附件 1

测试场景说明

场景 1：基于智能体的网络安全自动化分析响应

使用 AI 智能体实现对钓鱼邮件攻击、终端异常行为、DNS 隐蔽隧道异常行为的检测，通过关联分析找出属于同一攻击链的攻击行为，并针对攻击行为给出相应的处置方案。测试数据为邮件、终端日志和 DNS 日志等 3 种数据。其中邮件数据包括时间、工号、邮件标题、邮件正文等字段；终端日志包括时间、工号、执行命令等字段；DNS 日志包括时间、工号、源目 IP 及端口、查询域名等字段。按照异常行为检测、攻击关联分析的准确率、漏报率以及处置方案的正确率等指标进行综合评分。

联系人：王老师 18910739015

场景 2：网络安全告警日志降噪

使用 AI 技术对网络威胁检测分析设备和系统产生的告警日志字段进行分析，从疑似网络安全威胁的告警日志中找出攻击成功、可以形成攻击事件的真实告警，并给出攻击类型、IOC 等信息。测试数据字段包括告警时间戳、请求内容、响应内容等。按照告警识别的准确率、漏报率等指标进行综合评分。

联系人：姚老师 15810664643

场景 3：基于互联网流量的漏洞利用攻击识别及 PoC 生成

使用 AI 技术对互联网流量 payload 进行分析，结合有关漏洞情报信息，识别出其中的漏洞利用攻击行为种类，给出相应的漏洞编号，生成该漏洞对应的验证程序 PoC。测试数据包括流量中的 payload、漏洞情报等信息。按照漏洞攻击识别的准确率、漏报率及 PoC 验证通过率等指标进行综合评分。

联系人：何老师 010-82992150

场景 4：基于局域网流量的漏洞利用攻击识别

使用 AI 技术对局域网流量 payload 进行分析，结合有关漏洞情报信息，识别出其中的漏洞利用攻击行为种类，给出相应的漏洞编号。测试数据包括流量中的 payload、漏洞情报等信息。按照准确率、漏报率等指标进行综合评分。

联系人：李老师 13811901791

场景 5：大模型生成内容安全风险检测

使用 AI 技术检测大模型生成的内容是否存在《生成式人工智能服务安全基本要求》中提及的安全风险。测试数据

为大模型的输入和输出内容（一一对应）。按照准确率、漏报率等指标进行综合评分。

联系人：郭老师 13811408139

场景 6：重点车辆船舶监控系统资产脆弱性识别

使用 AI 技术将非结构化的漏洞情报信息与重点车辆船舶监控系统中的资产信息进行关联匹配，发现资产的脆弱性。测试数据为漏洞情报和资产信息，数据字段包括漏洞描述、资产类别、资产的组件、操作系统和数据库等信息。按照准确率、漏报率等指标进行综合评分。

联系人：元老师 13911902705

场景 7：信用卡异常业务行为检测

使用 AI 技术对信用卡业务日志进行检测，分析识别出信用卡绑卡、支付等业务操作中的异常行为。测试数据为信用卡业务日志数据，字段包括用户名、卡号、请求时间、支付金额、源 IP 及所在地、客户端信息等。按照准确率、漏报率等指标进行综合评分。

联系人：赵老师 18514600630