INTELLIGENCE METHODOLOGIES
REFERENCE SHEET

RED TEAMING

Summary:
Red teaming is an independent group that thinks from the perspective of an organization's adversaries. Red teaming can help reveal gaps and weaknesses in an organization's existing processes or security and help in creating strategies to overcome possible exploits. Red teaming is most beneficial as done before deploying new security strategies or implementing new organizational processes.

How it is done:
Red teaming exercises examine what information an adversary would want. How the adversary could obtain this information and what impact the loss of the information would have on the organization or the adversary.

Required Tools:
Red teams utilize tools that would be available to an organization’s adversaries, including access to hardware, software, and network.

Required Data:
Red teams utilize data that would be available to an organization’s adversaries. This data includes open source information and information openly available, such as documents left in print or online, attacker’s tools, and malware.

SOCIAL NETWORK ANALYSIS

Summary:
Social network analysis (SNA) examines relationships. It helps organizations determine entities’ roles, relationships, and levels of influence over others. SNA should be performed after sufficient information is collected on the entities being compared.

How it is done:
SNA is performed by examining links between related entities. Relationships can include familial, business, connections on social media, ideological, or physical location. Typically, these links are represented on a visual social network diagram. Some software automates the link generation process based on user input or open source information, while other software requires links to be drawn manually.

Required Tools:
Several software tools help perform SNA, including Onyx, Maltego, U2 Analyst’s Notebook, Palantir, and Gephi. SNA could also be performed without software.

Required Data:
SNA requires information about the relationships between entities. For example, if an organization is examining the organizational structure of a cybercrime group, the organization may collect information on how different members interact, what operating system they use, or what other software they utilize.

Expected Outcome:
SNA can help organizations determine links between entities as well as what entities influence others.

References:

IMPACT V. PROBABILITY GRAPH

Summary:
An impact v. probability graph examines the probability an event will occur and the impact that event would have on an organization. As this methodology aids in prioritizing potential risks, organizations should gather information on threats before using this methodology.

How it is done:
This graph requires two axes, one labeled “Probability” and the other labeled “Impact.” The point where these axes meet is considered the lowest probability of the event occurring and the lowest impact an event would have. The probability and impact move farther from the origin. Probability is defined as the risk that an event will occur and the impact is defined as the negative effect an event will have on an organization. Each potential threat is plotted on the graph according to its probability and impact. Threats that are toward the top right corner are most severe threats in the bottom left corner are low level threats.

Required Tools:
This methodology can be performed using a pen and paper or whiteboard, but software may be helpful. Organizations may find spreadsheet and graphing software such as Microsoft Excel useful, especially if the organization wishes to weight certain factors (such as risk aversion). Additionally, organizations may employ binary risk analysis to help measure potential impacts and probabilities.

Required Data:
Organizations should gather information on potential threats, including the probability of an event occurring and the impact that event would have on an organization. To examine probability, organizations may collect information on potential threat actor’s capabilities for performing an attack or that actor’s intent to perform the attack. This information may include the tools and software available to the actor or the actor’s past history performing attacks. To examine impact, organizations may collect information on the monetary costs of an attack or the attack’s impact on reputation. This information may include the cost to a company to fix a vulnerability or the extent of an attack.

Expected Outcome:
As a result of this methodology, organizations can perform an attack or that actor’s intent to perform the attack. This information may include the tools and software available to the actor. This methodology can be used by organizations to prioritize potential threats based on probability of occurrence and potential impact. Additionally, this methodology can help organizations to monitor threats before using this methodology.

References:

AFFINITY CLUSTERING

Summary:
Affinity clustering is a technique for sorting items according to similarity. Affinity clustering can be performed after information is collected or revised patterns or gaps.

How it is done:
To perform affinity clustering, individual data points are captured in a conventional workspace. Those data points are then grouped into clusters based on similarity and the data clusters are assigned labels.

Required Tools:
Affinity clustering can be performed using cards or sticky notes for each piece of information, but mind mapping tools may be helpful. Mind mapping tools include MindMeister, Mindomo, or MindNode tools.

Required Data:
The specific data required depends on the relationship being examined. For example, if an organization is examining tools used by different cybercrime organizations to obtain personal information, they should gather information as the name of the tool, what other activities the tool can be used for, what operating system the tool runs on, and what type of information was stolen.

MULTI-CRITERIA DECISION MAKING

Summary:
Multi-criteria decision making (MCDM) evaluates possible courses of action (COAs) against an unbalanced set of criteria. Since MCDM requires an organization to specify criteria that should be most and possible COAs, MCDM is used during the decision-making process or at the end of an analysis phase.

How it is done:
MCDM is performed using a matrix with one axis containing criteria and the other containing possible COAs. The COAs then are given a score from one to three based on how well the COA satisfies the criteria, with a score of one given to a COA that does not affect any of the criteria and three given to a COA that effectively satisfies the criteria. After each criterion is evaluated, each COA's scores are added up and the COA with the highest score best satisfies all given criteria.

Expected Outcome:
MCDM can help organizations determine a course of action that best satisfies a list of established criteria.

References: