唯品会 | 唯品会安全应急响应中心

因唯安全 所以信赖

2017唯品会第二届电商安全峰会

——深度揭秘唯品会信息安全建设实践

苏州
中国·苏州

安全运营的艺术

唯品会 梁肇星

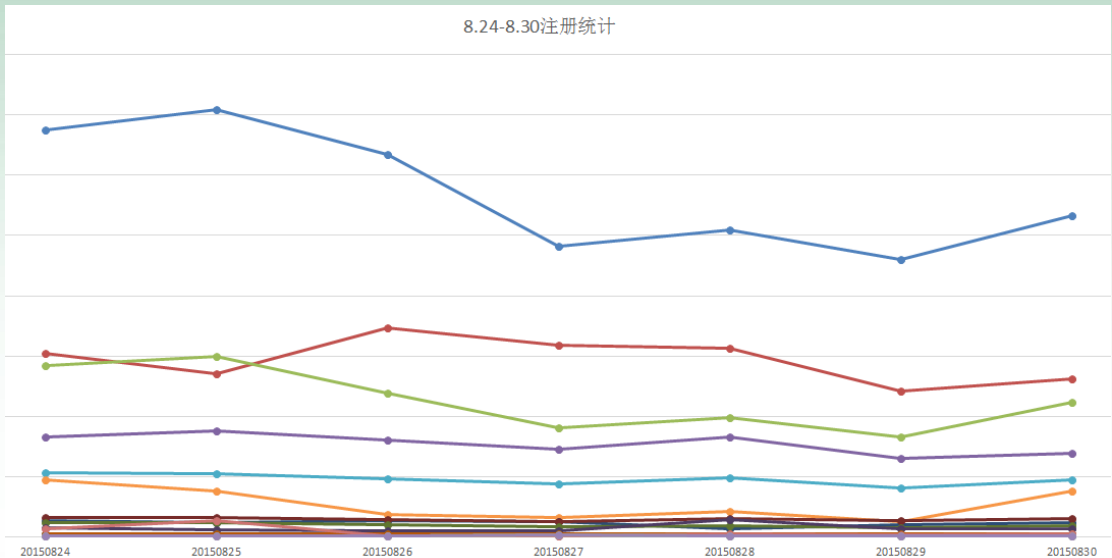
一日一电不曾休

人肉救火

权限审批

系统	详情	权限	使用方式	申请日期	释放日期
FDS用户登录注册日志数据库	[redacted]	数据库只读权限	访问跳板机后登录phpMyAdmin	2014-05	
网站订单数据库	[redacted]	数据库只读权限	访问跳板机后登录phpMyAdmin	2014-07	
网站后台数据库	[redacted]	数据库只读权限	访问跳板机后登录phpMyAdmin/	2014-08	
网站用户中心数据库	[redacted]	数据库只读权限	访问跳板机后登录phpMyAdmin	2015-03	
MAPI 业务实时分析系统	[redacted]	后台只读权限	浏览器直接访问	2015-07	
网站后台管理系统	[redacted]	后台只读权限	浏览器直接访问	2015-08-06	
pms优惠券系统数据库	[redacted]	数据库只读权限	访问跳板机后登录phpMyAdmin	2015-09	
pmswil优惠券系统数据库	[redacted]	数据库只读权限	访问跳板机后登录phpMyAdmin	2015-09	
PMS平台管理系统	[redacted]	后台只读权限	浏览器直接访问	2015-08-26	
TMS	[redacted]	后台只读权限	浏览器直接访问	2015-07	
119	[redacted]	后台只读权限	浏览器直接访问	2015-05-20	

手动统计


8.24-8.30注册统计
20150824
20150825
20150826
20150827
20150828
20150829
20150830

权限申请->数据库查询->统计分析

耗时：1小时

化繁为简

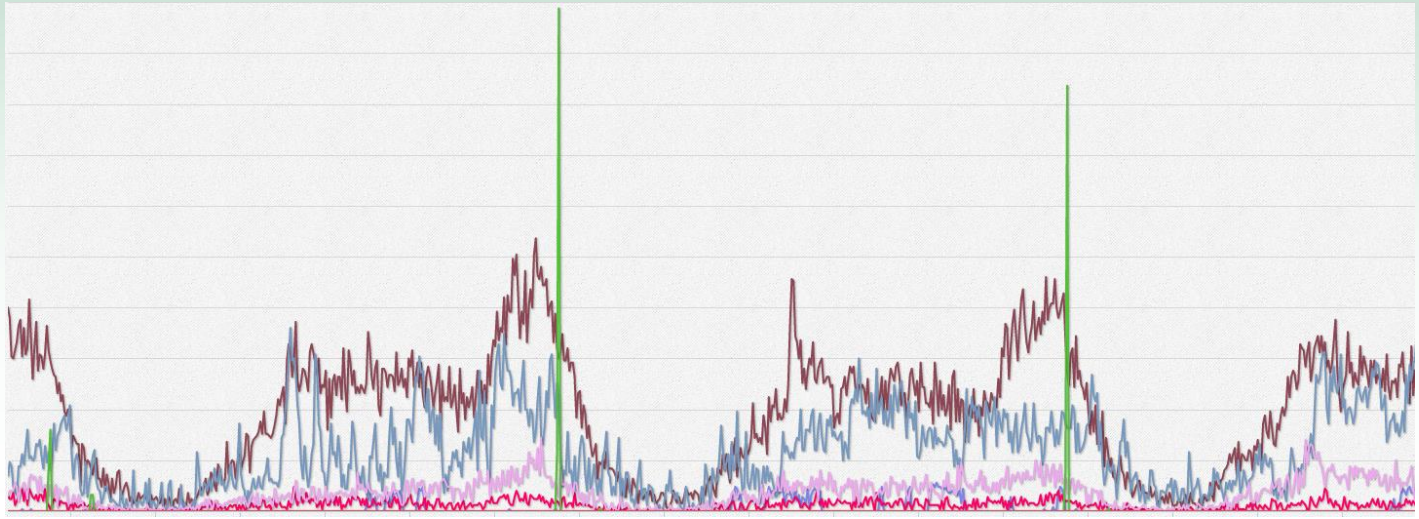
行为走势

历史同期

分类对比

事件关联

细化监控源



自动邮件告警

收件人: [redacted]

抄送: [redacted]

Hi all,

信息安全部-argus注册监控系统，检测到[redacted]批量账号注册，

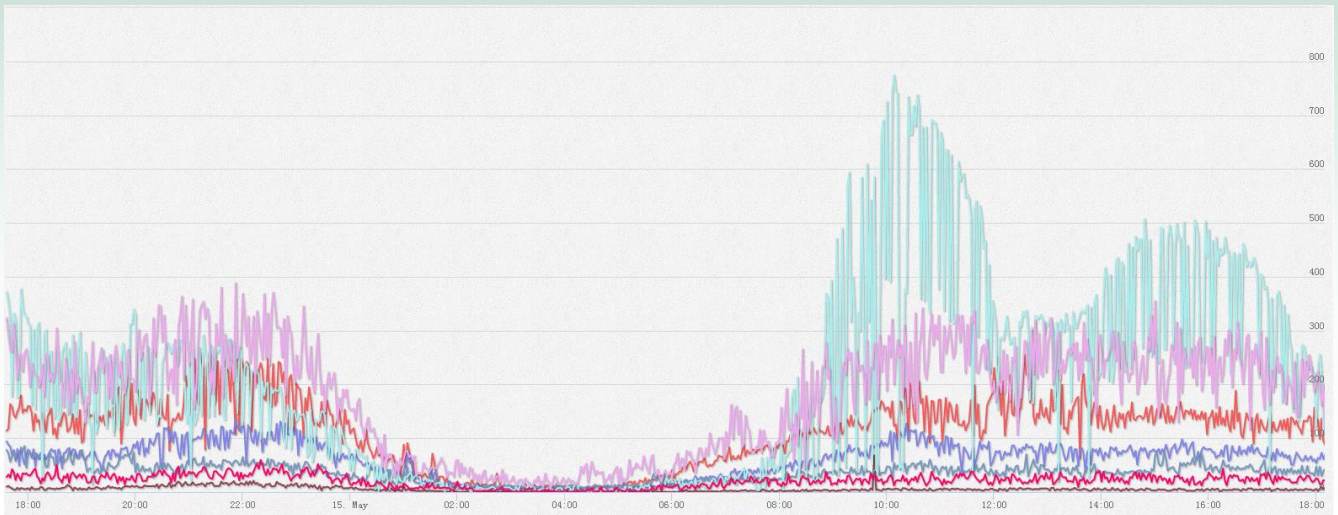
时间：2017-04-13 00:59:00

请关注！！！！！

耗时：0

每逢周五必有事

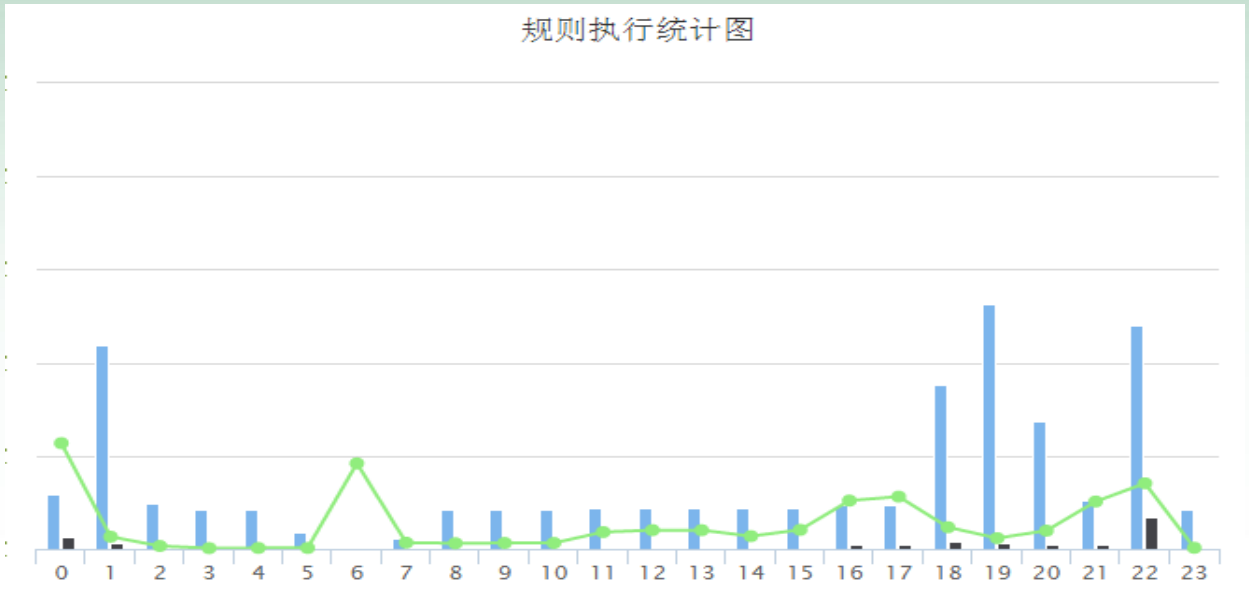
扫号不止，周末不休


800
700
600
500
400
300
200
18:00
20:00
22:00
15. May
02:00
04:00
06:00
08:00
10:00
12:00
14:00
16:00
18:00

封禁IP

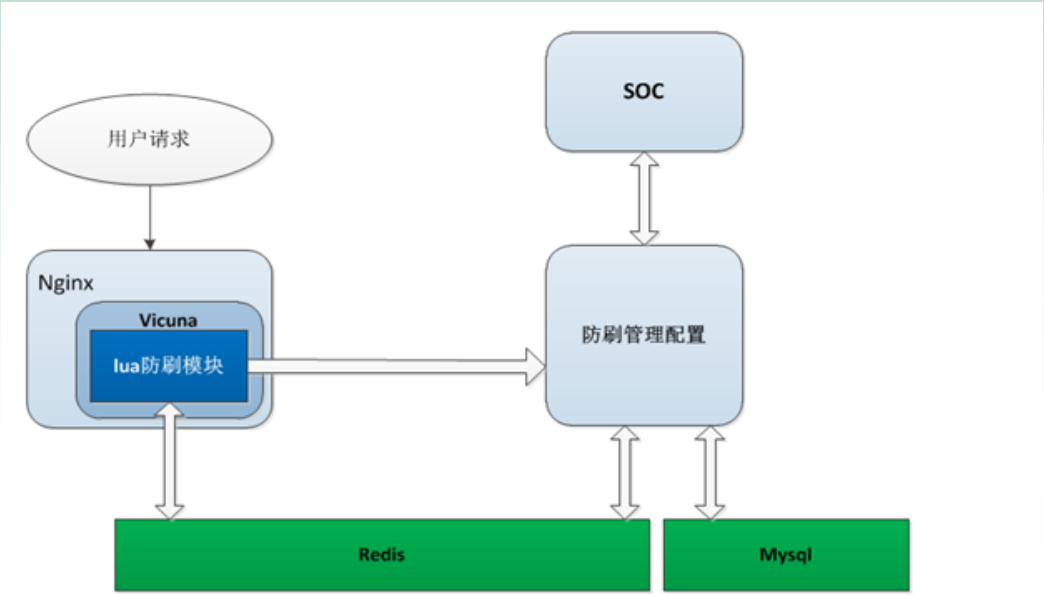
手动封禁IP：联系CDN、联系运维

风控拦截效果不理想

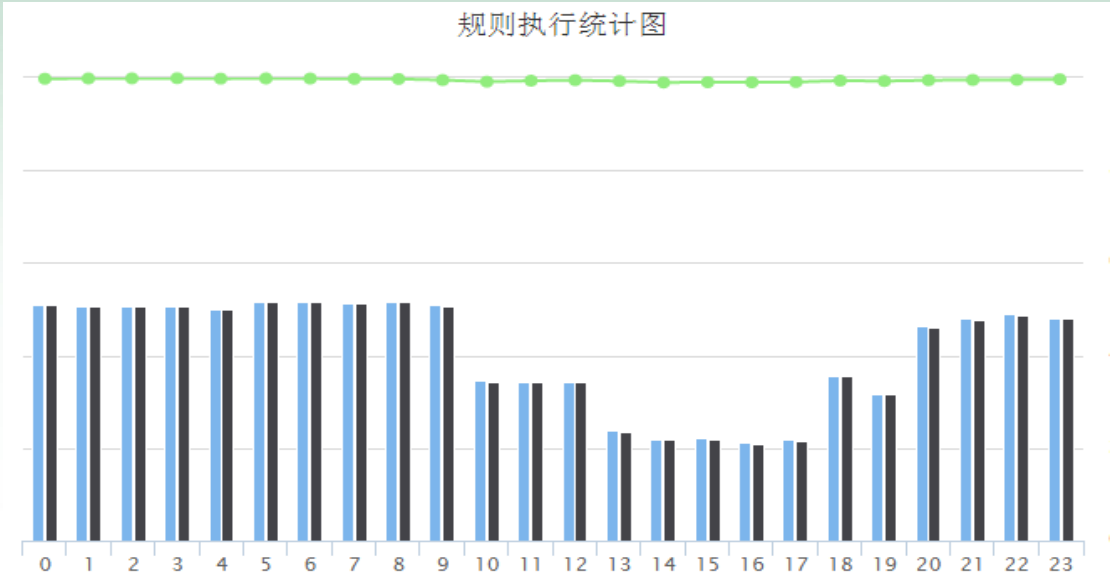


崩溃

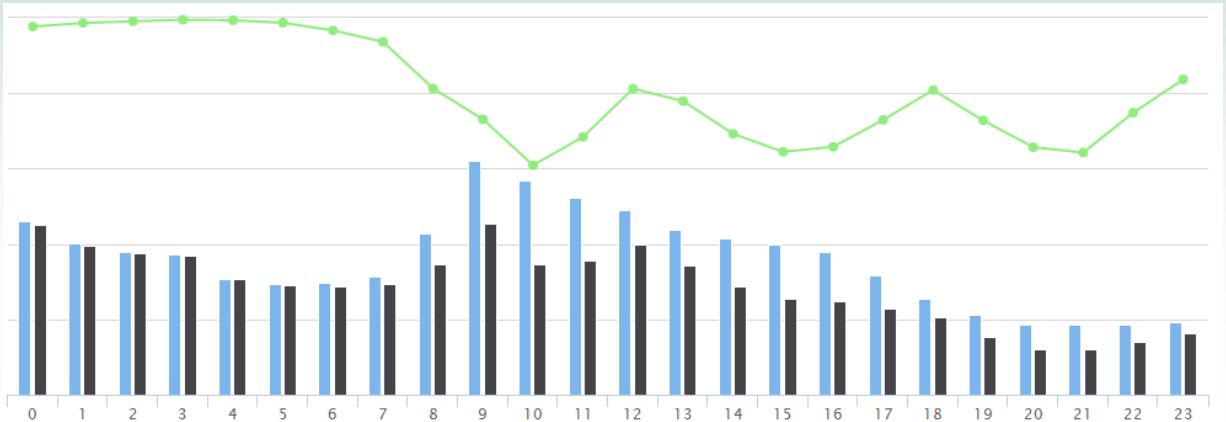
LUA



调整规则，增加挑战方式



撞库有所缓解，但仍远远不够



登录挑战

您的账户存在安全隐患，请选择身份验证方式：

通过绑定手机验证
如果您的手机还在正常使用，请选择此方法。 立即验证

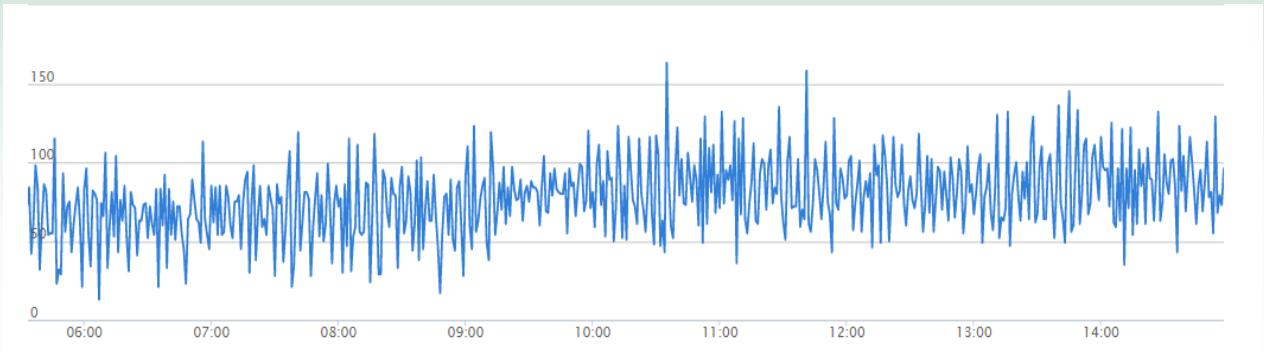
通过实名认证
如果您进行过实名验证，请选择此方式。 立即验证

通过购买商品验证
如果您记得近期购物的交易信息，请选择此方式。 立即验证

通过收货地址验证
如果您记得使用过的收货地址，请选择此方式。 立即验证

通过收藏品牌验证
如果您记得近期收藏过的品牌，请选择此方式。 立即验证

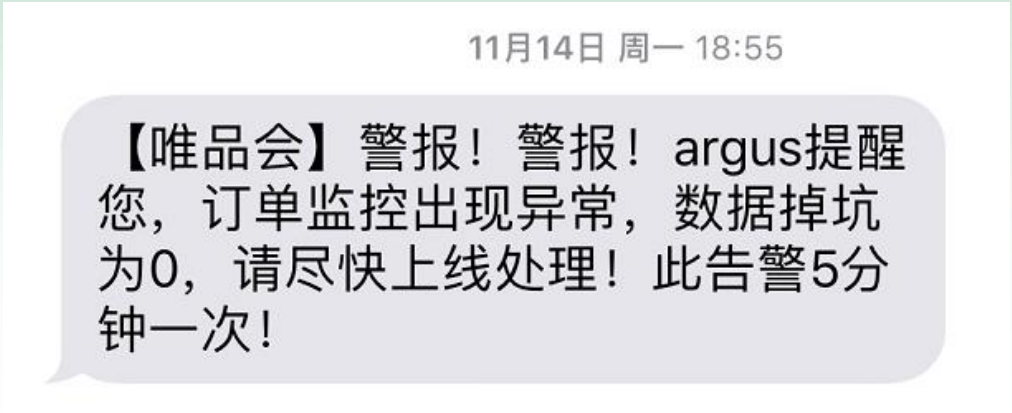
登录正常化



对抗永远是动态的

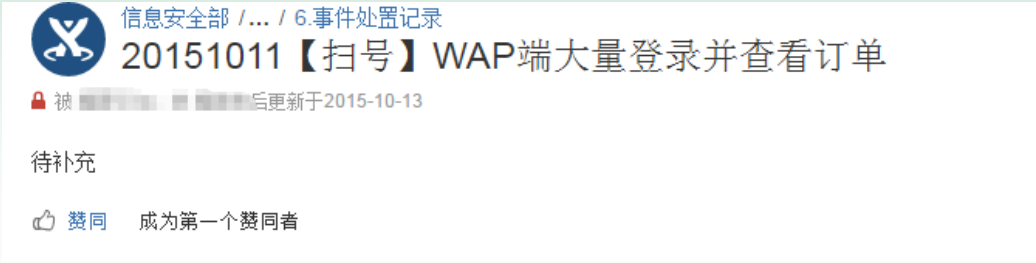
更好是我们努力的方向

警惕一切正常

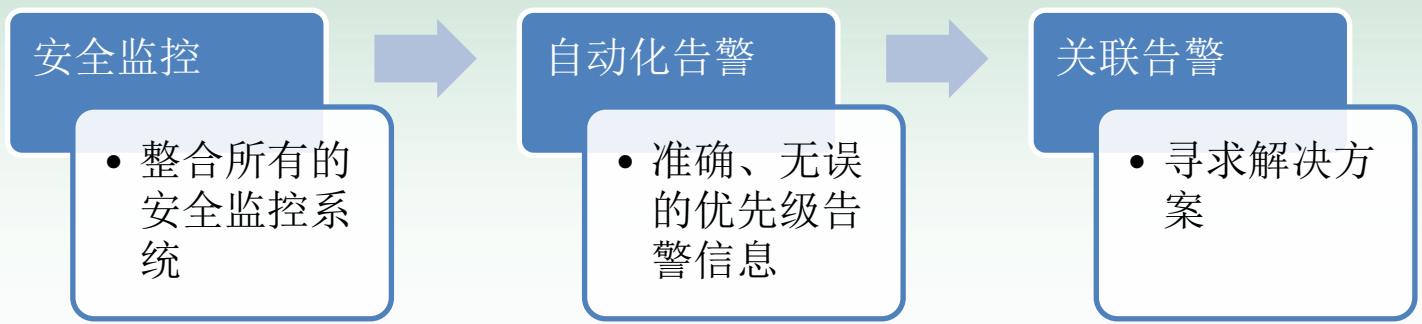

11月14日 周一 18:55
【唯品会】警报！警报！argus提醒您，订单监控出现异常，数据掉坑为0，请尽快上线处理！此告警5分钟一次！

事件记录和积累

买了一本如何克服拖延症的书，至今没翻过



事件关联



不喧哗，自有声

谢谢您的倾听！

唯品会 | 唯品会安全应急响应中心

VIP Security Response Center

唯品会安全应急响应中心

专业

我们致力于保护用户信息安全

我们积极营造更加安全的

线上电商购物平台

微信号：VIP_SRC

官方网站：http://sec.vip.com

微信公众号：唯品会安全应急响应中心

漏洞接收邮箱：sec@vipshop.com