**北京沃丰时代数据科技有限公司**

**安全事件及漏洞管理规范**

**文档信息：**

|  |  |  |  |
| --- | --- | --- | --- |
| **文档名称** | **安全事件及漏洞管理规范** | | |
| **文档编号** | WF-DM009 | | |
| **文档密级** | 内部 | **发布范围** | 公司内部 |
| **编制人** | 韦昭 | **编制日期** | 2022-02-11 |
| **评审人** | 周毅 | **评审日期** | 2023-03-23 |
| **批准人** | 张磊 | **批准日期** | 2023-04-23 |

**修订历史记录：**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 版本 | 状态 | 修订内容说明 | 编制人 | 日期 |
| V1.0 | 新建 | 新增 | 韦昭 | 2018-12-11 |
| V1.1 | 修订 | 合并事件管理 | 韦昭 | 2020-04-20 |
| V1.2 | 修订 | 添加范例及格式调整 | 韦昭 | 2022-01-20 |
| V1.3 | 修订 | 添加合作商时间处理要求 | 韦昭 | 2022-02-11 |
| V1.4 | 修订 | 修订文档信息 | 张帆 | 2023-04-23 |

目录

[1 概述 3](#_Toc95847922)

[1.1 文档目的 3](#_Toc95847923)

[1.2 术语 3](#_Toc95847924)

[2 适用范围 4](#_Toc95847925)

[3 事件发现 4](#_Toc95847926)

[4 事件报告 5](#_Toc95847927)

[5 事件评估 6](#_Toc95847928)

[5.1 事件评估 6](#_Toc95847929)

[5.2 漏洞评估 8](#_Toc95847930)

[6 事件处理 10](#_Toc95847931)

[7 修复验证 12](#_Toc95847932)

[8 整理归档 13](#_Toc95847933)

[附录1 《应急响应模板》 13](#_Toc95847934)

[1.  准备(Preparation) 13](#_Toc95847935)

[2. 诊断分析(Detection) 13](#_Toc95847936)

[问题来源 13](#_Toc95847937)

[分析过程 14](#_Toc95847938)

[结论 14](#_Toc95847939)

[3. 抑制(Containment) 14](#_Toc95847940)

[4. 清除(Eradication) 15](#_Toc95847941)

[5. 恢复(Recovery) 15](#_Toc95847942)

[6. 跟踪(Follow-up) 15](#_Toc95847943)

[附录2 《应用漏洞信息持续监控办法》 17](#_Toc95847944)

[附录3 《用户异常行为监控办法》 23](#_Toc95847945)

[附录4 《合作商处理时间特别要求》 25](#_Toc95847946)

# 概述

## 文档目的

为了更高效的处理应用安全事件，特制定《安全事件及漏洞管理规范》，用以指导安全事件和漏洞的发现、报告、评估、处理、修复验证及归档过程。

## 术语

**合作商户：购买沃丰时代产品的商户，也称合作商。**

**终端客户：合作商户的客户。**

**PDCERF应急响应模型:**应急响应模型，源于 [NIST SP800-61](https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final)，包括准备(Preparation) 诊断分析(Detection) 抑制(Containment) 清除(Eradication) 恢复(Recovery) 跟踪(Follow-up)**。**

**360补天:**国内知名安全厂商的漏洞报告和管理平台。网址：https://www.butian.net/

**国家信息安全漏洞共享平台： 基**于国家标准《信息安全技术信息安全漏洞管理规范》，由国家工信部组织的漏洞管理平台。网址：https://www.cnvd.org.cn/

**SonarQube:**SonarQube是一个开源的代码质量管理系统,支持代码质量和安全扫描。  官方主页：<https://www.sonarqube.org/>**。**

**dependency-check：**知名安全组织OWASP依赖扫描工具，用于发现项目中依赖包的公共漏洞。<https://owasp.org/www-project-dependency-check/>**。**

**华为漏洞扫描服务（华为VSS**）**：**漏洞扫描服务（Vulnerability Scan Service，简称VSS）是针对网站、主机、软件包/固件、移动应用进行漏洞扫描的一种安全检测服务，目前提供通用漏洞检测、漏洞生命周期管理、自定义扫描多项服务。扫描成功后，提供扫描报告详情，用于查看漏洞明细、修复建议等信息。 帮助文档详见：<https://support.huaweicloud.com/productdesc-vss/vss_01_0009.html>**。**

**阿里DDOS防护：**DDoS高防（Anti-DDoS）是阿里云提供的DDoS攻击代理防护服务。当您的互联网服务器遭受大流量的DDoS攻击时，DDoS高防可以保护其应用服务持续可用。帮助文档详见：**<https://help.aliyun.com/document_detail/153308.html>**

**阿里Web应用防火墙（WAF）：**阿里云提供的web应用防火墙服务。WAF可以有效识别Web业务流量的恶意特征，在对流量进行清洗和过滤后，将正常、安全的流量返回给服务器，避免网站服务器被恶意入侵导致服务器性能异常等问题，保障网站的业务安全和数据安全。帮助文档详见：<https://help.aliyun.com/document_detail/28517.html>

**阿里云态势感知服务：**也叫云安全中心，是一个实时识别、分析、预警安全威胁的统一安全管理系统，通过防勒索、防病毒、防篡改、合规检查等安全能力，实现威胁检测、告警响应、攻击溯源的自动化安全运营闭环，保护您的云上资产和本地服务器安全，并满足监管合规要求。文档详见：<https://help.aliyun.com/product/28498.html>

**Teambition** :是阿里巴巴旗下团队协作工具，以项目和任务的可视化管理来支撑企业团队协作，适合产品、研发、设计、市场、运营、销售、HR 等各类团队。

https://www.teambition.com/

# 适用范围

规范适用于公司技术部对外提供服务的应用系统，适用于研发部。

# 事件发现

应用安全漏洞的发现来自于以下渠道:

1 来自第三方或合作商户安全团队渗透测试报告；

2 来自内部安全、测试或开发人员发现的系统或组件漏洞；

3 来自漏洞平台如360补天或国家信息安全漏洞共享平台；

4 来自互联网安全厂商和CVE公告；

安全工程师负责处理来自以上渠道的漏洞信息，编写事件报告。

# 事件报告

事件报告包括报告漏洞的方法，同时规定了漏洞报告的格式和内容。

事件报告可以包括0个或多个漏洞。

#### 使用商户/第三方向我司报告漏洞

1）通过商务接口人向沃丰时代报告漏洞；

2）通过 沃丰时代官方客服系统 <https://udesk.udesk.cn> 向沃丰时代提交工单 ；

3）可提交 360 补天平台 <https://www.butian.net/>  国家信息安全漏洞共享平台 <https://www.cnvd.org.cn/> 指明厂商名称: 北京沃丰时代数据科技有限公司；

4）直接向沃丰时代安全负责人 周毅 报告邮箱 [security@udesk.cn](mailto:security@udesk.cn), [zhouyi@udesk.cn](mailto:zhouyi@udesk.cn) 18686471019。

#### 公司内部

1）企业微信 @周毅

2）邮件 zhouyi@udesk.cn, [security@udesk.cn](mailto:security@udesk.cn), @周毅

3) 电话 周毅 18686471019

#### 报告格式和内容

对于发现的漏洞，安全工程师必须编写详细的文档纪录，内容包括但不限于：

1 漏洞简明标题，标题相当包含影响，如 "XXX系统XXX漏洞" ，多个漏洞为 《xx系统渗透测试报告》或 《xx系统安全评估》  
2 漏洞对应的应用域名和负责人   
3 漏洞证据： 相关 URL 漏洞利用的详细POC和截图   
4 漏洞风险评估：会造成的危害说明   
5 漏洞修复建议

# 事件评估

本章规定对安全事件的整体评估和对事件涉及的每个漏洞的风险评估标准。

## 事件评估

分为五级

* 特别重大事件（1 级）

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：

a) 会使特别重要信息系统遭受特别严重的系统损失；

b) 产生特别重大的社会影响。

解读：公司部门中心的基础设施网络、重要信息系统（A类I类系统）、核心网站（如官网、管理后台）瘫痪，导致长时间业务中断，直接导致巨大经济损失的事件；绝密和机密数据（数据库或客户资料）被泄露导致大范围社会传播事件，严重影响公司声誉；对外发布公司内部机密信息、大范围传播损害公司形象利益的言论等事件，直接影响公司投资者关系或者上市进程或者公司股价等事件

* 重大事件（2级）

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：

a) 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；

b) 产生的重大的社会影响。

解读：公司部门中心的基础设施网络、重要信息系统（A类I类系统）、核心网站（如官网、管理后台）瘫痪，导致业务中断，造成严重影响或经济损失的事件；绝密和机密数据（数据库或客户资料）遭受非法访问或传播事件；未经授权对外发布公司内部机密信息、大范围传播损害公司形象利益的言论等事件。

* 较大事件（3级）

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：

a) 会使特别重要信息系统遭受较大的系统损失、或使重要信息系统遭受严重的系统损失、一般信息信息系统遭受特别严重的系统损失；

b) 产生较大的社会影响。

解读：公司信息系统、网站、部门范围内的网络通信或者应用系统受到影响，并关系到业务正常运行的事件和用户系统账户被非法使用，遭受非法访问和泄密、传播损害公司形象利益的言论等事件，但是这些事件仅出现社会舆论小范围报告，没有给公司带来实际的损失和影响的事件。

* 一般事件（4级）

一般事件是指不满足以上条件的信息安全事件，包括以下情况：

a) 会使特别重要信息系统遭受较小的系统损失、或使重要信息系统遭受较大的系统损失，一般信息系统遭受严重或严重以下级别的系统损失；

b) 产生一般的社会影响。

解读：公司内小范围出现的网络延时或故障，信息系统功能缺陷或者短暂不可用，导致个别用户或者业务受影响等技术层面的事件，或部分员工无意识的违反信息安全规定等管理层面的事件，但是这些事件没有给公司带来实际的损失和影响的事件。

* 咨询事件（5级）

当确认事件无风险，不需要做任何处理，则认为是咨询事件

## 漏洞评估

事件可以包含0个或多个漏洞。

漏洞文档编写完成后，由公司安全工程师、项目负责人组织内部召开小型会议评定漏洞级别，确定每个问题的优先级。

根据漏洞危害程度分为严重、高危、中危、低危、忽略五个等级，每个等级涵盖的漏洞以及评分标准如下:

#### 严重:

分值 9~10 分，本等级包括:

1、直接获取系统权限(服务器端权限、客户端权限)的漏洞。包括但不仅限于命令注入、远程命令执行、SQL 注⼊入获取系统权限、缓冲区溢出(包括可利⽤用的 ActiveX 缓冲区溢出)。

2、直接导致拒绝服务的漏洞。包括通过该远程拒绝服务漏洞直接导致线上应⽤用系统、⺴⽹网络设备、服务器⽆无法继续提供服务的漏洞。

3、严重的逻辑设计缺陷。包括但不仅限于任意账号登录、任意账号密码修改、任意账号资⾦金消费、订单遍历、交易⽀支付⽅方⾯面的严重问题。

4、严重级别的信息泄漏 。包括但不限于重要 DB 的 SQL 注⼊入漏洞、包含配置信息等敏感信息的源代码压缩包泄漏、包含订单、⽤用户信息的⽇日志⽂文件;

5、严重的登录及验证安全⻛风险。包括但不仅限于源代码压缩包泄漏;

#### 高危:

分值 6~8 分，本等级包括:

1、越权访问。包括但不仅限于绕过认证直接访问管理后台可操作、核心业务⾮非授权访问、核心业务后台弱密码等。

2、能直接盗取关键业务等用户身份信息的漏洞。包括:重点页面的存储型XSS 漏洞、普通系统的 SQL注⼊入漏洞。

3、⾼风险的逻辑设计缺陷。包括但不仅限于查看任意用户信息、修改相关状态等。

3、⾼风险的信息泄漏漏洞。包括但不限于普通源代码压缩包泄漏、配置信息泄露;

4、可获取客户端权限的漏洞。包括但不限于远程任意命令执⾏行、远程缓冲区溢出及其它逻辑问题导致的客户端漏洞；

#### 中危:

分值 3~5 分，本等级包括:

1、普通信息泄露。包括但不仅限于客户端明⽂文密码存储。

2、有条件利用：需交互才能获取用户身份信息的漏洞。包括但不限于反射型 XSS、JSON Hijacking、重要操作的CSRF、普通业务的存储型 XSS。

#### 低危:

分值 1~2 分，本等级包括:

1、轻微信息泄露。包括但不仅限于路径信息泄露、git信息泄露、异常信息泄露。

2、URL 跳转。

3、利用条件苛刻。如必须在内网、绕过防火墙。

#### 无危害:

分值 0 分，本等级包括:

1、不涉及安全问题的 bug。包括但不仅限于产品功能缺陷、页面乱码、样式混乱。

2、无法利⽤用的漏洞。

3、不能重现的漏洞。包括安全团队确认⽆无法重现的漏洞。

4、纯属用户猜测的问题。

5、非公司业务漏洞。

# 事件处理

安全工程师在收到漏洞报告，对事件或漏洞风险进行初步评定后，进入应急响应处理流程，按 《[应急响应模板](file:///D:/pages/viewpage.action%3fpageId=49512722)》进行记录。文档名格式为 “日期 事件名称”

流程遵守应急响应 PDCERF 模型，即

1. 准备(Preparation)

安全工程师收集事件和漏洞信息（第4章《漏洞报告》）；

安全工程师召集相关负责人，人员包括: 外部联系人、安全工程师、项目负责人、运维人员及其它相干人；

安全工程师向相干人通报相关信息。

2. 诊断分析(Detection)

安全工程师记录包括本文档第5章 涉及每个漏洞评估、追踪、取证、POC过程所用到的信息来源、工具、命令和执行记录。

安全工程师初步对每个漏洞给出风险评估结果，并判断是否需要采取抑制措施；

安全工程师向项目负责人解释漏洞形成原理、POC、检测方法；

安全工程师和项目负责人确定解决方案和完成时间表；

如果有明确的合作商户，要通过外部联系人得到合作商户对漏洞评估结果、解决方案及时间进度的同意。

安全工程师和项目负责人对事件评估最终达成一致。

3. 抑制(Containment)

安全工程师描述怎么防止正在发生扩大或阻止可能发生的入侵，由项目负责人执行。

如暂停某个接口或服务、对应服务器加入网络隔离环境。

4. 清除(Eradication)

安全工程师要在保留必要证据和数据后，对病毒或是脏数据进行清除；

项目负责人负责对代码漏洞修复上线或是配置进行清除；

5. 恢复(Recovery)

项目负责人负责将业务重新上线，并恢复步骤3降级的服务；

安全工程师负责验证；

在确认完毕，通知相关人和合作商户。

6. 跟踪(Follow-up)

安全工程师整理事件归档；

安全工程师判断是否需要扩大排查范围以发现不明显的相关攻击；

安全工程师判断是否需要建立新的安全基线以阻止类似事件发生。

#### 表6.1 安全事件处理时间表

安全专家要在 1-3个工作日内回复合作商漏洞的评估和修复时间信息。

已被利用的漏洞必须在24小时内实施 本章 3. 抑制(Containment) 中的抑制方案。

当合作商有明确特别的时间处理要求和通知要求，记录在 附录4 《合作商处理时间特别要求》。

|  |  |  |  |
| --- | --- | --- | --- |
| 漏 洞 等 级 | 修 复 时 间 | 修复方式 | 逾期未修复处理方式 |
| 严 重 | 7-14 天 | 1、安全设备 拦截;  2、代 码修复 | 1、关闭域名解析，禁用NAT;2、停止服务; |
| 高 危 | 14-30 天 | 1、安全设备 拦截;  2、代 码修复 | 1、关闭域名解析，禁用NAT;2、停止服务; |
| 中 危 | 1-3 个月 | 1、安全设备 拦截;  2、代 码修复 | 1、项目负责人说明未修复原因和后期处理方案，抄送 安全委员会，信息安全专员记录在案，到期追踪处理结果; |
| 低 危 | 4-12 个月 | 1、安全设备 拦截;  2、代 码修复 | 1、项目负责人说明未修复原因和后期处理方案，抄送 安全委员会，信息安全专员记录在案，到期追踪处理结果; |
| 无 危 害 |  |  |  |

安全事件产生的漏洞修复任务，由安全人员使用公司teambition 进行任务跟踪和管理，确保修复任务被按期完成和及时验证。



整改任务由项目负责人通过WF-DM003文档变更管理流程部署到线上。

# 修复验证

修复结果验证由安全工程师在到达指定修复期限或负责人明确上线后，通过安全工具或手工验证是否修复，记录到《应急响应记录》中，并通知相关人。

1.验证方式和结果；

2.针对漏洞逾期未修复的处理方式。

# 整理归档

安全工程师整理《应急响应记录》和关联的《漏洞报告》并保存到安全组Wiki文档中。

# 附录[1 《应急响应模板](file:///D:/pages/viewpage.action%3fpageId=49512722)》

本文档遵守 应急响应 PDCERF 模型 已经形成固定预案的见 [应急响应方案](file:////pages/viewpage.action%3fpageId=63899298)

|  |  |
| --- | --- |
| **描述** |  |
| **总结** |  |
| **等级** | [事件分级](file:////pages/viewpage.action%3fpageId=49512726) |
| **人员** |  |

## 1.  准备(Preparation)

主要描述参与人员及角色

|  |  |
| --- | --- |
| **角色** | **人员** |
| 外部联系人 |  |
| 安全人员 |  |
| 项目负责人 |  |
|  |  |

其它工具：

## 2. 诊断分析(Detection)

### 问题来源

描述问题来源，包括如下几个要素

|  |  |  |
| --- | --- | --- |
| **要素** | **描述** | **备注** |
| 人（谁第一个发现） |  |  |
| 哪里（区，主机，ip或客户） |  |  |
| 企业微信群 |  |  |
| 时间范围 |  |  |

#### 漏洞列表

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **编号** | **漏洞标题** | **复现方法** | **负责人** | **风险评估** | **分析** | **解决方案** | **上线时间** |
| 1 |  |  |  |  |  |  |  |

### 分析过程

注意：应当包括评估、追踪、取证、POC等过程所用的信息、工具、命令和执行记录。

1. 保留现场证据以提供以后取证用,可以是截图，最好是当时的日志文件（附件上传）

2. 需要保留对现场的操作

### 结论

处理的决策和结果

风险等级和结果要同步到文档首部表中

## 3. 抑制(Containment)

采取抑制措施 防止正在发生的损害扩大或阻止可能发生的入侵

抑制措施要尽量减少线上损失

抑制措施可能包括对服务进行降级和停止

## 4. 清除(Eradication)

保留必要数据，对病毒或是脏数据进行清除

## 5. 恢复(Recovery)

确保修复方案上线，包括发布新版本

验证上线修复方案正确处理了

对降级或停止的服务进行恢复

## 6. 跟踪(Follow-up)

扩大排查范围以发现类似或不明显的攻击

是否需要建立新基线防止问题或类似问题再次发生

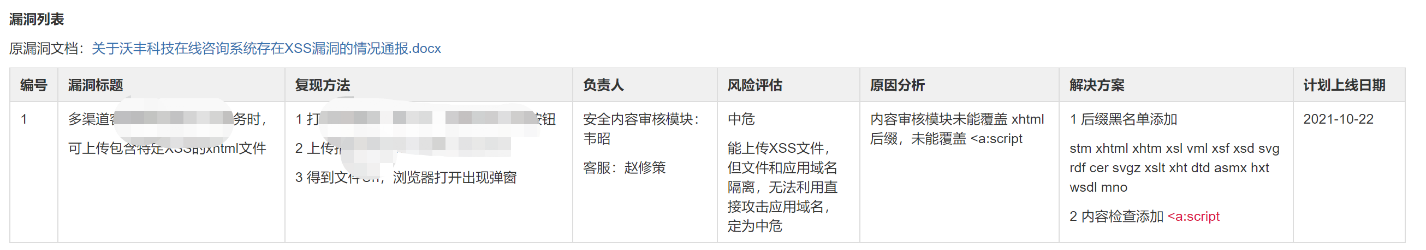
是否需要分配任务使系统更完善

整理归档

#### 应急响应记录示例



#### 应急响应记录示例



#### 应急响应记录示例



#### 安全事件任务上线记录显示



# 附录2 《应用漏洞信息持续监控办法》

1  订阅权威公共漏洞管理中心，包括 [nvd.nist.gov](http://nvd.nist.gov/) 中国国家信息安全漏洞[www.cnnvd.org.cn](http://www.cnnvd.org.cn) 阿里云态势感知服务漏洞管理等平台的漏洞报警，同时结合自身项目使用情况，对CVE公共漏洞进行评估和处理，填写：《[公共CVE风险评估](file:///D:/pages/viewpage.action%3fpageId=143425897) 》。每周巡检的记录和统计，在安全周报中通报。

2  每天定时使用 SonarQube + dependency-check 持续对项目代码变更进行扫描，确保及时发现新的CVE和代码漏洞。

3  每月使用华为漏洞扫描服务（华为VSS）等工具进行运行时扫描，以确保部署的应用漏洞能及时发现。安全人员对扫描结果进行分析并记录《系统动态扫描巡检》，如有新的漏洞被确认，启动事件处理流程。

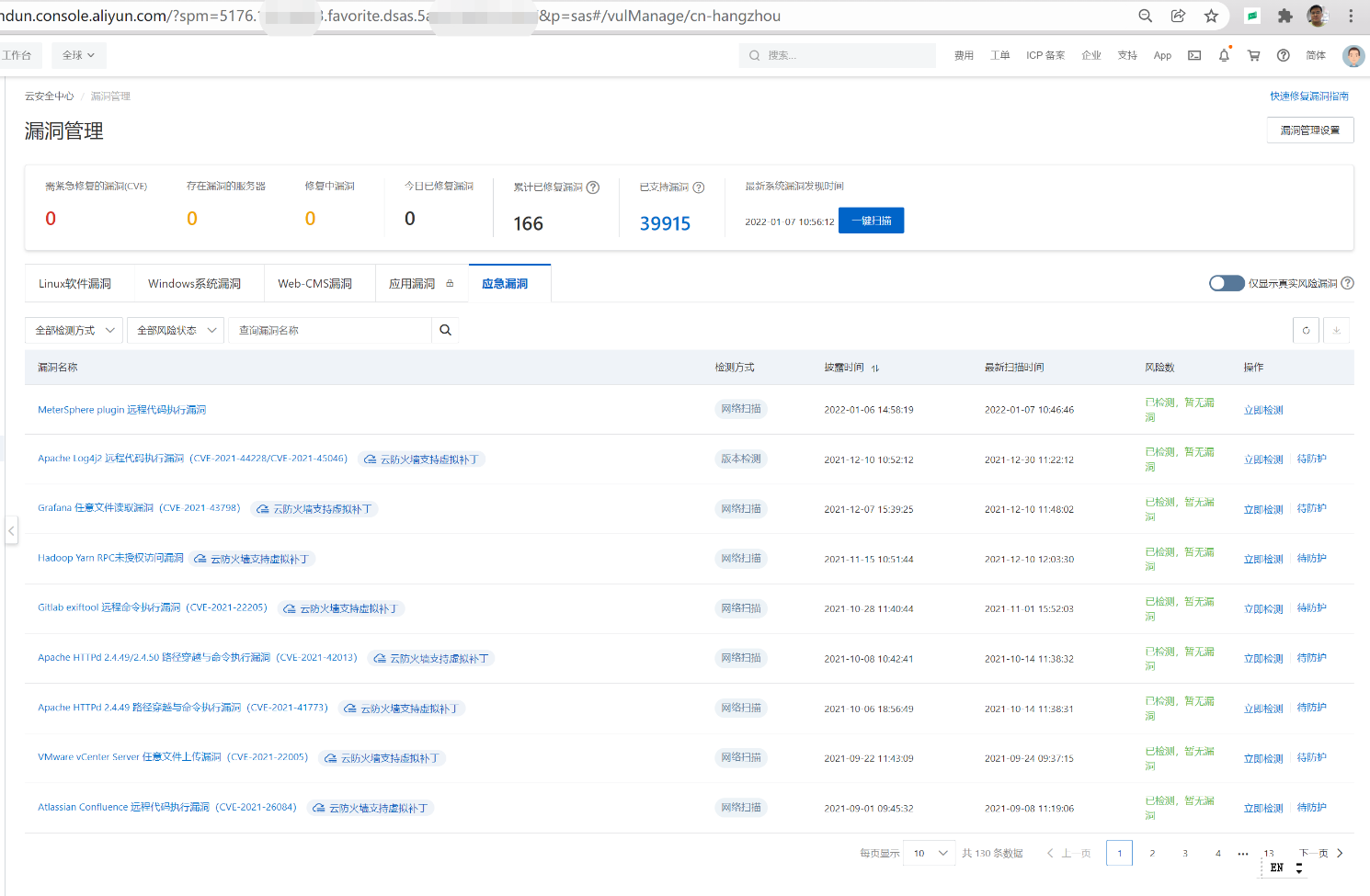
4  合作商户选择自己信任的第三方对对应我司服务进行第三方渗透测试，需向我方报备相关范围、时间和测试来源ip。

**阿里云态势感知服务漏洞管理服务**:

可以帮助我们扫描和发现部署在阿里云主机中的应用、系统等是否有漏洞。

安全工程师在收到相关漏洞后，点击“立即检测”进行检测。

帮助文档详见：<https://help.aliyun.com/document_detail/142154.html>



当发现漏洞时，阿里云显示相关漏洞的文件和主机



公共CVE风险评估示例：



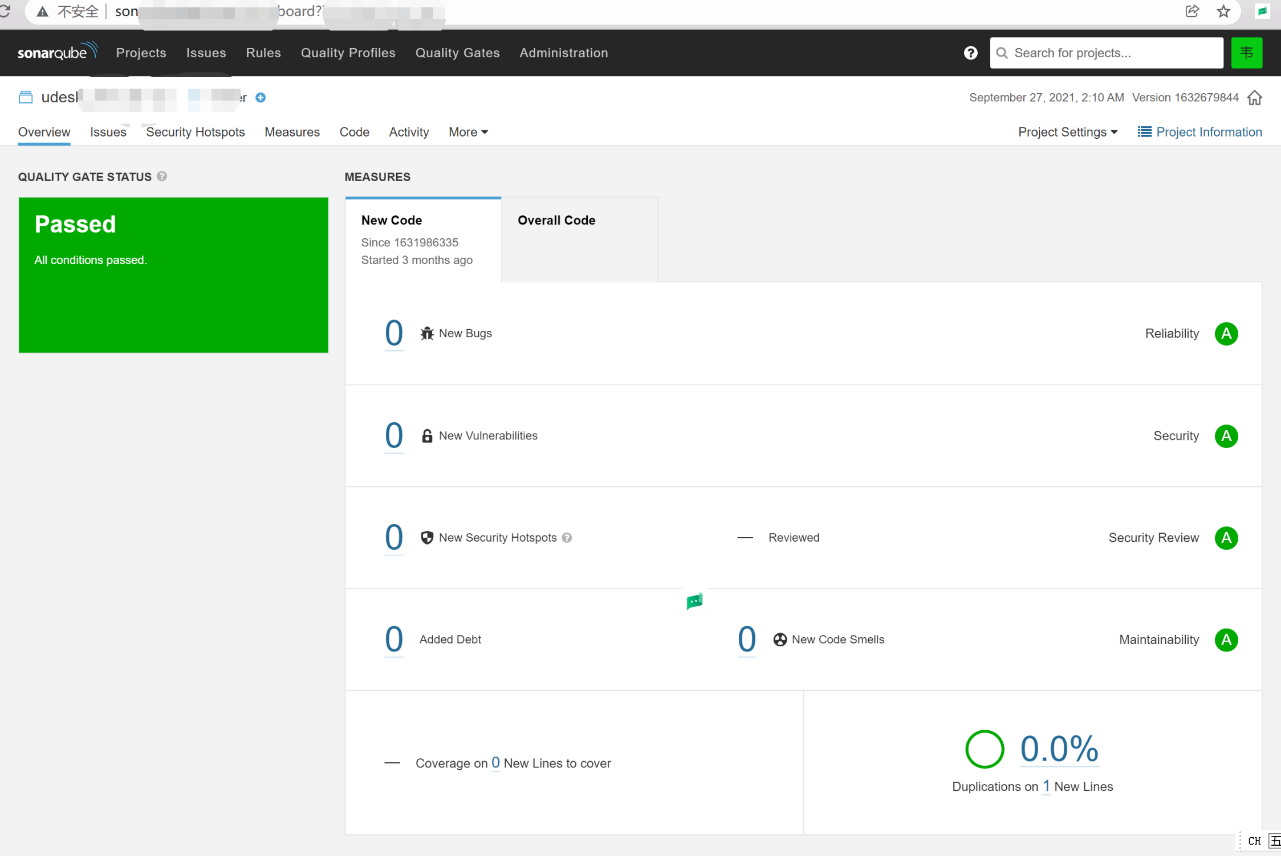
**安全周报示例**：





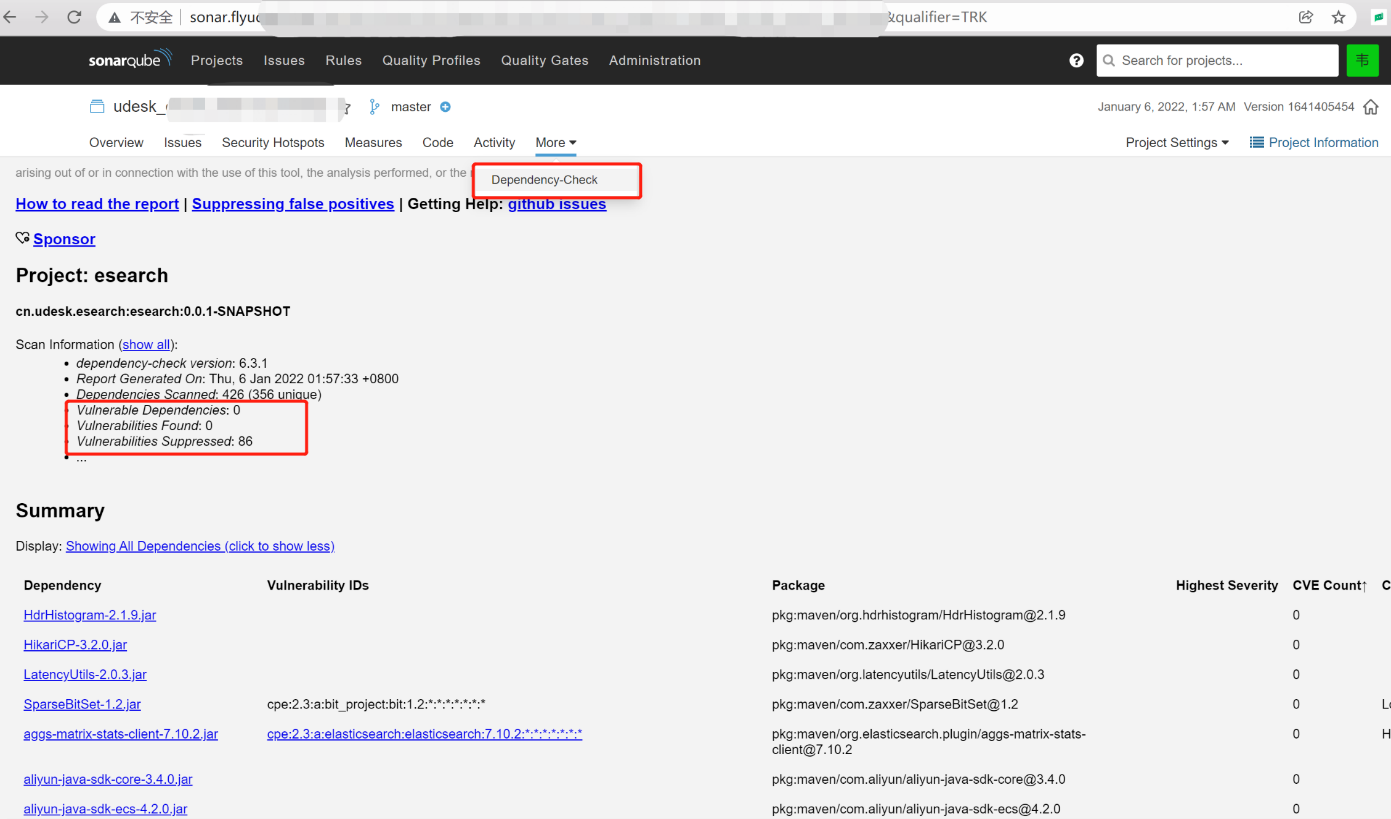
**SonarQube扫描记录**:

帮助文档 <https://docs.sonarqube.org/latest/>



**dependency check 扫描**

**帮助文档：**<https://owasp.org/www-project-dependency-check/>

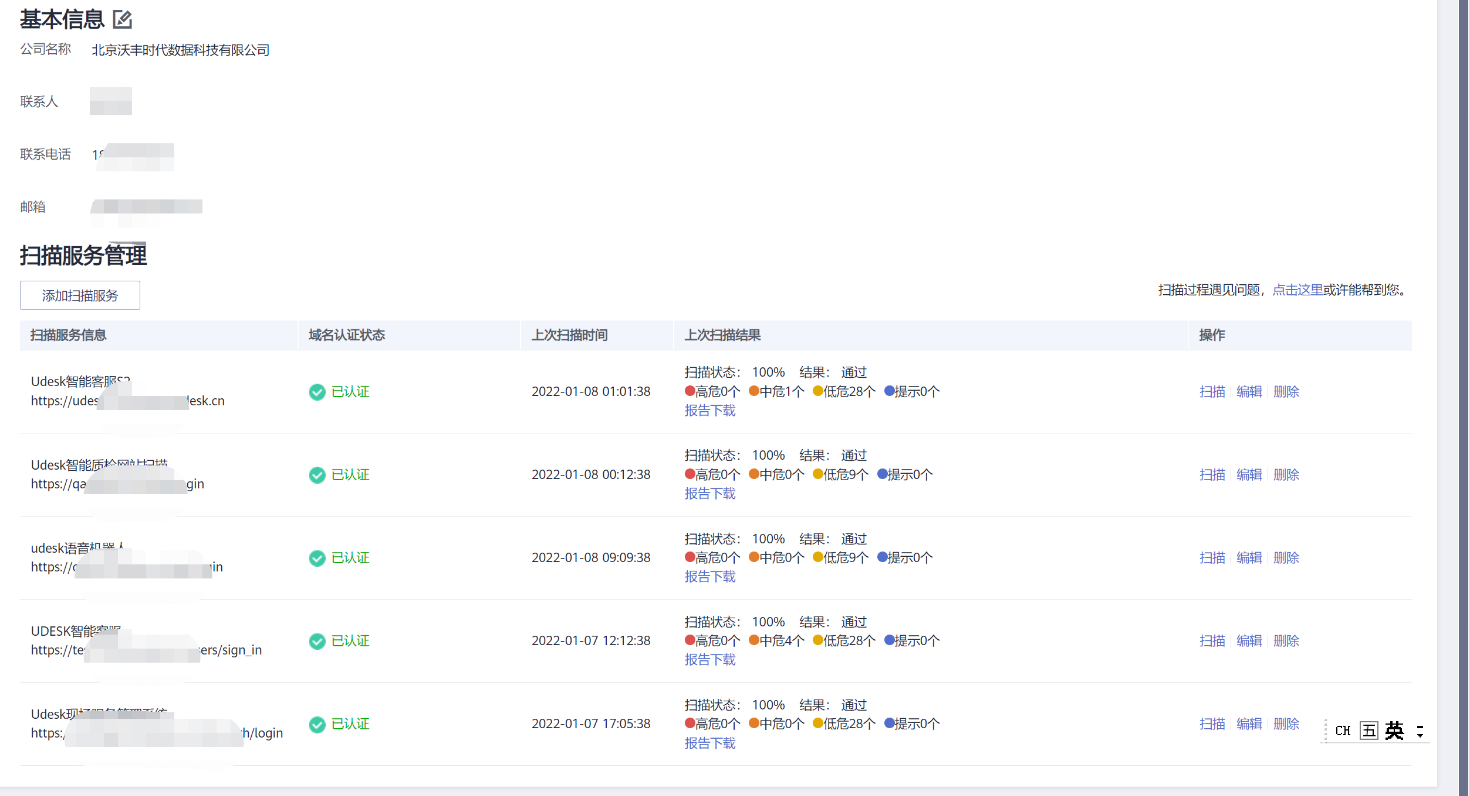


SonarQube每日扫描邮件报告：



**华为漏洞扫描服务**

帮助文档：<https://support.huaweicloud.com/productdesc-vss/vss_01_0009.html>



系统动态扫描巡检

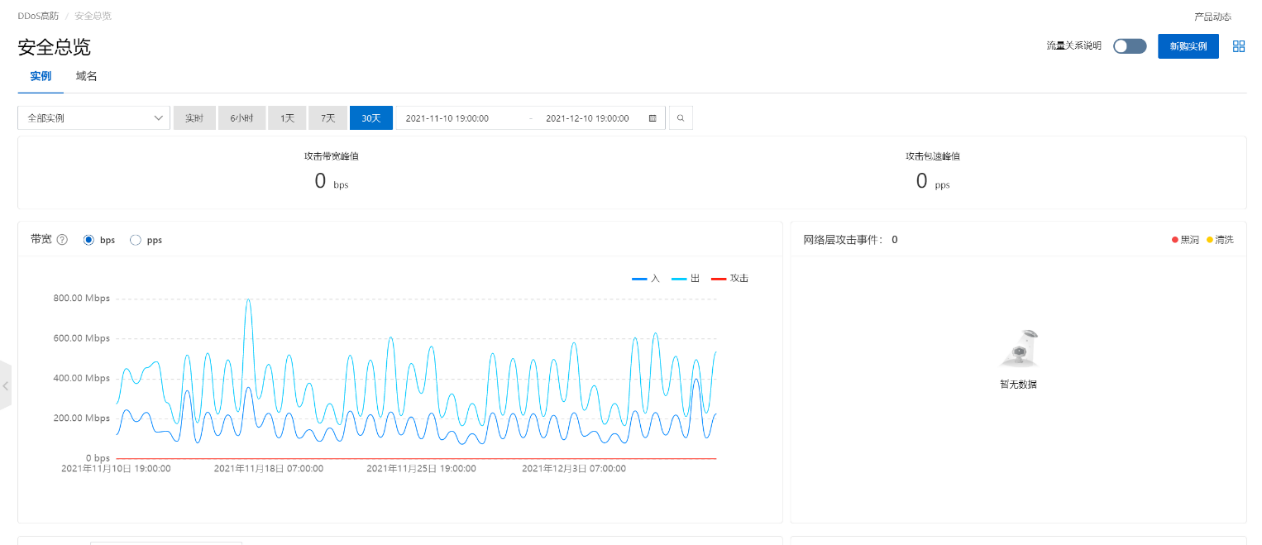


# 附录3 《用户异常行为监控办法》

1 我们使用阿里DDoS高防和WEB应用防火墙（WAF)作为第一道防线，以发现来自网络的流量、web攻击。

2 同时使用阿里云态势感知服务为我们提供入侵检测、监控和报警，

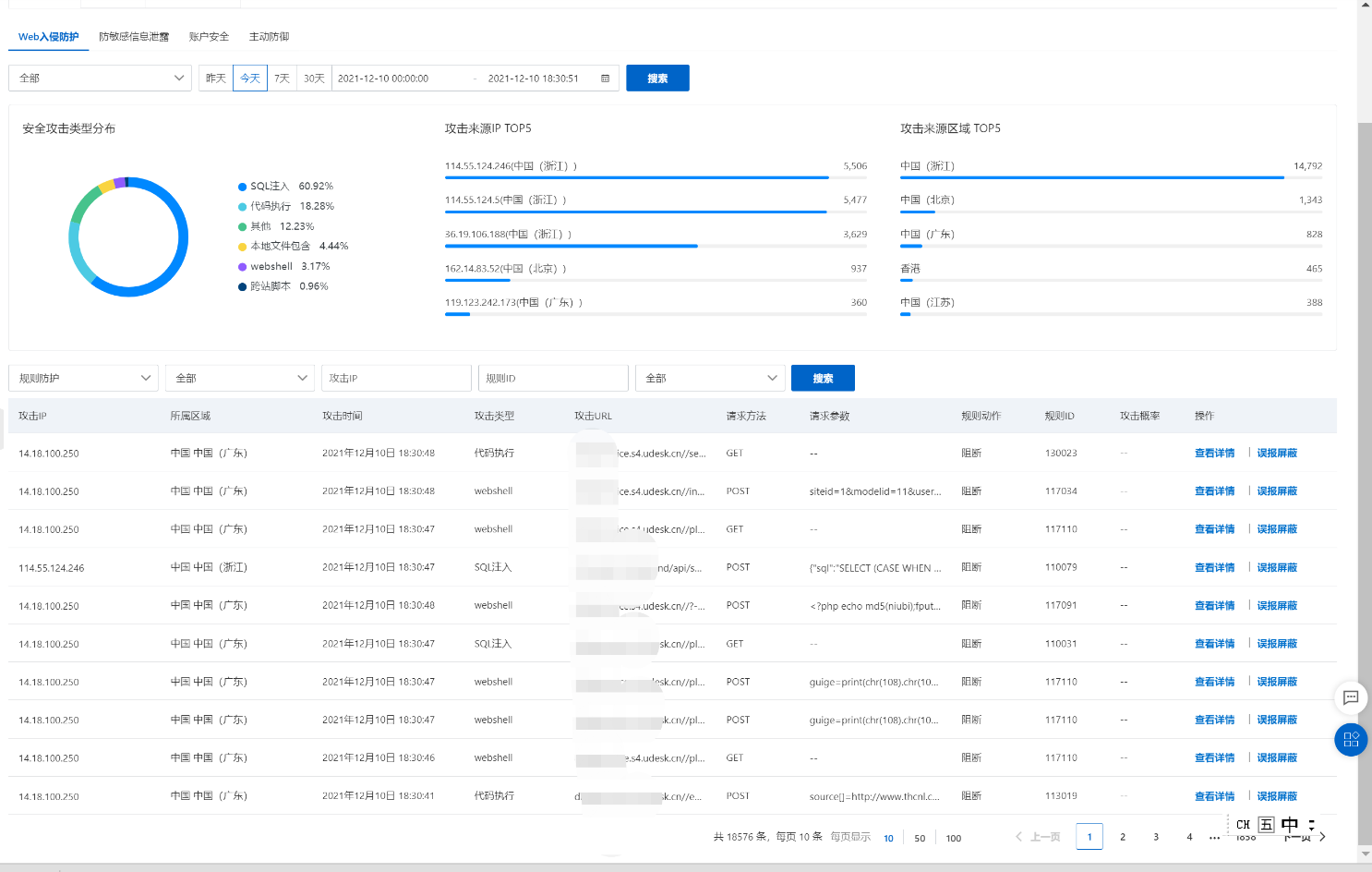
阿里DDOS防护：帮助文档详见：<https://help.aliyun.com/document_detail/153308.html>



阿里云高防报警：

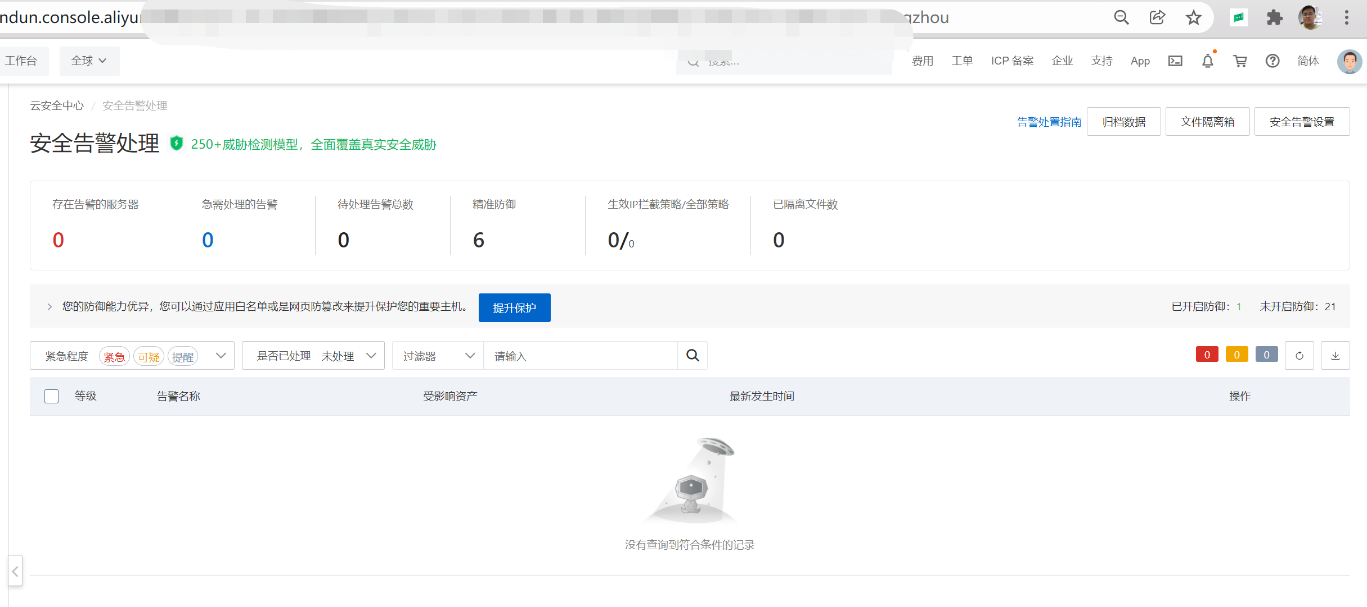


**阿里Web应用防火墙（WAF）**：帮助文档详见：<https://help.aliyun.com/document_detail/28517.html>



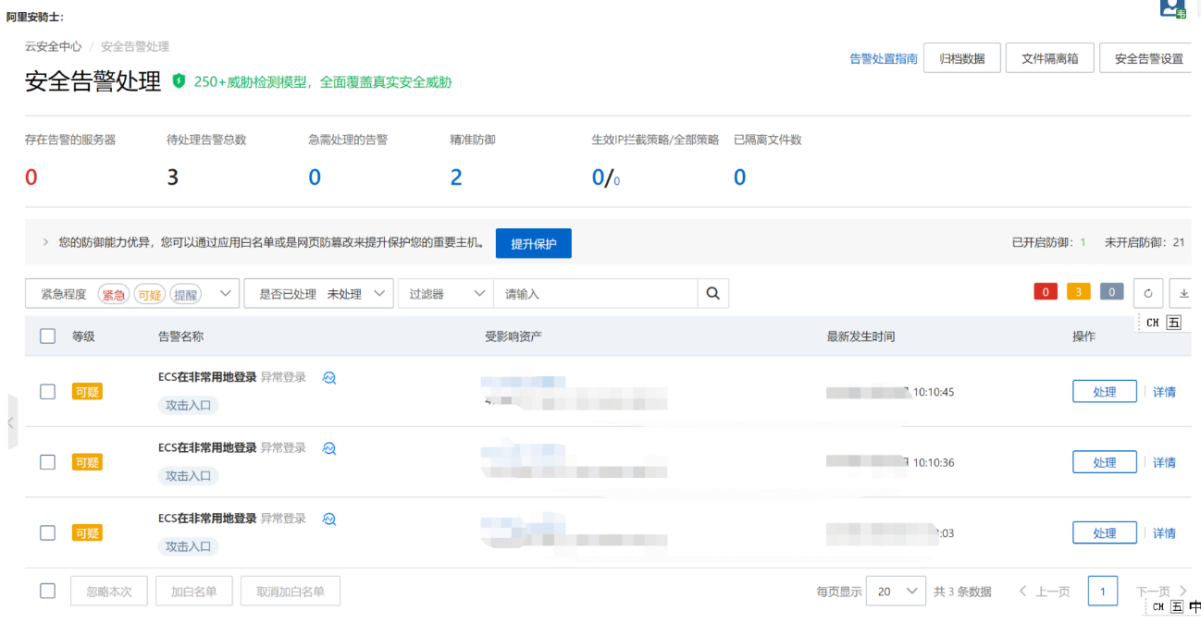
阿里云态势感知服务：

文档详见： <https://help.aliyun.com/product/28498.html>



当出现异常活动时，会发出邮件报警和相关信息





# 附录4 《合作商处理时间特别要求》

|  |  |  |
| --- | --- | --- |
| 编号 | 合作商 | 描述 |
| 1 | 西安杨森？ | 发生相关安全事件时24小时内通知 |
|  |
|  |  |  |