brushing up on…

exploiting the CTI models

2020 CTI-EU CONFERENCE, BRUSSELS | OMID RAGHIMI

BONDING EU CYBER THREAT INTELLIGENCE

$whoami

- Incident Response and Threat Intelligence Professional
- Member of the ENISA Threat Landscape Stakeholders Group
- Co-Author of ENISA Threat Landscape Report (2018)
- Experience in financial services & Tech industries
- Contributor to Cybersecurity Intelligence research at Kingston University

KEEP IN TOUCH …

@raghimi

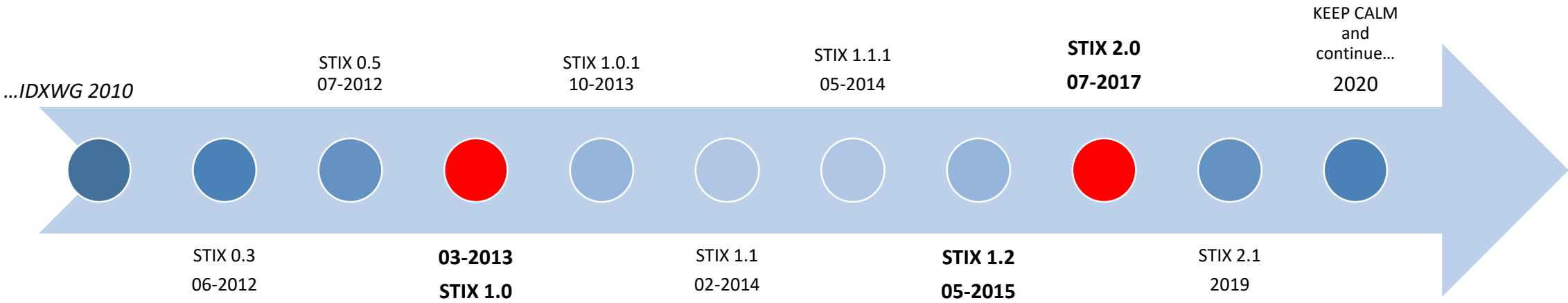
linkedin.com/in/raghimi

AGENDA

- **What we know about STIX & ATT&CK**
  - Going back & looking forward
  - ATT&CK
- **STIX in practice**
  - Customization (examples)
  - Refreshing (my thoughts on) the concept ☺
- **Takeaways**

STIX

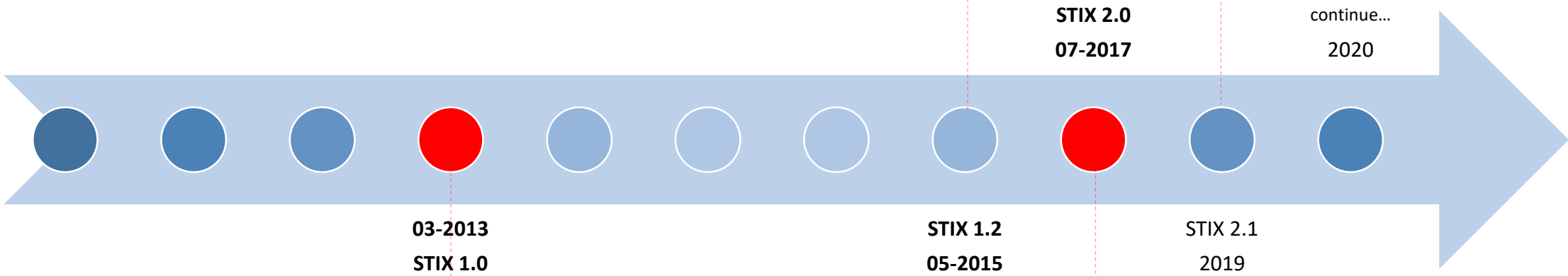
STRUCTURED THREAT
INFORMATION EXPRESSION



brushing up on…
STIX
ATT&CK
exploiting the CTI models

STIX

STRUCTURED THREAT
INFORMATION EXPRESSION



03-2013
STIX 1.0

STIX 1.2
05-2015

STIX 2.0
07-2017

STIX 2.1
2019

KEEP CALM
and
continue…
2020

<.xml>
+ CAMPAIGN
+ TTP
+ COURSE OF ACTION
+ EXPLOIT TARGET
+ INCIDENT
+ INDICATOR
+ THREAT ACTOR
…

Cybox integration

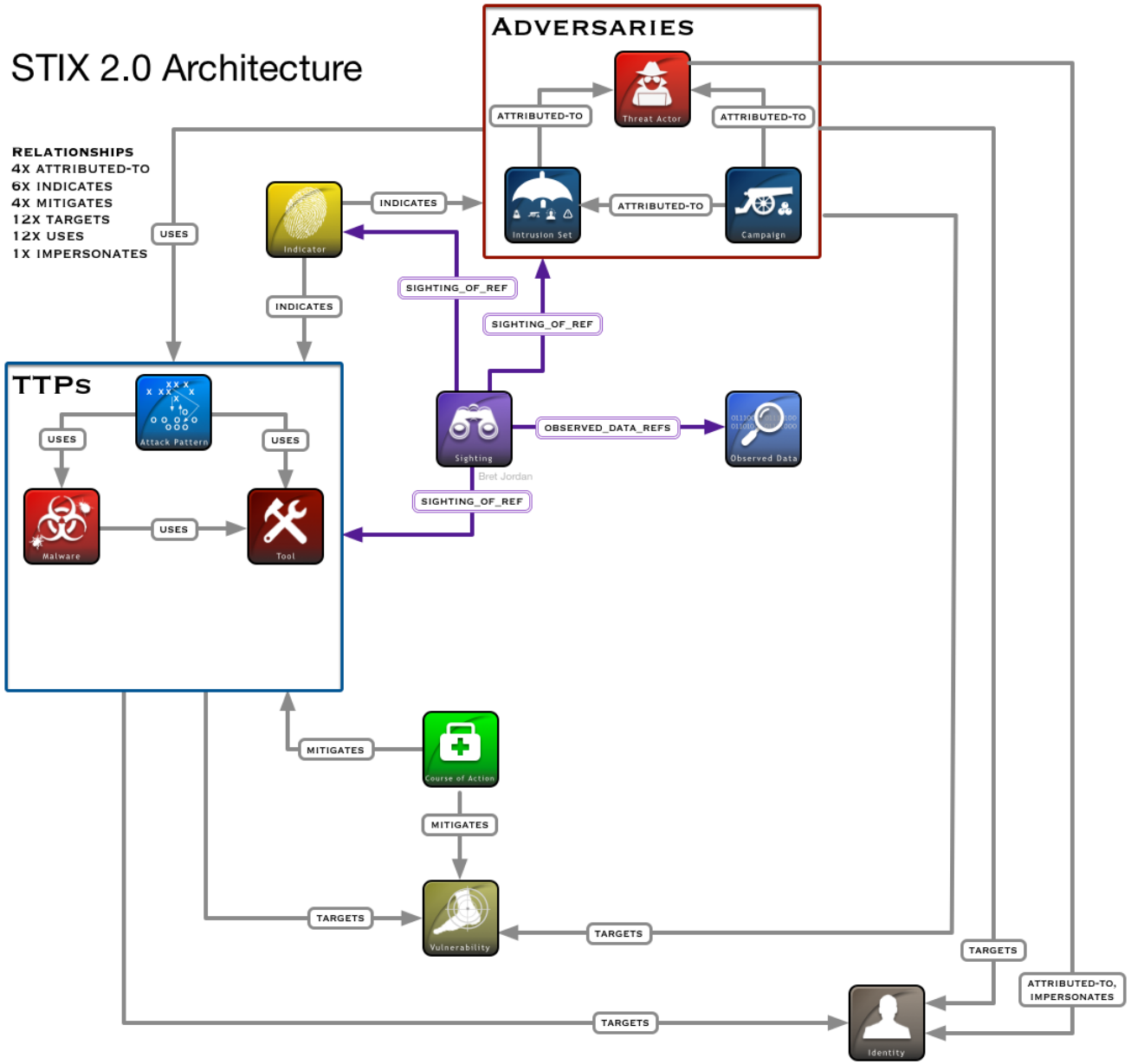
+ REPORT Object

<.json>
+ IDENTITY
+ INTRUSION SET
+ MALWARE
+ OBSERVED DATA
+ TOOL
+ VULNERABILITY
- ~~Incident~~
…

~~Cybox~~ cyber Observables
Relationships

+ Location
+ Infrastructure
+ Note
+ Opinion
+ Grouping
+ VULNERABILITY
+ Malware Analysis
- malware
…

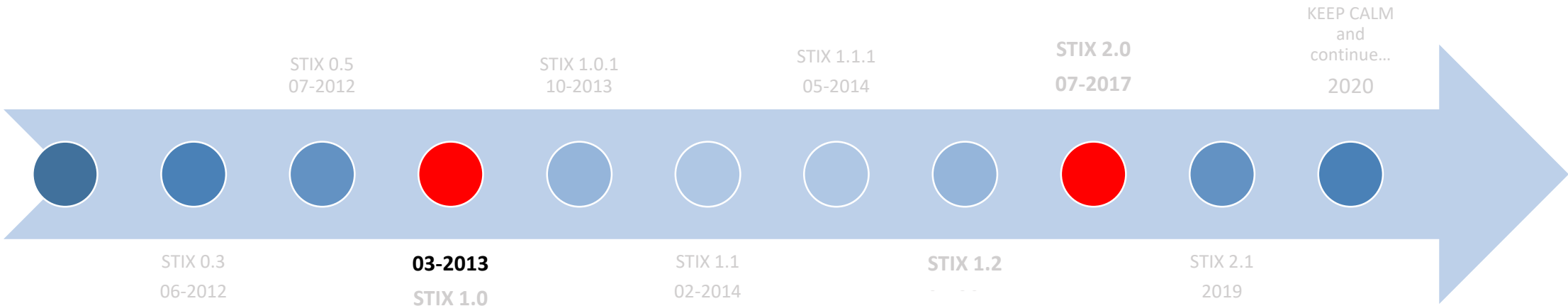
Confidence, Language,…



https://github.com/freetaxii/stix2-graphics/blob/master/diagrams/stix2-architecture-72dpi-v1.png

ATT&CK

ADVERSARIAL TACTICS, TECHNIQUES,
& COMMON KNOWLEDGE



ATT&CK

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	Scheduled Task			Binary Padding	Network Sniffing		AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	Launchctl		Access Token Manipulation		Account Manipulation	Account Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Local Job Scheduling		Bypass User Account Control		Bash History	Application Window Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	LSASS Driver		Extra Window Memory Injection		Brute Force	Browser Bookmark Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Trap		Process Injection		Credential Dumping	Domain Trust Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Other Network Medium	Disk Structure Wipe
Spearphishing Attachment	AppleScript	DLL Search Order Hijacking			Credentials in Files	File and Directory Discovery	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	CMSTP	Image File Execution Options Injection			Credentials in Registry	Network Service Scanning	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Alternative Protocol	Firmware Corruption
Spearphishing via Service	Command-Line Interface	Plist Modification			Exploitation for Credential Access	Network Share Discovery	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Compiled HTML File	Valid Accounts			Forced Authentication	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
Trusted Relationship	Control Panel Items	Accessibility Features		BITS Jobs	Hooking	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Resource Hijacking
Valid Accounts	Dynamic Data Exchange	AppCert DLLs		Clear Command History	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multiband Communication		Runtime Data Manipulation
	Execution through API	AppInit DLLs		CMSTP	Input Prompt	Process Discovery	Shared Webroot	Screen Capture	Multi-hop Proxy		Service Stop
	Execution through Module Load	Application Shimming		Code Signing	Kerberoasting	Query Registry	SSH Hijacking	Video Capture	Multilayer Encryption		Stored Data Manipulation
		Dylib Hijacking		Compiled HTML File	Keychain	Remote System Discovery	Taint Shared Content		Multi-Stage Channels		Transmitted Data Manipulation
	Exploitation for Client Execution	File System Permissions Weakness		Component Firmware	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery	Third-party Software		Port Knocking		
		Hooking		Component Object Model Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote Access Tools		
	Graphical User Interface	Launch Daemon		Control Panel Items	Private Keys	System Network Configuration Discovery	Windows Remote Management		Remote File Copy		
	InstallUtil	New Service		DCShadow	Securityd Memory	System Network Connections Discovery			Standard Application Layer Protocol		
	Mshta	Path Interception		Deobfuscate/Decode Files or Information	Two-Factor Authentication Interception	System Owner/User Discovery			Standard Cryptographic Protocol		
	PowerShell	Port Monitors		Disabling Security Tools		System Service Discovery			Standard Non-Application Layer Protocol		
	Regsvcs/Regasm	Service Registry Permissions Weakness		DLL Side-Loading		System Time Discovery			Uncommonly Used Port		
	Regsvr32	Setuid and Setgid		Execution Guardrails		Virtualization/Sandbox Evasion			Web Service		
	Rundll32	Startup Items		Exploitation for Defense Evasion							
	Scripting	Web Shell		File Deletion							
	Service Execution	.bash_profile and .bashrc	Exploitation for Privilege Escalation	File Permissions Modification							
	Signed Binary Proxy Execution	Account Manipulation		File System Logical Offsets							
		Authentication Package	SID-History Injection	Gatekeeper Bypass							
	Signed Script Proxy Execution	BITS Jobs	Sudo	Group Policy Modification							
		Bootkit	Sudo Caching	Hidden Files and Directories							
	Source	Browser Extensions		Hidden Users							
	Space after Filename	Change Default File Association		Hidden Window							
	Third-party Software	Component Firmware		HISTCONTROL							
	Trusted Developer Utilities	Component Object Model Hijacking		Image File Execution Options Injection							
	User Execution			Indicator Blocking							
	Windows Management			Indicator Removal from Tools							

brushing up on...
STIX
ATT&CK
exploiting the CTI models

REFRESHING MY THOUGHTS ON THE CONCEPT

What have I missed?

7 Customizing STIX™

There are two primary means to customize STIX: Custom Properties, and Custom Objects. Custom Properties provides a mechanism and requirements for adding properties not defined by this specification to existing STIX Objects. Custom Objects, on the other hand, provides a mechanism and requirements to create custom STIX Objects (objects not defined by this specification).

A consumer that receives a STIX document containing Custom Properties or Objects it does not understand **MAY** refuse to process the document or **MAY** ignore those properties or objects and continue processing the document.

Producers of STIX documents that contain Custom Properties or Objects should recognize that consumers may not understand them and may ignore them. Producers should define any Custom Properties and Objects they use, along with any rules for processing them, and make these definitions and rules accessible to any potential consumers. This specification does not specify a process for doing this.

7.1 Custom Properties

There will be cases where certain information exchanges can be improved by adding properties that are neither specified nor reserved in this document; these properties are called **Custom Properties**. This section provides guidance and requirements for how producers can use Custom Properties and how consumers should interpret them in order to extend STIX in an interoperable manner.

7.1.1 Requirements

- A STIX Object MAY have any number of Custom Properties.
- Custom Property names MUST be in ASCII and MUST only contain the characters a–z (lowercase ASCII), 0–9, and underscore (_).
- Custom Property names SHOULD start with "x_" followed by a source unique identifier (such as a domain name with dots replaced by underscores), an underscore and then the name. For example, **x_example_com_customfield**.
- Custom Property names MUST have a minimum length of 3 ASCII characters.
- Custom Property names MUST be no longer than 250 ASCII characters in length.
- Custom Property names that do not start with "x_" may be used in a future version of the specification for a different meaning. If compatibility with future versions of this specification is required, the "x_" prefix MUST be used.
- Custom Properties SHOULD only be used when there is no existing properties defined by the STIX specification that fulfils that need.

Examples

```
{
  ...,
  "x_acme_org_confidence": 10,
  "x_acme_org_scoring": {
    "impact": "high",
    "probability": "low"
  },
  ...
}
```

Customizing STIX

7.2 Custom Objects

There will be cases where certain information exchanges can be improved by adding objects that are not specified nor reserved in this document; these objects are called **Custom Objects**. This section provides guidance and requirements for how producers can use Custom Objects and how consumers should interpret them in order to extend STIX in an interoperable manner.

7.2.1 Requirements

- Producers MAY include any number of Custom Objects in STIX documents.
- Custom Objects MUST support the Common Properties as defined in section 3.1.
  - The definitions of these properties are the same as those defined in Common Properties and therefore those properties MUST NOT be used to represent the custom properties in the object.
- The **type** property in a Custom Object MUST be in ASCII and MUST only contain the characters a–z (lowercase ASCII), 0–9, and hyphen (-).
- The **type** property MUST NOT contain a hyphen (-) character immediately following another hyphen (-) character.
- Custom Object names MUST have a minimum length of 3 ASCII characters.
- Custom Object names MUST be no longer than 250 ASCII characters in length.
- The value of the **type** property in a Custom Object SHOULD start with "x-" followed by a source unique identifier (like a domain name with dots replaced by hyphens), a hyphen and then the name. For example, x-example-com-customobject.
- A Custom Object whose name is not prefixed with "x-" may be used in a future version of the specification with a different meaning. Therefore, if compatibility with future versions of this specification is required, the "x-" prefix MUST be used.
- The value of the **id** property in a Custom Object MUST use the same format as the identifier type, namely, [object-type]--[UUIDv4].
- Custom Objects SHOULD only be used when there is no existing STIX Object defined by the STIX specification that fulfils that need.

https://docs.oasis-open.org/cti/stix/v2.0/stix-v2.0-part1-stix-core.html

brushing up on... STIX ATT&CK exploiting the CTI models

Properties

- Example: T1047
  - x_mitre_data_sources

```
"x_mitre_data_sources": [
    "Authentication logs",
    "Netflow/Enclave netflow",
    "Process monitoring",
    "Process command-line parameters"
],
```

ATT&CK™

T1047


```
{
    "type": "bundle",
    "id": "bundle--00e82d9b-2598-4c17-b262-d09721958e29",
    "spec_version": "2.0",
    "objects": [
        {
            "x_mitre_permissions_required": [
                "User",
                "Administrator"
            ],
            "x_mitre_data_sources": [
                "Authentication logs",
                "Netflow/Enclave netflow",
                "Process monitoring",
                "Process command-line parameters"
            ],
            "name": "Windows Management Instrumentation",
            "description": "Windows Management Instrumentation (WMI) is a Windows administration
            "x_mitre_remote_support": true,
            "id": "attack-pattern--01a5a209-b94c-450b-b7f9-946497d91055",
            "x_mitre_platforms": [
                "Windows"
            ],
            "object_marking_refs": [
                "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
            ],
            "x_mitre_version": "1.0",
            "x_mitre_system_requirements": [
                "WMI service, winmgmt, running.\nHost/network firewalls allowing SMB and WMI ports
            ],
            "type": "attack-pattern",
            "x_mitre_detection": "Monitor network traffic for WMI connections; the use of WMI in
            "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
            "created": "2017-05-31T21:30:44.329Z",
            "kill_chain_phases": [
                {
                    "kill_chain_name": "mitre-attack",
                    "phase_name": "execution"
                }
            ],
```


https://github.com/mitre/cti/blob/master/enterprise-attack/attack-pattern/

Properties

- Need more context …

```
"x_foo_data_sources": [
    "process monitoring": "sysmon",
    "Authentication logs":"AD_security, azure_auth_logs",
    "process command-line parameters":"sysmon",
    "netflow":"bro_logs"
]
```

ATT&CK™

T1047


```
{
    "type": "bundle",
    "id": "bundle--00e82d9b-2598-4c17-b262-d09721958e29",
    "spec_version": "2.0",
    "objects": [
        {
            "x_mitre_permissions_required": [
                "User",
                "Administrator"
            ],
            "x_mitre_data_sources": [
                "Authentication logs",
                "Netflow/Enclave netflow",
                "Process monitoring",
                "Process command-line parameters"
            ],
            "name": "Windows Management Instrumentation",
            "description": "Windows Management Instrumentation (WMI) is a Windows administration
            "x_mitre_remote_support": true,
            "id": "attack-pattern--01a5a209-b94c-450b-b7f9-946497d91055",
            "x_mitre_platforms": [
                "Windows"
            ],
            "object_marking_refs": [
                "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
            ],
            "x_mitre_version": "1.0",
            "x_mitre_system_requirements": [
                "WMI service, winmgmt, running.\nHost/network firewalls allowing SMB and WMI ports
            ],
            "type": "attack-pattern",
            "x_mitre_detection": "Monitor network traffic for WMI connections; the use of WMI in
            "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
            "created": "2017-05-31T21:30:44.329Z",
            "kill_chain_phases": [
                {
                    "kill_chain_name": "mitre-attack",
                    "phase_name": "execution"
                }
            ],
```

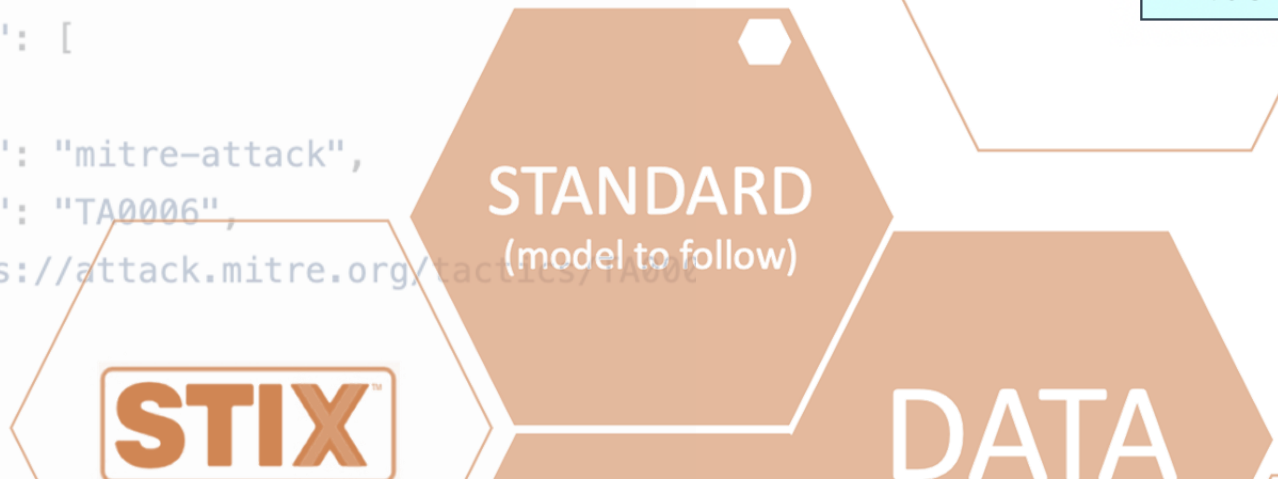

https://github.com/mitre/cti/blob/master/enterprise-attack/attack-pattern/

```
"type": "bundle",
"id": "bundle--5c043f6a-2281-4bdd-9b94-790caeae2269",
"spec_version": "2.0",
"objects": [
    {
        "type": "x-mitre-tactic",
        "name": "Credential Access",
        "description": "The adversary is trying to steal accou
        "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-c
        "created": "2018-10-17T00:14:20.652Z",
        "id": "x-mitre-tactic--2558fd61-8c75-4730-94c4-11926db
        "x_mitre_shortname": "credential-access",
        "modified": "2019-07-19T17:43:41.967Z",
        "object_marking_refs": [
            "marking-definition--fa42a846-8d90-4e51-bc29-71d5b
        ],
        "external_references": [
            {
                "source_name": "mitre-attack",
                "external_id": "TA0006",
                "url": "https://attack.mitre.org/tactics/TA000
            }
        ]
    }
```


Objects

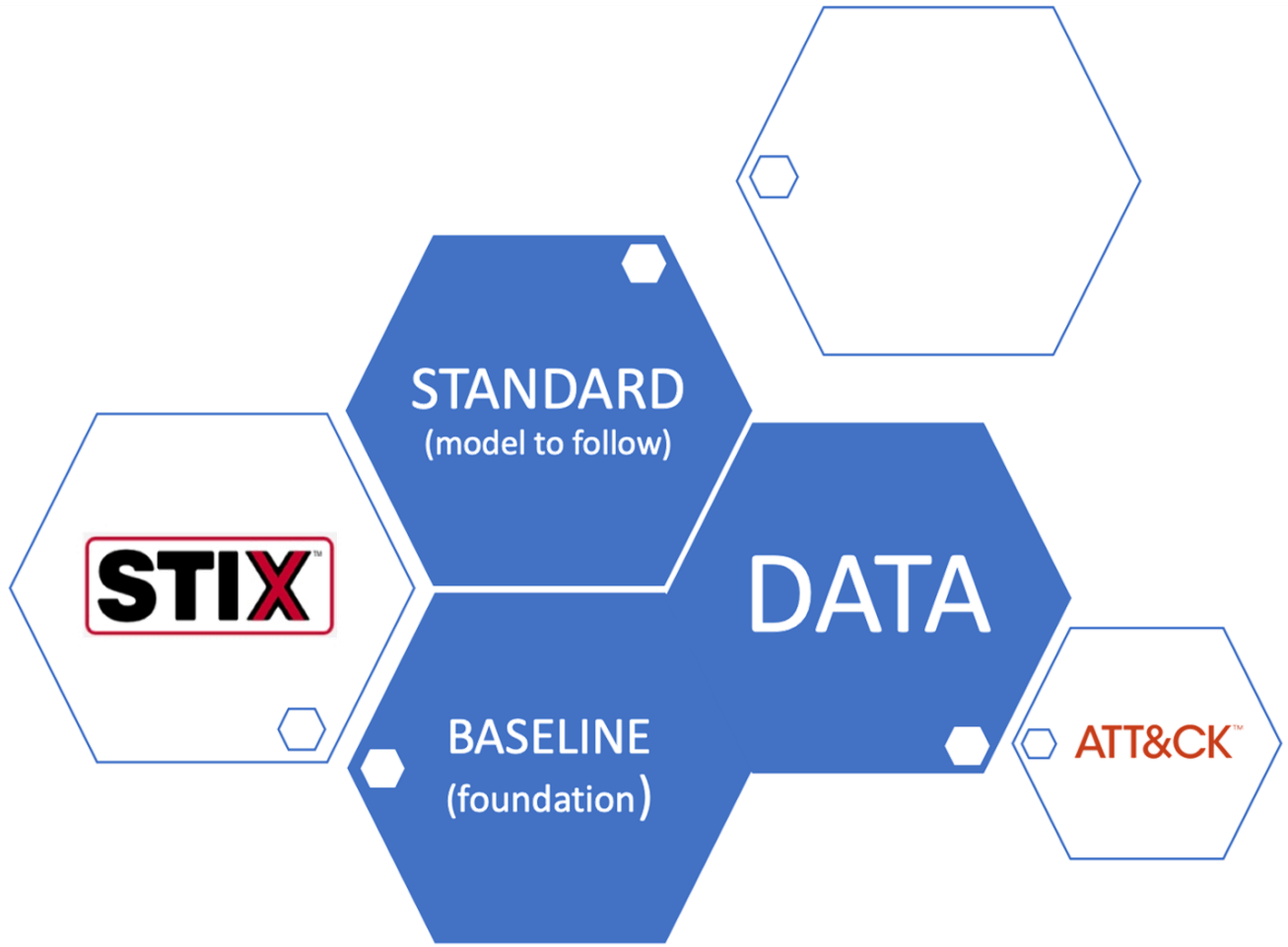
- Example: MITRE Tactics
  - Kept the baseline
  - Created extra needed properties

TACTIC
type = x-mitre-tactic id = x-mitre-tactic--<hash> name = description = ... x-mitre-shortname =



brushing up on... STIX ATT&CK exploiting the CTI models

What have I missed again?


STANDARD
(model to follow)
STIX
DATA
BASELINE
(foundation)
ATT&CK

A way of thinking...

Structuring my knowledge and data in CTI

STANDARD
(model to follow)

STIX

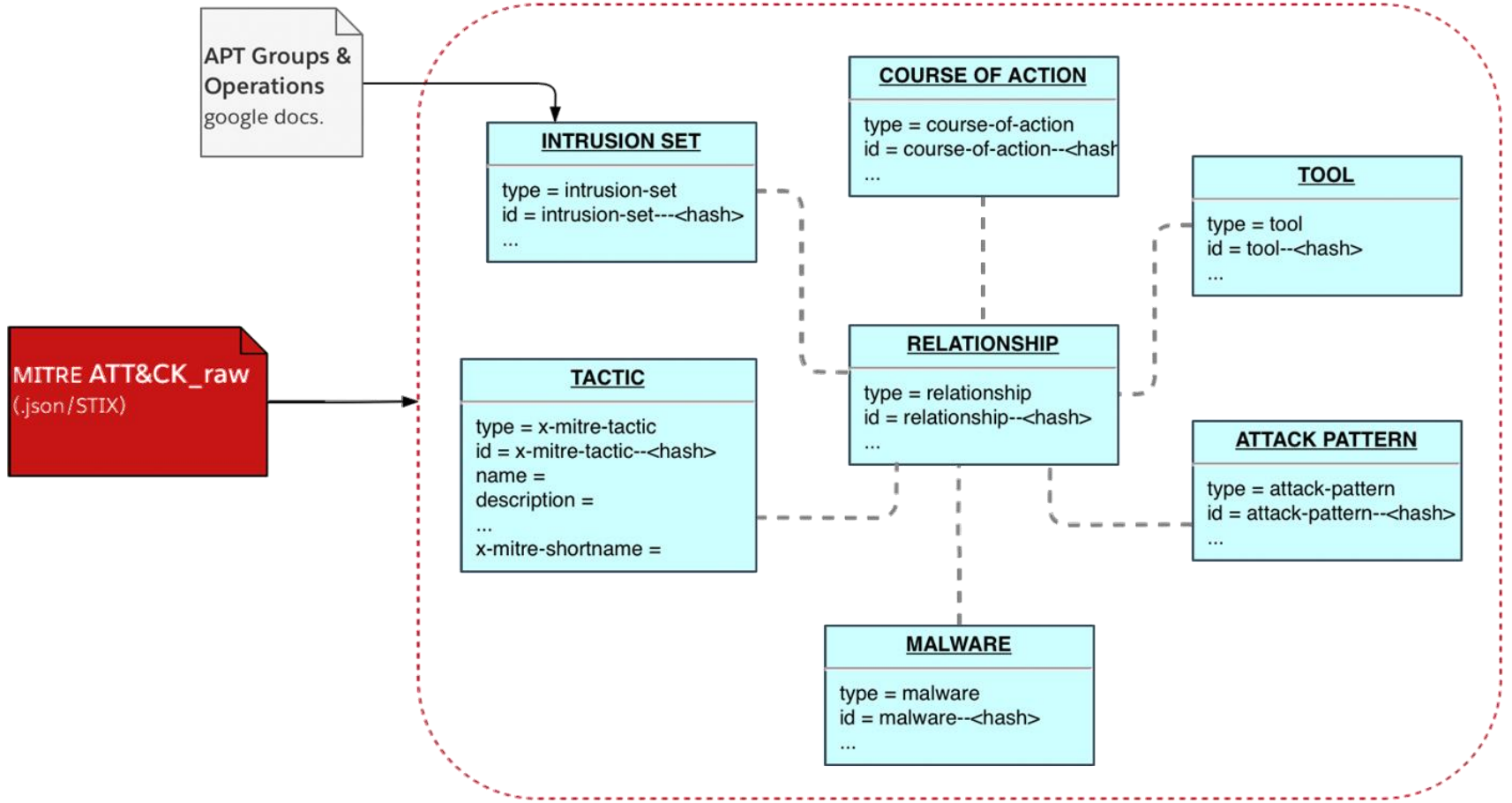
BASELINE
(foundation)

ATT&CK

brushing up on... STIX ATT&CK exploiting the CTI models

Let's look Back…

ATT&CK example:



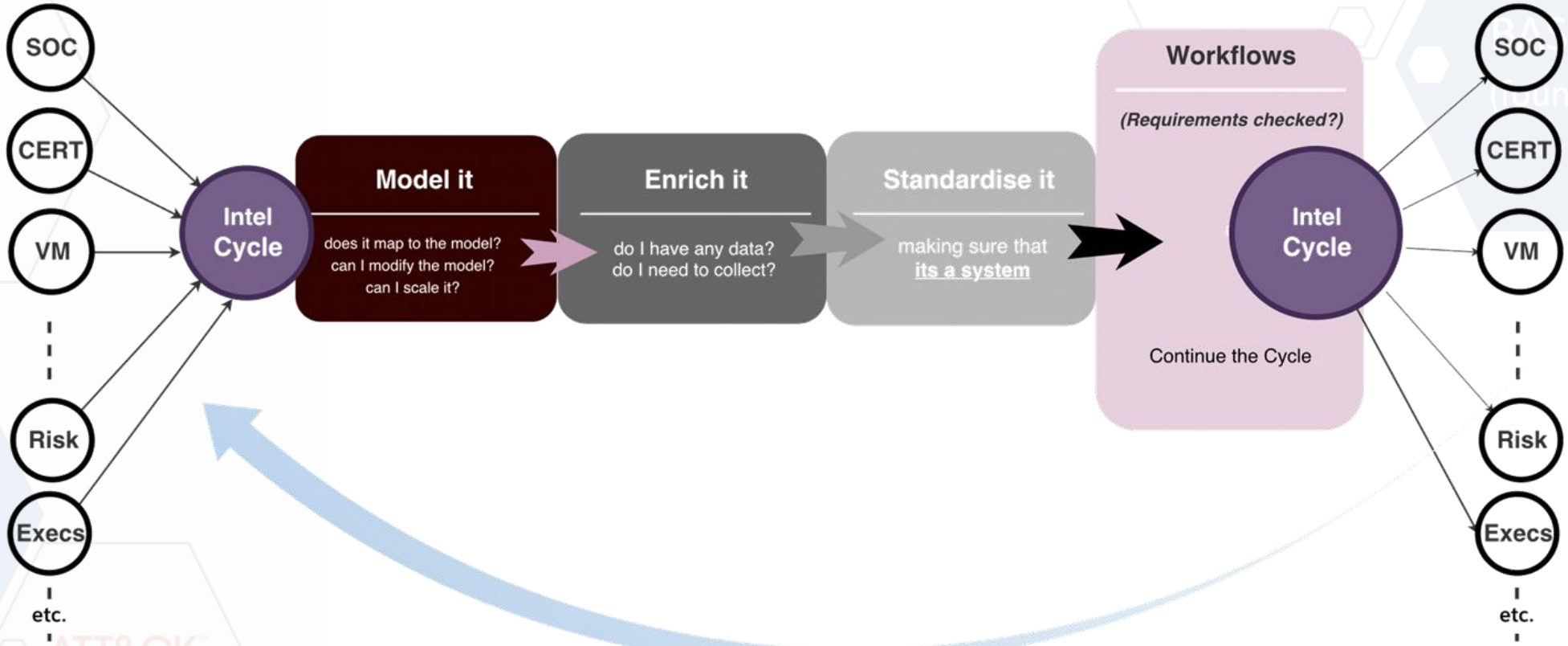
- Model it?
- Enrich it?
- Standardise it?

APT-Groups & Operation : https://apt.threattracking.com

brushing up on… STIX ATT&CK exploiting the CTI models

Can I go beyond?

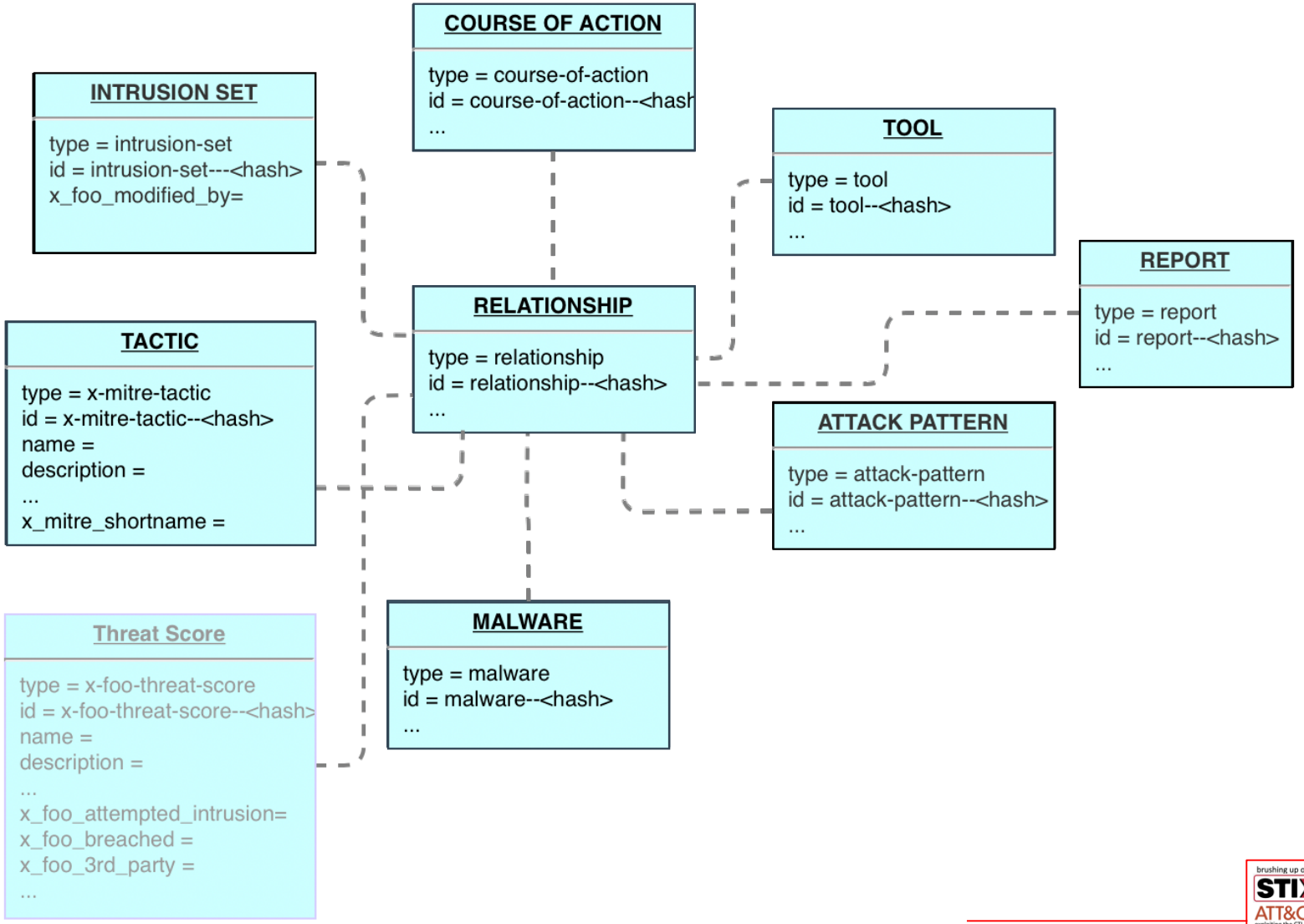
Intelligence Cycle!



...requirements

example: spoon feeding requirements!

- Keep the core
- Modify based on requirements



Takeaways

- **STIX**
  - … has been through **major changes**
  - … **customizable** & **extendable** – you can tailor it to your needs
  - … **more than** just a sharing standard
  - … File format (json) is just one small part of it

- **Points to talk/debate about:**
  - Shall I use this approach internally or via TIPs or both?
  - How much resources it requires to follow/build this?

brushing up on... STIX ATT&CK exploiting the CTI models

References & Related Readings

STIX reads & Docs:
STIX Documentation
STIX 2.1 – Draft
STIX Previous versions – intro (< 2.0)
It's All in the Name: A Guide to STIX Naming Conventions - EclecticIQ
CTI Automation is harder than it needs to be… (FIRST 2018)

CTI Sources:
APT-Groups & Operation
MITRE ATT&CK Framework - Philosophy
Your Requirements are not my Requirements (Pasquale Stirparo)
Exploring the opportunities and limitations of current Threat Intelligence Platforms (ENISA)

Data Models & Ontologies:
An Ontology for Cyber Threat Intelligence
What are Ontologies?
Ontologies and Data Models – are they the same? (2011 – a good overview)
Ontologies for Security Requirements: A Literature Survey and Classification (long version) (2014 – full review)

Thank You!

Looking forward to your feedback and comments on this!

& I hope…

@raghimi
linkedin.com/in/raghimi