

一、 企业基本情况

南天信息拥有三十余年深耕金融等行业信息化的丰富经验，如今结合云计算、大数据、人工智能、移动互联网、物联网、区块链等最新技术，以自有核心技术和关键应用为基础，为行业数字化提供规划与咨询、saas 解决方案和实施、云数据中心智能管理及服务、智能终端解决方案等软硬件产品、解决方案和服务，积极融入“信创”和“数字云南”建设，在金融科技、数字政府、智慧交通、智慧政务、智慧旅游、智慧党建、智慧教育、数字医疗等诸多领域，为客户提供贯穿其 IT 建设全生命周期的“一站式”数字化服务。

云南南天电子信息产业股份有限公司信息安全测评中心成立于 2010 年，是云南省首家信息安全等级保护测评机构。深耕网络安全领域十余年来，中心依托技术、经验与人才优势，获评国家信息安全漏洞库（CNNVD）技术支撑单位、全国网络安全标准化技术委员会成员单位等国家级资质，承担公安部第一研究所云南网防服务站职能，并被认定为云南省、昆明市两级网络安全应急技术服务支撑单位。凭借卓越实力，中心两度荣获“全国网络安全等级保护测评机构先进单位”称号，成为省内技术覆盖全面、服务能力领先的综合性网络安全服务商。

南天信息安全测评中心作为云南省内规模领先的网络与数据安全服务商，围绕“安全测评”“安全保障”“数据安全及密码应用”三大核心业务板块，构建了涵盖等级测评、风险评估、安全培训、应急响应等全方位的安全服务体系，为政府、医疗、金融等行业提供定制化解决方案，常态化地支撑公安、网信等部门及关基单位安全保障需求。

二、 安全服务

1. 以“安全能力”为基石，打造“1+4” 服务治理体系：

以“年”为单位提供全面的网络与信息系统安全运行保障服务，预防各类网络安全威胁，保障业务长期的安全运行。



2. 服务能力

a. 本地实战渗透攻防能力

1、攻防实验室竞赛能力

作为云南本土的安全服务企业，我公司筹建了一个攻防实验室。目前，实验室团队共有7人，他们参与各类比赛的具体情况如下（部分）：

2021年云南省信息通信网络安全技能竞赛第二名

2022年云南省网络安全职业资格技能大赛优胜奖

2022年云南省信息通信网络安全技能竞赛优秀奖

2022年网鼎杯初赛成绩互联网企业赛区云南第一名，全国第9名

2022年全国行业职业技能竞赛--优秀竞赛单位奖项

2023数字中国创新大赛网络数据安全赛道进入全国总决赛，总决赛100支队伍，排名全国第50名

2022云南省滇峰对决网络安全比武竞赛渗透测试三等奖

2022年全国行业职业技能竞赛--全国数据安全职业技能竞赛数据安全管理员职业技能竞赛 优秀竞赛单位

云南省信息通信网络安全实网攻防暨技能竞赛--一阶段第一名、全程第二名、二队优秀奖

2、攻防实验室人员挖掘漏洞证明（部分）

序号	原创漏洞证明证书
1	CNVD-2021-84310 (李锐鹏)
2	CNVD-2021-90581 (雷雨田)
3	CNVD-2022-15054 (段松)
4	CNVD-2022-69650 (付涵)
5	CNVD-2023-01125 (李锐鹏)
6	CNVD-2023-27631 (李锐鹏)
7	CNVD-2024-09436 (雷雨田)
8	CNVD-2024-07792 (段松)

3、具备向国家信息安全漏洞库提供技术支撑的能力证明



b. 本地化保障和应急能力

1、本地化保障能力

目前南天**共有八千余名正式员工**，分设昆明总部和北京总部，在北京、上海、广州、深圳、昆明、西安、成都、武汉、合肥等地均设有全资或控股子公司。在省内，信息安全测评中心团队规模发展到**120余人**，设有安全测评部、攻防实验室、应急响应部、安全保障部、安全运营部、商用密码和数据安全部等部门，常态化服务省公安厅、省委网信办以及各重要单位，是省内规模及技术覆盖较为全面的专业安全服务商。同时，我公司也配备6人的专业应急团队，支撑省内公安、网信以及多家重要单位进行应急处置。

同时，我公司自2016年就以多种身份参与国家及省级HW，至今已9年。**作为防守方**，**云南省某金融单位**在国家护网前期，我公司通过资产梳理、漏洞扫描、渗透测试、安全巡检等帮助客户梳理了有针对性的网络安全防护策略，并在关键节点部署两台网盾K01，大大提升了单位在攻击全链路的监控能力。同时我司也协助客户进行互联网暴露面收敛和风险整改，减少了大量互联网暴露面失分点。在护网期间，我司提供由6人组成的7*24小时专业防守团队（其中包括渗透攻防专家），结合K01和一所云监测平台实时对漏洞扫描、暴露破解、sql注入、命令执行等重大攻击、受控外联等安全事件进行监测和识别，并对发现的攻击行为进行分析研判，提出处置方法，拦截攻击行为等，并每日出具值守日报，在护网期间共计提交60份监测日报，拦截攻击流量1245062次，178292个ip攻击源，护网期间，整体防护状况良好，未发生攻击成功事件。**作为攻击队**，我公司多次担任国家护网及省级护网攻击队，深谙攻击队手法与思路。关键时期，能迅速摸清攻击意图，快速阻断并精准防御，筑牢网络安全防线；**作为裁判**，我们长期参与国家护网与省级护网赛事，了解历年赛事中的各类得分要点和失分环节。基于此，在重要时期，我们能够协助提前排查并加固以往容易出现失分的地方，助力其提升网络安全防护水平。

2、本地化应急能力

我公司已配备一支6人应急支撑团队，专门支撑省内网络安全应急事件。作为云南省及昆明市的应急支撑单位，多次参与多家单位应急处置。在2023年，我们成功应对了多起网络安全事件，展现了卓越的应急响应能力和深厚的专业功底。例如，当**云南省某研究所**的OA办公系统遭遇不明势力植入的后门病毒威胁时，南天测评中心迅速响应，启动应急机制，中心应急响应部进行细致排查与取证。我们不仅成功定位并清除了病毒，还发现了两个与后门病毒植入紧密相关的可疑IP地址，并及时阻断其访问，有效遏制了潜在的安全风险，为

该研究所避免了进一步的损失。另一案例某大学图书馆网站疑似被不法分子植入暗链，导致用户访问时可能跳转到违法网站。接到报告后，南天测评中心安全团队立即展开深入分析，发现攻击者在 2023 年 12 月 13 日通过上传 webshe11 的方式成功入侵服务器。面对这一紧急情况，我们果断采取行动，对涉事服务器进行全面封堵与隔离，成功阻断攻击者的进一步行动，最大限度地降低了该大学因此遭受的损失和负面影响。

我公司具体获得的保障及应急支撑单位证书如下：



《生物多样性公约》第十五次缔约方大会技术支撑单位及
云南省网络安全应急技术服务支撑单位（2022-2024 年）



昆明市（2021-2024 年度）网络安全应急技术支撑单位证书及
第一届云南省网络数据安全技术支撑单位



云南省网络数据安全技术支持单位证书
及昆明市第二届网络技术服务支撑单位入选公示

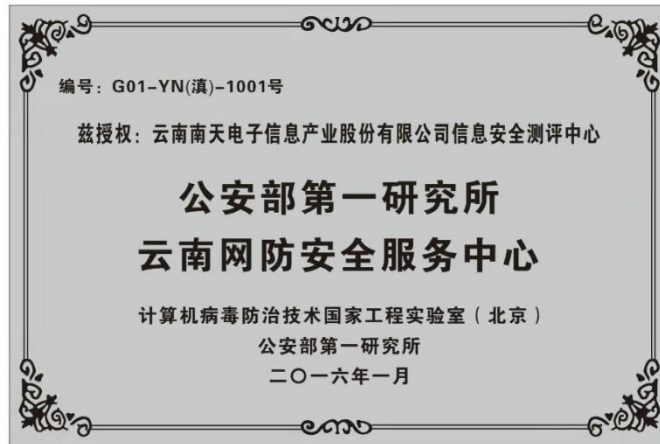
第二届云南省网络安全应急技术服务支撑单位（应急处置）
公示名单
（排名不分先后）

序号	单位名称
1	北京神州数码网络有限公司
2	北京天融信网络安全技术有限公司
3	杭州安恒信息技术股份有限公司
4	福建网康科技股份有限公司；北京天融信网络安全技术有限公司
5	湖南网安信息技术有限公司
6	国脉网络（成都）有限公司
7	云南网安信息技术有限公司；平安网安有限公司
8	云南网安信息技术有限公司
9	云南南天电子信息产业股份有限公司
10	云南安盟网络科技有限公司
11	浙江网安（北京）网络科技有限公司；网安（北京）网络科技有限公司

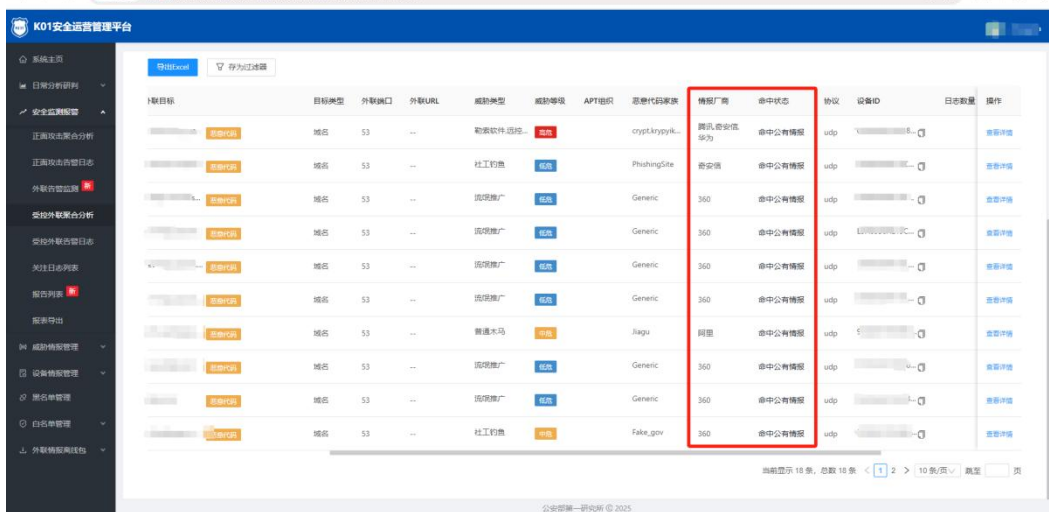
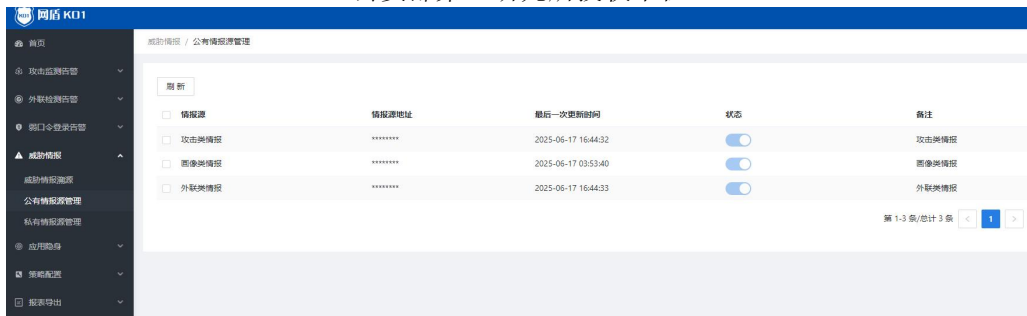
入选第二届云南省网络安全应急支撑单位通知

c. 公安部一所网络安全情报能力

我公司将基于公安部第一研究所实时情报数据（来自于各大关基单位部署的 1000 余台网盾 K01 及各大政府网站 G01 公有云），并融合腾讯、奇安信、360、华为及阿里等权威情报源。依托攻防专家分析经验，对所有数据进行研判确认，确保情报数据质量可靠。实时获取行业最新、行业最全的网络安全威胁情报信息。



(公安部第一研究所授权单位)



(公安部一所威胁情报源)

d. 技战法赋能能力

公安部第一研究所作为关键信息基础设施保护中心（关保中心），发挥着行业引领作用。我公司作为其在云南设立的服务站，始终紧跟步伐，深度参与关键信息基础设施保护培训的筹备工作，积累了丰富且专业的经验。凭借于此，无论是面向攻击方开展攻防技巧与策略的专项培训，还是针对防守方进行关键信息基础设施保护知识与技能的培训，我公司都具备强大的专业能力，能够高质量地完成各项培训任务。

e. 人工复核+多样工具结合能力

在互联网安全检测服务中，我公司将利用人工+三个工具（资产与数据风险感知雷达平台、互联网敏感信息监测系统、网站监控预警平台）的形式对互联网进行安全检测，通过服务工具实时监测，人工对结果进行复核，保证互联网数据的真实性。

在漏洞扫描服务中，我公司将利用多种漏洞扫描工具，包括：公安部第一研究所网络资产监测分析系统（网探 D01）、南天互联网安全风险管控平台、三种厂商漏洞扫描工具箱进行漏洞扫描，全方面发现系统中出现的安全漏洞。

在互联网安全检测服务领域，我公司采用“人工+智能工具”的复合模式开展工作。我公司将借助**资产与数据风险感知雷达平台、互联网敏感信息监测系统以及网站监控预警平台**这三大专业工具，对互联网环境进行全方位的安全检测，实时捕捉网络动态、监测潜在风险，运营团队则会对工具输出的检测结果进行细致复核，以此确保互联网数据的真实性与准确性。

在漏洞扫描服务方面，我公司将运用多种先进的漏洞扫描工具，包括**公安部第一研究所研发的网络资产监测分析系统（网探 D01）、南天互联网安全风险管控平台，以及来自不同厂商的三种漏洞扫描工具箱**。在扫描结束后，我公司将派出技术人员对扫描出来的漏洞进行二次验证。通过综合运用这些工具的同时结合人工复核，我们能够对系统进行深度扫描，全面发现系统中存在的各类安全漏洞，为客户的网络安全保驾护航。

f. 服务工具自主研发能力

历经十余年在云南省内深耕网络安全服务领域，为给本地客户提供更优质、更贴合需求的服务，我公司立足云南省实际的网络安全状况，自主投入研发力量，成功打造出三个用于支撑公司网络安全服务的专业工具。目前，这三个工具均已顺利获得软件著作权，相关证书信息如下：

