主线测试自动化专用_APEX底座客户安全运营第二季度报告

运营时间　2025年05月至2025年08月

汇报人　XXX

本季度运营工作概述

关键问题分析研讨

下季度运营计划

本季度安全运营详情

深信服安全服务
SANGFOR SECURITY SERVICE

本季度运营工作概述

安全托管服务概述

服务内容

安全托管服务是基于“**人机共智**”的安全运营中心，围绕业务的“**资产、脆弱性、威胁、事件**”四个核心要素，为客户提供**7*24**小时持续监测，主动发现风险进行闭环处置，**实现安全风险可知、风险可控、风险可管。**

运营组件

- **目前已接入安全运营中心的在线设备：**
- **SIP*1、AF*2、EDR*2**
- **当前处于离线的设备：**
- **TSS*6、AF*14、SIP*16、EDR*9、NTA*6、未知*2**
- **未接入的设备：TSS*1、AF*9、SIP*3、EDR*9、NTA*1、未知*1**
- **未接入原因：**
- **XXXXXXX**
- **运营组件可监测的网络/区域包括：**
- **XXXXXX（如：外网/DMZ、内网/服务器区）**
- **运营组件可防护的网络/区域包括：**
- **XXXXXX（如：外网/DMZ、内网/服务器区）**

服务范围

服务时间：6年

已购买MSS服务资产数量： 12370

MSSP平台已录入IP资产数量：673

- **服务内资产数量：128**
- **服务外资产数量：545**
- **业务系统数量 ：1**

（包括xos-00013-9326）

已录入Web业务资产：1

项目组成员介绍

角色名称	职责分工	对应人员	联系方式
安服工程师T1	1.负责按规范进行安全设备上架和安全组件运营中心接入 2.负责协助上门处置常见安全问题	XXXXXX	XXXXXX
销售经理	1.负责安全运营期间的关键步骤的讨论和资源的保障	XXXXXX	XXXXXX
服务经理（PM）	1.负责项目运营的整体的交付材料质量把控 2.负责安全运营过程中遇到的问题解决	XXXXXX	XXXXXX
信服小安	1.24小时对运营中心监测发现的安全问题进行分析预警及处置	当日值班人员	15347311173
运营中心T1	1.对项目整体的进度和服务质量进行监管 2.负责安全运营过程中遇到的问题解决 3.负责项目运营的整体的交付材料质量把控 4.负责参与安全运营的总结和汇报 5.负责安全运营期间的关键步骤的讨论和资源的保障	XXXXXX	XXXXXX
运营中心T2	1.负责受理运营中心T1上升的安全问题分析和处置的问题 2.问题无法处置、分析，上升至T3进行处置 3.安全日志综合分析，并输出威胁分析报告	XXXXXX	XXXXXX
运营中心T3	1.负责受理T2无法解决的问题并输出相关解决方案	XXXXXX	XXXXXX

项目交付进展

安全运营项目交付里程碑

日期时间	2022-08-19	XXXX-XX-XX	XXXX-XX-XX	XXXX-XX-XX（第二季度）	2028-08-19
	01	02	03	04	05
	服务启动	运营准备	持续运营&周期汇报	持续运营&周期汇报	项目结项
服务阶段及内容	服务需求对齐 方案制定 团队组建 服务人员进场	服务资产梳理 组件上线 首次脆弱性扫描与分析 首次威胁分析 首次处置	季度安全问题跟踪闭环 脆弱性管理 威胁管理 安全事件管理 安全运营周报 安全运营月度报告 安全运营季度报告	季度安全问题跟踪闭环 脆弱性管理 威胁管理 安全事件管理 安全运营周报 安全运营月度报告 安全运营季度报告	年度安全问题跟踪闭环 脆弱性管理 威胁管理 安全事件管理 安全运营周报 安全运营月度报告 安全运营季度报告 安全运营年度报告 项目结项验收报告

本季度安全运营工作目标

监管通报应对

1.梳理历史通报内容，主要是那些监管单位的通报以及通报内容，是脆弱性方面通报还是安全事件类通报。

2.针对脆弱性通报提前做预防工作：如互联网资产暴露面梳理，通过态势感知产品梳理弱口令，TSS漏洞扫描工具对资产进行漏洞扫描等工作。

3.针对安全事件类通报预防工作：终端侧部署终端管理管理杀软，边界侧部署防火墙阻断行为，对发现的安全事件以及异常情况进行及时处置。

安全事件闭环

1.安全托管服务针对服务资产一般事件从安全日志分析研判到通告，用时<1h;并协助闭环处置。

2.安全托管服务针对服务资产的重大事件从安全日志分析研判到通告，用时<30min；并协助闭环处置。

3.启用应急响应机制，工作时间 15 分钟，非工作时间 30 分钟之内云端专家进行响应，默认由专家团队进行远程协助解决，如远程无法解决的则采用最快的交通工具，省会 2 小时内上门处置，省内 8 小时内上门处置。

本季度安全运营工作目标

业务系统防护

1.每周对深信服安全设备如防火墙进行策略检查，保证持续最新的规则库。

2.通告最新的威胁情报，如漏洞信息，apt组织攻击，黑产数据等相关信息。

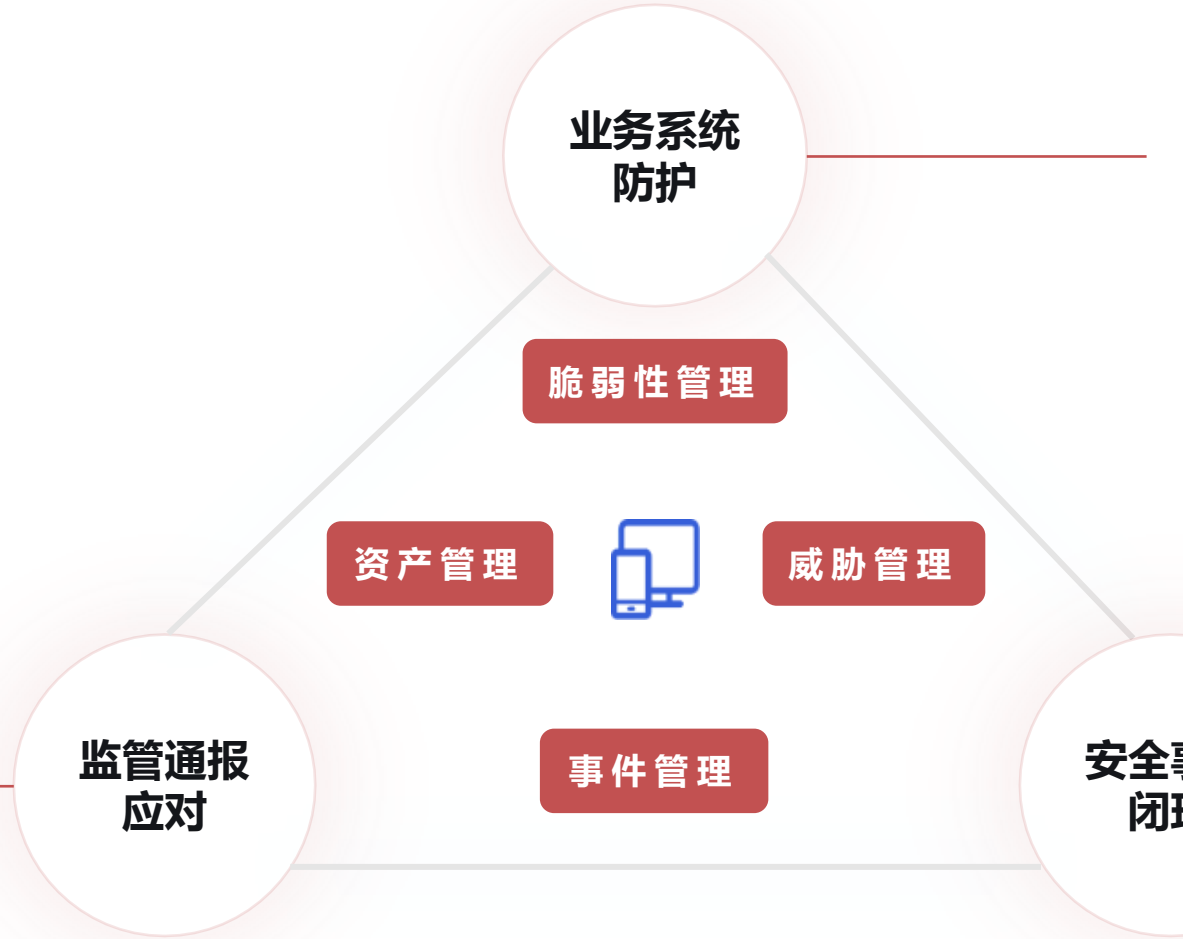
3.通过资产管理，漏洞管理，威胁管理，事件管理发现未知的风险以及解决已知的问题。要有健全的资产清单台账以及资产指纹，针对脆弱性有闭环。

其他安全运营目标

1.持续有效的监测网络安全威胁。

2.协助处置安全相关的一些事项。

保障安全运营目标的关键举措



资产管理：资产梳理、指纹库建立、暴露面识别

脆弱性管理：漏洞扫描、弱口令识别、威胁狩猎、漏洞复测

威胁管理：7*24威胁监测、外部攻击对抗、内部失陷排查、安全威胁通报、威胁情报主动验证、安全策略检查与调优

资产管理：资产梳理、暴露面识别

脆弱性管理：漏洞扫描、威胁狩猎、漏洞复测

威胁管理：最新漏洞通报、行业安全威胁情报、勒索/挖矿风险排查

事件管理：通报事件分析溯源、通报事件处置、闭环跟进、安全隐患排查

事件管理：安全事件处置、日志分析溯源、安全隐患排查、闭环跟进、加固方案

★ **服务价值：**

通过**资产、脆弱性、威胁和安全事件**四个维度进行持续安全运营，专家7*24H对业务的威胁进行全方位监控，努力实现以下安全目标：对威胁和事件监测并对处置避免对业务的持续性运行造成危害；持续发现业务的漏洞、弱口令脆弱性并加固、有效防范外部威胁入侵；及时响应并处理监管通报事件。

本季度安全运营工作内容概述

一、资产管理：

- 本季度共进行资产信息变更 34 次，新上线资产 476 个，新下线资产 7 个。
- 当前已录入服务内资产 128 个，服务外资产 545 个。
- 本季度服务期间，共发现风险资产 104 个，经过线上线下相互配合，目前对发现的风险资产已闭环 39 个，未闭环 65 个
- 如协助xxxx做了XXXXXXXXXXXXXXXXX……

二、脆弱性管理：

- 对服务内资产发起 X 次全量的漏洞扫描，服务内资产发现漏洞 3 个，已闭环漏洞 2 个。
- 对服务内资产主动发起 X 次弱密码分析和挖掘，共发现弱口令 3 个、其他弱点 8 个， 已闭环 0 个。
- 本季度共开展 0 次互联网暴露面检查/威胁狩猎，监测/发现到面向互联网开放高风险端口的风险资产 3 个，已闭环 0 个

三、威胁管理：

- 本季度全网外部攻击总次数达 0 多次，平均每周捕获网络攻击 0 次；对互联网外部的网络攻击行为，主动封锁黑客攻击IP 50 个
- 本季度主动对服务内的资产发起 xx 次安全日志分析工作， 发现并跟踪攻击威胁事件 1 起
- 本季度共进行安全组件策略检查 3 次，共发现策略隐患 24 个，已闭环 1 个。
- 推送 8 次行业安全威胁情报，主动协助贵单位完成 xx 次新威胁排查工作。

本季度安全运营工作内容概述

四、事件管理：

- 本季度共计配合完成 122 起服务内资产的事件处置，44 起服务外资产的事件处置，遗留未处置事件 135 起。
- 本季度出现最多的事件类型为“远程命令执行（ 62 个 ）”，占所发现安全事件总量 34.44 %，已重点关注该类事件。

五、增值服务：

- 本季度共进行网站篡改服务 1 次、可用性监测服务 0 次，公网web漏洞扫描 0 次。共发现网站篡改事件 0 个，其中已闭环 0 个，未闭环 0 个。共发现网站不可用事件 0 个，其中已恢复 0 个，未恢复 0 个。共发现公网web漏洞 0 个，其中已闭环 0 个，未闭环 0 个。
- 本季度进行勒索风险排查 X 次，对针对贵公司的勒索攻击行为进行持续监控。共发现漏洞类风险 X 个、高风险端口类风险 X 个、弱口令类风险 X 个、攻击行为类风险 X 个、安全策略类风险X个，其中已闭环 X 个，未闭环 X 个。

六、其他工作：

- 如本季度共进行节假日值守X次：
- X月X日-X月X日：中秋节值守。
- X月X日-X月X日：XX节值守。
- X月X日-X月X日：XX节值守。

本季度安全运营目标达成情况

监管通报应对

1.通过安全运营持续运营，本季度业务未被通报。
2.提供最新的威胁情报，总结月刊，包含实时政策以及热点事件，及时同步最新威胁。

安全事件闭环

1.安全事件均全部闭环。未闭环事件XXX，其原因是因为XX。
2.安全事件均快速响应处置。

业务系统防护

1.没有业务遭受攻击导致出现问题。
2.未发生真实攻击成功的事件，所有事件均被拦截。
3.发现潜在的攻击行为立马对其处理。
4.进行XX资产信息梳理。

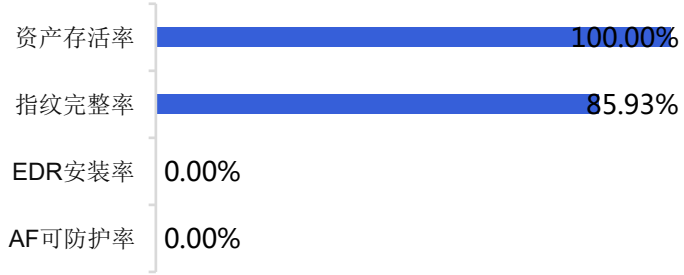
其他安全运营目标

1.持续有效的监测网络安全。
2.协助做好安全工作。

服务内资产安全状态总览

通过对**资产、脆弱性、威胁、事件**进行持续安全运营，本季度总体安全状态 **较差** ，当前有待重点关注的运营事项为 **XXX**，建议及时联系用户/供应商进行整改。

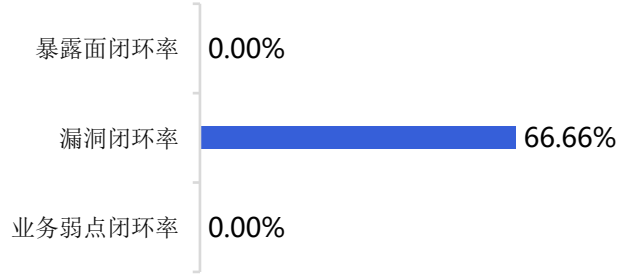
资产管理 46.48分



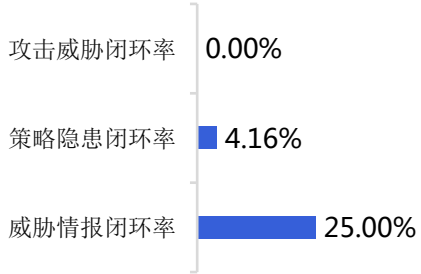
总体安全状态

30.46分

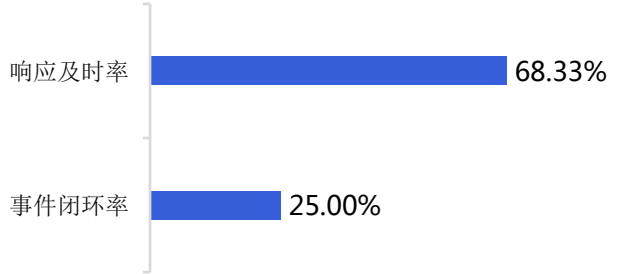
脆弱性管理 19.99分



威胁管理 8.74分



事件管理 46.66分



关键问题分析研讨

遗留安全问题及解决办法探讨（1）

问题

服务资产未录满：服务资产总数XX个，当前录入XX个，可继续录入XX个。

现状及影响

资产未录满可能导致重要业务系统未在全面监测中，导致安全事件漏报。

解决建议

【方案一】

资产情况清晰，有资产台账：梳理服务器优先级，将重要资产纳入服务资产中。

【方案二】

资产情况不清晰，无资产台账：

（1）使用TSS对服务器网段进行资产发现，梳理业务资产信息，选取重要性高的资产纳入服务资产。

（2）有SIP组件的，可以在SIP资产管理中导出服务器资产进行梳理，选取重要性高的资产纳入服务资产。

遗留安全问题及解决办法探讨（2）

问题

（1）高危可利用漏洞闭环困难，闭环率低。

（2）公网弱口令较多，整改缓慢。

现状及影响

（1）黑客可能利用该漏洞进行攻击，不及时修复可能会导致监管单位通报或者黑客攻击成功，造成业务系统数据丢失，甚至遭到勒索。

（2）公网弱口令容易遭受黑客爆破攻击成功，从而展开进一步攻击，以及敏感信息数据可能泄露等。

解决建议

【方案一】

（1）对于有防火墙规则的高危可利用漏洞，通过修改防火墙规则进行防护。

（2）对于没有防火墙规则防护的高危可利用漏洞，建议联系厂商及时进行修复，或者收敛其暴露面。

【方案二】

（1）联系厂商修改业务系统口令校验规则，必须为强口令。

（2）优先修改管理员弱密码，收敛暴露面等。

遗留安全问题及解决办法探讨（3）

问题

外部威胁事件不能及时制止，边界防护较弱。

现状及影响

高危攻击不能及时拦截，可能会导致攻击成功，业务遭受更深层次的攻击。

解决建议

【方案一】

每周运营中心服务经理整理高危攻击ip，由客户进行统一封堵。

授权服务经理封堵高危攻击ip，及时遏制攻击威胁。

【方案二】

部署深信服防火墙，联动态势感知进行高危攻击联动封堵。

下季度运营计划

深信服安全服务
SANGFOR SECURITY SERVICE

下季度安全运营工作目标

监管通报应对

1.梳理历史通报内容，主要是那些监管单位的通报以及通报内容，是脆弱性方面通报还是安全事件类通报。

2.针对脆弱性通报提前做预防工作：如互联网资产暴露面梳理，通过态势感知产品梳理弱口令，TSS漏洞扫描工具对资产进行漏洞扫描等工作。

3.针对安全事件类通报预防工作：终端侧部署终端管理管理杀软，边界侧部署防火墙阻断行为，对发现的安全事件以及异常情况进行及时处置。

安全事件闭环

1.安全托管服务针对服务资产一般事件从安全日志分析研判到通告，用时<1h;并协助闭环处置。

2.安全托管服务针对服务资产的重大事件从安全日志分析研判到通告，用时<30min；并协助闭环处置。

3.启用应急响应机制，工作时间 15 分钟，非工作时间 30 分钟之内云端专家进行响应，默认由专家团队进行远程协助解决，如远程无法解决的则采用最快的交通工具，省会 2 小时内上门处置，省内 8 小时内上门处置。

下季度安全运营工作目标

业务系统防护

1.每周对深信服安全设备如防火墙进行策略检查，保证持续最新的规则库。

2.通告最新的威胁情报，如漏洞信息，apt组织攻击，黑产数据等相关信息。

3.通过资产管理，漏洞管理，威胁管理，事件管理发现未知的风险以及解决已知的问题。要有健全的资产清单台账以及资产指纹，针对脆弱性有闭环。

其他安全运营目标

1.持续有效的监测网络安全威胁。

2.协助处置安全相关的一些事项。

下季度安全运营工作计划

一、资产管理：

- 如梳理服务器资产，补全资产信息……
- 如对服务外的资产XXX系统、XXX系统进行了资产盘点……
- 如完成XXXX系统/XXX区域的资产扫描和识别……
- 如运营中心持续监测，保障资产安全……

二、脆弱性管理：

- 如对上季度漏扫结果进行复测……
- 如对已发现的高危可利用漏洞，协助贵单位开展XXX、XXX漏洞的闭环修复工作……
- 如对服务内资产进行暴露面梳理，发现暴露面问题……
- 如对服务内资产主动发起弱密码分析和挖掘，梳理内外网弱密码等。

三、威胁管理：

- 如对互联网外部的网络攻击行为，及时封堵，优化防火墙策略等……
- 如开展服务内资产日志分析等……
- 如处理上季度遗留X台勒索病毒主机、X次木马病毒主机等……
- 如实时推送行业安全威胁情报，主动协助贵单位进行新威胁排查工作……

下季度安全运营工作计划

四、事件管理：

- 如处理本季度遗留安全问题XXX……
- 如……
- 如协助贵单位完成勒索病毒事件的应急处置流程制定……
- 如……

五、增值服务：

- 如下季度将开展勒索预防检测，发现勒索风险……
- 如针对即将到来的HW进行前期准备，如策略检查、暴露面梳理等工作……
- 如下季度将继续进行公网web漏洞扫描，持续进行篡改和可用性监测等……

六、其他工作：

- 如在xx节进行节假日值守，保障业务资产安全。

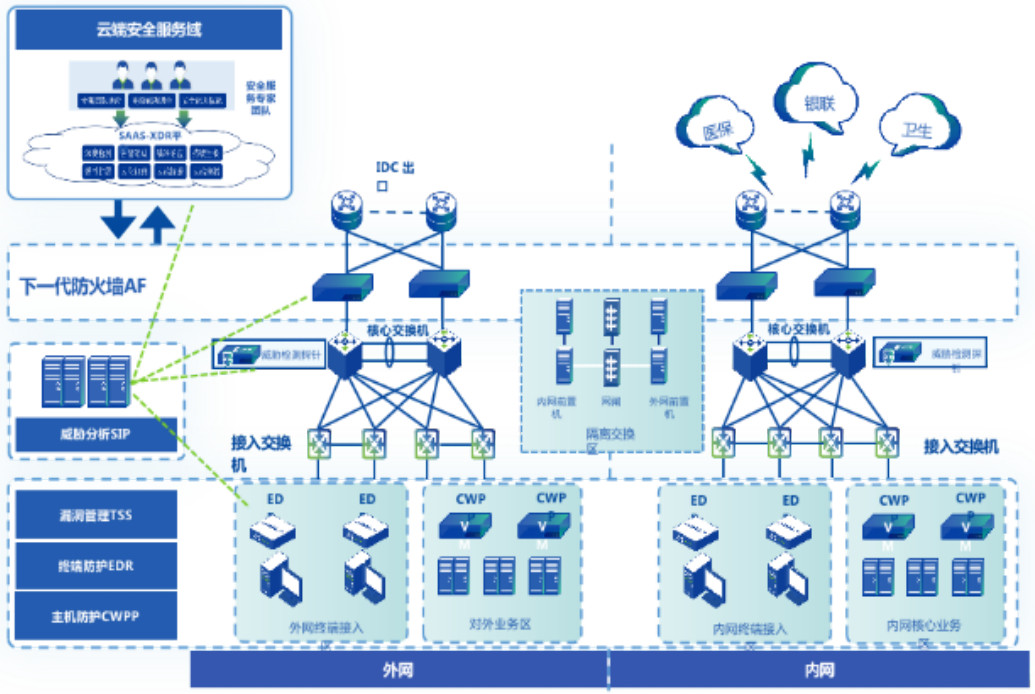
本季度安全运营详情

深信服安全服务
SANGFOR SECURITY SERVICE

资产管理 / 资产防护情况

- 服务内的资产有 **0** 个已经在防火墙的防护范围内，仍有 **128** 个暂无防火墙防护；
- 服务内的资产目前仍有 **128** 个未安装EDR/CWPP，未安装率 **100.0** %。

服务资产防护状态			
序号	区域	防护措施	状态
1	XXX	XXXXXXXXXX	已防护
2	XXX	XXXXXXXXXX	未防护
3	XXX	XXXXXXXXXX	XXX
4	XXX	XXXXXXXXXX	XXX



服务内未防护资产的整改建议（请自行根据客户业务调整内容）

1.未安装终端安全的主机需要覆盖安装EDR，加强服务内资产终端安全。

2.建议加强对资产指纹信息的梳理，以便威胁情报能与指纹精确比对及时预警。

资产管理 / 风险资产状况

• 本季度服务期间，共发现风险资产 **104** 个，经过现场工程师与贵单位安全责任人相互配合，目前对发现的风险资产已闭环 **39** 个，未闭环 **65** 个。

已闭环风险资产TOP5		
IP（业务名称）	风险次数	主要风险项
172.23.0.74 (未知业务)	13	命令执行
10.48.155.71 (未知业务)	8	命令执行
172.26.156.169 (未知业务)	2	SQL注入攻击成功
10.34.88.51 (xos-00013-9326)	2	漏洞、紧急漏洞
172.22.82.161 (未知业务)	2	WebShell上传成功

未闭环风险资产TOP5		
IP（业务名称）	风险次数	主要风险项
10.74.145.45 (xos-00013-9326)	53	远程命令执行、后门软件
10.74.145.44 (未知业务)	35	远程命令执行
10.128.165.106 (未知业务)	31	漏洞风险
10.64.5.37 (xos-00013-9326)	9	系统服务漏洞、明文密码
10.64.20.19 (xos-00013-9326)	7	SQL注入攻击成功、暴露风险

未闭环风险资产的整改建议（请自行根据客户业务调整内容）

1.尽快定位到未闭环风险资产，尽快对相关资产执行病毒查杀/漏洞修复/应急处置等。

2.关闭XX默认端口对公网开放，并修改密码为强口令。

脆弱性管理 / 漏洞总览

本季度运营中心对服务内资产共发起 **0** 次漏洞扫描，存在漏洞 **3** 个（新增 3 个；历史未闭环 0 个）。其中：

- 高危 **2** 个（高可利用漏洞 **2** 个），中危 **1** 个，低危 **0** 个；
- 服务内资产发现的漏洞较上季度增加 **3** 个;

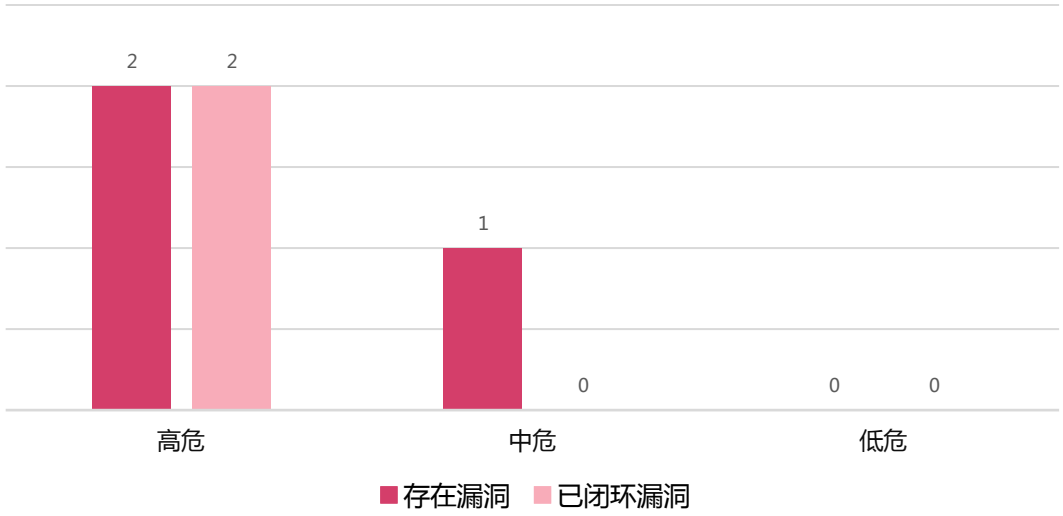
目前已闭环漏洞 **2** 个，其中：

- 通过防护规则有效防护 **0** 个，漏洞补丁更新闭环 **1** 个，业务原因接受风险 **1** 个，整体闭环率为 **66.66** %。

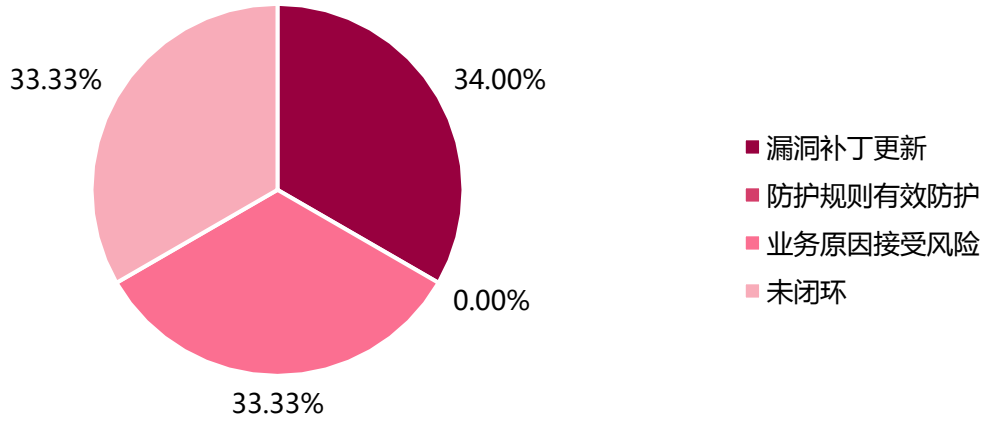
★ **服务价值：**

及时发现业务系统漏洞，及时修复可利用漏洞，有效降低服务资产的被入侵的风险。

本季度漏洞对比数据



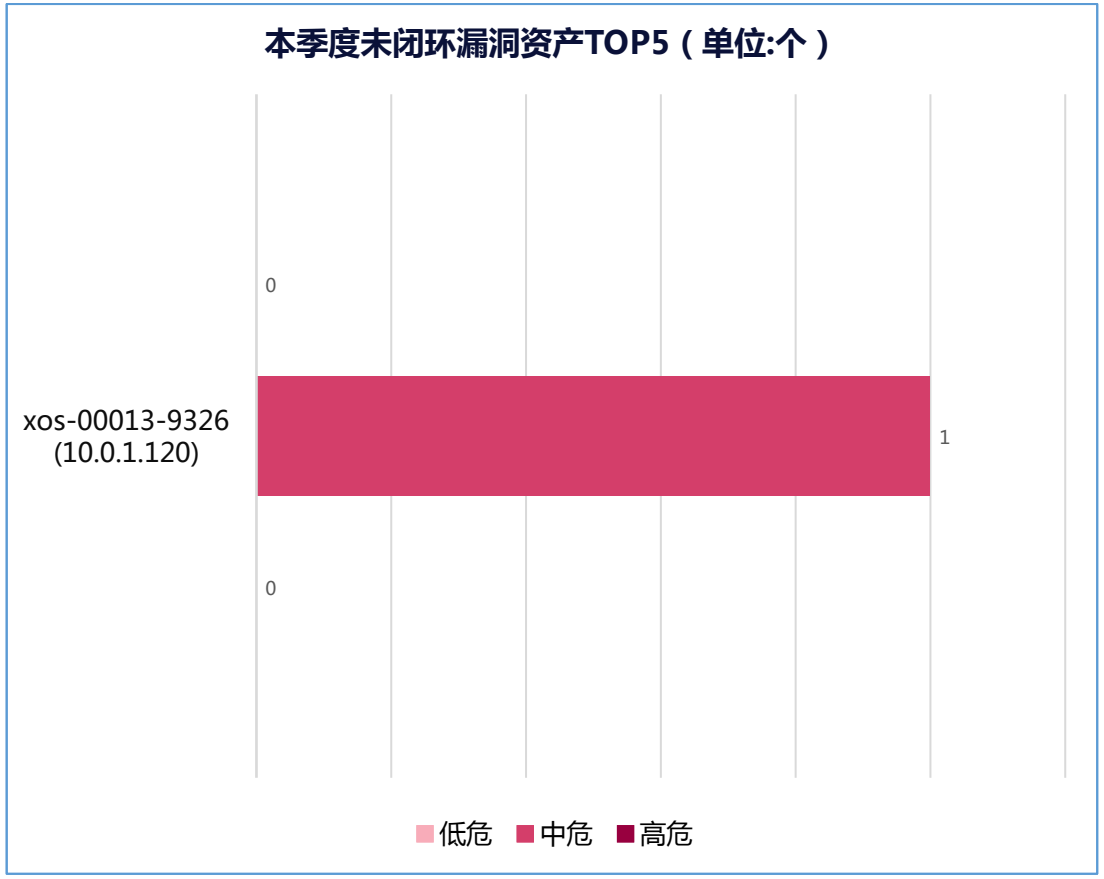
本季度漏洞闭环情况



脆弱性管理 / 未闭环漏洞

当前未闭环的漏洞共 **1** 个；其中高危 **0** 个（高可利用漏洞 **0** 个），中危 **1** 个，低危 **0** 个；

- 仍有 **1**个资产存在未闭环漏洞风险；未闭环原因：xxxx
- 存在未闭环漏洞最多的业务为 **xos-00013-9326**（10.0.1.120），其中高危 **0** 个（高可利用漏洞 **0** 个）、中危 **1** 个、低危 **0** 个。



未闭环漏洞举例				
漏洞名称	风险等级	覆盖资产数量	主要影响业务系统举例	对业务的主要影响描述
Apache HTTP Server 输入验证错误漏洞	中危	1	xos-00013-9326	影响apache:2.4.18版本(含)到2.4.34版本(含)

脆弱性管理 / 暴露面

本季度共进行暴露面风险资产发现 **0** 次，检测到存在暴露面风险的资产 **3** 个（新增 3 个；历史未闭环 0 个）。

- 较上季度增加**3**个;
- 已闭环 **0** 个，未闭环 **3** 个；仍存在暴露风险的资产有10.64.20.19（xos-00013-9326）等，整体闭环率为 **0.0** %。暴露面风险资产TOP5及未闭环风险端口TOP5概况如下：

★ **服务价值：**

及时发现互联网业务系统潜在的暴露面，通过手段降低暴露面的风险，减少被黑客利用机会。

暴露面风险资产排名TOP5

IP（业务名称）	风险端口数量	风险端口列举
10.64.20.19 (xos-00013-9326)	6	135、137、138、139、445等
20.25.8.18 (未知业务)	1	1234
10.34.88.50 (xos-00013-9326)	1	445

未闭环风险端口TOP5

风险端口	覆盖资产数量	潜伏风险描述
445	2	
135	1	
137	1	
138	1	
139	1	

未闭环暴露面风险的整改建议（请自行根据客户业务调整内容）

1.建议关闭风险端口对外开放，收敛高危暴露面。

脆弱性管理 / 业务弱点

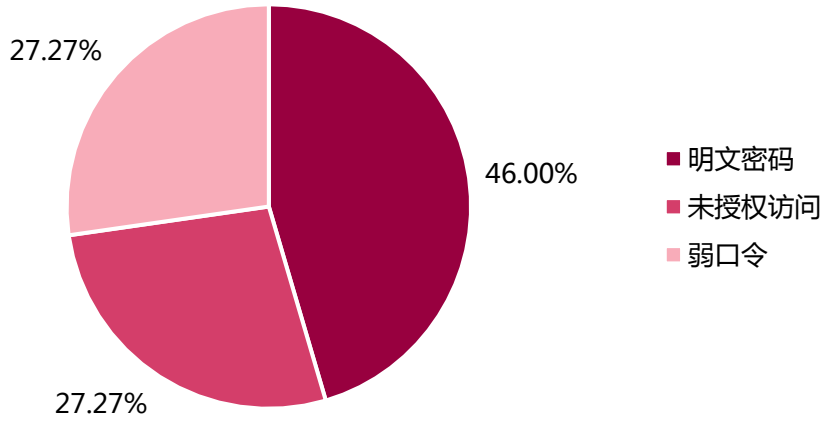
本季度服务内资产存在业务弱点 **11** 个（新增 8 个；历史未闭环 3 个），其中弱口令类型 **3** 个，其他脆弱性 **8** 个；

- 较上季度增加**11**个;
- 已闭环 **0** 个；未闭环 **11** 个，其中 **明文密码** 类型最多，占比 **45.45** %，整体闭环率为 **0.0** %；
- 当前存在业务弱点最多的资产为 10.64.5.37（xos-00013-9326），共 **5** 个，最多类型为：**明文密码**。

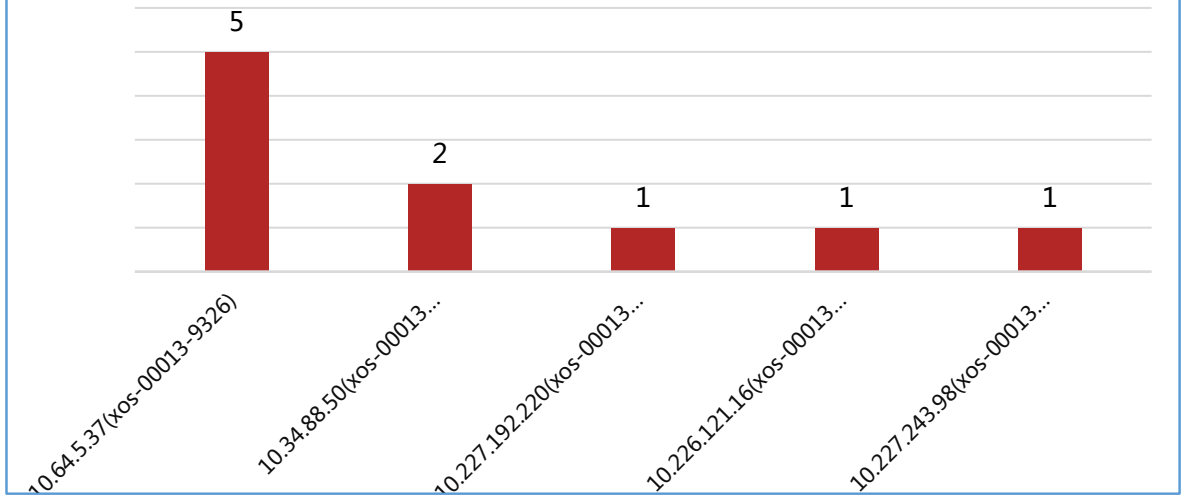
★ **服务价值：**

找到隐藏的业务弱点，减少被黑客利用的机会。

本季度业务弱点类型分布概况



本季度存在业务弱点的资产TOP5



服务内未防护资产的整改建议（请自行根据客户业务调整内容）

1.安全运营中心将对未闭环的业务弱点进行持续监测，为了您的业务安全请在运营专家的协助下尽快闭环处置。

2.建议对未闭环应用系统安全性配置问题进行整改，加强系统自身安全防护能力，避免造成信息泄露等危害。

脆弱性管理 / 下线资产脆弱性

本季度由于8月发生了资产变更，下线服务资产7个，这部分资产遗留脆弱性问题由于已不属于服务内资产，运营中心将不再进行跟进，但仍建议贵单位修复这些问题，避免业务遭受攻击。

- 这些资产本季度存在脆弱性问题 2 个（其中弱口令 0 个，漏洞 2 个，其他脆弱性 0 个）：
- 本季度已处置脆弱性问题 1 个，其中弱口令 0 个，漏洞 1 个，其他脆弱性 0 个；
- 遗留未闭环脆弱性问题 1 个，其中弱口令 0 个，漏洞 1 个，其他脆弱性 0 个。

★ **服务价值：**

找到隐藏的业务弱点，减少被黑客利用的机会。

下线资产脆弱性风险举例

资产下线时间	IP（业务名称）	脆弱性类型	遗留漏洞数	遗留业务弱点数
2025/08/15	10.65.162.174 (xos-00013-9326)	漏洞	1	0
2025/08/15	0.15.66.64 (xos-00013-9326)		0	0
2025/08/15	0.15.66.65 (xos-00013-9326)		0	0
2025/08/05	10.226.101.193 (xos-00013-9326)		0	0
2025/08/15	10.64.4.78 (xos-00013-9326)		0	0

下线资产脆弱性风险整改建议（请自行根据客户业务调整内容）

1.安全运营中心将对未闭环的业务弱点进行持续监测，为了您的业务安全请在运营专家的协助下尽快闭环处置。

2.建议通过系统制定密码强度规则要求，规避弱口令问题，同时加强安全意识的培训和宣传。

威胁管理 / 外部威胁

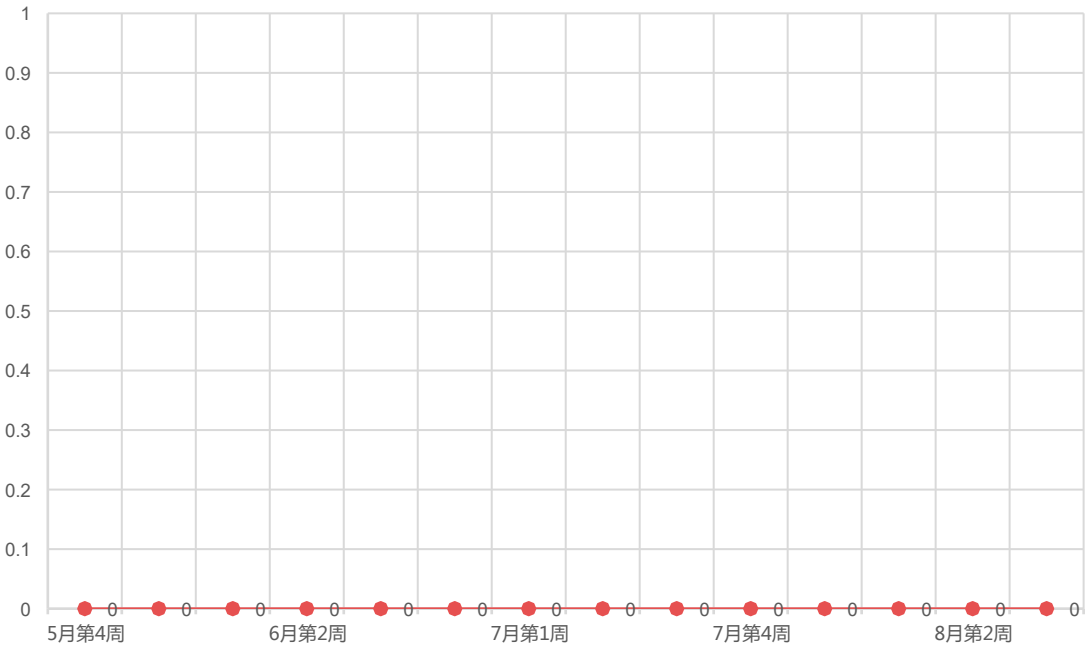
本季度运营中心通过服务组件日志分析，贵单位遭受外部攻击总次数达 **0** 次，平均每周捕获网络攻击 **0** 次。

- 外部攻击次数较上季度有所**下降**
- 业务资产遭受攻击次数较多的攻击类型：“**开源和商业应用漏洞**”和“**Web框架漏洞**”，占比分别 **0** %和 **0** %；
- 服务期间监测到的攻击均有效拦截（请根据实际情况人工调整话术）。

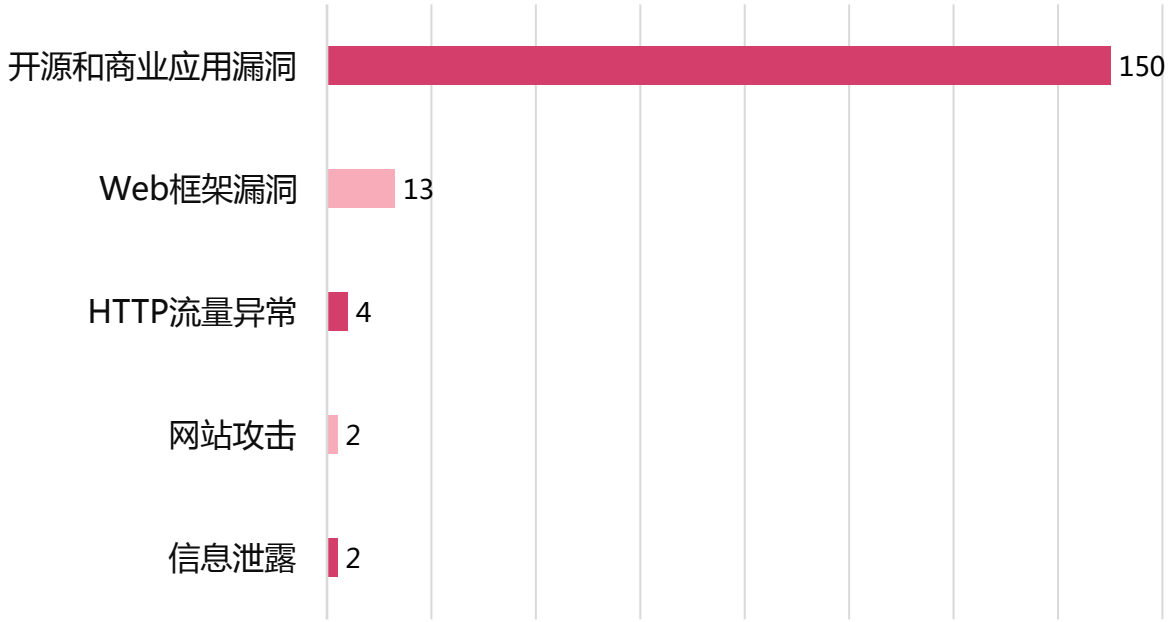
★ **服务价值：**

云端专家提供7*24小时持续监测，主动发现异常攻击行为，专业指导攻防对抗。

本季度外部攻击趋势图（单位：次）



外部威胁类型TOP5



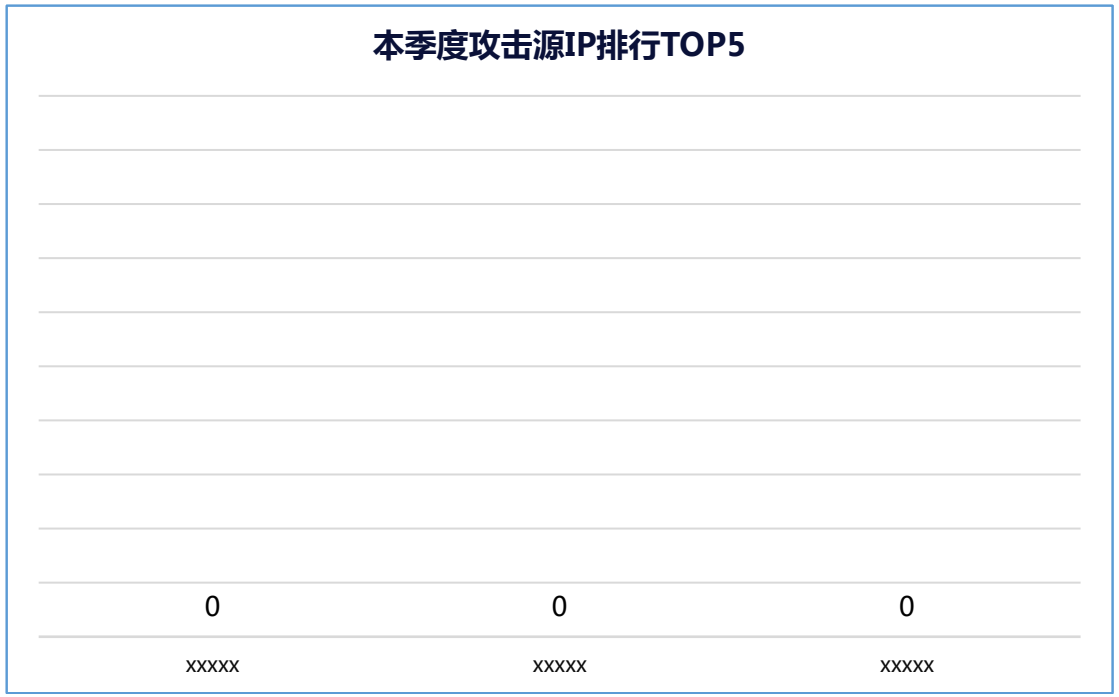
威胁管理 / 外部威胁

本季度攻击次数最多的源IP为：（ **0** 次），占总攻击次数 **0** %；本季度共发现外部威胁事件 **1** 起，运营中心已在互联网出口防火墙对 **50** 个高威胁攻击源IP进行了封锁，**未造成安全事件发生。**（请根据实际情况手动调整话术）

本季度遭受外部攻击次数最多的目的IP为：（ ），攻击类型包括等；

暂未发现攻击成功事件。（请根据实际情况手动调整话术）

建议加强对遭受攻击次数较高的IP（如：等）的访问可用性监测，及时发现潜在风险。



威胁管理 / 策略隐患

本季度检测到设备离线异常 **19** 次，主要原因是**XXXXXX**（此处人工填写未闭环原因）；

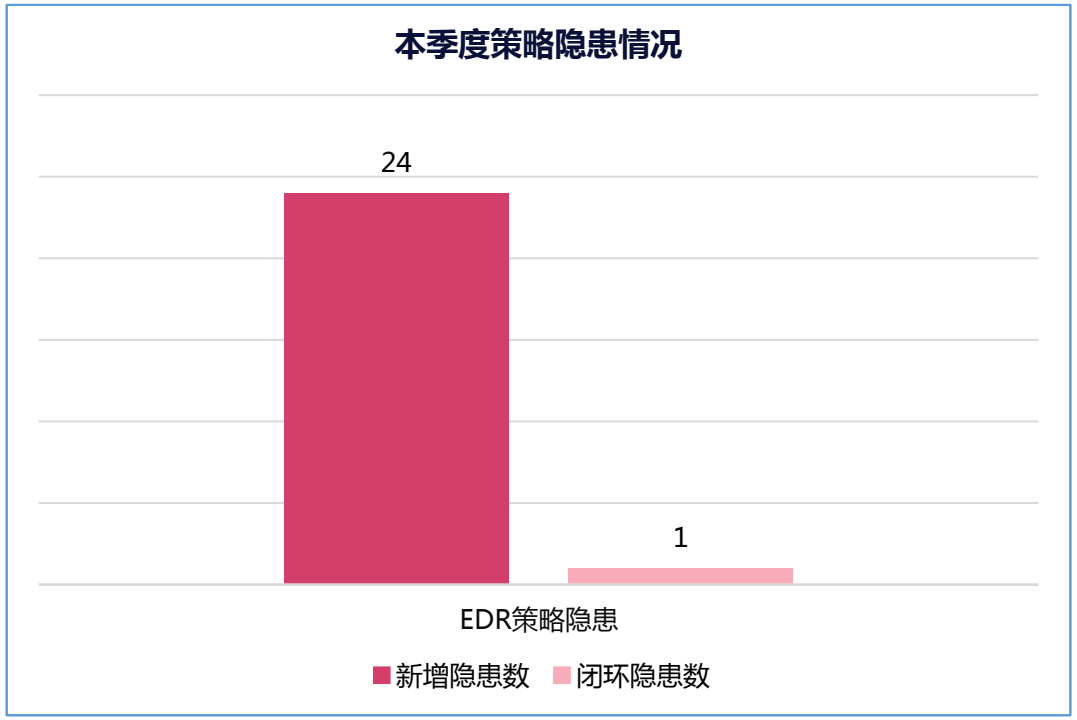
本季度共进行安全组件策略检查 **3** 次，共新增策略隐患 **24** 个，其中：

- EDR策略隐患 **24** 个；
- 当前仍剩余 **23** 个策略隐患待闭环，主要原因是**XXXXXX**（此处人工填写未闭环原因）；

部分策略隐患举例如下，运营中心服务经理将持续进行策略调优。

★ 服务价值：

及时调整有问题的策略，发挥现有安全设备的效果，提升组织的实时安全保障能力。



策略隐患举例				
序号	设备名称	IP地址	策略隐患项	处置状态
1	AF_008	-	EDRLinux webshell检测【未开启】	处置中
2	AF_008	-	EDRLinux webshell检测【未开启】	处置中
3	AF_008	-	EDRLinux webshell检测【未开启】	处置中
4	AF_008	-	EDRLinux webshell检测【未开启】	处置中
5	AF_008	-	EDRLinux webshell检测【未开启】	处置中

威胁管理 / 威胁情报推送

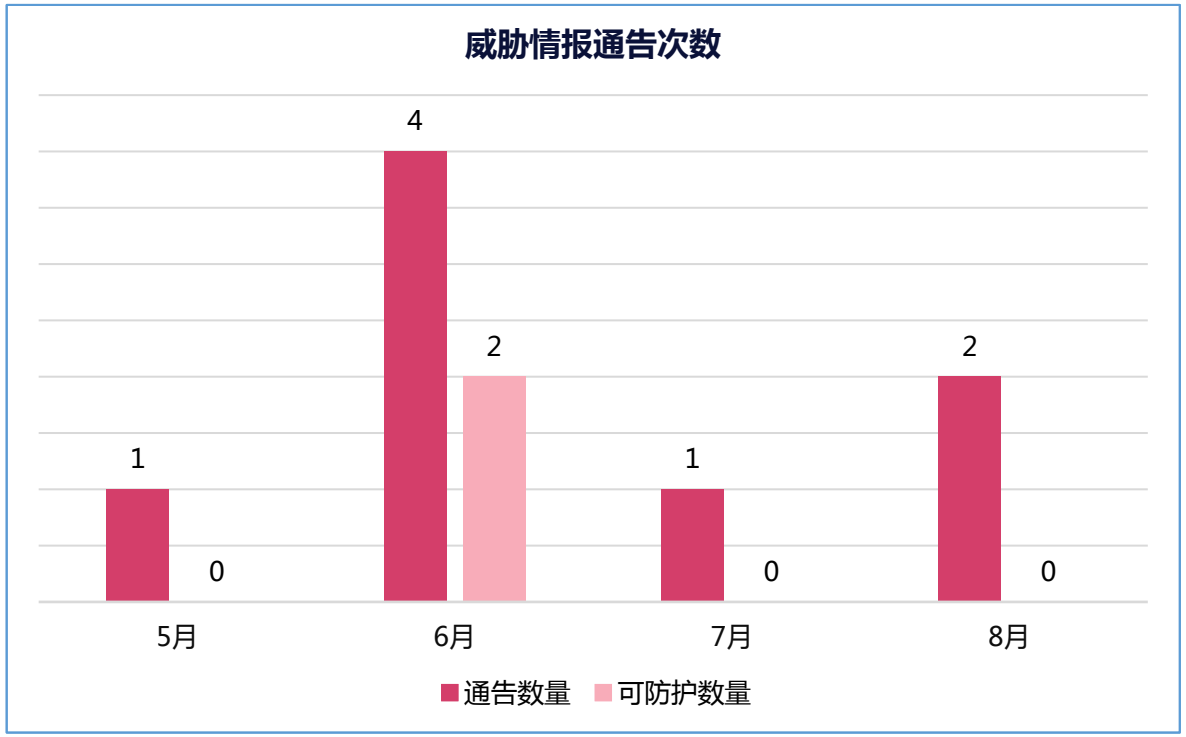
本季度运营期间推送威胁情报 **8** 次（威胁通告来源于深信服威胁情报中心），共 **6** 个紧急漏洞、**2** 个威胁狩猎；

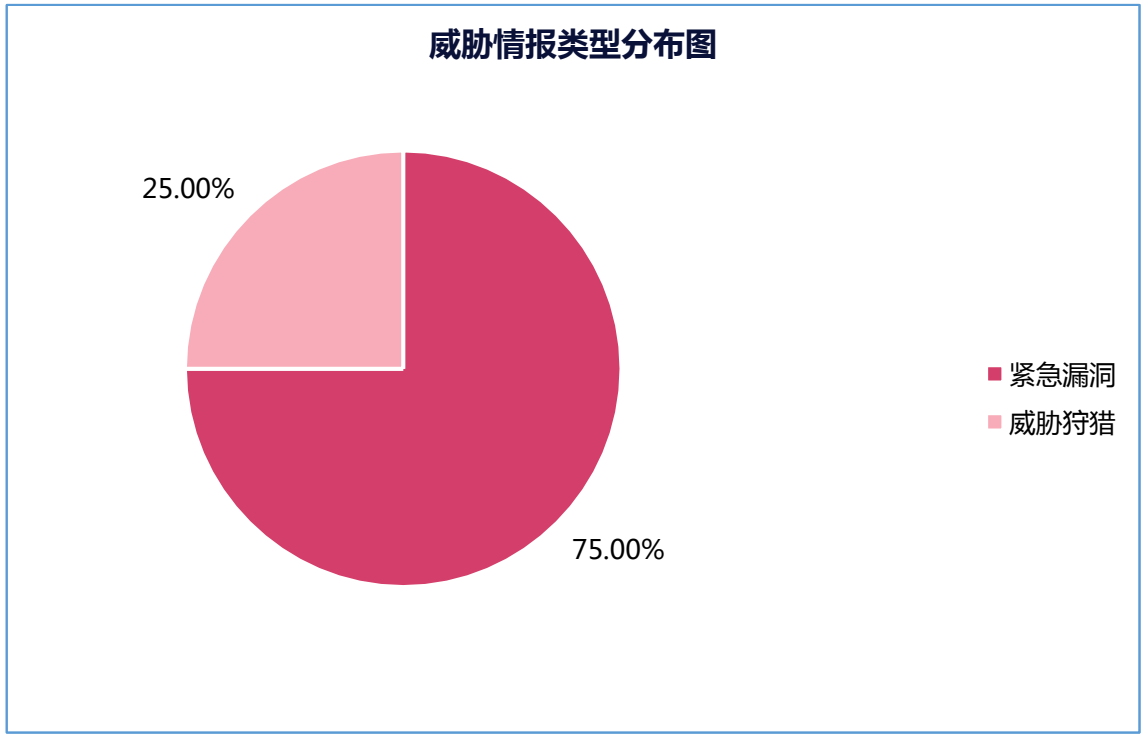
- 深信服安全设备可防护 **2** 个；
- 通告中受影响资产 **0** 个，已闭环 **0** 个。

经深信服安全组件进行联动检测，其余漏洞威胁给予缓解措施，深信服安全服务团队会持续追踪通告漏洞，及时推送最新的进展和响应举措。

★ 服务价值：

第一时间获取业内最新的安全威胁信息，安全专家提供专业的检测和应对方案，提高组织应对最新威胁的能力。





事件管理 / 整体概况

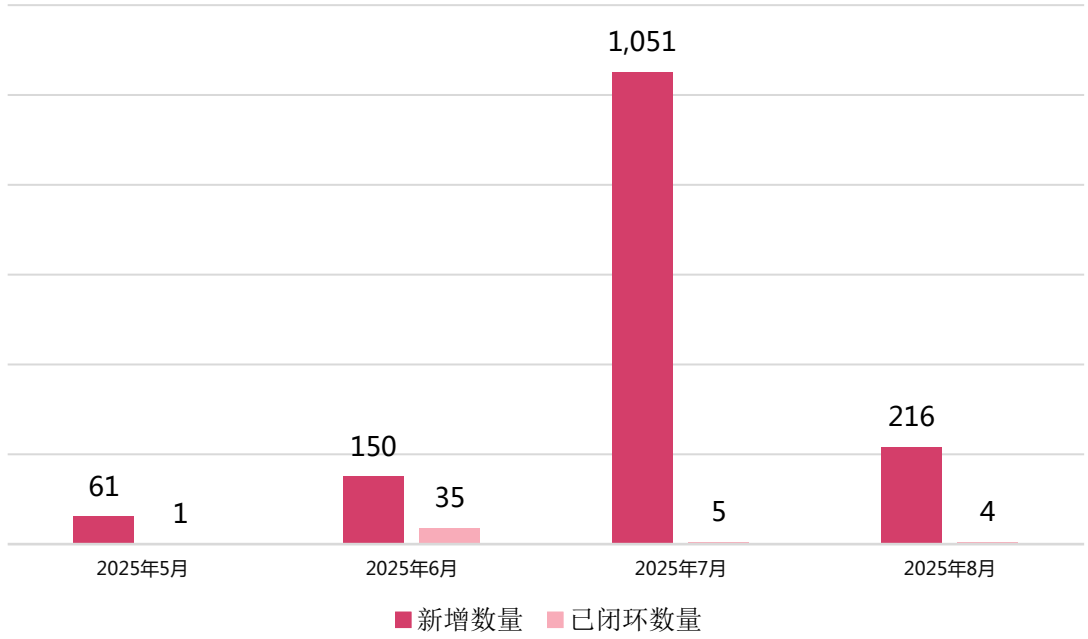
本季度新增安全事件 **180** 起，已针对全部失陷主机提供了处置方法、工具和远程协助，截止目前为止已闭环安全事件 **45** 起，闭环率 **25.0** %：

- 从资产范围：服务内资产安全事件 **122** 起，服务外资产安全事件 **44** 起；
- 从事件程度：严重事件 **17** 起，高危事件 **0** 起，中低危事件 **10** 起；
- 事件响应及时率为 **68.33** %，平均响应时间为 **3376.0** 分钟。

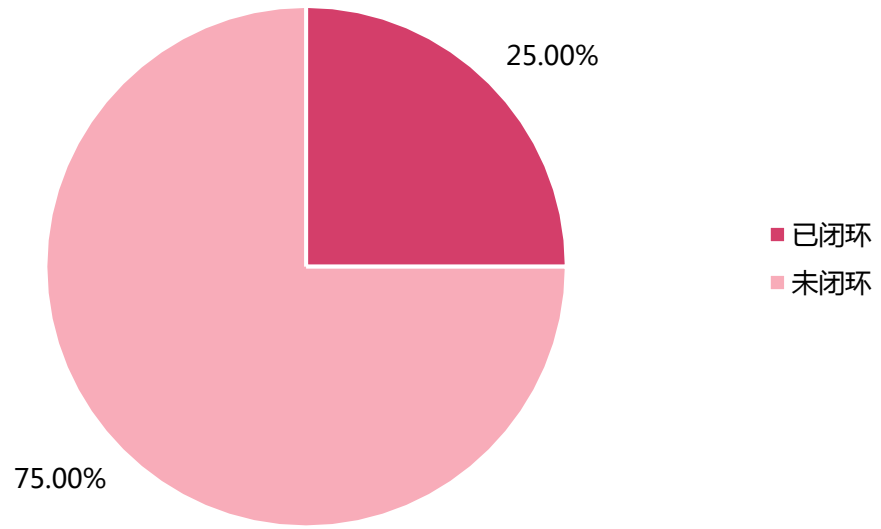
★ 服务价值：

通过云地协同快速闭环安全事件，从模式上颠覆了救火式应急响应“慢”、损失“大”、处置“不闭环”的问题。

本季度安全事件处置情况（单位：个）



本季度安全事件闭环情况（单位：个）



事件管理 / 事件分布

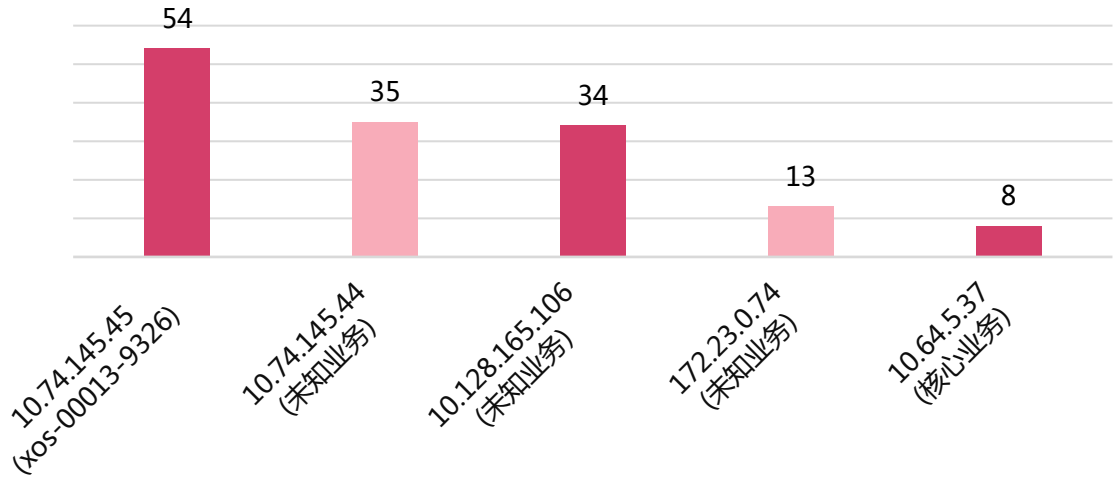
本季度发生的安全事件中：

- 次数最多的业务是“**10.74.145.45（未知资产）**”，占安全事件总量 **30.0** %，服务经理已重点关注该业务的安全情况；
- 出现最多的事件类型为“**远程命令执行**”，占安全事件总量 **34.44** %，已重点关注该类事件，发现风险会及时通告并进行协助处置工作；

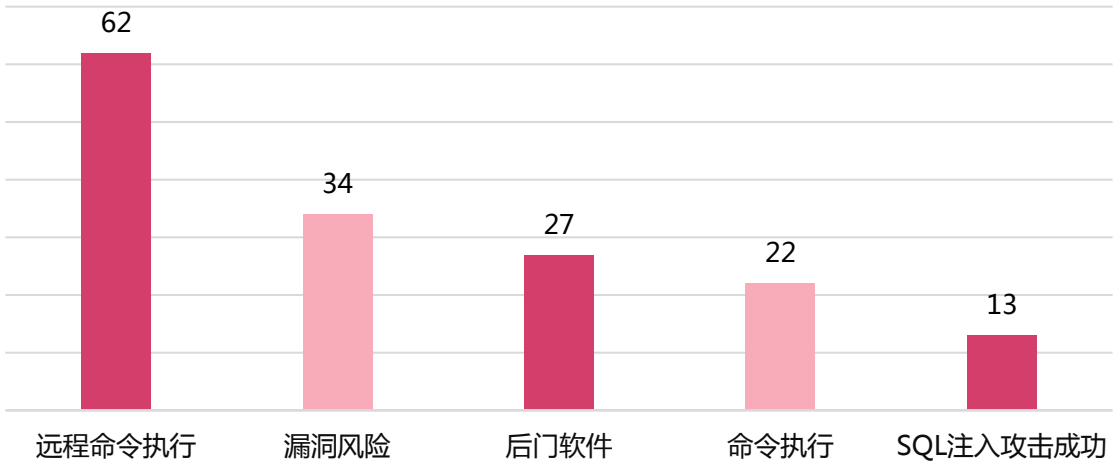
★ 服务价值：

深度溯源分析事件发生根因，持续关注事件闭关跟进，协助组织快速应对突发安全事件。

本季度受影响资产排行TOP5



本季度安全事件类型TOP5



未闭环安全事件的整改建议（请自行根据客户业务调整内容）

1.对于内网病毒失陷主机建议安装深信服EDR对其进行病毒查杀，隔离病毒文件。

2.对于存在代理工具通信的主机建议联系服务器管理员，非业务需要删除代理工具，或者在防火墙配置策略进行通信流量拦截。

3.对主机存在异常的，请尽快进行溯源排查，删除恶意后门文件等。

事件管理 / 事件举例

Sql注入攻击

Sql注入成功-5.7.x以上版本报错

事件类型：SQL注入攻击成功
事件等级：已失陷
发现时间：2025-06-25 16:03
影响资产：172.26.156.169
事件危害：-

事件跟踪分析

影响范围分析：
-

事件根因分析：
-

闭环结论：
确认关闭

安全建议：
-

事件管理 / 事件举例

Sql注入

Sql注入成功-获取user信息

事件类型：SQL注入攻击成功
事件等级：已失陷
发现时间：2025-06-25 15:31
影响资产：60.45.52.118
事件危害：存在sql注入漏洞，攻击者可能未经授权访问数据库中的数据，盗取用户的隐私以及个人信息，造成用户的信息泄露，在一定条件下甚至可以获取服务器最高权限。

事件跟踪分析

影响范围分析：
-

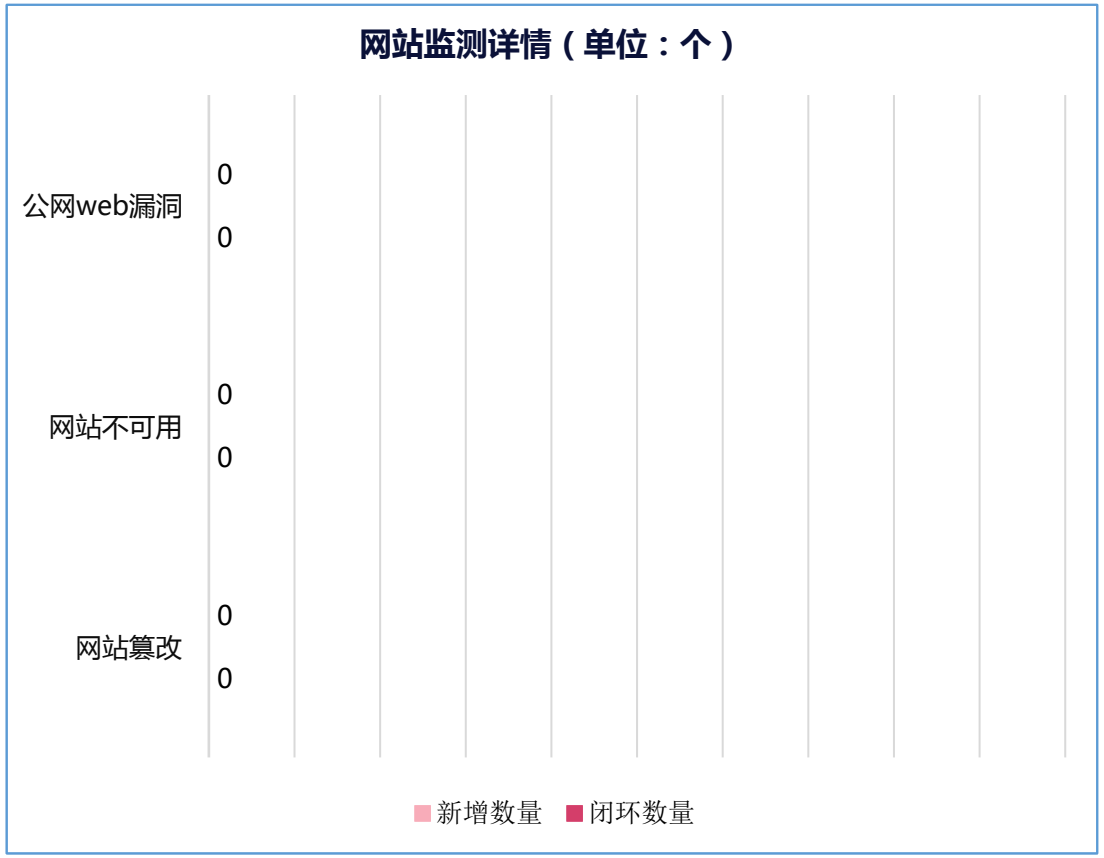
事件根因分析：
-

闭环结论：
确认关闭

安全建议：
Sql注入:
1、若源IP非代理IP，则建议优先对该IP进行封锁。
2、为避免攻击者进行脱库操作。建议确认是否需要对该网站下，此url暂时进行封禁。
3、及时在代码层面进行sql注入的修复，
修复方案如下：
代码层最佳防御sql漏洞方案：使用预编译sql语句查询和绑定变量。
1、使用预编译语句，使用PDO需要注意不要将变量直接拼接到PDO语句中。所有的查询语句都使用数据库提供的参数化查询接口，参数化的语句使用参数而不是将用户输入变量嵌入到SQL语句中。当前几乎所有的数据库系统都提供了参数化SQL语句执行接口，使用此接口可以非常有效的防止SQL注入攻击。
2、对进入数据库的特殊字符（’ ” <>&*;等）进行转义处理，或编码转换。

增值服务 / 网站监测服务

云端对您互联网网站（ - ）进行7*24持续监测，本季度暂未发生网站篡改和网站不可用性事件，暂未发现公网web漏洞。



未闭环网站监测清单			
URL	风险数量	风险类型	未闭环原因

其他运营工作 / 勒索风险排查

深信服安全研究团队基于多年勒索事件的实践经验，对500+个勒索样本及其变种进行分析，编制了94个勒索风险检查的Checklist，包含漏洞类、高风险端口类、弱口令类、攻击行为类、安全策略类等。本季度进行勒索预防风险排查的结果如下：

- 漏洞类勒索风险检查项 **X** 个；
- 高风险端口开放类勒索风险检查项 **X** 个；
- 弱口令类勒索风险检查项 **X** 个；
- 攻击行为类勒索风险检查项 **X** 个；
- 策略类勒索风险检查项 **X** 个；

其他运营工作 / 勒索风险排查

深信服安全研究团队基于多年勒索事件的实践经验，对500+个勒索样本及其变种进行分析，编制了94个勒索风险检查的Checklist，包含漏洞类、高风险端口类、弱口令类、攻击行为类、安全策略类等。本季度进行勒索预防风险排查的结果如下：

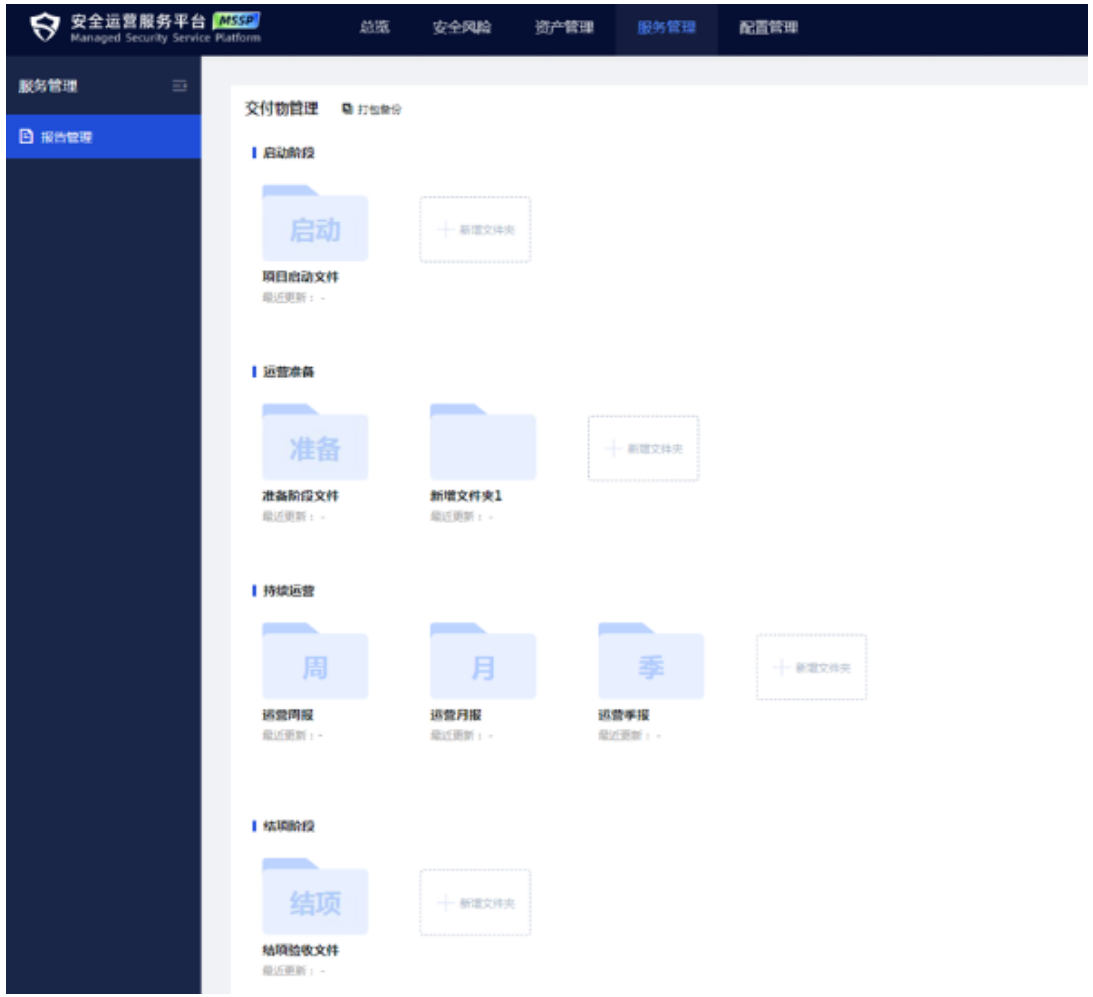
勒索排查清单				
排查类型	排查数量	风险个数	修复个数	修复率
漏洞	100	5	5	100%
端口	100	4	3	75%
策略	100	6	6	100%
弱口令	100	2	1	50%
攻击监测	100	0	0	100%

未闭环勒索排查清单				
排查类型	排查数量	漏洞名称	漏洞级别	未闭环原因
漏洞	xxx.xxx.xxx.xxx (HIS系统)	永恒之蓝	高危	xx
端口	xxx.xxx.xxx.xxx (HIS系统)	445	高危	xx
策略	xxx.xxx.xxx.xxx (LIS系统)	3389	高危	xx
弱口令	xxx.xxx.xxx.xxx (出口防火墙)	勒索防护策略未开启	高危	xx
攻击监测	xxx.xxx.xxx.xxx (HIS系统)	SSH	高危	xx

运营工作交付物汇总

安全运营项目交付物

交付物	《安全运营周报》	X份
	《安全运营月度报告》	X份
	《安全运营季度报告》	X份
	《最新安全威胁通告》	X份
	《首次安全威胁分析报告》	X份
	《服务资产信息确认表》	X份
	《服务资产安全漏洞评估报告》	X份
	《XX期间网络安全保障工作简报》	X份



谢谢聆听