Security+ Chapter 2

Threat Actors

Author: Justin McAfee
@IaintShootinMis
Twitter|Github

Who Am I?

- Former PSYOP Soldier
- Current Incident Response Analyst for a global food and beverage supplier
- Dad, husband and National Park enthusiast

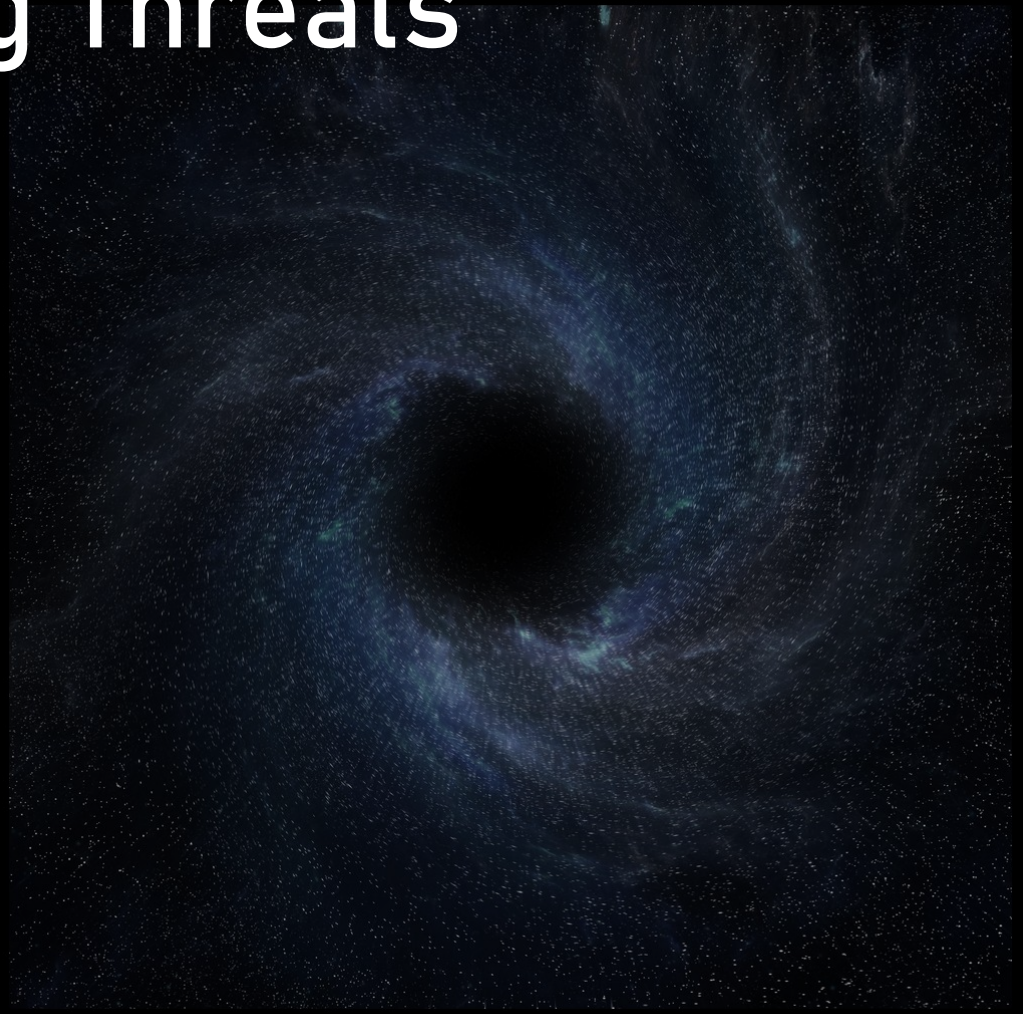
What's In It?

- Classifying Threats
- Hackers Hats
- Threat Actor Definitions
- Deep v. Dark v. Surface Web
- Threat Vectors
- Threat Intelligence

Classifying Threats

4 Classifications

- Internal vs External
- Level of Sophistication
- Resources / Funding
- Intent / Motivation

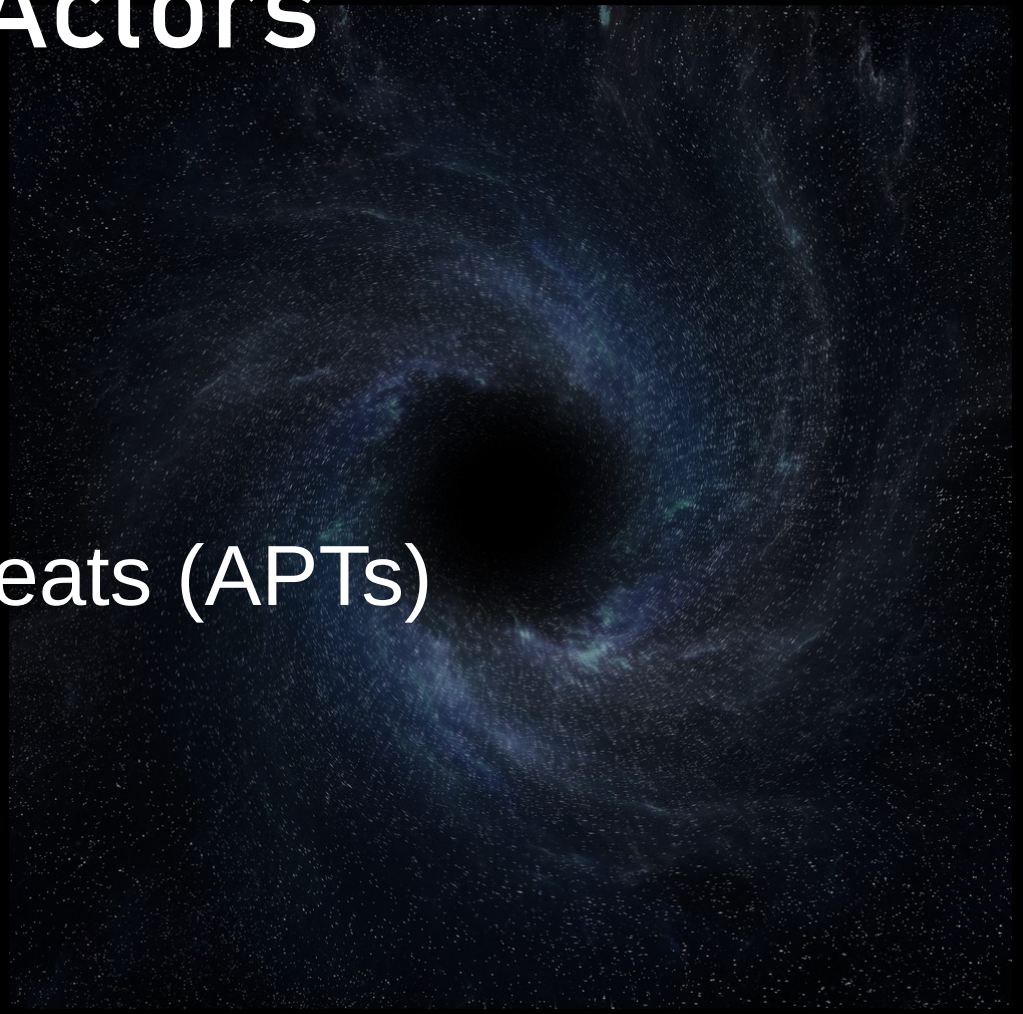


1 Hat 2 Hat White Hat Grey Hat

- White Hat
  - Legal, authorized, employed, “good”
- Black Hat
  - Illegal, unauthorized, maybe employed, “bad”
- Grey Hat
  - Illegal, unauthorized, customer/outsider, “good”, morally questionable in some instances.

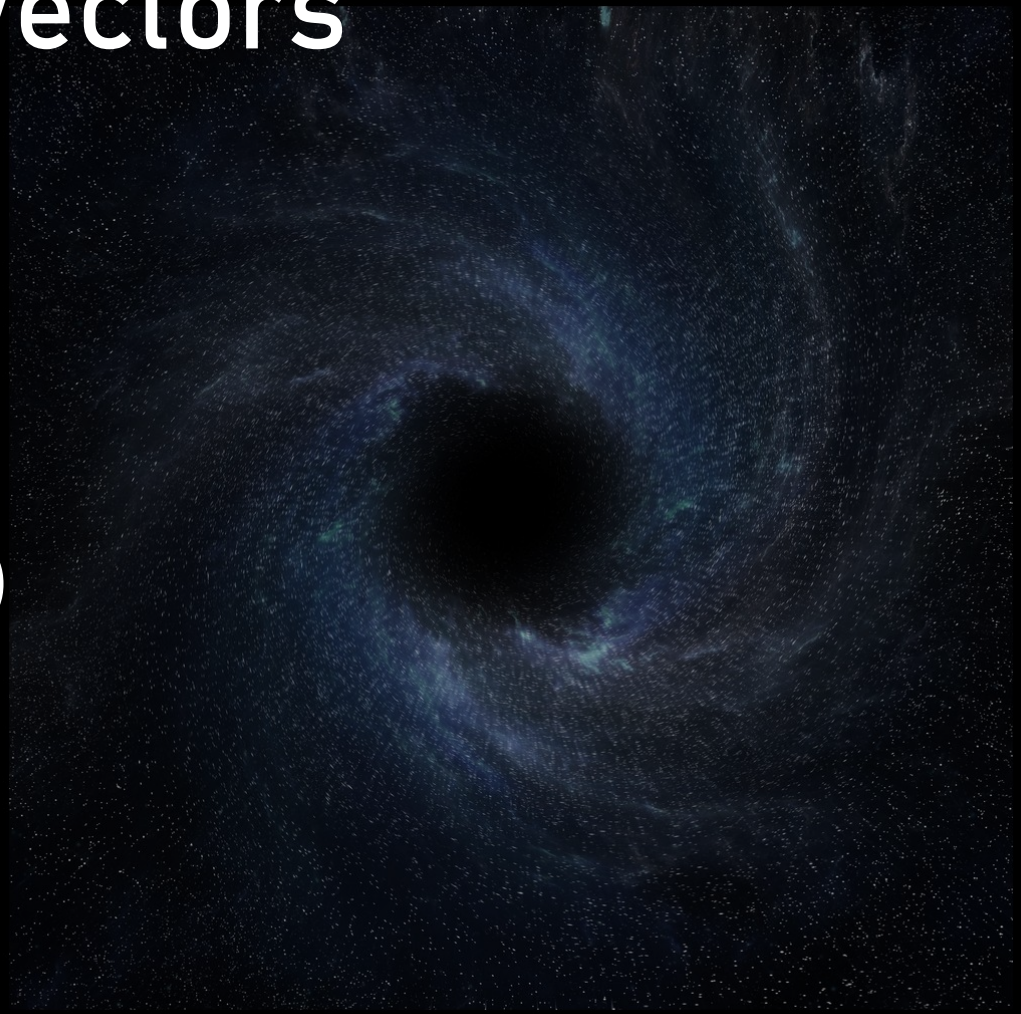
Threat Actors

6 Types of Threat Actors
- Script Kiddies
- Hacktivists
- Criminal Syndicates
- Advanced Persistent Threats (APTs)
- Insiders
- Competitors



Threat Vectors

6 Types of Access
- Email/Social Media
- Direct Access
- Wireless Networks
- Removable Media (USB)
- Cloud
- 3rd Party



Threat Data and Intelligence

- Open Source Intelligence (OSINT)
  - Community
  - Gov’t
  - Vendor
  - Public
- Proprietary and Closed Source

Vocabulary

Indicators of Compromise – fingerprints or telltale signs that a compromise has occurred.

e.g.; Hashes, file signatures, log patterns, and any other evidence left behind.

TTP’s – Tactics, Techniques, and Procedures

Assessing Threat Intel

- Is it timely?
  How old is this info?
- Is it accurate?
  How reliable is the source? Are there multiple sources?
- Is it relevant?
  Is it the right software? Platform? Industry? Etc...

Admiralty Codes

- Quick way to Confidence Score Threat Intel
- Adopted by NATO for Threat Intelligence Scoring
- Works from two Factors
    - Reliability (A-F)
    - Credibility (1-6)
- A1 is the highest, F6 the lowest

Admiralty Code - Reliability

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

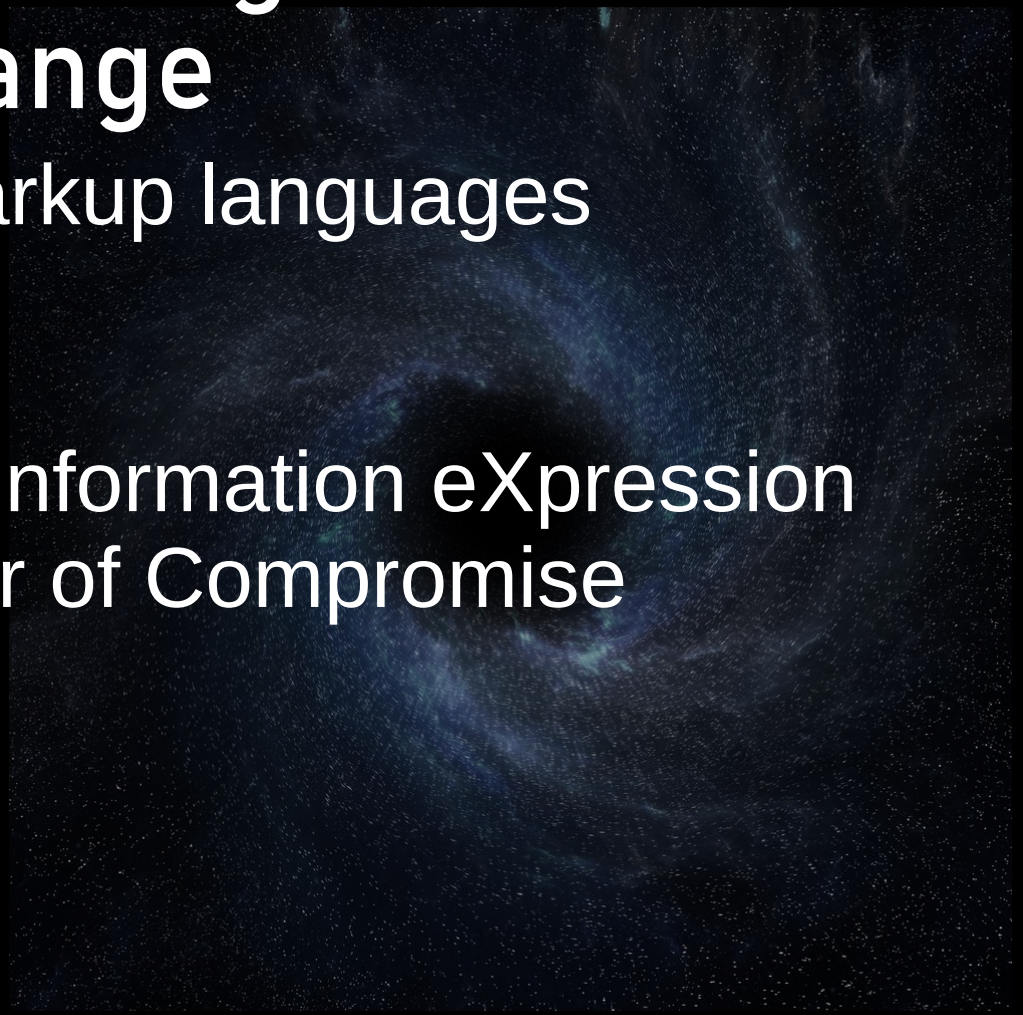
Admiralty Code -Credibility

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

Threat Indicator Management and Exchange

- The use of structured markup languages
  2 Major languages

STIX – Structured Threat Information eXpression
OpenIOC – Open Indicator of Compromise



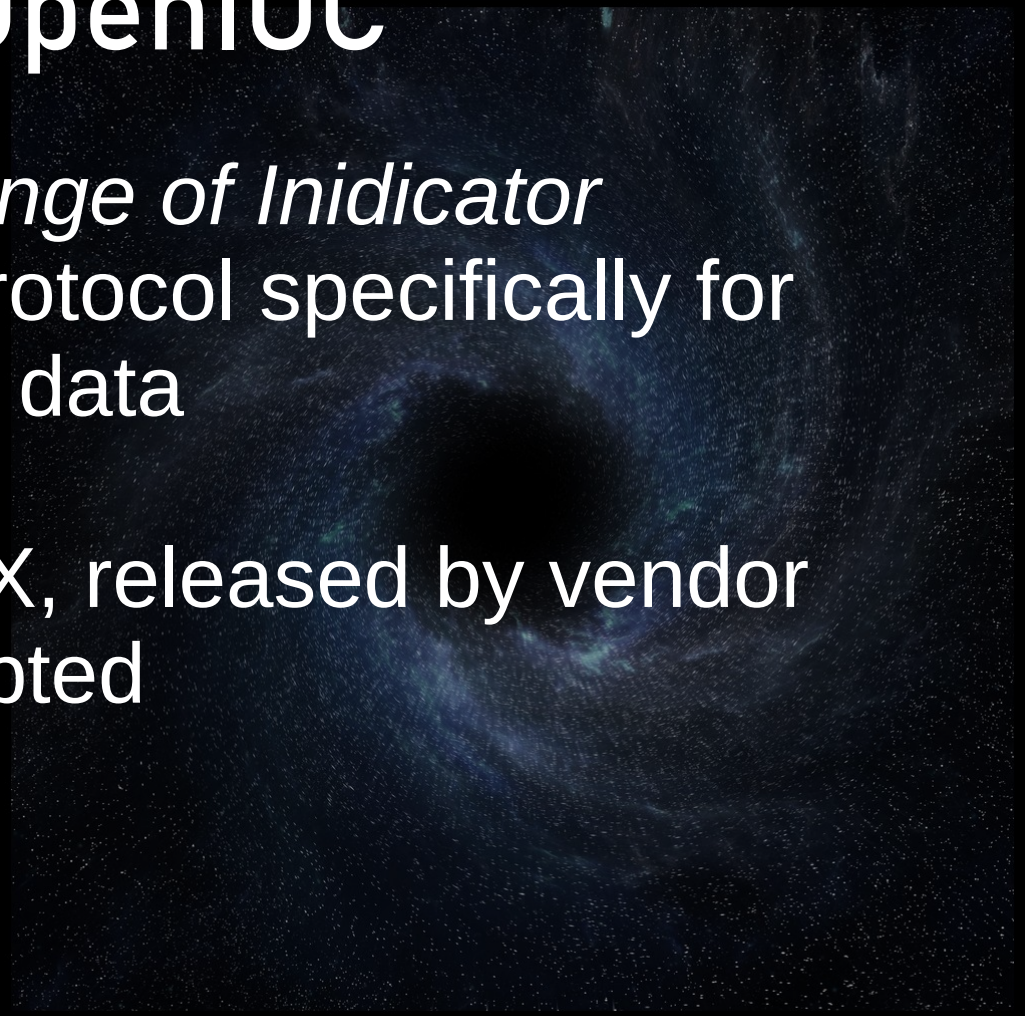
STIX and Structured Data


```
{
 "type": "threat-actor",
 "created": "2019-10-20T19:17:05.000Z",
 "modified": "2019-10-21T12:22:20.000Z",
 "labels": [ "crime-syndicate"],
 "name": "Evil Maid, Inc",
 "description": "Threat actors with access to hotel rooms",
 "aliases": ["Local USB threats"],
 "goals": ["Gain physical access to devices", "Acquire data"],
 "sophistication": "intermediate",
 "resource:level": "government",
 "primary_motivation": "organizational-gain"
}
```

TAXII & OpenIOC

Trusted Automated eXchange of Inidicator Information protocol – a protocol specifically for sharing and sending STIX data

OpenIOC – Similar to STIX, released by vendor Mandiant, not as well adopted



Information Sharing and Analysis Centers

Public or Private
Specifically created to share information about threats and vulnerabilities in specific industries.

Questions?