AI-Powered Cybersecurity

Amro, Bianca, Emily, Marc-Olivier, Valeria G. and Valeria P.

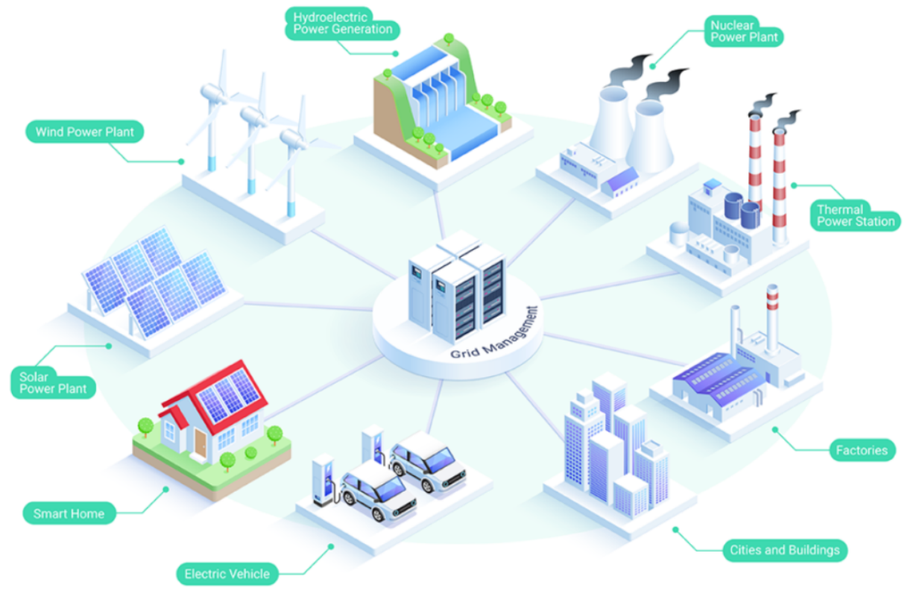
Project overview

What are smart grids?

- Electrical networks that monitor the flow of electricity (production → consumption)
- They are Cyber-Physical systems (mechanical systems managed by computer algorithms and connected to Internet and its network users)

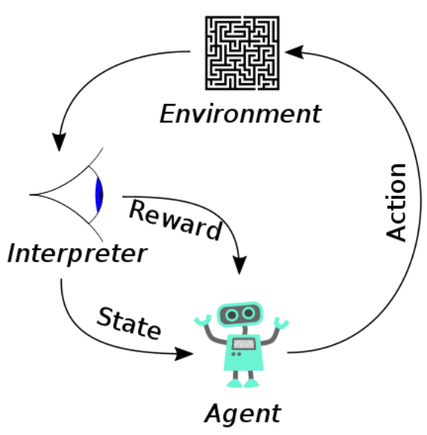
What problem are we tackling?

- Smart grids are prone to cyberattacks
- Using AI to perform penetration testing → "ethically hacking" into a system to identify and locate vulnerabilities in its cybersecurity
- Improving cyber-physical systems' defences to minimize cyberattacks and shutdowns



Example of a smart grid

Reinforcement Learning



What is it?

- An area of machine learning where an agent (the AI) interacts with its environment trying to take smart actions to maximize cumulative rewards

How does it work?

- The agent starts at a certain state and will choose an action to take to try to switch states
- The environment will react according to its model by rewarding the agent (+/-)
- The agent accumulates and uses its knowledge to try to obtain the optimal policy.

Our Tools & Methods

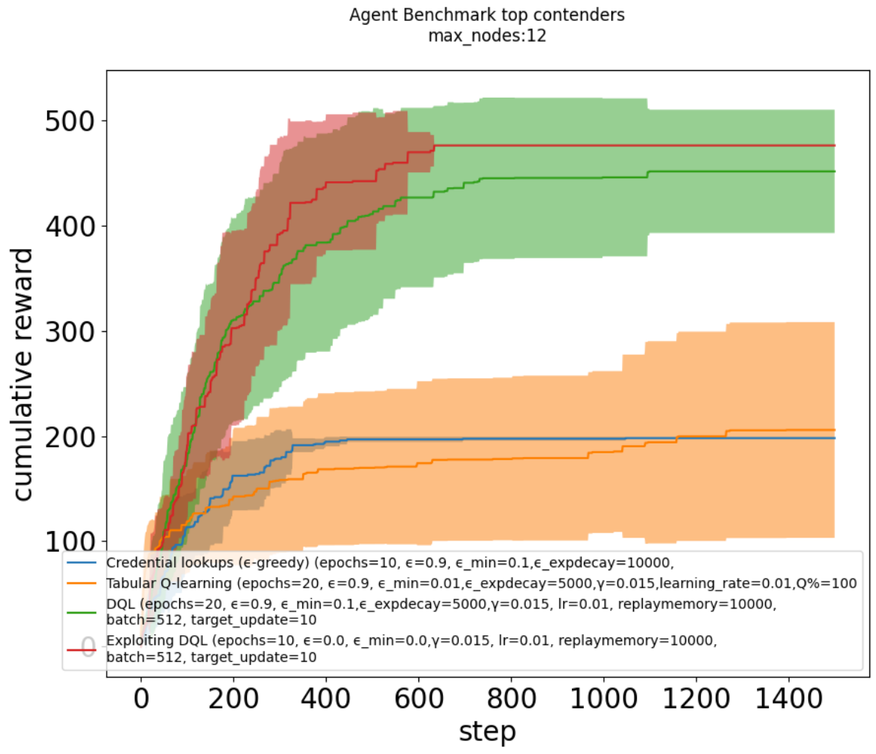
What is OpenAI Gym?

- It's an interface that provides a wide range of environments for developing and comparing reinforcement learning algorithms
- It provided us with graphs so we could measure the accuracy of our penetration testing (PT) and optimize our results.

What is CyberBattleSim?

- An open source experimentation and research platform that specializes in training agents to penetrate virtual environments.
- The different agents go through multiple episodes and reward functions to determine the best pathway to exploit the environment's vulnerabilities.

Performance of different agents



Performance of the top contender