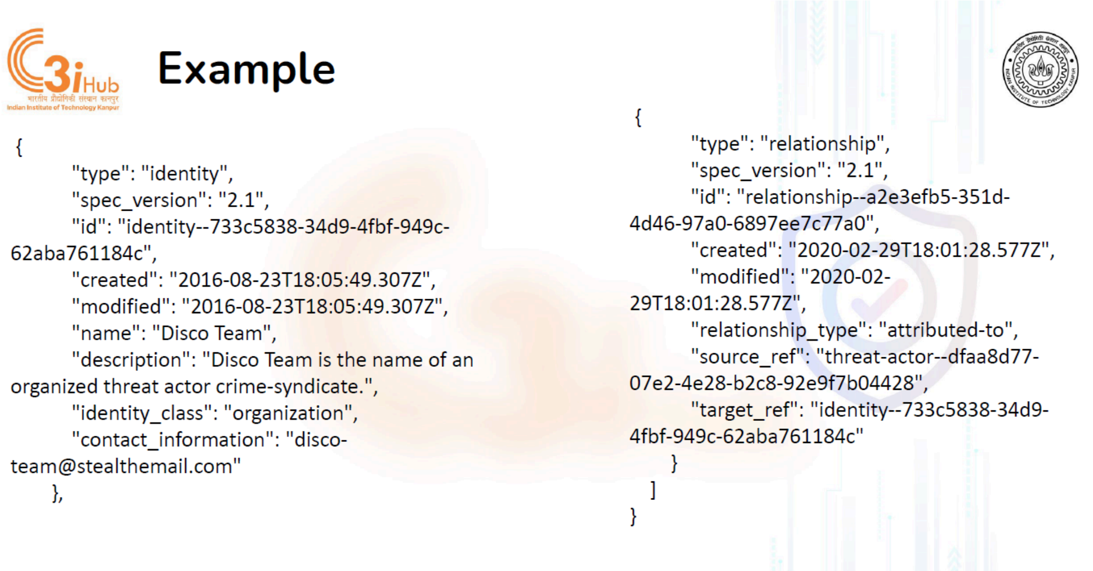
So, usually it is actually a way of expressing string patterns, but it is more than you know regular expression because it has all this different type of operators. So, that is what it is like. and we do not need to learn this patterning language here, but just to give you an idea. So, here we are saying that you know when you are writing a pattern you are writing that this IPv4 address or that IPv4 address followed by a particular specific domain name within 600 seconds.

So, if you see anything like that in the traffic pattern for example, then it is an indicator. So that is what you are saying. So you are saying an indicator. So it has some temporal aspect.



Example 1: Identifying a Threat Actor Profile

```
{
   "type": "bundle",
   "id": "bundle--601cee35-6b16-4e68-a3e7-9ec7d755b4c3",
   "objects": [
     {
        "type": "threat-actor",
        "spec_version": "2.1",
        "id": "threat-actor--dfaa8d77-07e2-4e28-b2c8-92e9f7b04428",
        "created": "2014-11-19T23:39:03.893Z",
        "modified": "2014-11-19T23:39:03.893Z",
        "name": "Disco Team Threat Actor Group",
        "description": "This organized threat actor group operates to create profit
from all types of crime.",
         "threat_actor_types": [
               "crime-syndicate"
           ],
           "aliases": [
               "Equipo del
Discoteca"
           ],
           "roles": [
               "agent"
           ],
           "goals": [
               "Steal Credit Card
Information"
           ],
           "sophistication":
"expert",
           "resource_level":
"organization",
           "primary_motivation":
"personal-gain"
       },
```



Example

```
{
       "type": "identity",
       "spec_version": "2.1",
       "id": "identity--733c5838-34d9-4fbf-949c-
62aba761184c",
       "created": "2016-08-23T18:05:49.307Z",
       "modified": "2016-08-23T18:05:49.307Z",
       "name": "Disco Team",
       "description": "Disco Team is the name of an
organized threat actor crime-syndicate.",
       "identity_class": "organization",
       "contact_information": "disco-
team@stealthemail.com"
     },
```

```
{
       "type": "relationship",
       "spec_version": "2.1",
       "id": "relationship--a2e3efb5-351d-
4d46-97a0-6897ee7c77a0",
       "created": "2020-02-29T18:01:28.577Z",
       "modified": "2020-02-
29T18:01:28.577Z",
       "relationship_type": "attributed-to",
       "source_ref": "threat-actor--dfaa8d77-
07e2-4e28-b2c8-92e9f7b04428",
       "target_ref": "identity--733c5838-34d9-
4fbf-949c-62aba761184c"
     }
   ]
}
```

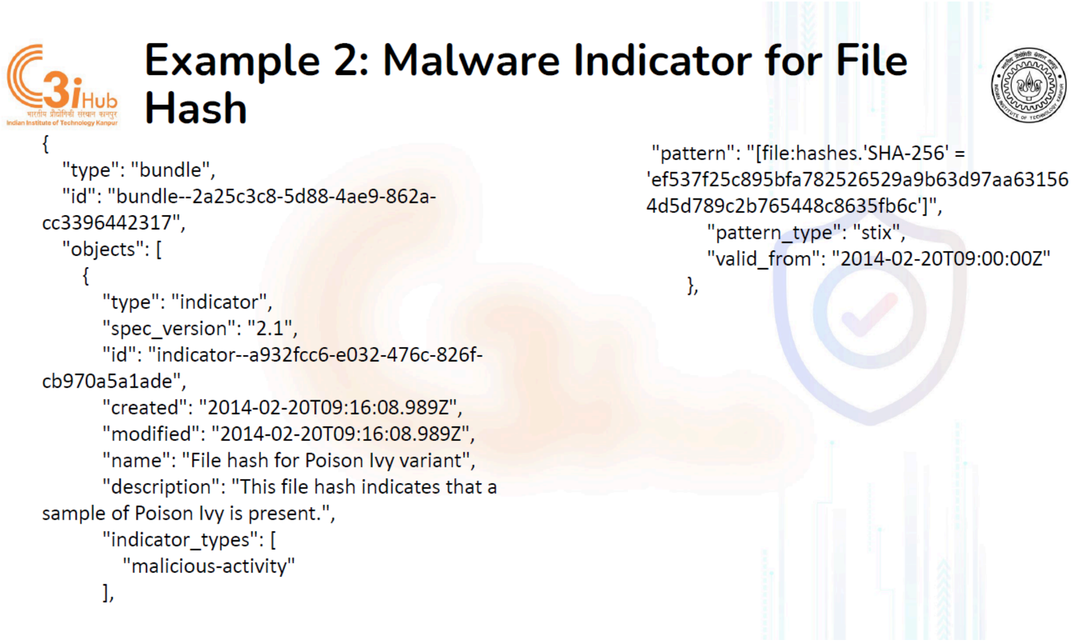
It has some sequencing aspect and it has Boolean operators. So it is kind of mixture of things. So just to give you examples, so here is a bundle object. It has a bundle ID. and within the bundle object many objects.

So, many SDOs and SCOs and SROs. So, here is an SDO within the bundle object. So, this curly parenthesis basically indicates the start of an object. So, this object has a type which is a threat actor spec version id created modified name description then it has what threat actor type it is. So, here it is an array it is a crime syndicate then it has aliases like whatever equipo del discoteca it has roles like agent goals the steel credit card information, sophistication, expert, resource level, organization, And, primary motivation is personal gain. So, this threat actor is more like a criminal than a national level threat actor or something.

But, this bundle contains more things. This is just a beginning of an array. See, you see we have not finished this array. This array has first object in that array is this. There is a comma here, which means this object is finished.

Now, the next object will start. So, here is an identity object. So, this identity object starts here, ends here and you have some information about that identity like the identity ID, description, name of the identity object, what class of identity it is, it is an organization, it also has a contact information. Now, the third object inside the bundle is the relationship object which has an ID and the relationship is attributed to. Here is a threat actor and here is an identity. So this threat actor is attributed to this identity. So if this identity is ever mentioned, it basically means this threat actor and any other information related to this threat actor will be relevant.

So this is how this relationship is this. So this is one example. Here is another example again given as a bundle. So, the objects in the bundle is an indicator and then other things. So, you see that this object is actually ends at that comma at the very end. So, it is an indicator It has an ID created, modified.

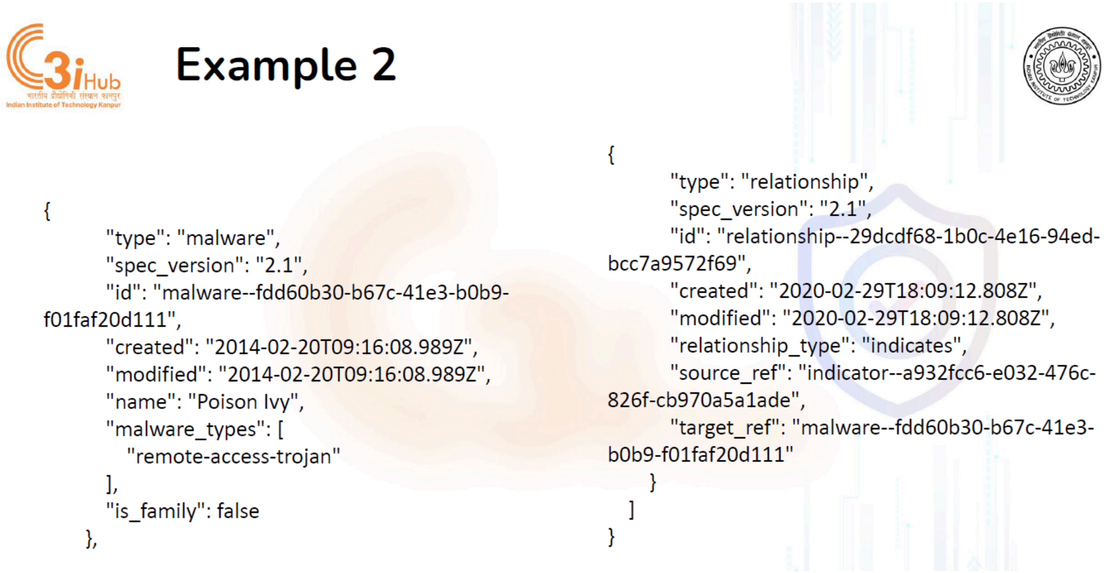


Example 2: Malware Indicator for File Hash

```
{
   "type": "bundle",
   "id": "bundle--2a25c3c8-5d88-4ae9-862a-
cc3396442317",
   "objects": [
      {
         "type": "indicator",
         "spec_version": "2.1",
         "id": "indicator--a932fcc6-e032-476c-826f-
cb970a5a1ade",
         "created": "2014-02-20T09:16:08.989Z",
         "modified": "2014-02-20T09:16:08.989Z",
         "name": "File hash for Poison Ivy variant",
         "description": "This file hash indicates that a
sample of Poison Ivy is present.",
         "indicator_types": [
            "malicious-activity"
         ],
```

```
 "pattern": "[file:hashes.'SHA-256' =
'ef537f25c895bfa782526529a9b63d97aa63156
4d5d789c2b765448c8635fb6c']",
       "pattern_type": "stix",
       "valid_from": "2014-02-20T09:00:00Z"
     },
```

It has a name. It is a file hash for poison ivy variant, a particular variant of poison ivy malware. This file hash indicates that a sample of poison ivy is present. an indicator type malicious activity now the pattern. So, pattern type is STIX pattern and you see that it is basically a pattern that says SHA 256 of the file is so it is valid from certain date.



Example 2

```
{
        "type": "malware",
        "spec_version": "2.1",
        "id": "malware--fdd60b30-b67c-41e3-b0b9-
f01faf20d111",
        "created": "2014-02-20T09:16:08.989Z",
        "modified": "2014-02-20T09:16:08.989Z",
        "name": "Poison Ivy",
        "malware_types": [
          "remote-access-trojan"
        ],
        "is_family": false
     },
```

```
{
        "type": "relationship",
        "spec_version": "2.1",
        "id": "relationship--29dcdf68-1b0c-4e16-94ed-
bcc7a9572f69",
        "created": "2020-02-29T18:09:12.808Z",
        "modified": "2020-02-29T18:09:12.808Z",
        "relationship_type": "indicates",
        "source_ref": "indicator--a932fcc6-e032-476c-
826f-cb970a5a1ade",
        "target_ref": "malware--fdd60b30-b67c-41e3-
b0b9-f01faf20d111"
      }
   ]
}
```

So, this is one object in this bundle we will go and see the next object.

So, there is an indicator object and here is a malware object. The malware object finishes in the comma here down on the left. So, malware name is poison ivy, it is a remote access trojan, it is not a family, it is just a single special case. Now, a relationship object relates. this malware to that indicator. So, it says indicates this that that indicated that we saw the hash that we saw indicates that the presence of this malware.

So, this is the relationship. So, this is now the entire bundle completes. So, this is a small example now marking. So, marking is example like we say that marking is for traffic light protocol or something like to say whether something can be shared, whether something has to be suppressed etcetera. So, you see that in this example we have again a bundle within the bundle there are objects. Within the objects array, first object is an identity and this is the Stark Industries name and it has an ID.

It is a defense sector industry. It has a contact information. Second object there, the opening bracket is missing on the top. No, actually it is there, but it is kind of hidden by the marking, the header marking.

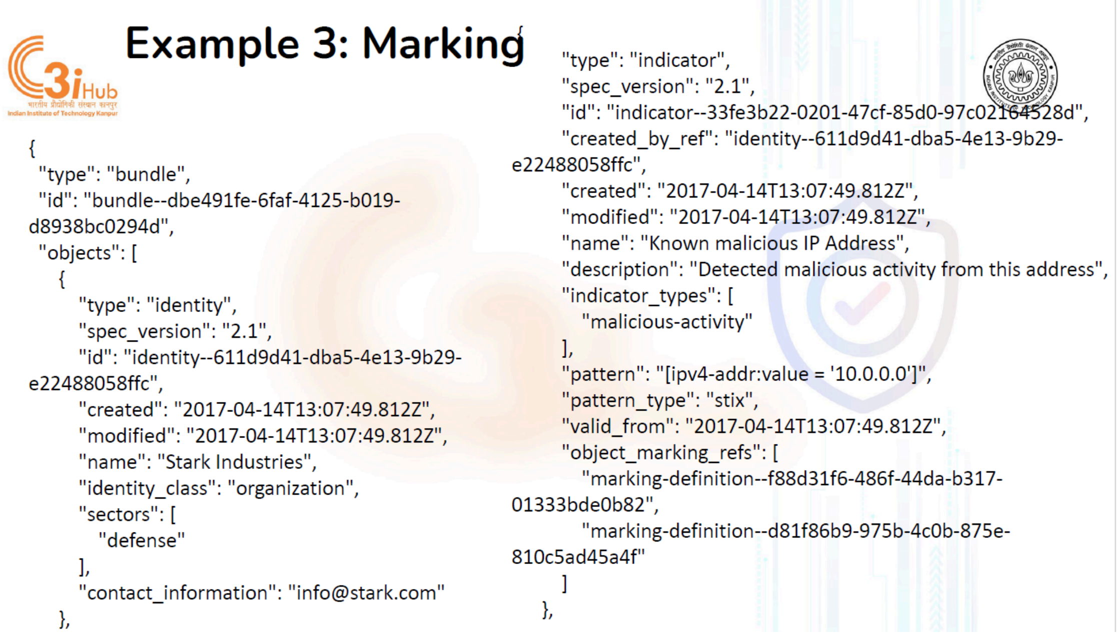
Indicator is actually known IP addresses. So, it is for there is a pattern IPv4 address is 10.0.0.0 and pattern type is stix valid from object marking reference. So, it is now referencing two markings which we will look at later, right. So, marking definition and marking definition they say, so it is saying something about this indicator that this indicator is not free to be shared, it has some markings. So, what let us see what those markings are.

So, marking definition first, marking definition says it is amber, so it can be shared within the organization. And then second one is saying that there is a copyright of this indicator to Stark Industries. So, that means that Stark Industries created this threat intelligence and they created that indicator object to let others know about what IP address can be seen for this particular malicious activity. but they have put some restriction on the sharing of that information. So, that is that is basically how it is written.

So, that is all I wanted to say about sticks and you have already seen that we have this stix viewer. So, you can go to the stix viewer and you can actually put one of the stix files there. For example, I can try to put this one that I had here if there is no mistake.

If there is a syntax problem, then it will not work, but I can try. So, this does not have a relationship object, I guess. Let us see. There is a relationship object. I do not know if I could not parse it properly or what. It is just showing two SDOs. One is indicator, another is the identity object or threat actor.

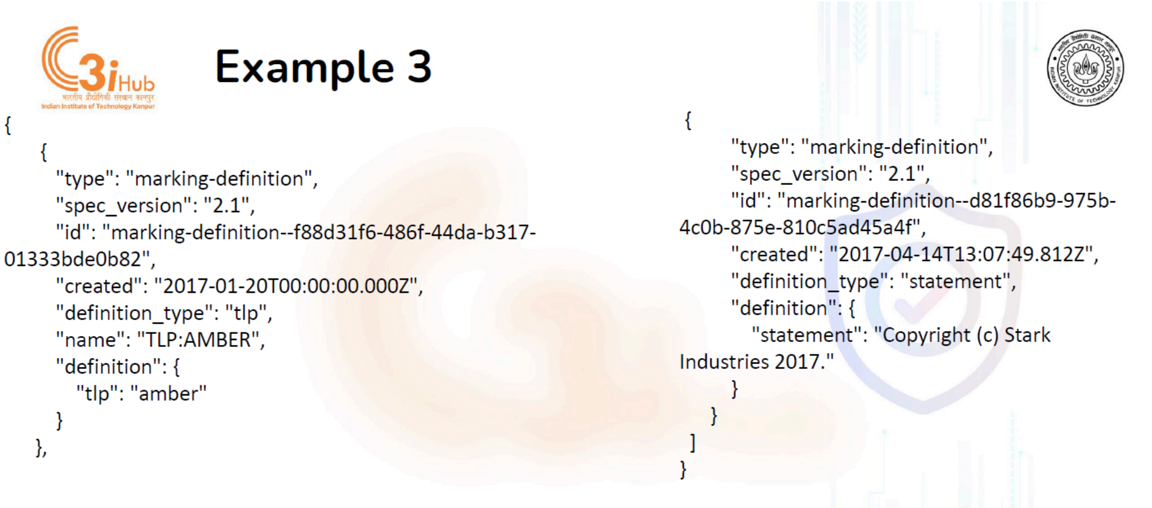
It is a threat actor identity object, but it is not showing the rest of the information. I will have to check, but when you for your homework when you write your stix file you can use this to actually visualize to check. So, any other questions? What? Pattern and bundle. No so bundle is a meta object it is for clubbing things together right so you are saying that like in C well C is not the right example but you know you cannot write standalone set of functions right so you have to put a main and in from the main the functions have to be called right so bundle is sort of like that the top of top level object within which you are putting an array of SDOs, SCOs and SROs right.



Example 3: Marking

```
{
  "type": "bundle",
  "id": "bundle--dbe491fe-6faf-4125-b019-
d8938bc0294d",
  "objects": [
    {
      "type": "identity",
      "spec_version": "2.1",
      "id": "identity--611d9d41-dba5-4e13-9b29-
e22488058ffc",
      "created": "2017-04-14T13:07:49.812Z",
      "modified": "2017-04-14T13:07:49.812Z",
      "name": "Stark Industries",
      "identity_class": "organization",
      "sectors": [
        "defense"
      ],
      "contact_information": "info@stark.com"
    },
{
      "type": "indicator",
      "spec_version": "2.1",
      "id": "indicator--33fe3b22-0201-47cf-85d0-97c02164528d",
      "created_by_ref": "identity--611d9d41-dba5-4e13-9b29-
e22488058ffc",
      "created": "2017-04-14T13:07:49.812Z",
      "modified": "2017-04-14T13:07:49.812Z",
      "name": "Known malicious IP Address",
      "description": "Detected malicious activity from this address",
      "indicator_types": [
        "malicious-activity"
      ],
      "pattern": "[ipv4-addr:value = '10.0.0.0']",
      "pattern_type": "stix",
      "valid_from": "2017-04-14T13:07:49.812Z",
      "object_marking_refs": [
        "marking-definition--f88d31f6-486f-44da-b317-
01333bde0b82",
        "marking-definition--d81f86b9-975b-4c0b-875e-
810c5ad45a4f"
      ]
    },
```

Now, each SDO or some of the SDO and SCO may have patterns in them right. Otherwise bundle and pattern has nothing. No, so report is different from bundle. So bundle is usually may contain a report, right. So bundle is basically the top level object in most STIX files, we put them as a bundle. Yeah, report will still be an SDO, so it will be inside a bundle.



Example 3

```
{
    {
      "type": "marking-definition",
      "spec_version": "2.1",
      "id": "marking-definition--f88d31f6-486f-44da-b317-
01333bde0b82",
      "created": "2017-01-20T00:00:00.000Z",
      "definition_type": "tlp",
      "name": "TLP:AMBER",
      "definition": {
         "tlp": "amber"
      }
    },
```

```
{
      "type": "marking-definition",
      "spec_version": "2.1",
      "id": "marking-definition--d81f86b9-975b-
4c0b-875e-810c5ad45a4f",
      "created": "2017-04-14T13:07:49.812Z",
      "definition_type": "statement",
      "definition": {
         "statement": "Copyright (c) Stark
Industries 2017."
      }
    }
  ]
}
```

So, I do not think that it can refer it I do not know, but most probably I mean ideally it should be able to reference id of another bundle right. So, because otherwise if you see that let us say I have some threat intelligence in some stix file and I want to, but See there is a bundle ID which means other bundles should be able to refer to this bundle. So similarly I would think that report should be able to also reference another bundle to just reference to a threat report, but I have not seen it because I am not using it on a daily basis. So those who are using STIX on a regular basis they can tell you more on that kind of nuances.

So, there are tools. So, normally you do not do this yourself. So, I will show you that, what was that tool? I was looking at it earlier today. Scout threat. So, scout threat is a tool which allows you to creation of Threat Intel. So, when you are creating this it will automatically generate those IDs and stuff. So, you do not do this manually very often you can, but then you have to know how to generate the IDs and stuff.

So, I think we are done with the stix. So, the reason why I wanted to cover stix is that if you go and work for security in an organization and they are using threat intelligence from NCIPC or certain etcetera you will encounter stix and taxi and all that. So, you are going to be familiar with stix and also you will be probably be able if you do your homework then you will be able to probably do some further processing of stix information in reach it with further information and so on. And then you also understand what are the components of threat intelligence, what is it that threat intelligence contains. So, threat intelligence contains mostly information about threat actors, malware, various indicators, and there are 18 types of observables, this kind of stuff. So, that gives you some basic idea about this.