



Module 9

Wrap-up Workshop



Icebreaker- Icebreaker – Secure or Risky?

Which of these actions supports data security? Type: S = Secure, R = Risky

1. Encrypting sensitive fields
2. Sharing raw data in Slack
3. Auditing access logs regularly
4. Reusing credentials across projects



Module 9

Wrap-up Workshop



Agenda

- **Key takeaways**
- **Finding opportunities and generating impact**
- **Project check-in**
- **Q&A**
- **Wrapping up and next steps**
- **Module 9: Hackathon**



Module 9

key takeaways

Key takeaways

1

Robust security measures throughout ML workflows protect sensitive data assets and models, safeguarding your organisation from breaches while maintaining stakeholder trust in AI-driven solutions.

2

Data governance strategies ensure compliance with evolving regulations and ethical standards, reducing legal risks while enhancing the credibility and sustainability of your ML initiatives.

3

Proactive risk management approaches for ML projects empower you to identify and mitigate potential privacy concerns before they escalate, fostering a security-conscious culture that preserves organisational reputation in an increasingly data-sensitive landscape.



What key takeaway do you think will have the biggest impact on your work?



Applying key takeaways

1

Apply ML security principles to safeguard sensitive data and protect stakeholder trust

2

Use governance frameworks to align with compliance standards and reduce legal risk

3

Proactively identify and mitigate privacy risks before they impact project credibility



Share your plan to apply Module 9 skills

Go to My Multiverse, Module 9
Wrap-up Workshop



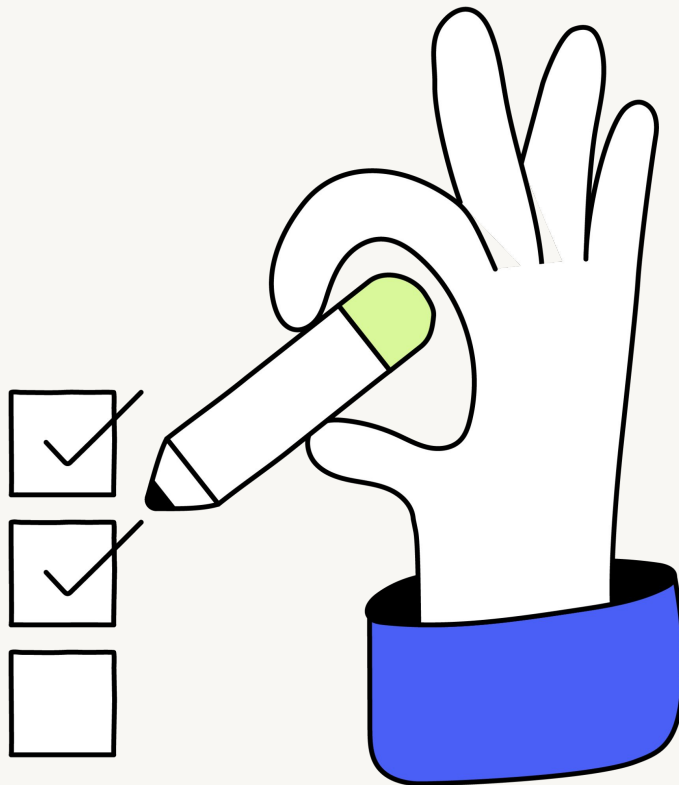
On page "Applying your skills", find the
discussion activity



Take 5 minutes to share how you will
apply this skill in your role



Take time this week to read what
others have written and get new ideas!





Phase 2 project

Module 9 milestone

Access phase 2 project milestone

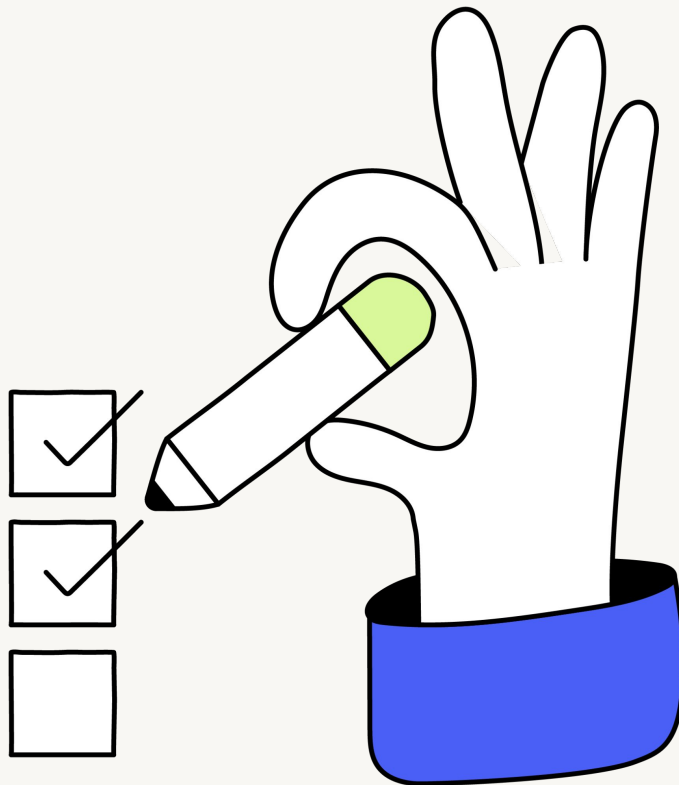
Go to My Multiverse, Projects



Find "AIMLF Phase 2 Project: Milestone 9"



Review milestone tasks





Module 9 milestone: Applying ML techniques

Phase project objective: Build and refine an ML model for performance, fairness, and security. Use XAI to address bias, define key metrics, and ensure full compliance with robust documentation and retraining plans.

Milestone task 1



Security fundamentals in machine learning: Assess cybersecurity risks related to the ML model, including data access controls, adversarial attacks, and security vulnerabilities.

Milestone task 2



Data privacy and governance in machine learning: Apply organisational policies and industry frameworks (e.g., AREA, SAFE-D) to ensure compliance with data privacy and governance regulations.

Milestone task 3



Regulatory compliance and risk management in machine learning Conduct an audit to verify compliance with legal, ethical, and governance requirements. Document the full lifecycle of the ML model from development to deployment.

Module 9 milestone: KSB requirements

Phase project objective: Build and refine an ML model for performance, fairness, and security. Use XAI to address bias, define key metrics, and ensure full compliance with robust documentation and retraining plans.

Task 1 KSBs



Security fundamentals in machine learning: K27

Task 2 KSBs



Data privacy and governance in machine learning: K25, S11, S32

Task 3 KSBs



Regulatory compliance and risk management in machine learning: S6, S17, S32

Module 9 milestone tips for success

- 1 Make security a design principle, not a patch job
- 2 Treat compliance as a living practice
- 3 Document like it matters—because it does
- 4 Build transparency into your model design





Questions?



Wrapping up

Action items

- Attend Group Coaching session
- Complete your project milestone
- Share your project progress with your manager
- **Take the Module Survey** on My Multiverse



Next steps

Action items

- **Have questions?**
 - Chat with Atlas
 - Reach out to your Cohort Coach
 - Sign up for Tutoring
- **Log your OTJ hours**
- **Take the Module Survey** on My Multiverse



Looking ahead

Module 10: Hackathon

multiverse