天翼云托管检测与响应服务（原生版）
服务白皮书

天翼云科技有限公司

2024 年 03 月

目录

1. 适用范围

该文档主要用于定义并约束天翼云面向公有云租户的托管检测与响应服务（原生版）产品（后续简称 MDR 服务）。客户需要了解的服务定义、SLA、服务管理保障机制等服务产品信息均会在该文档中进行说明。该文档原则上会作为服务合同附件对服务合同进行细致约定，以保障客户的利益。

2. 名词解释

托管检测与响应 Managed detection and response
托管检测与响应一种以远程交付为主的为用户提供持续威胁检测、分析、响应的安全服务。

应急响应 Incident Response/ Emergency Response
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。

信息安全漏洞 Information security vulnerability
信息安全漏洞（以下简称“安全漏洞”）是指计算机信息系统在需求、设计、实现、配置、运行等过程中，有意或无意产生的缺陷，这些缺陷以不同形式存在于计算机信息系统的各个层次和环节之中，一旦被恶意主体所利用，就会对计算机信息系统的安全造成损害，从而影响计算机信息系统的正常运行。

威胁 Threat
可能对信息系统造成危害的不期望事件的潜在原由。

威胁情报 Threat Intelligence
威胁情报是某种基于证据的知识，包括上下文、机制、标示、含义和能够执行的建议，这些知识与资产所面临已有的或酝酿中的威胁或危害相关，可用于资产相关主体对威胁或危害的响应或处理决策提供信息支持。业内大多数所说的威胁情报可以认为是狭义的威胁情报，其主要内容为用于识别和检测威胁的失陷标识，如文件 HASH，IP，域名，程序运行路径，注册表项等，以及相关的归属标签。

基线 Baseline
指主机操作系统、数据库、软件、容器等组件的配置、权限分配、管理规则等。

安全编排自动化响应 SOAR，Security Orchestration, Automation andResponse
一系列技术的合集，它能够帮助企业和组织收集安全运维团队监控到的各种信息（包括各种安全系统产生的告警），并对这些信息进行事件分析和告警分诊。

3. 服务概览

天翼云托管检测与响应服务（MDR）是一种为客户提供远程交付安全运营能力的服务，

该服务通过汇聚云上安全数据，快速检测、分析、发现、响应威胁，云端专家 7*24 小时全天候值守，以帮助用户处置突发安全事件，为用户构建低成本、标准化的安全防护运营能力。

天翼云托管检测与响应服务面向用户提供持续的安全监测和全面的保护服务，依托托管运营平台对租户的云上资产包括用户主机、Web 应用、数据库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。

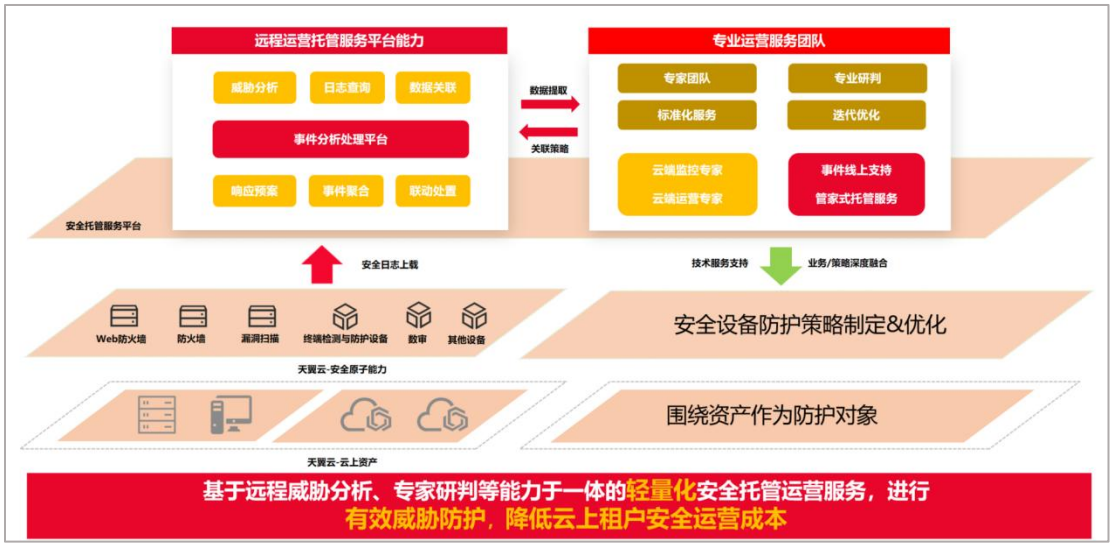

图 1 托管检测与响应服务方案

托管检测与响应服务围绕用户的云上资产，通过将已部署安全产品（WAF、防火墙、漏扫、EDR 等）的日志汇聚到托管服务平台，对安全日志进行集中分析，结合威胁情报、关联分析、机器学习等分析技术，发现真实威胁。

云端安全运营服务团队通过远程接入托管服务平台，7*24 小时监控安全事件，及时响应研判内外部威胁，提供处置建议，协助用户完成安全处置工作，完成事件闭环。通过安全运营工作，安全服务团队不断针对当前网络环境制定、优化安全设备防护策略，持续提升安全产品防护能力。

4. 标准服务项

4.1. 服务工作项

服务工作项	服务内容	服务交付方式	服务频次	服务交付物
托管资产梳理	与用户确认纳入本次托管服务的资产列表，形成托管服务资产台账并录入托管运营平台。 如用户需增加资产服务范围，可通过天翼云控制台或客户经理升级产品订单。	远程	首次接入	《托管资产台账》

安全日志接入	服务开通后，托管运营平台支持接入用户通过云等保专区购买开通的防火墙、WAF、EDR、漏洞扫描、堡垒机等安全产品日志。 如有其他日志接入需求，需与客户经理或服务经理确认技术方案。	远程	首次接入	
7*24 小时安全监控	依托托管运营平台对用户防火墙、WAF、EDR、漏洞扫描、堡垒机等安全产品安全事件的采集及分析，服务团队 7*24 小时监控用户资产安全状况，发现各类安全威胁，并生成工单	远程	7*24 小时	
安全产品策略优化	依据用户业务特点及运营中产品未配置、防护不到位、安全事件误报漏报等情况，安全服务团队整理提供安全产品策略优化建议，协助完成策略优化配置	远程	7*24 小时	
威胁分析及处置建议	安全专家针对各类威胁，进行深度分析验证，判断受影响范围及是否攻击成功，并将结果通过服务群/邮件等方式告知用户。 安全专家针对分析结果提供对应的处置或加固建议（如封锁攻击源、设置安全策略防护等措施）	远程	7*24 小时	《威胁分析报告》
事件分析与处置建议	对用户上报的安全事件进行及时响应。 实时针对异常流量、攻击日志和病毒日志进行分析，聚合发现安全事件。 针对分析得到的勒索病毒、挖矿病毒、篡改事件、webshell、僵尸网络等安全事件，通过工具和方法对恶意文件、代码进行根除，帮助客户快速恢复业务，消除或减轻影响。 事件跟踪：对发生的安全事件进行分级分类，并通过工单系统跟踪处置情况。	远程	7*24 小时	《事件分析报告》
应急响应	入侵影响抑制：通过事件检测分析，提供抑制手段，降低入侵影响，协助快速恢复业务。	远程	7*24 小时	《应急响应报告》

	入侵威胁清除：排查攻击路径，恶意文件清除。 入侵原因分析：还原攻击路径，分析入侵事件原因。 加固建议指导：结合现有安全防御体系，指导用户进行安全加固、提供整改建议、防止再次入侵。			
安全评估服务	服务团队定期对当前用户资产安全状况进行评估，扫描分析资产脆弱性。	远程	每季度	《安全评估报告》
漏洞扫描服务	服务接入后，服务团队定期通过用户漏洞扫描产品，对托管资产进行内外部漏洞扫描，全面了解资产漏洞开放情况。	远程	每季度	《漏洞清单》
最新漏洞通告	实时监测互联网最新漏洞披露情况，并与托管资产进行匹配，对最新漏洞进行通告与排查。通告信息中包含最新漏洞信息、服务资产受影响情况。 安全服务专家提供专业处置建议，包含修复方案及临时规避措施，并对该漏洞建立工单进行持续跟踪。	远程	7*24 小时	《漏洞通告及处置建议》
运营汇报	服务经理定期将安全运营工作情况形成报告推送给客户 服务经理梳理客户半年度、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	远程	每周、每月、每半年、每年	《安全运营周报》 《安全运营月报》 《半年度总结汇报》 《年度总结汇报》
日常咨询	提供日常安全技术咨询服务，用户可与服务经理联系，咨询网络安全、服务内容、服务流程等相关问题	远程	按需	

4.2. 工作项说明

4.2.1. 托管资产梳理

资产梳理及确认工作旨在全面清查和核实安全托管服务所覆盖的所有资产，确保资产信

息的准确性、完整性和一致性，确定后续的安全运营服务服务范围，确保安全监控的全面性。

MDR 服务资产梳理范围包括：云主机、物理服务器、安全产品、网络设备、数据库等。服务人员将对网络内的资产信息按照设备类型、系统类型等进行分类，评估资产的重要性，确定其在网络中的重要性和敏感程度，以便合理分配安全资源和采取相应的安全措施。

资产梳理完成后，服务人员将建立资产台账，与客户确认纳入安全托管服务的资产范围，并录入托管运营平台。

4.2.2. 安全日志接入

安全组件指客户网络环境中已经部署的安全产品。安全托管服务依赖客户网络内已经部署的安全产品，在购买服务前，客户应至少部署了防火墙、WAF、EDR 等安全产品，或在服务交付过程中，同期部署安全产品。

安全组件接入工作主要包括：

1、安全产品日志接入：当前网络环境中具备安全检测能力的安全且支持安全事件外发的安全产品，需配置通过 syslog、kafka、http 等协议将安全日志发送到托管运营平台，安全服务人员对日志解析后，将通过安全运营平台集中监控安全产品检测到的安全事件。

2、安全产品处置接口接入：为保证安全处置响应时间，托管运营平台支持 SOAR 技术，客户网络内的安全产品如支持 API 调用处置能力，需与托管运营平台对接。

针对无法对接监测设备的情况，暂时无法提供完整的安全威胁分析与研判服务，具体服务执行需根据实际情况进一步评估和沟通确认。

4.2.3. 7*24 小时安全监控

云端安全专家团队依托托管运营平台，对托管资产安全态势进行 7*24 小时统一监测，统一预警。一旦发现规安全事件，安全服务人员将及时通知用户，提供处置建议，并可在用户授权或预授权情况下，进行快速处置。对于 webshell、后门等高阶事件，可以及时升级到高级安全专家进行研判，一旦确认，服务人员将会即时响应处置。

4.2.4. 安全产品策略优化

安全产品种类多、专业度高，部分用户存在购买安全产品后不会配置的情况，导致出现安全产品防护能力未启用、防护不到位、策略不合理等问题。

MDR 服务团队在服务介入前及介入后，将针对用户业务情况及安全产品部署情况，检查当前安全配置是否合理，针对不合理的配置项，提供策略优化建议，并协助用户完成配置，将安全产品防护能力最大化。

4.2.5. 威胁分析及处置建议

网络威胁事件是指对网络安全构成潜在或实际损害的行为或事件。这些威胁可能包括窃听、重传、伪造、篡改、非授权访问、拒绝服务攻击、行为否认、旁路控制、电磁/射频截

获、人为疏忽等。随着互联网的快速发展和广泛应用，网络威胁事件日益增多，例如网络病毒、黑客攻击、网络钓鱼、数据泄露等。这些威胁不仅对个人用户造成威胁，也对企业、政府机构、金融机构等重要网络系统构成严重威胁。

安全服务团队依托防火墙、WAF、EDR 等具备威胁检测能力的产品，实时针对外部攻击如黑客攻击、病毒、DDOS 攻击、钓鱼等进行监测与响应；同时安全运营中心安全专家将针对每一类威胁，进行深度分析验证，分析判断是否存在其他可疑主机，结合海量数据脱敏、聚合发现安全事件，并将结果通过邮件、微信等方式告知用户并进行跟踪。

4.2.6. 事件分析与处置建议

4.2.6.1. 服务描述

网络安全事件是指由于人为原因、软硬件缺陷或故障、自然灾害等对网络和信息系统或者其中的数据造成危害，对社会造成负面影响的事件。这些危害可能包括网络服务中断、数据泄露、系统瘫痪等，这些事件的发生可能会对个人、组织或国家造成重大的损失。

安全服务团队依托托管运营团队，7*24 小时监控网络中发生的安全事件并响应由用户上报的安全事件，高级安全分析人员对安全事件进行分析研判，确定安全事件真实性及响应范围，并及时提出处置意见。服务团队通过工单系统，全流程跟踪安全事件流转，确保事件闭环。

4.2.6.2. 服务流程

1. 托管运营平台检测发现或用户上报安全事件
2. 安全分析人员据事件详情进行研判
3. 当安全事件研判为真时对该事件进行预警
4. 快速分析事件危害并及时告知用户影响并提供临时抑制手段
5. 针对安全事件进行深入调查和原因分析
6. 根据安全事件的原因分析结果，针对性提出安全加固建议
7. 输出包含加固建议的《事件分析与处置报告》

4.2.7. 应急响应

4.2.7.1. 服务描述

应急响应服务包括主动响应和被动响应流程，对客户的页面篡改、通报、断网、webshell、黑链等各类严重安全事件进行紧急响应和处置。通过及时联系客户进行溯源分析排查，根据 WEB 安全事件、恶意程序事件、网络流量攻击、信息破坏事件等不同事件的定级和响应级别，提供给客户专业的安全整改加固建议。

依托于安全防护组件和检测响应组件，实现入侵检测（分钟级检测）、0Day 检测、后门检测、篡改检测、勒索病毒、挖矿病毒等安全检测，支持紧急电话、邮件、微信等多种响

应渠道和方式，结合云端安全专家团队，对安全事件进行入侵影响抑制、入侵威胁清除、入侵原因分析、加固建议指导等服务实施。

4.2.7.2. 服务流程

1．事件检测阶段

安全服务团队第一时间对接了解事件具体详情根据事件的原始描述、各方面收集的信息确定事件性质和影响范围。

根据事件类型进行针对性检测被入侵业务系统或网络查看当前状态，确定安全事件的应急处理方案并包含方案失败的应变和回退措施。

2．入侵抑制阶段

如果在响应过程中，发现攻击正在扩散、持续，或者正在对当前业务正常运行造成影响，安全服务团队将采取抑制手段， 抑制事态发展是为了将事故的损害降低到最小化。

在入侵抑制阶段，包含但不限于以下手段：

- 断开部分网络连接
- 暂停入侵业务的系统服务
- 关闭入侵主机的操作系统

3．根除恢复阶段

在对安全事件进行原因初步分析和影响抑制后，安全团队将对当前安全事件进行进一步处理并对证据进行留存，具体工作包括：

- 扫描并清除系统中存在的病毒、木马、恶意代码等可疑程序
- 清理 WEB 站点中存在的暗链、木马等页面
- 恢复被入侵篡改的系统配置，清理黑客创建的后门账号
- 删除异常系统服务、清理异常进程
- 验证入侵威胁清除并协助恢复正常业务服务

4．入侵原因分析

安全团队将从网络流量情况、主机系统日志、网站服务日志、业务应用日志、数据库日志等，结合已有安全设备数据，分析入侵方式，还原造成安全事件的过程。（部分安全事件由于入侵过程中攻击者对日志进行清除或者系统未进行保留相关日志的配置从而导致无法定位入侵原因，故乙方安全团队将尽可能的分析潜在的原因，但不承诺能给出入侵原因的全部原因和入侵全部过程。）

5．跟进总结阶段

事件处理完毕后，根据整个事件情况进行分析汇总并提交《应急响应报告》，针对安全事件现象、处理过程、处理结果进行陈述，同时对入侵原因进行分析，并给出相应的安全加固建议和安全防御体系建设指导。

- 执行完整的检测阶段流程。
- 确认系统是否再次被入侵。如果有请回到抑制和根除阶段。
- 总结安全事件的处理过程和技能，调整安全策略，输出总结文档。
- 输出跟进阶段的报告内容。

4.2.8. 安全评估服务

服务团队会对安全态势做整体评估，形成安全评估报告，帮助用户更加全面地了解自身资产漏洞、脆弱性及风险。主要评估流程如下：

4.2.8.1. 资产脆弱性扫描

利用用户漏洞扫描产品进行资产扫描，同时整合托管运营平台的脆弱性分析，从主动和被动识别两个维度进行业务资产现存漏洞问题的交叉识别，输出《业务资产安全漏洞清单》，安全服务专家对扫描出来的漏洞进行威胁分析和重要程度排序。漏洞扫描范围包含云主机、WEB 业务系统、数据库。

4.2.8.2. 业务资产脆弱性分析

云端安全专家结合服务资产的业务特征和托管运营平台所采集的流量分析日志，综合分析业务资产存在的弱密码和明文传输等脆弱性问题，并执行脆弱性风险分析，对脆弱性问题进行排序，整合《业务资产安全漏洞清单》输出《业务资产脆弱性问题清单》。

4.2.9. 漏洞扫描服务

4.2.9.1. 服务描述

服务团队定期针对系统、设备、应用的脆弱性进行自动化检测。漏洞扫描服务帮助企业侦测、扫描和改善其信息系统面临的风险隐患，执行安全评估和漏洞检测，提供漏洞修补和补丁管理，是企业和组织进行信息系统合规度量和审计的一种基础技术手段。

4.2.9.2. 服务范围

网络中的信息系统所涉及网络设备、操作系统、数据库、常见应用服务器以及 WEB 应用等范围进行扫描。

漏洞扫描的详细服务范围如下：

- 操作系统

Windows、Linux、AIX、UNIX 通用、Solaris、FreeBSD、HP-UX、BSD 等主流操作系统。

- 数据库

Oracle、MySQL、MSSQL、Sybase、DB2、Informix 等主流数据库。

- 常见应用服务

Apache、IIS、Tomcat、Weblogic 等主流应用服务，常见 FTP、EMAIL、DNS、TELENT、POP3、SNMP、SMTP、Proxy、RPC 服务等。

- Web 应用程序

ASP、PHP、JSP、.NET、Perl、Python、Shell 等语言编写的 WEB 应用程序。

4.2.9.3. 服务内容

漏洞扫描会对用户云上资产如云主机、应用软件、中间件和服务等进行安全漏洞识别，详细内容如下：

1．云主机操作系统漏洞识别

- 操作系统（包括 Windows、Linu 等）的系统补丁、漏洞、病毒等各类异常缺陷。
- 空/弱口令系统帐户检测。
- 访问控制：注册表 HKEY_LOCAL_MACHINE 普通用户可写，远程主机允许匿名 FTP 登录，ftp 服务器存在匿名可写目录。
- 系统漏洞：System V 系统 Login 远程缓冲区溢出漏洞，Microsoft Windows Locator 服务远程缓冲区溢出漏洞。
- 安全配置问题：部分 SMB 用户存在薄弱口令，试图使用 rsh 登录进入远程系统。

2．应用层漏洞识别

- 应用程序（包括但不限于数据库 Oracle、DB2、MS SQL，Web 服务，如 Apache、WebSphere、Tomcat、IIS 等，其他 SSH、FTP 等）缺失补丁或版本漏洞检测。
- 空弱口令应用帐户检测。
- 数据库软件：Oracle tnslsnr 没有设置口令，Microsoft SQL Server 2000 Resolution 服务多个安全漏洞。
- Web 服务器：Apache Mod_SSL/Apache-SSL 远程缓冲区溢出漏洞，Microsoft IIS 5.0 .printer ISAPI 远程缓冲区溢出，Sun ONE/iPlanet Web 服务程序分块编码传输漏洞。
- 电子邮件系统：Sendmail 头处理远程溢出漏洞，Microsoft Windows 2000 SMTP 服务认证错误漏洞。
- 防火墙及应用网管系统：Axent Raptor 防火墙拒绝服务漏洞。
- 其它网络服务系统：Wingate POP3 USER 命令远程溢出漏洞，Linux 系统 LPRng 远程格式化串漏洞。

4.2.10. 最新漏洞通告

4.2.10.1. 服务描述

对于最新出现的流行、未公开威胁如 0Day 漏洞、致命性漏洞、新型病毒、APT 组织化攻击等进行实时预警。安全服务团队将密切关注安全威胁，并结合安全威胁情报进行针对性评估与排查，将排查结果与加固建议提交至用户进行风险通告，并协调促进整改。

未知威胁快速规避措施：通过安全策略的运营（例：自定义策略临时防护）临时应对、规避最新爆发的风险。

安全功能迭代升级（例：更新规则库、升级安全组件）将防护能力整合到安全设备。

4.2.10.2. 服务流程

1．未知威胁爆发

2. 威胁情报团队制定未公开威胁分析方案，建立应急预案
3. 云端安全专家对此威胁进行数据采集、材料整理
4. 针对此威胁输出规则并输出各产品规则库
5. 推送此威胁预警同时提醒用户进行相关系统或应用自检，输出加固建议
6. 服务团队依据威胁情报安全规则库及用户授权对用户资产进行排查
7. 检测组件更新检测规则/防御组件更新防御规则
8. 针对高级别安全风险采用升级机制协调安全专家分析研判
9. 输出《未公开威胁报告》并将排查结果及加固建议通过邮件、微信或书面形式告知用户，同时提供全面加固建议

4.2.11. 运营汇报

服务经理针对项目服务情况和组织安全状态提交阶段性服务成果报告，安全专家针对组织遗留安全运营问题给出建议性指导和方案。

4.2.12. 日常咨询

在托管服务过程中，服务团队支持通过电话、邮件、微信、企业微信等方式为用户提供网络安全相关的咨询服务，包括网络安全规划、安全产品能力、安全测试与评估等方面的服务，帮助企业全面提升网络安全水平。

5. 非标服务工作说明

天翼云在标准服务的基础上，可以接受客户一定程度上的服务定制化诉求，针对各类可能出现的服务定制化诉求相关说明如下。

5.1. 服务频次更改

服务对象可以对标准化服务工作项的服务频次进行修改，以符合服务对象内部的运营管理需要或各类合规要求。但由此可能会带来服务工作量上的变更和调整，需要在项目合同签署前提出服务频次的修改诉求，并由天翼云基于实际服务人力消耗情况给出定制化服务报价。

5.2. 服务内容更改

服务对象可以在项目合同签署前提出对服务工作项的服务内容的调整诉求，以更好的匹配服务对象内部的管理需要。调整的内容可以包括：交付物模板、服务流程、服务工作范围。针对各类调整诉求，天翼云将基于以下原则进行处理。

交付物模板修改：

可在标准交付物模板上增加客户要求的输出内容，但不建议裁剪标准交付物模板中的内容，所有裁剪动作将可能导致天翼云服务质量存在下降风险。

服务流程修改：

在项目早期，服务项目经理和服务人员会与服务对象沟通每个服务的工作流程，对于变更类的服务内容将尽可能与客户要求衔接。但服务流程修改并不能对服务中各类安全主体责任进行修改。

服务工作范围修改：

服务工作范围可以在服务工作项的工作约定范围内基于客户实际需求对工作内容进行适当调整，这些调整包括但不限于增加部分报告撰写、通知等工作，但由于不同的服务工作内容可能涉及到的工作难度和工作量差异巨大，需要在合同签署前进行细致沟通。

以上所有服务内容更改，均可能导致服务工作量的变化，天翼云将基于服务内容修改给出合理的定制化服务报价。

5.3. 超出服务工作项约定的工作

对于超出服务工作项约定的工作内容，服务对象可在项目合同签署前提出要求，具体由天翼云项目经理进行评估和管理，给出结论，并评估服务定制化报价。对于符合以下所有条件的服务工作项，天翼云才会采纳。

1、服务工作项应可标准化复制，并非单一客户的独特要求。（独特要求的例子：针对客户自行开发的自用平台进行运维托管。）

2、服务工作项不应和其他服务产品重叠，如果重叠，天翼云将额外提供其他服务产品以解决客户需求。

3、服务工作项不应超出天翼云运托管检测与响应服务的责任权限，不得变更安全责任主体。

6. 服务交付流程

6.1. 服务售前沟通

为保障用户安全服务述求得到满足，我们的产品运营团队针对服务方案、服务内容、服务特点、适用场景等内容提供售前沟通服务，帮助用户了解 MDR 服务，明确服务方案及预

期目标，降低因标准服务内容与实际项目情况差异带来的困扰。售前联系人信息如下：

区域	联系人	联系电话
北方大区	张松帅	18618168813
华南大区	刘伟然	18123641562
华东大区	李强	13319272463
西北大区	李强	13319272463
西南大区	张松帅	18618168813

除服务内容外，我们的售前人员会与您沟通服务接入所需前置条件，包括计算资源、存储资源、网络情况、已部署安全产品等内容，确保服务方案可顺利落地。

6.2. 服务条款和 SLA 确认

服务合同签署前，您需仔细阅读标准服务项及服务 SLA 内容。若本文档 SLA 的条款与条件与协议中的条款和条件相冲突或不一致，则以本文档 SLA 内容为准，但仅在该冲突或不一致范围内适用。我们会适时修改 SLA 协议，但在您的订购期限内，我们不会以实质性降低服务水平的方式修改您的 SLA 条款；如果您续订服务，则续订之时届时适用的 SLA 协议的版本将适用于您的续订期。您继续服务即代表您同意届时适用的 SLA。

6.3. 服务合同签署

双方根据服务需求，协商并达成一致后，签订服务合同。合同中需明确服务范围、服务交付时间与方式、服务内容、服务等级、服务期限、价格和支付方式等内容，同时需包括违约责任、解决争议的方式等条款。

服务合同签署时，同时阅读《天翼云 MDR 服务说明及风险告知书》及签订服务授权书，明确具体服务项目、授权期间及资产对象。

6.4. 服务准备

6.4.1. 组建服务团队

服务签订后，我们将会根据项目情况快速组建服务团队，确保服务顺利开展，服务团队主要角色如下：

天翼云侧：

角色	描述
项目经理	负责项目沟通，统筹项目进展，协调内外部工作内容
服务经理	负责安全服务工作汇报、跟踪事件处置进展、日常安全咨询、根据处置建议协助用户完成处置流程等
安全分析工程师	负责日常安全监控，负责常见威胁的研判
服务专家	云端高级服务专家，负责高级别威胁的研判及提供处置建议
客户经理	负责处理用户投诉建议等

用户侧：

角色	描述
项目经理	负责项目沟通，统筹项目进展，协调内外部工作内容
运维经理	负责与服务团队对接事件处置及安全产品策略配置等

6.4.2. 项目启动会

MDR 服务团队与用户在项目正式实施前召集所有项目相关人员就项目的细节，项目范围,项目组织架构和近阶段工作计划等内容进行沟通和确认,为项目今后的相关工作做准备。其中，MDR 服务团队主要工作内容：

- 项目介绍：明确项目目标及预期成果。
- 团队成员介绍：介绍 MDR 服务团队主要人员。
- 沟通协作计划：明确服务沟通主要方式方法，明确双方服务主要项目负责人。
- 培训赋能：就 MDR 托管服务做相关介绍。
- 会议纪要：形成会议纪要并发送双方主要项目人员。

6.4.3. 托管资产确认

MDR 服务开始前，需由用户提供资产台账，确认接入本次服务的资产范围及资产明细。如用户无资产台账，服务团队将协助用户开展资产梳理工作。

资产梳理主要工作是对现有的资产进行调查和统计，包括网络设备、安全设备、服务器、数据库、应用等资产，统计信息主要包括 IP 地址、设备型号、网络区域、系统软件情况、业务情况、操作系统等。

托管资产台账确认完成后，需由用户确认，确认完成后，导入托管运营平台，做持续安全监控。

6.4.4. 安全产品接入

MDR 服务依赖用户已部署安全产品，服务接入前，用户需至少部署了防火墙、WAF、EDR、漏洞扫描、堡垒机等产品，且已部署安全产品具备日志外发能力，能够将安全日志通过现有网络架构发送至托管运营平台。MDR 服务建议用户接入云等保专区产品，快速接入服务，减少安全产品接入问题。

用户需提供现有安全产品明细表，至少包括产品名称、产品类型、IP 地址、用户手册、日志格式说明文档、处置接口调用文档、登录地址、登录用户名及密码、运维管理员等信息，协助安全服务团队完成产品接入、日志解析、设备登录、事件处置等。

如接入非天翼云安全产品，用户需协调安全产品原厂商，支撑完成日志接入及处置接口接入工作。

6.4.5. 处置授权流程确认

在服务过程中，如需由安全服务人员提供配置变更、策略变更、上机处置等实操工作时，需由用户提供授权，在未授权的情况下，服务人员不会对用户的资产做任何实际的变更操作。

用户可以选择统一授权或有实际操作需求时临时授权，统一授权需提供授权协议，临时授权可通过即时通讯完成，服务团队在每次变更实操前，均会向用户询问授权意见。

6.5. 服务试运行

6.5.1. 首次安全分析

托管资产录入及安全产品接入完成后，MDR 服务完成上线并进入试运行阶段，试运行阶段周期为一周。服务上线 3 天后，安全服务团队将对用户整体安全情况做首次分析，分析内容包括：脆弱性分析、受攻击情况、潜在威胁分析、安全事件分析，并提供处置建议，形成《首次安全分析及处置报告》。

用户可根据《首次安全分析及处置报告》内容，确定服务范围及内容是否符合预期，并提出整改建议，服务团队将根据用户建议，及时调整服务内容及流程，确保服务顺利进行。

6.5.2. 处置流程验证

服务试运行阶段，安全服务人员将针对处置流程做首次验证，根据真实或者模拟安全事件创建处置工单，跟踪事件处置全流程，并根据已确认的用户沟通方式实时通知用户，提供处置建议，协助用户完成安全事件处置。针对高级别安全事件，服务团队将根据流程级别，升级安全事件，由服务专家完成事件研判，反馈处置建议。

6.6. 服务执行

持续运营阶段，安全服务团队将围绕资产、脆弱性、威胁、事件四个核心风险要素开展 7*24 小时安全保障工作，并持续对安全策略进行优化调整，针对高级别威胁事件及安全事件，及时汇报用户，提供处置建议，及时响应各种安全问题。

6.7. 总结汇报

服务结束后，项目经理针对项目服务情况和企业整体安全态势提交服务成果报告，安全专家针对组织遗留安全运营问题给出建议性指导和方案。

7. 服务 SLA

7.1. 服务效果承诺

天翼云托管检测与响应服务的效果承诺将围绕安全事件、威胁与漏洞三个维度进行详细定义，详情如下：

7.1.1. 安全事件级别定义

安全事件级别	具体定义
一般事件 **（对标国家标准 IV 级事件）**	一般事件是指个别用户或业务受影响的信息安全事件，包括以下情况：1) 会使特别重要信息系统遭受较小的系统损失、使重要信息系统遭受较大的系统损失或一般信息系统遭受严重或严重以下级别的系统损失；2) 产生一般的社会影响。
较大事件 **（对标国家标准 III 级事件）**	较大事件是指能够导致较严重影响或破坏的信息安全事件，包括以下情况：1) 会使特别重要信息系统遭受较大的系统损失、使重要信息系统遭受严重的系统损失或一般信息信息系统遭受特别严重的系统损失；2) 产生较大的社会影响。
重大事件 **（对标国家标准 II 级事件）**	重大事件是指能够导致严重影响或破坏的信息安全事件，包括以下情况：1) 会使特别重要信息系统遭受严重的系统损失或使重要信息系统遭受特别严重的系统损失； 2) 产生重大的社会影响。
特大事件 **（对标国家标准 I 级事件）**	特别重大事件是指能够导致特别严重影响或破坏的信息安全事件，包括以下情况：1) 会使特别重要信息系统遭受特别严重的系统损失；2) 产生特别重大的社会影响。

7.1.2. 安全事件服务效果承诺

事件等级	事件通知	遏制影响时限	准确率	闭环率	超时补偿
一般事件	从安全日志分析研判到通告，用时<1 小时	遏制影响时间<4 小时	安全事件经过人工确认后，准确率达到 99%	闭环率 100%	服务时长增加 7 天
较大及重大事件	从安全日志分析研判到通告，用时<30 分钟	遏制影响时间<1 小时	安全事件经过人工确认后，准确率达 99%	闭环率 100%	服务时长增加 15 天
特大事件	启用应急响应机制，工作时间 30 分钟，非工作时间 60 分钟之内云端专家进行响应，由专家团队进行远程全程协助解决。				服务时长增加 30 天

7.1.3. 威胁及漏洞级别定义

威胁及漏洞级别	具体定义
一般威胁	攻击者对云网发起的网络安全攻击，对客户业务造成一定影响。
重大威胁	攻击者对云网发起的成功的有组织、有预谋的持续性网络攻击（如 APT），可造成客户系统异常、数据泄露、经济损失等严重影响。
一般漏洞	非高危可利用的漏洞均属于一般漏洞。

高危漏洞	高危可利用的漏洞指能够通过远程执行代码、命令执行等手段，控制业务系统权限、导致大量关键敏感数据泄露。

7.1.4. 威胁及漏洞服务效果承诺

威胁及漏洞级别	威胁及漏洞通知	遏制影响时限	准确率	闭环率	超时补偿
一般威胁	从安全日志分析研判到通告，用时<1 小时	遏制影响时间<4 小时	威胁经过人工确认后，准确率达到 99%	闭环率 100%	服务时长增加 7 天
重大威胁	从安全日志分析研判到通告，用时<30 分钟	遏制影响时间<1 小时	威胁经过人工确认后，准确率达到 99%	闭环率 100%	服务时长增加 15 天
一般漏洞	云端专家使用漏扫工具完成漏扫后 2 个工作日内推送漏洞报告	配合客户修复漏洞，从漏洞报告到闭环<14 个工作日	漏洞经过人工确认后，准确率达到 80%	闭环率 80%	服务时长增加 3 天
高危可利用漏洞		配合客户修复漏洞，从漏洞报告到闭环<7 个工作日	漏洞经过人工确认后，准确率达到 99%	闭环率 99%	服务时长增加 7 天
最新漏洞预警与响应	0day、新型威胁从发现到预警<24 小时	0day 检测规则更新时间<2 个工作日	/	/	服务时长增加 3 天

7.2. 服务补偿

7.2.1. 补偿方式说明

如果天翼云未达到本 SLA 承诺的服务可用性，则您可依照本 SLA 的规定申请补偿，补偿将以服务补偿时间的方式发放，且该补偿是天翼云针对服务不满足服务可用性承诺向您提供的全部及唯一补偿。本 SLA 适用于云托管用户使用天翼云原生安全产品且服务资产属于其保护范围，其他情况按需提供处置建议和指导，闭环率指在此基础上问题得以解决或用户接受风险，不计入用户无法解决问题的情况，最终解释权归天翼云 MDR 服务团队所有。

7.2.2. 补偿申请时限

您可在每个服务周期账单结清后对该服务周期没有达到服务可用性承诺的服务内容提出补偿申请，且补偿申请必须在该云服务没有达到服务可用性承诺的服务周期结束后两个月内提出。超出申请时限的补偿申请将不被受理。天翼云将对您的申请进行合理评估，并依据本 SLA 约定及诚信原则就是否适用补偿做出决定。

7.2.3. 补偿申请方法

您可以在天翼云用户中心提交工单或联系用户经理申请补偿。

8. 服务管理保障

8.1. 远程服务管理保障

8.1.1. 人员管理

建立组织结构，规定职务或职位，明确责权关系，以使组织中的成员互相协作配合，是项目顺利按计划进行的重要保证。本项目采用在项目经理的领导下，各级项目组成员责任制，并明确规范了个相关干系人的职责及各部门之间的协调关系。在项目验收上，设置由项目经理、用户项目经理等共同组成的验收小组。

8.1.2. 交付进度及成果管理

服务经理对交付进度和结果做好评估和管理工作，针对项目过程中识别到的人员能力风险、及资源投入，主动进行风险控制与资源协调；对于人员能力不足或人员离职等不可控的客观风险因素，及时同步反馈相关干系人，制定应对措施。

8.1.3. 协作沟通管理

服务经理要在项目组建时完成项目角色与职责划分，并根据项目交付计划建立项目沟通与协作机制，保障项目进度可控，项目信息能够有效及时做好内外部同步；形式不限于内部项目例会、客户侧项目例会，频率可根据项目实际情况设定；

协作沟通管理内容包括：各内外部会议纪要、服务里程碑内容及进展、交付内容、汇报纪要、验收结果等，要求各项活动在工作完成后，通过公司邮箱邮件发给用户，内部同步信息给区域及销售等项目相关人员，并且确保项目组成员清晰了解的项目目标、计划等。 为方便交流可以组建 QQ/微信群，分为公司内部交流群、项目组内部交流群、外部交流群（含用户），任何沟通纪要、交付物等项目材料最终结果要求具备完整邮件记录。

8.2. 服务质量监控

我们将根据服务合同明确本次安全服务项目的目标及范围，找出可能影响服务质量的技术要点，并逐一分析，确定需要监控的关键元素，设置整体项目实施过程中合理的检查点及度量指标，把满足项目质量标准的活动或者过程规划到项目的产品和管理项目的过程中。

8.2.1. 进度管理

根据安全服务项目总体进度要求、设计方案制定项目进度计划表，且满足磋商文件的时限规定，明确各节点的工程内容和考核指标。

严格按照进度计划按期按质完成每一阶段的工作任务。

涉及与用户协调导致工期延误的，及时提出风险并提出补救措施。

因不可抗拒因素导致延缓的，提供相关文件说明。预计工期将延时，提早报告用户，并提出补救措施。

8.2.2. 质量控制

针对用户安全服务建设项目，我们针对各阶段设置以下审查控制点:

- 对支撑平台设备安装阶段：
  1. 托管运营平台是否按照预期目标正常运营，包括平台运行状态及数据接入情况；
  2. 是否满足产品部署及网络接入规范；
  3. 初始配置是否完善。
- 试运行阶段
  1. 整体网络构架是否满足设计要求；
  2. 安全基线是否满足要求；
  3. 网络连接是否满足要求；
  4. 事件处置流程是否满足要求。
- 持续运营阶段
  1. 服务 SLA 是否达到标准要求；
  2. 日常沟通是否畅通；
  3. 工作职责是否按要求完成。

8.2.3. 沟通策略

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。

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。

8.2.4. 文档管理

项目文档的编写和管理是项目管理的一个重要部分。在项目实施各个时期，项目小组将会组织编写规范的项目技术文档。在项目通过验收后，我方将全部文档移交给您。

9. 数据隐私保护

服务开始前，我们将为您签订保密协议，在法律上明确服务过程中所涉服务人员要承担的责任，确保如果发现项目实施过程中，服务人员有信息泄露、出售及攻击行为后，可以依据保密协议追究法律责任，并尽可能将损失降到最小。

针对与授权合作伙伴共享信息的情况，我们仅会根据合法、正当、必要的原则，基于特定、明确的目的与授权合作伙伴共享您的信息，仅会共享提供服务所必要的信息。对于我们与之共享信息的第三方，我们会在完成并通过针对第三方的信息安全风险评估后，与其签署必要的保密协定，要求他们严格遵守相关法律法规与监管要求，遵照隐私政策采取保密和安全措施来处理个人信息，未经您的授权严禁用于营销活动或其他处理活动。