Threat Actor
Open Repository
User Group

KICK-OFF MEETING | AUGUST 2, 2019
Agenda

- Harmonizing Threat Actor Frameworks
- Discuss Open Repository Coordination
- Discuss Resources
## STIX 2.1 Threat Actor SDO Summary

<table>
<thead>
<tr>
<th>SDO</th>
<th>Required Common Properties</th>
<th>Optional Common Properties</th>
<th>Not Applicable Common Properties</th>
<th>Threat Actor Specific Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Actor</td>
<td>type</td>
<td>created_by_ref</td>
<td>defanged</td>
<td>name</td>
</tr>
<tr>
<td></td>
<td>spec_version</td>
<td>revoked</td>
<td>extensions</td>
<td>description</td>
</tr>
<tr>
<td></td>
<td>id</td>
<td>labels</td>
<td></td>
<td>threat_actor_types</td>
</tr>
<tr>
<td></td>
<td>created</td>
<td>confidence</td>
<td></td>
<td>aliases</td>
</tr>
<tr>
<td></td>
<td>modified</td>
<td>lang</td>
<td></td>
<td>first_seen</td>
</tr>
<tr>
<td></td>
<td></td>
<td>external_references</td>
<td></td>
<td>last_seen</td>
</tr>
<tr>
<td></td>
<td></td>
<td>object_marking_ref</td>
<td></td>
<td>roles</td>
</tr>
<tr>
<td></td>
<td></td>
<td>granular_markings</td>
<td></td>
<td>goals</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>sophistication</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>resource_level</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>primary_motivation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>secondary_motivation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>personal_motivations</td>
</tr>
</tbody>
</table>

Source: 4.16 Threat Actor, WD05 - [https://docs.google.com/document/d/1bkMmU1PxlwlAwjrMmyWV147rvLcRs2x62FicHbpH2gU/edit#heading=h.k017w16zutw](https://docs.google.com/document/d/1bkMmU1PxlwlAwjrMmyWV147rvLcRs2x62FicHbpH2gU/edit#heading=h.k017w16zutw)
Existing OS Resources

- Florian Roth et. al. Matrix
  - https://docs.google.com/spreadsheets/u/1/d/1H9_xaxQHpWaa4O_Son4Gx0YOIzlcBWMsdvePFX68EKU/pubhtml
- ATT&CK 'Groups'
  - https://attack.mitre.org/groups/
- MISP-Galaxy
- CERT.be
- Other???
Framework

- Authorization
  - OASIS TC Open Repository Policies
    - https://www.oasis-open.org/policies-guidelines/open-repositories

- Membership
  - CTI TC Members & non-Member Contributors

- Governance
Definition

“An OASIS TC Open Repository ("TC Open Repository") is a distinct facility operated by OASIS for collection of voluntarily contributed information relevant to the work of a specific TC, under the rules set forth in these procedures. TC Open Repositories may reside on third-party server resources.”
Contributions

“Each TC Open Repository will be subject to a declared "Applicable License," selected from the list of licenses at the end of this section. The Applicable License for a repository will apply to all repo contributions donated to the repository, by posting it or requesting its inclusion in that repository. Anyone, whether an OASIS member or TC member or not, may contribute into a TC Open Repository”
All Participants Must Sign a CLA

“Each TC Open Repository shall be subject to a Contributor License Agreement ("CLA") by which all persons making repo contributions into it are bound. The CLA shall bind each donor of a repo contribution to the repository's Applicable License and such other consistent terms as OASIS may require as a publisher to assure its availability.”
“Each TC Open Repository should have a purpose statement, indicating its intended contents or topic, declared by the TC that creates it, as part of its approval action.”
Resources

▪ CTI TC Ad Hoc Meeting Link
  ▪ [https://newcontext.zoom.us/j/332585406](https://newcontext.zoom.us/j/332585406)

▪ OASIS Github
  ▪ “OASIS initially will create TC Open Repositories as either distinct GitHub projects, or distinct Subversion repositories.”

▪ Visual Diagrams
  ▪ See Appendix

▪ Icons
Open Discussion
Visual Resources
Threat Actor Definition

Threat Actors are actual individuals, groups, or organizations believed to be operating with malicious intent.

Examples

- Evil Org, an organization
- John Doe, a malware author associated with Evil Org and several other criminal groups
Forward & Reverse Relationships
Sample Use Cases with SDOs

Adversary Bravo
- **Identity_class:** unknown
- **description:** Adversary Bravo is a threat actor that utilizes phishing attacks.

**Adversary Bravo**
- **labels:** spy, criminal
- **description:** Known to use phishing attacks to deliver remote access malware to targets.

**Threat Actor**
- **Attributed-to**:

**Identity**
- **Adversary Bravo** as the identity

**Attack Pattern**
- **Phishing**
  - **external_references**:
    - source_name: capem
    - description: phishing
    - url: https://capem.nist.gov/
    - external_id: CAPEC-90
  - **kill_chain_phases**:
    - kill_chain_name: mandiant-attack-lifecycle-model
    - phase_name: initial-compromise

**Malware**
- **Poison Ivy Variant dico**
  - **labels:** remote-access-trojan
  - **kill_chain_phases**:
    - kill_chain_name: mandiant-attack-lifecycle-model
    - phase_name: initial-compromise
Threat Actor Required Types

• activist
• competitor
• crime-syndicate
• criminal
• hacker
• insider-accidental
• insider-disgruntled
• nation-state
• sensationalist
• spy
• terrorist
• unknown

REQUIRED PROPERTY
Threat Actor Attack Resource Level (-ov)

- individual
- club
- contest
- team
- organization
- government

OPTIONAL PROPERTY
<table>
<thead>
<tr>
<th>Threat Actor Motivations (-ov)*</th>
</tr>
</thead>
<tbody>
<tr>
<td>accidental</td>
</tr>
<tr>
<td>coercion</td>
</tr>
<tr>
<td>dominance</td>
</tr>
<tr>
<td>ideology</td>
</tr>
<tr>
<td>notoriety</td>
</tr>
</tbody>
</table>

* Primary, Secondary & Personal
Threat Actor Roles (-ov)

agent
director
independent
infrastructure-architect
infrastructure-operator
malware-author
sponsor

OPTIONAL PROPERTY
Threat Actor Sophistication (-ov)

- none
- minimal
- intermediate
- advanced
- expert
- innovator
- strategic