途牛安全响应中心威胁情报处理规范流程

1. 情报价值计算方法

情报贡献最终评分由情报对应的危险程度及提报的完整性决定。

情报价值=基础价值×完整性系数；

安全币对应表:

基础价值 完整性	严重情报 (15~20)	高危情报 (10~14)	中危情报 (5~9)	低危情报 (1~4)
最完整(10)	150-200	100-140	50-90	10-40
~	~	~	~	~
最不完整(1)	15-20	10-14	5-9	1-4

如:一个入侵事件的完整严重情报的贡献值为 200,计算方法为:完整性(10)×情报贡献值(20)。

1.1 完整性系数

威胁情报的完整性由以下 7 点进行评估，下表为线索评分对照表:

<table>
<tr><td colspan="7">情报线索</td></tr>
<tr><td colspan="4">核心线索</td><td colspan="3">辅助线索</td></tr>
<tr><td>Who
(0~3)</td><td>Where
(0~3)</td><td>How
(0~3)</td><td>What
(0~1)</td><td>When
(0~1)</td><td>Why
(0~1)</td><td>How much
(0~1)</td></tr>
<tr><td>谁</td><td>在什么地方</td><td>用什么方法</td><td>做什么</td><td>什么时间</td><td>什么原因</td><td>产生多大影响</td></tr>
<tr><td colspan="7">完整评分将按照组合产生情报完整度进行评分。*注：辅助关注点仅当在对情报有突出意义时才计分。</td></tr>
</table>

1.2 情报基础价值

1.2.1 严重:【15~20】

对核心业务、系统、办公网络造成重大影响，或对集团造成大量资金损失以及严重伤害品牌形象的威胁情报，如:

1) 途牛大规模敏感信息泄露，并验证真实有效的情报，如用户信息、商家信息、订单信息等；
2) 针对途牛重要业务、核心系统、办公网络发现被入侵或被拖库的有效情报；

1.2.2 高危:【10~14】

对核心业务、系统、办公网络造成一定影响，或对集团造成一定资金损失以及伤害品牌形象的威胁情报，如:

1) 对途牛已造成重大影响的蠕虫、病毒、木马、钓鱼等有效情报；
2) 针对途牛进行有组织的威胁活动以及正在进行的重大威胁情报，如撞库、刷单、秒杀、薅羊毛等；
3) 发现途牛可造成大量数据泄露或被窃的有效方法、攻击代码、工具等情报；
4) 途牛现有支付渠道的安全漏洞、支付风控规则被绕过的漏洞；

1.2.3 中危:【5~9】

对核心业务、系统、办公网络造成一定影响，或对集团造成一定资金损失以及伤害品牌形象的威胁情报，如:

1) 因业务规则问题导致被一定量级商家利用的刷单行为；

2) 大批量优惠券领用漏洞；

1.2.4 低危:【1~4】

对业务、系统、办公网络造成轻微影响的威胁情报。

1) 大批量出售途牛旅游卷行为(淘宝等公开平台出售的不计)；

1.2.5 无危害:【0】

1) 经验证情报为虚假捏造或制造情报信息；

2) 上报可能刷单、秒杀的群号而未能提供有效信息；

3) 与途牛无关产品或业务的相关情报；

4) 已得知或失效的情报；

5) 违冒集团的钓鱼网站；

2.奖励发放原则

奖品使用积分进行兑换，多个漏洞产生的积分可累加，除非特别声明，未使用的积分不会过期。如因报告者未能完善资料导致的延误，将顺延下批次进行寄出；如因报告者过失，快递等问题及人力不可抗因素产生的奖品丢失或者损坏，TNSRC 不承担责任。

3.争议解决办法

在漏洞处理过程中，如果报告者对处理流程、漏洞评定、漏洞评分有争议的，请通过邮件 sec.tuniu.com 并以邮件标题【途牛漏洞处理异议】进行反馈，我们会有专门工作人员负责优先处理此类反馈。

途牛安全应急响应中心

Tuniu Security Response Center