JUMING 聚铭®

让安全更简单

# 聚铭 安全服务

EASIER WAY FOR SECURITY

累计服务10000+政企客户

# 聚铭下一代
# 智慧安全运营中心
# (AISOC)

聚铭网络

www.juminfo.com

# 聚铭下一代智慧安全运营中心

聚铭下一代智慧安全运营中心是提升用户网络安全建设管理工作的智能化指挥作战中心。平台以“人机共生，智慧运营”为核心理念，依靠大数据挖掘、AI 算法、智能降噪等关键技术，构筑全流程自动化的安全动态防御体系。结合用户实际安全场景和业务需求提供专业报告和安全指导，动态优化安全工作流程、组织架构和配套制度，做到弱人工化、重智能化的安全运营，最终实现安全设备、安全数据、安全管理“效能最大化”的目标。


平台功能示意

## 现状分析

**安全风险高**

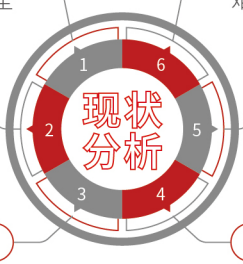
网络攻击、数据泄露等事件频发，传统静态防御方式无法应对，安全理念逐渐从单点安全设备转向全面安全运营。

**工作价值体现难**

安全运维成果讲不清、安全工作绩效难衡量，安全工作价值难以获得认可。

**安全设备多**

安全设备增多，需要对各类设备做到统一纳管和联防联控，进一步提升安全效果和安全价值。




**数智化程度低**

安全处置及安全运维智能化、自动化程度低，缺乏持续迭代自优自学习能力。

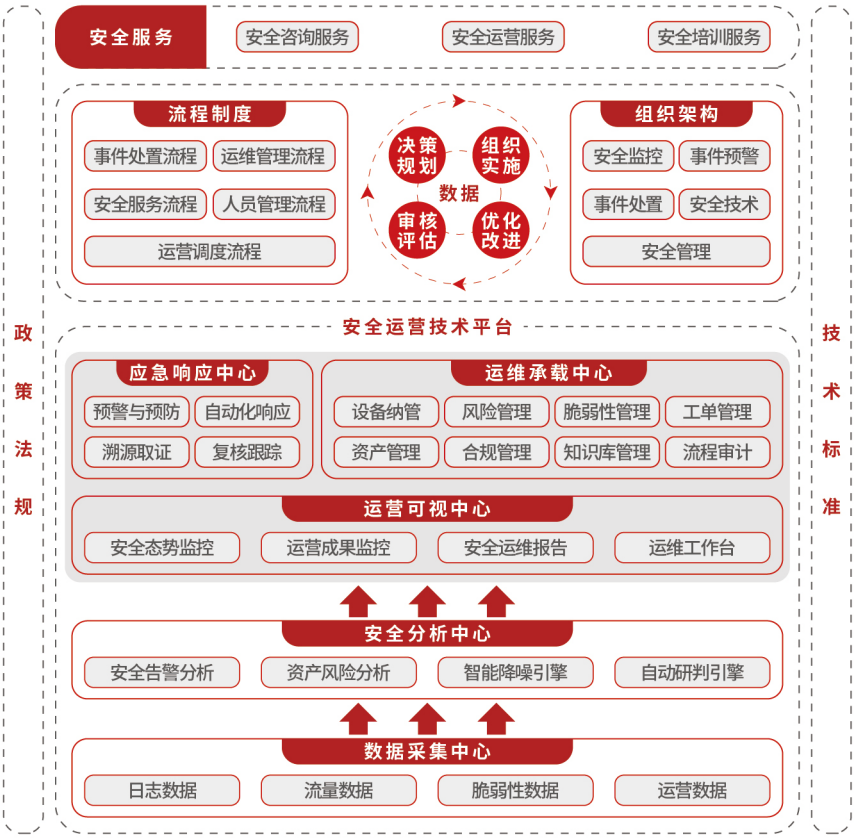
**运维压力大**

安全管理工作体系制度不完善，工作流程冗杂，同时又过度依赖专家服务保障，人力成本高。

**监管要求严**

随着《网络安全法》、《等保 2.0》等政策法规落地，对安全建设提出了更加严格的标准，监管压力倍增。

## 2 安全运营体系建设




## 3 建设阶段

### 第一阶段 基础运营能力建设

完成多维数据的统一采集分析，安全设备的统一纳管，以及用户资产的统一梳理评估。通过补全安全设备、数据维度和安全服务，做到对安全威胁的深度分析，及时响应处置安全事件。

### 第二阶段 自动化运营能力建设

形成标准、合规、实用的专属流程制度和组织架构，自动化完成安全事件响应、安全运维、资产管理、安全管理等流程。

### 第三阶段 数智化运营能力持续建设

基于“云＋端”体系持续迭代平台运营能力，形成专属数智化安全运营生态，提升已建安全体系的对抗性和实战性，打造持续沉淀、共享、可生长的安全运营体系。

## 4 核心优势

### 多维融合 纵深威胁检测

以资产为核心，统一采集日志、流量、脆弱性等多维度数据，基于关联分析引擎实时纵深检测，精准挖掘威胁。

### 智能降噪 流量“标签”模型

从海量数据中，通过流量特性筛选高精准数据，结合算法模型精准狙击安全威胁，实现1000万：1的千万级安全事件降噪能力。

### 自动研判 多种训练模型

结合ATT&CK战术研判模型、网络攻击链研判模型、数据包研判智能模型等多种AI训练模型，自动判定安全事件真实性，并提供数据包佐证。

### 高效响应 自动化闭环管控

集中式安全设备管控，周期性安全管理流程优化，实现对安全事件应急响应的“预警-检测-研判-溯源”全链闭环，自动化地识别和处置各类信息网络安全风险。

### 云端安全赋能 打造实时检测引擎

依托云端安全数脑，将海量威胁情报数据赋能本地，实时同步最新的预警情报、专家经验、算法模型，保持安全能力实时在线。

### 全局掌控 安全运营效能分析

从各个维度进行安全运营数据统计分析，全局掌握安全建设效果和安全管理成果，持续优化安全设备、安全平台协同作战能力，提升安全建设体系效能。

## 5 建设效果

### 融合共建 高效运营

对接三方安全设备，采集多维安全数据，
构建异构融合的安全生态基座，提升安全运营效能。

### 设备纳管 联防联控

集中管控各类安全设备，实时监控运行状态及可用性，
通过安全接口的统一策略联动，形成联防联控安全防御体系。

### 人机共生 化繁为简

通过自动化、智能化的内置流程模块，规范安全运维工作，
大大降低对应急响应和日常巡检的人工投入，让安全工作化繁为简。

### 云端赋能 持续生长

云端安全中心实时同步最新情报、配置、策略、运营等安全数据，
在云端高级安全专家协同服务加持下驱动安全运营体系持续生长。

# 6 配套产品及服务

## 安全咨询服务

| 信息安全管理体系建设咨询 | 安全运营规范咨询 | 等级保护咨询 |
|---|---|---|
| 体系咨询 | 运营管理制度 | 差距分析评估 |
| 体系规划 | 运营技术规范 | 等保合规设计 |
| 应用开发生命周期咨询 | 运营手册 | 系统整改 |
| 应急体系建设咨询 | 接口标准定制 | |

## 安全运营服务

| 安全评估渗透服务 | 威胁分析检测服务 | 持续响应服务 | 运维运营服务 | 攻防演习服务 |
|---|---|---|---|---|
| 基础环境评估 | 服务器失陷检测 | 应急响应 | 重要时期保障 | 实战攻防演习 |
| web 应用评估 | 终端失陷检测 | 溯源取证 | 安全加固支撑 | |
| 移动应用评估 | 网站失陷检测 | 互联网资产发现 | 安全巡检 | |
| 无线网络评估 | 全流量安全事件分析 | 网络安全态势推送 | 安全配置核查 | |
| 工控测评检查 | 高级持续性威胁分析 | 安全事件报告 | 漏洞扫描 | |
| 代码安全评估 | | | 失陷检查 | |
| 渗透测试 | | | | |

## 安全服务培训

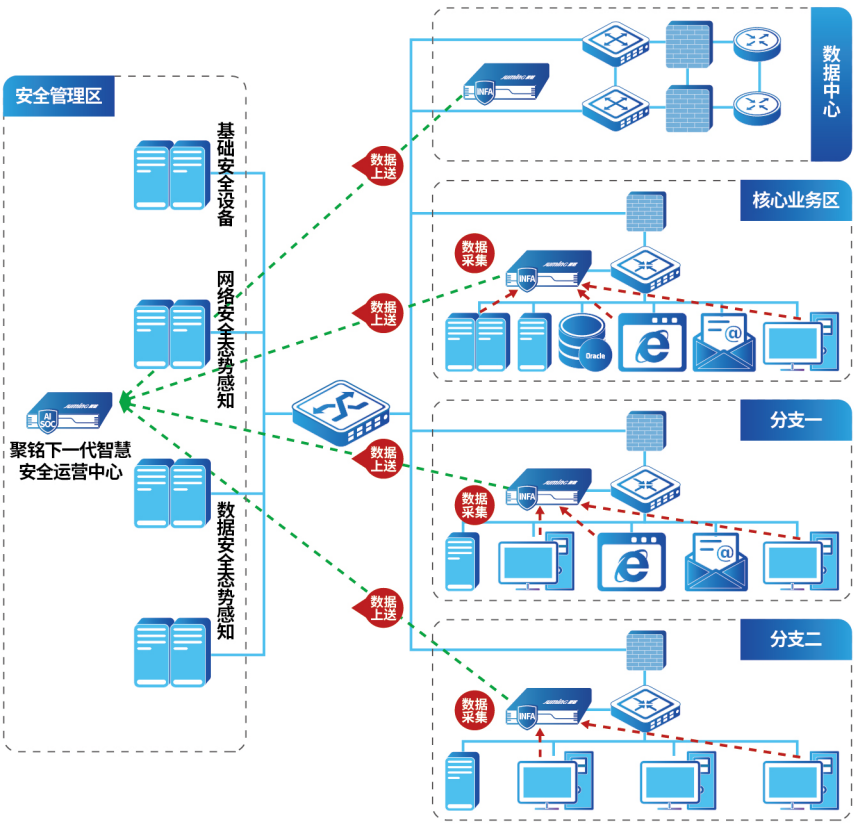
| | | |
|---|---|---|
| 基础知识培训 | 员工安全意识培训 |
| 安全发展趋势培训 | 红蓝对抗技术培训 |
| 安全管理培训 | 重要时期安全保障服务 |

## 产品列表

| | | | | | | |
|---|---|---|---|---|---|---|
| 下一代防火墙 | 脆弱性扫描 | 流量审计 | EDR | 数据备份 | IDS | …… |
| 日志审计 | 数据库审计 | 堡垒机 | 安全态势感知 | IPS | WAF | |

* 均可提供远程及本地驻场服务

# 7 部署方式



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】【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】

北京总部：北京市海淀区丹棱街18号创富大厦9层
南京总部：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：010-82666399 / 025-52205520　　传真：010-82669679 / 025-52205565
全国统一服务热线：400-1158-400　　公司官网：www.juminfo.com