长沙农村商业银行股份有限公司

态势感知平台项目需求

信息技术部

2021年2月

目 录

一、项目背景 1

二、建设目标 2

三、建设内容 3

3.1功能需求 4

3.2系统部署方式 12

# 一、项目背景

随着国内外网络安全问题日益凸显，企业面临的网络安全威胁也不断提升，越来越多的黑客组织开始对企业进行入侵以获取高额利润，包括虚拟货币勒索服务、挖矿木马和境外势力支持的APT（高级持续性威胁）组织；攻击行为也呈现出隐秘性和潜伏性。

国家层面对网络安全工作的重视程度也不断提升，国家、金融监管机构在信息科技监管要求中明确提出网络安全监测预警和追踪溯源要求：

（1）《中华人民共和国网络安全法》：“要加强网络安全检测预警”和“加强网络安全态势感知”；

（2）银监会发布《中国银监会办公厅关于加强网络信息安全与客户信息保护有关事项的通知》简称（银监会发布（2017）2号文），指出金融机构及银行应加强应用安全防护，建立事前、事中、事后的安全控制体系；支持日志的检测审计，对入侵事件的危害和范围进行事后溯源和评估；

（3）等保2.0关键技术使用要求：“应依据国家网络安全等级保护政策和标准，开展安全监测、通报预警、应急处置、态势感知等工作”，“建立事件分析模型，发现高级安全威胁，并追查威胁路径和定位威胁源头，实现对攻击行为的有效防范和追查”。

为将我行信息安全建设从单点防护状态提升到立体掌控体系，并可建立持续性的监测、分析、溯源、预警、响应的整体机制，我行需统一规划并建设态势感知平台。

# **二、建设目标**

**2.1、项目目标**

在我行现有安全措施基础上，以网络安全、数据安全、安全运维为核心驱动力，不断满足新的网络架构和安全支撑保障需求，并利用统计分析、分类/聚类分析、关联分析、相似性分析、时间序列预测、机器学习等多种分析技术，通过对各类安全告警日志的深度分析和挖掘，构建多个场景的安全威胁分析模型，形成以多源分析、预警通报、事件回溯等议题的安全分析和预警体系，帮助我行更直观、实时的跟踪和监测整个生产环境的安全态势和资产安全趋势。

**2.2、业务目标**

建立全方位的安全分析感知与防护体系；具备安全威胁要素分析和异常行为快速发现能力；实现利用威胁情报、大数据安全分析等技术建立协同处置、全生命周期跟踪安全事件的工作模式；具备直观、清晰的整体安全可视化感知能力；具备安全威胁排除、攻击链分析、事件溯源等高级安全威胁溯源能力，提升我行的整体安全事件分析和应急响应能力，并辅助安全决策。

**2.3、技术目标**

（1）对生产环境的远控木马外联行为、横向、纵向攻击行为进行识别、追踪和处置；

（2）强化整体安全态势可视化感知能力。通过网络安全态势感知系统实现预警通知效果，并对其范围、类型、危害以图形化展示，为安全分析人员提供直观、强大、清晰的安全威胁预警能力，以及重大问题、事件的整体性报告，为安全管理员，安全决策人员提供可靠的数据支撑；

（3）实现溯源高级安全威胁。建设实现利用大数据安全分析、协同分析、全生命周期跟踪安全事件的溯源流程，可极大程度的方便运维人员进行安全威胁排除、攻击链分析、事件溯源等需求；

（4）提升安全运营能力。针对发现的安全威胁事件，可提供对应的安全响应的处置策略和任务，协同各安全产品对于威胁事件进行终止、隔离、取证等安全手段，快速终止威胁的持续，提升联动防护能力。

# **三、建设内容**

本次态势感知平台项目内容范围包括①**态势感知系统**（1套）、②**全流量采集检测分析系统**（2台）、③**配套安全培训服务**等。

## 3.1功能需求

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **编号** | **模块** | **序号** | **功能分类** | **功能描述** |
| 一 | 态势感知系统 | 1 | 数据采集 | ①支持采集汇总的信息种类应至少包括：网络流量、日志、资产信息、威胁情报、上报数据、漏洞库等。②支持通过多种方式采集日志或文件，采集方式支持被动采集和主动采集两种方式，其中被动采集应至少支持Syslog、SNMP、Netflow、FTP等方式，主动采集方式支持通过插件代理主动采集日志。③支持通过自定义威胁情报、网络升级、第三方导入等方式进行情报采集。④支持通过API接口方式采集上报数据。⑤可支持第三方采集器接入。⑥支持通过配置相关解析规则、过滤规则、富化规则、日志类型，来达到归一化、过滤、丰富、分类日志信息的目的；支持自定义预处理解析规则文件定义日志格式范式化预处理过程。⑦日志接入支持界面交互式配置，简化日志接入复杂度，通过图形化界面配置日志解析条件，利用正则表达式、分隔符、Key-Value、JSON等方法定义解析规则，实现灵活的日志格式范式化，系统自动生成解析规则，无需通过代码编写解析规则。⑧支持自定义过滤规则功能，通过配置AND、OR等嵌套关联逻辑、条件及丰富的操作符来实现复杂的日志过滤需求，减少无用日志数量。⑨支持对主流安全设备的快速解析，至少支持对启明WAF、绿盟ADS、绿盟IPS、绿盟IDS、绿盟防火墙NF、山石网科防火墙、亚信杀毒服务器、北信源桌管服务器、华为和华三防火墙等设备的解析，支持快速解析和对接新增安全设备，具备丰富的解析规则库并可自定义解析规则。 |
| 2 | 数据分析 | ①支持大数据架构进行分析，支持根据业务和数据量进行分析能力升级扩充。②支持接入各种类型数据，数据类型应至少包括：安全日志、网络流量日志、服务器日志、中间件日志、失陷类威胁情报数据、资产数据、漏洞数据其他日志等数据进行关联分析，以发现网络攻击、僵尸网络、勒索软件、APT事件、业务违规事件和远控木马等高级威胁事件。③平台应内置包括规则模型、关联模型、统计模型、情报模型、离线模型等在内的≥5大类安全分析模型。④安全分析模型支持自定义创建，可通过字段映射、静态值、模板、表达式等多种方式自由定义分析模型的告警名称、威胁等级、告警类型、攻击链、可选字段、告警描述、处置建议等内容。⑤支持对安全日志中字段，包括但不限于应用协议、目的IP、目的主机名、目的端口、目的用户名、数据流方向、情报IOC等进行任意形式的逻辑与或非形式组合建模，运算方式包括但不限于AND、OR、等于、不等于、大于、小于、属于、不属于、存在、不存在等，并能根据组合方式自动生成运算表达式。⑥具备针对招标方实际安全管控场景，完成安全分析模型自定义开发的能力，且每种场景分别提供对应的可视化数据展示界面。分析场景主要包括但不限于：账户异地登录、非法外联外访、HTTP代理发现场景、DNS Tunnel发现场景、reGeorg Tunnel发现场景、SOCKS代理发现场景、暴力破解场景、DGA域名检测发现场景、弱口令检测场景、邮件敏感词、邮件敏感后缀等。⑦支持基于攻击链场景分析功能，统计分析应至少应包括侦查跟踪、武器构建、载荷投递、突防利用、安装植入、通信控制、达成目标七个分析维度。⑧支持通过对命中规则后产生的关联事件的分析，以对规则的有效性进行验证。⑨支持统计模型，支持从安全日志中发现重要的统计型特征，发现如频繁暴力破解尝试等恶意行为；支持在实时流计算过程中统计日志中的任意字段中的数值，统计策略应至少包含事件数统计、求和、均值、最大值、最小值等，可设定阈值并触发超阈值异常告警。⑩支持情报模型，支持通过最新的威胁情报信息与安全日志碰撞发现最新和潜在的安全威胁，威胁情报库导入，情报分类包含DDoS、C&C、僵尸网络、木马、恶意域名等；与安全日志中的IP、域名等信息实时碰撞产生告警，通知用户及时处置。日志检索功能提供自定义统计视图，根据搜索结果进行视图统计，支持多种视图类型，包括但不限于：“指标卡/柱状图/堆积柱状图/折线图/条形图/堆积条形图/面积图/堆积面积图/饼图/玫瑰图/词云图/散点图等，并支持将视图引用到仪表板进行监控。 |
| 3 | 调查处置和漏洞、资产管理 | ①支持通过创建调查任务对威胁事件和可疑事件进行调查分析，通过人工调查分析确定威胁以及威胁的严重程度和影响范围；调查任务中可添加完整的：日志数据、关联事件数据、告警数据、漏洞数据、自定义富文本数据（调查分析者从其他途径获取的相关数据）；支持对以攻击者和受害者情况视角对调查任务中的数据做统计分析；支持调查结果的图形化展示。②告警信息可直接调用工单系统，告警信息可直接添加到调查任务，支持添加到已有任务或创建新的调查任务。③支持对第三方漏洞扫描和基线检查设备进行扫描任务调度，可自动获取扫描器的扫描策略；支持扫描任务的建立、删除、修改、启动、停止等操作；支持周期性扫描任务和快速扫描任务扫描；漏洞信息可直接调用工单系统，漏洞信息可直接添加到调查任务，支持添。加到已有任务或创建新的调查任务。④支持导入第三方漏洞扫描报告和基线检查报告，系统至少要默认支持绿盟等主流扫描器厂家漏扫和基线报告的解析识别和导入管理，支持人工漏扫报告和基线报告的导入，用户根据系统自带的导入模板进行漏洞信息的导入（提供截图证明，并加盖原厂商公章）；同时在项目实施时通过定制化功能支持自动导入漏扫报告和基线检查报告。⑤支持通过流量无侵入式自动发现资产，支持发现终端、Web服务器、DNS服务器、邮件服务器、FTP文件服务器等类型。⑥支持资产信息的自动发现和维护，支持资产的手工批量导入导出、补充导入、集中修改资产属性值。⑦支持对IPV6资产的管理。 |
| 4 | 自动化编排响应 | ①支持前端拖拽式交互设计安全风险分析研判策略和联动响应剧本，支持多种策略编排动作，包括但不限于数据源、分析组件、处置响应等，可自动判断策略编排是否合理并弹窗提示。②支持通过任务看板查看自动响应任务的数量、状态、运行趋势；可查询并追踪每条自动化响应任务的运行阶段查看详细信息，任务执行过程中可加入安管人员控制环节，通过邮件、短信方式将告警和分析报告推送到对应用户。③支持与不同品牌的网关类安全产品进行联动防护，防护策略支持设置每次阻断不同时长生效时间。 |
| 5 | 态势展示 | ①态势展示大屏包括但不限于：资产风险态势、全网漏洞态势、外部威胁态势、内网威胁态势、业务资产外联态势、安全运营态势等。②平台应具有统一的安全运营门户，作为多个安全态势分析与感知功能的统一入口，集成态势感知、威胁狩猎、通报预警、异常监测、运行监测等多个功能模块，实现平台内部业务、数据、服务、资源的无缝整合与集成。 |
| 6 | 平台管理 | ①支持提供帐号管理、角色管理、权限管理、组织机构管理，实现对用户账号整个生命周期的管理，提供对态势感知平台用户管理本身的创建、修改、删除和查询等功能。②支持用户自定义界面logo和态势大屏名称，并可根据实际地址，设定内部地址地理定位。③支持对平台运行状态阈值的配置，监测自身运行状态，支持状态异常告警；支持对采集对象地址的配置。支持对数据存储时间的配置。④能够对集群进行状态监控，可对集群CPU、内存、磁盘使用率进行监控。⑤支持对用户操作审计和系统事件审计；监测敏感数据操作日志，定期执行日志审计。⑥支持将系统告警日志以syslog形式发送其他平台。 |
| 7 | 自定义报表 | ①支持用户自定义编辑报告模板，根据实际的业务需求自定义统计分析的指标对象，生成有针对性的分析报告，安全分析中的所有字段内容，都可以作为报告的统计对象，并自定义时间范围实现报告导出。②可以针对某类特定的攻击，例如蠕虫病毒分类或者某具体病毒“WannaMiner挖矿木马”，按照IP段（不同的地区）导出分类统计报表，每个IP段（地区）哪些IP(主机)已中毒，中毒的行为是什么(例如访问了多少次哪个域名)，以excel、word等报表形式导出。 |
| 8 | 预警通告 | ①支持将安全事件以工单形式通过邮件、短信、消息中心通知责任人，并对工单处理流程进行跟踪；提供告警类型、漏洞类型、通用类型3类工单，可对告警、漏洞等内容进行下发处置；提供对应的功能授权。 |
| 9 | 威胁情报 | ①威胁情报种类应至少包括：失陷检测情报、IP信誉情报、文件信誉情报等类型，支持威胁情报升级服务。支持威胁情报库的在线升级和手动升级。②支持通过离线导入或手动编辑添加的方式，形成本地威胁情报，允许用户自建行业情报库，并实现情报库的增删改查、导入、导出功能。 |
| 10 | 对接兼容 | ①投标产品能够和湖南省农信社态势感知平台对接，如无法对接，提供无条件开发对接承诺函。②支持人行数据上报。参考《金融行业态势感知与信息共享平台数据接入与信息共享标准v1.3.3》提供安全事件数据上报和威胁情报实时消费获取功能（注：安全事件从甲方现网中采集），提供数据上报策略功能等。 |
| 11 | 实配功能要求 | ①本项目需提供以上功能模块的所有授权，以及≥500个设备日志采集数据源授权。 |
| 12 | 实配硬件及性能要求 | 支持10G内网全流量分析，部署设备数量≥2台2U机架式集群设备，并且支持设备无限制集群扩容，含机架安装导轨；单台设备配置如下：①CPU：至少两颗十核CPU，主频≥2.20GHz；②内存：≥256GB；③硬盘：≥48T；④网卡：配置≥6个千兆以太网口；⑤电源：标配冗余双电源。 |
| 二 | 全流量采集检测分析系统 | 1 | 部署模式 | ①支持通过流量镜像的方式旁路部署在数据链路中，实现网络流量数据采集、威胁检测和日志外发。②支持同时接入多个镜像口，每个口相互独立不影响。 |
| 2 | 策略配置 | ①支持基于源地址、目的地址、应用、流量采样比、时间进行选择数据采集对象，可以针对采集对象进行网络流量数据采集和威胁检测数据采集，网络流量数据采集支持自定义流量载荷字节数。②支持基于SSL协议的HTTPS流量进行解密，可添加基于源地址、目的地址的解密策略。③支持明文流量镜像。④支持添加SSL入站检查配置文件。SSL入站检查配置文件中指定SSL解密证书。⑤支持IP地理信息重映射，用户可新增指定IP或IP段的地理信息，支持IP或IP段地理信息导入导出，确保输出数据地理信息准确。 |
| 3 | 数据采集 | ①支持解析、生成及外发TCP流量日志。包括：传感器序列号、TCP数据流的结束方式、TCP数据流开始的时间、源IP、源端口、目的IP、目的端口、源mac、目的mac、协议、上行字节数、下行字节数、客户端系统信息、服务端系统信息、TCP流的统计信息等字段。②支持解析、生成及外发UDP流量日志。包含：传感器序列号、UDP数据流开始的时间、UDP数据流结束的时间、源ip、源端口、目的ip、目的端口、源mac、目的mac、协议、上行字节数、下行字节数、上行包数、下行包数字段。③支持解析、生成及外发Web访问日志。包括：传感器序列号、日志生成时间、源ip、源端口、目的ip、目的端口、HTTP请求方法、HTTP包头的URI字段、uri\_md5值、host字段、host\_md5值、origin字段、cookie字段、ser-Agent字段、referer字段、链接来源、原始数据、http状态码、Content类型等字段。支持解析、生成及外发域名解析日志。包括：时间、源ip、源端口、目的ip、目的端口、DNS访问类型、Host、Host字段\_MD5值、地址资源、MX记录、响应结果状态、域名规范名称等字段。④支持FTP/SMB/TFTP三种协议的解析、生成及外发文件传输日志。包括：传感器序列号、协议、日志生成时间、客户端IP、客户端应用端口、服务端IP、服务端应用口、传输模式、文件名字、文件md5、文件类型等字段。⑤支持解析、生成及外发LDAP行为日志。包括：传感器序列号、协议、日志生成时间、源ip、源端口、目的ip、目的端口、用户名、LDAP版本、ldap操作类别、op的具体操作描述等字段。⑥支持解析、生成及外发ftp、smb、oracle、mysql、mssql、postgresql、ssh、pop3、smtp协议的登陆动作日志。包括：日志生成时间、源ip、源端口、目的ip、目的端口、协议、登陆密码、登陆结果、用户名等字段。⑦支持解析、生成及外发pop3、smtp、imap、webmail协议的邮件行为日志。包括：传感器序列号、协议、message-id信息、生成时间、源ip、源端口、目的ip、目的端口、邮件发送/接收时间、邮件抄送人、主题、被当前邮件回复的邮件ID、密送人、附件名字、回访路径、邮件实际接收者、附件md5、mime\_type、邮件正文等字段。⑧支持解析、生成及外发Oracle、MySQL、MSSQL、PostgreSQL、MongoDB、DB2、Redis等协议的数据库操作日志。包括：传感器序列号、日志生成时间、源ip、源端口、目的ip、目的端口、协议、协议版本、登录用户、数据库类型、数据库操作返回的状态信息、操作信息等字段。⑨支持解析、生成及外发FTP控制通道日志。包括：传感器序列号、日志生成时间、源ip、源端口、目的ip、目的端口、用户名、标记操作顺序、操作命令、操作结果等字段。⑩支持解析、生成及外发SSL加密协商日志。包括：传感器序列号、日志生成时间、源IP、源端口、目的IP、目的端口、版本号、会话id、服务器名字、证书中的颁发者的名字、证书的有效期的起始时间、证书的公钥、Sever端证书的持有者等字段。支持分析多种文件传输协议，包括：邮件（SMTP、POP3、IMAP、webmail）、Web（HTTP）、FTP、SMB；可执行文件还原格式包含：EXE、DLL、OCX、SYS、COM、apk等；压缩文件还原格式包含：RAR、ZIP、GZ、7Z等；文档类型的还原格式包含：word、excel、pdf、rtf、ppt等。 |
| 4 | 漏洞检测 | ①支持多种类型的漏洞检测，包括：缓缓冲区溢出、拒绝服务和恶意扫描。②支持自定义漏洞，允许通过文本匹配或正则匹配定义漏洞特征。③漏洞特征库支持自动及手动升级。 |
| 5 | Web攻击检测 | ①支持对Webshell请求、XSS攻击、SQL注入、远程代码执行、命令注入、远程文件包含、本地文件包含、文件上传、路径遍历、信息泄露、越权访问、XXE注入、网页篡改等web攻击检测，对任意单条检测规则支持启用和禁用。 |
| 6 | 恶意文件检测 | ①支持挖矿活动、流氓软件、可疑文件、勒索软件、僵木蠕、Webshell、木马后门、间谍软件等恶意程序检测规则，可针对任意单条规则进行启用和禁用。②支持自定义检测规则，允许通过文本匹配或正则匹配等定义恶意特征。 |
| 7 | 网络安全检测 | ①支持Flood攻击检测，包括SYN Flood、ICMP Flood、UDP Flood和IP Flood。②支持恶意扫描检测，包括Tracert检测、IP地址扫描、端口扫描。③支持异常包攻击检测，包括Ping of Death、Teardrop、IP选项、TCP异常、Smurf、Fraggle、Land、Winnuke、DNS异常和IP分片④支持应用层Flood攻击检测，包括DNS Flood和HTTP Flood。 |
| 8 | 行为审计与可疑通信检测 | ①支持违规操作、违规访问、违规应用、违规外发等行为审计检测规则，可针对任意单条规则进行启用和禁用。②支持隧道通信、可疑内容、恶意IP、恶意域名、恶意证书、远程控制等可疑通信检测规则，可针对任意单条规则进行启用和禁用。 |
| 9 | 实配硬件及性能要求 | ①单台硬件要求：标准2U及2U以上机架设备，冗余电源；提供≥4个千兆以太网口，≥1个千兆管理口。②单台性能要求：同时开启流量采集、分析、日志上报等全功能情况下，可支持的混合数据流吞吐量≥5Gbps，HTTP并发连接数≥400万，HTTP新建连接速率≥15万/秒。 |
| 三 | 安全培训服务 | 1 | 全员安全意识培训 | 针对招标人的全体员工进行2次安全意识培训。 |
| 2 | 安全专业知识培训 | 针对招标人的科技条线或安全条线人员进行4次安全专业知识技能培训。 |
| 3 | 安全专业认证培训 | 提供CISSP、Security+或其他同类型的4人次安全培训和认证服务。 |

## **3.2系统****部署方式**

本次态势感知平台建设内容主要分为态势感知系统与全流量采集检测分析系统。运维管理区部署一套本次态势感知系统，核心交换机区域旁路部署2台全流量采集检测分析系统，通过流量镜像的方式对所有进出核心区域的流量进行安全分析。

通过部署全流量采集检测分析系统，将不同区域之间采集到的流量风险数据和日志信息数据传送到态势感知系统，进行统一收集、解析、关联分析，并在态势感知进行安全大数据关联分析及处理，最终通过大屏展示我行整体安全态势。