How to Enumerate Threat Actors Using CrowdStrike Falcon X

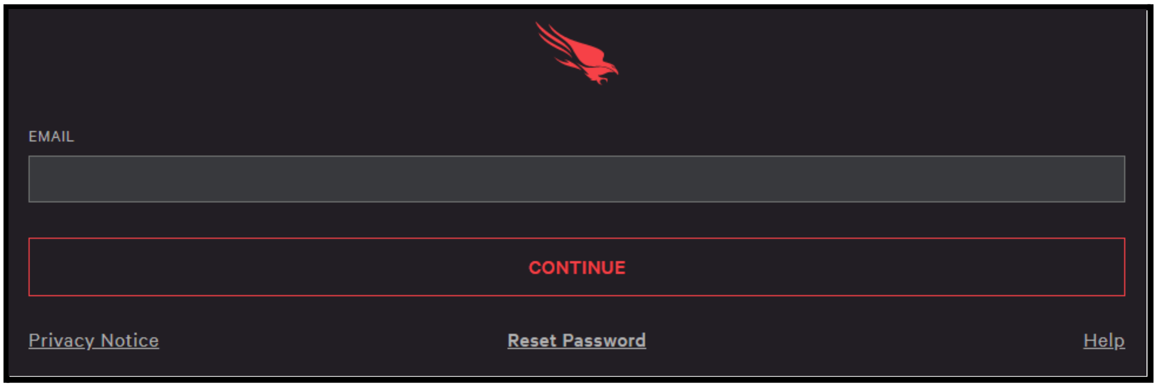
Task. Enumerate threat actors using CrowdStrike Falcon X.

Purpose. A threat model represents the assets, vulnerabilities, and threats of an organization. One major component of developing a threat model is enumerating the threat actors most likely to target the organization. With this insight, cybersecurity personnel can focus their Protection, Detection, and Response capabilities on adversarial techniques they will eventually have to defend the organization against.

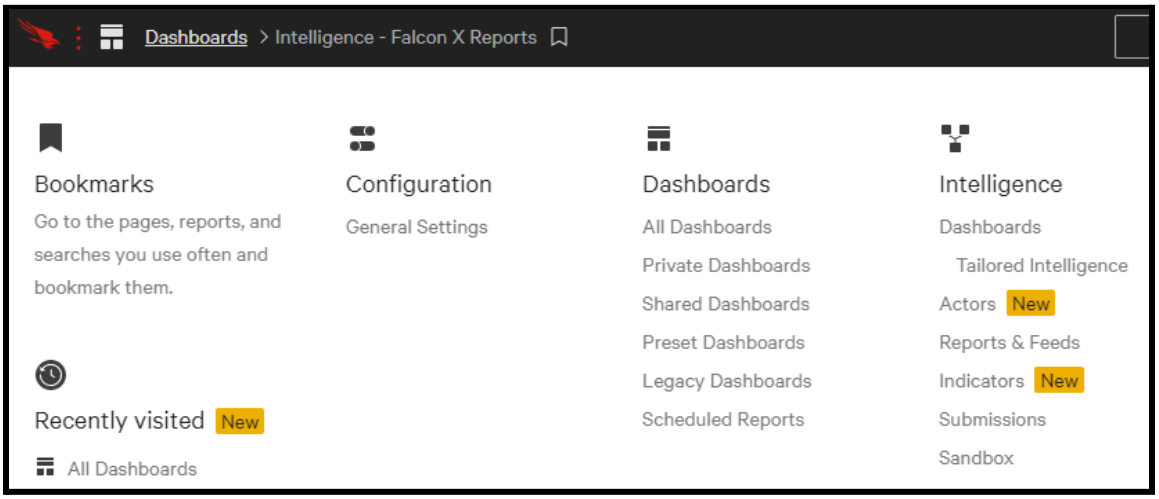
Conditions. You have access to CrowdStrike Falcon X.

Standard. You were able to enumerate threat actors using CrowdStrike Falcon X.

Step 1. Login to CrowdStrike Falcon X (https://falcon.crowdstrike.com/login/).

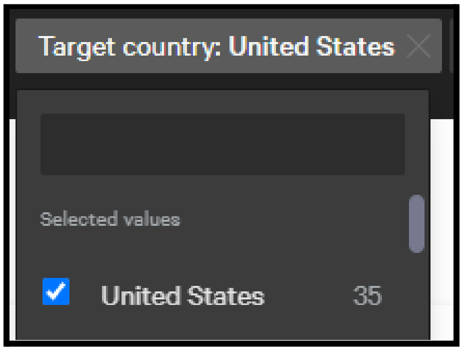


Step 2. Click-on the falcon icon in the top-left corner. Click-on "Actors" under the "Intelligence" column.



How to Enumerate Threat Actors Using CrowdStrike Falcon X

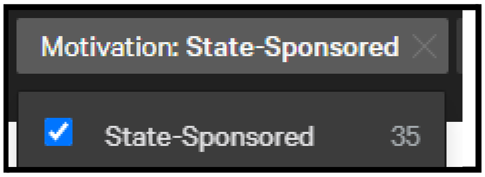
Step 3. Using the drop-down menus provided at the top of the page, select the values applicable to your organization. The screenshots below show values a United States government or military organization would use based on the nation state cyber threats identified by the CISA (reference: https://www.cisa.gov/cybersecurity).



Target country: United States

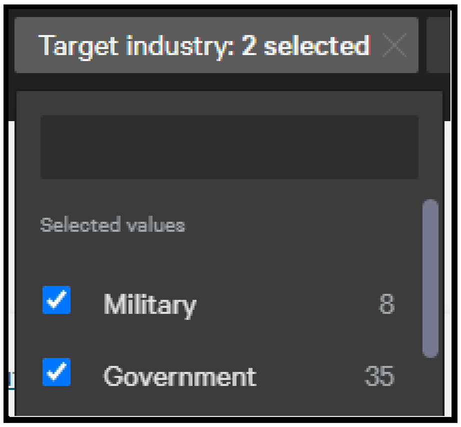
Selected values

☑ United States 35



Motivation: State-Sponsored

☑ State-Sponsored 35

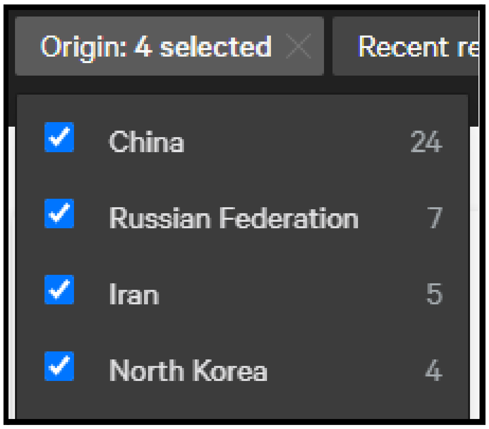


Target industry: 2 selected

Selected values

☑ Military 8

☑ Government 35



Origin: 4 selected

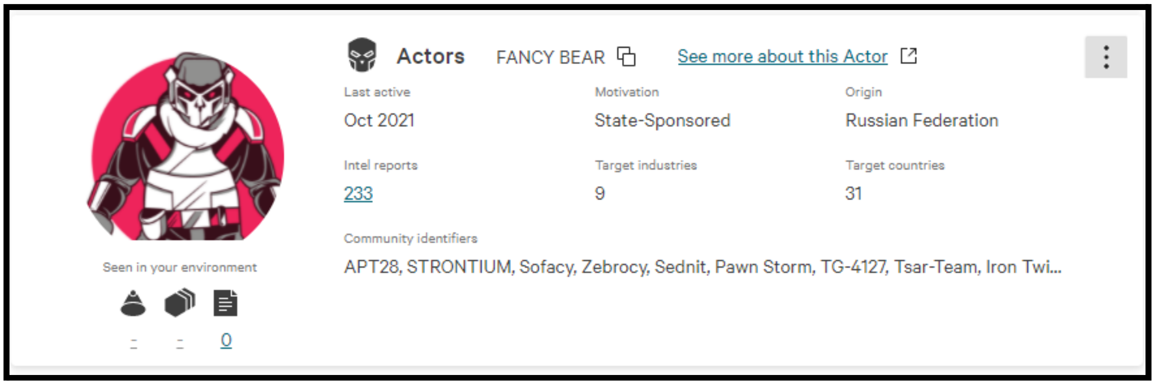
☑ China 24

☑ Russian Federation 7

☑ Iran 5

☑ North Korea 4

Once the filters you selected have been applied, the page should display a number of information cards like the one shown in the screenshot below.



Actors FANCY BEAR

Last active: Oct 2021

Motivation: State-Sponsored

Origin: Russian Federation

Intel reports: 233

Target industries: 9

Target countries: 31

Community identifiers: APT28, STRONTIUM, Sofacy, Zebrocy, Sednit, Pawn Storm, TG-4127, Tsar-Team, Iron Twi...

Seen in your environment: - - 0

Step 4. For each threat group listed, click-on “See more about this Actor” and review the following details: Last Active, Community Identifiers, and Kill Chain. Use this information to build a Cyber Threat Intelligence (CTI) overlay and enhance the organization’s Protection, Detection, and Response capabilities.