Artificial Intelligence Cyber Risk Management Framework (RMF)Tool, v 1.0JD

WWU Academic Year 24-25 Students:

Colson Swope swopec2@wwu.edu

Jonathan Ly lyj5@wwu.edu

Ripken Stork storkr@wwu.edu

WWU Professor Blake Pedrini pedrinb@wwu.edu

WWU Cybersecurity Director: Erik Fretheim frethee@wwu.edu

NUWC DIV KPT Mentor: Jason Omens (primary)
Jason.f.omens.civ@us.navy.mil, Robert Alvey (secondary)
robert.w.alvey.civ@us.navy.mil

NUWC DIV KPT Coordinator: John Diaz, cptdiaz@uw.edu,
john.m.diaz8.civ@us.navy.mil

Objective: The primary goal of this project is to review AI risk management procedures as defined by NIST and ENISA, and to develop an AI solution that assists human cybersecurity analysts in performing RMF procedures to document compliance effectively.

Project Outline:

1. **Introduction and Background:**
   - Overview of AI and its applications in cybersecurity.
   - Importance of risk management in AI systems.
   - Introduction to NIST and ENISA risk management frameworks.
2. **Literature Review:**
   - Detailed review of NIST AI Risk Management Framework (AI RMF) and ENISA guidelines.
   - Case studies of AI applications in cybersecurity risk management.
   - Analysis of existing AI tools aiding RMF procedures.
3. **Methodology:**
   - Identification of key risk management procedures from NIST and ENISA.
   - Development of an AI model to assist in these procedures.
   - Integration of the AI model with existing RMF tools.
4. **AI Solution Development:**
   - Design and implementation of the AI solution.
   - Training the AI model using relevant datasets.
   - Testing the AI solution in a simulated environment.
5. **Implementation:**

    - Deployment of the AI solution in a controlled setting.
    - Collaboration with cybersecurity analysts to refine the tool.
    - Documentation of the AI solution's performance and feedback.
6. **Results and Discussion:**
    - Presentation of findings from the AI solution's deployment.
    - Evaluation of the AI solution's effectiveness in aiding RMF procedures.
    - Discussion on the implications for future AI applications in cybersecurity.
7. **Conclusion and Future Work:**
    - Summary of key findings.
    - Recommendations for further development and research.
    - Potential for scaling the AI solution to broader applications.

References:

1. **NIST Special Publication (SP) 800-53 Rev. 5:**
    - Provides a comprehensive catalog of security and privacy controls for information systems and organizations[1].
2. **NIST Cybersecurity Framework (CSF):**
    - Offers guidelines for managing and reducing cybersecurity risks[2].
3. **NIST Special Publication (SP) 800-30 Rev. 1:**
    - Guide for conducting risk assessments, including the identification of threats and vulnerabilities[3].
4. **NIST Special Publication (SP) 800-37 Rev. 2:**
    - Guidelines for applying the Risk Management Framework (RMF) to information systems[3].
5. **ENISA Guidelines:**
    - European Union Agency for Cybersecurity provides comprehensive guidelines on AI risk management and cybersecurity[4].

Tasks Required to Conduct the Research and Development

1. **Literature Review and Analysis**:
    - Conduct an extensive review of existing literature on cybersecurity RMF for AI systems, relevant guides and forensically documented attacks.
    - Create an annotated bibliography of identified applicable sources.
2. **Identify, evaluate, test and recommend cybersecurity tools to use for AI systems**:
    - Conduct open source review, document and test tools and toolkits.

Deliverable(s):

1. Project Wiki page (see prior Senior CAPSTONEs) for example. This product is to include at a minimum team, roles, schedules, approved work breakdown/scope, products from the tasks.
2. AI and cybersecurity RMF-related cybersecurity tools, listed and packaged for use.

3. Final presentation products.