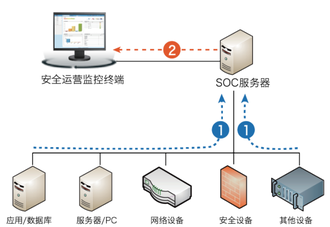
致力于大数据和信息安全的发展

典型应用

安全运营中心广泛应用于电信、能源、公安等大中型企事业单位。能够满足客户信息安全管理、等级保护和企业内部控制等方面的需求，可以部署在任意网络可达的区域，实现对企业资产的集中化信息采集、分析和管控。系统可支持一体式部署和分布式部署。

一体式部署

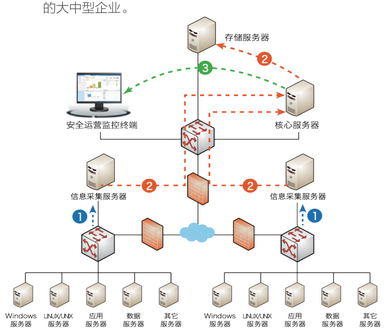
此部署方式适用于网络架构较为简单的中小型企业。



1. SOC服务器采集网络内各设备的安全信息并集中分析
2. 分析产生的安全告警等信息可在监控终端统一展示

分布式部署

此部署方式适用于网络架构较复杂、需要跨网络区域运营的大中型企业。



1. 信息采集服务器收集本网络区域内资产的安全信息
2. 核心服务器获取各区域的安全信息、集中存储并分析
3. 安全运营监控终端统一集中展示分析产生的安全告警等信息

产品规格

安全运营中心(SOC)，分硬件版和软件版，可根据不同客户需求进行选择。以下为硬件规格型号：

型号	JUMING-SOC-50AH	JUMING-SOC-100AH	JUMING-SOC-200AH	JUMING-SOC-500AH
尺寸	1U	1U	2U	2U
电源	单电源	单电源	单电源	冗余电源
电口	2（千兆）	2（千兆）	2（4）（千兆）	4（6）（千兆）
硬盘	1T	2T	4T	8T（raid5）
部署方式	一体式	一体式	一体式	一体式、分布式
采集控制器	1个	1个	1个	不限
可管理设备数量	50个	100个	200个	500个（可扩展）

注：规格配置仅供参考，实际交付以合同约定为准。

关注微信公众号　　关注新浪微博

JUMING 聚铭

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07栋406室
电 话：025-52205520 / 025-52205570　　传 真：025-52205565
全国统一服务热线：400-1158-400

欢迎访问公司官方网站 http://www.juminfo.com

JUMING 聚铭

2016年4月 第一版

安全运营中心
Security Operation Center

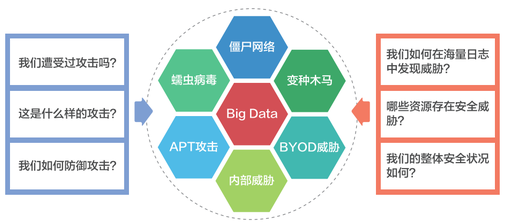
综合防御　智慧安全

南京聚铭网络科技有限公司
Nanjing JuMing Network Technology Co., Ltd

问题与挑战

信息安全事件的不断发生，以及国家对网络与信息安全的政策推动，促使政府机构和企事业单位对信息安全工作愈加重视。如何更好的展现信息安全工作的成果，是企业急需解决的问题。

- 问题一：信息安全投入越来越多，但缺乏展现形式，似乎“看不到”明显效果
- 问题二：部署了大量安全产品，但对新型威胁应对乏力，安全事故仍然不断发生
- 问题三：紧急事件严重损害业务，甚至引发危机，但被海量信息淹没，难以及时发现和处理
- 问题四：信息系统纷繁复杂，但专业人员缺乏、安全技能不足，导致安全运营管理难度很大



如何掌控整体安全状况，如何发现和降低安全风险，如何精确应对新型安全威胁和违规行为，如何快速发现和处理紧急安全事件，完整可靠地记录和保存安全日志，如何节约安全人员的投入、提高安全运维效率、降低管理成本，如何保障合规等，都是企业信息安全工作应该解决的问题。

从基础安全走向智慧安全

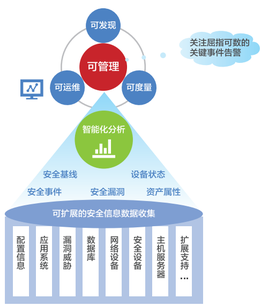
无论是“老三样”的防病毒、防火墙、入侵检测，还是新型安全产品，尽管起到了防御威胁的作用。为更好实现安全防御效果，聚铭网络经过十多年的企业服务和信息安全技术积累，隆重推出新一代信息安全运营管理平台，将产品、服务、流程、组织管理有机结合起来，统一策略、统一管理、智能分析、协同防御，帮助企业级用户从基础安全跨越到智慧安全，全面提升信息安全管理水平。

产品概述

安全运营中心（Security Operation Center，简称SOC）是企业信息安全体系的支撑平台，以资产为核心，安全事件分析处理为主线，监控企业安全风险状况的同时，确保企业信息安全闭环。安全运营中心通过内置综合分析、集中监控、集中运维、统一管理的功能，配合企业安全业务流程，将技术、流程、人进行有机的结合，实现企业全面、综合的信息安全管理。

客户收益

- 全面监测企业安全状况，实时发现企业安全威胁
- 大幅度降低企业的业务风险，有效减少客户损失
- 更好地满足违规检查、合规、安全取证的需要
- 节省安全人员的时间和精力，提高安全运维效率
- 从海量日志信息中，准确发现已知和未知安全威胁
- 快速的检索性能和智能的关联分析，节省了安全问题的处理时间
- 实时掌握企业信息系统的安全态势，为安全决策提供依据



产品优势

便捷	智能	开放	适应
一键式安装	风险自动评估	简单、可扩展的接口	全面支持IPv6格式
无代理信息采集	规则智能调整	第三方系统强力集成	分布式信息采集
监控对象自动发现	丰富的安全知识经验	开放的体系框架	全面支持各种合规审计
灵活丰富的报表报告	自动化的运维处理	强大的定制开发	上亿数据的分析处理
安全仪表灵活定义			灵活的系统配置
人性化的个人工作台			

产品特点

有效地降低企业安全威胁

安全运营中心将企业内信息安全相关的海量信息汇总分析，挖掘出潜在的安全威胁，将客户损失降至最低。

全面地监测企业安全状况

安全运营中心支持近百种IT基础设备，包括国内外知名厂商的安全设备、网络设备、操作系统、数据库、业务系统等，准确定位事件紧急程度，帮助客户快速处理安全问题，节省了处理问题的时间成本。

显著地提高安全运维效率

安全运营中心将专业复杂的安全分析工作以简单直观的图形化界面展示，运营中心仅需有限的人员、资源即可规范、高效地进行安全运维管理工作，节省了安全人员的时间和精力。

准确地发现已知和未知安全威胁

安全运营中心内置丰富的告警分析策略，及时准确地发现海量日志信息中的已知、未知安全威胁，同时客户可根据企业的业务状况自行建立分析模型，分析企业关注的安全威胁。

丰富的安全应用和攻防实例

凭借多年的信息安全应用和攻防经验，在安全运营中心内置了几十种关联分析模型，帮助用户分析高等级安全事件，此外，系统还开放了自定义关联分析，用户可以自行建立模型，分析企业关注的安全事件。

体系化的事前、事中、事后安全防护

安全运营中心涵盖事前防范（安全基线策略、内置关联策略）、事中监控（整体态势展现、关联分析、事件告警、风险监测、工单）、事后审计（日志记录、集中安全存储）的全过程安全防护。

卓越的安全服务能力

公司凭借十多年来对超大型国有企业提供全生命周期的信息安全服务经验和对SIEM/SOC技术研究及应用的研究成果，为企业提供7×24小时的信息安全监测代维服务。

新型攻击方式的智能发掘

安全运营中心内置对新型攻击行为或异常行为的智能发现引擎，以行为和效果为条件进行关联分析，提前感知新型攻击威胁，降低客户损失。

统一的设备日志标准化

安全运营中心将众多设备日志统一标准化，降低告警数量的同时，也为客户整理归纳了标准的事件类别，将客户的精力集中在安全事件的处理上。

海量日志的检索和处理能力

安全运营中心支持海量日志的处理和分析，可以在海量日志中准确定位关键问题，配合快速的检索能力，有效减少解决问题的时间。

更好地满足合规审计要求

安全运营中心通过磁盘阵列、数据库优化等技术手段，支持海量日志的快速查询和存储，从而满足企业自身日志审计需求和国家对企业日志存储的合规要求。

灵活的报表自定义能力

安全运营中心具备灵活的自定义报表能力，可快速集成国家合规报表和企业自身要求报表，结合系统内置的报表模板，充分满足上级检查和企业自查的需求。

其它特点

可灵活定制的界面风格、展示布局、个人工作台和安全业务流程；快速的安装部署和简单可扩展的接口；稳定可靠的系统和无代理的采集方式；系统兼容支持IPV6。