安全小课堂第七十一期【大数据安全】

京东安全应急响应中心 2017-09-01

各类复杂的安全数据使传统数据分析能力变的力不从心，而新型威胁的兴起，内控与合规的深入，也暴露了传统的分析方法的缺陷。因此，信息安全面临大数据带来的巨大挑战。JSRC **安全小课堂第七十一期**，邀请两位老师分享大数据安全分析中的那些事，本期小课堂邀请到了小胖胖、**高渐离**老师进行分享。同时感谢JSRC白帽子们的精彩讨论。

大数据安全的概念?

京安小妹

大数据安全分析，我认为的关键还是能否从数据中寻找线索，我们的系统网站是否被攻击，是否攻击成功，我们的系统网站是否安全，其中也可以使用可视化来对行为进行展现。

通过有针对性的数据采集汇聚，采用包括特征匹配机器学习之类的方法，对数据进行综合征分析，解决安全问题。

讲师： 小胖胖、高渐离

大数据可能涉及哪些技术安全问题?

京安小妹

我们这边主要是web应用，主要针对用户访问日志做的大数据实时+异步的处理，包括常见的web攻击，以及包括如蠕虫病毒对外恶意请求的监控等。
第一个问题就是数据汇聚之后，对黑客而言，目标更集中了只要进去之后，找到数据平台。
第二个问题数据访问控制，加密脱敏还有隐私。

:

讲师： 小胖胖、高渐离

白帽子提问:如何保证大数据的安全呢?

对于大数据本身的安全，可以在汇聚层做敏感数据脱敏，但是前期会涉及各业务使用和数据本身的分散程度会有较大的工作量，但是长期来看，数据落地脱敏是一个趋势。
本身从消息到数据库，kafka到mysql等，都可以使用数据脱敏方式来满足业务需求，部分场景需要增加一些辅助字段来保证业务正常运行，在遇到必须明文场景进行统一权限控制的解密服务，同时保证调用的可监控和权限控制，这点不管在大公司和小公司，本身对数据安全性的意义非常大。

讲师： 小胖胖、高渐离

白帽子提问:有些业务需要在后台系统看到用户的一些隐私数据，这种情况下，数据库跟后台在数据安全方面咋搞?

这个数据库直接存密文，后台页面展示统一调用解密服务即可，api本身做授权和监控。

讲师： 小胖胖、高渐离

白帽子提问:能不能就脱敏安全问题稍微全面讲解一下?

脱敏本身涉及常见的一些字段，如手机号，身份号，银行卡等，内部约定一个方式即可，如打码或者做数据的映射关系，海量数据要满足性能则需要架构上的支持。

讲师： 小胖胖、高渐离

企业为什么会需要大数据安全分析?

京安小妹

大数据安全分析在海量数据的情况下，获取数据中的信息变更越来越困难，本身单纯的正则匹配的方式，无论在性能还是在准确性方面很难满足海量数据下的数据分析，所以大家可以尝试机器学习，使用分类模型算法对数据进行处理，已满足后续对数据的处理。
因为被黑总是个常见的事情,但是人工分析和传统分析手段成本太高难以实施,企业使用大数据安全分析可以更轻松的关联各个角度的数据,避免安全人员崩溃。

：

讲师： 小胖胖、高渐离

白帽子提问:在安全数据分析上的投入成本？以及分析多大的数据量？

成本这块本身看部门对这块的定义，单纯的我这边实践来说2-3个不同角色来执行，包括数据处理，模型及引擎开发，以及运营人员。
从当前看，storm的实时分析基本能满足大部分公司的海量数据，引入机器学习即可提高近10倍于正则的性能进行数据处理。spark的处理性能高于storm。

讲师： 小胖胖、高渐离

大数据分析与传统数据分析相比它的优势在哪里？

京安小妹

从系统的演变来看，海量数据和精准判断是我们所面临的问题，传统数据分析难以满足当前的数据趋势，在新技术的引入同时，基础架构和工具使用也必须与时俱进，大数据分析只是一个名称，落地还是用什么架构处理多少数据，产出是什么。

因为维度更多海量数据有利于关联分析数据更全机器自动化能力更强。

：

讲师： 小胖胖、高渐离

是否有成熟的大数据分析工具或者平台推荐呢?

京安小妹

storm、spark、impala、hadoop、scikit-learn、weka

：

讲师： 小胖胖、高渐离

白帽子提问:能不能举两个你们觉得现在应用的比较成熟的例子?

账号安全僵尸机器识别以及web入侵识别。

讲师： 小胖胖、高渐离

白帽子提问:web入侵识别现在都收集了哪些数据来判断?

只收集了acesslog加waf日志。

讲师： 小胖胖、高渐离

本期JSRC 安全小课堂到此结束。更多内容请期待下期安全小课堂如果还有你希望出现在安全小课堂内容暂时未出现，也欢迎留言告诉我们。

安全小课堂的往期内容开通了自助查询，回复“安全小课堂”或者点击阅读原文进行查看。

最后，广告时间，京东安全招人，安全开发、运营、风控、安全研究等多个职位虚位以待，招聘内容具体信息请扫描二维码了解。

简历请发送：cv-security@jd.com

微信公众号：jsrc_team

新浪官方微博：京东安全应急响应中心

阅读原文