完美世界安全应急响应中心

威胁情报处理流程与奖励说明（试行版）

完美世界安全应急响应中心
security.wanmei.com

编写人	完美世界安全应急响应中心
版本号	试行版
更新时间	2018-11-16

版本号	修订内容	发布日期
V1.0	发布试行版	2018-11-16

基本原则

1. 完美世界非常重视自身产品和业务的安全问题，我们承诺，每一位报告者反馈的问题都有专人进行跟进、分析和处理，并及时给予答复；
2. 完美世界承诺，对于每位恪守“白帽子精神”，保护用户利益，帮助完美世界提升安全质量的白帽子，我们会给予感谢和回馈；
3. 完美世界严禁一切以提交威胁情报为借口，利用所发现的威胁情报进行破坏、损害用户利益的恶意行为，包括但不限于利用所发现的威胁情报盗取用户隐私数据及虚拟财产、入侵业务系统、恶意传播漏洞、暗藏木马后门等；
4. 完美世界希望通过此平台与白帽子和安全爱好者建立良好的关系，为完美安全添砖加瓦，为建设安全健康的互联网环境而努力。

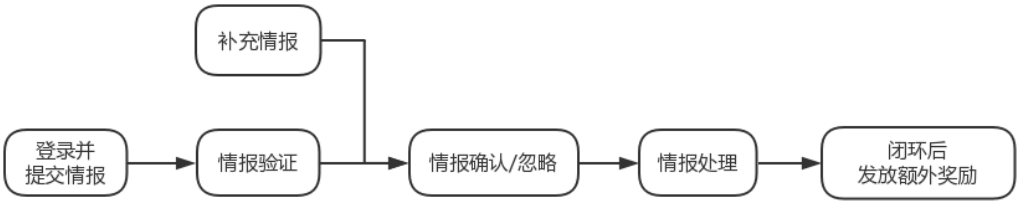
一、 适用范围

威胁情报是指可能对完美世界的产品和业务产生不利影响的相关情报，包括但不限于与漏洞相关（如漏洞线索、攻击线索、攻击方式、攻击者信息等）、数据隐私安全（用户信息泄漏、私服外挂、代码或其他知识产权泄漏）相关的情报。本流程适用于处理完美世界安全应急响应中心（http://security.wanmei.com）所收到的威胁情报，公司内部人员与职务/工作职责相关的发现的威胁情报除外。

二、 实施日期

本文档自发布之日起实行 。

三、 威胁情报处理流程



1. 预报告阶段

报告者注册完美通行证账号，并访问 http://security.wanmei.com/（PWSRC 平台）进行登录。

2. 报告阶段

报告者向 PWSRC 提交威胁情报报告（状态：未处理）

3. 验证阶段

一个工作日内，PWSRC 工作人员会确认收到的报告并跟进评估问题（状态：处理中）。

威胁情报分析和溯源花费的时间较长，因此确认周期相比安全漏洞的时间较长，具体确认时间根据情况而定，必要时会与报告者沟通确认或要求补充更多的情报信息，请报告

者予以协助。

4. 确认阶段

根据情报对溯源的帮助给予相应的奖励（状态：已确认）

5. 闭环阶段

针对高质量的威胁情报，PWSRC 工作人员会在该事件闭环后进行复盘。根据该情报闭环处理产生的价值给予额外现金奖励。

四、 威胁情报评分标准

收到威胁情报后 ,我们会结合威胁情报的实际价值 ,给出具体的奖励。威胁情报的分类、奖励积分计算规则如下：

威胁情报积分 = 基础威胁系数 * 情报完整性系数

1）基数威胁系数

情报等级	基础威胁系数
严重	80-120
高危	30-60
中危	8-12
低危	2-3

2）情报完整性评判标准

由于情报的完整性对情报的价值有着重要的影响 ,因此我们对所上报的威胁情报的价值会进行情报完整性考量。**能否溯源因素**将作为情报完整性的重要标准，PWSRC 会根据情报完整度给出 0-10 的报告完整性系数评定。

基本完整的情报	情报来源可靠，根据情报可直接溯源，报告内容细节清晰明了，能基

（9 - 10）	本覆盖整个事件内容，有重要证据的详细截图链接等证明。
部分完整的情报 （5 - 8）	情报来源大部分准确可靠，该情报对溯源工作起到了部分作用，报告内容细节清晰明了，能基本覆盖整个事件内容，有重要证据的的截图链接等证明。
残缺的情报 （0 - 4）	情报来源部分可靠，该情报对溯源工作起到了部分作用，情报内容细节不够清晰明了，只有相关证据的截图链接等证明。

3）威胁情报等级

情报的危害程度共分为【严重】、【高危】、【中危】、【低危】、【无效情报】五个等级。每种等级包含的评分标准及情报类型如下：

【严重】

1、盗取完美世界核心数据、核心产品的源码等核心数据、信息，以及利用进行获利行为；

2、服务器被恶意攻击，例如被拖库、重要业务逻辑被篡改，造成用户或公司的重大财产损失；

3、针对完美世界 APT 攻击事件的重要信息，例如：目标、沦陷范围、C2 地址、特征、组织等；

4、利用漏洞，攻击或修改完美世界的充值支付类业务，造成重大的财产损失。

注：涉及核心数据泄露、盗取，和利用漏洞进行大额获利，或形成产业链的举报，需提供相应有效确凿的线索，如规模、源头，涉及的人员等。若无法提供详细信息则降低报告完整性系数或威胁情报等级。

【对于有重大影响的高质量情报 ,或在 PWSRC 处理情报的过程中给予重要支持的 ,PWSRC 会给予额外奖励人民币 10,000 元-人民币 50,000 元。额外奖励需在 PWSRC 处理结束该威

胁情报后发放。是否属于高质量情报以及是否发放额外奖励，以 PWSRC 最终解释为准。】

【高危】

1、大规模的老虎游戏账户，完美通行证账户的敏感信息泄漏及非法利用；

2、敏感的内部业务信息、员工信息、敏感数据、敏感文档泄漏；

3、利用完美世界产品、源代码进行大额非法获利，或形成相关产业链。

【中危】

1、中等规模的老虎游戏账户，完美通行证账户的敏感信息泄漏及非法利用；

2、利用漏洞、业务逻辑恶意刷取积分换取较大额度奖励，非法获取以及贩卖内测名额、激活 key、礼包行为，以及其他利用漏洞获取不当利益的行为；

3、盗取、散播、非法利用完美世界知识产权的行为。

【低危】

1、对核心业务以及少量用户造成的轻微损失，如钓鱼网站，钓鱼 qq、微信群等。

2、对完美世界造成损失或不良影响的舆情舆论。包括但不限于涉及到完美世界的恶意言论、谣言等。

【无效情报】

1、个别用户账户被盗、或少量用户信息泄露；

2、对业务用户影响不大，在可承受范围内的；

3、较少的恶意评论，个别的钓鱼网站；

4、情报内容过于简单，无法从源头追溯威胁的。

五、 威胁情报评分原则

1. 评分标准适用于完美世界的所有产品和服务。包括完美世界各 PC、移动和 web 端的网游、完美世界公司内部系统、数据、人员等。

2. 由于业务调整，我们不再接收重庆星游传媒有限公司所属网站的相关情报，包含但不限于 :stargame.com、178.com、tgbus.com、a9vg.com、dospy.com、nga.cn、ngacn.cc、ptbus.com、766.com、xyous.com 等。
3. 针对完美世界使用的第三方系统及部分子公司，或与我们相关的一些边缘业务，情报可能将不完全按照上述评分标准，而是根据业务实际运营情况及所涉及的业务数据进行综合评分。
4. 同一威胁情报在由多位报告者提交，认定最先提交并且情报完整性最高的为有效报告者。如有多位报告者提交的情报内容有交叉补充的情况，奖励情报完整性最高的报告者主体部分积分，其他报告者只奖励互补部分积分。
5. 情报未核实、未处理完之前，情报提供者使用情报内容、或是泄露情报导致对完美世界公司造成损失，将不给予积分奖励，并且会根据损失程度追究其法律责任。

六、 奖励兑换

PWSRC 工作人员会在**每个月第一个工作日进行订单确认并进行礼品采购**，首次在平台兑换现金奖励的用户，应公司要求，需要根据平台的引导进行实名认证。如有任何疑问，请联系 src@pwrd.com。奖励的发放需要一定的时间，请各位白帽子耐心等待，感谢理解!

七、 争议解决办法

在情报报告处理过程中，如果报告者对流程处理、情报定级、评分等有异议的，可以通过 src@pwrd.com 与工作人员及时沟通。

本流程由完美世界集团信息安全部负责修订和解释。