Project Proposal: The Watsonx DevSecOps Agent

A Submission for the Orchestrate What's Next with AI Agents Hackathon

Team 3MITM

October 19, 2025

Executive Summary

This proposal outlines the development of the *Watsonx DevSecOps Agent*, an AI-powered solution designed for the "Orchestrate What's Next with AI Agents Hackathon." Building upon our proof-of-concept, "ProxyMind", we are pivoting from an offensive security tool to a defensive, developer-centric agent. The core of our solution will be IBM Watsonx Orchestrate, which will serve as the central nervous system for an automated security workflow. This agent will analyze an application's network traffic in real-time, use `watsonx.ai` to identify vulnerabilities, leverage `watsonx Code Assistant` for remediation, and automate ticketing, thereby enabling development teams to innovate faster and more securely.

1 Project Vision & Reframing

Our initial concept, ProxyMind, was designed as an AI-enhanced Man-in-the-Middle (MITM) proxy to assist penetration testers by highlighting attack surfaces and suggesting exploits. While technically robust, we recognize that for this hackathon, a more impactful application is to empower developers and defend systems.

Our new vision is to create a proactive **AI DevSecOps Agent**. Instead of helping attackers, it will assist developers. It acts as an automated security partner that integrates seamlessly into the development lifecycle, catching vulnerabilities before they reach production. This aligns perfectly with the "Agent mode activated challenge" by creating a solution that helps teams innovate faster and more safely.

2 Proposed Technical Architecture

The agent's architecture will be centered entirely around **IBM Watsonx Orchestrate**. It will connect a series of custom-built "skills" (APIs) to form an end-to-end security analysis and remediation pipeline.

1. **Traffic Interception:** A standard `mitmproxy` instance will intercept HTTP/S traffic generated by a target web application during testing. A custom script will forward this traffic as a JSON object to our agent's ingestion API.

2. **Orchestration Core (IBM Watsonx Orchestrate):** The agent built on Watsonx Orchestrate will be triggered upon receiving new traffic data. It will then execute the following sequence of skills:

   - **Skill 1: AI Threat Analysis:** The agent passes the traffic data to `watsonx.ai`. A carefully engineered prompt will instruct the model to analyze the request/response for potential vulnerabilities (e.g., SQLi, XSS), assign a risk score, and provide a plain-language explanation.

- **Skill 2: Code Remediation:** If a high-risk vulnerability is detected, the agent passes the vulnerability context to `watsonx Code Assistant` to generate a secure code snippet for remediation.
- **Skill 3: Automated Ticketing:** The agent then uses the Jira API to automatically create a new issue, populating it with the AI analysis, risk score, and suggested code fix.
- **Skill 4: Team Alerting:** Finally, the agent sends a concise notification to a designated Slack or Discord channel with a link to the newly created Jira ticket.

This architecture is highly feasible within the hackathon timeline due to the low-code nature of Watsonx Orchestrate.

3 Team Roles and Responsibilities

Ahmed Samir - AI Engineer

- **Primary Focus:** `watsonx.ai` and `watsonx Code Assistant`.
- **Responsibilities:**
  - Develop and refine the prompts for vulnerability detection and code remediation.
  - Interface with the Backend Engineer to package the AI models as callable "skills" for the Orchestrate agent.
  - Validate the accuracy and relevance of the AI-generated outputs.

Mohammad Emad - Backend Engineer

- **Primary Focus:** IBM Watsonx Orchestrate and API development.
- **Responsibilities:**
  - Become the team expert on the Watsonx Orchestrate platform.
  - Develop the lightweight APIs (skills) for traffic ingestion, Jira integration, and Slack/Discord alerting.
  - Assemble and configure the complete agent workflow within Watsonx Orchestrate.
  - Manage the deployment of the proxy and the API microservices.

Mohammad Sabry - Cybersecurity Engineer

- **Primary Focus:** Domain Expertise, Quality Assurance, and Project Narrative.
- **Responsibilities:**
  - Define the target vulnerabilities and create a test suite of sample malicious HTTP requests.
  - Conduct end-to-end testing of the system to ensure it correctly identifies threats.
  - Lead the development of the final presentation, video demo, and submission text, ensuring it aligns with the hackathon's judging criteria.

4 Direct Plan & Timeline (Oct 23 - Nov 3)

- **Phase 1: Setup & Foundation (Days 1-3: Oct 23-25)**
  - All members complete IBM Watsonx pre-event educational materials.
  - Backend Engineer sets up the Watsonx Orchestrate environment and develops the initial ”traffic ingestion” skill.
  - AI Engineer begins prompt engineering in the `watsonx.ai` studio.
  - Cybersecurity Engineer develops the test cases and sets up a vulnerable target application.
- **Phase 2: Integration & Core Build (Days 4-8: Oct 26-30)**
  - Backend Engineer integrates all required skills (AI, Jira, Slack) into the Orchestrate agent.
  - AI Engineer refines prompts based on test results from the Cybersecurity Engineer.
  - Team achieves the first successful end-to-end run: Traffic -¿ Detection -¿ Ticketing.
- **Phase 3: Testing, Polish & Submission (Days 9-12: Oct 31-Nov 3)**
  - Rigorous testing and bug fixing.
  - Cybersecurity Engineer and team craft the final pitch and presentation.
  - Record a compelling video demonstration of the agent in action.
  - Finalize and submit the project well before the deadline.