Thinking on Defense

从安全的角度完善现有的软件开发流程

View

Software development process should also produce the standand behaviors specifications of the target sofeware, which can be used to check the abnormal behaviors or malware behaviors.

观点

1、软件的生产过程除了应该产出源码、程序、文档等传统形式的产出之外，还应该包含安全方面的产出，比如：标准行为规范。 2、安全需要开发者的参与，安全需要改变或者融入现有的软件开发流程。

前言

业界在想各种方法改进软件的安全性及对恶意行为的检测，本文记录了自己的一点思考，希望能起到抛砖引玉的作用。

基础

恶意行为或者攻击行为之所以可以被检测是因为在整个攻击过程中存在“异常”，这个异常包括但不限于：API 行为、网络行为、文件系统行为、程序状态等。
对恶意行为或者攻击行为的检测最终可以归结为对异常的检测，目前业界基本上也是这样做的。

问题

如何定义一个程序的异常行为?

解答

异常之所以是异常，是相对于正常来说的。将这个问题换种说法就是：谁能完整的、综合的定义程序的正常行为？我的回答是：程序的开发者。

解决方法

在现有的软件开发过程中，具体来说是在程序的全功能回归阶段，通过技术手段记录程序的行为与状态，将记录的行为与状态进行标准化、去隐私化，将此作为程序的标准行为规范，并与程序、文档等一起发布。
XDR 会记录程序在真实场景中的行为，将真实行为与标准行为做比对，寻找异常。

程序行为描述标准

从甲方考虑，为自家的程序定义好行为标准就足够。
但是从乙方，以及从整个行业的角度考虑，需要一个统一的、分领域的程序行为标准，这样才能实现安全最大化。

程序标准行为中心数据库

将各种程序的标准行为统一存储，目的是安全最大化。
这个应该是最难推进的，需要强势的力量来推进，比如：应用商店，或者具有更强力量的角色来推进。

安全生态

如果程序标准行为数据库可以建立起来，那么开发者、甲方、乙方都可以参与其中，从非利益的角度来说，相当于建立了一个安全生态，当然对于一个生态来说最重要的还是利益。

竞争与合作

乙方是甲方能力的补充。
乙方与乙方之间基于相同的行为标准，基于相同或者不同的程序真实行为，竞争的是记录程序行为与状态的能力，竞争的是捕获异常行为的能力。

Proteas
2021-03-10