Acquisition

Based on the product technical specifications / conops
- -identifyLogical and physical architecture,
- Management interfaces,
- External interfaces,
- Mission data stored and processed,
- Mission capabilities,
- Critical program information,
- Security perimeters,
- Security capabilities,
- Operational TTPs,
- Security incident data,
- User roles and permissions, and: COTS

CJA: Crown jewels analysis

It is not cost effective to design every Cyber Asset to operate through an attack. Instead, we must find the mission-critical Cyber Assets and assure they can operate through.

TARA

- Knowledge Management
- CTSA
- CRRA

Develop the AV, CM, mapping catalog using CAPEC, ATT&CK, CAR and D3FEND

3.3.CRRA: Cyber Risk Remediation Analysis

1.Obtain initial mitigation mapping table

2.Amend countermeasures list

Add countermeasures and/or mappings to fill gaps and address scoping requirements; remove countermeasures that don't apply. Associate CM effects

3.countermeasure scoring

- Utility
- Cost

1.Total the number of P's and R's across all attack vector columns
2. Optional: Select a weighting scheme for P's and R's
3. Utility Score = (Total P's)*Weighting(P) + (Total R's)*Weighting(R)

Compute utility/cost (U/C) ratio for each CM and rank them in the mitigation table

4.Mitigation selection

Mapping table architecture

•Attack vectors with the highest risk scores are solved first
– order attack vectors (columns) from left to right by descending risk
• Countermeasures with the highest ranking are selected first
– order countermeasure (rows) from top to bottom
using the preferred reordering strategy
• Once selected, the countermeasure applies to all attack vectors
– The goal is to select the minimum number of CMs

Selection strategy

ex: Construct a solution set containing at least 3 CMs for each attack
vector with high risk, at least 2 CMs for each attack vector with moderate risk, and at least 1 CM for each attack vector with low risk

Optimal Solution minimize the number of CMs

5.Prepare Recommendations

Translate the CM solution list into well-formed recommendations.Each including:
1. The action, device, procedure or technique recommended, i.e., which CM to be applied
2. The reason why the CM is required, i.e., the TTPs that it mitigates
3. The implication or effect if the CM is not applied, i.e., the potential impact to mission capability resulting from compromise of the cyber asset

Mitigation mapping data & Countermeasures

input

3.2.CTSA: Cyber threat susceptibility analysis

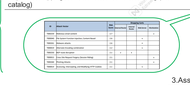
Identify the important attack vectors that we will deal with:

filter/ narrow down the list of AVs. use keyword search from the catalog according to your product

Identify shopping carts categories

Populate shopping carts with AVs from the catalog (filter catalog)

2.Create shopping carts



3.Assess attack vector risk (score)

Risk Score = Σ (risk factor value) * (factor weighting))

4.susceptibility matrix

input

Attack vectors

input

Threat actor profiles

Exploitable attack surface features (entry points & targets)

Threat scenarios

1.Develop a cyber threat model

Solution Effectiveness Table

For each CM it identifies the preventative or mitigating effect(s) it has over the range of attack vectors.
It also provides a cost summary and indicates whether the selection strategy is satisfied for each attack vector, or where gaps exist.