### ­­1 异构新型末端工业设备内嵌安全隔离防护平台硬件架构兼容性测试项

|  |
| --- |
| **测试项目：**异构新型末端工业设备内嵌安全隔离防护平台硬件架构兼容性测试 |
| **测试依据：** |
| **测试目的：**  测试异构新型末端工业设备内嵌安全隔离防护平台支持3种指令集架构测试异构新型末端工业设备内嵌安全隔离防护平台支持3种指令集架构 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）编译一个合适的linux镜像文件和dtb文件  2）设置各架构硬件对应的配置文件  3）编译安全基座内核镜像  4）替换安全基座内核镜像  5）断电重新  6）检查安全基座是否正常启动 |
| **预期结果：**  测试应覆盖以下内容：  1）平台能够运行在x86指令集架构的硬件设备上  2）平台能够运行在arm指令集架构的硬件设备上  3）平台能够运行在qemu模拟的riscv指令集架构的硬件设备上 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 2 异构新型末端工业设备内嵌安全隔离防护平台操作系统兼容性测试项

|  |
| --- |
| **测试项目：**异构新型末端工业设备内嵌安全隔离防护平台操作系统兼容性测试 |
| **测试依据：** |
| **测试目的：**  测试异构新型末端工业设备内嵌安全隔离防护平台支持3种以上主流嵌入式操作系统，支持实时性业务、非实时业务与安全功能的并行执行与安全隔离测试异构新型末端工业设备内嵌安全隔离防护平台支持3种以上主流嵌入式操作系统，支持实时性业务、非实时业务与安全功能的并行执行与安全隔离 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）部署启动异构新型末端工业设备内嵌安全隔离防护平台  2）准备Linux、linux-rt、arceos系统镜像  3）依次安装Linux、linux-rt、srceos操作系统  4）验证各操作系统是否正常运行 |
| **预期结果：**  测试应覆盖以下内容：  1）平台能够运型linux操作系统  2）平台能够运行linux-rt操作系统  3）平台能够运行arceos操作系统 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 3 异构新型末端工业设备内嵌安全隔离防护平台安全隔离测试项

|  |
| --- |
| **测试项目：**异构新型末端工业设备内嵌安全隔离防护平台实时性业务、非实时业务与安全功能的并行执行与安全隔离测试 |
| **测试依据：** |
| **测试目的：**  测试异构新型末端工业设备内嵌安全隔离防护平台支持创建多个隔离域，分别运行实时任务与非实时任务测试异构新型末端工业设备内嵌安全隔离防护平台支持创建多个隔离域，分别运行实时任务与非实时任务 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）部署启动异构新型末端工业设备内嵌安全隔离防护平台  2）创建两个VM  3）分别安装Linux、linux-rt  4）linux-rt中安装plc runtime和国密模块  5）linux中安装北向异常检测模块、设备指纹、南向异常检测模型  6）验证各功能模块是否正常运行 |
| **预期结果：**  测试应覆盖以下内容：  1）平台创建隔离域  2）隔离域分别运行操作系统  3）实时域运行plc runtime，非实时域运行内嵌安全增强功能 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 4 异常检测功能测试项

|  |
| --- |
| **测试项目：**异常检测功能 |
| **测试依据：** |
| **测试目的：**  验证系统能否准确检测负载当中存在的异常指令验证系统能否准确检测负载当中存在的异常指令 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）分别在各自的环境当中安装Agent 1和Agent 2，并进行相关参数的调试，从而保证能够相互连接。  2）开启IDE并连接Agent 1，同时在PLC上运行Agent 2。Agent 2会同时运行实时域监控拦截系统和非实时域监控记录系统。同时，Agent 1和Agent 2之间会采用国密加密通讯。  3) 通过JS生成满足定义的工控协议的包，包括以下负载类型：正常指令、频繁登录、可能的DDoS攻击指令、频繁的APP指令、带有非法参数的APP指令、带有错误参数的config指令、带有错误参数的URL查询、访问不存在的URL指令、以及过大负载的请求，并将其加密后发送至Agent 2。随后对其输出日志进行分析，日志当中所示检测出的异常应具有90%以上的准确率。  4) 对于检测出的异常，对比其输出的日志与报告给大屏的显示结果，需要保证其显示结果与记录的日志在事件数量及异常数量上能够对应。 |
| **预期结果：**  测试应覆盖以下内容：  1）对于满足协议的包，检查其输出日志，查看是否成功检测出异常指令。  2）对于检测出的异常，检查其是否报告给大屏。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 5 设备指纹识别功能测试项

|  |
| --- |
| **测试项目：**设备指纹识别功能测试 |
| **测试依据：** |
| **测试目的：**  验证系统能否正确从真实南向设备或数据包文件读取扫描周期数据、能否准确分析扫描周期数据判断设备身份 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）连接真实南向设备，启动系统向设备指定地址、指定端口读取数据100条，对比读取数据与设备实际输出数据数量是否对应，丢包率应小于10%。 2）将测试用例集中.jsonl格式数据包文件放入指纹.py程序同路径下的fingerprints文件夹下，检查能否正常读取。 3）准备多组已知设备身份数据，导入系统分析，对比分析结果与实际情况，准确率应大于90%。 4）连接真实南向设备，使用测试用例集里的数据配置设备响应周期特征。启动系统读取数据，记录指纹，再读取一次数据，根据读取数据确认设备身份信息，对比分析结果与实际情况，准确率应大于90%。 |
| **预期结果：**  测试应覆盖以下内容：  测试从真实南向设备实时读取数据功能，检查数据准确性和连续性。  2）测试从不同格式数据包文件读取数据功能，验证数据读取成功率。  3）使用已知设备身份的扫描周期数据进行分析，检查判断结果准确性。  4）测试实时读取真实设备数据情况下系统分析结果的准确性。 |
| **测试结果：**  两台同类设备，从机ID分别为1和2，初始情况下没有指纹：  对    没有找到对应设备，因为指纹库为空，保存并再次扫描；    显示扫描结果与之前保存的指纹对应。切换为设备2，再次扫描    显示没有找到对应指纹，因为前一设备与该设备身份不匹配。    两台设备扫描周期分布的实际差异。测试完全准确，准确率100%,通过所有测试项。 |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 6 国密加密功能测试项

|  |
| --- |
| **测试项目：**国密加密功能 |
| **测试依据：** |
| **测试目的：**  验证系统能否正确进行数据的加解密与加密传输验证系统能否正确进行数据的加解密与加密传输 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）加解密登录信息：agent1端，关闭加解密开关后开启服务：python agent1.py，在agent2端关闭解密开关，开启服务：sudo bash run.sh  在IDE中输入IP，点击登录，输入密码。通过抓包工具Wireshark查看ide(172.0.0.1:随机端口)与PLC runtime(172.29.124.160:9527)网络数据报文的记录信息。重复前面操作，但需先打开agent1、agent2的加解密开关，对比加密后的网络数据报文。  2) 加解密数据包：agent1端，关闭加解密开关后开启服务：python agent1.py，在agent2端关闭解密开关，开启服务：sudo bash run.sh  在IDE中输入IP，点击登录，输入密码，新建一个项目，选择梯形图程序，插入INFO函数，设置初始值，编译后点击下装APP。通过抓包工具查看网络数据报文的记录信息。重复前面操作，但需先打开agent1、agent2的加解密开关，对比加密后的网络数据报文。  3) 加解密控制指令：agent1端，关闭加解密开关后开启服务：python agent1.py，在agent2端关闭解密开关，开启服务：sudo bash run.sh  在IDE中输入IP，点击登录，输入密码，新建一个项目，选择梯形图程序，插入DIV函数，设置初始输入输出，点击左侧编译，在目标设备栏中点击下装APP。通过抓包工具查看网络数据报文的记录信息。点击IN1参数，更改参数值，在程序段上方点击写入强制值，再次查看报文信息。重复前面操作，但需先打开agent1、agent2的加解密开关，对比加密后的网络数据报文。  4) 打开agent1、agent2的加解密开关，在encrypt\_decrpt\_service.py文件中找到\_\_init\_\_函数，将debug设为True（此为打印报文填充和解填充开关）。在agent1中开启转发及加解密服务：python agent1.py，在agent2中运行sudo bash run.sh。在IDE中输入IP，点击登录，输入密码。在agent1终端中查看打印输出。（加解密数据块为固定长度） |
| **预期结果：**  测试应覆盖以下内容：  1）验证实时加解密网关功能（包含加解密登录信息、数据包、控制指令）  2）验证报文填充与流量混淆功能 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 7 数据流异常检测功能测试项

|  |
| --- |
| **测试项目：**数据流异常检测功能 |
| **测试依据：** |
| **测试目的：**  验证系统能否准确检测异常数据验证系统能否准确检测异常数据 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）导入模型。通过先前定义好的config和model.pth进行模型导入。  2）处理数据，预处理数据，随后通过data\_queue将测试集模拟为数据流形式  3）数据重构，将数据流输入模型，获得重构后的数据流  4）确定阈值，计算重构数据与原始数据的MSE并记录在threshold\_queue中，将该队列中高于99%数值的点作为阈值  5）动态调整阈值：将计算获得的MSE输入threshold\_queue，从而动态调整阈值  6）检测异常，MSE将高于阈值的点视作异常值 |
| **预期结果：**  测试应覆盖以下内容：  1）对于以数据流形式输入模型的数据，检测器是否能输出异常值。  2）对于检测出的异常，检查其是否能够进行记录。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 8 信捷PLC设备XG2-26T4的工业通用通信协议攻击与协同检测测试项

|  |
| --- |
| **测试项目：**信捷PLC设备XG2-26T4的工业通用通信协议攻击与协同检测 |
| **测试依据：** |
| **测试目的：**  在信捷PLC设备XG2-26T4上进行工业通用通信协议攻击，并能够检测到攻击在信捷PLC设备XG2-26T4上进行工业通用通信协议攻击，并能够检测到攻击 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动信捷PLC设备型号为XG2-26T4的工业通用Modbus通信协议的拒绝服务漏洞的监测模式；  3）测试机向信捷PLC设备型号为XG2-26T4发送工业通用Modbus通信协议的拒绝服务攻击；  4）查看系统是否检测到工业通用Modbus通信协议的拒绝服务攻击，并查到相对应的告警。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业通用Modbus通信协议的拒绝服务攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 9 Sixnet网关SYS-800-021的工业组态通信协议攻击与协同检测测试项

|  |
| --- |
| **测试项目：**Sixnet网关SYS-800-021的工业组态通信协议攻击与协同检测 |
| **测试依据：** |
| **测试目的：**  在Sixnet网关SYS-800-021上进行工业组态通信协议攻击，并能够检测到攻击在Sixnet网关SYS-800-021上进行工业组态通信协议攻击，并能够检测到攻击 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动Sixnet网关SYS-800-021的工业组态私有通信协议拒绝服务漏洞的监测模式；  3）测试机向Sixnet网关SYS-800-021发送工业组态私有通信协议拒绝服务攻击；  4）查看系统是否检测到工业组态私有通信协议拒绝服务攻击，并查到相对应的告警。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业组态私有通信协议拒绝服务攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 10信捷PLC设备XD5E-24R-C的工业通用通信协议攻击与协同检测测试项

|  |
| --- |
| **测试项目：**信捷PLC设备信捷PLC设备XD5E-24R-C的工业通用通信协议攻击与协同检测 |
| **测试依据：** |
| **测试目的：**  在信捷PLC设备XD5E-24R-C上进行工业通用通信协议攻击，并能够检测到攻击。在信捷PLC设备XD5E-24R-C上进行工业通用通信协议攻击，并能够检测到攻击。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动信捷PLC设备XD5E-24R-C的工业通用Modbus通信协议的拒绝服务漏洞的监测模式；  3）测试机向信捷PLC设备XD5E-24R-C发送工业通用Modbus通信协议的拒绝服务攻击；  4）查看系统是否检测到工业通用Modbus通信协议的拒绝服务攻击，并查到相对应的告警。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业通用Modbus通信协议的拒绝服务攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **11 汇川PLC AM 401-CPU1608TP的工业设备命令注入攻击与协同检测试项**

|  |
| --- |
| **测试项目：**汇川PLC AM 401-CPU1608TP的工业设备命令注入攻击与协同检测 |
| **测试依据：** |
| **测试目的：**  在汇川PLC AM 401-CPU1608TP上进行工业设备命令注入攻击，并能够检测到该攻击。在汇川PLC AM 401-CPU1608TP上进行工业设备命令注入攻击，并能够检测到该攻击。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动汇川PLC设备AM 401-CPU1608TP的工业设备命令注入漏洞的监测模式；  3）测试机向汇川PLC设备AM 401-CPU1608TP发送工业设备命令注入漏洞攻击；  4）查看系统是否检测到工业设备命令注入攻击，并查到相对应的告警。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业设备命令注入攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **12 汇川PLC设备AM600-PS2的工业组态通信协议攻击与协同检测试项**

|  |
| --- |
| **测试项目：**汇川PLC设备AM600-PS2的工业组态通信协议攻击与协同检测 |
| **测试依据：** |
| **测试目的：**  在汇川PLC设备AM600-PS2上进行工业组态通信协议攻击，并能够检测到该攻击。在汇川PLC设备AM600-PS2上进行工业组态通信协议攻击，并能够检测到该攻击。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动汇川PLC设备AM600-PS2的工业组态私有通信协议缓冲区溢出漏洞的监测模式；  3）测试机向汇川PLC设备AM600-PS2发送工业组态私有通信协议缓冲区溢出攻击；  4）查看系统是否检测到工业组态私有通信协议缓冲区溢出攻击，并查到相对应的告警。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业组态私有通信协议缓冲区溢出攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **13 台达PLC设备DVP15MC11T的工业通用通信协议攻击与协同检测试项**

|  |
| --- |
| **测试项目：**台达PLC设备DVP15MC11T的工业通用通信协议攻击与协同检测 |
| **测试依据：** |
| **测试目的：**  在台达PLC设备DVP15MC11T上进行工业通用通信协议攻击，并能够检测到该攻击。在台达PLC设备DVP15MC11T上进行工业通用通信协议攻击，并能够检测到该攻击。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动台达PLC设备DVP15MC11T的工业通用CIP通信协议拒绝服务漏洞的监测模式；  3）测试机向台达PLC设备DVP15MC11T发送工业通用CIP通信协议拒绝服务攻击；  4）查看系统是否检测到工业通用CIP通信协议拒绝服务攻击，并查到相对应的告警。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业通用CIP通信协议拒绝服务攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **14 信捷PLC设备XD5E-30T4-E的工业通用通信协议攻击与协同检测测试项**

|  |
| --- |
| **测试项目：**信捷PLC设备XD5E-30T4-E的工业通用通信协议攻击与协同检测 |
| **测试依据：** |
| **测试目的：**  在信捷PLC设备XD5E-30T4-E上进行工业通用通信协议攻击，并能够检测到该攻击。在信捷PLC设备XD5E-30T4-E上进行工业通用通信协议攻击，并能够检测到该攻击。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动信捷PLC设备XD5E-30T4-E的工业通用ModbusTCP通信协议逻辑处理错误漏洞的监测模式；  3）测试机向信捷PLC设备XD5E-30T4-E发送工业通用ModbusTCP通信协议逻辑处理错误攻击；  4）查看系统是否检测到工业通用ModbusTCP通信协议逻辑处理错误攻击，并查到相对应的告警。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业通用ModbusTCP通信协议逻辑处理错误攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **15 施耐德PLC设备Quantum140的工业通用通信协议攻击与协同检测试项**

|  |
| --- |
| **测试项目：**施耐德PLC设备Quantum140的工业通用通信协议攻击与协同检测 |
| **测试依据：** |
| **测试目的：**  在施耐德PLC设备Quantum140上进行工业通用通信协议攻击，并能够检测到该攻击。在施耐德PLC设备Quantum140上进行工业通用通信协议攻击，并能够检测到该攻击。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动施耐德PLC设备Quantum140的工业通用UMAS通信协议的拒绝服务漏洞的监测模式；  3）测试机向施耐德PLC设备Quantum140发送工业通用UMAS通信协议的拒绝服务攻击；  4）查看系统是否检测到工业通用UMAS通信协议的拒绝服务攻击，并查到相对应的告警。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业通用UMAS通信协议的拒绝服务攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **16 华茂PLC设备CPU 812-1B0AA-H的工业基础通信协议攻击与协同检测试项**

|  |
| --- |
| **测试项目：**华茂PLC设备CPU 812-1B0AA-H的工业基础通信协议攻击与协同检测 |
| **测试依据：** |
| **测试目的：**  在华茂PLC设备CPU 812-1B0AA-H上进行工业基础通信协议攻击，并能够检测到该攻击。在华茂PLC设备CPU 812-1B0AA-H上进行工业基础通信协议攻击，并能够检测到该攻击。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动华茂PLC设备CPU 812-1B0AA-H的私有通信协议缓冲区溢出漏洞的监测模式；  3）测试机向华茂PLC设备CPU 812-1B0AA-H发送私有通信协议缓冲区溢出攻击；  4）查看系统是否检测到私有通信协议缓冲区溢出，并查到相对应的告警。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到私有通信协议缓冲区溢出攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **17 合信PLC设备CTH2 214-1AD33的工业基础通信协议拒绝服务攻击检测试项**

|  |
| --- |
| **测试项目：**合信PLC设备CTH2 214-1AD33的工业基础通信协议拒绝服务攻击检测 |
| **测试依据：** |
| **测试目的：**  在合信PLC设备CTH2 214-1AD33上进行工业基础通信协议拒绝服务攻击检测，并能够检测到该攻击。在合信PLC设备CTH2 214-1AD33上进行工业基础通信协议拒绝服务攻击检测，并能够检测到该攻击。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动合信PLC设备CTH2 214-1AD33的工业基础TCP协议通信协议拒绝服务漏洞的监测模式；  3）测试机向合信PLC设备CTH2 214-1AD33发送工业通用Modbus通信协议的拒绝服务攻击；  4）查看系统是否检测到工业基础TCP协议通信协议拒绝服务攻击，并查到相对应的告警。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业基础TCP协议通信协议拒绝服务，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **18 傲拓科技PLC设备NA2000的工业基础通信协议拒绝服务攻击检测试项**

|  |
| --- |
| **测试项目：**傲拓科技PLC设备NA2000的工业基础通信协议拒绝服务攻击检测 |
| **测试依据：** |
| **测试目的：**  在傲拓科技PLC设备NA2000上进行工业基础通信协议拒绝服务攻击检测，并能够检测到该攻击。在傲拓科技PLC设备NA2000上进行工业基础通信协议拒绝服务攻击检测，并能够检测到该攻击。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动傲拓科技PLC设备NA2000的工业基础IPv4协议通信协议拒绝服务漏洞的监测模式；  3）测试机向傲拓科技PLC设备NA2000发送工业基础IPv4协议通信协议拒绝服务攻击；  4）查看系统是否检测到工业基础IPv4协议通信协议拒绝服务攻击，并查到相对应的告警。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业基础IPv4协议通信协议拒绝服务攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **19 施耐德PLC设备TM241CE40T\_U的工业通用通信协议攻击与协同检测试项**

|  |
| --- |
| **测试项目：**施耐德PLC设备TM241CE40T\_U的工业通用通信协议攻击与协同检测 |
| **测试依据：** |
| **测试目的：**  在施耐德PLC设备TM241CE40T\_U上进行工业通用通信协议攻击，并能够检测到该攻击。在施耐德PLC设备TM241CE40T\_U上进行工业通用通信协议攻击，并能够检测到该攻击。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动施耐德PLC设备TM241CE40T\_U工业基础协议TCP逻辑处理漏洞的监测模式；  3）测试机向施耐德PLC设备TM241CE40T\_U发送工业基础协议TCP逻辑处理攻击；  4）查看系统是否检测到工业基础TCP协议逻辑处理攻击，并查到相对应的告警。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业基础TCP协议逻辑处理攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **20 显控科技PLC设备FGPR-C8X8T的工业组态通信协议攻击与协同检测试项**

|  |
| --- |
| **测试项目：**显控科技PLC设备FGPR-C8X8T的工业组态通信协议攻击与协同检测 |
| **测试依据：** |
| **测试目的：**  在显控科技PLC设备FGPR-C8X8T上进行工业组态通信协议攻击，并能够检测到该攻击。在显控科技PLC设备FGPR-C8X8T上进行工业组态通信协议攻击，并能够检测到该攻击。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动显控科技PLC设备FGPR-C8X8T的工业组态私有通信协议拒绝服务漏洞的监测模式；  3）测试机向显控科技PLC设备FGPR-C8X8T发送工业组态私有通信协议拒绝服务攻击；  4）查看系统是否检测到工业组态私有通信协议拒绝服务攻击，并查到相对应的告警。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业组态私有通信协议拒绝服务攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **21 和利时PLC设备LK202的工业组态通信协议攻击与协同检测试项**

|  |
| --- |
| **测试项目：**和利时PLC设备LK202的工业组态通信协议攻击与协同检测 |
| **测试依据：** |
| **测试目的：**  在和利时PLC设备LK202上进行工业组态通信协议攻击，并能够检测到该攻击。在和利时PLC设备LK202上进行工业组态通信协议攻击，并能够检测到该攻击。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动和利时PLC设备LK202的工业通用Modbus通信协议的拒绝服务漏洞的监测模式；  3）测试机向和利时PLC设备LK202发送工业通用Modbus通信协议的拒绝服务攻击；  4）查看系统是否检测到工业通用Modbus通信协议的拒绝服务攻击，并查到相对应的告警。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业通用Modbus通信协议的拒绝服务攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **22 MELSEC PLC设备L02CPU-CM的工业组态通信协议攻击与协同检测试项**

|  |
| --- |
| **测试项目：**MELSEC PLC设备L02CPU-CM的工业组态私有通信协议攻击与协同检测 |
| **测试依据：** |
| **测试目的：**  在MELSEC PLC设备L02CPU-CM上进行工业组态私有通信协议攻击，并能够检测到该攻击。在MELSEC PLC设备L02CPU-CM上进行工业组态私有通信协议攻击，并能够检测到该攻击。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动MELSEC PLC设备L02CPU-CM的工业组态私有通信协议的拒绝服务漏洞的监测模式；  3）测试机向MELSEC PLC设备L02CPU-CM发送工业组态私有通信协议的拒绝服务攻击；  4）查看系统是否检测到工业组态私有通信协议的拒绝服务攻击，并查到相对应的告警。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业组态私有通信协议的拒绝服务攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **23 TP-LINK的云台网络摄像机TL-IPC43AN-4GY的工业基础通信协议攻击与协同检测测试项**

|  |
| --- |
| **测试项目：**TP-LINK的云台网络摄像机TL-IPC43AN-4GY的工业基础通信协议攻击与协同检测 |
| **测试依据：** |
| **测试目的：**  在TP-LINK的云台网络摄像机TL-IPC43AN-4GY上进行工业基础通信协议攻击，并能够检测到该攻击。在TP-LINK的云台网络摄像机TL-IPC43AN-4GY上进行工业基础通信协议攻击，并能够检测到该攻击。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动TP-LINK的云台网络摄像机TL-IPC43AN-4GY的工业基础TCP协议存在逻辑处理错误漏洞的监测模式；  3）测试机向TP-LINK的云台网络摄像机TL-IPC43AN-4GY发送工业基础TCP协议存在逻辑处理错误漏洞攻击；  4）查看系统是否检测到工业基础TCP协议逻辑处理错误攻击，并查到相对应的告警。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业基础TCP协议逻辑处理错误攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **24 海康威视网络摄像机 DS-2CD7A4XYZ-XZS的工业通用通信协议攻击与协同检测测试项**

|  |
| --- |
| **测试项目：**海康威视网络摄像机 DS-2CD7A4XYZ-XZS的工业通用通信协议攻击与协同检测 |
| **测试依据：** |
| **测试目的：**  在海康威视网络摄像机DS-2CD7A4XYZ-XZS上进行工业通用通信协议攻击，并能够检测到该攻击。在海康威视网络摄像机DS-2CD7A4XYZ-XZS上进行工业通用通信协议攻击，并能够检测到该攻击。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动海康威视网络摄像机 DS-2CD7A4XYZ-XZS的工业通用ONVIF协议内存溢出漏洞的监测模式；  3）测试机向海康威视网络摄像机 DS-2CD7A4XYZ-XZS发送工业通用ONVIF协议内存溢出攻击；  4）查看系统是否检测到工业通用ONVIF协议内存溢出攻击，并查到相对应的告警。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业通用ONVIF协议内存溢出攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **25 SIEMENS PLC设备S7-1200的工业通用通信协议攻击与协同检测测试项**

|  |
| --- |
| **测试项目：**SIEMENS PLC设备S7-1200的工业通用通信协议攻击与协同检测 |
| **测试依据：** |
| **测试目的：**  在SIEMENS PLC设备S7-1200上进行工业通用通信协议攻击，并能够检测到该攻击。在SIEMENS PLC设备S7-1200上进行工业通用通信协议攻击，并能够检测到该攻击。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动SIEMENS PLC设备S7-1200的工业通用S7-Comm通信协议拒绝服务漏洞的监测模式；  3）测试机向SIEMENS PLC设备S7-1200发送工工业通用S7-Comm通信协议拒绝服务攻击；  4）查看系统是否检测到工业通用S7-Comm通信协议拒绝服务攻击，并查到相对应的告警。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业通用S7-Comm通信协议拒绝服务攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **26 中油瑞飞RTU设备的工业组态私有通信协议攻击与协同检测测试项**

|  |
| --- |
| **测试项目：**中油瑞飞RTU设备的工业组态私有通信协议攻击与协同检测 |
| **测试依据：** |
| **测试目的：**  在中油瑞飞RTU设备上进行工业组态私有通信协议攻击，并能够检测到该攻击。在中油瑞飞RTU设备上进行工业组态私有通信协议攻击，并能够检测到该攻击。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动中油瑞飞RTU设备的工业组态私有通信协议反序列化漏洞的监测模式；  3）测试机向中油瑞飞RTU设备发送工业组态私有通信协议反序列化攻击；  4）查看系统是否检测到工业组态私有通信协议反序列化攻击，并查到相对应的告警。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业组态私有通信协议反序列化攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **27 360Wi-Fi6路由器T7U 的工业基础通信协议攻击与协同检测测试项**

|  |
| --- |
| **测试项目：**360Wi-Fi6路由器T7U 的工业基础通信协议攻击与协同检测 |
| **测试依据：** |
| **测试目的：**  对360Wi-Fi6路由器T7U设备进行工业基础通信协议的针对性攻击，并验证系统能否有效检测到该攻击。对360Wi-Fi6路由器T7U设备进行工业基础通信协议的针对性攻击，并验证系统能否有效检测到该攻击。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动360Wi-Fi6路由器T7U 的工业基础TCP协议拒绝服务的监测模式；  3）测试机向360Wi-Fi6路由器T7U 设备发送工业基础TCP协议拒绝服务攻击；  4）查看系统是否检测到工业基础TCP协议拒绝服务攻击，并查到相对应的告警。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业基础通信协议拒绝服务攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **28 南自保护测控装置PSL-642UA-GZK的工业通用通信协议攻击与协同检测测试项**

|  |
| --- |
| **测试项目：**南自保护测控装置PSL-642UA-GZK的工业通用通信协议攻击与协同检测 |
| **测试依据：** |
| **测试目的：**  在南自保护测控装置PSL-642UA-GZK上进行工业通用通信协议攻击，并能够检测到该攻击。在南自保护测控装置PSL-642UA-GZK上进行工业通用通信协议攻击，并能够检测到该攻击。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动南自保护测控装置PSL-642UA-GZK的工业通用MMS协议逻辑处理错误漏洞的监测模式；  3）测试机向南自保护测控装置PSL-642UA-GZK发送工业通用MMS协议逻辑处理错误攻击；  4）查看系统是否检测到工业通用MMS协议逻辑处理错误攻击，并查到相对应的告警。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业通用MMS协议逻辑处理错误攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **29 倍福PLC设备CX2030的工业通用通信协议攻击与协同检测测试项**

|  |
| --- |
| **测试项目：**倍福PLC设备CX2030的工业通用通信协议攻击与协同检测 |
| **测试依据：** |
| **测试目的：**  在倍福PLC设备CX2030上进行工业通用通信协议攻击，并能够检测到该攻击。在倍福PLC设备CX2030上进行工业通用通信协议攻击，并能够检测到该攻击。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动倍福PLC设备CX2030的工业通用通信AMS协议缓冲区溢出漏洞的监测模式；  3）测试机向倍福PLC设备CX2030发送工业通用通信AMS协议缓冲区溢出攻击；  4）查看系统是否检测到工业通用通信AMS协议缓冲区溢出攻击，并查到相对应的告警。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业通用通信AMS协议缓冲区溢出攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **30 倍福PLC设备CX8080的工业通用通信协议攻击与协同检测测试项**

|  |
| --- |
| **测试项目：**倍福PLC设备CX8080的工业通用通信协议攻击与协同检测 |
| **测试依据：** |
| **测试目的：**  在倍福PLC设备CX8080上进行工业通用通信协议攻击，并能够检测到该攻击。在倍福PLC设备CX8080上进行工业通用通信协议攻击，并能够检测到该攻击。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动倍福PLC设备CX8080的工业通用通信AMS协议逻辑处理错误漏洞的监测模式；  3）测试机向倍福PLC设备CX8080发送工业通用通信AMS协议逻辑处理错误攻击；  4）查看系统是否检测到工业通用通信AMS协议逻辑处理错误攻击，并查到相对应的告警。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业通用通信AMS协议逻辑处理错误攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **31 得捷串口服务器DIGI PortServer TS1工业基础通信协议攻击与协同检测测试项**

|  |
| --- |
| **测试项目：**得捷串口服务器DIGI PortServer TS1工业基础通信协议攻击与协同检测 |
| **测试依据：** |
| **测试目的：**  在得捷串口服务器DIGI PortServer TS1上进行工业基础通信协议攻击，并能够检测到该攻击。在得捷串口服务器DIGI PortServer TS1上进行工业基础通信协议攻击，并能够检测到该攻击。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动得捷串口服务器DIGI PortServer TS1的工业基础通信TCP协议缓冲区溢出漏洞的监测模式；  3）测试机向得捷串口服务器DIGI PortServer TS1发送工业基础通信TCP协议缓冲区溢出攻击；  4）查看系统是否检测到工业基础通信TCP协议缓冲区溢出攻击，并查到相对应的告警。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业基础通信TCP协议缓冲区溢出攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **32 研华串口服务器EKI-1511X工业通用通信协议攻击与协同检测测试项**

|  |
| --- |
| **测试项目：**研华串口服务器EKI-1511X工业通用通信协议攻击与协同检测 |
| **测试依据：** |
| **测试目的：**  在研华串口服务器EKI-1511X上进行工业通用通信协议攻击，并能够检测到该攻击。在研华串口服务器EKI-1511X上进行工业通用通信协议攻击，并能够检测到该攻击。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动研华串口服务器EKI-1511X的工业通用HTTP协议缓冲区溢出漏洞的监测模式；  3）测试机向研华串口服务器EKI-1511X发送工业通用HTTP协议缓冲区溢出攻击；  4）查看系统是否检测到工业通用HTTP协议缓冲区溢出攻击，并查到相对应的告警。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业通用HTTP协议缓冲区溢出攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **33 研华串口服务器EKI-1521CE工业设备WEB服务命令执行攻击与协同检测测试项**

|  |
| --- |
| **测试项目：**研华串口服务器EKI-1521CE工业设备WEB服务命令执行攻击与协同检测 |
| **测试依据：** |
| **测试目的：**  在研华串口服务器EKI-1521CE上进行工业设备WEB服务命令执行攻击，并能够检测到该攻击。在研华串口服务器EKI-1521CE上进行工业设备WEB服务命令执行攻击，并能够检测到该攻击。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动研华串口服务器EKI-1521CE的工业设备WEB服务命令执行漏洞的监测模式；  3）测试机向研华串口服务器EKI-1521CE发送工业设备WEB服务命令执行攻击；  4）查看系统是否检测到工业设备WEB服务命令执行攻击，并查到相对应的告警。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业设备WEB服务命令执行攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **34 信捷PLC设备XDME-30T4-E工业通用通信协议攻击与协同检测测试项**

|  |
| --- |
| **测试项目：**信捷PLC设备XDME-30T4-E工业通用通信协议攻击与协同检测 |
| **测试依据：** |
| **测试目的：**  在信捷PLC设备XDME-30T4-E上进行工业通用通信协议攻击，并能够检测到该攻击。在信捷PLC设备XDME-30T4-E上进行工业通用通信协议攻击，并能够检测到该攻击。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动信捷PLC设备XDME-30T4-E的工业通用Modbus协议缓冲区溢出漏洞的监测模式；  3）测试机向信捷PLC设备XDME-30T4-E发送工业通用Modbus协议缓冲区溢出攻击；  4）查看系统是否检测到工业通用Modbus协议缓冲区溢出攻击，并查到相对应的告警。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业通用Modbus协议缓冲区溢出攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **35 康耐得串口服务器 C2000-B2-SFE0101-BB1工业基础通信协议攻击与协同检测测试项**

|  |
| --- |
| **测试项目：**康耐得串口服务器 C2000-B2-SFE0101-BB1工业基础通信协议攻击与协同检测 |
| **测试依据：** |
| **测试目的：**  在康耐得串口服务器C2000-B2-SFE0101-BB1上进行工业基工业基础通信协议攻击，，并能够检测到该攻击。在康耐得串口服务器C2000-B2-SFE0101-BB1上进行工业基工业基础通信协议攻击，，并能够检测到该攻击。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动康耐得串口服务器 C2000-B2-SFE0101-BB1的工业基础通信TCP协议缓冲区溢出漏洞的监测模式；  3）测试机向康耐得串口服务器 C2000-B2-SFE0101-BB1发送工业基础通信TCP协议缓冲区溢出攻击；  4）查看系统是否检测到工业基础通信TCP协议缓冲区溢出攻击，并查到相对应的告警。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业基础通信TCP协议缓冲区溢出攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **36 欧姆龙PLC设备 NX102-9000工业通用通信协议攻击与协同检测测试项**

|  |
| --- |
| **测试项目：**欧姆龙PLC设备 NX102-9000工业通用通信协议攻击与协同检测 |
| **测试依据：** |
| **测试目的：**  在欧姆龙PLC设备NX102-9000上进行工业通用通信协议攻击，并能够检测到该攻击。在欧姆龙PLC设备NX102-9000上进行工业通用通信协议攻击，并能够检测到该攻击。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动欧姆龙PLC设备 NX102-9000的工业通用HTTP协议逻辑处理错误漏洞的监测模式；  3）测试机向欧姆龙PLC设备 NX102-9000发送工业通用HTTP协议逻辑处理错误攻击；  4）查看系统是否检测到工业通用HTTP协议逻辑处理错误攻击，并查到相对应的告警。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业通用HTTP协议逻辑处理错误攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **37 台达PLC设备AS332T工业通用协议通信协议攻击与协同检测测试项**

|  |
| --- |
| **测试项目：**台达PLC设备AS332T工业通用协议通信协议攻击与协同检测 |
| **测试依据：** |
| **测试目的：**  在台达PLC设备AS332T上进行工业通用协议通信协议攻击，并能够检测到该攻击。在台达PLC设备AS332T上进行工业通用协议通信协议攻击，并能够检测到该攻击。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动台达PLC设备AS332T工业通用CIP协议通信协议拒绝服务漏洞的监测模式；  3）测试机台达PLC设备AS332T工业通用CIP协议通信协议拒绝服务攻击；  4）查看系统是否检测到工业通用CIP协议通信协议拒绝服务攻击，并查到相对应的告警。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业通用CIP协议通信协议拒绝服务攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **38 信捷PLC设备XG2-26T4的工业通用通信协议安全防护测试项**

|  |
| --- |
| **测试项目：**信捷PLC设备XG2-26T4的工业通用通信协议安全防护 |
| **测试依据：** |
| **测试目的：**  在信捷PLC设备XG2-26T4上进行工业通用通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。在信捷PLC设备XG2-26T4上进行工业通用通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动信捷PLC设备型号为XG2-26T4的工业通用Modbus通信协议的拒绝服务漏洞的防护模式；  3）测试机向信捷PLC设备型号为XG2-26T4发送工业通用Modbus通信协议的拒绝服务攻击；  4）查看系统是否检测到工业通用Modbus通信协议的拒绝服务攻击，同时给出相对应的告警，并对攻击流量进行拦截。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业通用Modbus通信协议的拒绝服务攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **39 Sixnet网关SYS-800-021的工业组态通信协议安全防护测试项**

|  |
| --- |
| **测试项目：**Sixnet网关SYS-800-021的工业组态通信协议安全防护 |
| **测试依据：** |
| **测试目的：**  在Sixnet网关SYS-800-021上进行工业组态通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。在Sixnet网关SYS-800-021上进行工业组态通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动Sixnet网关SYS-800-021的工业组态私有通信协议拒绝服务漏洞的防护模式；  3）测试机向信捷Sixnet网关SYS-800-021发送工业组态私有通信协议拒绝服务攻击；  4）查看系统是否检测到工业组态私有通信协议拒绝服务攻击，同时给出相对应的告警，并对攻击流量进行拦截。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业组态私有通信协议拒绝服务攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **40 信捷PLC设备XD5E-24R-C的工业通用通信协议安全防护测试项**

|  |
| --- |
| **测试项目：**信捷PLC设备XD5E-24R-C的工业通用通信协议安全防护 |
| **测试依据：** |
| **测试目的：**  在信捷PLC设备XD5E-24R-C上进行工业通用通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。在信捷PLC设备XD5E-24R-C上进行工业通用通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动信捷PLC设备XD5E-24R-C的工业通用Modbus通信协议的拒绝服务漏洞的防护模式；  3）测试机向信捷PLC设备XD5E-24R-C发送工业通用Modbus通信协议的拒绝服务攻击；  4）查看系统是否检测到工业通用Modbus通信协议的拒绝服务攻击，同时给出相对应的告警，并对攻击流量进行拦截。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业通用Modbus通信协议的拒绝服务攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **41 汇川PLC AM 401-CPU1608TP的工业设备命令注入安全防护测试项**

|  |
| --- |
| **测试项目：**汇川PLC AM 401-CPU1608TP的工业设备命令注入安全防护 |
| **测试依据：** |
| **测试目的：**  在汇川PLC AM 401-CPU1608TP上进行工业设备命令注入安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。在汇川PLC AM 401-CPU1608TP上进行工业设备命令注入安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动汇川PLC AM 401-CPU1608TP的工业设备命令注入漏洞的防护模式；  3）测试机向汇川PLC AM 401-CPU1608TP发送工业设备命令注入攻击；  4）查看系统是否检测到工业设备命令注入攻击，同时给出相对应的告警，并对攻击流量进行拦截。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业设备命令注入攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **42 汇川PLC设备AM600-PS2的工业组态通信协议安全防护测试项**

|  |
| --- |
| **测试项目：**汇川PLC设备AM600-PS2的工业组态通信协议安全防护 |
| **测试依据：** |
| **测试目的：**  在汇川PLC设备AM600-PS2上进行工业组态通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。在汇川PLC设备AM600-PS2上进行工业组态通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动汇川PLC设备AM600-PS2的工业组态私有通信协议缓冲区溢出漏洞的防护模式；  3）测试机向汇川PLC设备AM600-PS2发送工业组态私有通信协议缓冲区溢出攻击；  4）查看系统是否检测到工业组态私有通信协议缓冲区溢出攻击，同时给出相对应的告警，并对攻击流量进行拦截。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业组态私有通信协议缓冲区溢出攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **43 台达PLC设备DVP15MC11T的工业通用通信协议安全防护测试项**

|  |
| --- |
| **测试项目：**台达PLC设备DVP15MC11T的工业通用通信协议安全防护 |
| **测试依据：** |
| **测试目的：**  在台达PLC设备DVP15MC11T上进行工业通用通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。在台达PLC设备DVP15MC11T上进行工业通用通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动台达PLC设备DVP15MC11T的工业通用CIP通信协议拒绝服务漏洞的防护模式；  3）测试机向台达PLC设备DVP15MC11T发送工业通用CIP通信协议拒绝服务攻击；  4）查看系统是否检测到工业通用CIP通信协议拒绝服务攻击，同时给出相对应的告警，并对攻击流量进行拦截。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业通用CIP通信协议拒绝服务攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **44 信捷PLC设备XD5E-30T4-E的工业通用通信协议安全防护测试项**

|  |
| --- |
| **测试项目：**信捷PLC设备XD5E-30T4-E的工业通用通信协议安全防护 |
| **测试依据：** |
| **测试目的：**  在信捷PLC设备XD5E-30T4-E上进行工业通用通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。在信捷PLC设备XD5E-30T4-E上进行工业通用通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动信捷PLC设备XD5E-30T4-E的工业通用通信协议逻辑处理错误漏洞的防护模式；  3）测试机向信捷PLC设备XD5E-30T4-E的工业通用通信协议逻辑处理错误攻击；  4）查看系统是否检测到工业通用ModbusTCP通信协议逻辑处理错误攻击，同时给出相对应的告警，并对攻击流量进行阻断拦截。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业通用ModbusTCP通信协议逻辑处理错误攻击，并查到相对应的告警，并对攻击流量进行阻断拦截。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **45 施耐德PLC设备Quantum140的工业通用通信协议安全防护测试项**

|  |
| --- |
| **测试项目：**施耐德PLC设备Quantum140的工业通用通信协议安全防护 |
| **测试依据：** |
| **测试目的：**  在施耐德PLC设备Quantum140上进行工业通用通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。在施耐德PLC设备Quantum140上进行工业通用通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动施耐德PLC设备Quantum140的工业通用UMAS通信协议拒绝服务漏洞的防护模式；  3）测试机向施耐德PLC设备Quantum140发送工业通用UMAS通信协议拒绝服务攻击；  4）查看系统是否检测到工业通用UMAS通信协议拒绝服务攻击，同时给出相对应的告警，并对攻击流量进行拦截。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业通用UMAS通信协议拒绝服务攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **46 华茂PLC设备CPU 812-1B0AA-H的工业基础通信协议安全防护测试项**

|  |
| --- |
| **测试项目：**华茂PLC设备CPU 812-1B0AA-H的工业基础通信协议安全防护 |
| **测试依据：** |
| **测试目的：**  在华茂PLC设备CPU 812-1B0AA-H上进行工业基础通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。在华茂PLC设备CPU 812-1B0AA-H上进行工业基础通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动华茂PLC设备CPU 812-1B0AA-H的私有通信协议缓冲区溢出漏洞的防护模式；  3）测试机向信捷华茂PLC设备CPU 812-1B0AA-H发送私有通信协议缓冲区溢出攻击；  4）查看系统是否检测到私有通信协议缓冲区溢出攻击，同时给出相对应的告警，并对攻击流量进行拦截。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到私有通信协议缓冲区溢出攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **47 合信PLC设备CTH2 214-1AD33的工业基础通信协议安全防护测试项**

|  |
| --- |
| **测试项目：**合信PLC设备CTH2 214-1AD33的工业基础通信协议安全防护 |
| **测试依据：** |
| **测试目的：**  在合信PLC设备CTH2 214-1AD33上进行工业基础通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。在合信PLC设备CTH2 214-1AD33上进行工业基础通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动合信PLC设备CTH2 214-1AD33的工业基础TCP协议通信协议拒绝服务漏洞的防护模式；  3）测试机向合信PLC设备CTH2 214-1AD33发送工工业基础TCP协议通信协议拒绝服务攻击；  4）查看系统是否检测到工业基础TCP协议通信协议拒绝服务攻击，同时给出相对应的告警，并对攻击流量进行拦截。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业基础TCP协议通信协议拒绝服务攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **48 傲拓科技PLC设备NA2000的工业基础通信协议安全防护测试项**

|  |
| --- |
| **测试项目：**傲拓科技PLC设备NA2000的工业基础通信协议安全防护 |
| **测试依据：** |
| **测试目的：**  在傲拓科技PLC设备NA2000上进行工业基础通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。在傲拓科技PLC设备NA2000上进行工业基础通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动傲拓科技PLC设备NA2000的工业基础IPv4协议通信协议拒绝服务漏洞的防护模式；  3）测试机向傲拓科技PLC设备NA2000发送工业基础IPv4协议通信协议拒绝服务攻击；  4）查看系统是否检测到工业基础IPv4协议通信协议拒绝服务攻击，同时给出相对应的告警，并对攻击流量进行拦截。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业基础IPv4协议通信协议拒绝服务攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **49 施耐德PLC设备TM241CE40T\_U的工业通用通信协议安全防护测试项**

|  |
| --- |
| **测试项目：**施耐德PLC设备TM241CE40T\_U的工业通用通信协议协议安全防护 |
| **测试依据：** |
| **测试目的：**  在施耐德PLC设备TM241CE40T\_U上进行工业通用通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。在施耐德PLC设备TM241CE40T\_U上进行工业通用通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动施耐德PLC设备TM241CE40T\_U的工业通用TCP协议逻辑处理漏洞的防护模式；  3）测试机向施耐德PLC设备TM241CE40T\_U的工业通用TCP协议逻辑处理攻击；  4）查看系统是否检测到工业基础TCP协议逻辑处理攻击，同时给出相对应的告警，并对攻击流量进行阻断拦截。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业基础TCP协议逻辑处理攻击，并查到相对应的告警，并对攻击流量进行阻断拦截。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **50 显控科技PLC设备FGPR-C8X8T的工业组态通信协议安全防护测试项**

|  |
| --- |
| **测试项目：**显控科技PLC设备FGPR-C8X8T的工业组态通信协议安全防护 |
| **测试依据：** |
| **测试目的：**  在显控科技PLC设备FGPR-C8X8T上进行工业组态通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。在显控科技PLC设备FGPR-C8X8T上进行工业组态通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动显控科技PLC设备FGPR-C8X8T的工业组态私有通信协议拒绝服务漏洞的防护模式；  3）测试机向显控科技PLC设备FGPR-C8X8T发送工业组态私有通信协议拒绝服务攻击；  4）查看系统是否检测到工业组态私有通信协议拒绝服务攻击，同时给出相对应的告警，并对攻击流量进行拦截。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业组态私有通信协议拒绝服务攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **51 和利时PLC设备LK202的工业组态通信协议安全防护测试项**

|  |
| --- |
| **测试项目：**和利时PLC设备LK202的工业组态通信协议安全防护 |
| **测试依据：** |
| **测试目的：**  在和利时PLC设备LK202上进行工业组态通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。在和利时PLC设备LK202上进行工业组态通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动和利时PLC设备LK202的工业组态私有通信协议拒绝服务漏洞的防护模式；  3）测试机向和利时PLC设备LK202发送工业组态私有通信协议拒绝服务攻击；  4）查看系统是否检测到工业组态私有通信协议拒绝服务攻击，同时给出相对应的告警，并对攻击流量进行拦截。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业组态私有通信协议拒绝服务攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **52 MELSEC PLC设备L02CPU-CM的工业组态通信协议安全防护测试项**

|  |
| --- |
| **测试项目：**MELSEC PLC设备L02CPU-CM的工业组态通信协议安全防护 |
| **测试依据：** |
| **测试目的：**  在MELSEC PLC设备L02CPU-CM上进行工业组态通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。在MELSEC PLC设备L02CPU-CM上进行工业组态通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动MELSEC PLC设备L02CPU-CM的工业组态私有通信协议拒绝服务漏洞的防护模式；  3）测试机向MELSEC PLC设备L02CPU-CM发送工业组态私有通信协议拒绝服务攻击；  4）查看系统是否检测到工业组态私有通信协议拒绝服务攻击，同时给出相对应的告警，并对攻击流量进行拦截。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业组态私有通信协议拒绝服务攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **53 TP-LINK的云台网络摄像机TL-IPC43AN-4GY的工业基础通信协议安全防护测试项**

|  |
| --- |
| **测试项目：**TP-LINK的云台网络摄像机TL-IPC43AN-4GY的工业基础通信协议安全防护 |
| **测试依据：** |
| **测试目的：**  在TP-LINK的云台网络摄像机TL-IPC43AN-4GY上进行工业基础通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。在TP-LINK的云台网络摄像机TL-IPC43AN-4GY上进行工业基础通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动TP-LINK的云台网络摄像机TL-IPC43AN-4GY的工业基础TCP协议存在逻辑处理错误漏洞的防护模式；  3）测试机向TP-LINK的云台网络摄像机TL-IPC43AN-4GY发送工业基础TCP协议存在逻辑处理错误漏洞攻击；  4）查看系统是否检测到工业基础TCP协议逻辑处理错误攻击，并查到相对应的告警，并对攻击流量进行阻断拦截。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业基础TCP协议逻辑处理错误攻击，并查到相对应的告警，并对攻击流量进行阻断拦截。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **54 海康威视网络摄像机 DS-2CD7A4XYZ-XZS的工业通用通信协议安全防护测试项**

|  |
| --- |
| **测试项目：**海康威视网络摄像机 DS-2CD7A4XYZ-XZS的工业通用通信协议安全防护 |
| **测试依据：** |
| **测试目的：**  在海康威视网络摄像机DS-2CD7A4XYZ-XZS上进行工业通用通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。在海康威视网络摄像机DS-2CD7A4XYZ-XZS上进行工业通用通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动海康威视网络摄像机 DS-2CD7A4XYZ-XZS的工业通用ONVIF协议内存溢出漏洞的防护模式；  3）测试机向海康威视网络摄像机 DS-2CD7A4XYZ-XZS发送工业通用ONVIF协议内存溢出攻击；  4）查看系统是否检测到工业通用ONVIF协议内存溢出攻击，同时给出相对应的告警，并对攻击流量进行拦截。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业通用ONVIF协议内存溢出攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **55 SIEMENS PLC设备S7-1200的工业通用通信协议安全防护测试项**

|  |
| --- |
| **测试项目：**SIEMENS PLC设备S7-1200的工业通用通信协议安全防护 |
| **测试依据：** |
| **测试目的：**  在SIEMENS PLC设备S7-1200上进行工业通用通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。在SIEMENS PLC设备S7-1200上进行工业通用通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动SIEMENS PLC设备S7-1200的工业通用S7-Comm通信协议拒绝服务漏洞的防护模式；  3）测试机向SIEMENS PLC设备S7-1200发送工业通用S7-Comm通信协议拒绝服务攻击；  4）查看系统是否检测到工业通用S7-Comm通信协议拒绝服务攻击，同时给出相对应的告警，并对攻击流量进行拦截。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业通用S7-Comm通信协议拒绝服务攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **56 中油瑞飞RTU设备的工业组态私有通信协议安全防护测试项**

|  |
| --- |
| **测试项目：**中油瑞飞RTU设备的工业组态私有通信协议安全防护 |
| **测试依据：** |
| **测试目的：**  在中油瑞飞RTU设备上进行工业组态私有通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。在中油瑞飞RTU设备上进行工业组态私有通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动中油瑞飞RTU设备的工业组态私有通信协议反序列化漏洞的防护模式；  3）测试机向中油瑞飞RTU设备发送工业组态私有通信协议反序列化攻击；  4）查看系统是否检测到工业组态私有通信协议反序列化攻击，同时给出相对应的告警，并对攻击流量进行拦截。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业组态私有通信协议反序列化攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **57 360Wi-Fi6路由器T7U 的工业基础通信协议安全防护测试项**

|  |
| --- |
| **测试项目：**360Wi-Fi6路由器T7U 的工业基础通信协议安全防护 |
| **测试依据：** |
| **测试目的：**  在360Wi-Fi6路由器T7U设备上进一步进行工业基础通信协议的安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。在360Wi-Fi6路由器T7U设备上进一步进行工业基础通信协议的安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动360Wi-Fi6路由器T7U 的工业基础TCP协议拒绝服务的防护模式；  3）测试机向360Wi-Fi6路由器T7U 设备发送工业基础TCP协议拒绝服务攻击；  4）查看系统是否检测到工业基础TCP协议拒绝服务攻击，并查到相对应的告警，并对攻击流量进行拦截。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业基础通信协议拒绝服务攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **58 南自保护测控装置PSL-642UA-GZK的工业通用通信协议安全防护测试项**

|  |
| --- |
| **测试项目：**南自保护测控装置PSL-642UA-GZK的工业通用通信协议安全防护 |
| **测试依据：** |
| **测试目的：**  在南自保护测控装置PSL-642UA-GZK上进行工业通用通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。在南自保护测控装置PSL-642UA-GZK上进行工业通用通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动南自保护测控装置PSL-642UA-GZK的工业通用MMS协议逻辑处理错误漏洞的防护模式；  3）测试机向南自保护测控装置PSL-642UA-GZK发送工业通用MMS协议逻辑处理错误攻击；  4）查看系统是否检测到工业通用MMS协议逻辑处理错误攻击，同时给出相对应的告警，并对攻击流量进行拦截。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业通用MMS协议逻辑处理错误攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **59 倍福PLC设备CX2030的工业通用通信协议安全防护测试项**

|  |
| --- |
| **测试项目：**倍福PLC设备CX2030的工业通用通信协议安全防护 |
| **测试依据：** |
| **测试目的：**  在倍福PLC设备CX2030上进行工业通用通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。在倍福PLC设备CX2030上进行工业通用通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动倍福PLC设备CX2030的工业通用通信AMS协议缓冲区溢出漏洞的防护模式；  3）测试机向倍福PLC设备CX2030发送工业通用通信AMS协议缓冲区溢出攻击；  4）查看系统是否检测到工业通用通信AMS协议缓冲区溢出攻击，同时给出相对应的告警，并对攻击流量进行拦截。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业通用通信AMS协议缓冲区溢出攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **60 倍福PLC设备CX8080的工业通用通信协议安全防护测试项**

|  |
| --- |
| **测试项目：**倍福PLC设备CX8080的工业通用通信协议安全防护 |
| **测试依据：** |
| **测试目的：**  在倍福PLC设备CX8080上进行工业通用通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。在倍福PLC设备CX8080上进行工业通用通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动倍福PLC设备CX8080的工业通用通信AMS协议逻辑处理错误漏洞的防护模式；  3）测试机向倍福PLC设备CX8080发送工业通用通信AMS协议逻辑处理错误攻击；  4）查看系统是否检测到工业通用通信AMS协议逻辑处理错误攻击，同时给出相对应的告警，并对攻击流量进行拦截。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业通用通信AMS协议逻辑处理错误攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **61 得捷串口服务器DIGI PortServer TS1工业基础通信协议安全防护测试项**

|  |
| --- |
| **测试项目：**得捷串口服务器DIGI PortServer TS1工业基础通信协议安全防护 |
| **测试依据：** |
| **测试目的：**  在得捷串口服务器DIGI PortServer TS1上进行工业基础通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。在得捷串口服务器DIGI PortServer TS1上进行工业基础通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动得捷串口服务器DIGI PortServer TS1的工业基础通信TCP协议缓冲区溢出漏洞的防护模式；  3）测试机向得捷串口服务器DIGI PortServer TS1发送工业基础通信TCP协议缓冲区溢出攻击；  4）查看系统是否检测到工业基础通信TCP协议缓冲区溢出攻击，同时给出相对应的告警，并对攻击流量进行拦截。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业基础通信TCP协议缓冲区溢出攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **62 研华串口服务器EKI-1511X工业通用通信协议安全防护测试项**

|  |
| --- |
| **测试项目：**研华串口服务器EKI-1511X工业通用通信协议安全防护 |
| **测试依据：** |
| **测试目的：**  在研华串口服务器EKI-1511X上进行工业通用通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。在研华串口服务器EKI-1511X上进行工业通用通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动研华串口服务器EKI-1511X的工业通用HTTP协议缓冲区溢出漏洞的防护模式；  3）测试机向研华串口服务器EKI-1511X发送工业通用HTTP协议缓冲区溢出攻击；  4）查看系统是否检测到工业通用HTTP协议缓冲区溢出攻击，同时给出相对应的告警，并对攻击流量进行拦截。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业通用HTTP协议缓冲区溢出攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **63 研华串口服务器EKI-1521CE工业设备WEB服务命令执行安全防护测试项**

|  |
| --- |
| **测试项目：**研华串口服务器EKI-1521CE工业设备WEB服务命令执行安全防护 |
| **测试依据：** |
| **测试目的：**  在研华串口服务器EKI-1521CE上进行工业设备WEB服务命令执行安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。在研华串口服务器EKI-1521CE上进行工业设备WEB服务命令执行安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动研华串口服务器EKI-1521CE的工业设备WEB服务命令执行漏洞的防护模式；  3）测试机向研华串口服务器EKI-1521CE发送工业设备WEB服务命令执行攻击；  4）查看系统是否检测到工业设备WEB服务命令执行攻击，同时给出相对应的告警，并对攻击流量进行拦截。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业设备WEB服务命令执行攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **64 信捷PLC设备XDME-30T4-E工业通用通信协议安全防护测试项**

|  |
| --- |
| **测试项目：**信捷PLC设备XDME-30T4-E工业通用通信协议安全防护 |
| **测试依据：** |
| **测试目的：**  在信捷PLC设备XDME-30T4-E上进行工业通用通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。在信捷PLC设备XDME-30T4-E上进行工业通用通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动信捷PLC设备XDME-30T4-E工业通用通信Modbus协议缓冲区溢出漏洞的防护模式；  3）测试机向信捷PLC设备XDME-30T4-E发送工业通用通信Modbus协议缓冲区溢出攻击；  4）查看系统是否检测到工业通用Modbus协议缓冲区溢出攻击，同时给出相对应的告警，并对攻击流量进行阻断拦截。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业通用Modbus协议缓冲区溢出攻击，并查到相对应的告警，并对攻击流量进行阻断拦截。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **65 康耐得串口服务器 C2000-B2-SFE0101-BB1工业基础通信协议安全防护测试项**

|  |
| --- |
| **测试项目：**康耐得串口服务器 C2000-B2-SFE0101-BB1工业基础通信协议安全防护 |
| **测试依据：** |
| **测试目的：**  在康耐得串口服务器C2000-B2-SFE0101-BB1上进行工业基础通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。在康耐得串口服务器C2000-B2-SFE0101-BB1上进行工业基础通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动康耐得串口服务器 C2000-B2-SFE0101-BB1的工业基础通信TCP协议缓冲区溢出漏洞的防护模式；  3）测试机向康耐得串口服务器 C2000-B2-SFE0101-BB1发送工业基础通信TCP协议缓冲区溢出攻击；  4）查看系统是否检测到工业基础通信TCP协议缓冲区溢出攻击，同时给出相对应的告警，并对攻击流量进行拦截。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业基础通信TCP协议缓冲区溢出攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **66 欧姆龙PLC设备 NX102-9000工业通用通信协议安全防护测试项**

|  |
| --- |
| **测试项目：**欧姆龙PLC设备 NX102-9000工业通用通信协议安全防护 |
| **测试依据：** |
| **测试目的：**  在欧姆龙PLC设备NX102-9000上进行工业通用通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。在欧姆龙PLC设备NX102-9000上进行工业通用通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动欧姆龙PLC设备 NX102-9000的工业通用HTTP协议逻辑处理错误漏洞的防护模式；  3）测试机向欧姆龙PLC设备 NX102-9000发送工业通用HTTP协议逻辑处理错误攻击；  4）查看系统是否检测到工业通用HTTP协议逻辑处理错误攻击，同时给出相对应的告警，并对攻击流量进行拦截。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业通用HTTP协议逻辑处理错误攻击，并查到相对应的告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **67 台达PLC设备AS332T工业通用通信协议安全防护测试项**

|  |
| --- |
| **测试项目：**台达PLC设备AS332T工业通用通信协议安全防护 |
| **测试依据：** |
| **测试目的：**  在台达PLC设备AS332T上进行工业通用通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。在台达PLC设备AS332T上进行工业通用通信协议安全防护测试，确保设备在面对潜在攻击时能够保持通信协议的安全性和稳定性。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）将系统串接在测试机和被测设备的攻击路径之间；  2）在系统中启动台达PLC设备AS332T工业通用CIP通信协议拒绝服务漏洞的防护模式；  3）测试机向台达PLC设备AS332T发送工业通用CIP通信协议拒绝服务攻击；  4）查看系统是否检测到工业基础CIP协议通信协议拒绝服务攻击，同时给出相对应的告警，并对攻击流量进行阻断拦截。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能检测到工业通用CIP通信协议拒绝服务攻击，查到相对应的告警，并对攻击流量进行阻断拦截。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **68 基于攻击检测与重构的弹性协同控制算法攻击检测与响应功能验证测试项**

|  |
| --- |
| **测试项目：**基于攻击检测与重构的弹性协同控制算法攻击检测与响应功能验证测试项 |
| **测试依据：** |
| **测试目的：**  验证基于攻击检测与重构的弹性协同控制算法攻击检测能否正确检测到典型攻击行为，并验证车辆在协同运行中的稳定跟踪能力验证基于攻击检测与重构的弹性协同控制算法攻击检测能否正确检测到典型攻击行为，并验证车辆在协同运行中的稳定跟踪能力 |
| **测试配置：** |
| **测试步骤：**  功能测试方法：   1. 人工注入攻击数据并记录系统响应行为。   性能测试方法：  1）记录恢复时间与误差曲线，自动化比对参考阈值。 |
| **预期结果：**  功能测试应覆盖以下内容：  1）模拟攻击后系统报警/响应是否及时；  2）间距/误差恢复功能是否启动。  3）是否支持欺骗、DoS、重放攻击三种攻击的注入。  性能测试应覆盖以下内容：  1）针对三种攻击，攻击识别时间是否≤5s；  2）针对三种攻击，误差恢复后是否稳定小于5%。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **69 基于信道重构的安全协同控制算法检测与响应功能验证测试项**

|  |
| --- |
| **测试项目：**基于信道重构的安全协同控制算法检测与响应功能验证测试项 |
| **测试依据：** |
| **测试目的：**  验证基于信道重构的安全协同控制算法检测与响应功能验证测试项能否正确检测到典型攻击行为，并验证车辆在协同运行中的稳定跟踪能力验证基于信道重构的安全协同控制算法检测与响应功能验证测试项能否正确检测到典型攻击行为，并验证车辆在协同运行中的稳定跟踪能力 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）人工注入攻击数据并记录系统响应行为。  性能测试方法：  1）记录恢复时间与误差曲线，自动化比对参考阈值。 |
| **预期结果：**  功能测试应覆盖以下内容：  1）模拟攻击后系统报警/响应是否及时；  2）间距/误差恢复功能是否启动。  3）是否支持欺骗、DoS、重放攻击三种攻击的注入。 性能测试应覆盖以下内容：  1）针对三种攻击，攻击识别时间是否≤0.5s；  2）针对三种攻击，误差恢复后是否稳定小于5%。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **70 云端数据记录与可视化测试测试项**

|  |
| --- |
| **测试项目：**云端数据记录与可视化测试测试项 |
| **测试依据：** |
| **测试目的：**  验证系统状态上传、日志记录、UI显示正确验证系统状态上传、日志记录、UI显示正确 |
| **测试配置：** |
| **测试步骤：**  功能测试方法：  1）人工操作测试、日志比对。  性能测试方法：  1）人工操作测试 |
| **预期结果：**  功能测试应覆盖以下内容：  1）验证正常或攻击条件下功能是否正确；  2）相关控制模块能否触发相应应急机制； 性能测试应覆盖以下内容：  1）评估正常或攻击条件下功能是否正确；  2）评估控制模块等核心性能项。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **71 工业软件脆弱性检测与防护模块的登录测试项**

|  |
| --- |
| **测试项目：**工业软件脆弱性检测与防护模块的登录测试 |
| **测试依据：** |
| **测试目的：**  在工业软件脆弱性检测与防护模块上进行登录功能测试，验证模块的登录机制是否健全在工业软件脆弱性检测与防护模块上进行登录功能测试，验证模块的登录机制是否健全 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）启动系统并进入登录界面；  2）在用户名输入框中输入有效用户名，在密码输入框中输入对应密码；  3）点击“登录”按钮；  4）验证系统是否允许登录并跳转至系统主界面。 |
| **预期结果：**  测试应覆盖以下内容：  1）用户通过输入正确的用户名和密码，能够成功完成身份验证并进入系统主界面。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **72 工业软件脆弱性检测与防护模块的退出测试项**

|  |
| --- |
| **测试项目：**工业软件脆弱性检测与防护模块的退出测试 |
| **测试依据：** |
| **测试目的：**  在工业软件脆弱性检测与防护模块上进行退出功能测试，验证模块的退出机制是否健全在工业软件脆弱性检测与防护模块上进行退出功能测试，验证模块的退出机制是否健全 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）登录进入系统主界面；  2）点击系统界面中的“退出”或“注销”按钮；  3）观察系统是否成功退出并跳转到登录页面。 |
| **预期结果：**  测试应覆盖以下内容：  1）用户点击退出按钮后，系统能够正常退出当前登录状态，并跳转回登录页面。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **73工业软件脆弱性检测与防护模块的病毒木马检测任务列表展示测试项**

|  |
| --- |
| **测试项目：**工业软件脆弱性检测与防护模块的病毒木马检测任务列表展示测试 |
| **测试依据：** |
| **测试目的：**  在工业软件脆弱性检测与防护模块上，测试病毒木马检测任务列表的展示功能，确保列表能准确、全面地展示所有已创建的病毒木马检测任务。在工业软件脆弱性检测与防护模块上，测试病毒木马检测任务列表的展示功能，确保列表能准确、全面地展示所有已创建的病毒木马检测任务。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）确保系统处于正常运行状态，进入工业软件脆弱性检测与防护模块；  2）点击进入病毒木马检测任务管理界面，或新建病毒木马检测任务并启动；  3）查看系统是否能够成功展示任务列表页面；  4）检查任务列表中是否准确显示任务编号、任务名称、启动时间、扫描进度、更新时间和任务状态等关键信息。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能够正常展示病毒木马检测任务列表页面，并准确显示各任务的相关信息，包括任务编号、任务名称、启动时间、扫描进度、更新时间和任务状态。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **74 工业软件脆弱性检测与防护模块的病毒木马检测任务查询测试项**

|  |
| --- |
| **测试项目：**工业软件脆弱性检测与防护模块的病毒木马检测任务查询测试 |
| **测试依据：** |
| **测试目的：**  在工业软件脆弱性检测与防护模块上，测试病毒木马检测任务的查询功能，确保用户能够通过查询条件准确查找到特定的病毒木马检测任务。在工业软件脆弱性检测与防护模块上，测试病毒木马检测任务的查询功能，确保用户能够通过查询条件准确查找到特定的病毒木马检测任务。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）登录系统并进入工业软件脆弱性检测与防护模块中的病毒木马检测任务列表页面；  2）在查询区域输入或选择相应的查询条件（如任务名称、启动时间范围、任务状态等）；  3）点击“查询”按钮；  4）核对系统展示的查询结果是否与设置的条件一致，并确认列表中显示任务编号、任务名称、启动时间、扫描进度、更新时间和任务状态等字段信息。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能够根据用户输入的查询条件，准确筛选并展示符合条件的病毒木马检测任务列表信息。列表中需显示任务编号、任务名称、启动时间、扫描进度、更新时间和任务状态。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **75 工业软件脆弱性检测与防护模块的病毒木马检测任务创建测试项**

|  |
| --- |
| **测试项目：**工业软件脆弱性检测与防护模块的病毒木马检测任务创建测试 |
| **测试依据：** |
| **测试目的：**  在工业软件脆弱性检测与防护模块上，测试病毒木马检测任务的创建功能，确保用户能够顺利创建病毒木马检测任务，并配置相应的检测参数。通过此测试项，验证系统的任务创建机制是否健全，能否为用户提供灵活且高效的病毒木马检测任务配置能力。在工业软件脆弱性检测与防护模块上，测试病毒木马检测任务的创建功能，确保用户能够顺利创建病毒木马检测任务，并配置相应的检测参数。通过此测试项，验证系统的任务创建机制是否健全，能否为用户提供灵活且高效的病毒木马检测任务配置能力。 |
| **测试配置：** |
| **测试步骤：**  1）登录系统并进入工业软件脆弱性检测与防护模块中的病毒木马检测任务管理界面；  2）点击“新建任务”按钮，填写任务名称、扫描目标、检测范围等必要信息；  3）点击“确定”或“创建”按钮提交；  4）观察系统是否提示“创建成功”，并检查新建任务是否出现在任务列表中，字段信息完整。 |
| **预期结果：**  每一步骤都有正确结果。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **76 工业软件脆弱性检测与防护模块的病毒木马检测任务单条删除测试项**

|  |
| --- |
| **测试项目：**工业软件脆弱性检测与防护模块的病毒木马检测任务单条删除测试 |
| **测试依据：** |
| **测试目的：**  在工业软件脆弱性检测与防护模块中，测试病毒木马检测任务的单条删除功能，确保用户能够准确删除指定的病毒木马检测任务，且删除操作不会对系统其他功能造成不良影响。通过此测试项，验证系统的任务删除机制是否健全，能否为用户提供安全、高效的病毒木马检测任务管理功能。在工业软件脆弱性检测与防护模块中，测试病毒木马检测任务的单条删除功能，确保用户能够准确删除指定的病毒木马检测任务，且删除操作不会对系统其他功能造成不良影响。通过此测试项，验证系统的任务删除机制是否健全，能否为用户提供安全、高效的病毒木马检测任务管理功能。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）登录系统并进入工业软件脆弱性检测与防护模块的病毒木马检测任务管理界面；  2）在任务列表中选择一条已有的病毒木马检测任务；  3）点击“删除”按钮，系统弹出确认提示后确认删除；  4）观察是否弹出“操作成功”的提示，任务是否从任务列表中移除。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能够成功删除用户选择的单条病毒木马检测任务，并弹出提示“操作成功”，任务从列表中移除。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **77 工业软件脆弱性检测与防护模块的病毒木马检测任务批量删除测试项**

|  |
| --- |
| **测试项目：**工业软件脆弱性检测与防护模块的病毒木马检测任务批量删除测试 |
| **测试依据：** |
| **测试目的：**  在工业软件脆弱性检测与防护模块中，测试病毒木马检测任务的批量删除功能，确保用户能够高效地管理和清理不再需要的检测任务。通过此测试项，验证系统是否支持批量删除操作，以及该操作是否能准确、安全地执行，避免对系统其他功能造成干扰或数据丢失。在工业软件脆弱性检测与防护模块中，测试病毒木马检测任务的批量删除功能，确保用户能够高效地管理和清理不再需要的检测任务。通过此测试项，验证系统是否支持批量删除操作，以及该操作是否能准确、安全地执行，避免对系统其他功能造成干扰或数据丢失。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）登录系统并进入工业软件脆弱性检测与防护模块的病毒木马检测任务管理界面；  2）在任务列表中勾选多条需要删除的病毒木马检测任务；  3）点击“批量删除”按钮，系统弹出确认提示后确认删除操作；  4）检查系统是否提示“操作成功”，并确认所选任务均从任务列表中移除。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能够成功批量删除用户勾选的多条病毒木马检测任务，操作完成后弹出提示“操作成功”，被删除的任务从任务列表中移除。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **78 工业软件脆弱性检测与防护模块的病毒木马检测报告详情查看测试项**

|  |
| --- |
| **测试项目：**工业软件脆弱性检测与防护模块的病毒木马检测报告详情查看测试 |
| **测试依据：** |
| **测试目的：**  在工业软件脆弱性检测与防护模块中，测试用户是否能够详细查看病毒木马检测报告的详细内容，确保报告信息准确、完整，并能为用户提供有价值的安全分析和改进建议。通过此测试项，验证系统是否支持详尽的报告查看功能，以及该功能是否稳定、易用。在工业软件脆弱性检测与防护模块中，测试用户是否能够详细查看病毒木马检测报告的详细内容，确保报告信息准确、完整，并能为用户提供有价值的安全分析和改进建议。通过此测试项，验证系统是否支持详尽的报告查看功能，以及该功能是否稳定、易用。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）登录系统并进入工业软件脆弱性检测与防护模块的病毒木马检测任务管理界面；  2）在任务列表中选择一条已完成的病毒木马检测任务；  3）点击“查看报告”或“详情”按钮；  4）核对进入的页面是否展示任务基本信息和漏洞列表；  5）检查漏洞列表中是否准确显示漏洞ID、漏洞名称、漏洞等级、漏洞描述等信息。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能够成功进入病毒木马检测报告详情页面，页面展示任务的基本信息及对应的漏洞列表。漏洞列表应完整显示漏洞ID、漏洞名称、漏洞等级、漏洞描述等字段。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **79 工业软件脆弱性检测与防护模块的工业终端协议安全检测任务列表展示测试项**

|  |
| --- |
| **测试项目：**工业软件脆弱性检测与防护模块的工业终端协议安全检测任务列表展示测试 |
| **测试依据：** |
| **测试目的：**  在工业软件脆弱性检测与防护模块上，测试工业终端协议安全检测任务列表的展示功能，确保列表能够准确、全面地展示所有已创建的工业终端协议安全检测任务。通过此测试项，验证系统是否支持任务列表的高效展示，以及展示的信息是否详尽、准确，能否为用户提供便捷的任务管理体验。在工业软件脆弱性检测与防护模块上，测试工业终端协议安全检测任务列表的展示功能，确保列表能够准确、全面地展示所有已创建的工业终端协议安全检测任务。通过此测试项，验证系统是否支持任务列表的高效展示，以及展示的信息是否详尽、准确，能否为用户提供便捷的任务管理体验。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）登录系统并进入工业软件脆弱性检测与防护模块的工业终端协议安全检测功能界面；  2）点击进入“任务列表”页面；  3）检查页面是否成功加载并显示所有已存在的工业终端协议安全检测任务；  4）核对列表中是否展示任务编号、任务名称、启动时间、扫描进度、更新时间和任务状态等字段信息。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能够成功进入工业终端协议安全检测任务列表页面，页面正确显示所有任务的基本信息，包括任务编号、任务名称、启动时间、扫描进度、更新时间和任务状态。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **80 工业软件脆弱性检测与防护模块的工业终端协议安全检测任务查询测试项**

|  |
| --- |
| **测试项目：**工业软件脆弱性检测与防护模块的工业终端协议安全检测任务查询测试 |
| **测试依据：** |
| **测试目的：**  在工业软件脆弱性检测与防护模块上，测试工业终端协议安全检测任务的查询功能，确保用户能够通过合理的查询条件快速定位到特定的工业终端协议安全检测任务。此测试项旨在验证系统的查询机制是否高效、准确，能否为用户提供便捷的任务检索能力。在工业软件脆弱性检测与防护模块上，测试工业终端协议安全检测任务的查询功能，确保用户能够通过合理的查询条件快速定位到特定的工业终端协议安全检测任务。此测试项旨在验证系统的查询机制是否高效、准确，能否为用户提供便捷的任务检索能力。 |
| **测试配置：** |
| **测试步骤：**  1）登录系统并进入工业软件脆弱性检测与防护模块的工业终端协议安全检测任务管理界面；  2）在查询区域输入或选择查询条件（如任务名称、启动时间范围、任务状态等）；  3）点击“查询”按钮；  4）验证查询结果是否准确，并确认列表中显示任务编号、任务名称、启动时间、扫描进度、更新时间和任务状态等字段信息。 |
| **预期结果：**  每一步骤都有正确结果。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **81 工业软件脆弱性检测与防护模块的工业终端协议安全检测任务创建测试项**

|  |
| --- |
| **测试项目：**工业软件脆弱性检测与防护模块的工业终端协议安全检测任务创建测试 |
| **测试依据：** |
| **测试目的：**  在工业软件脆弱性检测与防护模块上，测试用户能否成功创建工业终端协议安全检测任务。此测试项旨在确保用户能够顺利配置所需的检测参数，并验证系统的任务创建流程是否顺畅、高效。在工业软件脆弱性检测与防护模块上，测试用户能否成功创建工业终端协议安全检测任务。此测试项旨在确保用户能够顺利配置所需的检测参数，并验证系统的任务创建流程是否顺畅、高效。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）登录系统并进入工业软件脆弱性检测与防护模块的工业终端协议安全检测功能界面；  2）点击“新建任务”按钮，填写任务名称、检测协议类型、扫描目标、检测范围等必要信息；  3）点击“确定”或“创建”按钮提交；  4）观察系统是否提示“创建成功”，并检查新建任务是否出现在工业终端协议安全检测任务列表中，字段信息完整。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能够成功创建一条新的工业终端协议安全检测任务，创建完成后提示“创建成功”，并将该任务自动添加到工业终端协议安全检测任务列表中，显示任务编号、任务名称、启动时间等信息。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **82 工业软件脆弱性检测与防护模块的工业终端协议安全检测任务单条删除测试项**

|  |
| --- |
| **测试项目：**工业软件脆弱性检测与防护模块的工业终端协议安全检测任务单条删除测试 |
| **测试依据：** |
| **测试目的：**  在工业软件脆弱性检测与防护模块中，测试用户能否准确删除指定的工业终端协议安全检测任务，确保删除操作不会对系统其他功能造成不良影响。此测试项旨在验证系统的任务删除机制是否健全，能否为用户提供安全、高效的工业终端协议安全检测任务管理功能。在工业软件脆弱性检测与防护模块中，测试用户能否准确删除指定的工业终端协议安全检测任务，确保删除操作不会对系统其他功能造成不良影响。此测试项旨在验证系统的任务删除机制是否健全，能否为用户提供安全、高效的工业终端协议安全检测任务管理功能。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）登录系统并进入工业软件脆弱性检测与防护模块的工业终端协议安全检测任务管理界面；  2）在任务列表中选择一条待删除的工业终端协议安全检测任务；  3）点击“删除”按钮，确认删除操作；  4）观察是否弹出“操作成功”提示，并确认该任务已从列表中移除。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能够成功删除用户选择的单条工业终端协议安全检测任务，并弹出提示“操作成功”，任务从列表中移除。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **83 工业软件脆弱性检测与防护模块的工业终端协议安全检测任务批量删除测试项**

|  |
| --- |
| **测试项目：**工业软件脆弱性检测与防护模块的工业终端协议安全检测任务批量删除测试 |
| **测试依据：** |
| **测试目的：**  在工业软件脆弱性检测与防护模块中，测试用户能否批量删除指定的工业终端协议安全检测任务，确保批量删除操作高效、准确，且不会对系统其他功能造成不良影响。此测试项旨在验证系统是否支持批量删除工业终端协议安全检测任务的功能，以及该功能是否健全、安全，能否为用户提供便捷的任务管理手段。在工业软件脆弱性检测与防护模块中，测试用户能否批量删除指定的工业终端协议安全检测任务，确保批量删除操作高效、准确，且不会对系统其他功能造成不良影响。此测试项旨在验证系统是否支持批量删除工业终端协议安全检测任务的功能，以及该功能是否健全、安全，能否为用户提供便捷的任务管理手段。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）登录系统并进入工业软件脆弱性检测与防护模块的工业终端协议安全检测任务管理界面；  2）在任务列表中勾选多条待删除的工业终端协议安全检测任务；  3）点击“批量删除”按钮，确认删除操作；  4）观察系统是否提示“操作成功”，并确认所选任务均从列表中移除。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能够成功批量删除用户勾选的多条工业终端协议安全检测任务，删除操作完成后弹出提示“操作成功”，已删除的任务从任务列表中移除。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **84 工业软件脆弱性检测与防护模块的工业终端协议安全检测报告详情查看测试项**

|  |
| --- |
| **测试项目：**工业软件脆弱性检测与防护模块的工业终端协议安全检测报告详情查看测试 |
| **测试依据：** |
| **测试目的：**  在工业软件脆弱性检测与防护模块中，测试用户能否详细查看工业终端协议安全检测报告的详细内容。此测试项旨在确保用户能够获取到详尽、准确的检测报告信息，包括检测任务的基本信息、漏洞列表、漏洞详情等，以便用户根据报告进行安全分析和改进。通过此测试项，验证系统是否支持工业终端协议安全检测报告的详细查看功能，以及该功能是否稳定、易用，能否为用户提供有价值的安全参考。在工业软件脆弱性检测与防护模块中，测试用户能否详细查看工业终端协议安全检测报告的详细内容。此测试项旨在确保用户能够获取到详尽、准确的检测报告信息，包括检测任务的基本信息、漏洞列表、漏洞详情等，以便用户根据报告进行安全分析和改进。通过此测试项，验证系统是否支持工业终端协议安全检测报告的详细查看功能，以及该功能是否稳定、易用，能否为用户提供有价值的安全参考。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）登录系统并进入工业软件脆弱性检测与防护模块的工业终端协议安全检测任务管理界面；  2）在任务列表中选择一条已完成的检测任务；  3）点击“查看报告”或“详情”按钮；  4）核对进入的页面是否展示任务基本信息；  5）检查漏洞列表中是否准确显示漏洞ID、漏洞名称、漏洞等级、漏洞描述等信息。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能够成功进入工业终端协议安全检测报告详情页面，页面展示任务的基本信息和漏洞列表。漏洞列表应完整显示漏洞ID、漏洞名称、漏洞等级、漏洞描述等字段。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **85 工业软件脆弱性检测与防护模块的工业软件漏洞检测任务列表展示测试项**

|  |
| --- |
| **测试项目：**工业软件脆弱性检测与防护模块的工业软件漏洞检测任务列表展示测试 |
| **测试依据：** |
| **测试目的：**  在工业软件脆弱性检测与防护模块中，测试工业软件漏洞检测任务列表的展示功能，确保列表能够准确、全面地展示所有已创建的工业软件漏洞检测任务。此测试项旨在验证系统是否支持工业软件漏洞检测任务列表的高效展示，以及展示的信息是否详尽、准确，能否为用户提供便捷的任务管理体验。通过此测试项，用户能够直观地查看和管理已创建的工业软件漏洞检测任务，从而提高工作效率和安全性。在工业软件脆弱性检测与防护模块中，测试工业软件漏洞检测任务列表的展示功能，确保列表能够准确、全面地展示所有已创建的工业软件漏洞检测任务。此测试项旨在验证系统是否支持工业软件漏洞检测任务列表的高效展示，以及展示的信息是否详尽、准确，能否为用户提供便捷的任务管理体验。通过此测试项，用户能够直观地查看和管理已创建的工业软件漏洞检测任务，从而提高工作效率和安全性。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）登录系统并进入工业软件脆弱性检测与防护模块的工业软件漏洞检测功能界面；  2）点击“任务列表”或进入任务管理模块；  3）验证页面是否正常加载并展示任务列表；  4）确认任务列表中是否显示任务名称、执行类型、启动时间、扫描进度、存活资产统计、风险统计、风险资产统计、更新时间和任务状态字段。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能够成功进入工业软件漏洞检测任务列表页面，并正确展示任务信息。页面应完整显示任务名称、执行类型、启动时间、扫描进度、存活资产统计、风险统计、风险资产统计、更新时间和任务状态等字段。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **86 工业软件脆弱性检测与防护模块的工业软件漏洞检测任务查询测试项**

|  |
| --- |
| **测试项目：**工业软件脆弱性检测与防护模块的工业软件漏洞检测任务查询测试 |
| **测试依据：** |
| **测试目的：**  在工业软件脆弱性检测与防护模块上，测试用户能否通过合理的查询条件快速定位到特定的工业软件漏洞检测任务。此测试项旨在验证系统的查询功能是否高效、准确，能否为用户提供便捷的任务检索体验。在工业软件脆弱性检测与防护模块上，测试用户能否通过合理的查询条件快速定位到特定的工业软件漏洞检测任务。此测试项旨在验证系统的查询功能是否高效、准确，能否为用户提供便捷的任务检索体验。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）登录系统并进入工业软件脆弱性检测与防护模块的工业软件漏洞检测任务管理界面；  2）在查询区域填写或选择查询条件（如任务名称、执行类型、任务状态、启动时间范围等）；  3）点击“查询”按钮；  4）核对系统是否成功返回匹配结果，并确认列表显示字段完整，包括任务名称、执行类型、启动时间、扫描进度、存活资产统计、风险统计、风险资产统计、更新时间和任务状态。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能够根据用户设定的查询条件，成功筛选并展示符合条件的工业软件漏洞检测任务列表，列表中应完整显示任务名称、执行类型、启动时间、扫描进度、存活资产统计、风险统计、风险资产统计、更新时间和任务状态等字段。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **87 工业软件脆弱性检测与防护模块的工业软件漏洞检测任务创建测试项**

|  |
| --- |
| **测试项目：**工业软件脆弱性检测与防护模块的工业软件漏洞检测任务创建测试 |
| **测试依据：** |
| **测试目的：**  在工业软件脆弱性检测与防护模块上，测试用户能否成功创建工业软件漏洞检测任务。此测试项旨在确保用户能够顺利配置所需的检测参数，包括目标软件、检测范围、检测深度等，并验证系统的任务创建流程是否顺畅、高效。通过此测试项，可以评估系统对用户输入的响应速度、任务创建的准确性以及系统资源的分配效率。在工业软件脆弱性检测与防护模块上，测试用户能否成功创建工业软件漏洞检测任务。此测试项旨在确保用户能够顺利配置所需的检测参数，包括目标软件、检测范围、检测深度等，并验证系统的任务创建流程是否顺畅、高效。通过此测试项，可以评估系统对用户输入的响应速度、任务创建的准确性以及系统资源的分配效率。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）登录系统并进入工业软件脆弱性检测与防护模块的工业软件漏洞检测功能界面；  2）点击“新建任务”按钮，填写任务名称、目标资产范围、执行方式（如手动/自动）、扫描策略等必要信息；  3）点击“确定”或“创建”按钮提交任务；  4）观察是否弹出“创建成功”的提示；  5）进入任务列表页面，确认新任务已添加至列表，并显示任务名称、执行类型、启动时间等字段。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能够成功创建一条新的工业软件漏洞检测任务，创建后弹出提示“创建成功”，并将新任务显示在工业软件漏洞检测任务列表中，展示任务名称、执行类型、启动时间等相关信息。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **88 工业软件脆弱性检测与防护模块的工业软件漏洞检测任务单条删除测试项**

|  |
| --- |
| **测试项目：**工业软件脆弱性检测与防护模块的工业软件漏洞检测任务单条删除测试 |
| **测试依据：** |
| **测试目的：**  在工业软件脆弱性检测与防护模块中，验证用户执行单条工业软件漏洞检测任务删除操作的准确性和系统响应情况。确保删除操作不仅能够有效移除指定的任务，同时不会干扰或影响系统中其他正在运行或待执行的任务。通过此测试项，进一步巩固系统的任务管理功能，为用户提供更加精确和可靠的任务操作体验。在工业软件脆弱性检测与防护模块中，验证用户执行单条工业软件漏洞检测任务删除操作的准确性和系统响应情况。确保删除操作不仅能够有效移除指定的任务，同时不会干扰或影响系统中其他正在运行或待执行的任务。通过此测试项，进一步巩固系统的任务管理功能，为用户提供更加精确和可靠的任务操作体验。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）登录系统并进入工业软件脆弱性检测与防护模块的工业软件漏洞检测任务管理界面；  2）在任务列表中勾选一条需要删除的任务；  3）点击“删除”按钮，确认执行删除操作；  4）检查系统是否提示“操作成功”，并确认该任务从列表中被移除。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能够成功删除用户选定的单条工业软件漏洞检测任务，删除后弹出提示“操作成功”，并从任务列表中移除该任务项。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **89 工业软件脆弱性检测与防护模块的工业软件漏洞检测任务批量删除测试项**

|  |
| --- |
| **测试项目：**工业软件脆弱性检测与防护模块的工业软件漏洞检测任务批量删除测试 |
| **测试依据：** |
| **测试目的：**  通过此测试项，旨在验证在工业软件脆弱性检测与防护模块中，系统批量删除工业软件漏洞检测任务的效率、准确性以及对系统其他功能的影响。确保批量删除操作不仅能够有效移除多条指定的检测任务，同时不会对系统的其他功能造成任何干扰或不良影响。此测试项对于提升系统的任务管理效率、确保系统稳定性具有重要意义。通过此测试项，旨在验证在工业软件脆弱性检测与防护模块中，系统批量删除工业软件漏洞检测任务的效率、准确性以及对系统其他功能的影响。确保批量删除操作不仅能够有效移除多条指定的检测任务，同时不会对系统的其他功能造成任何干扰或不良影响。此测试项对于提升系统的任务管理效率、确保系统稳定性具有重要意义。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）登录系统并进入工业软件脆弱性检测与防护模块的工业软件漏洞检测任务管理界面；  2）在任务列表中勾选多条待删除的工业软件漏洞检测任务；  3）点击“批量删除”按钮，确认删除操作；  4）观察系统是否提示“操作成功”，并确认所选任务均从列表中移除。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能够成功批量删除用户选中的多条工业软件漏洞检测任务，删除操作完成后弹出提示“操作成功”，被删除的任务从任务列表中移除。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **90 工业软件脆弱性检测与防护模块的工业软件漏洞检测报告详情查看测试项**

|  |
| --- |
| **测试项目：**工业软件脆弱性检测与防护模块的工业软件漏洞检测报告详情查看测试 |
| **测试依据：** |
| **测试目的：**  该测试项重点考察用户在工业软件脆弱性检测与防护模块中，对工业软件漏洞检测报告的深入了解和分析能力。通过详细查看报告内容，用户可以全面掌握检测任务的关键信息，包括但不限于漏洞的具体位置、潜在威胁级别、修复建议等。这不仅有助于用户及时识别并应对潜在的安全风险，也为后续的安全加固和漏洞修复工作提供了重要的参考依据。该测试项重点考察用户在工业软件脆弱性检测与防护模块中，对工业软件漏洞检测报告的深入了解和分析能力。通过详细查看报告内容，用户可以全面掌握检测任务的关键信息，包括但不限于漏洞的具体位置、潜在威胁级别、修复建议等。这不仅有助于用户及时识别并应对潜在的安全风险，也为后续的安全加固和漏洞修复工作提供了重要的参考依据。 |
| **测试配置：** |
| **测试步骤：**  系统能够成功进入工业软件漏洞检测报告详情页面，页面内容完整，包含任务基本信息、任务概述、资产概览、风险资产统计列表和漏洞分布列表。  1）任务概述应包含风险资产统计数据、漏洞统计数量和弱口令统计数据；  2）资产概览应展示厂商分布、类型分布、资产型号分布、固件版本分布、操作系统分布、端口分布和服务分布TOP5；  3）风险资产统计列表应包含IP、厂商、操作系统、设备类型、弱口令、漏洞风险信息；  4）漏洞分布列表应包含漏洞厂商、名称、级别、验证状态、影响IP数量和漏洞详情。  测试方法：  1）登录系统并进入工业软件脆弱性检测与防护模块的工业软件漏洞检测任务管理界面；  2）在任务列表中选择一条已完成的检测任务；  3）点击“查看报告”或“报告详情”按钮进入报告页面；  4）核查页面是否正确显示任务基本信息和任务概述（包括风险资产统计数据、漏洞统计数量、弱口令统计数据）；  5）检查资产概览各分布图是否显示正常，包括厂商、类型、资产型号、固件版本、操作系统、端口和服务分布TOP5；  6）核对风险资产统计列表中的字段完整性（IP、厂商、操作系统、设备类型、弱口令、漏洞风险信息）；  7）核对漏洞分布列表中是否正确显示漏洞厂商、名称、级别、验证状态、影响IP数量和漏洞详情。 |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **91 工业软件脆弱性检测与防护模块的工业软件基线检测任务列表展示测试项**

|  |
| --- |
| **测试项目：**工业软件脆弱性检测与防护模块的工业软件基线检测任务列表展示测试 |
| **测试依据：** |
| **测试目的：**  在工业软件脆弱性检测与防护模块中，此测试项旨在验证系统能否准确、全面地展示已创建的工业软件基线检测任务列表。通过直观的列表展示，用户可以方便地浏览、管理和监控各项基线检测任务的执行状态和结果，从而有效提升安全检测工作的效率和准确性。在工业软件脆弱性检测与防护模块中，此测试项旨在验证系统能否准确、全面地展示已创建的工业软件基线检测任务列表。通过直观的列表展示，用户可以方便地浏览、管理和监控各项基线检测任务的执行状态和结果，从而有效提升安全检测工作的效率和准确性。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）登录系统并进入工业软件脆弱性检测与防护模块的工业软件基线检测功能界面；  2）点击“任务管理”或进入基线检测任务列表页面；  3）验证页面是否正常加载并显示任务列表；  4）确认任务列表中字段是否完整显示，包括任务编号、任务名称、启动时间、扫描进度、更新时间和任务状态。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能够成功进入工业软件基线检测任务列表页面，页面应完整显示以下字段信息：任务编号、任务名称、启动时间、扫描进度、更新时间和任务状态。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **92 工业软件脆弱性检测与防护模块的工业软件基线检测任务查询测试项**

|  |
| --- |
| **测试项目：**工业软件脆弱性检测与防护模块的工业软件基线检测任务查询测试 |
| **测试依据：** |
| **测试目的：**  此测试项旨在验证用户在工业软件脆弱性检测与防护模块中，对工业软件基线检测任务的查询功能是否完善。通过此测试项，可以确保用户能够根据自己的需求，快速准确地检索到相关的基线检测任务信息，从而有效支持安全检测工作的管理和决策。此测试项旨在验证用户在工业软件脆弱性检测与防护模块中，对工业软件基线检测任务的查询功能是否完善。通过此测试项，可以确保用户能够根据自己的需求，快速准确地检索到相关的基线检测任务信息，从而有效支持安全检测工作的管理和决策。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）登录系统并进入工业软件脆弱性检测与防护模块的工业软件基线检测任务管理页面；  2）在查询条件区域输入关键词（如任务名称、启动时间等）；  3）点击“查询”或“搜索”按钮；  4）系统根据条件返回匹配的任务列表，核查是否仅展示符合条件的任务；  5）确认列表显示字段包括任务编号、任务名称、启动时间、扫描进度、更新时间和任务状态。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能够根据用户设定的查询条件（如任务名称、启动时间范围等）准确筛选出对应的工业软件基线检测任务，并在列表中显示结果，字段包括任务编号、任务名称、启动时间、扫描进度、更新时间和任务状态。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **93 工业软件脆弱性检测与防护模块的工业软件基线检测任务创建测试项**

|  |
| --- |
| **测试项目：**工业软件脆弱性检测与防护模块的工业软件基线检测任务创建测试 |
| **测试依据：** |
| **测试目的：**  该测试项旨在验证在工业软件脆弱性检测与防护模块中，用户是否能够顺利创建工业软件基线检测任务，并确保任务创建过程的准确性和高效性。通过此测试项，可以评估系统对用户输入的响应速度、任务创建的稳定性以及系统资源的合理分配。该测试项旨在验证在工业软件脆弱性检测与防护模块中，用户是否能够顺利创建工业软件基线检测任务，并确保任务创建过程的准确性和高效性。通过此测试项，可以评估系统对用户输入的响应速度、任务创建的稳定性以及系统资源的合理分配。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）登录系统并进入工业软件脆弱性检测与防护模块的工业软件基线检测任务管理界面；  2）点击“新建任务”按钮，填写任务名称、检测目标、检测策略等必要信息；  3）点击“创建”或“提交”按钮；  4）确认系统提示“创建成功”；  5）返回任务列表页面，确认新建任务已出现在列表中，并包含正确的任务编号、任务名称、启动时间等信息。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能够成功创建一条新的工业软件基线检测任务，在用户提交任务后弹出“创建成功”的提示信息，并能在任务列表中显示该新建任务，包含任务编号、任务名称、启动时间、扫描进度、更新时间和任务状态等字段。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **94 工业软件脆弱性检测与防护模块的工业软件基线检测任务单条删除测试项**

|  |
| --- |
| **测试项目：**工业软件脆弱性检测与防护模块的工业软件基线检测任务单条删除测试 |
| **测试依据：** |
| **测试目的：**  在执行单条删除操作时，系统应确保数据的一致性和完整性。具体而言，除了验证删除操作的准确性和系统响应外，还需确认删除后的数据库记录是否同步更新，避免产生孤立数据或引发数据不一致的问题。在执行单条删除操作时，系统应确保数据的一致性和完整性。具体而言，除了验证删除操作的准确性和系统响应外，还需确认删除后的数据库记录是否同步更新，避免产生孤立数据或引发数据不一致的问题。 |
| **测试配置：** |
| **测试步骤：**  1）登录系统并进入工业软件脆弱性检测与防护模块的工业软件基线检测任务管理页面；  2）在任务列表中选中一条要删除的工业软件基线检测任务；  3）点击“删除”按钮，确认删除操作；  4）观察系统是否弹出“操作成功”的提示信息；  5）验证被删除任务是否从任务列表中移除。 |
| **预期结果：**  每一步骤都有正确结果。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **95 工业软件脆弱性检测与防护模块的工业软件基线检测任务批量删除测试项**

|  |
| --- |
| **测试项目：**工业软件脆弱性检测与防护模块的工业软件基线检测任务批量删除测试 |
| **测试依据：** |
| **测试目的：**  通过此测试项，将进一步验证系统对工业软件基线检测任务批量删除功能的稳定性和可靠性。在批量删除过程中，系统不仅要能够快速响应用户的操作请求，还需要确保删除操作的一致性，即所有被选中的任务都能被准确删除，且不会遗漏或误删其他未选中的任务。此外，批量删除操作完成后，系统应能够及时更新任务列表，确保显示的任务信息与实际数据库记录保持一致，从而避免数据不一致或孤立数据的问题。通过此测试项，将进一步验证系统对工业软件基线检测任务批量删除功能的稳定性和可靠性。在批量删除过程中，系统不仅要能够快速响应用户的操作请求，还需要确保删除操作的一致性，即所有被选中的任务都能被准确删除，且不会遗漏或误删其他未选中的任务。此外，批量删除操作完成后，系统应能够及时更新任务列表，确保显示的任务信息与实际数据库记录保持一致，从而避免数据不一致或孤立数据的问题。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）登录系统并进入工业软件脆弱性检测与防护模块的工业软件基线检测任务管理页面；  2）在任务列表中勾选多条需删除的工业软件基线检测任务；  3）点击“批量删除”按钮，确认删除操作；  4）观察系统是否弹出“操作成功”的提示信息；  5）验证所选任务是否全部从任务列表中移除。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能够成功批量删除用户所选择的多条工业软件基线检测任务，操作完成后弹出“操作成功”的提示信息，所选任务从任务列表中全部移除。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **96 工业软件脆弱性检测与防护模块的工业软件基线检测报告详情查看测试项**

|  |
| --- |
| **测试项目：**工业软件脆弱性检测与防护模块的工业软件基线检测报告详情查看测试 |
| **测试依据：** |
| **测试目的：**  该测试项旨在验证用户在工业软件脆弱性检测与防护模块中，能否顺利查看工业软件基线检测报告的详细信息。通过此测试项，可以确保系统提供的报告详情查看功能稳定可靠，用户能够轻松获取检测任务的关键数据和分析结果，这对于及时发现并应对潜在安全风险至关重要。该测试项旨在验证用户在工业软件脆弱性检测与防护模块中，能否顺利查看工业软件基线检测报告的详细信息。通过此测试项，可以确保系统提供的报告详情查看功能稳定可靠，用户能够轻松获取检测任务的关键数据和分析结果，这对于及时发现并应对潜在安全风险至关重要。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）登录系统并进入工业软件脆弱性检测与防护模块的工业软件基线检测任务列表页面；  2）选择一条已完成的基线检测任务，点击“查看报告”或“详情”按钮；  3）验证是否成功跳转到报告详情页面；  4）检查页面是否完整显示任务基础信息；  5）核实漏洞列表字段是否包括漏洞ID、漏洞名称、漏洞等级和漏洞描述。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能够成功进入查看工业软件基线检测报告详情页面，页面应显示完整的报告内容，包括任务基础信息和漏洞列表，漏洞列表中包含漏洞ID、漏洞名称、漏洞等级、漏洞描述等字段。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **97 工业软件脆弱性检测与防护模块的工控主机资产注册展示测试项**

|  |
| --- |
| **测试项目：**工业软件脆弱性检测与防护模块的工控主机资产注册展示测试 |
| **测试依据：** |
| **测试目的：**  该测试项旨在验证工控主机资产注册信息在工业软件脆弱性检测与防护模块中的展示功能是否准确和完善。通过此测试项，可以确保系统能够全面、清晰地展示已注册的工控主机资产信息，包括风险资产统计数据、漏洞统计数量、弱口令统计数据等关键指标，从而帮助用户更好地了解资产安全状况，及时采取必要的安全措施。该测试项旨在验证工控主机资产注册信息在工业软件脆弱性检测与防护模块中的展示功能是否准确和完善。通过此测试项，可以确保系统能够全面、清晰地展示已注册的工控主机资产信息，包括风险资产统计数据、漏洞统计数量、弱口令统计数据等关键指标，从而帮助用户更好地了解资产安全状况，及时采取必要的安全措施。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）登录系统并进入工业软件脆弱性检测与防护模块的工控主机资产管理页面；  2）查看已注册的工控主机资产信息列表；  3）核实列表中是否完整显示以下字段：资产IP、操作系统、主机名、主机启动时间、更新时间；  4）确认显示的数据准确、与实际注册信息一致。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能够成功展示已注册的工控主机资产信息，列表中包含并正确显示资产IP、操作系统、主机名、主机启动时间、更新时间等字段。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **98 工业软件脆弱性检测与防护模块的工控主机病毒检测任务创建测试项**

|  |
| --- |
| **测试项目：**工业软件脆弱性检测与防护模块的工控主机病毒检测任务创建测试 |
| **测试依据：** |
| **测试目的：**  该测试项旨在验证用户在工业软件脆弱性检测与防护模块中，是否能够顺利创建工控主机病毒检测任务，并确保任务创建过程的准确性和高效性。通过此测试项，可以评估系统对用户输入的响应速度、任务创建的稳定性以及系统资源的合理分配。该测试项旨在验证用户在工业软件脆弱性检测与防护模块中，是否能够顺利创建工控主机病毒检测任务，并确保任务创建过程的准确性和高效性。通过此测试项，可以评估系统对用户输入的响应速度、任务创建的稳定性以及系统资源的合理分配。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）登录系统并进入工业软件脆弱性检测与防护模块的工控主机病毒检测任务管理页面；  2）点击“新建任务”按钮，填写任务名称、目标主机、扫描方式等必要信息；  3）点击“发布”或“创建”按钮；  4）验证系统是否弹出“发布成功”的提示信息；  5）返回任务展示页面，确认新建任务显示在列表中，包含任务相关信息如任务名称、启动时间、扫描状态等。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能够成功创建一条新的工控主机病毒检测任务，任务提交后提示“发布成功”，新建任务能够在工控主机病毒检测任务展示页面中正确显示。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **99 工业软件脆弱性检测与防护模块的工控主机病毒检测任务查询测试项**

|  |
| --- |
| **测试项目：**工业软件脆弱性检测与防护模块的工控主机病毒检测任务查询测试 |
| **测试依据：** |
| **测试目的：**  该测试项旨在验证用户是否能够在工业软件脆弱性检测与防护模块中，通过查询功能准确检索到工控主机病毒检测任务的相关信息。通过此测试项，可以确保系统的查询功能稳定可靠，用户能够高效地从大量任务中筛选出符合特定条件的结果，这对于及时获取任务状态和进度、优化安全管理流程具有重要意义。该测试项旨在验证用户是否能够在工业软件脆弱性检测与防护模块中，通过查询功能准确检索到工控主机病毒检测任务的相关信息。通过此测试项，可以确保系统的查询功能稳定可靠，用户能够高效地从大量任务中筛选出符合特定条件的结果，这对于及时获取任务状态和进度、优化安全管理流程具有重要意义。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）登录系统并进入工业软件脆弱性检测与防护模块的工控主机病毒检测任务管理页面；  2）设置查询条件，如任务名称、状态或时间范围等，点击“查询”按钮；  3）观察任务列表是否刷新为符合查询条件的记录；  4）核对每条任务记录是否显示以下字段：任务类型、成功下发/终端总数、扫描完成数量、扫描终止终端数量、操作者名称、查杀状态和发现风险项数量；  5）检查数据准确性和显示完整性。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能够根据用户设定的筛选条件（如任务名称、时间范围、任务状态等）成功查询出符合条件的工控主机病毒检测任务，并展示任务详细信息：任务类型、成功下发/终端总数、扫描完成数量、扫描终止终端数量、操作者名称、查杀状态和发现风险项数量。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **100 工业软件脆弱性检测与防护模块的工控主机病毒检测任务详情查看测试项**

|  |
| --- |
| **测试项目：**工业软件脆弱性检测与防护模块的工控主机病毒检测任务详情查看测试 |
| **测试依据：** |
| **测试目的：**  该测试项主要验证用户在工业软件脆弱性检测与防护模块中，能否顺利查看工控主机病毒检测任务的详细信息。通过此测试项，可以确保系统提供的任务详情查看功能稳定可靠，用户能够轻松获取任务的关键数据和分析结果，这对于及时了解任务状态和进度、优化病毒检测策略至关重要。该测试项主要验证用户在工业软件脆弱性检测与防护模块中，能否顺利查看工控主机病毒检测任务的详细信息。通过此测试项，可以确保系统提供的任务详情查看功能稳定可靠，用户能够轻松获取任务的关键数据和分析结果，这对于及时了解任务状态和进度、优化病毒检测策略至关重要。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）登录系统并进入工业软件脆弱性检测与防护模块的工控主机病毒检测任务管理页面；  2）选择一条目标任务，点击“查看”或“详情”按钮；  3）验证是否成功跳转至病毒检测任务详情页面；  4）检查页面是否显示任务详情、IP、下发状态、扫描状态等信息；  5）核实病毒详情列表字段是否完整显示发现时间、资产IP、感染文件、感染病毒及处理状态。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能够成功进入工控主机病毒检测任务详情页面，页面应显示完整的任务详情信息，包括任务基本信息、IP列表、下发状态、扫描状态及病毒详情列表。病毒详情列表应包含发现时间、资产IP、感染文件、感染病毒名称和处理状态等字段。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **101 工业软件脆弱性检测与防护模块的工控主机病毒删除测试项**

|  |
| --- |
| **测试项目：**工业软件脆弱性检测与防护模块的工控主机病毒删除测试 |
| **测试依据：** |
| **测试目的：**  该测试项旨在验证用户在工业软件脆弱性检测与防护模块中，是否能够成功删除工控主机上的病毒。通过此测试项，可以确保系统提供的病毒删除功能稳定可靠，用户能够高效地从受感染的主机中清除病毒，从而维护系统的安全性和稳定性。该测试项旨在验证用户在工业软件脆弱性检测与防护模块中，是否能够成功删除工控主机上的病毒。通过此测试项，可以确保系统提供的病毒删除功能稳定可靠，用户能够高效地从受感染的主机中清除病毒，从而维护系统的安全性和稳定性。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）登录系统并进入工业软件脆弱性检测与防护模块的工控主机病毒检测任务详情页面；  2）在病毒详情列表中选择一条或多条病毒文件记录；  3）点击“删除”按钮，确认删除操作；  4）观察系统是否更新处理状态为“已删除”；  5）验证病毒文件是否从活跃威胁列表中移除或状态正确反映删除结果。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统能够成功删除用户选择的工控主机中发现的病毒文件，删除操作完成后，病毒文件的处理状态应更新为“已删除”。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **102 对型号为DS-2CD4012F-SDI的工业相机进行工业终端协议安全检测测试项**

|  |
| --- |
| **测试项目：**对型号为DS-2CD4012F-SDI的工业相机进行工业终端协议安全检测测试 |
| **测试依据：** |
| **测试目的：**  该测试项主要评估型号为DS-2CD4012F-SDI的工业相机在安全性方面的表现。通过对其进行全面的工业终端协议安全检测，旨在发现潜在的安全威胁。该测试项主要评估型号为DS-2CD4012F-SDI的工业相机在安全性方面的表现。通过对其进行全面的工业终端协议安全检测，旨在发现潜在的安全威胁。 |
| **测试配置：** |
| **测试步骤：**  可以成功创建型号为DS-2CD4012F-SDI的工业相机的工业终端协议安全检测任务，测试终端IP为10.19.199.230，完成扫描，并可查看工业终端协议安全检测报告  测试方法：  1.准备环境：配置型号为DS-2CD4012F-SDI的工业相机及自研平台。  2.创建检测任务：发起针对型号为DS-2CD4012F-SDI的工业相机的工业终端协议安全扫描任务。  3.执行扫描：监控任务完成，确保覆盖所有组件。  4.查看报告：验证工业软件协议安全检测报告的完整性与风险详情。 |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **103 对ToolsTalk MT（阿特拉斯打钉机软件）进行病毒木马检测测试项**

|  |
| --- |
| **测试项目：**对ToolsTalk MT（阿特拉斯打钉机软件）进行病毒木马检测测试项 |
| **测试依据：** |
| **测试目的：**  该测试项主要评估ToolsTalk MT（阿特拉斯打钉机软件）在安全性方面的表现。通过对其进行全面的安全检测，旨在发现潜在的风险点，为后续的安全防护和加固工作提供重要依据。通过此测试项，可以确保阿特拉斯打钉机软件的安全性能符合相关标准和要求。该测试项主要评估ToolsTalk MT（阿特拉斯打钉机软件）在安全性方面的表现。通过对其进行全面的安全检测，旨在发现潜在的风险点，为后续的安全防护和加固工作提供重要依据。通过此测试项，可以确保阿特拉斯打钉机软件的安全性能符合相关标准和要求。 |
| **测试配置：** |
| **测试步骤：**  系统可以成功创建对ToolsTalk MT（阿特拉斯打钉机软件）的病毒木马安全检测任务，完成扫描，并可查看病毒木马安全检测报告。  测试方法：  1.准备环境：配置ToolsTalk MT（阿特拉斯打钉机软件）系统及自研平台。  2.创建检测任务：发起针对ToolsTalk MT（阿特拉斯打钉机软件）的病毒木马安全检测任务。  3.执行扫描：监控任务完成，确保覆盖所有组件。  4.查看报告：验证病毒木马安全检测报告的完整性与风险详情。 |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **104对STEP 7-MicroWIN V40（西门子200 PLC)软件进行病毒木马检测测试项**

|  |
| --- |
| **测试项目：**对STEP 7-MicroWIN V40（西门子200 PLC)软件进行病毒木马检测测试项 |
| **测试依据：** |
| **测试目的：**  该测试项旨在评估STEP 7-MicroWIN V40（西门子200 PLC）软件在安全性方面的表现。通过对其进行详尽的安全检测，旨在揭示潜在的风险点，为后续的安全防护措施和加固工作奠定坚实基础。通过此测试项，可以确保西门子200 PLC软件的安全性能满足相关标准和规范。该测试项旨在评估STEP 7-MicroWIN V40（西门子200 PLC）软件在安全性方面的表现。通过对其进行详尽的安全检测，旨在揭示潜在的风险点，为后续的安全防护措施和加固工作奠定坚实基础。通过此测试项，可以确保西门子200 PLC软件的安全性能满足相关标准和规范。 |
| **测试配置：** |
| **测试步骤：**  系统可以成功创建对STEP 7-MicroWIN V40（西门子200 PLC)软件的病毒木马安全检测任务，完成扫描，并可查看病毒木马安全检测报告。  测试方法：  1.准备环境：配置XC系列编程工具(信捷PLC）软件及自研平台。  2.创建检测任务：发起针对XC系列编程工具(信捷PLC）软件的病毒木马安全检测任务。  3.执行扫描：监控任务完成，确保覆盖所有组件。  4.查看报告：验证病毒木马安全检测报告的完整性与风险详情。 |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **105对WinCC Pro (西门1200PLC）软件进行病毒木马检测测试项**

|  |
| --- |
| **测试项目：**对WinCC Pro (西门1200PLC）软件进行病毒木马检测测试项 |
| **测试依据：** |
| **测试目的：**  该测试项主要评估WinCC Pro (西门1200PLC）软件在安全性方面的性能。通过对其进行全面的安全检测，旨在识别潜在的风险点，为后续的安全防护和加固措施提供关键依据。通过此测试项，可以确保WinCC Pro (西门1200PLC）软件的安全性能符合相关标准和要求。该测试项主要评估WinCC Pro (西门1200PLC）软件在安全性方面的性能。通过对其进行全面的安全检测，旨在识别潜在的风险点，为后续的安全防护和加固措施提供关键依据。通过此测试项，可以确保WinCC Pro (西门1200PLC）软件的安全性能符合相关标准和要求。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1.准备环境：配置WinCC Pro (西门1200PLC）软件及自研平台。  2.创建检测任务：发起针对WinCC Pro (西门1200PLC）软件的病毒木马安全检测任务。  3.执行扫描：监控任务完成，确保覆盖所有组件。  4.查看报告：验证病毒木马安全检测报告的完整性与风险详情。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统可以成功创建对WinCC Pro (西门1200PLC）软件的病毒木马安全检测任务，完成扫描，并可查看病毒木马安全检测报告。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **106对XC系列编程工具(信捷PLC）软件进行病毒木马检测测试项**

|  |
| --- |
| **测试项目：**对XC系列编程工具(信捷PLC）软件进行病毒木马检测测试 |
| **测试依据：** |
| **测试目的：**  该测试项主要评估XC系列编程工具(信捷PLC）软件在安全性方面的表现。通过对其进行全面的安全检测，旨在识别并修复潜在的风险点，以确保软件的安全性能符合相关标准和要求。此测试项对于维护工业控制系统的整体安全性和稳定性至关重要。该测试项主要评估XC系列编程工具(信捷PLC）软件在安全性方面的表现。通过对其进行全面的安全检测，旨在识别并修复潜在的风险点，以确保软件的安全性能符合相关标准和要求。此测试项对于维护工业控制系统的整体安全性和稳定性至关重要。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1.准备环境：配置XC系列编程工具(信捷PLC）软件及自研平台。  2.创建检测任务：发起针对XC系列编程工具(信捷PLC）软件的病毒木马安全检测任务。  3.执行扫描：监控任务完成，确保覆盖所有组件。  4.查看报告：验证病毒木马安全检测报告的完整性与风险详情。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统可以成功创建对XC系列编程工具(信捷PLC）软件的病毒木马安全检测任务，完成扫描，并可查看病毒木马安全检测报告。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **107对S7-PLCSIM V16(西门1200PLC）软件进行病毒木马检测测试项**

|  |
| --- |
| **测试项目：**对S7-PLCSIM V16(西门1200PLC）软件进行病毒木马检测 |
| **测试依据：** |
| **测试目的：**  该测试项着重评估S7-PLCSIM V16(西门1200PLC）软件在安全性层面的性能。通过对其执行全面的安全检测，目标在于发现并修补可能存在的风险点，从而确保该软件的安全性能达到相关标准和要求。此测试项对于保障工业控制系统的整体安全性与稳定性具有重要意义该测试项着重评估S7-PLCSIM V16(西门1200PLC）软件在安全性层面的性能。通过对其执行全面的安全检测，目标在于发现并修补可能存在的风险点，从而确保该软件的安全性能达到相关标准和要求。此测试项对于保障工业控制系统的整体安全性与稳定性具有重要意义 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1.准备环境：配置S7-PLCSIM V16(西门1200PLC）软件及自研平台。  2.创建检测任务：发起针对S7-PLCSIM V16(西门1200PLC）软件的病毒木马安全检测任务。  3.执行扫描：监控任务完成，确保覆盖所有组件。  4.查看报告：验证病毒木马安全检测报告的完整性与风险详情。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统可以成功创建对S7-PLCSIM V16(西门1200PLC）软件的病毒木马安全检测任务，完成扫描，并可查看病毒木马安全检测报告。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **108对V-ASSISTANT(西门1200PLC）软件进行病毒木马检测测试项**

|  |
| --- |
| **测试项目：**对V-ASSISTANT(西门1200PLC）软件进行病毒木马检测 |
| **测试依据：** |
| **测试目的：**  该测试项着重评估V-ASSISTANT(西门1200PLC）软件在安全性方面的性能。通过对其进行详尽的安全检测，旨在识别并修复可能存在的风险点，以确保该软件的安全性能满足相关标准和规范。此测试项对于保障工业控制系统的整体安全性和稳定性具有关键作用。该测试项着重评估V-ASSISTANT(西门1200PLC）软件在安全性方面的性能。通过对其进行详尽的安全检测，旨在识别并修复可能存在的风险点，以确保该软件的安全性能满足相关标准和规范。此测试项对于保障工业控制系统的整体安全性和稳定性具有关键作用。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1.准备环境：配置V-ASSISTANT(西门1200PLC）软件及自研平台。  2.创建检测任务：发起针对V-ASSISTANT(西门1200PLC）软件的病毒木马安全检测任务。  3.执行扫描：监控任务完成，确保覆盖所有组件。  4.查看报告：验证病毒木马安全检测报告的完整性与风险详情。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统可以成功创建对V-ASSISTANT(西门1200PLC）软件的病毒木马安全检测任务，完成扫描，并可查看病毒木马安全检测报告。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **109对CX-Programmer（欧姆龙PLC）进行病毒木马检测测试项**

|  |
| --- |
| **测试项目：**对CX-Programmer（欧姆龙PLC）进行病毒木马检测 |
| **测试依据：** |
| **测试目的：**  该测试项主要评估CX-Programmer（欧姆龙PLC）软件在安全性方面的性能。通过对其进行全面的安全检测，旨在发现潜在的安全漏洞和风险点，为后续的安全防护和加固工作提供重要依据。通过此测试项，可以确保欧姆龙PLC软件的安全性能符合相关标准和要求，从而降低因软件漏洞而引发的安全风险。此测试项对于维护工业控制系统的整体安全性和稳定性具有重要意义。该测试项主要评估CX-Programmer（欧姆龙PLC）软件在安全性方面的性能。通过对其进行全面的安全检测，旨在发现潜在的安全漏洞和风险点，为后续的安全防护和加固工作提供重要依据。通过此测试项，可以确保欧姆龙PLC软件的安全性能符合相关标准和要求，从而降低因软件漏洞而引发的安全风险。此测试项对于维护工业控制系统的整体安全性和稳定性具有重要意义。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1.准备环境：配置V-ASSISTANT(西门1200PLC）软件及自研平台。  2.创建检测任务：发起针对V-ASSISTANT(西门1200PLC）软件的病毒木马安全检测任务。  3.执行扫描：监控任务完成，确保覆盖所有组件。  4.查看报告：验证病毒木马安全检测报告的完整性与风险详情。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统可以成功创建对CX-Programmer（欧姆龙PLC）软件的病毒木马安全检测任务，完成扫描，并可查看病毒木马安全检测报告。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **110对PANATERM Ver.6.0（松下伺服软件）进行病毒木马检测测试项**

|  |
| --- |
| **测试项目：**对PANATERM Ver.6.0（松下伺服软件）进行病毒木马检测 |
| **测试依据：** |
| **测试目的：**  该测试项旨在全面评估PANATERM Ver.6.0（松下伺服软件）在安全性方面的表现。通过对其进行深入的安全检测，目标是揭示并修复可能存在的风险点，以确保该软件的安全性能符合相关标准和规范。此测试项对于维护工业控制系统的整体安全性和可靠性至关重要。该测试项旨在全面评估PANATERM Ver.6.0（松下伺服软件）在安全性方面的表现。通过对其进行深入的安全检测，目标是揭示并修复可能存在的风险点，以确保该软件的安全性能符合相关标准和规范。此测试项对于维护工业控制系统的整体安全性和可靠性至关重要。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1.准备环境：配置V-ASSISTANT(西门1200PLC）软件及自研平台。  2.创建检测任务：发起针对V-ASSISTANT(西门1200PLC）软件的病毒木马安全检测任务。  3.执行扫描：监控任务完成，确保覆盖所有组件。  4.查看报告：验证病毒木马安全检测报告的完整性与风险详情。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统可以成功创建对PANATERM Ver.6.0（松下伺服软件）的病毒木马安全检测任务，完成扫描，并可查看病毒木马安全检测报告。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **111对Utility Manager（威纶通触摸屏软件）进行病毒木马检测测试项**

|  |
| --- |
| **测试项目：**对Utility Manager（威纶通触摸屏软件）进行病毒木马检测 |
| **测试依据：** |
| **测试目的：**  该测试项专注于评估Utility Manager（威纶通触摸屏软件）在安全性层面的表现。通过对其进行严谨的安全检测，旨在发现并解决潜在的风险点，以确保该软件的安全性能达到相关标准和要求。通过此测试项，可以进一步确保威纶通触摸屏软件的安全性能符合行业标准，为工业控制系统的稳定运行提供有力支持。该测试项专注于评估Utility Manager（威纶通触摸屏软件）在安全性层面的表现。通过对其进行严谨的安全检测，旨在发现并解决潜在的风险点，以确保该软件的安全性能达到相关标准和要求。通过此测试项，可以进一步确保威纶通触摸屏软件的安全性能符合行业标准，为工业控制系统的稳定运行提供有力支持。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1.准备环境：配置Utility Manager（威纶通触摸屏软件）及自研平台。  2.创建检测任务：发起针对Utility Manager（威纶通触摸屏软件）的病毒木马安全检测任务。  3.执行扫描：监控任务完成，确保覆盖所有组件。  4.查看报告：验证病毒木马安全检测报告的完整性与风险详情。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统可以成功创建对Utility Manager（威纶通触摸屏软件）的病毒木马安全检测任务，完成扫描，并可查看病毒木马安全检测报告。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **112对威纶通EasyBuilder8000进行工业软件漏洞检测测试项**

|  |
| --- |
| **测试项目：**对威纶通EasyBuilder8000进行工业软件漏洞检测 |
| **测试依据：** |
| **测试目的：**  该测试项专注于评估威纶通EasyBuilder8000软件在安全性方面的性能。通过对其进行全面的安全检测，旨在识别并修复可能存在的风险点，以确保该软件的安全性能符合相关标准和规范。通过此测试项，可以进一步确保威纶通EasyBuilder8000软件的安全性能达到行业要求，为工业控制系统的安全运行提供坚实保障。该测试项专注于评估威纶通EasyBuilder8000软件在安全性方面的性能。通过对其进行全面的安全检测，旨在识别并修复可能存在的风险点，以确保该软件的安全性能符合相关标准和规范。通过此测试项，可以进一步确保威纶通EasyBuilder8000软件的安全性能达到行业要求，为工业控制系统的安全运行提供坚实保障。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1.准备环境：配置威纶通EasyBuilder8000软件及自研平台。  2.创建检测任务：发起针对威纶通EasyBuilder8000软件的工业软件漏洞检测任务。  3.执行扫描：监控任务完成，确保覆盖所有组件。  4.查看报告：验证漏洞安全检测报告的完整性与风险详情。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统可以成功创建对威纶通EasyBuilder8000的工业软件漏洞检测任务，完成扫描，并可查看漏洞检测报告。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **113对MVCC(AGV视觉标定)软件进行病毒木马检测测试项**

|  |
| --- |
| **测试项目：**对MVCC(AGV视觉标定)软件进行病毒木马检测 |
| **测试依据：** |
| **测试目的：**  该测试项着重评估MVCC(AGV视觉标定)软件在安全性层面的表现。通过对其进行详尽的安全检测，旨在识别并修复潜在的风险点，以确保该软件的安全性能满足相关标准和规范。通过此测试项，可以进一步确保MVCC(AGV视觉标定)软件的安全性能达到行业要求，为工业AGV系统的安全运行提供有力支持。该测试项着重评估MVCC(AGV视觉标定)软件在安全性层面的表现。通过对其进行详尽的安全检测，旨在识别并修复潜在的风险点，以确保该软件的安全性能满足相关标准和规范。通过此测试项，可以进一步确保MVCC(AGV视觉标定)软件的安全性能达到行业要求，为工业AGV系统的安全运行提供有力支持。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1.准备环境：配置MVCC(AGV视觉标定)软件及自研平台。  2.创建检测任务：发起针对MVCC(AGV视觉标定)软件的病毒木马安全检测任务。  3.执行扫描：监控任务完成，确保覆盖所有组件。  4.查看报告：验证病毒木马安全检测报告的完整性与风险详情。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统可以成功创建对MVCC(AGV视觉标定)软件的病毒木马安全检测任务，完成扫描，并可查看病毒木马安全检测报告。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **114对VisionMaster--控制标定的机械臂控制软件进行病毒木马检测测试项**

|  |
| --- |
| **测试项目：**对VisionMaster--控制标定的机械臂控制软件进行病毒木马检测 |
| **测试依据：** |
| **测试目的：**  该测试项专注于评估VisionMaster——控制标定的机械臂控制软件在安全性方面的性能。通过对其进行全面的安全检测，旨在发现并修复可能存在的风险点，以确保该软件的安全性能符合相关标准和规范。此测试项对于保障机械臂控制系统的整体安全性和稳定性具有重要意义。该测试项专注于评估VisionMaster——控制标定的机械臂控制软件在安全性方面的性能。通过对其进行全面的安全检测，旨在发现并修复可能存在的风险点，以确保该软件的安全性能符合相关标准和规范。此测试项对于保障机械臂控制系统的整体安全性和稳定性具有重要意义。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1.准备环境：配置VisionMaster--控制标定的机械臂控制软件及自研平台。  2.创建检测任务：发起针对VisionMaster--控制标定的机械臂控制软件的病毒木马安全检测任务。  3.执行扫描：监控任务完成，确保覆盖所有组件。  4.查看报告：验证病毒木马安全检测报告的完整性与风险详情。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统可以成功创建对VisionMaster--控制标定的机械臂控制软件的病毒木马安全检测任务，完成扫描，并可查看病毒木马安全检测报告。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **115对AGVMonitorClient\_CN\_STD- AGV控制软件进行病毒木马检测测试项**

|  |
| --- |
| **测试项目：**对AGVMonitorClient\_CN\_STD- AGV控制软件进行病毒木马检测 |
| **测试依据：** |
| **测试目的：**  该测试项旨在全面评估AGVMonitorClient\_CN\_STD- AGV控制软件在安全性方面的性能。通过对其进行深入的安全检测，目标是揭示并修复可能存在的风险点，以确保该软件的安全性能满足相关标准和规范。此测试项对于维护AGV系统的整体安全性和稳定性至关重要。该测试项旨在全面评估AGVMonitorClient\_CN\_STD- AGV控制软件在安全性方面的性能。通过对其进行深入的安全检测，目标是揭示并修复可能存在的风险点，以确保该软件的安全性能满足相关标准和规范。此测试项对于维护AGV系统的整体安全性和稳定性至关重要。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1.准备环境：配置AGVMonitorClient\_CN\_STD- AGV控制软件及自研平台。  2.创建检测任务：发起针对AGVMonitorClient\_CN\_STD- AGV控制软件的病毒木马安全检测任务。  3.执行扫描：监控任务完成，确保覆盖所有组件。  4.查看报告：验证病毒木马安全检测报告的完整性与风险详情。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统可以成功创建对AGVMonitorClient\_CN\_STD-AGV控制软件的病毒木马安全检测任务，完成扫描，并可查看病毒木马安全检测报告。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **116对博途V16进行病毒木马检测测试项**

|  |
| --- |
| **测试项目：**对博途V16进行病毒木马检测 |
| **测试依据：** |
| **测试目的：**  该测试项主要评估博途V16软件在安全性方面的综合性能。通过对其进行全面的安全检测，旨在深入发现和修复可能存在的风险点，以确保该软件的安全性能符合相关标准和要求。通过此测试项的实施，可以进一步确保博途V16软件的安全性能达到行业领先水平，为工业自动化生产的可靠运行提供坚实保障。该测试项主要评估博途V16软件在安全性方面的综合性能。通过对其进行全面的安全检测，旨在深入发现和修复可能存在的风险点，以确保该软件的安全性能符合相关标准和要求。通过此测试项的实施，可以进一步确保博途V16软件的安全性能达到行业领先水平，为工业自动化生产的可靠运行提供坚实保障。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1.准备环境：配置博途V16软件及自研平台。  2.创建检测任务：发起针对博途V16软件的病毒木马安全检测任务。  3.执行扫描：监控任务完成，确保覆盖所有组件。  4.查看报告：验证病毒木马安全检测报告的完整性与风险详情。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统可以成功创建对博途V16软件的漏洞安全检测任务，完成扫描，并可查看病毒木马安全检测报告。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **117对EPSON RC+7.0-机械手单机软件进行病毒木马检测测试项**

|  |
| --- |
| **测试项目：**对EPSON RC+7.0-机械手单机软件进行病毒木马检测 |
| **测试依据：** |
| **测试目的：**  该测试项主要关注EPSON RC+7.0-机械手单机软件在安全性上的综合表现。通过对其进行详细的安全检测，旨在发现和解决可能存在的风险点，以确保该软件的安全性能满足相关标准和规范。该测试项主要关注EPSON RC+7.0-机械手单机软件在安全性上的综合表现。通过对其进行详细的安全检测，旨在发现和解决可能存在的风险点，以确保该软件的安全性能满足相关标准和规范。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1.准备环境：配置EPSON RC+7.0-机械手单机软件及自研平台。  2.创建检测任务：发起针对EPSON RC+7.0-机械手单机软件的病毒木马安全检测任务。  3.执行扫描：监控任务完成，确保覆盖所有组件。  4.查看报告：验证病毒木马安全检测报告的完整性与风险详情。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统可以成功创建对EPSON RC+7.0-机械手单机软件的病毒木马安全检测任务，完成扫描，并可查看病毒木马安全检测报告。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **118对EPSON RC Express-机械手单机软件进行病毒木马检测测试项**

|  |
| --- |
| **测试项目：**对EPSON RC Express-机械手单机软件进行病毒木马检测 |
| **测试依据：** |
| **测试目的：**  对EPSON RC Express-机械手单机软件进行安全检测。此测试项着重评估EPSON RC Express-机械手单机软件在安全性层面的综合性能。通过对其进行全面的安全检测，旨在识别并修复潜在的风险点，以确保该软件的安全性能符合相关标准和规范。对EPSON RC Express-机械手单机软件进行安全检测。此测试项着重评估EPSON RC Express-机械手单机软件在安全性层面的综合性能。通过对其进行全面的安全检测，旨在识别并修复潜在的风险点，以确保该软件的安全性能符合相关标准和规范。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1.准备环境：配置EPSON RC Express-机械手单机软件及自研平台。  2.创建检测任务：发起针对EPSON RC Express-机械手单机软件的病毒木马安全检测任务。  3.执行扫描：监控任务完成，确保覆盖所有组件。  4.查看报告：验证病毒木马安全检测报告的完整性与风险详情。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统可以成功创建对EPSON RC Express-机械手单机软件的病毒木马安全检测任务，完成扫描，并可查看病毒木马安全检测报告。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **119对HIK-TStand-燃气产品测试软件进行病毒木马检测测试项**

|  |
| --- |
| **测试项目：**对HIK-TStand-燃气产品测试软件进行病毒木马检测 |
| **测试依据：** |
| **测试目的：**  该测试项主要关注HIK-TStand-燃气产品测试软件在安全性方面的综合性能。通过对其进行全面的安全检测，旨在深入揭示并修复可能存在的风险点，以确保该软件的安全性能达到相关标准和规范。该测试项主要关注HIK-TStand-燃气产品测试软件在安全性方面的综合性能。通过对其进行全面的安全检测，旨在深入揭示并修复可能存在的风险点，以确保该软件的安全性能达到相关标准和规范。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1.准备环境：配置HIK-TStand-燃气产品测试软件及自研平台。  2.创建检测任务：发起针对HIK-TStand-燃气产品测试软件的病毒木马安全检测任务。  3.执行扫描：监控任务完成，确保覆盖所有组件。  4.查看报告：验证病毒木马安全检测报告的完整性与风险详情。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统可以成功创建对HIK-TStand-燃气产品测试软件的病毒木马安全检测任务，完成扫描，并可查看病毒木马安全检测报告。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **120对MES系统软件（messtart-MES）进行病毒木马检测测试项**

|  |
| --- |
| **测试项目：**对MES系统软件（messtart-MES）进行病毒木马检测 |
| **测试依据：** |
| **测试目的：**  该测试项致力于全面评估MES系统软件（messtart-MES）在安全性方面的综合性能。通过对其进行深入的安全检测，旨在发现并修复可能存在的风险点，以确保该软件的安全性能符合相关标准和规范。该测试项致力于全面评估MES系统软件（messtart-MES）在安全性方面的综合性能。通过对其进行深入的安全检测，旨在发现并修复可能存在的风险点，以确保该软件的安全性能符合相关标准和规范。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1.准备环境：配置MES系统软件（messtart-MES）及自研平台。  2.创建检测任务：发起针对MES系统软件（messtart-MES）软件的病毒木马安全检测任务。  3.执行扫描：监控任务完成，确保覆盖所有组件。  4.查看报告：验证病毒木马安全检测报告的完整性与风险详情。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统可以成功创建对MES系统软件（MESSTART）的病毒木马安全检测任务，完成扫描，并可查看病毒木马安全检测报告。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **121对mpm-client-pro-MPM数字化工艺管理平台进行病毒木马检测测试项**

|  |
| --- |
| **测试项目：**对mpm-client-pro-MPM数字化工艺管理平台进行病毒木马检测 |
| **测试依据：** |
| **测试目的：**  该测试项专注于评估mpm-client-pro-MPM数字化工艺管理平台在安全性层面的综合性能。通过对其进行全面的安全检测，旨在揭示并修复潜在的风险点，以确保该平台的安全性能符合相关标准和规范。该测试项专注于评估mpm-client-pro-MPM数字化工艺管理平台在安全性层面的综合性能。通过对其进行全面的安全检测，旨在揭示并修复潜在的风险点，以确保该平台的安全性能符合相关标准和规范。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1.准备环境：配置mpm-client-pro-MPM数字化工艺管理平台及自研平台。  2.创建检测任务：发起针对mpm-client-pro-MPM数字化工艺管理平台的病毒木马安全检测任务。  3.执行扫描：监控任务完成，确保覆盖所有组件。  4.查看报告：验证病毒木马安全检测报告的完整性与风险详情。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统可以成功创建对mpm-client-pro-MPM数字化工艺管理平台的病毒木马安全检测任务，完成扫描，并可查看病毒木马安全检测报告。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **122对工装查询软件进行病毒木马检测测试项**

|  |
| --- |
| **测试项目：**对工装查询软件进行病毒木马检测 |
| **测试依据：** |
| **测试目的：**  该测试项主要评估工装查询软件在安全性方面的表现。通过对其进行全面的安全检测，旨在发现和解决可能存在的风险点，以确保该软件的安全性能满足相关标准和规范。该测试项主要评估工装查询软件在安全性方面的表现。通过对其进行全面的安全检测，旨在发现和解决可能存在的风险点，以确保该软件的安全性能满足相关标准和规范。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1.准备环境：配置工装查询软件及自研平台。  2.创建检测任务：发起针对工装查询软件的病毒木马安全检测任务。  3.执行扫描：监控任务完成，确保覆盖所有组件。  4.查看报告：验证病毒木马安全检测报告的完整性与风险详情。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统可以成功创建对工装查询软件的病毒木马安全检测任务，完成扫描，并可查看病毒木马安全检测报告。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **123对ResolutionDetection新版多目标定工具软件进行病毒木马检测测试项**

|  |
| --- |
| **测试项目：**对ResolutionDetection新版多目标定工具软件进行病毒木马安全检测 |
| **测试依据：** |
| **测试目的：**  该测试项旨在全面评估ResolutionDetection新版多目标定工具软件在安全性方面的性能。通过对其进行深入的安全检测，目标是揭示并修复可能存在的风险点，以确保该软件的安全性能符合相关标准和规范。该测试项旨在全面评估ResolutionDetection新版多目标定工具软件在安全性方面的性能。通过对其进行深入的安全检测，目标是揭示并修复可能存在的风险点，以确保该软件的安全性能符合相关标准和规范。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1.准备环境：配置ResolutionDetection新版多目标定工具软件及自研平台。  2.创建检测任务：发起针对ResolutionDetection新版多目标定工具软件的病毒木马安全检测任务。  3.执行扫描：监控任务完成，确保覆盖所有组件。  4.查看报告：验证病毒木马安全检测报告的完整性与风险详情。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统可以成功创建对ResolutionDetection新版多目标定工具软件的病毒木马安全检测任务，完成扫描，并可查看病毒木马安全检测报告。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **124对转盘高清调试-自动化网络测试软件进行病毒木马检测测试项**

|  |
| --- |
| **测试项目：**对转盘高清调试-自动化网络测试软件进行病毒木马检测 |
| **测试依据：** |
| **测试目的：**  该测试项专注于转盘高清调试-自动化网络测试软件在安全性上的综合性能评估。通过对其进行详尽的安全检测，旨在发现和解决潜在的风险点，以确保该软件的安全性能达到相关标准和规范。该测试项专注于转盘高清调试-自动化网络测试软件在安全性上的综合性能评估。通过对其进行详尽的安全检测，旨在发现和解决潜在的风险点，以确保该软件的安全性能达到相关标准和规范。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1.准备环境：配置转盘高清调试-自动化网络测试软件及自研平台。  2.创建检测任务：发起针对转盘高清调试-自动化网络测试软件的病毒木马安全检测任务。  3.执行扫描：监控任务完成，确保覆盖所有组件。  4.查看报告：验证病毒木马安全检测报告的完整性与风险详情。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统可以成功创建对转盘高清调试-自动化网络测试软件的病毒木马安全检测任务，完成扫描，并可查看病毒木马安全检测报告。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **125对筒机45气密测试-气密测试专用软件进行病毒木马检测测试项**

|  |
| --- |
| **测试项目：**对筒机45气密测试-气密测试专用软件进行病毒木马安全检测 |
| **测试依据：** |
| **测试目的：**  该测试项主要关注筒机45气密测试-气密测试专用软件在安全性方面的综合性能。通过对其进行全面的安全检测，旨在深入揭示并修复可能存在的风险点，以确保该软件的安全性能满足相关标准和规范。该测试项主要关注筒机45气密测试-气密测试专用软件在安全性方面的综合性能。通过对其进行全面的安全检测，旨在深入揭示并修复可能存在的风险点，以确保该软件的安全性能满足相关标准和规范。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1.准备环境：配置对筒机45气密测试-气密测试专用软件及自研平台。  2.创建检测任务：发起针对对筒机45气密测试-气密测试专用软件的病毒木马安全检测任务。  3.执行扫描：监控任务完成，确保覆盖所有组件。  4.查看报告：验证病毒木马安全检测报告的完整性与风险详情。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统可以成功创建对筒机45气密测试-气密测试专用软件的病毒木马安全检测任务，完成扫描，并可查看病毒木马安全检测报告。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **126对MVS-工厂标定软件进行病毒木马检测测试项**

|  |
| --- |
| **测试项目：**对MVS-工厂标定软件进行病毒木马检测 |
| **测试依据：** |
| **测试目的：**  该测试项着重评估MVS-工厂标定软件在安全性方面的综合性能。通过对其进行深入且全面的安全检测，目标是发现和解决可能隐藏的风险点，以确保该软件的安全性能完全符合相关标准和规范，从而为用户提供更加安全可靠的软件环境。该测试项着重评估MVS-工厂标定软件在安全性方面的综合性能。通过对其进行深入且全面的安全检测，目标是发现和解决可能隐藏的风险点，以确保该软件的安全性能完全符合相关标准和规范，从而为用户提供更加安全可靠的软件环境。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1.准备环境：配置MVS-工厂标定软件及自研平台。  2.创建检测任务：发起针对MVS-工厂标定软件的病毒木马安全检测任务。  3.执行扫描：监控任务完成，确保覆盖所有组件。  4.查看报告：验证病毒木马安全检测报告的完整性与风险详情。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统可以成功创建对MVS-工厂标定软件的病毒木马安全检测任务，完成扫描，并可查看病毒木马安全检测报告。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **127对型号为DS-B81-HR0804的工业网关进行工业软件基线检测测试项**

|  |
| --- |
| **测试项目：**对型号为DS-B81-HR0804的工业网关进行工业软件基线检测 |
| **测试依据：** |
| **测试目的：**  该测试项致力于全面评估型号为DS-B81-HR0804的工业网关在安全性方面的综合性能。通过对其进行详尽的安全检测，旨在深入揭示并修复可能存在的风险点，以确保该工业网关的安全性能符合相关标准和规范，进而保障工业控制系统的整体安全性。该测试项致力于全面评估型号为DS-B81-HR0804的工业网关在安全性方面的综合性能。通过对其进行详尽的安全检测，旨在深入揭示并修复可能存在的风险点，以确保该工业网关的安全性能符合相关标准和规范，进而保障工业控制系统的整体安全性。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1.准备环境：配置型号为DS-B81-HR0804的工业网关及自研平台。  2.创建检测任务：发起针对型号为DS-B81-HR0804的工业网关的工业软件基线检测任务。  3.执行扫描：监控任务完成，确保覆盖所有组件。  4.查看报告：验证工业软件基线检测检测报告的完整性与风险详情。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统可以成功创建对型号为DS-B81-HR0804的工业网关的工业软件基线检测任务，完成扫描，并可查看工业软件基线检测报告。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **128对型号为DS-B82-MR1608的工业视频网关进行工业软件基线检测测试项**

|  |
| --- |
| **测试项目：**对型号为DS-B82-MR1608的工业视频网关进行工业软件基线检测 |
| **测试依据：** |
| **测试目的：**  该测试项专注于评估型号为DS-B82-MR1608的工业视频网关在安全性上的综合表现。通过对其进行全面的安全检测，旨在深入揭示并修复潜在的风险点，以确保该工业视频网关的安全性能达到相关标准和规范，从而有效保障工业视频传输的安全性和稳定性。该测试项专注于评估型号为DS-B82-MR1608的工业视频网关在安全性上的综合表现。通过对其进行全面的安全检测，旨在深入揭示并修复潜在的风险点，以确保该工业视频网关的安全性能达到相关标准和规范，从而有效保障工业视频传输的安全性和稳定性。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1.准备环境：配置型号为DS-B82-MR1608的的工业视频网关及自研平台。  2.创建检测任务：发起针对型号为DS-B82-MR1608的的工业视频网关的工业软件基线检测任务。  3.执行扫描：监控任务完成，确保覆盖所有组件。  4.查看报告：验证工业软件基线检测检测报告的完整性与风险详情。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统可以成功创建对型号为DS-B82-MR1608的的工业视频网关工业软件基线检测任务，完成扫描，并可查看工业软件基线检测报告。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **129对型号为DS-MDS003的工业相机进行工业软件基线检测测试项**

|  |
| --- |
| **测试项目：**对型号为DS-MDS003的工业相机进行工业软件基线检测 |
| **测试依据：** |
| **测试目的：**  该测试项主要关注型号为DS-MDS003的工业相机在安全性方面的综合性能表现。通过对其进行全面且深入的安全检测，旨在发现并修复可能存在的风险点，以确保该工业相机的安全性能满足相关标准和规范，从而保障工业相机在数据采集和传输过程中的安全性和可靠性。该测试项主要关注型号为DS-MDS003的工业相机在安全性方面的综合性能表现。通过对其进行全面且深入的安全检测，旨在发现并修复可能存在的风险点，以确保该工业相机的安全性能满足相关标准和规范，从而保障工业相机在数据采集和传输过程中的安全性和可靠性。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1.准备环境：配置型号为DS-MDS003的工业相机及自研平台。  2.创建检测任务：发起针对型号为DS-MDS003的工业相机的工业软件基线检测任务。  3.执行扫描：监控任务完成，确保覆盖所有组件。  4.查看报告：验证工业软件基线检测检测报告的完整性与风险详情。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统可以成功创建对型号为DS-MDS003的工业相机的工业软件基线检测任务，完成扫描，并可查看工业软件基线检测报告。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **130对型号为iDS-2CD9396-GES的工业相机进行工业软件基线检测测试项**

|  |
| --- |
| **测试项目：**对型号为iDS-2CD9396-GES的工业相机进行工业软件基线检测 |
| **测试依据：** |
| **测试目的：**  该测试项着重评估型号为iDS-2CD9396-GES的工业相机在安全性上的综合性能。通过对其进行详尽且全面的安全检测，目标是深入揭示并修复可能隐藏的风险点，以确保该工业相机的安全性能完全符合相关标准和规范，从而为用户提供更加安全可靠的工业相机产品。该测试项着重评估型号为iDS-2CD9396-GES的工业相机在安全性上的综合性能。通过对其进行详尽且全面的安全检测，目标是深入揭示并修复可能隐藏的风险点，以确保该工业相机的安全性能完全符合相关标准和规范，从而为用户提供更加安全可靠的工业相机产品。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1.准备环境：配置型号为iDS-2CD9396-GES的工业相机及自研平台。  2.创建检测任务：发起针对型号为iDS-2CD9396-GES的工业相机的工业软件基线检测任务。  3.执行扫描：监控任务完成，确保覆盖所有组件。  4.查看报告：验证工业软件基线检测检测报告的完整性与风险详情。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统可以成功创建对型号为iDS-2CD9396-GES的工业相机的工业软件基线检测任务，完成扫描，并可工业软件基线检测报告。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **131对型号为KM9503的工控移动终端管理机进行工业软件基线检测测试项**

|  |
| --- |
| **测试项目：**对型号为KM9503的工控移动终端管理机进行工业软件基线检测 |
| **测试依据：** |
| **测试目的：**  该测试项旨在全面评估型号为KM9503的工控移动终端管理机在安全性方面的综合性能。通过对其进行深入且系统的安全检测，目标是揭示并修复可能存在的风险点，以确保该工控移动终端管理机的安全性能符合相关标准和规范，进而保障工业控制系统的整体安全性和稳定性。该测试项旨在全面评估型号为KM9503的工控移动终端管理机在安全性方面的综合性能。通过对其进行深入且系统的安全检测，目标是揭示并修复可能存在的风险点，以确保该工控移动终端管理机的安全性能符合相关标准和规范，进而保障工业控制系统的整体安全性和稳定性。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1.准备环境：配置型号为KM9503的工控移动终端管理机及自研平台。  2.创建检测任务：发起针对型号为KM9503的工控移动终端管理机的工业软件基线检测任务。  3.执行扫描：监控任务完成，确保覆盖所有组件。  4.查看报告：验证工业软件基线检测检测报告的完整性与风险详情。 |
| **预期结果：**  测试应覆盖以下内容：  1）系统可以成功创建对型号为KM9503的工控移动终端管理机的工业软件基线检测任务，完成扫描，并可查看工业软件基线检测报告。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **132 关于工业协同控制系统的结构识别与风险传播安全的成果测试项**

|  |
| --- |
| **测试项目：**关于工业协同控制系统的结构识别与风险传播安全的成果测试项 |
| **测试依据：** |
| **测试目的：**  审查软件成果之一关于工业协同控制系统的结构识别与风险传播安全的论文，是否满足技术指标，包括”数据空间网络模型”、“优势传播源探测算法”、“自主纠偏算法”审查软件成果之一关于工业协同控制系统的结构识别与风险传播安全的论文，是否满足技术指标，包括”数据空间网络模型”、“优势传播源探测算法”、“自主纠偏算法” |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）人工阅读审核 |
| **预期结果：**  测试应覆盖以下内容：  1）查阅成果是否为论文  2）查阅提供的说明文档是否和论文内容一致  3）查阅说明文档是否满足技术指标 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **133 关于“抓牛鼻子”主动协同安全控制的成果测试项**

|  |
| --- |
| **测试项目：**关于“抓牛鼻子”主动协同安全控制的成果测试项 |
| **测试依据：** |
| **测试目的：**  审查软件成果之一关于“抓牛鼻子”主动协同安全控制的技术报告，是否满足技术指标审查软件成果之一关于“抓牛鼻子”主动协同安全控制的技术报告，是否满足技术指标 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）人工阅读审核 |
| **预期结果：**  测试应覆盖以下内容：  1）查阅成果是否为技术报告  3）查阅技术报告中的内容是否满足技术指标 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **134 关于工业软件脆弱性检测与协同防护关键技术的成果测试项**

|  |
| --- |
| **测试项目：**关于工业软件脆弱性检测与协同防护关键技术的成果测试项 |
| **测试依据：** |
| **测试目的：**  审查软件成果之一关于工业软件脆弱性检测与协同防护关键技术的软著是否与平台相关审查软件成果之一关于工业软件脆弱性检测与协同防护关键技术的软著是否与平台相关 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）人工阅读审核 |
| **预期结果：**  测试应覆盖以下内容：  1）查阅成果是否为软著  3）查阅技术报告中的内容是否与平台相关 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **135 动态攻击图拓扑协同关联测试项**

|  |
| --- |
| **测试项目：**动态攻击图拓扑协同关联测试 |
| **测试依据：** |
| **测试目的：**  验证工业控制协同检测系统能够准确展示物理网络拓扑节点，并动态可视化攻击拓扑关系，实现物理节点与攻击路径的关联匹配功能验证工业控制协同检测系统能够准确展示物理网络拓扑节点，并动态可视化攻击拓扑关系，实现物理节点与攻击路径的关联匹配功能 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1) 启动工业控制协同检测系统，验证左下角物理拓扑节点是否清晰可见  2) 查看不同攻击场景，观察系统生成的攻击拓扑图是否准确反映攻击路径  3) 验证攻击图动态展示效果，确认攻击路径能够从上到下依次显示  4) 检查物理节点与攻击图节点的关联匹配准确性  5) 系统是否能够正确显示完整的攻击链路信息 性能测试方法：  1) 测量从场景到攻击图生成的端到端响应时间（目标≤10秒）  2) 模拟2个并发用户同时使用攻击图功能，监控系统稳定性 |
| **预期结果：**  功能测试应覆盖以下内容：  1) 物理拓扑节点清晰展示功能验证  2) 不同场景攻击拓扑动态展示功能验证  3) 攻击拓扑从上到下依次展示的动态效果验证  4) 左下角物理节点与攻击图的关联匹配功能验证  5) 能够显示攻击链路功能验证 性能测试应覆盖以下内容：  1) 动态攻击图生成的响应时间  2) 频繁切换场景下的系统稳定性 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **136 动态添加协同攻击图拓扑场景测试项**

|  |
| --- |
| **测试项目：**动态添加协同攻击图拓扑场景测试 |
| **测试依据：** |
| **测试目的：**  验证工业控制协同检测系统能够支持用户动态添加新场景，并正确显示攻击拓扑图和攻击关系链。测试系统场景管理功能的完整性，包括场景创建、数据文件上传、场景列表更新和攻击图可视化展示。验证工业控制协同检测系统能够支持用户动态添加新场景，并正确显示攻击拓扑图和攻击关系链。测试系统场景管理功能的完整性，包括场景创建、数据文件上传、场景列表更新和攻击图可视化展示。 |
| **测试配置：** |
| **测试步骤：**  功能测试方法：  1) 手动功能测试验证各个操作步骤  2) 界面元素交互测试  3) 文件上传功能测试  4) 数据完整性验证测试 性能测试方法：  1) 监控攻击图加载和渲染时间  2) 测试连续场景切换的系统响应  3) 使用性能监控工具检测资源使用情况 |
| **预期结果：**  功能测试应覆盖以下内容：  1) 场景添加按钮的可访问性和响应性  2) 添加场景对话框的正确显示和字段验证  4) 场景数据的正确解析和存储  5) 场景列表的实时更新  6) 新增场景的攻击图显示功能  7) 攻击关系链的正确渲染  8) 场景切换功能的正确性 性能测试应覆盖以下内容：  1) 攻击图渲染的性能表现  2) 多场景切换的响应速度  3) 系统资源占用情况 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **137 工控组件业务逻辑协同告警测试项**

|  |
| --- |
| **测试项目：**工控组件业务逻辑协同告警测试 |
| **测试依据：** |
| **测试目的：**  验证工业控制协同检测系统能够实时接收并显示攻击告警日志，当攻击告警触发时，系统能够准确识别受影响的业务逻辑节点并在拓扑图上进行高亮显示，确保告警信息与业务拓扑的可视化联动功能正常验证工业控制协同检测系统能够实时接收并显示攻击告警日志，当攻击告警触发时，系统能够准确识别受影响的业务逻辑节点并在拓扑图上进行高亮显示，确保告警信息与业务拓扑的可视化联动功能正常 |
| **测试配置：** |
| **测试步骤：**  功能测试方法：  1) 检查告警触发时对应业务节点的高亮效果  2) 验证告警与拓扑节点映射关系的准确性  3) 测试并发告警场景下的系统响应能 性能测试方法：  1) 测量从攻击事件发生到告警显示的端到端延迟  2) 进行压力测试，模拟高频率告警场景  3) 监控系统资源使用情况和响应时间  4) 执行24小时连续运行测试 |
| **预期结果：**  功能测试应覆盖以下内容：  1) 攻击告警日志的实时接收和显示功能  2) 告警信息的解析和分类处理  3) 业务拓扑图节点与告警源的映射关系  4) 节点高亮显示的准确性和及时性 性能测试应覆盖以下内容：  1) 告警信息的接收和显示响应时间  2) 大量告警并发处理的系统性能  3) 拓扑图节点高亮渲染的性能表现  4) 长时间运行下的系统稳定性 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **138 工控组件状态与物理拓扑协同关联测试项**

|  |
| --- |
| **测试项目：**工控组件状态与物理拓扑协同关联测试 |
| **测试依据：** |
| **测试目的：**  验证攻击告警发生时，物理拓扑图能够同步显示对应设备的状态变化，确保物理设备状态与告警信息的关联准确性，以及多设备同时告警时的状态显示正确性验证攻击告警发生时，物理拓扑图能够同步显示对应设备的状态变化，确保物理设备状态与告警信息的关联准确性，以及多设备同时告警时的状态显示正确性 |
| **测试配置：** |
| **测试步骤：**  功能测试方法：  1) 模拟攻击场景触发告警，观察物理拓扑图设备状态变化  2) 同时触发多个设备告警，验证拓扑图状态显示的准确性  3) 验证告警解除后设备状态的正确恢复 性能测试方法：  1) 测量告警发生到拓扑图状态更新的时延  2) 模拟高负载告警场景，监控系统资源使用情况  3) 验证拓扑图更新的流畅性和稳定性 |
| **预期结果：**  功能测试应覆盖以下内容：  1) 单设备告警触发时的物理拓扑状态显示  2) 多设备同时告警时的物理拓扑状态显示  3) 告警状态变化时的拓扑图实时更新  4) 设备状态恢复后的拓扑图状态同步  5) 不同类型告警对应的设备状态标识准确性 性能测试应覆盖以下内容：  1) 告警触发到物理拓扑状态更新的响应时间  2) 大量设备同时告警时的系统性能  3) 拓扑图刷新频率和资源占用 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **139 基于攻击链路的工控系统协同风险评估测试项**

|  |
| --- |
| **测试项目：**基于攻击链路的工控系统协同风险评估测试 |
| **测试依据：** |
| **测试目的：**  验证工业控制协同检测系统能够基于不同场景的攻击链路、暴露面、漏洞等因素进行准确的风险评估，提供威胁评估分值、综合风险指数，并清晰展示攻击链路各个环节的得分情况验证工业控制协同检测系统能够基于不同场景的攻击链路、暴露面、漏洞等因素进行准确的风险评估，提供威胁评估分值、综合风险指数，并清晰展示攻击链路各个环节的得分情况 |
| **测试配置：** |
| **测试步骤：**  功能测试方法：  1) 检查综合风险指数的实时更新效果  2) 验证攻击链路中每个节点的风险得分能够正确显示和计算  3) 切换不同场景，对比风险评估结果的变化情况 性能测试方法：  模拟20个并发用户同时使用风险评估功能，监控系统稳定性 |
| **预期结果：**  功能测试应覆盖以下内容：  1) 不同设备类型的威胁评估分值计算准确性验证  2) 攻击链路各环节风险得分的详细展示验证  3) 基于CVE漏洞库的威胁等级评估验证  4) 多场景下风险评估结果的对比展示验证 性能测试应覆盖以下内容：  风险评估数据的存储和查询性能 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### **140 工业协同控制特征参数测试项**

|  |
| --- |
| **测试项目：**工业协同控制特征参数 |
| **测试依据：** |
| **测试目的：**  在数据库的特征库中查看到10种特征在数据库的特征库中查看到10种特征 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）用数据库客户端连接数据库；  2）点击特征库可以看到系统支撑的全部工业协同控制特征，包括  工控设备会话管理缺陷特征、工控设备计算资源缺陷特征、工控设备缓冲区溢出特征、工控设备缓冲区欠载特征、工控设备时序敏感性与状态同步特征、工控设备确定性与脆弱性共生的架构特征、工控设备通信过程的行为攻击特征、工控设备资源约束的绝对性特征、工控设备功能码洪泛攻击特征。 |
| **预期结果：**  测试应覆盖以下内容：  1）在数据库的特征库中查看到10种特征 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 141 工业零信任分布协同安全管控平台桌面零信任客户端登录功能测试项

|  |
| --- |
| **测试项目：**工业零信任分布协同安全管控平台桌面零信任客户端登录功能 |
| **测试依据：** |
| **测试目的：**  该测试项用于测试指标3.1：跨域融合数据流和控制流异常检测与防护套件：初步研制工业零信任分布协同安全管控平台，包括跨域融合数据流和控制流异常检测与防护套件。该项测试具体验证了工业零信任分布协同安全管控平台桌面零信任客户端的登录及应用界面功能。该测试项用于测试指标3.1：跨域融合数据流和控制流异常检测与防护套件：初步研制工业零信任分布协同安全管控平台，包括跨域融合数据流和控制流异常检测与防护套件。该项测试具体验证了工业零信任分布协同安全管控平台桌面零信任客户端的登录及应用界面功能。 |
| **测试配置：** |
| **测试步骤：**  工业零信任分布协同安全管控平台桌面零信任客户端应能够正常登录，能够正确的验证用户名与密码，能够正确建立通道并访问工业零信任分布协同安全管控平台、零信任访问控制平台、ZGC高级威胁检测系统、ZGC工业互联防火墙应用。  测试方法：  1）配置测试机IPV4 IP为172.120.1.87，接入IT域交换机网络；  2）桌面双击ZGC零信任客户端，点击右上角设置，配置服务器地址为172.120.1.1,端口为9000，点击保存；  3）输入用户名:zhanggq,密码：zgq26717,点击登录；[check1]  4）点击我的应用，观察是否包括工业零信任分布协同安全管控平台、零信任访问控制平台、ZGC高级威胁检测系统、ZGC工业互联防火墙应用[check2]  5）分别双击点击这些应该用，观察是否能够正常跳转浏览器进入应用系统界面。[check3]  预期结果：  [check1]可以进入ZGC零信任客户端，可以显示我的应用、我的设备、版本信息模块，并显示隧道已链接。  [check2]我的应用界面可以显示工业零信任分布协同安全管控平台、零信任访问控制平台、ZGC高级威胁检测系统、ZGC工业互联防火墙。  [check3]能够正常跳转浏览器进入工业零信任分布协同安全管控平台、零信任访问控制平台、ZGC高级威胁检测系统、ZGC工业互联防火墙应用系统界面 |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 142 零信任访问控制平台管理端用户登录认证及系统界面功能测试

|  |
| --- |
| **测试项目：**零信任访问控制平台管理端用户登录认证及系统界面功能测试 |
| **测试依据：** |
| **测试目的：**  测试指标3.1：跨域融合数据流和控制流异常检测与防护套件：初步研制工业零信任分布协同安全管控平台，包括跨域融合数据流和控制流异常检测与防护套件。该测试项用于测试零信任访问控制平台的服务管理端，包括管理员登录，管理端界面功能等。测试指标3.1：跨域融合数据流和控制流异常检测与防护套件：初步研制工业零信任分布协同安全管控平台，包括跨域融合数据流和控制流异常检测与防护套件。该测试项用于测试零信任访问控制平台的服务管理端，包括管理员登录，管理端界面功能等。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1、进入零信任访问控制桌面客户端并登录，点击我的应用，双击零信任访问控制平台，填写用户名：admin、密码：Admin@123，点击登录，观察是否能够正常访问零信任访问控制平台 [check 2];  2、观察系统是否包含系统概览、用户数据管理、设备数据管理、零信任策略中心、日志中心等菜单且各个模块可正常显示  预期结果：  [check 1]：界面显示工业零信任分布协同安全管控平台、ZGC工业互联防火墙、ZGC高级威胁检测系统、零信任访问控制平台等组件。  [check 2]：能够在输入正确用户名密码的情况下正常登录零信任访问控制平台系统后端；  [check 3]：系统是否包含系统概览、用户数据管理、设备数据管理、零信任策略中心、日志中心等菜单且各个模块可正常显示。 |
| **预期结果：**  测试应覆盖以下内容：  1) 零信任访问控制平台管理端的用户登录认证功能是否正常，包括使用正确的用户名和密码进行登录。  2) 登录后系统界面是否能够正常显示所有预期的组件，如工业零信任分布协同安全管控平台、ZGC 工业互联防火墙等。  3) 系统是否包含并能正常显示“系统概览”、“用户数据管理”、“设备数据管理”、“零信任策略中心”和“日志中心”等各个模块。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 143 零信任访问控制平台管理端用户管理功能测试

|  |
| --- |
| **测试项目：**工业零信任访问控制平台管理端用户管理功能测试 |
| **测试依据：** |
| **测试目的：**  测试指标3.1：跨域融合数据流和控制流异常检测与防护套件：初步研制工业零信任分布协同安全管控平台，包括跨域融合数据流和控制流异常检测与防护套件。该测试项具体测试零信任访问控制平台管理端的用户管理模块功能。测试指标3.1：跨域融合数据流和控制流异常检测与防护套件：初步研制工业零信任分布协同安全管控平台，包括跨域融合数据流和控制流异常检测与防护套件。该测试项具体测试零信任访问控制平台管理端的用户管理模块功能。 |
| **测试配置：** |
| **测试步骤：**  零信任访问控制系统应包含用户管理功能，包括新增用户、删除用户等基本功能。  测试方法：  1、从桌面双击ZGC零信任客户端并登录，在我的应用中双击零信任访问控制系统后端进入并使用管理员账号登录，用户名为：admin，密码为Admin@123;  2、点击左侧菜单栏用户数据管理，点击在线用户，观察是否可以看到当前登录零信任设备的用户zhanggq，且可以正常显示用户状态、终端、接收、发送流量等项；[check1]  3、点击左侧菜单栏用户数据管理，点击用户管理，观察是否可以显示当前系统所有用户  4、点击右上角“添加账户”按钮，输入账户名: test1，密码: Admin@123，其余选项保持默认，点击确认，观察是否能够新建用户test1；[check2]  5、使用另外一台测试机进入桌面零信任客户端，点击右上角退出当前用户zhanggq，使用新建账户test1登录桌面客户端，观察是否可以正常登录；[check 3]  6、点击左侧菜单栏用户数据管理，点击用户管理，选择test1用户，点击该行最右侧删除按钮，点击确定，观察该用户是否被删除[check4]  7、使用新增测试机电脑使用客户端进行接入登录，观察用户是否登录失败[check5]；  [check 1] 可以看到当前登录零信任设备的用户zhanggq，且可以正常显示用户状态、终端、接收、发送流量等项  [check 2] 用户列表能够显示新建用户test1  [check 3] 新建用户test1能够成功登录桌面零信任客户端  [check 4] 用户列表不存在用户test1  [check 5] 用户登录失败 |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 144 零信任访问控制平台管理端终端接入审核功能测试

|  |
| --- |
| **测试项目：**零信任访问控制平台终端接入审核功能测试 |
| **测试依据：** |
| **测试目的：**  测试指标3.1：跨域融合数据流和控制流异常检测与防护套件：初步研制工业零信任分布协同安全管控平台，包括跨域融合数据流和控制流异常检测与防护套件。该测试项具体测试零信任访问控制平台管理端的终端接入审核功能。测试指标3.1：跨域融合数据流和控制流异常检测与防护套件：初步研制工业零信任分布协同安全管控平台，包括跨域融合数据流和控制流异常检测与防护套件。该测试项具体测试零信任访问控制平台管理端的终端接入审核功能。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1) 从桌面双击ZGC零信任客户端并登录，在我的应用中双击零信任访问控制系统后端进入并使用管理员账号登录，用户名为：admin，密码为Admin@123;  2) 点击左侧菜单栏设备数据管理-设备管理，进入设备管理模块，点击右侧智能审核，能够选择新增设备登录策略，动作包括手动审核与自动审核。  3) 设置新增设备登录策略为手动审核，并开启告警；[check 1]  4) 使用新增测试机电脑使用客户端进行接入登录，观察结果；[check 2]  5) 设备管理中修改新增设备登录策略为动作为自动，开启告警；  6) 使用新增电脑使用客户端进行接入登录，观察结果；[check 3]  预期结果：  [check 1] 修改完成后，界面显示“更新智能审核策略成功! ”  [check 2] 客户端不能登录成功，提示需要管理审核，产生告警；管理员在设备管理中审核通过后，客户端可以登录成功；  [check 3] 客户端可以登录成功，自动审核通过，产生告警； |
| **预期结果：**  测试应覆盖以下内容：  1) 零信任访问控制平台终端接入审核功能，包括手动和自动两种审核策略的设置和生效。  2) 在手动审核策略下，新设备接入是否能正确触发管理员审核，以及审核通过后客户端的登录功能。  3) 在自动审核策略下，新设备接入是否能自动通过审核并成功登录，以及是否能正确产生告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 145 零信任访问控制平台管理端策略配置功能测试

|  |
| --- |
| **测试项目：**零信任访问控制平台策略配置功能测试 |
| **测试依据：** |
| **测试目的：**  测试指标3.1：跨域融合数据流和控制流异常检测与防护套件：初步研制工业零信任分布协同安全管控平台，包括跨域融合数据流和控制流异常检测与防护套件。该测试项具体测试零信任访问控制平台策略配置功能。测试指标3.1：跨域融合数据流和控制流异常检测与防护套件：初步研制工业零信任分布协同安全管控平台，包括跨域融合数据流和控制流异常检测与防护套件。该测试项具体测试零信任访问控制平台策略配置功能。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1) 从桌面双击ZGC零信任客户端并登录，在我的应用中双击零信任访问控制系统后端进入并使用管理员账号登录，用户名为：admin，密码为Admin@123;  2) 点击左侧菜单栏零信任策略中心，点击零信任安全策略，能够配置不同级别策略；[check 1]  3) 点击左侧菜单栏零信任策略中心，点击零信任策略授权，能够添加策略，或将已有策略绑定至用户/组及应用标签。[check 2]  预期结果：  [check 1] 可以配置不同级别策略，包含：基本级、专业级、特权级策略。具体包括非常用设备登录、未开启系统防火墙、异常认证过程、长时间未登录、异地登录、异常旅行速度、操作系统版本不满足，分别可设置采取禁止登录、账户锁定、增强认证、系统告警、禁止访问指定应用措施；  [check 2] 点击安全策略，点击授权策略，能够新建策略，或将已有策略绑定置用户组及应用资源。 |
| **预期结果：**  测试应覆盖以下内容：  1) 零信任安全策略的配置功能，包括不同级别策略的设置及其对应的管控措施。  2) 零信任策略的授权和绑定功能，确保策略能正确应用于用户组和应用资源。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 146 零信任访问控制平台管理端日志管理功能测试

|  |
| --- |
| **测试项目：**零信任访问控制平台日志管理功能 |
| **测试依据：** |
| **测试目的：**  测试指标3.1：跨域融合数据流和控制流异常检测与防护套件：初步研制工业零信任分布协同安全管控平台，包括跨域融合数据流和控制流异常检测与防护套件。该测试项具体测试零信任访问控制平台日志管理功能。测试指标3.1：跨域融合数据流和控制流异常检测与防护套件：初步研制工业零信任分布协同安全管控平台，包括跨域融合数据流和控制流异常检测与防护套件。该测试项具体测试零信任访问控制平台日志管理功能。 |
| **测试配置：** |
| **测试步骤：**  系统日志、行为日志和安全日志界面的显示完整性和信息准确性。  测试方法：  1) 从桌面双击ZGC零信任客户端并登录，在我的应用中双击零信任访问控制系统后端进入并使用管理员账号登录，用户名为：admin，密码为Admin@123;  2) 点击左侧菜单栏日志中心，点击系统日志，观察是否能够显示系统日志界面，包括日志类型、操作类型、来源、地址等[check 1]  3) 点击日志中心-行为日志，显示行为日志界面，包括用户登陆日志与访问控制日志两大组件[check 2]  4) 点击日志中心-安全日志，显示安全日志界面，包括分析组件、风险类型、风险等级等内容[check 3]  预期结果：  [check 1] 可查看系统日志界面，包括日志类型、操作类型、来源、地址等；  [check 2] 可查看行为日志界面，包括用户登陆日志与访问控制日志两大组件；  [check 3] 可查看安全日志界面，包括分析组件、风险类型、风险等级等内容 |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 147 零信任访问控制平台持续监测功能测试

|  |
| --- |
| **测试项目：**工业零信任访问控制平台持续监测功能 |
| **测试依据：** |
| **测试目的：**  该测试项针对测试指标3.1：跨域融合数据流和控制流异常检测与防护套件：初步研制工业零信任分布协同安全管控平台，包括跨域融合数据流和控制流异常检测与防护套件。该测试项具体测试零信任访问控制平台的用户持续监测功能。该测试项针对测试指标3.1：跨域融合数据流和控制流异常检测与防护套件：初步研制工业零信任分布协同安全管控平台，包括跨域融合数据流和控制流异常检测与防护套件。该测试项具体测试零信任访问控制平台的用户持续监测功能。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）从桌面双击ZGC零信任客户端并登录，在我的应用中双击零信任访问控制系统后端进入并使用管理员账号登录，用户名为：admin，密码为Admin@123;  2）登录零信安全访问控制任进入，点击零信任策略中心，点击零信任安全策略，修改基本级策略，点击添加，选择类型为是否安装远控软件，动作为禁止登录，点击确定；  3）零信任管理平台应通过用户是否安装远程控制软件判断该用户是否可登录，且在用户登录访问应用期间进行持续监测；  4）使用未安装远程控制软件的测试机器登录桌面零信任客户端，使用zhanggq用户登录，密码为zgq26717  5）观察用户是否被允许登录，观察是否可登录，  6）用户登录后，安装远程控制软件，观察用户是否被强制下线；[check1]  7）进入零信任访问控制平台，点击日志中心，点击安全日志，观察是否存在“用户安装了远程控制软件”告警[check2]  预期结果：  [check1]客户端可以正常登录；  [check2]用户被踢下线，客户端提示“客户端存在安全风险，禁止登录”，零信任访问控制平台安全日志可查看告警记录，显示风险类型为“安装了远程控制软件”； |
| **预期结果：**  测试应覆盖以下内容：  1) 零信任访问控制平台持续监测功能，包括配置和应用安全策略以检测用户行为和环境变化。  2) 当用户触发持续监测策略时，系统能正确执行预设的管控动作，如强制下线或禁止登录。  3) 系统能够生成并记录相应的安全告警日志，准确显示风险类型。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 148 工业零信任分布协同安全管控平台登录及功能界面测试

|  |
| --- |
| **测试项目：**工业零信任分布协同安全管控平台登录及功能界面 |
| **测试依据：** |
| **测试目的：**  该测试项用于测试指标3.1：跨域融合数据流和控制流异常检测与防护套件：初步研制工业零信任分布协同安全管控平台，包括跨域融合数据流和控制流异常检测与防护套件。该测试项主要测试工业零信任分布协同安全管控平台的登录及功能界面。该测试项用于测试指标3.1：跨域融合数据流和控制流异常检测与防护套件：初步研制工业零信任分布协同安全管控平台，包括跨域融合数据流和控制流异常检测与防护套件。该测试项主要测试工业零信任分布协同安全管控平台的登录及功能界面。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）从桌面双击ZGC零信任客户端并登录，在我的应用中点击“工业零信任分布协同安全管控平台”，能够进入系统登录界面;  2）使用operator账户进行登录，填写用户名:operator、密码: Admin@123456，并点击登录 [check 1]  3）进入系统首页界面，能够查看顶部菜单栏包含缺陷及风险可视化、异常检测、工业资产管理、日志管理等模块。[check 2]  4）点击顶部菜单栏“缺陷及风险可视化”，能够进入可视化工具管理界面，能够对大屏展示可视化组件进行选择与设置；[check 3]  5）点击顶部菜单栏“异常检测”，该界面包含异常告警概览、异常处置、关联分析、异常白名单等组件。点击左侧菜单栏的异常处置菜单，可以查看分布平台的所有异常告警，包括告警时间、异常类型、源IP、目的IP、异常告警描述等，并且可对告警进行处置或加白操作；[check 4]  6）点击系统顶部工业资产管理菜单，可以查看左侧菜单栏包含资产概览、资产管理以及拓扑管理模块，点击资产管理，包含已确认资产、未确认资产、主动资产发现、被动资产发现功能，点击已确认资产，可以查看当前模拟环境网络下所有资产，点击拓扑管理，可以查看与管理网络域内拓扑结构；[check 5]  预期结果：  [check 1] 可以进入工业零信任分布协同安全管控平台主界面，包含登录窗口，输入正确的用户名密码可以正常登录；  [check 2] 系统顶部菜单栏包含这些模块；  [check 3] “缺陷及风险可视化”相应模块可以正常显示及操作；  [check 4] “异常检测”相应模块可以正常显示及操作；  [check 5] ”工业资产管理”模块可以正常显示及操作。 |
| **预期结果：**  测试应覆盖以下内容：  1） 应能够根据地址正常进入工业零信任分布协同安全管控平台的用户登录界面  2） 正确填写用户名密码后能够正常登录  3） 可以进入系统主界面，系统能够包含任务指标的工业资产管理、异常监测等功能 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 149 工业零信任分布协同安全管控平台管理端登录及功能测试

|  |
| --- |
| **测试项目：**工业零信任分布协同安全管控平台管理端系统登录功能 |
| **测试依据：** |
| **测试目的：**  该测试项用于测试指标3.1：跨域融合数据流和控制流异常检测与防护套件：初步研制工业零信任分布协同安全管控平台，包括跨域融合数据流和控制流异常检测与防护套件。该测试项具体验证工业零信任分布协同安全管控平台系统应能够进入系统管理员登录界面，并具备管理员的常见功能。该测试项用于测试指标3.1：跨域融合数据流和控制流异常检测与防护套件：初步研制工业零信任分布协同安全管控平台，包括跨域融合数据流和控制流异常检测与防护套件。该测试项具体验证工业零信任分布协同安全管控平台系统应能够进入系统管理员登录界面，并具备管理员的常见功能。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）配置电脑ip地址为：192.168.10.77，打开浏览器，输入访问地址https://192.168.10.15:8440 ,能够进入系统登录界面 [check1]  2）填写用户名:admin、密码: Admin@123456，并点击登录 [check2]  3）登陆成功后，进入系统主界面，该界面包含用户权限、网络配置、时钟配置、工单管理、授权管理等模块。 [check3]  预期结果：  [check 1]可以进入工业零信任分布协同安全管控平台主界面，包含登录窗口  [check 2]可以通过填写管理员用户名、密码登录成功  [check 3]能够进入工业零信任分布协同安全管控平台的系统管理界面，包含用户权限、网络配置、时钟配置、工单管理、授权管理等模块 。 |
| **预期结果：**  测试应覆盖以下内容：  1） 应能够根据地址正常进入工业零信任分布协同安全管控平台的用户登录界面  2） 正确填写用户名密码后能够正常登录  3） 可以进入系统主界面 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 150 工业零信任分布协同安全管控平台系统管理端用户管理功能测试

|  |
| --- |
| **测试项目：**工业零信任分布协同安全管控平台系统用户管理功能 |
| **测试依据：** |
| **测试目的：**  测试指标3.1：跨域融合数据流和控制流异常检测与防护套件：初步研制工业零信任分布协同安全管控平台，包括跨域融合数据流和控制流异常检测与防护套件。该项主要针对工业零信任分布协同安全管控平台系统应具备用户管理功能进行测试测试指标3.1：跨域融合数据流和控制流异常检测与防护套件：初步研制工业零信任分布协同安全管控平台，包括跨域融合数据流和控制流异常检测与防护套件。该项主要针对工业零信任分布协同安全管控平台系统应具备用户管理功能进行测试 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）配置电脑ip地址为：192.168.10.77，打开浏览器，输入访问地址https://192.168.10.15:8440 ,能够进入工业零信任分布协同安全管控平台登录界面 [check1]  2）使用管理员账号进行登录，填写用户名:admin、密码: Admin@123456，并点击登录 [check2]  3）左侧菜单栏点击用户权限，点击用户管理，观察是否能够查看所有用户，包括用户名称、所属角色、上次登陆时间、创建时间、状态等信息 [check3]  4）点击用户权限，点击用户管理，点击新增，观察是否能可以新增用户，能够设置用户名称、用户描述、所属角色、密码等基本信息 [check 4]  5) 点击用户权限，点击用户管理，选择一个用户点击编辑，观察是否能够可以对用户名称、描述、角色以及密码进行修改 [check 5]  6) 点击用户权限，点击用户管理，选中所需删除用户，点击删除，观察该用户是否被正确删除。[check 6]  预期结果：  [check 1] 可以进入工业零信任分布协同安全管控平台主界面，包含登录窗口  [check 2] 可以通过填写管理员用户名、密码登录成功  [check 3]能够进入工业零信任分布协同安全管控平台的系统管理界面，包含用户权限、网络配置、时钟配置、工单管理、授权管理等模块 ；并通过左侧菜单栏点击用户权限，点击用户管理，观察是否能够查看所有用户，包括用户名称、所属角色、上次登陆时间、创建时间、状态等信息  [check 4]新增对应用户信息，包括用户名称、所属角色、上次登陆时间、创建时间、状态等信息  [check 5]用户名称、描述、角色以及密码变更为修改后的内容  [check 6]用户信息被删除 |
| **预期结果：**  测试应覆盖以下内容：  1） 工业零信任分布协同安全管控平台能够对所有用户进行查看操作  2） 工业零信任分布协同安全管控平台能够新增用户  3） 工业零信任分布协同安全管控平台能够对已有用户信息进行编辑  4） 工业零信任分布协同安全管控平台能够删除现有用户 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 151 OT域机械臂状态数据流异常检测与防护套件测试

|  |
| --- |
| **测试项目：**OT域机械臂状态数据流异常检测与防护套件 |
| **测试依据：** |
| **测试目的：**  测试指标3.1：跨域融合数据流和控制流异常检测与防护套件：初步研制工业零信任分布协同安全管控平台，包括跨域融合数据流和控制流异常检测与防护套件。工业零信任分布协同安全管控平台系统应具备数据流异常检测功能，根据OT域机械臂的状态数据流判断机械臂异常检测并进行防护。测试指标3.1：跨域融合数据流和控制流异常检测与防护套件：初步研制工业零信任分布协同安全管控平台，包括跨域融合数据流和控制流异常检测与防护套件。工业零信任分布协同安全管控平台系统应具备数据流异常检测功能，根据OT域机械臂的状态数据流判断机械臂异常检测并进行防护。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）进入机械臂控制界面，打开工程师站笔记本，从桌面进入：/robotsdio2.0.0/win-unpacked/目录下，双击打开robot-pick-studio.exe文件，最大化窗口，点击开始下“所有项目”，选择创建时间未2025-04-16的项目点击打开，左侧栏目机械臂/代码下，双击打开dataTest3.c  2）进入攻击机代码执行界面，在攻击机桌面双击Pycharm，进入后自动进入robot-socket项目，双击左侧“attack1.py”打开攻击代码  3）模拟机械臂正常执行，首先点击客户端右上角上电，机械臂可正常上电，在代码界面点击右键，点击运行，机械臂开始进行打磨作业，直至打磨任务结束后机械臂复位[check1]  4）再次在工程师站中重复步骤3，使机械臂进入正常运行状态。  5）此时在攻击机的“attack1.py”代码中点击右键运行。机械臂此时被攻击，运行状态中发出较为剧烈的异响[check2]  6）测试异常检测与防护效果的功能性，打开工业控制流异常检测与防护模块，在工程师站中再次执行步骤3，此时机械臂进入正常执行状态。此时在攻击机中再次执行步骤5。  7）数据流异常检测模块可以根据机械臂传感器采集的设备电力、力矩、速度决策参数判断机械臂进入异常状态，此时观察机械臂是否被自动停止[check3]  8）进入工业零信任分布协同安全管控平台，点击顶部菜单栏“异常检测”，点击左侧菜单栏“异常处置”，观察是否出现“机械臂状态参数异常”类型告警，观察异常告警描述是否出现“机械臂正常执行状态下遭受其它客户端调用使能命令导致机械臂异常响动”[check 4]  预期结果：  [check1]机械臂能够正常上电，且机械臂正常重复执行打磨动作  [check2]发起攻击后，机械臂持续存在剧烈异响，进入异常状态  [check3]机械臂被攻击后立刻停止当前打磨任务和异常动作  [check4]异常处置界面出现“机械臂状态参数异常”类型告警，观察异常告警描述是否出现“机械臂正常执行状态下遭受其它客户端调用使能命令导致机械臂异常响动” |
| **预期结果：**  测试应覆盖以下内容：  1） 检测机械臂被攻击后异常检测与防护套件是否可以进行检测  2） 是否可以对攻击后的危险动作进行干扰，防止OT域工业设备的损坏 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 152 OT域机械臂控制流白名单异常检测套件测试项

|  |
| --- |
| **测试项目：**OT域机械臂控制流白名单异常检测套件 |
| **测试依据：** |
| **测试目的：**  测试指标3.1：跨域融合数据流和控制流异常检测与防护套件：初步研制工业零信任分布协同安全管控平台，包括跨域融合数据流和控制流异常检测与防护套件。该项主要测试工业零信任分布协同安全管控平台系统应能够具备白名单算法，对OT域机械臂的异常操作进行检测并告警。测试指标3.1：跨域融合数据流和控制流异常检测与防护套件：初步研制工业零信任分布协同安全管控平台，包括跨域融合数据流和控制流异常检测与防护套件。该项主要测试工业零信任分布协同安全管控平台系统应能够具备白名单算法，对OT域机械臂的异常操作进行检测并告警。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1） 进入机械臂控制界面，打开工程师站笔记本，从桌面进入：/robotsdio2.0.0/win-unpacked/目录下，双击打开robot-pick-studio.exe文件，最大化窗口，点击开始下“所有项目”，选择创建时间未2025-04-16的项目点击打开，左侧栏目机械臂/代码下，双击打开dataTest3.c  2） 进入攻击机代码执行界面，在攻击机桌面双击Pycharm，进入后自动进入robot-socket项目，双击左侧“attack1\_data.py”打开攻击代码  3） 模拟机械臂正常执行，首先点击客户端右上角上电，机械臂可正常上电，在代码界面点击右键，点击运行，机械臂开始进行打磨作业，直至打磨任务结束后机械臂复位[check1]  4） 再次在工程师站中重复步骤3，使机械臂进入正常运行状态。  5） 此时在攻击机的“attack2\_control.py”代码中点击右键运行。观察机械臂是否在正常打磨过程被中断，执行未定义的异常操作 [check2]  6） 控制流异常检测白名单算法可以通过解码经过交换机进入机械臂的工控协议，根据白名单算法策略判断机械臂异常[check3]  7） 进入工业零信任分布协同安全管控平台，点击顶部菜单栏“异常检测”，点击左侧菜单栏“异常处置”，观察是否出现“机械臂状态参数异常”类型告警，观察异常告警描述是否出现“机械臂正常执行状态下遭受其它客户端调用使能命令导致机械臂异常响动”[check 4]  预期结果：  系统可检测出设备状态异常，并产生告警，系统调用预定义指令停止传感器工作  [check1] 机械臂能够正常上电，且机械臂正常重复执行打磨动作  [check2] 发起攻击后，机械臂持续存在剧烈异响，进入异常状态  [check3] 机械臂被攻击后立刻停止当前打磨任务和异常动作  [check4] 异常处置界面出现“机械臂状态参数异常”类型告警，观察异常告警描述是否出现“机械臂正常执行状态下遭受其它客户端调用使能命令导致机械臂异常响动” |
| **预期结果：**  测试应覆盖以下内容：  1) 机械臂在正常运行和遭受攻击后的异常状态下，系统能否正确识别并显示其状态。  2) OT 域机械臂控制流白名单算法能否有效检测到机械臂的异常操作。  3) 系统是否能针对检测到的异常产生准确的告警，并采取相应的防护措施。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 153 IT域网络流攻击入侵异常检测防护套件测试项

|  |
| --- |
| **测试项目：**IT域网络流入侵异常检测防护套件 |
| **测试依据：** |
| **测试目的：**  测试指标3.1：跨域融合数据流和控制流异常检测与防护套件：初步研制工业零信任分布协同安全管控平台，包括跨域融合数据流和控制流异常检测与防护套件。该项用于测试IT/OT域网络流入侵异常防护套件。测试指标3.1：跨域融合数据流和控制流异常检测与防护套件：初步研制工业零信任分布协同安全管控平台，包括跨域融合数据流和控制流异常检测与防护套件。该项用于测试IT/OT域网络流入侵异常防护套件。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1） 配置测试机网络连接工业互联防火墙，在测试机桌面打开科来数据包播放器，  2） 选择网卡处选择第二张网卡，点击添加文件，进入E:\北航项目\中关村实验室项目\2025年上半年zgc项目推进\所有测试统一脚本及用例入口目录下，选择攻击大全数据包；  3） 选择播放速度为原始，其余都为默认，点击开始，该软件会向被攻击服务器发送携带永恒之蓝木马的流量数据报文；  4） 浏览器输入https://192.168.10.11，登录工业互联墙管理平台，点击日志中心，点击安全日志，点击入侵防御日志。观察是否可看到攻击告警信息。[check 1]  预期结果：  [check1] 入侵防御日志表单可以显示攻击大全相应攻击流的告警信息。包括时间、级别、用户名称、源地址、源端口、归属地、目的地址、端口、事件名称、事件类型等，可以看到行为列表为拒绝 |
| **预期结果：**  测试应覆盖以下内容：  1) IT 域网络入侵攻击的检测能力，特别是对已知攻击流量的识别。  2) 入侵防御日志记录的完整性和准确性，确保日志包含攻击的时间、级别、源/目的信息及事件类型。  3) 系统对入侵攻击的告警功能和防护措施是否有效。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 154 病毒攻击异常防护套件测试项

|  |
| --- |
| **测试项目：**病毒攻击异常防护套件 |
| **测试依据：** |
| **测试目的：**  测试指标3.1：跨域融合数据流和控制流异常检测与防护套件：初步研制工业零信任分布协同安全管控平台，包括跨域融合数据流和控制流异常检测与防护套件测试指标3.1：跨域融合数据流和控制流异常检测与防护套件：初步研制工业零信任分布协同安全管控平台，包括跨域融合数据流和控制流异常检测与防护套件 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1） 打开科来数据包播放器，选择网卡，点击添加文件，选择病毒文件流量仿真数据报文包  2） 选择播放速度为原始，其余都为默认，点击开始。该软件会向被攻击服务器发送携带病毒的流量数据报文。  3） 浏览器输入https://192.168.10.11，输入用户名：admin，密码：Admin@123456，登录工业互联墙管理平台，在顶部菜单点击数据中心，侧栏点击日志中心，点击安全日志，点击入侵防御日志。观察是否可看到病毒攻击异常攻击告警信息。[check1]  预期结果：  [check1]产生恶意文件告警信息并列表展示。列表内容包括：序号、告警时间、受影响IP、文件名称、传输层协议、应用层协议、病毒名称、病毒类型、告警信息、告警级别、处理状态、操作。 |
| **预期结果：**  测试应覆盖以下内容：  1）验证系统对模拟病毒攻击流量的检测能力。  2）验证系统生成告警信息的完整性。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 155 高级威胁检测套件测试项

|  |
| --- |
| **测试项目：**高级威胁检测套件测试项 |
| **测试依据：** |
| **测试目的：**  测试指标3.1：跨域融合数据流和控制流异常检测与防护套件：初步研制工业零信任分布协同安全管控平台，包括跨域融合数据流和控制流异常检测与防护套件测试指标3.1：跨域融合数据流和控制流异常检测与防护套件：初步研制工业零信任分布协同安全管控平台，包括跨域融合数据流和控制流异常检测与防护套件 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1)）在测试机打开浏览器，输入https://192.168.10.14，进入高级威胁检测系统，输入用户名：admin，密码Admin@123456，点击策略中心，点击攻击检测策略，选择网络攻击，点击右上角全部开启。  2）在攻击检测策略中选择高级威胁策略，对内高级威胁策略可选择停用或启用。  3）在异常行为策略中选择异常连接，对隐蔽通道、恶意加密流量可选择启用，推送对应攻击策略流量[check1]  4）打开科来数据包播放器，选择网卡，点击添加文件，选择永恒之蓝攻击数据包（攻击包中包含源IP与靶机IP，报文中包含永恒之蓝木马），选择播放速度为原始，其余都为默认，点击开始。该软件会向被攻击服务器发送携带永恒之蓝木马的流量数据报文。  5）点击分析中心，点击安全事件分析，观察是否能查看异常流量攻击事件[check1] |
| **预期结果：**  测试应覆盖以下内容：  1）验证高级威胁检测系统的检测能力。  2）验证高级威胁策略和异常行为策略的有效性及配置功能。  3）验证系统在安全事件分析中正确展示异常流量攻击事件。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 156 ACL防护套件功能测试项

|  |
| --- |
| **测试项目：**ACL防护套件功能测试 |
| **测试依据：** |
| **测试目的：**  测试指标3.1：跨域融合数据流和控制流异常检测与防护套件：初步研制工业零信任分布协同安全管控平台，包括跨域融合数据流和控制流异常检测与防护套件测试指标3.1：跨域融合数据流和控制流异常检测与防护套件：初步研制工业零信任分布协同安全管控平台，包括跨域融合数据流和控制流异常检测与防护套件 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1. 浏览器输入在测试机打开浏览器，输入https://192.168.10.14，进入工业零信任分布协同安全管控平台  2. 输入用户名:operator\_p，密码Admin@123456，登入防火墙后端 [check1]；  3. 点击防火墙，点击ALC配置，点击添加，新建一条ACL配置模版名称为acl-3。  4. 点击编辑，进入ACL规则信息中，点击添加，源地址设置为攻IT域攻击机IP:172.120.1.3,目的地址:192.168.0.99,服务：双向ping，执行动作：阻断。  3. 进入防火墙管理，点击配置，ACL模版选择步骤2新建的acl-1  ACL是访问控制列表，  4. 在攻击机172.120.1.3上 ping机械臂ip 192.168.0.99  5. 使用operator用户登录工业零信任分布协同安全管控平台，进入日志管理-工业防火墙-安全事件检索查看告警日志【check 2】  1.在攻击机172.120.1.3的cmd中输入 ping 192.168.0.99  预期结果：  [check1]能够进入防火墙后端界面  [check2]产生ACL告警，告警详细信息中包含“违反acl规则，非法ping请求”； |
| **预期结果：**  测试应覆盖以下内容：  1）验证ACL规则的配置功能及其对非法流量（如特定ping请求）的阻断能力。  2）验证系统能对违反ACL规则的流量生成准确的告警信息，并可在安全日志中查询。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 157 流量异常检测防护套件-SYN Flood攻击检测测试项

|  |
| --- |
| **测试项目：**流量异常检测防护套件-SYN Flood攻击检测测试 |
| **测试依据：** |
| **测试目的：**  指标3.1：跨域融合数据流和控制流异常检测与防护套件：初步研制工业零信任分布协同安全管控平台，包括跨域融合数据流和控制流异常检测与防护套件（功能性）指标3.1：跨域融合数据流和控制流异常检测与防护套件：初步研制工业零信任分布协同安全管控平台，包括跨域融合数据流和控制流异常检测与防护套件（功能性） |
| **测试配置：** |
| **测试步骤：**  测试方法：  1） 在测试机打开浏览器，输入https://192.168.10.14，进入工业零信任分布协同安全管控平台  2） 输入用户名:operator\_p，密码Admin@123456，登入防火墙后端  3） 进入安全域配置A，添加一条安全域，输入安全域名：安全域B，，关联防火墙选择工业安全网关，选择所有接口  4） 进入攻击防范-异常流量检测，编辑SYN Flood连接速率阀值5PPS  5） 在攻击机上打开科来数据包播放器，选择回放报文synflood.pcap  6） 使用operator用户登录工业零信任分布协同安全管控平台，进入日志管理-工业防火墙-安全事件检索查看告警日志【check1】  预期结果：  [check1]产生SYN Flood攻击告警，告警详细信息中包含“发生SYN Flood攻击”； |
| **预期结果：**  测试应覆盖以下内容：  1）验证系统对SYN Flood攻击的检测能力；  2）验证系统在不同模块（如安全运营管理平台和监控审计）中生成SYN Flood攻击告警的准确性和一致性；  3）验证SYN Flood连接速率阈值配置的有效性。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 158 TCP扫描检测攻击检测套件测试项

|  |
| --- |
| **测试项目：**TCP扫描检测攻击检测套件测试 |
| **测试依据：** |
| **测试目的：**  指标3.1：跨域融合数据流和控制流异常检测与防护套件：初步研制工业零信任分布协同安全管控平台，包括跨域融合数据流和控制流异常检测与防护套件（功能性）指标3.1：跨域融合数据流和控制流异常检测与防护套件：初步研制工业零信任分布协同安全管控平台，包括跨域融合数据流和控制流异常检测与防护套件（功能性） |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）浏览器输入在测试机打开浏览器，输入https://192.168.10.14，进入工业零信任分布协同安全管控平台。输入用户名:operator\_p，密码Admin@123456，登入防火墙后端  2）2.进入扫描防护，添加一条扫描防护模版，接口数量选择12.  3）3.编辑刚才创建的防护规则，防火墙接口选择全部，勾选启动TCP扫描防护，阈值1000，检测周期和抑制时长默认值。  4）4.进入防火墙配置-防火墙管理-配置，点击修改，下滑到扫描防护配模板，扫描防护模版选择步骤2新建的扫描防护模版，点击保存  5）5.打开IT域攻击机，打开科来数据包播放器，点击添加文件，上回放报文“TCP扫描\_1000.pcap”  6）6）进入工业零信任分布协同管理平台，点击顶部菜单栏异常检测，点击异常处置查看告警日志【check1】  7）预期结果：  8）[check1] 产生防火墙扫描防护事件告警，告警信息详细中包含“发生TCP扫描告警” |
| **预期结果：**  测试应覆盖以下内容：  1）验证TCP扫描防护规则的配置和启用功能。  2）验证系统对TCP扫描攻击的检测能力。  3）验证系统生成TCP扫描告警事件并记录到日志的功能。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 159 非法外联异常检测套件测试项

|  |
| --- |
| **测试项目：**非法外联异常检测套件 |
| **测试依据：** |
| **测试目的：**  指标3.1：跨域融合数据流和控制流异常检测与防护套件：初步研制工业零信任分布协同安全管控平台，包括跨域融合数据流和控制流异常检测与防护套件（功能性）指标3.1：跨域融合数据流和控制流异常检测与防护套件：初步研制工业零信任分布协同安全管控平台，包括跨域融合数据流和控制流异常检测与防护套件（功能性） |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）浏览器输入在测试机打开浏览器，输入https://192.168.10.14，进入工业零信任分布协同安全管控平台。输入用户名:operator\_p，密码Admin@123456，登入防火墙后端  2）进入监控审计-策略管理-外联白名单模版，新建一条外联白名单模版A  3）编辑模版规则，监测地址：172.120.1.3，外联地址：192.168.0.99，外联TCP端口：200，外联UDP端口：300，点击保存；【check1】  4）点击【监测审计】-【配置】-【修改】，异常行为检测中引用步骤2添加的外联白名单模版A  5）在攻击机172.120.1.3上连接机械臂ip 192.168.0.99的端口200  6）使用operator用户登录工业零信任分布协同安全管控平台，进入日志管理-监控审计-安全事件检索查看告警日志【check1】  预期结果：  [check1] 产生外联白名单告警事件告警，告警信息详细中包含“外联白名单告警” |
| **预期结果：**  测试应覆盖以下内容：  1）验证外联白名单规则的配置和引用功能。  2）验证系统对违反外联白名单规则的非法外联行为的检测能力。  3）验证系统生成外联白名单告警并记录到日志的功能。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 160 基于增量学习的OT域异常检测算法测试项

|  |
| --- |
| **测试项目：**基于增量学习的OT域异常检测算法 |
| **测试依据：** |
| **测试目的：**  指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）；该测试项用于测试基于增量学习的异常检测算法指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）；该测试项用于测试基于增量学习的异常检测算法 |
| **测试配置：** |
| **测试步骤：**  输入OT域异常检测测试样本数据，基于增量学习的异常检测算法算法应能够返识别样本的正常及异常状态，且输出异常检测的分类精度。  测试方法：  1.执行python OT/increment.py  2. 输入1或2选择测试数据，1代表全部数据，2代表随机单条数据  预期结果：  算法能够识别正常状态及异常状态，在全部数据测试模式下输出算法分类精确度，在单条数据测试模式下输出数据标签。 |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 161 双向LSTM网络OT域异常检测算法测试项

|  |
| --- |
| **测试项目：**双向LSTM网络识别算法 |
| **测试依据：** |
| **测试目的：**  指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）；指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）； |
| **测试配置：** |
| **测试步骤：**  输入OT域异常检测测试样本数据，双向LSTM网络识别算法应能够返识别样本的正常及异常状态，且输出异常检测的分类精度。  测试方法：  1.执行python OT/lstm.py  2. 输入1或2选择测试数据，1代表全部数据，2代表随机单条数据  预期结果：  算法能够识别正常状态及异常状态，在全部数据测试模式下输出算法分类精确度，在单条数据测试模式下输出数据标签。 |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 162 基于SVM的OT域异常检测算法测试项

|  |
| --- |
| **测试项目：**基于SVM的OT异常检测算法 |
| **测试依据：** |
| **测试目的：**  指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）；指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）； |
| **测试配置：** |
| **测试步骤：**  输入OT域异常检测测试样本数据，基于SVM的识别算法应能够返识别样本的正常及异常状态，且输出异常检测的分类精度。  测试方法：  1.执行python OT/SVM.py  2. 输入1或2选择测试数据，1代表全部数据，2代表随机单条数据  预期结果：  算法能够识别正常状态及异常状态，在全部数据测试模式下输出算法分类精确度，在单条数据测试模式下输出数据标签。 |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 163 基于随机树的OT域异常检测算法测试项

|  |
| --- |
| **测试项目：**基于随机树的OT域异常检测算法 |
| **测试依据：** |
| **测试目的：**  指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）；指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）； |
| **测试配置：** |
| **测试步骤：**  输入OT域异常检测测试样本数据，基于随机树的识别算法应能够返识别样本的正常及异常状态，且输出异常检测的分类精度。  测试方法：  1.执行python OT/randomtree.py  2. 输入1或2选择测试数据，1代表全部数据，2代表随机单条数据  预期结果：  算法能够识别正常状态及异常状态，在全部数据测试模式下输出算法分类精确度，在单条数据测试模式下输出数据标签。 |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 164 基于logistic回归OT异常检测算法测试项

|  |
| --- |
| **测试项目：**基于logistic回归的OT域异常检测算法 |
| **测试依据：** |
| **测试目的：**  指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）；指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）； |
| **测试配置：** |
| **测试步骤：**  输入OT域异常检测测试样本数据，基于logistic回归的识别算法应能够返识别样本的正常及异常状态，且输出异常检测的分类精度。  测试方法：  1.执行python OT/logistic.py  2. 输入1或2选择测试数据，1代表全部数据，2代表随机单条数据  预期结果：  算法能够识别正常状态及异常状态，在全部数据测试模式下输出算法分类精确度，在单条数据测试模式下输出数据标签。 |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 165 基于CNN-LSTM模型的IT流量异常检测算法测试项

|  |
| --- |
| **测试项目：**基于CNN-LSTM模型的IT流量异常检测算法 |
| **测试依据：** |
| **测试目的：**  指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）；指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）； |
| **测试配置：** |
| **测试步骤：**  输入IT域异常检测测试样本数据，基于CNN-LSTM模型的识别算法应能够返识别样本的正常及异常状态，且输出异常检测的分类精度。  测试方法：  1.执行python IT/cnn\_lstm.py  2. 输入1或2选择测试数据，1代表全部数据，2代表随机单条数据  预期结果：  算法能够识别正常流量及异常流量，在全部数据测试模式下输出算法分类精确度，在单条数据测试模式下输出数据标签。 |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 166 基于RNN模型的IT流量异常检测算法测试项

|  |
| --- |
| **测试项目：**基于RNN模型的IT流量异常检测算法 |
| **测试依据：** |
| **测试目的：**  指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）；指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）； |
| **测试配置：** |
| **测试步骤：**  输入IT域异常检测测试样本数据，基于RNN模型的识别算法应能够返识别样本的正常及异常状态，且输出异常检测的分类精度。  测试方法：  1.执行python IT/rnn.py  2.输入1或2选择测试数据，1代表全部数据，2代表随机单条数据  预期结果：  算法能够识别正常流量及异常流量，在全部数据测试模式下输出算法分类精确度，在单条数据测试模式下输出数据标签。 |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 167 基于DNN模型的IT流量异常检测算法测试项

|  |
| --- |
| **测试项目：**基于DNN模型的IT流量异常检测算法 |
| **测试依据：** |
| **测试目的：**  指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）；指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）； |
| **测试配置：** |
| **测试步骤：**  输入IT域异常检测测试样本数据，基于DNN模型的识别算法应能够返识别样本的正常及异常状态，且输出异常检测的分类精度。  测试方法：  1.执行python IT/dnn.py  2. 输入1或2选择测试数据，1代表全部数据，2代表随机单条数据  预期结果：  算法能够识别正常流量及异常流量，在全部数据测试模式下输出算法分类精确度，在单条数据测试模式下输出数据标签。 |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 168 基于朴素贝叶斯的IT流量异常检测算法测试项

|  |
| --- |
| **测试项目：**基于朴素贝叶斯的IT流量异常检测算法 |
| **测试依据：** |
| **测试目的：**  指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）；指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）； |
| **测试配置：** |
| **测试步骤：**  输入IT域异常检测测试样本数据，基于朴素贝叶斯模型的识别算法应能够返识别样本的正常及异常状态，且输出异常检测的分类精度。  测试方法：  1. 启动Anaconda Powershell Promt，执行conda activate it，导航到zgcslslog\_IT文件夹下执行python IT/bayes.py  2. 输入1或2选择测试数据，1代表全部数据，2代表随机单条数据  预期结果：  算法能够识别正常流量及异常流量，在全部数据测试模式下输出算法分类精确度，在单条数据测试模式下输出数据标签。 |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 169 基于随机森林的IT流量异常检测算法测试项

|  |
| --- |
| **测试项目：**基于随机森林的IT流量异常检测算法 |
| **测试依据：** |
| **测试目的：**  指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）；指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）； |
| **测试配置：** |
| **测试步骤：**  输入IT域异常检测测试样本数据，基于随机森林模型的识别算法应能够返识别样本的正常及异常状态，且输出异常检测的分类精度。  测试方法：  1. 启动Anaconda Powershell Promt，执行conda activate it，导航到zgcslslog\_IT文件夹下执行python IT/rf.py  2. 输入1或2选择测试数据，1代表全部数据，2代表随机单条数据  预期结果：  算法能够识别正常流量及异常流量，在全部数据测试模式下输出算法分类精确度，在单条数据测试模式下输出数据标签。 |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 170 基于Adaboost模型的IT流异常检测算法测试项

|  |
| --- |
| **测试项目：**基于Adaboost的IT流异常检测算法 |
| **测试依据：** |
| **测试目的：**  指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）；指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）； |
| **测试配置：** |
| **测试步骤：**  输入IT域异常检测测试样本数据，基于Adaboost模型的识别算法应能够返识别样本的正常及异常状态，且输出异常检测的分类精度。  测试方法：  1. 启动Anaconda Powershell Promt，执行conda activate it，导航到zgcslslog\_IT文件夹下执行python IT/adaboost.py  2. 输入1或2选择测试数据，1代表全部数据，2代表随机单条数据  预期结果：  算法能够识别正常流量及异常流量，在全部数据测试模式下输出算法分类精确度，在单条数据测试模式下输出数据标签。 |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 171 基于K近邻的IT流量异常检测算法测试项

|  |
| --- |
| **测试项目：**基于K近邻的IT流量异常检测算法 |
| **测试依据：** |
| **测试目的：**  指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）；指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）； |
| **测试配置：** |
| **测试步骤：**  输入IT域异常检测测试样本数据，基于K近邻模型的识别算法应能够返识别样本的正常及异常状态，且输出异常检测的分类精度。  测试方法：  1. 启动Anaconda Powershell Promt，执行conda activate it，导航到zgcslslog\_IT文件夹下执行python IT/knn.py  2. 输入1或2选择测试数据，1代表全部数据，2代表随机单条数据  预期结果：  算法能够识别正常流量及异常流量，在全部数据测试模式下输出算法分类精确度，在单条数据测试模式下输出数据标签。 |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 172 基于决策树的IT流量异常检测算法测试项

|  |
| --- |
| **测试项目：**基于决策树的IT流量异常检测算法 |
| **测试依据：** |
| **测试目的：**  指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）；指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）； |
| **测试配置：** |
| **测试步骤：**  输入IT域异常检测测试样本数据，基于决策树模型的识别算法应能够返识别样本的正常及异常状态，且输出异常检测的分类精度。  测试方法：  1. 启动Anaconda Powershell Promt，执行conda activate it，导航到zgcslslog\_IT文件夹下执行python IT/dt.py  2. 输入1或2选择测试数据，1代表全部数据，2代表随机单条数据  算法能够识别正常流量及异常流量，在全部数据测试模式下输出算法分类精确度，在单条数据测试模式下输出数据标签。 |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 173 基于LSTM的OT域异常检测算法接口测试项

|  |
| --- |
| **测试项目：**基于LSTM的OT域异常检测算法接口 |
| **测试依据：** |
| **测试目的：**  指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）；指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）； |
| **测试配置：** |
| **测试步骤：**  采用接口测试软件postman向基于LSTM的OT异常检测算法接口发送带有符合接口数据格式的请求后，服务应能够响应该请求并返回JSON格式的异常分类结果。  测试方法：  1.执行python run.py  2.点击postman Collection中的LSTM接口，点击Send  预期结果：  异常检测算法库服务返回状态success及机械臂状态标签，0表示正常状态，1表示异常结果； |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 174 基于增量学习的OT域异常检测算法接口测试项

|  |
| --- |
| **测试项目：**基于增量学习的OT域异常检测算法接口 |
| **测试依据：** |
| **测试目的：**  指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）；指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）； |
| **测试配置：** |
| **测试步骤：**  采用接口测试软件postman向基于增量学习的OT异常检测算法接口发送带有符合接口数据格式的请求后，服务应能够响应该请求并返回JSON格式的异常分类结果。  测试方法：  1.执行python run.py  2.点击postman Collection中的INCREMENTAL接口，点击Send  预期结果：  异常检测算法库服务返回状态success及机械臂状态标签，0表示正常状态，1表示异常结果； |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 175 基于SVM的OT域异常检测算法接口测试项

|  |
| --- |
| **测试项目：**基于增量学习的OT域异常检测算法接口 |
| **测试依据：** |
| **测试目的：**  指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）；指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）； |
| **测试配置：** |
| **测试步骤：**  采用接口测试软件postman向基于SVM的OT异常检测算法接口发送带有符合接口数据格式的请求后，服务应能够响应该请求并返回JSON格式的异常分类结果。  测试方法：  1.执行python run.py  2.点击postman Collection中的SVM接口，点击Send  预期结果：  异常检测算法库服务返回状态success及机械臂状态标签，0表示正常状态，1表示异常结果； |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 176 基于随机树的OT域异常检测算法接口测试项

|  |
| --- |
| **测试项目：**基于随机树的OT域异常检测算法接口 |
| **测试依据：** |
| **测试目的：**  指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）；指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）； |
| **测试配置：** |
| **测试步骤：**  采用接口测试软件postman向基于随机树的OT异常检测算法接口发送带有符合接口数据格式的请求后，服务应能够响应该请求并返回JSON格式的异常分类结果。  测试方法：  1.执行python run.py  2.点击postman Collection中的RANDOMTREE接口，点击Send  预期结果：  异常检测算法库服务返回状态success及机械臂状态标签，0表示正常状态，1表示异常结果； |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 177 基于logistic回归的OT域异常检测算法接口测试项

|  |
| --- |
| **测试项目：**基于增量学习的OT域异常检测算法接口 |
| **测试依据：** |
| **测试目的：**  指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）；指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）； |
| **测试配置：** |
| **测试步骤：**  采用接口测试软件postman向基于logistic回归的OT异常检测算法接口发送带有符合接口数据格式的请求后，服务应能够响应该请求并返回JSON格式的异常分类结果。  测试方法：  1.执行python run.py  2.点击postman Collection中的LOGISTIC接口，点击Send  预期结果：  异常检测算法库服务返回状态success及机械臂状态标签，0表示正常状态，1表示异常结果； |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 178 基于CNN-LSTM的IT流量异常检测算法接口测试项

|  |
| --- |
| **测试项目：**基于CNN-LSTM的IT流量异常检测算法接口 |
| **测试依据：** |
| **测试目的：**  指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）；指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）； |
| **测试配置：** |
| **测试步骤：**  采用接口测试软件postman向基于CNN-LSTM的IT异常检测算法接口发送带有符合接口数据格式的请求后，服务应能够响应该请求并返回JSON格式的异常分类结果。  测试方法：  1.执行python run.py  2.点击postman Collection中的CNN-LSTM接口，点击Send  预期结果：  异常检测算法库服务返回状态success及网络流量状态标签，0表示正常流量，1表示异常流量 |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 179 基于RNN的IT流量异常检测算法接口测试项

|  |
| --- |
| **测试项目：**基于RNN的IT流量异常检测算法接口 |
| **测试依据：** |
| **测试目的：**  指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）；指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）； |
| **测试配置：** |
| **测试步骤：**  采用接口测试软件postman向基于RNN的IT异常检测算法接口发送带有符合接口数据格式的请求后，服务应能够响应该请求并返回JSON格式的异常分类结果。  测试方法：  1.执行python run.py  2.点击postman Collection中的RNN接口，点击Send  预期结果：  异常检测算法库服务返回状态success及网络流量状态标签，0表示正常流量，1表示异常流量 |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 180 基于DNN的IT流量异常检测算法接口测试项

|  |
| --- |
| **测试项目：**基于DNN的IT流量异常检测算法接口 |
| **测试依据：** |
| **测试目的：**  指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）；指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）； |
| **测试配置：** |
| **测试步骤：**  采用接口测试软件postman向基于DNN的IT异常检测算法接口发送带有符合接口数据格式的请求后，服务应能够响应该请求并返回JSON格式的异常分类结果。  测试方法：  1.执行python run.py  2.点postman Collection中的DNN接口，点击Send  预期结果：  异常检测算法库服务返回状态success及网络流量状态标签，0表示正常流量，1表示异常流量 |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 181 基于朴素贝叶斯的IT流量异常检测算法接口测试项

|  |
| --- |
| **测试项目：**基于朴素贝叶斯的IT流量异常检测算法接口 |
| **测试依据：** |
| **测试目的：**  指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）；指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）； |
| **测试配置：** |
| **测试步骤：**  采用接口测试软件postman向基于朴素贝叶斯模型的IT异常检测算法接口发送带有符合接口数据格式的请求后，服务应能够响应该请求并返回JSON格式的异常分类结果。  测试方法：  1. 启动Anaconda Powershell Promt，执行conda activate it，导航到zgcslslog\_IT文件夹下执行python run.py  2.点postman Collection中的BAYES接口，点击Send  异常检测算法库服务返回状态success及网络流量状态标签，0表示正常流量，1表示异常流量 |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 182 基于随机森林的IT流量异常检测算法接口测试项

|  |
| --- |
| **测试项目：**基于随机森林的IT流量异常检测算法接口 |
| **测试依据：** |
| **测试目的：**  指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）；指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）； |
| **测试配置：** |
| **测试步骤：**  采用接口测试软件postman向基于随机森林的IT异常检测算法接口发送带有符合接口数据格式的请求后，服务应能够响应该请求并返回JSON格式的异常分类结果。  测试方法：  1. 启动Anaconda Powershell Promt，执行conda activate it，导航到zgcslslog\_IT文件夹下执行python run.py  2.点postman Collection中的RF接口，点击Send  异常检测算法库服务返回状态success及网络流量状态标签，0表示正常流量，1表示异常流量 |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 183 基于Adaboost的IT流量异常检测算法接口测试项

|  |
| --- |
| **测试项目：**基于Adaboost的IT流量异常检测算法接口 |
| **测试依据：** |
| **测试目的：**  指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）；指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）； |
| **测试配置：** |
| **测试步骤：**  采用接口测试软件postman向基于Adaboost的IT异常检测算法接口发送带有符合接口数据格式的请求后，服务应能够响应该请求并返回JSON格式的异常分类结果。  测试方法：  1. 启动Anaconda Powershell Promt，执行conda activate it，导航到zgcslslog\_IT文件夹下执行python run.py  2.点postman Collection中的ADABOOST接口，点击Send  异常检测算法库服务返回状态success及网络流量状态标签，0表示正常流量，1表示异常流量 |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 184 基于K近邻的IT流量异常检测算法接口测试项

|  |
| --- |
| **测试项目：**基于K近邻的IT流量异常检测算法接口 |
| **测试依据：** |
| **测试目的：**  指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）；指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）； |
| **测试配置：** |
| **测试步骤：**  采用接口测试软件postman向基于K近邻的IT异常检测算法接口发送带有符合接口数据格式的请求后，服务应能够响应该请求并返回JSON格式的异常分类结果。  测试方法：  1. 启动Anaconda Powershell Promt，执行conda activate it，导航到zgcslslog\_IT文件夹下执行python run.py  2.点postman Collection中的KNN接口，点击Send  异常检测算法库服务返回状态success及网络流量状态标签，0表示正常流量，1表示异常流量 |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 185 基于决策树的IT流量异常检测算法接口测试项

|  |
| --- |
| **测试项目：**基于决策树的IT流量异常检测算法接口 |
| **测试依据：** |
| **测试目的：**  指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）；指标3.2：一套智能异常检测与防护算法库并提供应用开发接口：一套智能异常检测与防护算法库并提供应用开发接口（功能性）； |
| **测试配置：** |
| **测试步骤：**  采用接口测试软件postman向基于决策树的IT异常检测算法接口发送带有符合接口数据格式的请求后，服务应能够响应该请求并返回JSON格式的异常分类结果。  测试方法：  1. 启动Anaconda Powershell Promt，执行conda activate it，导航到zgcslslog\_IT文件夹下执行python run.py  2.点postman Collection中的DT接口，点击Send  异常检测算法库服务返回状态success及网络流量状态标签，0表示正常流量，1表示异常流量 |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 186 支持通过工业下游机器设备状态参数测试项

|  |
| --- |
| **测试项目：**支持通过工业下游机器设备状态参数 |
| **测试依据：** |
| **测试目的：**  指标3.3：支撑工业协同安全决策参数不低于30种：支撑工业协同安全决策参数不低于30种，包括但不限于设备安全状态、风险识别、网络和主机行为等（功能性），该项用于测试设备电力、力矩、速度3项决策参数指标3.3：支撑工业协同安全决策参数不低于30种：支撑工业协同安全决策参数不低于30种，包括但不限于设备安全状态、风险识别、网络和主机行为等（功能性），该项用于测试设备电力、力矩、速度3项决策参数 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1.进入机械臂控制界面，打开工程师站笔记本，从桌面进入：/robotsdio2.0.0/win-unpacked/目录下，双击打开robot-pick-studio.exe文件，最大化窗口，点击开始下“所有项目”，选择创建时间未2025-04-16的项目点击打开，左侧栏目机械臂/代码下，双击打开dataTest3.c  2.进入攻击机代码执行界面，在攻击机桌面双击Pycharm，进入后自动进入robot-socket项目，双击左侧“attack1.py”打开攻击代码  3.模拟机械臂正常执行，首先点击客户端右上角上电，观察机械臂是否可正常上电，在代码界面点击右键，点击运行，机械臂开始进行打磨作业，直至打磨任务结束后机械臂复位[check1]  4.再次在工程师站中重复步骤3，使机械臂进入正常运行状态。  5.此时在攻击机的“attack1.py”代码中点击右键运行。机械臂此时被攻击，观察机械臂运行状态中是否发出较为剧烈的异响[check2]  6.测试异常检测与防护效果的功能性，打开工业控制流异常检测与防护模块，在工程师站中再次执行步骤3，此时机械臂进入正常执行状态。此时在攻击机中再次执行步骤5。  7.数据流异常检测模块可以根据机械臂传感器采集的设备电力、力矩、速度决策参数判断机械臂进入异常状态，此时观察机械臂是否被自动停止[check3]  进入工业零信任分布协同安全管控平台，点击顶部菜单栏“异常检测”，点击左侧菜单栏“异常处置”，观察是否出现“机械臂状态参数异常”类型告警，观察异常告警描述是否出现“机械臂正常执行状态下遭受其它客户端调用使能命令导致机械臂异常响动”  预期结果：  系统可检测出设备状态异常，并产生告警，系统调用预定义指令停止传感器工作  [check1]机械臂可以正常上电，且机械臂正常重复执行打磨动作  [check2]发起攻击后，机械臂持续存在剧烈异响，进入异常状态  [check3]机械臂被攻击后立刻停止当前打磨任务和异常动作  [check4]异常处置界面出现“机械臂状态参数异常”类型告警，观察异常告警描述是否出现“机械臂正常执行状态下遭受其它客户端调用使能命令导致机械臂异常响动” |
| **预期结果：**  测试应覆盖以下内容：  1）验证在未开启防护时，机械臂被攻击下会进入异常状态  2）验证开启算法防护后，算法能够通过获取并分析设备的电力、力矩、速度参数进行异常判断  3）验证异常情况发生后，系统能够可视化告警信息并显示 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 187 支持工业协同安全决策参数源IP地址、目的IP地址测试项

|  |
| --- |
| **测试项目：**支持工业协同安全决策参数（网络参数:源IP地址、目的IP地址）Land攻击防范 |
| **测试依据：** |
| **测试目的：**  指标3.3：支撑工业协同安全决策参数不低于30种：支撑工业协同安全决策参数不低于30种，包括但不限于设备安全状态、风险识别、网络和主机行为等（功能性），本项测试用于验证系统支持工业协同安全决策参数，包括网络参数:源IP地址、目的IP地址2项，采用Land攻击防范进行决策参数测试指标3.3：支撑工业协同安全决策参数不低于30种：支撑工业协同安全决策参数不低于30种，包括但不限于设备安全状态、风险识别、网络和主机行为等（功能性），本项测试用于验证系统支持工业协同安全决策参数，包括网络参数:源IP地址、目的IP地址2项，采用Land攻击防范进行决策参数测试 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1.使浏览器输入在测试机打开浏览器，输入https://192.168.10.14，进入工业零信任分布协同安全管控平台。输入用户名:operator\_p，密码Admin@123456，登入防火墙后端  2.进入安全域配置A，添加一条安全域，选择所有接口  3.进入攻击防范-异常报文检测，编辑勾选Land启动检测  4.在攻击机上打开科来数据包播放器，点击添加文件，回放报文“landattack.pcap”  5.使用operator用户登录工业零信任分布协同安全管控平台，进入日志管理-工业防火墙-安全事件检索查看告警日志[check1]  预期结果：  [check 1]产生Land攻击事件告警，告警信息详细中包含解析出来的源ip和目的ip |
| **预期结果：**  测试应覆盖以下内容：  1）验证系统对Land攻击的检测能力。  2）验证系统生成Land攻击告警信息，并能正确解析和显示源IP和目的IP。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 188 支持工业协同安全决策参数测试项

|  |
| --- |
| **测试项目：**支持工业协同安全决策参数（网络参数:连接频率）SYN Flood攻击防范 |
| **测试依据：** |
| **测试目的：**  指标3.3：支撑工业协同安全决策参数不低于30种：支撑工业协同安全决策参数不低于30种，包括但不限于设备安全状态、风险识别、网络和主机行为等（功能性），该项用于测试连接频率决策参数指标3.3：支撑工业协同安全决策参数不低于30种：支撑工业协同安全决策参数不低于30种，包括但不限于设备安全状态、风险识别、网络和主机行为等（功能性），该项用于测试连接频率决策参数 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1. 使用operator\_p用户登录工业零信任分布协同安全管控平台  2. 进入安全域配置A，添加一条安全域，选择所有接口  3. 进入攻击防范-异常流量检测，编辑SYN Flood连接速率阀值5PPS  4. 在攻击机上回放报文synflood.pcap  使用operator用户登录工业零信任分布协同安全管控平台，进入日志管理-工业防火墙-安全事件检索查看告警日志[check 1]  预期结果：  [check1]产生SYN Flood攻击告警，告警详细信息中包含“发生SYN Flood攻击”； |
| **预期结果：**  测试应覆盖以下内容：  1）验证系统对SYN Flood攻击的检测能力。  2）验证系统生成SYN Flood状态告警并记录到日志的功能。。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 189 支持工业协同安全决策参数测试项（网络参数：连接状态、协议类型）

|  |
| --- |
| **测试项目：**支持工业协同安全决策参数（网络参数：连接状态、协议类型） |
| **测试依据：** |
| **测试目的：**  指标3.3：支撑工业协同安全决策参数不低于30种：支撑工业协同安全决策参数不低于30种，包括但不限于设备安全状态、风险识别、网络和主机行为等（功能性），该项用于测试连接状态、协议类型2项决策参数指标3.3：支撑工业协同安全决策参数不低于30种：支撑工业协同安全决策参数不低于30种，包括但不限于设备安全状态、风险识别、网络和主机行为等（功能性），该项用于测试连接状态、协议类型2项决策参数 |
| **测试配置：** |
| **测试步骤：**  测试方法：  参数：连接状态、协议类型  1.使浏览器输入在测试机打开浏览器，输入https://192.168.10.14，进入工业零信任分布协同安全管控平台。输入用户名:operator\_p，密码Admin@123456，登入防火墙后端  2.进入防火墙-防火墙管理-编辑-状态检测，勾选tcp启用。  3.在攻击机上回放报文“tcpztyc.pcap”  4.使用operator用户登录工业零信任分布协同安全管控平台，进入日志管理-工业防火墙-安全事件检索查看告警日志[check1]  预期结果：  [check1] 产生tcp状态事件告警，告警信息详细中包含“tcp状态告警” |
| **预期结果：**  测试应覆盖以下内容：  1）验证系统对TCP状态异常的检测能力。  2）验证系统生成TCP状态告警并记录到日志的功能。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 190 支持工业协同安全决策参数测试项（网络参数：报文长度）

|  |
| --- |
| **测试项目：**支持工业协同安全决策参数（网络参数：报文长度） |
| **测试依据：** |
| **测试目的：**  指标3.3：支撑工业协同安全决策参数不低于30种：支撑工业协同安全决策参数不低于30种，包括但不限于设备安全状态、风险识别、网络和主机行为等（功能性），该项用于测试报文长度决策参数指标3.3：支撑工业协同安全决策参数不低于30种：支撑工业协同安全决策参数不低于30种，包括但不限于设备安全状态、风险识别、网络和主机行为等（功能性），该项用于测试报文长度决策参数 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1.使浏览器输入在测试机打开浏览器，输入https://192.168.10.14，进入工业零信任分布协同安全管控平台。输入用户名:operator\_p，密码Admin@123456，登入防火墙后端  2.进入安全域配置A，添加一条安全域，选择所有接口  3.进入攻击防范-异常报文检测，编辑勾选Ping of Death启动检测  4.在攻击机172.120.1.3 上 ping 192.168.0.99 -t -l 65500  5.使用operator用户登录工业零信任分布协同安全管控平台，进入日志管理-工业防火墙-安全事件检索查看告警日志[check1]  预期结果：  [check1]产生Ping of Death攻击告警，告警详细信息中包含“发生Ping of Death攻击”； |
| **预期结果：**  测试应覆盖以下内容：  1）验证系统对Ping of Death攻击的检测能力。  2）验证系统生成Ping of Death攻击告警并记录到日志的功能。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 191 支持工业协同安全决策参数测试项（网络参数:分片信息）

|  |
| --- |
| **测试项目：**支持工业协同安全决策参数（网络参数:分片信息） |
| **测试依据：** |
| **测试目的：**  指标3.3：支撑工业协同安全决策参数不低于30种：支撑工业协同安全决策参数不低于30种，包括但不限于设备安全状态、风险识别、网络和主机行为等（功能性），该项用于测试分片信息决策参数指标3.3：支撑工业协同安全决策参数不低于30种：支撑工业协同安全决策参数不低于30种，包括但不限于设备安全状态、风险识别、网络和主机行为等（功能性），该项用于测试分片信息决策参数 |
| **测试配置：** |
| **测试步骤：**  测试方法：  参数：分片信息  1.使浏览器输入在测试机打开浏览器，输入https://192.168.10.14，进入工业零信任分布协同安全管控平台。输入用户名:operator\_p，密码Admin@123456，登入防火墙后端  2.进入安全域配置A，添加一条安全域，选择所有接口  3.进入攻击防范-异常报文检测，编辑勾选Teardrop启动检测  4.在攻击机上回放报文teardorp.pcap  5.使用operator用户登录工业零信任分布协同安全管控平台，进入日志管理-工业防火墙-安全事件检索查看告警日志[check1]  预期结果：  [check1]产生Teardrop攻击告警，告警详细信息中包含“发生Teardrop攻击”； |
| **预期结果：**  测试应覆盖以下内容：  1）验证系统根据安全决策参数分片信息对Teardrop攻击的检测能力。  2）验证系统生成Teardrop攻击告警并记录到日志的功能。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 192 支持工业协同安全决策参数测试项（网络参数：报文Flag）

|  |
| --- |
| **测试项目：**支持工业协同安全决策参数（网络参数：报文Flag） |
| **测试依据：** |
| **测试目的：**  指标3.3：支撑工业协同安全决策参数不低于30种：支撑工业协同安全决策参数不低于30种，包括但不限于设备安全状态、风险识别、网络和主机行为等（功能性），该项用于测试报文Flag决策参数指标3.3：支撑工业协同安全决策参数不低于30种：支撑工业协同安全决策参数不低于30种，包括但不限于设备安全状态、风险识别、网络和主机行为等（功能性），该项用于测试报文Flag决策参数 |
| **测试配置：** |
| **测试步骤：**  测试方法：  参数：报文Flag  1.使浏览器输入在测试机打开浏览器，输入https://192.168.10.14，进入工业零信任分布协同安全管控平台。输入用户名:operator\_p，密码Admin@123456，登入防火墙后端  2.进入安全域配置A，添加一条安全域，选择所有接口  3.进入攻击防范-异常报文检测，编辑勾选TCP Flag启动检测  4.在攻击机上回放报文tcpflag.pcap  5.使用operator用户登录工业零信任分布协同安全管控平台，进入日志管理-工业防火墙-安全事件检索查看告警日志[check1]  预期结果：  [check1]产生TCP Flag攻击告警，告警详细信息中包含“发生TCP Flag攻击”； |
| **预期结果：**  测试应覆盖以下内容：  1）验证系统对TCP Flag攻击的检测能力。  2）验证系统生成TCP Flag攻击告警并记录到日志的功能。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 193 工业协同安全决策参数测试项（网络参数：上行报文数、下行报文数、上行字节数、下行字节数）

|  |
| --- |
| **测试项目：**支持工业协同安全决策参数（网络参数：上行报文数、下行报文数、上行字节数、下行字节数） |
| **测试依据：** |
| **测试目的：**  指标3.3：支撑工业协同安全决策参数不低于30种：支撑工业协同安全决策参数不低于30种，包括但不限于设备安全状态、风险识别、网络和主机行为等（功能性）配置好监测对象和流量监测模板，按相应的源IP和目的IP构造流量报文，发送超阈值的上行报文数、下行报文数、上行字节数、下行字节数相关字段。指标3.3：支撑工业协同安全决策参数不低于30种：支撑工业协同安全决策参数不低于30种，包括但不限于设备安全状态、风险识别、网络和主机行为等（功能性）配置好监测对象和流量监测模板，按相应的源IP和目的IP构造流量报文，发送超阈值的上行报文数、下行报文数、上行字节数、下行字节数相关字段。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1.使浏览器输入在测试机打开浏览器，输入https://192.168.10.14，进入工业零信任分布协同安全管控平台。输入用户名:operator\_p，密码Admin@123456，登入防火墙后端  2.进入防火墙-对象配置-监测对象，添加一条监控对象all，源地址目的地址都选择any，服务选择ALL  3.进入防火墙-流量监控，添加一条流量监控模版A,点击编辑，配置监控对象为ALL,选择执行动作为告警，在告警阈值点击配置，选择流量大小行，将上行流量报文数设置为10pps  4.在攻击机172.120.1.3 上 访问 ftp://192.168.0.100，去下载一个大文件  5.使用operator用户工业零信任分布协同安全管控平台，进入日志管理-工业防火墙-安全事件检索查看告警日志[check1]  6.修改步骤3中的流量监控模版，将下行报文数10pps，其他全为0，重复步骤4,5[check2]  7.修改步骤3中的流量监控模版，将上行字节数10Kbps，其他全为0，重复步骤4,5[check3]  8.修改步骤3中的流量监控模版，将下行字节数10Kbps，其他全为0，重复步骤4,5[check4]  预期结果：  [check1]产生流量阀值告警，告警详细信息中包含“上行流量报文超阈值”；  [check2]产生流量阀值告警，告警详细信息中包含“下行流量报文超阈值”；  [check3]产生流量阀值告警，告警详细信息中包含“上行流量字节超阈值”；  [check4]产生流量阀值告警，告警详细信息中包含“下行流量字节超阀值”； |
| **预期结果：**  测试应覆盖以下内容：  1）验证系统对上行报文数和下行报文数异常的检测能力。  2）验证系统对上行字节数和下行字节数异常的检测能力。  3）验证系统在流量超出阈值时生成告警并记录到日志的功能。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 194 支持工业协同安全决策参数测试项（工业网络S7协议参数：寄存器区、功能码、DB区区号、点类型、值域内容）

|  |
| --- |
| **测试项目：**支持工业协同安全决策参数（工业网络S7协议参数：寄存器区、功能码、DB区区号、点类型、值域内容） |
| **测试依据：** |
| **测试目的：**  指标3.3：支撑工业协同安全决策参数不低于30种：支撑工业协同安全决策参数不低于30种，包括但不限于设备安全状态、风险识别、网络和主机行为等（功能性），该项用于测试工业网络S7协议参数：寄存器区、功能码、DB区区号、点类型、值域内容决策参数指标3.3：支撑工业协同安全决策参数不低于30种：支撑工业协同安全决策参数不低于30种，包括但不限于设备安全状态、风险识别、网络和主机行为等（功能性），该项用于测试工业网络S7协议参数：寄存器区、功能码、DB区区号、点类型、值域内容决策参数 |
| **测试配置：** |
| **测试步骤：**  测试方法：  配置好S7白名单策略，构造不符合白名单的S7协议报文，比如寄存器区、功能码、DB区区号、点类型、值域内容不符合要求。  1) 浏览器输入https://192.168.10.14，进入工业零信任分布协同安全管控平台。输入用户名:operator\_p，密码Admin@123456，登入防火墙后端  2) 进入防火墙配置修改，工作模式修改为学习模式  3) 使用科来回放报文工具，回放报文s7.pcap；  4) 进入防火墙，点击防火墙工作模式下面的学习模式，会跳转到学习数据页面检查s7是否学习到白名单[check1]  5) 配置防火墙为学习完成，并生成白名单模版A  6) 配置防火墙为防护模式，并应用白名单模版A  7) 再次回放报文s7.pcap [check2]  8) 修改白名单模版的任一字段  9) 再次回放报文s7.pcap [check3]  预期结果：  • 系统可检测/阻断出网络异常报文，可生成查看到相应的告警  [check1]有学习到白名单，学习内容和报文内容一致，源地址1.251.251.101目的地址16.16.16.34  [check2]不会产生白名单告警，白名单有命中计数  [check3]会产生白名单告警，报警内容“违反S7白名单规则告警,写寄存器区DB区,DB区区号(0),点类型(S7WLByte)起始地址(0),结束地址(127)” |
| **预期结果：**  测试应覆盖以下内容：  1）验证工业网络S7协议白名单的学习功能。  2）验证S7白名单策略在防护模式下对符合规则报文的放行能力。  3）验证S7白名单策略对不符合规则报文（如非法写寄存器区）的检测和告警能力。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 195 支持工业网络协议Modbus特有参数测试项

|  |
| --- |
| **测试项目：**支持工业网络协议Modbus特有参数 |
| **测试依据：** |
| **测试目的：**  指标3.3：支撑工业协同安全决策参数不低于30种：支撑工业协同安全决策参数不低于30种，包括但不限于设备安全状态、风险识别、网络和主机行为等（功能性）该项用于测试工业网络Modbus协议功能码、值域内容、起始地址、结束地址值决策参数指标3.3：支撑工业协同安全决策参数不低于30种：支撑工业协同安全决策参数不低于30种，包括但不限于设备安全状态、风险识别、网络和主机行为等（功能性）该项用于测试工业网络Modbus协议功能码、值域内容、起始地址、结束地址值决策参数 |
| **测试配置：** |
| **测试步骤：**  测试工业零信任分布协同管控平台是否能使用白名单策略，根据Modbus协议功能码、值域内容、起始地址、结束地址值项参数判断异常报文  测试方法：  配置好Modbus白名单策略，构造不符合白名单的Modbus协议报文，比如功能码、值域内容、起始地址、结束地址不符合要求  1）浏览器输入https://192.168.10.14，进入工业零信任分布协同安全管控平台。输入用户名:operator\_p，密码Admin@123456，登入防火墙后端  2）进入防火墙配置修改，工作模式修改为学习模式  3）使用科来回放报文工具，回放附件中报文modbus.pcap  4）进入防火墙，点击防火墙工作模式下面的学习模式，会跳转到学习数据页面检查modbus是否学习到白名单[check1]  5）配置防火墙为学习完成，并生成白名单模版A  6）配置防火墙为防护模式，并应用白名单模版A  7）再次回放报文modbus.pcap [check2]  8）修改白名单模版的任一字段  9）再次回放报文modbus.pcap [check3]  预期结果：  • 系统可检测/阻断出网络异常报文，可生成查看到相应的告警  预期结果：  [check1]有学习到白名单，学习内容和报文内容一致，源地址1.251.251.101目的地址16.16.16.34  [check2]不会产生白名单告警，白名单有命中计数  [check3]会产生白名单告警，报警内容“违反MODBUS白名单规则告警功能码03 Read Holding Registers起始地址100结束地址199” |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 196支持工业协同安全决策参数测试项（用户参数：用户操作系统）

|  |
| --- |
| **测试项目：**支持工业协同安全决策参数（用户参数：用户操作系统） |
| **测试依据：** |
| **测试目的：**  指标3.3：支撑工业协同安全决策参数不低于30种：支撑工业协同安全决策参数不低于30种，包括但不限于设备安全状态、风险识别、网络和主机行为等（功能性），该项用于测试用户操作系统决策参数指标3.3：支撑工业协同安全决策参数不低于30种：支撑工业协同安全决策参数不低于30种，包括但不限于设备安全状态、风险识别、网络和主机行为等（功能性），该项用于测试用户操作系统决策参数 |
| **测试配置：** |
| **测试步骤：**  系统应能够设置允许访问应用的用户所使用主机的操作系统，当用户采用非允许操作系统的主机登录零信任桌面客户端时会被拒绝  测试方法：  1）打开零信任访问控制桌面客户端并登录，点击零信安全访问控制任进入进行登录，用户名为zhanggq，密码为：zgq26717  2）点击零信任策略中心，点击基本级策略，点击添加，选择类型为系统版本不满足，动作为禁止登录，点击确定  3）点击零信任策略中心，点击环境库，选择操作系统项，设置Windows操作系统版本为11；  4）零信任管理平台应通过用户操作系统决策参数判断该用户是否可登录  5）使用装有Windows11的测试机器登录桌面零信任客户端  6）观察用户是否被允许登录，观察是否可访问相应的引用；[check1]  7）使用装有Windows10的测试机器登录桌面零信任客户端  8）观察用户是否被允许登录，观察是否可登录，进入零信任访问控制平台，点击日志中心，点击安全日志，观察是否存在“操作系统版本不满足告警”[check2]  预期结果：  [check1]正常登录  [check2]可以看到测试机用户被拒绝登录，进入零信任访问控制平台中，点击日志中心，点击行为日志，点击访问控制日志，可以看到“操作系统版本不满足告警”。 |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 197支持工业协同安全决策参数测试项（用户参数：用户IP地址）

|  |
| --- |
| **测试项目：**支持工业协同安全决策参数（用户参数：用户IP地址） |
| **测试依据：** |
| **测试目的：**  指标3.3：支撑工业协同安全决策参数不低于30种：支撑工业协同安全决策参数不低于30种，包括但不限于设备安全状态、风险识别、网络和主机行为等（功能性），该项用于测试用户IP地址决策参数指标3.3：支撑工业协同安全决策参数不低于30种：支撑工业协同安全决策参数不低于30种，包括但不限于设备安全状态、风险识别、网络和主机行为等（功能性），该项用于测试用户IP地址决策参数 |
| **测试配置：** |
| **测试步骤：**  零信任访问控制系统应能够设置访问应用的白名单IP，通过白名单策略限制非白名单用户登录系统访问应用。  测试方法：  1） 使用管理员账户登录零信安全访问控制平台： https://192.168.10.10，用户名：admin，密码：Admin@123  2）在菜单栏点击系统设置，点击系统运维，点击系统设置  2） 在访问设置IP白名单中输入可信IP:“192.168.10.111/32”  3） 使用测试机器，zhanggq，密码：zgq26717，登录ZGC零信任桌面客户端，零信任管理平台应通过用户操作系统决策参数判断该用户被拒绝登录  5） 观察用户是否被允许登录，观察是否可访问相应的引用[check1]  6） 配置测试访问主机IP为: 192.168.10.111，并使用测试机器使用zhanggq用户访问零信任访问零信任访问控制系统，或者登录零信任桌面客户端，密码为zgq26717，观察用户是否被允许登录，观察是否可访问相应的引用[check2]  预期结果：  [check1]可以看到测试机用户被拒绝登录，进入零信任访问控制平台中，点击日志中心，点击行为日志，点击访问控制日志，可以看到 192.168.10.123 用户被阻止接入。  [check2]正常登录 |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 198支持工业协同安全决策参数测试项（用户参数：工作时间）

|  |
| --- |
| **测试项目：**支持工业协同安全决策参数（用户参数：工作时间） |
| **测试依据：** |
| **测试目的：**  指标3.3：支撑工业协同安全决策参数不低于30种：支撑工业协同安全决策参数不低于30种，包括但不限于设备安全状态、风险识别、网络和主机行为等（功能性），该项用于测试用户参数：工作时间指标3.3：支撑工业协同安全决策参数不低于30种：支撑工业协同安全决策参数不低于30种，包括但不限于设备安全状态、风险识别、网络和主机行为等（功能性），该项用于测试用户参数：工作时间 |
| **测试配置：** |
| **测试步骤：**  系统应能够通过设置零信任桌面客户端入口应用的访问时间，当用户在非允许访问时间尝试访问应用时应被拒绝  测试方法：  1) 打开零信任访问控制桌面客户端并登录，点击零信安全访问控制任进入进行登录，用户名为zhanggq，密码为：zgq26717  2) 点击零信任策略中心，点击时间段管理，点击工作时间修改，选择工作时间包含当前测试时间  3) 零信任管理平台应通过用户工作时间决策参数判断该用户是否可登录  4) 采用测试机器在所设置工作时间段内登录桌面零信任客户端，点击工业零信任分布协同安全管控平台应用进入应用  5) 观察用户是否被允许登录，是否可以访问工业零信任分布协同安全管控平台应用[check1]  6) 点击零信任策略中心，点击时间段管理，点击工作时间修改，修改工作时间包含当前测试时间之外  7) 采用测试机器在所设置工作时间段内登录桌面零信任客户端，点击工业零信任分布协同安全管控平台应用进入应用  8) 观察用户是否被允许登录，进入零信任访问控制平台，点击日志中心，点击安全日志，观察是否存在“非工作时间登录告警”[check2]  预期结果：  [check1]正常登录，可以正藏访问工业零信任分布协同安全管控平台应用  [check2]可以看到测试用户无法访问工业零信任分布协同安全管控平台应用，进入零信任访问控制平台中，点击日志中心，点击行为日志，点击访问控制日志，可以看到“非工作时间登录”告警。 |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 199 支持工业协同安全决策参数测试项（主机参数：CPU异常）

|  |
| --- |
| **测试项目：**支持工业协同安全决策参数（主机参数：CPU异常） |
| **测试依据：** |
| **测试目的：**  指标3.3：支撑工业协同安全决策参数不低于30种：支撑工业协同安全决策参数不低于30种，包括但不限于设备安全状态、风险识别、网络和主机行为等（功能性），该项用于测试主机CPU异常决策参数指标3.3：支撑工业协同安全决策参数不低于30种：支撑工业协同安全决策参数不低于30种，包括但不限于设备安全状态、风险识别、网络和主机行为等（功能性），该项用于测试主机CPU异常决策参数 |
| **测试配置：** |
| **测试步骤：**  系统应能够通过设置登录主机CPU使用异常阈值，当域内主机磁盘倍攻击等情况造成CPU使用异常时系统能够检测并发出告警  测试方法：  1) 浏览器输入https://192.168.10.14，进入工业零信任分布协同安全管控平台。输入用户名:operator，密码Admin@123456  2) 点击顶部菜单栏策略中心，点击进入终端策略页面；  3) 选择目标终端操作列，点击配置，进入常规设置页，勾选开启 操作系统资源告警，设置 CPU 20% ，点击应用，下发策略；  预期结果：  使用operator用户登录工业零信任分布协同安全管控平台，点击异常检测->异常处置，可以看到产生资产内存使用超标告警 |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 200 支持工业协同安全决策参数测试项（主机参数：资产内存异常）

|  |
| --- |
| **测试项目：**支持工业协同安全决策参数（主机参数：资产内存异常） |
| **测试依据：** |
| **测试目的：**  指标3.3：支撑工业协同安全决策参数不低于30种：支撑工业协同安全决策参数不低于30种，包括但不限于设备安全状态、风险识别、网络和主机行为等（功能性），该项用于测试主机资产内存异常决策参数指标3.3：支撑工业协同安全决策参数不低于30种：支撑工业协同安全决策参数不低于30种，包括但不限于设备安全状态、风险识别、网络和主机行为等（功能性），该项用于测试主机资产内存异常决策参数 |
| **测试配置：** |
| **测试步骤：**  系统应能够通过设置登录主机内存使用异常阈值，当域内主机磁盘倍攻击等情况造成内存使用异常时系统能够检测并发出告警  测试方法：  1) 浏览器输入https://192.168.10.14，进入工业零信任分布协同安全管控平台。输入用户名:operator，密码Admin@123456  2) 点击顶部菜单栏策略中心，点击进入终端策略页面；  3) 选择目标终端操作列，点击配置，进入常规设置页，勾选开启 操作系统资源告警，设置内存20% ，点击应用，下发策略；  4) 查看异常处置界面是否出现告警[check1]  预期结果：  [check1]使用operator用户登录工业零信任分布协同安全管控平台，点击异常检测，异常处置，可以看到产生资产内存使用率超标告警 |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 201 支持工业协同安全决策参数测试项（主机参数：磁盘异常）

|  |
| --- |
| **测试项目：**支持工业协同安全决策参数（主机参数：磁盘异常） |
| **测试依据：** |
| **测试目的：**  指标3.3：支撑工业协同安全决策参数不低于30种：支撑工业协同安全决策参数不低于30种，包括但不限于设备安全状态、风险识别、网络和主机行为等（功能性），该项用于测试主机磁盘异常决策参数指标3.3：支撑工业协同安全决策参数不低于30种：支撑工业协同安全决策参数不低于30种，包括但不限于设备安全状态、风险识别、网络和主机行为等（功能性），该项用于测试主机磁盘异常决策参数 |
| **测试配置：** |
| **测试步骤：**  系统应能够通过设置登录主机磁盘使用异常阈值，当域内主机磁盘倍攻击等情况造成磁盘使用异常时系统能够检测并发出告警  测试方法：  1) 浏览器输入https://192.168.10.14，进入工业零信任分布协同安全管控平台。输入用户名:operator，密码Admin@123456  2) 点击顶部菜单栏策略中心，点击进入终端策略页面；  3) 选择目标终端操作列，点击配置，进入常规设置页，勾选开启 操作系统资源告警，设置磁盘10% ，点击应用，下发策略；  预期结果：  使用operator用户登录工业零信任分布协同安全管控平台，点击异常检测->异常处置，可以看到产生资产磁盘使用率超标告警 |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 202 支持用户登陆地点决策参数测试项

|  |
| --- |
| **测试项目：**支持用户登陆地点决策参数 |
| **测试依据：** |
| **测试目的：**  指标3.3：支撑工业协同安全决策参数不低于30种：支撑工业协同安全决策参数不低于30种，包括但不限于设备安全状态、风险识别、网络和主机行为等（功能性），该项用于测试用户登录地点决策参数指标3.3：支撑工业协同安全决策参数不低于30种：支撑工业协同安全决策参数不低于30种，包括但不限于设备安全状态、风险识别、网络和主机行为等（功能性），该项用于测试用户登录地点决策参数 |
| **测试配置：** |
| **测试步骤：**  采用正常账户在非常用地点登录零信任桌面客户端，验证系统是否能够通过用户登录地点异常发出告警  测试方法：  1）配置测试登录机IP地点为非常用地区，并连接国外VPN；  2）在测试机使用zhanggq账号访问ZGC零信任桌面客户端，密码为zgq26717；工业零信任分布协同安全管控平台能够根据用户登陆地点判断用户行为异常;  4) 通过ZGC零信任客户端访问零信任访问控制平台管理端，使用管理员账户进行登录，用户名：admin，密码：Admin@123，点击日志中心，点击安全日志，观察是否出现“访问控制发出地不在常见地区”告警[check1]  预期结果：  [check1]零信任访问控制系统的安全日志界面，出现“访问控制发出地不在常见地区”告警 |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 203 支持主机风险识别参数是否安装杀毒软件测试项

|  |
| --- |
| **测试项目：**支持主机风险识别参数是否安装杀毒软件 |
| **测试依据：** |
| **测试目的：**  指标3.3：支撑工业协同安全决策参数不低于30种：支撑工业协同安全决策参数不低于30种，包括但不限于设备安全状态、风险识别、网络和主机行为等（功能性），该项用于测试支持主机风险识别参数是否安装杀毒软件测试项指标3.3：支撑工业协同安全决策参数不低于30种：支撑工业协同安全决策参数不低于30种，包括但不限于设备安全状态、风险识别、网络和主机行为等（功能性），该项用于测试支持主机风险识别参数是否安装杀毒软件测试项 |
| **测试配置：** |
| **测试步骤：**  采用正常账户在未安装杀毒软件的主机登录零信任桌面客户端，验证系统是否能够通过检测用户是否安装杀毒软件决策参数项异常发出告警  测试方法：  1）登录零信安全访问控制任进入，点击零信任策略中心，点击零信任安全策略，修改基本级策略，点击添加，选择类型为是否安装杀毒软件，动作为禁止登录，点击确定  2）点击零信任策略中心，点击环境库，选择杀毒软件项，设置检测杀毒软件为火绒；  3）零信任管理平台应通过用户是否安装杀毒软件决策参数判断该用户是否可登录  4）使用装有火绒杀毒软件的测试机器登录桌面零信任客户端  5）观察用户是否被允许登录，观察是否可访问相应的引用；[check1]  6）使用未装杀毒软件的测试机器登录桌面零信任客户端  7）观察用户是否被允许登录，观察是否可登录，进入零信任访问控制平台，点击日志中心，点击安全日志，观察是否存在“用户未安装杀毒软件”告警[check2]  预期结果：  [check 1]客户端可以正常登录；  [check 2]客户端无法登录，客户端提示“客户端存在安全风险，禁止登录”，零信任访问控制平台安全日志可查看告警记录，显示风险类型为“未安装杀毒软件”； |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 204 支持主机风险识别参数是否安装远控软件测试项

|  |
| --- |
| **测试项目：**支持主机风险识别参数是否安装远控软件 |
| **测试依据：** |
| **测试目的：**  指标3.3：支撑工业协同安全决策参数不低于30种：支撑工业协同安全决策参数不低于30种，包括但不限于设备安全状态、风险识别、网络和主机行为等（功能性），该项用于测试支持主机风险识别参数是否安装远程控制软件测试项指标3.3：支撑工业协同安全决策参数不低于30种：支撑工业协同安全决策参数不低于30种，包括但不限于设备安全状态、风险识别、网络和主机行为等（功能性），该项用于测试支持主机风险识别参数是否安装远程控制软件测试项 |
| **测试配置：** |
| **测试步骤：**  采用正常账户在安装远控软件的情况下登录零信任桌面客户端访问应用，验证系统是否能够通过用户是否安装远程控制软件发出告警  测试方法：  1）登录零信安全访问控制任进入，点击零信任策略中心，点击零信任安全策略，修改基本级策略，点击添加，选择类型为是否安装远控软件，动作为禁止登录，点击确定  2）点击零信任策略中心，点击环境库，选择远程控制软件项，设置检测远控软件为向日葵；  3）零信任管理平台应通过用户是否安装否安装远程控制软件决策参数判断该用户是否可登录  4）使用装有远程控制的测试机器登录桌面零信任客户端  5）观察用户是否被允许登录，观察是否可访问相应的引用进入零信任访问控制平台，点击日志中心，点击安全日志，观察是否存在“用户安装远控软件”告警；[check1]  6）使用未装远控软件的测试机器登录桌面零信任客户端  7）观察用户是否被允许登录，观察是否可登录 [check2]  预期结果：  [check 1]客户端无法登录，客户端提示“客户端存在安全风险，禁止登录”，零信任访问控制平台安全日志可查看告警记录，显示风险类型为“安装远控软件”；  [check 2]客户端不可可以正常登录； |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 205 支持主机风险识别参数是否开启防火墙测试项

|  |
| --- |
| **测试项目：**支持主机风险识别参数是否开启防火墙 |
| **测试依据：** |
| **测试目的：**  指标3.3：支撑工业协同安全决策参数不低于30种：支撑工业协同安全决策参数不低于30种，包括但不限于设备安全状态、风险识别、网络和主机行为等（功能性），该项用于测试支持主机风险识别参数是否开启防火墙指标3.3：支撑工业协同安全决策参数不低于30种：支撑工业协同安全决策参数不低于30种，包括但不限于设备安全状态、风险识别、网络和主机行为等（功能性），该项用于测试支持主机风险识别参数是否开启防火墙 |
| **测试配置：** |
| **测试步骤：**  采用正常账户在未开启防火墙的情况下登录零信任桌面客户端访问应用，验证系统是否能够通过用户是否安装远程控制软件发出告警  测试方法：  1）登录零信安全访问控制任进入，点击零信任策略中心，点击零信任安全策略，修改基本级策略，点击添加，选择类型为是否开启系统防火墙，动作为禁止登录，点击确定  2）零信任管理平台应通过用户是否安装杀毒软件决策参数判断该用户是否可登录  3）测试机器进入控制面板->系统和安全->Windows Defender 防火墙->启用或关闭Windows Defender 防火墙，关闭所有防火墙。  4）登录桌面零信任客户端，用户名zhanggq,密码 zgq26717。  5）观察用户是否被允许登录；[check1]  6）测试机器进入控制面板->系统和安全->Windows Defender 防火墙->启用或关闭Windows Defender 防火墙，开启所有防火墙。  7）观察用户是否被允许登录，观察是否可登录，进入零信任访问控制平台，点击日志中心，点击安全日志，观察是否存在“用户未开启防火墙”告警[check2]  预期结果：  [check 1]客户端可以正常登录；  [check 2]客户端无法登录，客户端提示“客户端存在安全风险，禁止登录”，零信任访问控制平台安全日志可查看告警记录，显示风险类型为“未开启防火墙”； |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 206 网络资产管理功能测试项

|  |
| --- |
| **测试项目：**网络资产管理功能 |
| **测试依据：** |
| **测试目的：**  指标:3.4：支持多种工业网络资产管理功能：网络资产及拓扑结构探测支持主流网络协议不少于5种（功能性）；指标:3.4：支持多种工业网络资产管理功能：网络资产及拓扑结构探测支持主流网络协议不少于5种（功能性）； |
| **测试配置：** |
| **测试步骤：**  工业零信任分布协同安全管控平台应具备资产管理功能，系统应能显示当前网络的所有资产及其详细信息  测试方法：  1.使用operator用户登录工业零信任分布协同安全管控平台https://192.168.10.15:8440，用户名：operator，密码：Admin@123456，点击工业资产管理-资产管理-已确认资产菜单[check1]  2.点击test资产网格[check2]  预期结果：  [check1]以网格形式显示已确认资产的资产名称、设备IP、告警总数、设备状态  [check2]跳转到test资产画像页面，显示资产名称、设备IP、设备MAC、设备类型、操作系统、漏洞信息等 |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 207 网络资产探测功能测试项

|  |
| --- |
| **测试项目：**网络资产探测功能 |
| **测试依据：** |
| **测试目的：**  指标:3.4：支持多种工业网络资产管理功能：网络资产及拓扑结构探测支持主流网络协议不少于5种（功能性）；指标:3.4：支持多种工业网络资产管理功能：网络资产及拓扑结构探测支持主流网络协议不少于5种（功能性）； |
| **测试配置：** |
| **测试步骤：**  测试方法：  1.使用operator用户登录工业零信任分布协同安全管控平台，点击顶部菜单栏工业资产管理，点击左侧菜单栏资产管理，点击主动资产发现[check1]  2.点击<扫描配置>，选择进行扫描的网口，点击确定[check2]  3.点击<任务列表>，点击<新增>按钮[check3]  4.输入任务名称：扫描OT域工程师站，需要扫描的IP网段:192.168.0.100，扫描速度：高，所属区域：Area-A/Area-default，其余默认，点击确定[check4]  5.系统主页点击资产中心-资产管理-未确认资产[check5]  6.点击一个未确认资产的设备名称[check5]  预期结果：  [check1]跳转到任务列表页面，可以进行资产扫描任务  [check2]提示操作成功  [check3]弹出新增任务弹窗，可以输入任务名称、地址范围、TCP端口、UDP端口，可以选择执行方式、执行周期、扫描速度，所属区域  [check4]列表中新增一条正在扫描的任务“扫描OT域工程师站”，等待状态变为扫描完成后，点击扫描结果，可以查看扫描IP范围内所以扫描到的资产  [check5]显示主动或被动发现的资产  [check6]跳转到资产画像页面，显示未确认资产的设备名称、设备IP、设备MAC、设备类型、操作系统、漏洞信息等 |
| **预期结果：**  测试应覆盖以下内容：  1）工业零信任分布协同安全管控平台应能够进行主动的资产发现  2）对未被计入平台资产管理的主机IP扫描，应能够探测到该资产 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 208 未知设备接入检测功能测试项

|  |
| --- |
| **测试项目：**未知设备接入检测功能 |
| **测试依据：** |
| **测试目的：**  指标:3.4：支持多种工业网络资产管理功能：网络资产及拓扑结构探测支持主流网络协议不少于5种（功能性）；指标:3.4：支持多种工业网络资产管理功能：网络资产及拓扑结构探测支持主流网络协议不少于5种（功能性）； |
| **测试配置：** |
| **测试步骤：**  开启工业零信任分布协同安全管控平台的资产被动发现开关，采用udpSend配测软件模拟未知资产接入网络过程，观察系统是否可以产生告警  测试方法：  1）使用operator用户登录工业零信任分布协同安全管控平台，点击工业资产管理-资产管理-被动资产发现；[check1]  2）开启“是否启用资产发现”开关、开启“开启告警”开关；[check2]  3）在ZGQ测试机进入E:\北航项目\中关村实验室项目\第三方测试ZGQ测试机脚本及用例\网络资产相关目录，打开udpSend工具；  4）发送一次syslog日志(网络会话日志) ，输入IP：192.168.10.15，端口输入514，点击添加；上传文件，选择网络会话日志，点击发送。（发送含有未确认资产的网络会话日志，）  5）查看资产中心-资产管理-未确认资产[check3]  6）点击告警管理-告警处置[check4]  预期结果：  [check1]页面显示启用资产发现开关、开启告警开关、告警判断依据  [check2]提示操作成功  [check3]可以查看到网络会话中的未确认资产  [check4]可以查看到未知设备接入告警 |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 209 自动探测网络拓扑并生成拓扑图测试项

|  |
| --- |
| **测试项目：**网络拓扑结构功能 |
| **测试依据：** |
| **测试目的：**  指标:3.4：支持多种工业网络资产管理功能：网络资产及拓扑结构探测支持主流网络协议不少于5种（功能性）；指标:3.4：支持多种工业网络资产管理功能：网络资产及拓扑结构探测支持主流网络协议不少于5种（功能性）； |
| **测试配置：** |
| **测试步骤：**  工业零信任分布协同安全管控平台应包含工业资产管理模块，该模块应具备拓扑结构的自动化扫描功能，能够自动生成当前网络资产拓扑图，探测各个资产之间的网络连接关系  测试方法：  1）打开工业零信任分布协同安全管控平台，输入账号：operator，密码：Admin@123456，登入该平台[check 1]；  2）在上方菜单栏点击“工业资产管理”；  3）点击右侧“拓扑管理-我的拓扑”  4）点击“拓扑结构探测”[check 2]；  5）选择当前时间下最新版本拓扑结构，进行查看  预期结果：  [check 1] 登入管控平台，显示该平台界面  [check 2] 界面显示“正在进行拓扑结构探测，请耐心等待！”  生成当前的网络资产拓扑结构图，可查看资产拓扑图。 |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 210 网络拓扑结构绘制测试项

|  |
| --- |
| **测试项目：**网络拓扑结构功能 |
| **测试依据：** |
| **测试目的：**  指标:3.4：支持多种工业网络资产管理功能：网络资产及拓扑结构探测支持主流网络协议不少于5种（功能性）；指标:3.4：支持多种工业网络资产管理功能：网络资产及拓扑结构探测支持主流网络协议不少于5种（功能性）； |
| **测试配置：** |
| **测试步骤：**  工业零信任分布协同安全管控平台应包含工业资产管理模块，该模块应具备网络资产拓扑图的手动绘制功能，且能够在可视化工具显示  测试方法：  1.使用operator用户登录工业零信任分布协同安全管控平台，进入资产中心-拓扑管理-我的拓扑[check1]  2.点击新增按钮，不使用模板[check2]  3.任意编辑后点击上方保存按钮，输入拓扑图名称：test11后再次点击保存[check3]  4.点击资产中心-拓扑管理-我的拓扑[check 4]  点击test拓扑图操作列的查看按钮[check 5]  预期结果：  [check 1]页面显示已创建的拓扑图，可以进行编辑、查看等操作  [check 2]进入拓扑图编辑页面  [check 3]拓扑图保存成功  [check 4]可以查看到新增的拓扑图test111  [check 5]显示刚刚新建的拓扑图内容 |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 211 支持以太网S7协议测试项

|  |
| --- |
| **测试项目：**支持以太网S7协议 |
| **测试依据：** |
| **测试目的：**  指标:3.4：支持多种工业网络资产管理功能：网络资产及拓扑结构探测支持主流网络协议不少于5种（功能性）；指标:3.4：支持多种工业网络资产管理功能：网络资产及拓扑结构探测支持主流网络协议不少于5种（功能性）； |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）使用operator用户登录工业零信任分布协同安全管控平台，进入资产中心-资产管理-主动资产发现[check 1]  2）点击<扫描配置>，选择进行扫描的网口，点击确定[check 2]  3）点击<任务列表>，点击<新增>按钮[check 3]  4）输入任务名称：S7，地址范围输入以S7协议接入的设备IP为:192.168.0.204，TCP端口：102,UDP端口：空，扫描速度：高，所属区域：Area-A/Area-default，其余默认，点击确定[check 4]  5）进入资产中心-资产管理-未确认资产菜单，点击刚刚扫到的S7协议资产的设备名称，进入资产画像页面，点击网络检测-端口信息[check 5]  预期结果：  [check 1]跳转到任务列表页面，可以进行资产扫描任务  [check 2]提示操作成功  [check 3]弹出新增任务弹窗，可以输入任务名称、地址范围、TCP端口、UDP端口，可以选择执行方式、执行周期、扫描速度，所属区域  [check 4]列表中新增一条正在扫描的任务S7，等待状态变为扫描完成后，点击扫描结果，可以查看到以S7协议接入的资产信息  [check 5]查看服务为S7协议 |
| **预期结果：**  测试应覆盖以下内容：  1）在测试环境网络接入采用S7协议通信的西门子S7 1500 PLC至OT域交换机  2）在工业零信任分布协同安全管控平台执行主动资产发现，观察是否可以扫描到使用S7工业通信协议的西门子PLC |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 212支持Modbus协议测试项

|  |
| --- |
| **测试项目：**支持Modbus协议 |
| **测试依据：** |
| **测试目的：**  指标:3.4：支持多种工业网络资产管理功能：网络资产及拓扑结构探测支持主流网络协议不少于5种（功能性）；指标:3.4：支持多种工业网络资产管理功能：网络资产及拓扑结构探测支持主流网络协议不少于5种（功能性）； |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）使用operator用户登录工业零信任分布协同安全管控平台，进入资产中心-资产管理-主动资产发现[check 1]  2）点击<扫描配置>，选择进行扫描的网口，点击确定[check2]  3）点击<任务列表>，点击<新增>按钮[check3]  4）输入任务名称：Modbus，地址范围输入以Modbus协议接入的设备IP：192.168.0.160，TCP端口：502,UDP端口：空，扫描速度：高，所属区域：Area-A/Area-default，其余默认，点击确定[check 4]  5）进入资产中心-资产管理-未确认资产菜单，点击刚刚扫到的Modbus协议资产的设备名称，进入资产画像页面，点击网络检测-端口信息[check 5]  预期结果：  [check 1]跳转到任务列表页面，可以进行资产扫描任务  [check 2]提示操作成功  [check 3]弹出新增任务弹窗，可以输入任务名称、地址范围、TCP端口、UDP端口，可以选择执行方式、执行周期、扫描速度，所属区域  [check 4]列表中新增一条正在扫描的任务Modbus，等待状态变为扫描完成后，点击扫描结果，可以查看到以Modbus协议接入的资产信息  [check 5]查看协议为Modbus协议 |
| **预期结果：**  测试应覆盖以下内容：  1）在测试环境网络接入采用Modbus协议通信的和利时LE5109L PLC至OT域交换机  2）在工业零信任分布协同安全管控平台执行主动资产发现，观察是否可以扫描到使用Modbus协议工业通信协议的和利时PLC |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 213 支持IEC104协议测试项

|  |
| --- |
| **测试项目：**支持IEC104协议（模拟器） |
| **测试依据：** |
| **测试目的：**  指标:3.4：支持多种工业网络资产管理功能：网络资产及拓扑结构探测支持主流网络协议不少于5种（功能性）；指标:3.4：支持多种工业网络资产管理功能：网络资产及拓扑结构探测支持主流网络协议不少于5种（功能性）； |
| **测试配置：** |
| **测试步骤：**  测试方法：  1） 进入工程师站，打开D:\ZGC-341\ics-simulator\web目录下，双击start.bat，进入工业控制协议模拟器管理平台  2） 点击启动IEC104模拟器  3） 使用operator用户登录工业零信任分布协同安全管控平台，进入资产中心-资产管理-主动资产发现[check 1]  4） 点击<任务列表>，点击<新增>按钮  5） 输入任务名称：IEC104协议，地址范围输入以IEC104协议协议接入的模拟器IP：192.168.0.100，TCP端口：2404，扫描速度：高，所属区域：Area-A/Area-default，其余默认，点击确定[check 2]  6） 进入资产中心-资产管理-未确认资产菜单，点击刚刚扫到的IEC104协议资产的设备名称，进入资产画像页面，点击网络检测-端口信息[check 3]  预期结果：  [check 1]跳转到任务列表页面，可以进行资产扫描任务  [check 2]列表中新增一条正在扫描的任务IEC104，等待状态变为扫描完成后，点击扫描结果，可以查看到以IEC104协议接入的资产信息  [check 3]查看协议为IEC104协议 |
| **预期结果：**  测试应覆盖以下内容：  1）在测试环境网络接入装有采用IEC104协议通信模拟器的主机至OT域交换机  2）在工业零信任分布协同安全管控平台执行主动资产发现，观察是否可以扫描到使用IEC104协议通信的模拟器资产 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 214 支持Profinet测试项

|  |
| --- |
| **测试项目：**支持Profinet协议 |
| **测试依据：** |
| **测试目的：**  指标:3.4：支持多种工业网络资产管理功能：网络资产及拓扑结构探测支持主流网络协议不少于5种（功能性）；指标:3.4：支持多种工业网络资产管理功能：网络资产及拓扑结构探测支持主流网络协议不少于5种（功能性）； |
| **测试配置：** |
| **测试步骤：**  测试方法：  1） 进入工程师站，打开D:\ZGC-341\ics-simulator\web目录下，双击start.bat，进入工业控制协议模拟器管理平台  2） 点击启动Profinet模拟器  3） 使用operator用户登录工业零信任分布协同安全管控平台，进入资产中心-资产管理-主动资产发现[check 1]  4） 点击<扫描配置>，选择进行扫描的网口，点击确定[check 2]  5） 点击<任务列表>，点击<新增>按钮[check 3]  6） 输入任务名称：Profinet，地址范围输入以Profinet协议接入的设备IP：192.168.0.100，TCP端口：空,UDP端口：34964，扫描速度：高，所属区域：Area-A/Area-default，其余默认，点击确定[check 4]  7） 进入资产中心-资产管理-未确认资产菜单，点击刚刚扫到的Profinet协议资产的设备名称，进入资产画像页面，点击网络检测-端口信息[check 5]  预期结果：  [check 1]跳转到任务列表页面，可以进行资产扫描任务  [check 2]提示操作成功  [check 3]弹出新增任务弹窗，可以输入任务名称、地址范围、TCP端口、UDP端口，可以选择执行方式、执行周期、扫描速度，所属区域  [check 4]列表中新增一条正在扫描的任务Profinet，等待状态变为扫描完成后，点击扫描结果，可以查看到以Profinet协议接入的资产信息  [check 5]查看协议为Profinet协议 |
| **预期结果：**  测试应覆盖以下内容：  1）在测试环境网络接入装有采用Profinet协议通信模拟器的主机至OT域交换机  2）在工业零信任分布协同安全管控平台执行主动资产发现，观察是否可以扫描到使用Profinet协议通信的模拟器资产 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 215 支持DNP3协议测试项

|  |
| --- |
| **测试项目：**支持DNP3协议 |
| **测试依据：** |
| **测试目的：**  指标:3.4：支持多种工业网络资产管理功能：网络资产及拓扑结构探测支持主流网络协议不少于5种（功能性）；指标:3.4：支持多种工业网络资产管理功能：网络资产及拓扑结构探测支持主流网络协议不少于5种（功能性）； |
| **测试配置：** |
| **测试步骤：**  测试方法：  1.进入工程师站，打开D:\ZGC-341\ics-simulator\web目录下，双击start.bat，进入工业控制协议模拟器管理平台  2. 点击启动DNP3模拟器  3. 使用operator用户登录工业零信任分布协同安全管控平台，进入资产中心-资产管理-主动资产发现[check 1]  4. 点击<扫描配置>，选择进行扫描的网口，点击确定[check 2]  5. 点击<任务列表>，点击<新增>按钮[check 3]  6.输入任务名称：DNP3，地址范围输入以DNP3协议接入的设备IP：192.168.0.100，TCP端口：空,UDP端口：34964，扫描速度：高，所属区域：Area-A/Area-default，其余默认，点击确定[check 4]  7.进入资产中心-资产管理-未确认资产菜单，点击刚刚扫到的Profinet协议资产的设备名称，进入资产画像页面，点击网络检测-端口信息[check 5]  预期结果：  [check 1]跳转到任务列表页面，可以进行资产扫描任务  [check 2]提示操作成功  [check 3]弹出新增任务弹窗，可以输入任务名称、地址范围、TCP端口、UDP端口，可以选择执行方式、执行周期、扫描速度，所属区域  [check 4]列表中新增一条正在扫描的任务DNP3，等待状态变为扫描完成后，点击扫描结果，可以查看到以DNP3协议接入的资产信息  [check 5]查看协议为DNP3协议 |
| **预期结果：**  测试应覆盖以下内容：  1）在测试环境网络接入装有采用DNP3协议通信模拟器的主机至OT域交换机  2）在工业零信任分布协同安全管控平台执行主动资产发现，观察是否可以扫描到使用DNP3协议通信的模拟器资产 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 216 缺陷可视化测试项

|  |
| --- |
| **测试项目：**缺陷可视化 |
| **测试依据：** |
| **测试目的：**  指标3.5：缺陷及风险可视化工具：提供1套支持缺陷及风险可视化工具（功能性）；指标3.5：缺陷及风险可视化工具：提供1套支持缺陷及风险可视化工具（功能性）； |
| **测试配置：** |
| **测试步骤：**  能够打开并查看资产脆弱性态势界面，能够单独投放该可视化界面  测试方法：  1.使用operator用户登录工业零信任分布协同安全管控平台  2.进入资产中心-资产管理-已确认资产-列表 页面，点击新增按钮[check 1]  资产名称输入：test，IP：192.168.1.2，所属区域：Area-A/Area-default，设备类型：工控系统信息设备 / 工作站 / 操作员站，操作系统：microsoft windows server 2008 sp2，点击确定[check 2]  3.进入监控中心-大屏管理菜单，双击脆弱性态势页面[check 3]  预期结果：  [check 1]弹出新增资产弹窗  [check 2]新增资产成功  [check 3]进入脆弱性态势页面，能够显示不同区域的网络设备、工控设备、物联网设备、安全设备、主机设备及其他设备的设备数、漏洞数、不合规项 |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 217 综合风险可视化测试项

|  |
| --- |
| **测试项目：**综合风险可视化（日志告警趋势可视化界面） |
| **测试依据：** |
| **测试目的：**  指标3.5：缺陷及风险可视化工具：提供1套支持缺陷及风险可视化工具（功能性）；指标3.5：缺陷及风险可视化工具：提供1套支持缺陷及风险可视化工具（功能性）； |
| **测试配置：** |
| **测试步骤：**  能够打开并查看综合风险可视化界面，能够单独投放该可视化界面，该界面能够显示当前系统的综合风险，如资产风险、告警等  测试方法：  1）在安全操作服务器使用udpSend工具发送一次syslog日志[check 1]  2）进入监控中心-大屏管理页面，双击综合安全态势页面[check 2]  预期结果：  [check 1]发送成功，平台收到日志  [check 2]可以显示当前资产运行状态统计，风险告警，包括告警级别、告警类型、告警描述，告警趋势 |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 218 网络攻击风险测试项

|  |
| --- |
| **测试项目：**网络攻击风险 |
| **测试依据：** |
| **测试目的：**  指标3.5：缺陷及风险可视化工具：提供1套支持缺陷及风险可视化工具（功能性）；指标3.5：缺陷及风险可视化工具：提供1套支持缺陷及风险可视化工具（功能性）； |
| **测试配置：** |
| **测试步骤：**  能够打开并查看网络攻击异常态势界面，能够单独投放该可视化界面，该界面能够显示当前系统的网络攻击告警  测试方法：  1）在安全操作服务器使用udpSend工具发送一次syslog日志[check 1]  2）点击监控中心-大屏管理-双击网络攻击态势页面[check 2]  预期结果：  [check 1]发送成功，平台收到日志  [check 2]可以显示当前系统网络攻击告警，包括处于扫描探测、渗透入侵、下载植入、横向扩散、命令控制到攻击生效的各个阶段的告警数量 |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 219 未知资产接入检测测试项

|  |
| --- |
| **测试项目：**未知资产接入检测测试项 |
| **测试依据：** |
| **测试目的：**  指标3.6：IT/OT跨域融合网络环境下自适应智能防护功能：实现IT/OT融合网络环境下典型的15种安全威胁防护功能（功能性）；指标3.6：IT/OT跨域融合网络环境下自适应智能防护功能：实现IT/OT融合网络环境下典型的15种安全威胁防护功能（功能性）； |
| **测试配置：** |
| **测试步骤：**  采用未知新主机接入OT网络内，采用工业零信任分布协同安全管控平台的资产探测功能进行未知设备探测，验证系统是否能自动探测到未知资产接入  测试方法：  1）使用operator用户登录工业零信任分布协同安全管控平台，进入资产中心-资产管理-主动资产发现[check 1]  2）点击<扫描配置>，选择进行扫描的网口，点击确定[check 2]  3）点击<任务列表>，点击<新增>按钮[check 3]  4）输入任务名称：扫描OT域工程师站，需要扫描的IP网段:192.168.0.100，扫描速度：高，所属区域：Area-A/Area-default，其余默认，点击确定[check 4]  5）系统主页点击资产中心-资产管理-未确认资产[check 5]  6）点击一个未确认资产的设备名称[check 6]  预期结果：  [check 1]跳转到任务列表页面，可以进行资产扫描任务  [check 2]提示操作成功  [check 3]弹出新增任务弹窗，可以输入任务名称、地址范围、TCP端口、UDP端口，可以选择执行方式、执行周期、扫描速度，所属区域  [check 4]列表中新增一条正在扫描的任务“扫描OT域工程师站”，等待状态变为扫描完成后，点击扫描结果，可以查看扫描IP范围内所以扫描到的资产  [check 5]显示主动或被动发现的资产  [check 6]跳转到资产画像页面，显示未确认资产的设备名称、设备IP、设备MAC、设备类型、操作系统、漏洞信息等 |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 220 网络扫描检测测试项

|  |
| --- |
| **测试项目：**网络扫描检测 |
| **测试依据：** |
| **测试目的：**  指标3.6：IT/OT跨域融合网络环境下自适应智能防护功能：实现IT/OT融合网络环境下典型的15种安全威胁防护功能（功能性）；指标3.6：IT/OT跨域融合网络环境下自适应智能防护功能：实现IT/OT融合网络环境下典型的15种安全威胁防护功能（功能性）； |
| **测试配置：** |
| **测试步骤：**  采用Namp扫描攻击对IT域服务器进行扫描，测试工业零信任分布协同安全管控平台是否能检测到网络扫描  测试方法：  1）进入D:/ZGC341课题攻击测试用例/1.6.2网络扫描检测目录下，打开Nmap-Zenmap GUI工，在Target项输入被攻击目标机IT域服务器IP, 192.168.1.90, Comand栏出现：nmap -T4 -A -v 192.168.1.90点击scan，开始对IT域服务器进行扫描，等待Nmap Output输出Nmap done，表示完成扫描  2）在浏览器输入 https://192.168.10.14，进入高级威胁检测系统，点击顶侧菜单栏分析中心，点击安全事件分析 [check1]  预期结果：  [check1] 在高级威胁检测系统的安全事件分析界面可以显示告警“主机受到NMAP工具发送的TCP协议的ack包进行探测”“服务器收到Nmap脚本引擎用户代理请求” |
| **预期结果：**  测试应覆盖以下内容： |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 221 WEB应用SQL注入防护测试项

|  |
| --- |
| **测试项目：**WEB应用SQL注入防护 |
| **测试依据：** |
| **测试目的：**  指标3.6：IT/OT跨域融合网络环境下自适应智能防护功能：实现IT/OT融合网络环境下典型的15种安全威胁防护功能（功能性）；指标3.6：IT/OT跨域融合网络环境下自适应智能防护功能：实现IT/OT融合网络环境下典型的15种安全威胁防护功能（功能性）； |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）进入D:/ZGC341课题攻击测试用例/1.6.3 SQL注入攻击检测/ 目录下  2）打开浏览器进入 https://192.168.1.90/sql-injection，  3）在界面中间输入框输入 “’OR’1’=’1”，点击搜索，向OT域服务器中Mysql服务器发送SQL注入攻击  4）观察页面搜索结果项是否出现mysql服务器中存储数据[check1]  5）使用operator用户零信任分布协同安全管控平台，点击异常检测，异常告警，查看是否出现SQL注入攻击告警[check2]  6）开启安全防护，在连接管理口主机进入E:\北航项目\中关村实验室项目\2025年上半年zgc项目推进\所有测试统一脚本及用例入口\15种攻击防护最新版\ZGC341课题辅助程序脚本\工业防火墙规则告警阻断及恢复脚本\ids-rule-control目录下执行python ids\_control.py -a block开启攻击阻断功能；  7）使用operator\_p用户进入工业零信任分布协同安全管控平台，https://192.168.10.15:8440，点击入侵规则配置，点击第一条规则配置按钮，点击保存，提示配置成功，点击上方下发规则配置，直至提示下发成功；  8）重复执行1）-4）步骤，再次从IT域攻击机发起SQL注入攻击，观察攻击是否成功[check 2]  预期结果：  [check1]能获取用户表三行内容  [check2]零信任分布协同安全管控平台的异常告警列表能够观察到存在“SQL注入攻击”告警 |
| **预期结果：**  测试应覆盖以下内容：  1）采用IT域攻击机对DMZ区服务器发起攻击，验证威胁防护效果  2）未开启防护下，针对Web应用的SQL攻击能够实施成功，系统应能够实现安全威胁告警  3）开启防护后，针对Web应用的SQL攻击应被阻断，攻击失败，且系统应可以展示威胁告警和阻断处理。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 222 钓鱼邮件攻击防护测试项

|  |
| --- |
| **测试项目：**钓鱼邮件攻击防护 |
| **测试依据：** |
| **测试目的：**  指标3.6：IT/OT跨域融合网络环境下自适应智能防护功能：实现IT/OT融合网络环境下典型的15种安全威胁防护功能（功能性）；指标3.6：IT/OT跨域融合网络环境下自适应智能防护功能：实现IT/OT融合网络环境下典型的15种安全威胁防护功能（功能性）； |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）首先处于未开启防护状态，在IT域攻击机打开win7\_32虚拟机，密码为123456，打开邮件服务器。  2）攻击机中打开foxmail，使用test@zgc.com邮箱账号，点击已发送邮件，寻找“新款报价请查收邮件”，该邮件附件包含病毒文件，点击再次编辑，点击发送。该邮件会经由邮件服务器发送至172.120.1.80服务器中  3）在172.120.1.80服务器中打开foxmail，选中user@zgc.com邮箱用户，按F2收信  4）未开启防护状态下，病毒邮件被发送至客户端。进入工业零信任分布协同安全管控平台，点击异常告警，异常处置界面，观察是否出现钓鱼邮件告警[check1]  5）开启安全防护，进入工业互联防火墙https://192.168.10.11，点击顶部菜单栏策略配置，点击控制策略，点击表单右侧编辑操作，点击入侵防御，选择规则模板为ALL，勾选防护模式，点击确定  6）重复执行操作2）至操作4）  7）观察该攻击是否被拦截[check2]  预期结果：  [check1] 未开启防护下，钓鱼邮件攻击成功，管理平台可查看钓鱼邮件告警  [check2]开启防护后，钓鱼邮件攻击被成功阻断，管理平台可查看阻断信息 |
| **预期结果：**  测试应覆盖以下内容：  1）未开启防护状态下，在攻击机执行钓鱼邮件攻击向DMZ服务器靶机发送病毒邮件，攻击成功；  2）开启防护状态下，在攻击机执行钓鱼邮件攻击攻击向DMZ服务器靶机发送病毒邮件，攻击失败，工业零信任分布协同安全管控平台能对攻击进行阻断且同时告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 223 Web服务弱口令爆破测试项

|  |
| --- |
| **测试项目：**Web服务弱口令爆破 |
| **测试依据：** |
| **测试目的：**  指标3.6：IT/OT跨域融合网络环境下自适应智能防护功能：实现IT/OT融合网络环境下典型的15种安全威胁防护功能（功能性）；指标3.6：IT/OT跨域融合网络环境下自适应智能防护功能：实现IT/OT融合网络环境下典型的15种安全威胁防护功能（功能性）； |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）进入D:/ZGC341课题攻击测试用例/1.6.5 Web服务弱口令爆破攻击检测目录下，进入http-brute文件夹  2）右键空白处，点击在终端处打开  3）输入 python http\_brute.py -u http://192.168.1.90/weak-password/ -U users..txt -P passwords.txt  4）观察窗口是否能获取用户名与密码 [check1]  5）观察高级威胁检测系统是否出现弱口令爆破相关告警[check2]  6）开启安全防护，进入工业互联防火墙https://192.168.10.11，点击顶部菜单栏策略配置，点击控制策略，点击表单右侧编辑操作，点击入侵防御，选择规则模板为ALL，勾选防护模式，点击确定  7）再次执行操作1）至操作3）  8）观察该攻击是否被拦截[check2]  预期结果：  [check1] cmd窗口可以看到能够通过弱口令爆破破解IT域服务器的弱口令账户，用户名：admin，密码：123456  [check2] 攻击被拦截，系统可查看阻断告警 |
| **预期结果：**  测试应覆盖以下内容：  1）未开启防护状态下，在攻击机执行Web服务弱口令爆破攻击对靶机进行攻击，攻击成功；  2）开启防护状态下，在攻击机执行Web服务弱口令爆破攻击对靶机进行攻击，攻击失败，工业零信任分布协同安全管控平台能对攻击进行阻断且同时告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 224 XSS攻击检测测试项

|  |
| --- |
| **测试项目：**XSS攻击检测 |
| **测试依据：** |
| **测试目的：**  指标3.6：IT/OT跨域融合网络环境下自适应智能防护功能：实现IT/OT融合网络环境下典型的15种安全威胁防护功能（功能性）；指标3.6：IT/OT跨域融合网络环境下自适应智能防护功能：实现IT/OT融合网络环境下典型的15种安全威胁防护功能（功能性）； |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）在攻击机中打开浏览器，打开 http://192.168.1.90/cross-site-scripting/index.php，进入 XSS漏洞演示系统  2）输入账号admin，密码admin123进行登录  3）执行XSS攻击，在浏览器输入：http://192.168.1.90/cross-site-scripting/index.php?search=<script>alert(document.cookie)</script>，可获取cookies [check 1]  4）观察高级威胁检测系统是否出现XSS攻击相关告警[check2]  5）开启安全防护，进入工业互联防火墙https://192.168.10.11，点击顶部菜单栏策略配置，点击控制策略，点击表单右侧编辑操作，点击入侵防御，选择规则模板为ALL，勾选防护模式，点击确定  6）再次执行操作1）至操作3）执行XSS攻击  7）观察该攻击是否被拦截[check3]  预期结果：  [check1] 浏览器弹出 192.168.1.90 cookies弹窗  [check2] 高级威胁检测系统可识别XSS攻击，显示“注入攻击XSS攻击”告警与“漏洞利用-xss攻击-JS标签”  [check3] 攻击被拦截，系统可查看阻断告警 |
| **预期结果：**  测试应覆盖以下内容：  1）未开启防护状态下，在攻击机执行XSS攻击对靶机进行攻击，攻击成功；  2）开启防护状态下，在攻击机执行XSS攻击对靶机进行攻击，攻击失败，工业零信任分布协同安全管控平台能对攻击进行阻断且同时告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 225 MySQL数据库暴力破解检测防护测试项

|  |
| --- |
| **测试项目：**MySQL数据库暴力破解检测防护 |
| **测试依据：** |
| **测试目的：**  指标3.6：IT/OT跨域融合网络环境下自适应智能防护功能：实现IT/OT融合网络环境下典型的15种安全威胁防护功能（功能性）；指标3.6：IT/OT跨域融合网络环境下自适应智能防护功能：实现IT/OT融合网络环境下典型的15种安全威胁防护功能（功能性）； |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）进入IT域攻击机D:/ZGC341课题攻击测试用例/1.6.7MySQL数据库暴力破解检测目录下  2）右键空白处，点击在终端处打开  3）输入 .\fscan.exe -h 192.168.1.90 -m mysql  4）观察是否可获取IT域服务器MySQL服务端账号密码 [check1]  5）观察高级威胁检测系统是否出现MySQL破解攻击相关告警 [check 2]  6）开启安全防护，进入工业互联防火墙https://192.168.10.11，点击顶部菜单栏策略配置，点击控制策略，点击表单右侧编辑操作，点击入侵防御，选择规则模板为ALL，勾选防护模式，点击确定  7）重复执行操作1）至操作3）  8）观察该攻击是否被拦截[check3]  预期结果：  [check1] Windows PowerShell界面显示扫描结束，并成功获取到IT域服务器账号密码为 root, Admin@123  [check2] 高级威胁检测系统可识别Mysql暴力破解攻击，显示“MySQL服务器遭受暴力登录破解”告警与“mysql服务器遭受root登录暴力破解”  [check3] 攻击被拦截，系统可查看阻断告警 |
| **预期结果：**  测试应覆盖以下内容：  1）未开启防护状态下，在攻击机执行MySQL数据库暴力破解攻击对靶机进行攻击，攻击成功；  2）开启防护状态下，在攻击机执行MySQL数据库暴力破解攻击对靶机进行攻击，攻击失败，工业零信任分布协同安全管控平台能对攻击进行阻断且同时告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 226 redis提权攻击检测防护测试项

|  |
| --- |
| **测试项目：**Redis提权攻击检测防护 |
| **测试依据：** |
| **测试目的：**  指标3.6：IT/OT跨域融合网络环境下自适应智能防护功能：实现IT/OT融合网络环境下典型的15种安全威胁防护功能（功能性）；指标3.6：IT/OT跨域融合网络环境下自适应智能防护功能：实现IT/OT融合网络环境下典型的15种安全威胁防护功能（功能性）； |
| **测试配置：** |
| **测试步骤：**  测试方法：  1） 打开攻击机E:\北航项目\中关村实验室项目\2025年上半年zgc项目推进\所有测试统一脚本及用例入口\15种攻击防护最新版\ZGC341课题攻击机测试用例\1.6.8 Redis提权攻击检测目录下；  2） 输入Win+R，输入CMD打开命令提示符界面，添加 Redis Key 设置 SSH 公钥type .\ssh-key.txt|.\redis-cli.exe -h 192.168.1.80 -x set crackit；  3） 执行 Redis 提权命令，本机 Redis 客户端连接 192.168.1.80 服务端：.\redis-cli.exe -h 192.168.1.80；  4） 设置工作目录：config set dir /root/.ssh/；  5） 保存公钥到 /root/.ssh/authorized\_keys 文件：config set dbfilename authorized\_keys，执行持久生效命令：save，观察写入公钥是否成功[check1]  6） 开启安全防护，进入工业互联防火墙https://192.168.10.11，点击顶部菜单栏策略配置，点击控制策略，点击表单右侧编辑操作，点击入侵防御，选择规则模板为ALL，勾选防护模式，点击确定  7） 重复执行操作1）至操作5）  8） 观察该攻击是否被拦截[check2]  预期结果：  [check1] 防护未开启，公钥写入成功，系统显示Redis提权攻击告警  [check2] 开启防御，则写入公钥失败 |
| **预期结果：**  测试应覆盖以下内容：  1）未开启防护状态下，在攻击机执行redis提权攻击对靶机进行攻击，攻击成功；  2）开启防护状态下，在攻击机执行redis提权攻击对靶机进行攻击，攻击失败，工业零信任分布协同安全管控平台能对攻击进行阻断且同时告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 227 LOIC DoS攻击检测防护测试项

|  |
| --- |
| **测试项目：**LOIC DoS攻击检测防护 |
| **测试依据：** |
| **测试目的：**  指标3.6：IT/OT跨域融合网络环境下自适应智能防护功能：实现IT/OT融合网络环境下典型的15种安全威胁防护功能（功能性）；指标3.6：IT/OT跨域融合网络环境下自适应智能防护功能：实现IT/OT融合网络环境下典型的15种安全威胁防护功能（功能性）； |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）进入D:/ZGC341课题攻击测试用例/1.6.9 Loic DoS攻击检测  2）双击打开LOIC工具wic\_x86\_chs.exe  3）填写目标IP：192.168.1.90，点击Lock on， 填写Port端口为:80，Method选择TCP，Thread更改为100000  4）点击IMMA CHARGIN MAH LAZER 进行攻击，观察高级威胁检测系统是否出现DOS攻击相关告警 [check 1]  5）开启安全防护，进入工业互联防火墙https://192.168.10.11，点击顶部菜单栏策略配置，点击控制策略，点击表单右侧编辑操作，点击入侵防御，选择规则模板为ALL，勾选防护模式，点击确定  6）重复执行操作1）至操作4）  7）观察该攻击是否被拦截[check2]  预期结果  [check1] 防护未开启，LOIC Dos攻击成功，系统显示LOIC Dos攻击攻击告警  [check2] 开启防御后，在目标设备上抓包，可见包数被控制在指定频率内 |
| **预期结果：**  测试应覆盖以下内容：  1）未开启防护状态下，在攻击机执行LOIC DoS攻击对靶机进行攻击，攻击成功；  2）开启防护状态下，在攻击机执行LOIC DoS攻击对靶机进行攻击，攻击失败，工业零信任分布协同安全管控平台能对攻击进行阻断且同时告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 228 远程命令执行检测与防护测试项

|  |
| --- |
| **测试项目：**远程命令执行检测与防护 |
| **测试依据：** |
| **测试目的：**  指标3.6：IT/OT跨域融合网络环境下自适应智能防护功能：实现IT/OT融合网络环境下典型的15种安全威胁防护功能（功能性）；指标3.6：IT/OT跨域融合网络环境下自适应智能防护功能：实现IT/OT融合网络环境下典型的15种安全威胁防护功能（功能性）； |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）在攻击机打开浏览器，输入http://192.168.1.90/remote-command-execution/  2）输入以下命令测试（任一即可）：whoami、ifconfig、ip addr  、cat /etc/passwd、cat /etc/shadow，观察命令是否执行成功 [check 1]  3）开启安全防护，进入工业互联防火墙https://192.168.10.11，点击顶部菜单栏策略配置，点击控制策略，点击表单右侧编辑操作，点击入侵防御，选择规则模板为ALL，勾选防护模式，点击确定  4）重复执行操作1）至操作2）  5）观察该攻击是否被拦截[check2]  预期结果：  [check1] 远程命令执行成功  [check2] 开启防御，远程命令执行失败，系统平台前端可显示告警与阻断 |
| **预期结果：**  测试应覆盖以下内容：  1）未开启防护状态下，在攻击机执行远程命令执行攻击对靶机进行攻击，攻击成功；  2）开启防护状态下，在攻击机执行远程命令执行攻击对靶机进行攻击，攻击失败，工业零信任分布协同安全管控平台能对攻击进行阻断且同时告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 229 Webshell上传检测与防护测试项

|  |
| --- |
| **测试项目：**Webshell 上传检测与防护 |
| **测试依据：** |
| **测试目的：**  指标3.6：IT/OT跨域融合网络环境下自适应智能防护功能：实现IT/OT融合网络环境下典型的15种安全威胁防护功能（功能性）；指标3.6：IT/OT跨域融合网络环境下自适应智能防护功能：实现IT/OT融合网络环境下典型的15种安全威胁防护功能（功能性）； |
| **测试配置：** |
| **测试步骤：**  测试方法：  1） 打开浏览器输入 http://192.168.1.90/web-shell/，进入WebShell上传演示系统；  2） 点击选择文件按钮，D:/ZGC341课题攻击测试用例/1.6.11 WebShell文件上传/shell目录，将shell.php文件上传至演示系统，点击上传，观察是否攻击成功； [check 1]  3） 开启安全防护，在连接管理口主机进入E:\北航项目\中关村实验室项目\2025年上半年zgc项目推进\所有测试统一脚本及用例入口\15种攻击防护最新版\ZGC341课题辅助程序脚本\工业防火墙规则告警阻断及恢复脚本\ids-rule-control目录下执行python ids\_control.py -a block开启攻击阻断功能；  4） 使用operator\_p用户进入工业零信任分布协同安全管控平台，https://192.168.10.15:8440，点击入侵规则配置，点击第一条规则配置按钮，点击保存，提示配置成功，点击上方下发规则配置，直至提示下发成功；  5） 重复执行操作1）至操作2）；  6） 观察该攻击是否被拦截[check2]  预期结果：  [check 1] 攻击机对靶机攻击成功；  [check2] 威胁检测系统出现“WEB服务器接收到包含PHP标签的POST请求”告警 |
| **预期结果：**  测试应覆盖以下内容：  1）未开启防护状态下，在攻击机执行Webshell上传攻击对靶机进行攻击，攻击成功；  2）开启防护状态下，在攻击机执行WebShell攻击对靶机进行攻击，攻击失败，工业零信任分布协同安全管控平台能对攻击进行阻断且同时告警。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 230永恒之蓝漏洞利用检测与防护测试项

|  |
| --- |
| **测试项目：**永恒之蓝漏洞利用检测与防护 |
| **测试依据：** |
| **测试目的：**  指标3.6：IT/OT跨域融合网络环境下自适应智能防护功能：实现IT/OT融合网络环境下典型的15种安全威胁防护功能（功能性）；指标3.6：IT/OT跨域融合网络环境下自适应智能防护功能：实现IT/OT融合网络环境下典型的15种安全威胁防护功能（功能性）； |
| **测试配置：** |
| **测试步骤：**  测试方法：  1） 打开D:/ZGC341课题攻击测试用例/1.6.12永恒之蓝漏洞利用检测/EquationToolsGUI\_V0.42/方程式工具包图形界面V0.42\目录下  2） 执行“方程式工具包图形界面版V0.42.jar”  3） 攻击类型默认为NSA扫描，修改被攻击IP地址为：172.120.1.81，点击扫描漏洞  4） 执行完毕后，点击顶部菜单永恒之蓝，点击漏洞利用，观察工具返回结果 [check 1]  5） 开启安全防护，进入工业互联防火墙https://192.168.10.11，点击顶部菜单栏策略配置，点击控制策略，点击表单右侧编辑操作，点击入侵防御，选择规则模板为ALL，勾选防护模式，点击确定  6） 重复执行操作1）至操作2）  7） 观察该攻击是否被拦截[check2]  预期结果：  [check1] 攻击工具返回Success！，攻击成功；  [check2] 开启防御，远程命令执行失败，威胁检测系统出现“永恒之蓝漏洞利用检测”告警 |
| **预期结果：**  测试应覆盖以下内容：  1）未开启防护状态下，在攻击机执行永恒之蓝漏洞利用攻击对靶机进行攻击，攻击成功  2）开启防护状态下，在攻击机执行永恒之蓝漏洞利用攻击对靶机进行攻击，攻击失败，工业零信任分布协同安全管控平台能对攻击进行阻断且同时告警 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 231 Struts 远程代码执行漏洞检测与防护测试项

|  |
| --- |
| **测试项目：**Struts 远程代码执行漏洞检测与防护 |
| **测试依据：** |
| **测试目的：**  指标3.6：IT/OT跨域融合网络环境下自适应智能防护功能：实现IT/OT融合网络环境下典型的15种安全威胁防护功能（功能性）；指标3.6：IT/OT跨域融合网络环境下自适应智能防护功能：实现IT/OT融合网络环境下典型的15种安全威胁防护功能（功能性）； |
| **测试配置：** |
| **测试步骤：**  测试方法：  1） 打开D:/ZGC341课题攻击测试用例/1.6.13 Struts远程代码执行漏洞检测/Fsacn/目录下  2） 右键空白处点击在终端打开，输入 .\fscan.exe -h 192.168.1.90 -m webonly -pocpath .\poc-struts\ 并执行  3） 观察Windows PowerShell是否出现扫描结束，如出现表示攻击成功  4） 开启安全防护，进入工业互联防火墙https://192.168.10.11，点击顶部菜单栏策略配置，点击控制策略，点击表单右侧编辑操作，点击入侵防御，选择规则模板为ALL，勾选防护模式，点击确定  5） 重复执行操作1）至操作3）  6） 观察该攻击是否被拦截[check2]  预期结果：  [check1] 威胁检测系统出现“Struts 远程代码执行漏洞”告警  [check2] 开启防御，远程命令执行失败 |
| **预期结果：**  测试应覆盖以下内容：  1）未开启防护状态下，在攻击机执行struts远程代码执行漏洞攻击对靶机进行攻击，攻击成功  2）开启防护状态下，在攻击机执行struts远程代码执行漏洞攻击对靶机进行攻击，攻击失败，工业零信任分布协同安全管控平台能对攻击进行阻断且同时告警 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 232 敏感文件passwd探测检测测试项

|  |
| --- |
| **测试项目：**敏感文件passwd探测检测 |
| **测试依据：** |
| **测试目的：**  指标3.6：IT/OT跨域融合网络环境下自适应智能防护功能：实现IT/OT融合网络环境下典型的15种安全威胁防护功能（功能性）；指标3.6：IT/OT跨域融合网络环境下自适应智能防护功能：实现IT/OT融合网络环境下典型的15种安全威胁防护功能（功能性）； |
| **测试配置：** |
| **测试步骤：**  测试方法：  1） 打开D:/ZGC341课题攻击测试用例/1.6.14 IT域敏感文件passwd探测检测/7kbscan-WebPathBrute目录下，打开7kbscan-WebPathBrute.exe文件  2） 输入扫描目标：http://192.168.1.90/  3） 设置字典，点击“切换加载dic”，选择字典为Dic目录下的dir.txt  4） 点击开始攻击，观察是否获取敏感文件账号密码 [check 1]  5） 开启安全防护，在连接管理口主机进入E:\北航项目\中关村实验室项目\2025年上半年zgc项目推进\所有测试统一脚本及用例入口\15种攻击防护最新版\ZGC341课题辅助程序脚本\工业防火墙规则告警阻断及恢复脚本\ids-rule-control目录下，执行python ids\_control.py -a block开启攻击阻断功能  6） 使用operator\_p用户进入工业零信任分布协同安全管控平台，https://192.168.10.15:8440，点击入侵规则配置，点击第一条规则配置按钮，点击保存，提示配置成功。点击上方下发规则配置，直至提示下发成功  7） 重复执行操作1）至操作4），观察该攻击是否被拦截[check2]  预期结果：  [check1] 获取敏感文件账号密码，攻击成功  [check2] 开启防御，攻击被阻断，防火墙系统可查看该攻击被拦截 |
| **预期结果：**  测试应覆盖以下内容：  1）未开启防护状态下，在攻击机执行敏感文件passwd探测攻击对靶机进行攻击，攻击成功  2）开启防护状态下，在攻击机执行敏感文件passwd探测攻击对靶机进行攻击，攻击失败，工业零信任分布协同安全管控平台能对攻击进行阻断且同时告警 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 233 机械臂状态控制流异常检测与防护测试项

|  |
| --- |
| **测试项目：**机械臂状态控制流异常检测与防护 |
| **测试依据：** |
| **测试目的：**  指标3.6：IT/OT跨域融合网络环境下自适应智能防护功能：实现IT/OT融合网络环境下典型的15种安全威胁防护功能（功能性）；指标3.6：IT/OT跨域融合网络环境下自适应智能防护功能：实现IT/OT融合网络环境下典型的15种安全威胁防护功能（功能性）； |
| **测试配置：** |
| **测试步骤：**  测试方法：  1) 进入机械臂控制界面，打开工程师站笔记本，从桌面进入：/robotsdio2.0.0/win-unpacked/目录下，双击打开robot-pick-studio.exe文件，最大化窗口，点击开始下“所有项目”，选择创建时间未2025-04-16的项目点击打开，左侧栏目机械臂/代码下，双击打开dataTest3.c  2) 进入攻击机代码执行界面，在攻击机桌面双击Pycharm，进入后自动进入robot-socket项目，双击左侧“attack1.py”打开攻击代码  3) 模拟机械臂正常执行，首先点击客户端右上角上电，机械臂可正常上电，在代码界面点击右键，点击运行，机械臂开始进行打磨作业，直至打磨任务结束后机械臂复位[check1]  4) 再次在工程师站中重复步骤3，使机械臂进入正常运行状态。  5) 此时在攻击机的“attack1.py”代码中点击右键运行。机械臂此时被攻击，运行状态中发出较为剧烈的异响[check2]  6) 测试异常检测与防护效果的功能性，打开工业控制流异常检测与防护模块，在工程师站中再次执行步骤3，此时机械臂进入正常执行状态。此时在攻击机中再次执行步骤5。  7) 数据流异常检测模块可以根据机械臂传感器采集的设备电力、力矩、速度决策参数判断机械臂进入异常状态，此时观察机械臂是否被自动停止[check3]  8) 进入工业零信任分布协同安全管控平台，点击顶部菜单栏“异常检测”，点击左侧菜单栏“异常处置”，观察是否出现“机械臂状态参数异常”类型告警，观察异常告警描述是否出现“机械臂正常执行状态下遭受其它客户端调用使能命令导致机械臂异常响动”  预期结果：  • 系统可检测出设备状态异常，并产生告警，系统调用预定义指令停止传感器工作  [check1] 机械臂可以正常上电，且机械臂正常重复执行打磨动作  [check2] 发起攻击后，机械臂持续存在剧烈异响，进入异常状态  [check3] 机械臂被攻击后立刻停止当前打磨任务和异常动作  [check4] 异常处置界面出现“机械臂状态参数异常”类型告警，观察异常告警描述是否出现“机械臂正常执行状态下遭受其它客户端调用使能命令导致机械臂异常响动” |
| **预期结果：**  测试应覆盖以下内容：  1）验证在未开启防护时，机械臂被攻击下会进入异常状态  2）验证开启算法防护后，算法能够通过获取并分析设备的电力、力矩、速度参数进行异常判断  3）验证异常情况发生后，系统能够可视化告警信息并显示 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 234 机械臂控制流攻击异常白名单检测检测测试项

|  |
| --- |
| **测试项目：**机械臂控制流攻击异常白名单检测检测 |
| **测试依据：** |
| **测试目的：**  指标3.6：IT/OT跨域融合网络环境下自适应智能防护功能：实现IT/OT融合网络环境下典型的15种安全威胁防护功能（功能性）；指标3.6：IT/OT跨域融合网络环境下自适应智能防护功能：实现IT/OT融合网络环境下典型的15种安全威胁防护功能（功能性）； |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）进入机械臂控制界面，打开工程师站笔记本，从桌面进入：/robotsdio2.0.0/win-unpacked/目录下，双击打开robot-pick-studio.exe文件，最大化窗口，点击开始下“所有项目”，选择创建时间未2025-04-16的项目点击打开，左侧栏目机械臂/代码下，双击打开dataTest3.c  2）进入攻击机代码执行界面，在攻击机桌面双击Pycharm，进入后自动进入robot-socket项目，双击左侧“attack1\_data.py”打开攻击代码  3）模拟机械臂正常执行，首先点击客户端右上角上电，机械臂可正常上电，在代码界面点击右键，点击运行，机械臂开始进行打磨作业，直至打磨任务结束后机械臂复位[check1]  4）再次在工程师站中重复步骤3，使机械臂进入正常运行状态。  5）此时在攻击机的“attack2\_control.py”代码中点击右键运行。观察机械臂是否在正常打磨过程被中断，执行非预定动作[check2]  6）控制流异常检测白名单算法可以通过解码经过交换机进入机械臂的工控协议，根据白名单算法策略判断机械臂异常[check3]  7）进入工业零信任分布协同安全管控平台，点击顶部菜单栏“异常检测”，点击左侧菜单栏“异常处置”，观察是否出现“机械臂状态参数异常”类型告警，观察异常告警描述是否出现“机械臂正常执行状态下遭受其它客户端调用使能命令导致机械臂异常响动”  预期结果：  系统可检测出设备状态异常，并产生告警，系统调用预定义指令停止传感器工作  [check1] 机械臂能够正常上电，且机械臂正常重复执行打磨动作  [check2] 发起攻击后，机械臂持续存在剧烈异响，进入异常状态  [check3] 机械臂被攻击后立刻停止当前打磨任务和异常动作  [check4] 异常处置界面出现“机械臂状态参数异常”类型告警，观察异常告警描述是否出现“机械臂正常执行状态下遭受其它客户端调用使能命令导致机械臂异常响动” |
| **预期结果：**  测试应覆盖以下内容：  1）工程师站正常下发命令执行机械臂，机械臂能够正常运行，系统无告警  2）模拟执行预定义异常脚本，系统应能够判断机械臂执行了异常控制流，工业零信任分布协同管控平台异常告警界面提示机械臂异常 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 235 非结构化数据分级分类模块测试项

|  |
| --- |
| **测试项目：**非结构化数据分级分类模块 |
| **测试依据：** |
| **测试目的：**  验证用户可以对非结构化数据进行标注，选择传统机器学习模型和深度学习模型，配置训练参数，训练模型，并能够上传测试数据，使用训练好的模型对数据进行预测并记录相关指标。验证用户可以对非结构化数据进行标注，选择传统机器学习模型和深度学习模型，配置训练参数，训练模型，并能够上传测试数据，使用训练好的模型对数据进行预测并记录相关指标。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）准备不同规模和格式（标注完整/缺失）的训练数据集，以测试数据标注功能。  2）通过UI操作选择不同模型（传统机器学习模型/智能学习模型/深度学习模型）、配置参数、上传数据、启动训练，以测试模型训练功能。  3）观察训练过程中的界面反馈和后台日志，并在训练结束后检查训练生成的模型文件和评估报告，测试训练结果和评估指标查看功能。  4）准备好未标注的测试数据集，在系统中上传测试数据，并选择已训练的模型进行预测，以测试数据预测功能。  5）预测完成后，在系统中查看预测结果，并导出为 csv 文件，已测试预测结果查看和导出功能。 |
| **预期结果：**  测试应覆盖以下内容：  1）数据标注-文本数据分类与分级标注  2）模型训练-训练数据上传与校验  3）模型训练-传统机器学习模型选择与训练 (KNN, SVM等)  4）模型训练-智能学习模型训练  5）模型训练-深度学习模型选择与训练 (LSTM)  6）模型训练-训练参数配置与生效  7）模型训练-训练结果与评估指标查看  8）数据预测-预测数据上传与校验  9）数据预测-选择模型进行预测  10）数据预测-预测结果（分类、风险等级）查看与导出  11）任务管理-训练/预测任务状态查看与管理 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 236 结构化数据分级分类模块测试项

|  |
| --- |
| **测试项目：**结构化数据分级分类模块 |
| **测试依据：** |
| **测试目的：**  验证系统能够正确选择数据库和数据表，并准确计算和展示所选对象的库级别价值、表级别价值（包括规模、质量、应用、风险四个一级指标及其二级指标的得分与权重）、以及列（字段）级别价值。验证系统能够正确选择数据库和数据表，并准确计算和展示所选对象的库级别价值、表级别价值（包括规模、质量、应用、风险四个一级指标及其二级指标的得分与权重）、以及列（字段）级别价值。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）准备包含不同特征的测试数据库和数据表，在系统中选择，观察它们在数据概览界面下的不同表现。  2）在高价值评估界面，观察数据规模，数据质量，数据应用，数据风险价值评估结果，评估其数值排序和雷达图可视化结果是否符合预期  3）在高价值发现界面，选择分类模型和要进行发现的数据库，进行高价值数据发现，查看行级发现结果。  4）在数据标注页面，使用专家验证码进入标注系统，对行级数据和表级数据进行评分，观察表级和库级数据价值评分结果是否随着标注的不同而变化。 |
| **预期结果：**  测试应覆盖以下内容：  1）数据概览-数据库/表选择与基本情况展示  2）数据概览-各层级高价值数据要素数量统计  3）数据概览-数据表多维度价值得分展示  4）高价值评估-库/表/列/字段价值计算与展示  5）高价值评估-数据规模价值计算 (种类、规模)  6）高价值评估-数据质量价值计算 (完整性、一致性等)  7）高价值评估-数据应用价值计算 (多维性、及时性等)  8）高价值评估-数据风险价值计算  9）高价值评估-雷达图可视化与数据排序  10）高价值发现-分类模型导入、选择与训练 (SVM, NB)  11）高价值发现-聚类结果可视化 (散点图、饼图)  12）高价值发现-行数据价值分类结果展示  13）数据标注-身份验证  14）数据标注-表级别价值打分  15）数据标注-行级别高/低价值标注 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 237 数据图谱模块测试项

|  |
| --- |
| **测试项目：**数据图谱模块 |
| **测试依据：** |
| **测试目的：**  验证用户能够通过输入节点名称、选择实体类型、限定查询数量来搜索图谱中的节点，查询结果在图谱界面正确展示。验证用户能够通过输入节点名称、选择实体类型、限定查询数量来搜索图谱中的节点，查询结果在图谱界面正确展示。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）在Neo4j中准备包含多种节点类型和关系的测试图数据。  2）通过UI的搜索框和下拉菜单输入查询条件。  3）观察图谱可视化区域的展示结果是否符合预期。  4）检查查询结果的准确性和完整性。 |
| **预期结果：**  测试应覆盖以下内容：  1）图谱可视化-节点聚类/分类结果展示  2）图谱查询-按名称、类型等查询节点与关系  3）图谱交互-节点扩展与关系追溯  4）图谱交互-节点/关系属性信息查看  5）图谱可视化操作-布局切换 (力导向、层次)  6）图谱可视化操作-缩放/平移/居中 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 238 异构数据安全存储模块测试项

|  |
| --- |
| **测试项目：**异构数据安全存储模块 |
| **测试依据：** |
| **测试目的：**  异构数据安全存储。异构数据安全存储。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）通过对不同限制级别的文件上传，访问来检验异构数据的安全存储；  2)通过输入不同可信执行环境下的指令来实现可信执行环境下对文件的写入，删除，修改等操作；  3)通过人为底层对系统文件进行破坏，来检验开放执行区的文件数据完整性校验。 |
| **预期结果：**  功能测试应覆盖以下内容：  1）异构数据安全存储:对应不同分类级别的数据存储，且区分数据访问级别限制，包括四种级别的文件类型上传，下载，共享等操作；  2)不同可信执行环境下对文件的写入，修改等操作执行；  3)文件完整性校验: 文件在开放执行区被改写之后哈希特征值被改变，导致安全性校验出错。  性能测试：  可支持两种以上可信执行环境的数据存储。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 239 操作行为溯源模块测试项

|  |
| --- |
| **测试项目：**操作行为溯源 |
| **测试依据：** |
| **测试目的：**  对用户的数据操作行为溯源对用户的数据操作行为溯源 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）通过不同权限的用户对文件的执行操作，前端点击查看溯源所有用户的行为操作；  2）系统自动记录所有对文件的行为操作，前端点击查看溯源所有对文件的行为操作。 |
| **预期结果：**  测试应覆盖以下内容：  1）用户操作行为溯源:能够查看某一用户的所有操作行为，例如对文件的下载，上传，修改等；  2)文件操作溯源:对文件的所有行为操作记录，包括所有的下载，修改，上传和分享记录进行溯源，浏览文件操作历史，实现异构数据的完整血缘溯源。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 240 数据溯源系统部署与启动测试项

|  |
| --- |
| **测试项目：**系统部署与启动 |
| **测试依据：** |
| **测试目的：**  系统部署与启动，启动虚拟环境系统部署与启动，启动虚拟环境 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）执行bash start.sh后，确认无报错输出；  2）执行 docker-compose ps，确认所有服务已正常启动；  3）浏览器访问 http://<虚拟机IP>:30010，确认页面加载正常、功能模块完整显示。  4）在INT-net/INT-MX/switch-tree目录下执行命令 make，确认无报错输出；  5）执行后确认终端提示切换为 mininet>。 |
| **预期结果：**  测试应覆盖以下内容：  1）服务启动脚本功能完整；  2）服务状态验证；  3）前端页面可访问。  4）指定路径下make命令执行成功；  5）成功进入 Mininet 交互终端。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 241 配置交换机流量转发规则测试项

|  |
| --- |
| **测试项目：**配置交换机流量转发规则 |
| **测试依据：** |
| **测试目的：**  验证交换机流量转发规则能够成功配置。验证交换机流量转发规则能够成功配置。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）在INT-net/INT-MX/switch-tree目录下重新启动一个终端并执行switch\_config.sh脚本，确认无报错输出。 |
| **预期结果：**  测试应覆盖以下内容：  1）成功执行switch\_config.sh脚本。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 242数据采集和上传服务启动测试项

|  |
| --- |
| **测试项目：**数据采集和上传服务启动 |
| **测试依据：** |
| **测试目的：**  验证数据采集与上传模块是否能成功启动并正常运行。验证数据采集与上传模块是否能成功启动并正常运行。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）在Mininet终端中执行xterm h82打开h82主机终端，在h82终端窗口中运行python3 collector.py > collect.log，检查是否生成 collect.log文件；  2）在新的Mininet终端中执行python3 monitor.py > monitor.log，检查是否生成monitor.log文件。 |
| **预期结果：**  测试应覆盖以下内容：  1）数据采集服务启动验证；  2）数据上传服务启动验证。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 243发送数据包测试项

|  |
| --- |
| **测试项目：**发送数据包 |
| **测试依据：** |
| **测试目的：**  验证Mininet虚拟网络中不同主机之间的数据通信能力。验证Mininet虚拟网络中不同主机之间的数据通信能力。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）在Mininet终端中通过指令xterm h12 h42成功打开两个主机终端，确认主机实例正常运行。  2）在h12主机终端通过指令nc -u <h12主机IP> 1234向h42指定端口（以1234端口为例）发送两条消息。  3）在h42主机终端通过指令nc -ul 1234监听1234端口，确认正确显示来自h12的数据包内容。 |
| **预期结果：**  测试应覆盖以下内容：  1）主机终端可用性验证；  2）数据发送功能验证；  3）数据接收功能验证； |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 244数据记录与前端展示测试项

|  |
| --- |
| **测试项目：**数据记录与前端展示 |
| **测试依据：** |
| **测试目的：**  验证Mininet虚拟网络中不同主机之间的数据通信能力。验证Mininet虚拟网络中不同主机之间的数据通信能力。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）查看collect.log文件中接收到的监控数据包信息，确认数据报信息正确显示，并查看monitor.log文件，确认数据报信息上传成功；  2）在浏览器访问数据记录总览页面，确认正确显示trace记录。 |
| **预期结果：**  测试应覆盖以下内容：  1）日志文件数据接收验证；  2）前端页面可视化展示验证。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 245 数据包详情展示测试项

|  |
| --- |
| **测试项目：**数据包详情展示 |
| **测试依据：** |
| **测试目的：**  支撑指标4.2中面向异构数据溯源的数据血缘分析工具的数据溯源的可视化展示。支撑指标4.2中面向异构数据溯源的数据血缘分析工具的数据溯源的可视化展示。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）在数据记录总览页面中点击一条trace项，检查是否弹出数据包详情展示页面；  2）弹出数据包详情展示页面后，确认页面上方正确显示数据包经过的站点名称和编号；  3）点击“捕获的监控数据包”菜单项，确认页面展示的原始数据包内容是否正确显示、完整；  4）点击“解析后的数据”菜单项，确认各字段信息是否完整且格式正确；  5）点击“网络拓扑图”菜单项，检查当前拓扑图是否正确显示，且trace 所经过路径是否以蓝色标出；  6）点击“地理信息图”菜单项，确认是否展示站点地图，路径线是否按照数据包实际路径连接站点节点；  7）将当前的trace记录内容与每项详情中的内容进行字段比对，确认其一致性。 |
| **预期结果：**  测试应覆盖以下内容：  1）Trace记录点击响应验证；  2）数据包详细属性展示验证；  3）捕获的监控数据包展示验证；  4）解析后的数据展示验证；  5）网络拓扑图展示验证；  6）地理信息图展示验证；  7）数据一致性验证。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 246 自定义组织和Peer节点数量测试项

|  |
| --- |
| **测试项目：**自定义组织和Peer节点数量 |
| **测试依据：** |
| **测试目的：**  用户可以自定义组织和Peer节点的数量，系统自动构建对应配置的区块链，并将链码安装到区块链用户可以自定义组织和Peer节点的数量，系统自动构建对应配置的区块链，并将链码安装到区块链 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1） 用户输入组织和Peer节点配置并等待系统自动构建区块链完成后，在后端服务器上使用终端指令可查看运行的Peer节点容器和链码容器 |
| **预期结果：**  测试应覆盖以下内容：  1）输入组织和Peer节点的数量后，系统构建出对应配置的区块链  2）区块链构建完成后，链码成功安装到区块链 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 247数据上传区块链测试项

|  |
| --- |
| **测试项目：**数据上传区块链 |
| **测试依据：** |
| **测试目的：**  用户提供明文、数据标识（自定义）、自身组织编号以及访问策略给前端，后端进行加密得到密文并存入区块链用户提供明文、数据标识（自定义）、自身组织编号以及访问策略给前端，后端进行加密得到密文并存入区块链 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）模拟用户，在前端填写示例明文、数据标识、组织编号以及访问策略  2）点击提交后，后端进行加密，可以通过终端指令从区块链中查看密文 |
| **预期结果：**  测试应覆盖以下内容：  1）用户在前端填写必要信息  2）前端将信息传递给后端，后端进行加密得到密文  3）后端将密文上链 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 248 数据下载测试项

|  |
| --- |
| **测试项目：**数据下载 |
| **测试依据：** |
| **测试目的：**  用户提供想要获得的数据项所对应数据标识、自身的组织编号、自身的属性列表给前端，后端根据属性生成私钥，解密数据标识对应的密文，返回明文用户提供想要获得的数据项所对应数据标识、自身的组织编号、自身的属性列表给前端，后端根据属性生成私钥，解密数据标识对应的密文，返回明文 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）模拟用户，在前端填写示例数据标识、组织编号以及属性列表  2）点击提交后，后端进行解密并返回明文，可以在前端查看结果 |
| **预期结果：**  测试应覆盖以下内容：  1）用户在前端填写必要信息  2）前端将信息传递给后端，后端根据属性生成私钥，解密数据标识对应的密文  3）后端将解密后的信息返回给前端进行展示 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 249西门子PLC拒绝服务风险测试项

|  |
| --- |
| **测试项目：**西门子PLC拒绝服务 |
| **测试依据：** |
| **测试目的：**  验证执行风险载荷后西门子PLC拒绝服务风险的测试，支持S7commPlus协议特定版本的西门子PLC进行的风险测试验证执行风险载荷后西门子PLC拒绝服务风险的测试，支持S7commPlus协议特定版本的西门子PLC进行的风险测试 |
| **测试配置：** |
| **测试步骤：**  功能测试方法：  1）设置好一套S7-1500PLC和上位机环境，确保两者之间网络通畅；  2）将基本逻辑控制程序和配置下载到PLC中；  3）在上位机打开CMD终端行；  4）输入风险测试命令后回车，几秒钟后PLC由于资源耗尽处于故障状态；  5）故障状态导致PLC所有服务均中断，通讯也出现故障，此时无法ping通PLC控制器；  6）1min后PLC重启进入Stop状态；  7）按压Run按钮PLC控制器恢复正常。 性能测试方法：  1）风险测试完成后PLC处于故障状态，等待约1分钟后重启，此时处于Stop状态，按压Run按钮PLC恢复正常；  2）风险测试完成后PLC处于故障状态，等待约1分钟后重启，此时处于Stop状态，对于没有Run按钮的PLC使用编程软件进行操作后PLC恢复正常。 |
| **预期结果：**  功能功能测试应覆盖以下内容：  1）验证西门子PLC终端资源耗尽功能  2）验证西门子PLC终端服务中断功能  3）验证西门子PLC终端通讯故障功能  性能测试应覆盖以下内容：  1）验证西门子PLC终端风险测试后的恢复能力和响应时间 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 250西门子PLC芯片内存Dump风险测试项

|  |
| --- |
| **测试项目：**西门子PLC密码绕过风险 |
| **测试依据：** |
| **测试目的：**  验证执行风险载荷西门子PLC密码绕过风险的测试，支持西门子S7-1200特定版本的PLC进行的风险测试验证执行风险载荷西门子PLC密码绕过风险的测试，支持西门子S7-1200特定版本的PLC进行的风险测试 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）打开S7-1200风险测试工具箱；  2）连接三根线到上位机：1根网线、2根串口线；  3）在上位机打开TIA16虚拟机，将UART-com插到物理USB接口，物理机识别后导入TIA16虚拟机中；  4）在风险测试文件夹下打开cmd终端；  5）在cmd命令行下输入dump内存密码提取指令，按回车后会提取出密码的hash值；  6）双击TIA16快捷方式打开该软件，按照风险测试对应的PLC配置创建一个新项目；  7）右击桌面x64dbg，选择以管理员身份运行，软件打开后，选择文件菜单》附加选项，将TIA16新建的项目附加进去；  8）双击打开待调试工程项目，如遇到已停止现象，持续按F9直到调试程序处正常显示【运行中】；  9）切换到TIA16编程软件，点击【在线】下【将设备作为新站上传（硬件和软件）】；  10）在弹窗中点击【开始搜索】，选择S7-1200控制器，点击【从设备上传】；  11）上传期间会弹出对话框提示输入密码，此时可以任意输入一个密码，如1234567；  12）当输入密码后，x64dbg调试软件会在核心代码处中断，点击断点处转入内存窗口，将5）步提取出来的hash值拷贝到断点处对应的地址；  13）在x64dbg界面持续按F9按键则可以突破密码保护，将控制器中的程序上传到了上位机中；  14）打开上传的工程文件，可以看到只有输入密码才能查看访问，也同时验证了上传PLC程序时绕过了密码保护。 |
| **预期结果：**  测试应覆盖以下内容：  1）验证西门子PLC内存镜像URAT提取功能  2）验证西门子PLC内存dump功能  3）验证西门子PLC密码获取功能 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 251西门子PLC内存寄存器数据篡改风险测试项

|  |
| --- |
| **测试项目：**西门子PLC内存寄存器数据篡改风险 |
| **测试依据：** |
| **测试目的：**  验证执行风险载荷后西门子PLC内存寄存器篡改风险的测试，支持所有西门子PLC系列进行的风险测试验证执行风险载荷后西门子PLC内存寄存器篡改风险的测试，支持所有西门子PLC系列进行的风险测试 |
| **测试配置：** |
| **测试步骤：**  功能测试方法：  1）建立西门子PLC硬件测试环境：上位机、PLC；  2）用网线连接上位机和PLC，并确保网络通畅；  3）上位机上安装并打开西门子PLC的IDE环境（观测PLC内存寄存器数据变化）；  4）在风险测试文件夹下打开cmd终端；  5）在cmd命令行下输入内存寄存器篡改风险测试指令，按回车后从上位机IDE环境中可以看到对应的内存寄存器的数据已经被篡改；  6）在实际生产环境中，当篡改数据为PID参数时，会颠覆生产工艺逻辑的混乱。 性能测试方法：  1）PLC风险持续到对应寄存器恢复初始值为止；  2）PLC风险响应时间约等于PLC扫描周期。 |
| **预期结果：**  功能测试应覆盖以下内容：  1）验证PLC数据完整性/合理性的破坏功能  2）验证PLC颠覆工艺逻辑功能 性能测试应覆盖以下内容：  1）PLC风险持久性；  2）PLC风险响应时间； |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 252西门子PLC内存映像区数据篡改风险测试项

|  |
| --- |
| **测试项目：**西门子PLC内存寄存器数据篡改风险 |
| **测试依据：** |
| **测试目的：**  验证执行风险载荷后西门子PLC内存映像区数据篡改风险的测试，支持所有西门子PLC系列进行的风险测试验证执行风险载荷后西门子PLC内存映像区数据篡改风险的测试，支持所有西门子PLC系列进行的风险测试 |
| **测试配置：** |
| **测试步骤：**  功能测试方法：  1）建立西门子PLC硬件测试环境：上位机、PLC；  2）用网线连接上位机和PLC，并确保网络通畅；  3）上位机上安装并打开西门子PLC的IDE环境（观测PLC内存寄存器数据变化）；  4）在风险测试文件夹下打开cmd终端；  5）在cmd命令行下输入内存映像区数据篡改风险测试指令，按回车后从上位机IDE环境中可以看到对应的内存映像区的数据已经被篡改；  6）在实际生产环境中，当篡改映像区数据时，会造成设备异常停机或者强制启机，从而导致生产中断。 性能测试方法：  1）PLC风险持续到对应映像区数据恢复初始值为止；  2）PLC风险响应时间约等于PLC扫描周期 |
| **预期结果：**  功能测试应覆盖以下内容：  1）验证PLC数据完整性/合理性的破坏功能  2）验证PLC直接控制设备的破坏功能  性能测试应覆盖以下内容：  1）PLC风险持久性；  2）PLC风险响应时间 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 253倍福PLC缓冲区溢出风险测试项

|  |
| --- |
| **测试项目：**倍福PLC缓冲区溢出风险 |
| **测试依据：** |
| **测试目的：**  验证执行风险载荷后倍福PLC缓冲区溢出风险的测试，支持倍福CX5130系列进行的风险测试验证执行风险载荷后倍福PLC缓冲区溢出风险的测试，支持倍福CX5130系列进行的风险测试 |
| **测试配置：** |
| **测试步骤：**  功能测试方法：  1）建立倍福PLC硬件测试环境：上位机、PLC；  2）用网线连接上位机和PLC，并确保网络通畅；  3）准备秒表等工具（用于监测PLC崩溃时间）；  4）在风险测试文件夹下打开cmd终端；  5）在cmd命令行下输入PLC缓冲区溢出风险测试指令，按回车后PLC崩溃重启。 性能测试方法：  1）使用秒表等工具计算从执行风险测试脚本后到PLC崩溃的时间；  2）PLC风险响应时间的测试结果为3-5秒。 |
| **预期结果：**  功能测试应覆盖以下内容：  1）验证倍福PLC ipv6数据包分割功能  2）验证倍福PLC畸形分片包触发溢出功能 性能测试应覆盖以下内容：  1）倍福PLC风险响应时间 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 254倍福PLC端口扫描风险测试项

|  |
| --- |
| **测试项目：**倍福PLC端口扫描风险 |
| **测试依据：** |
| **测试目的：**  验证执行风险载荷后倍福PLC存在端口扫描风险的测试，支持倍福系列PLC进行的风险测试验证执行风险载荷后倍福PLC存在端口扫描风险的测试，支持倍福系列PLC进行的风险测试 |
| **测试配置：** |
| **测试步骤：**  功能测试方法：  1）建立倍福PLC硬件测试环境：上位机、PLC；  2）用网线连接上位机和PLC，并确保网络通畅；  3）在上位机打开nmap工具；  4）在命令行输入nmap扫描倍福plc命令，执行；  5）会依次扫描出倍福plc的端口号/版本号等信息。 |
| **预期结果：**  功能测试应覆盖以下内容：  1）验证倍福PLC 开放端口探测功能  2）验证倍福PLC服务试别功能  性能测试应覆盖以下内容：  1）倍福PLC扫描端口 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 255西门子PLC控制协议风险测试项

|  |
| --- |
| **测试项目：**西门子PLC控制协议风险 |
| **测试依据：** |
| **测试目的：**  验证执行风险载荷后西门子PLC控制协议风险的测试，支持西门子系列PLC进行的风险测试验证执行风险载荷后西门子PLC控制协议风险的测试，支持西门子系列PLC进行的风险测试 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）建立西门子PLC硬件测试环境：上位机（安装有组态软件，可以读取PLC数据）、PLC；  2）用网线连接上位机和PLC，并确保网络通畅；  3）在风险脚本所在文件夹下打开cmd中断执行脚本；  4）解析出协议关键字段参数：源/目标TSAP、COTP连接参数等；  5）提取出需要劫持的会话，将修改后的数据发送到上位机组态软件，破坏原有协议机制，造成上位机组态显示的数据与实际数据不一致。 |
| **预期结果：**  功能测试应覆盖以下内容：  1）验证西门子PLC 协议解析功能  2）验证西门子PLC会话劫持功能  3）验证西门子PLC协议机制破坏功能  性能测试应覆盖以下内容：  1）西门子PLC控制系统风险延时性 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 256西门子PLC未授权访问风险测试项

|  |
| --- |
| **测试项目：**西门子PLC未授权访问风险 |
| **测试依据：** |
| **测试目的：**  验证执行风险载荷后西门子PLC未授权访问风险的测试，支持西门子系列PLC进行的风险测试验证执行风险载荷后西门子PLC未授权访问风险的测试，支持西门子系列PLC进行的风险测试 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）建立西门子PLC硬件测试环境：上位机、PLC；  2）用网线连接上位机和PLC，并确保网络通畅；  3）在风险脚本所在文件夹下打开cmd终端执行脚本；  4）执行脚本后，会伪造一个plc信任的客户端；  5）以合法客户端的形式发送信息到plc以获取其型号、固件版本号等敏感信息。 |
| **预期结果：**  功能测试应覆盖以下内容：  1）验证西门子PLC 身份伪造功能  2）验证西门子PLC敏感信息获取功能 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 257西门子PLC内存数据窃取风险测试项

|  |
| --- |
| **测试项目：**西门子PLC内存数据窃取风险 |
| **测试依据：** |
| **测试目的：**  验证执行风险载荷后西门子PLC内存数据窃取风险的测试，支持西门子系列PLC进行的风险测试验证执行风险载荷后西门子PLC内存数据窃取风险的测试，支持西门子系列PLC进行的风险测试 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）建立西门子PLC硬件测试环境：上位机、PLC；  2）用网线连接上位机和PLC，并确保网络通畅；  3）在风险脚本所在文件夹下打开cmd终端运行脚本；  4）先进行网络探测，确定通讯协议并进行分析；  5）定位待窃取存储区并进行数据提取。 |
| **预期结果：**  功能测试应覆盖以下内容：  1）验证西门子PLC待窃取存储区扫描定位功能  2）验证西门子PLC工艺数据提取功能  性能测试应覆盖以下内容：  1）西门子PLC控制系统风险延时性<3s |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 258 安全增强新型PLC虚拟化与资源静态分配能力测试项

|  |
| --- |
| **测试项目：**安全增强新型PLC虚拟化与资源静态分配能力 |
| **测试依据：** |
| **测试目的：**  验证安全增强新型PLC采用的虚拟化架构的虚拟化基本能力与资源静态分配能力验证安全增强新型PLC采用的虚拟化架构的虚拟化基本能力与资源静态分配能力 |
| **测试配置：** |
| **测试步骤：**  测试方法：  功能测试：  1）安全增强新型PLC开机，查看串口终端打印，有预期结果1、2、3；  2）在安全增强新型PLC的RTVM0中，运行lspci -tv，有预期结果4；  3）在安全增强新型PLC的RTVM0中，使用phymem工具填充物理内存区域0x140001000-0x140001050为全“FF”。在GPVM中，使用phymem工具读取物理内存区域0x140001000-0x140001050，有预期结果5；  4）在安全增强新型PLC的四个虚拟机（GPVM、RTVM0、RTVM1、RTVM2）中分别运行cat /proc/cpuinfo，有预期结果6；  5）在安全增强新型PLC的四个虚拟机（GPVM、RTVM0、RTVM1、RTVM2）中分别运行ifconfig，有预期结果7；  性能测试：  1）在安全增强新型PLC的RTVM0中，运行./cyclictest -a -m -t -p30，查看虚拟机系统平均抖动，有预期结果8。 |
| **预期结果：**  功能测试应覆盖以下内容：  1）验证安全增强新型PLC具备LoongArch CPU虚拟化功能  2）验证安全增强新型PLC具备stage-2⻚表管理功能  3）验证安全增强新型PLC具备 LoongArch中断控制功能  4）验证安全增强新型PLC具备PCIe虚拟化功能  5）验证安全增强新型PLC虚拟机间具备基于共享内存的通信功能  6）验证安全增强新型PLC具备LoongArch CPU静态分配功能  7）验证安全增强新型PLC具备PCIe网口静态分配功能 性能测试应覆盖以下内容：   1. 验证安全增强新型PLC实时虚拟机操作系统抖动性能<1ms |
| **测试结果：**   1. 安全增强新型PLC具备LoongArch CPU虚拟化功能   2）安全增强新型PLC具备stage-2⻚表管理功能    3)安全增强新型PLC具备 LoongArch中断控制功能 |
| 4)安全增强新型PLC具备PCIe虚拟化功能    5）安全增强新型PLC虚拟机间具备基于共享内存的通信功能    6）安全增强新型PLC具备LoongArch CPU静态分配功能    7）安全增强新型PLC具备PCIe网口静态分配功能    8）安全增强新型PLC实时虚拟机操作系统抖动性能<1ms（平均抖动为4 us）    **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 259 安全增强新型PLC运行时（Runtime）能力测试项

|  |
| --- |
| **测试项目：**安全增强新型PLC运行时（Runtime）能力 |
| **测试依据：** |
| **测试目的：**  验证安全增强新型PLC采用的运行时的基本功能与实时性指标验证安全增强新型PLC采用的运行时的基本功能与实时性指标 |
| **测试配置：** |
| **测试步骤：**  功能测试方法：  1）安全增强新型PLC启动运行样例控制程序；  2）在安全增强新型PLC的上位机IDE中，将控制程序下载至PLC运行时中，有预期结果1；  3）在安全增强新型PLC的上位机IDE中，通过UI界面查看控制程序的参数，有预期结果2；  4）在安全增强新型PLC的上位机IDE中，通过UI界面修改控制程序的参数，有预期结果3； 性能测试方法：  1）安全增强新型PLC启动运行样例控制程序，重复10000个扫描周期的执行，测量记录10000次周期执行时间数据。  2）根据安全增强新型PLC的10000次周期执行时间数据，计算扫描周期执行时间的平均值、标准差、平均相邻周期抖动；  3）安全增强新型PLC切换为（非安全的）常规运行时模式，启动运行样例控制程序，重复10000个扫描周期的执行，测量记录10000次周期执行时间数据； 4）根据常规PLC的10000次周期执行时间数据，计算扫描周期执行时间的平均值、标准差、平均相邻周期抖动；  5）比较安全增强新型PLC和常规运行时模式PLC的周期执行时间的平均值、标准差、平均相邻周期抖动，有预期结果4、5、6。 |
| **预期结果：**  功能测试应覆盖以下内容：  1）验证安全增强新型PLC具备控制程序下载功能  2）验证安全增强新型PLC具备控制程序参数监控功能  3）验证安全增强新型PLC具备控制程序参数配置修改功能  性能测试应覆盖以下内容：  4）验证安全增强新型PLC控制程序扫描周期执行时间开销<1ms  5）验证安全增强新型PLC控制程序扫描周期执行时间标准差开销<1ms  6）验证安全增强新型PLC控制程序扫描周期相邻周期抖动开销<1ms |
| **测试结果：**   1. 安全增强新型PLC具备控制程序下载功能      1. 安全增强新型PLC具备控制程序参数监控功能     3）安全增强新型PLC具备控制程序参数配置修改功能 |
| * 1. 安全增强新型PLC和常规运行时模式PLC的周期执行时间的平均值分别为3037 us和3024 us，安全增强新型PLC控制程序扫描周期执行时间开销<1ms        * 1. 安全增强新型PLC和常规运行时模式PLC的周期执行时间的标准差分别为84 us和61 us，安全增强新型PLC控制程序扫描周期执行时间标准差开销<1ms        * 1. 安全增强新型PLC和常规运行时模式PLC的周期执行时间的相邻周期抖动分别为16 us和9 us，安全增强新型PLC控制程序扫描周期相邻周期抖动开销<1ms |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 260 安全增强新型PLC攻击防护能力测试项

|  |
| --- |
| **测试项目：**安全增强新型PLC攻击防护能力 |
| **测试依据：** |
| **测试目的：**  验证PLC典型攻击载荷执行后的安全增强新型PLC攻击防护能力，赋予攻击者在安全增强新型PLC系统侧进行典型PLC攻击的模拟执行，无需从ICS网络侧执行层层的攻击渗透验证PLC典型攻击载荷执行后的安全增强新型PLC攻击防护能力，赋予攻击者在安全增强新型PLC系统侧进行典型PLC攻击的模拟执行，无需从ICS网络侧执行层层的攻击渗透 |
| **测试配置：** |
| **测试步骤：**  功能测试方法：  1）安全增强新型PLC启动运行样例控制程序；  2）攻击者SSH远程登录安全增强新型PLC的vPLC1（RTVM1）；  3）登录后，执行控制逻辑篡改攻击脚本，对vPLC1当前执行的样例控制程序的逻辑进行篡改。有预期结果1；  4）安全增强新型PLC复位，重新启动运行样例控制程序；  5）攻击者SSH远程登录安全增强新型PLC的vPLC1（RTVM1）；  6）登录后，执行DoS攻击脚本，使vPLC1当前系统崩溃。有预期结果2；  7）安全增强新型PLC复位，重新启动运行样例控制程序；  8）攻击者SSH远程登录安全增强新型PLC的vPLC1（RTVM1）；  9）登录后，执行控制参数篡改攻击脚本，对vPLC1当前执行的样例控制程序的配置参数进行篡改。有预期结果3； |
| **预期结果：**  功能测试应覆盖以下内容：  1）验证安全增强新型PLC具备控制逻辑篡改攻击防护功能  2）验证安全增强新型PLC具备控制参数篡改攻击防护功能  3）验证安全增强新型PLC具备DoS攻击防护功能 |
| **测试结果：**   1. 安全增强新型PLC中的RTVM0能够检测到攻击（攻击状态：1）；安全增强新型PLC的GPVM最终记录的输出仍维持正常，未受到攻击影响，安全增强新型PLC具备控制逻辑篡改攻击防护功能      1. 安全增强新型PLC中的RTVM0能够检测到攻击（攻击状态：1）；安全增强新型PLC的GPVM最终记录的输出仍维持正常，未受到攻击影响，安全增强新型PLC具备控制参数篡改攻击防护功能     3）安全增强新型PLC中的RTVM0能够检测到攻击（攻击状态：3）；安全增强新型PLC的GPVM最终记录的输出仍维持正常，未受到攻击影响，安全增强新型PLC具备DoS攻击防护功能 |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 261 安全增强新型PLC轻量化I/O异常检测算法测试项

|  |
| --- |
| **测试项目：**安全增强新型 PLC 轻量化 I/O 异常检测算法 |
| **测试依据：** |
| **测试目的：**  验证安全增强新型 PLC 采用的轻量化 I/O 异常检测算法的功能、准确性、误报率及综合性能指标。验证安全增强新型 PLC 采用的轻量化 I/O 异常检测算法的功能、准确性、误报率及综合性能指标。 |
| **测试配置：** |
| **测试步骤：**  功能测试方法：  1） 将预处理后的SWaT数据集输入至安全增强新型PLC，启动轻量化I/O异常检测算法。  2） 记录检测结果中识别到的异常数据点和正常数据点的数量及比例。  3） 查看轻量化I/O异常检测算法对SWaT数据集的检测结果，观察是否能够识别出异常数据点，有预期结果1。 性能测试方法：  1） 安全增强新型 PLC 启动运行基于SWaT数据集数据处理程序，并生成降噪处理后包含已标注的正常和异常数据的测试数据集，数据集大小为 496800个数据样本；  2） 使用轻量化 I/O 异常检测算法对测试数据集进行检测，记录检测结果中的不同统计特征检测到的异常数据与正常数据比例； 根据记录的数据计算准确率、误报率和调和平均分数（F1）。有预期结果2、3、4。 |
| **预期结果：**  功能测试应覆盖以下内容：  1）验证安全增强新型 PLC 采用的轻量化 I/O 异常检测算法具备异常检测功能。 性能测试应覆盖以下内容：  2） 验证安全增强新型 PLC 轻量化 I/O 异常检测算法准确率 ≥95%  3） 验证安全增强新型 PLC 轻量化 I/O 异常检测算法误报率 ≤16%  4） 验证安全增强新型 PLC 轻量化 I/O 异常检测算法调和平均分数（F1）≥0.7 |
| **测试结果：**   1. 安全增强新型 PLC 采用的轻量化 I/O 异常检测算法具备异常检测功能      1. 安全增强新型 PLC 轻量化 I/O 异常检测算法准确率 ≥95%      1. 安全增强新型 PLC 轻量化 I/O 异常检测算法误报率 ≤16%     4） 安全增强新型 PLC 轻量化 I/O 异常检测算法调和平均分数（F1）≥0.7 |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 262 新型复合智能机器人PLC渗透攻击大飞机移载对接自动化攻击测试项

|  |
| --- |
| **测试项目：**新型复合智能机器人PLC渗透攻击大飞机移载对接自动化攻击测试 |
| **测试依据：** |
| **测试目的：**  验证新型复合智能机器人PLC渗透攻击大飞机移载对接自动化攻击，网络拓扑图，脚本执行过程和结果实时显示，攻击功能需稳定可靠验证新型复合智能机器人PLC渗透攻击大飞机移载对接自动化攻击，网络拓扑图，脚本执行过程和结果实时显示，攻击功能需稳定可靠 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1) 进入【靶标管理/PLC渗透攻击大飞机移载对接】界面，点击<调试靶标>按钮  2) 调试成功以后，点击选择ATTACK节点，点击<系统>、<远程连接>，进入虚拟window远程页面  3) 输入命令cmd，打开命令终端，输入命令patk2.3.exe 10.10.11.100 s1 par\_v1 60，进行水平方向攻击  4) 终端输入patk2.3.exe 10.10.11.100 s1 ver\_h1 3，进垂直方向攻击  5) 执行步骤1，调试成功以后，点击<自动化攻击>  6) 执行步骤1、2，点击<一键攻击>，进入执行中状态  7) 执行步骤1、2，切换到分步骤渗透，点击<执行>，开始进行分过程攻击  8) 前一过程攻击完成后，进行下一攻击过程，顺序进行  9) 执行步骤1、2，点击<重置>，进入重置中  10) 执行步骤4，攻击脚本执行过程实时显示攻击命令和结果  11) 执行步骤4，网络拓扑图节点设备和连线展示攻击链 |
| **预期结果：**  测试应覆盖以下内容：  1) 支持脚本直接对移载对接垂直参数（高度）攻击  2) 支持脚本直接对移载对接水平参数（平移速度）攻击  3) 支持移载对接自动化一键渗透  4) 支持移载对接分步骤渗透，顺序进行  5) 支持移载对接重置恢复到攻击初始状态  6) 支持移载对接自动化攻击实时显示攻击脚本执行过程  7) 支持移载对接自动化攻击移载对接同步显示攻击点位网络拓扑 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 263 新型复合智能机器人PLC渗透攻击大飞机移载对接仿真可视化验证测试项

|  |
| --- |
| **测试项目：**新型复合智能机器人PLC渗透攻击大飞机移载对接仿真可视化验证测试 |
| **测试依据：** |
| **测试目的：**  新型复合智能机器人PLC渗透攻击大飞机移载对接仿真可视化验证，网络拓扑图，脚本执行过程和结果实时显示，仿真可视化验证功能需稳定可靠新型复合智能机器人PLC渗透攻击大飞机移载对接仿真可视化验证，网络拓扑图，脚本执行过程和结果实时显示，仿真可视化验证功能需稳定可靠 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1) 进入【靶标管理/PLC渗透攻击大飞机移载对接】界面，点击<调试靶标>按钮  2) 调试成功以后，点击<自动化攻击>  3) 进入自动化攻击页面后，自动化一键渗透下拉  4) 点击<一键攻击>，进入执行中状态  5) 重新回到PLC渗透攻击大飞机移载对接页面，点击<仿真视图>  6) 进入仿真视图，加载完成以后，视图中设备进行移动切换  7) 执行步骤1、2、3、4、5，网络拓扑图根据攻击链路红色闪烁  8) 执行步骤1、2、3、4、5，脚本执行过程根据设备点切换输出对应执行脚本  9) 执行步骤1、2、3、4、5，攻击类型同步展示根据攻击设备点输出对应攻击节点和时间  10) 执行步骤1、2、3、4、5，攻击到最后节点PLC被篡改，实时参数显示实时对接  11) 执行步骤1、2、3、4、5，攻击完成以后，仿真视图移载对接中设备进行实时对接，最后发生偏移 |
| **预期结果：**  测试应覆盖以下内容：  1) 支持移载对接仿真可视化验证进行攻击，被攻击视图设备实时切换  2) 支持移载对接仿真可视化验证进行攻击，实时显示被攻击点位网络拓扑图  3) 支持移载对接仿真可视化验证进行攻击，分析实时获取攻击脚本  4) 支持移载对接仿真可视化验证进行攻击，攻击日志同步展示  5) 支持移载对接仿真可视化验证进行攻击，实时显示舱段对接细节 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 264 安全增强PLC渗透攻击大飞机移载对接防御测试项

|  |
| --- |
| **测试项目：**安全增强PLC渗透攻击大飞机移载对接防御测试项 |
| **测试依据：** |
| **测试目的：**  安全增强PLC渗透攻击大飞机移载对接防御，网络拓扑图，脚本执行过程和结果实时显示，移载对接防御功能需稳定可靠安全增强PLC渗透攻击大飞机移载对接防御，网络拓扑图，脚本执行过程和结果实时显示，移载对接防御功能需稳定可靠 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1) 系统切换至安全增强新型PLC，替代西门子PLC操控移载对接业务场景；  2) 对安全增强新型PLC执行水平参数篡改攻击脚本；  3) 验证安全增强新型PLC（防御数字孪生系统）可以检测到攻击并告警；  4) 同步验证移载对接过程正常；  5) 系统状态复位；  6) 对安全增强新型PLC执行垂直参数篡改攻击脚本；  7) 验证安全增强新型PLC（防御数字孪生系统）可以检测到攻击并告警；  8) 同步验证移载对接过程正常。 |
| **预期结果：**  测试应覆盖以下内容：  1) 支持切换安全增强新型PLC后水平参数篡改攻击下可检测攻击并告警  2) 支持切换安全增强新型PLC后水平参数篡改攻击下移载对接正常  3) 支持切换安全增强新型PLC后垂直参数篡改攻击下可检测攻击并告警  4) 支持切换安全增强新型PLC后垂直参数篡改攻击下移载对接正常 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 265 新型复合智能机器人PLC渗透攻击大飞机协同装配自动化攻击测试项

|  |
| --- |
| **测试项目：**新型复合智能机器人PLC渗透攻击大飞机协同装配自动化攻击测试 |
| **测试依据：** |
| **测试目的：**  验证新型复合智能机器人PLC渗透攻击大飞机协同装配自动化攻击，网络拓扑图，脚本执行过程和结果实时显示，攻击功能需稳定可靠验证新型复合智能机器人PLC渗透攻击大飞机协同装配自动化攻击，网络拓扑图，脚本执行过程和结果实时显示，攻击功能需稳定可靠 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1) 进入【靶标管理/PLC渗透攻击大飞机协同装配】界面，点击<调试靶标>按钮  2) 调试成功以后，点击选择ATTACK节点，点击<系统>、<远程连接>，进入虚拟window远程页面  3) 输入命令cmd，打开命令终端，输入命令patk2.3.exe 10.10.12.100 s1 dhlv\_x 12，patk2.3.exe 10.10.12.100 s1 dhlv\_y 12，进行平面参数攻击  4) 终端输入patk2.3.exe 10.10.12.100 s1 dhlv\_z 12，进深度参数攻击  5) 执行步骤1，调试成功以后，点击<自动化攻击>  6) 执行步骤1、2，点击<一键攻击>，进入执行中状态  7) 执行步骤1、2，切换到分步骤渗透，点击<执行>，开始进行分过程攻击  8) 前一过程攻击完成后，进行下一攻击过程，顺序进行  9) 执行步骤1、2，点击<重置>，进入重置中  10) 执行步骤4，攻击脚本执行过程实时显示攻击命令和结果  11) 执行步骤4，网络拓扑图节点设备和连线展示攻击链 |
| **预期结果：**  测试应覆盖以下内容：  1) 支持脚本直接对协同装配平面参数（机械臂X轴、Y轴）攻击  2) 支持脚本直接对协同装配深度参数（机械臂Z轴）攻击  3) 支持协同装配自动化一键渗透  4) 支持协同装配分步骤渗透  5) 支持协同装配重置恢复到攻击初始状态  6) 支持协同装配自动化攻击实时显示攻击脚本执行过程  7) 支持协同装配自动化攻击同步显示攻击点位网络拓扑 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 266 新型复合智能机器人PLC渗透攻击大飞机协同装配仿真可视化验证测试项

|  |
| --- |
| **测试项目：**新型复合智能机器人PLC渗透攻击大飞机协同装配仿真可视化验证测试 |
| **测试依据：** |
| **测试目的：**  新型复合智能机器人PLC渗透攻击大飞机协同装配仿真可视化验证，网络拓扑图，脚本执行过程和结果实时显示，仿真可视化验证功能需稳定可靠新型复合智能机器人PLC渗透攻击大飞机协同装配仿真可视化验证，网络拓扑图，脚本执行过程和结果实时显示，仿真可视化验证功能需稳定可靠 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1) 进入【靶标管理/PLC渗透攻击大飞机协同装配】界面，点击<调试靶标>按钮  2) 调试成功以后，点击<自动化攻击>  3) 进入自动化攻击页面后，自动化一键渗透下拉  4) 点击<一键攻击>，进入执行中状态  5) 重新回到PLC渗透攻击大飞机移载对接页面，点击<仿真视图>  6) 进入仿真视图，加载完成以后，视图中设备进行移动切换  7) 执行步骤1、2、3、4、5，网络拓扑图根据攻击链路红色闪烁  8) 执行步骤1、2、3、4、5，脚本执行过程根据设备点切换输出对应执行脚本  9) 执行步骤1、2、3、4、5，攻击类型同步展示根据攻击设备点输出对应攻击节点和时间  10) 执行步骤1、2、3、4、5，攻击到最后节点PLC被篡改，实时参数显示实时对接  11) 执行步骤1、2、3、4、5，攻击完成以后，仿真视图协同装配钻孔中设备进行实时对接，最后发生偏移 |
| **预期结果：**  测试应覆盖以下内容：  1) 支持协同装配仿真可视化验证攻击中设备实时切换  2) 支持协同装配仿真可视化验证实时显示网络拓扑图  3) 支持协同装配仿真可视化验证实时显示脚本执行过程  4) 支持协同装配仿真可视化验证攻击类型同步展示  5) 支持仿协同装配真视图支持显示实时参数  6) 支持协同装配设备被攻击仿真可视化验证钻孔发生偏移 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 267 安全增强PLC渗透攻击大飞机协同装配防御测试项

|  |
| --- |
| **测试项目：**安全增强PLC渗透攻击大飞机协同装配防御测试 |
| **测试依据：** |
| **测试目的：**  安全增强PLC渗透攻击大飞机协同装配防御，网络拓扑图，脚本执行过程和结果实时显示，协同装配防御功能需稳定可靠安全增强PLC渗透攻击大飞机协同装配防御，网络拓扑图，脚本执行过程和结果实时显示，协同装配防御功能需稳定可靠 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1) 系统切换至安全增强新型PLC，替代西门子PLC操控协同钻孔业务场景；  2) 对安全增强新型PLC执行平面参数篡改攻击脚本；  3) 验证安全增强新型PLC（防御数字孪生系统）可以检测到攻击并告警；  4) 同步验证协同钻孔过程正常；  5) 系统状态复位；  6) 对安全增强新型PLC执行深度参数篡改攻击脚本；  7) 验证安全增强新型PLC（防御数字孪生系统）可以检测到攻击并告警；  8) 同步验证协同钻孔过程正常。 |
| **预期结果：**  测试应覆盖以下内容：  1) 切换安全增强新型PLC后平面参数篡改攻击下可检测攻击并告警  2) 切换安全增强新型PLC后平面参数篡改攻击下协同钻孔正常  3) 切换安全增强新型PLC后深度参数篡改攻击下可检测攻击并告警  4) 切换安全增强新型PLC后深度参数篡改攻击下协同钻孔正常 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 268 安全增强PLC渗透窃取边缘侧关键数据自动化攻击测试项

|  |
| --- |
| **测试项目：**安全增强PLC渗透窃取边缘侧关键数据自动化攻击测试 |
| **测试依据：** |
| **测试目的：**  验证安全增强PLC渗透窃取边缘侧关键数据自动化攻击，网络拓扑图，脚本执行过程和结果实时显示，攻击功能需稳定可靠验证安全增强PLC渗透窃取边缘侧关键数据自动化攻击，网络拓扑图，脚本执行过程和结果实时显示，攻击功能需稳定可靠 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1) 进入【靶标管理/PLC渗透窃取边缘侧关键数据】界面，点击<调试靶标>按钮  2) 调试成功以后，点击选择ATTACK节点，点击<系统>、<远程连接>，进入虚拟window远程页面  3) 输入命令cmd，打开命令终端，输入命令patk2.3.exe 10.10.13.100 s3 dt，进行数据窃取攻击  4) 执行步骤1，调试成功以后，点击<自动化攻击>  5) 执行步骤1、2，点击<一键攻击>，进入执行中状态  6) 执行步骤1、2，切换到分步骤渗透，点击<执行>，开始进行分过程攻击  7) 前一过程攻击完成后，进行下一攻击过程，顺序进行  8) 执行步骤1、2，点击<重置>，进入重置中  9) 执行步骤4，攻击脚本执行过程实时显示攻击命令和结果  10) 执行步骤4，网络拓扑图节点设备和连线展示攻击链 |
| **预期结果：**  测试应覆盖以下内容：  1) 支持脚本直接对plc关键数据窃取攻击  2) 支持窃取边缘侧关键数据自动化一键渗透  3) 支持窃取边缘侧关键数据分步骤渗透  4) 支持窃取边缘侧关键数据重置恢复到攻击初始状态  5) 支持窃取边缘侧关键数据自动化攻击实时显示攻击脚本执行过程  6) 窃取边缘侧关键数据自动化攻击显示网络实时拓扑 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 269 安全增强PLC渗透窃取边缘侧关键数据仿真可视化验证测试项

|  |
| --- |
| **测试项目：**新型复合智能机器人PLC渗透攻击大飞机协同装配仿真可视化验证测试 |
| **测试依据：** |
| **测试目的：**  安全增强PLC渗透窃取边缘侧关键数据仿真可视化验证，网络拓扑图，脚本执行过程和结果实时显示，仿真可视化验证功能需稳定可靠安全增强PLC渗透窃取边缘侧关键数据仿真可视化验证，网络拓扑图，脚本执行过程和结果实时显示，仿真可视化验证功能需稳定可靠 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1) 进入【靶标管理/PLC渗透窃取边缘侧关键数据】界面，点击<调试靶标>按钮  2) 调试成功以后，点击<自动化攻击>  3) 进入自动化攻击页面后，自动化一键渗透下拉  4) 点击<一键攻击>，进入执行中状态  5) 重新回到PLC渗透攻击大飞机移载对接页面，点击<仿真视图>  6) 进入仿真视图，加载完成以后，视图中设备进行移动切换  7) 执行步骤1、2、3、4、5，网络拓扑图根据攻击链路红色闪烁  8) 执行步骤1、2、3、4、5，脚本执行过程根据设备点切换输出对应执行脚本  9) 执行步骤1、2、3、4、5，攻击类型同步展示根据攻击设备点输出对应攻击节点和时间  10) 执行步骤1、2、3、4、5，攻击到最后节点PLC被篡改，实时参数显示实时数据 |
| **预期结果：**  测试应覆盖以下内容：  1) 支持窃取边缘侧关键数据仿真可视化验证攻击中设备实时切换  2) 支持窃取边缘侧关键数据仿真可视化验证实时显示网络拓扑图  3) 支持窃取边缘侧关键数据仿真可视化验证实时显示脚本执行过程  4) 支持窃取边缘侧关键数据仿真可视化验证攻击类型同步展示  5) 支持窃取边缘侧关键数据仿真可视化验证支持显示实时参数 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 270 安全增强PLC渗透窃取边缘侧关键数据防御测试项

|  |
| --- |
| **测试项目：**安全增强PLC渗透窃取边缘侧关键数据防御测试 |
| **测试依据：** |
| **测试目的：**  安全增强PLC渗透窃取边缘侧关键数据防御，验证PLC典型渗透攻击的联动防护能力，赋予攻击者在安全增强新型PLC攻击时，通过联动设备防护手段进行防护安全增强PLC渗透窃取边缘侧关键数据防御，验证PLC典型渗透攻击的联动防护能力，赋予攻击者在安全增强新型PLC攻击时，通过联动设备防护手段进行防护 |
| **测试配置：** |
| **测试步骤：**  测试方法：  (1) 将白名单外的 xxx.exe，复制到 U 盘中，插入PLC上位主机；  (2) 在 U 盘中执行 xxx.exe；  (3) 将白名单外的 xxx.exe，复制到上位机桌面上；  (4) 在桌面上执行 xxx.exe。  (5) 进入安全基线模块；  (6) 点击[一键加固]；  (7) 加固包含密码长度至少8字符；新密码设置至少包含一个大写密码长度至少8字符；新密码设置至少包含一个大写字母；新密码设置至少包含一个小写字母；新密码设置至少包含一个数字字符；密码最长使用期限为90天；密码最短使用时间为0天；etc/passwd文件访问权限为644等20多项基线加固。  (8) 点击[恢复初始]。  (9) 进入安全增强新型PLC系统；  (10) 启用系统安全防火墙，设置IP安全防护规则；  (11) 合法IP主机尝试连接安全增强新型PLC；  (12) 非法IP主机尝试连接安全增强新型PLC；  (13) 启用业务逻辑组态校验功能；  (14) 上位机下发合法业务逻辑组态至安全增强新型PLC  (15) 上位机下发非法业务逻辑组态至安全增强新型PLC  验证：  1、步骤 （2）程序不可执行，查看“实时风险报警”中产生报警日志；  2、步骤（4） 程序不可执行，查看“实时风险报警”中产生报警日志。  3、步骤( 6），点击一键加固成功，主机卫士安全基线项与操作建议项一致 ；  5、步骤( 7)，恢复初始成功，安全基线项还原回安装主机卫士前的初始状态；  6、步骤(10），合法IP主机可以连接安全增强新型PLC；  7、步骤(11），非法IP主机无法连接安全增强新型PLC；  8、步骤(13），PLC执行合法业务逻辑组态，正常运行；  9、步骤(14），PLC检测到非法业务逻辑组态，非法组态不能运行。 |
| **预期结果：**  测试应覆盖以下内容：  1、安终端组态软件安全防护功能  2、安终端安全基线灵活部署能力  3、安全增强新型PLC IP防火墙功能，步骤(10），合法IP主机可以连接安全增强新型PLC，步骤(11），非法IP主机无法连接安全增强新型PLC。  4、安全增强新型PLC业务逻辑组态校验功能，步骤(13），PLC执行合法业务逻辑组态，正常运行，步骤(14），PLC检测到非法业务逻辑组态，非法组态不能运行。 |
|  |
| **测试结果：**  3、安全增强新型PLC IP防火墙功能，步骤(10），合法IP主机可以连接安全增强新型PLC，步骤(11），非法IP主机无法连接安全增强新型PLC。        4、安全增强新型PLC业务逻辑组态校验功能，步骤(13），PLC执行合法业务逻辑组态，正常运行，步骤(14），PLC检测到非法业务逻辑组态，非法组态不能运行。 |
|  |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 271 异构新型末端工业设备内嵌安全隔离防护平台硬件架构兼容性测试项

|  |
| --- |
| **测试项目：**异构新型末端工业设备内嵌安全隔离防护平台硬件架构兼容性测试 |
| **测试依据：** |
| **测试目的：**  测试异构新型末端工业设备内嵌安全隔离防护平台支持3种指令集架构测试异构新型末端工业设备内嵌安全隔离防护平台支持3种指令集架构 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）编译一个合适的linux镜像文件和dtb文件  2）设置各架构硬件对应的配置文件  3）编译安全基座内核镜像  4）替换安全基座内核镜像  5）断电重新  6）检查安全基座是否正常启动 |
| **预期结果：**  测试应覆盖以下内容：  1）平台能够运行在x86指令集架构的硬件设备上  2）平台能够运行在arm指令集架构的硬件设备上  3）平台能够运行在qemu模拟的riscv指令集架构的硬件设备上 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 272 异构新型末端工业设备内嵌安全隔离防护平台操作系统兼容性测试项

|  |
| --- |
| **测试项目：**异构新型末端工业设备内嵌安全隔离防护平台操作系统兼容性测试 |
| **测试依据：** |
| **测试目的：**  测试异构新型末端工业设备内嵌安全隔离防护平台支持3种以上主流嵌入式操作系统，支持实时性业务、非实时业务与安全功能的并行执行与安全隔离测试异构新型末端工业设备内嵌安全隔离防护平台支持3种以上主流嵌入式操作系统，支持实时性业务、非实时业务与安全功能的并行执行与安全隔离 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）部署启动异构新型末端工业设备内嵌安全隔离防护平台  2）准备Linux、linux-rt、nimbos系统镜像  3）依次安装Linux、linux-rt、nimbos操作系统  4）验证各操作系统是否正常运行 |
| **预期结果：**  测试应覆盖以下内容：  1）平台能够运型linux操作系统  2）平台能够运行linux-rt操作系统  3）平台能够运行nimbos操作系统 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 273 异构新型末端工业设备内嵌安全隔离防护平台安全隔离测试项

|  |
| --- |
| **测试项目：**异构新型末端工业设备内嵌安全隔离防护平台实时性业务、非实时业务与安全功能的并行执行与安全隔离测试 |
| **测试依据：** |
| **测试目的：**  测试异构新型末端工业设备内嵌安全隔离防护平台支持创建多个隔离域，分别运行实时任务与非实时任务测试异构新型末端工业设备内嵌安全隔离防护平台支持创建多个隔离域，分别运行实时任务与非实时任务 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）部署启动异构新型末端工业设备内嵌安全隔离防护平台  2）创建两个VM  3）分别安装Linux、linux-rt  4）linux-rt中安装plc runtime和国密模块  5）linux中安装北向异常检测模块、设备指纹、南向异常检测模型  6）验证各功能模块是否正常运行 |
| **预期结果：**  测试应覆盖以下内容：  1）平台创建隔离域  2）隔离域分别运行操作系统  3）实时域运行plc runtime，非实时域运行内嵌安全增强功能 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 274 北向异常检测功能测试项

|  |
| --- |
| **测试项目：**异常检测功能 |
| **测试依据：** |
| **测试目的：**  验证系统能否准确检测负载当中存在的异常指令验证系统能否准确检测负载当中存在的异常指令 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）通过JS生成满足定义的工控协议的包，包括以下负载类型：正常指令、频繁登录、可能的DDoS攻击指令、频繁的APP指令、带有非法参数的APP指令、带有错误参数的config指令、带有错误参数的URL查询、访问不存在的URL指令、以及过大负载的请求，并将其加密后发送至Agent 2。随后对其输出日志进行分析，日志当中所示检测出的异常应具有90%以上的准确率。  2）对于检测出的异常，对比其输出的日志与报告给大屏的显示结果，需要保证其显示结果与记录的日志在事件数量及异常数量上能够对应。 |
| **预期结果：**  测试应覆盖以下内容：  3）对于满足协议的包，检查其输出日志，查看是否成功检测出异常指令。  4）对于检测出的异常，检查其是否报告给大屏。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 275 设备指纹识别功能测试项

|  |
| --- |
| **测试项目：**设备指纹识别功能测试 |
| **测试依据：** |
| **测试目的：**  验证系统能否正确从模拟南向设备或数据包文件读取扫描周期数据、能否准确分析扫描周期数据判断设备身份验证系统能否正确从模拟南向设备或数据包文件读取扫描周期数据、能否准确分析扫描周期数据判断设备身份 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）在模拟南向设备上运行模拟器程序，启动系统向指定地址、指定端口的设备读取数据100条，对比读取数据与生成数据数量是否对应，丢包率应小于10%。  2）将测试用例集中.jsonl格式数据包文件放入 指纹.py 程序同路径下的fingerprints文件夹下，检查能否正常读取。  3）准备多组已知设备身份数据，导入系统分析，对比分析结果与实际情况，准确率应大于90%。  4）在模拟南向设备上运行模拟器程序，使用测试用例集里的数据模拟实际南向设备的响应周期特征。启动系统读取数据，记录指纹，再读取一次数据，根据读取数据确认设备身份信息，对比分析结果与实际情况，准确率应大于90%。 |
| **预期结果：**  测试应覆盖以下内容：  1）测试从模拟南向设备实时读取数据功能，检查数据准确性和连续性。  2）测试从不同格式数据包文件读取数据功能，验证数据读取成功率。  3）使用已知设备身份的扫描周期数据进行分析，检查判断结果准确性。  4）测试实时读取情况下系统分析结果的准确性。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 276 国密加密功能测试项

|  |
| --- |
| **测试项目：**国密加密功能 |
| **测试依据：** |
| **测试目的：**  验证系统能否正确进行数据的加解密与加密传输验证系统能否正确进行数据的加解密与加密传输 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）自动生成可能的数据并由Agent 1或者Agent2进行加密解密操作，对于多条生成数据，需要保证解密后的数据与加密之前的数据完全对应。  2）使用wireshark等工具抓取PLC与上位机之间的通讯包，检查是否为加密状态。 |
| **预期结果：**  测试应覆盖以下内容：  1）测试数据的加密和解密功能，检查加密算法的准确性  2）测试数据传输过程中的加密状况，保证全程加密传输 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 277 南向异常检测功能测试项

|  |
| --- |
| **测试项目：**异常检测功能 |
| **测试依据：** |
| **测试目的：**  验证系统能否准确检测异常数据验证系统能否准确检测异常数据 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）导入模型。通过先前定义好的config和model.pth进行模型导入。  2）处理数据，预处理数据，随后通过data\_queue将测试集模拟为数据流形式  3）数据重构，将数据流输入模型，获得重构后的数据流  4）确定阈值，计算重构数据与原始数据的MSE并记录在threshold\_queue中，将该队列中高于99%数值的点作为阈值  5）动态调整阈值：将计算获得的MSE输入threshold\_queue，从而动态调整阈值  6）检测异常，MSE将高于阈值的点视作异常值 |
| **预期结果：**  测试应覆盖以下内容：  1）对于以数据流形式输入模型的数据，检测器是否能输出异常值。  2）对于检测出的异常，检查其是否能够进行记录。 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 278 形式化验证：模式验证-案例1测试项

|  |
| --- |
| **测试项目：**形式化验证：模式验证-案例1 |
| **测试依据：** |
| **测试目的：**  测试模式验证第一种模式 pattern-implication测试模式验证第一种模式 pattern-implication |
| **测试配置：** |
| **测试步骤：**  测试方法：  1） 点击项目按钮，点击右上角导入项目按钮，选择提供的test\_plc\_verif.zip压缩包，点击项目按钮右上角的设置按钮。进入设置页面后勾选启用形式化验证，并填写下方的可执行文件路径分别为提供的nuXmv-2.1.0-win64.zip的bin文件夹中的nuXmv.exe和plcverif\_cli.zip解压后的eclipsec.exe（此操作只需进行一次）。  2） 点击页面左侧形式化验证文字右侧加号按钮填写验证信息（根据附件） 填写完成后点击右上角对号按钮。点击验证按钮开始验证  3） 点击验证按钮开始验证 |
| **预期结果：**  测试应覆盖以下内容：  1）模式验证第一种模式 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 279 形式化验证：模式验证-案例2测试项

|  |
| --- |
| **测试项目：**形式化验证：模式验证-案例2 |
| **测试依据：** |
| **测试目的：**  测试模式验证第二种模式 pattern-invariant测试模式验证第二种模式 pattern-invariant |
| **测试配置：** |
| **测试步骤：**  测试方法：  1） 点击项目按钮，点击右上角导入项目按钮，选择提供的test\_plc\_verif.zip压缩包，点击项目按钮右上角的设置按钮。进入设置页面后勾选启用形式化验证，并填写下方的可执行文件路径分别为提供的nuXmv-2.1.0-win64.zip的bin文件夹中的nuXmv.exe和plcverif\_cli.zip解压后的eclipsec.exe（此操作只需进行一次）。  2） 点击页面左侧形式化验证文字右侧加号按钮填写验证信息（根据附件） 填写完成后点击右上角对号按钮。点击验证按钮开始验证  3） 点击验证按钮开始验证 |
| **预期结果：**  测试应覆盖以下内容：  1）模式验证第二种模式 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 280 形式化验证：模式验证-案例3测试项

|  |
| --- |
| **测试项目：**形式化验证：模式验证-案例3 |
| **测试依据：** |
| **测试目的：**  测试模式验证第三种模式 pattern-forbidden测试模式验证第三种模式 pattern-forbidden |
| **测试配置：** |
| **测试步骤：**  测试方法：  1） 点击项目按钮，点击右上角导入项目按钮，选择提供的test\_plc\_verif.zip压缩包，点击项目按钮右上角的设置按钮。进入设置页面后勾选启用形式化验证，并填写下方的可执行文件路径分别为提供的nuXmv-2.1.0-win64.zip的bin文件夹中的nuXmv.exe和plcverif\_cli.zip解压后的eclipsec.exe（此操作只需进行一次）。  2） 点击页面左侧形式化验证文字右侧加号按钮填写验证信息（根据附件） 填写完成后点击右上角对号按钮。点击验证按钮开始验证  3） 点击验证按钮开始验证 |
| **预期结果：**  测试应覆盖以下内容：  1）模式验证第三种模式 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 281 形式化验证：模式验证-案例4测试项

|  |
| --- |
| **测试项目：**形式化验证：模式验证-案例4 |
| **测试依据：** |
| **测试目的：**  测试模式验证第四种模式 pattern-statechange-duringcycle测试模式验证第四种模式 pattern-statechange-duringcycle |
| **测试配置：** |
| **测试步骤：**  测试方法：  1） 点击项目按钮，点击右上角导入项目按钮，选择提供的test\_plc\_verif.zip压缩包，点击项目按钮右上角的设置按钮。进入设置页面后勾选启用形式化验证，并填写下方的可执行文件路径分别为提供的nuXmv-2.1.0-win64.zip的bin文件夹中的nuXmv.exe和plcverif\_cli.zip解压后的eclipsec.exe（此操作只需进行一次）。  2） 点击页面左侧形式化验证文字右侧加号按钮填写验证信息（根据附件） 填写完成后点击右上角对号按钮。点击验证按钮开始验证  3） 点击验证按钮开始验证 |
| **预期结果：**  测试应覆盖以下内容：  1）模式验证第四种模式 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 282 形式化验证：模式验证-案例5测试项

|  |
| --- |
| **测试项目：**形式化验证：模式验证-案例5 |
| **测试依据：** |
| **测试目的：**  测试模式验证第五种模式 pattern-statechange-betweencycles测试模式验证第五种模式 pattern-statechange-betweencycles |
| **测试配置：** |
| **测试步骤：**  测试方法：  1） 点击项目按钮，点击右上角导入项目按钮，选择提供的test\_plc\_verif.zip压缩包，点击项目按钮右上角的设置按钮。进入设置页面后勾选启用形式化验证，并填写下方的可执行文件路径分别为提供的nuXmv-2.1.0-win64.zip的bin文件夹中的nuXmv.exe和plcverif\_cli.zip解压后的eclipsec.exe（此操作只需进行一次）。  2） 点击页面左侧形式化验证文字右侧加号按钮填写验证信息（根据附件） 填写完成后点击右上角对号按钮。点击验证按钮开始验证  3） 点击验证按钮开始验证 |
| **预期结果：**  测试应覆盖以下内容：  1）模式验证第五种模式 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 283 形式化验证：模式验证-案例6测试项

|  |
| --- |
| **测试项目：**形式化验证：模式验证-案例6 |
| **测试依据：** |
| **测试目的：**  测试模式验证第六种模式 pattern-reachability测试模式验证第六种模式 pattern-reachability |
| **测试配置：** |
| **测试步骤：**  测试方法：  1） 点击项目按钮，点击右上角导入项目按钮，选择提供的test\_plc\_verif.zip压缩包，点击项目按钮右上角的设置按钮。进入设置页面后勾选启用形式化验证，并填写下方的可执行文件路径分别为提供的nuXmv-2.1.0-win64.zip的bin文件夹中的nuXmv.exe和plcverif\_cli.zip解压后的eclipsec.exe（此操作只需进行一次）。  2） 点击页面左侧形式化验证文字右侧加号按钮填写验证信息（根据附件） 填写完成后点击右上角对号按钮。点击验证按钮开始验证  3） 点击验证按钮开始验证 |
| **预期结果：**  测试应覆盖以下内容：  1）模式验证第六种模式 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 284 形式化验证：模式验证-案例7测试项

|  |
| --- |
| **测试项目：**形式化验证：模式验证-案例7 |
| **测试依据：** |
| **测试目的：**  测试模式验证第七种模式 pattern-repeatability测试模式验证第七种模式 pattern-repeatability |
| **测试配置：** |
| **测试步骤：**  测试方法：  1） 点击项目按钮，点击右上角导入项目按钮，选择提供的test\_plc\_verif.zip压缩包，点击项目按钮右上角的设置按钮。进入设置页面后勾选启用形式化验证，并填写下方的可执行文件路径分别为提供的nuXmv-2.1.0-win64.zip的bin文件夹中的nuXmv.exe和plcverif\_cli.zip解压后的eclipsec.exe（此操作只需进行一次）。  2） 点击页面左侧形式化验证文字右侧加号按钮填写验证信息（根据附件） 填写完成后点击右上角对号按钮。点击验证按钮开始验证  3） 点击验证按钮开始验证 |
| **预期结果：**  测试应覆盖以下内容：  1）模式验证第七种模式 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 285 形式化验证：模式验证-案例8测试项

|  |
| --- |
| **测试项目：**形式化验证：模式验证-案例8 |
| **测试依据：** |
| **测试目的：**  测试模式验证第八种模式 pattern-leadsto测试模式验证第八种模式 pattern-leadsto |
| **测试配置：** |
| **测试步骤：**  测试方法：  1） 点击项目按钮，点击右上角导入项目按钮，选择提供的test\_plc\_verif.zip压缩包，点击项目按钮右上角的设置按钮。进入设置页面后勾选启用形式化验证，并填写下方的可执行文件路径分别为提供的nuXmv-2.1.0-win64.zip的bin文件夹中的nuXmv.exe和plcverif\_cli.zip解压后的eclipsec.exe（此操作只需进行一次）。  2） 点击页面左侧形式化验证文字右侧加号按钮填写验证信息（根据附件） 填写完成后点击右上角对号按钮。点击验证按钮开始验证  3） 点击验证按钮开始验证 |
| **预期结果：**  测试应覆盖以下内容：  1）模式验证第八种模式 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 286 形式化验证：断言验证测试项

|  |
| --- |
| **测试项目：**形式化验证：断言验证 |
| **测试依据：** |
| **测试目的：**  测试断言验证测试断言验证 |
| **测试配置：** |
| **测试步骤：**  测试方法：  2） 点击项目按钮，点击右上角导入项目按钮，选择提供的test\_plc\_verif.zip压缩包，点击项目按钮右上角的设置按钮。进入设置页面后勾选启用形式化验证，并填写下方的可执行文件路径分别为提供的nuXmv-2.1.0-win64.zip的bin文件夹中的nuXmv.exe和plcverif\_cli.zip解压后的eclipsec.exe（此操作只需进行一次）。  3） 点击页面左侧形式化验证文字右侧加号按钮填写验证信息（根据附件） 填写完成后点击右上角对号按钮。点击验证按钮开始验证  4） 点击验证按钮开始验证 |
| **预期结果：**  测试应覆盖以下内容：  1） 断言验证功能 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 287 形式化验证：实数功能验证测试项

|  |
| --- |
| **测试项目：**形式化验证：实数功能验证 |
| **测试依据：** |
| **测试目的：**  测试实数变量类型是否被支持测试实数变量类型是否被支持 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1） 点击项目按钮，点击右上角导入项目按钮，选择提供的test\_plc\_verif.zip压缩包，点击项目按钮右上角的设置按钮。进入设置页面后勾选启用形式化验证，并填写下方的可执行文件路径分别为提供的nuXmv-2.1.0-win64.zip的bin文件夹中的nuXmv.exe和plcverif\_cli.zip解压后的eclipsec.exe（此操作只需进行一次）。  2） 点击页面左侧形式化验证文字右侧加号按钮填写验证信息（根据附件） 填写完成后点击右上角对号按钮。点击验证按钮开始验证  3） 点击验证按钮开始验证 |
| **预期结果：**  测试应覆盖以下内容：  1）测试验证支持实数变量 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 288 形式化验证：反例生成测试项

|  |
| --- |
| **测试项目：**形式化验证：反例生成 |
| **测试依据：** |
| **测试目的：**  测试生成反例的功能测试生成反例的功能 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1） 点击项目按钮，点击右上角导入项目按钮，选择提供的test\_plc\_verif.zip压缩包，点击项目按钮右上角的设置按钮。进入设置页面后勾选启用形式化验证，并填写下方的可执行文件路径分别为提供的nuXmv-2.1.0-win64.zip的bin文件夹中的nuXmv.exe和plcverif\_cli.zip解压后的eclipsec.exe（此操作只需进行一次）。  2） 点击页面左侧形式化验证文字右侧加号按钮填写验证信息（根据附件） 填写完成后点击右上角对号按钮。点击验证按钮开始验证  3） 点击验证按钮开始验证 |
| **预期结果：**  测试应覆盖以下内容：  1）测试形式验证可以输出反例信息 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 289 形式化验证：并行求解功能测试项

|  |
| --- |
| **测试项目：**并行求解功能 |
| **测试依据：** |
| **测试目的：**  测试并行求解的功能测试并行求解的功能 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1） 解压plcveirf\_cli(linux版本)，将plcverif\_cli、NuSMV-glucose-parallel、glucose-syrup添加到系统路径中以便在任何路径下都能调用  2） 修改文件cli\_set-parallel.txt中的相关路径。将它替换为解压缩后各个文件的路径。使用./plcverif-cli cli\_set-parallel.txt命令开始运行  3） 当输出中”Building the step for k = num”的num>20时，在另一终端使用top -H命令 观察COMMAND名为glucose-syrup的线程数量，存在多个线程证明进行了并行求解。或查看目录下生成的tempresult文件，文件表格中数据列出了各个线程求解的数据 |
| **预期结果：**  测试应覆盖以下内容：  1）测试插件调用的后端支持并行求解 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 290 多语言编程测试项

|  |
| --- |
| **测试项目：**多语言编译器功能测试 |
| **测试依据：** |
| **测试目的：**  验证支持IEC61131-3（ST/LD/FBD）与C/C++/Rust的混合编程、编译及调试功能验证支持IEC61131-3（ST/LD/FBD）与C/C++/Rust的混合编程、编译及调试功能 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）分别使用语言C/C++/Rust/ST/LD各自创建一个用户库，编写用于测试中被调用的功能块/函数  2）使用ST语言编写PLC程序(PROGRAM)，调用各个语言所创建的功能和功能块，通过IDE编译之后，并在线监视变量值  3）在ST程序中调用RUST/C/C++语言编写的函数，触发断点并查看变量的值  4） 注入语法错误验证报错机制 |
| **预期结果：**  测试应覆盖以下内容：  1）ST/LD/FBD/C/C++/RUST编程语法支持  2）语法错误处理  3）跨语言调用（LD调用C++功能块等）  4）IDE调试功能（断点、堆栈跟踪） |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 291 沙箱机制测试项

|  |
| --- |
| **测试项目：**沙箱资源隔离验证 |
| **测试依据：** |
| **测试目的：**  验证内存沙箱对越界访问的隔离效果。验证内存沙箱对越界访问的隔离效果。 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1） 使用C语言创建一个带有非法地址访问的函数，比如访问一个非法地址0XFFFFFFFF。函数名为do\_illegal()  2） 编写 ST 程序在某个触发条件满足时，调用 C 函数do\_illegal()，故意访问超出分配范围的内存地址  3） 打开runtime的log  4） 下装APP, 并且触发该函数的调用  5） 非法访问触发时应用程序的本次执行被终止  6） 当通过日志或监控工具检测沙箱是否阻断越界行为  7） 查看告警发现相关的告警内容 |
| **预期结果：**  测试应覆盖以下内容：  1）PLC 程序故意访问非法内存地址（如数组越界、野指针） |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |

### 292 热更新测试项

|  |
| --- |
| **测试项目：**热更新稳定性验证 |
| **测试依据：** |
| **测试目的：**  测试服务不中断下的代码替换测试服务不中断下的代码替换 |
| **测试配置：** |
| **测试步骤：**  测试方法：  1）热更新前后引用计数及对象内容比对 |
| **预期结果：**  测试应覆盖以下内容：  1）C++指针迁移后数据一致性 |
| **测试结果：** |
| **测试结论：**  **（√）通过 （ ）部分通过 （ ）未通过 （ ）未测试** |
| **备注：--** |