**深圳市宝安纯中医治疗医院网络威胁态势检测分析与审计安全建设项目需求书**

**建设单位：深圳市宝安纯中医治疗医院**

**编制部门：信息管理部**

**编制日期：2025年5月6日**

# **第一章 项目概况**

## 1.项目背景

随着信息化新技术的不断发展与国内居民在自身健康需求关注度的逐渐提升，医院为了提升居民医疗健康的管理与服务水平，通过信息化手段，例如远程诊疗、移动诊疗、医疗物联网、电子病历、电子支付的方式拓展了医疗信息化的应用场景，互联网医院的开展，也改变了传统线下就诊的服务模式。随着“互联网+医疗健康”、大数据、人工智能、5G以及区块链等新兴技术的飞速发展，让医疗信息化不再受传统IT服务架构的桎梏，医疗数据的价值进一步得到提升，上述内容使得我国医疗信息化出现明显的开放化、智能化、数据化特征。

**开放化，万物皆可互联：**医院逐步开展医联体或医共体的区域医疗服务模式，在这样的大环境下，医院加强了各类互联网挂号及在线诊疗相关业务应用的建设，医院间的数据交互更是成为了开展分级诊疗、远程会诊等业务协同的基本需求，打破了医院原有相对封闭的应用及数据使用环境。

同时在医院的线下与线上诊疗服务中，更多的智能自助服务终端、移动设备终端、医疗物联网终端通过有线网络、无线网络、物联网络的方式相互连通并提供服务，业务暴露面越来越多，攻击可以通过网络不受时空限制，导致医院的安全风险也越来越大。

**智能化，一切皆可编程：**目前医院信息化已步入智慧医疗建设阶段，智能导诊、电子病历、电子支付等网络信息技术在健康医疗便捷普惠，医院各个业务系统均承载在软件基础上，智能化、软件化使的一切皆可编程，可是软件都有漏洞，不规范的应用开发导致的漏洞越来越多，例如应用程序中包含的第三方组件可能原生存在漏洞、对输入数据不进行格式内容校验、对个人信息数据的采集不符合国家规定标准等，这些应用又承载着患者、医生、医院的重要敏感数据，一旦被不法分子利用漏洞进行渗透和破坏，将会造成严重的数据泄露事件发生。

**数据化，数据驱动业务：**医院的医疗卫生信息系统及数据，往往记录着关于居民的各类个人基础信息、以及电子病历及电子健康档案等敏感信息，同时也记录着关于医院处方、科研等重要医院运营管理数据，而且随着大数据技术在医疗行业的应用，这些基础数据不断被进行二次汇总及大数据分析，分析结果往往用于临床诊断以及公共卫生决策，其价值较原始数据又有了更高的提升。医院间、监管机构、第三方应用对数据的交换及使用的普及也促进了医疗数据的共享。在医疗数据价值凸显的背后医疗行业数据泄露事件却频频发生，大量的病人数据、处方数据通过非正常渠道方式流通到医疗产业、黑色产业的各个链条，数据倒卖行为、非法统方行为屡禁不止，如果在医疗行业数据安全方面不加以重视，将给居民、医疗行业乃至国家社会带来非常严重的不良影响。

近年来络安全形势日益严峻，各种挑战与风险增大，国家层面对网络安全工作的重视程度也不断提升，通过《中华人民共和国网络安全法》立法指出要“加强网络安全监测预警”和“加强网络安全态势感知”，习近平总书记在2016年和2018年的全国网信工作会议也指出“要全天候全方位感知网络安全态势”并且“要做到关口前移，防患于未然”。

深圳市宝安纯中医治疗医院自2019年开业以来，在信息化建设和发展过程中，严格落实网络安全法，监管政策法规和网络安全等级保护要求，始终将网络安全体系及安全能力建设放在首位。目前，我院已制定较为完善的网络安全管理制度、数据安全及个人信息安全管理制度、供应链管理制度、应急预案等制度体系，并配套建立了基于链路负载、应用防火墙、流量防火墙、防病毒系统、网闸、应用负载等为边界的基础安全防护体系，当前医院已初步建立了相对完善的安全防护体系，为医院的网络安全及业务安全提供了可靠保障。较好地支撑了我院各类业务系统尤其是HIS、LIS、PACS等核心核心业务系统和预约挂号系统等互联网类系统安全可靠的运行。但面对日益复杂的外部网络环境和持续不断的高级网络攻击，我院也深刻认识到网络与数据安全工作的重要性和紧迫性，依靠传统的以孤立单点防御为主的网络安全防御体系已不能更好地评估、预测、处置日益严峻的网络安全威胁和攻击。

为改善我院单一安全设备防护能力的不足，提高对安全威胁事件及网络攻击的准确识别和有效追溯，确保安全防护工作的及时性和有效性，网络安全态势感知平台。我院计划开展网络威胁态势检测分析与审计安全建设，以态势感知平台建设为抓手，实现院内全流量管控、资产管理、安全监测、通报预警、工单下发及安全威胁自动处置。并通过对接现有边界安全设备，并将各类安全日志、系统日志及流量日志汇总至平台和日志审计系统，实现威胁情报数据共享和多重研判预警和对网络安全整体长效的“可见、可查、可控”能力。通过对全网网络安全态势的“全面感知、准确感知、实时感知”，进一步提升我院网络安全整体防护能力，降低网络安全风险。

## 2.项目目标

为贯彻落实《基本医疗卫生与健康促进法》《网络安全法》《密码法》《数据安全法》《个人信息保护法》《关键信息基础设施安全保护条例》《网络安全审查办法》以及《信息安全等级保护管理办法》《医疗卫生机构网络安全管理办法》等有关法律法规和制度规定，加强和规范卫生健康行业网络与数据安全工作，保护网络与数据安全，助力卫生健康事业高质量发展的要求，在现有安全建设体系下，充分发挥“技防”和“人防”作用，建设深圳市宝安纯中医治疗医院网络威胁态势检测分析平台与审计安全系统。通过引入多源网络行为关联分析技术，基于知识图谱的多维并列可视化技术，高级安全威胁分析技术，AI安全建模分析技术等进一步提升网络安全整体防护能力，降低网络安全风险。

具体目标包括以下几点：

（一）构建安全统一管理平台。通过构建以态势感知平台为核心，对安全设备和网络设备进行统一纳管，打破原本孤立的安全防护局面，实现以点到面的全方位多设备安全信息共享、资产管理、安全监测、通报预警、情报溯源的全面防护能力，并通过场景建模、剧本编排，智能联动处置技术实现全流程闭环管理和安全运营机制。

（二）大数据安全分析研判。首先，通过探针对业务全流量数据进行采集、利用、分析完善网站相关服务资产信息，发现相关的的安全漏洞和未知威胁。其次，基于传统威胁特征库，加入AI人工智能大模型，将各安全设备的安全日志和威胁情况集成在态势感知平台进行自动化分析研判，通过多设备的研判结果比对、多维度多层级安全攻击分析溯源，深入安全事件的起因、攻击路径和影响分析，不断完善系统攻击特征库和网络安全威胁情报库，强化平台对攻击威胁的特征分析能力，获得更精准的研判效果，进一步提升安全预警和安全处置的精准度。  
 （三）完善安全合规评价体系。通过对全业务全流量数据的采集、存储、分析，完善医院信息安全资产信息，发现相关安全漏洞和威胁攻击，以及对历史安全事件进行数据分析统计、安全预计预测，从多维度对安全运行状况进行分析展示，从而在业务流程规范、系统应用安全、风险评估、安全合规评价等方面给予支撑。

## 3.建设内容

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **建设内容** | **功能模块** | **功能需求** | **数量** | **单位** |
| 网络威胁态势检测分系统 | 威胁检测探针 | 1.动态沙箱分析  2.恶意行为检测  3.恶意文件检测  4.威胁分析及联动验伤 | 1 | 台 |
| 态势管理分析平台 | 1.安全监测、分析、响应、管理、处置、报告等；  2.内置关联分析引擎，数百种基本分析规则  3.安全威胁情报库  4.多设备接入和联动  5.自动化编排处置 | 1 | 台 |
| 审计系统 | 日志审计 | 500台设备和服务器安全日志、系统日志、应用日志收集、分析、存储，留存时间大于6个月 | 1 | 台 |

## 4.编制依据

* 1. 国家政策
* 《中华人民共和国网络安全法》（主席令12届第53号）；
* 《中华人民共和国数据安全法》（主席令第八十四号）；
* 《国家信息化发展战略纲要》（中办发【2016】48号）；
* 《计算机信息网络国际联网安全保护管理办法》（公安部令33号）；
* 《信息安全等级保护管理办法》（公通字[2007]43号）；
* 《网络安全审查办法》（网信办令6号）；
* 《关于加强信息安全保障工作的意见》（中办发[2003]27号）；
* 《政府信息系统安全检查办法》（国办发[2009]28号）；
* 《关于开展信息安全风险评估工作的意见》（国信办[2006]5号）；
* 《关于大力推进信息化发展和切实保障信息安全的若干意见》（国发[2012]23号）；
* 《关于印发国家网络与信息安全事件应急预案的通知》（国办函[2008]168号）；
* 《关于加强党政机关计算机信息系统安全和保密管理的若干规定》的通知（国保发[2007]13号）；
  1. 本地政策
* 《广东省数字政府建设总体规划（2018-2020）实施方案》（粤府办〔2018〕48号）；
* 《广东省人民政府办公厅关于印发广东省“数字政府”网络安全体系建设总体规划2022年的通知》（粤办函〔2022〕24号）；
* 《深圳市电子政务项目运行维护经费指导意见》（深经贸信息信息字【2017】201号）；
* 《深圳市电子政务信息安全管理试行办法》（深府办〔2013〕23号）。
  1. 3、技术规范
* 《信息安全风险评估规范》（GB/T 20984-2007）；
* 《信息安全风险管理指南》（GB/Z 24364-2009）；
* 《信息安全管理体系要求》（GB/T 22080-2008）；
* 《信息安全管理实用规则》（GB/T 22081-2008）；
* 《信息系统安全管理要求》（GB/T 20269-2006）；
* 《信息安全事件分类分级指南》（GB/Z 20986-2007）；
* 《信息安全事件管理指南》（GB/Z 20985-2007）；
* 《信息安全等级保护管理办法》（公通字[2007]43号)；
* 《信息安全技术网络安全监测基本要求与实施指南》（GB/T 36635-2018）；
* 《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）；
* 《信息安全技术个人信息安全规范》（GB/T 35273-2017）；
* 《信息安全技术数据安全能力成熟度模型》(GB/T 37988-2019)；
* 《信息安全技术大数据安全管理指南》（GB\_T 37973-2019）；
* 《信息安全技术大数据服务安全能力要求》（GB\_T 35274-2017）；
* 《深圳市电子政务信息安全管理试行办法》（深府办〔2013〕23号）；
* 《信息安全技术基于互联网电子政务信息安全实施指南》（GB/Z 24294-2009）；
* 《信息安全技术数据库管理系统安全技术要求》（GB/T 20273-2019）；
* 《信息系统安全等级保护基本要求》（GB/T22239-2019）；
* 《信息系统安全等级保护定级指南》（GB/T 22240-2019）；
* 《信息系统安全管理要求》（GB/T20269-2006）；

# **第二章 项目建设必要性**

## 1.现状及存在问题

深圳市宝安纯中医治疗医院院网络系统包括三套网络（内网、外网、智能专网），本项目只涉及对内网、外网的信息安全监测和审计。

在进行各应用系统建设的同时，建立医院的信息安全体系，从保障医院信息系统的整体安全出发，从物理安全、边界安全、桌面终端安全、业务监控与审计、病毒防护、流量分析等方面进行全面布署，切实提高医院信息化安全水平。

图示

AI 生成的内容可能不正确。

图1.医院网络拓扑结构

* 内网为医院的核心生产网络；主要用于开展日常医疗业务（HIS、LIS、PACS、财务、体检系统等）业务。医院内网划分为：核心区、安全运维区、数据中心区、外联区、汇聚区及接入区等区域。
* 外网为医院提供Internet接入及部署网络预约挂号系统、后勤办公、信息查询等业务。医院外网划分为：核心区、外联区、DMZ区、汇聚区及接入区等区域。

目前医院内外网和业务系统主要通过边界安全、网络安全、应用安全、终端安全、主机安全等设备或系统进行安全防护。目前，经过多年网络安全基础建设，安全防护体系日趋完善。但是现阶段不同网络、不同区域、不同品牌型号的安全设备由于厂商不同、技术架构不同、接口不同，尚未实现安全能力融合和联动。目前我院存在安全自动化程度低、大数据关联分析能力不足以及异构设备联动处置能力不足等问题。

1）威胁信息和事件数量多

近年来，随着网络开放化，万物泛在互联，系统智能化，漏洞无处不在，面临的威胁挑战也不断攀增。为了保障业务系统安全网络中部署了各类安全防护设备，不同网络、不同的网络区域（互联网边界接入区、内网办公区、外网办公区、服务器区、核心区等）、不同品牌型号的安全设备组成（华为防火墙、华三防火墙、深信服上网行为管理、深信服WAF、360防病毒系统等），设备部署分散，各类安全设备“各自为战”，形成信息孤岛。

同时现网中的安全设备，每天在进行网络检测和安全防护时产生海量的告警和日志，由于各类原始安全数据来自于华为、华三、深信服、360等多个厂商的安全设备/系统，因此数据的准确性、可用性均无法评估，是安全运营人员在工作过程中极其困扰的问题，分析一个安全告警，往往需要登录多台设备/系统获取信息，并仍需对这些信息的准确性进行人工判断分析，这些过程中信息查询工作、关联分析工作往往耗费巨大的人工精力。然而根据一项互联网上2023年的调研显示，目前攻击者平均突破时间已经缩短至79分钟，创历史新低，其中记录到的最快突破时间仅为7分钟，如何在从复杂威胁、新型威胁中快速发现安全风险，如何从如何从海量信息中收集有效告警，如何从海量告警中快速、精准定位高危、高风险、高价值安全事件，是提升安全运营、安全能力的基础。

2）安全事件人工处置效率低

目前我院网络安全防护采取了纵深防护体系，安全设备类型如下：

边界侧：部署了边界防火墙、上网行为管理、WAF；

终端和主机侧：部署了防病毒软件；

目前这些产品都是基于单点防护工作机制，网络安全技术之间的整合度低、缺乏联动响应机制，出现安全事件时需要登陆到各个系统执行处置动作，而大部分设备并来自不同厂家，接口不一，无法做到自动化联动处置。例如，当在发现未知威胁告警时，需要切换到防火墙和WAF、防病毒系统中分别添加策略进行处置。使得在应对网络安全事件时应急处置效率不高。

而且，安全操作仍然主要依赖手动维护，每个安全事件处置人员的处置经验、安全技能、处置流程存在不一致性的问题。并且伴随着保障业务安全、高及时响应的要求，网页篡改、勒索挖矿、webshell攻击、数据泄密等在非工作时间段的重大安全事件、紧急风险排查的工作任务，都需要具备7\*24全天候处置、处置时效短的能力。

因此仅仅依靠现有的人工处置，存在处置效率低、处置时效难以保障、处置规范难以统一的问题，亟需通过自动化、智能化技术，实现单点防御向整体防护的转变，共同构建体系化、自动化、流程化的安全响应机制，从而更加有效地保障我院网络安全和稳定。

## 2.项目必要性分析

### 2.1 业务安全保障必要性

医院作为关键信息基础设施的重要组成部分，也是网络安全的重点。近年来，随着关键信息基础设施的互联互通，网络攻击的组织化现象日益明显，医院网络安全工作面临新的挑战。云计算、大数据、人工智能、区块链等新技术的发展，拓展了网络安全领域。医院要聚焦网络安全新发展、新技术，共同促进数字化转型和高质量发展。

医院是经济运行和社会发展的命脉，也是对信息系统依存度非常高的行业。在智慧医疗发展背景下，外部网络安全环境恶化以及自身系统架构日趋复杂的新形势下，医院正面临着愈发严峻的网络安全威胁。依托现有传统安全能力，实现对安全威胁的提前感知与预测预防，对正在发生安全事件的实时防御和响应处置，对潜在的安全威胁的持续监测，对已发生安全事件的分析溯源，以全面提升攻防能力为目标的安全建设，以保障智慧医疗业务安全势在必行。

### 2.2 统一安全管控必要性

随着信息化建设步伐的不断加快，信息网络技术在业务上的应用日趋广泛，这些先进的技术带来了前所未有的便利，大幅提升了医院的信息化管理质量和服务水平，但同时对网络信息和数据的依赖程度也越来越高。随着网络规模不断扩大，网络越来越复杂，网络资产、安全系统数量也越来越多，告警日志数量级越来越大，网络中的流量数据信息越来越复杂、庞大，如何保障网络的持续、安全、高效运行是安全管理人员面对的巨大挑战。在这种情况下，安全管理人员必须对整网的告警信息、资产状况、漏洞状况、流量状况、威胁状况、网络攻击数据包原始内容等网络安全基础元素以及整个网络的运行情况进行充分的了解和掌握，才能在网络出现性能和安全问题时，能够快速准确的分析问题原因，定位故障点和攻击点并将其排除，从而实现网络价值最大化。现有的安全监测与防护手段面对不断恶化的网络安全形势应接不暇，体现出以下不足之处：

* 静态检测规则落后于先进的攻击手段
* 安全设备各自为战无法形成协同防御
* 网络攻击溯源能力不足
* 无力应对信息系统大规模数据量
* 海量告警不容易发现威胁
* 响应处置依赖人工，安全运维效率低下

分散管理，难以高效管控：医院分为内外网，不同网络存在不同品牌、不同类型的安全设备，各个安全设备上的安全数据未能打通，导致风险难以统一掌控；

风险剧增，安全能力不足：医院昨晚国家的关键基础设施，业务价值高，容易遭到外部攻击和数据窃密。现有安全防御设备数量多，各自独立，每天海量的安全吿警，无法从海量安全数据中挖掘出真正的攻击事件，难以识别防范高级威胁。

因此，如何对全网安全风险统一管控，如何深度挖掘安全风险、防范高级威胁，如何提高安全运营处置效率，如何是当前亟须解决的关键问题。

### 2.3 网络安全风险检测需要

随着新技术的快速发展，愈演愈烈的网络战已成为关键基础设施安全面临的新挑战，关键信息基础设施时刻受到各方的威胁，智慧医疗也面临更加严峻的考验。Web攻击、渗透入侵、服务器控制、横向渗透、无文件攻击、APT攻击、0day漏洞利用等多种攻击技术和手段层出不穷，网络攻击逐步向有组织、常态化、定向攻击的方向发展，攻击的针对性、持续性、隐蔽性显著增强，增加了网络安全防护难度，安全威胁已经弥漫在该行云边端的各个角落。

同时随着网络规模不断扩大，网络越来越复杂，网络资产、安全系统数量也越来越多，告警日志数量级越来越大，资产漏洞发现越来越困难，网络中的流量数据信息越来越复杂、庞大，如何保障网络的持续、安全、高效运行是安全管理人员面对的巨大挑战。在这种情况下，必须消除安全孤岛所导致的数据割裂问题，才能在网络出现安全问题时，快速准确的分析问题原因，定位攻击行为。同时对全网安全设备、主机、终端、操作系统、中间件、数据库等进行多维度关联分析，以全维度的安全大数据为基础，利用多维度分析引擎对数据进行深度检测，从威胁的各个阶段针对威胁的特征、行为、攻击方式等进行全面关联分析，结合知识和情报驱动实现对高级威胁攻击的全方位威胁发现、实时监测、研判溯源，深度发现医院集团面临的整体网络威胁。

### 2.4 提升运营效率需要

从技术层面将当前各自独立的、多元化的系统日志信息、网络流量、资漏信息等横向整合，从管理层面将各区域、各网络、各厂商的安全设备纵向拉通，构建以安全对抗为核心的 “全局指挥+快速响应”协同机制。从全视角维度发现潜在的真实攻击事件，为处置决策提供支持。构建多元协同、深入融合的安全防御体系，形成一体化安全运营体系，有效提升全局一体的动态防御、主动防御、整体防控、联防联控的安全能力，实现高效协同的安全防护与运营。

通过云端情报支撑对攻击者、攻击路径、恶意样本进行识别，形成攻击者画像，支撑对攻击者进行研判；通过安全事件关联的attck全景攻防知识库，以图谱方式，支撑运营团队对攻击者技战术进行研判识别；通过安全事件原始日志下钻溯源，攻击链路图以及针对安全事件提供的处置建议，支撑运维团队进行事件分析和研判。为安全管理人员智能决策提供数据支撑。

针对发现的安全事件通过平台落地标准化运营流程，实现安全风险实时监测、联动处置、标准化运营。运营团队对处置结果进行监控，并根据处置状态对事件处置剧本流程进行持续的优化，为运营人员安全事件的分析、溯源、响应、处置提供决策支撑，提升整体的安全运营效率。

## 3.项目可行性分析

深圳市宝安纯中医治疗医院经过多年的发展，具备丰富的大型项目建设和管理经验，信息化建设具备一定的基础，拥有专业技术过硬的管理和技术人员。

本次项目将在医院现有信息化建设和宝安区区域医疗信息化建设的基础上，以医院二期信息化项目规划要求和医院总体发展战略为指引，建设满足业务发展需要的信息化系统，提升医院数字化建设和应用能力。

本项目经过充分认证与分析，项目建设所需的技术等条件切实可行，并且根据市场调查，本项目所涉及到的各项软件及硬件产品国内均有成熟的案例以及可供选择的多种可靠的先进产品，项目建设过程和建设成效都将在可控范围内，基于当前技术，对把控系统的开放性、兼容性、高效性、完整性等具有切实可行性，项目支撑技术成熟可行。因此，本项目能够确保在限期内进行建设，并且能保证快速见效。

综上所述，经过综合分析与充分认证得知，本项目建设具有充分的建设必要性和可行性

# **第三章 项目需求分析**

1. 详细技术参数和配置要求

|  |  |
| --- | --- |
| 一、态势管理分析平台 | |
| 1 | 硬件指标 |
| 1.1 | 机架式设备；CPU为国产CPU，性能不低于24核，主频不低于2.20GHz；内存：≥256GB；硬盘：≥48TB；RAID卡：≥RAID5；接口：≥6个千兆电口；扩展槽：≥4个PCIE槽位；电源：冗余电源 |
| 2 | 性能指标 |
| 2.1 | 支持日志源数量：≥200个 |
| 2.2 | 支持单个探针最大流量：≥2Gbp |
| 2.3 | 数据性能：≥20000EPS |
| 3 | 功能指标 |
| 3.1 | 全方位多角度监测网络安全现状与态势，支持对安全事件、外部攻击者、攻击能力图谱等维度实现实时告警展示，并支持大屏轮播，并自定义播放顺序。  支持安全报告分析和阅览。 |
| 3.2 | 支持对采集标准化的日志进行普通检索和高级检索分析。可以灵活便捷地设置检索查询条件，筛选条件可以是单个字段，也可以是添加多个逻辑组合。普通检索：支持系统推荐常用字段检索日志；高级检索：检索分析引擎基于检索语言生成检索分析模型，可对长周期安全日志数据进行复杂运算，支持输入查询语句检索，支持NOT/AND/OR/Group By，支持=、>、<、>=、<=、!=、in、like、rlike等运算符来检索日志。 |
| 3.3 | 支持通过TCP，UDP，Syslog，WebService、SSH、Telnet、JDBC、WMI、FTP、SNMP、FTP、SFTP、HDFS、目录、文件、Kafka等采集协议，无需单独部署日志采集设备，实现多种设备（包括医院现有安全设备）的告警日志直接接入平台 |
| 3.4 | 支持界面化配置规范化规则，实现采集的日志格式归一化，解析规则支持正则表达式，支持多级解析提取嵌套字段，并对提取的字段进行字段类型、名称、取值的规范化。 |
| 3.5 | ▲日志解析支持划词提取，支持划词选中日志中任意字符串，自动生成正则解析语句。支持日志解析规则的在线测试和结果预览，能够直观展示日志字段的解析结果，并且支持解析的日志记录，能够通过执行日志记录每条子解析规则的字段映射情况和结果。（需提供产品功能截图证明） |
| 3.6 | ▲支持日志字段映射，能够将原始日志映射为统一标准日志。支持字段映射方式包括：直接赋值、值映射、默认值、时间戳、时间格式化等，支持针对不同的日志格式在赋值时选择Unicode解码、Base64解码、Hex解码、Url解码等方式进行直接解码转换，提高日志格式转换工作效率。（需提供产品功能截图证明） |
| 3.7 | ▲基于端网融合数据，不断扩展安全专项场景检测，支持挖矿场景化专项分析。统计挖矿受害资产、展示挖矿阶段，包括挖矿木马下载-挖矿木马安装-与控制端建立通信-挖矿获利，统计每个阶段受影响的资产信息。（需提供产品功能截图证明） |
| 3.8 | 支持挖矿受害资产视角统计该资产下相关的挖矿告警，展示挖矿告警名称、威胁等级、攻击次数、挖矿阶段、矿池域名、矿池地址、最后活跃时间、处置状态等。支持下钻查看挖矿告警详情。支持对挖矿相关告警进行处置、发起工单。处置动作支持：IP封堵、域名封堵、终端隔离、终端查杀、虚拟补丁、忽略、加白、线下处置。针对封堵、隔离、查杀等动作能够调用联动设备插件下发自动执行处置动作。 |
| 3.9 | ▲支持基于IP的可视化关系图谱方式进行威胁狩猎，实现风险钻取分析功能，根据不同的时间维度、攻击方向、威胁类型、ATTCK&CK战术查看攻击者和受害者的风险要素，对整网安全进行可视化逐层分析和逐级追踪，可以从IP进行下钻分析，聚合关联与该IP相关的所有安全告警与日志，支持逐层节点下钻呈现告警上下游关系。  具备狩猎报告一键快照能力：支持创建、修改、删除狩猎报告，支持将狩猎关系图、通过狩猎下钻检索的日志和告警等元素一键添加到威胁狩猎报告内容中。  （需提供上述产品功能截图证明） |
| 3.10 | 支持对告警字段进行排序。支持对展示的告警字段进行聚合分析，选择某个告警字段能够统计该字段的值、告警总数、告警占比，支持选择某个字段值添加、排除到检索查询条件中，根据用户需要提高检索效率。 |
| 3.11 | 支持查看告警详情，包括告警信息、标准日志、关联脆弱性、关联资产、处置响应和告警字段。在告警信息中展示攻击者、受害者信息、告警摘要、取证信息。 |
| 3.12 | 支持从告警或安全事件页面查看与资产的关联性，能够展示告警中相关资产的资产名称、资产IP、设备类型、资产责任人、端口、组件、版本号等。 |
| 3.13 | 支持从告警或安全事件页面查看与脆弱性的关联性，能够展示告警中相关资产的脆弱性信息；能够从告警TAB页面直接查看影响的资产、以及该资产存在的脆弱性信息，包括脆弱性类型、脆弱性名称、漏洞CVE编号、漏洞CNNVD编号、资产名称、资产IP等。 |
| 3.14 | 支持对告警或安全事件进行手动或批量处置、发起工单。处置动作支持：IP封堵、域名封堵、终端隔离、忽略、加白、线下处置。针对封堵、隔离等动作能够调用联动设备插件下发自动执行处置动作 |
| 3.15 | 精准的安全事件（实现安全告警事件少量精准），通过多数据源多维关联分析、告警聚合，减少告警数量，方便安全分析人员在海量告警中聚焦有效、高频的告警信息；结合XDR融合云端、网络、端点行为关联分析，定位攻击成功、端点失陷的安全事件。 |
| 3.16 | 支持高亮展示命中ATT&CK战术的阶段。支持查看安全事件的攻击路径、时间线、告警列表、关联资产、关联脆弱性、处置响应和事件字段信息 |
| 3.17 | 增强云端网融合关联分析，支持TDA的告警和终端EDR IOA的告警关联。支持安全事件页面深度溯源分析，还原攻击故事线、进程树。 |
| 3.18 | ▲支持端网融合安全事件深度溯源分析，还原攻击路径，能够通过链路图方式展示攻击者对应的告警名称以及攻击结果。支持在攻击链路图中下钻查看攻击详情，包括查看该攻击相关的告警信息、标准日志信息、关联的资产、关联脆弱性、处置响应信息，支持展示该攻击的告警威胁定性结果。（需提供产品功能截图证明） |
| 3.19 | 支持端网融合还原攻击故事线，以时间线的方式还原攻击者过程，支持在时间线中展示攻击者、受害者、攻击结果、来源设备类型等。支持在时间线中下钻查看每个攻击过程相关的告警详情。 |
| 3.20 | ▲支持还原进程树，在进程树能能够溯源进程信息、进程路径、进程运行账号、进程命令等。便于对终端行为进行溯源分析。（需提供产品功能截图证明） |
| 3.21 | 支持将黑客所使用的各类攻击技术直观的展示出来，将告警映射到ATT&CK攻击技术二维矩阵图，按照攻击战术或阶段划分黑客可能使用到的全部攻击技术。  支持在ATT&CK 热力图中统计当前网络中遭受黑客攻击使用的战术、技术产生的告警数量，并已不同的颜色进行标注和区分。 |
| 3.22 | 支持以插件形式接入第三方产品的联动处置功能，支持插件热插拔，插件数量不低于100种；预置多种主流设备系统联动，比如防火墙、IPS、WAF、终端安全、主机安全、漏扫、上网行为管理、钉钉、企业微信、威胁情报、CDN、邮件等。 |
| 3.23 | 支持剧本自定义编排，可根据不同联动需求，通过拖拽插件、剧本自定义形成安全预案，实现安全流程的自动化处置。支持对自动化动作以及人工动作的逻辑编排。 |
| 3.24 | ▲支持新建工单流程，支持可视化编排工单流程。在可视化工单流程编排时支持根据需求新增受理人节点；支持对受理人节点进行参数配置，配置节点名称、工单受理参与人、此节点的工单处置截止时间、超时流转时间（超时通知时间）、工单的通知方式、选择此节点的工单操作（包括通过、驳回、转派、指派、加固、复核、签收等）、配置下一步的流转节点。（需提供产品功能截图证明） |
| 3.25 | 支持针对发现的安全告警、安全事件下发通报功能。  支持发起预警，选择预警类型、预警级别、事件类型、影响对象、涉及组织，输入预警详情，填写防范方式，选择发布方式（支持系统支持、邮件、钉钉、企业微信）和接收组织，配置是否要求签收，设置签收时间等。 |
| 3.26 | ▲平台支持主动测绘发现资产信息，探测到的资产数据自动装载到资产数据库。支持资产探测任务，以IP或者IP段、端口或者端口段进行扫描，能够识别操作系统、开放端口、组件名称、组件版本、MAC地址等，所得的资产数据可以自动或者人工确认装载到资产数据库进行统一管理。平台支持设置资产测绘任务执行周期，支持手动执行、单次执行和周期性执行，执行设置周期性执行频率。（需提供产品功能截图证明） |
| 3.27 | ▲支持多源资产融合，支持与同品牌的终端安全、主机安全、TDA等系统对接获取多来源资产，并支持根据设备类型设置资产融合的优先级配置。（需提供产品功能截图证明） |
| 3.28 | ▲平台支持创建脆弱性检测任务，对检测对象发起系统漏扫、基线检测、弱口令检测、WEB漏洞检测等，支持设置任务的执行时间和执行周期。支持展示脆弱性检测任务结果明细，能够分类查看系统漏洞、web漏洞、基线违规、弱口令的脆弱性数量以及待派单、待加固、待复核的数量。（需提供产品功能截图证明） |
| 3.29 | 支持为不同组织、角色的用户设定不同的页面访问权限。对所有菜单的一级功能项、二级功能项、三级功能项可以进行选择性启用或禁用 |
| 3.30 | 支持数据外发，外发方式支持syslog和kafka，支持数据外发时进行加密和认证，保障外发数据安全。 |
| 二、态势威胁检测探针 | |
| 1 | 硬件指标 |
| 1.1 | 软硬一体化1U标准机架式设备； 千兆电口≥6个，CPU≥4C，内存≥32G，硬盘容量≥4T，可扩展插槽≥2个，沙箱个数≥1个，冗余电源 |
| 2 | 性能指标 |
| 2.1 | 吞吐量：≥1.5Gbps； |
| 3 | 功能指标 |
| 3.1 | 支持动态沙箱分析、恶意行为检测、恶意文件检测、威胁回溯调查分析。 |
| 3.2 | 支持HTTP、FTP、SMTP、POP3、SMB、IMAP、DNS、HTTPS、SMTPS、POP3S、IMAPS、RADIUS、KRB5、SNMP、NETFLOW、TFTP、NNTP等176种协议报文识别，支持1000+种应用识别。 |
| 3.3 | 支持多层 VLAN、VxLAN、MPLS、GRE、IP-IP、PPPoE等封装的网络报文流量解析和检测。 |
| 3.4 | 恶意文件传输的实时还原和检测能力，支持针对常用的文件传输协议包括：HTTP、FTP、SMTP、POP3、IMAP、SMB等协议进行网络传输文件的实时还原，并使用病毒检测引擎做实时检测的能力。 |
| 3.5 | ▲提供内置沙箱系统，内置沙箱允许用户导入自定义镜像，并支持包括但不限于Win XP、Win 2003 & 2008 & 2012 server、Win 7 & Win 10等主流Windows平台沙箱镜像。（需提供产品功能截图证明） |
| 3.6 | 支持25000条以上攻击检测规则，涵盖Web攻击、漏洞利用、恶意软件、隐蔽隧道、黑客工具、Webshell、内网安全等多种威胁类型。支持通过机器学习引擎，对XSS跨站脚本、SQL注入攻击、代码执行、命令执行等15种以上Web攻击场景进行检测。 |
| 3.6 | 沙箱能够对未知漏洞利用代码和恶意程序的以下行为进行动态分析，包括：  1).进程操作行为；  2).文件操作行为，文件删除、下载、共享或者复制；  3).系统配置操作行为，自运行或其他系统配置；  4).网络通信行为，控制与命令 (C&C)违规外联；  5).恶意未知威胁逃逸行为；  6).内存镜像分析，畸形，有瑕疵，或者带有已知威胁特征，劫持、重定向，或数据窃取，进程、服务，或者内存对象被篡改。 |
| 3.7 | 支持8000多CVE漏洞检测规则，支持2000多种信创漏洞检测，支持200多个国产厂商的系统或软件的漏洞检测，涵盖国产化系统常见的OA、ERP、CRM、数据库等系统. |
| 3.8 | 支持识别流量中的个人敏感信息，包括身份证、银行卡、手机号、港澳通行证等，并展示传输信息的协议、网站域名、URL、客户端IP、服务端IP，便于用户发现敏感信息的传输安全隐患和处置。 |
| 3.9 | 具备DGA域名检测和DGA家族识别的能力，涵盖50个以上的DGA家族。支持使用机器学习算法检测未知的DGA域名。可以支持10种以上DNS隐蔽隧道工具检测，具备独立的DNS异常分析模块，支持基于机器学习算法的DNS隧道工具检测。 |
| 3.10 | ▲弱密码和明文密码检测：  1）内置常见的弱密码字典，条数不低于一万条，并且每一条都包含对应的MD5、SHA1和Base64编码等常见的变化方式，适应更多的密码检测场景。其中每一条内置的弱密码都可以单独的开启和关闭。  2）支持自定义Web登陆密码的提取规则。可以编写提取规则从Web登陆页面中提取出用户名和密码信息，并使用弱密码检测规则判断登录密码是否为弱密码。  3）检测的结果包含登录账号、登录密码、登录API、登录结果等信息，登录密码需要管理员权限才能查看，并支持导出弱密码和明文口令的报告。  （需提供上述产品功能截图证明） |
| 3.11 | 支持自定义XFF检测规则。允许添加多条XFF提取的规则，并可以在规则中指定XFF提取的具体方式。 |
| 3.12 | 自适应告警抑制是通过对告警进行实时统计分析挖掘其中存在的噪声并对其进行实时抑制，告警抑制的计算和管理模块能够感知到规则和检测模型的变化，及时管理抑制规则。 |
| 3.13 | ▲支持pcap回放功能。对导入的pcap进行回放并进行威胁检测，回放产生的告警必须和正常的网络流量告警分页面展示，避免干扰正常安全运营。  可以在同一台设备上通过扩展硬盘的方式实现全流量的元数据基础信息和全流量报文留存的功能，无需接外部存储。（需提供以上两项产品功能截图证明） |
| 3.14 | ▲能够以某个恶意文件为中心，溯源整个文件的流转记录，并以图形化方式展示出来，直观展示在不同时间点上该恶意文件在不同主机服务器上的传播路径，支持文件下载。需具备带有“威胁情报的图谱构建”的自主知识产权证明。（需提供①产品功能截图证明；②同时提供自主知识产权证明文件扫描件） |
| 3.15 | 支持Syslog方式的日志传输，Syslog日志为CEF格式，可以和第三方SIEM/SOC系统无缝集成。Syslog传输协议支持UDP/TCP/TLS加密等方式。支持Kafka方式的日志传输。 |
| 三、日志审计 | |
| 1 | 硬件指标 |
| 1.1 | 软硬一体化2U标准机架式设备；内存≥16G，硬盘≥6T机械硬盘和500G固态硬盘，网口：千兆电口≥6个，千兆光口≥4个，千兆多模光模块≥2个； |
| 1.2 | 具有国产芯片和国产操作系统 |
| 2 | 性能指标 |
| 2.1 | 授权资产数≥500个 |
| 3 | 功能指标 |
| 3.1 | ▲支持将插件安装在目标主机上对主机的CPU利用率、内存使用率、磁盘使用率、磁盘使用情况、流量等信息进行转发，在产品监控界面中即可查看目标主机的监控信息（需提供第三方检测机构出具的带有CMA和CNAS标识的检测报告） |
| 3.2 | 支持使用代理（Agent）方式提取日志并收集，安装包支持界面下载，且安装支持可视化向导。 |
| 3.3 | ▲资产进行安全综合评分（需提供第三方检测机构出具的带有CMA和CNAS标识的检测报告） |
| 3.4 | 支持对Agent进行统一管控，包括卸载、升级、启动及停止操作，支持将日志收集策略统一分发 |
| 3.5 | 采用解决方案包上传对产品进行功能扩展 |
| 3.6 | 支持对收集到的重复日志进行自动聚合归并，减少日志量，并可由用户定义和修改的日志聚合归并逻辑规则 |
| 3.7 | 注册用户资产时，提供自动发现识别能力 |
| 3.8 | 支持亿级的日志里根据任意的关键字及其它的检索条件，秒级返回查询结果 |
| 3.9 | 支持设置日志存储备份策略，包括系统日志保存期（天）、硬盘使用率百分比等策略 |
| 3.10 | 支持日志备份自动传送到远程服务器，支持FTP、SAMBA、NFS等方式的远程服务器，并支持从远程服务器中恢复数据 |
| 3.11 | 自定义的报表支持多个统计维度的数据集合 |
| 3.12 | 内置综合性审计报告，并支持用户自定义报表 |
| 3.13 | 支持硬盘空间阈值告警，当硬盘使用率达到设定的阈值时可产生并外发告警 |
| 3.14 | ▲对日志数据进行SM4加密转发（需提供第三方检测机构出具的带有CMA和CNAS标识的检测报告） |
| 3.15 | 可以通过邮件、短信和屏幕显示进行告警 |
| 3.16 | 支持报表导出为PDF和Word格式文件 |
| 3.17 | ▲支持将安全事件通过资产、安全知识库、弱点库三个维度进行联动分析和匹配，将安全事件进行联动整合并生成安全事件日志（需提供第三方检测机构出具的带有CMA和CNAS标识的检测报告） |

1. 商务要求

（一）维保服务：

★1.本项目购买货物的免费维保期为原厂维保3年。维保期限自货物通过验收之日起算。

2.在维保期内，中标人提供软件升级以及常态化服务，中标人应为本项目配备常态化服务人员，服务人员需具有计算机科学与技术/软件工程/电子科学与技术/信息与通信工程等相关专业背景，两年以上相关从业经验。常态化服务包括：设备巡检、周期性服务总结、运维手册梳理、变更支持、关键时刻值守、技能传递培训等服务内容。

3.在维保期内，如货物非因采购人原因而出现的质量问题由中标人负责保修、包换或包退，并承担修理、调换或退货的实际费用。采购人不能修复、调换或不能退货的，应承担相应的违约责任。 4.维保范围含项目涉及的设备、安装涉及的网线及相关耗材。5.设备发生故障时，中标人需在 0.5 小时（含）内响应，1 小时(含）内无法远程定位问题或无法远程指导客户恢复业务，需安排售后工程师在2 小时（含）内到达现场协助排除故障，如故障在短时间内无法排除，需在4 小时（含）内提供备件或解决方案。

（二）安装要求： 中标人必须依照招标文件的要求和投标文件的承诺，将设备、系统安装并调试至正常运行的最佳状态。设备安装所需的网线等配件、耗材由中标人提供。中标人应提供主机设备的用户手册、保修手册、有关单证资料及配备件、随机工具。以上费用由中标人负责，包含在投标报价中。

（三）培训要求：提供仪器的使用说明，设备安装完后，由专业工程师对操作使用人员进行现场操作培训，介绍操作方法以及运行注意事项，直至用户相关人员熟练掌握为止。

1. 工期要求

30个工作日内完成交货、安装、调试和验收。