JUMING 聚铭
让安全更简单

聚铭 安全产品

EASIER WAY FOR SECURITY

累计服务10000+政企客户

聚铭网络流量智能分析审计系统

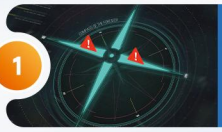
(iNFA)

聚铭网络
www.juminfo.com

聚铭网络流量智能分析审计系统（iNFA）

全流量监控 零死角防御

您是否有这些安全困扰？



1

常规流量 监控局限

传统流量监控主要关注南北向流量，忽视了内部的东西向流量，造成安全盲区。

2

资产繁杂 风险难控

企业资产种类繁多，管理难度大，潜在威胁难以全面掌握。

3

攻击隐蔽 威胁难察

防火墙、IPS、WAF等传统安全设备，对于藏匿于数据包中未知威胁检测能力较为薄弱。

4

海量告警 真伪难辨

传统安全检测机制易产生误报，导致海量告警真假难辨，增加运维团队工作负担。

5

数据匮乏 溯源受限

安全检测信息缺失严重影响了对攻击行为的全面理解，导致威胁溯源难度增加。

6

响应滞后 应对不足

高级威胁研判工作对人员能力要求高，被动防御疲于奔命，安全防护应对不足。

全流量智能化审计能手

聚铭网络流量智能分析审计，以旁路方式接入网络，实时分析南北向及东西向流量，深度识别、解析、检测，挖掘已知及未知威胁，同时对网络威胁或异常流量进行追踪溯源、响应拦截、安全处置，从而保障整个信息化系统安全高效的运行。

产品亮点

千余种协议解析，网络全流量采集

精准解析2-7层千余种应用协议，具备解析工控、5G、物联网等非常规流量协议，助力用户多场景下流量安全检测。

基于AI的威胁分析识别技术
已知未知威胁一网打尽

全量采集东西南北向流量数据，结合威胁样本生成算法模型，针对恶意加密流量、隐蔽外连、DGA、域名快闪攻击等进行智能AI分析，挖掘潜在高级威胁。

安全告警研判技术
去伪存真降低误报

双向全流量分析，自动判断攻击成功失败，精准识别针对性攻击，让用户聚焦真实威胁。

全量留存溯源取证技术
完整还原攻击路径定位真凶

多维度溯源取证

千余种应用协议深度还原，全量会话及威胁数据包留存、结合恶意程序抓捕工具方式无死角回溯取证。

实名溯源取证

针对DHCP场景中发现的未知威胁，可实名追溯攻击链上的各个设备，定位攻击源和被攻击目标的实名账号。

攻击路径溯源

以时间线聚合展示安全事件，清晰梳理攻击路径和活动轨迹。

万能联动 智能布控

万能联动

不受第三方设备API限制,可智能化完成第三方设备的对接,对防火墙、EDR等设备实现万能联动,及时完成对未知威胁的反制。

智能布控

基于可视化预定义的场景策略,利用精准研判、万能联动技术,实现安全事件自动研判处置,实现主动防御避免扩散能力。

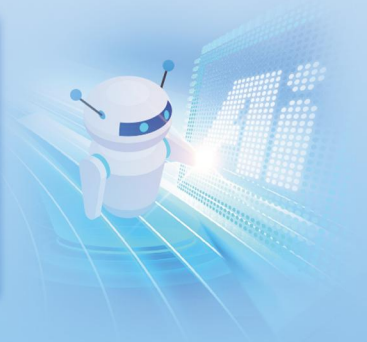
AI大模型赋能 运维省心省力

告警智能分析

小白变专家: 融合安全垂直领域的先进大模型技术,实现告警一键分析解读,安全运维研判分析简单易用。

智能客服 随叫随到

聚铭AI助手随时待命,即时解答您的所有疑问,让运维工作更加得心应手。



四 更多威胁分析能力

资产全面测绘

识别资产端口、服务、应用名称和版本; 动态发掘影子资产。

攻击面收敛

智能判定应用对外开放动态,识别登录入口风险,协助梳理验证管理策略,实现攻击面收敛。

安全事件分析

从主机视角、外部攻击视角、内部溯源视角全面剖析威胁事件。

攻击者分析

将攻击者特征聚合,并对攻击进行自动化分析和提取,勾勒完整的攻击者画像。

聚铭 juminc

聚铭订阅号

荣获国家发明专利20余项
通过【ISO9001质量管理体系认证】【ISO27001信息安全管理体系认证】
【ISO20000信息技术服务管理体系认证】
【ISO14001环境管理体系认证】【ISO45001职业健康安全管理体系认证】
【CCRC信息安全风险评估服务资质认证】【CCRC信息安全应急处理服务资质认证】

公司地址：江苏省南京市雨花台区软件大道180号南京大数据产业基地7栋4层
电话：025-52205520　　传真：025-52205565
全国统一服务热线：400-1158-400　　公司官网：www.juminfo.com