# 通过性测试用例

## 整体指标

### 部署要求

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 测试编号 | 1.1.1 | 测试日期 |  | |
| 测试地点 |  | 供应商 |  | |
| 测试项目 | 支持elasticsearch非关系型数据库 | | | |
| 测试目的 | 检查平台是否支持特定版本的数据库 | | | |
| 测试条件 |  | | | |
| 测试方法 | 1.在所提供得操作平台上安装平台软件后，后端安装的数据库应为elasticsearch非关系型数据库；  2.连接数据库测试成功。 | | | |
| 测试结果 | 支持elasticsearch非关系型数据库。  填写数据库类型 | | | □通过 □未通过 |
| 备注 | 不满足此功能，该型号产品不通过 | | | |
| 测试员签名 | 建行\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 供应商\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | |

### 承诺项

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 测试编号 | 1.1.2 | 测试日期 |  | |
| 测试地点 |  | 供应商 |  | |
| 测试项目 | 1.承诺依托建行大数据云平台提供安全数据  2.承诺能够安全分析应用的形式和建行大数据云平台整合  3.产品以B/S架构交付，用户无需安装客户端，通过浏览器就能完成对设计器的访问  4.具备二次开发能力，提供开发平台和开发规范 | | | |
| 测试目的 | 平台是否满足承诺项 | | | |
| 测试方法 | 供应商根据产品指标要求提供产品数据及承诺 | | | |
| 测试结果 | 承诺能在建行大数据云平台独立部署（提供纸质盖章承诺）。 | | | □通过 □未通过 |
| 产品以B/S架构交付，用户无需安装客户端，通过浏览器就能完成对平台的访问（提供纸质盖章承诺）。 | | | □通过 □未通过 |
| 具备二次开发能力，提供开发平台和开发规范（提供纸质盖章承诺）。 | | | □通过 □未通过 |
| 备注 | 不满足此功能，该型号产品不通过 | | | |
| 测试员签名 | 建行\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 供应商\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | |

## 非功能测试

### 运维监控

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 测试编号 | 1.2.1 | 测试日期 |  | |
| 测试地点 |  | 供应商 |  | |
| 测试项目 | 承诺按照建行运维监控的方式，在项目建设过程中对接建行运维监控平台并记录相关运维监控信息。 | | | |
| 测试目的 |  | | | |
| 测试方法 | 供应商根据产品指标要求提供产品数据及承诺 | | | |
| 测试结果 |  | | | □通过 □未通过 |
| 备注 | 不满足此功能，该型号产品不通过 | | | |
| 测试员签名 | 建行\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 供应商\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | |

## 功能测试

### 数据接入

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 测试编号 | 1.3.1 | 测试日期 |  | |
| 测试地点 |  | 供应商 |  | |
| 测试项目 | 支持多种安全设备、网络设备、主机的数据接入功能，包括但不限于：防火墙、IPS/IDS、WAF、APT、安全客户端等 | | | |
| 测试目的 | 测试平台是否满足特定数据源接入 | | | |
| 测试条件 |  | | | |
| 测试方法 | 1. 在平台中新建一个数据接入的任务或规则，可以选择接入设备类型； 2. 能够看到包含安全设备、网络设备、主机等主要数据类型的接入选项 | | | |
| 测试结果 | 支持上述数据源接入  测试结果\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 评分\_\_\_\_\_ | | | □通过 □未通过 |
| 备注 | 不满足此功能，该型号产品不通过 | | | |
| 测试员签名 | 建行\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 供应商\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | |

### 数据范式化

#### 日志范式化规则

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 测试编号 | 1.3.2.1 | 测试日期 |  | |
| 测试地点 |  | 供应商 |  | |
| 测试项目 | 日志范式化规则应内置开箱即用的条范式化解析规则，支持解析规则的导入导出 | | | |
| 测试目的 | 平台支持日志范式化规则的导入导出 | | | |
| 测试条件 |  | | | |
| 测试方法 | 1. 在平台能够看到内置解析规则。 2. 在平台数据解析界面有导入导出的选项。 3. 点击并选择内置规则验证规则的导入导出。 | | | |
| 测试结果 | 测试结果\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 评分\_\_\_\_\_ | | | □通过 □未通过 |
| 备注 | 不满足此功能，该型号产品不通过 | | | |
| 测试员签名 | 建行\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 供应商\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | |

#### 解析方式

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 测试编号 | 1.3.2.2 | 测试日期 |  | |
| 测试地点 |  | 供应商 |  | |
| 测试项目 | 支持多种解析方式，如正则表达式、分隔符、键值对、XML、JSON等解析方式，支持解析插件的二次开发 | | | |
| 测试目的 | 平台是否具有可使用的日志解析方式 | | | |
| 测试条件 |  | | | |
| 测试方法 | 1. 平台支持可视化的数据解析配置界面，必须通过界面配置的方式进行数据解析； 2. 新建一条数据解析规则，点击解析方式选项。 3. 是否能够看到正则解析，键值对解析，分隔符解析。 | | | |
| 测试结果 | 测试结果\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 评分\_\_\_\_\_ | | | □通过 □未通过 |
| 备注 | 不满足此功能，该型号产品不通过 | | | |
| 测试员签名 | 建行\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 供应商\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | |

### 实时数据关联分析

#### 实时流计算引擎

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 测试编号 | 1.3.3.1 | 测试日期 |  | |
| 测试地点 |  | 供应商 |  | |
| 测试项目 | 被测系统应基于大数据流式计算，支持攻击告警的实时关联分析 | | | |
| 测试目的 | 检验是否具备实时流计算并关联实时告警进行关联分析 | | | |
| 测试条件 |  | | | |
| 测试方法 | 1. 新建关联分析规则，可以在关联分析规则的关联条件里面选择告警事件并配置关联分析规则。 | | | |
| 测试结果 | 测试结果\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 评分\_\_\_\_\_ | | | □通过 □未通过 |
| 备注 | 不满足此功能，该型号产品不通过 | | | |
| 测试员签名 | 建行\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 供应商\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | |

#### 基于情报的关联分析

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 测试编号 | 1.3.3.2 | 测试日期 |  | |
| 测试地点 |  | 供应商 |  | |
| 测试项目 | 支持外部威胁情报的关联分析，能够将解析后的事件与情报IOC进行自动关联，生成情报类关联告警 | | | |
| 测试目的 | 平台是否具有关联威胁情报分析的能力 | | | |
| 测试条件 |  | | | |
| 测试方法 | 1. 新建关联分析规则，可以在关联分析规则的关联条件里面选择关联情报。 | | | |
| 测试结果 | 测试结果\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 评分\_\_\_\_\_ | | | □通过 □未通过 |
| 备注 | 不满足此功能，该型号产品不通过 | | | |
| 测试员签名 | 建行\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 供应商\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | |

#### 关联分析场景

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 测试编号 | 1.3.3.3 | 测试日期 |  | |
| 测试地点 |  | 供应商 |  | |
| 测试项目 | 内置多种已知攻击类型的关联分析规则。如探测扫描、网站攻击、暴力破解、漏洞利用等 | | | |
| 测试目的 | 平台是否具有内置的关联分析场景模型 | | | |
| 测试条件 |  | | | |
| 测试方法 | 1. 打开平台，点击关联分析规则，能够看到内置的关联分析规则。 2. 关联分析规则至少包含探测扫描、网站攻击、暴力破解、漏洞利用等场景。 | | | |
| 测试结果 | 测试结果\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 评分\_\_\_\_\_ | | | □通过 □未通过 |
| 备注 | 不满足此功能，该型号产品不通过 | | | |
| 测试员签名 | 建行\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 供应商\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | |

#### 快速新建关联分析规则

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 测试编号 | 1.3.3.4 | 测试日期 |  | |
| 测试地点 |  | 供应商 |  | |
| 测试项目 | 支持安全运营人员在界面快速创建、部署新的关联分析规则 | | | |
| 测试目的 | 验证平台的灵活配置能力和友好性 | | | |
| 测试条件 |  | | | |
| 测试方法 | 1. 新建关联分析规则，可打开界面的关联规则配置窗口，新建关联分析规则，可以选择关联条件，至少包括顺序发生、统计关联、A先发生B后发生等关联条件。 2. 可以在界面选择添加分析的事件源。 | | | |
| 测试结果 | 测试结果\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 评分\_\_\_\_\_ | | | □通过 □未通过 |
| 备注 | 不满足此功能，该型号产品不通过 | | | |
| 测试员签名 | 建行\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 供应商\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | |

### 安全事件管理

#### 安全事件集中展示

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 测试编号 | 1.3.4.1 | 测试日期 |  | |
| 测试地点 |  | 供应商 |  | |
| 测试项目 | 支持安全事件集中呈现，可根据多视角、多维度呈现安全事件详情，可通过交互式方式对安全事件进行查看和分析 | | | |
| 测试目的 | 平台是否能将各类安全事件以多维度视角进行集中展示。 | | | |
| 测试条件 |  | | | |
| 测试方法 | 1. 打开平台，点击告警集中展示页面，能够呈现全部告警。 2. 告警呈现的维度包括告警级别，告警类型等。 3. 可点击告警进行详细信息的查看和分析。 | | | |
| 测试结果 | 测试结果\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 评分\_\_\_\_\_ | | | □通过 □未通过 |
| 备注 | 不满足此功能，该型号产品不通过 | | | |
| 测试员签名 | 建行\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 供应商\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | |

#### 溯源分析

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 测试编号 | 1.3.4.2 | 测试日期 |  | |
| 测试地点 |  | 供应商 |  | |
| 测试项目 | 支持安全事件快速溯源，集中展示安全事件发生过程和相关线索。可还原安全事件发生过程 | | | |
| 测试目的 | 平台是否能对安全事件进行快速的溯源定位。 | | | |
| 测试条件 |  | | | |
| 测试方法 | 1. 打开安全分析平台,具备统一窗口呈现安全事件详情. 2. 点击安全事件详情可以查看安全事件关联的原始日志进行溯源. | | | |
| 测试结果 | 测试结果\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 评分\_\_\_\_\_ | | | □通过 □未通过 |
| 备注 | 不满足此功能，该型号产品不通过 | | | |
| 测试员签名 | 建行\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 供应商\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | |

#### 基础监控

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 测试编号 | 1.3.4.3 | 测试日期 |  | |
| 测试地点 |  | 供应商 |  | |
| 测试项目 | 支持对安全事件类型、级别、阶段及状态进行图表展示 | | | |
| 测试目的 | 平台是否能对安全事件进行基础监控 | | | |
| 测试条件 |  | | | |
| 测试方法 | 1.打开平台安全监控中心,能够看到对安全事件的类型、级别、阶段及状态进行图表展示 | | | |
| 测试结果 | 测试结果\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 评分\_\_\_\_\_ | | | □通过 □未通过 |
| 备注 | 不满足此功能，该型号产品不通过 | | | |
| 测试员签名 | 建行\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 供应商\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | |

### 审计管理

#### 审计日志

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 测试编号 | 1.3.5.1 | 测试日期 |  | |
| 测试地点 |  | 供应商 |  | |
| 测试项目 | 审计日志管理支持用户操作日志记录保存，保留期限设置，超出期限的日志由平台进行归档删除等处理 | | | |
| 测试目的 | 平台是否具有审计日志的功能。 | | | |
| 测试条件 |  | | | |
| 测试方法 | 1. 登陆系统，可以查看系统审计日志,可以看到登陆日志记录. | | | |
| 测试结果 | 测试结果\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 评分\_\_\_\_\_ | | | □通过 □未通过 |
| 备注 | 不满足此功能，该型号产品不通过 | | | |
| 测试员签名 | 建行\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 供应商\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | |

## 资质证书

### 软件著作权

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 测试编号 | 1.4.1 | 测试日期 |  | |
| 测试地点 |  | 供应商 |  | |
| 测试项目 | 提供被测系统软件著作权。 | | | |
| 测试目的 | 验证供应商基本入围指标 | | | |
| 测试条件 |  | | | |
| 测试方法 |  | | | |
| 测试结果 | 测试结果\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 评分\_\_\_\_\_ | | | □通过 □未通过 |
| 备注 | 不满足此功能，该型号产品不通过 | | | |
| 测试员签名 | 建行\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 供应商\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | |