Assignment

CSN3614 - Cybersecurity: Theory and Practice

Deadline: 22nd June 2025 before 11.59 pm (Sunday)

Group Member: 2 to 4 members

Objective:

Evaluate threats to supply chains and other kinds of threat intelligence by researching well-defined cybersecurity frameworks.

Part 1: Threats to Supply Chains

1. **Introduction to Supply Chain Threats**
    - Explain what **supply chain cybersecurity** is and why it is a critical concern for organizations.
    - Provide examples of recent cyberattacks on supply chains, highlighting how attackers exploited vulnerabilities in the supply chain. For example, discuss the **SolarWinds** cyberattack or other relevant incidents.
2. **Types of Threats to Supply Chains**
    - Identify and explain at least **three types of cybersecurity threats** that commonly affect supply chains (e.g., **malware**, **third-party vendor vulnerabilities**, **data breaches**).
    - For each threat, explain how attackers exploit the weaknesses in the supply chain and provide an example of a real-world incident or case.

3. **Impact of Supply Chain Attacks**

    - Discuss the potential impact of a supply chain attack on an organization, focusing on both **short-term** and **long-term** consequences. Consider aspects such as **revenue loss**, **reputation damage**, and **legal consequences**.

Part 2: Cybersecurity Frameworks for Threat Intelligence

1. **Overview of Cybersecurity Frameworks**

    - Research and describe at least **two cybersecurity frameworks** used for identifying and mitigating threats in the context of supply chains. Possible frameworks may include:

        - **NIST Cybersecurity Framework (CSF)**

        - **ISO/IEC 27001**

        - **CIS Critical Security Controls**

        - **Cybersecurity Maturity Model Certification (CMMC)**

2. **Framework Application to Supply Chain Security**

    - For each framework discussed, explain how it can be applied to manage and mitigate supply chain threats. Focus on specific aspects of the framework, such as:

        - Risk management strategies
        - Incident response and recovery
        - Access control and vendor management

3. **Threat Intelligence and Framework Integration**
    - Explain how **threat intelligence** (e.g., information about known vulnerabilities, attack vectors, or malicious actors) can be integrated into a cybersecurity framework to enhance protection against supply chain attacks. Discuss the role of threat intelligence in proactive defense and its application within the selected frameworks.

Part 3: Recommendations and Mitigation Strategies

1. **Best Practices for Supply Chain Cybersecurity**
    - Provide **five actionable best practices** that organizations should implement to strengthen their supply chain security. Base these practices on your research of cybersecurity frameworks and real-world threat intelligence.
2. **Vendor and Third-Party Risk Management**
    - Explain how organizations can assess and manage **third-party risk** within their supply chains. What steps can be taken to ensure that vendors and suppliers meet cybersecurity requirements? Provide examples of **vendor risk management policies** that organizations can adopt.

Deliverables

- **Written Report** (1500–2000 words) covering the points listed above.
- **Power Point Slides**
- **Completion of Peer Evaluation Report (to be done by each student) - https://forms.gle/W8g8ti2J9HXGwp5p7**
- **References**: Use at least **five sources**, including research papers, cybersecurity standards, and real-world case studies (cite in APA or MLA format).

Non completion of Peer Evaluation Report will result in a penalty of 5% from the total mark.

Late Submission Rubric

Time Late	Penalty Applied
On time	**Full credit**
Up to 24 hours late	**-10% of total possible points**
24 to 48 hours late	**-20% of total possible points**

48 to 72 hours late	**-30% of total possible points**
More than 72 hours late	**-50% of total possible points**

Grading Rubric

Written Report (50%)

Criteria	Excellent: 4 marks	Good: 3 marks	Satisfactory: 2 marks	Fair: 1 mark	Total
1. Understanding of Supply Chain Threats (13%)	Provides a comprehensive, detailed explanation of supply chain cybersecurity with multiple recent examples of cyberattacks. Identifies and thoroughly explains at least three types of cybersecurity threats, backed by real-world case studies. Explains how attackers exploit vulnerabilities clearly.	Solid explanation of supply chain cybersecurity with at least two relevant examples of cyberattacks. Identifies and explains three types of cybersecurity threats. Provides examples of how attackers exploit weaknesses, but some explanations may lack depth.	General explanation of supply chain cybersecurity, lacks detail in examples or depth of explanation. Identifies fewer than three types of threats or provides limited examples. Weak or incomplete connection between attacker exploitation and vulnerabilities.	Vague or overly general explanation of supply chain cybersecurity with few or no real-world examples. Fewer than two types of threats identified, with minimal or unclear explanation of how attackers exploit them.	__/52
2. Research on Cybersecurity Frameworks (14%)	Thoroughly describes at least two widely-recognized frameworks (e.g., NIST CSF, ISO/IEC 27001, CMMC). Well-supported with clear insights into how the frameworks address supply chain threats. Details risk management, incident response, and access control.	Describes two frameworks with some lack of detail or clarity. Frameworks are applicable to supply chain threats, but more specific examples or applications could be included.	Describes one framework adequately, or multiple frameworks with limited detail. The discussion lacks critical insight into how the frameworks apply to supply chains.	Only one framework described with a superficial explanation. Many key aspects (e.g., risk management, incident response) are missing or poorly explained.	__/56
3. Threat Intelligence and Framework Integration (9%)	Explains how threat intelligence enhances protection against supply chain attacks and integrates within frameworks (e.g., proactive defense, vulnerability detection).	Describes the integration of threat intelligence into frameworks, but lacks specific details or examples.	Basic explanation of threat intelligence, but weak connection to cybersecurity frameworks. Importance of threat intelligence noted, but integration not fully explained.	Little or no explanation of threat intelligence and its integration with cybersecurity frameworks. The connection is unclear or absent.	__/36
4. Recommendatio	Provides five clear, practical best practices for supply chain security, backed by research, frameworks, and case studies. Thoroughly	Offers five practical recommendations, but some may lack depth or specific application. Vendor and third-party risk	Lists recommendations that are too general or not fully applicable to supply	Fewer than five recommendations or vague suggestions. Vendor and	__/32

ns and Mitigation Strategies (8%)	addresses vendor and third-party risk management with practical solutions.	management is addressed with less detail or fewer examples.	chains. Minimal discussion of third-party risk management.	third-party risk management not addressed or discussed minimally.	
5. Structure, Writing Quality, and References (6%)	Well-organized, clear, and concise report. Free of grammatical errors, with smooth transitions. Proper citation format with at least five credible sources in APA/MLA format.	Clear and organized report, minor grammatical issues or awkward phrasing. Mostly correct citation format with credible sources, but slight issues in referencing style.	Organized but with several grammar or clarity issues. Some sections may be underdeveloped or overly repetitive. Inconsistent citation format.	Difficult to follow report with multiple grammar and clarity issues. Poor organization and cohesion. Missing or improperly cited references.	__/24
TOTAL					___/200

Group Presentation (25%)

Criteria	Excellent: 4 marks	Good: 3 marks	Satisfactory: 2 marks	Fair: 1 mark	Total
Content & Clarity (4%) - Clear explanation of cybersecurity concepts and supply chain threats (Group)	Concepts clearly explained, well-connected to assignment	Mostly clear, minor gaps	Basic explanation, lacks depth or accuracy	Confusing, lacks clarity and relevance	__/16
Content & Clarity (4%) - Relevant case studies and real-world examples (Group)	Strong, well-integrated examples	Relevant examples but brief	Limited examples or not well connected	Few/no examples, unclear purpose	__/16

Visual Aids/Slides (3%) - Design and Professionalism (Group)	Visually clean, consistent, readable	Mostly clear and consistent	Adequate but cluttered or inconsistent	Poor design, hard to follow	__/12
Visual Aids/Slides (2%) - Use of Visuals (charts, diagrams, etc.) (Group)	Excellent use of visuals to support content	Good visuals with some support	Basic visuals, limited support	Few/no visuals, poorly integrated	__/8
Individual Delivery & Communication (4%) – Speaking clarity and engagement (Individual)	Confident, clear, and engaging	Clear but occasionally hesitant	Understandable but lacks energy or clarity	Mumbled, rushed, or disengaged	__/16
Individual Delivery & Communication (3%) – Time management & role fulfillment (Individual)	Well-timed and balanced, fulfilled role fully	Slightly over/under time, role mostly fulfilled	Uneven timing or minor gaps in role	Poor time use or did not fulfill part	__/12
Q&A & Understanding (3%) - Accuracy and clarity in answering questions (Individual)	Answers show deep understanding	Generally clear and informed	Basic understanding, some uncertainty	Unclear or incorrect responses	__/12
Q&A & Understanding (2%) - Contribution to group Q&A (Individual)	Actively answered or supported team answers	Participated but not strongly	Limited participation	Did not participate or avoided Q&A	__/8
TOTAL					___/100

Peer Evaluation Form (25%) - to be done using Google Form

Group Member Name (Your Name): ___________________________

Group Number or Members' Names: ___________________________

Please evaluate each member of your group (including yourself) based on their contribution to the project using the following scale:
5 = Excellent | 4 = Good | 3 = Satisfactory | 2 = Poor | 1 = Very Poor | 0 = No Contribution

Group Member Name	Quality of Work	Participation & Effort	Communication & Collaboration	Reliability (met deadlines)	Overall Contribution	Total (out of 25)
Member 1						
Member 2						
Member 3						
Member 4 (optional)						