网络安全风险预警防御系统建设方案（医疗行业）

北京融讯光通科技有限公司

2023 年 12 月

目　录

一、 项目背景

中共中央总书记、国家主席、中央军委主席、中央网络安全和信息化委员会主任习近平在全国网络安全和信息化工作会议上强调：信息化为中华民族带来了千载难逢的机遇，我们必须敏锐抓住信息化发展的历史机遇，加强网上正面宣传，维护网络安全，推动信息领域核心技术突破，发挥信息化对经济社会发展的引领作用，加强网信领域军民融合，主动参与网络空间国际治理进程，自主创新推进网络强国建设，为决胜全面建成小康社会、夺取新时代中国特色社会主义伟大胜利、实现中华民族伟大复兴的中国梦作出新的贡献。

随着现代医院 IT 技术架构的演变、新兴技术的引入，来自医院内外部的各种安全风险不断出现，对医院网络安全提出了更多挑战，医院网络安全在技术层面和管理层面都亟待完善。

外部网络安全威胁持续增加：随着医院信息化水平的不断提高，信息技术成为支撑医院智慧化运营的重要手段，在诊疗服务方面为患者带来便利的同时，也促使医院信息系统在以往内网运行的基础上不断增加外部服务。然而，由于信息系统的版本升级往往未能贯彻网络安全三同步原则，即“同步规划、同步建设、同步使用”，造成业务安全设计滞后于业务应用设计，导致被攻击面扩大。同时，医疗数据因其高隐私性和高价值性，乃至关乎社会公共利益和国家安全，一直是被黑产组织渗透攻击的重点。

安全制度制订不足落实不力：医院信息系统的核心价值是为医疗过程服务，其建设和管理过程的注意力集中在了应用效果方面，现阶段，很多医院尚无健全可靠的网络安全制度，或者虽已制定制度却未充分落实。医务人员和医院管理者常常认为网络安全是医院信息管理部门的职责，对信息系统使用者的信息安全教育缺乏，业务管理部门安全职责的划分也不明确。

人员安全意识与技能不足：医院信息安全管理是一项整体工程，其中主要包括主机安全、网络安全、数据安全、机房安全、应用安全等方面，不仅需要强化医院网络安全设施建设，还需要增强信息技术人员安全理论知识和实践经验。尽管近年来行业整体安全水平有所提升，但相对于金融业、电信业等信息化转型较早的行业，医疗行业安全情况仍有较多短板，

行业从业人员安全意识和安全能力仍有很大提升空间。医院管理层对信息化建设及网络安全工作缺乏足够重视，在日常工作中未配备足够的专业技术与管理人员、网络安全设施落后，往往导致医院信息系统出现的安全隐患与漏洞问题无法及时发现与处理。

数据交互引发安全风险：随着业务的发展，消除医院内各业务系统的信息孤岛，加速院内的信息互通共享是医疗信息化建设的重中之重。这使得原有医院内外网物理隔离的架构面临颠覆性的改变，也使得无论是结构化或者是非结构化数据的安全防护，均存在一定程度的隐患，如技术漏洞、物理故障、恶意攻击等。

数据交互层面的风险以医保系统为例，一方面要与医院信息系统相连，另一方面要与各级主管部门和定点药店相连，在数据共享和业务共享的基础上为被保险人提供服务。相关必要的交互还包括银行、运营商和其他辅助机构的业务系统，因此安全威胁来源更为广泛。除了纵横交错的外部交互，医疗机构自有的公共服务平台也存在安全隐患，例如医院官网、微信公众号和 App，任何人都可能通过网站对医院互联网服务器发起网络攻击，进而危害内部服务器的安全。

同时，愈加复杂的医院应用架构，导致了更为繁复的接口开放和相互调用，三甲医院普遍有上百个业务系统，系统间通过集成平台或单体业务系统开放接口的方式实现数据互通，这些接口往往存在数据被盗用的隐患。

新兴技术带来的新型安全风险：近年来，云计算、大数据、物联网等新技术在医院信息化中逐步应用，同时也带来了网络外来入侵、数据滥用、数据泄露的安全风险的隐患。

云计算的基础设施和运营普遍由第三方管理，医院通过互联网访问云平台，而公有云平台资源由多个机构或部门共享，彼此间只做到了逻辑隔离。平台管理不善就会增加网络入侵风险和造成数据泄露和毁坏。

大数据和人工智能技术已成为医院提升服务能力、开展精细化管理的重要支撑，然而许多医院并未掌握全流程的数据管理、存储和人工智能模型训练应用，需要通过第三方人员对数据进行处理，数据泄漏的风险也随之加大。

物联网拓展了医疗系统各实体之间的集成连接，显著提升了数据的采集、处理和应用实时性，为医院管理和决策提供了基础。但物联网设备的低功耗、低性能难以支持复杂的安全策略，易受到未经授权访问和其他恶意攻击，攻击者可通过算力优势破解薄弱的加密算法，窃取敏感信息，或者仅干扰物联网设备的正常运行即可造成严重的人身或环境危害。

习近平主席指出，要加强党中央对网信工作的集中统一领导，确保网信事业始终沿着正确方向前进。各地区各部门要高度重视网信工作，将其纳入重点工作计划和重要议事日程，及时解决新情况新问题。要充分发挥工青妇等群团组织优势，发挥好企业、科研院校、智库等作用，汇聚全社会力量齐心协力推动网信工作。各级领导干部特别是高级干部要主动适应信息化要求、强化互联网思维，不断提高对信息化发展的驾驭能力、对网络安全的保障能力。

1.1 网络安全形势严峻

近年来，国内外网络安全相关的事件频发，而且有组织、有目的的攻击行为也越来越多，甚至有些已经上升到了国家安全层面，网络安全形势日益严峻，敲响了大家对网络安全的警钟。

1.1.1 国际安全形势

国际环境日趋复杂，网络霸权主义对世界和平与发展构成威胁，全球产业链供应链遭受冲击，网络空间安全面临的形势持续复杂多变。网络空间对抗趋势更加突出，大规模针对性网络攻击行为增加，安全漏洞、数据泄露、网络诈骗等风险增加。

搭载 NSA 网络核武 WannaCry 勒索攻击全球爆发

在 2017 年 5 月份爆发了一个全球性的勒索攻击“WannaCry”，该勒索软件在短短数小时内就发动数万次攻击，袭击了全球数十个国家，而后受害国家增至 150 多个，政府、企业、医疗、高校等各行业均有 IT 设备中招。其利用 Windows SMB(服务器信息区块)服务远程溢出漏洞(MS17-010)，并搭载 NSA(美国国家安全局)制造“永恒之蓝”网络武器，导致攻击威力倍增。

该事件是“NSA 武器库”中漏洞与勒索蠕虫病毒的首次联合攻击，其波及之广，影响之大，让它必定在病毒攻击的历史上留下浓重的一笔。虽然此次事件为各界造成了一定的经济损失，但从长远来看，其作用仍然是利大于弊的。因为通过此次事件，国内各行业组织在应对勒索软件攻击上，必将提升至一个新的防护高度。

美国时间 2021 年 5 月 7 日，美国最大燃油运输管道商科洛尼尔（Colonial Pipeline）公司遭受勒索软件攻击，导致 5500 英里输油管系统被迫停运。该输油管系统从得克萨斯州到新泽西州，每天输送 250 万桶燃油到东海岸和纽约，供应东海岸 45%的燃料。由于网络攻击，美国东海岸燃油供应受到严重影响，美国国内汽油价格达到七年来的最高水平，引发了人们对汽油、柴油短缺的担忧，5 月 9 日美国宣布多州进入交通运输进入为期至少 1 个月的应急状态，以应对事件对燃油运输产生的影响。科洛尼尔公司勒索软件攻击事件暴漏出美国数字化关键基础设施安全威胁情报的缺失和安全检测能力的不足,碎片化各自为战的网络防御已经无力应对新型网络攻击，单个企业力量无力对抗专业化高级黑客组织，必须要依靠国家赋能、通过协同联防才能建立起新的整体防护体系。据报道，攻击者仅在实施攻击的前一天（即 5 月 6 日）进入科洛尼尔公司输油管线控制网络，可见在此之前攻击者早已完成了侦察踩点工作，对目标网络环境了如指掌。

据相关报告不完全统计,2021 年上半年全球就至少发生了 1200 多起勒索软件发起的攻击事件，接近 2020 年公布的 1420 起，其中针对医疗系统和教育行业的攻击增加了 45%，平

均赎金从 2020 年的 40 万美元提高到 2021 年的 80 万美元。

1.1.2 国内安全形势

网络安全形势已然变得更加复杂。随着云计算、大数据、物联网、人工智能等技术的发展，网络威胁持续进化，变得更加棘手、难以应对。同时，网络攻击手段更为多样，数据泄露、勒索软件、APT 攻击等安全事件频发。

据国家信息安全漏洞共享平台（CNVD）统计，2020 年共收录安全漏洞 20704 个，继续呈上升趋势，同比增长 27.9%，2016 年以来年均增长率为 17.6%。其中，0day 漏洞数量为 8902 个（占 43.0%），同比增长 56.0%。

基于国家信息安全漏洞共享平台（CNVD）的统计数据可以预测 2022 年企事业单位内网的安全漏洞数量还将不断增加，甚至变得越来越复杂。由于内网 Web 应用的保护严重不足，攻击者利用安全漏洞的攻击行为将变本加厉，尤其借助自动化的工具，在短时间内以更高效、隐蔽的方式对 Web 进行漏洞扫描和探测，使得企事业单位面临更为严重的安全风险和损失。

某知名品牌监控设备被境外 IP 控制

2015 年 2 月，被江苏省公安厅标记为“特急”的通知称，该通知告知江苏省各市公安局科技信息化处，近期省厅接到省互联网应急中心通报，省各级公关机关使用的某知名品牌监控设备存在严重安全隐患，部分设备已经被境外 IP 地址控制。对于此次爆出的事件，有位长期跟踪安防行业的资深券商分析师表示，就了解到的情况，可能是由于该品牌设备在公网上应用太多，很多用户没有更改设备初始密码， 被植入病毒以后，受到攻击。一家不愿具名的著名安防企业高管终于对此事予以了分析解读。他表示，从披露的信息中提到被境外 IP 控制，很难想象是因为初始密码没有修改这么简单的原因。深入想一下，这个事情的背后不止对安防行业，或许会对整个国家信息安全都会有大的促进作用。可能很多人提到信息安全就会想到芯片，如国产化替代。其实，视频信息传输加密也同样值得关注，未来，互联网时代到来，大家对数据都会应用，包括其他信息传输，传输的问题就十分重要，数据传输加密以及数据采集加密就十分重要。

1.2 国内外发展现状

面对日益复杂严峻的网络安全形势，各国都在加强网络安全防护体系的建设，传统的技术手段已经无法满足应对复杂多变的网络安全威胁的需求，需要从主动防御的角度出发，加强网络安全风险预警体系的建设，才能掌握网络安全防护的主动权，防患于未然，降低安全威胁，减少损失。

1.2.1 国外发展现状

2021 年，多国基础设施和重要信息系统遭受网络攻击，引发全球震荡，对国家安全稳定造成巨大风险，引发了全球关于加强关键信息基础设施安全保护的思考。

面对日益复杂严峻的网络安全形势，美国、俄罗斯、欧盟、日本、意大利等重点国家和地区强化网络安全在国家安全中的重要战略地位，不断完善网络安全战略布局，持续完善网络安全政策战略，重视网络安全主动防御，重视网络安全风险管理控制和预警，重点加强供应链安全、关键信息基础设施保护、数据安全、个人信息保护等领域工作，重点建设网络空间安全风险预警体系。

1.2.2 国内发展现状

国内风险预警体系建设还处在初期发展阶段，投入不足，现在主要是通过网络安全服务，靠人工周期性的去完成，效率低，实时性差，应急能力差。

深入分析导致联网信息系统风险严峻的原因，可以发现虽然各个组织都在不断的完善

自己的安全防御体系以此来抵制各种可能发生的威胁事件，但是仅凭借传统的安全防御体系被动防御还不足以保障联网信息系统的安全，还需要完善主动化的风险预警防御体系从而实现对联网信息和资产的保护，防患于未然，以此来实时发现当前防御体系存在的风险，保证风险被不法分子利用前对其进行修补，构建风险预警主动防御系统，只有这样才能提高整体安全保障能力。

目前各医院用户大部分都是请网络安全公司的安服人员做网络安全服务，因专业人力、用户环境和服务成本所限，只能定期做网络安全服务，出了问题只能由专业安服人员解决。这造成了以下突出问题：

◎ 实时性差，遇到安全问题再处理，要立项，从安全公司请安服工程师，安服团队排计划，极有可能耽误用户的很多工作；

◎ 自主性差，有些情况无法实时安服评估，包括新系统上线，网络结构和网络配置改变等。用户需要自己有手段保护自己的网络，对自己的网络安全负责；

◎ 监管漏洞大，对网络实时监控的缺失，在线状态、应用状态和性能等无法全天候掌控；

◎ 效率低，出问题怎么解决，用户自己解决很多情况下是费力解决不了问题；

◎ 疲于应对，用户面对繁杂的网络安全问题，仅靠人力已无法提升网络安全防范能力。

要深入贯彻落实习近平总书记关于网络强国的重要思想，坚持总体国家安全观和正确的网络安全观，贯彻新发展理念，构建网络安全新格局，全面加强网络安全保障体系和能力建设。

加强网络安全风险评估和审查。强化新技术新应用安全评估管理。建立健全关键信息基础设施保护体系，提升安全防护和维护政治安全能力。加强网络安全基础设施建设，加强网络空间安全风险预警系统建设，提高网络安全综合治理能力，强化跨领域网络安全信息共享和工作协同，提升网络安全威胁发现、监测预警、应急指挥、攻击溯源能力。

二、 需求分析

1.3 需求分析

1.3.1 网内有哪些设备与应用，是否有非法设备接入？

网络信息化建设不断完善，基础设备、服务器、网络设备、安全设备不断增多，网络越来越复杂，各类数据信息的获取通常处于被状态，不具备完善的网络基础信息库，无法自动化智能化的统计出网内设备与应用的数量，无法有效识别网内分别都上架了什么样的设备，存在那些应用。面对当前现状，需要采用多样化信息采集方式，主动全面获取网内各类信息，构建全网网络基础信息库。统计各类设备与应用，识别资产与应用的基本信息。

1.3.2 设备与应用开放了哪些端口及服务？

业务不断变化，需求不断变化，网络也不断变化，每个阶段网内设备与应用的状态依据业务及需求不断发生改变，新增了哪些设备，新开了什么端口和服务，设备及应用均处于什么样的运行状态，需要在基础信息库的基础上，不断实时更新覆盖全网网络基础信息库。

1.3.3 如何快速便捷查看网内安全现状与态势？

通过基础信息库的构建，通过各资产基础信息的识别，例如型号、版本、应用、端口、操作系统等，构建网络底图，展现网络空间安全态势。即时了解网内风险分布状况，设备安全运行状况，安全态势状况。

1.3.4 网内存在哪些风险？是否可自行验证利用？

构建了网络基础信息库，了解网内各类设备与应用的基本状况远不够，还需要我们从风险及安全管理的纬度，构建风险预警主动防御体系，更深入了解网内各类资产的安全状况，已存在风险漏洞分布状况及已存在的漏洞是否有效，如何进行自动化智能化的验证。是否有相应的风险验证与利用的技术框架与手段。

1.3.5 如何对网内安全风险进行实时监测？

利用安全风险基线，结合主动监测技术，实现对网内安全风险实时监测。

1.3.6 如何能够基于以上信息进行智能化的风险预警？

化被动为主动，基于以上的信息、数据、漏洞和风险建设风险预警指控系统。

1.4 关键需求指标

1.4.1 网络巡查

1)巡查在线状态：巡查设备、资产的在线状态；

2)巡查应用状态：巡查应用状态，是否可以正常访问；

3)巡查发现风险：巡查发现设备、资产和应用的风险指数，风险信息；

1.4.2 资产发现

1)主动发现联网的 IT 资产：主动发现联网的 IT 资产，并自动与资产登记表进行比对，如果发现是非法资产实时报警；

2)资产与应用识别：识别资产与应用信息，查看是否符合网络安全要求，是否合规；

3)服务指纹识别：识别服务与指纹信息，查看是否符合网络安全要求，是否合规；

1.4.3 场景仿真

1)特殊场景仿真：办公网络、物联网应用、工控网络等的特殊场景或者应用仿真模拟；

2)虚实结合：仿真场景支持虚实结合，可视化实时搭建网络；

3)仿真镜像模板：仿真镜像模板内置工具库，支持安全测评；

1.4.4 风险发现

1)多种工具发现安全风险：集成多种探测与识别工具主动发现网内存在的各种安全风险；

2)在线渗透检测风险：脆弱性、合规性风险在线渗透与检测；

1.4.5 风险验证

1)一键自动化、手动、定期多种方式基于渗透攻击脚本进行风险可利用性验证；

2)内置海量攻击脚本、工具支持在线渗透攻击与验证；

1.4.6 风险报告

1)根据探测与验证结果出具风险评估报告；

2)形成风险基线，定期评估；

1.4.7 异常报警

1)未许可资产报警；

2)巡检异常报警；

3)综合风险发现及评估结果，风险报警。

1.4.8 整改建议

1)未许可资产审查；

2)巡查异常结果处置；

3)安全风险整改建议；

三、 系统建设方案

1.5 系统设计思想

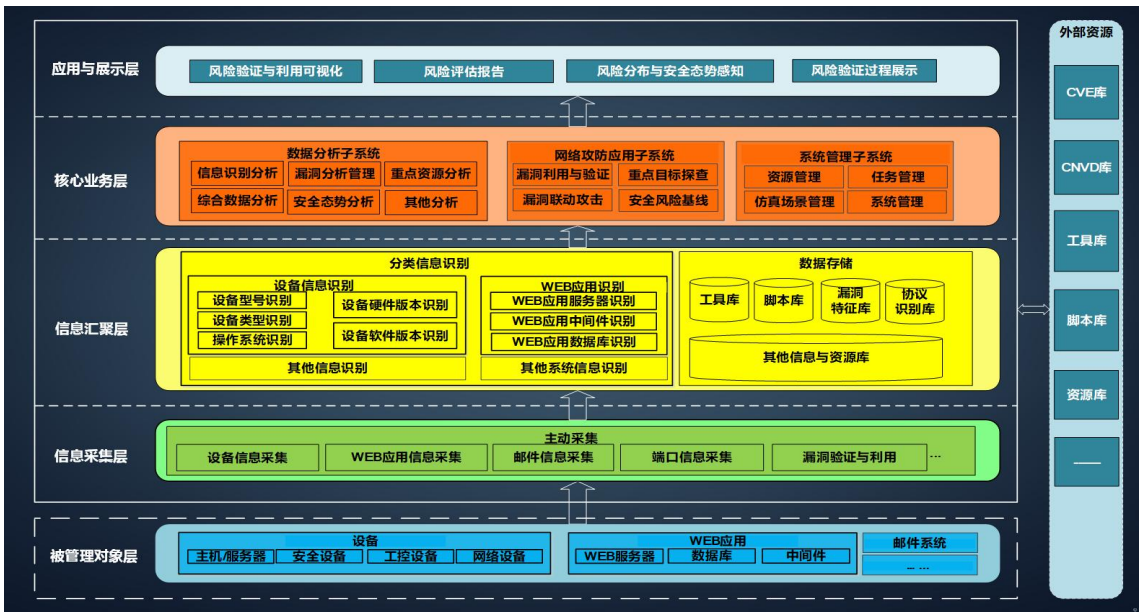
网络空间安全风险预警指控系统基于网络攻防技术融合云计算、大数据、人工智能等技术，将网络安全被动防御模式转变为主动防御模式。以自动化运行方式，完成资产巡检、风险发现、风险识别、渗透验证与风险评估，实现事前主动发现安全风险、主动验证风险可利用性、主动修复风险等，从而构建起网络空间安全风险管控体系。

1.6 系统建设目标

网络空间安全风险预警指控系统以主动防御为目标，基于网络攻防技术融合云计算、大数据、人工智能等技术，将网络安全被动防御模式转变为主动防御模式。

通过网络巡检、资产发现、指纹识别、风险发现、风险验证与风险报告，实现事前主动发现安全风险、主动验证风险、定位风险、处置风险等，从而构建起网络空间安全风险管控体系。

1.7 系统架构设计



网络空间安全风险预警指控系统从功能划分上由 5 个层次组成,包括：

1)被管理对象层

2)信息采集层

3)信息汇聚层

4)核心业务层

5)应用与展示层

此外，系统提供与外部资源和系统进行接口交互，最终实现对中心网络安全防护、网络攻防、网络风险评估业务的支撑。

被管理对象层包括各类主机/服务器、安全设备、网络设备、工控设备、WEB 应用、中间件、数据库、邮件系统和 DNS 系统等，通过在指定网络对这些对象信息的主动探测与收集，形成相关业务支撑的基础数据。

信息采集层包括主要包括设备信息采集、WEB 应用信息采集、邮件系统信息采集、DNS

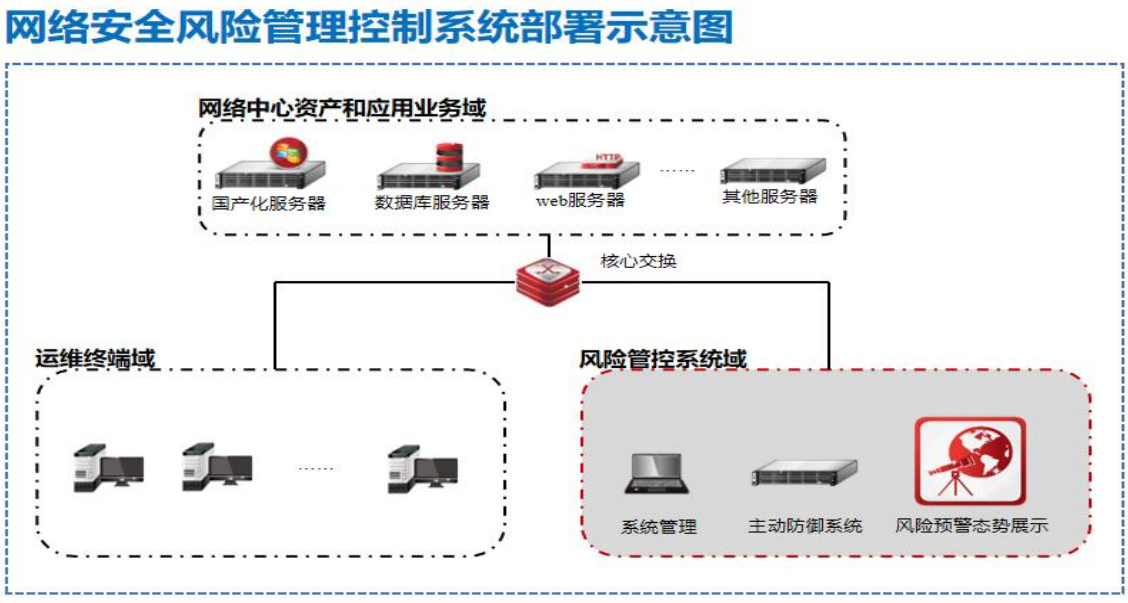
系统信息采集、日志采集、流量采集、风险发现以及风险验证与利用的功能，实现信息主动探测、风险利用与验证的执行层。

信息汇聚层将信息采集层获取的信息进行数据的抽取、转换和加载后，通过分类信息的识别，分别将原始信息和分类信息存储在原始信息库和汇总信息库中，同时提供工具库、脚本库、相关特征库的管理。

核心业务层包括数据分析子系统、网络攻防应用子系统和管理子系统，是系统核心业务的主要承载层。

应用与展示层为用户提供人机交互界面，实现可视化风险验证与利用、风险评估展示等功能。

1.8 系统网络拓扑



1.9 关键技术

1.9.1 基于风险管控的主动防御功能体系

基于资产识别与发现（网络设备、安全设备、终端、服务器等 IT 信息资源），通过漏洞库、脚本库、插件库、与场景模拟等发现风险，通过风险验证与利用评估风险，形成综合

风险报告。

1.9.2 基于渗透攻击脚本库的主动探测技术

系统首先能够实现漏洞探测技术，通过漏洞探测能够发现资产存在的漏洞。对于发现的漏洞，通过渗透攻击脚本，对漏洞进行主动渗透攻击探测，分析出综合的风险指标，该指标可以为用户提供安全运维指导。

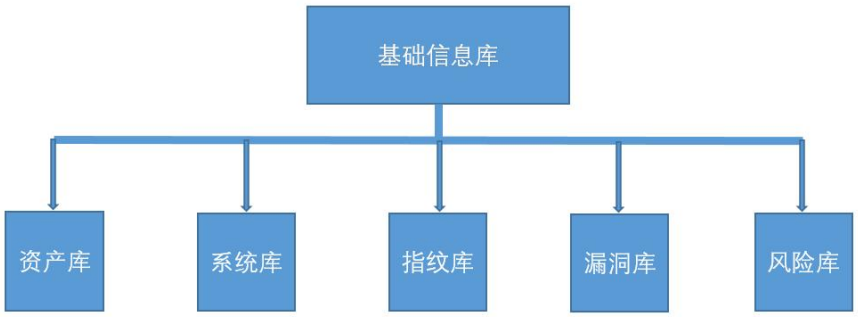
1.9.3 基于网络安全服务的实时监控与探测技术

基于该系统可以对资产进行实时监控，能够及时发现资产在线情况和系统运行状态，支持进行全自动的主动探测和定期探测风险。

四、 主要功能及性能指标

1.10 基础信息库

构建主机/服务器、安全设备、网络设备、工控设备、WEB 应用、中间件、数据库等基础信息识别指纹库，包含：资产库、系统库、指纹库、漏洞库和风险库等。



1.10.1 功能组成

1)设备基础信息识别：主动防御系统内置的探测引擎可以识别设备端口、服务、操作

系统类型；同时也可以识别设备类型、设备厂家等。

2)工控信息识别：主动防御系统通过探知可以识别工控设设备，识别工控协议。同时可以识别工控设备的端口、服务、操作系统等。

3)WEB 应用信息识别：主动防御系统通过指纹库的比对，WEB 应用信息采集引擎可探测 WEB 服务器操作系统版本类型和版本号、WEB 服务器类型和版本号、中间件类型和版本号以及数据库类型和版本号等信息收集和判断。不但可以识别国外应用系统,还可以识别国内应用系统。

4)邮件系统信息识别：主动防御系统通过指纹库的比对，设备信息采集可实现探测邮件服务器软件类型和版本号以及操作系统类型及版本号。主动防御系统不止能够识别国外邮箱,还支持国内邮箱如：盈世 coremail,易邮 eYou Email System 等邮箱的识别。

1.10.2 性能指标

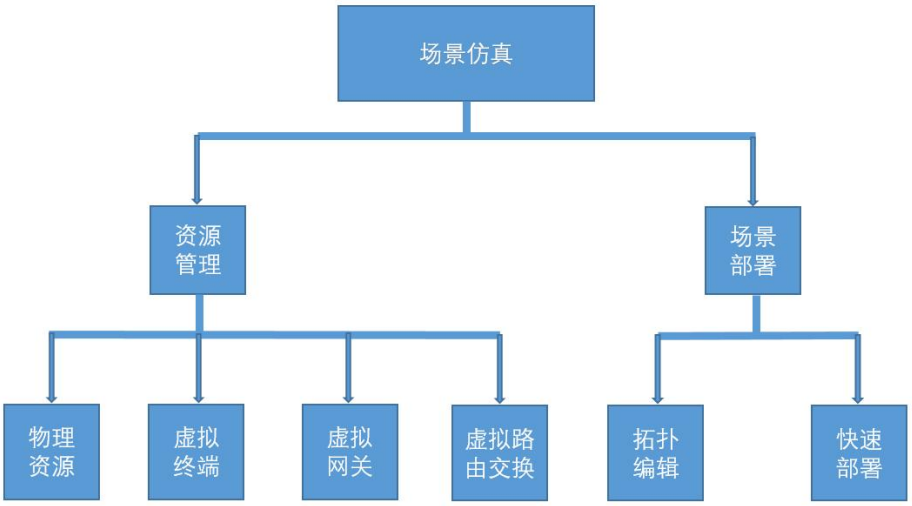
采用多样化探测技术包含：web 漏洞扫描技术、系统漏洞扫描技术、操作系统的探测技术、端口的探测技术、服务探测技术和 Web 爬虫技术等。

1.11 场景仿真

利用虚实结合技术，实现生产网络、工业控制网络、办公环境网络等所需网络环境的 1:1 快速可视化模拟仿真，仿真网络可以边部署边生成，方便实时调整网络结构。

功能组成

场景仿真包含资源管理和场景部署两个模块。



资源管理模块包含：物理资源管理、虚拟终端管理、虚拟网关管理和路由交换管理等。

场景部署模块包含：拓扑编辑和快速部署。

1.11.1 性能指标

场景仿真模块性能指标包含：

1)系统具备强大的虚实结合场景仿真能力；

2)支持界面拖拽方式可视化场景拓扑构建，所见既所得；

3)系统内置丰富镜像资源，同时支持动态调整网络；

4)支持虚拟远程管理：支持虚拟机 VNC 管理；

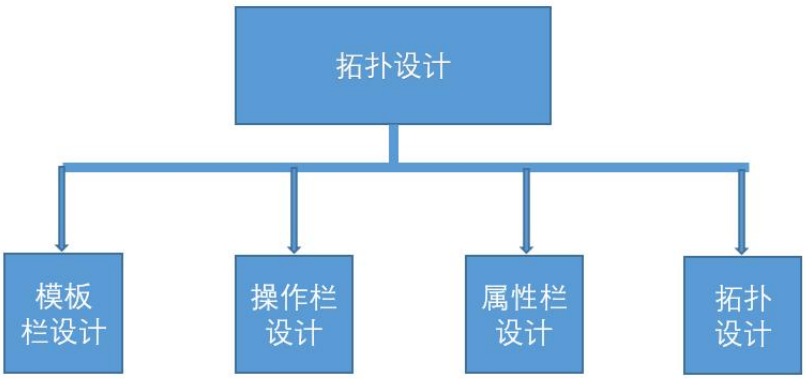
5)支持动态分配 IP：DHCP 动态分配 IP；

6)支持智能链接校验： 网段、端口等智能校验。

1.12 拓扑设计

1.12.1 系统组成

拓扑设计模块主要支持仿真场景的网络拓扑设计，包含模板栏设计、操作栏设计、属性栏设计和拓扑设计等主要功能。



模板栏设计模块主要物理设备栏、虚拟路由交换栏、虚拟网关栏和终端栏；操作栏包含拓扑设计的各种操作；属性栏包含设备属性，支持设置设备属性；拓扑设计支持通过拖拽方式可视化地搭建网络拓扑。

1.12.2 性能指标

支持在浏览器上通过拖拽形式可视化的创建或编辑拓扑，支持鼠标右键菜单功能，支持对虚拟主机进行 ip 配置，支持自动设置 ip，拓扑设计工具栏显示可用的物理资源、虚拟终端模板、虚拟安全设备模板、虚拟路由模板和虚拟交换模板，支持应用系统所有可配置的资源与模板进行拓扑搭建，包括虚拟防火墙，虚拟 IPS，虚拟 VPN，虚拟 UTM，虚拟路由器，虚拟交换机，虚拟主机，以及各种物理设备等；支持对虚拟化防火墙，虚拟化 IPS 和虚拟化 VPN 进行接口设置。

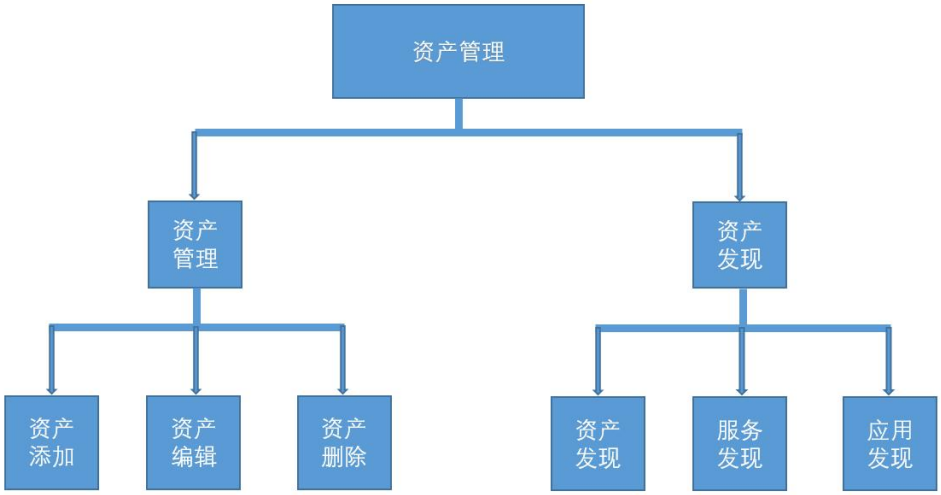
1.13 资产管理

资产管理模块包含主机资源、服务资源和应用资源管理。可以通过信息收集主动发现

主机资源，也可以通过手动方式直接添加已知 IP 地址的主机，并管理发现的服务资源和所有的应用资源。

1.13.1 功能组成

资产管理模块主要包含资产管理和资产发现。



资产管理模块，包含资产添加、资产编辑和资产删除，支持资产导入导出。

资产发现模块，包含资产发现、服务发现和应用发现。

1.13.2 性能指标

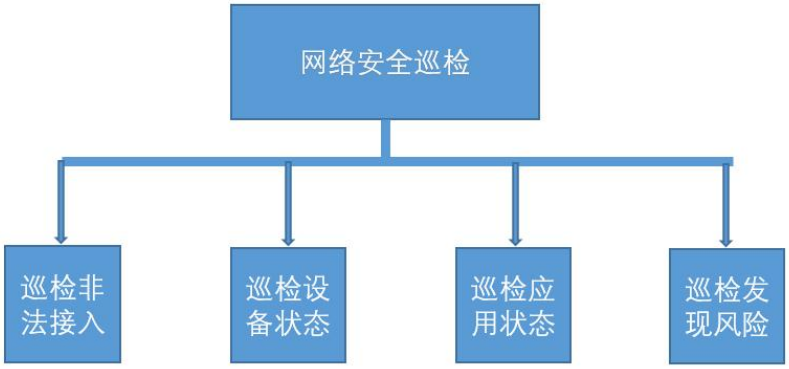
采用多样化技术手段发现资产、服务和应用。

1.14 网络安全巡检

网络安全巡检模块，支持巡检非法接入、巡查在线状态、巡查应用状态、巡查发现风险。

1.14.1 功能组成

网络安全巡检模块，包含巡检非法接入、巡检设备状态、巡检应用状态和巡检发现风险等。



1.14.2 性能指标

支持非法接入设备发现；

设备在线状态巡检；

应用在线状态巡检；

应用异常状态发现；

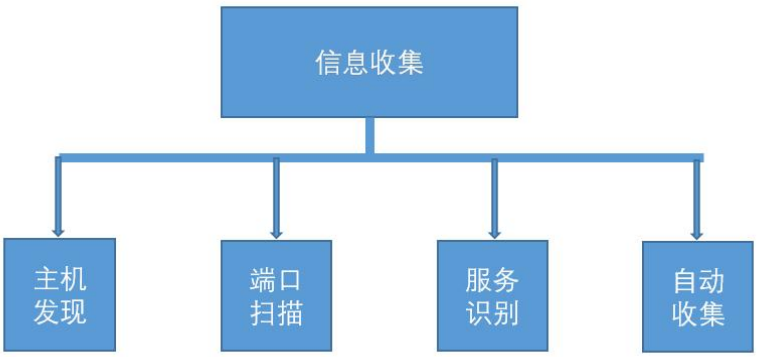
设备和应用风险发现。

1.15 信息收集

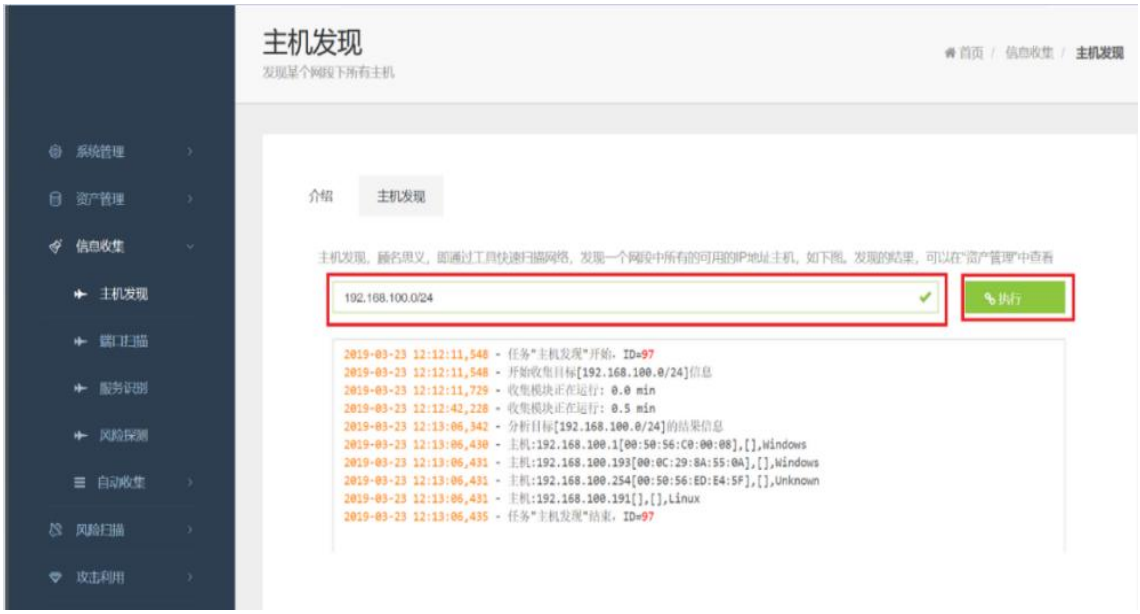
信息收集包含主机发现、端口扫描、服务识别、自动收集四部分，用于收集目标环境的相关基础信息。

1.15.1 功能组成

信息收集模块包含主机发现、端口扫描、服务识别、自动收集四部分。



主机发现模块，能够发现某个网段内所有主机，在输入框中，输入需要查询的网段信息，格式如：192.168.10.0/24，点击执行。



端口扫描模块，能够发现某个主机所有开放的端口。在输入框中，输入需要查询主机的 IP，格式如：192.168.10.110，点击执行。

服务识别模块，能够识别某个端口的应用或服务，以及其版本信息。在输入框中，输入需要查询的 IP 及端口，格式如：192.168.10.110:22，点击执行。

自动收集模块，新建“自动收集”任务，后台自动完成“主机发现”、“端口扫描”、“服务识别”、“漏洞探测”等功能，收集“主机资源”、“服务资源”、“漏洞资源”等相关资产

1.15.2 性能指标

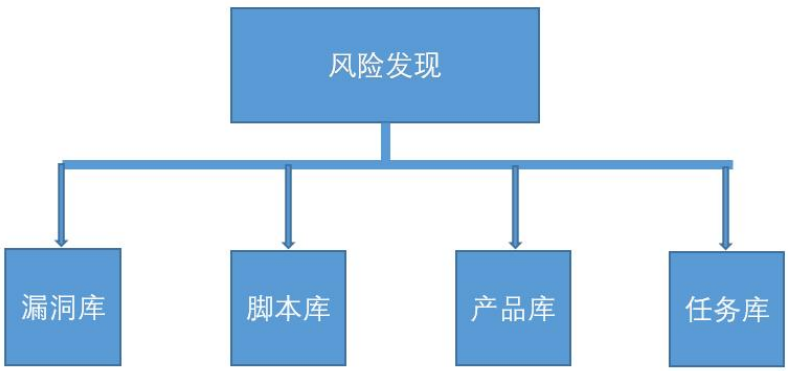
内置多种信息收集工具，能实现信息多维度收集。

1.16 风险发现

实现在指定网络区域内所有联网资产进行安全风险的主动发现。

1.16.1 功能组成

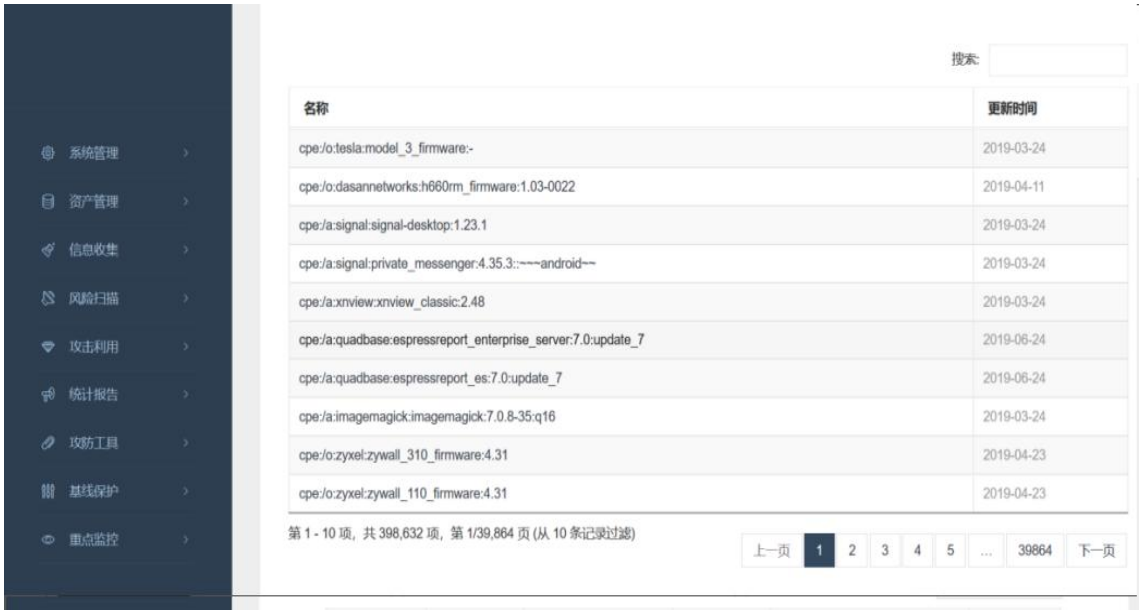
风险发现模块包含：漏洞库、脚本库、特有脚本库、产品库（常见检测插件、CMS 检测插件）和任务库等。



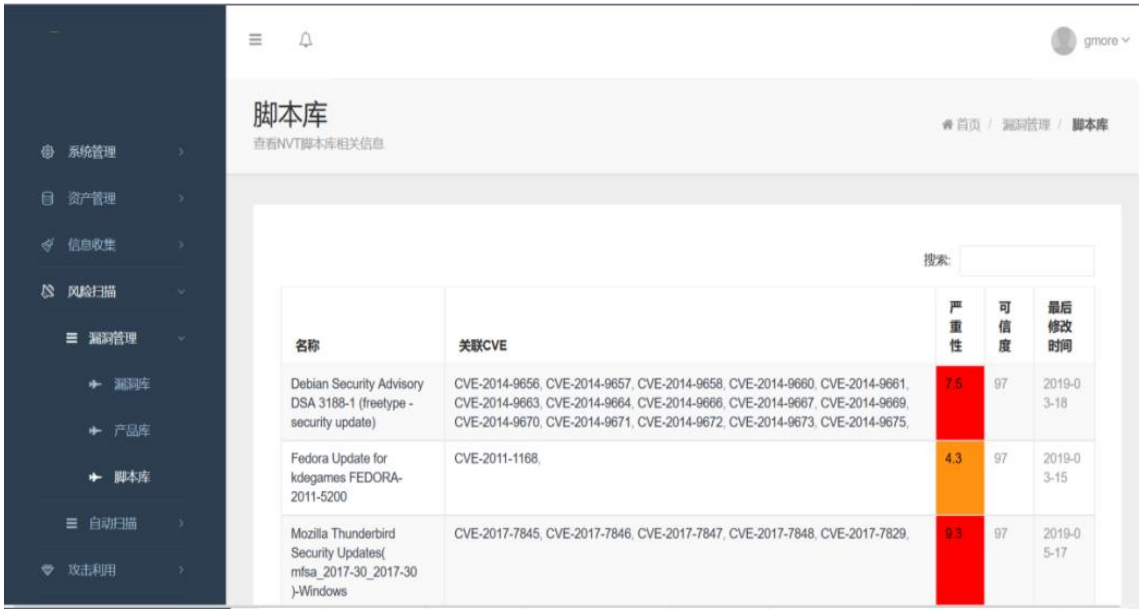
内置漏洞扫描引擎，实现漏洞风险全面扫描。系统采用插件式设计，支持可扩展。

漏洞库：

产品库：



脚本库：



自动扫描：新建“自动扫描”任务，后台自动对系统进行全面的漏洞扫描工作，在扫描任务中查看。

1.16.2 性能指标

内置漏洞库，包含漏洞>11 万个，月度更新；

内置脚本库，包含漏洞检测脚本>48000 个，月度更新；

内置特有脚本库>100，月度更新；

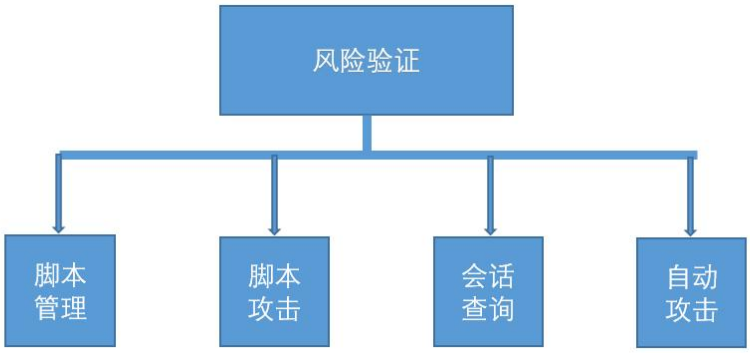
内置常见检测插件>40 个，常见 CMS 检测插件>300 个。

1.17 风险验证与利用

平台自动对目标进行信息收集，根据收集的资产信息，如端口、服务搜索可能存在的漏洞，并检索内置的产品库、漏洞库，智能选择合适的检测和攻击脚本，实现一键式自动化攻击验证。

1.17.1 功能组成

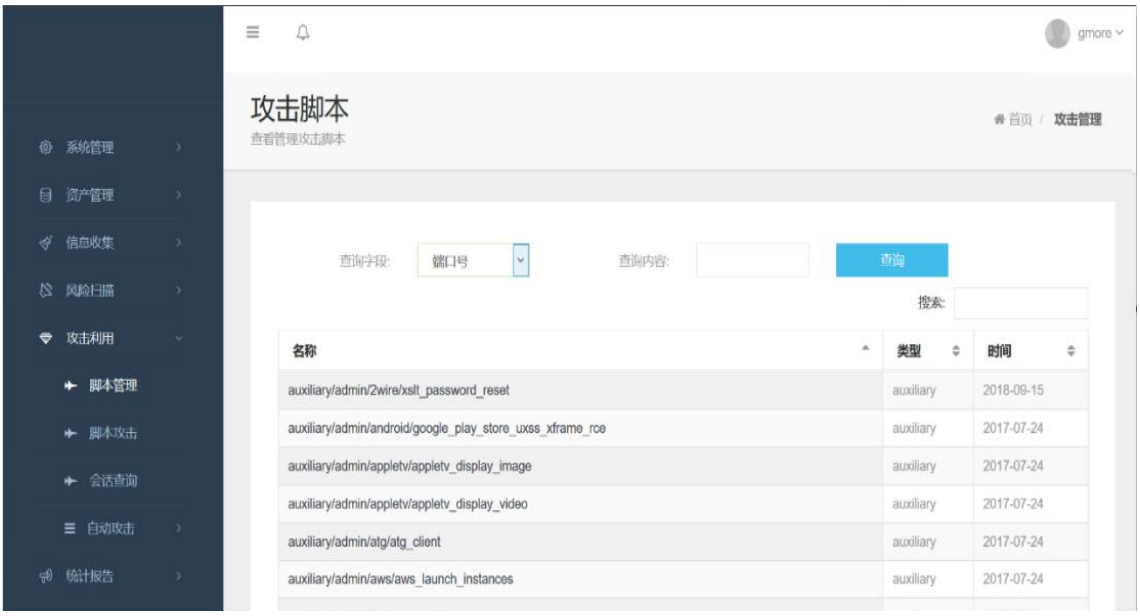
风险验证与利用模块包含：脚本管理、脚本攻击、会话查询和自动攻击等。



系统通过快速风险验证功能提供针对网络节点上发现的漏洞进行验证或发起攻击的能力。快速风险验证能够跟网络节点详细信息展示相关联，查看网络节点详细信息中的漏洞后调出快速风险验证功能，用户配置风险验证相关参数后就能快速进行风险验证或利用，快速风险验证参数设置包括但不限于风险验证、攻击的插件选择、目标网络节点 IP 地址、目标端口、有效载荷代码选择等。

系统支持根据联网资产类型及其安全风险类型自动化选择验证攻击脚本、工具进行自动化的漏洞利用验证。

脚本管理：根据关键字查询相关的攻击脚本



脚本攻击：

会话查询:查看并管理会话。

自动攻击：新建“自动攻击”任务，后台自动将发现的所有漏洞进行尝试进行验证攻击利用。

1.17.2 性能指标

平台内置渗透攻击攻击模块>1800 项。

1.18 风险评估报告

综合风险发现结果，异常状态报警，定位风险，生成风险评估报告，给出加固建议。

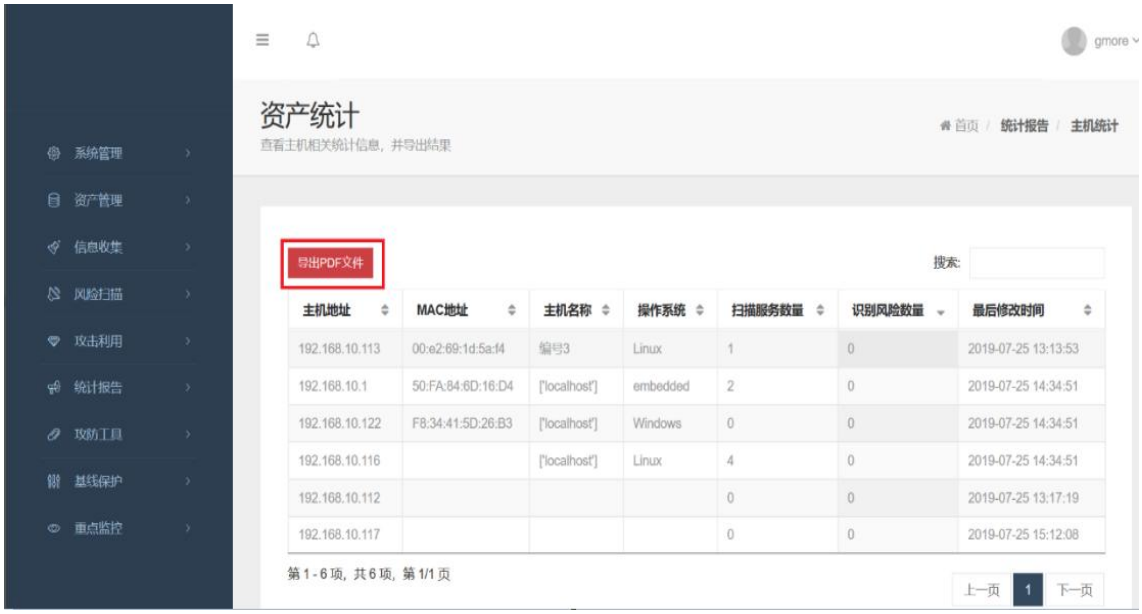
1.18.1 功能组成

风险评估报告模块包含：基础信息报告、总体报告、资产统计报告和风险统计报告等。

基础信息报告：主动防御系统内置的探测引擎可以识别设备端口、服务、操作系统类型；同时也可以识别设备类型、设备厂家等。

总体报告：

资产统计报告：



通过资产统计还可以导出主机相关信息。

风险统计报告：查看风险相关统计信息，并导出结果。

1.18.2 性能指标

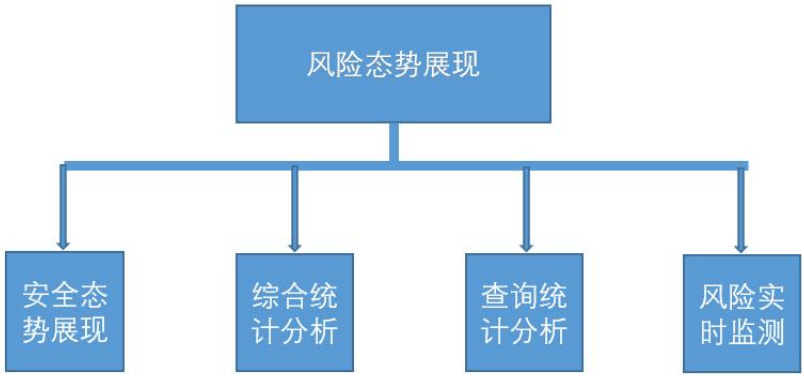
能够支持基础信息统计信息、资产统计信息和风险评估结果导出。

1.19 风险态势展现

将多维度的网络安全风险态势通过大屏展现出来，方便全方位了解系统风险。

1.19.1 功能组成

安全态势展现包含：安全态势展现、综合统计分析、查询统计分析和风险实时监测。



1)安全态势展现：将网络安全风险数据按各种场景分析之后提供多维度态势展示，并支持安全风险态势的大屏展示设置和展示信息筛选过滤设置。态势分析维度包括：全网态势、资产态势、风险态势、攻击态势，态势大屏中相关信息可以下钻跳转到对应的详细页面。

2)综合统计分析：综合统计分析功能能够通过图、表、地图等多种相结合的展现方式将探测结果进行统计分析后按照特定组合进行展示，供用户直观了解网络探测结果。综合统计分析的内容类型包括但不限于操作系统类型、设备类型、服务类型、web 服务器类型、应用类型等分布情况，包含高危端口网络节点分布情况，包含高危漏洞网络节点分布情况等。

3)查询统计分析：查询统计分析的内容类型包括但不限于 web 网站名称类、web 服务器类、操作系统类、设备类型类、数据库类、端口类、服务类、常见端口、漏洞级别类、组件类型类等。

4)风险实时监测：形成安全风险基线，实现对给定网络、指定资产进行给予安全基线的实时安全风险监测。

1.19.2 性能指标

采用多维度分析，全方位展现网络安全风险态势。

五、 重大价值

1.20 主动风险预警

采用多样化的手段，进行风险评估，主动发现风险，预警风险，实时提供风险评估报告，整改建议，优化网络风险防御策略，及时提升风险防御能力。

1.21 实时安全巡检

实时进行安全巡检，保障系统稳定运行，统筹规划风险基线保护，优化网络风险防御策略，及时提升风险防御能力。

1.22 管控非法接入

智慧监控网络资产状况，制度化建立网络资产清单，自动识别非法接入资产，自动预警非法资产接入。

1.23 智能风险验证

智能探知网络风险，海量的漏洞库、脚本库，自动化攻击验证与利用，攻击验证脚本基于插件式设计，扩展性好。

1.24 自主把控风险

降低安服专业技术难度，自主管理基线保护任务，科学规划人力物力，将复杂的工作，松散的工具和人力结合到一起，体系化，有效提升用户自主的风险把控能力。

1.25 提升防御能力

不同于传统的安全防护设备和基于被动防御的态势感知系统，安全风险预警指控系统能够主动发现风险、验证风险、监控风险，有效提升用户自主的风险把控能力和防御能力。

1.26 专网设备安全

网络空间安全风险预警指控系统从主动防御出发，在加强专网专用设备安全方面有重要作用，能有效提升用户自主的风险管控能力，保障专网专用设备的安全。