Hillstone®
山 石 网 科

智源智能安全运营平台常见问题及解答（FAQ）手册

Version 1.0

Hillstone Networks

本文档禁止用于任何商业用途。

联系信息

北京

地址：北京市海淀区宝盛南路1号院20号楼5层

邮编： 100192

苏州

地址：苏州高新区科技城景润路181号

邮编：215000

联系我们：http://www.hillstonenet.com.cn/about/contact_Hillstone.html

关于本手册

本手册为山石网科智源智能安全运营平台使用过程中的常见问题及解答。

获得更多的文档资料，请访问：https://docs.hillstonenet.com.cn

针对本文档的反馈，请发送邮件到：TechDocs@hillstonenet.com

山石网科

https://www.hillstonenet.com.cn

TWNO: TW-FAQ-iSource-CN-V1.0-6/21/2022

目 录

常见问题及解答介绍

本手册为山石网科智源智能安全运营平台使用过程中的常见问题及解答，包含以下章节：

- 产品优势及定位：解答产品的优势、竞争力、价值、选型等问题，帮助用户理解产品和功能，以及在实际网络环境中如何选择产品。
- 功能类问答：解答常见的硬件问题、许可证问题、特征库问题以及软件功能支持类问题。
- 故障类问答：解答产品使用过程中的基础常见故障。

更多资源

除本手册外，您还可以通过以下途径获取产品相关的信息及配置指导：

- 查看产品功能及配置手册：
  - PC端技术文档在线系统：https://docs.hillstonenet.com；
  - 移动端技术文档在线系统：用手机扫描以下二维码：

产品优势及定位问答

本节为智源产品优势及定位常见问答，主要向用户传递产品优势、竞争力、价值、选型等信息，帮助用户理解产品和功能，以及在实际网络环境中如何选择产品。

1. 智源的定位是什么？

智源智能安全运营平台，基于云、网、端综合分析的态势感知体系，通过全链条数据采集大数据关联分析，实现高级威胁检测预警溯源，配合SOAR，实现剧本可视化编排，同时联动安全实体，实现事件的处置闭环。

2. 智源有哪些功能特点？

主要有以下几方面：

- 云网端架构：云端/本地情报利用，探针接入流量，同时支持不同品牌/种类安全设备（网络侧、端侧等）数据接入
- 全息态势：多维度动态大屏、自定义统计大屏、威胁事件可视化
- 高级威胁：顶级情报库，威胁检测与分析引擎（NTA，Gartner国内唯一推荐级）
- 溯源取证：攻击阶段定位，证据信息留存（支持pacp包下载），SPL语言检索
- 响应闭环：可视化编排剧本，按需配置条件（自动/人工二次确认），联动实体响应处置
- 资产测绘：自动探测内网资产、精准识别资产类型，实现内网资产梳理，及时发现资产威胁

3. 智源能够匹配用户的哪些需求和技术趋势？

结合最近市场反馈较多的热词和技术趋势，智源可以实现和匹配的需求如下：

- **态势感知**：态势感知综合分析网络安全要素、评估网络安全状态及变化并预测其发展，将内网态势以可视化的方式展现给用户。重点在于通过大数据、关联分析等技术加深对内网威胁的捕捉和预测。
- **SOAR**：安全编排和自动化响应。通过预定义剧本形成标准化流程，对不同类型的安全事件实现自动化响应，将网络安全运营数字化、流程化管理，有效提高安全事件响应效率。

- **XDR**：XDR将云网端的安全数据（威胁情报、端点数据、安全日志、流量分析数据、云端安全数据等）综合到一个体系中，结合大数据、人工智能、自动化技术，实现对威胁或攻击的快速检测、自动化响应和自适应优化。
- **安全运营**：安全运营是技术、流程和人的有机结合。主要体现在平台+服务的AI+HI实现。主动管理安全问题、检测安全事件、响应及处理已知的风险定期排查资产，全量收集信息，持续分析、监测，动态提升整体防御能力。
- **全流量取证**：对内网全息流量进行采集与分析。具备完整攻击链的全过程信息存储和展示，实现对威胁事件的溯源。常在HW场景对全流量回溯取证技术提出要求。
- **资产测绘**：资产测绘主动对用户内网资产存活状态进行快速探测、对全网各类资产进行精准识别。通过自动分析与资产相关的威胁事件、风险行为和弱点判断资产的失陷情况，构建可持续安全运营体系。

4. 智源主要针对哪些目标市场？

目标市场是全行业。针对一些重点行业深入挖掘机会点，详表如下：

行业	销售机会
医疗	等保建设需求；卫健委对下级医院安全运营中心的监管场景；信息系统业务安全需求（挖矿/勒索、资产梳理、高级威胁监测溯源、安全运营闭环等）。
高校	校园等保建设；校园等保安全、教育行业完网络安全综合治理行动、挖矿/勒索清零计划、日常/重保安全运营保障、信息资产梳理、校园网络安全情况可视化等。
企业	XDR能力建设、总部与分支的安全运营、业务与安全融合需求（不同业务场景的威胁检测分析处置流程、未知威胁感知、威胁溯源、可视化运营）等。
政府	顶层设计规划、自监管/行业监管建设、运营闭环、可持续安全运营能力升级完善等。

5. 如何针对不同应用场景选择产品？

主要根据客户现网所需要检测的总流量大小（因流量模型不同可能产生差异）：

量级	产品	推荐型号	卖点	说明
小级	智源平台	SG-6000-ISC6205 SG-6000-ISC6210 SG-6000-ISC6220	具备基本平台级能力，可以收集并分析安全设备日志、漏扫信息、终	• 现网总流量＜1Gbps：SG-6000-ISC6205 + sBDS-I1837-

量级	产品	推荐型号	卖点	说明
			端安全等数据并与安全实体进行联动闭环。	ThreatSensor • 现网总流量1Gbps-2Gbps：SG-6000-ISC6205 + sBDS-I2835-ThreatSensor • 现网总流量2Gbps-5Gbps：SG-6000-ISC6210 + sBDS-I3835-ThreatSensor • 现网总流量5Gbps-6Gbps：SG-6000-ISC6210 + sBDS-I5835-ThreatSensor • 现网总流量6Gbps-10Gbps：SG-6000-ISC6220 + sBDS-I5835-ThreatSensor • 现网总流量 > 10Gbps：集群+探针下沉部署
常规	智源平台	SG-6000-ISC6205 SG-6000-ISC6210 SG-6000-ISC6220	具备安全运营平台级能力，在小量级基础上可对流量进行接入，强化威胁检测及流量分析能力。	
	威胁探针	sBDS-I1837-ThreatSensor sBDS-I2835-ThreatSensor sBDS-I3835-ThreatSensor sBDS-I5835-ThreatSensor		
强化	智源平台	SG-6000-ISC6205 SG-6000-ISC6210 SG-6000-ISC6220	更为强化的安全运营平台级能力，在常规级基础上，增加了对终端的管控能力，威胁及处置可定位到进程级。	
	威胁探针	sBDS-I1837-ThreatSensor sBDS-I2835-ThreatSensor sBDS-I3835-ThreatSensor sBDS-I5835-ThreatSensor		
	EDR	Server数量&PC数量		

注意: 探针型号sBDS-I1830-ThreatSensor、sBDS-I2830-ThreatSensor、sBDS-I3830-ThreatSensor、sBDS-I5830-ThreatSensor即将退市，故选型表格中不再推荐，在用客户正常维护。

功能类问答

本节为智源产品功能类问题及答案，主要解答用户常问的硬件问题、许可证问题、特征库问题以及软件功能问题。

硬件问答

1. 智源平台单机可以扩展至集群吗？

可以。智源平台单机扩展至集群，操作步骤如下：

1. 已经部署的智源平台当作Master
2. 后续添加的智源平台当作Slave
3. 将已部署的智源平台Master、Slave添加到集群

将智源平台单机扩展至集群的详细配置案例及步骤，请访问技术文档在线系统，查阅《智源智能安全运营平台 WebUI用户手册》。

2. 智源平台断电后，平台访问不了，需要人工去机房重新启动吗？

平台断电之后不会自动重启，需要人工给设备上电，短按设备上的电源键开关即可开机。电源键如下图红框所示：

3. 智源平台万兆扩展模块可以插入千兆光模块吗？

支持。智源平台支持的万兆扩展模块为IOC-IS-2SFP+，提供2个万兆SFP+接口，插入千兆光模块后，接口传输速率自动切换为1Gbps。

4. 智源前面板硬盘灯亮红灯怎么处置？

硬盘灯绿色是正常状态。如果硬盘灯为红色，请将智源关机，将硬盘重新插拔后开机，如果硬盘灯还显示为红色，表示该硬盘已损坏，需要返厂维修。

5. 智源设备如何关机？

智源设备有以下几种关机方法：

- 登录进入WebUI后，在“系统设置 > 系统信息”页面右上角，点击“关机”按钮；
- 登录进入CLI（命令行接口）后，输入**shutdown**命令；
- 短按设备上的电源键关机（待设备电源指示灯变成黄色，硬盘灯熄灭，风扇停止，即系统关机完毕）；
- 长按设备上的电源键关机（长按相当于强制断电，可能会造成系统文件损坏、历史数据丢失或者系统故障，**不建议使用**）。

许可证问答

6. 智源授权过期，平台能否继续使用？

智源授权过期，平台可以继续使用，已连接的探针也可以继续使用，但不能将新的探针注册到平台，且不能进行平台系统版本升级。

7. 智源授权过期，是否还能发现威胁事件？

智源授权过期，可以发现威胁事件，但不能将新的探针注册到平台，且不能进行平台系统版本升级。

特征库问答

8. 如何查看威胁情报库的历史升级情况？

通过系统日志可以查看到特征库升级的历史信息，在WebUI界面点击“系统设置 > 系统日志 > 操作日志”。

软件功能支持问答

9. 智源是否支持Ping?

智源从V2.0R3版本开始支持Ping。V2.0R4之前的版本中Ping功能默认关闭，可以在CLI使用ping on 命令开启；从V2.0R4以及V2.0R4之后的版本开始，Ping功能默认开启。

10. 态势感知平台与探针之间的数据传输是加密的吗？

是加密的。

11. 智源V2.0R5版本能不能作为软件化部署在客户的环境中？

智源V2.0R5版本及以后版本均支持软件化部署。

12. 挖矿通信行为和挖矿行为检测依据分别是什么？

挖矿通信行为检测依据：智源检测探针上送的MetaData中的挖矿域名；

挖矿行为检测依据：智源检测Sysmon上送的PC访问的挖矿IP；

挖矿恶意IP检测依据：智源检测探针上送的MetaData中的挖矿IP；

挖矿恶意URL检测依据：智源检测探针上送的MetaData中的挖矿URL。

13. 智源威胁情报库和云瞻是同步的吗？

网络连通的情况下，智源威胁情报库和云瞻是同步更新的；网络断开的情况下，需要手动导入最新威胁情报库包。

14. 智源Web界面能查询多长时间内的Syslog/MetaData/NetFlow/Sysmon日志？

Web界面可以查询最长180天内的Syslog日志信息，但一次查询的起止时间跨度不能超过30天；可以查询2天内的MetaData日志信息；可以查询2天内的NetFlow日志信息；可以查询2天内的Sysmon日志信息。

15. 智源威胁分析的日志模块中看不到其他设备发过来的日志，如何通过抓包确定日志有没有发送到智源？

请参考以下步骤：

1. 发邮件给智源TME申请shell密码，包含设备SN号和Version。
2. 后台输入shell，输入shell密码。
3. 开启抓包。抓包命令为**tcpdump -i***interface-name***udp and port***port-num***and host***ip-address* **– vv**（其中*interface-name*为接口名称，*port-num*为端口号，*ip-address*为其它设备的IP地址。例如**tcpdump -i br0 udp and port 514 and host 10.182.210.11 – vv**）。
4. 屏幕显示该IP的日志说明智源已接收到日志；屏幕不显示该IP说明智源未接收到日志，建议检查网络是否可达，对端是否发出Syslog日志。

16. 智源WebUI忘记密码怎么办？

目前智源使用WebUI和CLI两套认证机制，仅忘记WebUI密码，可使用SSH登录CLI，然后使用**password reset webui**命令重置WebUI密码。

17. 智源配置的剧本显示状态为失败如何处置?

请参考以下步骤:

1. 点击“事件响应 > 剧本管理”，打开剧本管理页面。
2. 在剧本总览部分，点击“失败任务”对应的数字，系统将跳转至<响应记录>标签页。
3. 点击“操作”列的响应详情展开对应剧本拓扑图，点击拓扑图中的红色节点（红色节点表示执行失败的节点）。
4. 查看失败节点的运行数据、提示消息以及配置详情，确定失败原因。

18. 智源添加威胁情报的实体，如何获取API Key?

访问网址https://ti.hillstonenet.com.cn/main，点击页面右上方的“用户 > 应用授权管理”即可获取API Key。

19. 不同的日志可以用相同的模板进行解析吗?

可以。解析方式主要分为三大类，Grok解析、Key-Value解析、JSON解析。其中Grok解析是较为精细化的匹配，Key-Value解析、JSON解析是较有规律的解析模板，相对较宽松。故如果解析规则中没有指定日志源IP，且日志规律、标准化配置也相同时，同一模板就可以解析不同的日志。因此在创建解析规则时指定日志源IP就可以避免解析重复或者混乱。

20. 第三方日志解析配置时，部分字符的解释?

第三方日志解析配置时，部分字符解释如下:

- /s+匹配至少一个空格，可以用grok表达式%{SPACE}代替；%{SPACE}的正则表达式\s*是0个或多个空格。
- %{SYSLOGTIMESTAMP}匹配Syslog标准的时间格式，匹配MONTH DAY HH:mm:ss，月份可以是全写March 也可以是简写Mar。但首字母须大写。日期为数字，时间为HH:MM:ss。（1可以写成01，也可以是1）。

故障类问答

本节为智源产品故障类问题及答案，主要解答产品使用过程中遇到的基础常见故障。

1. 为什么大屏运行一段时间后自动中断？

浏览器安全设置问题。可以在智源“系统信息”中下载根证书，然后导入到浏览器中。

2. 资产导入失败的原因有哪些？

资产导入失败的原因可能有：

- 导入的文件不是.csv格式的文件；
- 内容填写错误/重复；
- 将旧版本的资产管理文件导入到V2.0R4及以后版本的智源平台，平台报错“导入的文件内容格式不正确”。因为新模版中有些字段有“*”，老版本模板中没有，需要将老版本模板中对应字段也加上“*”。

	A	B	C	D	E	F	G	H	I	J	K	L
1	###服务器csv文件模版（服务器必填“IP地址”，服务器组必填“IP地址段”，其他带*的为必填字段 保存时请务必以另存为csv逗号分隔的形式保存 导入前请删除示例数据）											
2	服务器/组名称*	是否为组*	IP地址	IP地址段	所属区域*	资产价值*	业务	服务类型	操作系统	责任人姓名	责任人邮箱	描述
3	示例服务器1	否	192.168.0.1		上海区	重要	互联网金融	HTTP	Windows	张三	zs@hillstonenet.com	64字以内都行
4	示例服务器组2	是		192.168.1.1-192.168	江苏区	一般	电子商务	FTP/HTTPS/HT	Linux	李四	ls@hillstonenet.com	64字以内都行
5												
6												
7												
8												
9												

3. 智源版本升级失败的原因有哪些？

智源版本升级失败的原因可能有：

- 平台License已过期；
- 下载的升级文件MD5错误；
- 升级版本文件低于当前版本（智源不支持降级）。

4. 为什么智源登录UI后报服务器内部错误或者首页白屏？

智源仅支持Chrome 78及以上版本，使用低于78版本的Chrome浏览器会出现以上问题。

5. 为什么将流量接入到流量探针后，流量探针下行流量为0？

请参考以下步骤排查：

1. 首先查看是否在流量探针上插入了扩展模块；
2. 插入扩展模块后，查看是否开启了流量分析功能。启用流量分析功能后，流量探针才会对流量进行处理。

6. 使用科来发包工具发包到探针后，智源检测出的威胁源IP为什么不是用户内网和发包PC的IP地址，而是报文中的IP地址？

这与科来发包软件有关。采用科来软件进行发包时不会修改报文中的源目的IP，因此报文中的IP地址会被智源检测到。

7. 为什么在威胁探针上可以查看到疑似勒索病毒的事件，但是平台没有展示疑似勒索病毒的事件？

在V2.0R4版本之前，“疑似勒索病毒事件”在智源平台展示为“可疑的SMB行为”；从V2.0R4版本开始，智源平台上展示的威胁事件名称与威胁探针上的威胁事件名称一致。

8. 为什么将含有ARP欺骗攻击的流量镜像到威胁探针之后，智源平台并没有报出相关威胁？

智源平台已配置自定义威胁日志规则，可以报出所有威胁探针检测的事件。如果威胁探针未检测出ARP攻击的威胁事件，那平台就不会报出相应威胁。

9. 为什么威胁探针无法报ARP欺骗攻击？

威胁探针ARP防护的配置对于ARP欺骗的检测是基于二层的，当用户使用三层设备镜像流量，镜像流量中不包含ARP相关流量，就不会报出ARP欺骗攻击。如果通过二层设备镜像流量就可以正常报出威胁并上报智源。

10. 用户的环境ARP表被打满，为什么威胁探针没有报出相关威胁？

首先，需要确定用户环境中是否还有ARP流量；其次，威胁探针ARP防护对于ARP欺骗攻击的检测是基于二层的，对二层流量的检测是正常的。用户交换机MAC表被打满应该是ARP泛洪，应由AD引擎

进行检测，需在安全域配置页面进行配置，但镜像流量的Tap域没有ARP检测阈值的相关配置。因此，目前威胁探针无法检测出ARP泛洪攻击，可通过联动防火墙实现防护。

11. 为什么在威胁探针上可以通过命令行查看到UDP Flood的威胁日志，却无法通过WebUI查看到相应的威胁日志和威胁事件？

因为UDP Flood攻击是由AD引擎检出的，通常情况下仅记录威胁日志，不展示威胁事件。而威胁探针设备去掉了原先BDS中的威胁日志展示模块，所以在WebUI查看不到威胁日志。但该日志会上传到智源平台，通过配置威胁日志规则可以进一步报出威胁事件。

12. 为什么流量探针或威胁探针显示已连接平台，但在平台上却无法查看到探针？

主要因为智源平台授权过期或未授权，导致探针无法注册，因此在平台上无法查看到探针。

13. 智源平台和流量探针Web界面出现一些字码错乱（如序号‘5’显示成了‘五’等），是什么原因？

这是因为Chrome浏览器开启了自动翻译功能，导致Web界面字码错乱，关闭自动翻译即可。

14. 为什么根据其它厂商日志规范配置的解析模板，无法将日志解析入库？

请参考以下步骤排查：

1. 排查对方设备是否正确配置发送日志至智源（UDP、514）；
2. 从V2.0R4版本以后，可以在“威胁分析 > 日志 > Syslog > 其他日志 > 未识别日志”中查看上送的日志格式是否匹配解析模板；
3. 查看kafka topic的内容，检查实际的上送日志是否匹配解析模板，需根据实际上送的日志重新配置解析模板。

15. 智源触发剧本下发黑名单IP，为什么在智源上删除剧本后还是一直有黑名单下发到防火墙？

当前智源下发黑名单是根据剧本配置的IP阻断时长确定的，如果时长低于60分钟，那么会直接下发；如果时长大于60分钟，会每30分钟下发一次，触发剧本之后就和剧本就没有关系了，删除剧本后还是会每隔30分钟下发一次，直到配置的阻断时长。

取消黑名单下发，有以下几种方法：

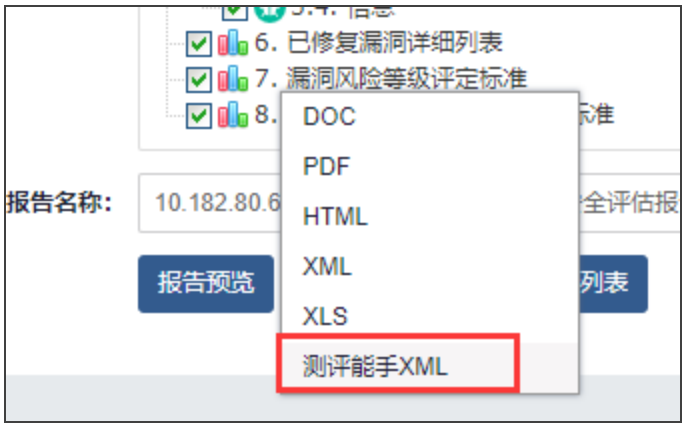
- 等待黑名单时间结束；
- 到联动实体（比如防火墙）删除下发的黑名单；
- 进入“事件响应 > 联动实体”，然后进入对应的联动实体的阻断IP详情中，删除对应IP的IP阻断。

16. 智源是否支持通过转接器连接平台网口和PC?

目前平台网口无法使用转接器连接，需要直连电脑网口。

17. 将山石RAS XML格式的报告导入到智源平台导入成功，但日志显示解析失败，是什么原因？

智源支持导入并进行解析的xml格式报告包括绿盟RSAS的xml格式报告、山石网科RAS（远程安全评估系统Remote Assessment System）的测评能手xml格式报告。山石网科RAS测评能手xml格式报告如下图：



18. 使用FTP传输文件类威胁为何无法检出威胁？

文件类威胁需要HTTP协议传输文件，FTP是无法检测出的。

19. 为什么智源硬盘显示大小小于标称值？

智源使用RAID 5和RAID 1，提升可靠性，实际可用小于标称值。

20. 为什么跨网段无法访问智源，同网段可以访问？

实际没有这个限制，特殊情况下因为智源内部使用了一些IP，跨网段IP和内部IP冲突会导致无法跨网段访问。内部IP如下：

- 默认内部IP：10.219.149.225/27（V2.0R4后新增默认内部IP：10.219.148.1/23）
- 默认docker0 IP：172.17.0.1/16
- flannel1 IP：10.244.0.0/16

另外，如果用户在智源上没有使用默认的内部IP，而是单独配置了内部IP网段，那么这个网段也不可以跨网段访问。