融讯光通
RONG XUN GUANG TONG

# 网络安全风险预警防御系统建设方案（能源电力）

北京融讯光通科技有限公司

2023 年 12 月

# 目　录

# 第 1 章　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。

习近平主席强调，没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障。要树立正确的网络安全观，加强信息基础设施网络安全防护，加强网络安全信息统筹机制、手段、平台建设，加强网络安全事件应急指挥能力建设，积极发展网络安全产业，做到关口前移，防患于未然。要落实关键信息基础设施防护责任，行业、企业作为关键信息基础设施运营者承担主体防护责任，主管部门履行好监管责任。要依法严厉打击网络黑客、电信网络诈骗、侵犯公民个人隐私等违法犯罪行为，切断网络犯罪利益链条，持续形成高压态势，维护人民群众合法权益。要深入开展网络安全知识技能宣传普及，提高广大人民群众网络安全意识和防护技能。

在中美贸易战、俄乌冲突、欧洲能源危机等复杂国际冲突背景下，全球黑客活动十分活跃，网络安全事件呈“爆发式”增长趋势。关键基础设施、核能航天能源等重点行业、政府机构等成为网络攻击的重点目标。作为重要行业领域，能源企业也遭受了大量网络攻击：2022 年 2 月美国科罗拉多能源公司遭内部 90%数据删除且难以恢复；2022 年 3 月 10 日，原油公司 Rosneft 遭遇 20TB 商业数据泄露，给公司运营及国家安全带来巨大隐患；2022 年 4 月 19 日天然气公司 Gazregion200G 邮件泄露，造成大量敏感数据被免费下载；2022 年以来国内能源企业也遭遇多起勒索病毒、DDoS 攻击、数据被盗取攻击事件.黑客除了使用 DDoS 攻击、钓鱼欺诈、漏洞利用、供应链攻击、恶意数据泄露擦除等攻击技术外，还采用大数据情报收集、关键基础设施漏洞扫描、星链技术应用等手段，给网络攻击带来新的思路和不确定性。

国内大型能源企业业务繁多，结构复杂，覆盖油气生产、炼化、销售等上中下游各个环节外，与社会各领域也多有网络和数据交互。随着业务的发展需求，能源企业内部网络也在逐步扩大，逐步建立了生产网、办公网、数据网、卫星网、保密网等多种类型的内网，范围覆盖国内多个区域，并延伸至国际网络。能源企业内网中信息基础设施规模十分庞大，企业信息系统多样且分散分布，互联网出口多，网络多区多管、复杂多变。随着信息基础设施数字化智能化的发展趋势，云计算应用平台、大数据应用平台等日益成为主流，动辄几千台的主机运维数量，给网络安全的科学化运维与精准化管控等提出了新挑战。在复杂网络安全威胁态势下，能源企业网络安全面对的攻防对抗从互联网侧移至内网侧.如何发现能源内网中存在的安全风险、如何阻断攻击行为、如何开展有效的安全防御措施等是迫切需要解决的问题。

## 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。

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。


WannaCry 勒索攻击全球爆发

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。

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。

在 2017 年 7 月份，美国最大的无线通信公司 Verizon 遭遇了一次大规模的数据泄露事件，由于使用了第三方 NICE Systems，导致超过 1.4 亿的美国用户个人信息暴露在网上。据悉，被暴露的信息中包含众多敏感信息，包括用户姓名、电话号码、账户 PIN 码(个人识别码)。


1.4 亿 Verizon 用户数据泄露

不管是黑客还是普通的用户，只要拥有这些信息就可以登录用户账户了，即便有双因素认证保护也无济于事。显然，该事件警告了所有企业，不是任何第三方公司都能成为你的合作伙伴，自己客户的资料并不应该交由第三方公司来处理。

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。

### 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。

**内网高级可持续性攻击防护能力普遍不足：**相较于互联网出口的集中防御，如入侵检测、态势感知、动态防御措施等一应俱全，能源企业内网往往没有部署同等安全防护级别的技术措施，仅在重要网络和数据节点如区域网络中心、数据中心部署了安全防护设备。

高级可持续性攻击包括多种多样的攻击手法，如 0day 攻击、规则绕过攻击、权限利用攻击、组建僵尸网络等。攻击者在取得一些主机权限后，首先就会利用主机中的权限尽可能

获得更多主机控制权，包括不能访问互联网的主机，攻击者往往会给其植入木马或者后门，进而维持住内网的主机控制权.这些木马后门往往较为隐蔽和难以发现，受害者发现异常关机后再次开机，主机还是被继续控制。上述这些情况需要安全防护人员对相关攻击方式有深入的了解，同时需要有极强的网络安全数据分析技术能力，这给内网安全防护人员带来极大的挑战。

**内网协同防御能力普遍缺失：**能源企业由于专业分公司、分支机构众多，内网范围往往非常大。在各分公司、分支机构之间，由于均处于企业内网中，一般相互之间网络安全防护措施较为缺乏或者开启的防护策略较粗。

在近年来攻防演习中，基于问题的改进措施使得各企业的网络安全信息体系得以提升，企业在其局域网中逐渐部署了一定的安全防护措施，包括防火墙、入侵检测系统、流量分析等，局域网与局域网之间、局域网与生产网之间有了一定的网络隔离措施。在实战检验中发现还是有横向渗透攻击行为存在，企业内网安全防护隔离措施并没有阻止所有的攻击行为。尤其是在取得区域一些主机的权限后，可以通过合法的访问路径绕过安全设备的检测；或者取得内网中某些设备的控制器，进而修改这些安全策略，放行其攻击流量，使内网中的安全防护设备成为“摆设”。

**内网僵尸网络难以根除：**近年来能源企业已经完成企业互联网出口收敛，对公网发布信息系统资产的梳理掌控和安全防护能力都有所提升，如 ZoomEye,FOFA 等网络空间探测系统暴露的资产，其网络安全攻防对抗已经具备很强能力，普通攻击者很难成功或者需要付出很大代价。这些目标已经不是攻击者的主要目标，攻击者在拿到“跳板机”后，往往在企业互联网出口系统上不会有太多额外动作。

实际工作中发现，当企业资产达到一定数量和运维年限后，僵尸信息资产的出现基本是必然的.这里指的僵尸信息资产包括常年无人值守的信息系统、智能终端、大数据平台、老旧服务器、工作站、交换机等，仅进行简单值守的服务器和信息系统也属于僵尸信息资产的范畴，这类资产存在无人管理、无人运维、仅保障存活等特点。与传统意义上的理解不同，智能终端、打印机、摄像头在今年攻防演习中，都有可能被利用发起攻击或者传输攻击。

**对社会工程学攻击缺乏防御手段：**在网络安全事件不断增多、国家各级网络安全演习、企业自身网络安全建设等不断推动下，各单位企业对内网互联网出口的防御已经日臻完善，通过常规攻击手段很难突破。

如今社会工程学攻击被广泛应用至实际网络攻击中。网络钓鱼、水坑攻击、鱼叉攻击等结合供应链、服务商等的社会工程学攻击技术普遍应用；在实际攻击中，形成了信息收集、技战法研究、载荷制作、载荷投递、端点维护、内网渗透等完整的攻击链。攻击往往能够击中企业网络安全防御的最薄弱点，攻击发起点即在企业内网，并且是受信任的主机、服务器，往往还会具有系统管理员的权限，具有自由的网络通路等，从这些地方发起攻击，目前的网络安全防御手段绝大部分都会失效。

**大数据、云计算平台安全防护薄弱：**随着大数据、云计算、物联网和移动计算等新型技术在能源企业的广泛应用，能源领域的信息业务正在逐步向内部私有云、混合云、基于大数据的业务平台和数据平台等迁移，各能源工控物联网平台也越来越多地建设，并投入实际生产。

各类平台部署后，其使用的技术复杂、组件众多、维护需要的专业技术和能力高，导致相关业务常会外包，管理和运维中产生的安全问题突出。

- 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。


- 58 同城的全国简历数据泄露

2017 年 3 月记者发现有淘宝电商出售“58 同城简历数据”，经记者探访和网络安全机构的研究，发现 58 同城存在多个安全技术漏洞的组合，导致黑客通过系统漏洞，利用爬虫工具，获取大量 58 同城简历数据


## 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。

目前大部分企业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。

# 第 2 章　需求分析

## 2.1　需求分析

### 2.1.1　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。

### 2.1.2　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。

### 2.1.3　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。

### 2.1.4　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。

### 2.1.5 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。

### 2.1.6 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防御系统。

## 2.2 关键需求指标

### 2.2.1 网络安全巡查

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；

### 2.2.2 资产发现与识别

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；

### 2.2.3 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；

### 2.2.4 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；

### 2.2.5 风险验证与利用

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；

### 2.2.6 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；

### 2.2.7 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。

### 2.2.8 风险整改建议

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；

### 2.2.9 集群部署

1)节点网络可达即可部署，支持旁路接入；

2)支持集群化部署；

3)支持节点联动；

### 2.2.10 三级网络

1)一级网络：包含一级指控系统、风险预警态势展现系统和一级风控预警节点集群网络；

2)二级网络：包含二级管控系统、风险预警管理中心和二级风控预警节点集群网络；

3)三级网络：包含三级风控预警节点集群网络；

# 第 3 章　系统建设方案

## 3.1　系统整体设计思想

网络空间安全风险预警防御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预警体系。

## 3.2　建设目标、规模与内容

### 3.2.1　建设目标

网络空间安全风险预警防御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、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、定位风险、评估风险等，从而构建起网络空间安全风险预警体系。

### 3.2.2　建设规模

网络空间安全风险预警防御系统包含三级网络，一级集群（部级）网络，二级集群（省级）网络和三级风控预警节点集群（地市级）网络。

### 3.2.3　建设内容

网络空间安全风险预警防御系统包含三级平台：

1)一级平台由一级指控系统、风险预警态势展示系统和风险预警节点集群等组成；

2)二级平台由二级管控系统、风险展示系统和风险预警节点集群等组成；

3)三级平台由节点风险预警管理系统，风险预警节点集群等组成。

网络空间安全风险预警防御系统以主动防御为目标，实现事前主动发现安全风险、主动验证风险、定位风险、评估风险等目的，构建网络空间安全风险预警体系，包含：

1)基础信息库（包含漏洞库、脚本库，插件库等）；

2)资产资源库（能够发现和识别资产，包含端口、服务、系统、中间件、web 服务器等）；

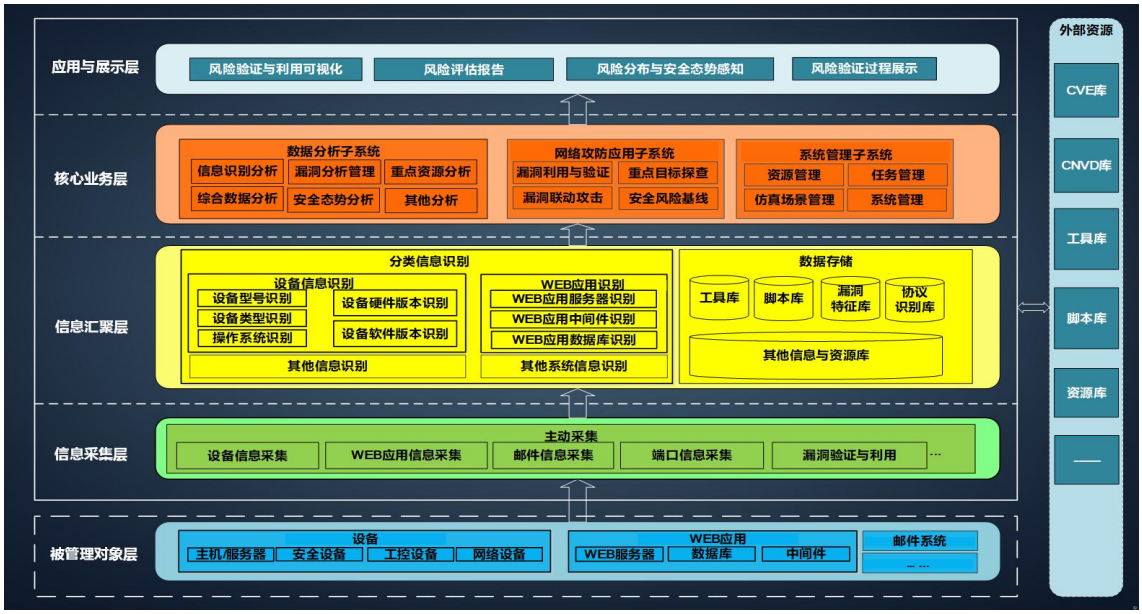
3)资产巡检（包含资产巡检、应用状态巡检、异常和风险巡检等），场景模拟（包含虚实结合、可视化实时组网等）；

4)风险发现（基于扫描引擎通过漏洞库、脚本库，插件库发现风险）；

5)风险验证与利用（自动化验证风险等级，对风险进行评定）；

6)综合风险报告和整改建议等组成。

## 3.3 系统整体架构设计




网络空间安全风险预警防御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。

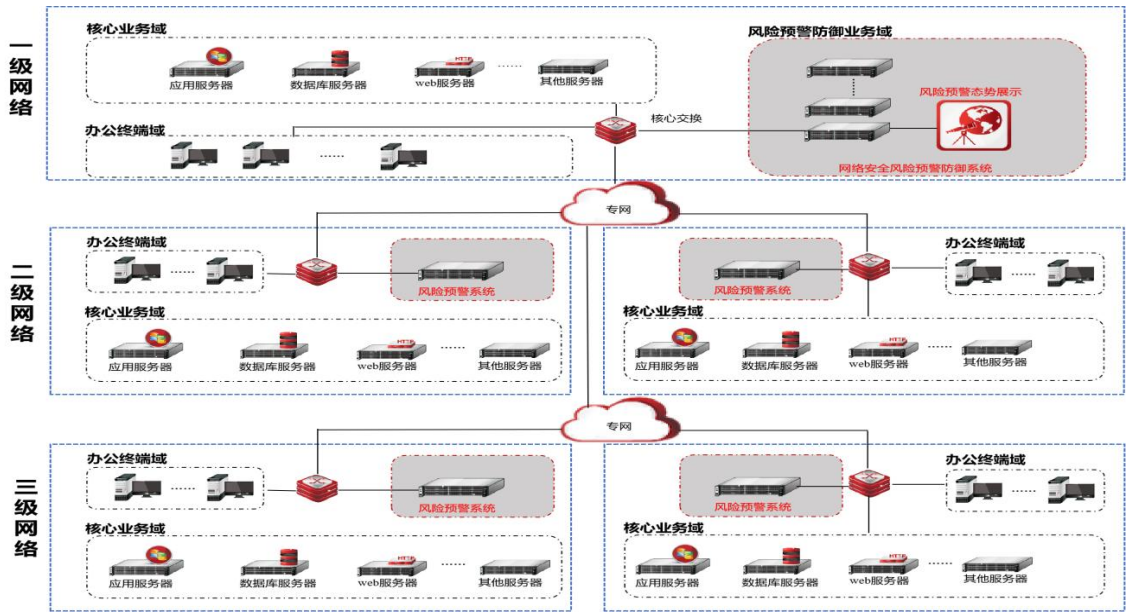
信息采集层包括主要包括设备信息采集、WEB 应用信息采集、邮件系统信息采集、DNS 系统信息采集、风险发现以及风险验证与利用的功能，实现信息主动探测、风险利用与验证的执行层。

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。

## 3.4 系统网络拓扑架构




网络空间安全风险预警防御系统支持旁路接入，网络可达即可。

1)一级部署:包含一级指控系统、风险预警态势展现系统和一级风控预警节点集群网络;

2)二级部署：包含二级级管控系统、风险态势展现系统和二级风控预警节点集群网络;

3)三级部署：包含三级风控预警节点集群网络;

风险态势展示：分为一级综合网络空间安全风险预警态势展示和二级综合预警风险态势展示。

## 3.5 关键技术

### 3.5.1 基于风险预警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。

### 3.5.2 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。

### 3.5.3 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。

### 3.5.4 全方位集中管控

集中管控可实现对基础信息库的统一管理能力，极大方便了安全运营处置工作和安全风险预警工作，提升了网络安全主动防御能力。

### 3.5.5 大数据计算架构

支持分布式集群部署；支持通过扩展集群节点增加计算性能；支持对大量数据流实时处理；支持基于内存计算机制；支持转换和执行两大类算子；支持基于缓存和检查点的分布式计算机制。

### 3.5.6 融合多种大数据技术的分析引擎

系统提供基于大数据分析技术的分析引擎，融合了包括 MapReduce、流式计算引擎、流式计算引擎、流处理框架等多种大数据分布式计算技术，支持批量式和流式数据分析处理。

### 3.5.7 简易式分析能力扩展

当系统默认提供的分析能力无法满足个性要求时，系统能够提供相关接口可扩展新的分析能力。

### 3.5.8 多维态势支撑决策

多维网络空间安全风险预警态势对组织机构的安全数据按各种场景分析之后提供多维度态势展示，并支持安全态势的大屏展示。态势分析维度包括全网态势、资产态势、漏洞态势，风险态势、辅助决策者做到态势全局掌控，进而提升风险预警能力，提升网络安全主动防御能力。

# 第 4 章　主要功能及性能指标

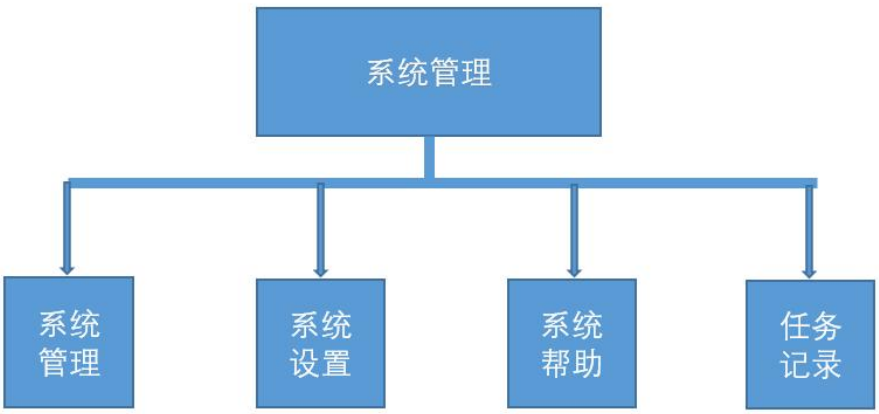
## 4.1　基础平台软件

基础平台软件包含系统管理模块、系统插件框架软件，计算中心支持负载均衡。

### 4.1.1　功能组成

基础平台软件包含系统管理模块、系统插件框架软件。

系统管理模块包含系统首页、系统设置、系统帮助和任务记录等。




### 4.1.2　性能指标

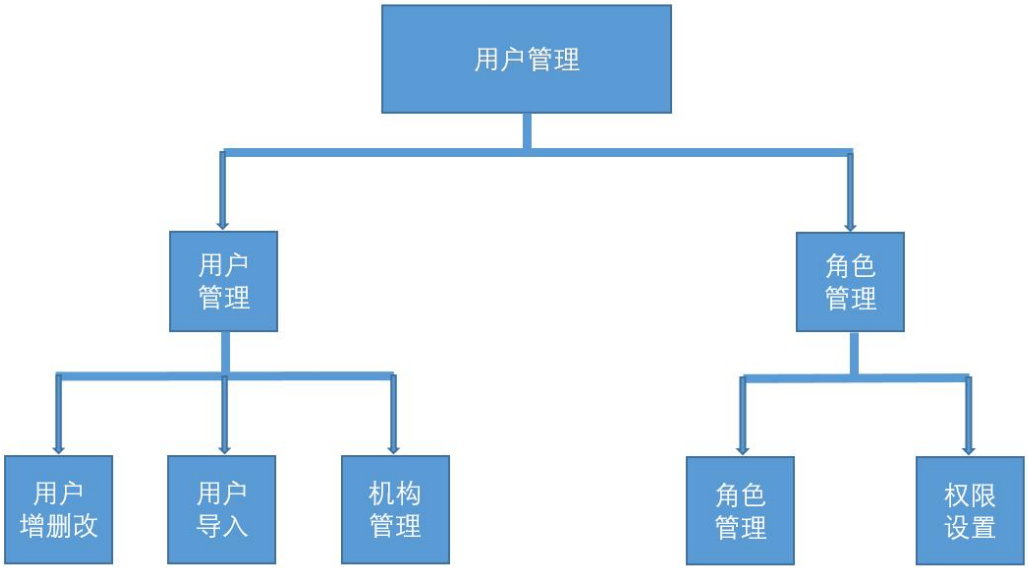
系统管理模块展示 CPU 利用率、内存利用率、创建任务数量、发现主机数量、扫描服务数量和识别风险数量等。

## 4.2　用户管理

用户管理模块包含：用户管理、角色管理。

### 4.2.1　功能组成

用户管理模块：包含用户管理、角色管理。




#### 4.2.2 性能指标

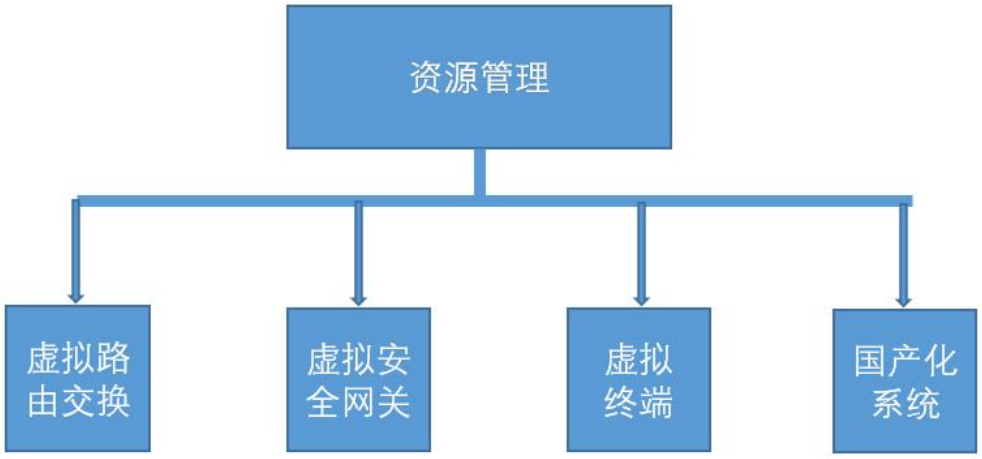
支持用户角色权限设置。

### 4.3 资源管理

资源管理模块：包含虚拟交换路由，虚拟网关、虚拟终端和国产化系统等。

#### 4.3.1 功能组成

资源管理模块：包含虚拟交换路由，虚拟网关、虚拟终端和国产化系统等。

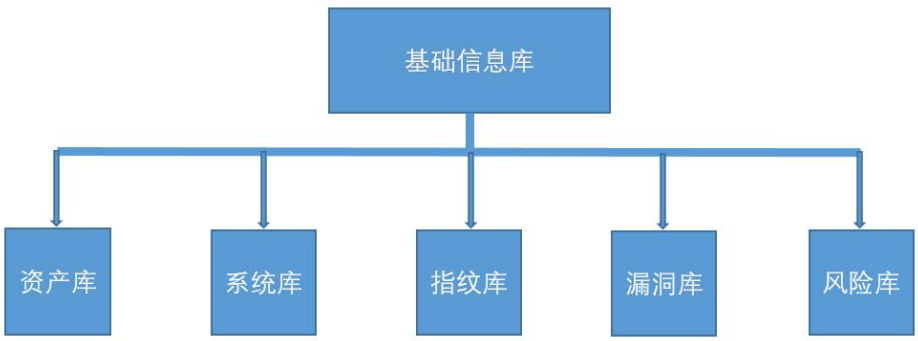



### 4.3.2 性能指标

支持镜像模板自定义。

## 4.4 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。




### 4.4.1 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。

### 4.4.2 性能指标

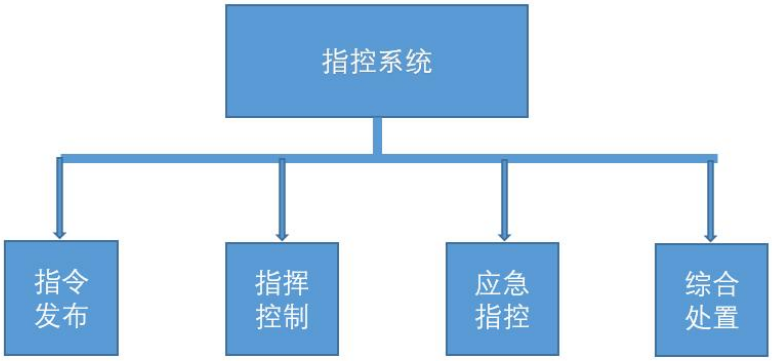
采用多样化探测技术包含：web 漏洞扫描技术、系统漏洞扫描技术、操作系统的探测技术、端口的探测技术、服务探测技术和 Web 爬虫技术等。

## 4.5 指控系统

指控系统作为网络空间安全风险预警系统的大脑，具备综合风险处置能力，指令发布能力，对某一节点或某级节点指控能力和应急指控能力。

### 4.5.1 功能组成

指控系统模块包含：指令发布、指挥控制、应急指控和综合预警处置等。




### 4.5.2 性能指标

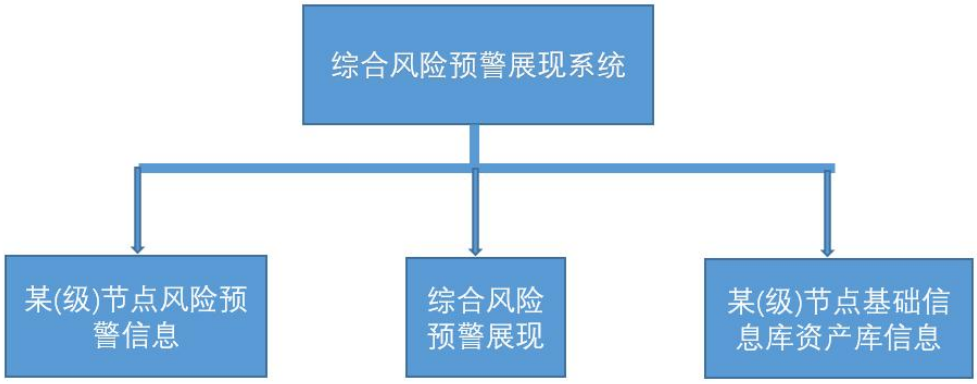
指控系统能够支持向下级节点发出指令、查看下级节点风险态势状况指挥控制；应急指控和进行综合网络空间安全风险预警处置。

## 4.6 综合风险预警展现系统

展现全网综合风险态势，展现某级节点综合风险态势，展现某节点综合风险态势。

### 4.6.1 功能组成

综合风险预警展现模块包含：展现综合风险预警信息、展现某节点风险预警信息、展现某节点基础信息库资产库信息、展现某级节点风险预警信息、展现某级节点基础信息库资产库信息。




### 4.6.2 性能指标

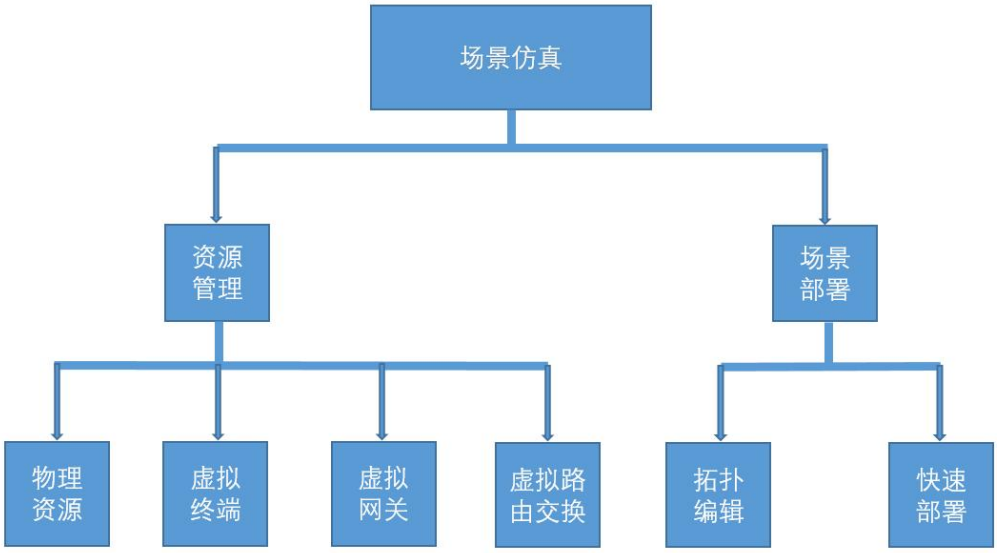
展现综合预警信息，支持某级节点或某节点的预警信息查询。

## 4.7 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。

### 4.7.1 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。

### 4.7.2 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；

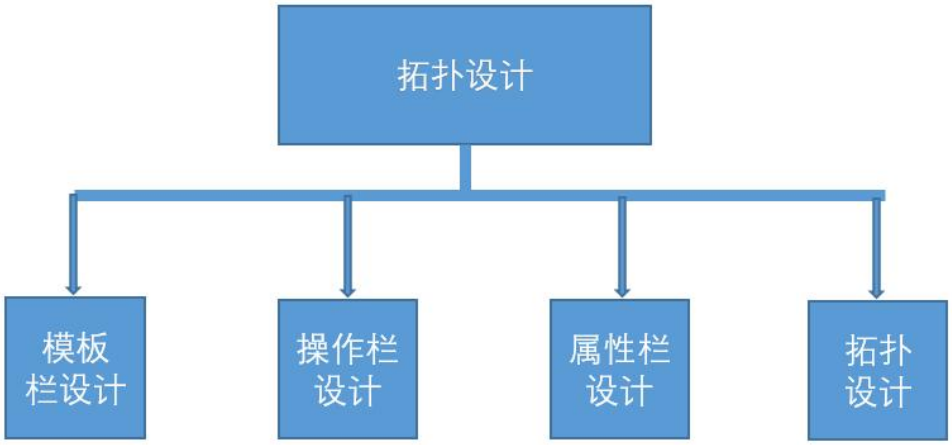
5)支持动态分配 IP：DHCP 动态分配 IP；

6)支持智能链接校验： 网段、端口等智能校验。

## 4.8 拓扑设计

### 4.8.1 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。

### 4.8.2 性能指标

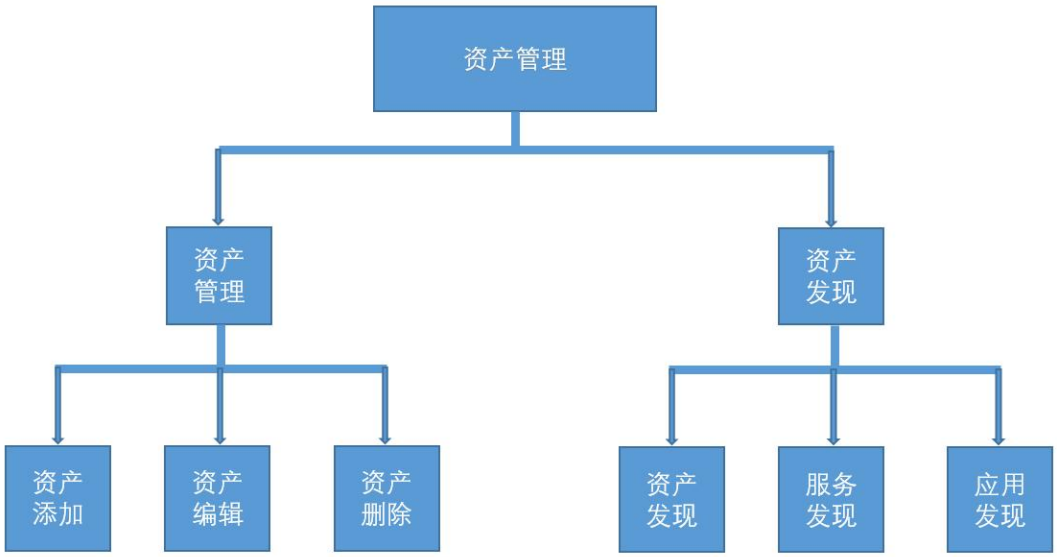
支持在浏览器上通过拖拽形式可视化的创建或编辑拓扑，支持鼠标右键菜单功能，支持对虚拟主机进行 ip 配置，支持自动设置 ip，拓扑设计工具栏显示可用的物理资源、虚拟终端模板、虚拟安全设备模板、虚拟路由模板和虚拟交换模板，支持应用系统所有可配置的资源与模板进行拓扑搭建，包括虚拟防火墙，虚拟 IPS，虚拟 VPN，虚拟 UTM，虚拟路由器，虚拟交换机，虚拟主机，以及各种物理设备等；支持对虚拟化防火墙，虚拟化 IPS 和虚拟化 VPN 进行接口设置。

## 4.9 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。

### 4.9.1 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。

### 4.9.2 性能指标

采用多样化技术手段发现资产、服务和应用。

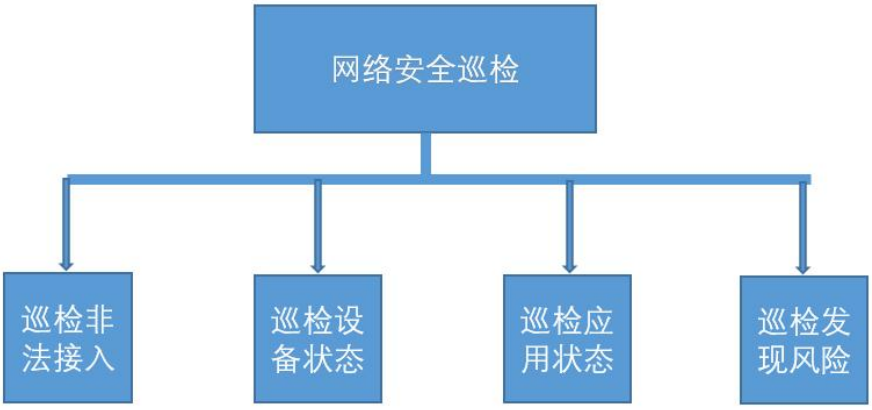
## 4.10 网络安全巡检

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。

### 4.10.1 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。




### 4.10.2 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；

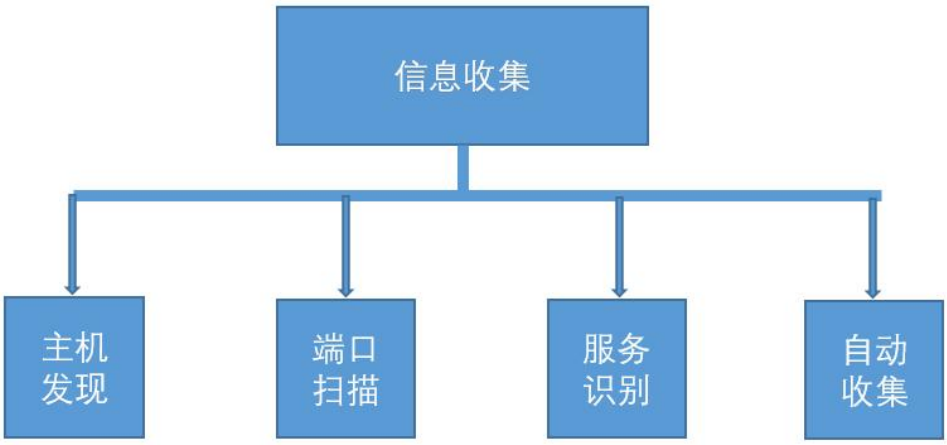
设备和应用风险发现。

## 4.11 信息收集

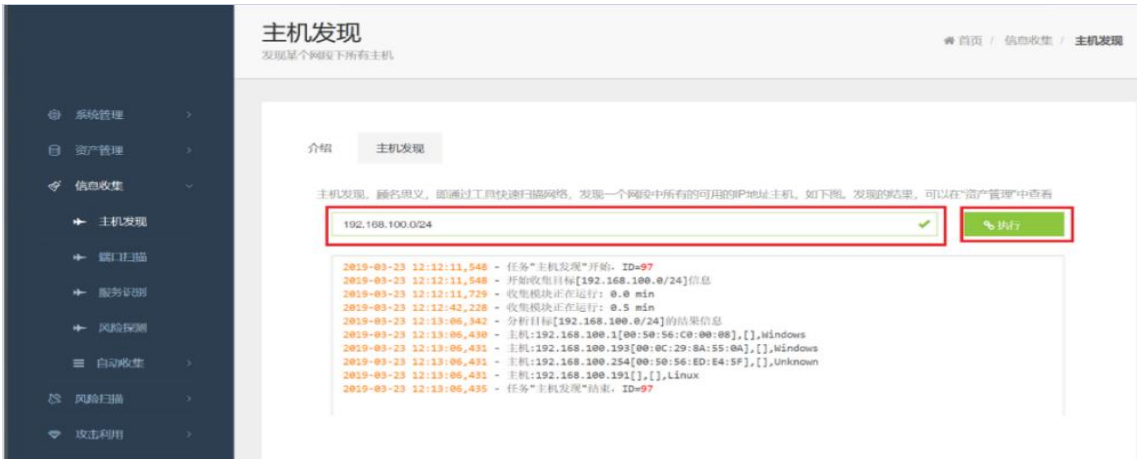
信息收集包含主机发现、端口扫描、服务识别、自动收集四部分，用于收集目标环境的相关基础信息。

### 4.11.1 功能组成

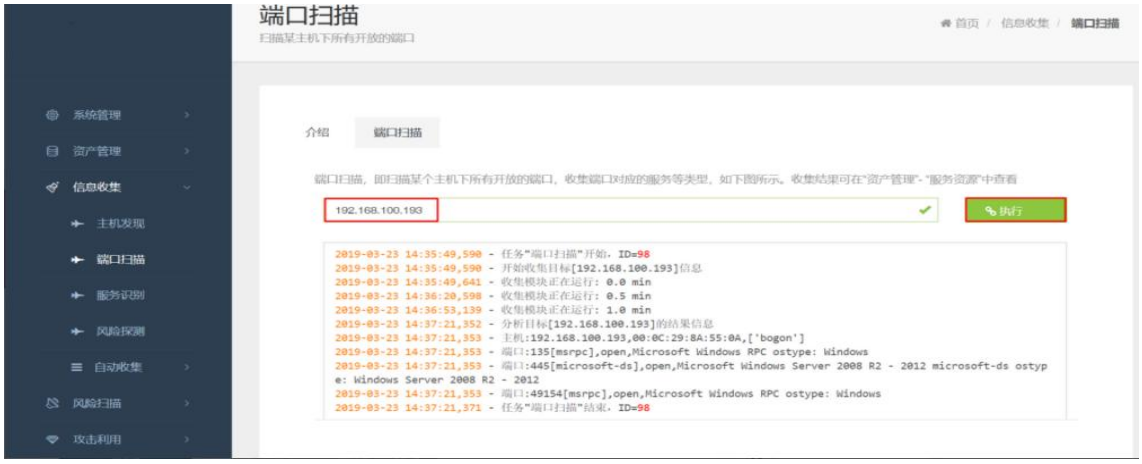
信息收集模块包含主机发现、端口扫描、服务识别、自动收集四部分。




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


### 4.11.2 性能指标

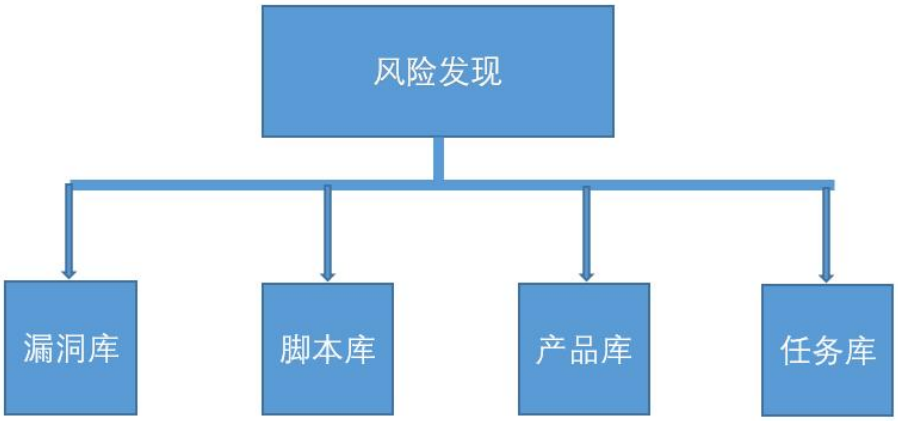
内置多种信息收集工具，能实现信息多维度收集。

## 4.12 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。

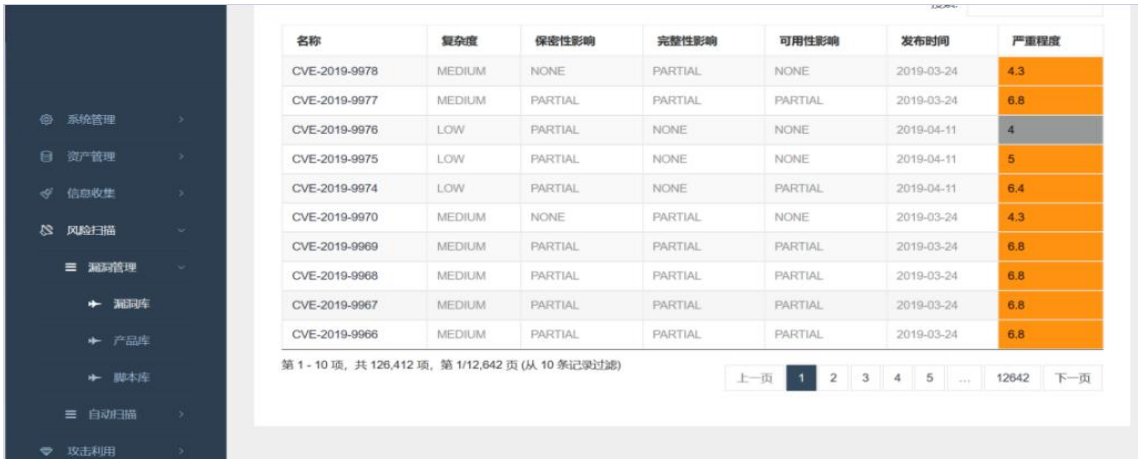
### 4.12.1 功能组成

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。

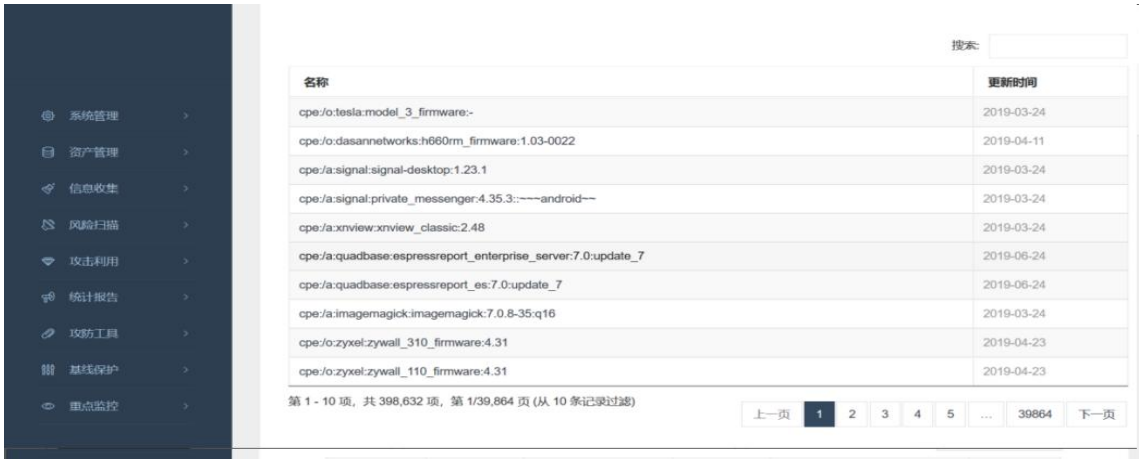



内置漏洞扫描引擎，实现漏洞风险全面扫描。系统采用插件式设计，支持可扩展。

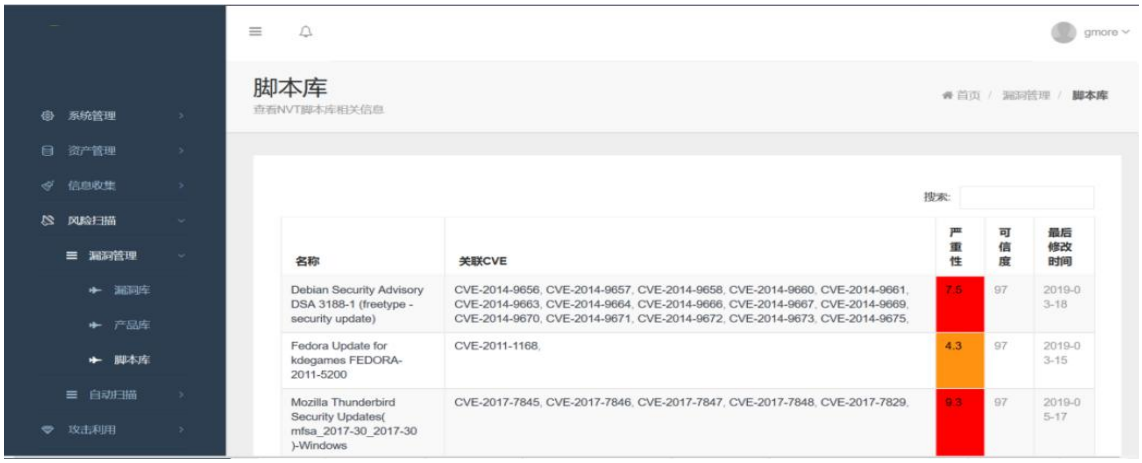
漏洞库：




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。

### 4.12.2 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；

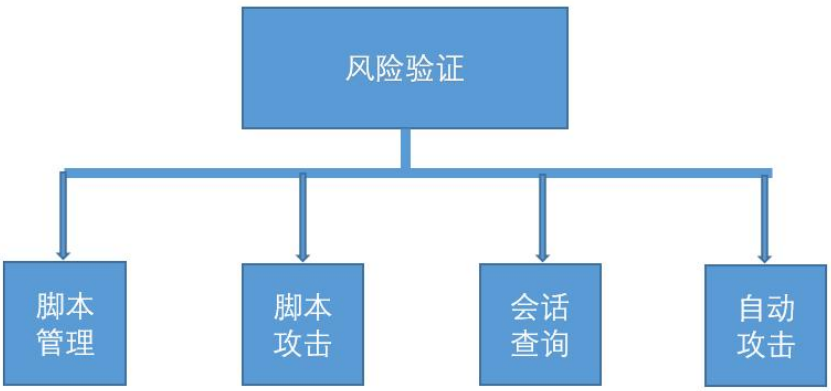
内置常见检测插件>40 个，常见 CMS 检测插件>300 个。

## 4.13 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。

### 4.13.1 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。

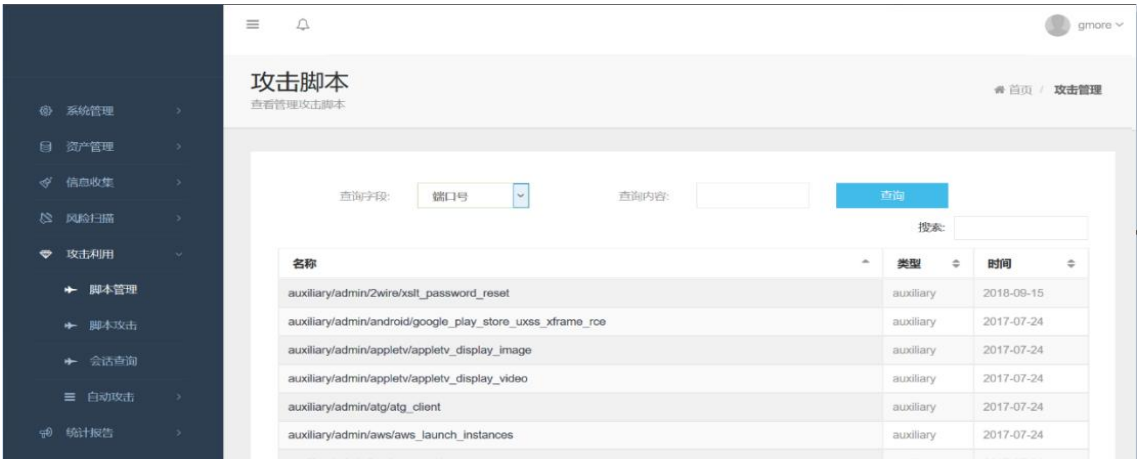



系统通过快速风险验证功能提供针对网络节点上发现的漏洞进行验证或发起攻击的能力。快速风险验证能够跟网络节点详细信息展示相关联，查看网络节点详细信息中的漏洞后

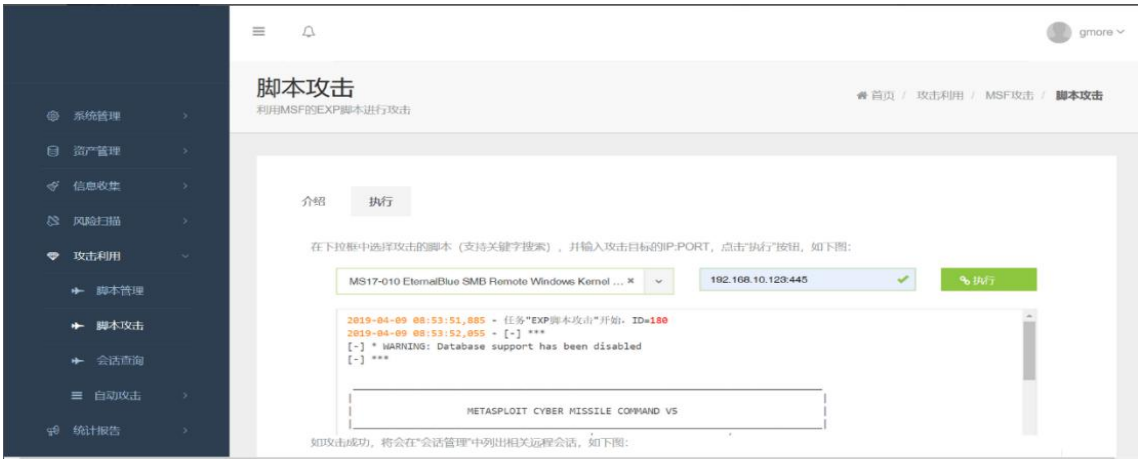
调出快速风险验证功能，用户配置风险验证相关参数后就能快速进行风险验证或利用，快速风险验证参数设置包括但不限于风险验证、攻击的插件选择、目标网络节点 IP 地址、目标端口、有效载荷代码选择等。

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



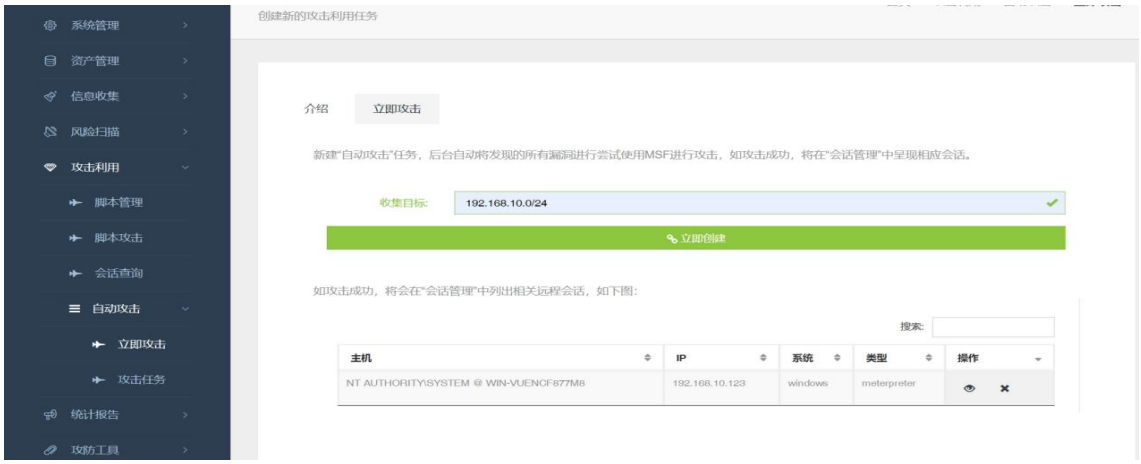

脚本攻击：




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。




### 4.13.2 性能指标

平台内置渗透攻击攻击模块>1800 项。

## 4.14 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。

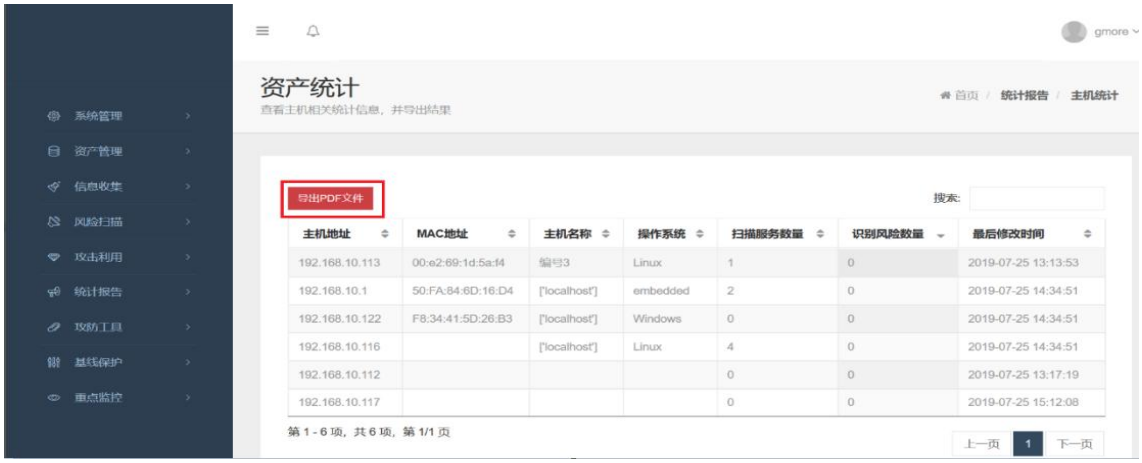
### 4.14.1 功能组成

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。

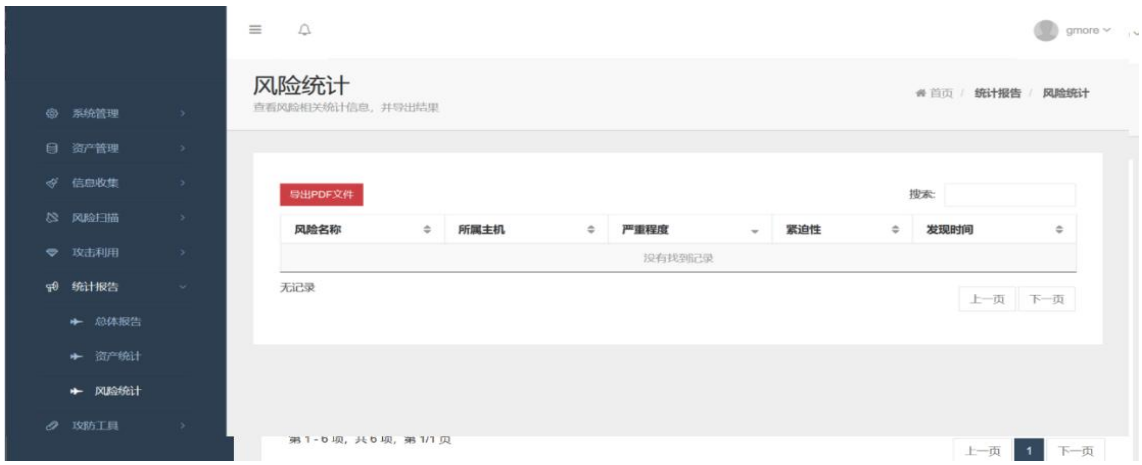
总体报告：


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。



### 4.14.2 性能指标

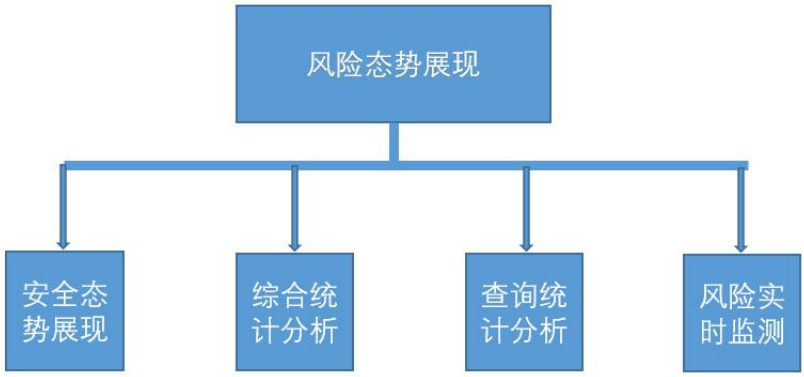
能够支持基础信息统计信息、资产统计信息和风险评估结果导出。

## 4.15 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。

### 4.15.1 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。

### 4.15.2 性能指标

采用多维度分析，全方位展现网络安全风险态势。

# 第 5 章　社会和经济效益

## 5.1　建立基础信息库

建立基础信息库，全方位了解网内资产情况，应用情况，中间件情况，了解网内设备和服务及端口情况。综合了解全网基础信息数据，便于进行建设规划，管控规划，安全风险防范规划，做好主动防御基础信息保障工作，提升全网安全风险防范能力。

## 5.2　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。

## 5.3　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。

## 5.4　智慧监控预警非法接入

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。

## 5.5　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。

## 5.6　自主把控风险能力

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。

## 5.7 提升风险防御能力

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，安全风险预警防御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。

## 5.8 加强基础设施安全

网络空间安全风险预警防御系统从主动防御出发，在加强基础设施安全方面有重要作用，能有效提升用户自主的风险预警能力，保障基础设施的安全。

# 第 6 章　系统配置装备清单

| 序号 | 装备名称 | 技术指标 | 单位 | 数量 | 单价 | 总价 |
|---|---|---|---|---|---|---|
| 1. | 网络安全风险预警防御系统（一、二级单位） | 硬件型态：4U 工控设备，CPU：英特尔 I7 内存：16G 硬盘：500G SSD ，网络接口：8 个。（可支持国产化硬件）<br>软件标准：以自动化方式，通过网络安全巡检、信息收集、风险发现、风险利用验证评估和风险报告等功能综合分析，建立防护方案，实现是事前主动发现安全风险，验证风险，评估风险等级，进而主动修复风险，最终推动网络安全防护模式由“事后追溯”向“事前感知”转变。<br>性能指标：单台设备推荐终端巡检数量不超过 100000，应用数量不超过 500。 | 台 | 1 | 39.8 | 39.8 |
| 2. | 网络安区风险预警防御系统（三级单位） | 硬件型态：2U 工控设备，CPU：英特尔 I7， 内存：8G，硬盘：500G SSD，网络接口：2 个。（可支持国产化硬件）<br>软件标准：以自动化方式，通过网络安全巡检、信息收集、风险发现、风险利用验证评估和风险报告等功能综合分析，建立防护方案，实现是事前主动发现安全风险，验证风险，评估风险等级，进而主动修复风险，最终推动网络安全防护模式由“事后追溯”向“事前感知”转变。<br>性能指标：单台设备推荐终端巡检数量不超过 50000，应用数量不超过 200。 | 台 | 1 | 25.8 | 25.8 |