苏宁安全架构演进及实践

架构之家 2018-04-19

一、前言

近年来，各类网络安全事件层出不穷，木马病毒、信息泄漏、网络诈骗等等字眼时常见诸媒体，就连年初美国的总统大选都被黑客闹得鸡飞狗跳，网络安全从未像今天这样受到整个社会的重视，那么对于绝大部分互联网企业尤其是电商平台而言，为消费者提供隐私信息保护以及安全可靠服务的重要性毋庸赘言。

苏宁安全架构是伴随苏宁易购一起成长的，经历了从无到有到逐步完善的过程，期间不管是在技术上还是在管理上，都遇到了非常多的难题，但一旦闭环安全体系完善起来后，安全事件发现、处理效率会得到极大提升。

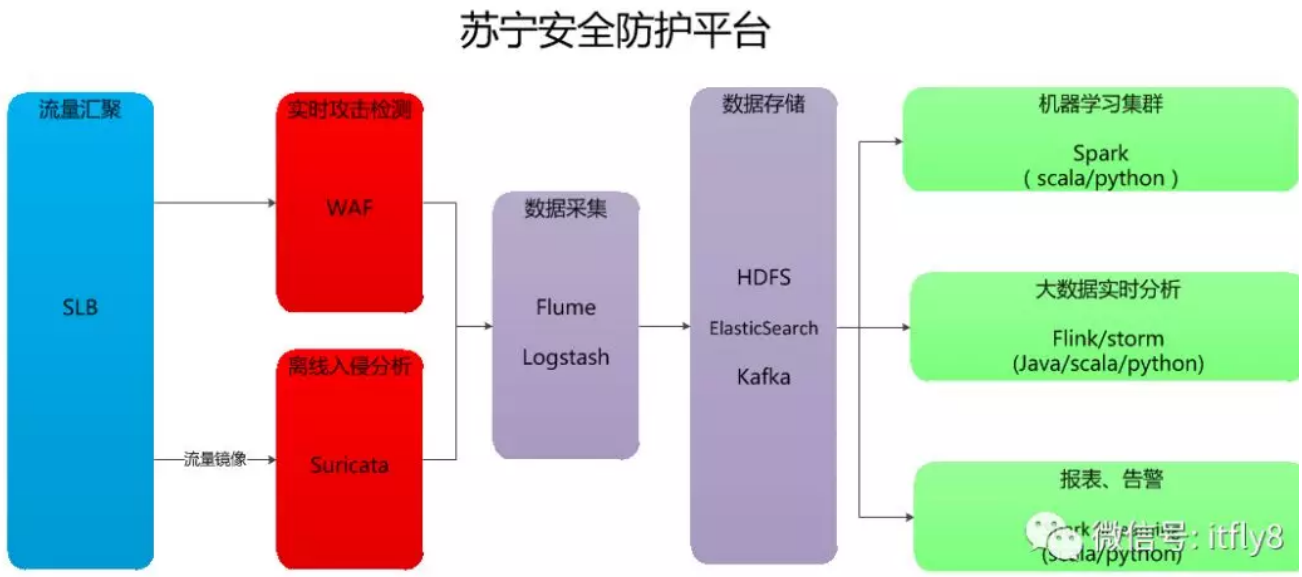
二、安全组织架构

首先需要明确安全部门的组织架构，苏宁的安全相关部门目前主要分为管理和研发两大类。由于企业安全不仅包含外部网络攻击防护，还包含企业内部安全威胁检查，所以安全部门非常特殊，必须要有一定的独立性，否则合规审计、内外风控、漏洞处理、应急响应等工作根本无法开展。一般互联网公司大都会成立一个较高级别的安全部门专门负责各类安全事务，因为这样即方便管理又能减少沟通成本。苏宁安全管理中心由CTO直接负责，集团所有安全相关事务都由它统一协调，安全研发工作主要由数据云团队负责，个别子公司因业务需要也会有相对独立的安全部门。

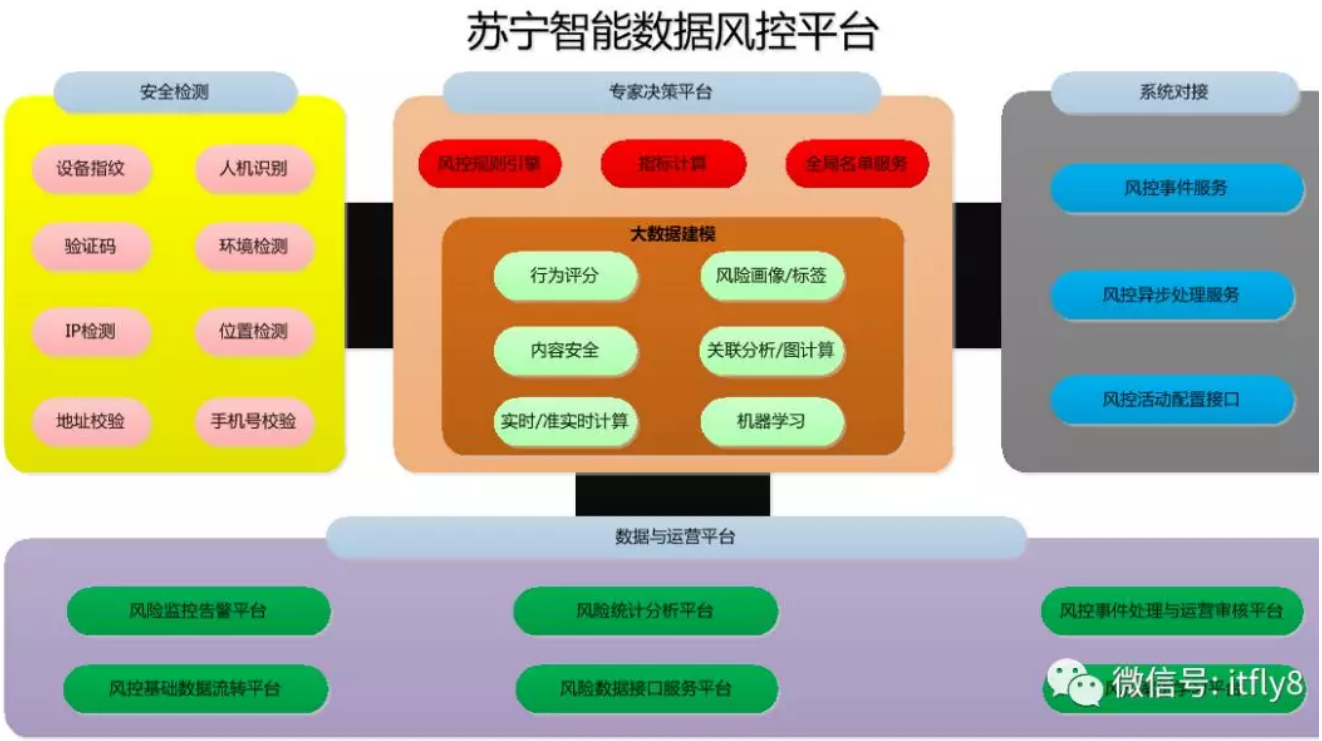
三、安全防护体系建设

苏宁的安全部门最初是从网络运维部门分离出来的，当时部门的工作内容也和安全开发完全无关，主要就是各类网络设备以及操作系统的安全基线检查，后来随着苏宁向互联网转型，安全部门才开始承担起攻击防护、风险检测、漏洞处理等职责，逐步开始自研各类安全系统。由于当时安全工作都是围绕苏宁易购开展的，而苏宁易购又是一个综合网上购物平台，所以保护消费者的个人信息和资金安全自然是重中之重，因此苏宁安全防护平台和苏宁智能数据风控平台是最早上线运行的两个安全系统，之后又陆续开发上线了苏宁安全服务平台、苏宁安全应急响应中心等系统。

苏宁安全防护平台：由离线入侵分析、实时攻击检测、大数据分析等模块组成，主要负责各类常见的网络攻击的检测和防御，是苏宁的第一道安全防线；



苏宁智能数据风控平台：提供设备指纹、人机识别、敏感信息过滤、风险信息库等功能，通过灵活的风控智能算法和风险措施保护消费者购物流程安全；



苏宁安全服务平台：主要是为苏宁内部所有系统提供各类安全服务，包括漏洞扫描、渗透测试、系统加固、安全培训等；

苏宁安全应急响应中心：主要负责漏洞管理和威胁情报收集，以帮助提升苏宁自身产品及业务的安全性，同时也希望借此加强与安全业界的合作与交流。

因为上述四个系统是苏宁安全研发部门最主要的产品，也是苏宁安全防护体系最核心的组成部分，基本囊括了企业安全的方方面面，限于篇幅，其它一些次要安全系统就不在此一一介绍了。

随着这些安全系统陆续上线运行后，苏宁的安全架构在逐渐完善，安全能力也得到了很大的提升，但是此时苏宁自己的安全防护体系依然没有建立起来，各个安全系统由不同安全团队开发维护，分散在不同的业务线上，各自为战，依然会遇到很多各个系统独自无法解决的安全问题。比如平时为了吸引消费者，苏宁易购经常会送大家很多

各类优惠券，也会对一些热门商品进行限时低价抢购，由于购买价格远低于市场价格，常常会吸引来大量黄牛薅羊毛。此时智能数据风控平台就开始起作用了，依赖访问特征和访问行为，能够及时从海量数据里分析出哪些是黄牛请求并进行阻断验证，但是黄牛们为了保证成功买到这些低价商品，往往会租用大量服务器并发购买请求，即使请求都被风控识别阻断，由于这些请求已经到了业务服务器，所有依然会对业务系统造成巨大的负载压力。

最好的解决方案当然是在这些黄牛的请求到达业务系统之前就被拦截，那么处在苏宁网络边界的安全防护平台实时攻击检测模块（WAF）自然是首选。其实黄牛并发的大量请求也可以看成CC攻击，尽管请求发起者目的不同，但攻击特征与攻击效果是一样的，而苏宁攻击防护平台本身是具备CC攻击防护能力的，可从实际效果看，还是有一部分请求绕过了CC攻击防护规则检测。这是由于黄牛发起的请求和正常用户是没有任何区别的，而且现在黄牛还会更换代理IP，伪造user-agent，一个帐号可能完成一次购买流程就结束了，普通CC攻击的特征非常不明显 ，安全防护平台对于此类攻击很难有效拦截阻断。数据风控平台善长识别却不适合拦截，安全防护平台适合拦截却不善长识别，那么将安全防护平台和数据风控平台结合起来进行黄牛防护自然是最好的选择了，所以我们对这两个系统进行了改造，在安全防护平台实时攻击检测模块增加了一个风险黑名单库，数据风控平台实时将高风险特征如IP、设备号、帐号、会员号等写入风险黑名单库，实时攻击检测模块会匹配每个请求是否有特征在此黑名单库里，同时将拦截信息如某帐号被拦截N次，某IP触犯什么规则等写入数据风控平台的风控规则库，形成了一个简单的闭环安全防护体系，这也是现在苏宁安全防护体系的雏形。

类似的情况还有很多，比如利用漏扫系统训练机器学习模型，用SRC漏洞完善安全规则等等，不过在不断完善苏宁安全防护体系的过程中，我们意识到仅仅两两系统之间实现数据交互依然是不够的，由于各个安全系统数据来源单一且分析标准不一致，导致这些共享数据适用性并不高，利用效率低下。不仅仅安全系统，苏宁几千个系统每天都在生产大量的数据，可是并没有任何一个系统会去专门分析这些数据，而潜在的攻击很可能就隐藏在这海量的数据里。所以我们目前正在开发苏宁自己的基于大数据架构的威胁感知系统，初期是将几个核心安全系统的流量日志以统一的格式汇聚到威胁感知系统，利用关联算法、异常分析算法等机器学习算法深入挖掘攻击行为，收集威胁

情报，积累攻击特征数据，为苏宁安全防护体系添加一颗无所不在、无所不知的聪明大脑，真正将苏宁所有安全系统融合成一体，不仅要做到固若金汤，还要做到防患于未然。

在我们的长期规划中，苏宁威胁感知系统会逐步将苏宁所有系统生产的流量数据纳入分析范围，并且还要与业界其它企业一起合作，共享威胁情报，加强安全信息交流，共建中国互联网威胁感知平台。

四、安全管理体系建设

对于外部攻击者来讲，企业是一个黑盒，虽然无从获知企业内部网络架构和安全系统详情，但为了找到一个有效可利用的的漏洞他可能会进行各种尝试，不同目的的攻击者发起请求的方式和特征也会不同，所以企业绝不能期望一个安全系统就解决所有安全问题，也不能期望无限增加安全开发投入，头痛医头脚痛医脚。企业首先需要部署WAF、IDS/IPS、风控、漏扫等基本的安全系统，在此基础上再将各个安全系统之间彻底打通，实现信息共享，融合成一套行之有效的安全防护体系，才能有效解决绝大部分安全问题。但是企业需要关注的不仅仅是外部威胁，堡垒往往是从内部攻破的，所以企业内部的安全威胁也不容忽视。从苏宁近年来内部几起安全事件发生原因总结看，基本都和安全意识淡薄、安全管理不规范密切相关，所以企业在搭建自己的安全防护体系的同时，也要搭建自己的安全管理体系。

苏宁内部安全事件的管理已有一套成熟的运转机制，在漏洞爆出之后，首先由安全管理中心评估此事故威胁程度并确认事故责任人，然后由安全研发中心协助给出解决方案，再由安全管理中心督促事故责任人所在部门修复漏洞，最后由安全管理中心总结本次事故经验教训并给予事故责任部门处罚。因为安全管理中心有考核其它研发中心安全规范的权限，所以这套管理方法还是行之有效的。但是安全问题的源头还是人，如果仅仅依靠制度规范，肯定是无法解决所有内部安全问题的，甚至可能会阻碍企业发展，因此安全管理部门还应该做好内部员工的安全培训，尤其是业务系统研发人员，定期进行安全相关培训和考核，提高所有人的安全意识。

五、总结

仅仅做到以上这些就可以高枕无忧了吗？答案当然是不，安全是一种攻防的对抗，是一种竞争，我们绝不能指望我们的敌人原地踏步，那只能自取灭亡。苏宁的安全体系建设并不是一蹴而就的，安全架构也不是一成不变的，从传统安全硬件到现在的各种云安全系统，从基于规则防护到现在的基于大数据、机器学习的自学习智能防护，不管是安全系统还是安全技术一直都在变化，我们必须脚踏实地地做好安全工作，不断突破和创新。

出处：http://www.uml.org.cn/zjjs/201803021.asp