Where do I want to be by the end of this period/year? What do I want to be doing? (Include as many learning needs as required to achieve agreed objectives)

Where do I want to be by the end of this period/year? What do I want to be	What do I want/need to learn? (Skills/Knowledge/Topics to cover)	What do I have to do to achieve this? (Courses, research, mentoring, etc.)	What resources or support will I need? (Tutors, library, advisors, managers, etc.)	How will I measure success? (Assessments, feedback, appraisals, etc.)	Target dates for review and completion
Have a strong foundational understanding of network security principles and be able to apply practical skills in real-world environments	- Network protocols and vulnerabilities - Use of security tools (Nmap, Nikto, Burp Suite) - Risk assessment and mitigation - Understanding logging and forensics in breach investigations - Knowledge of GDPR and ISO/IEC 27001 security standards - Implementation of secure authentication and encryption techniques	- Complete all module assignments and labs - Practice vulnerability scanning and penetration testing on labs or VMs - Read up-to-date literature on network security and compliance - Attend webinars or workshops on cybersecurity best	- Access to lab environments with security tools - Tutor and technical support for practical exercises - Library or online access to relevant security frameworks and compliance documentation	- Grades and feedback from assignments and labs - Practical demonstration of vulnerability scans - Positive tutor feedback on understanding and application of concepts	End of the module/ year (e.g., Dec 2025)
Develop capability to analyze and report security incidents effectively	- Forensics analysis - Log analysis and interpretation - Incident response frameworks and tools	- Engage in case studies and incident response simulations - Research real-world breach investigations - Collaborate in team-based incident response exercises	- Access to forensic tools and case study materials - Mentoring from experienced security professionals - Peer collaboration opportunities	- Assessment results on incident response tasks - Ability to produce incident reports - Feedback from mentors and peers	Mid-module review and final assessment

Gain skills in secure software development practices to reduce vulnerabilities	- Secure coding standards - Understanding common software vulnerabilities (e.g., injection attacks) - Use of static analysis tools (Pylint, Flake8) - Implementing MFA and secure password hashing	- Undertake additional training on secure coding - Apply static code analysis tools to projects - Develop and test secure authentication mechanisms	- Access to development environments and code analysis tools - Support from software development tutors - Online courses or	- Quality of code as per linter reports - Successful implementation of MFA and secure authentication - Tutor/code reviewer feedback	Ongoing with project milestones throughout the year
Understand and evaluate compliance requirements related to network security and data protection	- GDPR principles and their application - ISO/IEC 27001 controls and risk management - Legal and ethical considerations in cybersecurity	- Conduct research on compliance frameworks - Attend relevant seminars or workshops - Analyze case studies for compliance gaps	- Access to compliance documentation and case studies - Support from tutors or advisors familiar with legal aspects	- Written assessments or reports demonstrating compliance understanding - Feedback from tutors or legal	Before final module exam or project submission
Prepare for entry-level cybersecurity certifications and career readiness	- Exam preparation for certifications like CompTIA Security+ - Soft skills: communication, teamwork, reporting	- Follow structured certification prep courses - Participate in group projects and presentations - Seek coaching or mentoring for career advice	- Access to certification prep materials - Support from career advisors and tutors - Peer study groups	- Mock exam results - Positive feedback on teamwork and communication Successful completion of certification	Within 12 months from module start