Algorithms & Pseudocode

Algorithm 1: Hybrid Quantum–Neural Threat Detection

```
1. Ingest cybersecurity telemetry (network, endpoint, cloud logs)
2. Preprocess and normalize features
3. Encode features using variational quantum circuits
4. Train hybrid quantum–neural model
5. Evaluate robustness under adversarial perturbations
6. Generate predictive risk scores and alerts
```

Algorithm 2: Adversarial Robustness Evaluation

```
1. Select baseline trained hybrid model
2. Apply adversarial attack method (FGSM, PGD)
3. Measure detection accuracy degradation
4. Compute robustness and stability metrics
5. Report resilience indicators to management dashboard
```