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。

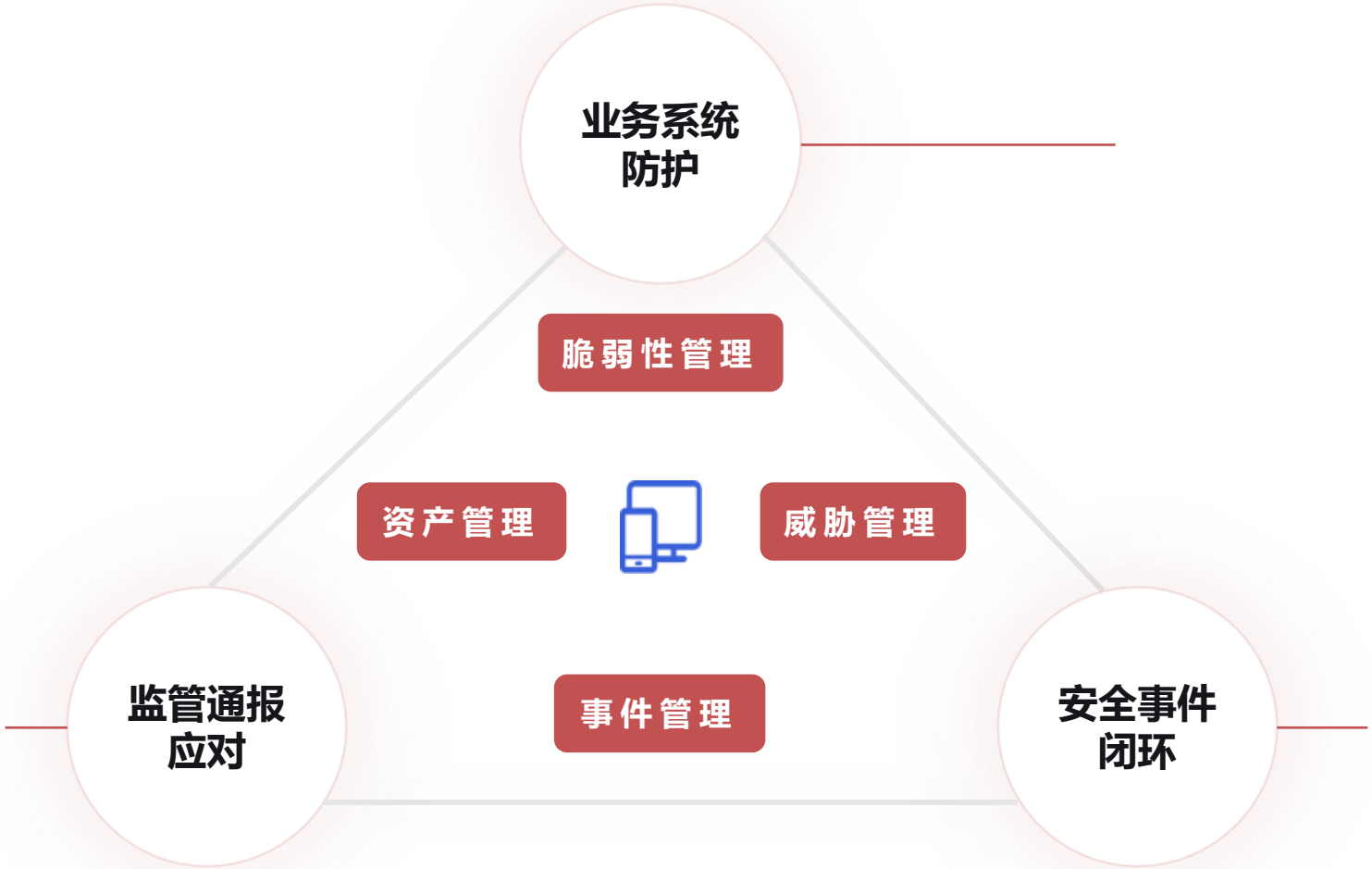
3.针对安全事件类通报预防工作：终端侧部署终端管理管理杀软，边界侧部署防火墙阻断行为，对发现的安全事件以及异常情况进行及时处置。

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。


业务系统
防护
脆弱性管理
资产管理
威胁管理
事件管理
监管通报
应对
安全事件
闭环

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。

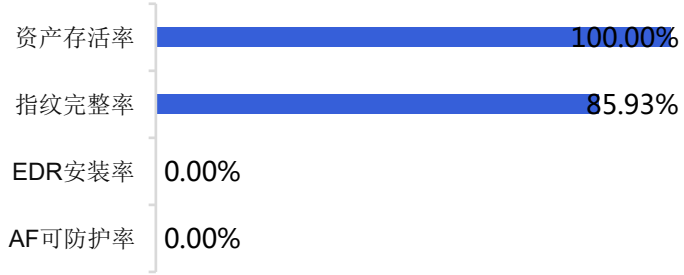
六、其他工作：

- 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。

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。

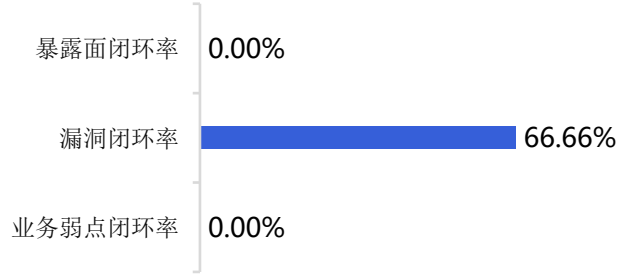
资产管理 46.48分



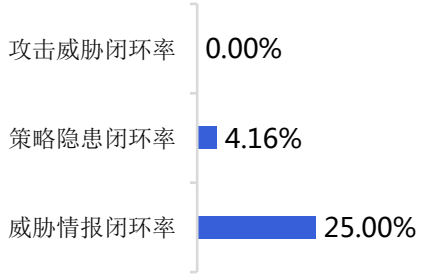
总体安全状态

30.46分

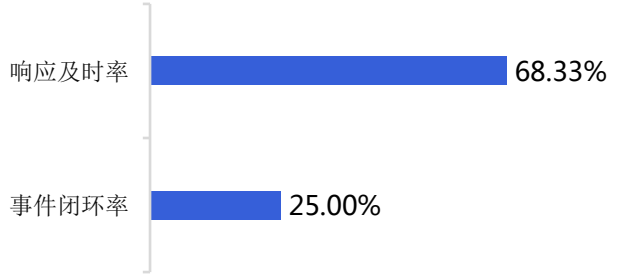
脆弱性管理 19.99分



威胁管理 8.74分



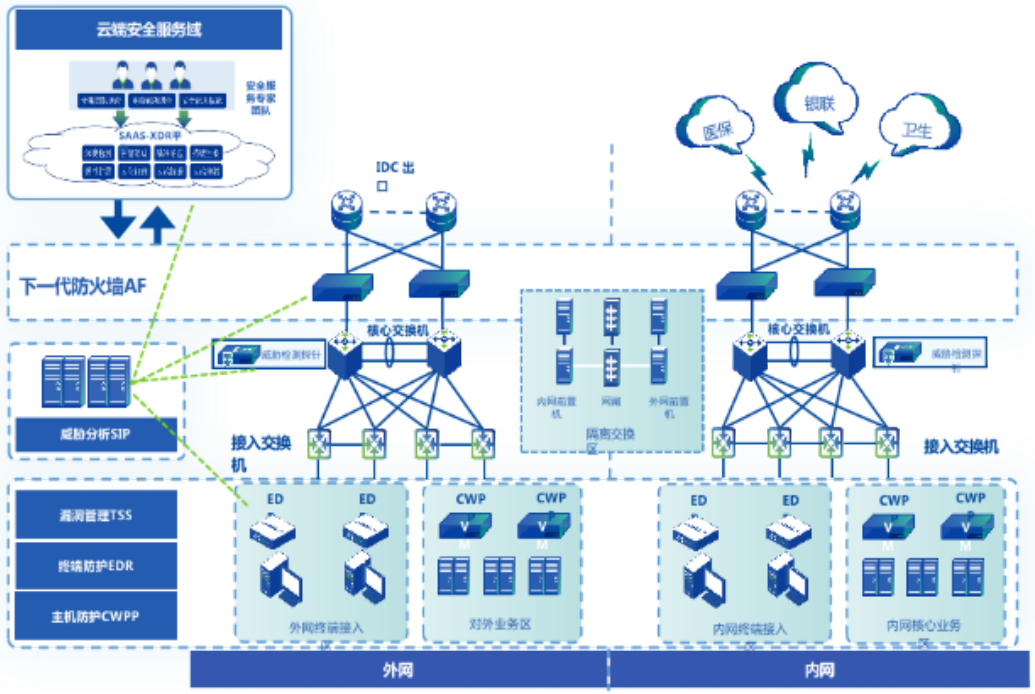
事件管理 46.66分



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。

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：

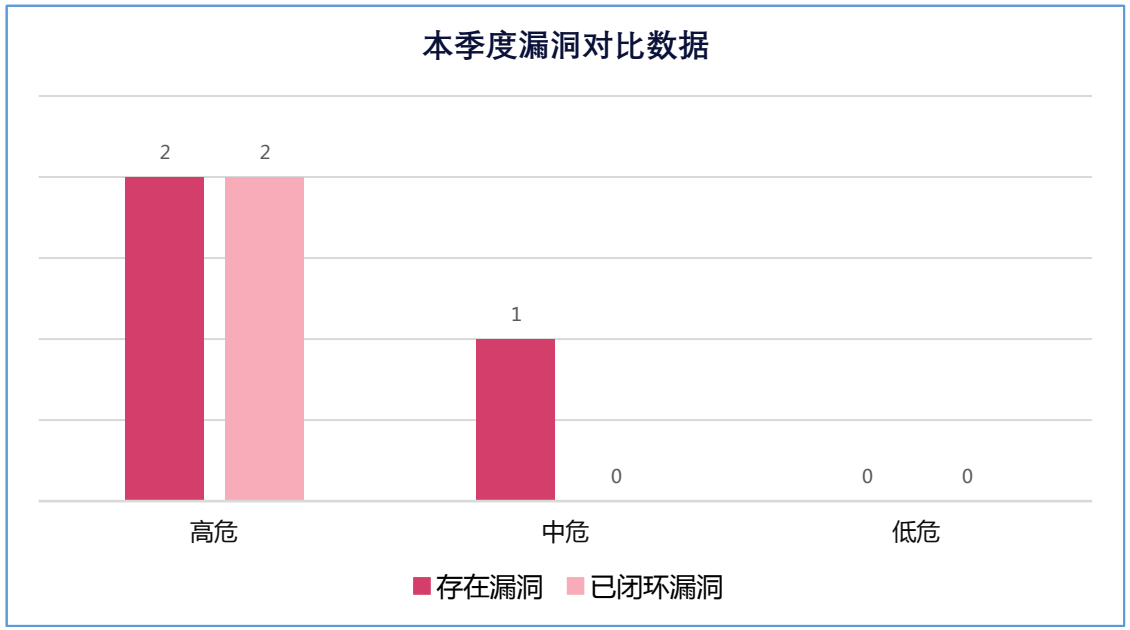
- 高危 **2** 个（高可利用漏洞 **2** 个），中危 **1** 个，低危 **0** 个；
- 服务内资产发现的漏洞较上季度增加 **3** 个;

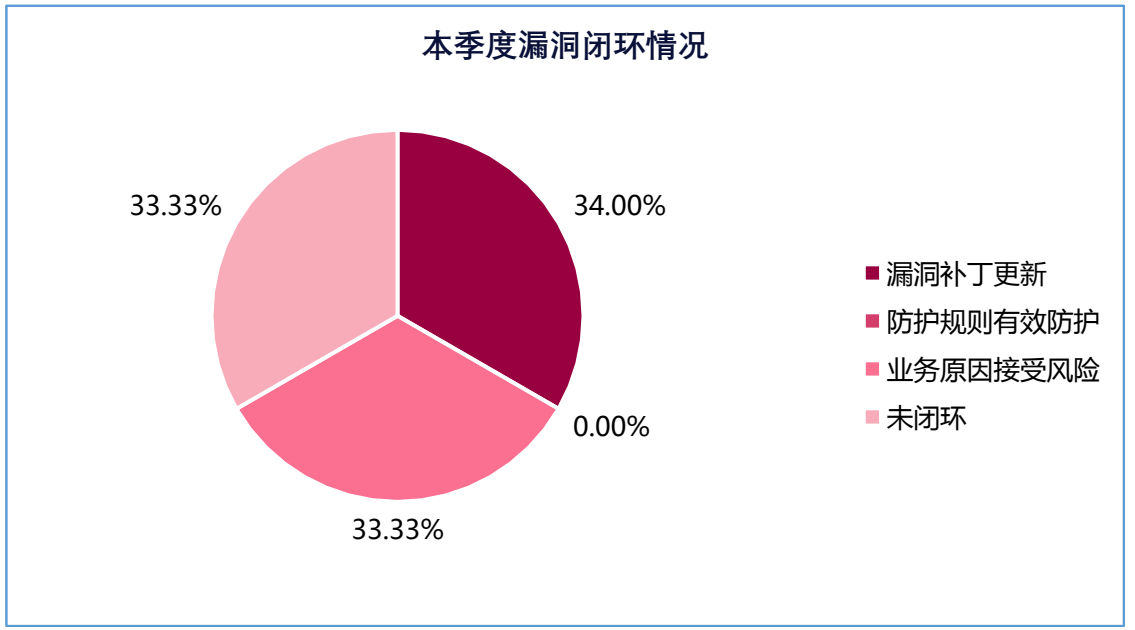
目前已闭环漏洞 **2** 个，其中：

- 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。

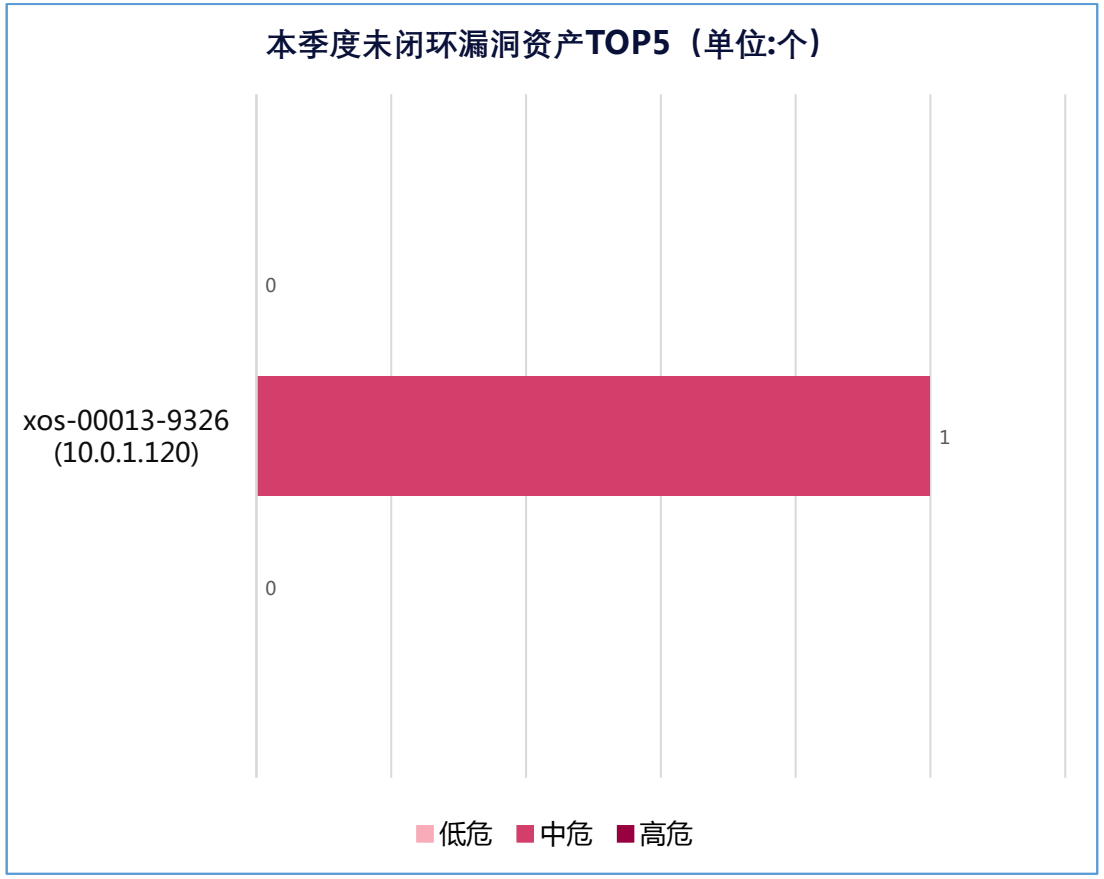




脆弱性管理 / 未闭环漏洞

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

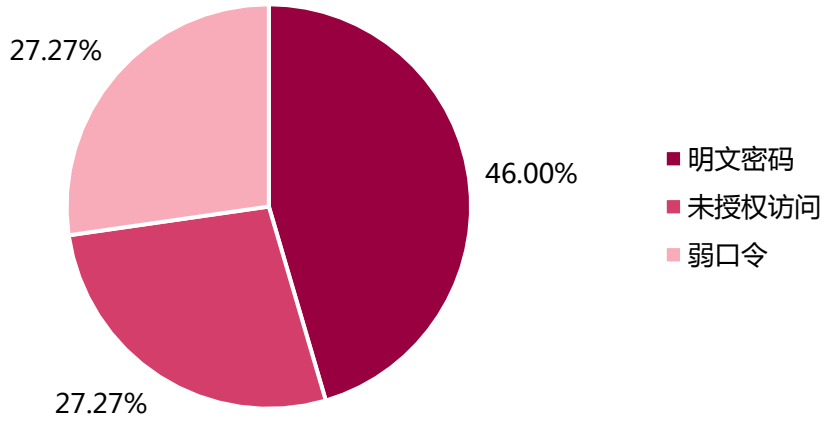
本季度服务内资产存在业务弱点 **11** 个（新增 8 个；历史未闭环 3 个），其中弱口令类型 **3** 个，其他脆弱性 **8** 个；

- 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**。

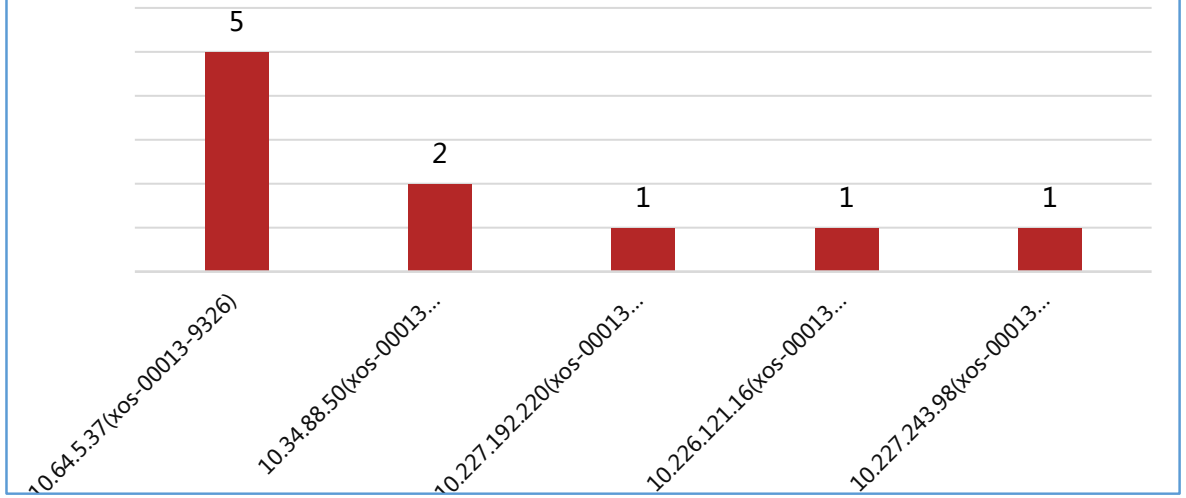
★ **服务价值：**

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。

威胁管理 / 外部威胁

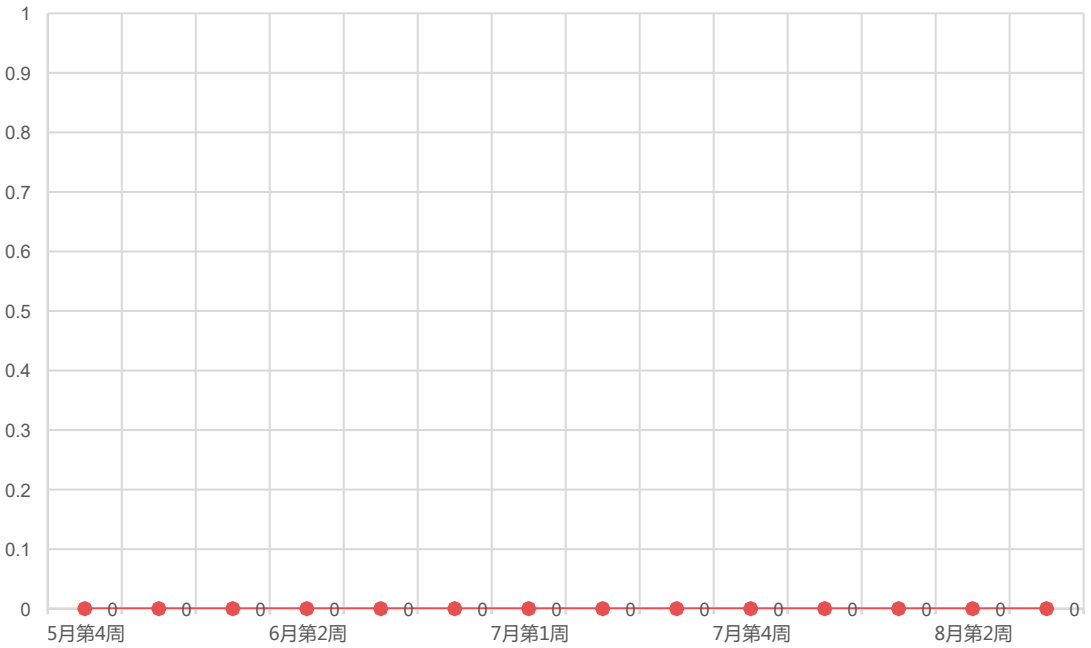
本季度运营中心通过服务组件日志分析，贵单位遭受外部攻击总次数达 **0** 次，平均每周捕获网络攻击 **0** 次。

- 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）。

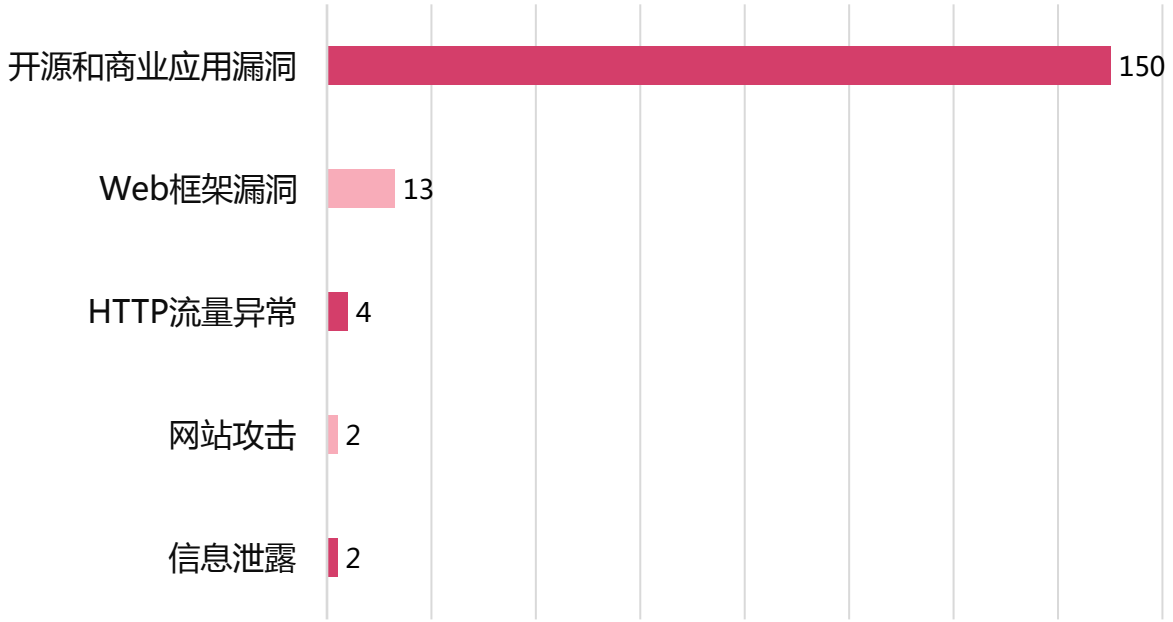
★ **服务价值：**

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 / 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）；

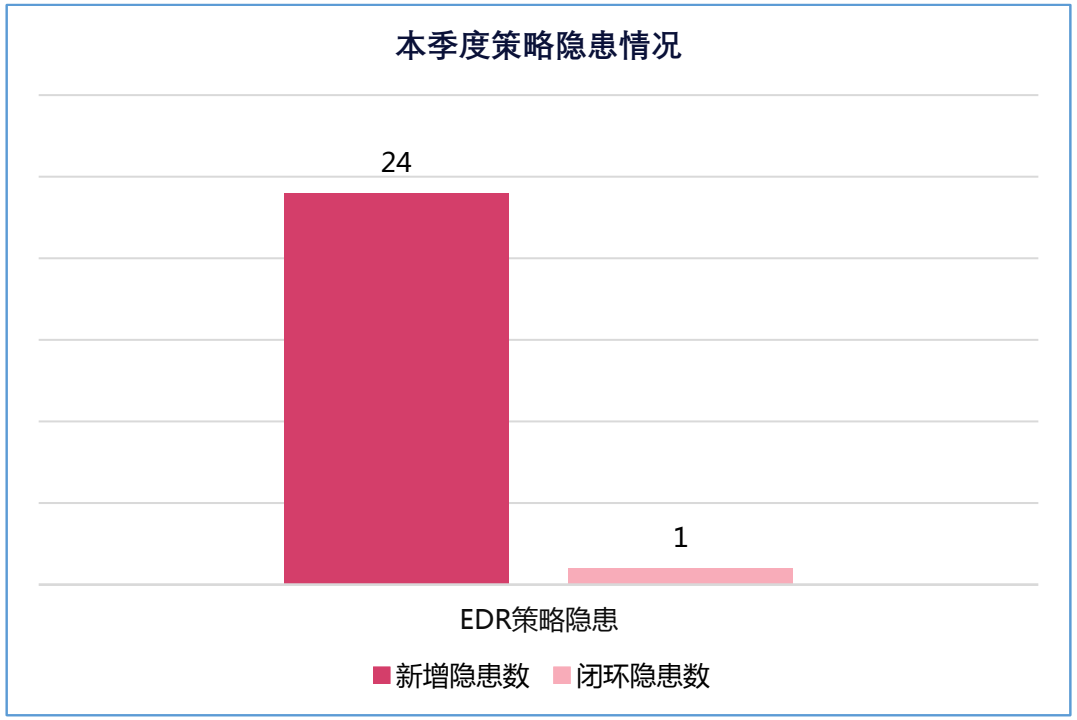
本季度共进行安全组件策略检查 **3** 次，共新增策略隐患 **24** 个，其中：

- 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

事件管理 / 整体概况

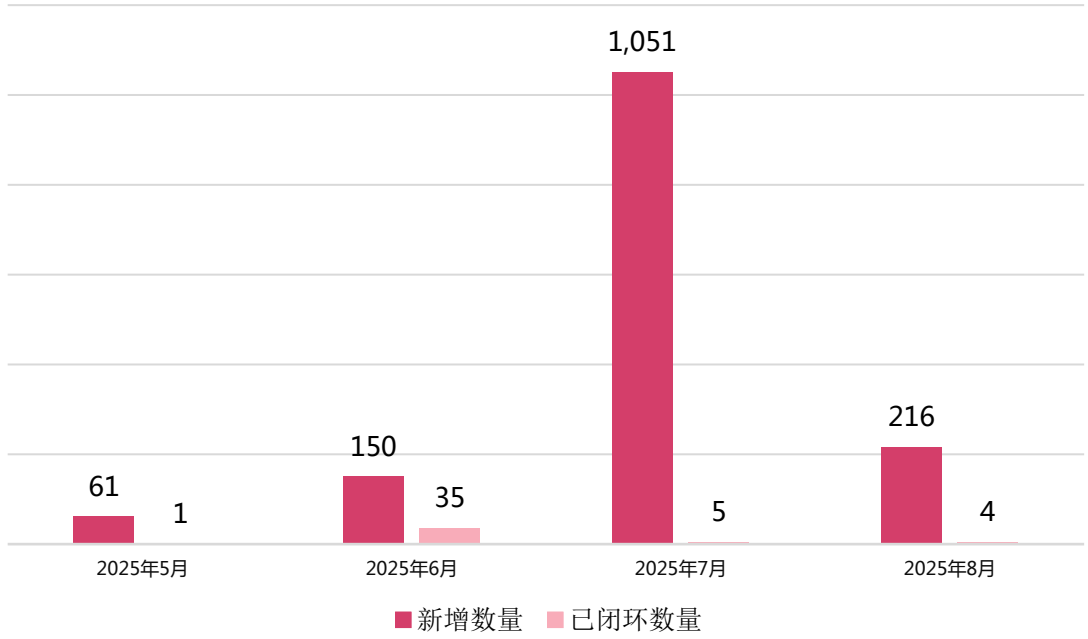
本季度新增安全事件 **180** 起，已针对全部失陷主机提供了处置方法、工具和远程协助，截止目前为止已闭环安全事件 **45** 起，闭环率 **25.0** %：

- 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。

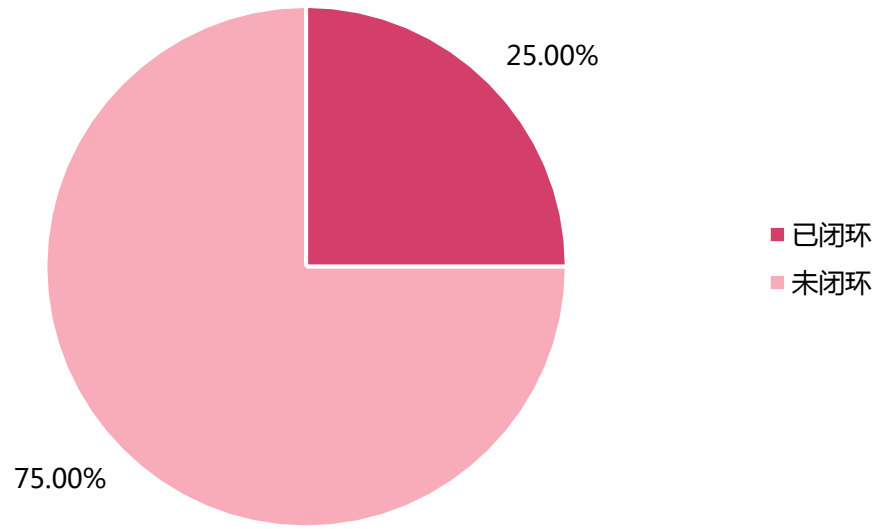
★ 服务价值：

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

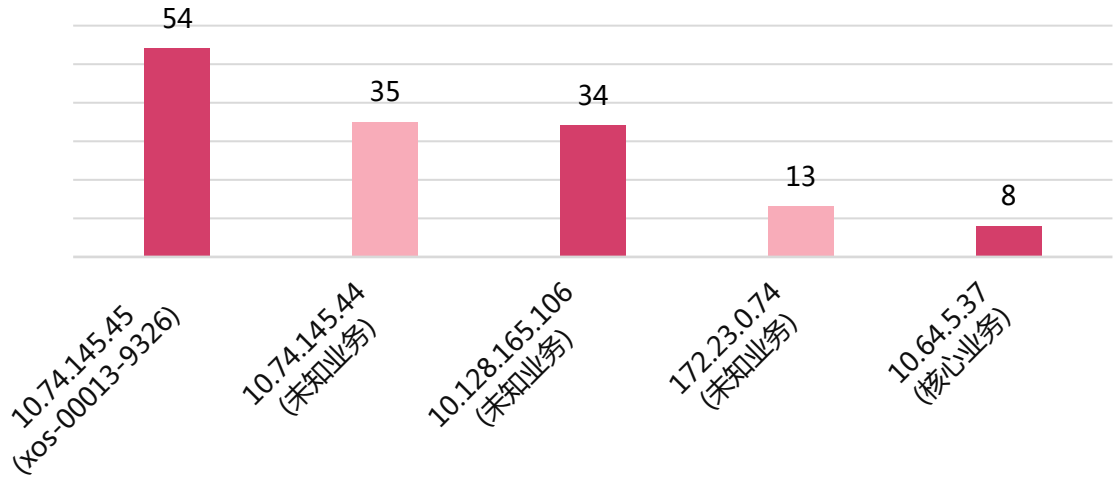
本季度发生的安全事件中：

- 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；

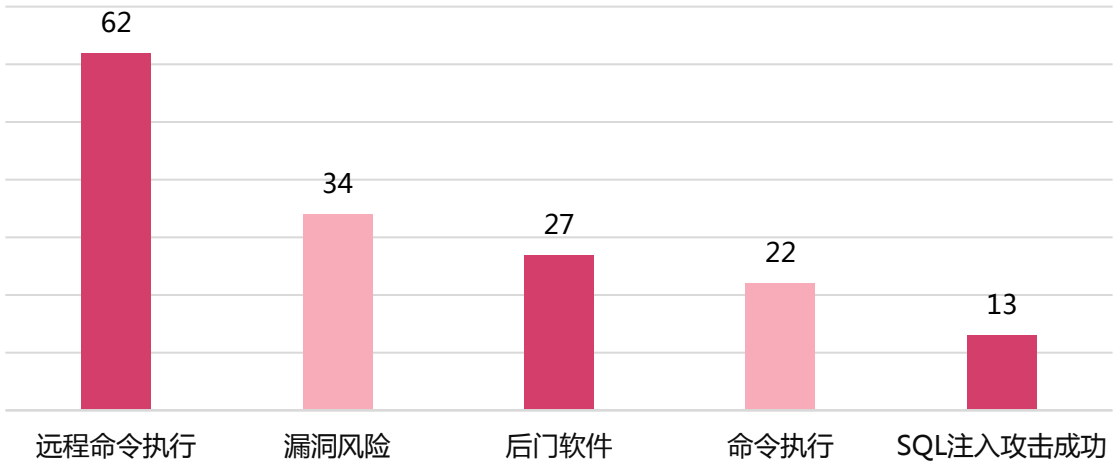
★ 服务价值：

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）

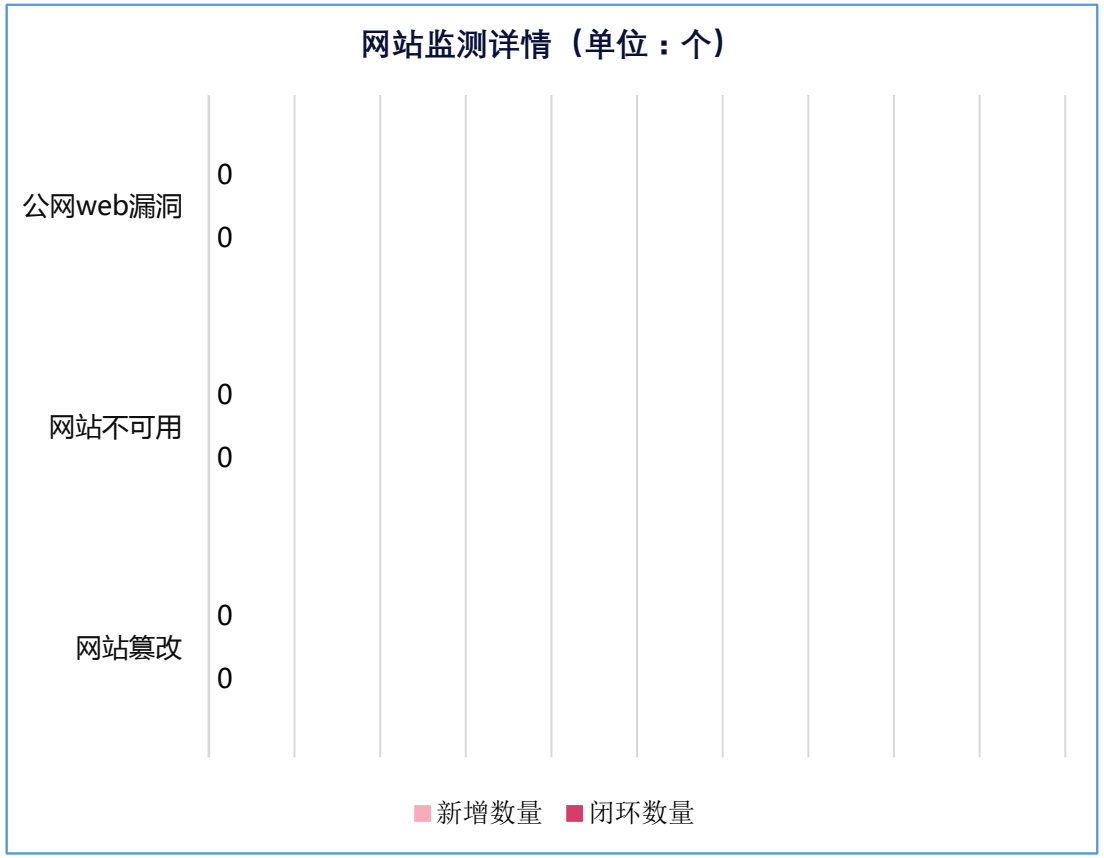
1.对于内网病毒失陷主机建议安装深信服EDR对其进行病毒查杀，隔离病毒文件。

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。

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

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