**附件2：网络安全态势感知平台三期采购清单**

**1.网络安全态势感知平台（安恒）扩容采购清单**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **模块** | **参数描述** | **维保** |
| 1 | 数据分析节点扩容 | 新增态势感知平台数据分析节点2个。 | 3年 |
| 2 | 统计分析模块 | 1、支持对无界流数据进行高效的实时处理和分析，同时也支持批量数据的处理。  2、支持定时间自定义统计数据，时间维度至秒级。  3、支持统计模型的统计数据按照分析规则触发数量进行统计。  4、支持统计模型的数据扩展多个字段。 | 3年 |
| 3 | 人行数据上报模块 | 1、支持与人行态势感知数据上报平台进行数据对接。  2、根据人行要求数据上传字段进行配置。  3、根据威胁研判后的数据进行精准上报。 | 3年 |
| 4 | CMDB数据对接 | 1.在二期对接用户新建CMDB系统基础上通过API接口对接形式，增加对接字段，如：资产名称、操作系统版本、负责人名称、开放端口信息、系统版本、IP地址、中间件版本等字段，并可将存在漏洞标识在资产之中。  2.资产每次同步新增更新后对资产进行重新漏洞匹配及标识，实现漏洞及资产可增量匹配。资产增删改后漏洞信息可自动同步调整。  3.可通过页面搜索相应漏洞名称、受害主机、漏洞编号等字段查询详细资产情况。  4.漏洞导入时间与CMDB同步资产后碰撞漏洞库或Nessus扫描同步时间保持一致。  5.当与CMDB同步资产信息后，部分过去存在漏洞不再存在，则将与CMDB同步时间用于表示漏洞修复完成时间。  漏洞可进行全生命周期展示，以资产为视角查看其过去时间存在漏洞数量及当下漏洞数量，通过图形化方式进行展示了解漏洞变化情况。 | 3年 |
| 5 | 漏洞管理平台对接 | 1、对接单位漏洞管理平台，实现统一收集资产的数量、分布、组件应用以及漏洞、威胁资产进行深入的态势感知及告警，实现资产、漏洞的安全监测。  2、对资产进行细颗粒度梳理、关联并以组织架构进行统一管理，满足各资产发现与管理部门对资产精细化管理的要求，同时为漏洞情报匹配及漏洞风险碰撞奠定数据基础。  3、对主流漏扫厂商联动及适配，实现多源归一与漏洞扫描紧耦合，能够主动地、定期自动化地发起漏洞扫描，并将扫描结果与资产进行匹配，进行资产和业务的脆弱性管理。 | 3年 |
| 6 | 弱点管理模块优化 | 1.将弱点管理模块中涉及弱点二字修改成漏洞二字。  2.在原有弱点管理模块字段的基础上增加以下字段：漏洞名称、漏洞等级、漏洞来源、漏洞类型、受影响主机、域名、系统名称、漏洞发现时间、漏洞详情、整改建议、处置情况（未处置、已处置待复测、已修复）。  以下对每一个字段进行详细说明：  漏洞名称：将弱点名称修改成漏洞名称。  漏洞等级：将威胁等级修改成漏洞等级。  漏洞来源：将扫描器名称修改成漏洞来源。  漏洞类型：手工填写漏洞类型。  受影响主机：保持不变。  域名：手工填写域名。  系统名称：手工填写系统名称。  漏洞发现时间：将漏洞导入时间修改成漏洞发现时间。  漏洞详情：将弱点描述修改成漏洞详情。  整改建议：将解决建议修改成整改建议。  处置情况：将处置状态内容修改成未处置、已处置待复测、已修复三项，进行手工选择。  处置情况：增加一个文本框用于填写处置情况。   1. 在弱点管理模块中点击受影响主机可以跳转到资产详情。 2. 在弱点管理模块中点击域名可以跳转到Web业务系统页面，查看详情。 3. 弱点重模块工单处置返回后，处置状态自动变为已处置待复测。   6.弱点管理模块中漏洞资产添加编辑按钮并且对属性具有编辑功能。  7.弱点模块增加手工添加漏洞功能，增加excel批量漏洞导入功能。  8.手工添加、漏洞导入的漏洞需要和IP资产、域名资产进行关联。  9.漏洞具备工单管理功能。  10.当从资产详情漏洞信息跳转到弱点管理模块时，需要展示所有与该资产关联的所有漏洞信息，包含：漏洞库。  11.添加漏洞知识库查询模块。支持知识库功能，支持对漏洞条目进行自定义编辑，可对漏洞名称、等级、类型、漏洞描述、漏洞修复建议、参考信息进行修改和完善，具备上传图片和附件的等功能，形成贵州农信专属的漏洞知识库。 | 3年 |
| 7 | 原厂驻场安全运营服务 | 工作内容描述：  1、安全设备定期巡检：驻场人员定期对于态势平台进行安全巡检工作，及时针对大数据组件健康性等内容进行实时监测，确保态势感知大数据平台安全稳定运行。  2、安全设备系统升级：当安全设备厂商发布了最新系统升级信息，且得到单位确认必须升级时，驻场人员对态势平台行同步升级，保证安全设备系统处于最新状态，安全设备系统版本一致。  3、安全设备故障处理：设备故障分为软件故障和硬件故障。当驻场人员在日常监控过程中发现设备存在故障时，立即以电话的方式汇报给单位相关人员，并告知故障详细内容并截图记录，在得到单位相关人员确认并同意故障处理后，驻场人员协助单位相关人员进行故障处理。  4、安全设备防护告警监测：通过分析态势感知产生的安全事件或日志信息，获取网络中存在的各类病毒、蠕虫、非法访问、攻击事件，并进行及时的处理。根据安全风险和安全问题情况有针对性地采取措施解决问题，配合及时进行策略调整和优化降低风险。  5、安全漏洞整改跟踪：在漏洞整改过程中，驻场人员对漏洞整改情况进行详细跟踪和记录，并在修复工作完成之后，及时更新漏洞知识库。  6、安全咨询支持：从安全的角度为其提供网络安全部署与部署流程的建议，积极参加应用系统上线前安全评审会，参与应用系统安全测试工作，并详细记录每项工作步骤和结果，并以邮件的形式汇报给单位相关人员。  7、专业的安全建议：根据贵州农信的攻击数据，提借专业的处理意见和建议，以期进一精准的处置攻击行为。  8、数据分析模型规则优化：模型能力优化增强，通过结合省联社告警现状及业务情况在现有模型基础上进行进一步完善补齐，确保告警数据精准有效。  9、数据告警分析及报表输出：驻场人员可对历史离线数据进行分析，对历史数据进行二次挖掘，发现隐藏异常行为；通过将现有告警与历史数据进行比对。驻场人员对于离线数据进行整理归纳，分析总结数据中关联性、时效性及与业务相关性，并定期离线数据分析处置报告，整体把控数据告警走向等内容。  10、数据编排：驻场人员通过自定义编程创建特征，通过python等语言进行创建，并提供语言创建模板等信息，按照客户需求进行定制开发相关工作。  11、数据推送：驻场人员通过对态势感知离线数据进行汇总整理并根据客户需求进行推送到SOAR等多平台，确保离线数据二次利用价值。  12、重大保障时期协助监控省联社体系网络安全风险及事件，进行相应安全验证及应急响应，确保省联社网络安全。  13、白名单策略梳理：结合现场告警数据与业务场景配置相应白名单策略。  14、攻击特征梳理：结合现场告警梳理攻击特征。 | 3年 |

## **2.自动化编排与响应系统（国舜）扩容采购清单**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **模块** | **参数描述** | **维保** |
| 1 | POC脚本管理 | 1. 提供至少500个针对近几年漏洞的POC脚本库。 2. 支持定期更新POC脚本库。 | 3年 |
| 2 | PYTHON脚本管理 | 1. 支持在线自定义脚本，默认支持以下场景：   (1)、取证分析脚本  支持对高风险或高价值资产进行取证，脚本自动对资产进行线索取证，研判分析后将对资产更新评分，取证维度包含以下：网络连接、系统进程、系统用户、计划任务、历史命令、可疑文件等方面。  (2)、日常事务脚本  临时策略自动化管理:对接内部工单系统、OA系统，将跨部门协作能力固化在脚本中。  通用紧急呼叫：适用于发生紧急安全事件的场景，或其他需要紧急呼叫相关人员的场景，如发生重大网络故障，需要紧急联系相关人员等。  3、日常运营脚本  资产漏洞扫描、系统监控与报警、定时日志清理、定时数据备份和网络可达性测试等脚本。 | 3年 |
| 3 | 关联分析引擎优化 | 1、简化策略配置  原每个场景n个数据源关联分析时由原来配置2n-1个规则简化为1个策略，并在每个关联分析策略添加时，将自带默认配置，降低关联分析策略的配置难度  2、关联分析引擎性优化。  对关联分析引擎进行优化，提高实时分析效率。 | 3年 |
| 4 | 白名单策略 | 通过白名单策略对业务场景数据进行加白处理，并生成相应的安全告警，自动研判为误报，当业务场景发生变更时能及时进行策略调整，提高了误报排查工作的便利性，场景维度如：  1、部分业务网段内告警加白  2、部分设备告警加白 | 3年 |
| 5 | 拓扑管理 | 1、支持搭建资产拓扑，并对资产拓扑进行管理。  2、支持以拓扑监控维度进行溯源分析。 | 3年 |
| 6 | 运营数据共享 | 提供平台间的数据共享能力：  1、能够自定义共享数据内容。  2、支持通过syslog、kafka进行主动推送，以及支持第三方平台通过api调用获取数据。  3、对数据共享行为进行可视化监控。 | 3年 |
| 7 | IP封堵模块 | 1、支持历史IP封堵记录进行管理。  2、支持剧本封堵和人工批量导入IP进行封堵。  3、支持对封堵的IP进行解封，以及对封堵失败的IP再次执行封堵。  4、增加攻击次数统计、增加多种查询条件等。  5、对网关IP、基站IP增加标签，并添加相应查询条件。  6、对网关IP封堵对应相应时长，剧本进行相应优化。 | 3年 |
| 8 | 安全运营报表 | 1、针对贵州农信现网安全事件，支持多维度展示告警的来源以及威胁状态。  2、针对贵州农信日常安全效果对告警降噪效果、处置方式、自动化安全运营效果进行统计。 | 3年 |
| 9 | 威胁研判列表 | 针对贵州农信在日常安全威胁研判时使用习惯对威胁研判列表模块进行优化，如：增加客户关注的常用字段，增加一键封堵、批量封堵等。 | 3年 |
| 10 | 资产安全画像 | 通过对接CMDB系统以及平台资产自发现能力，对资产进行风险暴露面梳理，如端口、组件、服务等，结合漏扫结果以及平台的漏洞版本库，对资产进行脆弱性评分，形成资产安全画像。 | 3年 |
| 11 | 自动基于网络拓扑溯源 | 支持对接现场设备提供自动还原拓扑结构能力，并基于拓扑结构对攻击进行溯源，还原真实攻击路径。 | 3年 |
| 12 | 第三方平台对接 | 对接观山湖数据中心、贵安数据中心、灾备数据中心和第三方外联DDOS或防火墙实施IP地址封禁。 | 3年 |
| 13 | 原厂驻场安全运营服务 | 工作内容描述：  1、安全设备定期巡检：驻场人员定期对于态势平台进行安全巡检工作，及时针对大数据组件健康性等内容进行实时监测，确保态势感知大数据平台安全稳定运行。  2、安全设备系统升级：当安全设备厂商发布了最新系统升级信息，且得到单位确认必须升级时，驻场人员对态势平台行同步升级，保证安全设备系统处于最新状态，安全设备系统版本一致。  3、安全设备故障处理：设备故障分为软件故障和硬件故障。当驻场人员在日常监控过程中发现设备存在故障时，立即以电话的方式汇报给单位相关人员，并告知故障详细内容并截图记录，在得到单位相关人员确认并同意故障处理后，驻场人员协助单位相关人员进行故障处理。  4、安全设备防护告警监测：通过分析态势感知产生的安全事件或日志信息，获取网络中存在的各类病毒、蠕虫、非法访问、攻击事件，并进行及时的处理。根据安全风险和安全问题情况有针对性地采取措施解决问题，配合及时进行策略调整和优化降低风险。  5、安全漏洞整改跟踪：在漏洞整改过程中，驻场人员对漏洞整改情况进行详细跟踪和记录，并在修复工作完成之后，及时更新漏洞知识库。  6、安全咨询支持：从安全的角度为其提供网络安全部署与部署流程的建议，积极参加应用系统上线前安全评审会，参与应用系统安全测试工作，并详细记录每项工作步骤和结果，并以邮件的形式汇报给单位相关人员。  7、专业的安全建议：根据贵州农信的攻击数据，提借专业的处理意见和建议，以期进一精准的处置攻击行为。  8、数据分析模型规则优化：模型能力优化增强，通过结合省联社告警现状及业务情况在现有模型基础上进行进一步完善补齐，确保告警数据精准有效。  9、数据告警分析及报表输出：驻场人员可对历史离线数据进行分析，对历史数据进行二次挖掘，发现隐藏异常行为；通过将现有告警与历史数据进行比对。驻场人员对于离线数据进行整理归纳，分析总结数据中关联性、时效性及与业务相关性，并定期离线数据分析处置报告，整体把控数据告警走向等内容。  10、数据编排：驻场人员通过自定义编程创建特征，通过python等语言进行创建，并提供语言创建模板等信息，按照客户需求进行定制开发相关工作。  11、数据推送：驻场人员通过对态势感知离线数据进行汇总整理并根据客户需求进行推送到SOAR等多平台，确保离线数据二次利用价值。  12、重大保障时期协助监控省联社体系网络安全风险及事件，进行相应安全验证及应急响应，确保省联社网络安全。  13、白名单策略梳理：结合现场告警数据与业务场景配置相应白名单策略。  14、攻击特征梳理：结合现场告警梳理攻击特征。 | 3年 |

## 3.网络安全威胁情报系统（微步）扩容采购清单

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **模块** | **参数描述** | **维保** |
| 1 | 威胁情报管理 | 1、失陷指标情报（IOC），支持每秒查询500条数据（500EPS）；  2、全网IP信誉情报，可支持每秒查询500条数据（500EPS）； | 3年 |