Mason Competitive Cyber

Threat Intel

Recent Competitions

- Got whooped at UMD CTF
- Fact: Maryland high school students start registering CVEs in kindergarten

Upcoming Competitions & Events

- Online ones
- idk check #ctf-watch

What is threat intel?

- Information vs Intelligence
- IOC (indicator of compromise) vs Intelligence
  - IP
  - Domain Name

What is threat intel?

- Information vs Intelligence
- IOC (indicator of compromise) vs Intelligence

- Threat intel - the output of analysis based on identification, collection, and enrichment of relevant data and information

Term Clarification

- threat, threat actor, vuvlnerability,

Threat Actors

Non-Hostile

- Reckless Employee
- Untrained Employee
- Partners

Hostile

- Script kiddies
- Cyber Crime Groups
- Nation States

Threat Intel Sources

- HUMINT
  - Manually collected
  - Reports with IOCs
- Threat Intel Data Feeds
  - Some open-source
  - Not much context
- Internal TIP
  - Customized to your company
  - Must be managed

Threat Intel for SOCs

- Alert fatigue
  - Form SIEM or EDR tool
- Context from threat intel helps

- Enrich alerts
  - Previous sightings
  - Associations with attack types

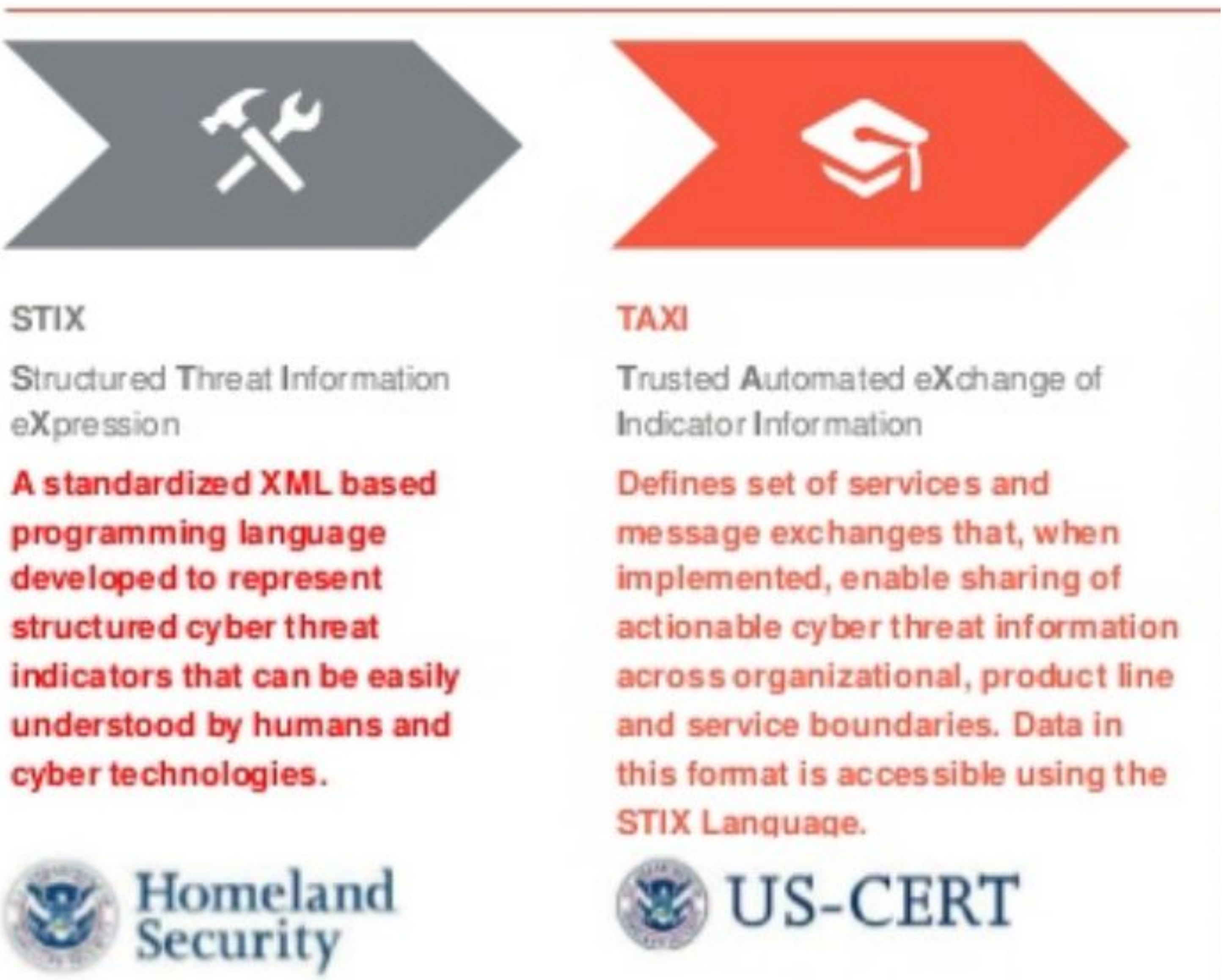
Threat Intel for DFIR

- Auto flagging IOCs
  - Speed up work
- Share TTPs
- Negotiations with threat actors
  - Group X never pays ransom
  - Group Y will negotiate ransom down when asked

Threat Intel for Vulnerability Management

- Prioritize vulnerabilities
- 0 day does not mean top priority
- Risk = Likelihood * Impact
  - Likelihood is exploitability and motivation in this case

Standards



STIX

Structured Threat Information eXpression

A standardized XML based programming language developed to represent structured cyber threat indicators that can be easily understood by humans and cyber technologies.

Homeland Security

TAXI

Trusted Automated eXchange of Indicator Information

Defines set of services and message exchanges that, when implemented, enable sharing of actionable cyber threat information across organizational, product line and service boundaries. Data in this format is accessible using the STIX Language.

US-CERT

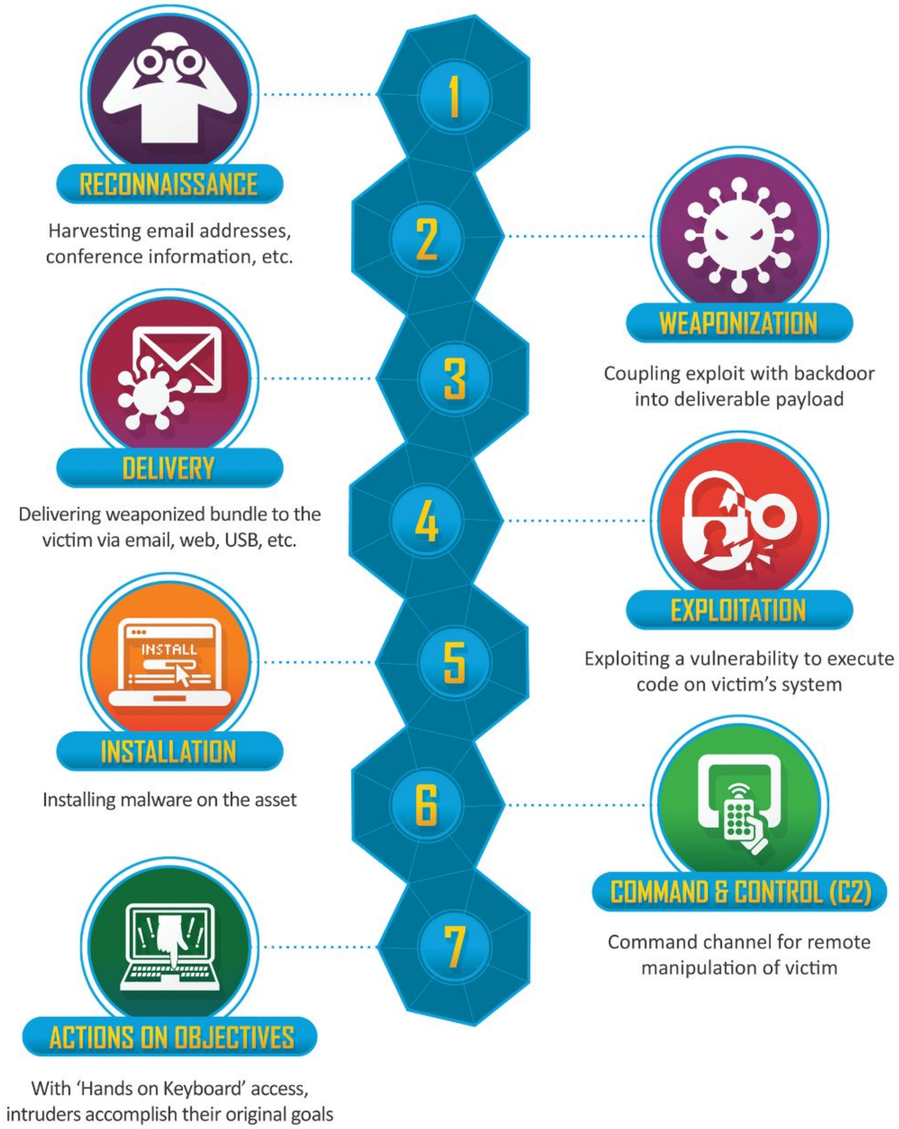
Just the TIP

- TIP = Threat Intelligence Platform
- Manually add Threat Intel
- Threat Intel feeds
- Use intel to add to firewalls, SIEMs, etc.

TIPs

- MISP
- YETI

Analytical Frameworks - Cyber Kill Chain



1 RECONNAISSANCE

Harvesting email addresses, conference information, etc.

2 WEAPONIZATION

Coupling exploit with backdoor into deliverable payload

3 DELIVERY

Delivering weaponized bundle to the victim via email, web, USB, etc.

4 EXPLOITATION

Exploiting a vulnerability to execute code on victim's system

5 INSTALLATION

Installing malware on the asset

6 COMMAND & CONTROL (C2)

Command channel for remote manipulation of victim

7 ACTIONS ON OBJECTIVES

With 'Hands on Keyboard' access, intruders accomplish their original goals

Analytical Frameworks - MITRE ATT&CK

- a

Proud Sponsors

Thank you to these organizations who give us their support:

BATTELLE

It can be done™

CRYPSIS™