## 动物研究所网络安全服务项目需求说明

为进一步加强研究所网络安全态势感知和监测预警能力，及时发现和处理网络安全隐患和网络安全问题，实现研究所网络安全管理的外部攻击风险、内部数据访问、核心业务资产评估的全局可视功能，实现与网络防火墙、上网行为管理等安全设备的联动安全保障与网关间的协同安全防御功能，对网络进行7X24小时的实时监测。研究所拟采购网络安全服务，安全服务专家通过定期或持续线上或现场服务的方式，对安全流量日志进行分析研判，包括对外部威胁的识别、对内部脆弱性问题的深挖、对内网安全事件的判断，以及对安全有效性的分析，通过分析尽早发现研究所网络安全关键风险问题，并通过提供可实施修复处置建议和指导，做到网络安全风险及时发现和处置，提升研究所网络安全监测预警能力和网络安全风险防护水平。

### 一、技术要求

1、监测系统授权数：支持30个信息系统安全保障服务。

2、响应情况：具备全天候 7\*24 小时安全专家服务和预言判断，威胁发现及时响应，并提供解决方案；

3、修复建议：供应商需提供客观的漏洞修复优先级指导，不能以漏洞危害等级 作为唯一的修复优先级排序依据。排序依据包含但不限于资产重要性、漏洞等级以及威胁情报（漏洞被利用的可能性）三个维度。

4、漏洞检测：提供漏洞验证服务，针对发现的漏洞进行验证，验证漏洞在已有的安全体系发生的风险及分析发生后可造成的危害。针对已经验证的漏洞，自动生成漏洞工单， 安全专家跟进漏洞状态，各个处理进度透明，方便采购方清晰了解当前漏洞的处置状态，将漏洞处理工作可视化。

5、漏洞修复：针对存在的漏洞提供修复建议， 能够提供精准、易懂、可落地的漏洞修复方案（漏洞修复方案需包含多种修复方案以及修复过程中可能引发的其他问题的解决方案）；

6、漏洞复测：需提供漏洞复测措施，及时检验漏洞真实修复情况。供应商要支持采购方可按需针对指定漏洞，指定资产等小范围进行，降低漏洞复测时的潜在影响范围

7、漏洞跟踪：对发现的漏洞建立状态总览机制， 自动化持续跟踪漏洞情况，清晰 直观地展示漏洞的修复情况，遗 留情况以及漏洞对比情况，使得 采购方可做到漏洞的可视、可管、可控

8、漏洞扫描：提供不少于每月一次针对服务范围内的资产的系统漏洞和 Web 漏洞进行全量扫描，并针对发现的漏洞进行验证，验证漏洞在已有的安全体系发生的风险及分析发生后可造成的危害；

9、平台要求：供应商需在服务期内提供安全检测与响应平台服务满足监控管理、威胁检测、安全调查、资产管理、订阅服务等功能，所提供安全检测与响应平台服务为软件化部署。可以支持与本次采的杀毒软件、用户原有的防火墙、态势感知设备进行联动，用户现有下一代防火墙、终端检测与响应系统、态势感知等设备作为流量探针设备收集数据，满足主要区域间的流量监测需求。

10、资产的收集与录入：安全专家对服务资产进行收集，并将资产信息录入到安全运营平台中进行管理。

11、资产指纹探测：持续服务过程中安全专家定期对资产进行指纹（操作系统、中间件、软件厂商等信息）探测，并对指纹信息进行确认与更新，确保深信服安全运营中心中资产指纹信息的准确性和全面性。

12、脆弱性评估：部署脆弱性识别工具，主动对系统与Web开展漏洞扫描：对操作系统、数据库、常见应用/协议、Web通用漏洞与常规漏洞进行漏洞扫描。

13、安全问题跟进和处置和脆弱性问题修复指导：针对脆弱性评估的结果，安全专家分析研判后提供实际佐证材料，并给出修复建议，在持续服务过程中协助用户修复。

14、漏洞可落地修复方案：对漏洞进行分析并输出可落地的修复方案，通过工单系统跟踪修复情况。

15、实现信息化资产不同应用弱口令猜解检测，如：SMB、Mssql、Mysql、Oracle、smtp、VNC、ftp、telnet、ssh、tomcat等。针对不同行业提供行业密码字典，有针对性的进行内网弱口令检测。并将检测发现的问题通过工单系统跟踪修复状态。

### 二、提供配套安全态势感知设备要求

在服务期限内需要提供配套的态势感知安全设备放置在用户处，配置要求如下：

1、性能规格 存储容量≥21.8T，在带宽性能1Gbps时存储时长≥1200天/1Gbps。

2、硬件规格 规格：2U，内存≥96GB DDR4 2933，系统盘≥240G SSD，数据盘≥32TB，标配盘位数≥8，冗余电源，接口≥4千兆电口。

3、大屏可视：支持安全态势的可视化呈现，以大屏的方式从全网安全态势感知大屏、分支安全态势、安全事件态势、全网攻击、资产态势、网络安全指挥调度安全态势、设备运行态势、外联风险态势大屏等提供不少于16块大屏展示界面，提供产品功能截图证明并加盖厂商公章。

4、资产识别：支持资产主动扫描和被动发现发现功能，主动扫描支持自动入库、手动入库、扫描目标、定时扫描等功能，提供产品功能截图证明并加盖厂商公章。

5、资产发现：支持通过主动发送微量包的扫描方式探测潜在的服务器（影子资产）以及学习服务器的基础信息，资产指纹信息包括资产类型、端口、操作系统、MAC地址、主机名等，提供产品功能截图证明并加盖厂商公章。

6、资产全生命周期管理：支持资产全生命周期自动管理，包括资产自动发现、多级资产、资产入库审核、资产离线风险识别、资产退库、资产数据更新，责任人管理机制等

7、弱口令检测：密码检测技术基于UEBA学习技术提取登陆成功的特征，通过UEBA技术对响应体内容和登录跳转路径进行持续学习训练登录成功特征，包括响应体内容Json、响应体关键字Keyword、响应体MD5值、响应体长度Length、登录跳转路径Location，可实时自动生成学习到的登陆成功规则。

8、漏洞分析：支持流量实时识别漏洞分析，漏洞分析类型包含配置错误漏洞、OpenSSH漏洞、OpenLDAP等操作系统、数据库、Web等，页面上支持展示业务脆弱性风险分布、漏洞类型分析、漏洞态势与危害和处置建议，并支持导出脆弱性感知报告。

9、弱口令识别：弱密码识别支持主动扫描，支持加密协议的弱口令登录检测，支持SMB、MySQL、Oracle、RDP、SSH、Redis、MongoDB、ElasticSearch、MSSQL、SHOPEX、74cmsb等协议。

10、联动处置：处置中心和重保中心的多个模块的安全事件内置多个处置策略模板，需要与现网运行防火墙联动、终端安全响应系统、超融合、负载均衡联动封锁、访问控制，支持与现网AC联动处置。提供厂商盖章证明文件。

11、探针硬件规格：2U，内存大小≥8G，硬盘容量≥480G SSD，冗余电源，接口≥6千兆电口，≥2万兆光口SFP+。

12、探针性能规格：网络层吞吐量≥2Gbp。

13、部署模式：旁路部署，支持探针接入多个镜像口，每个接口相互独立且不影响。

14、WEB智能检测：支持命令注入检测、PHP代码检测、XSS攻击检测、Webshell上传检测、SQL注入检测、XXE攻击检测、JAVA代码检测、SQL非注入型检测、MYSQL解析增强、php反序列化检测等自定义配置启用、高检出、低误报模式，提供产品功能截图证明并加盖厂商公章。

15、网站攻击检测：支持SQL注入、XSS攻击、网页木马、网站扫描、WEBSHELL、跨站请求伪造、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、Web整站系统漏洞、自定义WAF规则、WAF云防护等网站攻击检测，提供产品功能截图证明并加盖厂商公章

16、异常流量检测：支持标准端口运行非标准协议，非标准端口运行标准协议的异常流量检测，端口类型包括3389、53、80/8080、21、69、443、25、110、143、22等，提供产品功能截图证明并加盖厂商公章。

17、高级检测：支持5种场景的日志传输模式,包含标准模式、精简模式、高级模式、局域网模式、自定义模式，适应不同应用场景需求，提供产品功能截图证明并加盖厂商公章。

18、特征库 内置URL库、IPS漏洞特征识别库、应用识别库、WEB应用防护识别库、僵尸网络识别库、实时漏洞分析识别库、恶意链接库、白名单库，提供产品功能截图证明并加盖厂商公章。

19、安全专项告警联动处置：支持文件、邮件、勒索、挖矿相关安全事件专项页面展示，且所有专项告警支持直接进行联动处置，联动处置支持自动调用内置处置策略模板，也支持自动化编排的自定义处置流程策略。（需提供截图打印加盖原厂公章证明，且所投产品必须提供第三方权威机构功能项的产品检测报告）。

### 三、服务要求

1、人员配备：需提供配置一名经验丰富的云端安全专家作为云端专属服务经理，配备专属用户微信群，实时解决问题，在线响应需求；

2、快速响应：对于特别重大安全事件应启动应急响应机制，15分钟之内云端专家进行响应，2小时上门处置；

3、7\*24小时威胁分析研判 基于云端安全能力平台，云端专家提供7\*24小时的威胁监测：依托于安全防护组件、检测响应组件和安全平台，将海量安全数据脱敏，包括漏洞信息、共享威胁情报、异常流量、攻击日志等数据，经由大数据处理平台结合人工智能和云端安全专家使用多种数据分析算法模型进行数据归因关联分析，实时监测网络安全状态，对安全告警和威胁进行分析研判，并生成生成工单；

4、驻场服务：提供每月不少于2天的驻场服务，协助进行安全事件处理。

5、重保服务：重大节假日期间需要提供现场或远程在线保障服务。

6、安全运维报告：每半年总结阶段性安全运行情况，并提供《安全运行半年度报告》，必要时进行现场或远程总结汇报。

7、安全服务周期为三年，按年付费。