**1. Understanding Network Security Basics**

* **Foundations of network security** from *Kaufman et al. (2022)*, including how secure communication works in a public environment.
* Key **network protocols** and how they relate to security, as explained in *Orzach & Khuanna (2022)*, especially in Chapters 1 and 4.
* Real-world case study analysis of **major cyberattacks**, such as the *SolarWinds hack* (*Temple-Raston, 2021*), showing how attackers exploit network vulnerabilities.

**2. Identifying Threats and Vulnerabilities**

* How to **spot weaknesses in network systems** and understand their potential impact.
* Exploring different **types of vulnerabilities**, including those caused by poor configurations, outdated systems, or weak protocols.
* Insight into **vulnerability detection methods** through research articles like *Bennouk et al. (2024)*.

**3. Tools, Techniques, and Methodologies**

* Learning to apply the **right tools and techniques** to test, monitor, and secure networks.
* Understanding **risk management processes**, including how to prioritize and address security issues.
* Discussion on **best practices** for organizations moving toward full digital transformation, as explained in *Doroiman & Sîrghi (2024)*.

**4. Legal, Social, and Ethical Considerations**

* Addressing the **legal and ethical responsibilities** of cybersecurity professionals.
* Understanding the **professional role** in preventing, reporting, and managing security incidents.

**5. Practical Activities**

* **Collaborative Discussion 1:**
  + Reflect on what defines a fully digital enterprise.
  + Explore cybersecurity challenges for both digital-first companies and traditional SMEs going digital.
  + Share insights and solutions with peers.
* **Website Choice Activity:** Apply concepts by analyzing real-world websites for strengths and weaknesses.
* **Seminar Preparation:** Prepare for an in-depth look at the SolarWinds case study.

**Learning Outcomes**

By the end of this module, you will be able to:

1. **Identify and analyze network threats and vulnerabilities** and choose suitable methods to address them.
2. **Understand the ethical, legal, and professional challenges** in cybersecurity and risk management.
3. **Apply theoretical knowledge** through discussions, case studies, and hands-on activities.