## 安全应急响应中心之威胁情报探索—JSRC安全小课堂第二期

2016-03-18 京东安全应急响应中心



JSRC安全小课堂第二期如期和大家见面啦~本期很荣幸邀请到了来自阿里安全应急响应中心的项、腾讯安全应急响应中心的flyh4,来跟我们一起探索众安全响应中心均积极关注和推动的威胁情报。



豌豆妹

小伙伴们,欢迎大家来畅所欲言!首先,来说说威胁情报和漏洞的区别呗!



的。其中存在假情报和难追溯的情报。情报一般分为线索和 事件,我上报了一个黑客组织,可以作为线索;公司根据这 个线索发现了之前一个案子和他们有关,就可能引申出一个 事件。威胁情报并不一定是提前预知,作为甲方公司,很多 /J\M

已经发生的漏洞利用资金损失,我们也有很多没有发现的,这些也都是情报。而情报的奖励可能是白帽子同学比较关心

漏洞的概念较明确,而情报比较宽泛。威胁情报并不是虚

的,一般情况下很难像漏洞一样非常标准化,这里可能更加考验白帽子和src平台的信任关系了。



按照我的理解,情报分技术型情报和业务型情报,漏洞属于技术型情报。有的情报很全,有的只能算是线索。业务型的最难判定,我们这边也分两个维度,危害维度和完整度维度。





说的有道理,如果白帽子只给了一条线索,怎么去判定呢?

具体的看标准吧,至于完整度如何判定,内部是有标准的,但是不合适对外,太细了。



小〇



获取情报的来源渠道一般有哪些呢?

豌豆妹

这个看业务了。举个栗子®,有的白帽子已经成功混迹在高端游戏玩家群里,黑产卖异常装备的时候,就来举报。比较聪明的同学,会关注黑产变现的渠道。



小H



如果一条线索过来了,只是证明存在但不能做什么事。这种对于平台来说是不是一种成本浪费?

豌豆妹



溯源是一种能力,线索是一种沉淀。被证明有价值的情报, 是一种线索沉淀,不会是浪费的。安全行业内,不管是漏洞 还是情报,都是要不断求证的。只要投入产出比可控即可。 这其实也是一个二八原则。此外,没有产生价值的,可能只 是当前没有产生价值,后面业务变化了,可能就会产生相应 价值。





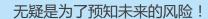
大家觉得建立威胁情报的目的是什么?

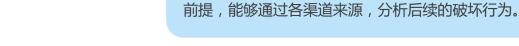






ΛM







那威胁情报的评定指标有哪些呢?



小田

主要看情报的详细程度和对业务的影响,来评定情报的等 级。不过低价值的情报分值不高。大致是看详细程度、涉及 业务、目前和潜在的影响,有一条就是基于漏洞的情报,不 会比按漏洞标准评定低就是了。目前来看提交者比较理性, 大都是遇到事件了来提交,线索其实没那么多。不同公司关 注的情报不一样,建议大家在看情报的时候,先看看这个公 司关注什么,根据公司实际业务多磨合磨合。

个人认为,威胁情报对于各公司来说可以把风险感知再次往



balabala···(此处有神秘问题)



白帽子

大家如想更加详细了解探讨内容,更多机会向业内大牛们探讨请教,请积极关注京东安全应急响应中心平台,积极挖掘漏洞,成为我们这个大家庭的一份子,并加油成为我们的核心白帽子喲~

