Lab#7: Threat and Event Catalog
Grade: 7%

Learning objectives:

- How to create a Cyber Threat Actor Profile
- How to define and describe a cybersecurity event

Part A: 50 Points

In this part you will research and document a threat profile for a cyber-attack. The part proceeds in three steps (1) Threat Actor Selection, (2) Threat Actor Research, (3) Threat Actor Documentation. These skills are crucial to success as a cybersecurity analyst.

Research cybersecurity threat actors and select one to become the basis of a Threat Catalog entry that you envision could threaten an organization with which you are familiar. That is, it is easier to figure out what the threat actor is after if you are familiar with the target. The target could be your home, school, office, volunteer organization, local or other government etc. Below are some websites that report on cybersecurity threats that you should peruse for ideas. You can also start with a threat actor you have read about in the newspaper or other media source. For general background on the types of activities engaged in by threat actors in general, see: https://krebsonsecurity.com/

Here are some websites that report on cybersecurity threats that you should peruse for ideas:
https://attack.mitre.org/groups/
https://www.us-cert.gov/ics/content/cyber-threat-source-descriptions

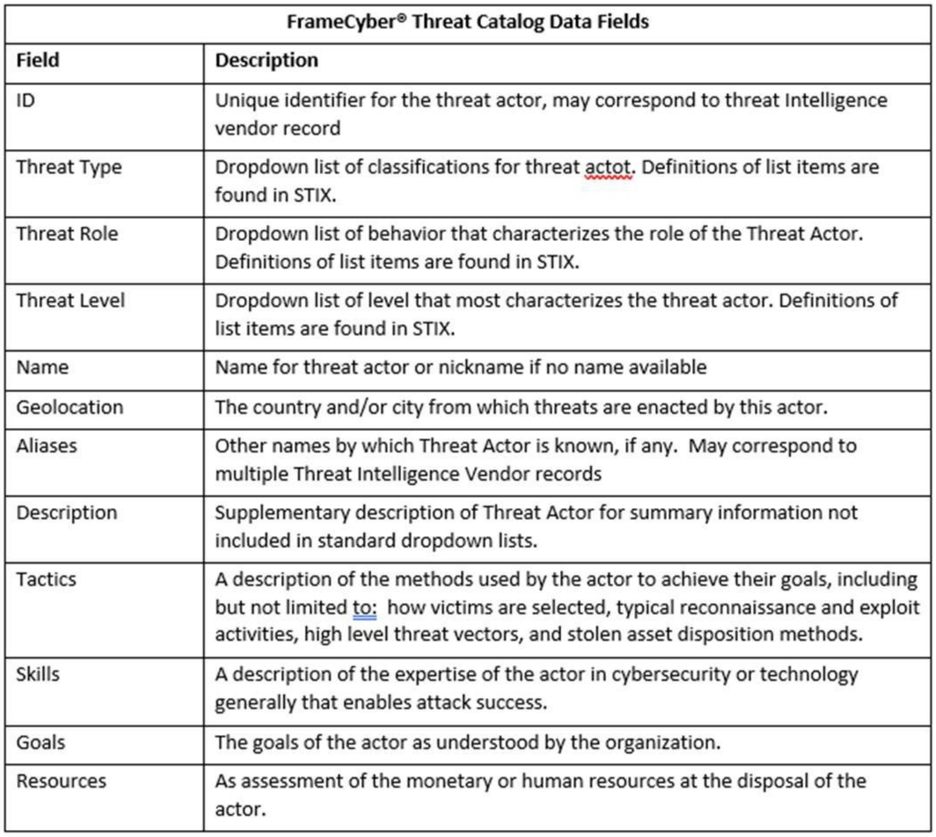
Posted in your assignment is the cybersecurity industry standard field reference for sharing information about threats (STIX-Version-2.1,pdf). Make sure to use the terms in this document consistent with the way they are used therein (the relevant Threat Actor Sections are 4.16 and 10.22 through 10.24).
Official site is:
http://docs.oasis-open.org/cti/stix/v2.0/stix-v2.0-part1-stix-core.html

Even if you understand the pdf in the assignment, you should look at these sites anyway to gain a deeper understanding of how Threat Actors are typically documented.
https://attack.mitre.org/groups/
https://www.us-cert.gov/ics/content/cyber-threat-source-descriptions
https://www.fireeye.com/current-threats/apt-groups.html
https://www.crowdstrike.com/blog/meet-the-adversaries/
http://docs.oasis-open.org/cti/stix/v2.0/stix-v2.0-part1-stix-core.html

Build A Threat:

Once you have chosen a Threat Actor, expand your research further to gather more details. Search for the fieldnames in the STIXTM documentation (the Threat Actor classification sections are 4.16 and 10.22 through 10.24) and if you think you need more information to be confident you know your threat actor, google them and search for them on the threat intelligence sites listed above in section 1, or others you find in the QU libraries or online. Use prudent judgment to try to make sure you do not to fall into sites that are purely advertising or possibility disinformation threats.

For each data field shown below, use the information you have gathered from your research to document your Actor using the industry standard specific terms you are discovering. Create a similar table and add your description you have gathered for the threat actor you have chosen. Submit it as one page pdf.



FrameCyber® Threat Catalog Data Fields

Field	Description
ID	Unique identifier for the threat actor, may correspond to threat Intelligence vendor record
Threat Type	Dropdown list of classifications for threat actot. Definitions of list items are found in STIX.
Threat Role	Dropdown list of behavior that characterizes the role of the Threat Actor. Definitions of list items are found in STIX.
Threat Level	Dropdown list of level that most characterizes the threat actor. Definitions of list items are found in STIX.
Name	Name for threat actor or nickname if no name available
Geolocation	The country and/or city from which threats are enacted by this actor.
Aliases	Other names by which Threat Actor is known, if any. May correspond to multiple Threat Intelligence Vendor records
Description	Supplementary description of Threat Actor for summary information not included in standard dropdown lists.
Tactics	A description of the methods used by the actor to achieve their goals, including but not limited to: how victims are selected, typical reconnaissance and exploit activities, high level threat vectors, and stolen asset disposition methods.
Skills	A description of the expertise of the actor in cybersecurity or technology generally that enables attack success.
Goals	The goals of the actor as understood by the organization.
Resources	As assessment of the monetary or human resources at the disposal of the actor.

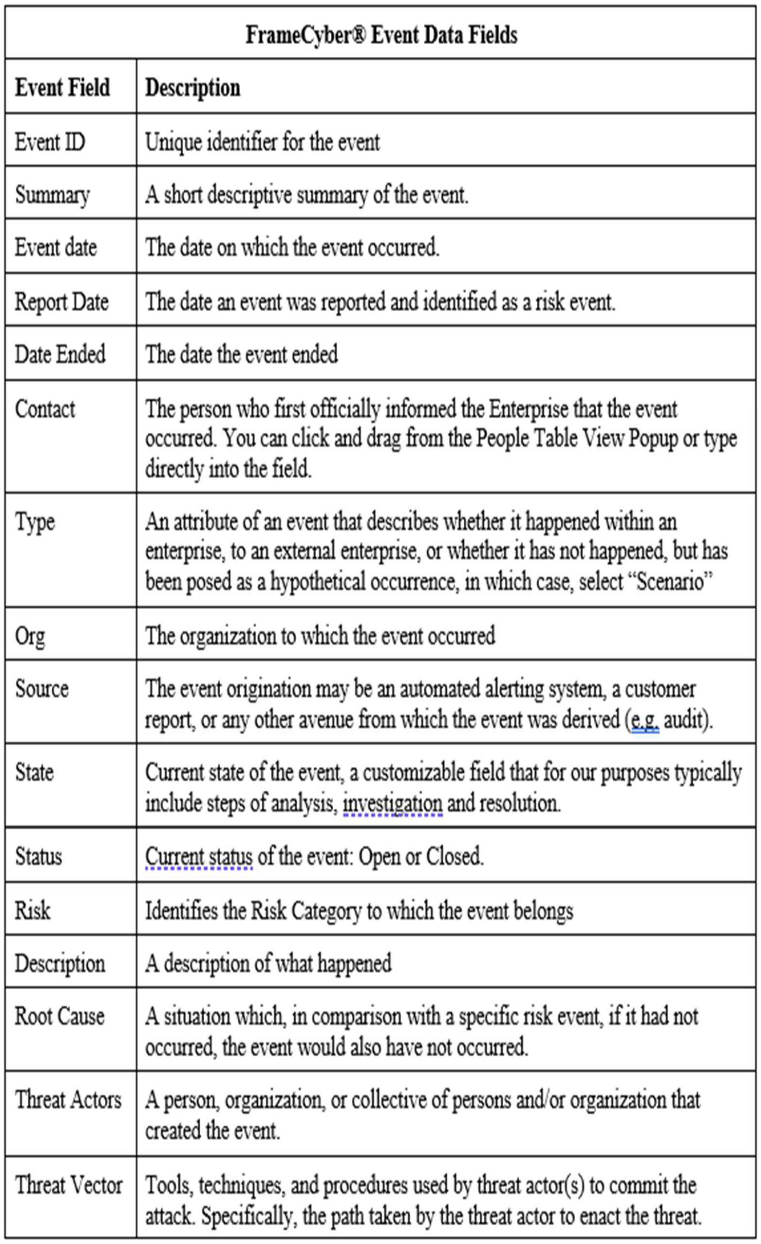
Part B: 50 Points

In this part you will document a cybersecurity event and corresponding impact analysis. The Assignment proceeds in four steps (1) Scenario Event Selection, (2) Define a Scenario Event (3) Build A Scenario Description and (4) Document the Event

These skills are crucial to success as a cybersecurity analyst.

Select a Scenario Event:
For this part, you will select a cybersecurity attack to become the basis of a hypothetical scenario that you envision could occur to an organization with which you are familiar. The attack must have significant impact on the organization, and this significant means financial losses. So, choose an attack that will have significant negative impact the organization and be able to explain why that impact results in dollars lost. Here are some websites that report on cybersecurity events that you should peruse for ideas:

https://attack.mitre.org/
https://krebsonsecurity.com/
https://news.cnet.com/
https://searchsecurity.techtarget.com/
https://threatpost.com/
https://www.csoonline.com/
https://www.darkreading.com/
https://www.networkcomputing.com
https://www.informationweek.com
https://www.infosecurity-magazine.com/
https://www.cio.com



FrameCyber® Event Data Fields	
Event Field	**Description**
Event ID	Unique identifier for the event
Summary	A short descriptive summary of the event.
Event date	The date on which the event occurred.
Report Date	The date an event was reported and identified as a risk event.
Date Ended	The date the event ended
Contact	The person who first officially informed the Enterprise that the event occurred. You can click and drag from the People Table View Popup or type directly into the field.
Type	An attribute of an event that describes whether it happened within an enterprise, to an external enterprise, or whether it has not happened, but has been posed as a hypothetical occurrence, in which case, select "Scenario"
Org	The organization to which the event occurred
Source	The event origination may be an automated alerting system, a customer report, or any other avenue from which the event was derived (e.g. audit).
State	Current state of the event, a customizable field that for our purposes typically include steps of analysis, investigation and resolution.
Status	Current status of the event: Open or Closed.
Risk	Identifies the Risk Category to which the event belongs
Description	A description of what happened
Root Cause	A situation which, in comparison with a specific risk event, if it had not occurred, the event would also have not occurred.
Threat Actors	A person, organization, or collective of persons and/or organization that created the event.
Threat Vector	Tools, techniques, and procedures used by threat actor(s) to commit the attack. Specifically, the path taken by the threat actor to enact the threat.

https://www.scmagazine.com/
https://www.verizon.com/business/resources/reports/dbir

Build A Scenario Description:

- Expand your research further to gather more details. See the list of Event data fields and their definitions below and use them to describe a hypothetical attack in industry standard terms.

- For each field given below, use the information you have gathered from your research to document your Scenario using the industry standard specific terms you are discovering. Create a similar table and add your description you have gathered for the event you have chosen. Submit it as one page pdf.

- Several of the fields are intended to classify the event so that busy executives can see quick summaries of events of interest to their cybersecurity team. For example, in this case, our event "Type" will be "Scenario" to distinguish it from events that are actual attacks in progress. The "Priority" field is used to convey a sense of urgency, an indication of the relative level of resources the cybersecurity program is devoting to investigating the event. “Status” and “State” further classify the event as “Open,” “Closed,” or in some intermediate state like “Analyze” or “Post-Mortem.”

- The Scenario Contact is a Senior Executive in the organization who presumably have all the business records required to estimate how much money may be lost or unexpectedly expended dur to a cyber event. This person is best equipped to be the to provide oversight to the scenario analysis process. Once you have completed your research, make sure your “contact” choice is based on the process of the organization that is under attack.

- Note that a root cause is: “A situation which, in comparison with a specific risk event, if it had not occurred, the event would also have not occurred.” This refers to an organizational situation that, if changed, would prevent the event’s recurrence. Note that a vulnerability is not a root cause, it is a proximate cause. There will always be vulnerabilities. The root cause is typically some organizational behavior that has to change to prevent an event’s recurrence.

- The Threat Vector is a sequence of activities undertaken by the threat actor or software working in concert with the threat actor to accomplish the attack. Use the MITRE ATT&CK framework as your guide in coming up with the set of activities your threat actor would need to perform to accomplish their objectives.

- There are date fields for the date of the event, the date the event was reported, and the date the event ended. The date reported is important because many organizations do not know they have been hacked until long after the event began. The end date is important because it is the date that the organization considers the attack to have been eradicated. Many organizations use the length of an attack as a performance measure for their cybersecurity program.

Submission:
Submit both PDF documents to D2L.