**Week 1 – AI Defenses: Guardrails & Access Controls**

1. OWASP Foundation, “OWASP Top 10 for Large Language Model Applications 2025,” 2025.

**Week 2 – Encryption, Masking, Redaction**  
2. Queen’s University Belfast, Study of Research and Guidance on the Cyber Security of AI (defensive practices section), UK Government Assets, 2024.

**Week 3 – Monitoring & Drift Detection**  
3. Chaos Search, “How to Detect Threats to AI Systems with MITRE ATLAS Framework,” Chaos Search Blog, Oct. 2024.

**Week 4 – Audit Trails & IR Playbooks**  
4. UC Berkeley Center for Long-Term Cybersecurity, Adversarial Machine Learning (IR strategies), Dec. 2019.

**Week 5 – AI-Assisted Security Tools (Code Analysis, Logs)**  
5. Center for Security and Emerging Technology, Adversarial Machine Learning and Cybersecurity, Georgetown University, Sep. 2024.

**Week 6 – AI in CI/CD & DevSecOps**  
6. A. Masood, “Responsible AI Revisited: Critical Changes and Updates Since Our 2023 Playbook,” Medium, May 2025.

**Week 7 – Governance Structures & Oversight**  
7. National Institute of Standards and Technology, “NIST AI Risk Management Framework (AI RMF 1.0),” NIST AI 100-1, Jan. 2023.

**Week 8 – Responsible AI (Fairness, Transparency, Accountability)**  
8. A. Masood, Responsible AI Revisited (fairness and updates), Medium, May 2025.

**Week 9 – NIST AI RMF Deep Dive**  
9. National Institute of Standards and Technology, “NIST AI RMF Playbook,” Feb. 2025.

**Week 10 – EU AI Act (Global Compliance)**  
10. European Commission, “EU AI Act | Shaping Europe’s digital future,” 2025.  
11. Future of Life Institute, “EU AI Act Compliance Checker,” 2025.

**Week 11 – Corporate Audit Readiness**  
12. A-LIGN, “Preparing for EU AI Act Compliance with ISO 42001,” Apr. 2025.  
13. International Association of Privacy Professionals, “EU AI Act Compliance Matrix,” 2025.

**Week 12 – Advanced Defenses & Layered Security**  
14. Artificial Intelligence Review, “Adversarial machine learning: a review of methods, tools, and critical industry sectors,” May 2025.

**Week 13 – Capstone Work Week (Team Progress)**  
15. S. H. Cen and R. Alur, “From Transparency to Accountability and Back: A Discussion of Access and Evidence in AI Auditing,” arXiv preprint arXiv:2410.04772, Oct. 2024.

**Week 14 – Capstone Presentations (Groups A & B)**  
16. S. Casper, C. Ezell, C. Siegmann, et al., “Black-Box Access is Insufficient for Rigorous AI Audits,” arXiv preprint arXiv:2401.14446, 2024.

**Week 15 – Final Exam & Course Reflection**  
17. A. Masood, Responsible AI Revisited (reflection sections), Medium, May 2025.