**Week 2 Overview: Advanced Persistent Threats and the Cyber Kill Chain**

This week focuses on **Advanced Persistent Threats (APTs)** and how to analyze them using the **Cyber Kill Chain model**. You’ll apply this framework to a real-world case study — the **SolarWinds exploit** — to determine whether this model is still effective for understanding and preventing modern cyberattacks.

**Key Learning Areas**

1. **Understanding Advanced Persistent Threats (APTs):**
   * Explore what APTs are and why they pose a significant risk to organizations.
   * Review attacker techniques, strategies, and the long-term impact of these threats.  
     *(Based on Alshamrani et al., 2019).*
2. **The Cyber Kill Chain Model:**
   * Learn about Lockheed Martin’s Cyber Kill Chain and its stages, from initial reconnaissance to data exfiltration.
   * Understand how it helps map out attacker behavior and identify weak points for defense.
3. **SolarWinds Case Study:**
   * Review how the **SolarWinds breach** happened and why it was so impactful (*Temple-Raston, 2021*).
   * Apply the Cyber Kill Chain model to analyze the attack step-by-step.
   * Evaluate whether this model is still effective for modern, sophisticated attacks like SolarWinds.
4. **Mitigation and Defense Strategies:**
   * Identify measures to **prevent or reduce the impact** of similar exploits in the future.
   * Understand penetration testing best practices (*NCSC, 2017*) and **Cyber Essentials requirements** (*NCSC, 2021*).

**Practical Activities**

* **Collaborative Discussion 1:**  
  Continue discussions about digital enterprises and cybersecurity challenges:
  + Define what makes a **fully digital enterprise**.
  + Explore cybersecurity concerns for both digital businesses and traditional SMEs moving online.
* **Vulnerability Analysis – Literature Review:**
  + Research potential vulnerabilities using software security databases and audit tools.
  + Create a **baseline vulnerability report** for assigned websites.
  + Reflect on challenges faced during the research and how you overcame them.
* **Seminar Preparation:**
  + Prepare for the **SolarWinds breach seminar** by reviewing threats and analyzing response strategies.
* **Module Wiki Contribution:**
  + Share useful terms, concepts, and references to help your peers.

**Learning Outcomes by the End of Week 2**

You will be able to:

1. **Describe and apply the Cyber Kill Chain model** to modern cyberattacks.
2. **Identify and analyze network vulnerabilities**, and select appropriate tools and methods to address them.
3. **Design and evaluate security solutions** for auditing and managing risks.
4. **Gather and synthesize data** from multiple sources, including vulnerability databases and security alerts.
5. **Understand legal, ethical, and professional responsibilities** in cybersecurity roles.