网神
SECWORLD

可控安全
Controllable
Security

奇安信网神威胁监测与分析系统

（天眼产品系列）

技术白皮书

奇安信网神信息技术（北京）股份有限公司
http:// www.legendsec.com

奇安信集团（以下简称“奇安信”）包括但不限于以下主体：奇安信网神信息技术（北京）股份有限公司、北京奇安信科技有限公司、北京网康科技有限公司，以及上述主体直接或者间接控制的法律实体。奇安信为客户提供全方位的技术支持和服务。直接向奇安信购买产品的用户，如果在使用过程中有任何问题，可与公司总部联系。

读者如有任何关于本产品的问题，或者有意进一步了解公司其他相关产品，可通过下列方式与我们联系：

公司网址： https://www.qianxin.com

技术支持热线：95015

公司总部地址：北京市西城区西直门外南路 26 号院 1 号

版权声明

免责声明

奇安信集团，是专注于为政府、军队、企业，教育、金融等机构和组织提供企业级网络安全技术、产品和服务的网络安全公司，包括但不限于以下主体：奇安信网神信息技术（北京）股份有限公司、北京奇安信科技有限公司、北京网康科技有限公司，以及上述主体直接或者间接控制的法律实体。奇安信集团在此特别声明，对如下事宜不承担任何法律责任：

1. 本产品经过详细的测试，但不能保证与所有的软硬件系统或产品完全兼容，不能保证本产品完全没有错误。如果出现不兼容或错误的情况，用户可拨打技术支持电话将情况报告奇安信集团，获得技术支持。
2. 在适用法律允许的最大范围内，对因使用或不能使用本产品所产生的损害及风险，包括但不限于直接或间接的个人损害、商业盈利的丧失、贸易中断、商业信息的丢失或任何其它经济损失，奇安信集团不承担任何责任。
3. 对于因电信系统或互联网网络故障、计算机故障或病毒、信息损坏或丢失、计算机系统问题或其它任何不可抗力原因而产生的损失，奇安信集团不承担任何责任，但将尽力减少因此而给用户造成的损失和影响。
4. 对于用户违反本协议规定，给奇安信集团造成损害的，奇安信集团将有权采取包括但不限于中断使用许可、停止提供服务、限制使用、法律追究等措施。
5. 对于从非奇安信集团指定站点下载的本产品以及从非奇安信集团发行的介质上获得的本产品，奇安信集团无法保证该产品是否感染计算机病毒、是否隐藏有伪装的特洛伊木马程序或者黑客软件，使用此类软件，将可能导致不可预测的风险，建议用户不要轻易下载、安装、使用，奇安信集团不承担任何由此产生的一切法律责任。
6. 无论在任何原因下（包括但不限于疏忽原因），对任何人通过使用本产品上的信息或由本产品链接的信息，或其他与本产品链接的网站信息所导致的损失或损害（包括直接、间接、特别或后果性的损失或损害，如收入或利润之损失，电脑系统之损坏或数据丢失等后果），奇安信集团不承担任何由此产生的一切法律责任。

以上声明最终解释权归奇安信集团所有。

目 录

1 产品概述

1.1 产品简介

当前网络中存在大量的恶意文件以及恶意文件变种，对网络安全造成很大的威胁。单一的网络安全设备无法保证网络的安全，只有掌握整个用户网络的流量和威胁情况并结合全球网络的威胁情报才可能发现各种高级威胁的蛛丝马迹。

目前存在多种大数据威胁感知分析平台，要进行网络威胁分析首先要掌握海量威胁数据，除了云端的威胁情报，同样重要的还有用户本地网络的特定威胁情报。

奇安信网神威胁监测与分析系统是一种用于采集网络流量和威胁数据的网络数据传感器（NDS），通过在网络的多个位置合理部署奇安信网神威胁监测与分析系统，采集尽量全面的网络流量和威胁数据，并发送到大数据威胁感知分析平台（如态势感知平台或 NGSOC 分析平台）进行威胁分析检测，从而掌握全网网络安全情况。

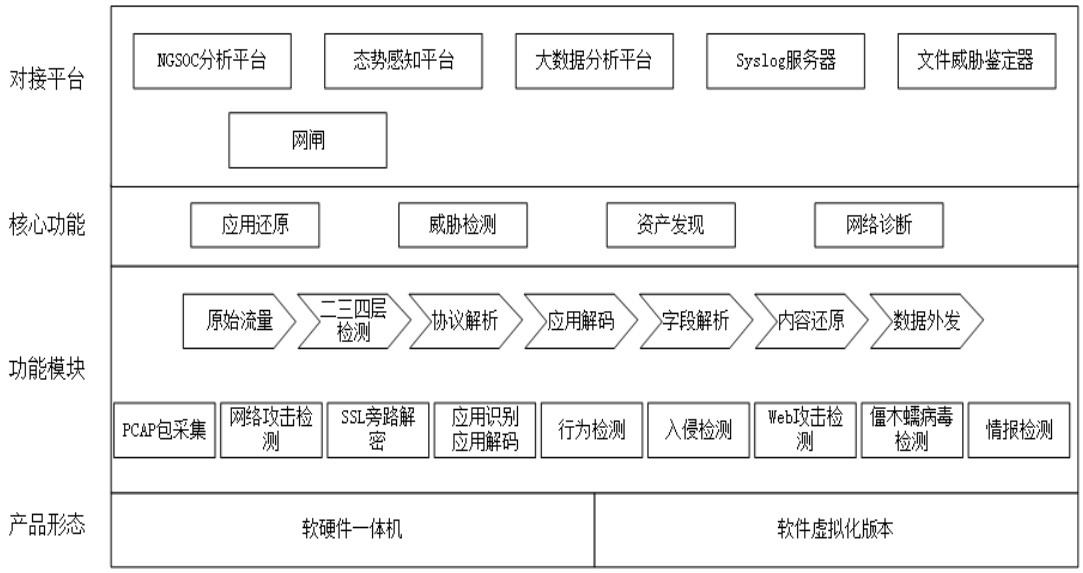
奇安信网神威胁监测与分析系统向外发送日志会在日志中标识本设备地址，从而在分析中可以进行日志溯源。

奇安信网神威胁监测与分析系统通过旁路方式部署，完全不需要改变用户的网络环境。通过把奇安信网神威胁监测与分析系统的数据采集接口连接在交换机的镜像口上实现对流量的检测，检测完成后所有镜像流量都会被丢弃。这种模式对用户的网络环境完全没有影响，旁路设备故障不会对业务链路造成影响。

1.2 产品形态及产品功能

奇安信网神威胁监测与分析系统属于我司“天眼产品（TY-TSS10000）”系列网络数据传感器，支持硬件一体机、软件虚拟化版本 2 种产品形态。系统整体功能框架如图 1-1 所示。产品采集的流量经过二三四层检查、协议解析、应用解码，并经过各种威胁检测后还原出多种流量日志和生产对应威胁日志，并支持将日志上传到多个分析平台和 Syslog 服务器。支持进行文件还原并上传文件威胁鉴定器进行二次检测。且在专网场景下支持直接将日志上传网闸，通过网闸设备再上送态势感知平台和 NGSOC 分析平台。

图1-1 系统形态及功能框架



2 产品能力

2.1 流量数据采集能力

2.1.1 在线和离线流量数据采集

奇安信网神威胁监测与分析系统不仅支持对镜像到接口的实时流量进行在线数据采集，生成流量日志；还支持离线数据采集。通过导入 PCAP 文件，对 PCAP 文件对应流量二次检测进行流量数据采集，生成流量日志。

2.1.2 基于多种参数定义采集流量

奇安信网神威胁监测与分析系统支持基于源地址/地区、目的地址/地区、服务、例外应用、流量采样比、时间等多种参数定义数据采集策略进行流量采集。

2.1.3 19 种流量日志还原能力

奇安信网神威胁监测与分析系统支持 19 种流量日志还原能力，支持解析、生成及外发 TCP 流量日志。包括：探针传感器序列号、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。

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。

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。

支持传输协议审计日志，包括 https、http、DNS、邮件协议审计日志、SMB、AD 域、WEB 登录、FTP、Telnet、ICMP、TELNET、ICMP 、SNMP、SSL 、SIP 、ONVIF 、mongo、NFS 、SOCKS 、dhcp、netbios_nbns、全流量元数据审计、数据库审计协议等。

支持登录认证，如 Kerberos 认证、Radius 认证、LDAP 行为日志、登录动作日志。支持邮件行为日志、数据库操作日志、异常报文日志、应用智能日志、定制日志。

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。

2.2 威胁数据采集能力

奇安信网神威胁监测与分析系统支持威胁情报检测、恶意文件检测、入侵检测（漏洞检测和间谍软件检测）、网络层攻击检测、文件威胁鉴定器联动等多种威胁检测能力。检测到威胁后生成威胁日志。

增加日志关联模型：通过模型对流量日志的分析，发现更多的不易识别的威胁；而且模型可以通过库升级的方式增加。

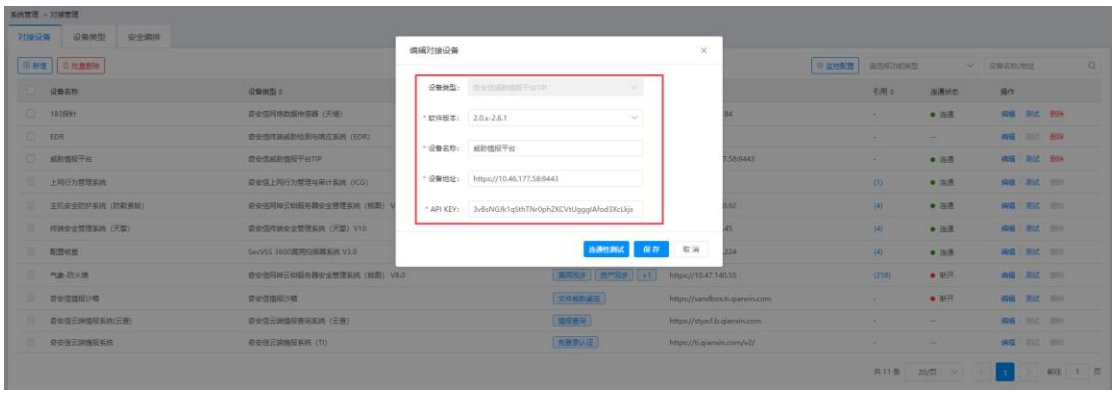
2.2.1 在线和离线威胁数据采集能力

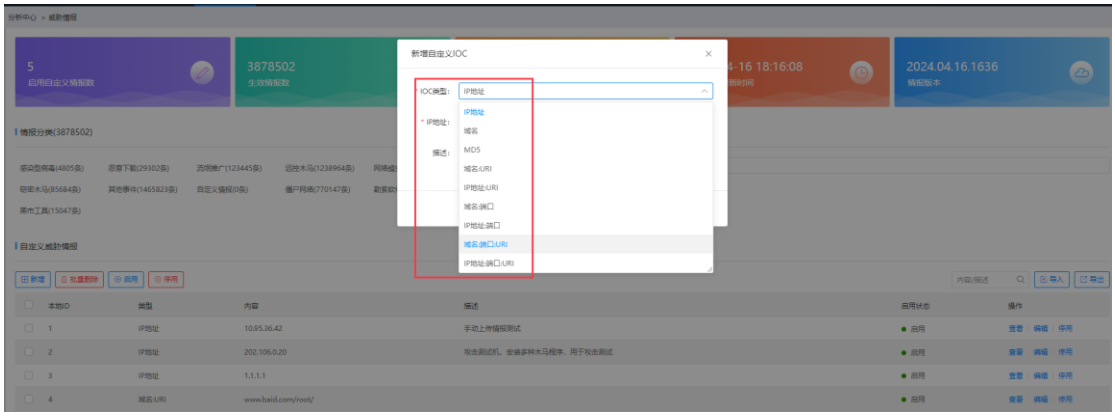
奇安信网神威胁监测与分析系统不仅支持对镜像到接口的实时流量进行在线威胁检测，生成威胁日志；还支持离线数据威胁采集。通过导入 PCAP 文件，对 PCAP 文件对应流量进行威胁检测，生成威胁日志。

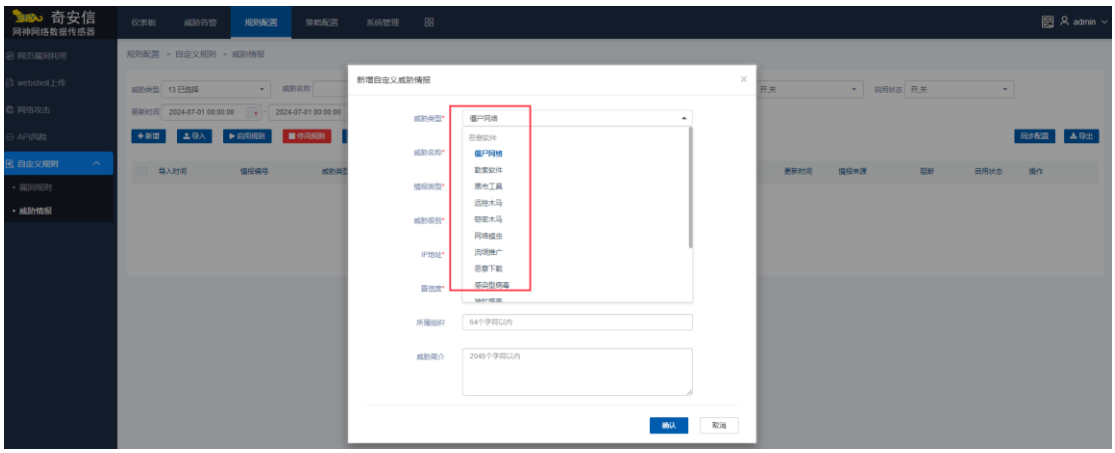
2.2.2 威胁情报能力

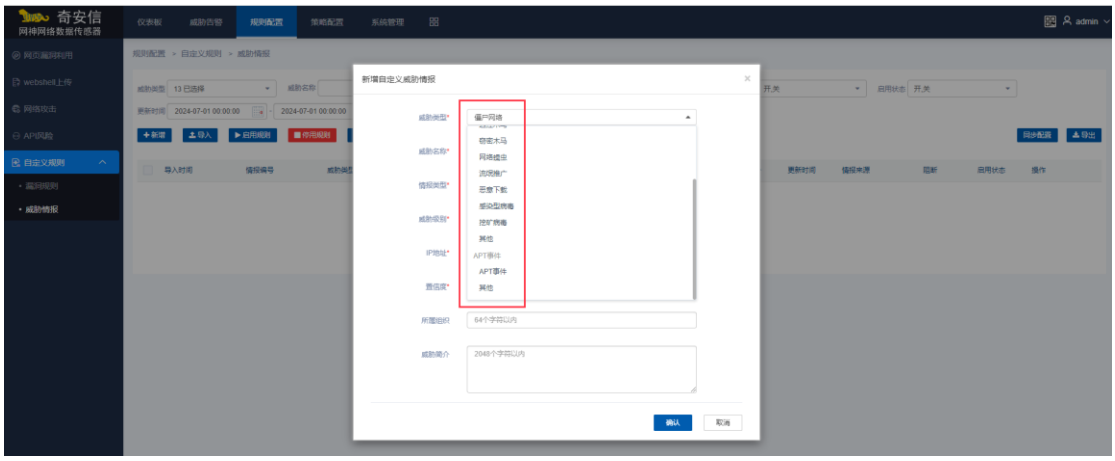
奇安信网神威胁监测与分析系统支持强大的本地威胁情报库（IOC 库），且可以定期更新 IOC 库。通过威胁情报可以快速发现用户网络中的未知威胁，从而迅速做出响应。

支持基于流量实时 IOC 匹配功能，设备具备主流的 IOC。支持基于威胁情报的威胁检测，检测类型包含 APT 事件、僵尸网络、勒索软件、黑市工具、远控木马、窃密木马、网络蠕虫、流氓推广、恶意下载、感染型病毒、挖矿病毒、其他恶意软件。









2.2.3 恶意文件检测能力

奇安信网神威胁监测与分析系统支持对 HTTP、FTP、SMTP、POP3、IMAP、SMB、TFTP、NFS，八种协议进行恶意文件检测，且可以对通过网络云盘、网页邮箱、论坛、博客等主流 HTTP 网络应用上传或下载的文件进行恶意文件检测。

本地恶意文件库支持超过 350 万恶意文件样本，并且定时进行更新。

支持恶意文件云检测，扩充恶意文件库至 20 亿。能动态形成本地文件黑白名单，并支持用户自定义。

支持云沙箱，可以对恶意文件功能无法确认的未知恶意文件进行二次检测。

2.2.4 入侵检测能力

奇安信网神威胁监测与分析系统采用全新先进的多维动态特征异常检测引擎，抛弃原有的异常行为特征码静态表达的方式，将异常行为、恶意行为特征码通过多维度提炼，动态进行表达，使得特征表达更加全面、精准、有效，极大提高了入侵检测的命中质量，解决了传统设备检测命中率高，但是误报率同样高的问题。

内置检测规则，支持检测 WEB 攻击、Webshell 攻击、网络攻击、后门程序、僵木蠕检测、C2 外连、恶意通信、SMB 远程溢出攻击、文件上传、弱口令、暴力猜解、挖矿、黑客工具、明文密码传输、漏洞利用、ARP 欺骗、恶意扫描等风险。

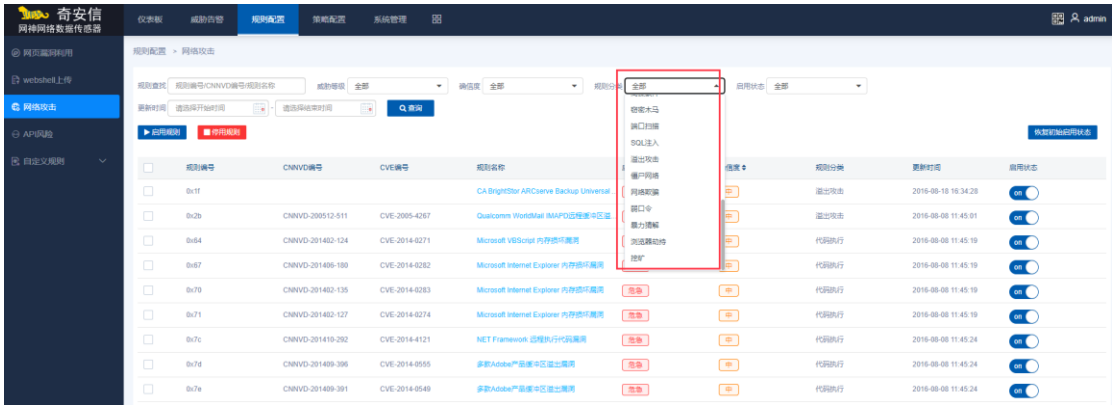
入侵特征库支持超过 9000 多种漏洞，包括 CVE 漏洞库、CNNVD 中国国家信息安全漏洞库中的漏洞和其他自主发现的漏洞，能够实时检测跨站脚本、拒绝服务、恶意扫描、暴力破解、SQL 注入、Web 攻击、缓冲区溢出及其他攻击漏洞以及病毒蠕虫、木马后门、僵尸网络等间谍软件。

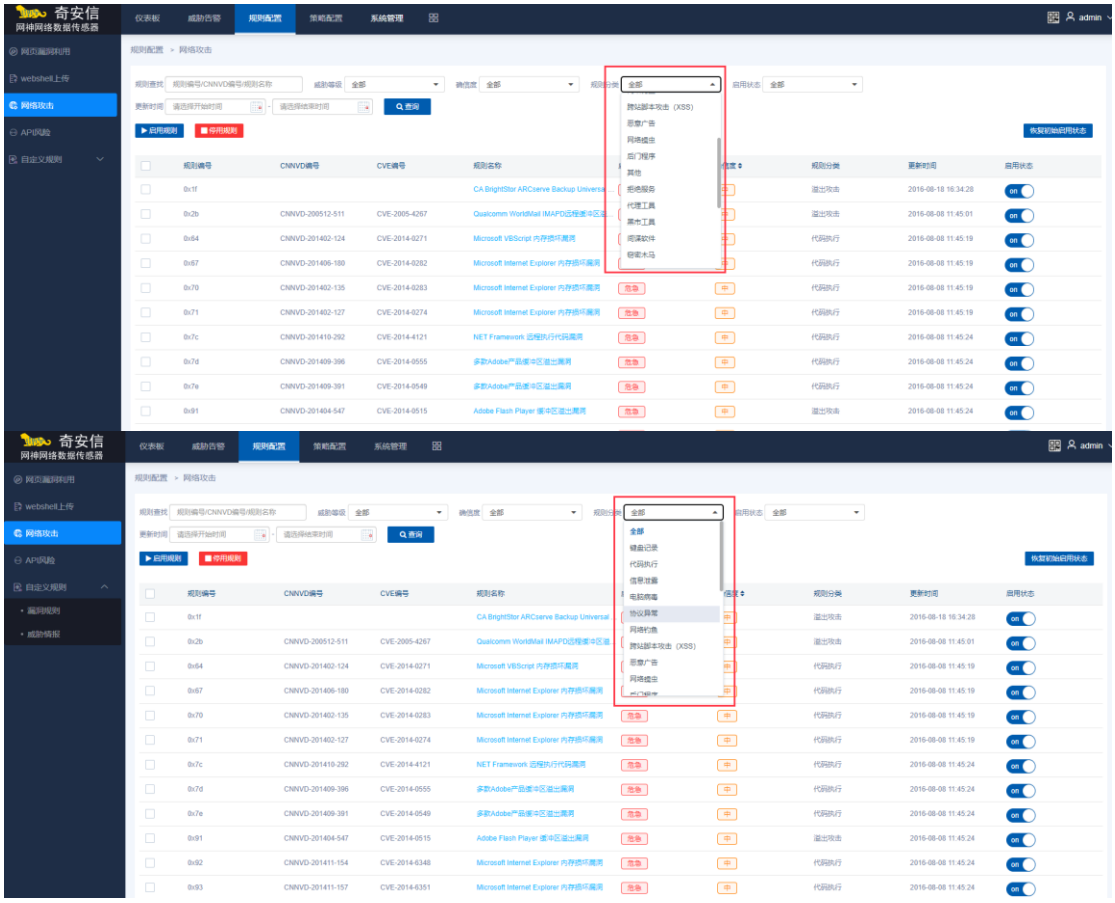
除入侵特征库中预定义的签名外，用户能够添加自定义漏洞签名和间谍软件签名。

不仅可以在网络层和传输层分析和跟踪 IP、ICMP、TCP、UDP 等协议，对这些协议的准确性进行验证；还可以对 FTP、HTTP、IMAP、POP3、SMB、SMTP 及其他应用协议的合法性进行分析。可以对 TCP 流进行流重组检测，并对重组后的数据进行攻击检测。

2.2.5 网络层攻击检测能力

奇安信网神威胁监测与分析系统支持多种攻击检测，能更全面的从流量中发现威胁，如：SQL 注入、XSS、信息泄露、间谍软件、协议异常、网络欺骗、黑市工具、代码执行、挖矿等。





奇安信网神威胁监测与分析系统支持网络层 Flood 检测（包括 SYN Flood、ICMP Flood、UDP Flood 和 IP Flood）、恶意扫描检测（包括 Tracert 检测、IP 地址扫描、端口扫描）、异常包攻击检测、ICMP 管控检测、应用层 Flood 检测、Web 应用漏洞检测、应用识别能力、库升级能力、文件威胁鉴定联动能力。

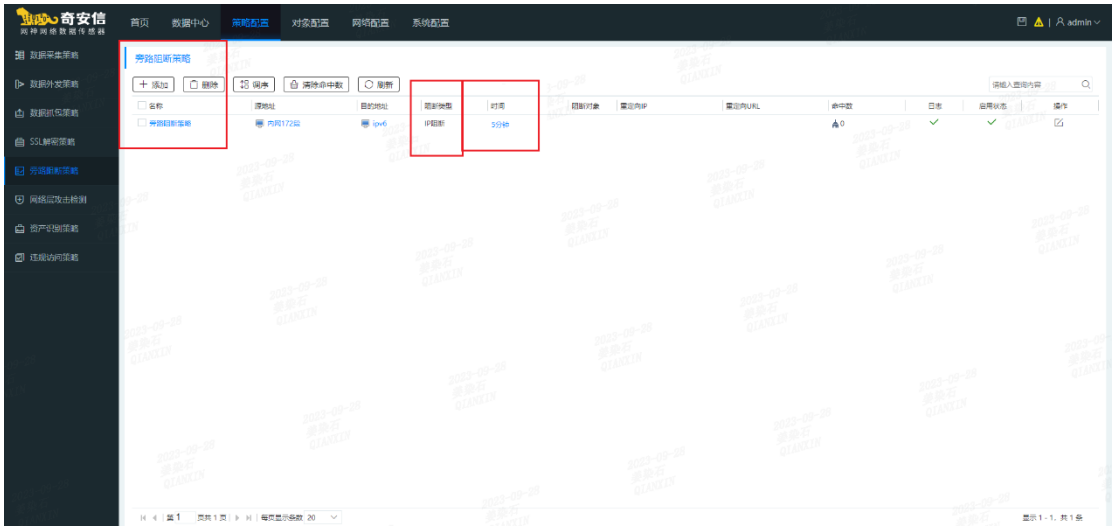
奇安信网神威胁监测与分析系统基于自定义目的 IP 的 DDoS 检测。流量 DDoS 检测通过将用户关键资产 IP 指定为 DDoS 目的 IP 保护下的 IP，对这些 IP 进行 DDoS 检测和单个攻击源 IP 的 DDoS 检测，针对性更好，且可以节省奇安信网神威胁监测与分析系统的资源。

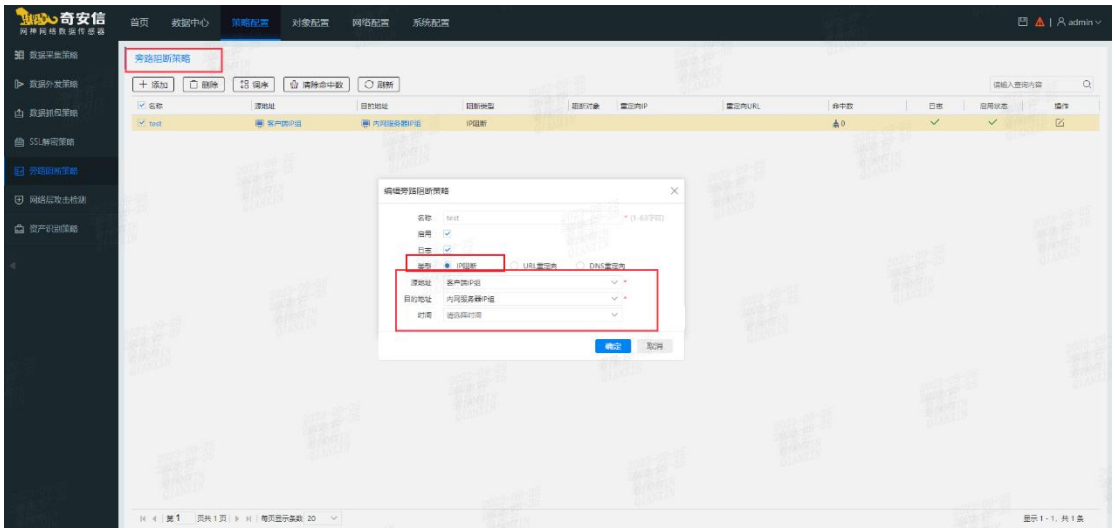
奇安信网神威胁监测与分析系统支持标准端口运行非标准协议，非标准端口运行标准协议的异常流量检测，端口类型包括 3389、53、80/8080、21、69、443、25、110、143、22 等。

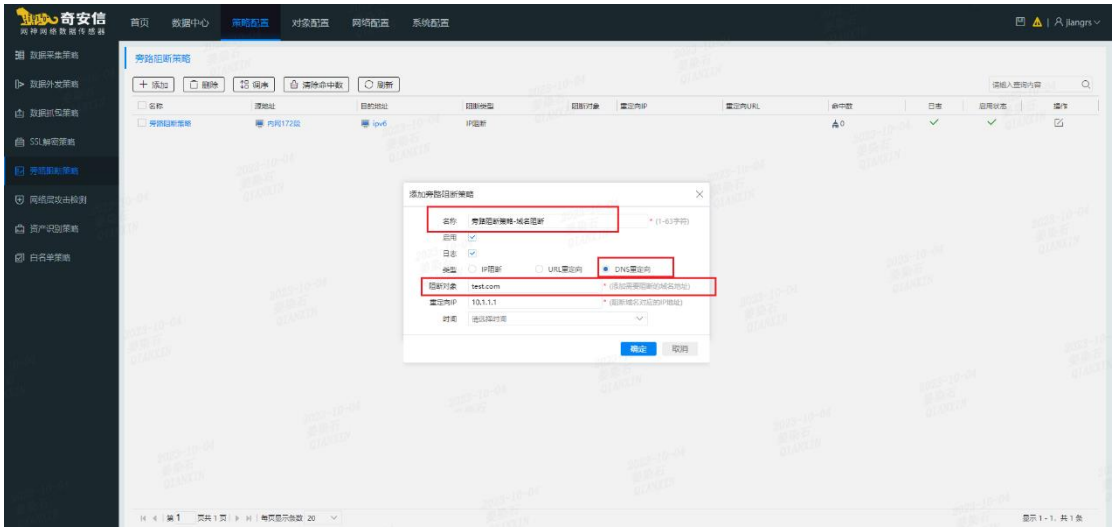
2.2.5.1 旁路阻断

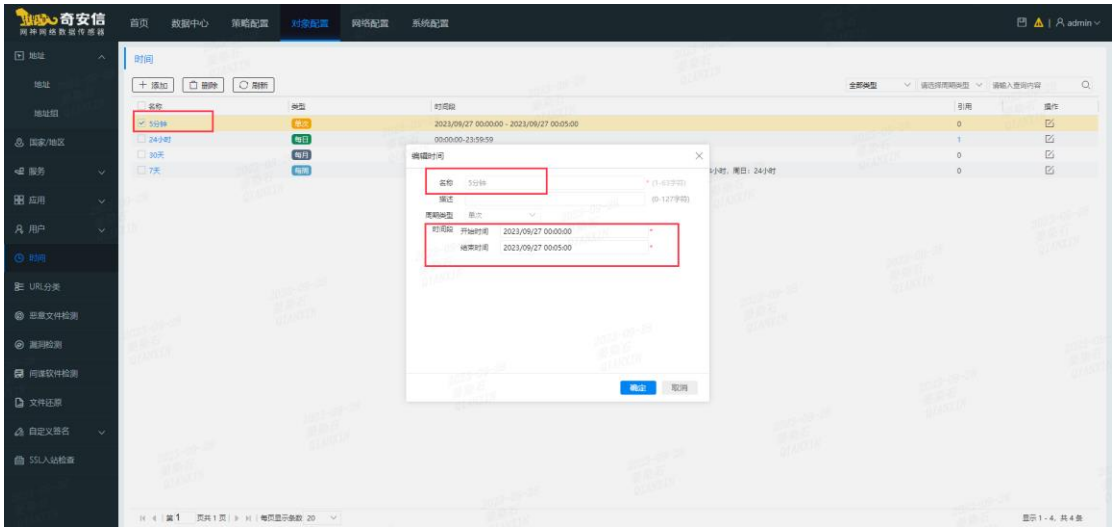
奇安信网神威胁监测与分析系统支持基于 IP 和域名的旁路阻断，能够在实时镜像的流量中发现恶意 IP 并实现实时阻断，支持 24 小时/7 天/30 或者自定义时间在 5 分钟内阻断威胁。

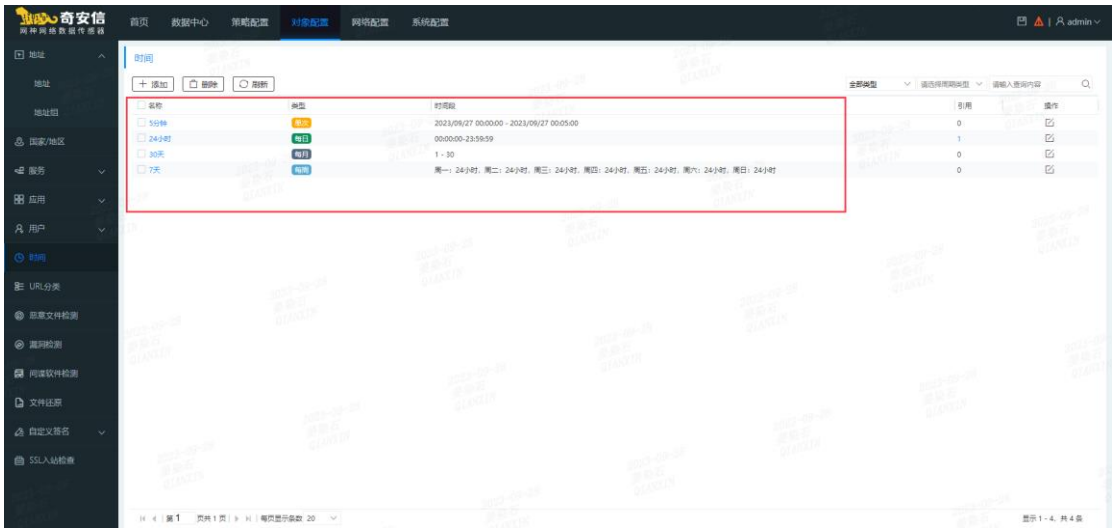
旁路阻断策略增加时间对象，分别 5 分钟/1 天——24 小时/1 周——7 天/1 月——30 天。





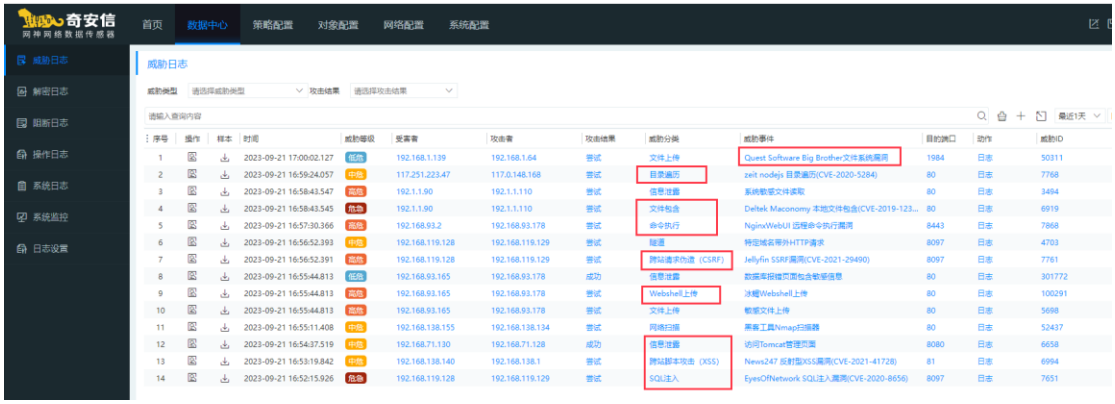

奇安信
首页
数据中心
策略配置
对象配置
网络配置
系统配置
旁路阻断策略
添加旁路阻断策略
DNS重定向
test.com
10.1.1.1
确定
取消

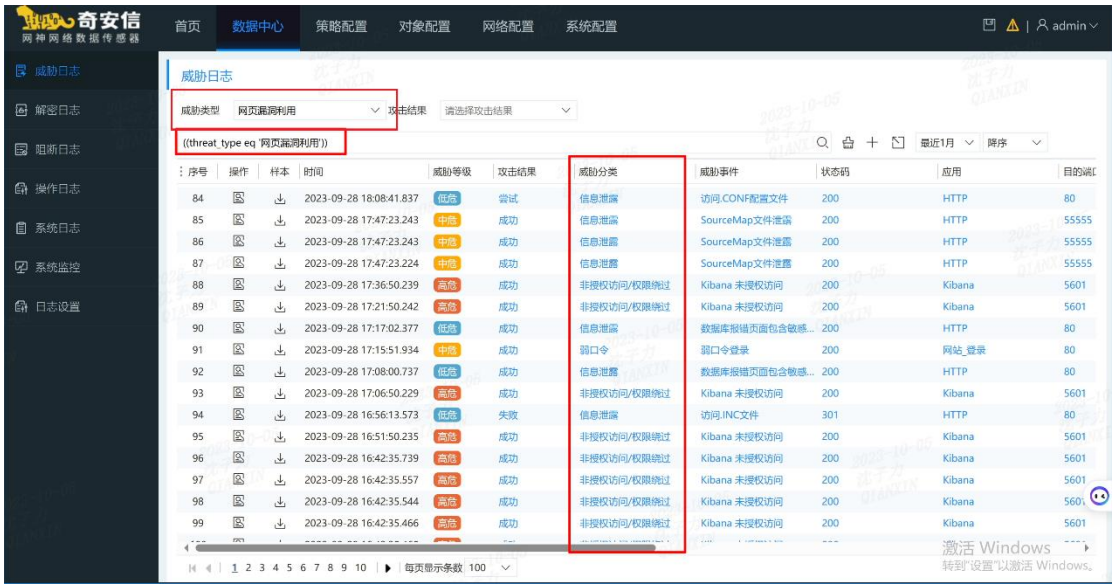

奇安信
首页
数据中心
策略配置
对象配置
网络配置
系统配置
admin
时间
5分钟
24小时
30天
7天
编辑时间
2023/09/27 00:00:00
2023/09/27 00:05:00
确定
取消


奇安信
首页
数据中心
策略配置
对象配置
网络配置
系统配置
admin
时间
5分钟
24小时
30天
7天
2023/09/27 00:00:00 - 2023/09/27 00:05:00
00:00:00-23:59:59
1 - 30

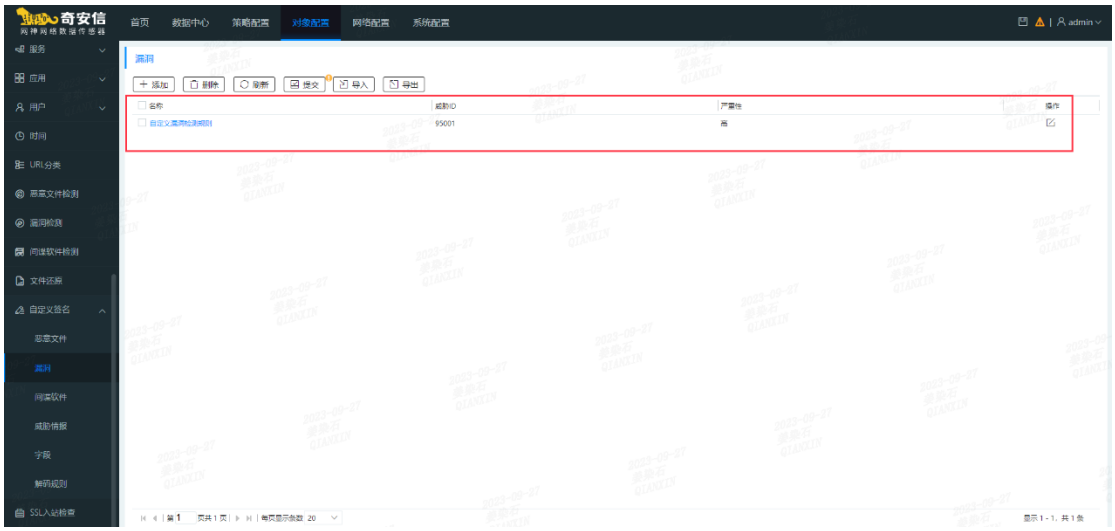
2.2.5.2Web 应用防护

奇安信网神威胁监测与分析系统支持 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。

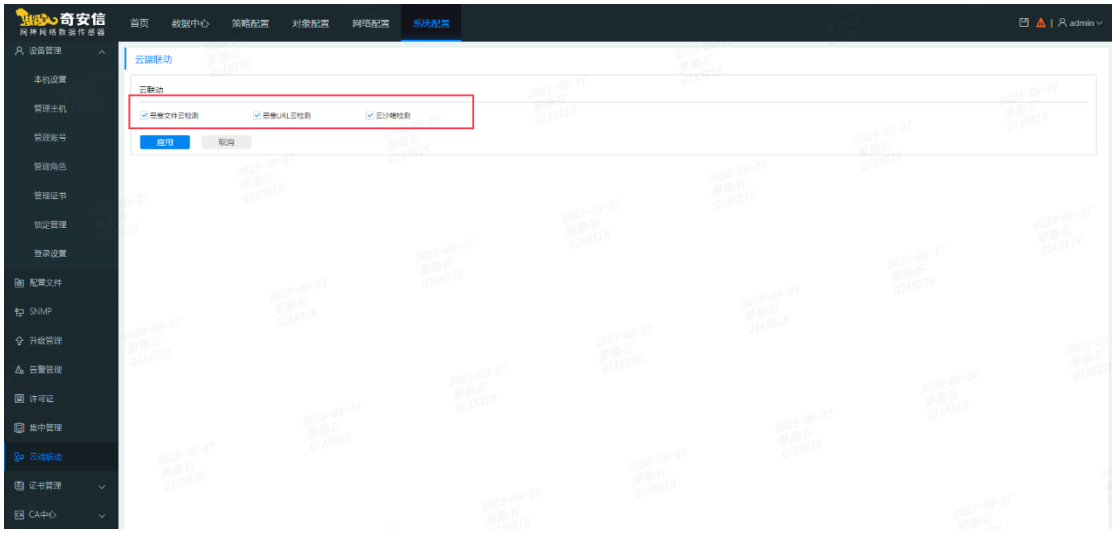




自定义 WAF 规则——自定义漏洞检测规则、自定义间谍软件检测规则



WAF 云防护（恶意文件云检测、恶意 URL 云检测、云沙箱检测）



2.2.5.3 应用识别能力

应用识别是进行威胁识别的基础能力，只有识别出具体的应用，才可以更好的识别出该应用的恶意文件、漏洞等威胁。

奇安信网神威胁监测与分析系统拥有丰富的应用识别特征库，可识别超过 1058 种网络应用。能够精确检测 115 网盘、彩云网盘、360 云盘、百度云盘、126 邮箱、139 邮箱、163 邮箱、189 邮箱、21CN 邮箱、51CTO 论坛、CSDN 论坛、猫扑论坛、百度贴吧、中华论坛网、51CTO 博客、新浪博客、CSDN 博客、新浪微博私信、微信、腾讯微博等主流网络应用。

在应用中增加自定义解码功能，可基于已经识别的应用或自定义应用，根据应用的通信格式，通过固定长度、正则表达式或 TLV 方式，进行应用解码提取用户需求的数据信息，丰富设备对于特殊协议、应用的解码能力。

2.2.5.4 库升级能力

奇安信网神威胁监测与分析系统支持定期自动升级恶意文件库、入侵检测库、威胁情报库、应用识别库，可以及时获取最新的恶意文件库、入侵检测库和威胁情报库，提高恶意文件检测的识别能力，降低误识别率。

2.2.5.5 文件威胁鉴定联动能力

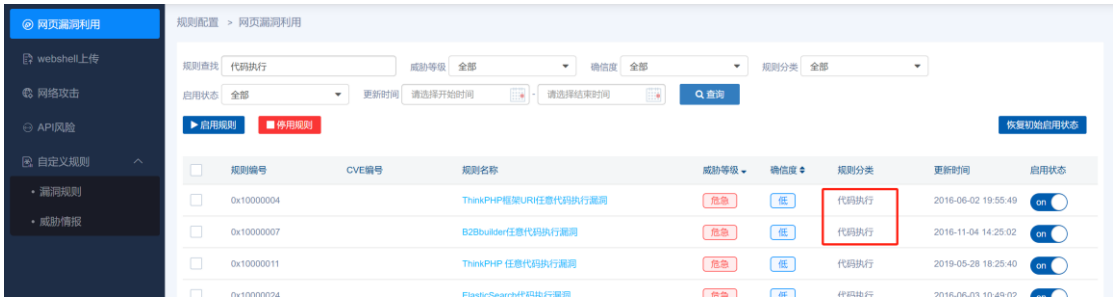
奇安信网神威胁监测与分析系统支持配置文件还原规则，对符合数据采集策略的流量进行文件还原。并支持将还原后的文件发送到文件威胁鉴定器进行威胁检测。

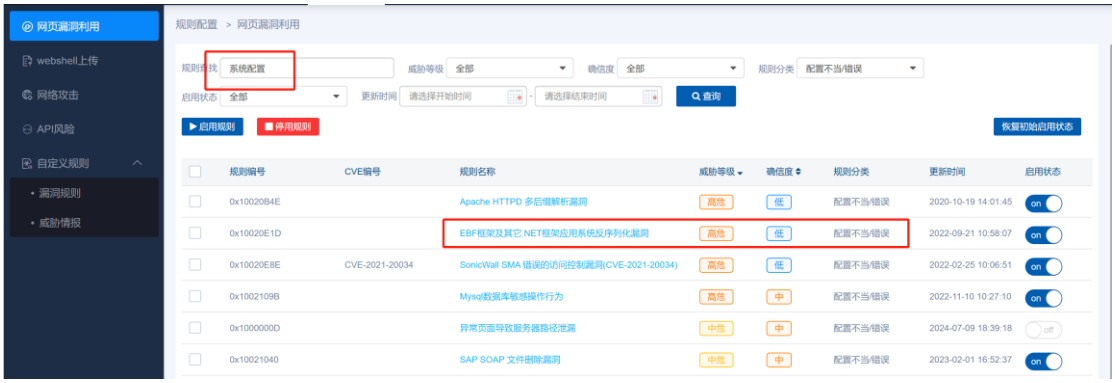
2.3 威胁场景检测能力

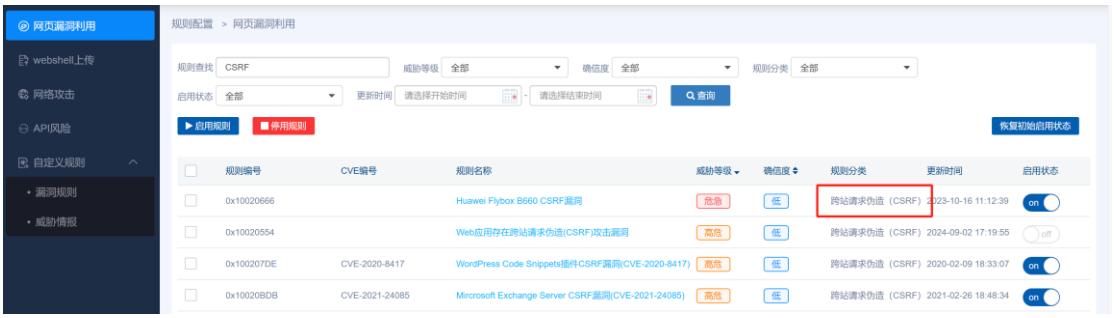
2.3.1 Web 攻击检测

奇安信网神威胁监测与分析系统支持检测针对 WEB 应用的攻击，如 SQL 注入、XSS、代码执行、系统配置等注入型攻击。支持跨站请求伪造 CSRF 攻击检测。支持其他类型的 WEB 攻击，如目录遍历、弱口令、权限绕过、命令执行、文件读写、信息泄漏、文件包含、文件写入攻击、挖矿等检测。

针对 WEB 应用的攻击类型；




网页漏洞利用
webshell上传
网络攻击
API风险
自定义规则
漏洞规则
威胁情报
规则配置 > 网页漏洞利用
规则查找 系统配置
威胁等级 全部
确信度 全部
规则分类 配置不当/错误
启用状态 全部
更新时间
查询
启用规则
停用规则
恢复初始启用状态
规则编号 CVE编号 规则名称 威胁等级 确信度 规则分类 更新时间 启用状态
0x10020B4E Apache HTTPD 多后缀解析漏洞 高危 低 配置不当/错误 2020-10-19 14:01:45
0x10020E1D EBF框架及其它.NET框架应用系统反序列化漏洞 高危 低 配置不当/错误 2022-09-21 10:58:07
0x10020E8E CVE-2021-20034 SonicWall SMA 错误的访问控制漏洞(CVE-2021-20034) 高危 低 配置不当/错误 2022-02-25 10:06:51
0x1002109B Mysql数据库敏感操作行为 高危 中 配置不当/错误 2022-11-10 10:27:10
0x1000000D 异常页面导致服务器路径泄露 中危 中 配置不当/错误 2024-07-09 18:39:18
0x10021040 SAP SOAP 文件删除漏洞 中危 中 配置不当/错误 2023-02-01 16:52:37


网页漏洞利用
webshell上传
网络攻击
API风险
自定义规则
漏洞规则
威胁情报
规则配置 > 网页漏洞利用
规则查找 CSRF
威胁等级 全部
确信度 全部
规则分类 全部
启用状态 全部
更新时间
查询
启用规则
停用规则
恢复初始启用状态
规则编号 CVE编号 规则名称 威胁等级 确信度 规则分类 更新时间 启用状态
0x10020666 Huawei Flybox B660 CSRF漏洞 危急 低 跨站请求伪造（CSRF） 2023-10-16 11:12:39
0x10020554 Web应用存在跨站请求伪造(CSRF)攻击漏洞 高危 低 跨站请求伪造（CSRF） 2024-09-02 17:19:55
0x100207DE CVE-2020-8417 WordPress Code Snippets插件CSRF漏洞(CVE-2020-8417) 高危 低 跨站请求伪造（CSRF） 2020-02-09 18:33:07
0x10020BDB CVE-2021-24085 Mircosoft Exchange Server CSRF漏洞(CVE-2021-24085) 高危 低 跨站请求伪造（CSRF） 2021-02-26 18:48:34

其他类型的 WEB 攻击；


网页漏洞利用
webshell上传
网络攻击
API风险
自定义规则
漏洞规则
威胁情报
规则配置 > 网页漏洞利用
规则查找 目录遍历
威胁等级 全部
确信度 全部
规则分类 全部
启用状态 全部
更新时间
查询
启用规则
停用规则
恢复初始启用状态
规则编号 CVE编号 规则名称 威胁等级 确信度 规则分类 更新时间 启用状态
0x10000013 应用程序存在文件包含漏洞(Win系统、目录遍历) 危急 低 文件包含 2016-06-03 10:34:59
0x10000C7C CVE-2013-0084 Microsoft SharePoint Server/Foundation 目录遍历漏洞 危急 中 目录遍历 2016-08-08 11:45:24
0x10000DF7 CVE-2015-1398 Magento Community Edition和Enterprise Edition 目录遍历... 危急 中 目录遍历 2016-08-08 11:45:28
0x10000E64 CVE-2016-0855 Advantech WebAccess 目录遍历漏洞 危急 中 目录遍历 2016-08-08 11:45:29


网页漏洞利用
webshell上传
网络攻击
API风险
自定义规则
漏洞规则
威胁情报
规则配置 > 网页漏洞利用
规则查找 弱口令
威胁等级 全部
确信度 全部
规则分类 全部
启用状态 全部
更新时间
查询
启用规则
停用规则
恢复初始启用状态
规则编号 CVE编号 规则名称 威胁等级 确信度 规则分类 更新时间 启用状态
0x100012AA Oracle WebLogic系统弱口令登录 危急 中 弱口令 2020-09-17 18:10:15
0x100203CB Wordpress后台弱口令登录 危急 低 弱口令 2019-07-01 11:24:53
0x100203CC Metinfo系统后台弱口令登录 危急 低 弱口令 2024-07-08 14:44:25
0x100203CD 发现PHPOA系统弱口令登录 危急 低 弱口令 2022-12-29 10:12:57


网页漏洞利用
webshell上传
网络攻击
API风险
自定义规则
漏洞规则
威胁情报
规则配置 > 网页漏洞利用
规则查找 权限绕过
威胁等级 全部
确信度 全部
规则分类 全部
启用状态 全部
更新时间
查询
启用规则
停用规则
恢复初始启用状态
规则编号 CVE编号 规则名称 威胁等级 确信度 规则分类 更新时间 启用状态
0x10020431 CVE-2017-12635 Apache Couchdb 垂直权限绕过漏洞(CVE-2017-12635) 危急 低 非授权访问/权限绕过 2023-04-20 14:23:33
0x10020441 CVE-2018-10106 Dlink dir815 路由器权限绕过和敏感信息泄露（CVE-2018-... 危急 低 非授权访问/权限绕过 2018-04-17 14:04:39
0x100003FA CVE-2013-0632 Adobe ColdFusion 权限绕过漏洞 高危 中 非授权访问/权限绕过 2016-08-08 11:45:20


网页漏洞利用
webshell上传
网络攻击
API风险
自定义规则
漏洞规则
威胁情报
规则配置 > 网页漏洞利用
规则查找 命令执行
威胁等级 全部
确信度 全部
规则分类 全部
启用状态 全部
更新时间 请选择开始时间 请选择结束时间
查询
启用规则
停用规则
恢复初始启用状态
规则编号 CVE编号 规则名称 威胁等级 确信度 规则分类 更新时间 启用状态
0x10000042 命令执行漏洞 危急 低 命令执行 2016-06-03 16:05:57 on
0x10000183 Moadmin.php find 远程命令执行漏洞 危急 低 命令执行 2016-06-03 12:08:07 on
0x10000262 Struts2-046远程命令执行漏洞 危急 低 命令执行 2020-12-16 09:22:27 on


网页漏洞利用
webshell上传
网络攻击
API风险
自定义规则
漏洞规则
威胁情报
规则配置 > 网页漏洞利用
规则查找 文件读写
威胁等级 全部
确信度 全部
规则分类 全部
启用状态 全部
更新时间 请选择开始时间 请选择结束时间
查询
启用规则
停用规则
恢复初始启用状态
规则编号 CVE编号 规则名称 威胁等级 确信度 规则分类 更新时间 启用状态
0x10020839 发现CobaltStrike进行文件读写操作 危急 低 黑市工具 2020-03-12 15:11:47 on


网页漏洞利用
webshell上传
网络攻击
API风险
自定义规则
漏洞规则
威胁情报
规则配置 > 网页漏洞利用
规则查找 信息泄漏
威胁等级 全部
确信度 全部
规则分类 全部
启用状态 全部
更新时间 请选择开始时间 请选择结束时间
查询
启用规则
停用规则
恢复初始启用状态
规则编号 CVE编号 规则名称 威胁等级 确信度 规则分类 更新时间 启用状态
0x1000016A Kingdee Eassso/Portal信息泄漏漏洞 危急 低 敏感信息/重要文件泄漏 2016-07-06 17:14:06 on
0x1000017D 动软系统api接口信息泄漏漏洞 高危 低 敏感信息/重要文件泄漏 2016-06-03 12:05:04 on
0x1000020E 易捷OA任意用户信息泄漏漏洞 高危 低 敏感信息/重要文件泄漏 2016-06-03 11:52:28 on
0x10020734 泛微e-cology OA数据库配置信息泄漏漏洞 高危 低 默认配置不当 2019-11-15 14:20:23 on

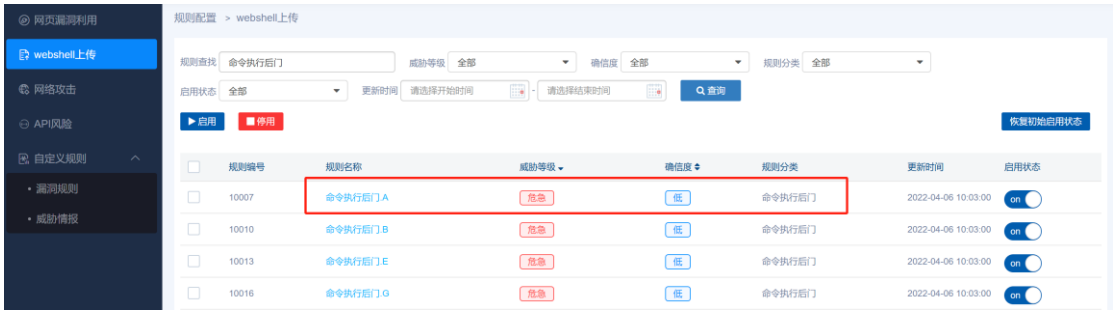

网页漏洞利用
webshell上传
网络攻击
API风险
自定义规则
漏洞规则
威胁情报
规则配置 > 网页漏洞利用
规则查找 文件包含
威胁等级 全部
确信度 全部
规则分类 全部
启用状态 全部
更新时间 请选择开始时间 请选择结束时间
查询
启用规则
停用规则
恢复初始启用状态
规则编号 CVE编号 规则名称 威胁等级 确信度 规则分类 更新时间 启用状态
0x10000008 Urpsoft file 文件包含漏洞 危急 低 文件包含 2016-06-03 10:03:59 on
0x1000000A igenus邮件系统用户登录处任意文件包含 危急 低 文件包含 2016-06-03 10:04:39 on
0x10000013 应用程序存在文件包含漏洞(Win系统，目录遍历) 危急 低 文件包含 2016-06-03 10:34:59 on


网页漏洞利用
webshell上传
网络攻击
API风险
自定义规则
漏洞规则
威胁情报
规则配置 > 网页漏洞利用
规则查找 文件写入
威胁等级 全部
确信度 全部
规则分类 全部
启用状态 全部
更新时间 请选择开始时间 请选择结束时间
查询
启用规则
停用规则
恢复初始启用状态
规则编号 CVE编号 规则名称 威胁等级 确信度 规则分类 更新时间 启用状态
0x10000196 Open Flash Chart任意文件写入漏洞 危急 低 文件写入 2016-06-13 11:57:20 on
0x10021400 蓝凌OA任意文件写入漏洞 危急 中 文件写入 2022-12-15 22:15:43 on
0x10021B36 cacti Weathermap 文件写入漏洞 危急 低 文件上传 2024-05-24 14:32:51 on

2.3.2 Webshell 攻击检测

奇安信网神威胁监测与分析系统支持基于 webshell 函数的攻击检测，如任意文件上传、任意函数执行后门、任意文件写入、任意文件包含、任意目录读取、命令执行后门、preg_replace 代码执行等。支持基于代理程序的攻击检测，如 TCP 代理程序、HTTP 代理程序等。

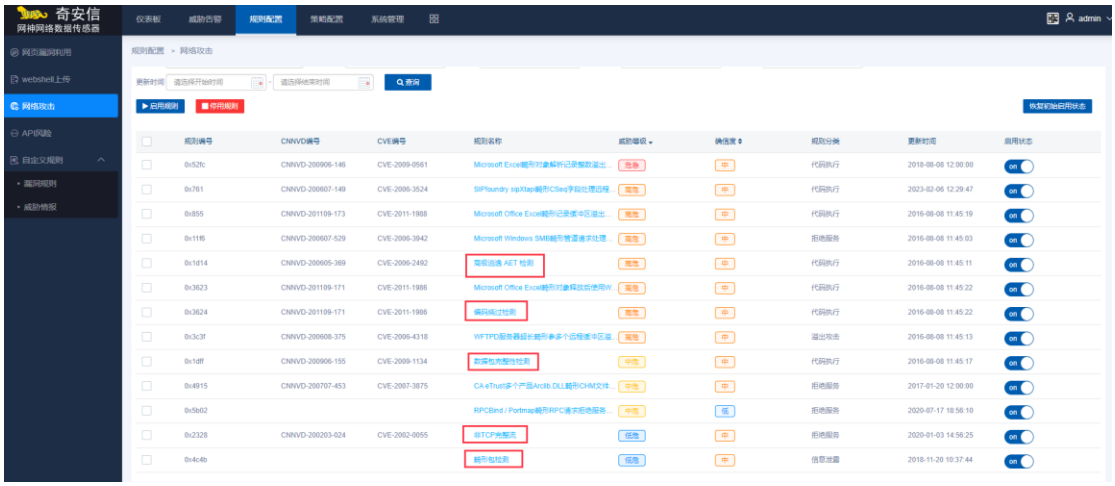
基于 webshell 函数的攻击检测；



基于代理程序的攻击检测；

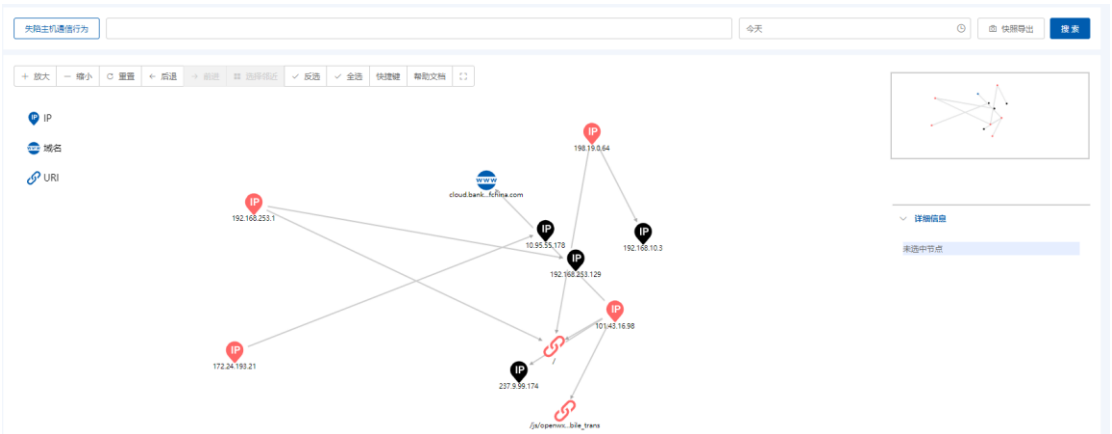
2.3.3 异常流量检测

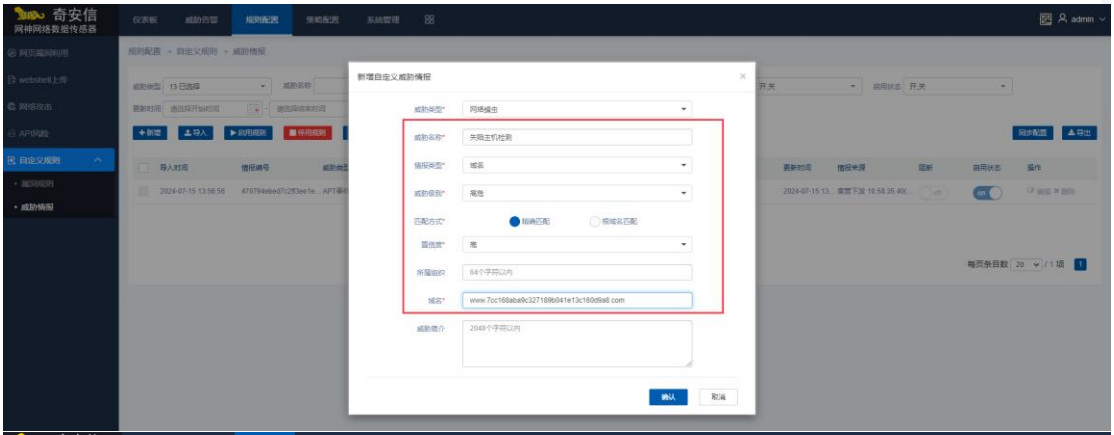
奇安信网神威胁监测与分析系统支持非 TCP 完整流、畸形包检测、数据包完整性检测、IP 碎片攻击检测、编码绕过检测、高级逃逸 AET 检测等防逃逸检测能力。

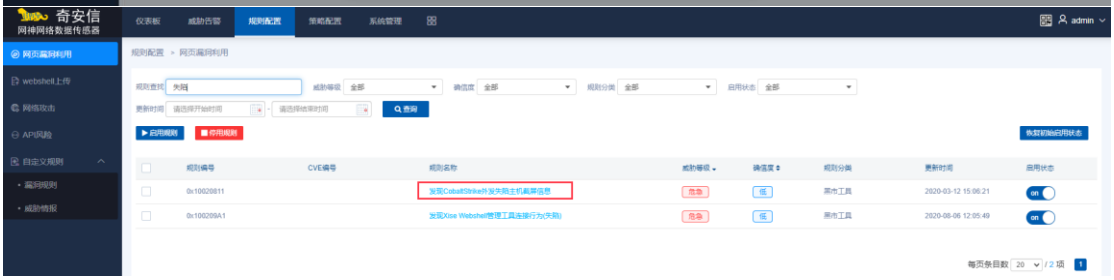


2.3.4 失陷主机检测

奇安信网神威胁监测与分析系统支持根据威胁情报、检测规则、用户配置数据，来检测失陷主机通信活动行为。

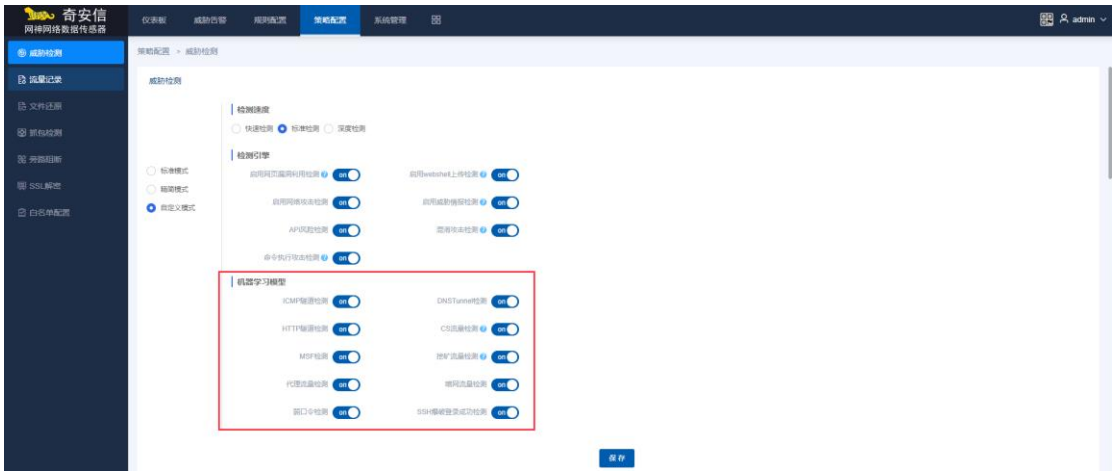

失陷主机通信行为
搜索
IP
域名
URI
198.19.0.64
cloud.bank...fchina.com
192.168.253.1
10.95.35.178
192.168.10.3
192.168.253.129
101.43.16.98
172.24.193.21
257.9.99.174
详细信息
未选中节点


奇安信
网神网络数据传感器
仪表板
威胁告警
规则配置
策略配置
系统管理
admin
新增自定义威胁情报
威胁类型*
网络攻击
威胁名称*
失陷主机检测
情报类型*
域名
威胁级别*
高危
匹配方式*
精确匹配
模糊匹配
置信度*
高
所属组织
64个字符以内
域名*
www.7cc168aba9c327189b041e13c160d9a8.com
威胁简介
2048个字符以内
确认
取消


奇安信
网神网络数据传感器
仪表板
威胁告警
规则配置
策略配置
系统管理
admin
网页篡改利用
webshell上传
网络攻击
API风险
自定义规则
漏洞规则
威胁情报
规则配置 > 网页篡改利用
失陷
查询
启用规则
停用规则
恢复初始启用状态
规则编号
CVE编号
规则名称
威胁等级
置信度
规则分类
更新时间
启用状态
0x10020811
发现CobaltStrike外发失陷主机扇降信息
危急
低
黑市工具
2020-03-12 15:06:21
on
0x100209A1
发现Xise Webshell管理工具连接行为(失陷)
危急
低
黑市工具
2020-08-06 12:05:49
on
每页条目数 20 / 2 项

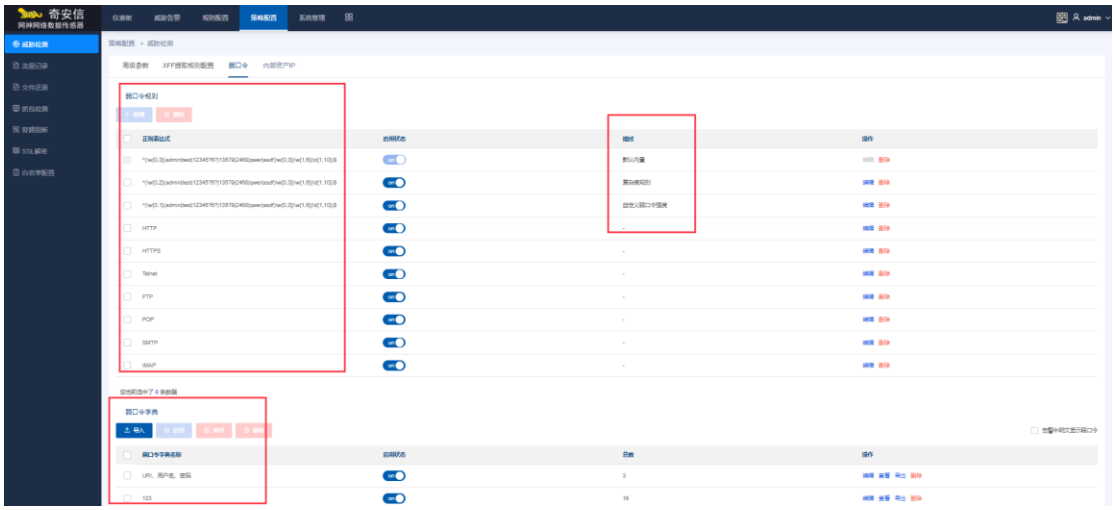
2.3.5 隐蔽信道检测

奇安信网神威胁监测与分析系统支持 DNS 隧道、HTTP 隧道、ICMP 隧道等常见隐蔽信道通信的检测。

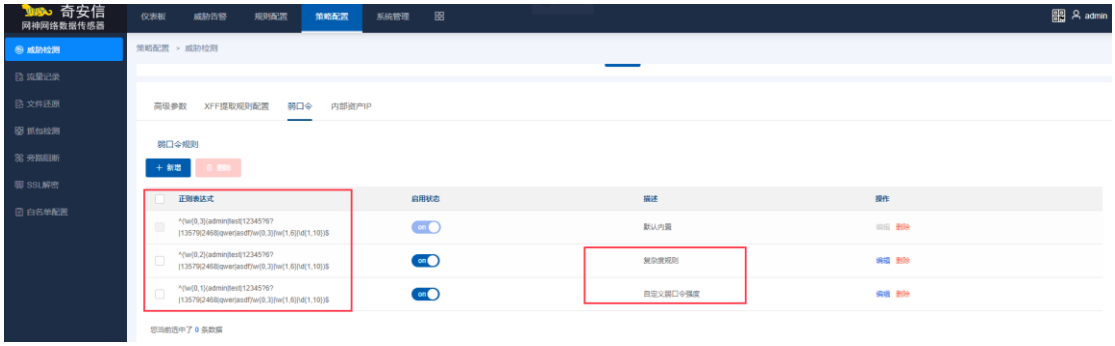


2.3.6 弱口令检测

奇安信网神威胁监测与分析系统支持自定义弱口令字典，支持 HTTP、HTTPS、SMB、Telnet、FTP、POP、SMTP、IMAP 等协议的自定义弱口令检测。

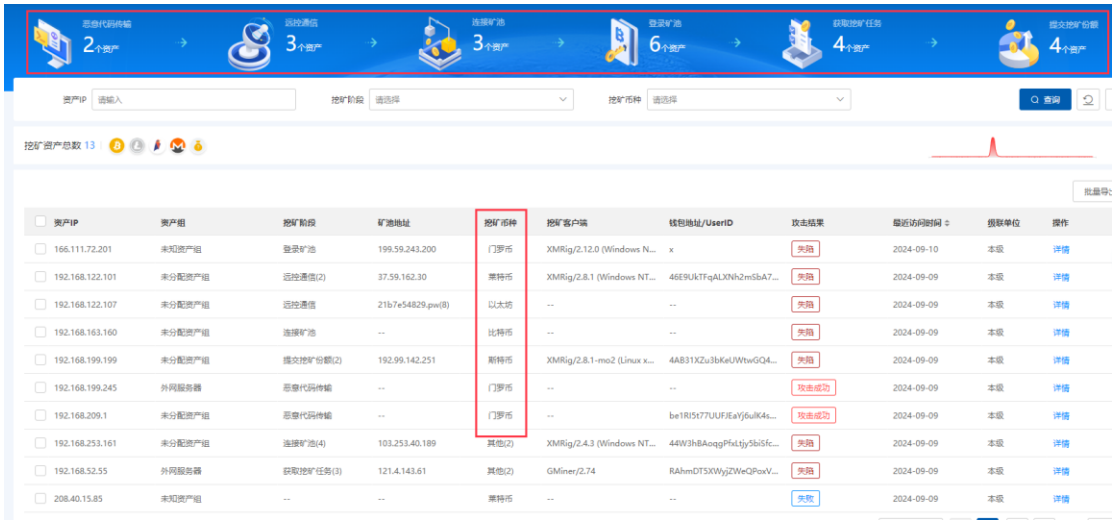


奇安信网神威胁监测与分析系统支持自定义弱口令规则，支持正则表达式方式自定义弱口令强度、复杂度规则。支持配置多条弱口令检测的正则表达式。



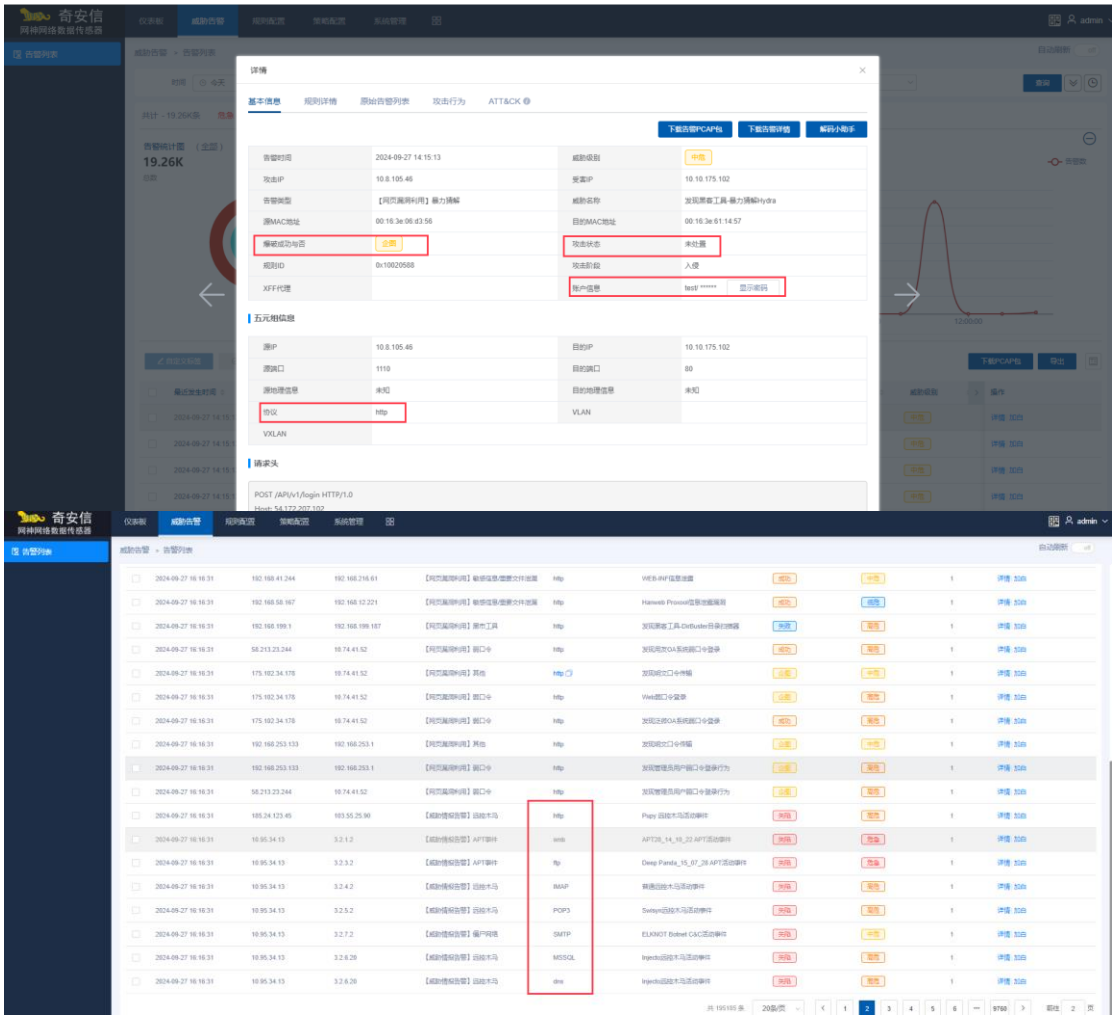
2.3.7 挖矿检测

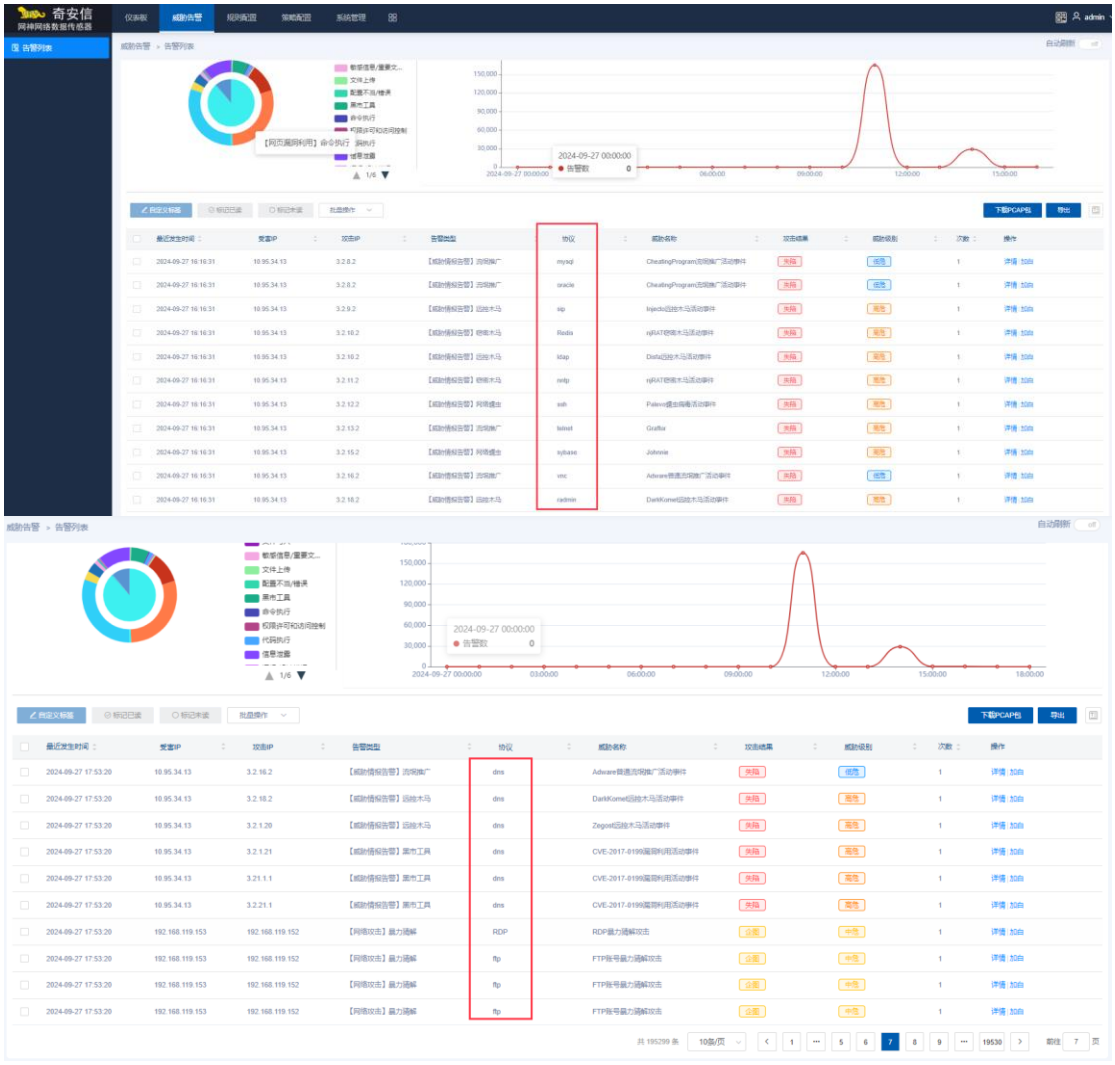
奇安信网神威胁监测与分析系统支持门罗币、莱特币、以太坊、比特币、斯特币等二十余种币种的检测，区分挖矿行为阶段：恶意代码传输、远控通信、连接矿池、登录矿池、获取挖矿任务、提交挖矿份额。

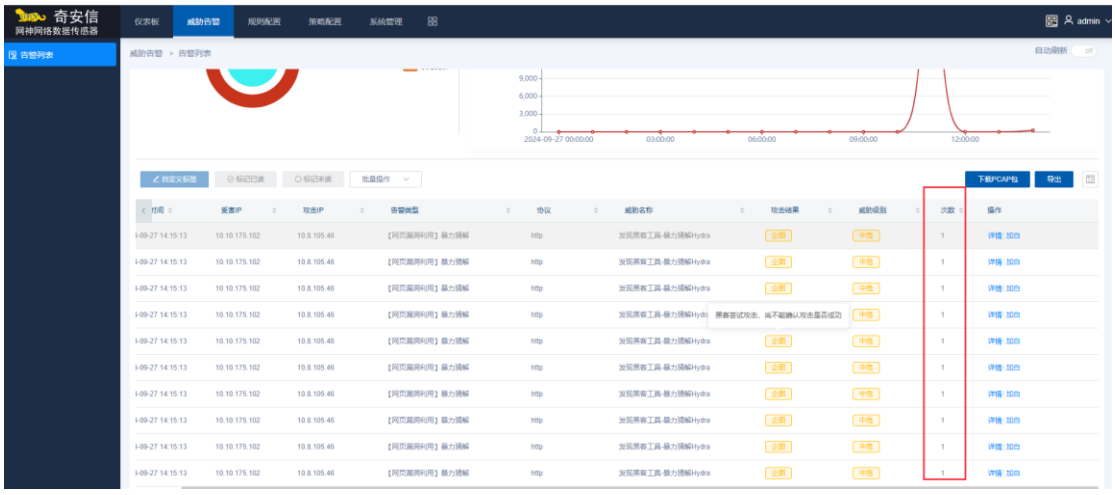


2.3.8 暴力猜解检测

奇安信网神威胁监测与分析系统支持 HTTP、SMB、FTP、IMAP、POP3、SMTP、MSSql、Mysql、Oracle、Sip 、Redis 、Ldap 、Nntp 、SSH、Telnet、Sybase 、VNC、RADMIN、RDP 等协议暴力破解检测，能识别出尝试登录次数、账户信息、爆破成功与否的攻击状态。


奇安信
网神网络数据传感器
详情
基本信息
规则详情
原始告警列表
攻击行为
ATT&CK
下载告警PCAP包
下载告警详情
解码小助手
五元组信息
请求头
POST /API/v1/login HTTP/1.0
威胁告警
规则配置
策略配置
系统管理
admin





2.3.9 黑客工具检测

奇安信网神威胁监测与分析系统支持 deimos，merlin，viper，silver 等黑客工具的检测。

2.4 流量数据和威胁数据外发能力

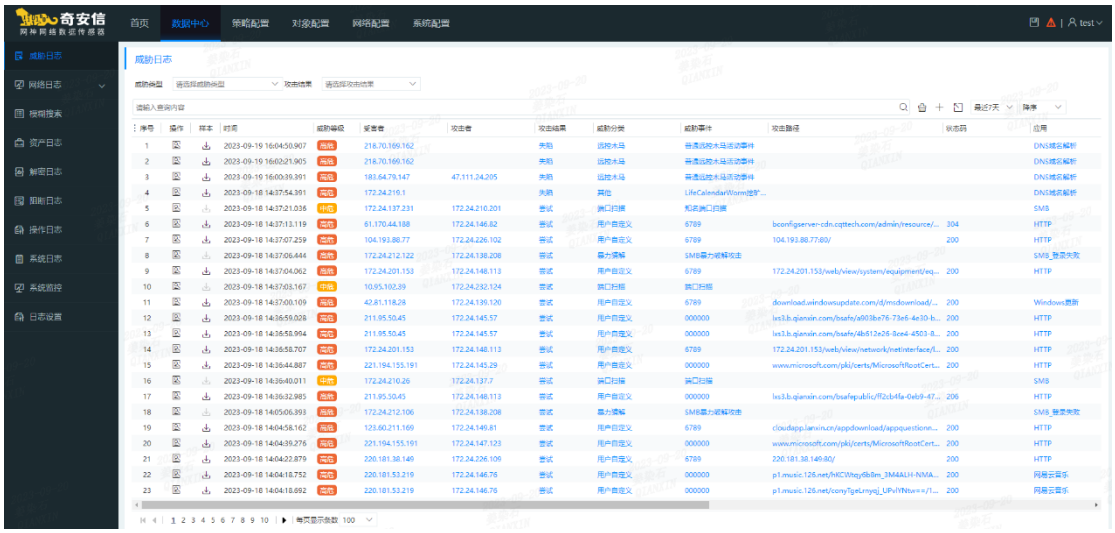
2.4.1 支持流量数据和威胁数据上传到多种分析平台

威胁日志和流量日志支持上传到态势感知平台、NGSOC 分析平台、大数据分析平台和 Syslog 服务器等多种分析平台。

2.4.1.1 日志上传安全态势感知平台

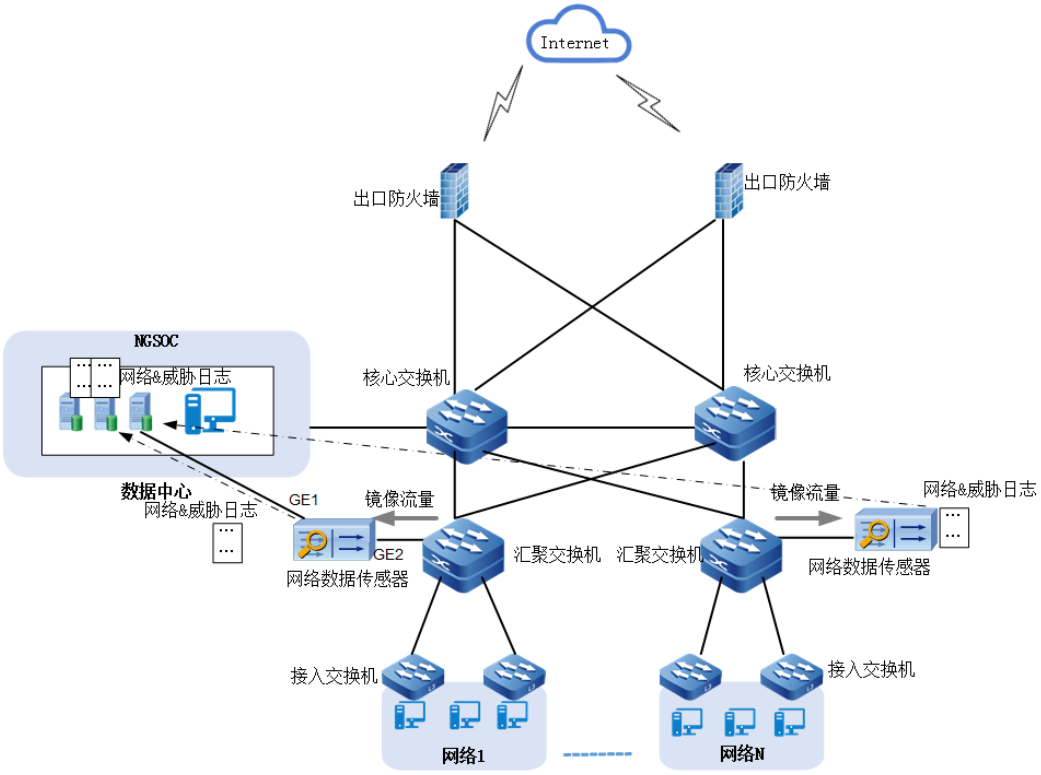
奇安信网神公司安全态势感知平台，是面向政府、金融、能源等大中型企事业单位的综合安全事件分析与全局安全态势感知系统。

该系统基于奇安信网神公司云端威胁情报和多种流量采集设备包括奇安信网神威胁监测与分析系统收集到的各单位本地安全大数据，通过对海量数据进行多维度快速、自动化的关联分析发现本地的威胁和异常行为，并及时与终端管理系统和下一代防火墙进行联动，对威胁和异常行为进行处置。同时，系统可通过图形化、可视化技术将这些威胁和异常的总体安全态势用最直观的方式展现给用户，有利于业务管理者迅速做出判断和决策。



奇安信网神威胁监测与分析系统作为态势感知平台的组成部分，通过在网络的关键节点部署奇安信网神威胁监测与分析系统，采集整个网络的网络日志和威胁日志，并将网络日志、威胁日志以及相关联的 pcap 上传到态势感知平台。

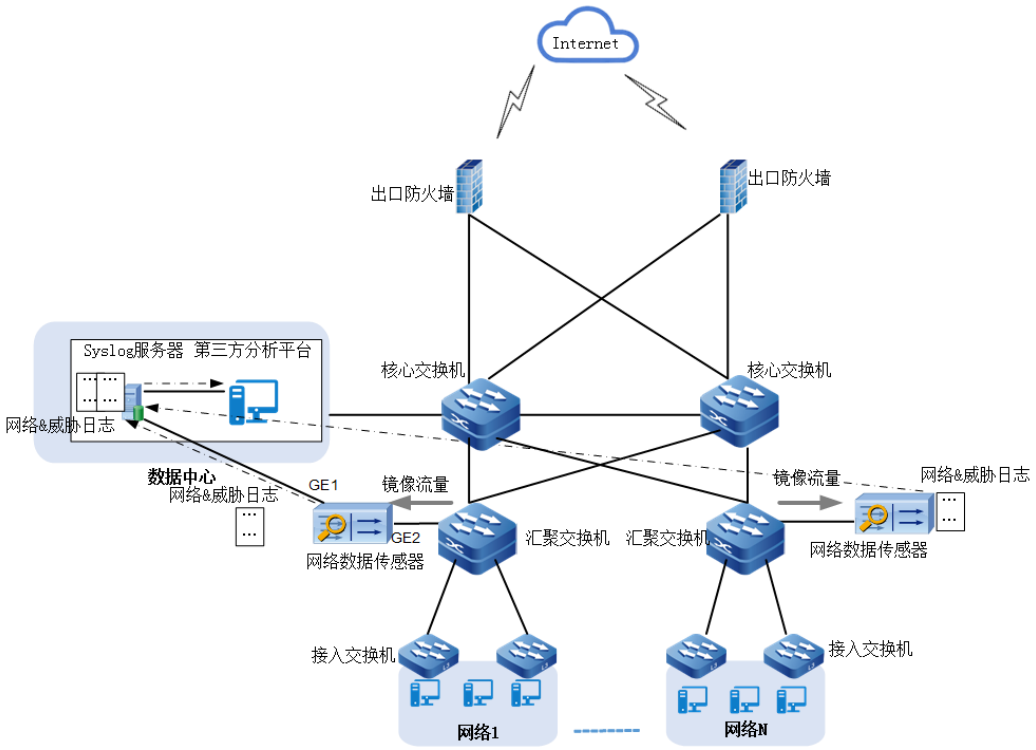
图2-1 奇安信网神威胁监测与分析系统作为态势感知平台的流量采集器



2.4.1.2 日志上传 SYSLOG 服务器

奇安信网神威胁监测与分析系统采集的网络日志和流量日志可以发送给 SYSLOG 服务器，作为内网安全数据供第三方分析平台使用，发送协议可使用 TCP 协议或 UDP 协议。

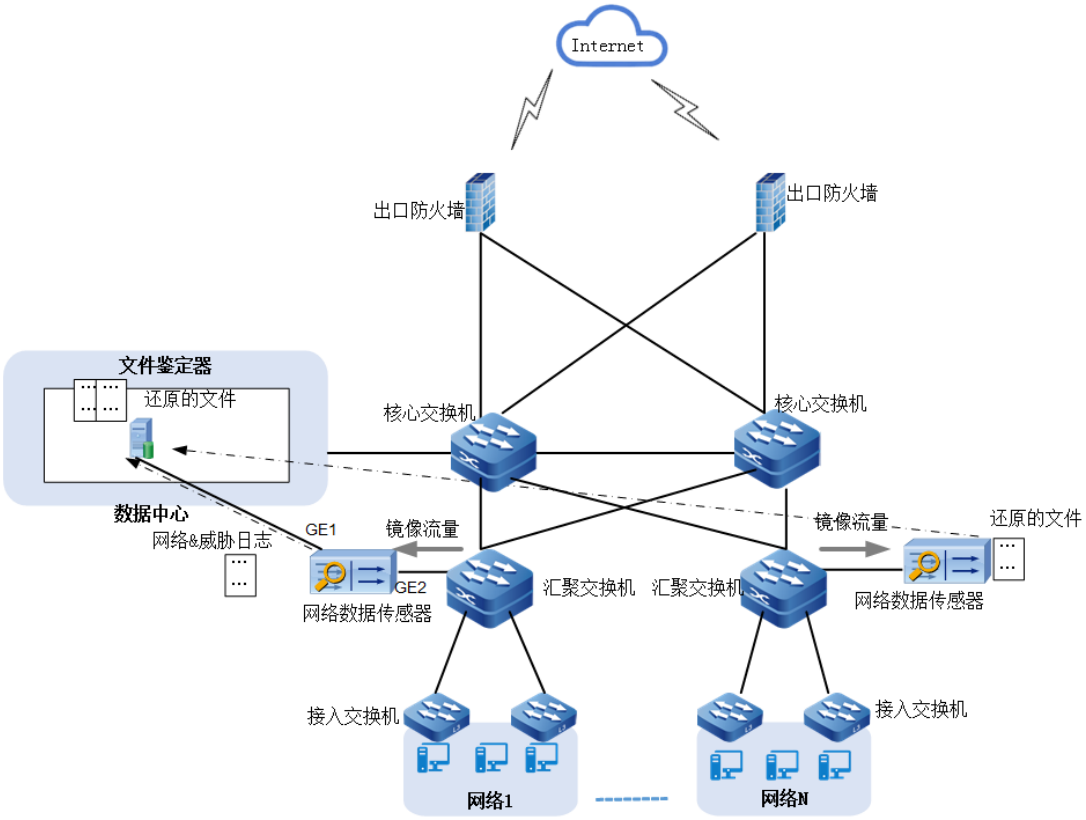
图2-2 奇安信网神威胁监测与分析系统发送日志到 SYSLOG 服务器



2.4.1.3 还原的文件上传至文件鉴定器

用户网络中在出口交换机上部署了奇安信网神威胁监测与分析系统，交换机接口流量直接镜像到奇安信网神威胁监测与分析系统的数据接收接口，按照配置的数据采集策略和引用的文件还原规则对可疑文件进行文件还原。将还原后的文件上传到文件鉴定器进行威胁检测，文件鉴定器会将检测结果上传到分析平台进行分析。

图2-3 还原后的文件上传文件鉴定器



2.4.2 数据外发策略支持对接平台负载均衡

数据外发策略向态势感知平台、NGSOC 分析平台、大数据分析平台发送数据时，支持多服务器负载均衡，可以添加多个 IP 地址。数据自动通过轮询算法发送到不同的服务器上。

2.4.3 支持流量还原文件发送到文件威胁鉴定器

奇安信网神威胁监测与分析系统支持对匹配规则的可疑文件进行文件还原。还原后的文件可以发送到文件威胁鉴定器进行威胁鉴定。支持基于应用和文件类型进行文件还原，应用的范围支持常用的 FTP、HTTP、SMTP、POP3、IMAP、SMB 协议，以及多种常用的即时通讯、论坛、博客、文件共享、网页邮件。

2.4.4 支持威胁样本外发

奇安信网神威胁监测与分析系统支持威胁样本外发策略，网络攻击、网页漏洞利用、威胁情报 PCAP 类型样本和恶意文件样本可以通过 FTP 或 SFTP 方式上传给对端 FTP 或 SFTP 服务器，外发必须设置好服务器地址、端口和用户名、密码参数。

2.4.5 支持自定义多场景日志外发

奇安信网神威胁监测与分析系统支持多种场景的探针日志外发，包含但不限于将日志字段全量外发、外发最小必要的字段，基于运营经验自行配置日志外发字段、非加密传输增加传输性能、根据需求自定义外发日志类型，适应不同应用场景需求。

2.5 资产自动发现能力

奇安信网神威胁监测与分析系统支持资产自动发现能力。镜像到奇安信网神威胁监测与分析系统的流量通过内置的资产识别规则进行资产规则匹配，从而自动识别资产，对重要资产进行监控。

2.6 异常数据抓包能力

奇安信网神威胁监测与分析系统支持数据抓包策略，可以基于 IP 地址、数据方向、应用、URL 进行异常流量抓包。抓包文件可以下载到用户本地进行异常分析。

奇安信网神威胁监测与分析系统具有全流量采集功能，通过全流量采集功能，收集设备的全部流量，采用定时自动的方式传送到服务器端，做到更好的证据留存。

2.7 加密数据检测能力

奇安信网神威胁监测与分析系统支持基于源地址、目的地址对 SMTPS、POP3S、IMAPS、HTTPS 应用类型进行 SSL 解密，然后对解密后的策略进行流量还原和威胁检测，生成威胁日志。

2.8 旁路阻断能力

奇安信网神威胁监测与分析系统支持基于 IPv4 地址和 IPv6 地址的 IP 进行旁路阻断。基于 URL、DNS 进行重定向，在进行流量还原和威胁采集前进行阻断和重定向，可以提高流量还原和威胁采集的能力。

奇安信网神威胁监测与分析系统支持以旁路方式部署在数据链路中，不影响网络结构。支持通过流量镜像的方式获取安全数据，通过被动指纹识别技术和浏览器识别技术，并根据资产识别的条件进行流量分析及应用检测，识别出网络中资产信息。

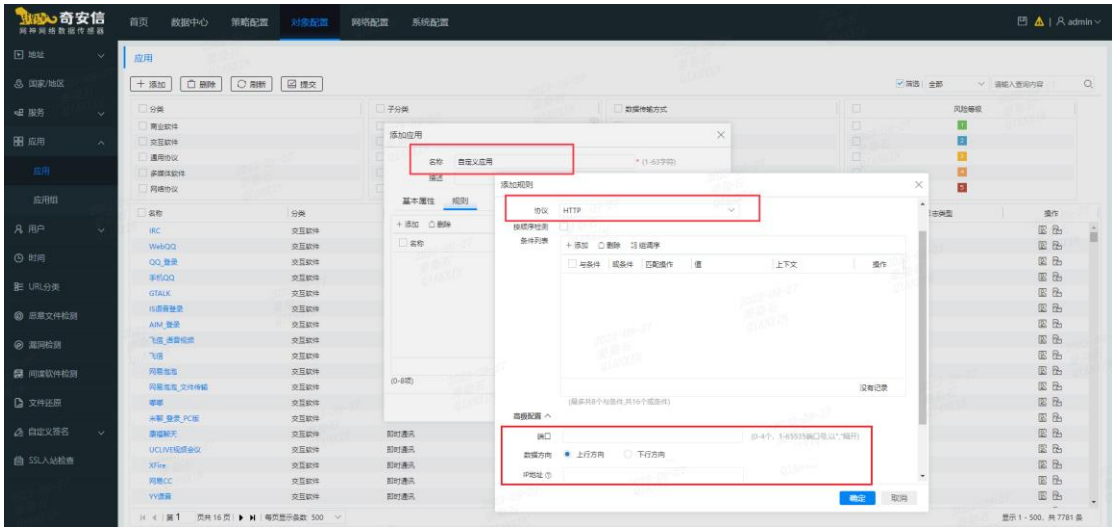
2.9 自定义解码能力

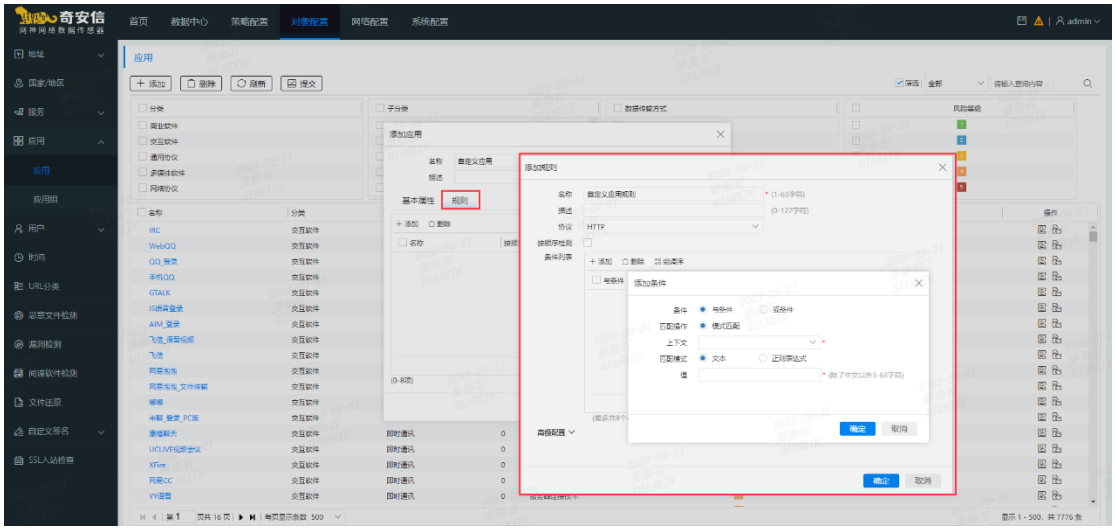
奇安信网神威胁监测与分析系统支持自定义解码能力，按照解码规则提取数据流中的信息，填充到预定义/自定义的字段中，输出带有自定义字段的预定义日志/定制日志/登录日志，提高探针原有的解码能力，增强数据运营能力。

2.10 策略配置

2.10.1 自定义规则

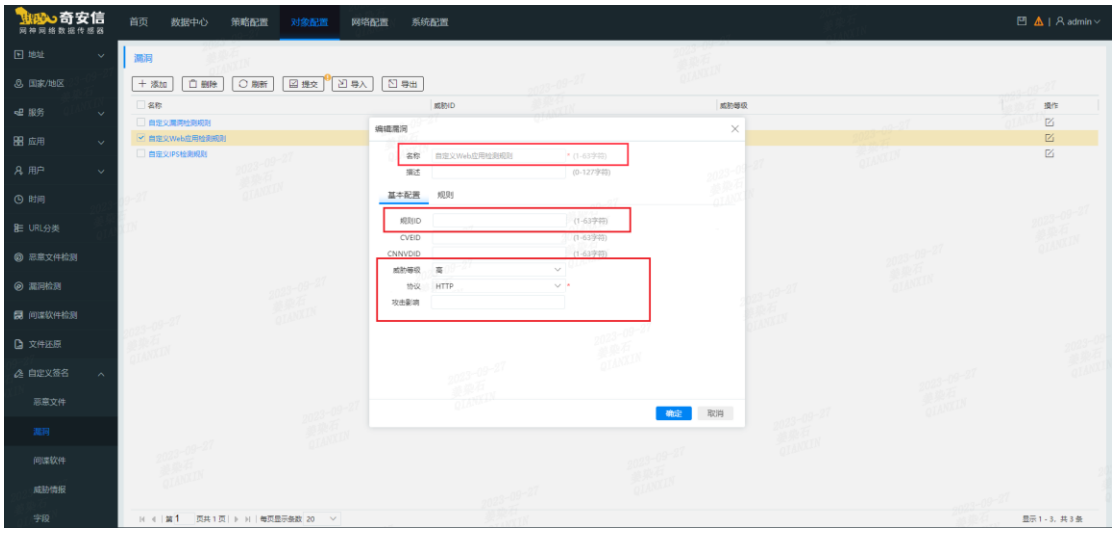
奇安信网神威胁监测与分析系统支持根据数据包方向、协议、端口、IP 地址等信息自定义应用规则来识别应用类型。



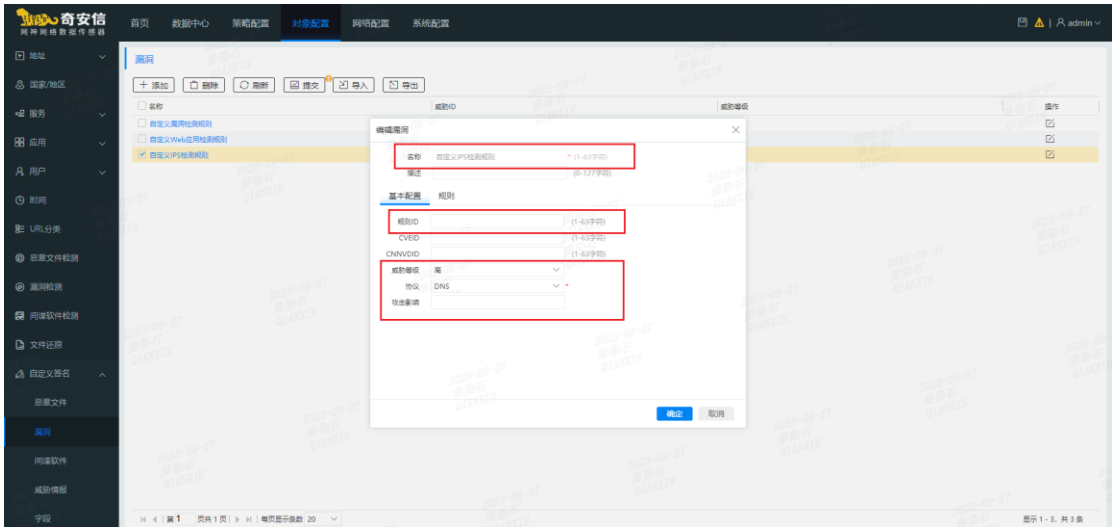


奇安信网神威胁监测与分析系统支持通过规则 ID、名称、攻击影响、威胁等级、字符串、正则表达式及匹配方向来自定义 web 应用检测规则库、自定义 IPS 规则库、及自定义登录规则库。支持自定义内网服务器 IP 组、客户端 IP 组，用于识别资产信息。定义的时间段内不能访问或能访问某服务器。

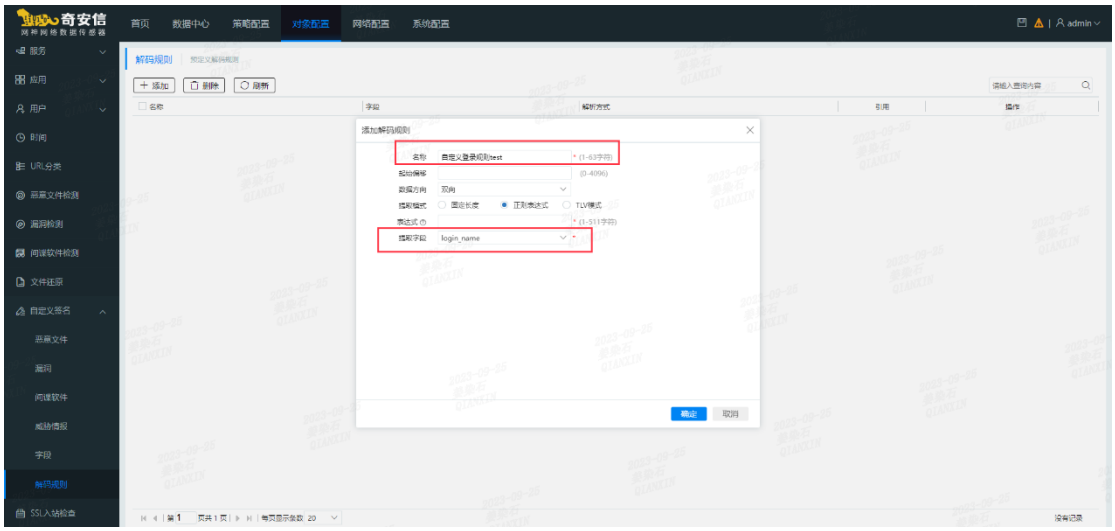
自定义 web 应用检测规则库；



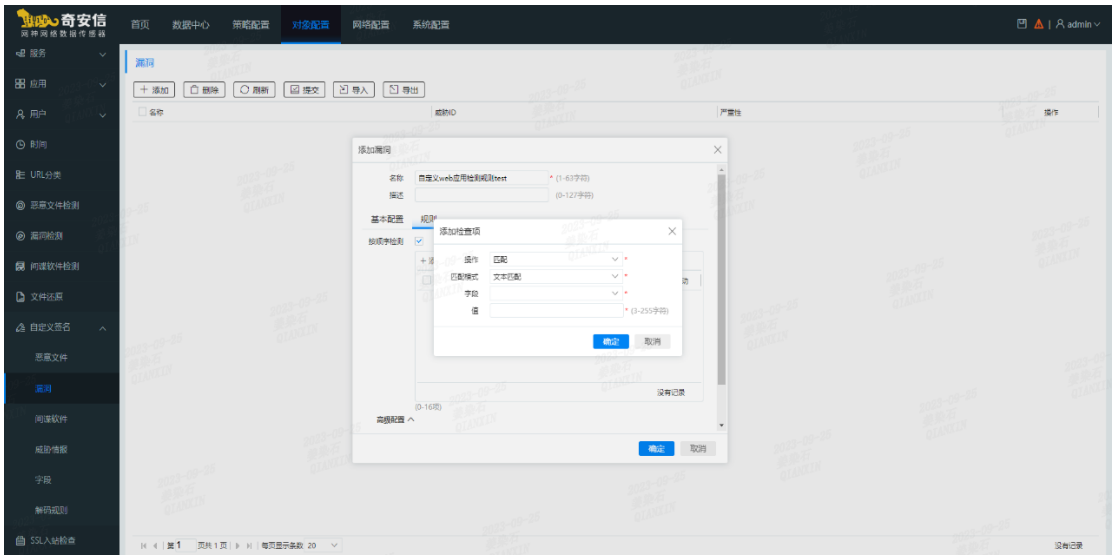
自定义 IPS 规则库；



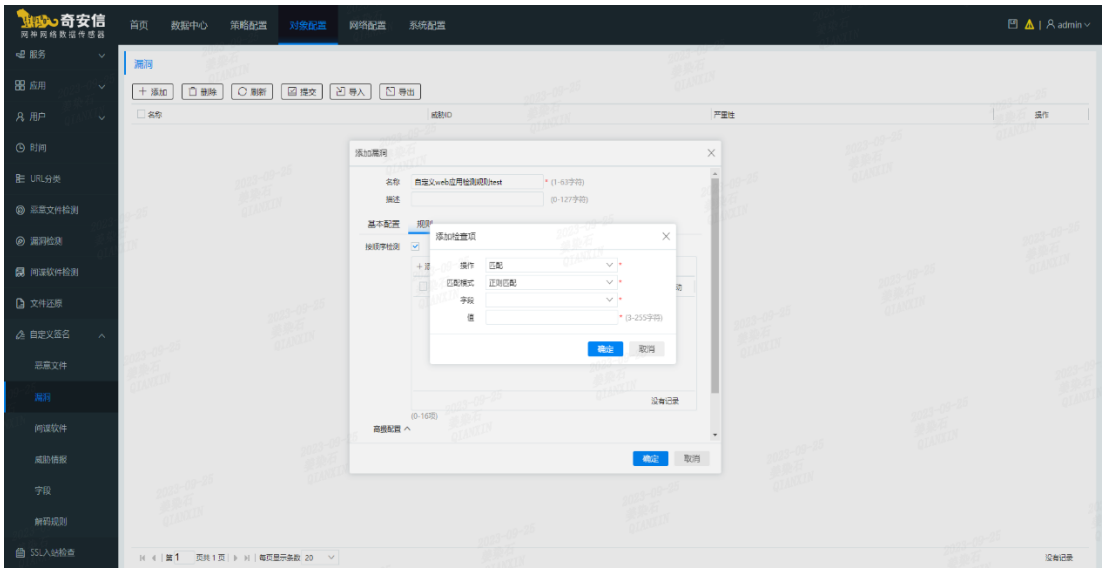
自定义登录规则库；



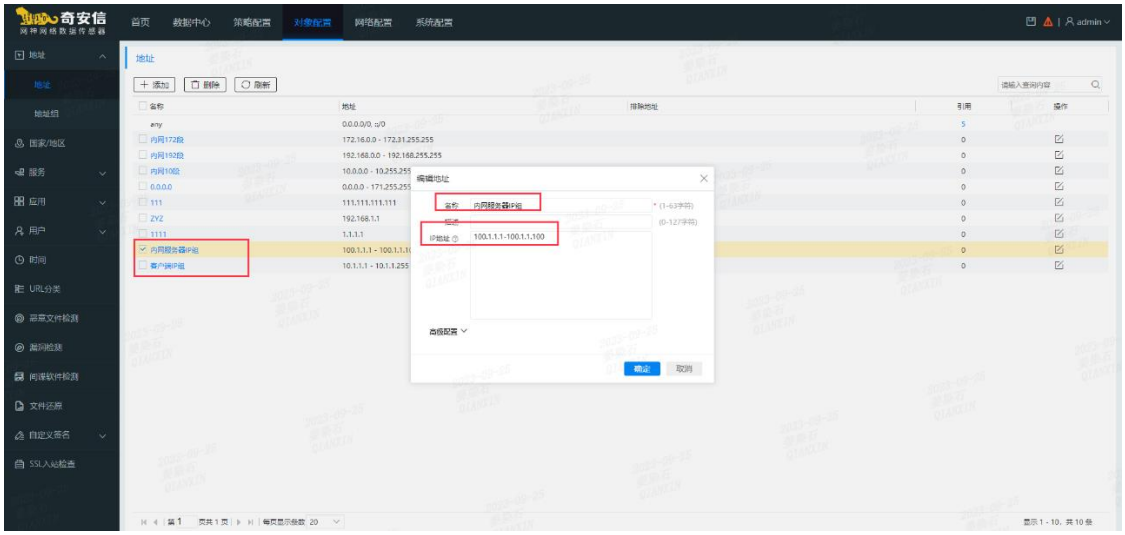
字符串匹配——文本匹配；

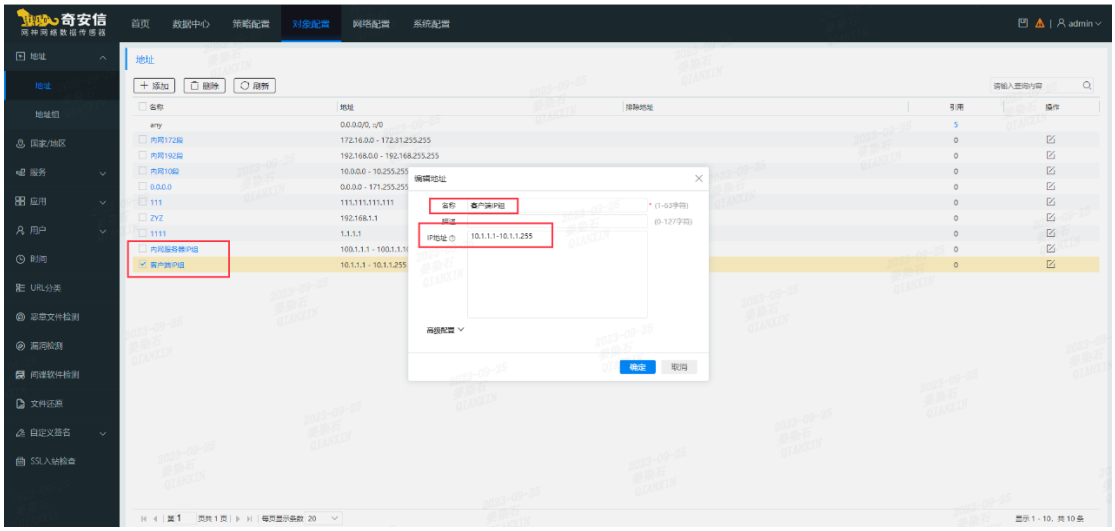


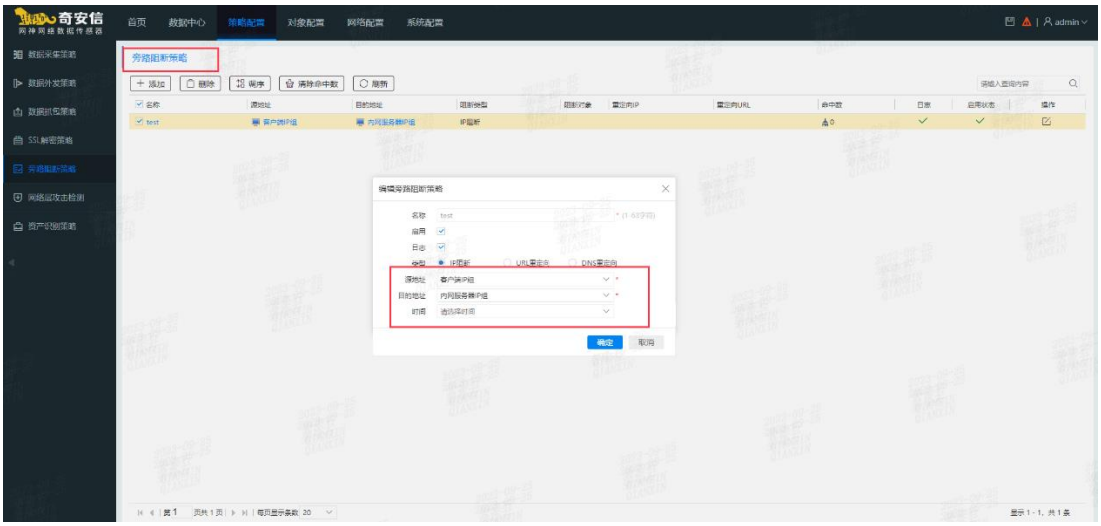
正则匹配；



支持自定义内网服务器 IP 组、客户端 IP 组，用于识别资产信息。定义的时间段内不能访问或能访问某服务器。

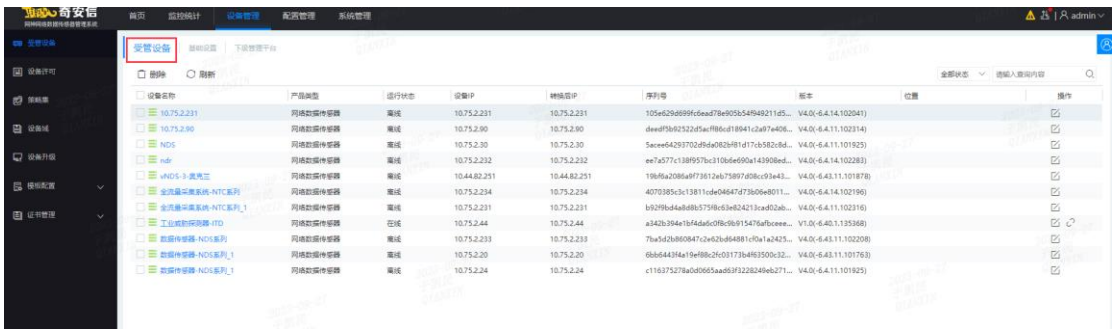




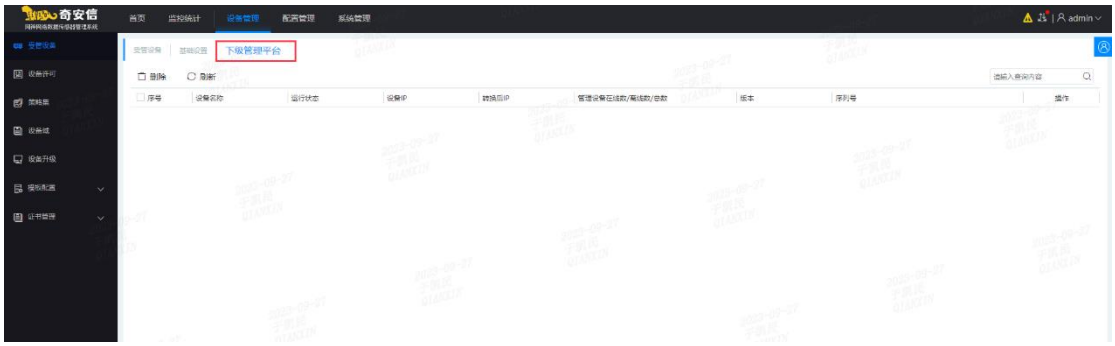


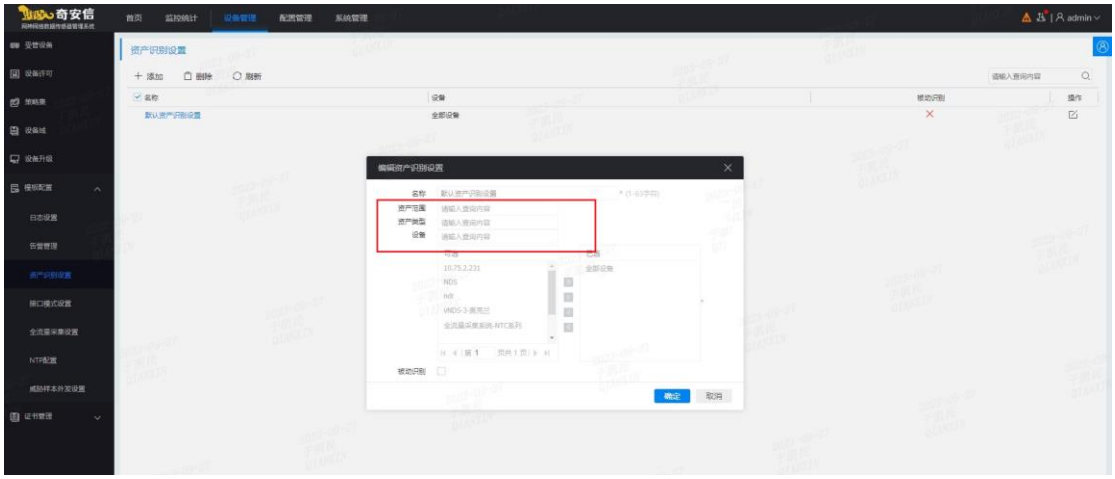
2.10.2 集中管理

奇安信网神威胁监测与分析系统支持设备内置简单命令行管理窗口，便于基础运维调试；可实时监控设备的 CPU、内存、存储空间使用情况；能够监控监听接口的实时流量情况。

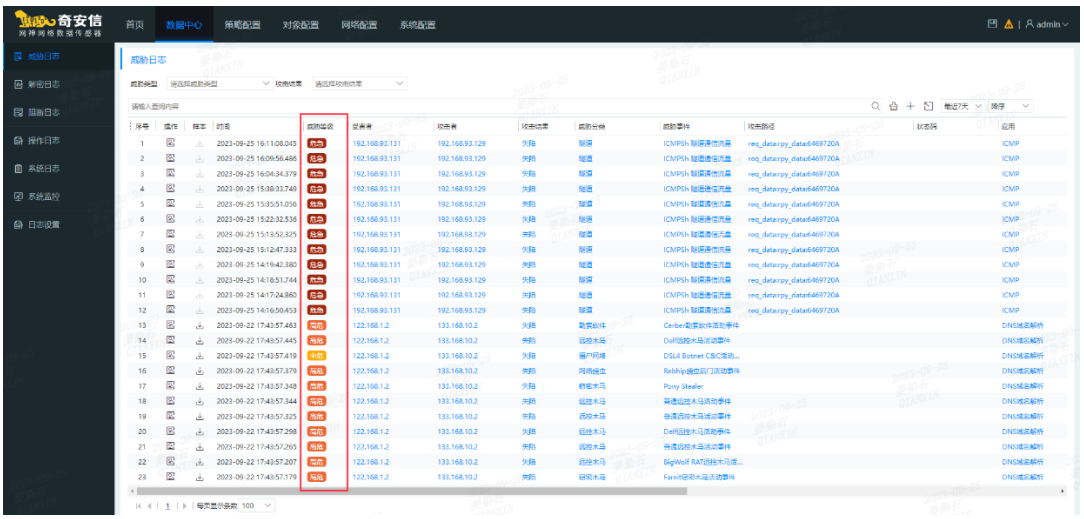


支持级联设置，可支持资产范围和资产类型自定义。

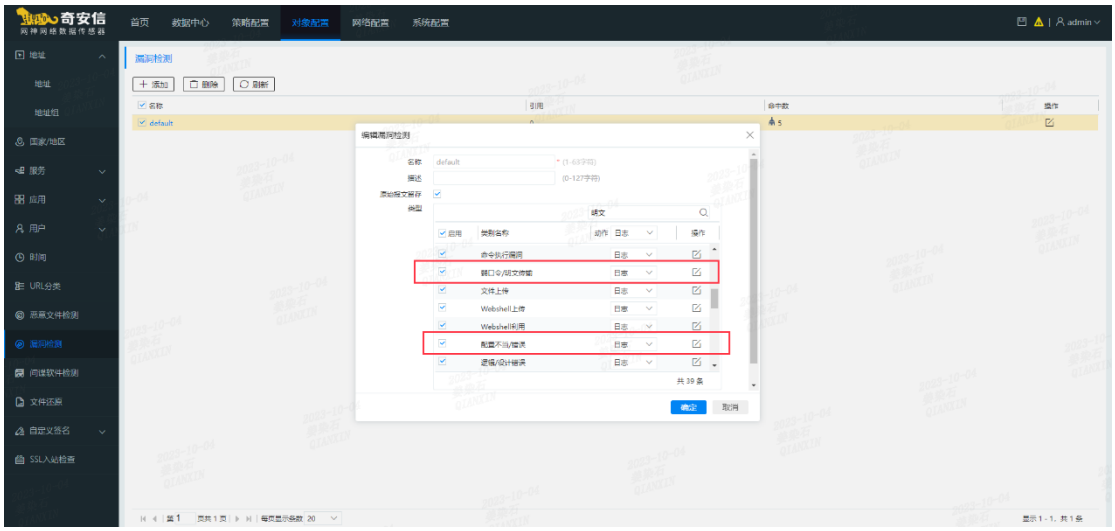




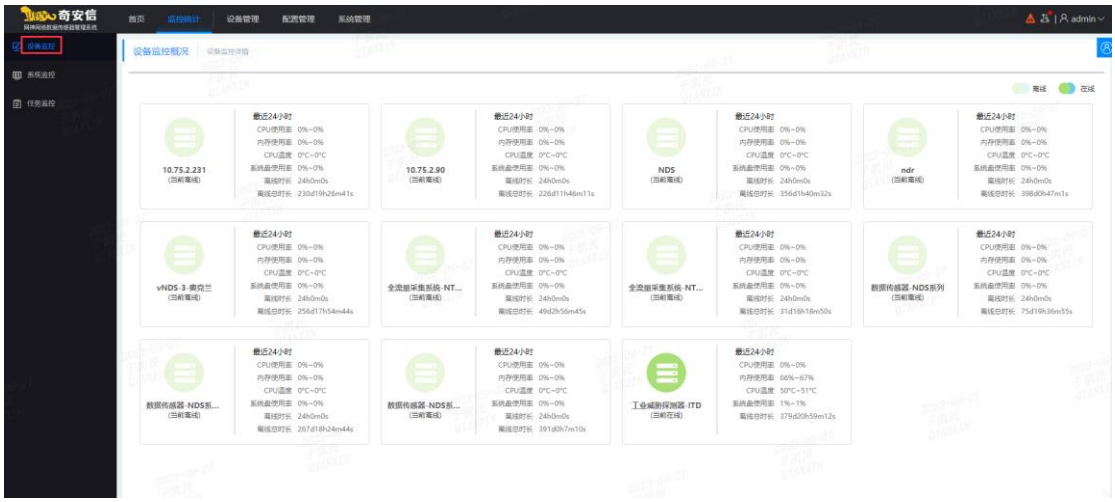
安全事件类型包括高、中、低危方式选择；

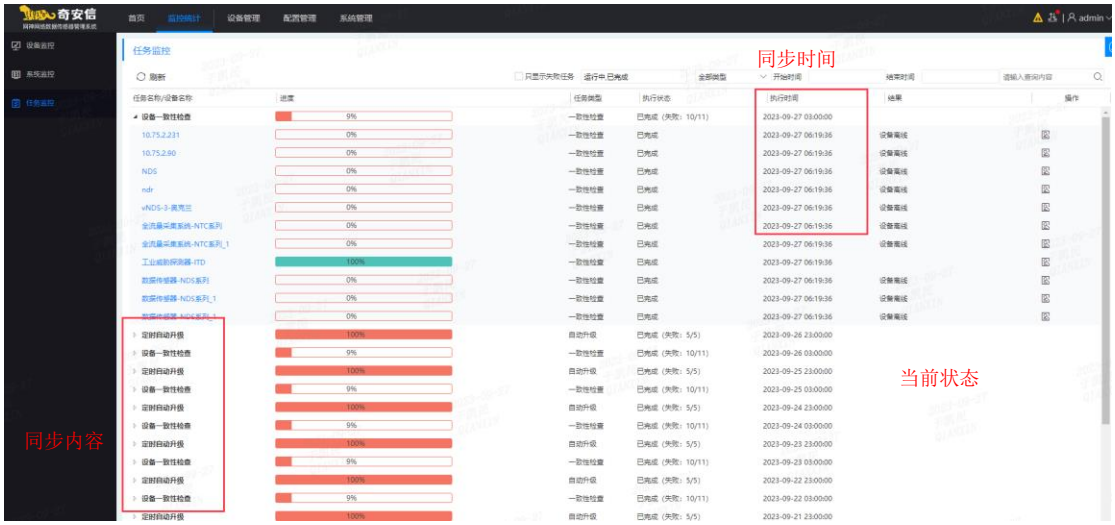


漏洞隐患风险包括漏洞风险、配置风险（不当/错误）、弱密码和明文传输；



支持页面展示平台的当前状态、同步内容、最近同步时间等。

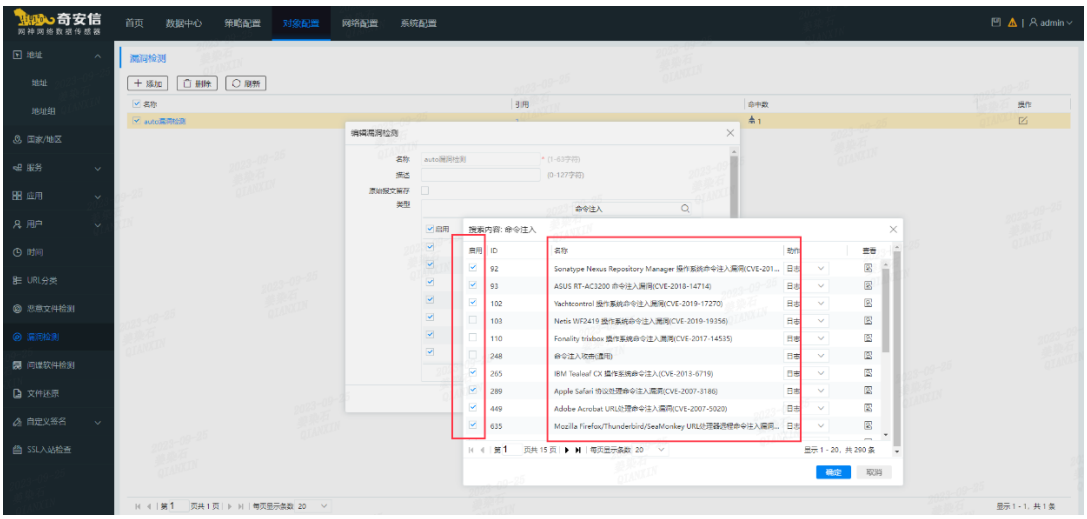




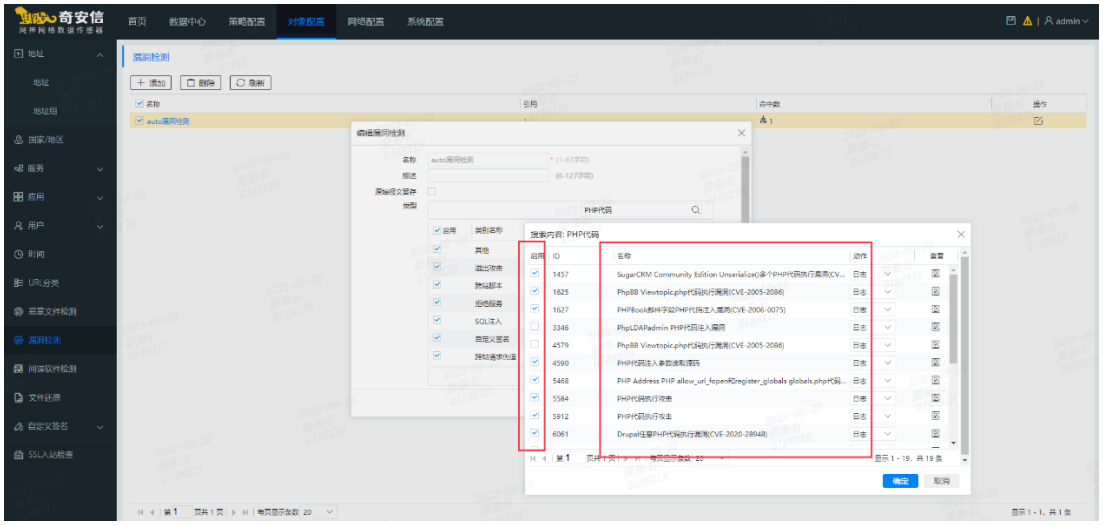
2.10.3 威胁检测子类型及启用开关

奇安信网神威胁监测与分析系统支持对包括 CVE 漏洞库、CNNVD 中国国家信息安全漏洞库中的漏洞和其他自主发现的漏洞，能够实时支持命令注入检测、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。

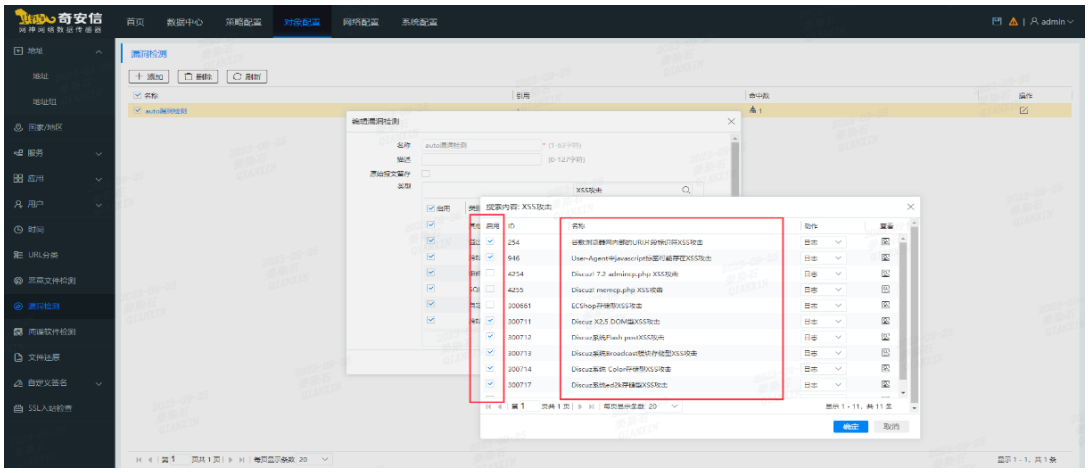
支持命令注入检测；



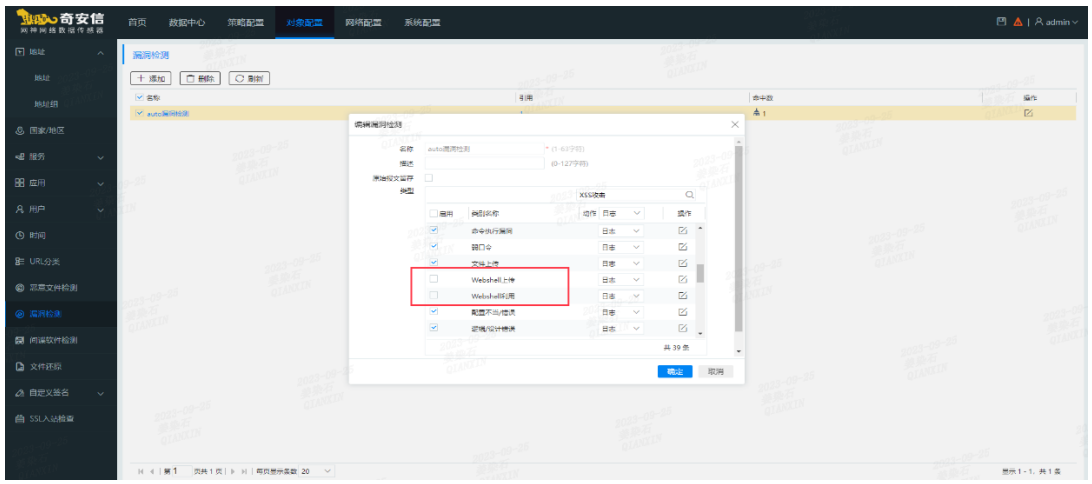
PHP 代码检测；



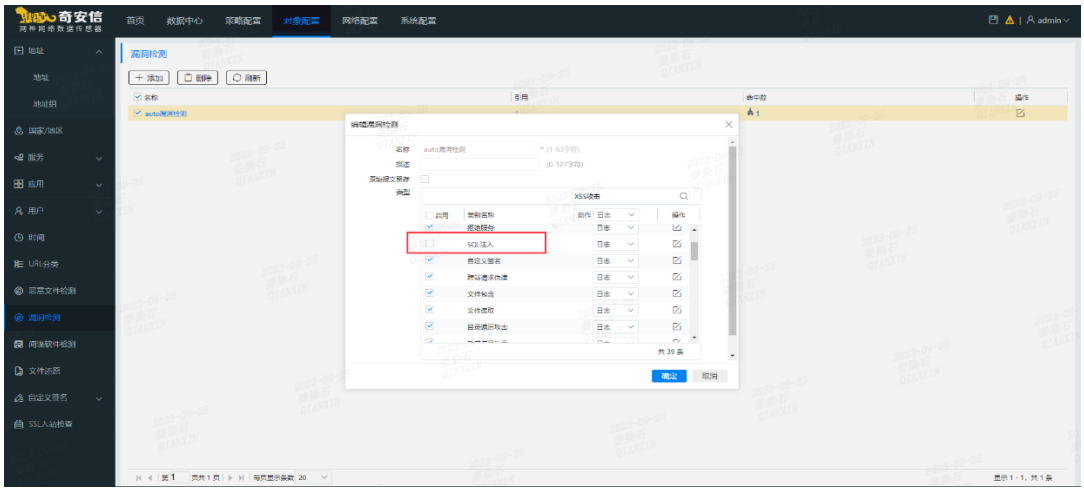
XSS 攻击检测；



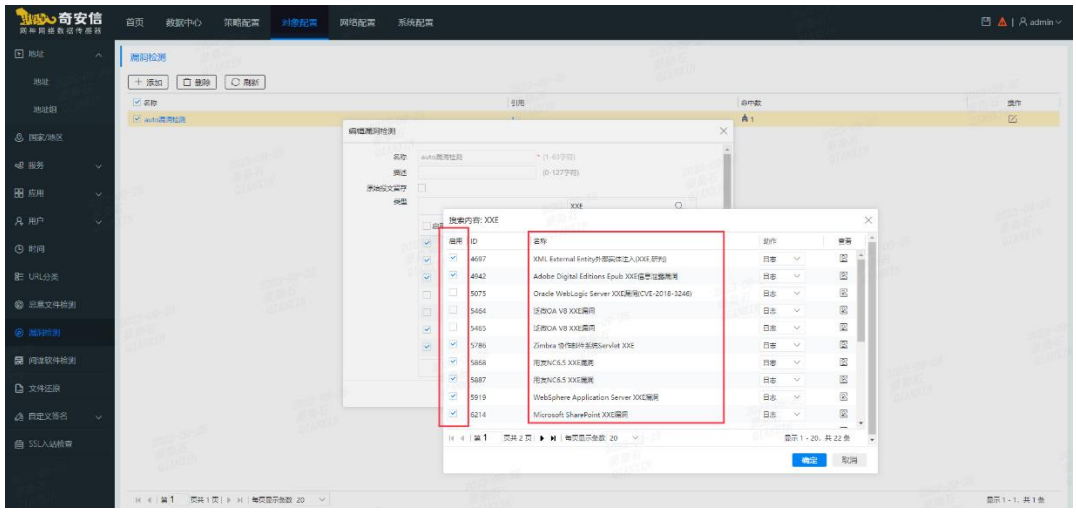
Webshell 上传检测；



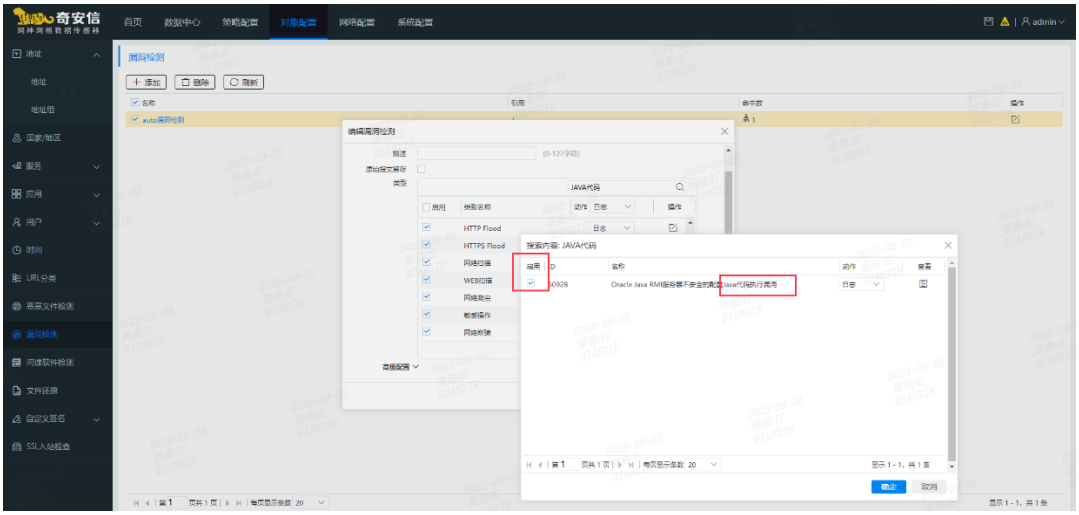
SQL 注入检测；



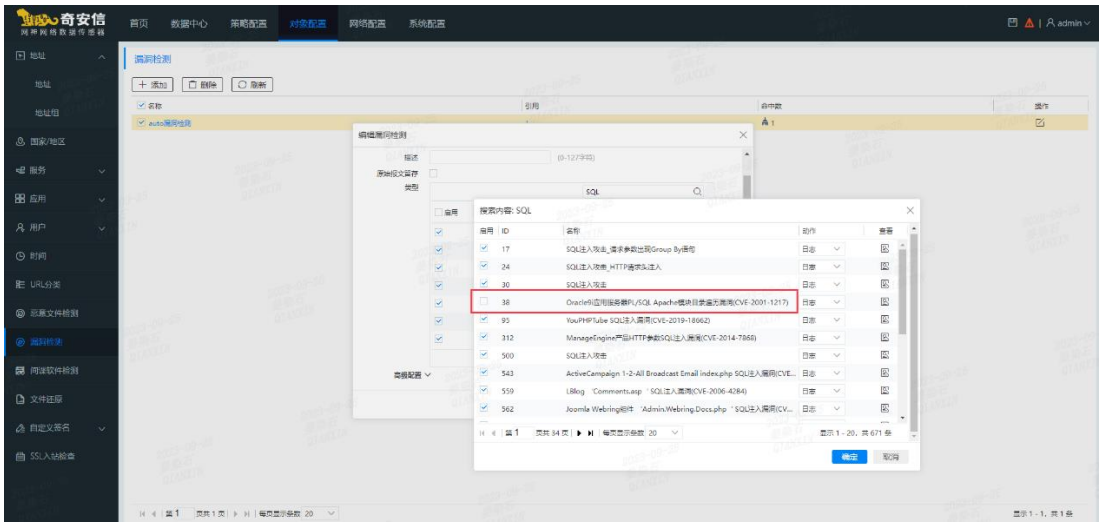
XXE 攻击检测；



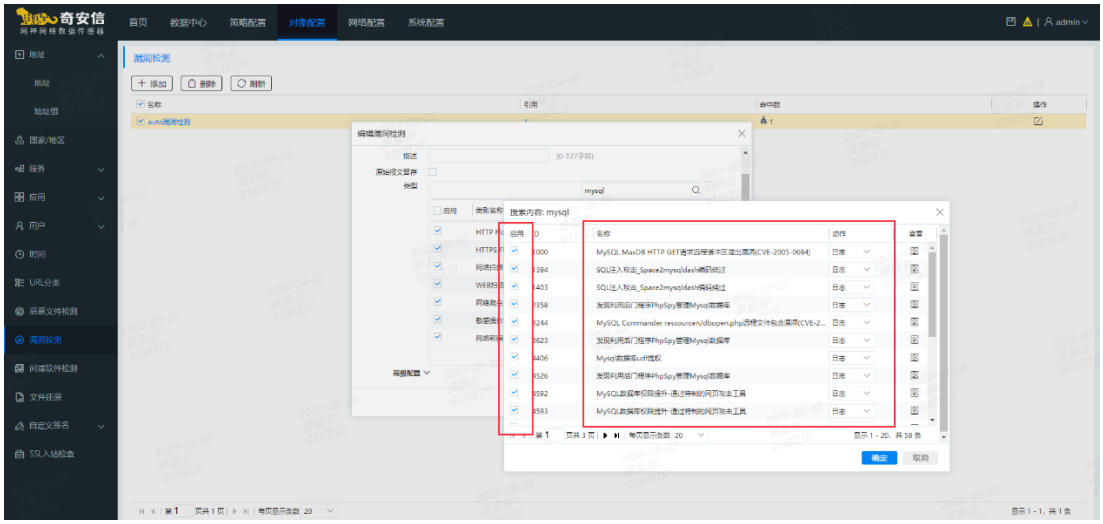
JAVA 代码检测；



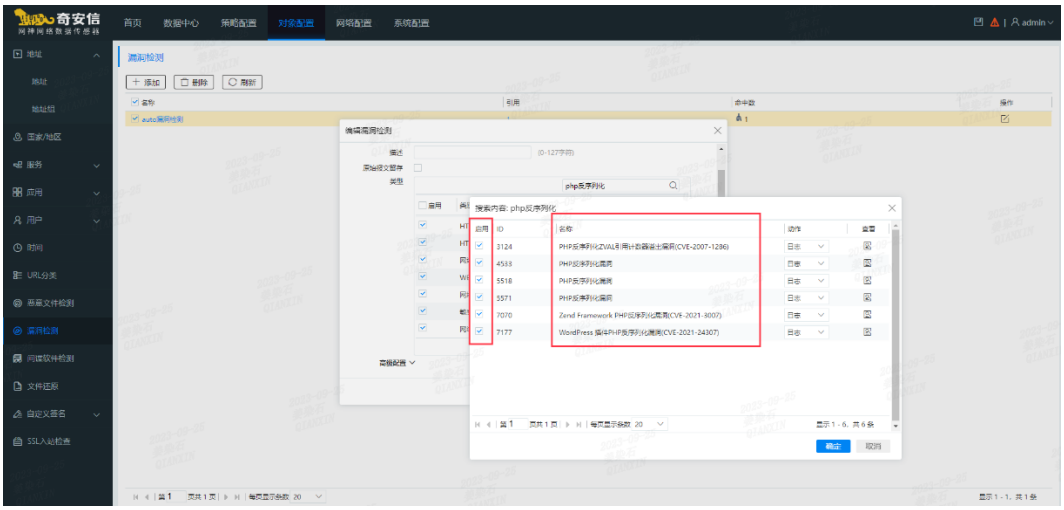
SQL 非注入型检测；



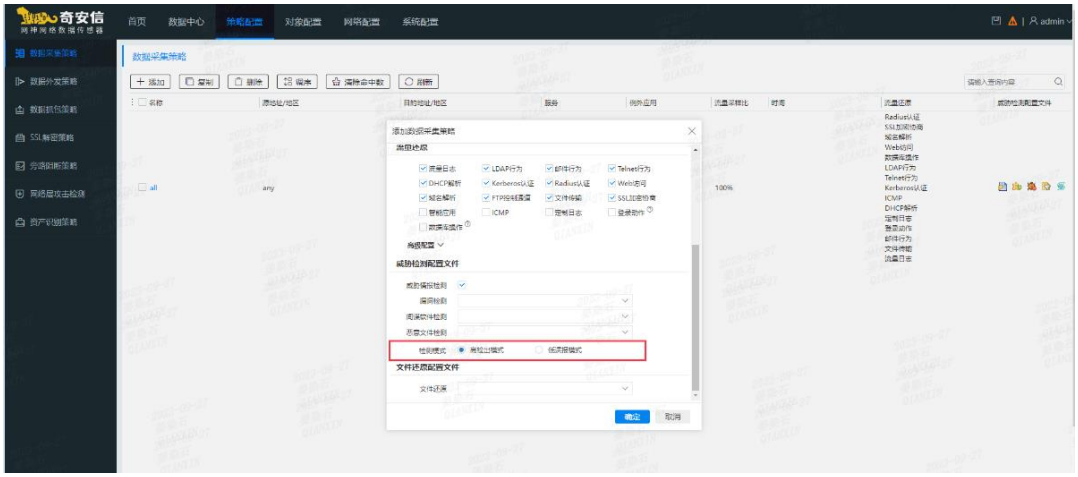
MYSQL 解析增强；



php 反序列化检测；

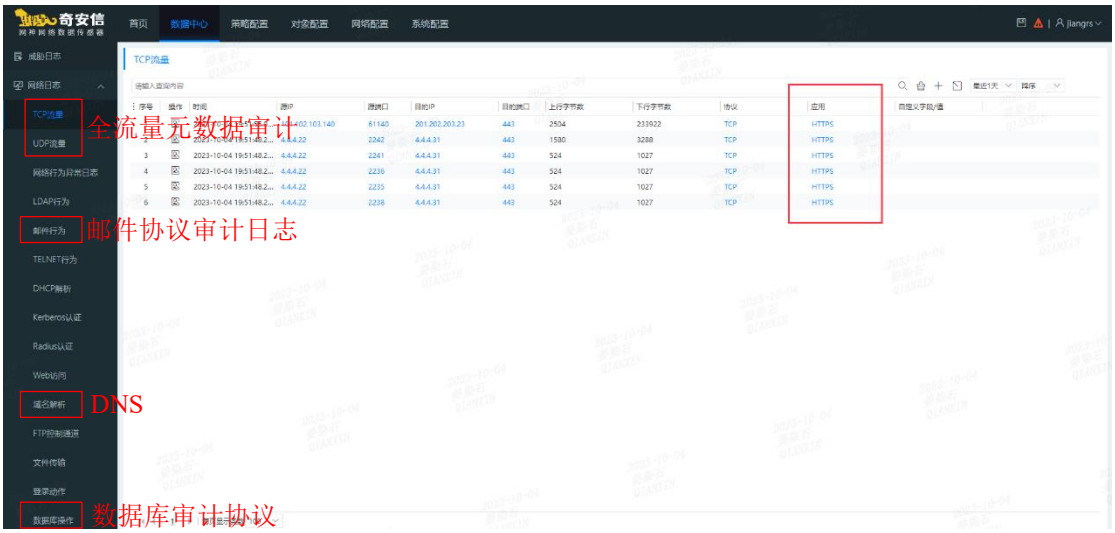


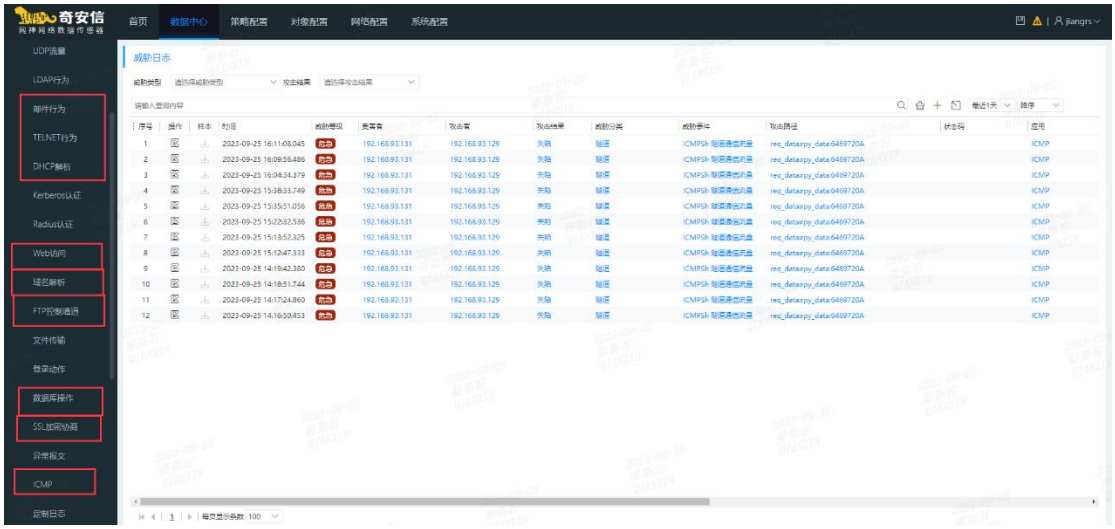
自定义配置启用、新增高检出、低误报模式。

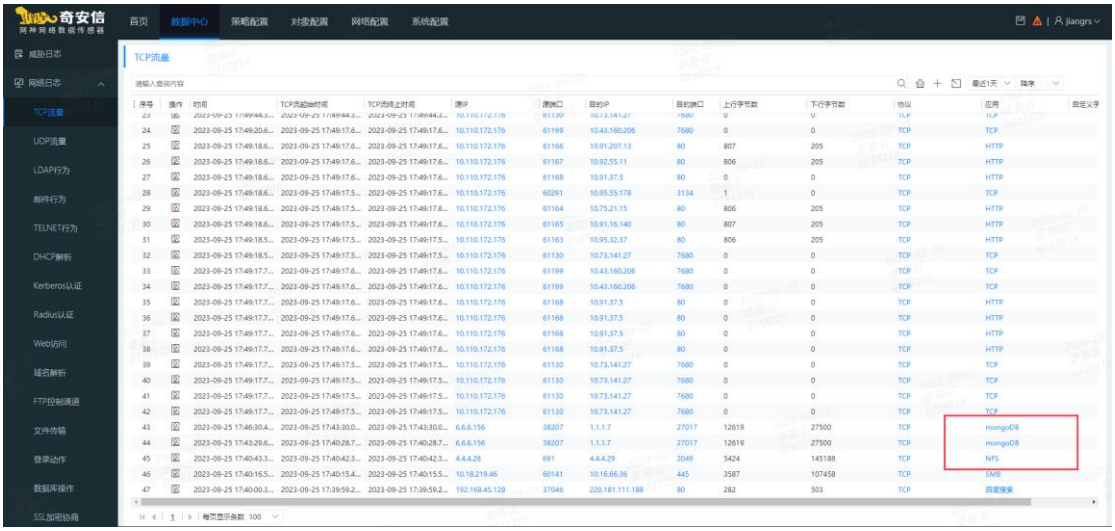


2.10.4 元数据类型

奇安信网神威胁监测与分析系统支持传输协议审计日志，包括https、http、DNS、邮件协议审计日志、SMB、AD 域、WEB 登录、FTP、Telnet、ICMP、TELNET、ICMP 、SNMP 、SSL 、SIP 、ONVIF 、mongo、NFS 、SOCKS 、dhcp、netbios_nbns、全流量元数据审计、数据库审计协议等。






奇安信 网神网络数据传感器
首页
数据中心
策略配置
对象配置
网络配置
系统配置
jiangrs
威胁日志
网络日志
TCP流量
UDP流量
LDAP行为
邮件行为
TELNET行为
DHCP解析
Kerberos认证
Radius认证
Web访问
域名解析
FTP控制通道
文件传输
登录动作
数据库操作
SSL加密协商
TCP流量
请输入查询内容
最近1天
降序
序号
操作
时间
TCP流起始时间
TCP流终止时间
源IP
源端口
目的IP
目的端口
上行字节数
下行字节数
协议
应用
自定义字段
mongoDB
NFS
SMB
百度搜索
每页显示条数 100


奇安信 网神网络数据传感器
首页
数据中心
策略配置
对象配置
网络配置
系统配置
test
威胁日志
网络日志
TCP流量
UDP流量
LDAP行为
TCP流终止方式
源MAC
目的MAC
源IP
源端口
目的IP
目的端口
上行字节数
下行字节数
协议
应用
自定义字段/值
RST
34:83:54:70:2D:73
F8:98:EF:AD:6A:AD
205.210.31.184
49895
183.146.28.100
389
0
0
TCP
AD域
RST
34:83:54:70:2D:73
F8:98:EF:AD:6A:AD
205.210.31.184
49989
183.146.28.74
5060
0
0
TCP
SIP
RST
34:83:54:70:2D:73
F8:98:EF:AD:6A:AD
205.210.31.184
49989
183.146.28.70
80
0
0
TCP
ONVIF

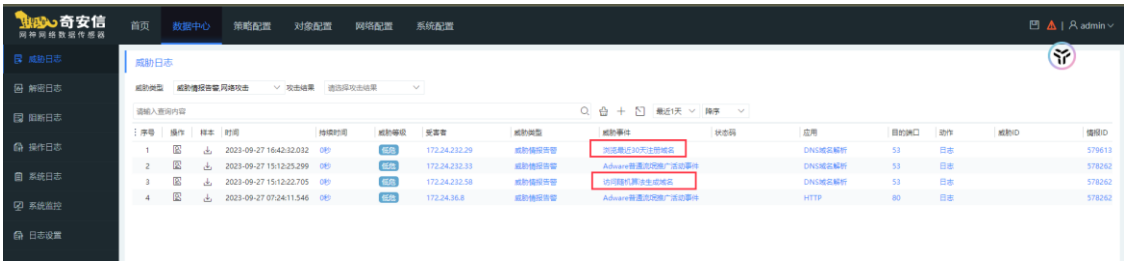

奇安信 网神网络数据传感器
首页
数据中心
策略配置
对象配置
网络配置
系统配置
test
威胁日志
网络日志
TCP流量
UDP流量
LDAP行为
TCP流终止方式
源MAC
目的MAC
源IP
源端口
目的IP
目的端口
上行字节数
下行字节数
协议
应用
自定义字段/值
FIN
34:83:54:70:2D:72
F8:98:EF:AD:6A:AC
124.228.193.5
15747
183.146.28.85
1080
1363
367932
TCP
SOCKS
RST
34:83:54:70:2D:72
F8:98:EF:AD:6A:AC
1.192.247.44
15747
183.146.28.90
443
1120
27456
TCP
SSL
FIN
34:83:54:70:2D:72
F8:98:EF:AD:6A:AC
112.23.97.150
15747
183.146.28.82
443
8616
54911
TCP
SSL
RST
34:83:54:70:2D:72
F8:98:EF:AD:6A:AC
36.99.136.129
15747
183.146.28.60
9070
280
7
TCP
SSL
FIN
34:83:54:70:2D:72
F8:98:EF:AD:6A:AC
124.76.128.44
15747
183.146.28.85
443
266
0
TCP
SSL

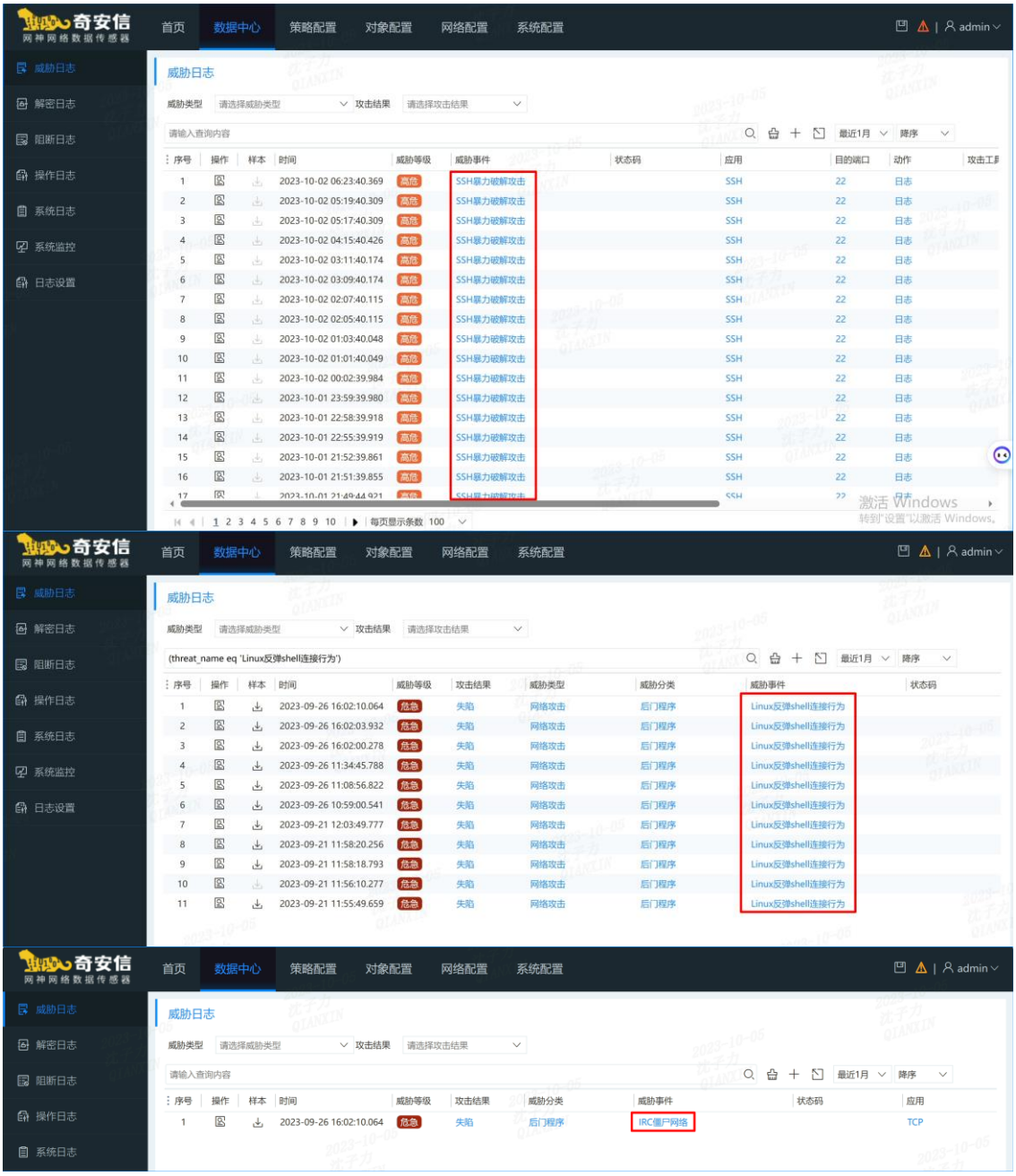

奇安信 网神网络数据传感器
首页
数据中心
策略配置
对象配置
网络配置
系统配置
test
威胁日志
网络日志
TCP流量
UDP流量
LDAP行为
邮件行为
TELNET行为
DHCP解析
UDP流量
请输入查询内容
最近1天
降序
UDP流起始时间
UDP流终止时间
源MAC
目的MAC
源IP
源端口
目的端口
上行字节数
下行字节数
协议
应用
自定义字段/值
NetBIOS
SNMP
DNS域名解析

2.11 高级安全检测

奇安信网神威胁监测与分析系统支持传输安全检测日志，包括网络攻击检测日志、漏洞利用攻击检测日志、僵尸网络检测日志、业务弱点发现日志。

奇安信网神威胁监测与分析系统支持 HTTP 未知站点下载可执行文件、浏览最近 30 天注册域名、浏览恶意动态域名、访问随机算法生成域名、暴力破解攻击、反弹连接、IRC 通信等僵尸网络行为检测。




奇安信 网神网络数据传感器
首页
数据中心
策略配置
对象配置
网络配置
系统配置
admin
威胁日志
解密日志
阻断日志
操作日志
系统日志
系统监控
日志设置
威胁日志
威胁类型
请选择威胁类型
攻击结果
请选择攻击结果
请输入查询内容
最近1月
降序
序号 操作 样本 时间 威胁等级 威胁事件 状态码 应用 目的端口 动作
1 2023-10-02 06:23:40.369 高危 SSH暴力破解攻击 SSH 22 日志
2 2023-10-02 05:19:40.309 高危 SSH暴力破解攻击 SSH 22 日志
3 2023-10-02 05:17:40.309 高危 SSH暴力破解攻击 SSH 22 日志
4 2023-10-02 04:15:40.426 高危 SSH暴力破解攻击 SSH 22 日志
5 2023-10-02 03:11:40.174 高危 SSH暴力破解攻击 SSH 22 日志
6 2023-10-02 03:09:40.174 高危 SSH暴力破解攻击 SSH 22 日志
7 2023-10-02 02:07:40.115 高危 SSH暴力破解攻击 SSH 22 日志
8 2023-10-02 02:05:40.115 高危 SSH暴力破解攻击 SSH 22 日志
9 2023-10-02 01:03:40.048 高危 SSH暴力破解攻击 SSH 22 日志
10 2023-10-02 01:01:40.049 高危 SSH暴力破解攻击 SSH 22 日志
11 2023-10-02 00:02:39.984 高危 SSH暴力破解攻击 SSH 22 日志
12 2023-10-01 23:59:39.980 高危 SSH暴力破解攻击 SSH 22 日志
13 2023-10-01 22:58:39.918 高危 SSH暴力破解攻击 SSH 22 日志
14 2023-10-01 22:55:39.919 高危 SSH暴力破解攻击 SSH 22 日志
15 2023-10-01 21:52:39.861 高危 SSH暴力破解攻击 SSH 22 日志
16 2023-10-01 21:51:39.855 高危 SSH暴力破解攻击 SSH 22 日志
1 2 3 4 5 6 7 8 9 10
每页显示条数 100
激活 Windows
转到"设置"以激活 Windows。

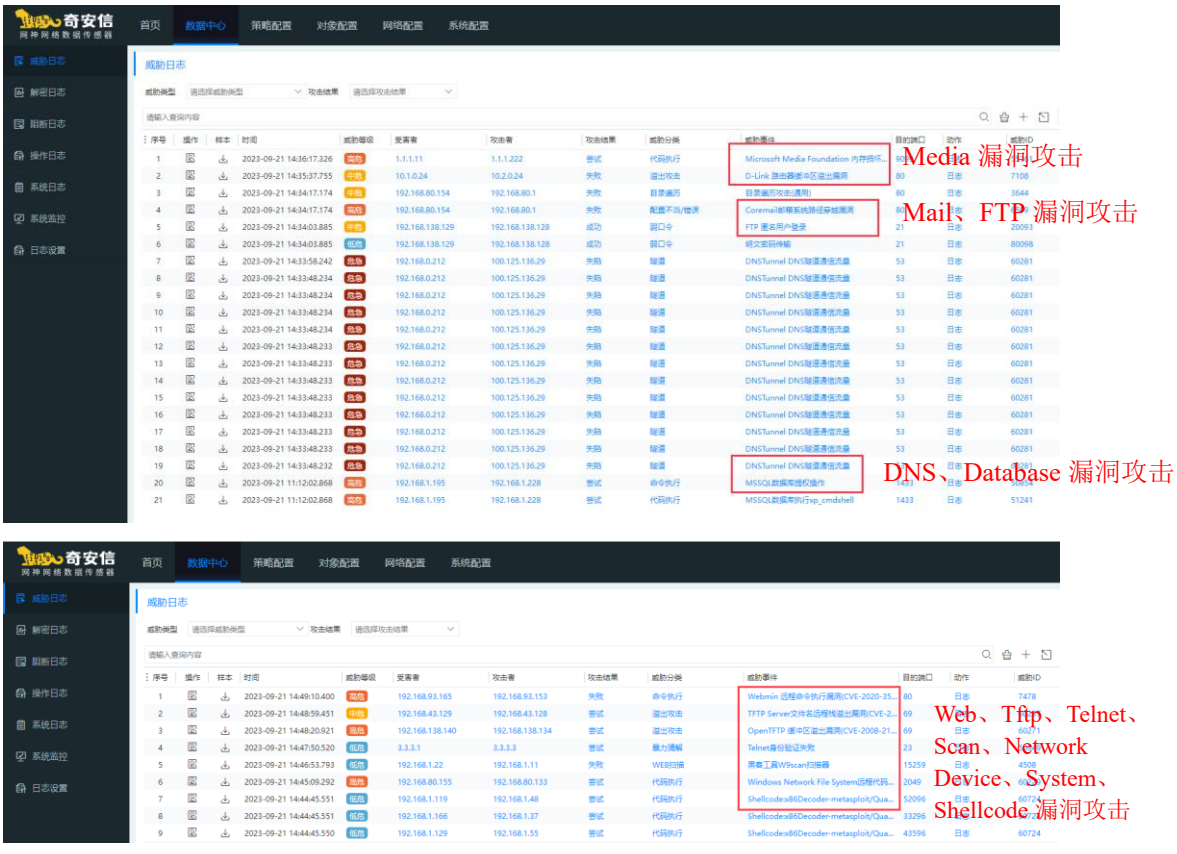
奇安信 网神网络数据传感器
首页
数据中心
策略配置
对象配置
网络配置
系统配置
admin
威胁日志
解密日志
阻断日志
操作日志
系统日志
系统监控
日志设置
威胁日志
威胁类型
请选择威胁类型
攻击结果
请选择攻击结果
(threat_name eq 'Linux反弹shell连接行为')
最近1月
降序
序号 操作 样本 时间 威胁等级 攻击结果 威胁类型 威胁分类 威胁事件 状态码
1 2023-09-26 16:02:10.064 危急 失陷 网络攻击 后门程序 Linux反弹shell连接行为
2 2023-09-26 16:02:03.932 危急 失陷 网络攻击 后门程序 Linux反弹shell连接行为
3 2023-09-26 16:02:00.278 危急 失陷 网络攻击 后门程序 Linux反弹shell连接行为
4 2023-09-26 11:34:45.788 危急 失陷 网络攻击 后门程序 Linux反弹shell连接行为
5 2023-09-26 11:08:56.822 危急 失陷 网络攻击 后门程序 Linux反弹shell连接行为
6 2023-09-26 10:59:00.541 危急 失陷 网络攻击 后门程序 Linux反弹shell连接行为
7 2023-09-21 12:03:49.777 危急 失陷 网络攻击 后门程序 Linux反弹shell连接行为
8 2023-09-21 11:58:20.256 危急 失陷 网络攻击 后门程序 Linux反弹shell连接行为
9 2023-09-21 11:58:18.793 危急 失陷 网络攻击 后门程序 Linux反弹shell连接行为
10 2023-09-21 11:56:10.277 危急 失陷 网络攻击 后门程序 Linux反弹shell连接行为
11 2023-09-21 11:55:49.659 危急 失陷 网络攻击 后门程序 Linux反弹shell连接行为

奇安信 网神网络数据传感器
首页
数据中心
策略配置
对象配置
网络配置
系统配置
admin
威胁日志
解密日志
阻断日志
操作日志
系统日志
威胁日志
威胁类型
请选择威胁类型
攻击结果
请选择攻击结果
请输入查询内容
最近1月
降序
序号 操作 样本 时间 威胁等级 攻击结果 威胁分类 威胁事件 状态码 应用
1 2023-09-26 16:02:10.064 危急 失陷 后门程序 IRC僵尸网络 TCP

2.12 漏洞检测

2.12.1 漏洞攻击检测

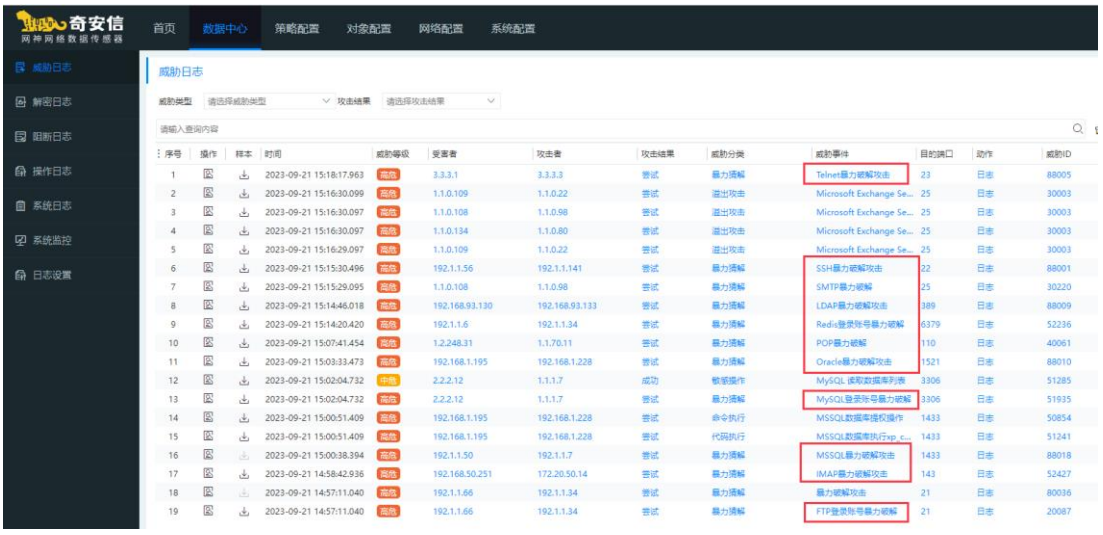
奇安信网神威胁监测与分析系统支持 Database 漏洞攻击、DNS 漏洞攻击、FTP 漏洞攻击、Mail 漏洞攻击、Network Device、Media 漏洞攻击、Shellcode 漏洞攻击、Scan 漏洞攻击、System 漏洞攻击、Telnet 漏洞攻击、Tftp 漏洞攻击、IPS 云防护、Web 漏洞攻击等服务漏洞攻击检测。

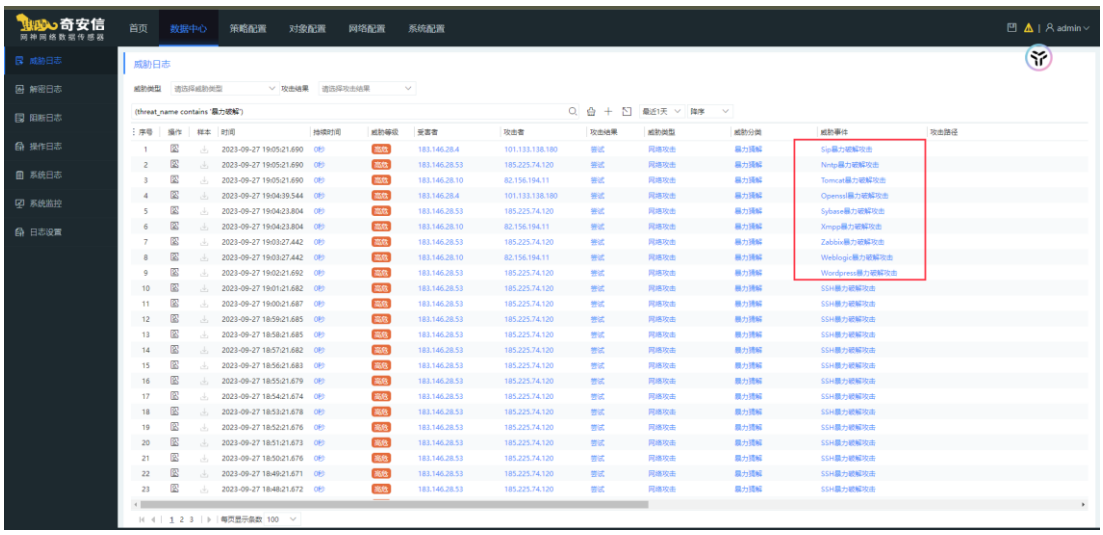


IPS 云防护（恶意文件云检测）、Web 漏洞攻击

2.12.2 暴破

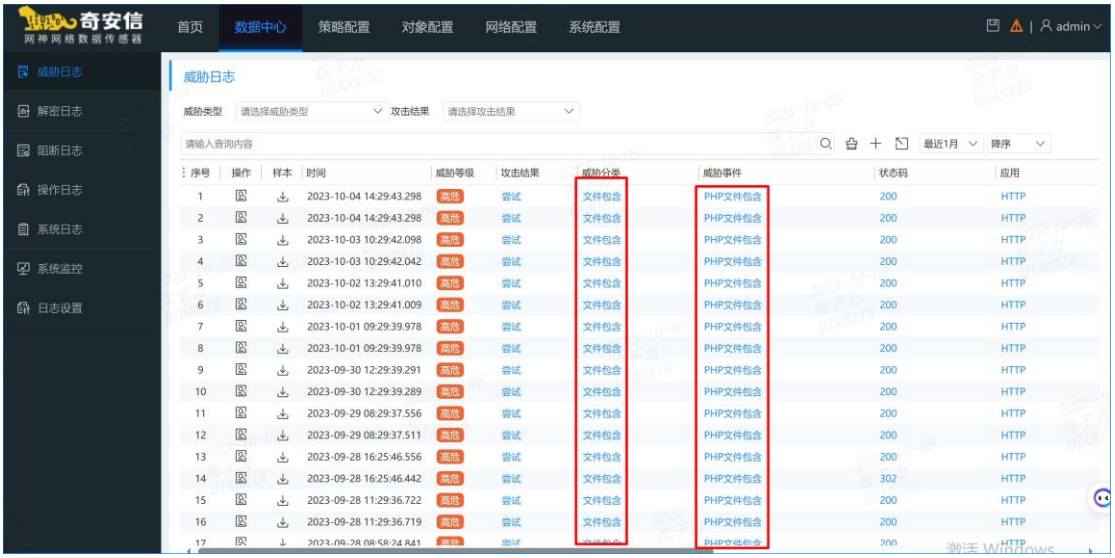
奇安信网神威胁监测与分析系统支持 FTP、IMAP、MS Sql、Mysql、Oracle、POP3、RDP、Sip 、Redis 、Ldap 、Nntp 、Openssl 、SMTP、SSH、Telnet、Tomcat、Sybase、Xmpp 、Zabbix 、Weblogic 、Wordpress 、VNC 等 72 种协议暴力破解检测。





2.12.3 客户端漏洞攻击检测

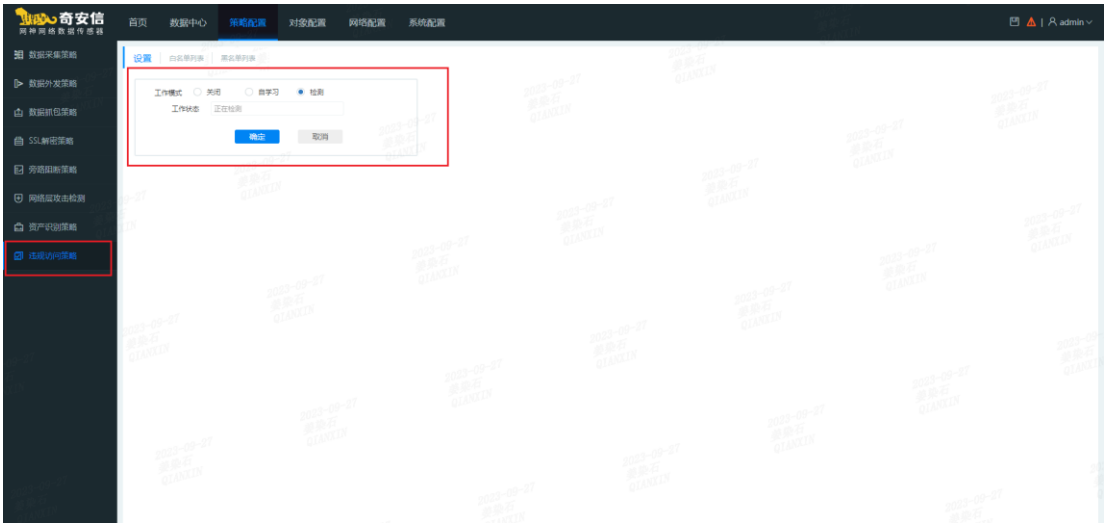
奇安信网神威胁监测与分析系统支持 Application 漏洞攻击、File 漏洞攻击、Scan 漏洞攻击、Shellcode 漏洞攻击、System 漏洞利用攻击、Web Activex 等客户端漏洞攻击检测。



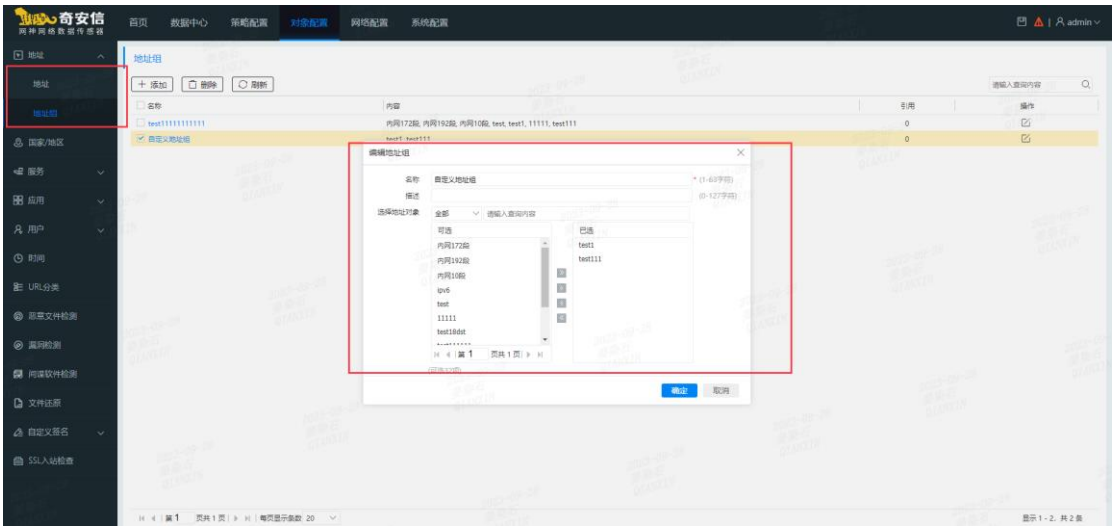
2.13 违规访问检测

奇安信网神威胁监测与分析系统可检测内网主机的访问情况是否符合规定，需要人工事先进行梳理好访问关系再进行配置。策略从上到下进行匹配，可以通过右侧置顶功能对策略优先级进行调节。

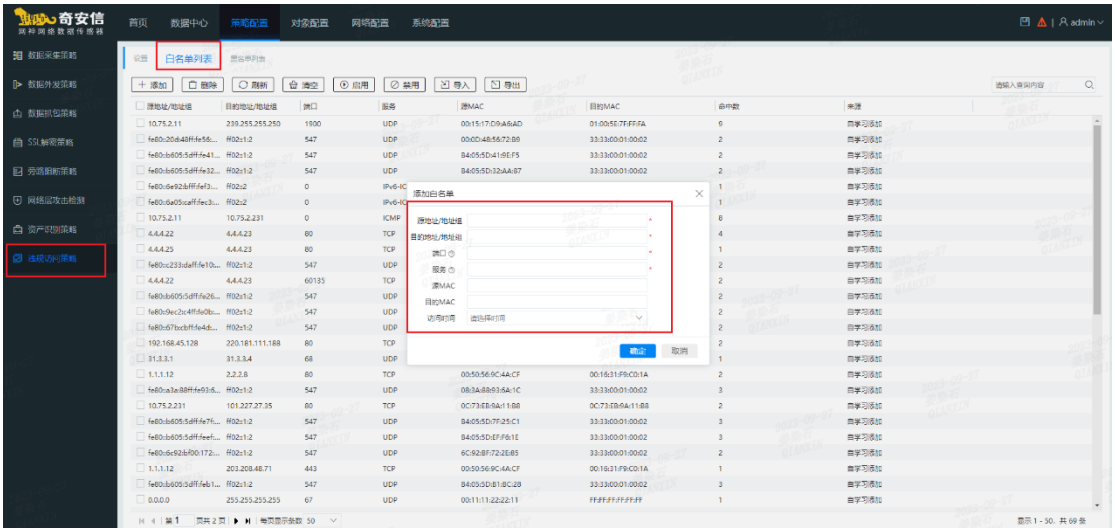
奇安信网神威胁监测与分析系统支持 IP，IP 组，服务，端口，访问时间等定义访问策略，主动建立针对性的业务和应用访问逻辑规则，包括白名单和黑名单方式。在违规访问策略设置中，支持学习模式，开启自学习模式基于接收的原始网络流量学习五元组信息，自动生成白名单，切换到检测模式后则基于白名单做检测，不匹配则生成告警。

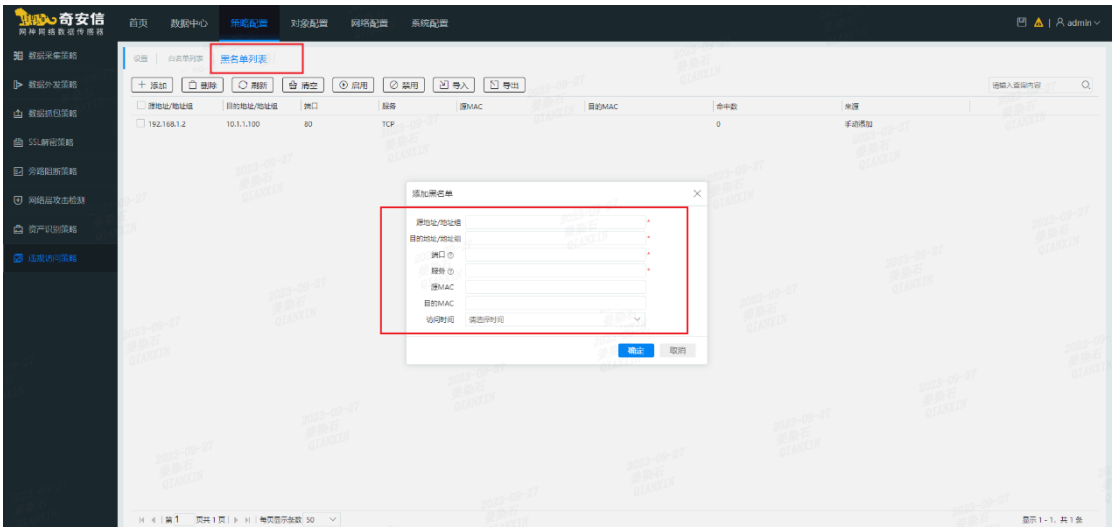


支持自定义 IP 地址/IP 地址组；



支持白名单/黑名单（引用地址/地址组）；





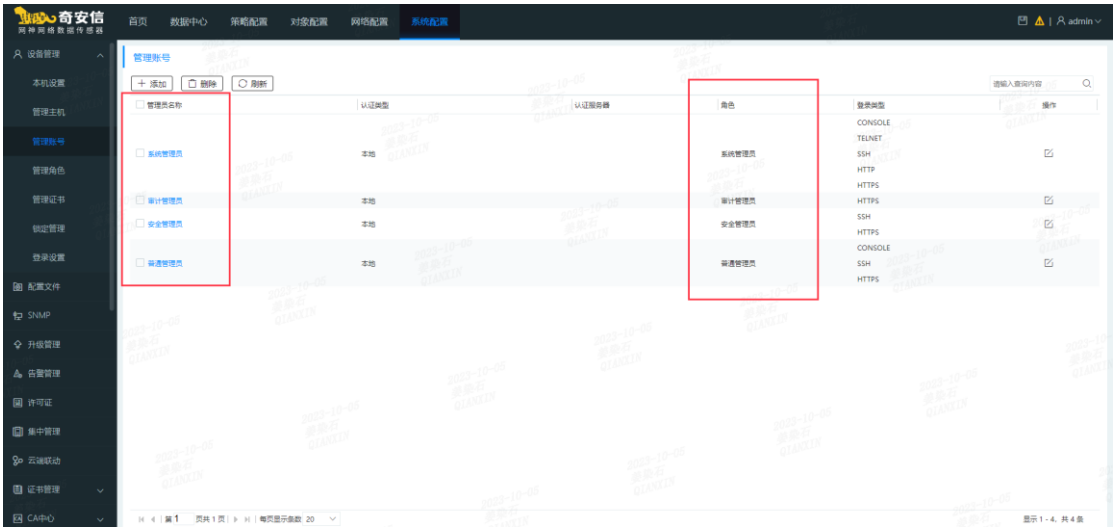
2.14 IPv4 和 IPv6 双栈支持

奇安信网神威胁监测与分析系统全面支持 IPv6,支持配置接口 IPv4 地址或 IPv6 地址；支持对 IPv6 协议流量检测，支持对 IPv4 路由监控和对 IPv6 路由监控。

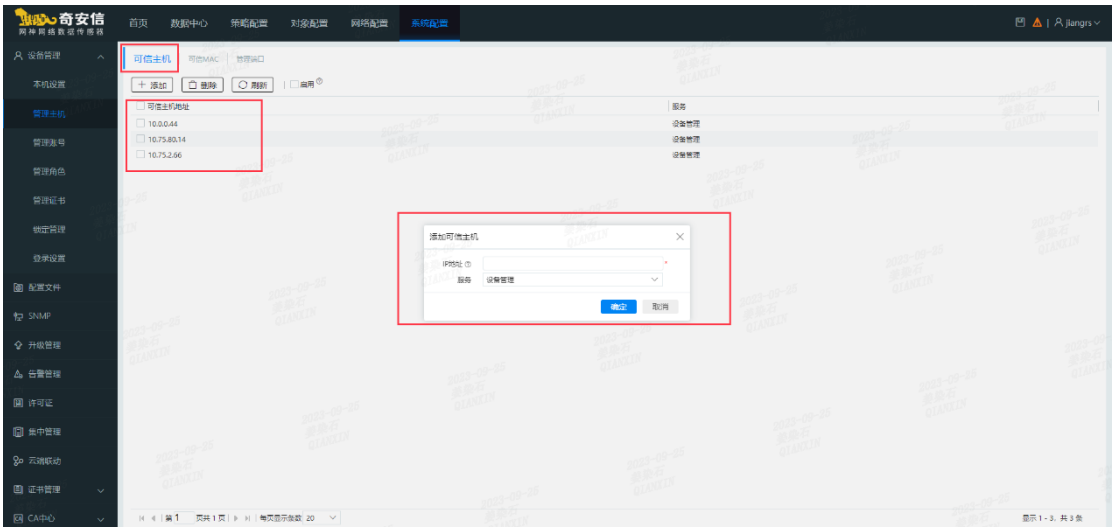
2.15 管理功能

2.15.1 用户管理

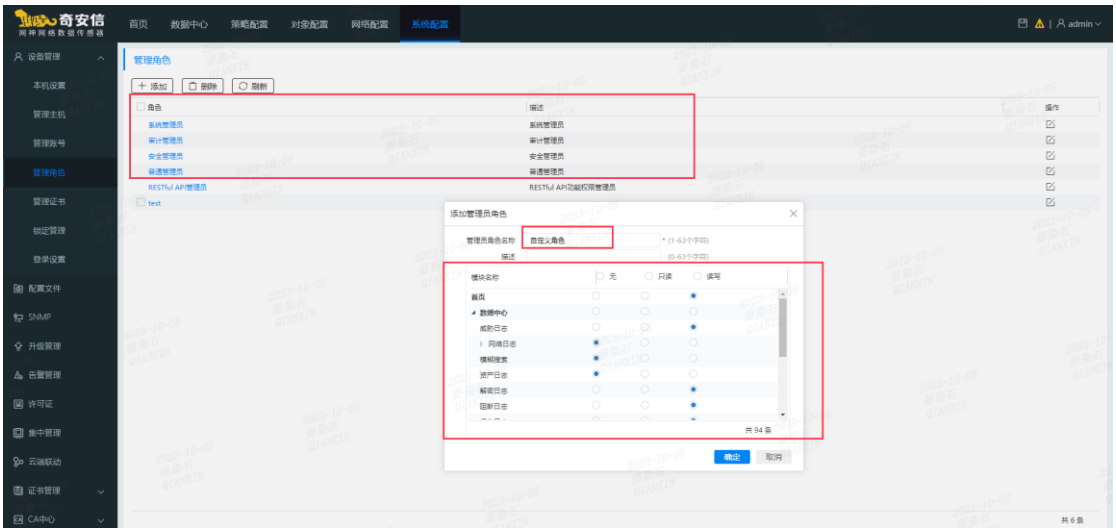
奇安信网神威胁监测与分析系统提供三权分立的用户管理能力：系统管理员、审计管理员、安全管理员、普通管理员四个角色相互独立；具备系统内用户的业务操作和运维操作；同时支持 IP 绑定的登录安全设置。普通管理员角色的权限可自定义模块页面的编辑和查看权限。



如 IP 绑定登录安全设置——可信 IP、可信 MAC。

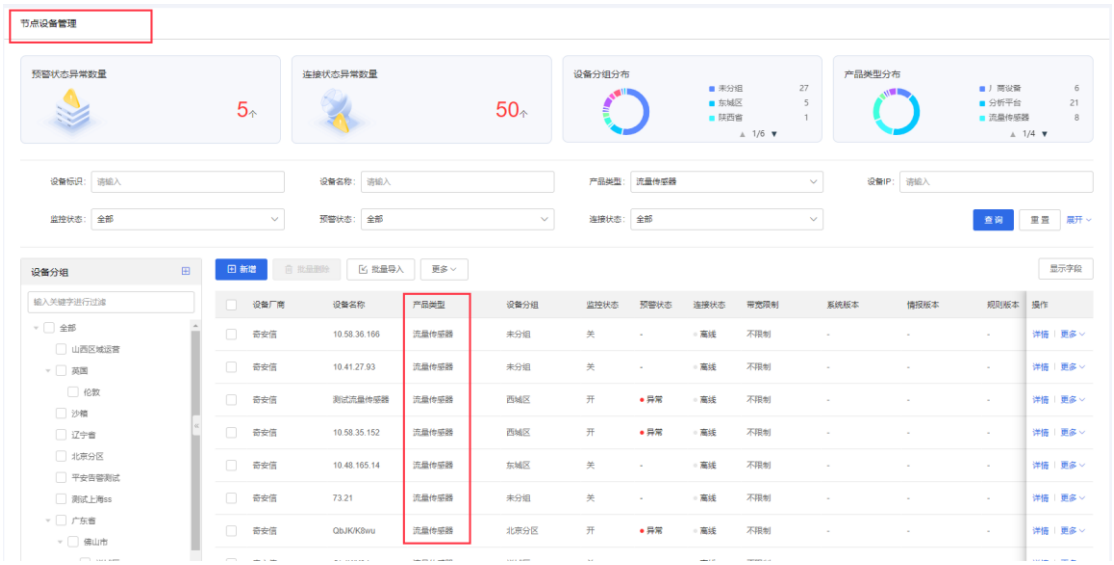


管理角色自定义：读写——编辑、只读——查看、无——页面不可见。



2.15.2 节点设备管理

奇安信网神威胁监测与分析系统支持通过态势感知平台、NGSOC 分析平台等网络安全监测分析平台进行各节点设备管理，能够对各节点设备策略配置、升级维护进行便捷管理，支持通过态势感知平台、NGSOC 分析平台等网络安全监测分析平台集中配置。

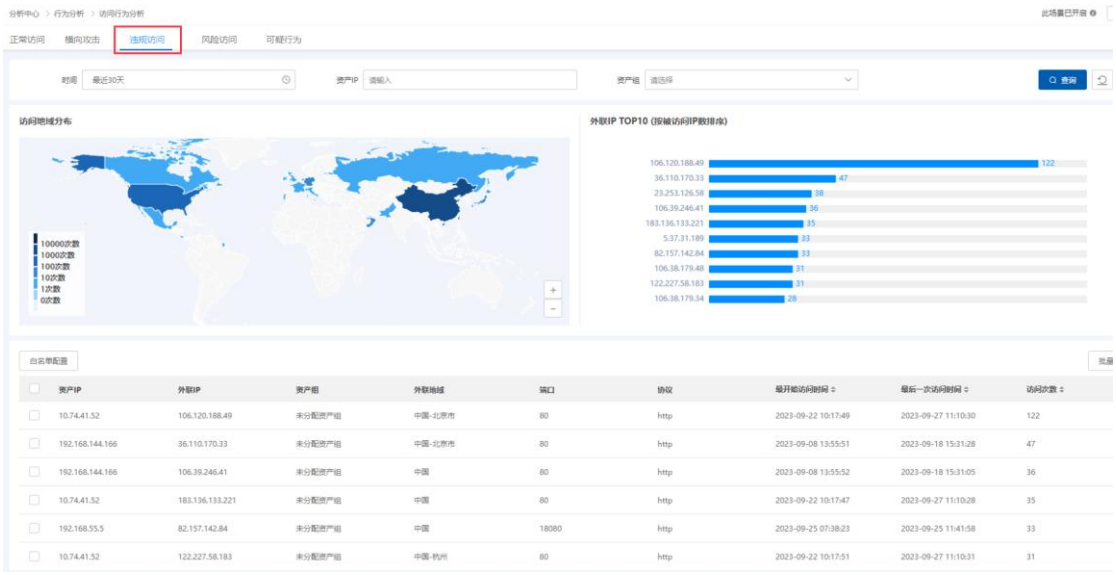


2.16 告警分析与查看

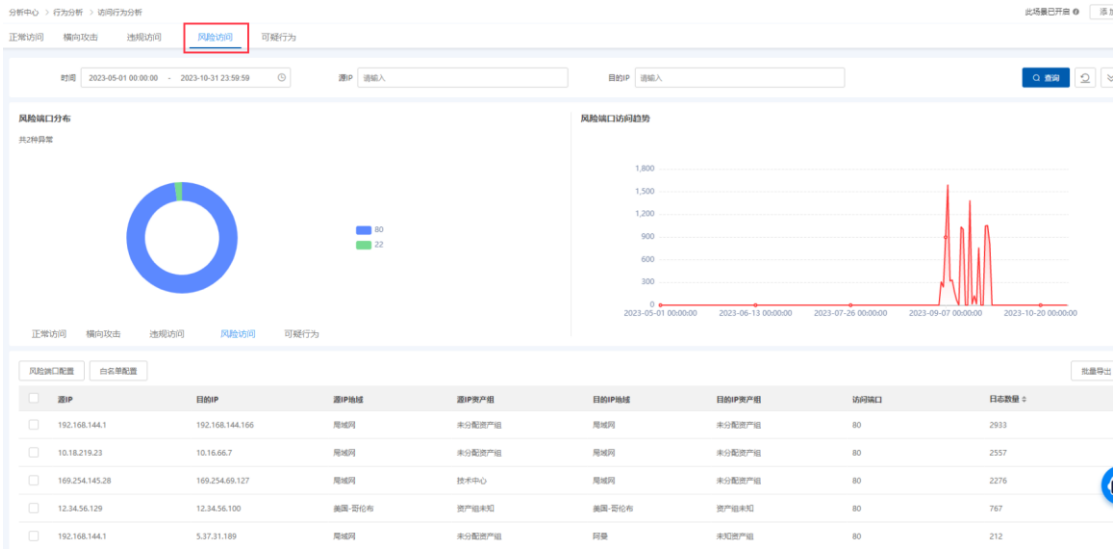
奇安信网神威胁监测与分析系统支持按照对外业务流量可视、横向流量可视、外联流量可视等开放的业务流量情况，展示服务器流量排行、最活跃源主机的内网服务器的流量情况，支持全球地图展示整体外联流量情况。

支持可视化的形式展示威胁的影响面，通过大数据分析和关联检索技术，能够直观的看到失陷主机的威胁影响面，同时基于列表模式展示攻击、违规访问、风险访问、可疑行为、正常访问等详细信息，支持攻击溯源功能，分析出首次失陷、疑似入口点、首次遭受攻击等信息；帮助管理人员及时了解威胁的影响，并找到攻击入口点。

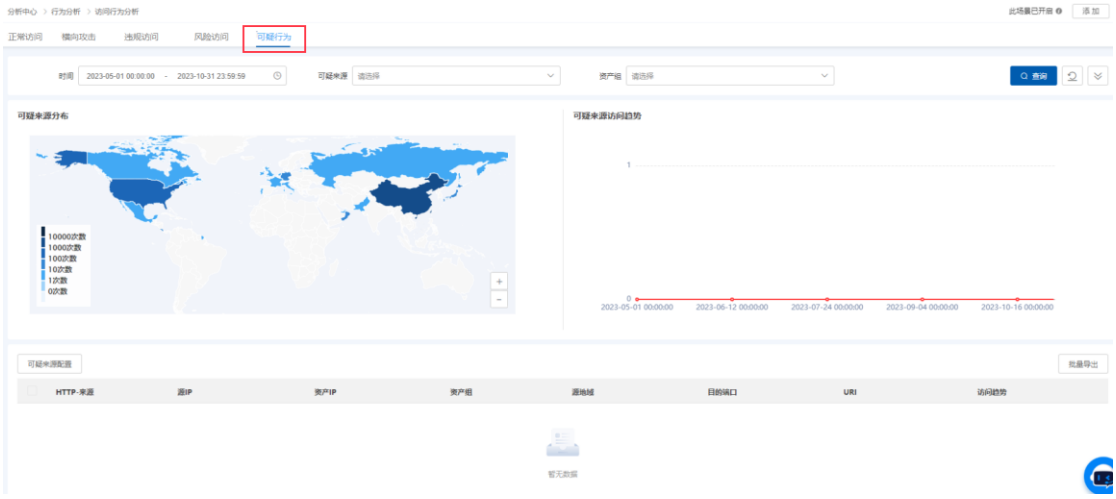
违规访问；



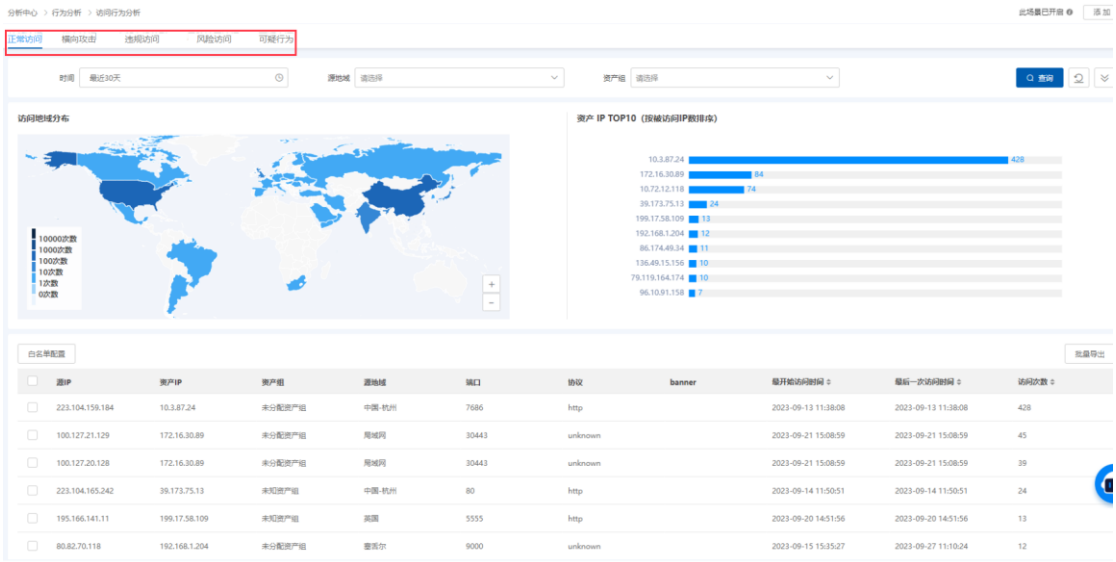
风险访问；



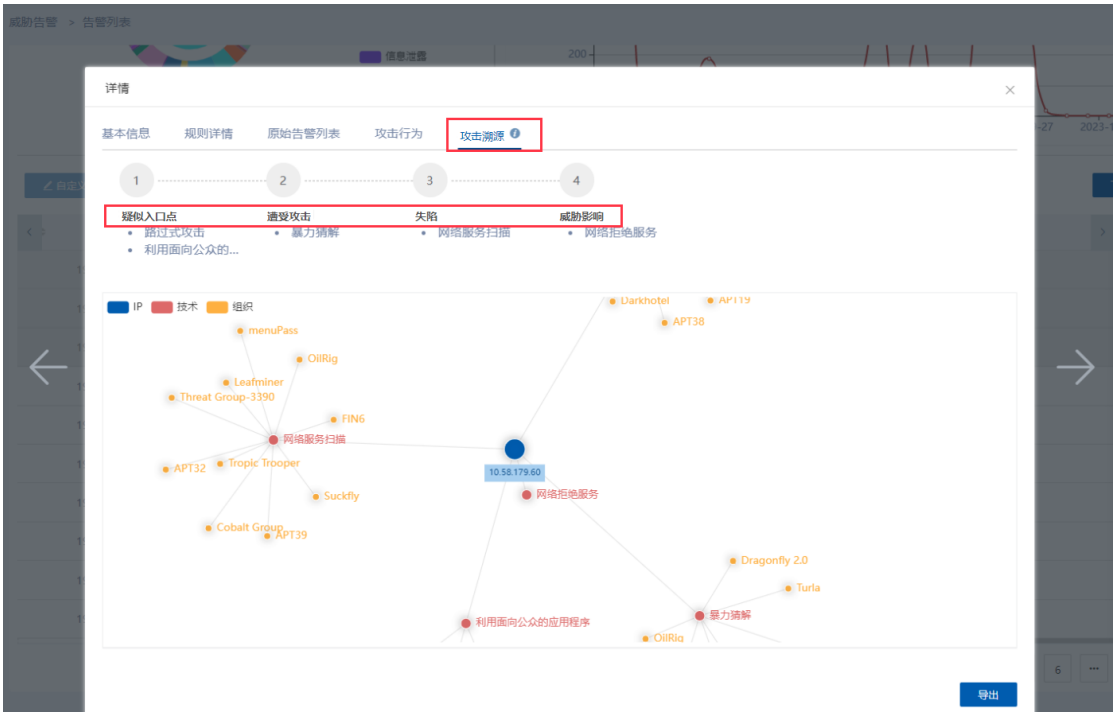
可疑行为；

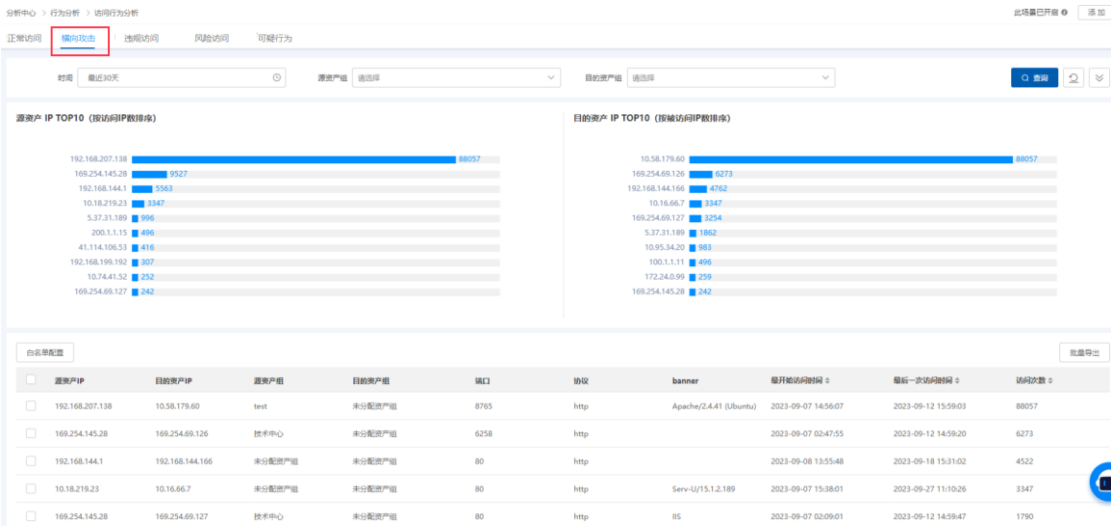


正常访问；

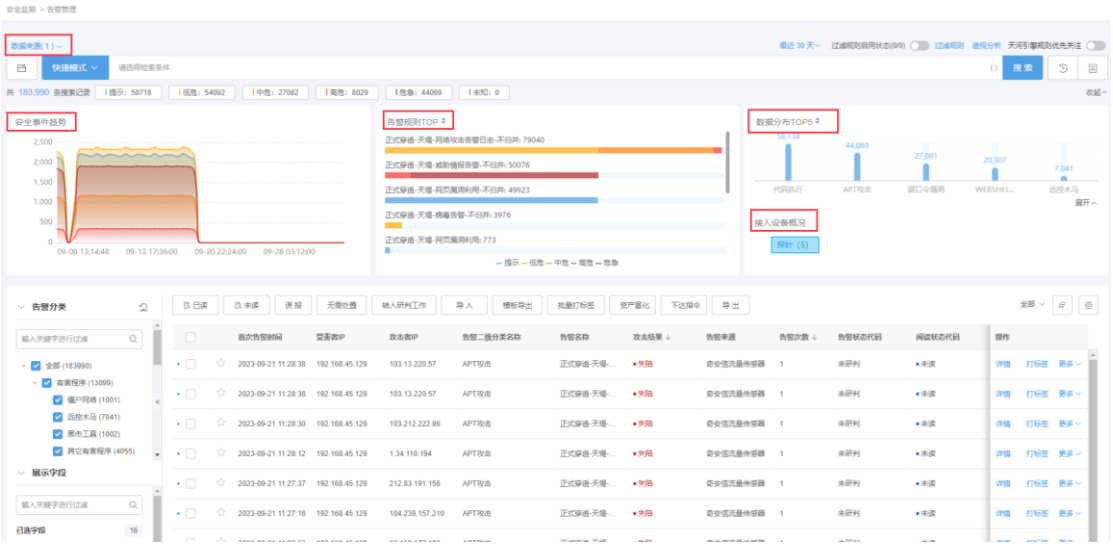

正常访问
横向攻击
违规访问
风险访问
可疑行为
访问地域分布
资产 IP TOP10（按被访问IP数排序）

攻击溯源。

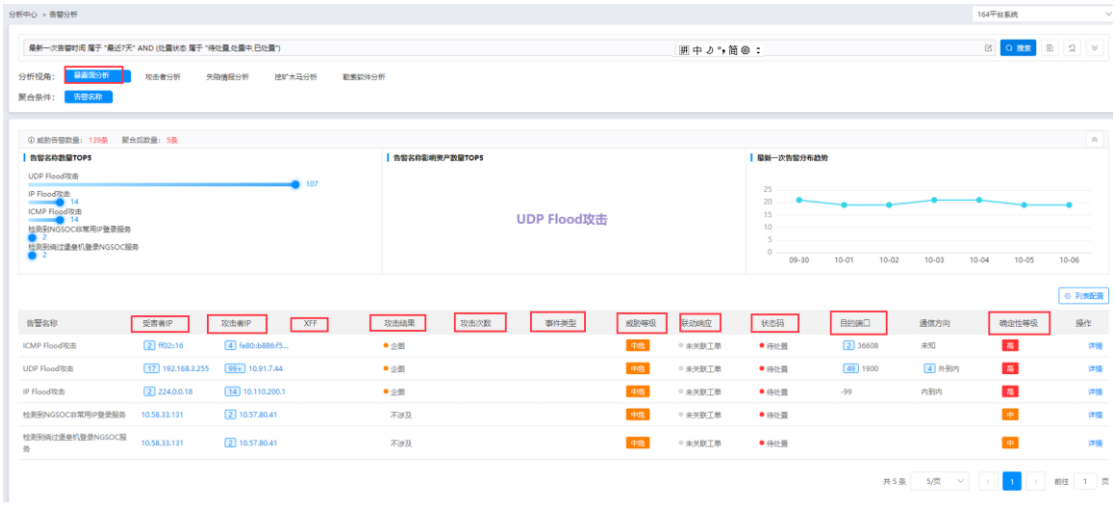

详情
基本信息
规则详情
原始告警列表
攻击行为
攻击溯源
疑似入口点
遭受攻击
失陷
威胁影响
IP
技术
组织
menuPass
OilRig
Leafminer
Threat Group-3390
FIN6
网络服务扫描
APT32
Tropic Trooper
Suckfly
Cobalt Group
APT39
10.58.179.60
网络拒绝服务
Darkhotel
APT38
Dragonfly 2.0
Turla
暴力猜解
利用面向公众的应用程序
导出



支持日志关联分析结果的可视化展示，分析结果可视化展示。包括数据分布、安全事件趋势图、关联规则告警趋势图、接入设备概况等。

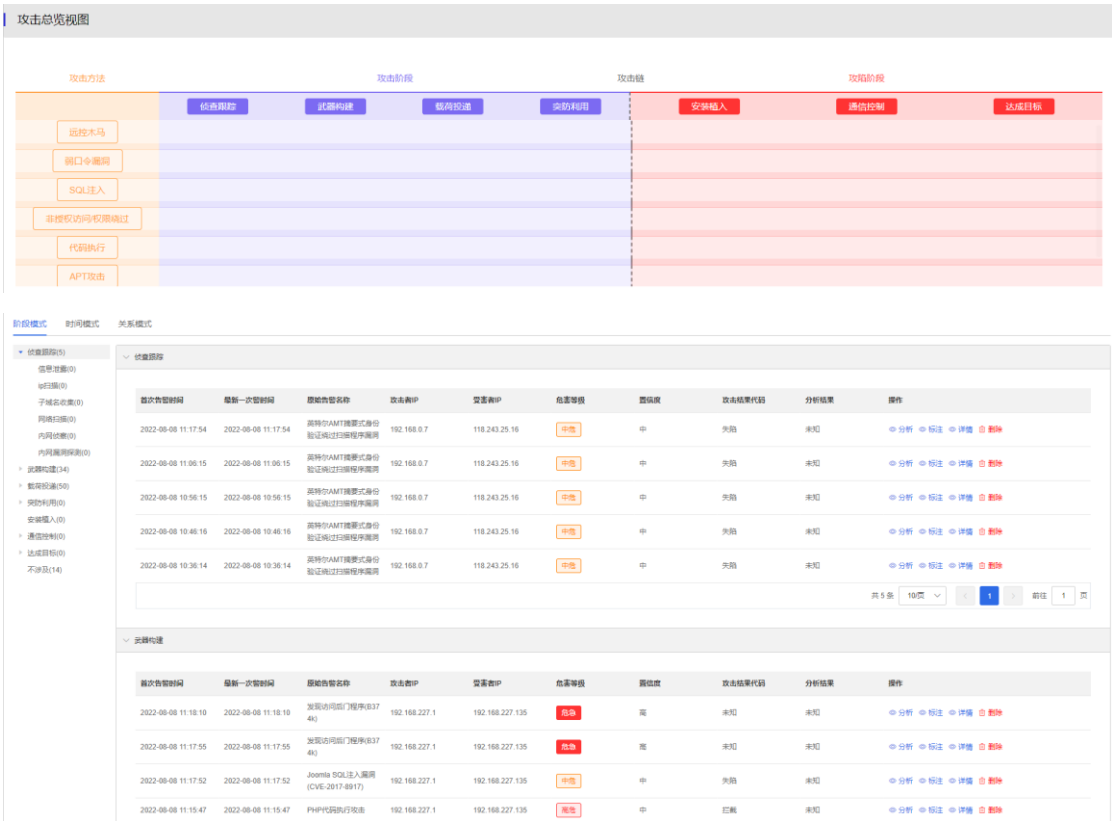


支持各节点对外服务器外网暴露面分析、内网服务器暴露面梳理。支持实时攻击分析结果展示，实时展示受害 IP、攻击 IP、XFF、攻击结果、攻击次数、事件类型、威胁等级、联动响应、状态码、确定性等级等数据。

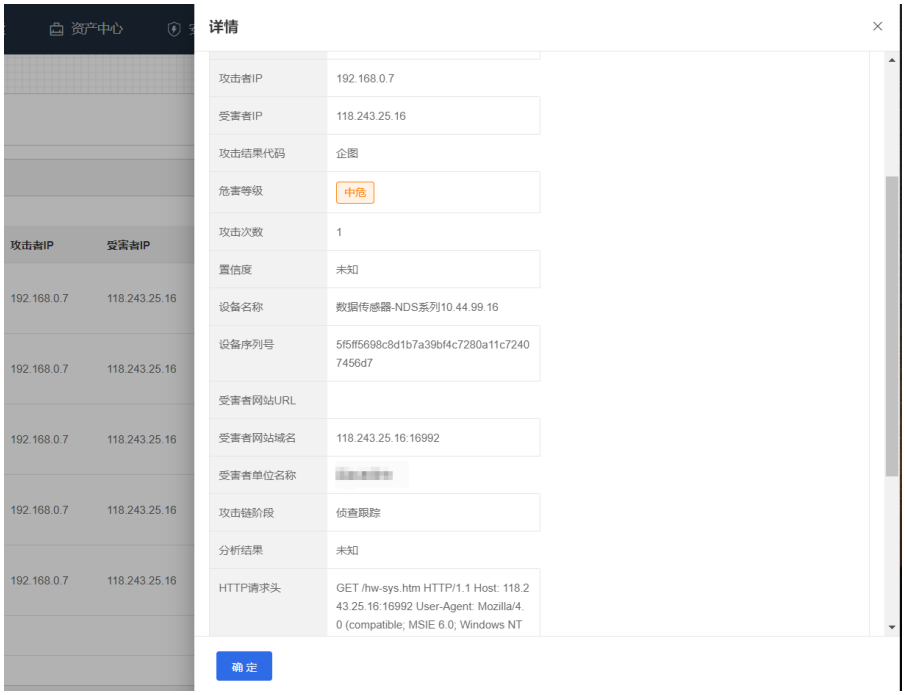


支持告警结果溯源和查询分析，可自动化复现自有资产从最开始的遭受攻击到权限维持各个阶段的黑客行为，包括攻击入口溯源。支持基于可视化的形式展示威胁的影响面，通过大数据分析和关联检索技术，能够直观的看到失陷主机的威胁影响面，同时基于列表模式展示攻击、违规访问、风险访问、可疑行为、正常访问等详细信息。支持攻击溯源功能，分析出首次失陷、疑似入口点、首次遭受攻击等信息。

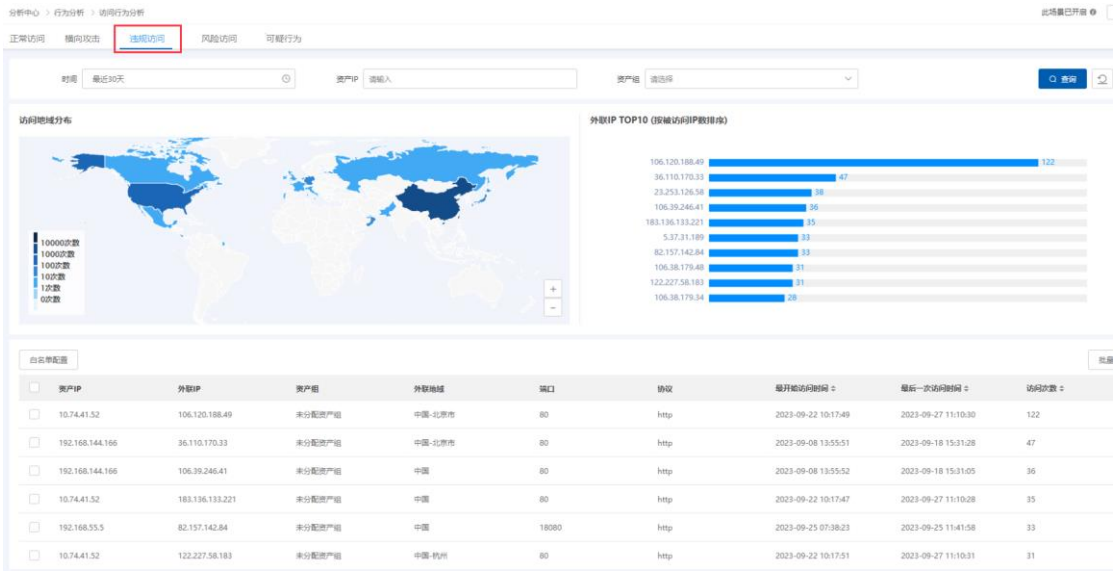
告警结果溯源和查询分析；



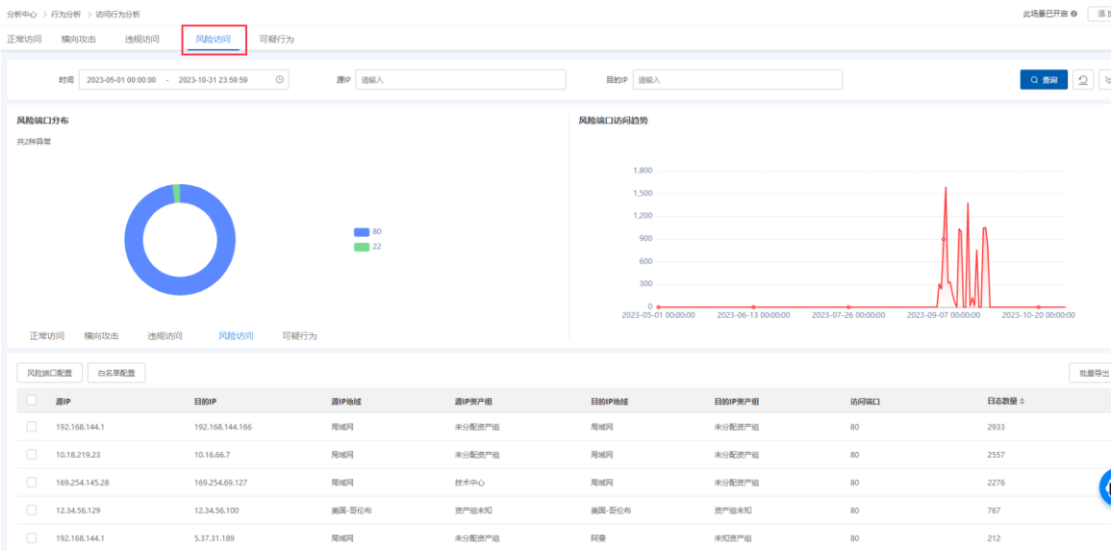
失陷主机的威胁影响面；



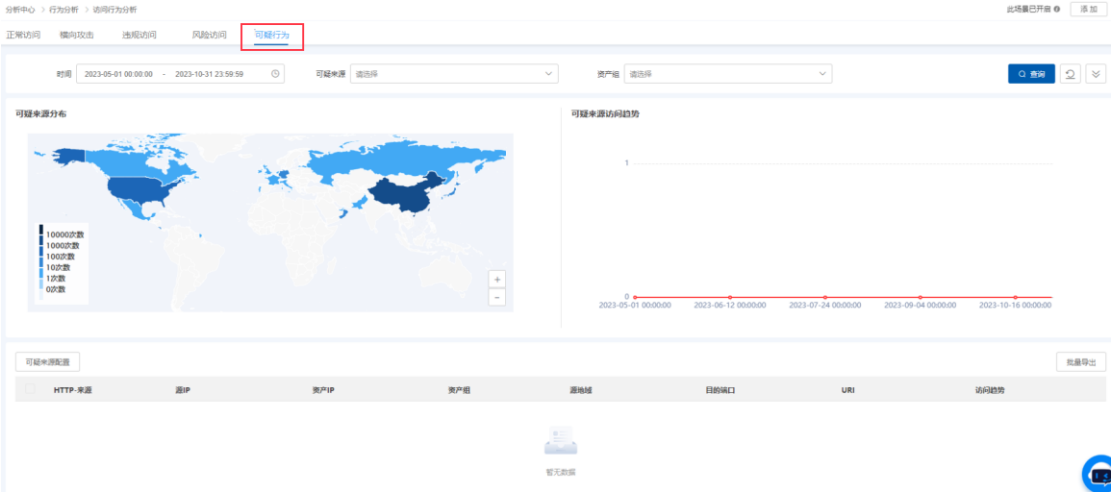
违规访问；



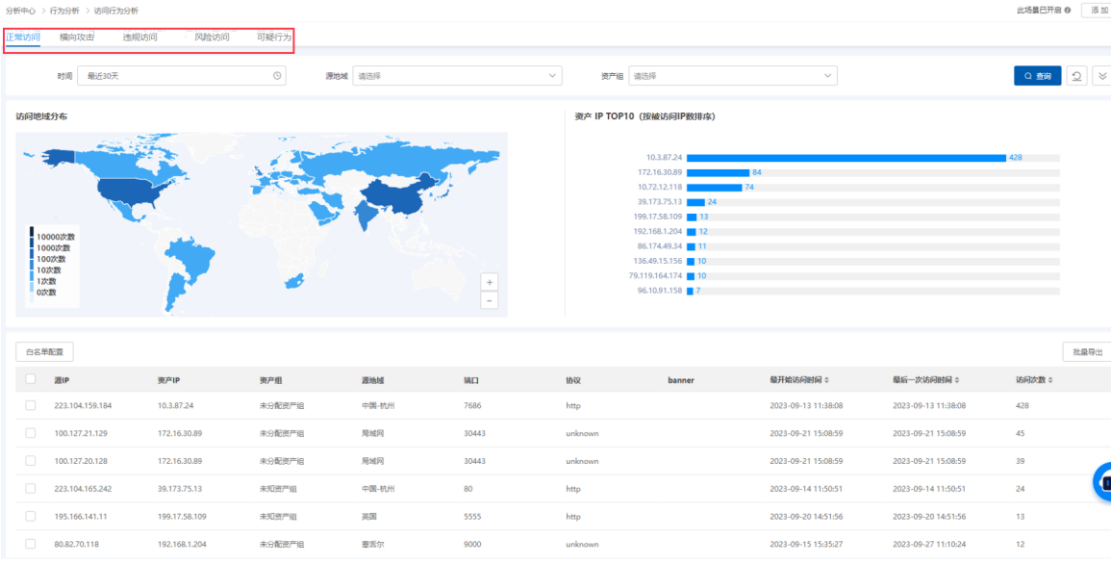
风险访问；



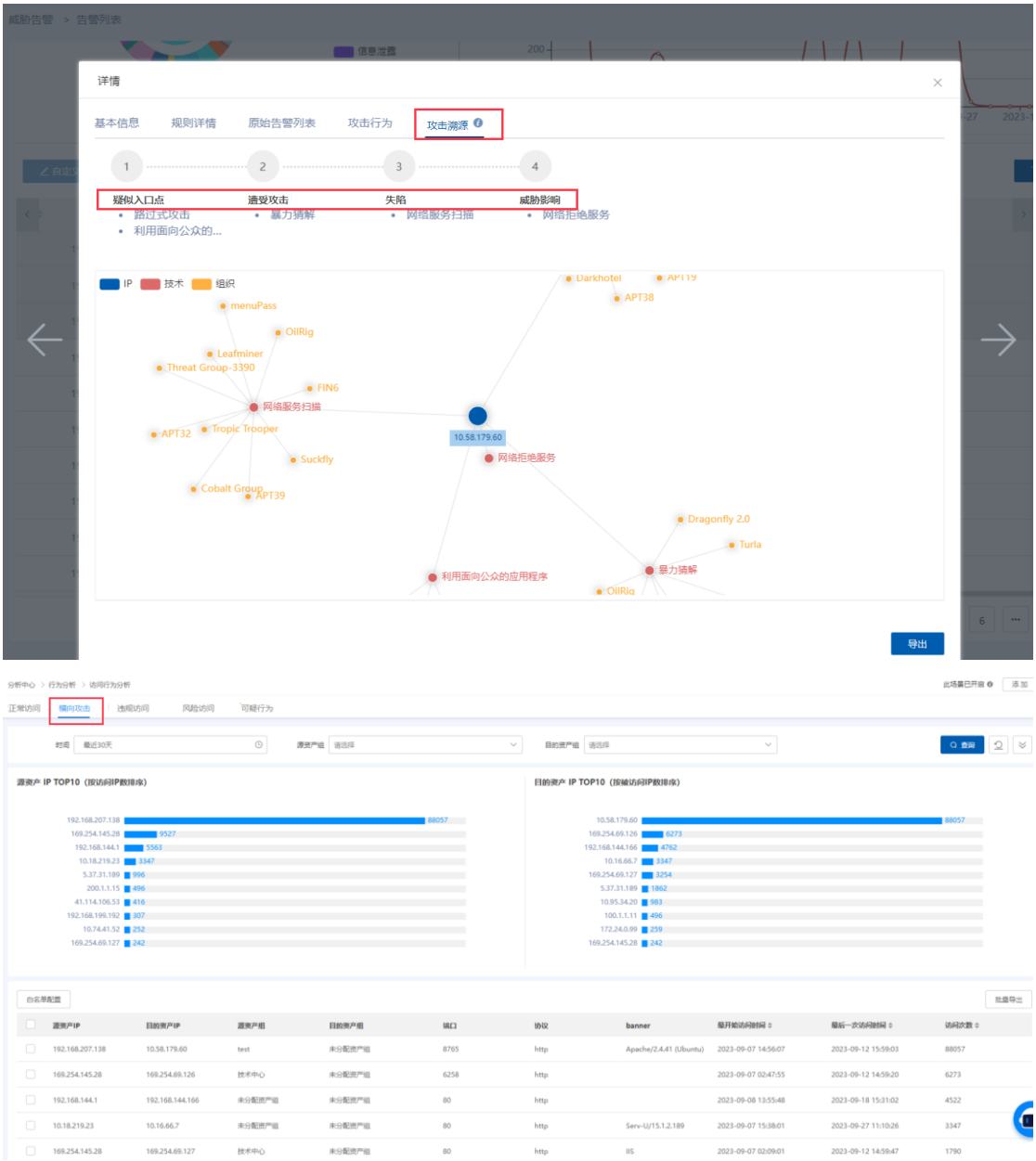
可疑行为；



正常访问；



攻击溯源。


详情
基本信息
规则详情
原始告警列表
攻击行为
攻击溯源
1
2
3
4
疑似入口点
遭受攻击
失陷
威胁影响
路过式攻击
利用面向公众的...
暴力猜解
网络服务扫描
网络拒绝服务
IP
技术
组织
menuPass
OilRig
Leafminer
Threat Group-3390
FIN6
网络服务扫描
APT32
Tropic Trooper
Suckfly
Cobalt Group
APT39
10.58.179.60
网络拒绝服务
Darkhotel
APT38
Dragonfly 2.0
Turla
暴力猜解
利用面向公众的应用程序
OilRig
导出

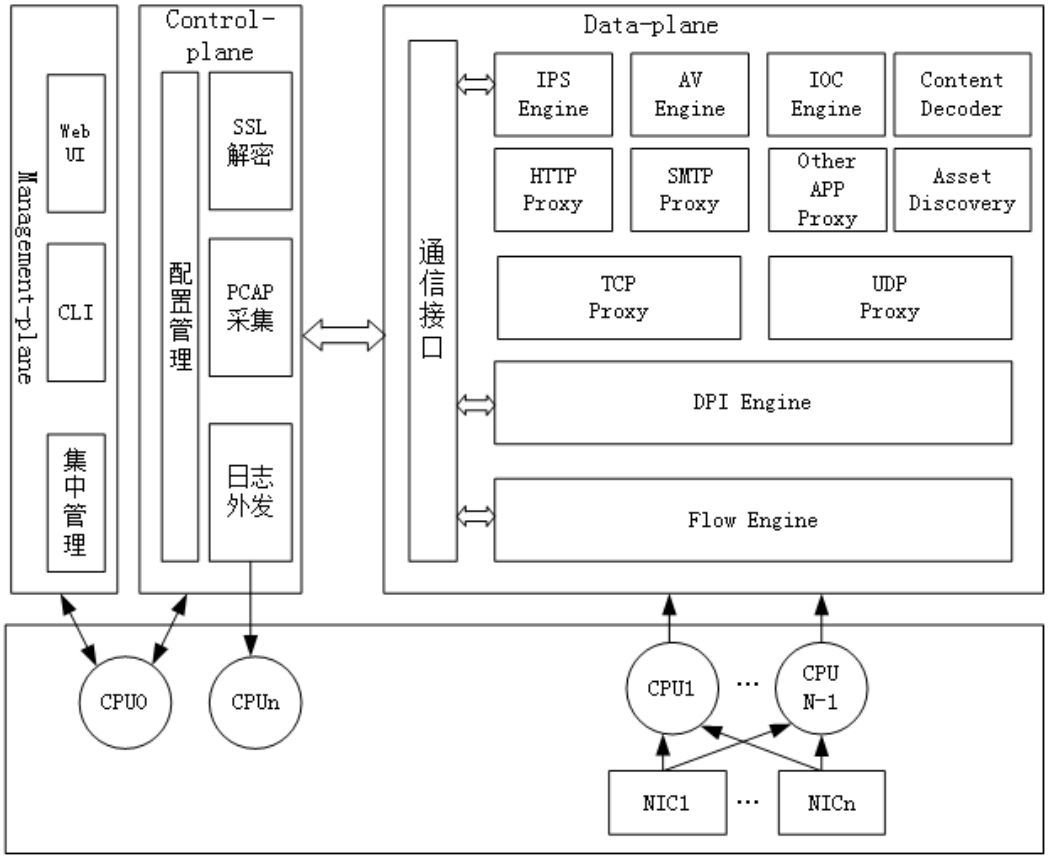
正常访问
横向攻击
违规访问
风险访问
可疑行为
源资产 IP TOP10（按访问IP数排序）
目的资产 IP TOP10（按被访问IP数排序）

3 产品优势

3.1 整体框架采用优化的 AMP+并行处理架构

奇安信网神威胁监测与分析系统的系统框架如图 3-1 所示。系统的整体框架采用 AMP+架构，AMP+架构是更加优化的多核异步并行处理架构。

图3-1 系统框架



AMP+并行处理架构主要分为三大部分：

- 管理平面由 CPU0 负责处理。

- 控制平面（control-plane）由 CPU0 负责处理，数据外发由最后一个核负责处理。
- 数据平面（data-plane）由剩余的 CPU 平均分配处理。

AMP+架构具备高稳定性和高性能的特点。

3.1.1 高稳定性

在 AMP+架构下，多个平面负责不同的任务，实现了分层、独立、异步并发的工作体系。为奇安信网神威胁监测与分析系统的性能带来了革命性的提升，配置管理平面、控制平面、数据平面的三层分离，保证了奇安信网神威胁监测与分析系统的高稳定性。

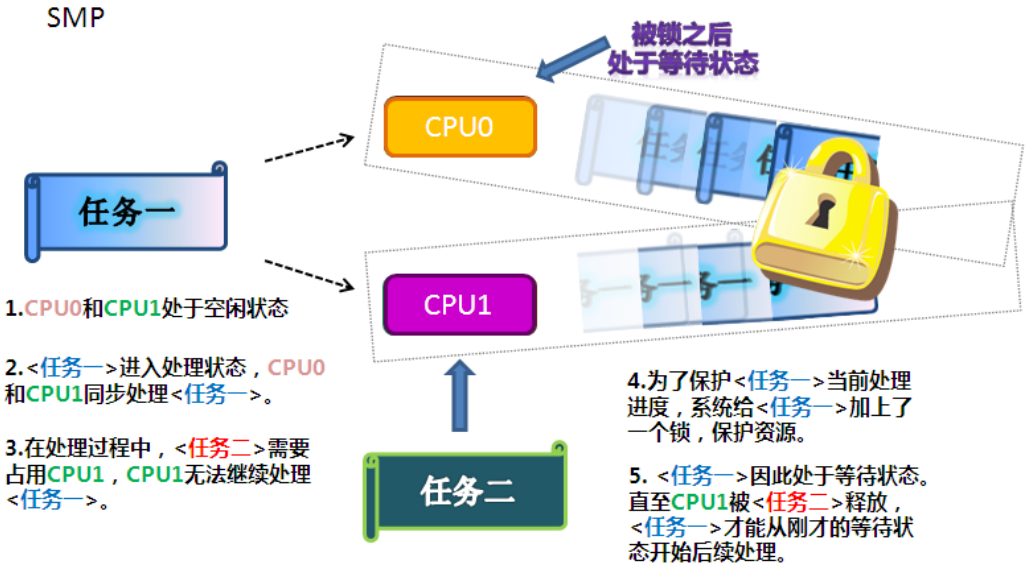
AMP+架构与传统的 SMP 架构相比，主要在两个方面提高了 CPU 利用率，从而获取更高的系统性能。

3.1.2 高性能

3.1.2.1 避免任务锁定

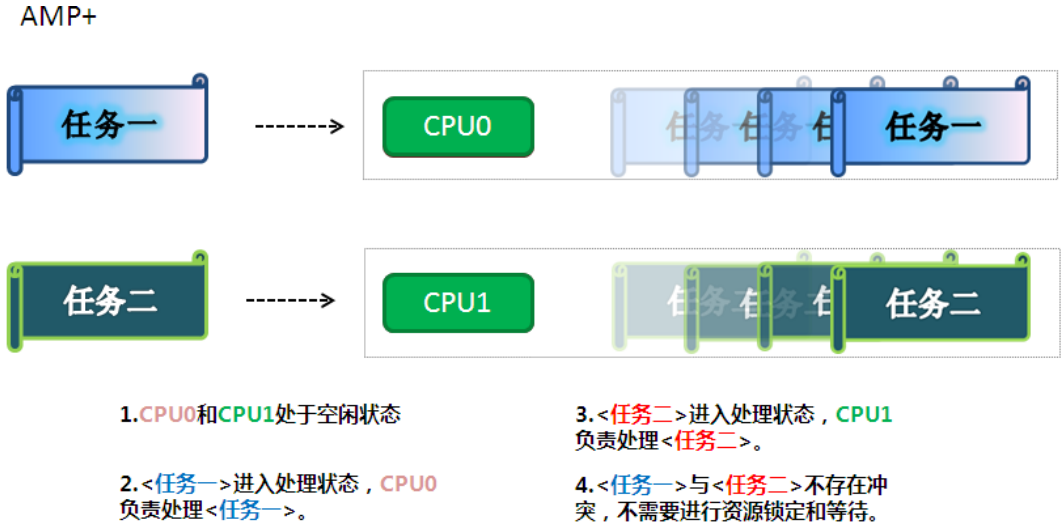
传统的 SMP 架构在进行多核并发处理时，会将同一个任务，例如任务 1 分配给多个不同的 CPU 处理。如图 3-2 所示，当其中一个 CPU 被其他任务占用，就会导致其他 CPU 上的任务 1 被锁，而处于等待状态。从而降低了 CPU 的效率，也延长了任务处理时间。

图3-2 传统 SMP 架构任务处理图



如图 3-3 所示，奇安信网神威胁监测与分析系统采用的 AMP+架构突破了传统的 SMP 架构瓶颈，不同的 CPU 可以处理不同的任务，这就极大减少了任务被锁住的情况，从而提升了 CPU 的效率，也极大的缩短了任务处理时间。从而提高了奇安信网神威胁监测与分析系统的处理速度。

图3-3 AMP+架构任务处理图



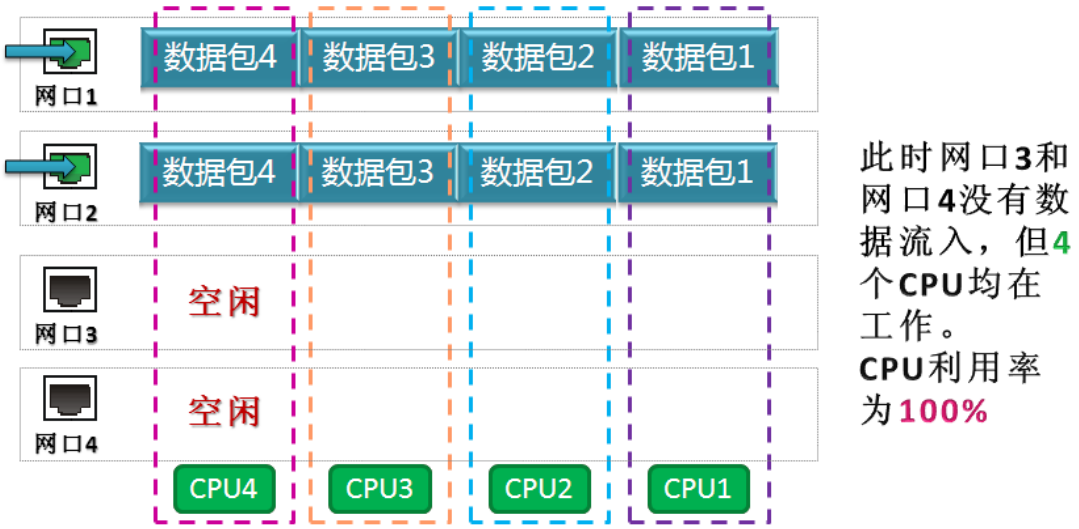
3.1.2.2 优化网口数据收发处理

传统的多核架构，为了实现多核并行处理，会将 CPU 与网口进行绑定。如图 3-4 所示，在传统的多核架构下，当网口没有接收到任何数据时，与其绑定的 CPU 就会处于空闲状态，CPU 的利用率并没有实现最大化。

图3-4 传统 SMP 架构网口数据处理图

AMP+架构对此进行了优化，CPU 不再与网口进行绑定，而是将网卡的收发包队列根据数据平面的 CPU 个数平均分配到每个 CPU 上，这样就保证了数据平面 CPU 的并行度，实现了 CPU 利用率的最大化。

图3-5 系统网口数据处理图

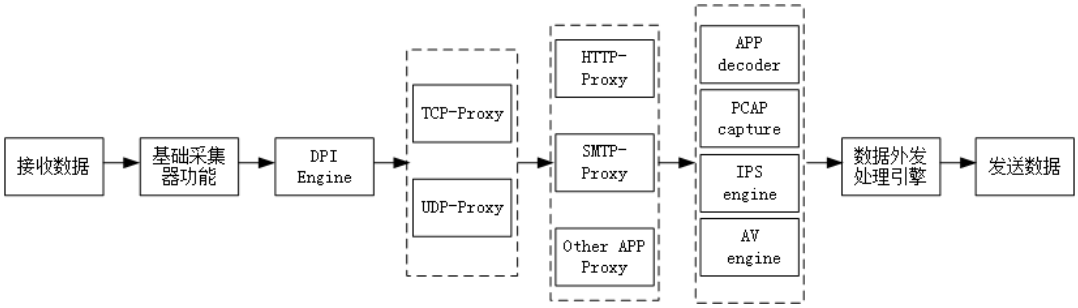


从图 3-5 中我们可以看出，只要任意一个网口有数据接收，所有的 CPU 就都会处于运行状态，CPU 的利用率到达了最大化。

3.2 高效的引擎一体化技术

奇安信网神威胁监测与分析系统依据 IP 网络层次对数据进行分层解析还原，采用一体化协议解析引擎，一次解析、多次引用，大大提升处理性能。奇安信网神威胁监测与分析系统一体化引擎一次处理数据的流程图如图 3-6 所示。

图3-6 一体化引擎数据处理流程图



整个数据的接收、数据的处理（包括应用层数据的处理，入侵检测、恶意文件等高级功能），数据的发送，都在数据平面完成，不涉及数据包的拷贝，进程切换等问题。同时数据的处理在整个转发阶段都使用同一个会话。这就极大的提高了应用层的处理速度，降低了整体数据转发的延迟。

3.3 多维度的威胁检测

拥有强大的恶意文件、漏洞库、海量情报储备能力，采集的流量通过机器学习等统计分析引擎、动态密码本比配、日志管关联分析引擎、Webshell 沙箱检测引擎、规则引擎等综合检测，能够及时有效识别网络中的威胁，产生威胁日志。此外具有 SSL 解密能力，让网络威胁无所遁形。

日志可外发到多种数据分析系统，供分析系统进行多种关联分析，同时，传感器本地可保留原始数据，降低大数据平台数据处理压力，具有事件追踪能力，支持以 pcap 包形式、文件形式的样本下载，攻击向量本地展示，支持跨 session 的关联分析，提高网络安全运营效率。

3.4 云端人工智能检测引擎

奇安信网神威胁监测与分析系统支持通过云检测和云沙箱检测新增恶意文件和未知恶意文件。

奇安信云检测引擎包含多项创新技术。具有基于安全大数据资源和强大的大数据存储和计算能力，把机器学习应用于在流量中发现安全威胁，采用机器学习的方法，在奇安信强大的云端大数据库基础上研发了全球首个人工智能杀毒引擎，这也是全球人工智能技术首次在杀毒领域的大规模应用。

云检测扫描速度快，而且检测效率高，即便是网上刚出现的木马，奇安信也能在几分钟内捕获并具备检测能力。

3.5 强大的威胁情报能力

奇安信网神公司云端威胁情报库拥有超过 100 亿样本、超过 90 亿 DNS 解析记录，13 亿 whois 信息，URL 数据库日查询量超过 300 亿，这些独特的海量原始数据是奇安信威胁情报最大的优势。

奇安信网神公司基于人工智能自学习的自动化数据处理技术，依靠以顶尖研究资源为基础的多个国内高水平安全研究实验室，为未知威胁的最终确认提供专业高水平的技术支撑。

- 所有大数据分析出的未知威胁都会通过专业的人员进行人工干预，做到精细分析，确认攻击手段、攻击对象以及攻击的目的。
- 通过人工智能结合大数据知识以及攻击者的多维度特征还原出攻击者的全貌，包括程序形态，不同编码风格和不同攻击原理的同源木马程序，恶意服务器（C&C）等，通过全貌特征‘跟踪’攻击者，持续的发现未知威胁，最终确保发现的未知威胁的准确性，并生成了可供终端平台使用的威胁情报。

同时，奇安信网神公司还是参与国际威胁情报交换共享项目最多的中国安全公司，合作过或正在合作的组织包括 Eicar、AMTSO、CSA、MVI、MAPP、MUTE、Wildlist 和 APWG 等。

3.6 强大的数据采集和外发能力

奇安信网神威胁监测与分析系统支持在线、离线流量、威胁数据数据采集，可基于多种参数定义采集流量，支持 19 种流量日志还原能力，支持威胁情报、恶意文件检测、入侵检测（漏洞检测和间谍软件检测）、网络层攻击检测、文件威胁鉴定器联动等多种威胁检测能力。同时支持将威胁日志和流量日志上传到态势感知平台、NGSOC 分析平台、大数据分析平台、Syslog 服务器、网闸以及日志收集与分析系统相关产品等支持传感器接入的产品设备。

3.7 采用高可用性奇安信 SecOS VI 操作系统

奇安信网神威胁监测与分析系统采用具备完全自主知识产权的网神第四代 SecOS 操作系统，整体框架采用 AMP+并行处理架构。AMP+架构是优化的多核异步并行处理架构。具备高稳定性、高性能的特点。

4 产品价值

4.1 最大限度识别网络威胁

基于奇安信网神公司大数据基础，强大的恶意文件、威胁、漏洞库等海量情报储备，配合高可用性 SecOS VI 操作系统，能够及时有效识别网络中的高级威胁。此外强大的 SSL 解密能力，让网络威胁无所遁形。

4.2 保障网络安全防护体系高效运营

通过合理部署奇安信网神威胁监测与分析系统，有效采集网络中的流量和威胁数据，并对流量进行多种威胁检测生成威胁日志。

通过将日志外发到多种数据分析系统，可以作为内网本地原始数据，供分析系统进行多种关联分析，降低大数据平台数据处理压力，提高网络安全运营效率。

4.3 威胁分类精细化，运营分析简易化

奇安信网神威胁监测与分析系统内置威胁分类 40+，增加威胁命中特征本地及外发高亮展示，促使运维人员分析威胁信息更快更准确。

4.4 SSL 解密通道的完善性

支持多种协议的解密，如 SMTPS/IMAPS/HTTPS/POP3S 等协议，并支持 session ticket 会话恢复机制。更大层面上展现出多维度协议的优势。并在 SSL 协商证书方面增加 ja3、ja3s 的字段，在分析解密层面更具有产出优势。

4.5 延伸存储、分析与解码能力

告警关联 pcap，平台可对威胁样本存储、关联等进行分析。并对邮件做了进一步的解密场景，效率更高。且基于框架实现可快速进行解码需求，支持巨帧，对主机增加攻击拦截的准确研判，有效的阻止非法恶意请求。

4.6 旁路阻断，做好第一层安全屏障

奇安信网神威胁监测与分析系统旁路部署，可针对特定源目的 IP 地址进行阻断、URL 重定向、DNS 重定向，增强防护，还可以针对阻断行为输出日志，便于管理员了解传感器行为，实现信息可查、可溯。

4.7 集中管控降低运维成本

奇安信网神威胁监测与分析系统，支持对接态势感知类平台实现集中管控、策略下发、特征库升级等，能够极大程度降低网络数据传感器在多区域分布部署场景下的运维成本。

4.8 增值服务提升产品使用体验

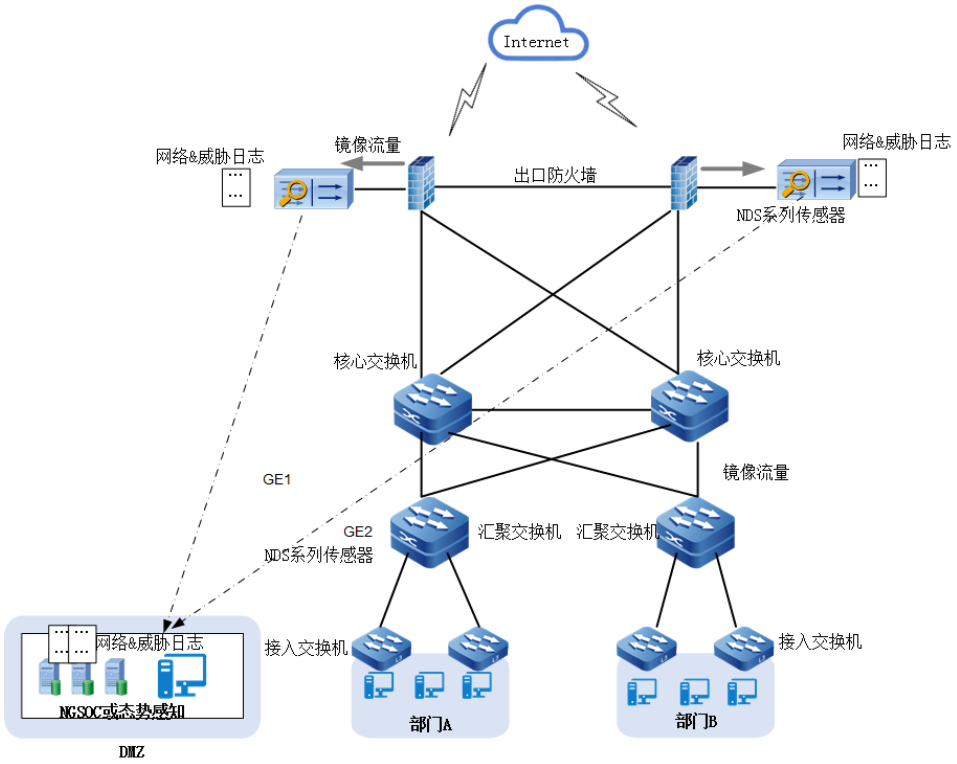
奇安信网神威胁监测与分析系统旁路接收镜像流量，通过被动指纹识别技术和浏览器识别技术，并根据资产识别的条件进行流量分析及应用检测，识别出用户网络中资产信息，为用户提供内网存活的详细资产清单，协助用户做到资产可见、可控。

5 典型应用场景

5.1 互联网出口安全检测

奇安信网神威胁监测与分析系统旁路部署在企业网或校园网的互联网出口设备上。互联网出口设备的流量镜像到奇安信网神威胁监测与分析系统，奇安信网神威胁监测与分析系统对流量协议类型、行为、域名等进行流量还原生成对应的网络日志，并可以对流量进行恶意文件、入侵行为等传统威胁检测，并通过威胁情报进行最新威胁检测，威胁检测生成对应的威胁日志。网络日志和威胁日志发送到态势感知平台或 NGSOC 分析平台进行分析展示。

图5-1 互联网出口应用场景



5.2 广域网（专网）边界安全检测

奇安信网神威胁监测与分析系统旁路部署在每个分支网络出口或专网出口设备上。隔离网络专网出口部署网闸。分支网络的奇安信网神威胁监测与分析系统的网络日志和威胁日志上传至网闸，通过网闸上传专网内的态势感知平台或 NGSOC 分析平台。多个奇安信网神威胁监测与分析系统可以通过态势感知平台或 NGSOC 分析平台进行统一配置升级等操作。内网的奇安信网神威胁监测与分析系统还原文件还可以上传文件鉴定器进行文件威胁检测。

图5-2 非隔离网络边界检测应用场景

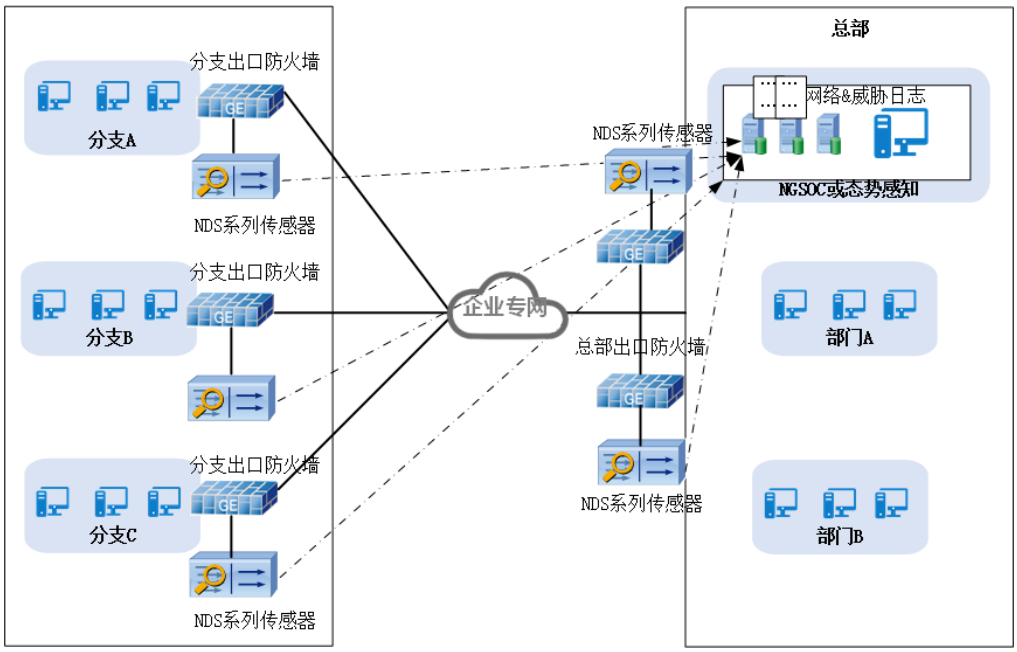
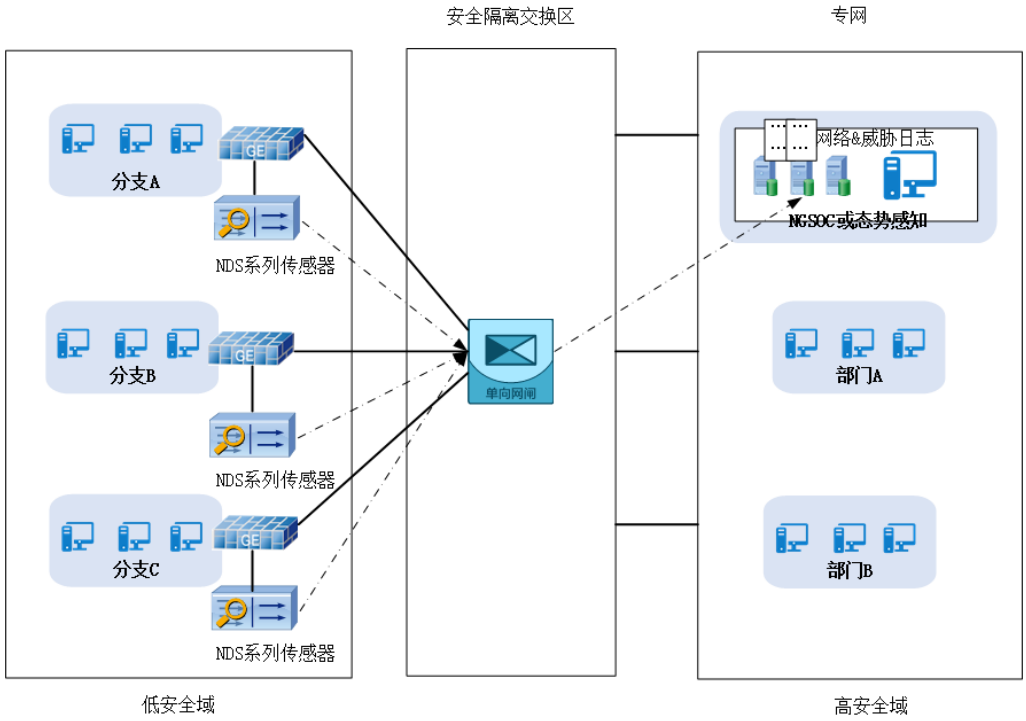


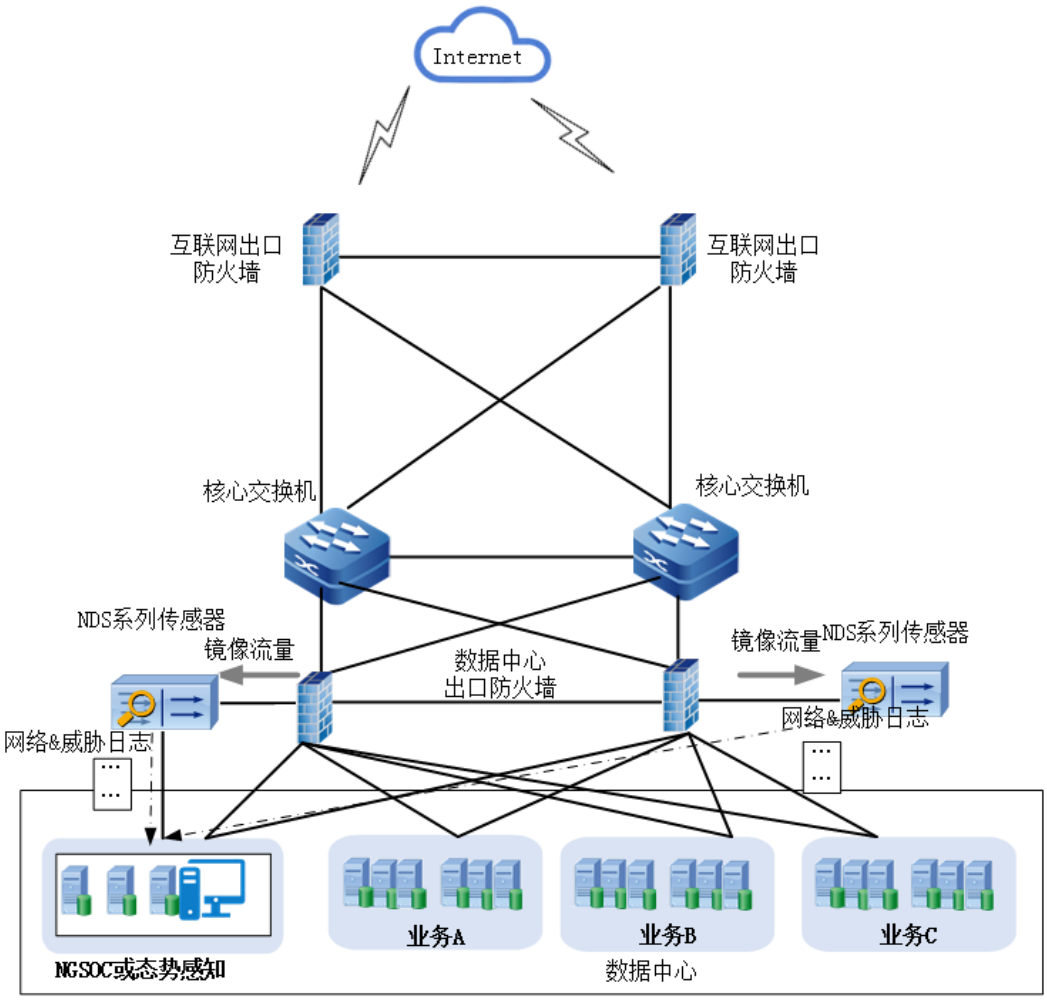
图5-3 隔离网络边界检测应用场景



5.3 IDC 出口安全检测

奇安信网神威胁监测与分析系统旁路部署在 IDC 出口设备上，全部 IDC 流量都由出口设备镜像到奇安信网神威胁监测与分析系统。奇安信网神威胁监测与分析系统对流量协议类型、行为、域名等进行流量还原生成对应的网络日志，并可以对流量进行恶意文件、入侵行为等传统威胁检测，并通过威胁情报进行最新威胁检测，威胁检测生成对应的威胁日志。网络日志和流量日志发送到态势感知平台或 NGSOC 分析平台进行分析展示。

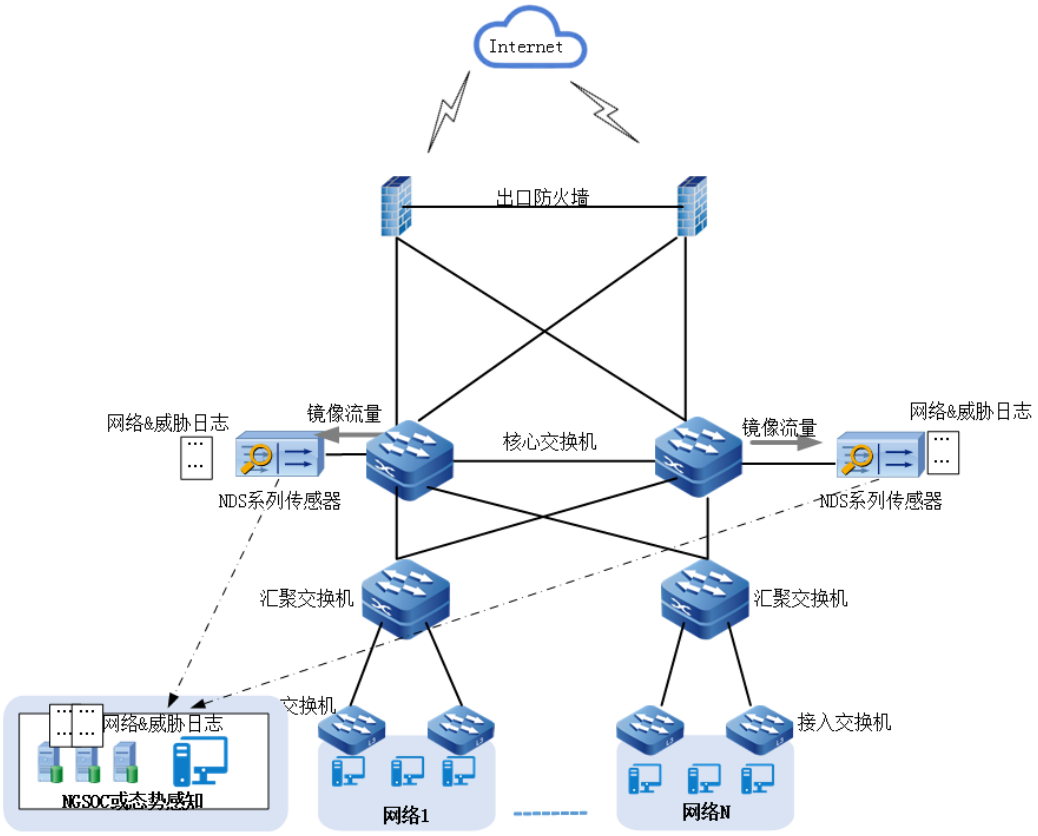
图5-4 IDC 出口应用场景



5.4 核心交换网安全检测

奇安信网神威胁监测与分析系统旁路部署在核心交换设备上，全部网络流量都由核心交换设备镜像到奇安信网神威胁监测与分析系统。奇安信网神威胁监测与分析系统对流量协议类型、行为、域名等进行流量还原生成对应的网络日志，并可以对流量进行恶意文件、入侵行为等传统威胁检测，并通过威胁情报进行最新威胁检测，威胁检测生成对应的威胁日志。网络日志和流量日志发送到态势感知平台或 NGSOC 分析平台进行分析展示。

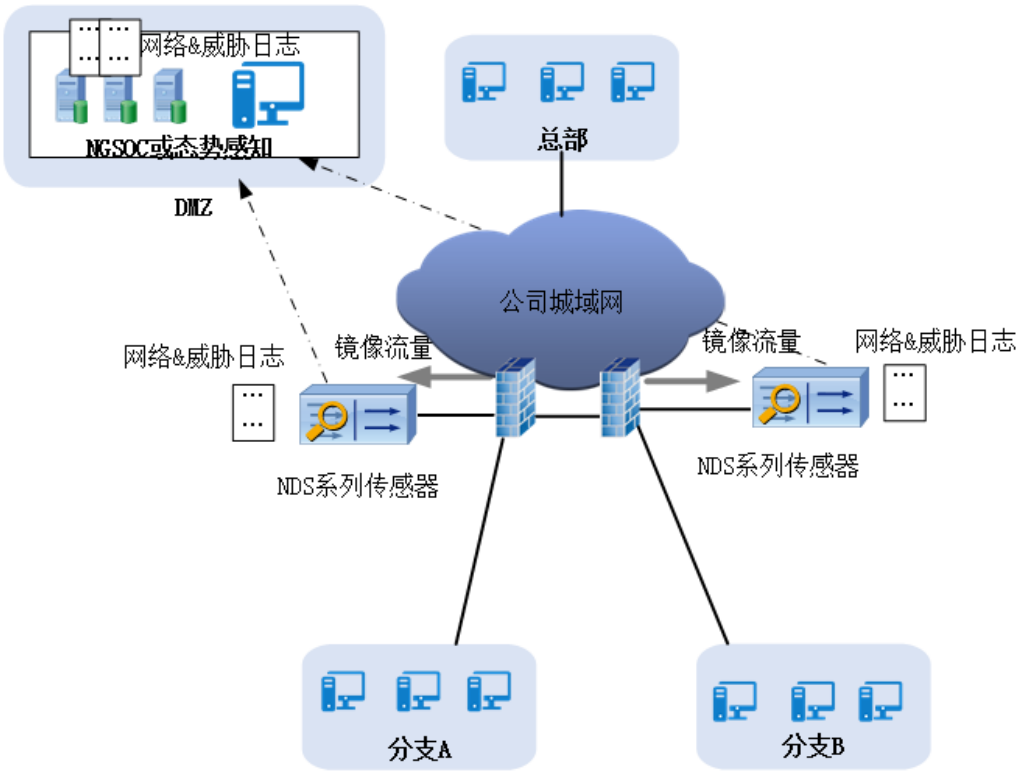
图5-5 核心交换网应用场景



5.5 城域网入口安全检测

奇安信网神威胁监测与分析系统旁路部署在城域网边界设备上，全部网络流量都有镜像到奇安信网神威胁监测与分析系统。奇安信网神威胁监测与分析系统对流量协议类型、行为、域名等进行流量还原生成对应的网络日志，并可以对流量进行恶意文件、入侵行为等传统威胁检测，并通过威胁情报进行最新威胁检测，威胁检测生成对应的威胁日志。网络日志和流量日志发送到态势感知平台或 NGSOC 分析平台进行分析展示。

图5-6 城域网入口应用场景



6 产品规格及组件

6.1 主机规格

产品指标	产品参数					
产品型号	TSS10000-S80	TSS10000-S81	TSS10000-S82	TSS10000-S83	TSS10000-S85	TSS10000-S86
传感器吞吐（bps）	2G	4G	5G	10G	15G	20G
标配并发连接数（万）	200	300	400	700	1000	1500
每秒新建连接数（万/秒）	8	10	15	30	40	60
板载电口 10/100/1000Base-T 个数	4	4	6	6	6	4
板载 SFP 千兆光口插槽个数	无					
板载 SFP 万兆光口插槽个数	无	2	4	4	4	4
扩展槽个数	2	2	2	2	2	1
网卡选配	按需选配（千兆电接口、千兆光接口、万兆光接口）型号网卡					
异步串行管理接口	1					
USB 接口个数	2					
标配存储容量	4TB					8TB
机箱规格&尺寸	1U（深 560mm* 宽 440mm*高 44mm）		2U（深 560mm* 宽 440mm*高 88mm）		2U（深 811.7mm*宽 478.8mm*高 87mm）	
温度和湿度	工作温度:0~40℃，存储温度:-25~70℃，相对湿度：5~90%不凝结					
电源	单电源	单电源/冗余电源		冗余电源		
	100-240V					
	250W 100-240V 1-2.5A			760W 11-5.5A		

6.2 接口板卡

板卡型号	板卡描述	适用主机
TY-TSS10000-QY-RJ45-4Q	千兆电接口扩展网卡，含 4 个千兆电网口	TSS10000-S80/S81/S82/S83/S85
TY-TSS10000-QY-SFP+-2W	万兆光接口扩展网卡，含 2 个万兆光接口	
TY-TSS10000-QY-SFP+-4W	万兆光接口扩展网卡，含 4 个万兆光接口	
TY-TSS10000-YSBT-RJ45-4Q	千兆电接口扩展网卡，含 4 个千兆电网口。	TSS10000- S86/S95G/S96G/S97G/S98G/ S99G、D84/D87/D94G/D97G(E)、/A95G(E)/A97G(E)/A98G(E) A82(E)/A84(E)/A85(E)/A87(E) /A88(E)/A92G(E)/A94G(E)/ A95G(E)/A97G(E)/A98G(E)
TY-TSS10000-YSBT-SFP+-2W	万兆光接口扩展网卡，含 2 个万兆光接口	
TY-TSS10000-YSBT-SFP+-4W	万兆光接口扩展网卡，含 4 个万兆光接口	

6.3 产品功能模块与特征库升级服务

授权类型	授权编码	授权描述
恶意文件分析功能模块规则升级授权	TY-TSS10000-S80-UDL-FIS	恶意文件分析功能模块一年恶意文件分析引擎规则库升级授权服务
规则库升级授权	TY-TSS10000-S80-UDL-RUL	提供 TSS10000-S80 引擎一年的规则升级授权服务
威胁情报升级授权	TY-TSS10000-S80-UDL-TI	提供 TSS10000-S80 引擎一年的威胁情报升级授权服务
恶意文件分析功能模块规则升级授权	TY-TSS10000-S81-UDL-FIS	恶意文件分析功能模块一年恶意文件分析引擎规则库升级授权服务
规则库升级授权	TY-TSS10000-S81-UDL-RUL	提供 TSS10000-S81 引擎一年的规则升级授权服务
威胁情报升级授权	TY-TSS10000-S81-UDL-TI	提供 TSS10000-S81 引擎一年的威胁情报升级授权服务
恶意文件分析功能模块规则升级授权	TY-TSS10000-S82-UDL-FIS	恶意文件分析功能模块一年恶意文件分析引擎规则库升级授权服务
规则库升级授权	TY-TSS10000-S82-UDL-RUL	提供 TSS10000-S82 引擎一年的规则升级授权服务
威胁情报升级授权	TY-TSS10000-S82-UDL-TI	提供 TSS10000-S82 引擎一年的威胁情报升级授权服务
恶意文件分析功能模块规则升级授权	TY-TSS10000-S83-UDL-FIS	恶意文件分析功能模块一年恶意文件分析引擎规则库升级授权服务
规则库升级授权	TY-TSS10000-S83-UDL-RUL	提供 TSS10000-S83 引擎一年的规则升级授权服务
威胁情报升级授权	TY-TSS10000-S83-UDL-TI	提供 TSS10000-S83 引擎一年的威胁情报升级授权服务
恶意文件分析功能模块规则升级授权	TY-TSS10000-S85-UDL-FIS	恶意文件分析功能模块一年恶意文件分析引擎规则库升级授权服务

规则库升级授权	TY-TSS10000-S85-UDL-RUL	提供 TSS10000-S85 引擎一年的规则升级授权服务
威胁情报升级授权	TY-TSS10000-S85-UDL-TI	提供 TSS10000-S85 引擎一年的威胁情报升级授权服务
规则库升级授权	TY-TSS10000-S86-UDL-RUL	提供 TSS10000-S86 引擎一年的规则升级授权服务
威胁情报升级授权	TY-TSS10000-S86-UDL-TI	提供 TSS10000-S86 引擎一年的威胁情报升级授权服务

6.4 接口模块

模块型号	模块类型	适用接口
NF-SFP-10GE-MM-550M	万兆光模块，多模（850nm，550m，LC）	TSS10000-S80/S81/S82/S83/S85/S86
NF-SFP-10GE-SM-10KM	万兆光模块，单模（1310nm，10km，LC）	
NF-SFP-GE-MM-550M	千兆光模块，多模（850nm，550m，LC）	
NF-SFP-GE-SM-10KM	千兆光模块，单模（1310nm，10km，LC）	