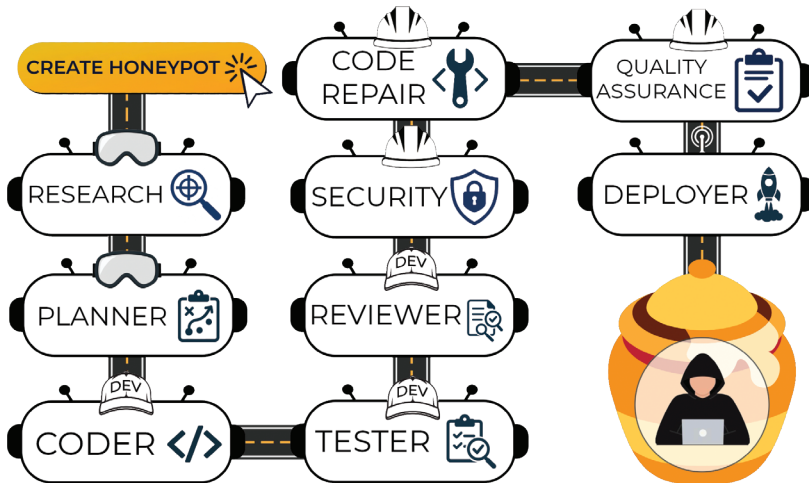# BEE-WARE

Adaptive cybersecurity powered by AI-generated honeypots crafted from real-world vulnerabilities in minutes, not days

STINGAR

CONTEXT

- We are using a **multi-agent AI** pipeline to automatically generate adaptive **honeypots**.
- **Honeypots** are decoy systems used to lure, detect, and study hackers.
- Hackers caught are **blocked** from 80+ universities through **STINGAR's** firewall.

CREATE HONEYPOT
CODE REPAIR
QUALITY ASSURANCE
RESEARCH
SECURITY
DEPLOYER
PLANNER
REVIEWER
CODER
TESTER

MULTI-AGENT PIPELINE

- **Research Crew:** Gathers CVE and honeypot info, creates a high-level task plan.
- **Coding Crew:** Executes tasks, tests outputs, and refines code through an error feedback loop.
- **Quality Crew:** Validates and hardens the honeypot, scoring its strength and completeness.
- **Deployment Agent:** Packages and deploys the final honeypot.

METHODS

- Our **multi-agent AI** system consists of 9 agents.
- We improve the knowledge of this LLM by feeding it 8,000+ honeypot specific training artifacts through Retrieval-Augmented Generation (**RAG**).

SKILLS DEVELOPED

- **AI Agent Orchestration**: Managed coordinated tasks across multiple AI agents.
- **Prompt Engineering**: Designed effective prompts for LLM tasks.
- **UI/UX Dashboard Design**: Created a user-friendly honeypot builder.

ACKNOWLEDGMENTS

Duke
Code