聚铭云端安全管家

产品白皮书

聚铭网络科技有限公司

2024 年 04 月

目录

声明

在本文中如无特别说明，聚铭网络均指南京聚铭网络科技有限公司和北京聚铭信安科技有限公司。

JUMING 聚铭图标为聚铭网络的商标。对于本手册出现的其他公司的商标、产品标识和商品名称，由各自权利人拥有。

除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

本手册内容如发生更改，恕不另行通知。

如需要获取最新手册，请联系聚铭网络技术服务部。

联系信息

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：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：025-52205520/52205570

传　　真：025-52205565

全国服务热线：400-1158-400

网　　址：www.juminfo.com

产品支持：support@juminfo.com

聚铭网络技术服务以及营销网络覆盖全国，并在各地设有办事处和分支机构，为客户提供无微不至的解决方案和高效的服务支持。聚铭专家团队 7x24 小时全天候在线，确保在安全事件发生时提供分钟级应急响应。

1. 前言

- 数字化带来的全新安全挑战

随着云计算、大数据、5G、人工智能、物联网技术等新技术发展，推动组织向数字化、智能化方向转型，日常生产经营管理与网络信息化结合日趋紧密，对网络信息系统的依赖程度越来越高。随着信息系统不断增加，网络基础架构日益复杂化，给安全运维带来更多的工作量和更加沉重的负担。

- 网络攻防战白热化

近年来，美国国家安全局（NSA）针对我国国内的网络目标实施上万次的恶意网络攻击。网络攻击者不再是单纯的个人，而逐渐组织化、国家化；攻击目的也不再是单纯的为了炫技，而是为了寻求一定的经济利益甚至国家利益；网络攻击手段也在不断演进，从木马、病毒进展到漏洞、后门、仿冒服务器及自动化工具等。

- 网络安全运营转向第三方托管模式

随着数字化转型的不断深入，对网络安全建设的重视度也不断提升，安全投入也逐步增长，但是采购的大量安全设备却带来了更多问题，让安全管理团队陷入了日志分析、事件响应和问题处置等大量工作中，疲于应对。仅依靠自身防护能力积累，实在难以满足安全防护需求。

面对常态化的高级威胁攻击，需要有力的运营团队来维护安全策略、管理安全告警、响应处置风险事件并定期评估风险，因此托管式安全运营理念应运而生且开始受到行业关注。对比传统安全建设与运营模式，托管安全服务通过专业化安全运营知识、实战化问题分析能力以及迅速的响应速度，提供全方位网络安全防护，使制度、人、技术保持高效协同，释放更多的安全能力，减轻整体安全防控压力，有效解决安全能力不足的难题。

- 共享经济催生云端安全运营

按照《“十四五”数字经济发展规划》，“深入发展共享经济”成为“数字经济新

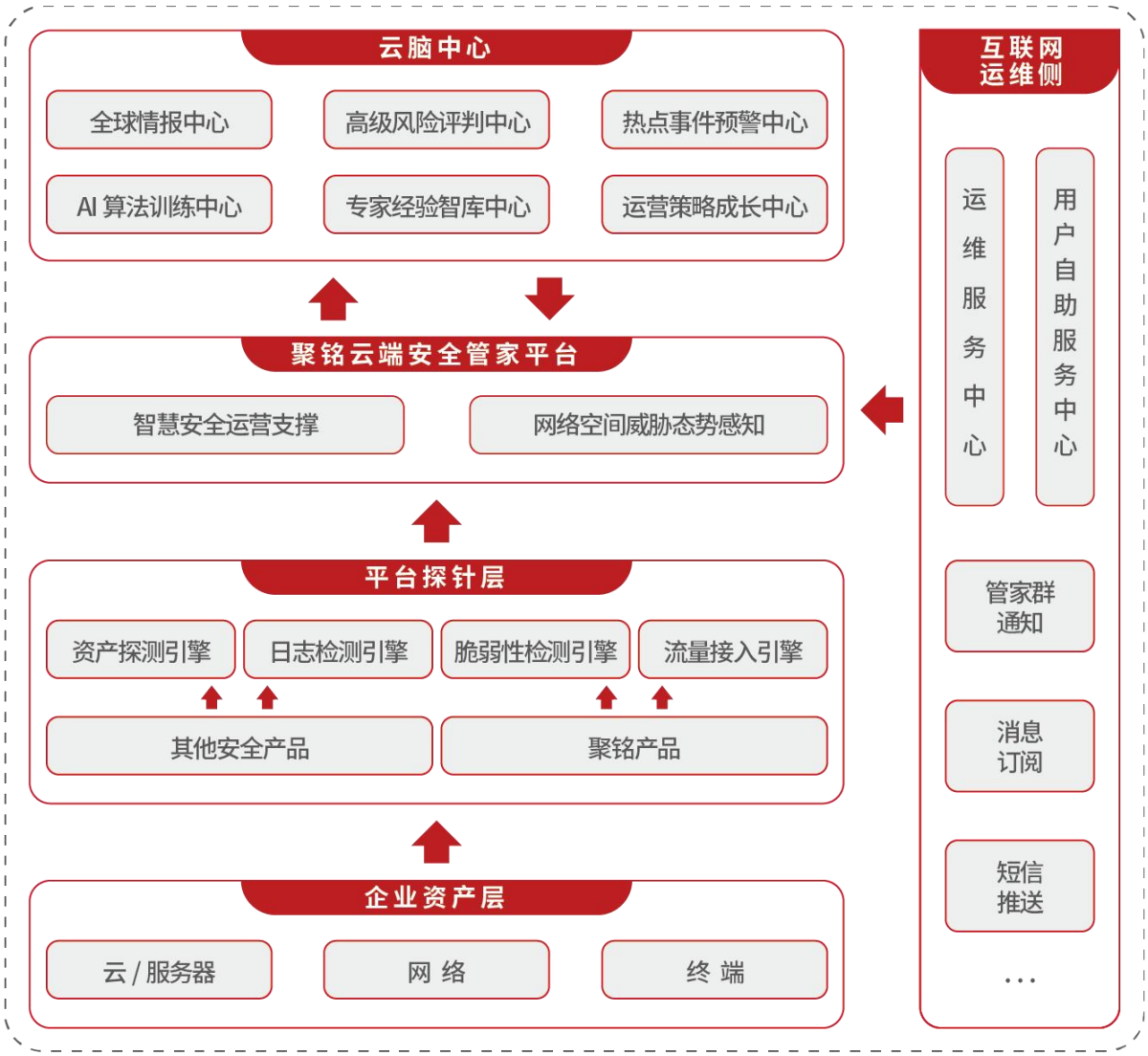
业态培育工程”的重要内容，这也意味着，共享经济将成为推进数字化转型的重要抓手。

随着经济提质转型增效的加快进行，许多领域的市场竞争将会更加激烈，行业洗牌的步伐将会加速，降本增效和开源节流成为各企业经营策略的首要选择。如何在品质、服务、安全等方面凸显企业优势，也将成为未来市场竞争的关键。共享经济新业态新模式，为企业开辟降本增效发展的新路径提供了突破口，并已呈现蓬勃发展态势。在面对网络安全领域思维、人才、运营等不足带来的挑战，“共享经济”思维仍然有效。云端托管模式正是这一理念的最好例证。网络安全专业人员是稀缺资源，尤其高阶人员更是如此。在云端托管服务模式下专业的安全服务团队依托成熟流程、运营机制提供服务，完美解决了机制缺失、人才不足的难题。

2. 解决方案

聚铭云端安全管家（Intelligence Security Operation Center，简称：iSOC）服务旨在保障企业网络持续安全、可用。以传统安全建设为基础，依托“大数据+AI”全息安全感知技术，通过云地专家协同方式，为企业提供 7*24 小时全网安全监控及响应服务，打造智慧安全运营体系。让客户一键获得常态化的网络安全防护服务。

2.1. 方案架构



2.2. 资产测绘及管控服务

2.2.1. 智能资产测绘服务

随着数字化转型步伐加快，大量信息化系统的叠加，全网资产总数、存活数不清晰，资产信息更新滞后，造成安全防护盲区，带来潜在风险。

平台通过资产测绘能力，对全网资产进行探查，云端安全专家针对探查到的资产进行梳理及风险治理。

2.2.2. 资产梳理服务

在资产梳理过程中，首先针对发现的设备进行基础备案，形成资产台账。在自动化资产测绘的基础上，对核心资产配置安全属性、管理属性，包括：资产CIA、名称、地理位置、责任人等，从而加强对关键业务的安全防护能力。

2.2.3. 资产治理协同服务

在资产的风险治理过程中，协同一线或客户，针对影子资产、资产服务存在的弱点等安全隐患进行防护；针对资产存在的潜在网络威胁进行深度挖掘；针对资产遭受攻击后造成的危害进行修复。

2.3. 脆弱性管控服务

2.3.1. 脆弱性巡检服务

资产的脆弱性会严重影响网络的安全性，甚至成为网络安全中的短板。因此，提前获悉资产和业务中存在的脆弱性信息，并采取补救措施或者做好应急预案，是网络安全建设的基础，也是核心能力之一。

云端安全专家将依据客户业务情况，制定专属多维巡检任务，包括主机漏洞扫描、弱口令扫描、安全基线检查等，全方位、多维度的进行资产安全性检查，发现各类脆弱性。并对脆弱性进行持续跟踪，待脆弱性处置完成后，平台专家复验脆弱性，确认是否已修复，完成脆弱性生命周期闭环管控。

2.3.2. 脆弱性评估服务

平台对巡检过程发现的重要资产漏洞、弱口令、配置弱点进行收集和管理，云端安全专家结合组织安全体系建设及业务情况进行人工评估，灵活实现了人工评估的自动化和常态化，降低了运维人员的运维成本。

2.3.3. 脆弱性治理协同服务

经专家评估后的脆弱性问题清单，协同客户或一线运维人员对清单内容进行修复。例如云端安全专家在巡检扫描站点、URL 等资产过程中，通过弱口令扫描引擎发现信息系统中存在的弱口令，安全专家将会出具扫描结果报告，客户可根据实际业务情况进行弱口令的更改。

2.3.4. 互联网暴露面巡检服务

通过采取主被动结合的风险测绘技术对互联网边界资产进行探测，比如：应用、系统、IP、端口、服务、域名、中间件等，全面梳理客户辖区内互联网资产基础信息，发现违规暴露在互联网中的资产、存在的漏洞以及漏洞利用情况。

云端安全专家在和客户进行充分沟通前提下，根据资产评估情况及资产暴露程度定制专属云端探测任务，在确保对目标网络正常业务运行影响最低的前提下，在指定时间进行探测。

2.3.5. 互联网暴露面收敛及防护协同服务

根据探测的结果对暴露资产进行收敛，缩小攻击面。比如对违规暴露、过期未关闭、临时发布的资产进行下线处理；关闭违规暴露的端口和服务；对高风险端口进行禁用；对漏洞利用情况进行深入排查并对漏洞进行修复；将非必须暴露资产收归内网。

在实时更新多种漏洞扫描插件基础上，全面监控暴露在互联网的资产，针对用户网络边界暴露面的违规行为进行监测。

2.4. 威胁及风险管控服务

2.4.1. 威胁检测服务

网络安全管理技术内容纷繁复杂，管理者因事务繁杂无法对安全事件做到实时知晓，一直处于被动响应状态，安全事件的实时获知对于管理者而言也是一大痛点。

平台通过整合流量、日志、脆弱性等多元数据，依托八大研判模型，实现全息动态威胁感知。云端安全专家不断调整威胁检测引擎，来适配客户个性化的网络情况，从而使平台威胁检测达到最佳状态。

此外，实时监控告警、失陷、安全事件、日志等多维数据，可根据管理者对安全事件的关注偏好进行个性化设置，当触发了管理者关注的安全事件时，可通过邮件、微信等渠道实时推送告警信息，便于管理者第一时间掌握情况。

2.4.2. 7*24 风险监控服务

基于业务场景，云端安全专家 7*24 小时持续在线守护，监控安全问题，快速检测处置威胁事件。当触发安全事件时，云端安全专家将及时响应，快速检测处置威胁事件，直至风险处置结束闭环。并且通过邮件、微信等渠道将告警、处置结果等信息推送至客户，便于管理者获知全局情况，占据主动地位。

2.4.3. 风险挖掘及研判服务

云端安全专家实时监测网络安全状态，持续网络中存在的威胁。对于常见的木马、病毒等有害程序提供查杀解决方案，对于攻击类事件，提供封锁方法等；对于危害、隐蔽性较大的挖矿、勒索、恶意加密流量，深度分析研判，溯源威胁，提供应急响应处置方案。

2.4.4. 风险处置协同服务

经云端安全专家研判确认后的威胁，将基于业务场景提供可落地的处置方案。

协同客户或一线运维人员在遵循客户内部操作规范前提下借助本地或远程部署的相关安全工具完成查杀、封锁等处置。

2.5. 配置保障服务

2.5.1. 配置巡检服务

以往对于设备或应用的配置审计，仅在上线前进行一次安全加固操作，但由于业务变更，安全配置需要频繁调整。以往安全产品无法准确捕捉设备上线后的更改记录，无法动态、精准的把握现网设备或应用配置情况，这些因素使系统存在巨大安全隐患。

云端安全专家将依据客户业务情况，制定专属配置变更巡检任务，可以检查系统/服务中文件、端口、进程等的变化信息，以便及时分析变更带来的隐患。并对配置变更进行持续跟踪，完成闭环管控。

2.5.2. 配置变更监控服务

每次风险进行处置完成后，自动巡检跟踪加固后的系统配置，包括注册表、服务、文件等，及时检测变更情况。

云端安全专家基于业务系统情况，针对配置变更内容进行分析，对确认需要变更的配置，设置为基准线，对于违规的配置变更给予修改建议，并协助完成配置回退。

2.6. 智慧安全运营支撑服务

2.6.1. 线上安全技术培训服务

结合聚铭在信息安全领域丰富的研究成果和安全经验，从安全意识、安全技能等多方面为客户在线提供网络安全培训服务，让员工从多方面了解掌握网络安全威胁，以保护自己和组织免受网络攻击。在网络意识方面，通过提供真实的网络钓鱼骗局案例、勒索现场还原、垃圾邮件展示等方式让员工了解网络安全威胁

可能出现的不同形式和场景，从而意识到网络安全的重要性。

2.6.2. 5*8 小时研判服务

云端专家 7*24 小时在线守护，分钟级的事件发现速度及响应效率，快速检测处置威胁事件，减少组织日常安全运营工作压力。提供高级专家组 5*8 小时在线研判服务，当专属云端安全专家遇到无法处理的未知威胁时，高级安全专家团队将会及时响应，组织专项研究团队，支撑威胁研判，直至风险处置闭环。

2.6.3. 行业运营策略定制服务

云端安全专家将基于现有安全体系，参考组织所属行业特性，定制专属安全运营策略，包括巡检检测策略、巡检任务、安全分析策略、风险处置策略等；另外，为保障安全运营更加高效的开展，专家团队可以为客户提供全方面安全基础建设评估，帮助客户完成网络安全基础建设提升。

此外，在面临突发风险、重大活动及节假日等重要时期，可根据具体情况配置脆弱性检查策略及任务，为网络环境提供全面体检。通过云端安全运维支撑服务，实时更新漏洞插件库及漏洞检测规则，缩短脆弱性风险发现周期，有效应对突发安全事件。

2.6.4. 风险处置全生命周期管控服务

凭借 SOC 团队丰富的企业服务运营经验以及云端安全专家风险处置经验，在融合风险管理模型、ISO13335、风险分析模型、PDCERF 风险闭环响应模型、SOP 处置流程等行业标准基础上，规范化安全服务团队“监测-分析-响应-跟踪-沉淀”运维全流程，高阶专家在规范化运维流程基础上从问题发现到协助处置全流程闭环跟踪。全流程闭环处置经验为后续安全运营和维护提供了知识来源以及安全问题的处理依据、方法或参考。

2.6.5. 热点事件、风险预警及预防服务

基于大数据技术结合区域及行业威胁监测，挖掘区域及行业热门事件、风险预警，专家结合组织安全架构实际情况提前全面检查，帮助用户了解设备防护状态，提供针对性防护措施或者防护建议。对于客户重点关注的热门事件，会通过邮件、微信等方式进行推送。

2.6.6. 风险通知推送服务

高阶安全专家结合组织安全架构以及资产评估等情况，全面分析评估后，将客户关注的风险及时推送给客户，例如教育行业中高校重点关注虚拟货币挖矿动态，医疗行业中医院更侧重于关注恶意勒索动态。

2.6.7. 威胁情报更新服务

威胁情报来源于腾讯安全威胁情报中心以及聚铭自有威胁情报中心，基于腾讯及聚铭多年的互联网安全大数据服务经验积累，为用户提供线索研判、攻击定型、关联分析、互联网资产漏洞/内容/业务监测等情报服务，并定期持续更新，可帮助组织及时调整防御策略，提前预知攻击的发生，从而实现精准的动态防御。

2.6.8. 脆弱性插件库更新服务

通过云端安全运维支撑服务，实时更新漏洞插件库及漏洞检测规则，缩短脆弱性风险发现周期，有效应对突发安全事件。

此外，也同步更新各类系统、网络设备、防火墙、Web 中间件及数据库等设备的安全配置基线插件，包含账号类、口令类、授权类、日志配置类、路由配置类等，将安全评估工作常态化，有利于提高设备自身防护能力。

2.6.9. 专家智库沉淀服务

根据安全事件类型，智能推荐专家标准处置预案。云端专家依据标准处置预案协助完成风险闭环处置，缩短处置时间；当处置过程发现更适合的方案，处置

完成后，云端专家结合实际情况，对预案进行定制化并形成知识沉淀，丰富本地专属专家智库。

2.6.10. 运营报告及推送服务

安全运营报告集中体现了检测到以及处置的安全问题，报告包括每日处置情况、每日/周/月安全运维总结。高阶专家在系统自动生成报告基础上会结合资产评估等情况给出具体可落地防护建议，完成报告编辑后会自动推送至相关用户邮箱。安全运营报告将从全网安全态势、失陷主机、内部资产脆弱性等场景充分展现运营概况。

2.6.11. 安全成果汇报服务

安全专家基于自身丰富的经验技术进行分析研判，按季、年等周期汇总安全事件趋势及下一阶段工作展望。专家将在线汇报、提供可落地的修复建议及方案，呈现安全工作价值。

2.7. 本地增值服务

2.7.1. 安全处置服务

聚铭提供安全专家上门、面对面解决用户“最后一公里”的网络安全难题。安全专家基于自身丰富的项目服务及风险处置经验，为用户提供挖掘、研判、处置、汇报等一对一专属本地化服务。

2.7.2. 安全加固支撑服务

对于客户或第三方厂商系统，支持安全专家本地支撑脆弱性安全加固操作，包括对网站、业务系统、操作系统、应用等进行基线加固和组件升级、修补潜在的各种高危漏洞、解决隐藏的安全威胁。

2.7.3. 安全培训服务

包括常规安全培训、安全技术培训、安全管理培。

安全意识培训包括：加强人员安全意识教育、了解安全发展趋势、了解防范措施等。

安全技术培训，模拟实战场景，采用实操教学，通过现场培训让学员掌握全流量威胁分析方法，以及漏洞攻击、钓鱼攻击、内网渗透攻击等攻击行为的检测发现与处置方法，并具备攻击链路分析与还原能力。

安全管理培训，了解国家相关部门对网络信息安全管理和建设的相关标准，如何建立具有针对性和适用性的安全管理办法。包括法律法规、信息安全管理体系、安全等级保护、风险评估与风险管理、安全规划、安全基线管理、软件安全开发管理体系等。

2.7.4. 应急响应服务

在遇到突发安全事件后，在客户授权前提下，采取紧急措施和行动，以最快的方法抑制安全事件的扩大，恢复业务的正常开展，调查安全事件发生的原因，提供安全事件过程报告及根除的解决方案。

2.7.5. 渗透测试服务

依据各项目渗透测试最佳实践，通过工具辅助，主要以人工测试方式，对客户授权下的应用系统进行非破坏性攻击测试、深度漏洞挖掘，发现应用系统隐藏的安全隐患和安全风险。

2.7.6. 红蓝对抗演练服务

通过结合“项目管理”、“安全专家”、“安全检测与防护设备”、“驻场服务”等服务建立综合整体的安全防御体系，构建安全保障专项组织架构，利用安全防护设备、监控平台、威胁情报、检测及处置分析工具，多维度立体化监测处置和防御，为客户提供完善的网络安全应急演练流程。

2.7.7. 重要保障服务

基于聚铭多年支撑重要时期保障工作的经验，聚铭保障团队对于信息安全事件的预防、监控、响应与恢复有着成熟的方法论。

在特殊时期、重要活动、重大节日期间，安全专家对重保前、临保、重保、总结四个阶段，使用不同的安全检测、监测及防护手段，为客户提供真实、有效的安全保障，保障客户业务系统在重要时期的平稳运行。

2.7.8. 等级保护咨询服务

提供信息系统定级、差距分析评估、安全规划与方案设计、系统整改、等保合规设计以及辅助测评等全等级保护周期咨询服务，并可根据客户实际需求提供定制化服务模块。

2.7.9. 安全体系咨询服务

通过对客户面临的国家及行业合规监管要求、信息系统运行全生命周期面临的安全服务需求等进行梳理总结，结合自身多年服务经验，以客户需求为导向提供覆盖信息系统规划、设计、建设、运行全生命周期的专业安全咨询服务。

3. 服务价值

3.1. 安全运营高性价比

- 以租代购、云化共享的创新方式，将安全建设投入成本降低到原有的 10%！
- 将安全体系方案、基础设备建设、安全专家协助、运营协作与监管，整个安全体系全面云化共享，以极高的性价比提供专业化安全运营服务。

3.2. 安全保障常态化

以“重大保障活动”为标准，全面保障为基础，精准定位为目标，为客户打造常态化安全运营！

- 全息网络空间威胁感知，覆盖动态安全+静态安全。将资产、日志、流量、脆弱性数据作为核心输入源，融合众多研判模型，全面检测无死角。
- 专家在线，7*24 专家在线防护，风险处置 100%闭环，安全隐患 0 容忍。

3.3. 安全服务分钟级

大数据赋能 AI，AI 辅助专家，将安全服务响应速度缩短到分钟级！

- 风险威胁预测，结合情报及安全运营数据，提炼行业、区域热点事件定制化运营策略，让网络安全未雨绸缪。
- 风险评估自动化、风险感知智能化，依托运营策略、样本数据、专家方案，采用大数据挖掘技术，训练模型、优化推荐，辅助专家加速安全闭环流程。
- 7*24 实时监控，专家在线，在 AI 的辅助下，分钟级安全服务响应。

3.4. 安全运维轻松监管

安全运维监管化繁为简，安全运营主、被动监管结合，随时随地，掌控全局！

- 将安全感知、安全运维成果相结合，采用多维大屏监控技术，使安全运营监管可视化、指标化。
- 将安全通告理念互联网化，公众号、管家群实时同步预警、风险、报告等信息，让客户随时随地轻松掌控全局。
- 运维动作全程留存，客户可随时审计所有操作细节。

4. 服务优势

4.1. 领先的安全运营技术

- **规范的安全运维管理流程：**凭借 SOC 团队丰富的企业服务运营经验，在融合风险管理模型、ISO13335、风险分析模型、PDCERF 风险闭环响应模型、SOP 处置流程等行业标准基础上，规范化安全服务团队“监测-分析-响应-跟踪-沉淀”运维全流程。
- **全息网络空间威胁感知无死角：**覆盖动态安全+静态安全。以资产、日志、流量、脆弱性为核心，在众多研判模型协同赋能作用下，全面检测无死角。

4.2. 专业的安全运营团队

- **中国安全运营中心（SOC）的首创团队**，服务客户已遍布电信、电力、能源等众多行业。
- **中国最早日志审计研发团队**，专注多源异构日志分析超 20 年，目前已能支持 800+种设备，超过 2 万种日志格式，全面支持主流厂家网络设备、安全设备接入。
- **团队已服务逾 6 千家云端托管客户**，系列产品拥有超过一万家政企客户，沉淀积累海量行业安全运营策略、专家处置经验以及安全检测分析能力。

4.3. 管家式服务

- **专家保障：**以“全天候 7*24 在线防护、安全隐患 0 容忍、风险处置 100%闭环”为宗旨，多阶安全专家协同保障。
- **专属安全保障持续生长：**企业专属运维知识库、风险预案、方案持续沉

淀，企业专属运营策略持续调整，动态适应企业个性化场景。

5. 技术优势

- **全息网络空间威胁感知无死角**，全面覆盖动态安全、静态安全检测。以资产风险为核心，依托大数据技术，对海量的日志、流量动态数据深度挖掘，感知网络中的动态威胁行为；结合公网遥测、内网渗透技术，全面覆盖内网、公网暴露面。

- **相似性分析**，多项目多场景监控聚合，对不同租户呈现的脆弱性、威胁事件进行相似性挖掘，汇聚呈现，提升安全分析效能。

- **自动化运维协助**，通过行业运营策略定制专属巡检任务；依据分析、响应过程，自动化构建安全分析处置报告；支持威胁半自动处置，编排联动交换机、防火墙进行风险处置；对处置后设备自动进行配置保障，持续跟踪安全运维成果，提升运维效率。

- **安全运维监管**，化繁为简，安全运营主被动监管结合，随时随地掌控全局。将安全感知、安全运维成果相结合，采用多维大屏监控技术，使安全运营监管可视化、指标化。将安全通告理念互联网化，预警、风险、报告等通告实时同步至公众号、管家群，让客户随时随地轻松掌控全局。运营过程全程留存，客户可随时审计所有操作细节。

- **规范化安全运维管控工作流程**，以丰富的企业服务运营经验为依托，在融合风险管理模型、ISO13335、风险分析模型、PDCERF 风险闭环响应模型、SOP 处置流程等行业标准基础上，通过流程管控，规范化安全服务团队“监测-分析-响应-跟踪-沉淀”运维全流程。

- **“大数据+AI”赋能精准分析**，依托平台收集海量数据，持续训练 AI 模型，为平台提供具有成长性的 AI 模型样本，使得 AI 在未知威胁分析中真正具备实战价值。

- **云脑赋能安全运营**，基于大数据技术，构建具有行业性、区域性的数据仓库，涵盖加固预防能力的热点事件预警中心；增强分析研判能力的全

球情报中心、多元分析决策算子中心；提升运维能力的专家经验智库中心、运营策略成长中心。