# **IT安全能力建设验收场景及标准**

# **集团云网运营部**

# **2020年1月**

# **1.资产管理任务（新炬）**

1.1场景1

实现主机层面资产的电子化维护、更新。 [该场景总分20分] 。

主机层面包括：服务器及操作系统、服务器承载的数据库、 中间件（含paas），应用/服务等软件系统。

### 要求

通过人工录入和采集自动识别实现主机资产对象运营状况变更维护（资产上线、下线、变更等）。通过人工录入或采集自动识别实现主机资产安全类属性的变更维护。

### 细则

#### 人工录入维护【该项10分】

提供录入界面，成功完成主机资产及安全类属性信息的增删改操作，安全类属性包括IP地址、开放端口、操作系统类型及版本、中间件版本信息、所属业务系统等等。未完成扣4分。

提供录入界面，成功完成主机资产运营状况（新增、变更、下线）的维护变更操作。未完成扣2分。

提供excel表格批量导入能力，完成主机资产运营状况的批量变更维护，未完成扣2分。

提供excel表格批量导入能力，完成主机资产安全类属性信息的批量变更维护，安全类属性包括IP地址、开放端口、操作系统类型及版本、中间件版本信息、所属业务系统等等。未完成扣2分。

#### 采集自动识别[该项10分]

1、通过网段扫描或接入预部署有agent的新入网主机，自动采集识别发现有新资产入网，未成功发现扣5分。

2、采集识别主机资产的安全类资产属性信息变更，包括IP地址、开放端口、操作系统类型及版本、中间件版本信息、所属业务系统等等属性，未发现扣5分，发现缺失1项扣1分，最多扣5分。

## 场景2：完成主机agent部署。[该场景总分20分] （新炬）

### 要求

通过Agent采集手段获取资产数据，为资产发现、资产管理、资产展示等功能提供支撑。

### 细则

#### 服务器信息采集【该项10分】

1、Agent具有采集服务器端口监听信息，支持资产管理实现端口变动信息和历史端口信息进行记录。未采集扣2分。

2、Agent具有采集服务器进程信息，支持资产管理系统对变动情况进行记录。未采集扣2分。

3、Agent具有采集iptable配置，ip地址与端口与归属系统（服务）三种之间的对应关系，支持资产管理系统对变动情况进行记录。未采集扣2分。

4、Agent具有采集服务器主机配置信息，支持资产管理系统实现操作系统版本、补丁等属性管理。未采集扣2分。

5、Agent具有采集服务器部署软件信息，支持资产管理系统管理呈现服务器承载部署的中间件、应用系统所属厂商、品牌、版本、进程路径等属性信息。未采集扣2分。

#### Agent部署能力【该项10分】

1、Agent具有版本发布自动升级能力，不支持扣2分

2、Agent具有自身心跳监控能力，支持对全网Agent分布状况监控，不支持扣2分

3、Agent具有采集频率参数远程调节能力，支持远程改变数据采集上报频率，不支持扣3分

4、Agent具有根据服务器负载状况自动调整自身资源占用策略，当服务器负载达到设定限值时Agent进入休眠，当服务器负载满足条件时Agent自动恢复数据上报。不支持扣3分

## 场景3: 完成各网段主机扫描能力部署。[该场景总分20分] （周娟）

1.3.1要求:通过扫描手段获取资产数据，为资产发现、资产管理、资产展示提供支撑。

### 细则

#### 扫描能力可达范围[该项10分]

1、从MSS、BOSS、ITM、EDA、测试、接口、互联网、维护等安全域内任选一资产，一个不可达扣2分，扣完为止

#### 资产信息获取丰富程度[该项10分]

1、对于任意主机可以采集IP、端口、协议等内容，每缺少一项减2分,扣完为止。

2、具备常见端口（443、23、3389等）、重要端口、自定义端口的扫描能力，每缺少一项减2分,扣完为止。

3、具备主流协议扫描能力，支持默认和非默认端口的扫描，如数据库、SSH、FTP、HTTP等；每缺少一项减2分,扣完为止。

## 1.4场景4：完成核心交换机流量采集探针部署。[该场景总分10分]（客支）

### 1.4.1要求

现场验收，验收范围包括所要求核心交换机流量采集探针部署情况以及所部属探针采集的全流量信息对获取资产及互访记录，为资产台账更新维护、互联互通关系维护、资产拓扑图绘制的数据支撑能力。

### 1.4.2细则

#### 1.4.2.1基本功能[该项10分]

1、支持基于流量包判断网络设备是否存活。[该项4分]

2、支持发现网络交互过程中活跃的资产IP，识别资产对外开放的端口。[该项4分]

1. 支持将网络流量日志发送至IT智能运维平台。[该项2分]

## 1.5场景5：完成web应用系统的非静态资源url清单管理。[该场景总分10分]（周娟）

### 1.5.1要求 web应用系统的URL清单可电子化管理

### 1.5.2细则

#### 1.5.2.1电子化管理内网web应用系统主入口url地址

1. 可目录树形式展现，参照系统定级备案情况，每缺少一个扣1分，扣完为止。

#### 1.5.2.1电子化管理互联网web应用系统全部url地址（不含非登录可见url、接口服务地址)

1. 可目录树形式展现，参照系统定级备案情况，每缺少一个扣1分，扣完为止。

## 1.6场景6：实现网络拓扑图、互联关系图电子化管理。[该场景总分20分]（周娟）

### 1.6.1要求

现场验收，验收范围包括网络拓扑图、业务系统互联关系图的手工导入和图形化展现。

### 1.6.2细则

#### 1.6.2.1拓扑图导入[该项10分]

1、支持网络拓扑图导入。不满足扣4分。

2、支持业务系统互联关系图导入。不满足扣4分。

3、支持批量导入。不满足扣2分。

#### 1.6.2.2图形化展现[该项10分]

1、支持按集团公司《关于明确拓扑图绘制工作的通知》（中国电信网信[2019]34号，附件1）格式展现网络拓扑图。不满足扣5分。

2、支持按集团公司《关于明确拓扑图绘制工作的通知》（中国电信网信[2019]34号，附件1）格式展现业务系统互联关系图。不满足扣5分。

# **2安全接入任务**

### 2.1场景1：完成统一WEB接入部署，二级以上系统实现通过统一WEB门户的访问。[该场景总分20分] （熊思敏）

### 2.1.1要求

现场验收，验收范围包括：账号管理、账号认证、逐步具备授权管理、审计管理功能，详细要求按照《IT安全能力建设规范\_2.安全能力分册V1.0》“2.3web统一接入”，通过统一web portal登录页面或统一后台认证两种模式的功能验收。

### 2.1.2细则

### 2.1.2.1默认开启功能[该项4分]

1、登录Web统一管理系统平台，查看系统访问人员的用户信息、角色和组织机构信息是否可进行统一化管理。[该项2分]

2、查看系统访问人员是否只需登录统一web接入系统即可实现访问应用系统，无须二次登录。[该项2分]

### 2.1.2.2默认策略开启[该项4分]

1、建立统一Web接入账号必须通过HTTPS安全套接字层【SSL】链接请求访问WEB接入系统，如HTTP模式也可以登录为不通过。 [该项2分]

2、查看统一Web接入系统是否采用主备/集群模式部署，保障高可用。[该项2分]

### 2.1.2.3 Web统一接入系统认证验收 [该项4分]

1、测试登录功能，验证使用非实名制的账号无法登录web统一门户，以及出现多次密码错误时对账号进行锁定。 [该项2分]

2、验证接入web接入平台后，仅可访问已授权应用，无法访问未授权应用。 [该项2分]

### 2.1.2.4、日志审计功能验收 [该项8分]

1、查看web接入平台是否记录有管理员对web接入平台的操作日志。[该项2分]

2、查看是否具备用户通过统一web接入平台登录业务系统的审计记录。[该项2分]

3、查看统一web接入系统运行日志。[该项2分]

4、验证统一web接入平台是否将平台管理员操作日志、用户访问日志、系统运行日志上传至IT智能运维平台。[该项2分]

### 2.2场景2: 完成运维堡垒机部署，所有运维操作均通过堡垒机。[该场景总分25分] （周娟）

### 2.2.1要求

现场验收，验收范围包括图形堡垒、字符堡垒、堡垒机节点管理、堡垒机操作日志、金库模式、文档访问管理等功能，详见《IT安全能力建设规范\_2. 安全接入能力分册V1.0》“2.5 运维管理统一接入”。

### 2.2.2细则

#### 2.2.2.1 默认开启功能[该项12分]

1、测试统一账号管理，查看是否实现了维护人员的用户信息、角色和组织机构信息的统一化管理。[该项3分]

2、测试统一认证，查看是否实现了维护人员的单点登录，只需登录统一运维接入系统，即刻访问所有服务器，无须进行二次登录。[该项3分]

3、测试统一授权，查看是否支持实体级控制和应用级控制。[该项3分]

4、测试统一审计，查看是否能够支持对字符操作及返回结果、图形操作的全程审计。[该项3分]

#### 2.2.2.2 默认开启的配置策略[该项6分]

1、测试文件上传下载权限，查看是否文件上传下载权限默认配置为不开启。[该项3分]

2、测试普通用户高危命令权限，查看是否普通用户高危命令权限默认配置为不开启。[该项3分]

#### 2.2.2.3 日志生成与上传。[该项4分]

1、测试堡垒机的日志生成功能，查看是否能够生成符合日志采集规范的日志。[该项2分]

2、测试堡垒机的日志上传功能，查看是否支持通过Syslog协议发送日志信息。[该项2分]

#### 2.2.2.4 支持通过主备/集群模式保障高可用。[该项3分]

1、测试堡垒机的高可用性，查看是否采取了主备或集群模式保障高可用。[该项3分]

### 2.3场景3：完成统一APP门户部署，非公众APP均通过统一APP门户管理。[该场景总分20分]（苗成）

### 2.3.1要求

现场验收，验收范围包括认证管理、数据安全传输、应用数据安全隔离、应用安全管理（应用商店）、安全审计功能，详见《IT安全能力建设规范\_2. 安全接入能力分册V1.0》“2.4 APP统一接入”。

### 2.3.2细则

#### 2.3.2.1 默认开启功能[该项8分]

1、测试传输加密功能，查看移动应用门户与安全接入网关是否建立了传输通道，采用密码技术来保障数据传输的通道安全。[该项4分]

2、测试数据防泄密功能，查看移动门户应用与移动终端个人桌面是否完全隔离。[该项4分]

#### 2.3.2.2 默认开启配置策略[该项8分]

1、测试管理员首次登陆是否强制修改登陆密码。[该项4分]

2、测试是否开启认证策略防暴力破解策略。[该项4分]

#### 2.3.2.3 日志生成与上传。[该项4分]

1、测试移动门户app的日志生成功能，查看是否具有用户接入以及管理员操作日志。[该项2分]

2、验证统一web接入平台是否将平台管理员操作日志、用户访问日志、系统运行日志上传至IT智能运维平台。[该项2分]

### 2.4场景4：定级备案系统的统一WEB接入率达到50%。[该场景总分10分]（周娟）

### 2.4.1要求

现场验收，验收范围包括：核心系统定期情况查看，核心系统Web统一接入率，详细要求按照《IT安全能力建设规范\_2.安全能力分册V1.0》“2.3web统一接入”，通过统一web portal登录页面进行功能验收。

### 2.4.2细则

#### 2.4.2.1核心系统Web统一接入率[该项10分]

1、查看核心业务系统备案信息，通过登录Web统一接入窗口，查看是否超过50%核心系统包含在Web统一接入窗口中，并且可成功访问。[该项10分]

### 2.5场景5：部署统一终端管理系统 [该场景总分25分] （张家坤）

### 2.5.1 要求

现场验收，验收范围包括终端入网注册、终端接入认证、终端安全检测、安全接入管控等功能，并检测对终端防泄漏、终端防病毒等功能模块的兼容扩展支持能力，详见《IT安全能力建设规范\_2. 安全接入能力分册V1.0》“2.6 终端统一接入”。

### 2.5.2 细则

#### 2.5.2.1 默认开启的功能[该项8分]

1、测试身份认证功能，查看默认要求输入账号密码对接入终端进行认证。[该项2分]

2、测试身份信息注册功能，查看是否默认要求在进行终端注册时必须填写管理员要求的信息。[该项2分]

3、测试设备审核功能，查看是否默认要求在进行设备安全检查时必须经过管理员手动审核。[该项2分]

4、测试对网络中存活终端的自动识别能力，查看是否默认开启了终端自动发现、按终端类型自动分类、边界设备自动发现功能。[该项2分]

#### 2.5.2.2 默认开启的配置策略[该项9分]

1、测试对入网终端的安全检查能力，查看是否默认配置了杀毒软件及系统补丁策略。[该项3分]

2、测试对入网终端所安装的软件进行检查的能力，查看是否默认配置了软件黑白名单策略。[该项3分]

3、测试加强账号密码的能力，查看是否默认开启了密码策略设置检查、弱口令检查配置。[该项3分]

#### 2.5.2.3 日志生成与上传[该项4分]

1、测试统一管理平台的日志生成功能，查看是否能够生成符合日志采集规范的日志。[该项2分]

2、测试统一管理平台的日志上传功能，查看是否支持通过Syslog协议发送日志信息。[该项2分]

#### 2.5.2.4 支持通过主备/集群模式保障高可用[该项4分]

1、测试统一管理平台的高可用性，查看是否采取了主备或集群模式保障高可用。[该项2分]

2、测试终端准入设备的高可用性，查看是否采取了主备或集群模式保障高可用。[该项2分]

# **3.安全防护任务**

## 3.1 场景1：按互联网接入域、开发测试域、生产域维度实现网络安全域分域控制和边界隔离、完成网络防火墙部署【该场景总分12分】（周娟）

### 3.1.1要求

远程及现场验收，由省公司配合人员在集团公司指定地点远程登陆相关系统进行验收。验收范围包括互联网接入域、开发测试域、各生产域网络域划分和边界隔离。允许合法用户访问受保护的网络资源，控制进出网络的访问行为。

### 3.1.2细则

#### 3.1.2.1互联网接入域边界防火墙部署【该项总分4分】

1.在资产系统中任意选择一个互联网系统，查看防火墙互联网IP地址及对应的内网IP地址，推理互联网接入域及内网域，登陆管理该网段的网络防火墙。【该项2分】

2.查看防火墙策略是否有默认拒绝所有访问权限前提下，开启明确允许的控制策略。【该项2分】

#### 3.1.2.2边界防火墙部署【该项总分8分】

1.具备终端域、开发测试域、管理域的划分，登陆各网络域边界防火墙，查看防火墙上的边界IP地址及内网IP地址配置情况及查看防火墙策略是否有默认拒绝所有访问权限前提下、开启明确允许的控制策略。【每个域3分】

## 3.2场景2：继续细分接口域、维护域实现网络安全域分域控制和边界隔离、完成网络防火墙部署【该场景总分16分】（周娟）

### 3.2.1要求

远程及现场验收，由省公司配合人员在集团公司指定地点远程登陆相关系统进行验收。验收范围包括从多纬度进行安全域划分，从业务、功能、网络流量等因素划分。

### 3.2.2细则

#### 3.2.2.1细分了接口域【该项总分4分】

1.在资产系统中查看相应的资产所属域，登录防火墙查看配置确认业务划分是否明确，比如接口配置及策略是否按照接口域控制。【该项4分】

#### 3.2.2.2接口域边界防火墙部署【该项总分4分】

1.在资产系统中任意选择一个属于接口域系统，查看防火墙接口域的配置，登陆管理该网段的网络防火墙。【该项2分】

2.查看防火墙策略是否有默认拒绝所有访问权限前提下，开启明确允许的控制策略。【该项2分】

#### 3.2.2.3划分了维护域【该项总分4分】

1.登录防火墙上查看资产系统维护域的IP地址，确认防火墙上是否有相关的IP地址配置及相关策略。【该项4分】

#### 3.2.2.4维护域边界防火墙部署【该项总分4分】

1.在资产系统中任意选择一个属于维护域系统，查看防火墙维护域的配置，登陆管理该网段的网络防火墙。【该项2分】

2.查看防火墙策略是否有默认拒绝所有访问权限前提下，开启明确允许的控制策略。【该项2分】

## 3.3场景3：细分终端域，完成网络防护墙部署【该场景总分8分】（张家坤）

### 3.3.1要求

远程及现场验收，由省公司配合人员在集团公司指定地点远程登陆相关系统进行验收。验收范围包括办公终端、运维终端部署防火墙。

### 3.3.2细则

#### 3.3.2.1细分了终端域【该项总分4分】

1.登录防火墙上查看办公终端运维终端的IP地址，确认防火墙上是否有终端域的IP地址配置及相关策略。【该项4分】

#### 3.3.2.2终端域边界防火墙部署【该项总分4分】

1.在资产系统中查看终端域的IP地址，登录每个终端域的防火墙的查看IP地址配置是否与办公终端、运维终端相同。【该项2分】

2.查看防火墙策略是否有默认拒绝所有访问权限前提下，开启明确允许的控制策略。【该项2分】

## 3.4场景4：完成互联网出口IPS、WAF串行部署；具备APP加壳能力【该场景总分16分】（客支、苗成）

### 3.4.1要求

远程及现场验收，由省公司配合人员在集团公司指定地点登录迎检系统进行验收。验收范围为互联网出口IPS、WAF，APP加壳能力。

### 3.4.2细则

#### 3.4.2.1互联网出口IPS部署【该项总分4分】

1.根据网络拓扑图与资产管理中心中的安全资产信息，选择一台互联网出口的IPS设备登录，查看IPS设备信息与资产信息是否一致，信息不一致的扣1分。【该项1分】

2.查看登录IPS设备的软件版本、系统规则库、病毒特征库等是否定期更新，低于设备厂商官网发布最新更新三个及以上版本的扣1分。【该项1分】

3.查看登录IPS设备的安全策略配置，未配置及未启用安全策略的扣1分。【该项1分】

4.查看登录IPS设备1-3个月内的威胁及阻断日志，查询不到日志的扣1分。【该项1分】

#### 3.4.2.2互联网出口WAF部署【该项总分4分】

1、根据网络拓扑图与资产管理中心中的安全资产信息，选择一台互联网出口的WAF设备登录，查看WAF设备信息与资产信息是否一致，信息不一致的扣1分。【该项1分】

2、查看登录WAF设备的软件版本、系统规则库等是否定期更新，低于设备厂商官网发布最新更新三个及以上版本的扣1分。【该项1分】

3、查看登录WAF设备的安全策略配置，未配置及未启用安全策略的扣1分。【该项1分】

4、查看登录WAF设备1-3个月内的威胁及阻断日志，查询不到日志的扣1分。【该项1分】

#### 3.4.2.3IPS与WAF串行部署【该项总分4分】

1、查看互联网出口IPS设备所在的交换机配置，IPS未进行物理或逻辑串行部署的扣2分。【该项2分】

2、查看互联网出口WAF设备所在的交换机配置，WAF未进行物理或逻辑串行部署的扣2分。【该项2分】

#### 3.4.2.4APP加壳能力部署【该项总分4分】

1.查看是否部署APP加壳能力，未部署APP加壳的扣2分。【该项2分】

2.抽查省公司两个生产用APP，看是否使用APP加壳，未进行加壳就发布的扣2分。【该项2分】

## 3.5场景5：完成网络病毒防火墙部署【该场景总分4分】（彭雅）

### 3.5.1要求

远程及现场验收，由省公司配合人员在集团公司指定地点登录迎检系统进行验收。验收范围为网络病毒防火墙。

### 3.5.2细则

#### 3.5.2.1网络病毒防火墙部署【该项总分4分】

1.登录网络病毒防火墙设备查看病毒库版本、系统规则库等是否定期更新，未更新的扣1分。【该项1分】

2.查看网络病毒防火墙设备的安全策略配置，未配置及未启用安全策略的扣1分。【该项1分】

3.查看网络病毒防火墙设备1-3个月内的病毒威胁及阻断日志，查询不到日志的扣2分。【该项2分】

## 3.6场景6：核心系统部署主机防病毒软件【该场景总分4分】（周娟）

### 3.6.1要求

远程及现场验收，由省公司配合人员在集团公司指定地点登录迎检系统进行验收。验收范围为网络病毒防火墙。

### 3.6.2细则

#### 3.6.2.1主机防病毒软件部署【该项总分4分】

1.登录主机病毒软件控制台查看病毒库版本、木马库版本等是否定期更新，超过1个月未更新的扣1分。【该项1分】

2.查看主机病毒软件控制台的扫描及杀毒策略配置，未配置及未启用杀毒策略的扣1分。【该项1分】

3.查看主机病毒软件控制台1-3个月内的病毒威胁及查杀日志，查询不到日志的扣1分。【该项1分】

4.在资产管理中心中抽查5-10台服务器，查看防病毒客户端的安装情况及策略开启情况，未安装及未开启客户端策略的扣1分。【该项1分】

## 3.7场景7：IT互联网出口部署全流量检测分析系统【该场景总分4分】（新炬）

### 3.7.1要求

针对IT互联网出口全流量分析系统进行验收，采用远程、现场验收，验收范围包括IT互联网出口全流量分析系统的部署及流量采集分析等。

### 3.7.2细则

#### 3.7.2.1互联网出口全流量检测分析系统【该项总分4分】

1.查看设备是否已在互联网出口交换机上完成旁路部署【该项2分】

2.登录流量分析系统，在相应的配置页面查看流量采集情况，并能够在相应页面进行流量分析等功能设置【该项2分】

## 3.8场景8：生产域新上线系统按MSS、BOSS、EDA进行业务域划分【该场景总分12分】（帅高）

### 3.8.1要求

在完成终端域、互联网接入域、开发测试域、接口域、管理域、生产域的网络安全域划分基础上，将按照业务不同将生产域划分为MSS业务域、BOSS业务域、EDA业务域。

### 3.8.2细则

#### 3.8.2.1MSS业务域划分【该项总分4分】

1.在资产管理中心抽查MSS域系统所在网段，查看MSS域系统所在网段是否有防火墙【该项2分】

2.查看防火墙具有默认拒绝、明确允许的访问控制策略。【2分】

#### 3.8.2.2BOSS业务域划分【该项总分4分】

1.在资产管理中心抽查BOSS域系统所在网段，查看MSS域系统所在网段是否有防火墙【该项2分】

2.查看防火墙具有默认拒绝、明确允许的访问控制策略。【2分】

#### 3.8.2.3EDA业务域划分【该项总分4分】

1.在资产管理中心抽查EDA域系统所在网段，查看MSS域系统所在网段是否有防火墙【该项2分】

2.查看防火墙具有默认拒绝、明确允许的访问控制策略。【2分】

## 3.9场景9：部署统一运维管理平台，实现基于主机(端点)的集中访问控制【该场景总分8分】（周娟）

### 3.9.1要求

远程及现场验收，由省公司配合人员在集团公司指定地点远程登陆统一运维平台进行验收。验收范围包括统一运维平台和统一运维平台基于主机的访问控制。

### 3.9.2细则

#### 3.9.2.1具有统一运维管理平台【该项总分4分】

1.查看堡垒主机已采用物理旁路的方式完成部署。远程登录堡垒机，提供某个服务器的远程服务端口，查看是否能够访问该台服务器或被管理资源。【该项2分】

2.登录堡垒机，选择特定的数据文件，查看是否能够通过特定的配置页面，将数据文件存储至日志服务器。【该项2分】

#### 3.9.2.2统一运维平台能够实现基于主机的访问控制【该项总分4分】

1.抽查统一运维平台5个账号远程登录系统，可以正常登录，非统一运维平台账号无法登录系统【该项2分】

2.已登录账号访问已授权的资源，分别执行已授权和未授权的命令操作，已授权命令操作能够正常执行生效，未授权命令操作无法执行生效【该项2分】

## 3.10场景10：完成DCN出口的IPS\WAF串行部署【该场景总分8分】（客支）

### 3.10.1要求

远程及现场验收，由省公司配合人员在集团公司指定地点远程登陆相关系统进行验收。验收范围包括DCN出口IPS、WAF部署及其功能开启和日志集中传送。

### 3.10.2细则

#### 3.10.2.1DCN出口IPS部署【该项总分4分】

1.根据网络拓扑图与资产管理中心中的安全资产信息，选择一台DCN出口的IPS设备登录，查看IPS设备信息与资产信息是否一致，信息不一致的扣1分。【该项1分】

2.查看登录IPS设备的软件版本、系统规则库、病毒特征库等是否定期更新，低于设备厂商官网发布最新更新三个及以上版本的扣1分。【该项1分】

3.查看登录IPS设备的安全策略配置，未配置及未启用安全策略的扣1分。【该项1分】

4.查看登录IPS设备1-3个月内的威胁及阻断日志，查询不到日志的扣1分。【该项1分】

#### 3.10.2.2DCN出口WAF部署【该项总分4分】

1.根据网络拓扑图与资产管理中心中的安全资产信息，选择一台DCN出口的WAF设备登录，查看WAF设备信息与资产信息是否一致，信息不一致的扣1分。【该项1分】

2.查看登录WAF设备的软件版本、系统规则库等是否定期更新，低于设备厂商官网发布最新更新三个及以上版本的扣1分。【该项1分】

3.查看登录WAF设备的安全策略配置，未配置及未启用安全策略的扣1分。【该项1分】

4.查看登录WAF设备1-3个月内的威胁及阻断日志，查询不到日志的扣1分。【该项1分】

#### 3.11场景11：核心应用部署应用防火墙或动态应用防护【该场景总分3分】（客支）

### 3.11.1要求

远程及现场验收，由省公司配合人员在集团公司指定地点远程登陆相关系统进行验收。验收范围包括核心应用的WAF部署、策略及功能开启和日志集中传送。

### 3.11.2细则

#### 3.11.2.1应用防火墙或动态应用防护部署【该项总分3分】

1.远程登录核心应用区域的WAF或应用防护设备，查看相应的应用防护设备是否已完成部署并开启防护策略【该项2分】

2.远程登录WAF或应用防护设备，查看设备日志存储状态是否正常【该项1分】

## 3.12场景12：（二级及以上系统）部署主机恶意代码防护【该场景总分3分】（张家坤）

### 3.12.1要求

远程及现场验收，由省公司配合人员在集团公司指定地点远程登陆相关系统进行验收。验收范围包括防病毒软件部署、策略及功能开启和日志采集上传。

### 3.12.2细则

#### 3.12.2.1二级以上系统恶意代码防护部署【该项总分3分】

1.远程登录服务器和终端设备，查看防病毒软件是否已完成部署并开启防护策略【该项2分】

2.远程登录防病毒控制中心，查看终端防病毒软件的日志情况，验证终端防病毒软件可将syslog日志上报至防病毒控制中心【该项1分】

## 3.13场景13：DCN出口部署全流量分析系统【该场景总分2分】（网络）

### 3.13.1要求

针对DCN出口全流量分析系统进行验收，采用远程、现场验收，验收范围包括DCN出口全流量分析系统的部署及流量采集分析等。。

### 3.13.2细则

#### 3.13.2.1 DCN出口全流量分析系统部署【该项总分2分】

1.查看设备是否已在DCN出口交换机上完成旁路部署【该项1分】

2.登录流量分析系统，在相应的配置页面查看流量采集情况，并能够在相应页面进行流量分析等功能设置【该项1分】

# **4安全分析任务**

## 4.1场景1：应用弱口令认证（新炬）

## 4.1.1要求

远程或现场验收，由待验收部门配合人员按照验收部门要求执行，进行特定操作开展相关验收，验收范围为安全分析系统，检查相应的攻击类操作能否正常产生告警。【该项总分1分】

## 4.1.2细则

## 4.1.2.1应用弱口令认证

对测试应用（如HTTP、WebLogic、IMAP、POP3、TELNET、SNMP、SSH）使用弱口令访问，检查分析中心1小时内有无告警产生。【该项总分1分】

## 4.2场景2：账户异常登录（新炬、彭雅）

## 4.2.1要求

现场验收，由待验收部门配合人员按照验收部门要求登录系统，进行特定操作开展检查验收，验收范围包含所有接入的主机或应用系统，检查相应的攻击类操作能否正常产生告警。【该项总分3分】

## 4.2.2细则

## 4.2.2.1登录时间异常：

任选一个主机\业务系统，在非工作时间“如晚10:00”登录成功登录。并且持续长时间在非工作时间成功登录，检查1小时内是否产生告警【该项总分1分】

## 4.2.2.2登录地点异常：

任选一个主机\业务系统的账号，在该账号非常用地点登录。检查是分析中心是否产生告警【该项总分1分】

## 4.2.2.3登录账号异常：

任选一个主机\业务系统的账号，选择3个以上账号在系统进行登录失败操作在该账号非常用地点登录。检查是1小时内是否产生告警【该项总分1分】

## 4.3场景3：账户提权（新炬）

## 4.3.1要求

现场验收，由待验收部门配合人员按照验收部门要求登录系统，进行特定操作开展检查验收，验收范围包含所有接入的主机系统。【该项总分1分】

## 4.3.2细则

## 4.3.2.1账户提取

任选一台主机，由业务系统人员在主机上创建一个普通权限账号，通过su到管理员权限，查看系统是否1小时内有告警产生【该项总分1分】。

## 4.4场景4：异常账号登录（新炬）

## 4.4.1要求

现场验收，由待验收部门配合人员按照验收部门要求登录系统，进行特定操作开展检查验收，验收范围包含所有接入的主机或应用系统。【该项总分2分】

## 4.4.2细则

## 4.4.2.1沉默账号异常登录

任选一个业务系统，选择30日以上未登录的账号登录业务系统，且登录成功。检查系统1小时内是否有告警产生【该项总分1分】。

## 4.4.2.2离职员工账号登录异常

任选一个业务系统，选择一状态为离职的账号成功登录。检查系统1小时内是否有告警产生【该项总分1分】。

## 4.5场景5：linux用户su至root多次失败（新炬）

## 4.5.1要求

远程或现场验收，由待验收部门配合人员按照验收部门要求执行，进行特定操作开展相关验收，验收范围为安全分析中心【该项总分1分】。

## 4.5.2细则

## 4.5.2.1 linux用户su至root多次失败

在linux主机上创建一个普通权限账号，使用普通账号用错误密码执行su至root命令多次，检查系统1小时内是否有告警产生【该项总分1分】。

## 4.6场景6：帐户的密码被更改或重置（新炬）

## 4.6.1要求

远程或现场验收，由待验收部门配合人员按照验收部门要求执行，进行特定操作开展相关验收，验收范围为安全分析中心【该项总分2分】。

## 4.6.2细则

## 4.6.2.1账户的密码被更改或重置

在linux主机选用某账号登录并修改或重置账户密码等操作，检查系统1小时内是否有告警产生【该项总分1分】。

在 windows主机选用某账号登录并修改或重置账户密码等操作，检查系统1小时内是否有告警产生【该项总分1分】。

## 4.7场景7：检测多人使用相同堡垒机帐号（周娟）

## 4.7.1要求

现场验收，由待验收部门配合人员按照验收部门要求登录系统，进行特定操作开展检查验收，验收范围包含堡垒、安全分析中心。【该项总分1分】

## 4.7.2细则

## 4.7.2.1 检测多人使用堡垒机账号

任选一个堡垒机，在不同的pc终端登录同一账号，若成功登录，检查分析中心能否1小时内有告警产生【该项总分1分】

## 4.8场景8：VPN账号暴力破解（客支、新炬）

## 4.8.1要求

远程或现场验收，由待验收部门配合人员按照验收部门要求执行，进行特定操作开展相关验收，验收范围包含vpn设备、安全分析中心。【该项总分2分】

## 4.8.2细则

## 4.8.2.1VPN账号暴力破解

1. 同一或多个PC终端对同一vpn账号多次登陆失败，检查分析中心能否1小时内有告警产生【该项总分1分】

2. 同一或多个PC终端对多个vpn账号多次登陆失败，检查分析中心能否1小时内有告警产生【该项总分1分】。

## 4.9场景9：VPN账号暴力成功（客支）

## 4.9.1要求

远程或现场验收，由待验收部门配合人员按照验收部门要求执行，进行特定操作开展相关验收，验收范围包含vpn主机，流量采集设备、安全分析中心。【该项总分2分】

## 4.9.2细则

## 4.9.2.1 VPN账号暴力成功

1. 同一或多个ip对同一vpn账号多次登陆失败后出现一次登陆成功，检查分析中心能否1小时内有告警产生【该项总分1分】

2. 同一ip对同一或多个vpn账号多次登陆失败后出现一次登陆成功，检查分析中心能否1小时内有告警产生【该项总分1分】

## 4.10场景10：VPN用户登陆异常（客支）

## 4.10.1要求

远程或现场验收，由待验收部门配合人员按照验收部门要求执行，进行特定操作开展相关验收，验收范围包含vpn主机，流量采集设备、安全分析中心。【该项总分2分】

## 4.10.2细则

## 4.10.2.1 VPN用户登录异常

1、使用国内ip地址与某VPN账号在一小时内频繁登录，检查分析中心能否1小时内有告警产生【该项总分0.5分】

2、使用国内ip地址与某VPN账号在非工作时间登录；检查分析中心能否1小时内有告警产生【该项总分0.5分】

3、使用国外ip地址，使用某vpn账号登录，检查分析中心能否1小时内有告警产生【该项总分0.5分】

4、使用国外ip地址和某VPN账号在一小时内频繁登录，检查分析中心能否1小时内有告警产生【该项总分0.5分】。

## 4.11场景11：文件数据外发（新炬）

## 4.11.1要求

远程或现场验收，由待验收部门配合人员按照验收部门要求执行，进行特定操作开展相关验收，验收范围安全分析中心【该项总分2分】。

## 4.11.2细则

## 4.11.2.1 文件数据外发

1、使用网盘、聊天工具以及邮件等形式发送包含敏感信息的文件到外网接收对象，检查分析中心能否1小时内有告警产生【该项总分1分】

2、使用FTP将文件传输到非公司IP的服务器，检查分析中心能否1小时内有告警产生【该项总分1分】

## 4.12场景12：敏感文件操作告警（新炬）

## 4.12.1要求

远程或现场验收，由待验收部门配合人员按照验收部门要求执行，进行特定操作开展相关验收，验收范围包含主机、安全分析中心。【该项总分1分】

## 4.12.2细则

## 4.12.2.1敏感文件操作告警

在测试主机并存放测试敏感文件（后缀名为.conf、.ini、.sys、.dll），访问、修改权限、删除、转移、重命名该敏感文件，检查分析中心能否1小时内有告警产生【该项总分1分】。

## 4.13场景13：超量文件传输（新炬）

## 4.13.1要求

现场验收，由待验收部门配合人员按照验收部门要求登录系统，进行特定操作开展检查验收，验收范围包含所有接入的主机及安全分析中心。【该项总分1分】

## 4.13.2细则

## 4.13.2.1 超量文件传输

选择一台主机进行文件下载，且在五分钟内下载10次以上，检查分析中心能否1小时内有告警产生【该项总分1分】

## 4.14场景14：绕过堡垒机/跳板机的成功登陆（彭雅）

## 4.14.1要求

远程或现场验收，由待验收部门配合人员按照验收部门要求执行，进行特定操作开展相关验收，验收范围包含主机、堡垒机、安全分析中心。【该项总分2分】

## 4.14.2细则

## 4.14.2.1绕过堡垒机/跳板机成功登录

绕过堡垒机直接ssh登录某主机，检查分析中心能否1小时内有告警产生【该项总分2分】。

## 4.15场景15：非法接入设备（张家坤）

## 4.15.1要求

远程或现场验收，由待验收部门配合人员按照验收部门要求执行，进行特定操作开展相关验收，验收范围包含安全分析中心。【该项总分1分】

## 4.15.2细则

## 4.15.2.1非法接入设备

确认网络准入系统部署完毕后，准备一台不在网络准入范围内的笔记本或主机，尝试访问内网网站或主机，若成功访问，检查分析中心能否1小时内有告警产生【该项总分1分】

## 4.16场景16：账号行为异常（新炬）

## 4.16.1要求

现场验收，由待验收部门配合人员按照验收部门要求登录系统，进行特定操作开展检查验收，验收范围为安全分析中心。【该项总分2分】

## 4.16.2细则

## 4.16.2.1 账号行为异常

选择一台主机登录后，创建一个账号，在账号创建后的短时间内（比如30分钟内），删除新创建的账号“。检查分析中心能否1小时内有告警产生【该项总分2分】

## 4.17场景17：邮件服务器向恶意IP发送邮件（集团）

## 4.17.1要求

远程或现场验收，由待验收部门配合人员按照验收部门要求登录系统，进行特定操作开展检查验收，验收范围为安全分析中心。【该项总分1分】

## 4.17.2细则

## 4.17.2.1 邮件服务器向恶意IP发送邮件

操作邮件服务器对已知某恶意ip发送邮件。检查分析中心能否1小时内有告警产生【该项总分1分】

## 4.18场景18：从服务器大规模下载资料（新炬）

## 4.18.1要求

远程或现场验收，由待验收部门配合人员按照验收部门要求执行，进行特定操作开展相关验收，验收范围包含安全分析中心。【该项总分1分】

## 4.18.2细则

## 4.18.2.1 从服务器大规模下载资料

准备FTP服务器和客户端测试主机，并在FTP服务器上存放大量文件，对文件服务器上或FTP服务器上短时间内进行大量文件拷贝（20文件以上），检查分析中心能否1小时内有告警产生【该项总分1分】

## 4.19场景19：邮件登录异常检测（集团）

## 4.19.1要求

远程或现场验收，由待验收部门配合人员按照验收部门要求执行，进行特定操作开展相关验收，验收范围包含安全分析中心。【该项总分1分】

## 4.19.2细则

## 4.19.2.1邮件登录异常检测

1、短时内同一邮箱账号多次登录失败，之后该邮箱账号成功登录了1次

2、短时内同一源IP使用邮箱账号多次登录失败。

3、检测发现邮件账号异地登陆

4、检测发现单IP登录多个邮箱账号

5、短时内，同一源IP使用邮箱账号多次登录失败

检查分析中心能否1小时内有告警产生，以上任一项无法产生告警扣0.2分【该项总分1分】

## 4.20场景20：邮件携带恶意附件（集团）

## 4.20.1要求

远程或现场验收，由待验收部门配合人员按照验收部门要求执行，进行特定操作开展相关验收，验收范围包含安全分析中心。【该项总分1分】

## 4.20.2细则

## 4.20.2.1 邮件携带恶意附件

发送携带恶意内容附件的邮件，打开恶意文件会导致进程操作，文件操作，网络操作，注册表操作等，检查分析中心能否1小时内有告警产生【该项总分1分】

## 4.21场景21：检测到大量垃圾邮件（集团）

## 4.21.1要求

远程或现场验收，由待验收部门配合人员按照验收部门要求执行，进行特定操作开展相关验收，验收范围包含安全分析中心。【该项总分1分】

## 4.21.2细则

## 4.21.2.1检测到大量垃圾邮件

对测试邮箱发送大量垃圾邮件，检查分析中心能否1小时内有告警产生【该项总分1分】

## 4.22场景22：邮件发送到恶意邮箱（集团）

## 4.22.1要求

远程或现场验收，由待验收部门配合人员按照验收部门要求执行，进行特定操作开展相关验收，验收范围包含安全分析中心。【该项总分1分】

## 4.21.2细则

## 4.21.2.1 邮件发送带恶意邮箱

向恶意邮箱发送邮件、邮件内嵌URL页面行为的恶意动作分析（场景演含义不明），检查分析中心能否1小时内有告警产生【该项总分1分】

## 4.23场景23：linux服务器执行敏感命令（新炬）

## 4.23.1要求

远程或现场验收，由待验收部门配合人员按照验收部门要求执行，进行特定操作开展相关验收，验收范围安全分析中心。【该项总分1分】

## 4.23.2细则

## 4.23.2.1 linux服务器执行敏感命令

准备一台linux系统测试主机，使用登录该主机并执行敏感命令，如chmod、chown、mkdir、cat /etc/passwd、/etc/shadow、rm -rf、os\_type= 'linux' and rule\_name='等，检查分析中心能否1小时内有告警产生【该项总分1分】

## 4.24场景24：linux的iptables被关闭（新炬）

## 4.24.1要求

远程或现场验收，由待验收部门配合人员按照验收部门要求执行，进行特定操作开展相关验收，验收范围为安全分析中心。【该项总分1分】

## 4.24.2细则

## 4.24.2.1 linux的iptable被关闭

准备一台linux系统测试主机，使用登录该主机并执行iptables关闭操作（service iptables stop、chkconfig iptables off），检查分析中心能否1小时内有告警产生【该项总分1分】。

## 4.25场景25：windows访问敏感的网络共享（新炬）

## 4.25.1要求

远程或现场验收，由待验收部门配合人员按照验收部门要求执行，进行特定操作开展相关验收，验收范围包含windows主机。【该项总分1分】

## 4.25.2细则

## 4.25.2.1 windows访问敏感的网络共享

预设A主机为敏感主机，在A主机上开启网络共享服务，并存放测试敏感文件。配合人员使用B主机（windows）访问该共享，读取存放的测试敏感文件。检查分析中心能否1小时内有告警产生【该项总分1分】

## 4.26场景26：内网DNS发起域名查询请求（客支、新炬）

## 4.26.1要求

远程或现场验收，由待验收部门配合人员按照验收部门要求执行，进行特定操作开展相关验收，验收范围安全分析中心。【该项总分1分】

## 4.26.2细则

## 4.26.2.1 内网DNS发起域名查询请求

使用内网环境，使用内网测试主机短时间对某个域名进行频繁请求（1分钟内大于10次），检查分析中心能否1小时内有告警产生【该项总分1分】。

## 4.27场景27：内网DNS访问特定蠕虫域名（新炬）

## 4.27.1要求

远程或现场验收，由待验收部门配合人员按照验收部门要求执行，进行特定操作开展相关验收，验收范围安全分析中心。【该项总分1分】

## 4.27.2细则

## 4.27.2.1 内网DNS访问特定蠕虫域名

使用内网环境，使用内网测试主机对访问特定蠕虫域名（安全分析中心内已配置的），检查分析中心能否1小时内有告警产生【该项总分1分】。

## 4.28场景28：数据库新增用户（新炬）

## 4.28.1要求

现场验收，由待验收部门配合人员按照验收部门要求登录系统，进行特定操作开展检查验收，验收范围包含数据库、安全分析中心。【该项总分1分】

## 4.28.2细则

## 4.28.2.1 数据库新增用户

任选某个数据库，通过数据库管理员成功执行相关sql语句，其中一条语句需要包含创建用户的语句。检查分析中心能否1小时内有告警产生【该项总分1分】。

## 4.29场景29：主机关机重启告警（新炬）

## 4.29.1要求

远程或现场验收，由待验收部门配合人员按照验收部门要求执行，进行特定操作开展相关验收，验收范围包含主机安全分析中心。【该项总分1分】

## 4.29.2细则

## 4.29.2.1 主机关机重启告警

对测试主机关机重启，检查分析中心能否1小时内有告警产生【该项总分1分】。

## 4.30场景30：SFTP服务器异常操作（新炬）

## 4.30.1要求

现场验收，由待验收部门配合人员按照验收部门要求登录系统，进行特定操作开展检查验收，验收范围为安全分析中心。【该项总分2分】

## 4.30.2细则

## 4.30.2.1 SFTP服务器异常操作

1、当前用户操作指令集合外的操作指令：检查分析中心能否1小时内有告警产生【该项总分1分】。（场景含义不明）

2、成功操作的文件、文件夹、路径中包含系统关键敏感路径（/etc目、/config、/configure、/conf等路径），检查分析中心能否1小时内有告警产生【该项总分0.5分】

3：成功操作的文件的后缀包含危险后缀（.ini，.sys，.dll等），检查分析中心能否1小时内有告警产生【该项总分0.5分】。

## 4.31场景31：FTP所有操作（周娟）

## 4.31.1要求

远程或现场验收，由待验收部门配合人员按照验收部门要求执行，进行特定操作开展相关验收，验收范围为安全分析中心。【该项总分1分】

## 4.31.2细则

## 4.31.2.1 FTP所有操作

使用测试主机进行FTP文件传输，检查分析中心能否1小时内有告警产生【该项总分1分】。

## 4.32场景32：疑似应用接口路径探测（椒图）

## 4.32.1要求

现场验收，由待验收部门配合人员按照验收部门执行操作，进行特定操作开展检查验收，验收范围为安全分析中心。【该项总分1分】

## 4.32.2细则

## 4.32.2.1 疑似应用接口路径探测

使用wwwscan、御剑等路径扫描工具对web服务进行路径扫描，检查分析中心能否1小时内有告警产生【该项总分1分】

## 4.33场景33：违规主机/终端行为（张家坤、彭雅）

## 4.33.1要求

现场验收，由待验收部门配合人员按照验收部门执行操作，进行特定操作开展检查验收，验收范围为安全分析中心。【该项总分1分】。

## 4.33.2细则

## *4.33.2.1 违规主机/终端行为*

1.在测试主机安装/卸载违规软件或恶意软件，检查分析中心能否1小时内有告警产生【该项总分0.5分】

2.主机插入不可信移动存储设备如U盘等，检查分析中心能否1小时内有告警产生【该项总分0.5分】

## 4.34场景*34*：暴力破解（新炬）

## 4.34.1要求

现场验收，由待验收部门配合人员按照验收部门执行操作，进行特定操作开展检查验收，验收范围为安全分析中心。【该项总分1分】。

## 4.34.2细则

## *4.34.2.1 暴力破解*

在测试主机执行如下几种操作能够触发暴力破解告警：

1.同一IP连续多次登录同一个目标（服务器、应用、设备）登录失败

2.同一IP对多个目的IP（服务器、应用、设备）登录失败；

3.同一IP使用多个账号在同一目标（服务器、应用、设备）登录失败；

4.多个IP使用一个账号登录目标（服务器、应用、设备）失败。

5.检查分析中心能否1小时内有告警产生【该项总分3分，每有一项不达标扣1分，扣完为止】

## 4.35场景35：暴力破解（AI）（新炬）

## 4.35.1要求

现场验收，由待验收部门配合人员按照验收部门执行操作，进行特定操作开展检查验收，验收范围为安全分析中心。【该项总分1分】。

## 4.35.2细则

## *4.35.2.1 暴力破解（AI）*

测试主机执行对目的服务器敏感端口（22、23、3389等）频繁进行暴力口令攻击尝试，检查分析中心能否1小时内有告警产生【该项总分1分】。

## 4.36场景36：DDoS攻击（新炬）

## 4.36.1要求

现场验收，由待验收部门配合人员按照验收部门执行操作，进行特定操作开展检查验收，验收范围为安全分析中心。【该项总分1分】

## 4.36.2细则

## *4.36.2.1 DDos攻击*

使用隔离的网络环境，对测试网段实施DDOS攻击，检查分析中心能否1小时内有告警产生【该项总分1分】。

## 4.37场景37：DDoS攻击（AI）（新炬）

## 4.37.1要求

现场验收，由待验收部门配合人员按照验收部门执行操作，进行特定操作开展检查验收，验收范围为安全分析中心。【该项总分1分】

## 4.37.2细则

## *4.37.2.1 DDOS攻击（AI）*

使用隔离的网络环境，对测试网段实施DDOS攻击，检查分析中心能否1小时内有告警产生【该项总分1分】。

## 4.38场景38：扫描行为 （新炬）

## 4.38.1要求

现场验收，由待验收部门配合人员按照验收部门执行操作，进行特定操作开展检查验收，验收范围为安全分析中心。【该项总分1分】

## 4.38.2细则

## *4.38.2.1 扫描行为*

使用扫描工具在办公网段对Web网站或主机或一段地址等进行在线扫描，扫描过程中变换扫描的IP地址。检查分析中心能否1小时内有告警产生【该项总分1分】。

## 4.39场景39：横向扫描行为（新炬）

## 4.39.1要求

现场验收，由待验收部门配合人员按照验收部门执行操作，进行特定操作开展检查验收，验收范围为安全分析中心。【该项总分2分】

## 4.39.2细则

## *4.39.2.1 横向扫描行为*

1、使用扫描工具在DMZ区域对生产网段Web网站或主机或一段地址等进行在线扫描，扫描过程中变换扫描的IP地址。检查分析中心能否1小时内有告警产生【该项总分1分】。

2、使用扫描工具在生产网段内部对Web网站或主机或一段地址等进行在线扫描，扫描过程中变换扫描的IP地址。检查分析中心能否1小时内有告警产生【该项总分1分】。

## 4.40场景40：系统被攻击后发生内网攻击行为（新炬）

## 4.40.1要求

现场验收，由待验收部门配合人员按照验收部门执行操作，进行特定操作开展检查验收，验收范围为安全分析中心。【该项总分2分】

## 4.40.2细则

## *4.40.2.1 系统被攻击后发生内网攻击行为*

对目标系统实施攻击，利用系统漏洞控制改应用系统所属主机后，在被控主机上实施对主机所在内网的攻击。检查分析中心能否1小时内有告警产生【该项总分2分】。

## 4.41场景41：僵尸主机外联（新炬）

## 4.41.1要求

现场验收，由待验收部门配合人员按照验收部门执行操作，进行特定操作开展检查验收，验收范围为安全分析中心。【该项总分1分】

## 4.41.2细则

## *4.41.2.1* 僵尸*主机外联*

使用隔离的网络环境，在测试主机中预置勒索病毒（特定）、木马（特定）、蠕虫（特定）三类恶意程序，检查分析中心能否1小时内有告警产生【该项总分1分】。

## 4.42场景42：病毒在局域网中传播（客支）

## 4.42.1要求

现场验收，由待验收部门配合人员按照验收部门执行操作，进行特定操作开展检查验收，验收范围为安全分析中心。【该项总分1分】。

## 4.42.2细则

## *4.42.2.1 病毒在局域网种传播*

使用局域网环境，在测试主机中预置特定的病毒程序，特定是指该恶意程序会在网络中进行端口扫描且危害相对较小，检查分析中心能否1小时内有告警产生【该项总分1分】。

## 4.43场景43：主机/终端病毒感染（张家坤、彭雅）

## 4.43.1*要求*

现场验收，由待验收部门配合人员按照验收部门执行操作，进行特定操作开展检查验收，验收范围为安全分析中心。【该项总分1分】

## 4.43.2细则

## *4.43.2.1 主机/终端病毒感染*

使用隔离的网络环境，在测试主机中预置特定的多个恶意软件，检查分析中心能否1小时内有告警产生【该项总分1分】。

## 4.44场景44：蠕虫传播行为（AI场景）（新炬）

## 4.44.1要求

现场验收，由待验收部门配合人员按照验收部门执行操作，进行特定操作开展检查验收，验收范围为安全分析中心。【该项总分3分】

## 4.44.2细则

## *4.44.2.1 蠕虫传播行为（AI场景）*

使用隔离的网络环境，在测试主机中释放某蠕虫病毒，并触发蠕虫传播条件，检查分析中心能否1小时内有告警产生【该项总分3分】

## 4.45场景45：C&C通信（AI场景）（新炬）

## 4.45.1要求

现场验收，由待验收部门配合人员按照验收部门执行操作，进行特定操作开展检查验收，验收范围为安全分析中心。【该项总分3分】

## 4.45.2细则

## *4.45.2.1 C&C通信（AI场景）*

使用隔离的网络环境，在测试主机中释放安装C&C木马客户端，触发其余C&C服务端的通信，检查分析中心能否1小时内有告警产生【该项总分3分】

## 4.46场景46：WebShell攻击（新炬、椒图）

## 4.*46*.1要求

远程或现场验收，由待验收部门配合人员按照验收部门执行操作，进行特定操作开展检查验收，验收范围为安全分析中心。【该项总分1分】。

## 4.46.2细则

## *4.46.2.1 webshell 攻击*

使用隔离的网络环境，在测试主机上上传webshell，并基于webshell实施攻击（查看主机文件、执行命令……）。检查分析中心能否1小时内有告警产生，检查该项告警是否基于流量特征匹配生成【该项总分1分】

## 4.47场景47：WebShell攻击（AI）（新炬、椒图）

## 4.47.1要求

远程或现场验收，由待验收部门配合人员按照验收部门执行操作，进行特定操作开展检查验收，验收范围为安全分析中心。【该项总分3分】。

## 4.47.2细则

## 4.47.2.1 webshell攻击（AI）

使用隔离的网络环境，在测试主机上上传webshell，并基于webshell实施攻击（查看主机文件、执行命令……）。检查分析中心能否1小时内有告警产生，检查该项告警是否基于机器学习算法模型生成【该项总分3分】

## 4.48场景48：命中漏洞POC请求（新炬）

## 4.48.1要求

远程或现场验收，由待验收部门配合人员按照验收部门执行操作，进行特定操作开展检查验收，验收范围为安全分析中心。【该项总分1分】。

## 4.48.2细则

## *4.48.2.1 命中*漏洞*POC请求*

测试主机想特定服务器发起漏洞POC利用请求，检查分析中心能否1小时内有告警产生【该项总分1分】。

## 4.49场景49：扫描后端口攻击（新炬）

## 4.49.1要求

远程或现场验收，由待验收部门配合人员按照验收部门执行操作，进行特定操作开展检查验收，验收范围为安全分析中心。【该项总分2分】。

## 4.49.2细则

## *4.49.2.1 扫描后端口攻击*

使用隔离的网络环境，在测试主机上使用端口扫描工具对测试的被攻击主机，发起扫描，检测到某个端口有漏洞后，对该端口实施攻击。检查分析中心能否1小时内有告警产生【该项总分2分】。

## 4.50场景50：远程漏洞利用成功并进行下一步攻击（新炬）

## 4.50.1*要求*

远程或现场验收，由待验收部门配合人员按照验收部门要求执行，进行特定操作开展相关验收，验收范围包含验收范围为安全分析中心。【该项总分3分】

## 4.50.2细则

## *4.50.2.1 远程漏洞利用成功并进行下一步攻击*

使用隔离的网络环境，准备一个测试攻击主机和具有漏洞的linux靶机，对靶机发起漏洞攻击并成功利用，接着（XX分钟内，XX值可自定义）登录靶机，并在靶机上执行账户创建、下载木马、反弹shell，检查分析中心能否1小时内有告警产生，对于账号创建、下载木马、反弹shell，每出现一项无告警产生，扣一分。【该项总分3分】

## 4.51场景51：web响应异常（新炬）

## 4.51.1要求

远程或现场验收，由待验收部门配合人员按照验收部门要求执行，进行特定操作开展相关验收，验收范围包含验收范围为安全分析中心。【该项总分2分】。

## 4.51.2细则

## *4.51.2.1 web响应异常*

使用Web扫描工具对特定的地址进行扫描（或者脚本化攻击工具）

同一源IP特定时间内出现超出预定阈值的相同告警日志

同一源IP特定时间内访问超出预定阈值

同一URL特定时间内访问命中SQL规则超出预定阈值

检查分析中心能否1小时内有告警产生，对以上三种情况，每出现一种无告警产生扣一分。【该项总分2分】

## 4.52场景52：高频waf告警（客支）

## 4.52.1要求

远程或现场验收，由待验收部门配合人员按照验收部门要求执行，进行特定操作开展相关验收，验收范围包含验收范围为安全分析中心。【该项总分1分】。

## 4.52.2细则

## *4.52.2.1 高频WAF告警*

使用隔离的网络环境，准备一个测试攻击主机和web被攻击站点，短时间内，使用攻击工具，对靶机实施多种web攻击尝试，检查分析中心能否1小时内有告警产生，且告警是否为waf命中规则次数或规则种类数量超频次产生【该项总分1分】

## 4.53场景53：动态安全防护告警（新炬）

## 4.53.1要求

远程或现场验收，由待验收部门配合人员按照验收部门要求执行，进行特定操作开展相关验收，验收范围包含验收范围为安全分析中心。【该项总分1分】。

## 4.53.2细则

## *4.53.2.1 动态安全*防护*告警*

使用隔离的网络环境，准备一个测试攻击主机和web被攻击站点，短时间内，使用攻击工具，对靶机实施多种web攻击尝试，检查分析中心能否1小时内有告警产生，且告警是否为动态防护设备命中规则次数或规则种类数量超频次产生【该项总分1分】。

## 4.54场景54：useragent命中爬虫特征（新炬）

## 4.54.1要求

远程或现场验收，由待验收部门配合人员按照验收部门要求执行，进行特定操作开展相关验收，验收范围包含验收范围为安全分析中心。【该项总分1分】。

## 4.54.2细则

## *4.54.2.1* useragent*命中爬虫特征*

使用爬虫工具或脚本对测试web站点进行爬虫操作，检查分析中心能否1小时内有告警产生【该项总分1分】。

## 4.55场景55：高频尝试备份及敏感文件（新炬）

## 4.55.1要求

远程或现场验收，由待验收部门配合人员按照验收部门要求执行，进行特定操作开展相关验收，验收范围包含验收范围为安全分析中心。【该项总分1分】。

## 4.55.2细则

## *4.55.2.1 高频尝试备份及敏感文件*

选定一个测试网站，准备网站目录扫描工具，目录字典设置为备份文件目录和敏感文件目录（如：etc/passwd），使用网站目录扫描工具对测试网站进行扫描，检查分析中心能否1小时内有告警产生【该项总分1分】。

## 4.56场景56：高频尝试目录遍历（新炬）

## 4.56.1要求

远程或现场验收，由待验收部门配合人员按照验收部门要求执行，进行特定操作开展相关验收，验收范围包含验收范围为安全分析中心。【该项总分1分】。

## 4.56.2细则

## *4.56.2.1 高频尝试目录遍历*

选定一个测试网站，准备网站目录扫描工具，目录字典设置为带有目录遍历特征的目录（如：/../），使用网站目录扫描工具对测试网站进行扫描，检查分析中心能否1小时内有告警产生【该项总分1分】。

## 4.57场景57：数据泄露（新炬、彭雅）

## 4.57.1*要求*

远程或现场验收，由待验收部门配合人员按照验收部门要求执行，进行特定操作开展相关验收，验收范围包含验收范围为安全分析中心。【该项总分1分】。

## 4.57.2细则

## *4.57.2.1 数据泄露*

选定一个测试网站，在网站中部署.ini、.conf等扩展名的敏感文件，在客户端浏览器直接下载上述文件类型，检查分析中心能否1小时内有告警产生【该项总分1分】。

## 4.58场景58：数据泄露（AI场景）（新炬、彭雅）

## 4.58.1*要求*

远程或现场验收，由待验收部门配合人员按照验收部门要求执行，进行特定操作开展相关验收，验收范围包含验收范围为安全分析中心。【该项总分2分】。

## 4.58.2*细则*

## *4.58.2.1 数据泄露（AI场景）*

准备测试主机和被攻击靶机，被攻击靶机上搭建隐蔽信道服务端或者数据库服务，使用测试主机通搭建隐蔽信道传输数据，或者在被攻击靶机上执行数据导出操作，检查分析中心能否1小时内有告警产生，且告警通过AI分析模型产生【该项总分2分】。

## 4.59场景59：数据泄露（综合场景）（新炬、彭雅）

## 4.59.1*要求*

远程或现场验收，由待验收部门配合人员按照验收部门要求执行，进行特定操作开展相关验收，验收范围包含验收范围为安全分析中心。【该项总分2分】。

## 4.59.2*细则*

## *4.59.2.1 数据泄露（综合场景）*

1、选定一个FTP服务器，配合人员准备暴力猜解工具，爆破密码成功后下载测试文件。检查分析中心能否1小时内有告警产生【该项总分1分】

2、对web站点实施攻击，并下载该web站点的敏感配置文件，检查分析中心能否1小时内有告警产生【该项总分1分】。

## 4.60场景60：SQL注入后发生数据泄露（新炬）

## 4.60.1要求

远程或现场验收，由待验收部门配合人员按照验收部门要求执行，进行特定操作开展相关验收，验收范围包含验收范围为安全分析中心。【该项总分2分】。

## 4.60.2细则

## 4.60.2.1 SQL注入后发生数据泄露

对有漏洞的测试站点实施sql注入攻击，在攻击成功后进行数据库的dump操作，检查分析中心能否1小时内有告警产生，且告警类型为“SQL注入后发生数据泄露”【该项总分2分】。

## 4.61场景61：敏感数据泄露（彭雅）

## 4.61.1要求

远程或现场验收，由待验收部门配合人员按照验收部门要求执行，进行特定操作开展相关验收，验收范围包含验收范围为安全分析中心。【该项总分2分】。

## 4.61.2细则

## 4.61.2.1 敏感数据泄露

对有漏洞的测试站点实施sql注入攻击，检查分析中心能否1小时内有告警产生，且告警内容要有攻击者ip及攻击是否成功【该项总分2分】。

## 4.62场景62：Webshell（新炬、椒图）

## 4.62.1要求

远程或现场验收，由待验收部门配合人员按照验收部门要求执行，进行特定操作开展相关验收，验收范围包含验收范围为安全分析中心。【该项总分2分】。

## 4.62.2细则

## 4.62.2.1 WEBSHELL

对用测试主机实施登录web后台，并上传一个webshell文件，检查分析中心能否1小时内有告警产生【该项总分2分】

## 4.63场景63：Webshell漏洞利用（新炬）

## 4.63.1要求

远程或现场验收，由待验收部门配合人员按照验收部门要求执行，进行特定操作开展相关验收，验收范围包含验收范围为安全分析中心。【该项总分2分】。

## 4.63.2细则

## 4.63.2.1 Webshell漏洞利用

对测试web系统上传一个webshell文件，使用该shell连接内网某主机（数据库、web服务调用等），检查分析中心能否1小时内有告警产生，且告警类型为“webshell漏洞利用”【该项总分2分】。

## 4.64场景64：SQL注入（新炬、椒图）

## 4.64.1要求

远程或现场验收，由待验收部门配合人员按照验收部门要求执行，进行特定操作开展相关验收，验收范围包含验收范围为安全分析中心。【该项总分1分】。

## 4.64.2细则

## 4.64.2.1 SQL注入

对测试web服务实施sql注入攻击，检查分析中心能否1小时内有告警产生，且告警类型为“sql注入”【该项总分1分】。

## 4.65场景65：网页篡改（彭雅）

## 4.65.1要求

远程或现场验收，由待验收部门配合人员按照验收部门要求执行，进行特定操作开展相关验收，验收范围包含验收范围为安全分析中心。【该项总分1分】。

## 4.65.2细则

## 4.65.2.1 网页篡改

对测试web系统首页实施页面内容篡改，检查分析中心能否1小时内有告警产生【该项总分1分】。

## 4.66场景66：XSS跨站脚本攻击（新炬）

## 4.66.1要求

远程或现场验收，由待验收部门配合人员按照验收部门要求执行，进行特定操作开展相关验收，验收范围包含验收范围为安全分析中心。【该项总分1分】。。

## 4.66.2细则

## 4.66.2.1 XSS跨站脚本攻击

对测试web系统首页XSS攻击，检查分析中心能否1小时内有告警产生【该项总分1分】。

# **5.安全运营任务**

## 5.1 场景1: 漏洞、基线、第三方检测生命周期管理【该场景总分40】（周娟）

### 5.1.1 要求

远程及现场验收，由省公司配合人员在集团公司指定地点远程登录相关系统验收。验收范围包括对常见主机、应用进行漏洞扫描，对操作系统、数据库等进行基线核查，对应用代码进行代码合规审计。其中漏洞检测对主机、web、APP等资产进行漏洞检测，识别资产漏洞信息及提供风险处置建议。此外，对操作系统、中间件、数据库、网络设备、开源组件等资产进行基线配置核查，识别基线配置不合规项并提供处置建议。此外，亦可提供渗透测试、代码审计功能，支持将第三方安全检测数据（如渗透测试、代码审计等）导入运营管理中心进行统一管控。

### 5.1.2 细则

#### 5.1.2.1漏洞管理【该项总分18分】

1.准确识别被扫描对象的各种信息，包括但不限于操作系统、端口、用户信息、非常规端口上开放的服务。【该项1分】

2.提供完整全面的主机漏洞库，至少支持国际标准通用CVE安全漏洞库，并且支持实现漏洞库的及时更新。【该项1分】

3.主机漏洞扫描可检测的系统包括但不限于：Microsoft Windows 9X/NT/2000/XP/2003/Vista/2008/7、Sun Solaris、HP Unix、IBM AIX、IRIX、Linux、BSD操作系统。【该项1分】

4.支持扫描策略定制，至少包括全端口扫描、常用端口扫描、全漏洞扫描、专项漏洞扫描中的2种扫描方式。【该项2分】

5.支持提供详细的主机漏洞扫描报告，扫描报告提供对于漏洞风险的分析和漏洞修复的建议。【该项2分】

6.支持对Web应用资产的安全漏洞扫描检测。【该项2分】

7.支持基于CWE（Common Weakness Enumeration）的安全弱点库或基于CVE（Common Vulnerabilities and Exposures）的安全漏洞库，通过详细分析网站的结构和链接，探测网站对异常行为的反应，指出可能存在的漏洞。【该项2分】

8.支持对已发现的Web应用的漏洞进行验证。【该项1分】

9.支持提供详细的Web应用漏洞扫描报告，扫描报告提供对于漏洞风险的分析和漏洞修复的建议。【该项2分】

10.支持应用APP客户端漏洞检测，以下项必须至少支持2项以上（包含2项）【该项2分】：

1）基础信息检测：支持对移动应用基本信息进行检测，包括应用权限，应用行为，第三方SDK 等检测项。

2）恶意风险检测：支持挖掘恶意应用的特征和相似性，提取分析病毒样本、快速发现新型风险病毒。

3）源码风险检测：支持对拒绝服务攻击风险，应用完整性检测，程序签名保护检测，应用二次打包风险，Activity、Sevice、Content Provider等组件进行检测。

4）调试风险检测：支持对Java 代码动态调试风险，C 代码动态调试风险，动态注入攻击风险等进行检测。

5）.通用风险检测：支持对Webview 明文存储密码漏洞，WebView 远程代码执行漏洞，WebView 组件忽略SSL 证书验证错误漏洞，数据库注入漏洞等检测。

6）数据风险检测：支持对内存Dump 风险，RSA 加密算法使用不当风险，密钥硬编码漏洞，动态注册Receiver 风险等检测。

11.支持漏洞生命周期的管理，具备漏洞识别、漏洞确认、漏洞整改、漏洞消除四个阶段的电子流程管理，实现漏洞全生命周期闭环。【该项2分】

#### 5.1.2.2基线【该项总分16分】

1.操作系统基线配置核查支持的操作系统类型包括但不限于Windows、Linux、Solaris、HP-UX、AIX等常见操作系统。【该项1分】

2.支持提供详细的操作系统基线配置核查报告，报告至少包括操作系统基线不合规项的风险分析以及整改建议。【该项2分】

3.中间件基线配置核查支持的中间件类型至少包括但不限于Apache、IIS、Tomcat、Nginx、Weblogic、WebSphere等常见中间件。【该项1分】

4.支持提供详细的中间件基线配置核查报告，报告包括但不限于对于中间件基线不合规项的风险分析以及整改建议。【该项1分】

5.数据库基线配置核查支持的数据库类型包括但不限于MySQL、SQL Server、Oracle、DB2、Sybase、Informix、PostgreSQL、Memcached、Redis、MongoDb等常见关系型和非关系型数据库。【该项1分】

6.支持提供详细的数据库基线配置核查报告，报告包括但不限于对于数据库基线不合规项的风险分析以及整改建议。【该项2分】

7.网络设备基线配置核查支持的网络设备类型包括但不限于Cisco、Huawei、Juniper、H3C、迪普等常见网络设备。【该项1分】

8.支持提供详细的网络设备基线配置核查报告，报告包括但不限于对于网络设备基线不合规项的风险分析以及整改建议。【该项2分】

9.PaaS组件基线配置核查支持集团研发中心提供的组件类型。【该项1分】

10.PaaS组件基线配置核查内容参照集团研发中心提供基线配置要求。【该项1分】

11.支持提供详细的PaaS组件基线配置核查报告，报告参照集团研发中心对于PaaS组件基线不合规项的风险分析以及整改建议。【该项1分】

12.支持基线生命周期的管理，具备不符合项发现、不符合项确认、不符合项整改、不符合项消除四个阶段的电子流程管理，实现对基线不合规项的闭环。【该项2分】

#### 5.1.2.3第三方检测生命周期管理【该项总分6分】

1.支持电子化接收集团或第三方高危安全情报，结合受影响的资产范围，实现风险预警的发布、删除、查询、报表统计、风险预警库管理的闭环管理工作。【该项2分】

2.支持第三方检测生命周期电子化管理，通过脆弱项发现、脆弱项确认、脆弱项整改、脆弱项消除四个阶段，实现代码合规检测的脆弱性闭环管理。【该项2分】

3.支持将脆弱项状态处理为确认误报、确认暂时不可整改的脆弱项，自动添加入白名单库。【该项2分】

## 5.2 场景2: 实现安全运营流程与安全作业调度【该场景总分30】（周娟）

### 5.2.1 要求

远程及现场验收，由省公司配合人员在集团公司指定地点远程登录相关系统验收。验收范围包括对安全事件管理、安全应急处置管理、风险处置管理、风险报表管理、安全任务管理等进行生命周期管理。

### 5.2.2 细则

#### 5.2.2.1 安全事件管理【该项总分5分】

1.支持通过电子化手段满足安全事件的采集，分类存储，海量检索，分维度统计。【该项1分】

2.支持告警策略配置、过滤规则配置，可进行安全事件实时关联触发有效告警，具备一定的策略规则库。【该项2分】

3.支持电子化告警结果管理和处置，包括告警结果的新增、查询、清除、处置、派单环节。【该项2分】

#### 5.2.2.2 安全应急处置【该项总分5分】

1.支持通过对安全防护能力下发命令实现防火墙策略优化。在紧急时刻，支持通过对安全防护能力下发命令实现防火墙封堵IP。【该项2分】

2.支持通过对安全接入能力下发命令实现应用系统、主机关停。【该项2分】

3.支持通过对安全防护能力下发命令实现异常流量清洗。【该项1分】

#### 5.2.2.3 风险处置【该项总分10分】

1.支持风险模型的配置，并生成预警信息。【该项2分】

2.支持配置风险响应工单模板，包括但不限于自定义告警名称、类型、等级、派单方式、派送对象、派送内容格式等等。【该项2分】

3.支持工单管理，包括增、删、改、查、启停。【该项2分】

4.支持工单处置审核流程，包括但不限于指派、处置、通过、驳回等。【该项2分】

5.支持工单分类统计，包括但不限于饼图、柱状图、趋势图等多种视图模型切换，亦可生成分类报表报告。【该项2分】

#### 5.2.2.4风险报表【该项总分3分】

1.提供IT资产风险情况的多维度统计分析视图，支持风险视图、风险趋势图展示；可以分别查看紧急漏洞、高危漏洞、中危漏洞、低危漏洞和提示漏洞的所对应的年、月、周以及日的风险趋势情况。【该项1分】

2.支持报表下载、风险评估，包括但不限于指定部门的某次扫描生成扫描报告、对同一部门前后不同的扫描结果进行对比分析，以获得同一个部门的安全管理状况、对同一部门的最后若干次扫描结果进行趋势分析。【该项1分】

3.支持合规统计和风险处置跟踪。【该项1分】

#### 5.2.2.5安全任务管理【该项总分3分】

1.支持上级单位派发的安全任务的接收、创建、下发、执行状态跟踪及结果查看。【该项3分】

2.支持任务的审核，任务结果的处置和上报。【该项1分】

#### 5.2.2.6作业调度【该项总分4分】

1.支持作业创建、分解、下发、执行、任务跟踪、查询功能提供操作和展示页面，实现检测作业任务灵活调度，检测资源高效利用。【该项1分】

2.支持作业分解功能，按照组织机构、业务系统、检查时间等将处于草稿状态的作业分解为多个子作业，子作业也可以继续分解为更细粒度的子作业，直到所有子作业都可以被执行。【该项1分】

3.支持作业执行功能，具备按照检查项类型进行人工填报、下发执行模块或检查工具进行检查。【该项1分】

4.具备作业跟踪能力，支持作业状态跟踪查看业务系统、分检查项类别的执行状态；支持作业详情查看，至少应包括作业名称、业务系统、合规项信息、执行状态。【该项1分】

## 5.3 场景3: 业务系统“三同步”管控流程【该场景总分20】（周娟）

### 5.3.1 要求

遵循三同步要求，对业务系统从系统立项到安全退网的全生命周期进行管理，包括：系统登记、系统设计审核、安全验收、定级备案和安全退网多个阶段，将安全工作落实到业务系统生命周期的各个阶段。

### 5.3.2 细则

#### 5.3.2.1 系统登记【该项4分】

1.具备针对业务系统的一个信息登记填报，支持业务系统的基本信息，包括系统名称、内/外网属性、归属部门、责任人、等保定级等信息上报登记到系统中，无法填报扣2分。【该项2分】

2.支持对于已经登记填报的业务系统进行审核通过或者不通过，不支持审核扣2分【该项2分】

#### 5.3.2.2 设计审核【该项4分】

1.支持对于登记审核通过的业务系统进行上传业务系统设计文档，不能上传业务系统设计文档的扣2分。【该项2分】

2.支持对于已经上传业务系统设计文档的业务系统进行审核通过或者不通过，不支持审核扣2分。【该项2分】

#### 5.3.2.3 安全验收【该项5分】

1.对审核通过的业务系统，支持发起验收申请。【该项1分】

2．支持通过手工或自动调度检测功能进行脆弱性检测，未要求进行脆弱性检测并上传扣1分。【该项2分】

3.支持通过手工或自动调度风险处置功能，对脆弱性检测进行闭环管理。【该项1分】

4.支持对于已经上传相关的安全材料的业务系统进行审核，审核结果可以为通过或者不通过，不支持审核扣1分。【该项1分】

#### 5.3.2.4 定级备案【该项3分】

1.支持上传定级备案材料，备案内容应包括备案信息表、定级报告、符合性测评【该项2分】

2.支持对定级备案材料进行人工审核。【该项1分】

#### 5.3.2.4 安全退网【该项4分】

1.对于已经在线上运行使用的业务系统，支持提出系统退网申请，不支持申请退网的扣1分。【该项1分】

2.业务系统退网的申请，支持通过人工或自动调度的工单派发的工作流程，不具备工单派发流程的扣1分。【该项1分】

3.退网工单具备审核环节，审核该工单处理是否通过，不具有审核环节的扣1分。【该项1分】

4.已经通过的退网申请，支持将当前业务系统进行标记为退网。【该项1分】

## 5.4 场景4: 代码审计能力【该场景总分10】（周娟）

### 5.4.1 要求

核心系统，互联网系统的项目，代码在部署上线前就需要进行代码审计任务，验收范围包括是否接入开发流程、代码缺陷检测、代码缺陷审计管理、代码检测结果的检测统计报表展示。

### 5.4.2 细则

#### 5.4.2.1 代码缺陷检测【该项4分】

1.通过代码审计任务，能够检查出代码缺陷及错误信息，不能检查出源代码缺陷及错误信息的扣1分。【该项2分】

2.通过代码审计任务，能够分析并找到具体的问题引发的安全漏洞，可分析出跨站脚本、数据注入、未验证用户输入、拒绝服务、弱加密、信息泄露等几大漏洞，实现细颗粒度的代码安全漏洞结果展示，不能分析出这部分结果的扣1分。【该项2分】

#### 5.4.2.2 缺陷审计【该项3分】

1.通过代码缺陷审计管理，能够定义源代码缺陷检测规则，不能自定义规则的扣0.5分。【该项0.5分】

2.通过代码缺陷审计管理，支持创建代码缺陷检测任务，对任务中的代码进行分析源代码缺陷，不支持扣1分。【该项1分】

3.通过代码缺陷审计管理，能够对代码缺陷检测任务的检测结果进行代码缺陷追踪、审计、整改，不能够对检测结果进行跟踪、审计、整改的扣1分。【该项1分】

4.通过代码缺陷审计管理，能够对代码缺陷任务进行关闭处置，实现代码缺陷的处置闭环，无法关闭任务的扣0.5分。【该项0.5分】

#### 5.4.2.3 检测报表【该项2分】

1.支持多维度展示代码的安全现状，至少包括缺陷分布、严重程度、审计情况、代码质量维度，不支持的扣1分。【该项1分】

2.支持对代码审计结果数据的多种格式的报表导出，不支持多种格式的报表导出扣1分。【该项1分】

#### 5.4.2.4 接入开发流程【该项1分】

1.需要对代码在部署上线前进行代码审计流程，未提供代码审计就验收的扣1分【该项1分】