# Cyber – Supply Chain Risk Management (C-SCRM) Assignment

**Objective:** Togain an understanding of C-SCRM by reviewing prior analysis of identified potential risks, and proposed risk mitigation plans. To learn how to use OSINT to better understand C-SCRM real and potential vulnerabilities.

1) Review example Software Bill of Materials (SBOM) provided by CAST Highlight and answer the questions that follow each:
    a. Closely examine the complete list of all detected open source and 3rd party components along with relevant data about each (hover over column headers to see a description of each).
        i. How many 3rd-party components were detected using the CAST HIGHLIGHT tool SBOM s/w composition analysis?
        ii. What is the oldest release date of the version of the components identified in use?
        iii. Were there any 'high' CVEs noted for possible vulnerabilities for the oldest release date? If so, what were they?
    b. Review the list of components that are referenced by the detected components, also known as "transitive dependencies," along with relevant data about each (hover over column headers to see a description of each).
        i. How many 3rd party components were detected that had a transitive dependency on another component?
    c. Cross reference the list of recommended safer component versions to use vs. the detected component which contained a critical security vulnerability that should be remediated (hover over column headers to see a description of each).
        i. Was going to Safer component versions able to mitigate all High CVE vulnerability risks? Medium? Low? If yes to any, how many risks were there to start? If no, how many components remained with High, Medium, or low risks still there, with the safest version alternative?
    d. Review the list of sever weaknesses automatically detected in components with a description of the weakness (hover over column headers to see a description of each).
        i. What 3rd party component created the most Common Weakness Enumeration issues?
        ii. Of the CWEs reviewed, were there any that were part of the Open Web Application Security Project 25 most dangerous software weaknesses? Which CWE?
        iii. Using OSINT, find the top 10 vendors affected by this vulnerability.
    e. Browse the list of detailed meta data about each detected component (e.g., the exact file path to the component in the codebase)
        i. How many names of the detected components that matched with a file fingerprint in the CAST Highlight component knowledgebase were found in the local path of the file?