托管检测与响应服务（原生版）

用户使用指南

天翼云科技有限公司

目录

1. 背景介绍

1.1. 背景概述

1.1.1. 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。

1.1.2. 建设必要性和功效

1.1.2.1. 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。

1.1.2.2. 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。

1.1.3. 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。

1.2. 安全现状分析

1.2.1. 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。

1.2.2. 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。

1.2.3. 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。

1.3. 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。

1.4. 安全托管建设方法设计

1.4.1. 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》

1.4.2. 国内外安全体系

1.4.2.1. IATF 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 - 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。

1.4.2.2. 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。

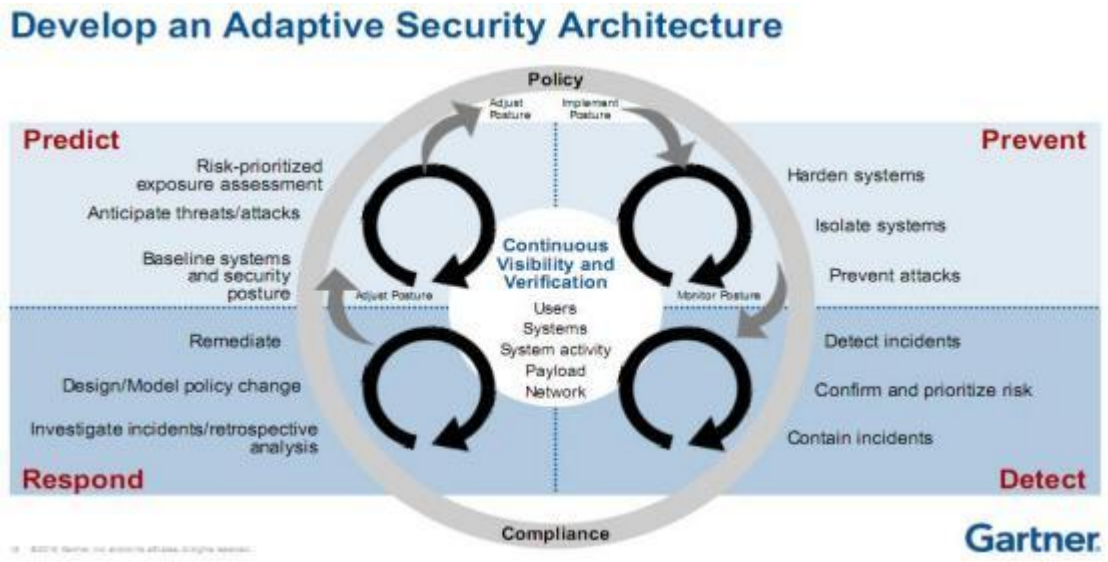


图 -ASA 自适应安全框架

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。

1.4.2.3. 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 - 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

1.4.3. 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。

2. 产品介绍

2.1. 产品定义

托管检测与响应服务（原生版）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，同时，结合安全评估、应急响应等其他可选服务，为用户构建一体化安全防护运营能力。

基础版

为中小型客户提供远程交付的基础安全运营能力，通过汇聚云上安全数据，7*24小时监测分析云防火墙、EDR等安全产品告警日志和安全事件，监控用户资产安全状况，安全事件及时告知客户并可联动安全产品处置。创新提供产品售后服务专属管家，5*8值守响应产品售后问题。

企业版

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。

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。

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。

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。

全流量分析服务

全流量分析服务通过对已接入托管检测与响应服务的云主机流量进行全面分析，人工验证病毒木马、APT攻击等安全事件，分析研判事件真实性，发现隐藏威胁，综合资产属性，制定有效的加固策略，提高托管服务价值。

2.2. 产品优势

100%处置闭环率

自动处置能力联动全网威胁情报，实时处置高级威胁，结合云端专家处置升级策略，保证重大事件处置闭环率100%。

持续安全保障

提供N × 24小时的安全保障，持续对云上资产进行告警分析、安全事件监测、漏洞情报捕获。

快速响应及时止损

第一时间介入安全事件发生的环境，对安全事件进行处置，避免类似情况再次发生，防止数据遭受泄露造成经济损失。

标准化服务内容

依托顶尖服务团队及行业标准，提供标准化服务流程和交付内容，保证服务质量。

2.3. 功能特性

7*24小时威胁检测与响应

全天候提供威胁检测与响应，通过汇聚云上安全产品数据，集中检测分析，及时发现威胁，快速处置。

SOAR自动处置

通过编排处置能力，秒级响应安全事件，并通过剧本库，持久化安全场景。

高级别威胁感知

通过集成漏洞库、威胁情报，实时感知高危漏洞开放及国内外APT攻击。

护航保障

提供护航保障服务，解决重要时期网络安全保障需求。

2.4. 应用场景

日常安全运营支撑

监控用户资产安全状况，发现各类安全威胁进行及时响应；提供产品咨询、技术支持、产品联动处置问题支持、产品故障/BUG解决等服务。

安全运营托管场景

基于丰富的云安全运营经验积累，面向云环境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，集威胁分析、攻击面梳理、漏洞管理、应急响应等功能于一体，为用户及时发现、有效分析、闭环处理安全问题，有效防护威胁，降低用户运营成本，为用户资产提供持续有效的安全保障。

关键时期重保场景

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。包括：监测分析、应急处置、攻击反制、设备布防、漏洞加固、基线评估、弱口令评估、敏感信息评估、安全意识培训、蜜罐运营等。

应急响应场景

针对网络安全事件进行应急处置，保证相关业务的连续性和可用性，同时将攻击带来的破坏程度降到最低。在客户已知或怀疑系统被攻击的情况下，可委托我方工程师对系统进行排查和处置。

风险评估场景

通过真实模拟攻击使用的工具、分析方法来对业务系统进行深度漏洞挖掘，利用系统漏洞获取权限从而获取敏感数据的测试，由测试人员进行深入的手工测试和分析，识别工具无法发现的问题。

2.5. 术语解释

基线核查

基线核查是指对主机操作系统、数据库、软件和容器的配置进行安全检测，并提供检测结果说明和加固建议。基线核查可以帮您进行系统安全加固，降低入侵风险并满足安全合规要求。

漏洞预警

为用户提供漏洞预警服务，第一时间向用户发布高危漏洞预警信息，向用户通告漏洞的危害程度、影响范围、检测方法、及相关解决方案，便于用户及时掌握高风险级别漏洞信息，应对外部威胁；通过多个信息安全专栏向用户分享最近出现的网络安全攻击事件、境外黑客组织攻击行为、软硬件漏洞技术、病毒或恶意代码等有害程序事件和技术原理分析、安全技术研究报告，安全新闻或事件动态。

资产发现与管理

基于用户原有资产台账，通过主动上报、内外部扫描、网络流量分析等方式对资产进行识别归类，在服务过程中持续完善资产信息，并周期性稽查更新。服务专家对服务范围内资产进行精细化管理，通过工具和人工相结合的方式，与用户配合补充资产信息，包括IP地址、端口、资产类型、操作系统类型、数据库类型、中间件类型在内的各项属性。

安全监控

基于已部署的平台系统对用户主机、Web系统、域名等资产的告警事件进行实时监测分析，对告警信息进行分析研判，并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，通过企业微信、钉钉等方式告知用户。

应急响应

在接到用户应急响应请求后，由应急专家小组根据事件类别进行研判，通过远程或现场的方式协助用户对遇到的突发性安全事件进行紧急分析和处理。主要工作内容包括但不

限于：突发事件信息收集、事件分析、分析报告提交、问题解决建议等在发生安全事件时协助业务恢复到正常服务状态，调查安全事件发生的原因，避免同类安全事件再次发生。

威胁分析溯源

安全运营专家团队利用安全编排、自动化及响应与大数据分析技术，在海量安全告警中对各类疑似安全事件的告警进行分析研判，进一步发现真实的安全事件，通过具备多年丰富经验的运营专家团队对安全事件进行深度分析、溯源，为用户判断整体威胁趋势，提供解决方案并协助用户及时进行处置。

攻击路径还原

在接到用户应急请求后，应急响应服务团队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。

蠕虫及后门清理

基于对事件场景的探测和发现，应急响应服务团队将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，涉及工具由服务人员自备，用户对工具进行评价后接入用户环境。

攻击者画像

应急响应服务团队通过对木马文件、安全日志及攻击痕迹等信息进行分析，对攻击行为信息进行关联分析，对攻击的虚拟身份进行模拟画像，在数据量充足的情况下定位攻击者的真实身份。

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。

2.6. 使用限制

全流量分析服务使用限制

需订购企业版或护航版后，才能使用全流量分析服务。

3.计费说明

3.1. 计费模式

本产品按照服务的类型、人员数、服务周期及服务资产数进行收费。

购买基础版、企业版前，应至少已订购主机安全、WAF、云防火墙安全产品。

服务项	细分项	资产数	单位	价格	应用场景	备注
基础版	基础版接入服务	-	元/年	40800	基础费用，包含服务接入、资源配置等	-
	基础版资产	1	元/台/年	720	单个资产托管费用	-
企业版	托管基础服务	-	元/年	60000	基础费用，包含服务接入、资源配置等	企业版包含托管资产的应急响应服务，新购一年赠送一次资产威胁分析服务。
	托管资产	1	元/台/年	1800	单个资产托管费用	
护航版	前期评估	1-50	元/天	10000	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	最低5天
	重保服务	1-50	元/天	12000	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	-
	防护资产扩展包	50	元/天/个	8000	扩展重保服务监控资产数量	每新增1个资产扩展包，安全检查最低天数增加1天
	蓝军攻击服务（3人*5天）	-	元/次	450000	提供3人*5天的蓝军攻击服务，提供攻击报告	-
应急响应服务	应急响应服务	1-20	元/次	50000	提供远程应急响应服务，受影响范围为1-20个资产	-
		21-100	元/次	100000	提供远程应急响应服务，受影响范	-

服务项	细分项	资产数	单位	价格	应用场景	备注
					围为21-100个资产	
		101-200	元/次	180000	提供远程应急响应服务，受影响范围为101-200个资产	-
		201-500	元/次	260000	提供远程应急响应服务，受影响范围为201-500个资产	-
安全评估	安全评估服务	-	元/次	30000	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	-
全流量分析服务	--	--	元/月	3500	单个规格支持网络层吞吐量500Mbps，应用层吞吐量≤250Mbps，可按需叠加。	-
			元/年	35000		

3.2. 升级扩容

购买了托管检测与响应服务（原生版）的基础版、企业版、全流量分析服务后，支持根据实际使用需求新增服务规格。

- 升级基础版托管资产数
- 升级企业版托管资产数
- 升级全流量分析服务规格

3.3. 续费

托管检测与响应服务（原生版）的基础版、企业版、全流量分析服务支持续费。

续订周期

- 基础版：可按月或按年续费。
- 企业版：仅支持按年续费。
- 全流量分析服务：可按月或按年续费。

续订步骤

- 续订基础版

- 续订企业版
- 续订全流量分析服务

3.4. 到期

基础版/企业版

根据订购时长提供服务，服务到期后，立即停止基础版/企业版服务，对使用过程中的安全数据进行清除。

护航版

护航版服务订购的有效期为1年，按照用户购买天数进行交付，交付完成或未交付但购买时长超过一年，则服务到期，到期仍未使用不退款。

应急响应

应急响应服务订购的有效期为1年，交付完或未交付但购买时长超过一年，则服务到期，到期仍未使用不退款。

安全评估

安全评估服务订购的有效期为1年，交付完或未交付但购买时长超过一年，则安全评估服务到期，到期仍未使用不退款。

全流量分析服务

根据订购时长提供服务，服务到期后，立即停止全流量分析服务。

3.5. 退订

本产品不支持退订。

4. 快速入门

4.1. 服务内容一览表

服务项	模式	服务项细分	服务内容

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
应急响应	远程	应急响应服务	提供远程应急响应服务

4.2. 基础版/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、	《项目启动会PPT》

服务阶段	实施任务	服务内容	交付物
		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	
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	《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	《威胁情报》

服务阶段	实施任务	服务内容	交付物
		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	
	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》

4.3. 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
购买阶段	购买护航版服务	按照购买指引，选择自身需要的服务内容及配置，并完成购买支付	-
	发起护航版服务需求	发起护航版服务需求	
准备阶段	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》
	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	渗透测试	通过模拟黑客攻击的方式，对网站或在线平	《漏洞扫描报告》

服务阶段	实施任务	实施内容	交付物
阶段		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	《基线核查报告》 《渗透测试报告》
	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	
	漏洞扫描	通过扫描工具对目标业务资产进行漏洞扫描	
	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	安全检测	通过远程值守的方式，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，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
	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

4.4. 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
购买阶段	购买应急响应服务	按照购买指引，选择自身需要的服务内容及配置，并完成购买支付	-
	发起应急响应服务需求	发起应急响应服务需求	
准备阶段	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	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》
	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	
	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	
	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	
	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	

4.5. 安全评估服务交付内容及流程

托管检测与响应服务团队通过安全评估服务，对用户托管服务范围内的资产安全状况进行整体评估，扫描分析资产脆弱性。

服务阶段	实施任务	实施内容	交付物
购买阶段	购买安全评估服务	请您根据实际需求及服务团队沟通建议购买安全评估服务	-

服务阶段	实施任务	实施内容	交付物
	发起安全评估服务需求	在控制台创建安全评估服务需求	
准备阶段	确定评估范围、评估人员、评估工具及计划	确定安全评估范围，评估人员及评估工具，制定评估计划，按照计划时间开展评估工作	-
评估阶段	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	《业务资产安全漏洞清单》
	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》	《业务资产脆弱性问题清单》
验收阶段	验收	汇总漏洞及业务脆弱性问题，提交安全评估服务报告	《安全评估服务报告》

4.6. 全流量分析服务接入流程

托管检测与响应服务团队通过全流量分析服务，对接入托管检测与响应服务的云主机流量进行全面分析，发现病毒木马、APT攻击等。

服务阶段	**实施内容**

服务阶段	实施内容
购买阶段	请您根据实际需求及服务团队沟通建议购买全流量分析服务。
准备阶段	明确需创建的虚拟机规格，是否需要对接终端引流插件。
部署阶段	上传私有镜像、创建全流量虚拟机、完成授权，全流量对接及外发策略配置。

5. 用户指南

5.1. 基础版

5.1.1. 购买基础版

购买须知

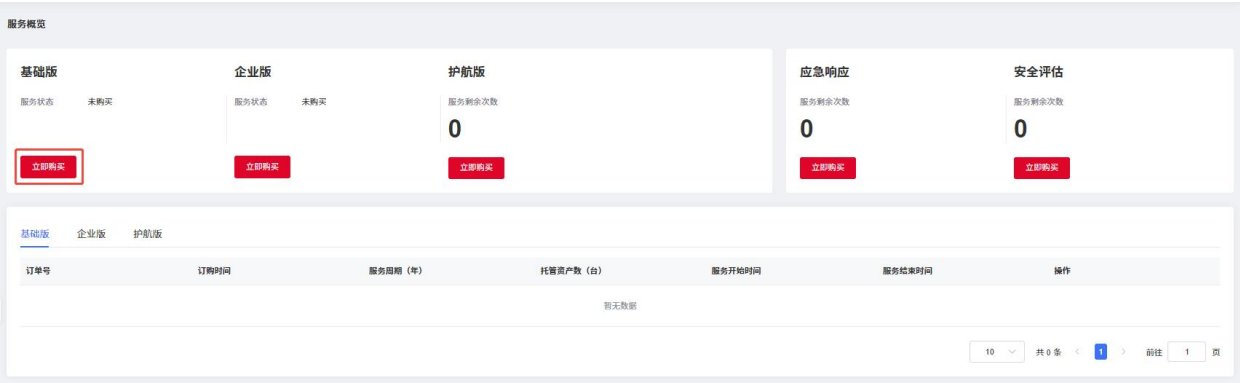
- 基础版提供安全托管服务，当前针对开通云等保专区、安全专区及托管服务组件的用户提供，请您提前配置相关安全产品。
- 购买服务后，我们的安全服务工程师将会联系您，并在整个服务周期内与您保持沟通。
- 一个账号仅支持购买一个基础版实例。

服务内容

- 持续监控安全产品（WAF、云防火墙、主机安全）事件。
- 提供漏洞感知，监控云主机、应用、服务脆弱性。
- 提供威胁情报，持续检测恶意IP、恶意域名、APT攻击等。
- 提供安全产品策略检查和调优，确保检测和防护效果。
- 提供安全产品售后管家，专人快速解决问题。
- 不支持退订操作。

操作步骤

1. 登录托管检测与响应服务（原生版）控制台。
2. 点击基础版“立即购买”按钮，跳转到基础版订购页面。



3. 在“产品配置”模块配置“托管云主机数”，根据客户需要托管的云主机台数，选择对应的数量。

4. 确认配置信息无误后，阅读并接受相关服务协议、服务等级协议，单击右下角“立即购买”，跳转到支付页面。
5. 在“支付”页面，请选择付款方式进行付款。
6. 付款成功后，返回托管检测与响应服务（原生版）控制台，查看订购状态。
7. 订购完成后，24小时内，我们的服务经理会与您联系。

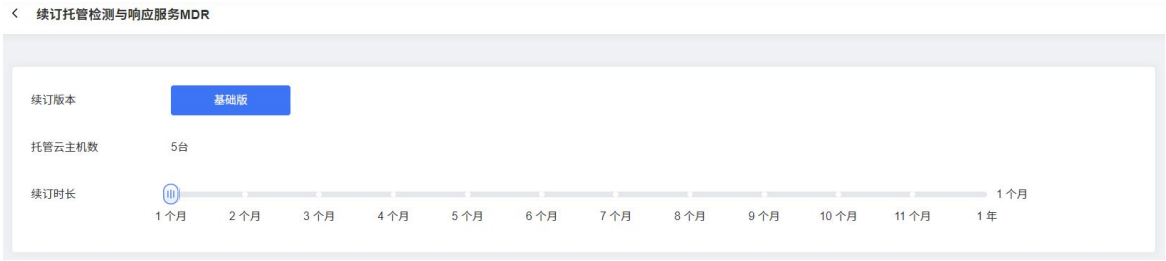
5.1.2. 续订基础版

基础版服务可按月或按年续费。

续订步骤

1. 登录托管检测与响应服务（原生版）控制台。
2. 点击基础版服务列表内的“续订”按钮，跳转到基础版续订界面。

3. 在基础版续订页面，选择“续订时长”，点击“立即购买“按钮，跳转到支付页面。



4. 在“支付”页面，请选择付款方式进行付款。

5. 付款成功后，返回产品控制台，查看续订结果。

5.1.3. 升级基础版托管资产数

基础版支持升级托管资产数，在服务概览界面，点击升级进入基础版升级页面进行托管资产数升级，用户可在【升级内容】模块根据自身需求选择要增加的资产数。然后点击立即购买并支付。

操作步骤

1. 登录托管检测与响应服务（原生版）控制台。

2. 点击基础版服务列表内的“升级”按钮，跳转到基础版升级界面。

3. 在基础版升级页面，输入“扩展托管云主机”数量，并点击“立即购买“按钮，跳转到支付页面。

4. 在“支付”页面，请选择付款方式进行付款。

5. 付款成功后，返回产品控制台，查看扩展结果。

5.2. 企业版

5.2.1. 购买企业版

购买须知

- 企业版提供安全托管服务，当前针对开通云等保专区、安全专区及托管服务组件的用户提供，请您提前配置相关安全产品。
- 购买服务后，我们的安全服务工程师将会联系您，并在整个服务周期内与您保持沟通。
- 一个账号仅支持购买一个企业版实例。

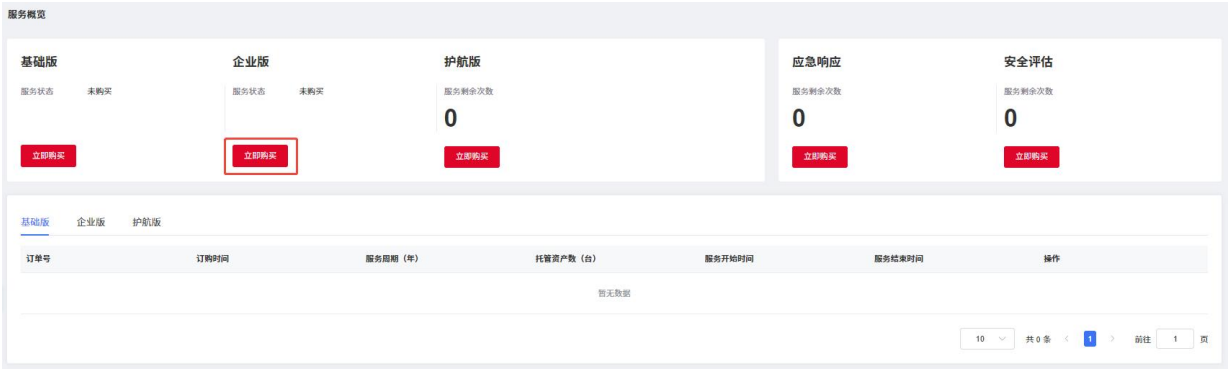
服务内容

- 持续监控安全产品（WAF、云防火墙、主机安全）事件。
- 提供漏洞感知，监控云主机、应用、服务脆弱性。
- 提供威胁情报，持续检测恶意IP、恶意域名、APT攻击等。
- 提供应急响应支撑，应对突发安全事件。
- 提供安全评估，评估云上资产整体安全状况，提供评估报告。
- 不支持退订操作。

操作步骤

1. 登录托管检测与响应服务（原生版）控制台。

2. 点击企业版“立即购买”按钮，跳转到企业版订购页面。



3. 在“产品配置”模块配置“托管云主机数”，根据客户需要托管的云主机台数，选择对应的数量。

4. 确认配置信息无误后，阅读并接受相关服务协议、服务等级协议，单击右下角“立即购买”，跳转到支付页面。
5. 在“支付”页面，请选择付款方式进行付款。
6. 付款成功后，返回托管检测与响应服务（原生版）控制台，查看订购状态。
7. 订购完成后，24小时内，我们的服务经理会与您联系。

5.2.2. 续订企业版

企业版仅支持按1年期续费。

操作步骤

1. 登录托管检测与响应服务（原生版）控制台。
2. 点击企业版服务列表内的“续订”按钮，跳转到企业版续订界面。

3. 在企业版续订页面，点击“立即购买“按钮，跳转到支付页面。

4. 在“支付”页面，请选择付款方式进行付款。

5. 付款成功后，返回产品控制台，查看续订结果。

5.2.3. 升级企业版托管资产数

购买了托管检测与响应服务（原生版）的基础版、企业版、全流量分析服务后，支持根据实际使用需求新增服务规格。

操作步骤

1. 登录托管检测与响应服务（原生版）控制台。

2. 点击企业版服务列表内的“升级”按钮，跳转到企业版升级界面。

3. 在企业版升级页面，输入“扩展托管云主机”，并点击“立即购买“按钮，跳转到支付页面。

4. 在“支付”页面，请选择付款方式进行付款。
5. 付款成功后，返回产品控制台，查看扩展结果。
6. 订购完成后，24小时内，我们的服务经理会与您取的联系。

5.3. 护航版

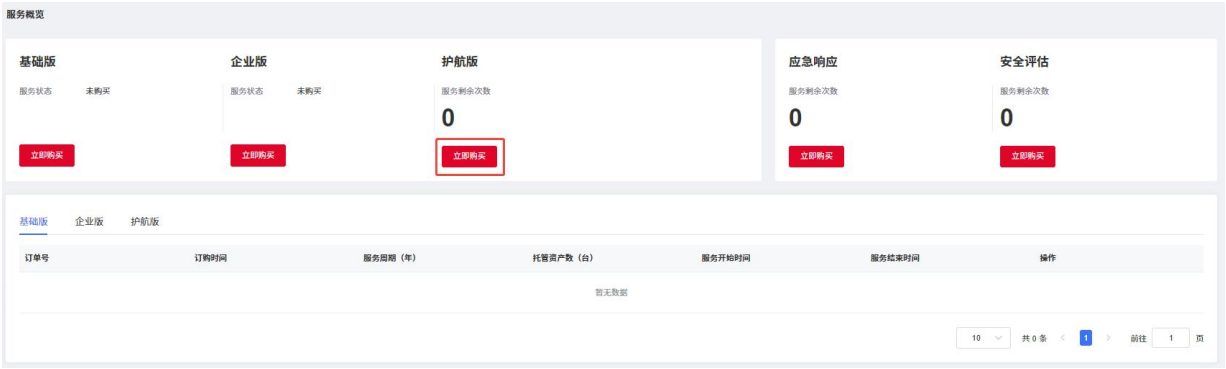
5.3.1. 购买护航版

服务内容

- 提供定制化护航保障方案。
- 提供安全检查，包括安全产品策略、资产基线配置、协助开展安全加固。
- 持续监控云上安全状态，提供护航日报。
- 提供应急响应服务。
- 提供关键业务渗透测试服务。
- 提供7*24小时云端专家团队值守。
- 服务1年内有效，订购后不支持退订。

操作步骤

1. 登录托管检测与响应服务（原生版）控制台。
2. 点击护航版“立即购买”按钮，跳转到护航版购买页面。



3. 在护航版服务购买详情页面，【产品配置】栏，按需求选择护航前安全检查、护航时长、防护资产扩展包、蓝军攻击服务。

- 护航前安全检查： 必选项，单位为天，最低选购时长为5天，每增加50个资产需要增加一天服务时长。
- 护航时长： 必选项，单位为天，最低选购时长为1天，用户可根据实际护航天数选购护航时长。
- 防护资产扩展包： 可选项，单位为个，每超过50个资产，需要购买一个扩展包，用户根据防护资产数量选择对应扩展包数量。
- 蓝军攻击服务： 可选项，单位为次，每次提供3人*5天蓝军攻击服务，用户根据自身需求选购次数。

4. 确认配置信息无误后，阅读并接受相关服务协议、服务等级协议，单击右下角“立即购买”，跳转到支付页面。

5. 在“支付”页面，请选择付款方式进行付款。

6. 付款成功后，返回托管检测与响应服务（原生版）控制台，查看订购状态。

7. 订购完成后，24小时内，我们的服务经理会与您联系。

5.3.2. 获取护航版服务序列号

操作场景

服务序列号用于唯一标识本次服务，安全服务经理在服务过程中，会向您索要服务序列号，用于标识本次服务已进入服务阶段。

前提条件

已订购护航版服务。

操作步骤

在服务概览页面，可查看订购记录，可以生成并查看服务序列号。

1. 登录托管检测与响应服务（原生版）控制台。

2. 在左侧导航栏，选择“服务概览”，进入服务概览页面。

3. 选择“护航版”页签，找到目标订单，点击“生成”按钮，可生成服务序列号。

4. 单击“服务序列号”列的“复制”，即可复制已生成的服务序列号。

5.4. 应急响应

5.4.1. 购买应急响应服务

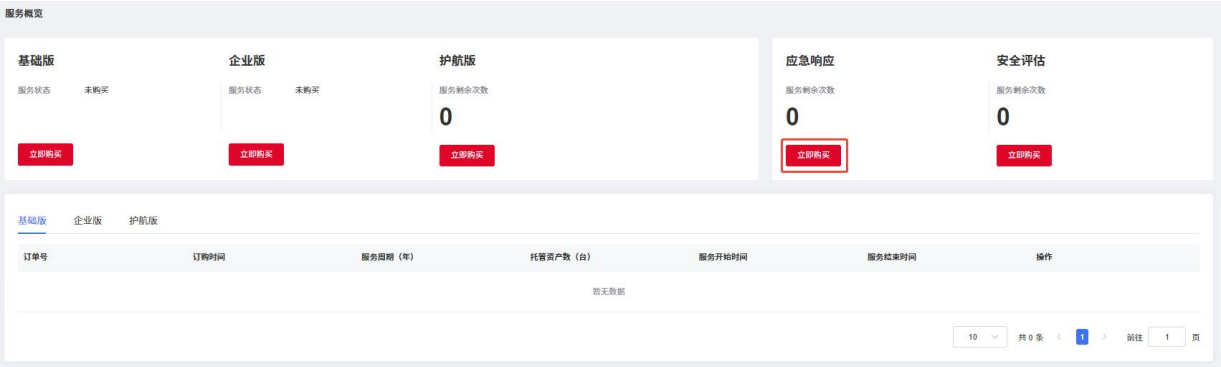
服务内容

- 提供远程应急响应服务。
- 提供攻击路径还原、蠕虫及后门清理、攻击者画像、安全漏洞附件等。
- 服务包含5个可选规格：1-20，21-100，101-200，201-500，超过500请联系客户服务人员。

- 提供应急响应报告。
- 服务有效期最长不超过1年，应急响应服务不支持退订。

操作步骤

1. 登录托管检测与响应服务（原生版）控制台。
2. 点击应急响应“立即购买”按钮，跳转到应急响应订购页面。



3. 在应急响应服务购买详情页面，【产品配置】栏，按需要保护的资产数量选择服务规格，并选择预计服务交付时间。此服务为单次交付，最长时效期为一年。配置完成点击立即购买并支付。

4. 在“支付”页面，请选择付款方式进行付款。
5. 付款成功后，返回产品控制台，查看订购状态。
6. 订购完成后，24小时内，我们的服务经理会与您联系。

5.4.2. 获取应急响应服务序列号

操作场景

服务序列号用于唯一标识本次应急响应服务，安全服务经理在服务过程中，会向您索要服务序列号，用于标识本次服务已进入服务阶段。

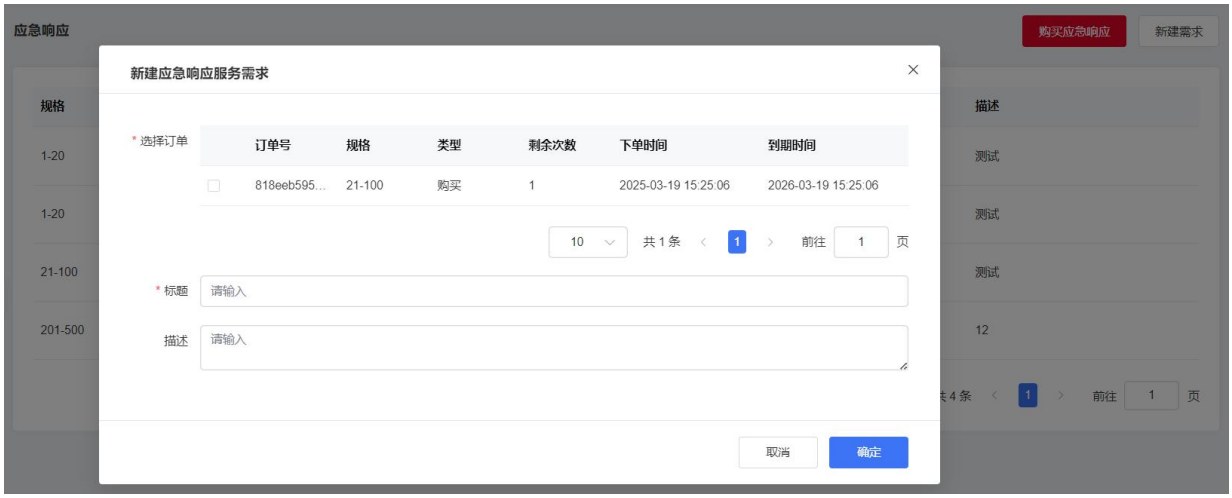
前提条件

已订购应急响应服务。

操作步骤

在应急响应页面，可查看订购记录，可通过新建需求获取服务序列号。

1. 登录托管检测与响应服务（原生版）控制台。
2. 在左侧导航栏，选择“应急响应”，进入应急响应页面。
3. 找到目标规格订单，点击页面右上角的“新建需求”，弹出新建应急响应服务需求对话框。



4. 配置服务需求相关参数。
   - **选择订单**：本次应急响应需求关联的服务订单，应急响应具有多个规格，每个订单规格所含服务资产数不同，请您根据实际需要选择服务规格。
   - **标题**：本次应急响应服务主要目的。
   - **描述**：本次应急响应服务详细内容。
5. 配置完成后，单击“确定”，即可返回服务需求列表，查看服务序列号。
5. 单击“服务序列号”列的“复制”，即可复制已生成的服务序列号。

5.5. 安全评估

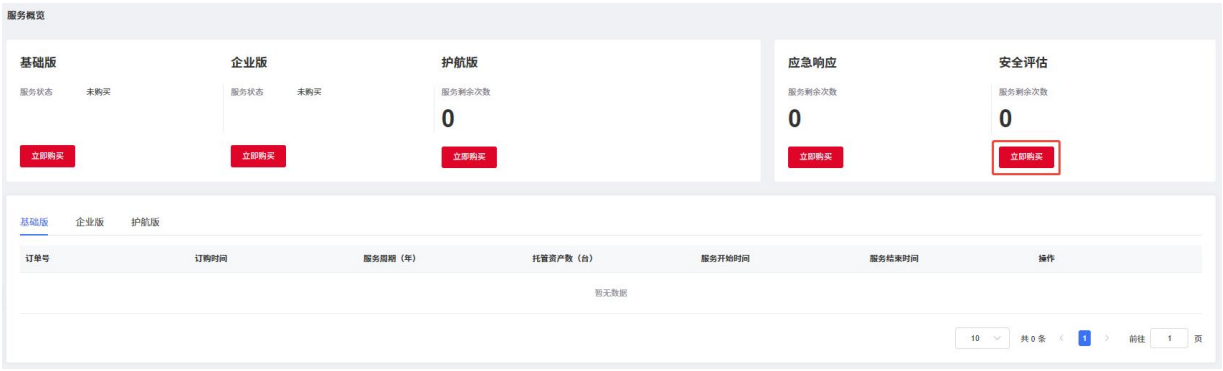
5.5.1. 购买安全评估

服务内容

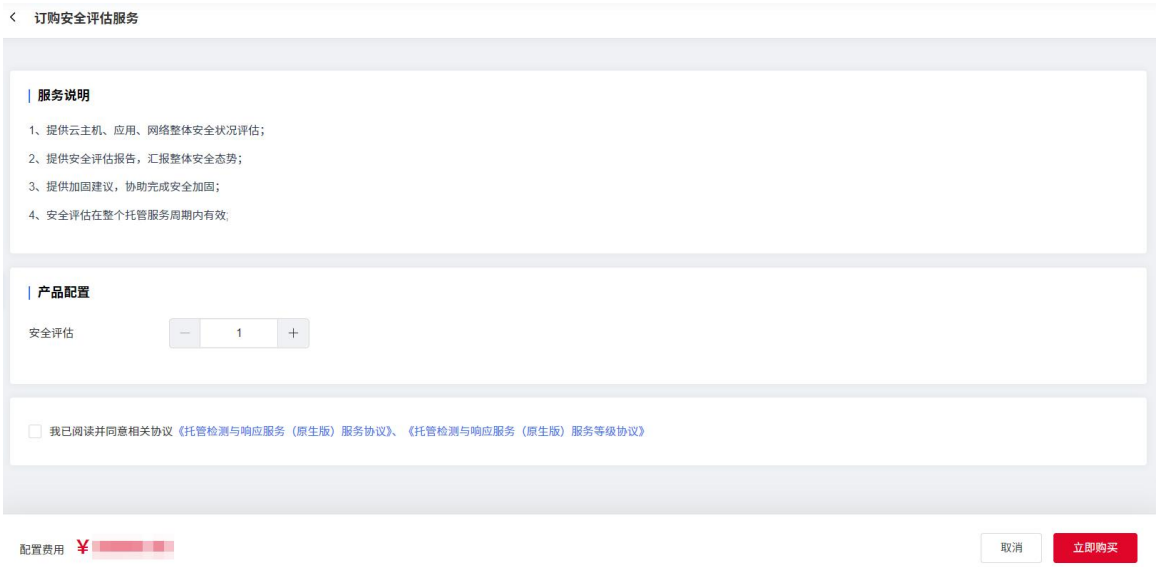
- 提供云主机、应用、网络整体安全状况评估。
- 提供安全评估报告，汇报整体安全态势。
- 提供加固建议，协助完成安全加固。
- 安全评估在整个托管服务周期内有效。

操作步骤

1. 登录托管检测与响应服务（原生版）控制台。
2. 点击安全评估“立即购买”按钮，跳转到安全评估订购页面。



3. 您可根据自身需求在【产品配置】栏选择评估次数，选择立即购买并支付。



4. 在“支付”页面，请选择付款方式进行付款。

5. 付款成功后，返回托管检测与响应服务（原生版）控制台，查看订购状态。

6. 订购完成后，24小时内，我们的服务经理会与您联系。

5.5.2. 获取安全评估服务序列号

操作场景

服务序列号用于唯一标识本次安全评估服务，安全服务经理在服务过程中，会向您索要服务序列号，用于标识本次服务已进入服务阶段。

前提条件

已订购安全评估服务。

操作步骤

在安全评估页面，可查看订购记录，可通过新建需求获取服务序列号。

1. 登录托管检测与响应服务（原生版）控制台。

2. 在左侧导航栏，选择“安全评估”，进入安全评估页面。

3. 点击页面右上角的“新建需求”，弹出新建安全评估需求对话框。

4. 配置服务需求相关参数。

   - 服务可用次数：代表您当前可用的安全评估服务总次数。
   - 标题：记录本次服务主要目的。
   - 描述：记录本次服务详细内容。

5. 配置完成后，单击“确定”按钮，即可返回服务需求列表，查看服务序列号。

6. 单击“服务序列号”列的“复制”，即可复制已生成的服务序列号。

5.6. 全流量分析服务

5.6.1. 购买全流量分析服务

购买须知

您需要提供单独的具备互联网访问权限的云主机，用于部署全流量分析服务探针；本服务需要在您的业务云主机上部署代理，用于分析主机网卡流量。

操作步骤

1. 登录托管检测与响应服务（原生版）控制台。
2. 在左侧导航栏，选择“全流量分析服务”，进入全流量分析服务页面。
3. 点击“立即购买”，进入全流量分析服务订购页面。
4. 在“产品配置”模块配置“订购规格数量”。

   单个规格支持500Mbps网络层吞吐量授权，250Mbps应用层吞吐量授权。

5. 配置订购时长。支持购买1个月~1年。

6. 确认配置信息无误后，阅读并接受相关服务协议、服务等级协议，单击右下角“立即购买”，跳转到支付页面。
7. 在“支付”页面，请选择付款方式进行付款。

8. 付款成功后，返回托管检测与响应服务（原生版）控制台，查看订购状态。

9. 订购完成后，24小时内，我们的服务经理会与您联系。

5.6.2. 续订全流量分析服务

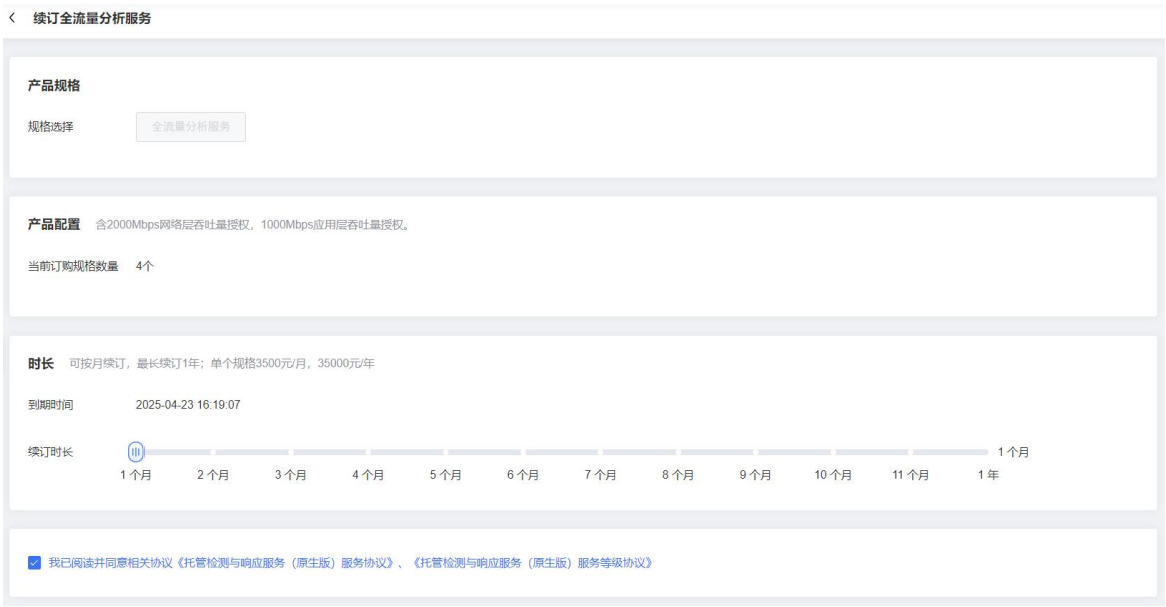
全流量分析服务根据订购时长提供服务，服务到期后，立即停止全流量分析服务。建议在服务到期前为服务手动续费。

续订步骤

1. 登录托管检测与响应服务（原生版）控制台。

2. 在左侧导航栏选择“全流量分析服务”，点击服务列表操作列的“续订”按钮，跳转到续订界面。

3. 在续订页面，选择续订的时长。可按月续订，最长支持续订1年。



4. 点击“立即购买“按钮，跳转到支付页面。

5. 在“支付”页面，请选择付款方式进行付款。

6. 付款成功后，返回产品控制台，查看续订结果。

5.6.3. 升级全流量分析服务规格

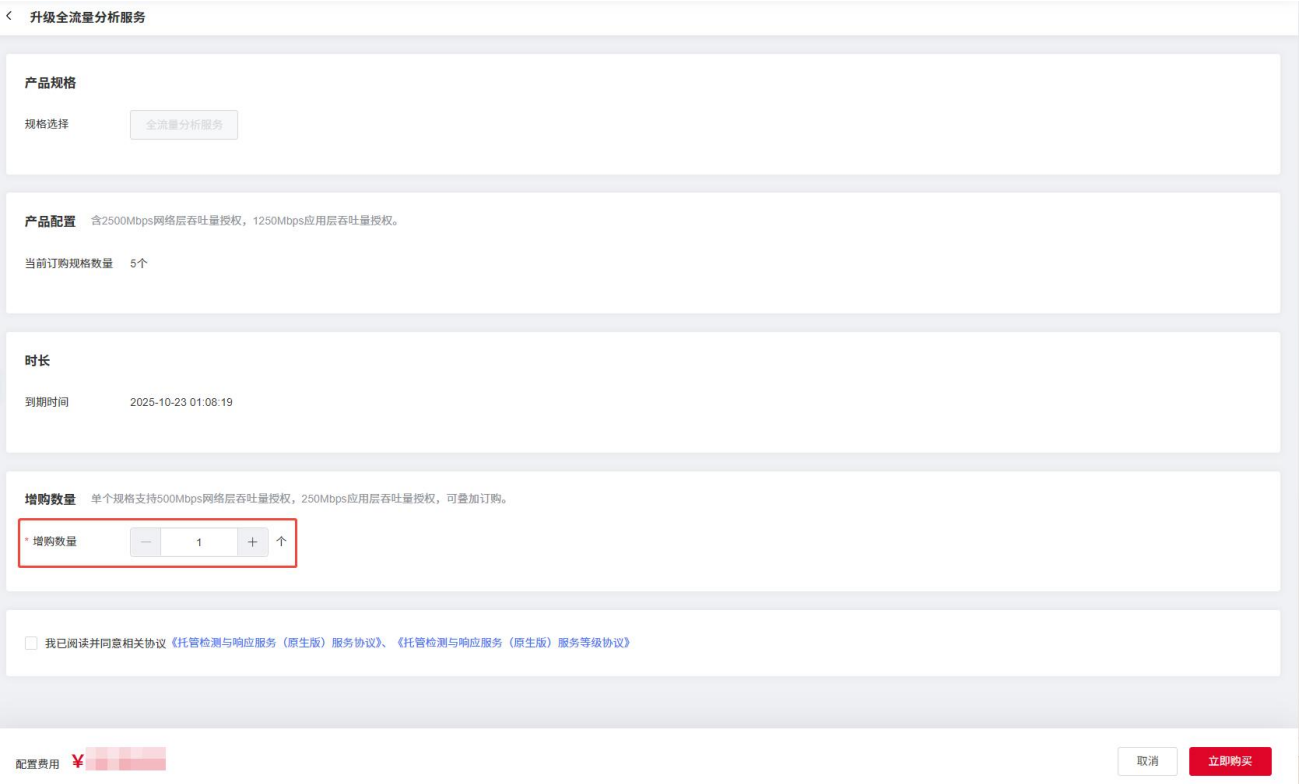
购买全流量分析服务后，若需要扩容规格，可执行升级操作，增加规格数量。

操作步骤

1. 登录托管检测与响应服务（原生版）控制台。
2. 在左侧导航栏，选择“全流量分析服务”，点击服务列表操作列的“升级”按钮，跳转到升级界面。

3. 在升级页面，选择需要增加的规格数量。

单个规格支持500Mbps网络层吞吐量授权，250Mbps应用层吞吐量授权。



4. 在“产品配置”模块配置“订购规格数量”。确认配置信息无误后，阅读并接受相关服务协议、服务等级协议，单击右下角“立即购买”，跳转到支付页面。
5. 在“支付”页面，请选择付款方式进行付款。

6. 常见问题

6.1. 产品类

托管检测与响应服务是什么？

MDR，Managed Detection and Response Service，也称为安全检测与响应服务，在云计算中，安全托管检测与响应服务（MDR）是指用户外包给云提供商的网络安全服务。根据最近的行业研究，大多数组织（74%）有内部管理IT安全，但82%的IT专业人员表示他们已经与托管安全服务提供商建立了伙伴关系，或计划与之合作。企业转向安全托管检测与响应服务提供商可以减轻他们每天面临的与信息安全有关的压力，例如针对性云安全攻击事件，云安全运营经验不足，客户数据窃取，技能短缺和资源限制。

托管检测与响应服务能提供哪些能力？

- 借助于用户在公有云多种环境中的网络安全设备与系统的日志数据和托管检测与响应服务平台能力，实现对用户在公有云中的网络安全运营工作的托管运营，减轻用户安全运营负担，提升用户公有云中业务系统的网络安全风险事件的响应与处置能力。
- 针对公有云提供丰富的网络安全运营服务，包括安全咨询、安全运营到应急响应等服务，充分满足用户在公有云上的合规与安全运营需求。
- 提供从云端EDR、合规处置工具到集成了SOAR能力的云端托管安全运营服务平台，满足公有云环境中的安全产品使用需求。
- 基于云上安全服务的最佳配置实践，为用户提供全面的安全评估服务，提供安全加固建议，并协助用户完成加固操作。

托管检测与响应服务主要分析哪些安全事件？

托管检测与响应服务主要分析以下事件：

- 安全产品的事件，例如主机安全、WAF、防火墙等安全产品的告警信息。

- 最新安全漏洞事件，依托主机安全、漏洞扫描等产品，监控用户资产漏洞开放情况，及时上报并提供处置意见。
- 数据泄露事件，依托数据库审计等数据安全产品，监控数据泄露事件，溯源分析威胁来源。

请注意，托管检测与响应服务依赖已部署的安全产品情况，具体服务内容，请以最终服务团队确认为准。

托管检测与响应服务是否需要购买或部署相关产品或组件？

由于托管服务中的安全监控服务涉及到对用户业务环境中的安全告警及攻击事件进行分析，因此需要用户具备基础安全检测和防护产品（如主机安全、云防火墙）获取安全事件，进而对事件进行深度分析，并提供基于云的可落地解决建议。

当前版本仅支持向订购了云等保专区产品的用户提供服务。

企业版服务怎么计费的？

托管检测与响应服务计费方式如下：

采用预付费的模式进行购买，支持按年的计费模式，即自用户购买当日起，享受购买期限内的服务，当购买的服务到期后，服务自动停止。

此外，您可以按年续订，同时支持扩展托管资产数量，当前仅支持向上扩容，暂不支持减少托管资产数。

托管检测与响应服务（原生版）提供几种服务项目？

托管检测与响应服务（原生版）提供：

- 基础版：为中小型客户提供远程交付的基础安全运营能力。
- 企业版：满足安全托管服务需求，解决日常安全运营人力不足、缺少标准流程的问题。
- 护航版：满足重要时期安全保障需求，护航版含蓝军攻击服务。
- 应急响应：满足突发安全事件时的应急处置需求，快速止损，威胁溯源。

- 安全评估：帮助您了解整体安全状况。
- 全流量分析服务：为用户提供更加强大的安全监控服务能力，全面检测主机流量，发现病毒木马、APT攻击等，提高托管服务价值。

护航版的有效期是多长？

从您成功购买托管检测与响应服务（原生版）护航版起计算，1年内您可以随时发起服务需求。我们的服务团队也会主动联系您，确认服务内容及服务时间。

请您务必在有效期内使用，到期以后，需重新购买本服务。

应急响应的有效期是多长？

从您成功购买托管检测与响应服务（原生版）应急响应起计算，1年内您可以随时发起服务需求。建议您提前购买应急服务，我们会指派专门的服务经理与您保持联系，第一时间响应，快速开展服务。

请您务必在有效期内使用，到期以后，需重新购买。

安全评估的有效期是多长？

安全评估服务订购的有效期为1年，交付完或未交付但购买时长超过一年，则安全评估服务到期，到期仍未使用不退款。您可以订购多次安全评估服务，满足季度、年度汇报需求。

请您务必在有效期内使用，到期以后，需重新购买。

如何获取服务报告？

您订购托管检测与响应服务（原生版）后，会有服务经理与您取得联系，在完成服务后，服务经理会将服务报告通过沟通约定的形式交付给您。

我们推荐以邮件的方式交付给您。如果对报告有其他要求，请您提前与服务经理沟通。

6.2. 购买类

服务购买后，有相应的操作指导吗？

服务购买后，我们将指派服务经理与您取得联系，沟通具体服务开展流程并指导您相关操作步骤。此外，您可以参考快速入门的服务接入流程。

服务购买后，有哪些服务保障？

服务购买后，天翼云安全服务团队将与您取得联系，确定服务内容及范围，定期输出整体安全风险服务报告，按照SLA协议承诺对客户服务内容进行交付。

若遇到问题，安全服务团队会提供支持和解答，其他问题，您可以通过天翼云客服反馈，我们将竭诚为您服务，保障您的业务安全。

托管检测与响应服务（原生版）可以根据用户需求提供个性化服务吗？

当前服务为标准化服务内容，如果您有个性化服务需求，可与服务经理沟通，确定需求范围及内容，经评估后，服务经理会向您反馈评估结果，如果在可接受范围内，您无需支付任何费用，如超出服务范围，我们将提供新的服务方案。

欢迎您向我们提出新的服务需求，我们将积极支持，不断优化服务内容及流程，更好地服务客户。

6.3. 服务类

什么是应急响应？

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。

应急处置的定义是什么？

启动应急响应计划后，应立即采取相关措施抑制信息安全事件影响，避免造成更大损失。在确定有效控制了信息安全事件影响后，开始实施恢复操作。恢复阶段的行动集中于建立临时业务处理能力、修复原系统的损害、在原系统或新设施中恢复运行业务能力等应急措施（信息安全应急响应计划规范GB/T 24363-2009）。

什么是渗透测试？

渗透测试是一种对抗性和定制化要求都非常高的一类安全测试，安全工程师在书面授权后尽可能完整地模拟黑客可能使用的漏洞发现技术与攻击技术（与黑客攻击相比其结果是可预知性的），对目标网络、主机、数据库与应用系统的安全性做深入的探测，发现系统薄弱环节的过程。能够直观的让管理人员知道当前网络、主机、数据库与应用系统存在的安全弱点以及可能造成的影响，以便采取必要的防范措施。

托管检测与响应服务（原生版）的主要应用场景有哪些？

主要包含4个场景：

- 日常运营：对整体安全防护效果有要求，但是缺乏专业安全人员能承担日常的安全管理工作，希望能通过服务提升整体安全防护体系能力。
- 重保合规：重大活动、会议、节假日等重要时期安全值守，保证不出安全事件；参加国家攻防演练活动希望取得好的成绩。
- 安全加固：发生安全事件或者被监管机构通报，希望能发现网络脆弱性并加固提升安全能力。
- 应急响应：发生重大安全事件时，需要专业人员帮助用户快速解决问题，恢复业务，并能定位出问题的根源并加固。

托管检测与响应服务（原生版）可以给企业带来哪些价值？

- 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。

- 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。
- 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。
- 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。

蓝军攻击服务与红蓝对抗的区别？

红蓝对抗演习是一种用攻防思想来解决机构威胁隐患的模式，通过接近实景的攻防演练，磨练安全运营人员应对安全威胁的能力。红蓝对抗是通过红蓝军围绕防守目标的基于实战化的攻防演练服务项目。

蓝军是演习中专注于“攻击”组织系统、IT基础设施和提供的IT服务的一只队伍。在军事活动中，早已有了特种部队之称，用于检验、提升传统的队伍，更好的适应实战，验证指定的业务系统和人员在重要时期的安全防护强度。

护航版的主要服务内容有哪些？

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。安全服务团队重保服务从前、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。

托管检测与响应服务（原生版）如何保护企业的隐私？

主要采取以下措施保护企业隐私：

- 建立严格的信息安全规范：通过信息安全规范，规范信息共享、网络管理以及技术安全等方面的行为。明确信息的收集、存储、传输和使用等方面的要求，以及员工和第三方合作伙伴的保密义务。

- 采取隐私保护技术：我们已经建立隐私保护机制，采取加密、安全传输等技术手段，确保用户的隐私信息不被泄漏、不被恶意利用。
- 签订隐私协议：天翼云隐私协议，明确数据的使用功能、权限和保护措施，明确双方的责任和义务，确保用户数据的安全性和隐私性。