Counter brief

*After setting the goals and objectives for the project process, the project teams create a Counter Brief to Communicate to the PO*

1. **The way that the team has understood the problem to be solved in the project**

Our goal is to analyze how secure/private the federated learning platform PoC is, by simulating cyber-attacks on it, and using different machine learning techniques to analyze the data, detect the threats and build a benchmarking platform/system based on that.

1. **How the team plans to solve the problem**
   * Develop a benchmarking tool that simulates common cybersecurity attacks (e.g., data poisoning, model inversion, membership inference) on FL systems.
   * Use Machine Learning models to both launch and evaluate these attacks, measuring how well they reconstruct data, infer membership, or degrade performance.
   * Integrate and test Privacy-Enhancing Technologies (PETs) such as Differential Privacy, Homomorphic Encryption, and Reinforcement Learning–based defenses under realistic attack scenarios.
   * Apply AI-driven analytics to compare resilience, accuracy, and compliance across PETs, producing a systematic performance benchmark.
   * Iterate with the customer to align the tool with their research and commercialization goals.
2. **What kind of benefits can be created by the project**
   * A functional prototype for benchmarking PETs in federated learning.
   * Evidence-based validation of the customer’s patented PET technologies.
   * Stronger competitive advantage and credibility with regulators, business partners, and clients.
   * Contribution to the customer’s Business Finland R2B project success and future funding opportunities.
3. **What kind of deliverables the project will create**

* A proof-of-concept Privacy Benchmarking Tool in Python.
* A report/documentation detailing attack simulations, PET evaluations, and recommendations.
* A presentation/demo for technical and non-technical stakeholders.

1. **Preliminary project schedule**

* Weeks 37–39 (Sept 2025)
  + Orientation, project presentations, Pre-Motorola.
  + Define learning objectives, reading program.
  + Draft Counter Brief and meet with Product Owner.
  + Create project roadmap and Gantt chart.
  + Contracts and project plan finalized.
* Weeks 40–47 (Oct–Nov 2025) – Project Implementation
  + Develop first versions of the benchmarking tool in Python.
  + Simulate initial cybersecurity attacks on FL.
  + Test and refine PETs.
  + Peer and self-feedback (week 43).
  + Ongoing feedback and iteration with the customer.
  + Motorola reflections at checkpoints (weeks 42, 44, 46).
* Weeks 48–50 (Nov–Dec 2025) – Project End & Reporting
  + Finalize benchmarking tool (proof of concept).
  + Prepare project report for PO.
  + Team and individual learning documentation.
  + Showroom presentation (week 49).
* Week 51 (mid-Dec 2025)
  + Submission of all final reports and documentation.
  + Wrap-up and reflection.

