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

SDO	Required Common Properties	Optional Common Properties	Not Applicable Common Properties	Threat Actor Specific Properties
Threat Actor	type spec_version id created modified	created_by_ref revoked labels confidence lang external_references object_marking_refs granular_markings	defanged extensions	name description threat_actor_types aliases first_seen last_seen roles goals sophistication resource_level primary_motivation secondary_motivation personal_motivations

Source: **4.16 Threat Actor, WD05 -** 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
  - https://github.com/MISP/misp-galaxy/blob/master/clusters/threat-actor.json
- 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.”

Purpose Statement

“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
- **OASIS Github**
  - "OASIS initially will create TC Open Repositories as either distinct GitHub projects, or distinct Subversion repositories."
- **Visual Diagrams**
  - See Appendix
- **Icons**
  - https://github.com/freetaxii/stix2-graphics/tree/master/icons/png/stix2-adversary-icons-png

Open Discussion

Visual Resources

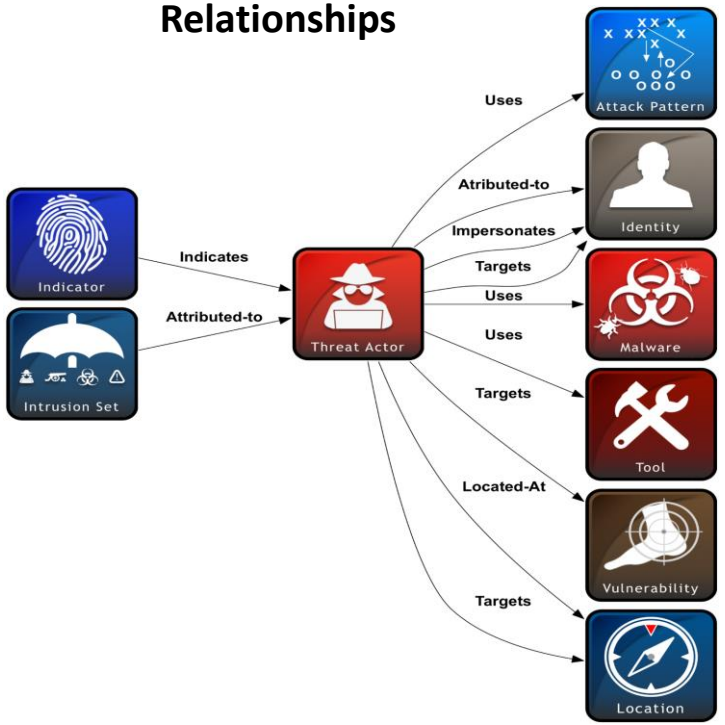
Threat Actor Definition

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

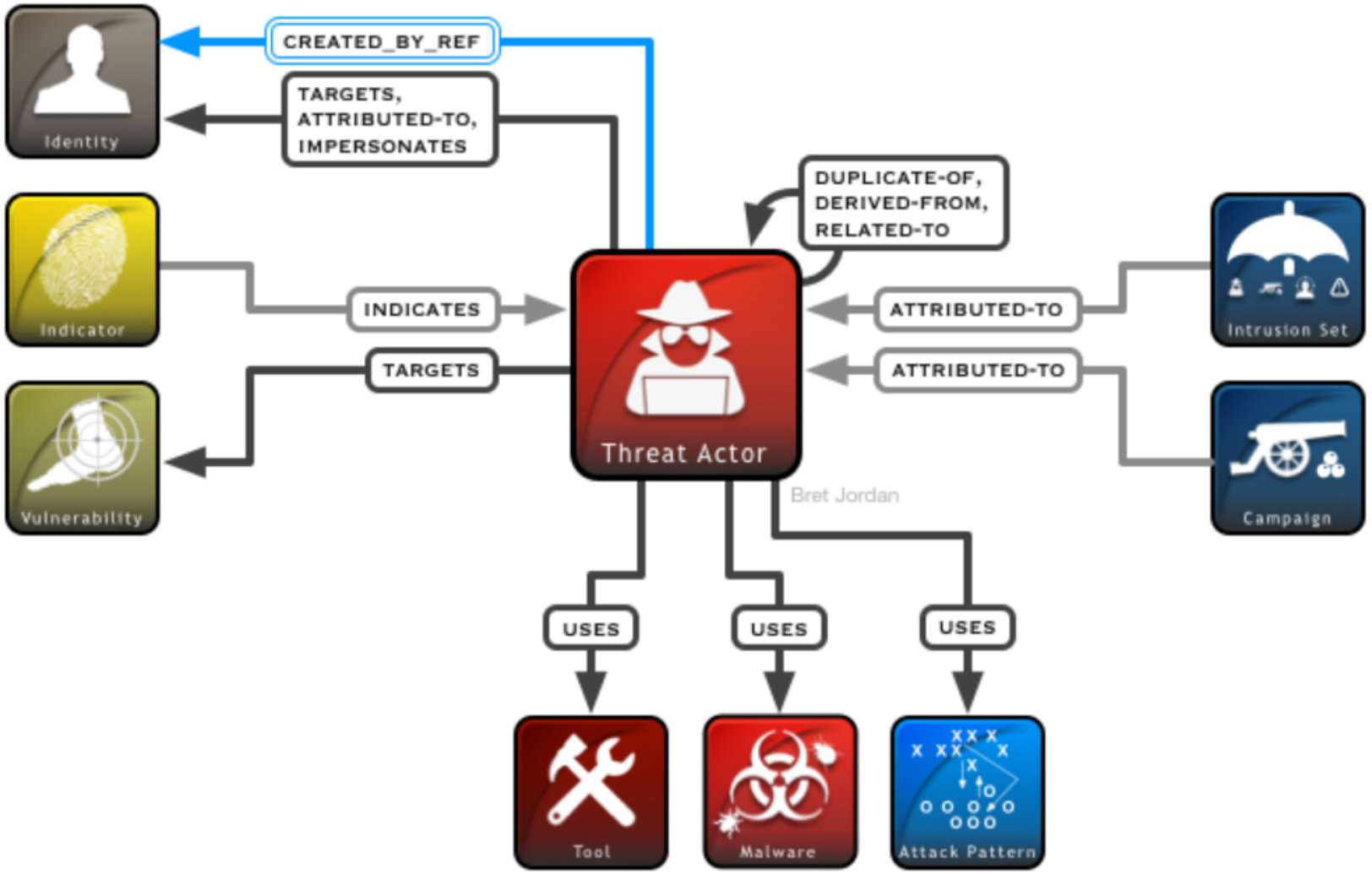
Examples

- Evil Org, an organization
- John Doe, a malware author associated with Evil Org and several other criminal groups

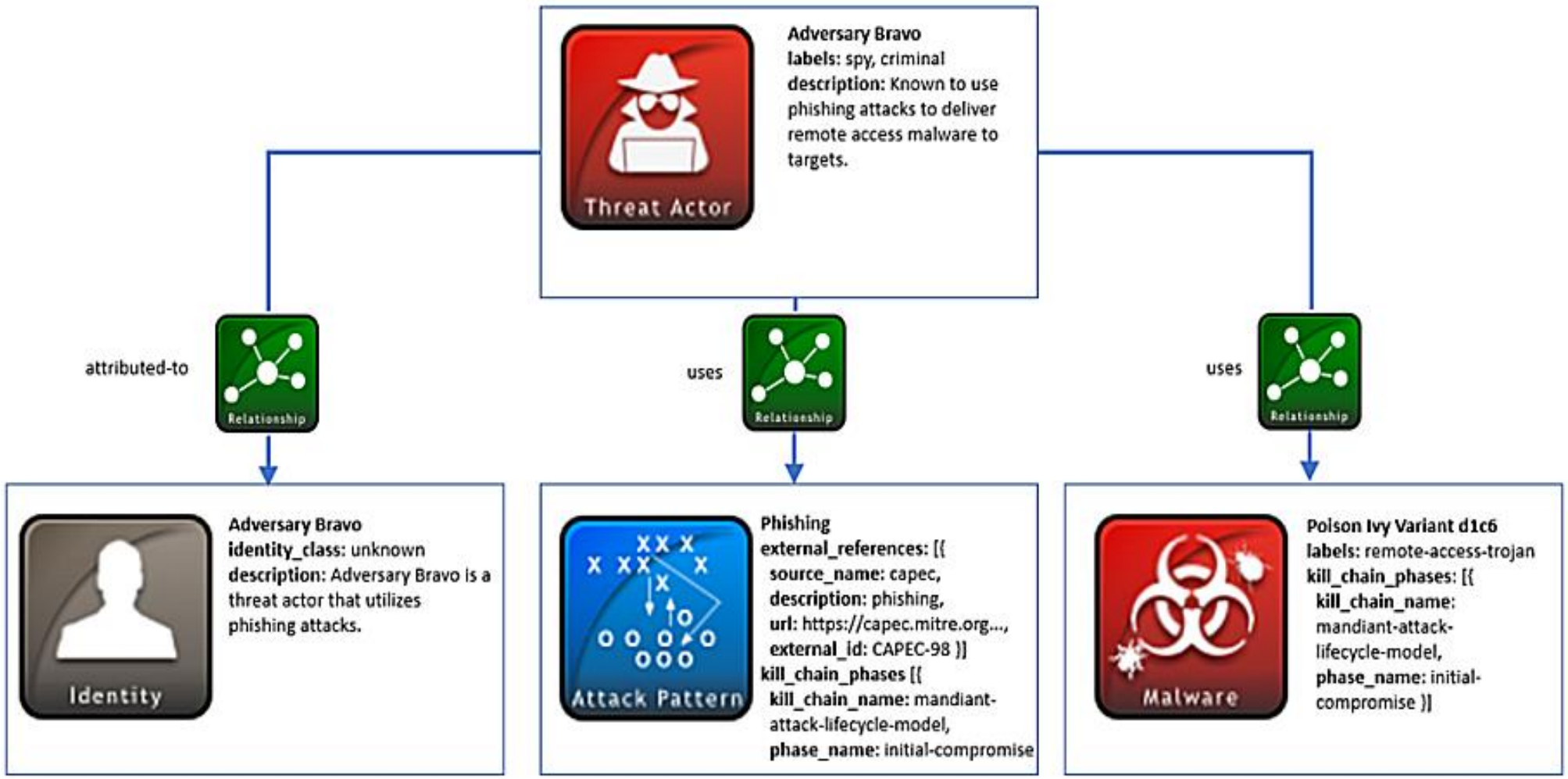
Relationships

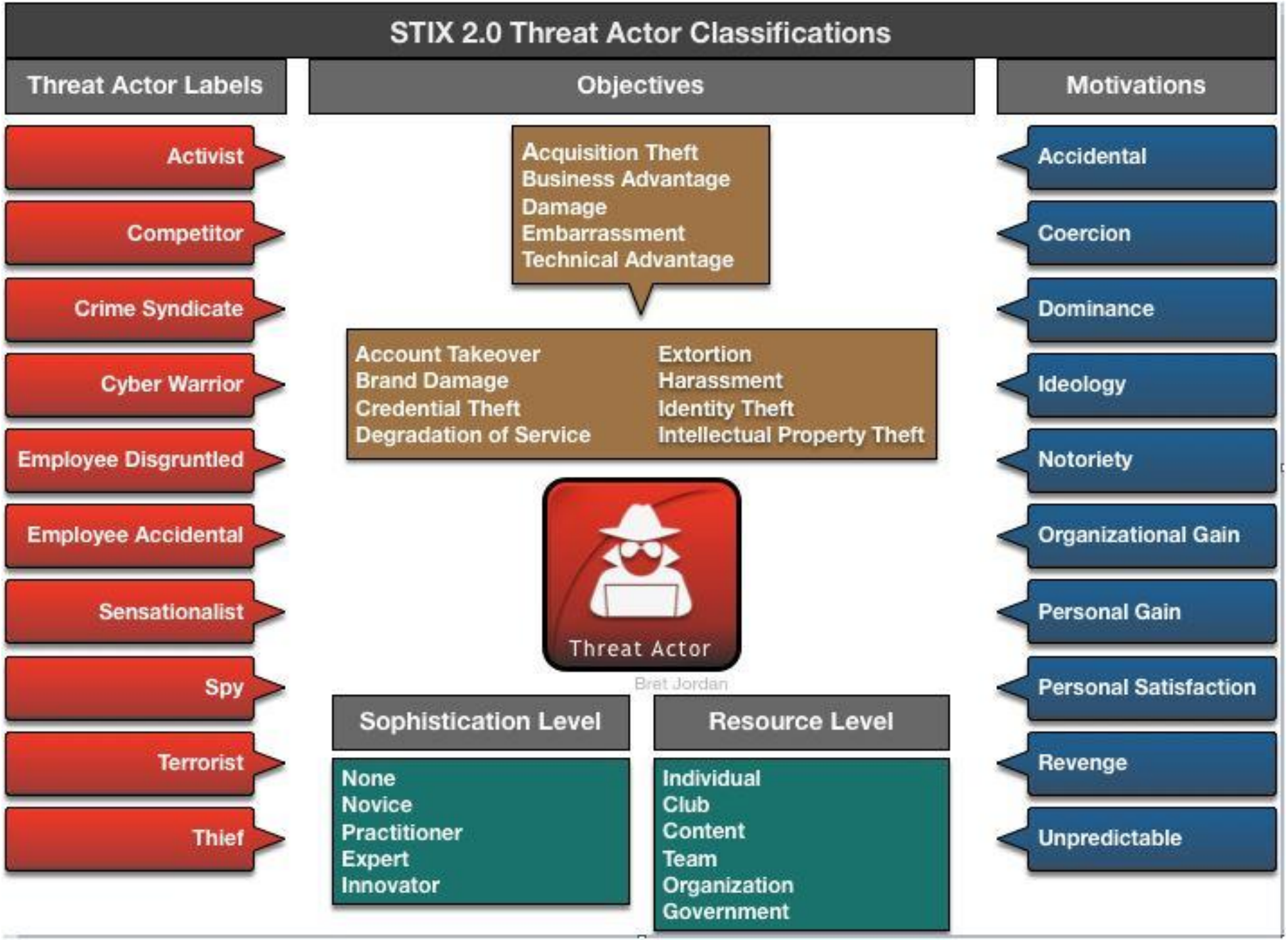


Forward & Reverse Relationships



Sample Use Cases with SDOs




STIX 2.0 Threat Actor Classifications
Threat Actor Labels
Objectives
Motivations
Activist
Competitor
Crime Syndicate
Cyber Warrior
Employee Disgruntled
Employee Accidental
Sensationalist
Spy
Terrorist
Thief
Acquisition Theft
Business Advantage
Damage
Embarrassment
Technical Advantage
Account Takeover
Brand Damage
Credential Theft
Degradation of Service
Extortion
Harassment
Identity Theft
Intellectual Property Theft
Threat Actor
Bret Jordan
Sophistication Level
None
Novice
Practitioner
Expert
Innovator
Resource Level
Individual
Club
Content
Team
Organization
Government
Accidental
Coercion
Dominance
Ideology
Notoriety
Organizational Gain
Personal Gain
Personal Satisfaction
Revenge
Unpredictable

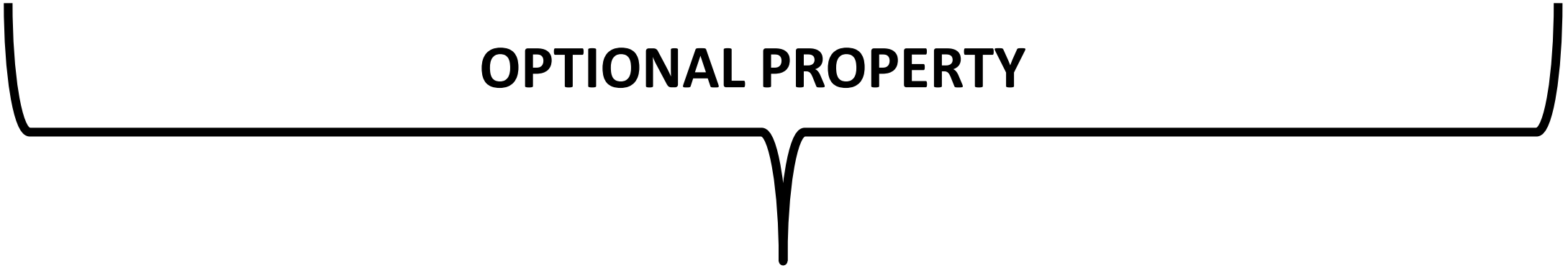
Threat Actor Required Types (-ov)

- 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	team
club	organization
contest	government



Threat Actor Motivations (-ov)*

accidental	organizational gain
coercion	personal-gain
dominance	personal-satisfaction
ideology	revenge
notoriety	unpredictable

OPTIONAL PROPERTY

* 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

OPTIONAL PROPERTY