托管检测与响应服务（原生版）

用户手册

天翼云科技有限公司

2023 年 08 月

目录

1 背景概述

1.1 安全背景

随着网络空间战竞争越来激烈，2014 年习近平主席提出“没有网络安全就没有国家安全”的重要思想，将网络安全提到国家战略层面。这一战略的层面给我们信息化安全工作带来了多方面改变，同时也使得单位的信息安全工作压力与日俱增。当前，单位信息安全工作压力主要来自两方面：

首先，国家监管的压力，越来越多监管以及重点时期保障行为着重强调实际安全防护效果。其次，当前外部威胁变化过快，监测到的安全攻击行为一直未定制，且攻击手法多变，单位内部存在安全攻防不对等的情况，因为需要有一种手段提升单位信息安全的实际防护效果。因此希望通过本次项目的建设，构建以安全效果为目标的托管检测与响应服务（MDR）框架。

1.2 建设必要性和功效

1.2.1快速构建组织检测与响应能力的必要性

组织安全的威胁检测与响应能力构建，不仅需要相关系统平台的建设，同时，也需要团队培养、流程建立、策略调优等等一系列内容，组织需要耗费大量时间成本和试错成本。

在当前外部安全形式快速变化的情况下，通过托管检测与响应服务，可以快速构建起组织的威胁检测与响应能力框架，实现组织安全能力补充。并利用“人机共智”的特点实现 7*24 小时不间断安全监控。

1.2.2高投入产出比实现检测与响应的必要性

网络安全表面看起来是攻防之间的博弈关系，但实际是海量攻击手法和海量防御手法之间的较量。这意味着企业或组织要想拥有较多的防御手法，就必须了解攻击的各个阶段，并根据各个攻击阶段快速评估下一阶段攻击手法，制定防御措施。这就对组织的安全人员和安全平台提出了很高的技术要求，既要了解攻击防御手段以及安全数据分析能力，也要有大数据快速分

析、自动化响应及快速迭代更新能力。

天翼云推出托管检测与主动响应服务（原生版），通过把安全专家资源池化和安全平台能力共享化的方式，让更多的用户能随时享受到专业安全服务；同时，天翼云将安全专家的经验固化到安全运营平台中，实现精准的监测效果并输出专业的处置建议，达到“7*24 小时”安全托管的效果。打造的检测与主动响应服务可帮助用户识别威胁并主动采取措施降低威胁可能造成的影响，协助客户闭环处置安全事件，同时分析安全威胁的趋势，提供长期的安全规划及改进建议。

1.3 服务目标

威胁是信息安全工作中一直存在且无法回避的问题，安全建设的核心在于对威胁的快速检测与响应。通过快速发现识别威胁，使组织可及时避免或降低威胁所造成的损失，通过快速响应威胁，减少危害面。使组织在减低损失基础上，优化完善安全建设架构，避免后续同类威胁攻击。

因此通过天翼云托管检测与响应服务可帮助用户实现组织安全威胁风险的快速检测、持续监控、响应处置、跟踪闭环的效果。具体效果指标为：

- 安全威胁的发现时间越来越短，发现速度越来越快；
- 安全威胁的响应时间越来越短，响应速度越来远快；
- 安全事件的数量越来越少，最后在可接受的范围内波动。

这些具体的效果指标意味着组织内部的安全体系正在健康、有效地运转。

2 安全现状分析

2.1 数字化转型趋势下组织对检测和响应要求越来越高

近些年，在数字化转型大趋势下，企业核心资产早已由实物资产转变为信息资产。同时，随着全球政治变化、加密货币技术发展等外部原因，整个网络空间安全形式发生了巨大变化，一方面黑产呈现出分工精细化、工具简单化、手段隐蔽化的趋势，互联网侧无目的攻击强度不断增加。另一方面，专业黑客团队通过供应链、社工等手段开展的高级可持续威胁攻击的范围不断扩大。

仅 2020 年 CNCERT 捕获勒索软件达 78.1 万个，呈现快速增长趋势。威瑞森数据泄露调查报告，攻击者启动攻击到攻击成功往往只需要数分钟甚至几十秒便可完成。而组织仅利用自身安全力量和工具情况，无法应对复杂多变的攻击，攻防对抗变得愈加不对等，在当前数字化转型的趋势下，组织不得不对自身威胁检测和响应的能力要求越来越高。

2.2 监管要求组织需要够条件常态化的威胁对抗能力

随着网络空间战竞争越来越激烈，2014 年 2 月 27 日习近平主席在中央网络安全和信息化领导小组第一次会议上的讲话中首次明确提出“没有网络安全就没有国家安全”的重要思想，将网络安全提升到国家安全的战略层面。国家安全战略的落实，给我们网络安全工作带来了多方面改变：

a） 大量的法律、法规不断完善，要求越来越严

《网络安全法》已于 2017 年 6 月 1 日正式实施，针对违法行为可直接处罚相关单位和相关人员，并首次在法律中明确国家实行网络安全等级保护制度。随后，“网络安全等级保护 2.0 系列国家标准”悉数正式发布，并于 2019 年 12 月 1 日起正式实施。等保 2.0 成为我国网络安全领域的基本国策、基本制度和基本方法。等保 2.0 系列标准相较于以往的等保标准更加注重全方位主动防御、动态防御、整体防控和精准防护，实现了对云计算、移动互联网、物联网、工业控制系统、大数据等保护对象的全覆盖，以及除个人及家庭自建自用网络之外的领域全覆盖。

b） 安全检查方式不断升级，检查频率及力度不断提高

自 2017 年起，全国人大常委会组织网络安全法、全国人大常委会关于加强网络信息保护的决定（简称“一法一决定”）执法检查组正式启动“一法一决定”执法检查。随着网络安全形势

逐步严峻，相关执法机构、行业监管单位正在积极履行执法监管职责，下发各类安全检查要求。从单位自查、技术检测、现场访谈检查发展到攻防演习，安全检查方式不断升级，以检测排查并督促整改网络安全漏洞隐患、风险和突出问题，其次，检查频率也发展到如今常态化的检查频率，检查力度也不断加大，以提升重点行业、重要部门的网络安全防护意识和综合防护水平。日常信息安全工作压力逐渐增大。

c） 重保时期网络安全保障压力越来越大

历年针对关键信息基础设施的实战攻防演习的目标范围有增无减，演习参与单位的数量均属空前，造成单位内部安全保障压力较大。演习行动的本质是以实战性的检验方法检验各单位的真实的信息安全防护水平。大量被攻破的案例告诉我们，真实安全防护水平的提升依靠现有安全产品的同时更需要高级安全专家经验，才能更好地发挥出现有防护体系的效果。

2.3 安全建设由传统安全建设转为关注安全效果

在过往传统安全防护中，主要关注安全系统的建设、合规的情况与安全技术的使用，但随着国家合规要求和业务要求的提高，组织安全建设遇到了新的挑战：

资源投入有限，安全作为业务的支撑，不可能无限度的投入，安全建设必须充分考虑投入产出比，通过安全运营利用有限资源防御最大限度攻击。

安全人员是组织安全的根本，根据《2019 中国网络安全与功能安全人才白皮书》调研，网络安全人才平均年薪 24w，国内安全人员缺口达 100W+，而高阶安全人才缺口更为明显，但组织无法承担高水平安全人才的成本。

安全资源投入有限和高阶安全人才缺失的促使组织逐步开始重视组织的安全运营能力，安全建设不仅仅是安全系统的建设和架构的应用，更加是要以安全效果为目的的建设。

3 解决思路

天翼云“人机共智”的托管检测与响应服务通过主要采用线上安全专家团队高度协同的方式为用户提供服务。

托管检测与响应服务以部署在用户侧的安全组件作为服务的基础工具，通过必要的安全日志及流量采集，经过脱敏、加密处理之后再对接到天翼云自研的 MDR 平台和安全运营服务平台。MDR 平台基于内置的大数据架构、AI 算法以及安全用例（Use Case）对安全日志和安全告警进行汇总、降噪、关联分析，从海量安全日志中精准识别真实攻击行为和安全事件，由不同梯度

的高阶安全专家基于安全运营平台为用户提供 7*24 小时的事件检测与响应服务。

当监测到安全事件，安全运营平台将自动生成工单并实时通知云端分析师介入，云端分析师按照标准化流程开展安全事件的研判和响应工作，云端资深专家和首席安全专家组作为团队的后端资源，为云端分析团队提供强大的技术支援，确保每种类型的安全事件都有专业知识的安全专家来解决。在此过程中，天翼云提供服务可视化手段让用户全程感受服务进度

4 安全托管建设方法设计

4.1 参考标准

《中华人民共和国网络安全法》

《信息安全技术 信息系统安全等级保护基本要求》

《信息安全技术 网络安全等级保护设计技术要求》

《信息安全技术 网络安全事件应急演练通用指南》

《信息安全技术 网络安全威胁信息表达模型》

《信息安全技术 网络产品和服务安全通用要求》

《信息安全技术 网络攻击定义及描述规范》

《信息安全技术 安全漏洞分类》

《信息安全技术 安全漏洞等级划分指南》

《信息安全技术 信息安全漏洞管理规范》

《国家网络安全事件应急预案》

《信息安全技术 信息安全事件分类分级指南》

《信息安全技术 网络安全事件应急演练通用指南》

《信息安全技术 信息安全应急响应计划规范》

《信息技术 安全技术 信息安全事件管理》

《信息安全技术 大数据服务安全能力要求》

4.2 国内外安全体系

4.2.1IATF 框架

IATF，《信息保障技术框架》（IATF：Information Assurance [ə'ʃuərəns] Technical Framework ）是美国国家安全局（NSA）National Security Agency 制定，用于描述其信息保障的指导性文件。2002 年，我们国家 973“信息与网络安全体系研究”课题组将 IATF3.0 版引进国内后，IATF 开始对我国信息安全工作的发展和信息安全保障体系的建设起重要的参考和指导作用。

图 4-1 IATF 框架

IATF 提出的信息保障的核心思想是纵深防御战略（Defense in Depth）。在纵深防御战略中指出，人、技术和操作（operations 也可以译为流程）是三个主要核心因素，要保障信息及信息系统的安全，三者缺一不可。人是信息系统的主体，是信息系统的拥有者、管理者和使用者，是信息保障体系核心。

安全运营中心旨在构建一个面向运营的安全保障体系，安全运营的目的是使“保障安全手段（产品+技术）的应用”能够达到预期的良好效果（Effect）和提高效率（Efficiency），其本质就是“人、技术、流程”的有效结合，IATF 对于安全运营中心的建设具有重要的参考价值。

4.2.2自适应安全框架

自适应安全框架（ASA）是 Gartner 于 2014 年提出的面向下一代的安全体系框架，以应对云大物移智时代所面临的安全形势。自适应安全框架（ASA）从预测、防御、检测、响应四个维

度，强调安全防护是一个持续处理的、循环的过程，细粒度、多角度、持续化的对安全威胁进行实时动态分析，自动适应不断变化的网络和威胁环境，并不断优化自身的安全防御机制。

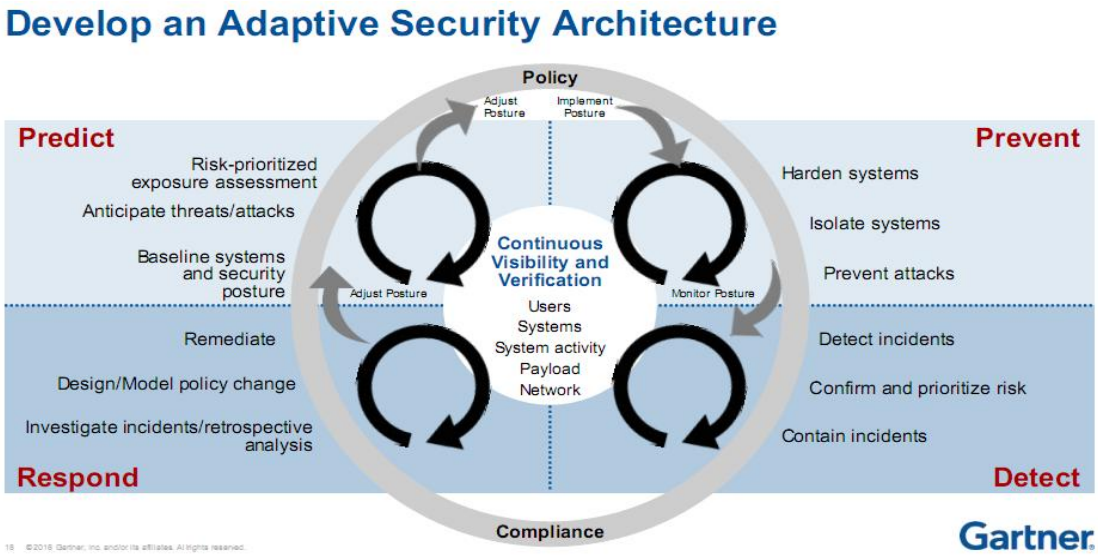


图 4-2　ASA 自适应安全框架

相对于 PDR 模型，自适应安全框架（ASA）框架增加了安全威胁“预测”的环节，其目的在于通过主动学习并识别未知的异常事件来嗅探潜在的、未暴露的安全威胁，更深入的诠释了“主动防御”的思想理念，这也是网络安全 2.0 时代新防御体系的核心内容之一。

4.2.3新时期的等级保护体系

为配合《中华人民共和国网络安全法》的实施，同时适应云计算、移动互联、物联网和工业控制等新技术、新应用情况下网络安全等级保护工作的开展，2019 年 5 月 13 日，《GBT22239-2019 信息安全技术网络安全等级保护基本要求》正式发布。

图 4-3　等保 2.0

新国家等级保护制度是以保护国家关键信息基础设施为重点的全新网络安全基本制度体系，为有效应对国际网络空间安全形势，新时期的等保不仅保护对象的范围扩大而且要求更加细化，具有以下突出的特点：

- 变被动防御为主动防御
- 变静态防御为动态防御
- 变单点防御为整体防御
- 变粗放防御为精准防御

4.3 建设落地方法

托管检测与响应主要的要素有工具、人员、流程。通过工具采集内外部的安全情况，形成安全素材；人员则对安全素材提供监测、分析、预警、处置；流程有助于整个托管检测与响应框架的质量管理。

托管检测与响应落地建设有存在两种方式，自运营和联合运营；自运营需要采购工具，培养人员，固化经验流程，存在成本高、周期长、团队建设困难的障碍；联合运营则是通过引入合作的方式，在工具、人员、流程方面结合自身情况引入第三方合作方，具备成本低，见效快，专家团队稳定等优势。本次方案建议采用联合运营这种方式开展持续化安全保障工作，建议以

安全效果为目标的托管检测与响应机制

5 服务内容

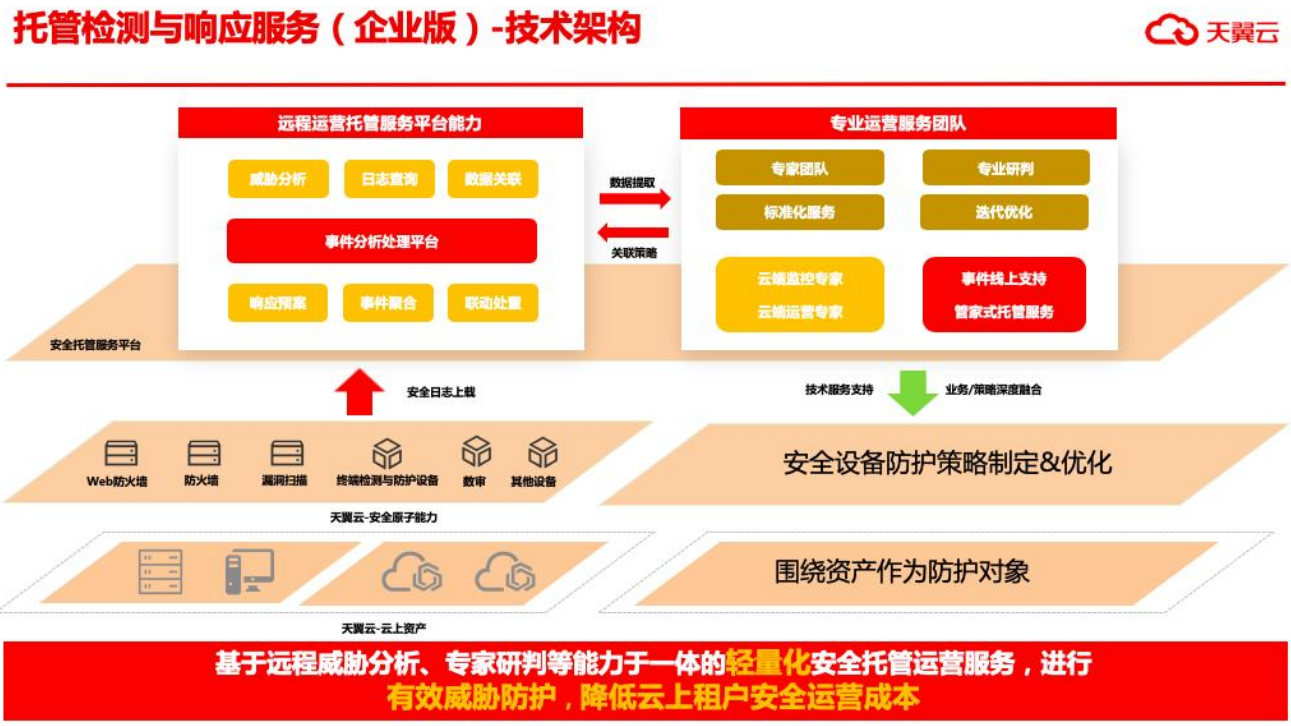
5.1 服务内容一览表

服务项	模式	服务项细分	服务内容
企业版	远程交付	企业版-托管基础服务	对用户的业务资产进行安全评估，通过将用户现有的安全设备接入 MDR 分析平台，对现有安全事件进行整体分析和实施监测，结合响应措施，保障业务安全
		安全评估	对云上资产、应用、网络进行整体安全评估，提供评估报告，提供加固建议
护航版	重要时期安全保障服务-远程	前期评估	对资产、网络、应用进行重保前的整体安全评估，协助用户完成安全加固
		重保服务	提供 7*24 小时不间断人工重保服务，持续进行安全监控及应急响应
	\	蓝军攻击服务	提供蓝军攻击服务，提供攻击报告
		威胁狩猎服务	重保期间提供蜜罐服务，单次服务时长 7 天，提供分析报告
应急响应	远程	应急响应服务	提供远程应急响应服务

5.2 服务介绍

5.2.1 托管检测与响应服务（原生版）企业版

天翼云基于丰富的公有云运营经验积累，面向公有云租户提供持续的安全监测和全面的保护服务，有效发挥云原生安全能力。依托安全运营工具对租户的云上资产包括：用户主机、web系统、域名等产生的安全告警事件进行实时监测分析，通过接入云上安全设备日志和告警，进行综合分析研判，协助用户对检测到的各项安全隐患包括且不限于漏洞利用、弱密码、Webshell写入、异常登录、木马回连等安全风险和异常行为进行处置，并通过企业微信、钉钉等方式告知用户。



5.2.2 托管检测与响应服务（原生版）护航版

为确保重大活动期间，业务系统的平稳安全运行，政企单位需提高网络安全保障强度，开展重要时期网络安全保障工作。托管检测与响应服务（原生版）护航版服务从前、中、后三个阶段，以梳理筹备、摸底评估、布防加固、模拟演练、值守保障、整改优化的工作步骤，密切关注重点网络基础设施和业务系统，通过明确的职责分工与协作，提供一体化保障体系，协助政企单位圆满完成安全重保任务，有效提升整体安全防护能力。

5.2.3 应急响应服务

应急响应（Incident Response/Emergency Response）通常是指一个组织为了应对各种意外事件的发生所做的准备工作以及在突发事件发生时或者发生后所采取的措施。 计算机网络应急响应的对象是指计算机或网络所存储、传输、处理的信息的安全事件， 事件的主体可能来自自然界、系统自身故障（这里的系统包括主机范畴内的问题，也包括网络范畴内的问题）、组织内部或外部的人、计算机病毒或蠕虫等。天翼云应急响应服务提供 7*24h 应急响应支持，一旦用户发生安全时间，将会第一时间响应并快速处置安全问题。

5.2.4 安全评估服务

安全评估服务通过用户现有的安全组件（如漏扫、EDR）及天翼云服务团队自有的安全评估工具，对用户的安全情况进行整体的安全脆弱性评估，全方位的发现目前用户资产存在的安全漏洞及脆弱性，并针对用户现状，提出切实可行的安全加固方案。

5.3 服务内容明细及交付流程

5.3.1 托管检测与响应服务（原生版）企业版交付内容及流程

服务阶段	实施任务	服务内容	交付物
购买阶段	选购服务	跟随购买指引，进入 MDR-企业版选购界面，根据需求选择对应的企业版服务内容并完成支付。服务团队将在 24h 内与用户进行对接，项目进入启动阶段。	

启动阶段	启动会	通过启动会，就项目的交付内容、范围、计划、以及项目预期达成的目标与客户充分完成讲解，并达成一致 1、充分讲解《项目启动会 PPT》，明确服务内容、服务范围、项目成员、《交付计划表》、验收标准、沟通计划、注意事项等，和客户充分的讲解，就客户痛点需求、项目预期目标达成一致。 2、同客户签署《保密协议》、《风险告知函》，并输出《会议纪要》；并完善《客户信息表》 3、会议达成一致后输出《项目启动会会议纪要》并邮件发送 4、建立客户专属服务群，默认为企业微信群，为客户提供专属服务	《项目启动会 PPT》
首次接入	资产梳理及确认	1.针对本次安全托管服务所购买的资产数，对服务资产进行二次确认并录入平台 2.进行资产指纹梳理，输出资产指纹信息表，在平台完善资产指纹信息录入	
	组件接入	1.梳理客户侧已有的关键安全设备及版本，配置相关的安全组件连接平台。 2.确认相关安全组件能正常从平台登录，数据能够正常上报平台	
	上线检查	1.针对本次对接上 MDR 平台的组件开展策略检查并记录检查结果至上线检查表中，风险策略与客户确认授权后进行策略调优工作； 2.对客户网络环境的拓扑图，组件信息及 DNS，其他代理地址进行初步梳理确认； 3.对服务资产进行确认并填写	
	首次威胁分析	1.安全组件的策略检查结果和结合首次安全组件安全日志接入分析结果输出首次威胁分析报告	

持续运营阶段	资产管理	1、根据收集的客户资产信息表，将资产信息录入到平台 2、对客户资产进行管理，包括资产上下线、资产变更、指纹收集等	《资产信息确认表》
	脆弱性管理	1.通过现有安全设备采集的日志信息进行漏洞分析，优先级排序，输出漏洞管理目录 2.负责整理和输出漏洞可落地修复方案及处置建议，并通告给客户进行处置 3.跟踪客户漏洞处置情况，处置漏洞修复过程中客户出现的问题	《漏洞清单》
	威胁管理	1.通过对安全日志的监测分析，识别内外部威胁，对真实威胁制定处置计划，通告给客户处置或由客户授权进行远程处置 2.根据客户的业务情况进行策略调优和其他加固措施的执行工作 3.对于公共的威胁情报根据用户业务情况判断是否存在威胁，及时推送给客户，若存在则协助进行处置 4.对跟踪的内外部威胁持续跟踪直至闭环	《威胁情报》
	事件管理	1.对客户反馈和 MDR 平台生成事件，通告给用户处置或由用户授权进行远程处置 2.对于无法处理的事件，进行有效上升处置，及时协调资源进行处置 3.对未解决的事件跟踪直至闭环	《事件处置报告》 《应急响应报告》
	沟通汇报	1、每周每月由服务经理针对客户时间段内所存在的安全工作情况形成报告推送给客户 2、由服务经理梳理客户半年度服务记录，输出服务总结报告，包括半年度汇报安全托管服务的交付进展及问题处置情况进行远程汇报。	《安全运营周报》 《安全运营月报》 《半年度总结汇报》

验收阶段	项目验收	1.输出年度总结汇报 PPT 并进行汇报 2.根据前期沟通的项目验收标准，输出《验收报告》，对 MDR 托管检测与响应服务交付整体验收	《年度总结汇报》 《项目验收报告》

5.3.2 托管检测与响应服务（原生版）护航版交付内容及流程

服务阶段	实施任务	实施内容	交付物
准备阶段	1、沟通需求、项目计划，准备《保密协议、授权书》、评估工具等	沟通具体需求，明确项目计划，确定安全评估范围，准备《保密协议、授权书》、评估工具	《保密协议、授权书》 《资产台账》
	2、资产识别/梳理	收集资产范围，核查现有的资产信息情况	
安全检查阶段	1、渗透测试	通过模拟黑客攻击的方式，对网站或在线平台进行全方位渗透入侵测试，提前发现系统潜在的各种高危漏洞和安全威胁，重点针对数据安全涉及漏洞进行检查，如越权漏洞、SQL 注入、会话固定、数据明文传输、验证失效等	《漏洞扫描报告》 《基线核查报告》 《渗透测试报告》
	2、基线核查	重要服务器、应用系统等基于信息安全风险的角度进行配置核查，从而达到相应的安全防护要求	
	3、漏洞扫描	通过扫描工具对目标业务资产进行漏洞扫描。	
	4、蓝军攻防演练	模拟真实场景中的攻防行动，对攻击行为进行防御演练，从实战中检验目前用户业务的安全程度及防护能力，在面临安全事件时，是否有充分的响应能力，并不断优化自身的安全运营防护体系	《安全实战攻防演练情况总结》 《实在中的安全脆弱点及加固建议》

重保值守	1、安全监测	通过现场值守的方式，在重保期间内依托于已经部署的安全设备或威胁检测与响应中心等产品，在现场对内外网系统以及安全设备告警信息进行实时监控分析，如内网流量监控、恶意扫描监控、数据窃取监控、网络病毒监控、恶意行为监控及告警信息监控等	《重保总结报告》《应急响应报告》按需
	2、应急响应	在业务遭受攻击或出现异常告警时，现场保障人员配合远程安全专家对攻击或告警进行应急处置，将突发事件带来的损失降到最低，并协助用户开展损失评估、加固指导等，提升网络安全防护水平	
验收阶段	验收	提交相关技术文档	技术文档

5.3.3 应急响应服务交付内容及流程

服务阶段	实施任务	实施内容	交付物
准备阶段	1、确定评估范围、小组成员、准备《保密协议、授权书》、漏扫等工具	确定安全评估范围，项目小组成员，准备《保密协议、授权书》、漏扫等工具	《保密协议、授权书》《服务确认及风险告知书》
应急响应阶段	1、信息收集	对网络现状进行资产评估，核查现有的资产信息情况	《应急响应报告》
	2、攻击路径还原	根据用户提供的信息对服务器日志、攻击者痕迹、安全设备日志及流量的分析，还原攻击者的攻击路径，理清安全事件的真实原因	
	3、问题文件清理	对用户服务器中可能隐藏的蠕虫病毒、后门程序、Rootkit 等恶意软件提供清理方案，通过上机排查，使用工具和手工对服务器后门进行清除	

	4、安全漏洞复检	基于网络安全事件应急响应资产问题，服务团队提供相应的安全加固建议，在用户对资产完成加固后提供漏洞复检工作，以确认资产漏洞完全修复，避免再次出现相同的安全事件	
	5、编制报告	编制应急响应报告	
验收阶段	工作总结会议	组织双方人员进行总结汇报	《验收材料汇编》
	验收	提交相关技术文档	

5.3.4 安全评估服务交付内容及流程

服务阶段	实施任务	实施内容	交付物
购买阶段	1.购买服务并完成支付 2.发起安全评估需求单	1.根据购买指引，在企业版服务有效期内，购买安全评估服务； 2.在控制台发起安全评估服务需求	
启动阶段	1、确定评估范围、小组成员、准备《保密协议、授权书》	确定安全评估范围，项目小组成员，准备《保密协议、授权书》、漏扫等工具	《安全风险评估范围清单》 《保密协议、授权书》 《服务确认及风险告知书》
	2、制定安全评估实施计划	对本次安全评估现有情况制定实施计划	
风险分析阶段	1、资产梳理	对网络现状进行资产评估，核查现有的资产信息情况	《信息安全风险评估报告》
	2、重要资产评估赋值	根据资产重要性程度判断确定系统的重要资产，从信息安全 CIA 三要素评估资产重要程度，明确资产的价值。通过与客户沟通判断每一项资产的 CIA 三性数值，根据赋值得出资	

		产价值	
	3、脆弱性分析	识别现有资产脆弱点。脆弱性评估需针对每一项需要保护的信息资产，找到其存在的弱点，包括技术性弱点、操作性弱点、管理性弱点	
	4、威胁性分析	识别脆弱性导致的威胁。根据资产目前所处的环境条件和以前的记录情况来判断，关键在于确认引发威胁的人或事物，即所谓的威胁源，包含人员威胁、系统威胁、环境威胁、自然威胁	
	5、风险分析	分析威胁可以利用脆弱性为资产带来危害的可能性及可能导致的影响	
	6、已有控制措施识别及有效性评估	识别已有的安全控制措施，分析安全措施的效力，确定威胁利用弱点的实际可能性，可以指出当前安全措施的不足	
	7、风险值评估	采用矩阵法计算出风险系数，核算并得出风险值	
	8、风险处置计划	根据安全风险评估发现的问题制定风险处置计划，协助完成整改	
	9、编制安全风险评估报告	通过识别资产现有的脆弱性，可能面临的威胁，并充分调研已有的安全控制措施，以综合判断存在的风险，帮助用户预知可能发生的安全事件	
验收阶段	工作总结会议	组织双方人员进行总结汇报	《验收材料汇编》
	验收	提交相关技术文档	

6 方案保障措施

6.1 人员保障

6.1.1项目组织保障

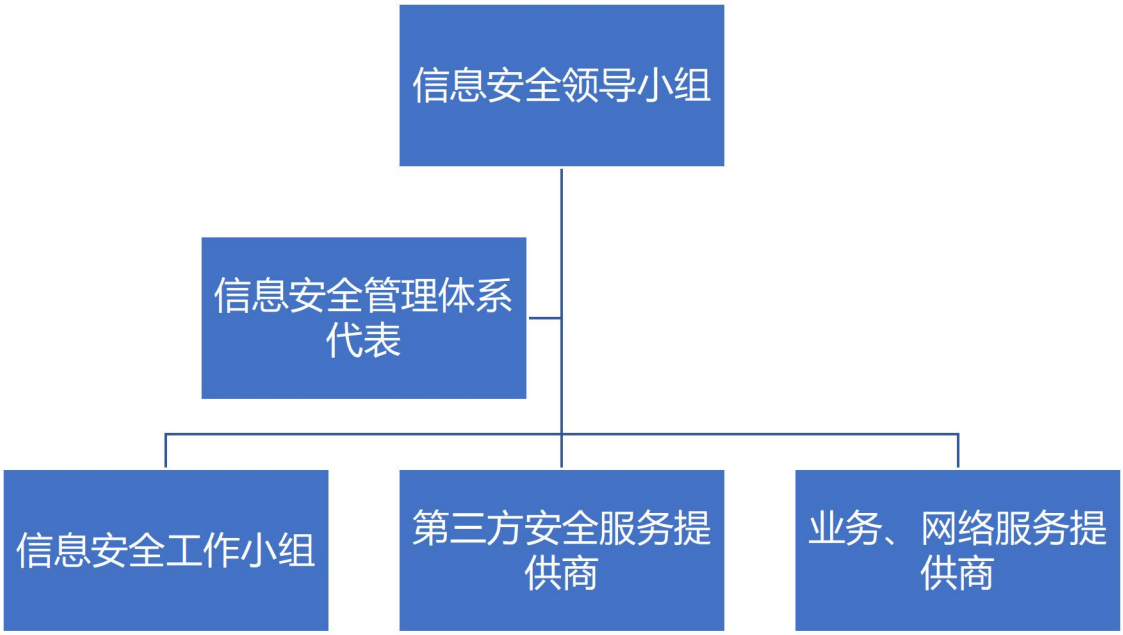


图 6-1 项目组织

6.1.1.1 组织结构及工作流程图

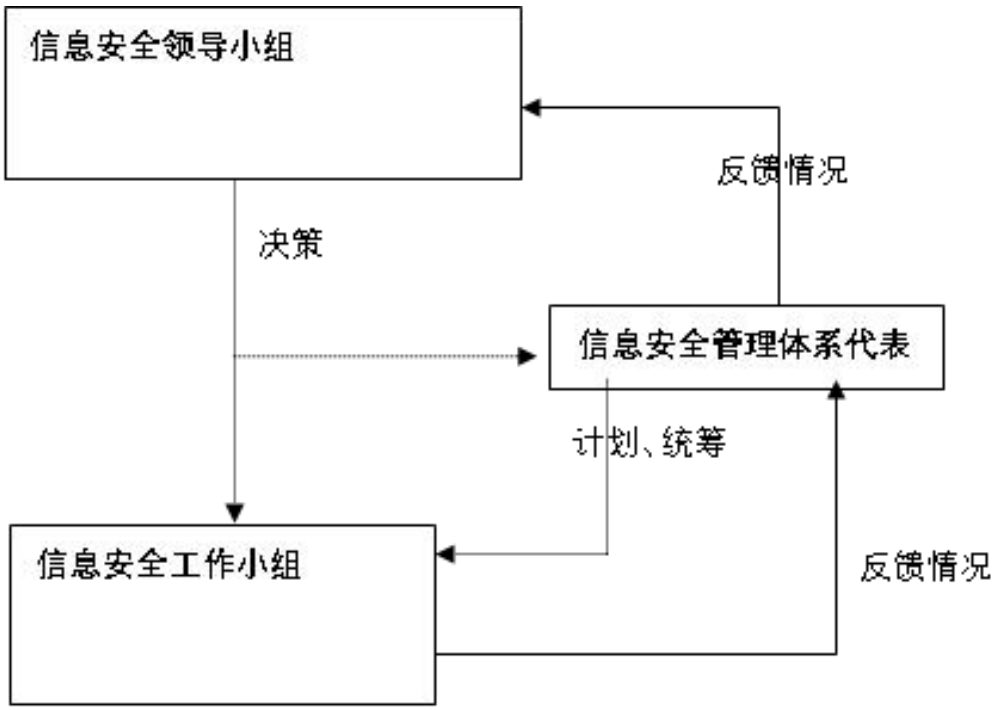


图 6-2 工作流程

6.1.1.2 工作流程说明

信息安全管理工作委员会需要定期向信息安全领导小组反映信息安全管理体系的运作情况；

信息安全领导小组通过会议，针对于信息安全管理体系运作的情况以及可能出现的问题，进行讨论做出决策；

信息安全管理体系代表根据信息安全委员会会议决策的结果，进行具体的实施计划工作，安排信息安全工作小组的人员开展实施；

信息安全工作小组的成员根据信息安全管理体系代表的计划，展开具体的实施工作。

6.1.2服务提供商人员组织团队

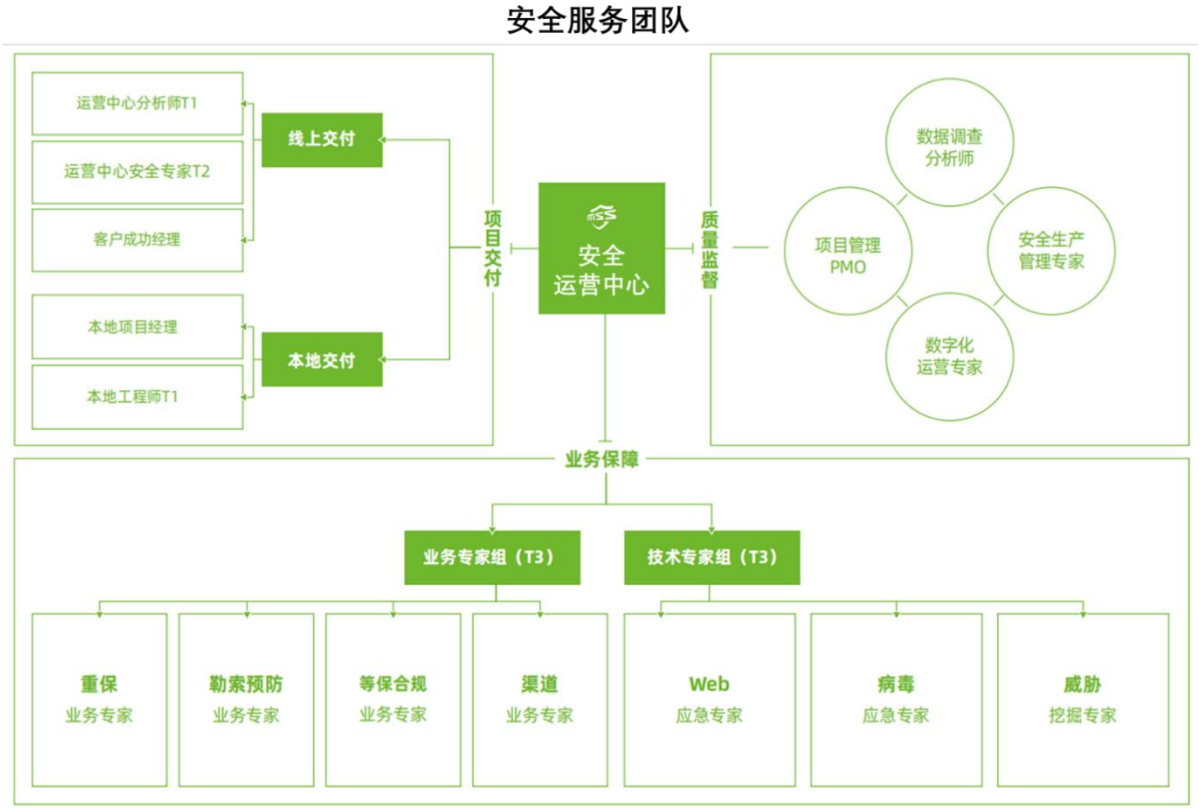


图 6-3 服务提供商人员组织

6.2 效果保障

6.2.1项目沟通管理

6.2.1.1 沟通策略

保持通畅的沟通渠道是项目成功的必要条件，采取如下沟通策略：

1. 客户项目经理和我方项目经理作为各自一方的总接口人，应保持密切的沟通，同时向各自的项目领导小组汇报；

2. 客户项目经理负责客户内部的沟通管理，客户项目相关人员向客户项目经理汇报；

3. 我方项目经理负责内部的沟通管理，项目组成员向项目经理汇报；

我方实施人员应就工程实施事宜与客户项目人员保持密切沟通，遇到无法解决的问题，应及时向各自的项目经理汇报，由双方项目经理协商解决，如果双方项目经理无法协商解决，应

向各自的项目领导小组汇报，由双方项目领导小组协商解决。

6.2.1.2 项目沟通渠道

项目沟通的主要方式包括口头沟通、会议沟通和书面沟通，主要内容见下表：

类别	适用范围	具体方式
口头沟通	只要双方确认的小问题	现场交流、电话
会议沟通	对项目实施中牵涉人员较广的某个专题	会议讨论、书面会议记录
书面沟通	需要详细描述、澄清的问题	书面材料、电子邮件、电子文档

会议制度

专题讨论会

针对规划设计或项目实施过程出现的各种问题，客户项目经理或我方项目经理可不定期的召集相关人员召开专题讨论会，明确问题的解决方法、解决时间和责任人，并监督解决过程。

会议结束后 3 个工作日内由我方项目经理输出会议纪要，并负责相关问题解决情况的督促和跟踪。

项目例会

根据项目进展，可每周或每两周进行一次项目例会，讨论项目状态和问题，沟通解决办法。由我方项目经理输出例会会议纪要并跟踪问题的解决。

报告制度

项目周报

项目实施期间，我方项目经理将定期向用户、我方项目相关人员发送周报，汇报项目状态，重点关注存在的问题，并提出建议解决方案。在后一周的周报中应报告前一周的问题解决状态。

6.2.1.3 问题管理制度

项目中出现的技术问题或其他严重问题，项目经理或技术负责人需要及时与项目组相关人员沟通处理，在可容忍的时间内不能有效解决，应该及时将问题进行垂直和职能升级，以保证项目获得更好的技术和资源支持，同时使用问题跟踪表进行跟踪处理，严重问题以日报形式通

报问题处理进展。

问题升级通道

职能升级：

我方执行组长/技术负责人->技术支持中心->研发中心；

垂直升级：

我方项目经理->项目管理团队->项目领导小组

问题跟踪表

问题跟踪表应包含如下内容：

1. 问题描述；
2. 问题优先级；
3. 原因分析；
4. 计划解决方案；
5. 责任人；
6. 计划解决时间；
7. 实际解决时间。

发生重要问题时，问题跟踪表作为周报或日报的附件发送。

6.2.2 项目风险及风险管理

6.2.2.1 风险分析

风险分析是一个持续实施的过程。在一个项目从始到终，任何新的或变更的风险应重新进行风险分析。对每一个风险确认应完成以下的风险列表和评估表：

风险描述

风险影响类型和可能影响的日期

风险告警标记

风险可能性

潜在的和可能的风险成本

风险优先级

6.2.2.2 风险确定

确定项目中潜在负面结果的不确定性。在项目生命周期中尽可能早的确定风险并存放在风险评估报表中，同时风险确定要在项目生命周期中持续进行。

在开始项目风险确定时，所有项目组成员有责任去发现自己负责部分工作中的潜在风险，并在每周的项目组例会上提交，或者在风险比较紧急的情况下直接提交给项目经理。

通过实现软件和技术结构的经验，我方设计了一个风险评估报表由以下几类构成：

与运行支持相关的风险。

与应用操作相关的风险。

与人力资源成本相关的风险。

与项目实施时间相关的风险。

与技术使用相关的风险。

每一类列出可能的风险项目，并询问客户此项风险在项目中作为低／中／高风险考虑。

这个评估或者由几个关键小组成员进行并交给项目组讨论，或者由关键的项目组成员在会议上讨论并记录下共同的评估结果。

在这些评估会议中，新的风险项目要加到风险评估报表中。

6.2.2.3 降低风险

降低风险即采取行动去除、减少、最小化项目风险的影响。

通过风险分析，形成一个风险降低计划，形式为风险降低策略表，其中包括一系列为项目成功而采取的最小化风险影响的行动，针对每一个风险都指定一个负责人，由负责人负责跟踪风险状态并随时更新风险降低计划。

对于那些影响低、可能性低的风险一般不需要制定风险降低计划，但是这些风险必须要监控，避免发展或转化为高风险。

对于需要降低的风险，有两个降低策略需要考虑：

预前处理策略：通过清除、减少或避免风险来最小化风险带来的威胁。

意外处理策略：在情况发生时采用一个意外处理计划可以最小化风险的影响。

6.2.2.4 风险降低控制

在整个项目过程中，为了有效的管理风险，如果需要，项目经理需执行下面的活动：

实施风险降低计划，如果通过发现风险告警标记为正面，那么可采用预前处理策略，执行风险降低计划。

评估风险降低计划的效率

再评估：针对项目中动态变化的风险，每周要再评估这些风险的状态

7 服务价值

7.1 降低安全风险

国内高水平的渗透攻击能力团队，助力客户全面和深度发现漏洞，及时进行修复与防护，降低业务面临的安全风险；

7.2 协助解决问题

全面的过程记录、测试报告，协助用户复测验证修复情况，确保机构能够清晰了解问题修复方法以及修复情况；

7.3 符合监管要求

面对公安部、网信、银监会等各行业标准化机构不定期进行突击检查，罚款额度高昂，可以帮助机构发现系统脆弱性，先于监管检查发现问题；

7.4 安全运营全闭环

事前实现精准预警，事中快速响应对抗，事后协助恢复和溯源加固，降本增效，提高安全能力水位线；