**Week 1 – Course Intro & AI Security Landscape**

1. Software Engineering Institute, Carnegie Mellon University, “The Challenge of Adversarial Machine Learning,” SEI Blog, 2024.

**Week 2 – AI Fundamentals (ML, DL, Transformers, LLMs, RAG)**  
2. A. Vassilev et al., “Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations,” NIST AI 100-2e2025, 2025.

**Week 3 – Data Security in the AI Lifecycle**  
3. Queen’s University Belfast, Study of Research and Guidance on the Cyber Security of AI, UK Government Assets, 2024.

**Week 4 – Threat Modeling with Frameworks**  
4. OWASP Foundation, “OWASP Machine Learning Security Top 10,” 2025.  
5. MITRE Corporation, “MITRE ATLAS: Adversarial Threat Landscape for Artificial-Intelligence Systems,” 2025.

**Week 5 – AI in Attackers’ Hands (Deepfakes, Phishing, OSINT)**  
6. Center for Security and Emerging Technology, Adversarial Machine Learning and Cybersecurity, Georgetown University, Sep. 2024.

**Week 6 – Model Attacks (Poisoning, Evasion, Inversion, Membership Inference)**  
7. UC Berkeley Center for Long-Term Cybersecurity, Adversarial Machine Learning, Dec. 2019.

**Week 7 – Jailbreaking, Prompt Injection, Model Theft**  
8. Cloudflare, “What are the OWASP Top 10 risks for LLMs?” Cloudflare Learning Center, Aug. 2025.

**Week 8 – Guardrails & Model Interfaces**  
9. OWASP Foundation, “OWASP Top 10 for Large Language Model Applications 2025,” 2025.

**Week 9 – Access Controls & Encryption**  
10. Chaos Search, “How to Detect Threats to AI Systems with MITRE ATLAS Framework,” Chaos Search Blog, Oct. 2024.

**Week 10 – Monitoring, Logging, IR Basics**  
11. T. Balarabe, “Understanding Generative AI-Based Attacks with MITRE ATLAS,” Medium, Dec. 2024.

**Week 11 – Midterm Review & Case Applications**  
12. P. Vadillo et al., “Adversarial Attacks in Explainable Machine Learning: A Survey of Threats Against Models and Humans,” WIREs Data Mining and Knowledge Discovery, Oct. 2024.

**Week 12 – Case Study: Adversarial ML in the Wild**  
13. Artificial Intelligence Review, “Adversarial machine learning: a review of methods, tools, and critical industry sectors,” May 2025.

**Week 13 – Case Study: AI-Enabled Exploits (Deepfakes, Phishing)**  
14. Center for Security and Emerging Technology, Adversarial Machine Learning and Cybersecurity (case study revisit), Georgetown University, Sep. 2024.

**Week 14 – Risk Assessments & Synthesis**  
15. A. Vassilev et al., Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations(mitigation strategies), NIST AI 100-2e2025, 2025.

**Week 15 – Practicum Presentations & Wrap-Up**  
16. Queen’s University Belfast, Study of Research and Guidance on the Cyber Security of AI (review sections), UK Government Assets, 2024.