AI/ML Policy Overview

Overview

We are committed to using Artificial Intelligence to enhance our customers' security in a reliable and ethical way. In line with this commitment, we have developed clear practical policies and operational procedures governing our use of AI technologies. The purpose of our AI/ML policy (the "Policy") is to ensure the ethical, compliant, and secure development, deployment and maintenance of Artificial Intelligence ("AI") and Machine Learning ("ML") technologies within Rapid7 and in our use of third-party vendors, while also fostering transparency, trust, and safety in AI applications for our customers.

Scope

The scope of the Policy applies to any employee, contractor or other person whose conduct is controlled by Rapid7, whether or not they are paid by Rapid7, and encompasses information systems, resources, vendors, products, and services, as well as restricted or internal data collected, created, maintained, and transmitted by Rapid7.

Applications

AI/ML applications involving software components that recognize patterns in data, generate predictions or decisions based on statistical reasoning, create generative output, or involve classification, predictive, anomaly detection, or generative models.

Key Aspects

- **Oversight:** Establishment of an AI/ML Council responsible for overseeing AI/ML technologies' usage and adoption.
- **Designated Roles and Responsibilities:** Clear roles and responsibilities for any model and/or system owners, users and business owners, including, but not limited to, the procurement department, the information security department and the legal department.
- **Design Requirements:** Requirements for AI/ML usage, including approval processes, data privacy compliance, model lifecycle management, and security measures.
- **Guidelines for Third-Parties:** Guidelines for vendor developed models, including evaluation, data usage, model lifecycle management, and security assessments.
- **Gen-AI Guardrails:** Specific considerations for Generative AI use, such as content validation, approval for external use, and prohibited purposes.
- **Process for Policy Exceptions:** Procedures for exceptions to the policy, which must be documented and approved through a prescribed security exception management process.
- **Compliance:** Compliance and enforcement measures, overseen by Rapid7's Chief Security Officer, including disciplinary actions for policy violations.