Practical Cyber Security for Cyber Security Practitioners

Prof. Sandeep Kumar Shukla

Department of Computer Science and Engineering

Indian Institute of Technology, Kanpur

Lecture 26

Cyber Threat Intelligence Sharing - STIX Tutorial - Part 1

All right, good morning. So, now we are moving on to a new topic regarding threat intelligence right. So, threat intelligence is very important because an organization needs to know what are the different threats that might affect its network or infrastructure. And in order for it to know what kind of threats are currently active in the environment for a specific sector or specific nations or specific geographical location etc. They need to figure out what is going on and what are the indicators for those threats. Because threats usually means that attacks are happening otherwise how would I know that there are threats.

Of course, I can get some threat information from dark web and telegram groups and other kinds of places. chats and you know various kinds of exploits might be sold in the forums in the dark web and so on. And therefore, I might be able to also get some information about various malware that might be going to be used and so on or what kind of command and control URLs or command and control IP addresses or what kind of TTPs are going to be used for attacks and so on. So, this kind of information every organization needs to every organization needs to actually get this kind of information on a regular basis.

actually on a daily basis and there are companies which actually collect such information and they actually then share this kind of information and when they share this kind of information they might share this in natural language right. So, if you send it in natural language, what would happen is that the organization when they receive that threat intelligence they have to convert it into a machine readable form. So, this threat intelligence can be fed into various tools. For example, if I know that there are certain command and control URLs or IP addresses, I have to make sure that my firewall has been fed that information, that is a firewall can block those IP addresses or URLs and so on. Similarly, if I know that there are certain malware hashes being seen then I might want to send that information to all my end point detection or of course, the network intrusion detection systems so that they can look for those hashes.

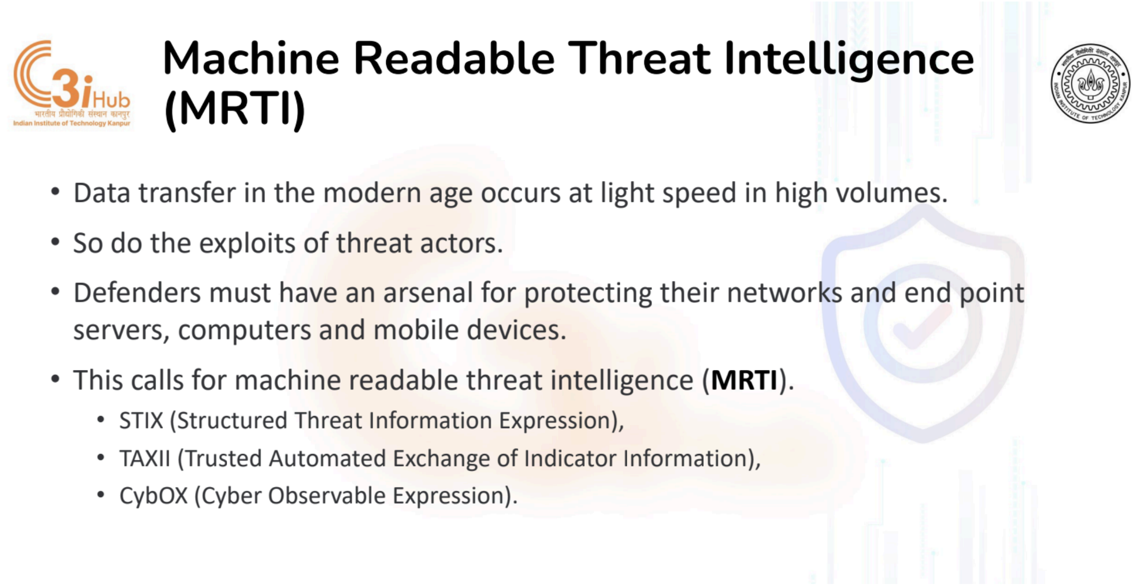
So, so making such information machine readable is you know quite a bit of work and most organizations may not have the right level of expertise or people to actually convert natural language reports of threats into machine readable form and that is how the this language this formalized language called STIX or sharing threat intelligence for sharing threat intelligence has been developed. And currently the version that is going on is STIX 2.1 and what we are going to do is to see what STIX is and what it looks like, what kind of data model it has and how to write threat intelligence information in STIX format. And the interesting thing is that not only they have developed sticks, they also have developed a protocol called taxi. So, the taxi servers.

So, a taxi is kind of like a server where the threat intelligence generators, that is companies that develop threat intelligence information, develop it in the STIX format and then they put it into the taxi servers and its subscribers. So, anybody who buys their threat intelligence will automatically communicate with the taxi servers to actually get the threat intelligence and have the automation to actually have the threat intelligence fed into all its necessary tools like firewalls and intrusion detection systems and so on. So, that threat intelligence is then processed and accordingly rules and configurations of those defense protection systems will be updated. So, this is when you go for threat intelligence companies where you buy the threat intelligence. There are also organizations such as CERT: computer emergency response team or CERT in India, it is CERT-IN.

There are also sector specific CERTs for example, there is CERT-FIN which is for the financial industry like banks and so on. There could be CERT power in fact there are CERT hydro, CERT thermal and CERT you know renewable this kind of CERTs are also there. These are sector specific CERTs. Now their job is also to generate threat intelligence based on any kind of research they do, any kind of threat intelligence information they receive from other organizations around the world, their peer organizations. Similarly NCIIPC, the National Critical Information Infrastructure Protection Center, also shares threat intelligence using STIX format.

So even if you do not subscribe to the threat intelligence from expensive threat intelligence companies like Recorded Future, etc., you can unit 42, etc., but you may still receive threat intelligence for free. from CERT-IN and other places. So this is a very common way in which organizations can receive threat intelligence.

And just by receiving threat intelligence you know is not enough you have to then act on it. So, if you use the STIX format then you most tools nowadays like firewall, if you buy a firewall from another company etc they actually speak the language of STIX. Therefore, they will be able to automatically process that information and accordingly change their rules or signatures and configuration etc as per requirement. So, that is why STIX is very important. There is a STIX which is maintained by a group called WESIS group and they have a website I will show you where you can find more information for those who are more interested in knowing about how threat intelligence is created and collected.

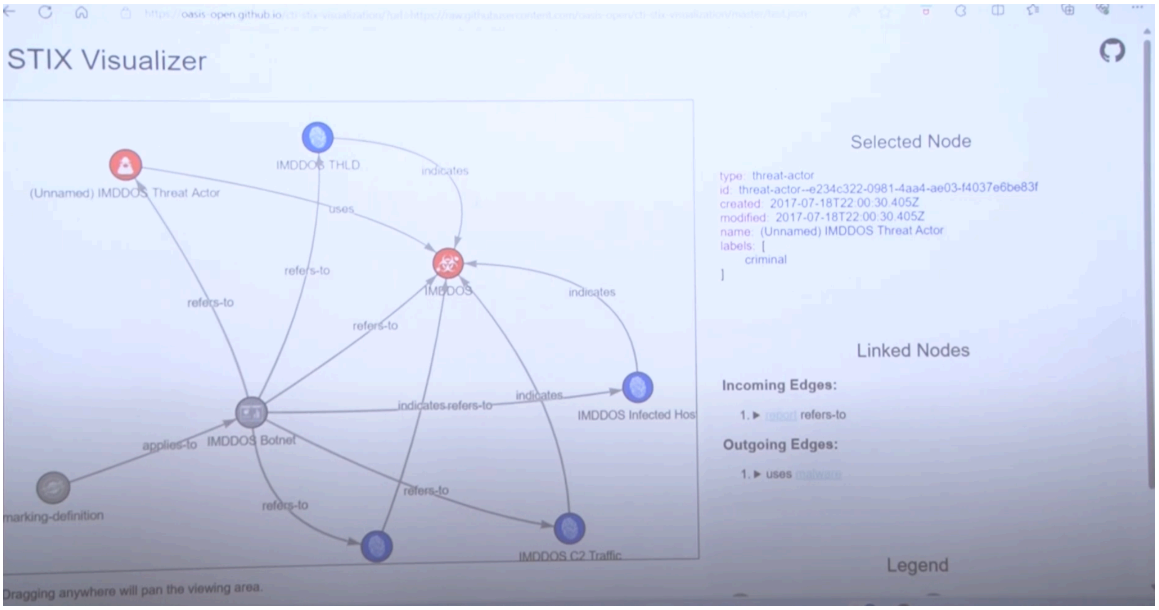


Machine Readable Threat Intelligence (MRTI)

- Data transfer in the modern age occurs at light speed in high volumes.
- So do the exploits of threat actors.
- Defenders must have an arsenal for protecting their networks and end point servers, computers and mobile devices.
- This calls for machine readable threat intelligence (**MRTI**).
  - STIX (Structured Threat Information Expression),
  - TAXII (Trusted Automated Exchange of Indicator Information),
  - CybOX (Cyber Observable Expression).

So, the main idea here is that you have to have machine readable threat intelligence right. So, or what we call MRTI, CTI cyber threat intelligence, TI threat intelligence these terms are very commonly used and MRTI means machine readable threat intelligence. So, the goal of this whole thing is that since data is transferred at lightning speed, the threat is also spreading at lightning speed and therefore I have no time to actually tell you in natural language that this be careful about this particular URL or IP address or this malware hash or this. kind of threat actor, this kind of TTPs are happening and then you will actually process that information and then act on it, it is going to be too late. So, therefore, the idea is that if you want to make this threat intelligence effective for helping out a lot of organizations, then you have to automate the process of sharing threat intelligence and that is the basic idea behind creating this language.

So, MRTI has 3 components, one is STIX, this is the structured the STIX stands for Structured Threat Information Expression, TAXI it is the Trusted Automated Exchange of Indicator Information and CYBOX is the Cyber Observable Expression, this is rather less this is in the MITRE you can find it in the MITRE website. taxi. So, taxi is the protocol for sharing threat information securely between a threat intelligence creator and threat intelligence consumer. Now, STIX aims to get a graphical model right. So, let me first show you what a STIX model looks like right.



STIX Visualizer

Selected Node

type: threat-actor
id: threat-actor--e234c322-0981-4aa4-ae03-f4037e6be83f
created: 2017-07-18T22:00:30.405Z
modified: 2017-07-18T22:00:30.405Z
name: (Unnamed) IMDDOS Threat Actor
labels: [
criminal
]

Linked Nodes

Incoming Edges:

1. ▶ report refers-to

Outgoing Edges:

1. ▶ uses malware

Legend

STIX Visualiser Link: https://oasis-open.github.io/cti-stix-visualization/

So, here is what we call a STIX visualizer right. So, STIX visualizer. So, here you see that I have let us see, sorry. So, I have the STIX file that describes a particular threat and here are the legends used in this graph. So, here you see that here I have, this is an indicator and this is an indicator.

I will explain what indicators are. This is an indicator. Now, this legend is for malware. So, this is malware and this legend where you have a person who is a threat actor. right and then we have a threat report.

So, it is a report and it is a marking definition. So, we will come to know what these things mean, but you see that here, I have a particular threat indicator, a particular type of traffic here. So, I have a particular type of traffic which is an indicator. Here I see C2 traffic the command and control traffic probably an URL or something and then here is an infected host right. So what is happening here is malware right.

So these indicators you see that this C2 is like if you find in your organization traffic going to this command and control server or if you find this infected infection or if you find this particular traffic threshold like this is a DOS threshold traffic then you know see all of them are pointing to this malware. So if you find these indicators you can kind of assume that this is the malware that is in your organization. And then you can also there is another indicator here which also has to be indicating this. Now this information is also saying that this particular threat actor in this case unnamed is actually using this malware to do this and this malware can be indicated by this indicator. So if you see this indicator you can kind of hypothesize that your system has been infected by this malware and this malware is associated with this particular threat actor.

And here is a report. So, the report is a top level object. Basically what it is saying is that this threat intelligence information is basically reporting. So, it is referring to a particular threat actor, it is referring to a particular malware, it is referring to certain types of indicators. So, overall this report contains all this information. And marking definition is basically something we will see later that whenever you share threat intelligence you may mark it by saying that this has this can be shared widely or this can be shared only within the organization, this can be shared within only within the or sector this kind of stuff.

So, there is a marking associated with this report which basically says who it can be shared with. So, what this tool is called the STIX viewer you can use you can take a STIX file and use this viewer to actually see this graphical representation of this threat information. Now, in some cases this is a very small report, right. It has one threat actor, four indicators and one malware, right. But in many cases you will have many other elements to this.

It can be part of an attack pattern. It may be part of an intrusion set. it may have a campaign associated with it and so on. So, sometimes this picture will be very very complex right. So, this is a simple one and if you can see that if I select a particular node for example, if I select this it is showing me the structured information.

The structured information has multiple different things like it has a type in the type of this object is that it is an indicator. it has an id, this id is required to uniquely identify this. Then I have the creation time, I have the creation time, I have the modification time, I have the name, I have some labels and then I have some description. This is a textual description. It says when this indicator is valid from.

and then it says which kill chain phases this particular indicator is visible right and then it says a pattern. So, this is since this is an indicator it has a this is basically a URL. So, an URL is an indicator. So, as an URL this indicator has, I think I am now looking at this one right.

Now this is a different one. This is a Windows registry key right. So this registry key will tell you that your host has been infected right. So this structured description is what you need to know to write this indicator in a format that is not only machine readable, but it is also unambiguous. That is, any other tool that is aware of STIX language will be able to process this information and accordingly do the necessary configuration changes so that it can detect this indicator and so on. So, that is the overall look of this, but what I want to do, I want to teach you the language of STIX for 3 reasons.

One is of course that you learn that threat intelligence can be actually made machine readable. and unambiguous so that it can be processed by algorithms to change the posture of firewalls and intrusion detectors or endpoint agents and so on. So, that they can be better at they can be more current on the threats that they might be fighting right. So otherwise they will be or they have to be seen the other way other way would be to hard code the indicators inside your tools right. So for example you can say ok I will put all the firewall rules in the beginning And then if I have to change any rule, then I have to bring it down and then restart it, right.

Change the new rules, put the new rules and then restart it. But that is not practical because you cannot take down the protection software and So, you have to actually dynamically be able to process this kind of information and change the posture of that software or equipment to actually do better at fighting the threats that are new that are coming as threat intelligence you know in real time. So that is the idea so I that is one reason why STIX is an important concept that everybody needs to know if they are going to be in charge of protecting your infrastructure. Plus you can get STIX information not only from vendors who are going to charge you money for subscription to their taxi service but also you can subscribe to the taxi servers and sector specific CERTs and ISACs and various other voluntary organizations or government regulatory organizations who share threat information. The second thing is that you get to know that this kind of language, this structured language has a very important role in all of software engineering including cyber security tools right.

Because, nowadays you will see that even configuration files are created using structured JSON JSON you know using JSON syntax basically right. So, in this case also it is a JSON syntax that is being stylized for this specific purpose. to create the language for STIX right. So, it is basically a data model and then the third thing is the third reason is of course that I want to give you a homework assignment in which you have to take a threat report and write the corresponding STIX correctly. So, that is the third reason why you are doing this right.

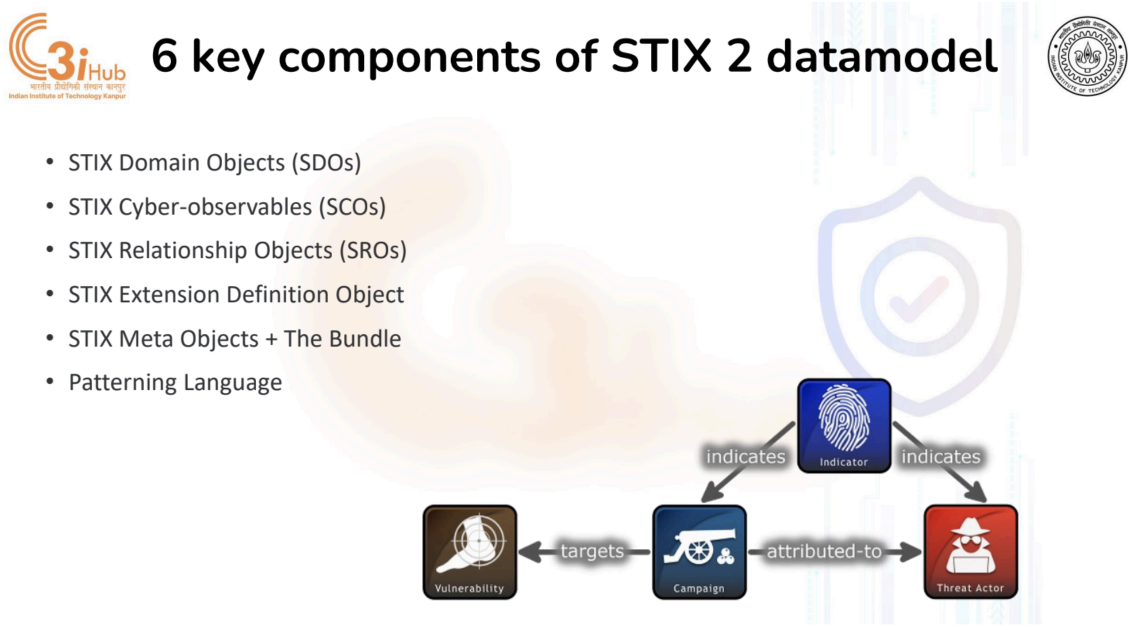
Here are your different types of objects right. So, we already saw this picture right. So, like we have an indicator which indicates something this is like it may indicate a presence of a threat actor, it may indicate the presence of an attack campaign And this campaign may be attributed to a threat actor like for example, APT 28 for example. And then you can also say what vulnerabilities it is targeting, right.

So, there are various types of objects. For example, here you see you have an indicator object, you have a threat actor object, you have a campaign object, you have a vulnerability object and so on, right. So, these are different types of objects. and each object can be described in a certain fashion right with certain attributes. So now these components of the STIX model first thing are called STIX domain objects.

So we will see what these domain objects are. For example campaign is a domain object, indicator is a domain object, threat actor is a domain object. So these are specific types of objects. There is also another object called cyber observables, anything that you can observe like for example, a file or a URL or something or an email message etc., these are cyber observables. And then you have relationship objects, relationship objects usually relate the domain objects to the cyber observables or maybe it can also relate to domain objects or to I guess observable objects.

There is also an extension definition object this is for because this is kind of object oriented. So there is a derivation process by which you can extend an object. So that is there. There is also meta object and bundle that is when all the objects for a specific threat intelligence have been created you put them in a bundle. So there are some meta objects and bundle is the top level object.

And then there is a patterning language like if you like regular expressions. So, this is a little more than a regular expression. So, there is a patterning language. So, these are 6 components of the STIX 2.

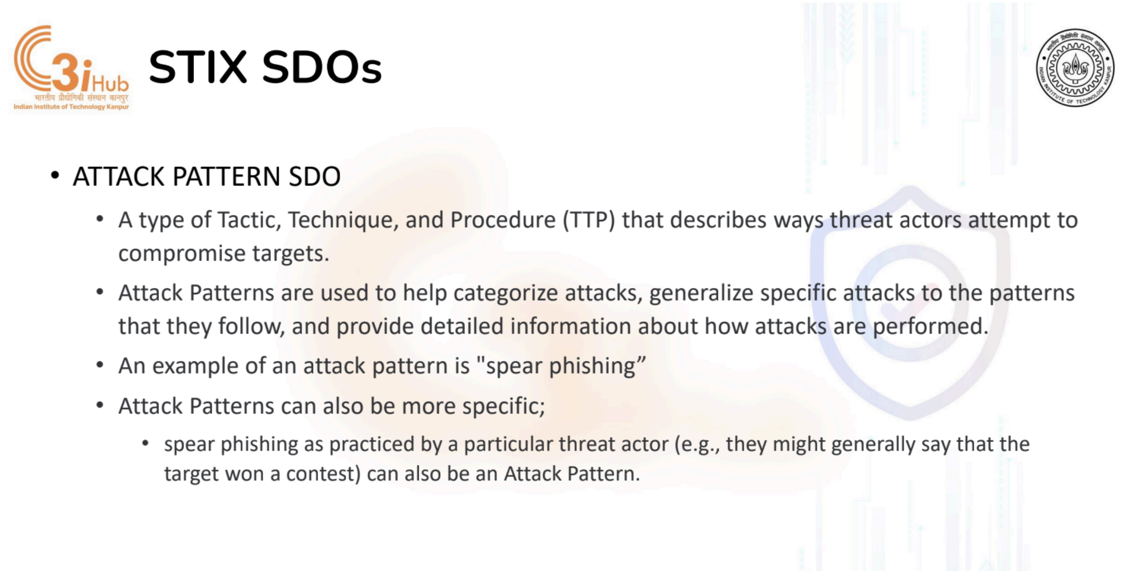


6 key components of STIX 2 datamodel

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

1 data model. So what we are going to do now is to actually look at the various domain objects because they are the most important part of the STIX you know data model and

these domain objects I am describing are in alphabetical order. So it is not like I am talking about an attack pattern object. First, it means that the attack pattern object is the most important object, nothing like that. I am just going through, I basically took this from the manual and the manual basically goes through all these object descriptions in an alphabetic order. So attack pattern, right. So an example of an attack pattern is spear phishing, right.

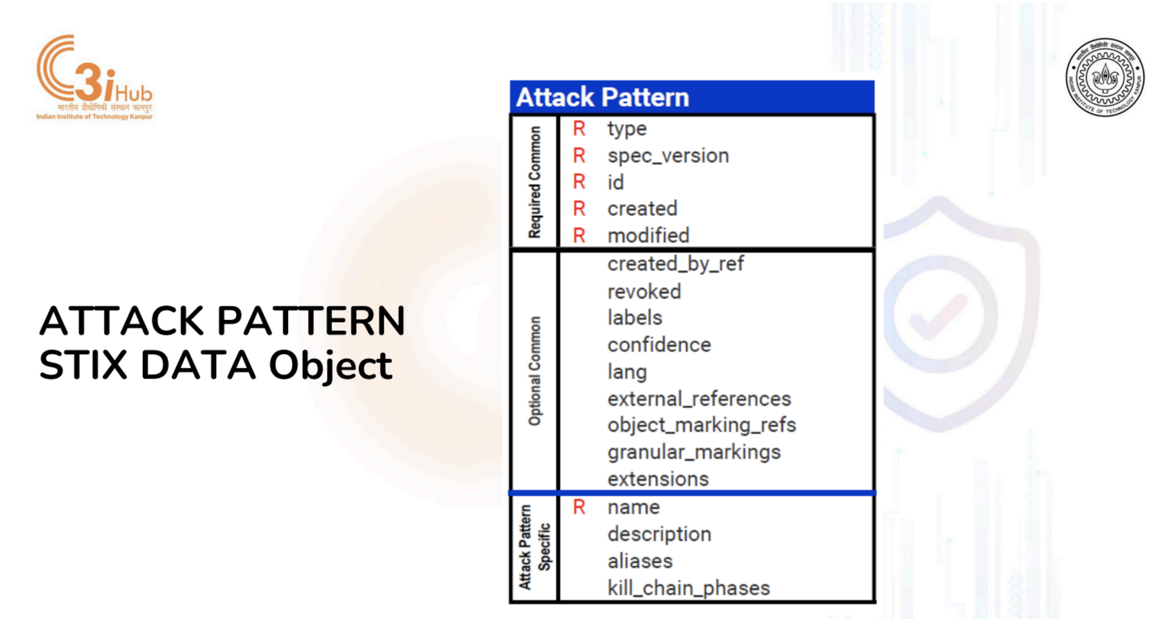


STIX SDOs

- ATTACK PATTERN SDO
  - A type of Tactic, Technique, and Procedure (TTP) that describes ways threat actors attempt to compromise targets.
  - Attack Patterns are used to help categorize attacks, generalize specific attacks to the patterns that they follow, and provide detailed information about how attacks are performed.
  - An example of an attack pattern is "spear phishing”
  - Attack Patterns can also be more specific;
    - spear phishing as practiced by a particular threat actor (e.g., they might generally say that the target won a contest) can also be an Attack Pattern.

So, spear phishing is an attack pattern or it may be a DDoS may be an attack pattern. So, when you might describe an attack pattern right. So, you can say an attack pattern is a type of TTP that describes a way. a threat actor attempts to compromise targets. So, I want to capture what it is that this particular actor does.

So, I can describe that as an attack pattern object. Attack pattern is used to help categorize attacks, generalize specific attacks to patterns that they follow and provide detailed information about how attacks are performed. So, we will see an example. So spear phishing would be an attack pattern, but you can also have more specific attack patterns. For example, a spear phishing as a practice by a particular threat actor, right. For example, they use a gen. Maybe a particular threat actor always uses a lottery winning type of phishing message.



ATTACK PATTERN
STIX DATA Object

Attack Pattern		
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
Attack Pattern Specific	R	name
		description
		aliases
		kill_chain_phases

So that could be a more specific attack pattern if I want to be more specific. So here is what the attack pattern object requires. So if I want to describe an attack pattern, I can describe the attack pattern with these attributes right. So attributes what is happening so I have to see I have to tell the values of these attributes right. So those of you who know JSON in JSON I can basically write this colon the type a string that basically describes this type spec version you can say for example colon the string that describes the spec version in this case this is tics 2.

1. ID of the attack pattern, the ID has to be a unique string identifying this attack pattern object. Why? Because if I am in a relationship object if I want to describe that this attack pattern is used by so and so threat actors. There is also a threat actor data object. So I have a threat actor data object and I have the attack pattern data object.

I have to relate the two. So I need this unique ID for this attack pattern to do that relationship. These are information like when was this object created, if it has been modified since those things. R here means that it is required. So if I want to create an attack pattern object, I must fill in these attributes and these attributes.

It has to give it a name, right? Other ones are optional. For example, created by whether it has been revoked, labels, confidence with which this attack pattern is being put out as a threat intelligence information, language associated with this attack pattern, some external references it might give you, additional documentation references to by using an URL. Object marking references this is about as I said that you know about marking has many different usage, but in this case it may be about who it can be shared with, how widely it can be shared, there may be more granular marking and there may be an extensions in case there will be a derivation from hierarchical derivation from this object. And then here you can give a description as a string. You can give some aliases for this attack pattern and then you can also describe the kill at least the kill chain phases in which this attack pattern has been used right.

So, all this information can be put into a JSON format, yes. At least locally unique right, globally you cannot do right. So, locally at least it has to be unique. Correct in what sense? Now the taxi server actually has authentication, encryption and all that stuff. Now the integrity of these STIX files from the threat intelligence company is their responsibility.

So you cannot guarantee this here. Because they might keep a hash of every file and continue to check and all that stuff. But that is their responsibility. For you it is difficult to check. I mean you will not be able to check whether it has been tampered with since its creation. No, so two companies might give you the, see if they created their own threat, they might also have derived it from the let us say CERT, US CERT, right.

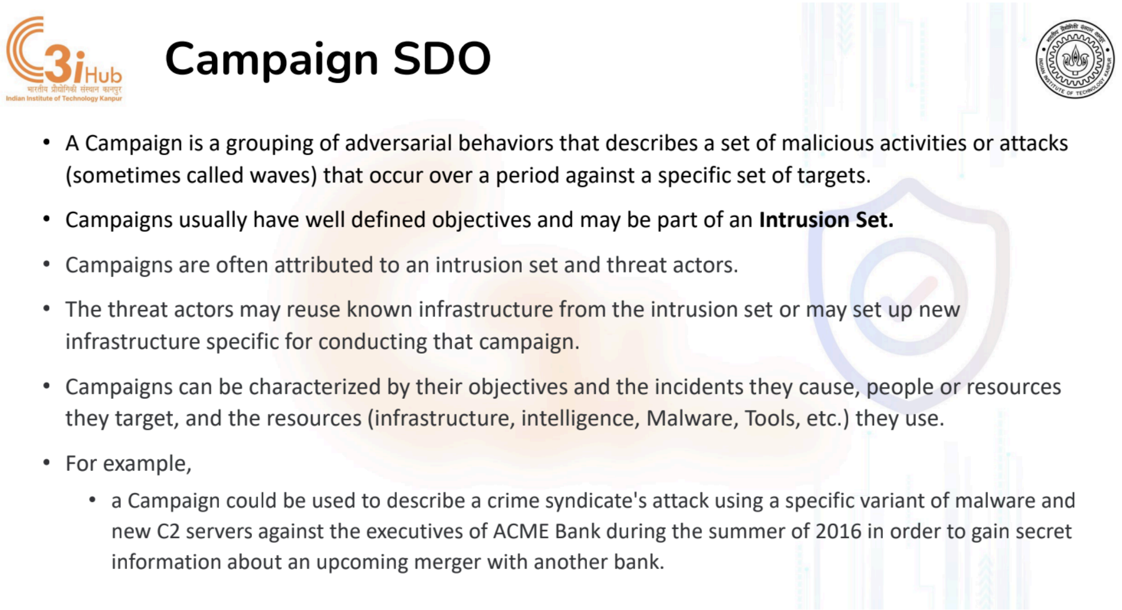
In that case they may have the same ID and all that stuff. But in case they have actually created it on their own, it is unlikely that IDs will match, right? In fact, to you, let us say two companies, you have subscribed to two companies and they are actually describing the same attack pattern. But you will not know that they are the same attack pattern, you will treat this as two separate threat intelligence. later on by now this by itself the attack pattern is not very useful right. What will happen is that this attack pattern will be related to some indicator objects.

The only way you can use the threat intelligence in your system in your organization is through the indicators. See if you see that you know indicators could be a CNC URL, it could be malware, it could be a registry change, it could be a particular type of file or hash value etc these are indicators right. So, let us say let us say one company saying that when you see these indicators that are associated with this attack pattern and this attack pattern is associated with a threat actor let us say APT 28 right. you go to another company, let us say Microsoft from which you again got a STIX and you saw some indicators and then using that threat intelligence you will see that if you see the same indicators you will relate that to a particular attack pattern ID which is associated with fancy bear right.

Now fancy bear and APT28 are the same. right is considered to be the same. So, later on that part you have to do manually right. So, when you are interpreting when you are catching a particular attack pattern in your system obviously you are not then doing automation you are then in the incidence response phase right. At that point when you see ok I have threat intelligence that is telling me that I have indicators of fancy bear and I also have indicators of APT28. then I will see whether they are the same or I am now being attacked by two different threat actors. And at that point you will consult Google or whatever or companies that will help you out and they will say this is the same.

But at the same point in time you may be attacked by two different threat actors as well right. So, the idea is that all this threat with all the threat intelligence is doing is increasing your capability to associate indicators to particular threat actors or particular attack patterns. And then the rest of the incident response activity is separate so that this thing does not help. This thing only helps you use the indicators and know what indicators to look for because indicators continue to evolve right. Like you know today you have some indicators that some C2C same threat actor may actually next week.

change their C2C IP addresses right which they do. So, unless you are subscribing to a feed like this you will not know that right. So, in that case you will see a traffic to a different IP address and you will say this is not in my threat intelligence. So, I am not going to do anything about it to avoid the need to have continuous updates of threat intelligence.



Campaign SDO

- A Campaign is a grouping of adversarial behaviors that describes a set of malicious activities or attacks (sometimes called waves) that occur over a period against a specific set of targets.
- Campaigns usually have well defined objectives and may be part of an **Intrusion Set.**
- Campaigns are often attributed to an intrusion set and threat actors.
- The threat actors may reuse known infrastructure from the intrusion set or may set up new infrastructure specific for conducting that campaign.
- Campaigns can be characterized by their objectives and the incidents they cause, people or resources they target, and the resources (infrastructure, intelligence, Malware, Tools, etc.) they use.
- For example,
  - a Campaign could be used to describe a crime syndicate's attack using a specific variant of malware and new C2 servers against the executives of ACME Bank during the summer of 2016 in order to gain secret information about an upcoming merger with another bank.

So then the next SDO is campaign SDO. So campaign SDO is basically a grouping of adversarial behaviors that describes malicious activities or attacks sometimes called waves that occur over a period against a specific set of targets.

Now campaigns usually are part of what is called an intrusion set, intrusion set. So let us say APT 28, right. So APT 28 did a campaign. during the covid time by using a supply chain attack on solar wind right.

So, all of us remember solar wind attacks. So, that was APT 28, but APT 28 also does many other attacks right. So, APT 28 is not just doing that solar wind attack. So, if I want to have threat intelligence about APT 28. I may describe an attack pattern that APT 28 is using for the solar wind attack. In that case it was a supply chain compromise right and they used a specific malware.

Tomorrow APT 28 is using a different set of malware and different C2 infrastructure. So, with a different attack pattern they might be doing spear phishing as well right. So, I have multiple attack patterns associated with APT 28. But, also I have different campaigns associated with. So, SolarWinds campaign is different from another campaign done by APT 28 and there are probably hundreds of campaigns of APT 28 including on the Ukraine during the Ukraine war right.

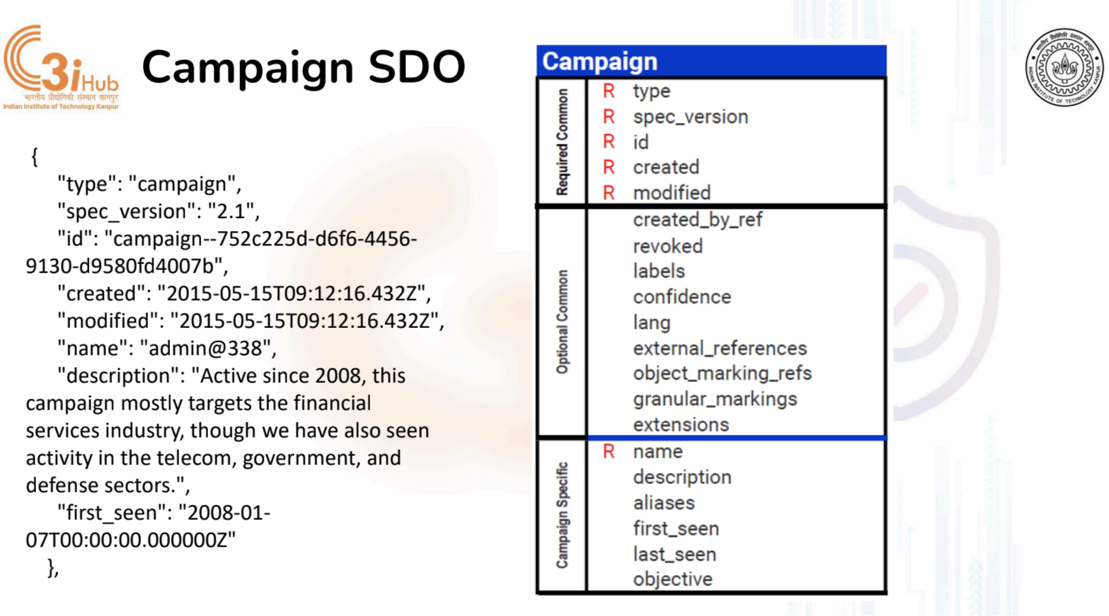
So, I will describe each of these campaigns separately. Then all these campaigns may come as part of what we call an intrusion set object. Intrusion set contains multiple different campaigns which is now associated with APT 28. So APT 28 will now be associated with an intrusion set which contains multiple campaigns and each campaign may contain multiple attack patterns and a multiple attack each attack pattern may contain multiple indicators. So, this is how the entire thing is.

So, now you might say what good it is, because all I need is indicators right. Why do I need to know whether these indicators are part of a particular attack pattern or particular campaign or intuition set? I might as well just get the indicators and I just stop banning those indicators. So, if I see a particular C2 traffic which I know is an indicator for certain APT I will just ban that traffic and if I see a particular malware I will quarantine that malware, if I see a particular IP address I will know to stop that IP address and so on. The reason is that eventually you need visibility about what is happening in your system right. They say the indicators suppose you only know the indicators right and you are being attacked by some group of thugs sitting in Noida versus APT 28 right. You want to know what the indicators I am seeing are, I know it is an attack right, I am going to stop those IP addresses and so on.

But I also want to know what is the situation with respect to me right. I mean am I being targeted by some not so sophisticated thugs sitting in some place Noida or some place or am I being attacked by the most resourceful attacker in the world you know one of the most resourceful attackers in the world APT 28 right. So, I need additional information not because that will help me automate. So, the only thing that helps me automate is the indicators mostly right. But this additional information enriches me, enriches my incident response capabilities and my you know ability to understand, respond and recover right and communicate.

For example, if I am getting attacked by APT 28. I should be very careful because that means that for some reason my business is in the target of a nation state attacker right versus if my business is a target of a regular cyber criminal right. So, that is why this enriched information of threat intelligence will help me to actually know what is going on inside my system and that is why this attack pattern campaign etc are useful. So, campaigns can be characterized by their objectives and incidents they cause people resources, the target etc. So, for example, this is 2016 ACME Bank.

So, a particular crime syndicate used particular C2 servers and a specific malware. to attack ACME bank during 2016 summer and they were and the objective was not to get money or something they were trying to get secret information about an upcoming merger with another bank so that they can do insider trading right. So that was a campaign right that was a specific campaign. So now here is what it looks like. So here is a campaign, this is a spec version, id, you see the id to make the id unique there is a randomized string generation. Usually if you have a software that helps you software editor for sticks creation, that will help you to do this unique ids.



Campaign SDO

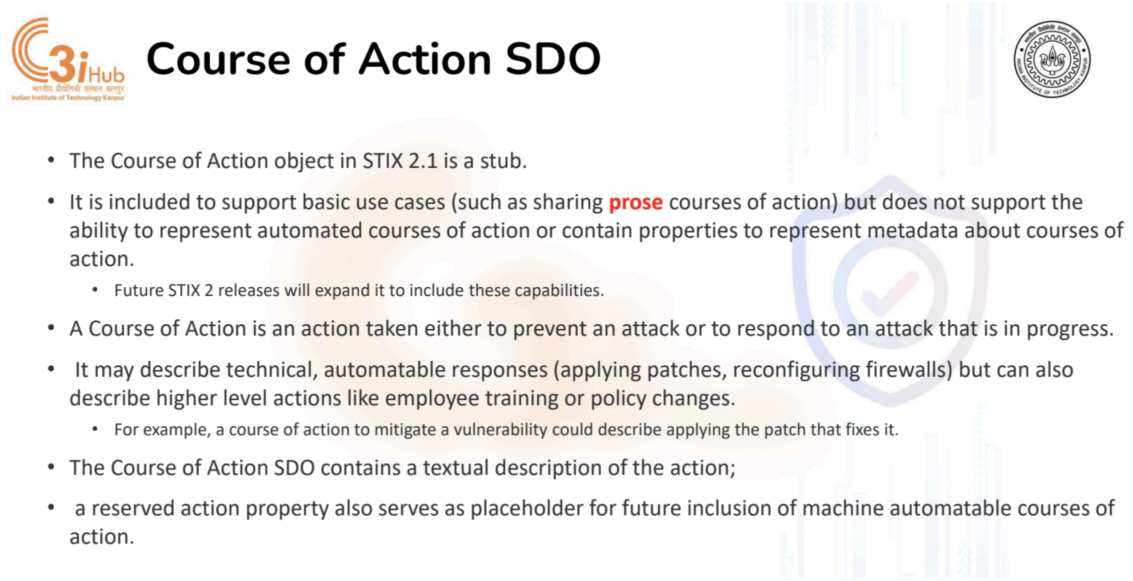
```
{
    "type": "campaign",
    "spec_version": "2.1",
    "id": "campaign--752c225d-d6f6-4456-
9130-d9580fd4007b",
    "created": "2015-05-15T09:12:16.432Z",
    "modified": "2015-05-15T09:12:16.432Z",
    "name": "admin@338",
    "description": "Active since 2008, this
campaign mostly targets the financial
services industry, though we have also seen
activity in the telecom, government, and
defense sectors.",
    "first_seen": "2008-01-
07T00:00:00.000000Z"
  },
```

Campaign		
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
Campaign Specific	R	name
		description
		aliases
		first_seen
		last_seen
		objective

creation date, modification date, etc., name and this particular campaign has been named admin at 338. So, this is a Chinese threat actor and there is a description which is optional where it says what it is. First scene is the date, the last scene is not there, the objective is not there, but you can put this additional information if you have them, right? But these are ones you have to provide.

So, when this threat intelligence comes, so campaign by itself will not come to you, right. So, campaigns will come with corresponding attack patterns, corresponding threat actors, corresponding indicators and all that stuff right. So this is just showing you a fragment of a STIX file. So nobody is going to send you a campaign SDO as threat intelligence without any indicator or anything right because it is not going to be useful for you if you just get this.

So now there is another SDO called course of action. The course of action SDO is thought of as a way to provide automation for what to do when an indicator is seen right.



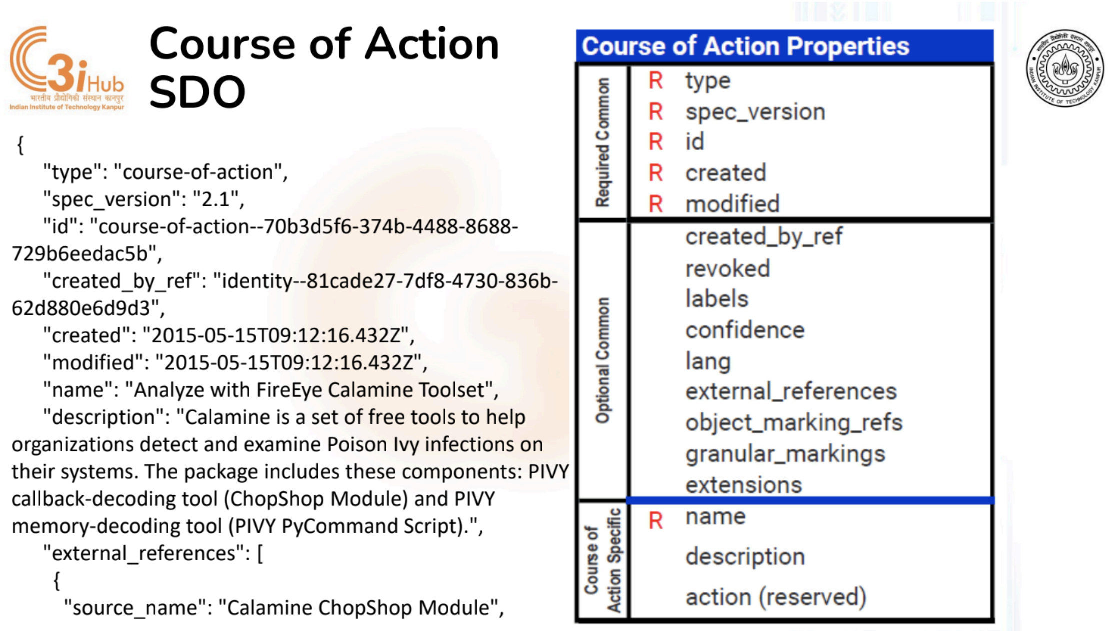
Course of Action SDO

- The Course of Action object in STIX 2.1 is a stub.
- It is included to support basic use cases (such as sharing **prose** courses of action) but does not support the ability to represent automated courses of action or contain properties to represent metadata about courses of action.
  - Future STIX 2 releases will expand it to include these capabilities.
- A Course of Action is an action taken either to prevent an attack or to respond to an attack that is in progress.
- It may describe technical, automatable responses (applying patches, reconfiguring firewalls) but can also describe higher level actions like employee training or policy changes.
  - For example, a course of action to mitigate a vulnerability could describe applying the patch that fixes it.
- The Course of Action SDO contains a textual description of the action;
- a reserved action property also serves as placeholder for future inclusion of machine automatable courses of action.

Right now in the current version it does not have the capability to provide automation instruction. So it only provides pros, pros information about what course of action to take when you see a particular campaign or when you see a particular attack pattern or something. So you can give a textual description of what course of action to take when you see something. But in the future it is supposed to be containing instructions for automatable responses like applying patches, reconfiguring firewalls etc right. So, right now the firewall company has a responsibility to automate.

So, when it gets a STIX file it automates certain things. Or if it wants to automatically block or something it is the firewall company that will give that as a feature. This is not part of the language. The language does not say anything about what the firewall company should do. So, every firewall company will do different things right in response to finding a particular indicator.

So it is a textual description of action. So it is a reserved action property that also serves as a placeholder for future inclusion of machine automatable courses of action. So courses of action, here is a SDO that has a course of action type. ID created by creation date, modification date, name, it says analyze with FireEye Calamine toolset. See, it is not giving you a script to do so, it is just saying so. So eventually your intrusion detection system might when this course of action will be associated with a particular indicator your intrusion detection system might flash to you that this is what you should do right that depends on the intrusion detection tool vendor.



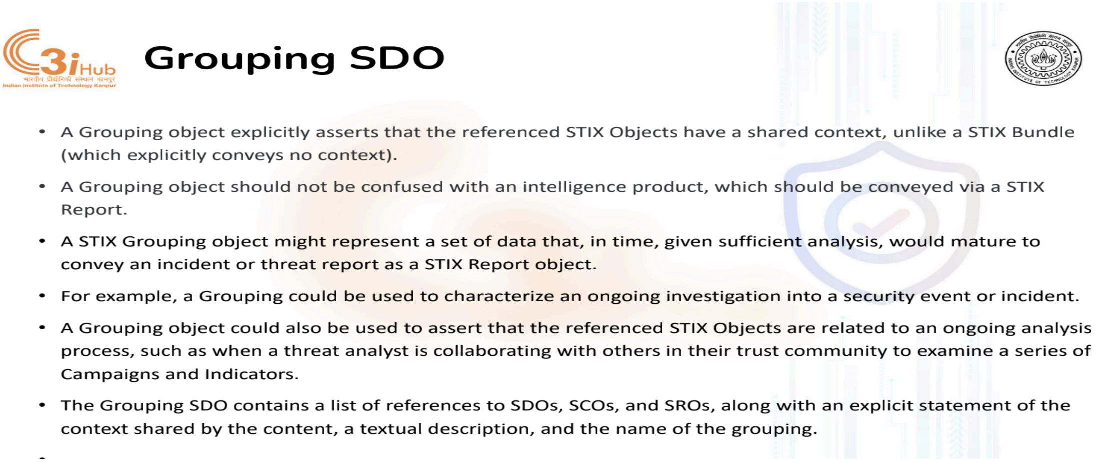
Course of Action SDO

```
{
    "type": "course-of-action",
    "spec_version": "2.1",
    "id": "course-of-action--70b3d5f6-374b-4488-8688-
729b6eedac5b",
    "created_by_ref": "identity--81cade27-7df8-4730-836b-
62d880e6d9d3",
    "created": "2015-05-15T09:12:16.432Z",
    "modified": "2015-05-15T09:12:16.432Z",
    "name": "Analyze with FireEye Calamine Toolset",
    "description": "Calamine is a set of free tools to help
organizations detect and examine Poison Ivy infections on
their systems. The package includes these components: PIVY
callback-decoding tool (ChopShop Module) and PIVY
memory-decoding tool (PIVY PyCommand Script).",
    "external_references": [
     {
      "source_name": "Calamine ChopShop Module",
```

Course of Action 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
Course of Action Specific	R	name
		description
		action (reserved)

And then it is giving a description that Calamine is a set of free tools to help organizations detect and examine poison ivy infection in the system. So, this is a particular malware. The package includes those components: PIVY callback decoding tool and memory decoding tool etcetera. So, you can and the source name is external reference. So, this is additional information. So, in the future probably this particular one will be very useful right now. It is just additional information and your tools, the intrusion detection tools etcetera, might be able to use it in some way to help you as a help message or something, but it is not going to automate anything.



Grouping SDO

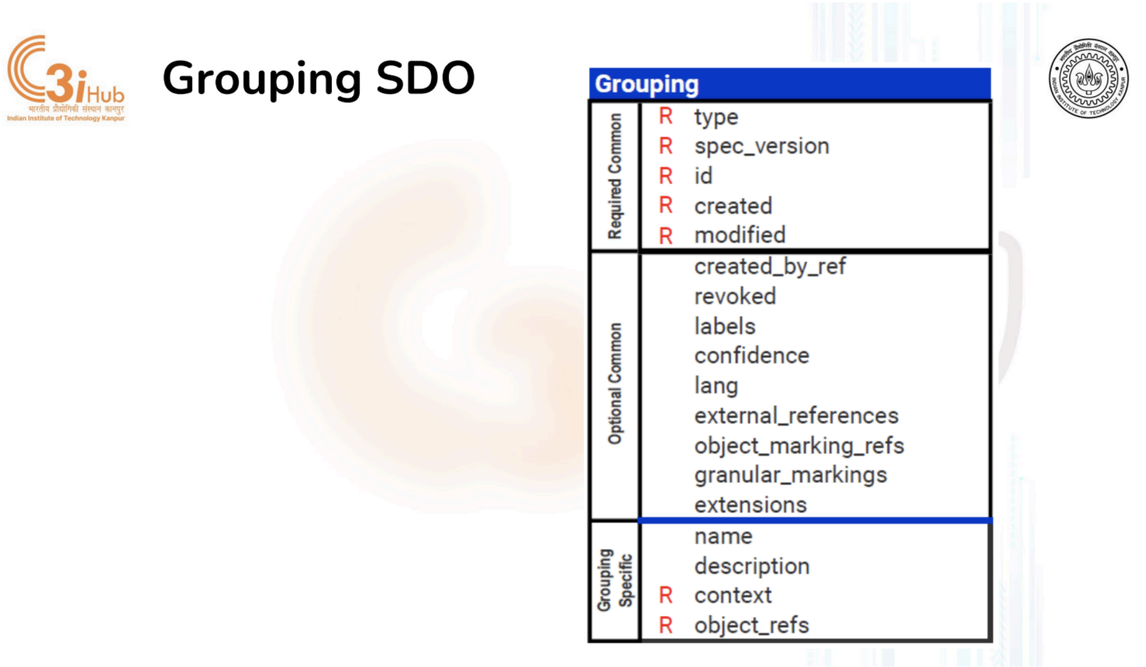
- A Grouping object explicitly asserts that the referenced STIX Objects have a shared context, unlike a STIX Bundle (which explicitly conveys no context).
- A Grouping object should not be confused with an intelligence product, which should be conveyed via a STIX Report.
- A STIX Grouping object might represent a set of data that, in time, given sufficient analysis, would mature to convey an incident or threat report as a STIX Report object.
- For example, a Grouping could be used to characterize an ongoing investigation into a security event or incident.
- A Grouping object could also be used to assert that the referenced STIX Objects are related to an ongoing analysis process, such as when a threat analyst is collaborating with others in their trust community to examine a series of Campaigns and Indicators.
- The Grouping SDO contains a list of references to SDOs, SCOs, and SROs, along with an explicit statement of the context shared by the content, a textual description, and the name of the grouping.

Now grouping SDO, grouping SDO is how you group different objects. So this is like so we already saw multiple objects right. So we saw this object as a course of action object, we saw an example of a campaign object, we saw an example of well we have not seen any other. But so while you are actually creating threat intelligence. So I am a threat intelligence company and I am a threat analyst. I am creating this threat intelligence information which I will sell to my subscribers right or I am certain in that case I am not selling, but I am going to have a pressure on me to share threat intelligence as soon as possible with all constituents because they have to be protected against this particular campaign and so on.

And I got the threat intelligence information. So, I first look at indicators. So, I create some indicator objects right. So, I have to create the JSON structures saying that this is a malware, this is a URL, this is a registry key to change all that stuff. These are the things that are going to be seen as part of this threat intelligence. Also I suspect that this is this threat actor.

And also I suspect that this is based on this attack pattern. So, I am writing multiple SDO objects correctly. Now I want to also I am going to work with another analyst who is also going to help me to add additional because this is time consuming activity to create correct STIX objects right. So, what I do is I create a group. So, I put it in a grouping object. The grouping object basically groups related objects which are related to a particular campaign, particular threat actor, whatever.

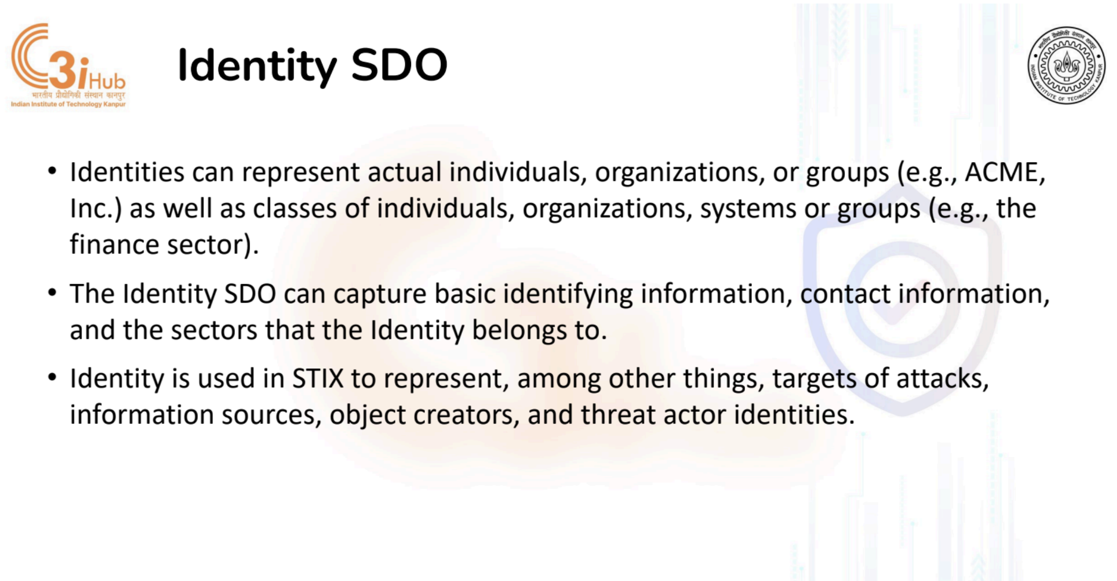
and this is kind of not useful for doing any protection or anything. This is useful while creating the threat intelligence because I basically shared the group with another person. So he can enrich it by adding additional objects inside it right. So that is what grouping objects are. So grouping is not so important but you will see a lot of grouping there.



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

So grouping has all these things type, spec, version, id, created, modified and there should be a context. So there should be a shared context and some object references. The objects that are grouped together that are referenced by their ids should be there. So when we actually look at multiple examples of STIX you will see a lot of grouping right. So grouping is something that is more for convenience if you know sharing the responsibility of creating a shared STIX file.

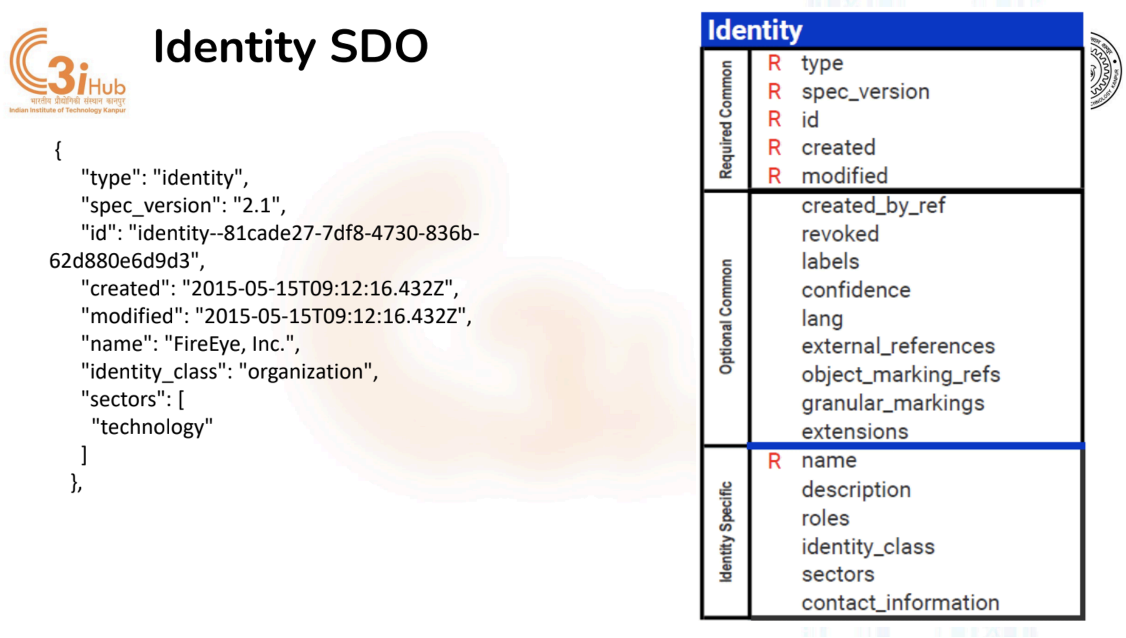


Identity SDO

- 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.

Identity SDO is, now identity is important for any threat intelligence. For example, I might want to say that this threat intelligence pertains to this particular sector. sector or finance sector or I might want to say that this group like the reliance group has been targeted with this particular organization or educational institutes are being targeted by this particular threat actor. So, I may want to add identity information. So identifying information, contact information and sectors the identity belongs to and they are used among other things as target of attacks, information sources, object creators, threat actor identities and so on.

So here is an example: FireEye , as you know, is a threat intelligence company. So it is an identity, it is an organization, its sector is technology and this is the information. Now why have I created this, because later on in my larger sticks file I might say what is the source of this information. Source of this information may be fire eyes. So, in that case I will use this id to associate the top level object, the bundle for example or the report object to this identity.



Identity SDO

```
{
   "type": "identity",
   "spec_version": "2.1",
   "id": "identity--81cade27-7df8-4730-836b-
62d880e6d9d3",
   "created": "2015-05-15T09:12:16.432Z",
   "modified": "2015-05-15T09:12:16.432Z",
   "name": "FireEye, Inc.",
   "identity_class": "organization",
   "sectors": [
     "technology"
   ]
  },
```

Identity		
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
Identity Specific	R	name
		description
		roles
		identity_class
		sectors
		contact_information

So, this identity is useful to give that kind of information. And again this information is not going to help me protect myself as such because as I again and again said that only thing that protects me is the indicator information right everything else is additional information however in my tools let us say I have a SOC and the SOC I am showing in that I am right now having an incident happening. How do I know an incident is happening? Because I am seeing the indicators that my threat intelligence is telling that if you see this URL traffic and if you see this malware etc then you know that you are being attacked by this kind of a campaign. Now when I am showing this to SOC to an SOC analyst, I see that there is an incident in progress and because I am seeing these indicators I also may want to tell him that this information comes from FireEye right. So that you know he knows where this information is coming from.

who is telling that these indicators are indicative of some kind of a problem. So therefore, this kind of information is additional enrichment of the threat intelligence information. Incident object is again a stub.

It does not have much. It is included to support use cases, right? So what constitutes an incident, right. So if you see these indicators, Can you say that right now I should treat this as an incident? So, that is what this incident SDO says. So, it has all these things it has a name, but it may also have other things like which sector this incident is from contact information and so on right. So, now the most important one is the indicator SDO, but I am running out of time.