



“互联网+”时代

# 大数据技术峰会

中国·深圳 | 2015.11.28-29

解码数据未来

# 京东金融宙斯Zeus安全防御平台



京东金融 刘明浩

一、业务安全的现状与挑战

二、如何保证业务安全运营

三、安全平台应用案例介绍

四、安全平台后续规划





# 业务面临的安全挑战

**传统安全解决方案无法解决**

## 业务安全风险

由于互联网金融业务特点，导致的安全漏洞，包括：

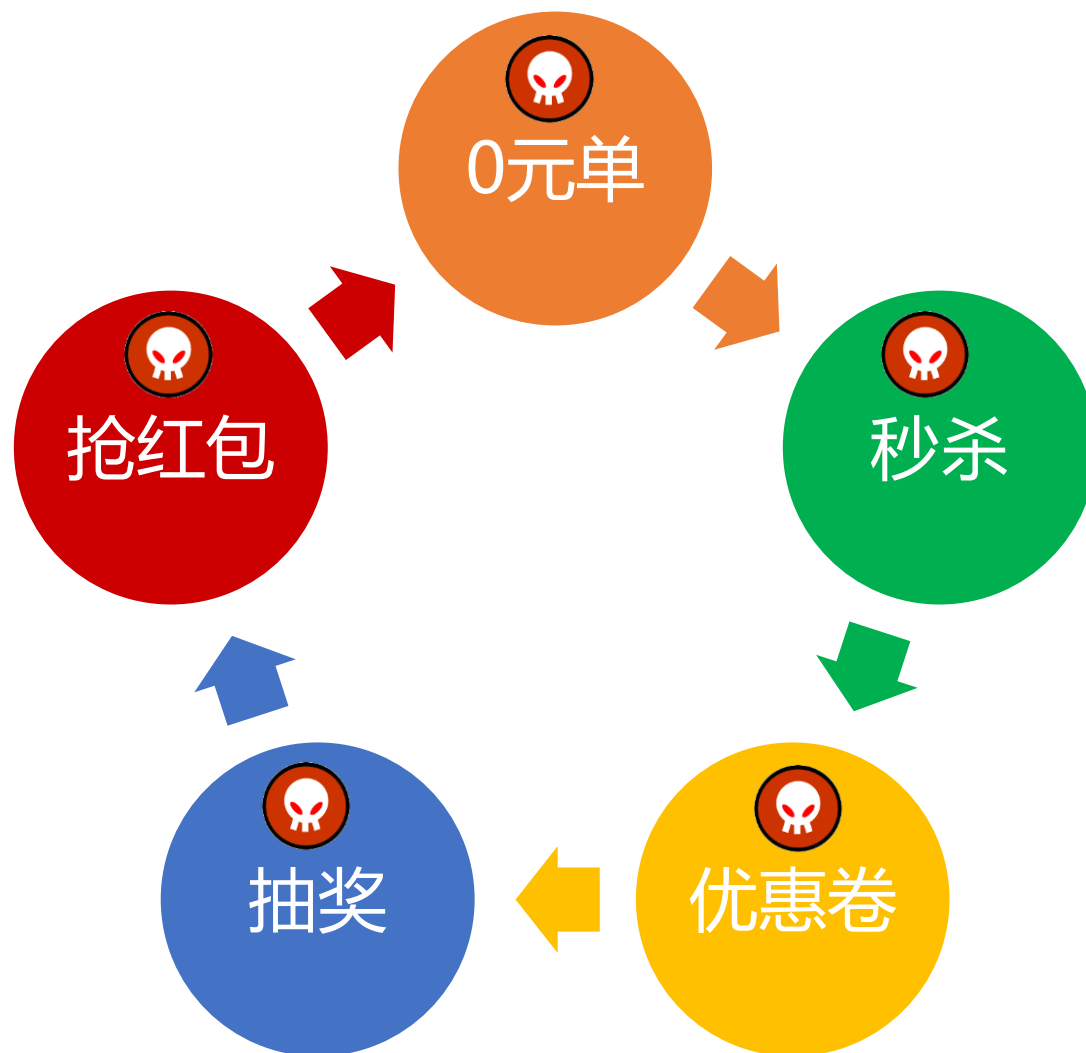
- ▶ 垃圾帐号注册
- ▶ 撞库扫号
- ▶ 平行权限
- ▶ 活动作弊
- ▶ 钓鱼欺诈

## 技术安全风险

所有互联网业务都可能面临的安全风险，包括：

- ▶ XSS跨站脚本
- ▶ CSRF跨站请求伪造
- ▶ Struts2
- ▶ SQL注入
- ▶ DDOS攻击

所以我们所面临的不仅仅是传统的黑客攻击



一、业务安全的现状与挑战

二、**如何保证业务安全运营**

三、业务应用典型案例介绍

四、安全平台后续规划





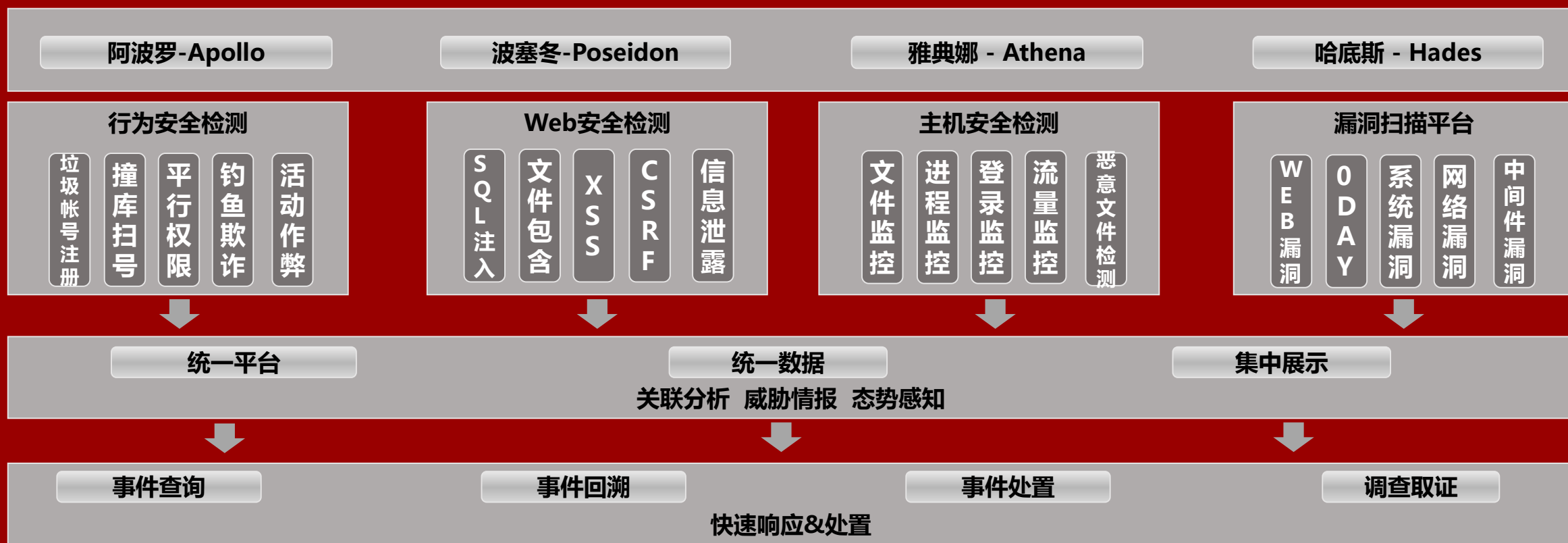
# 京东金融宙斯安全防御平台

京东金融宙斯平台的定位与初期目标：



# 京东金融宙斯安全防御平台

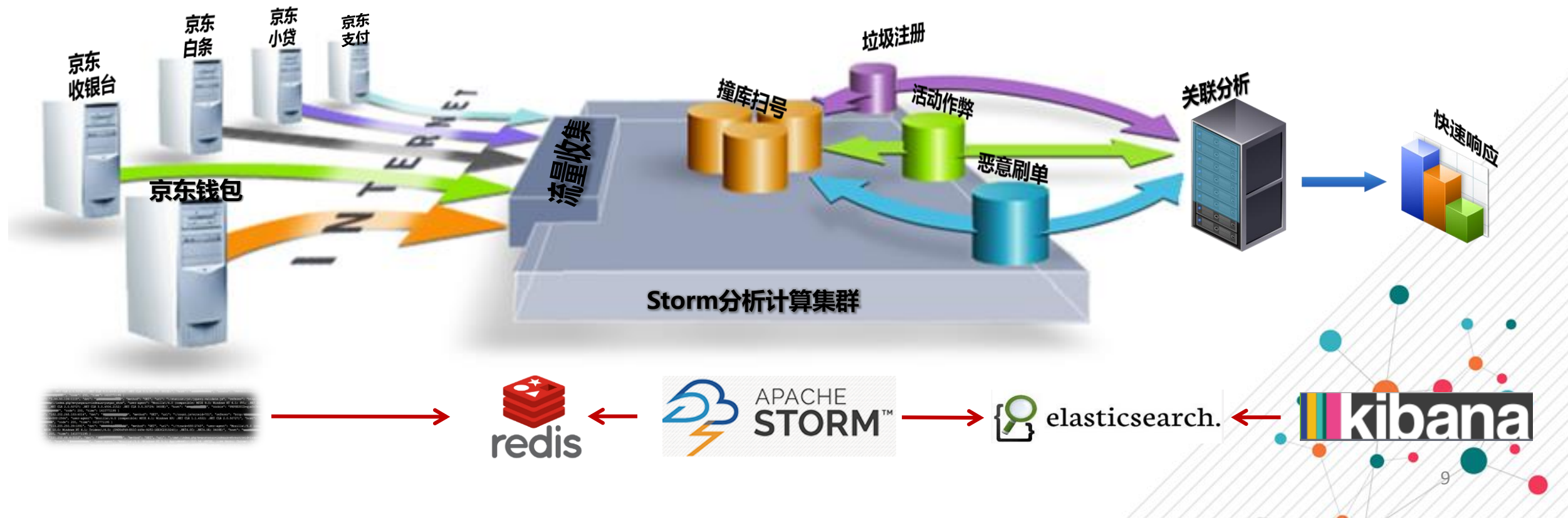
## 京东金融宙斯Zeus安全防御平台





# 行为安全检测平台(阿波罗Apollo)

行为安全检测平台：由流量收集、流量分析、数据存储与快速响应四部分组成。流量收集系统会将全流量中的访问请求进行收集与重组，并将重组后的HTTP日志打入Redis消息队列，流量分析Storm集群从Redis中取流量并根据分析模型进行异常行为分析，同时将流量存储到ElasticSearch中，再通过Kibana进行查询和展示



# 行为安全检测平台(阿波罗Apollo)

行为安全检测平台主要包括：流量收集、流量分析、数据存储与快速响应四部分组成。



# 行为安全检测平台(阿波罗Apollo)

风险领域		指标描述		阈值设定			数据收集方法				
风险领域	编号	描述	类型	容忍区	预警区	干预区	是否可收集到数据	数据来源	所需收集数据	预警及干预措施方法	备注
02.异常登录	R06	同一IP地址或同一IP地址段有大量用户频繁登录	预测型	<5个	≥5个,且≤10个	>10个	是	系统平台	a.同一IP地址或同一IP地址段有大量用户频繁登录	阈值到达干预区数据将IP地址或IP地址段发送风控	
02.异常登录	R07	用户多次输入密码错误	预测型	<5个	≥5个,且≤10个	>10个	是	系统平台	a.同一IP地址或同一IP地址段有大量用户频繁登录	阈值到达干预区数据将IP地址或IP地址段发送风控	
03.异常业务请求	R08	用户自动下单	预测型	<5个	≥5个,且≤10个	>10个	是	系统平台	a.同一IP地址或同一IP地址段有大量用户频繁登录	阈值到达干预区数据将IP地址或IP地址段发送风控	
03.异常业务请求	R09	用户修改绑定卡信息	预测型	<5个	≥5个,且≤10个	>10个	是	系统平台	a.同一IP地址或同一IP地址段有大量用户频繁登录	阈值到达干预区数据将IP地址或IP地址段发送风控	
04.异常支付	R10	用户转账支付时的表单重复提交	预测型	<5个	≥5个,且≤10个	>10个	是	系统平台	a.同一IP地址或同一IP地址段有大量用户频繁登录	阈值到达干预区数据将IP地址或IP地址段发送风控	



## 业务风险地图(业务安全风控模型)

1. 根据业务场景进行分析可能带来的业务安全风险
2. 根据风险容忍度设置监控预警阈值
3. 根据风险指标设计数据收集方法及干预/阻断措施

1

2

3

风险领域		指标描述		阈值设定			数据收集方法				
风险领域	编号	描述	类型	容忍区	预警区	干预区	是否可收集到数据	数据来源	所需收集数据	预警及干预措施方法	备注
02.异常登录	R06	同一IP地址或同一IP地址段有大量用户频繁登录	预测型	<5个	≥5个,且≤10个	>10个	是	系统平台	a.同一IP地址或同一IP地址段有大量用户频繁登录	阈值到达干预区数据将IP地址或IP地址段发送风控进行拦截	

# 行为安全检测平台(阿波罗Apollo)

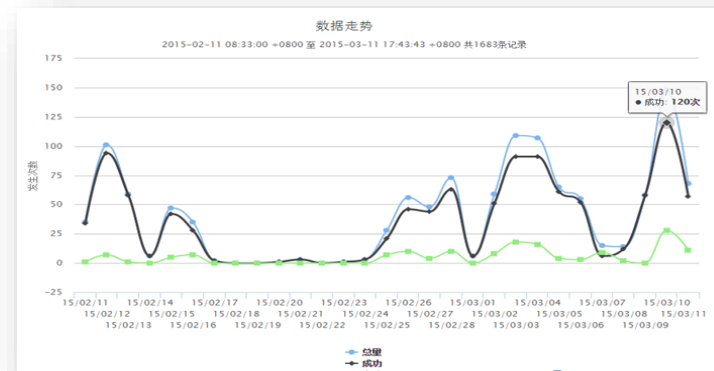
## 登录频率监控

通过对线上流量的实时监控，实现对登录URL请求进行实时监控，包括撞库扫号、暴力破解等行为可在第一时间产生报警及时作出响应。

时间	种类	用户	执行结果	国家	城市	详细数据
03/11 17:47:49	支付0		成功	CN	Chaoyang	{src_ip:"60.247.77.253", code:"200", method:"POST", real_url:"/cashier.js.com/quicklogin/GetVerifyCode.action", "amount":0}
03/11 17:47:49	支付0		成功	CN	Beijing	{src_ip:"123.88.246.209", code:"200", method:"POST", real_url:"/cashier.js.com/quicklogin/GetVerifyCode.action", "amount":0}
03/11 17:47:49	APP登录	13866444832	失败	CN	Hefei	{src_ip:"36.63.16.22", code:"200", method:"POST", real_url:"m.wangyin.com/userapp/login"}
03/11 17:47:48	APP登录	18287354563	成功	CN		{src_ip:"117.136.72.167", code:"200", method:"POST", real_url:"m.wangyin.com/userapp/login"}
03/11 17:47:48	支付0		成功	CN	Hefei	{src_ip:"120.210.161.94", code:"200", method:"POST", real_url:"/cashier.js.com/quicklogin/GetVerifyCode.action", "amount":0}
03/11	APP登录	15511297666	成功	CN	Hebei	{src_ip:"111.225.100.236", code:"200", method:"POST", "amount":0}

## 垃圾注册监控

通过对线上流量的实时监控，实现对注册URL请求进行实时监控，包括垃圾注册、养号等行为可在第一时间产生报警及时作出响应。



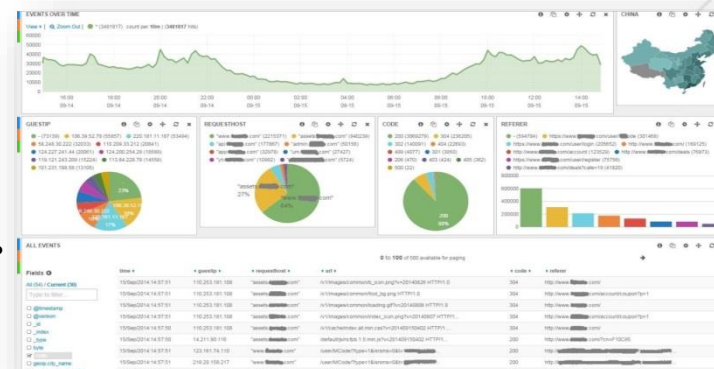
## 可疑用户跟踪

通过对账号体系建立基础数据库对用户的登录地点、登录时间、登录频率作出异常预警，及时保障用户账号安全。

源IP	国家	省市	总数	失败量	成功率	操作
218.68.5.140	CN	Tianjin	123	115	6%	时间段内所有行为  所有行为
114.251.186.16	CN	Beijing	77	0	100%	时间段内所有行为  所有行为
119.4.57.25	CN	Chengdu	68	0	100%	时间段内所有行为  所有行为
123.127.211.100	CN	Beijing	67	6	91%	时间段内所有行为  所有行为
115.228.238.76	CN	Jiaxing	56	47	16%	时间段内所有行为  所有行为
125.120.13.117	CN	Hangzhou	46	0	100%	时间段内所有行为  所有行为
218.201.184.231	CN	Jinan	43	0	100%	时间段内所有行为  所有行为
103.226.199.219	CN	Chengdu	43	1	97%	时间段内所有行为  所有行为
221.6.254.226	CN	Nanjing	42	1	97%	时间段内所有行为  所有行为
59.49.251.9	CN	Haikou	42	0	100%	时间段内所有行为  所有行为

## 安全态势感知

通过对业务安全事件的关联分析，导出威胁情报及业务安全态势感知。

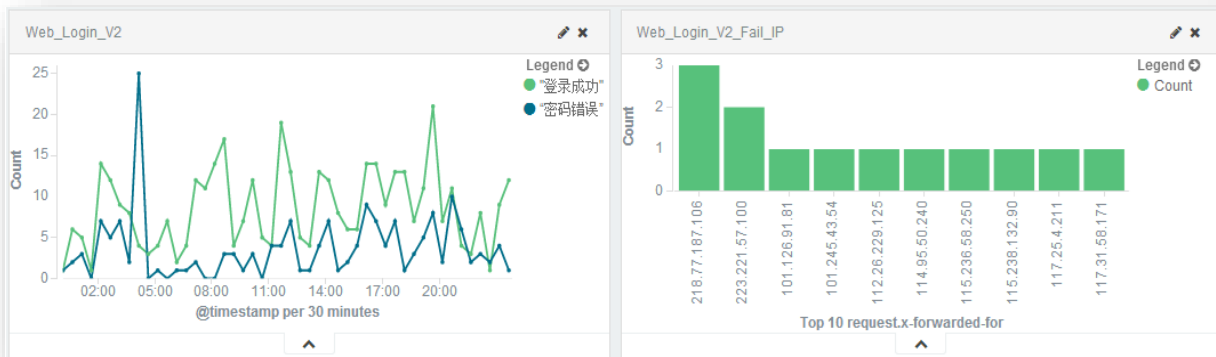




# 行为安全检测平台(阿波罗Apollo)

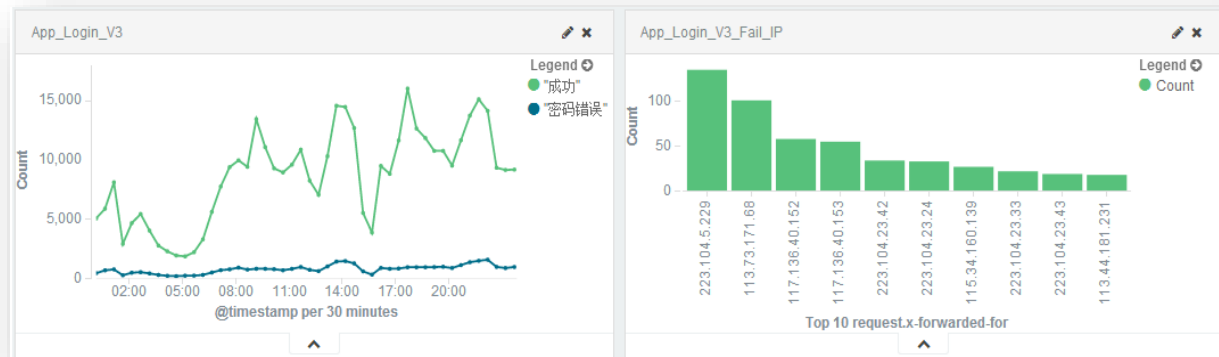
## “暴力破解”行为监控

通过对线上业务登录成功及失败行为的实时监控



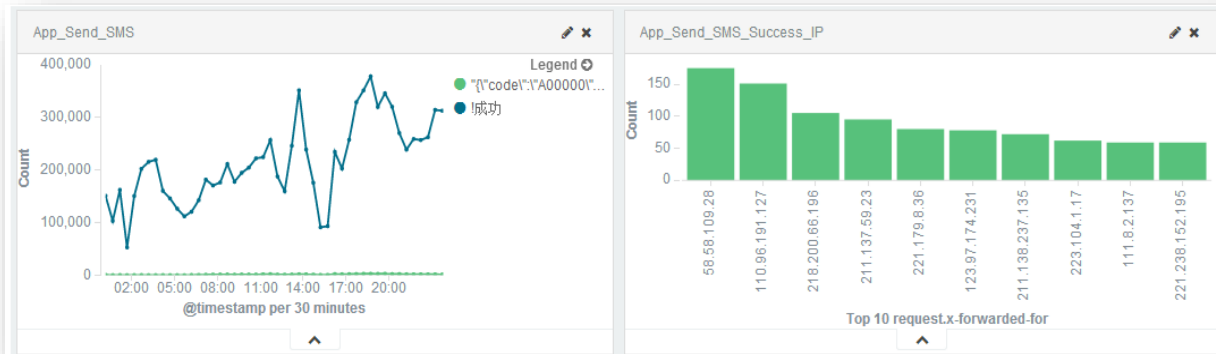
## “撞库扫号”行为监控

通过对线上业务登录成功及失败行为的实时监控



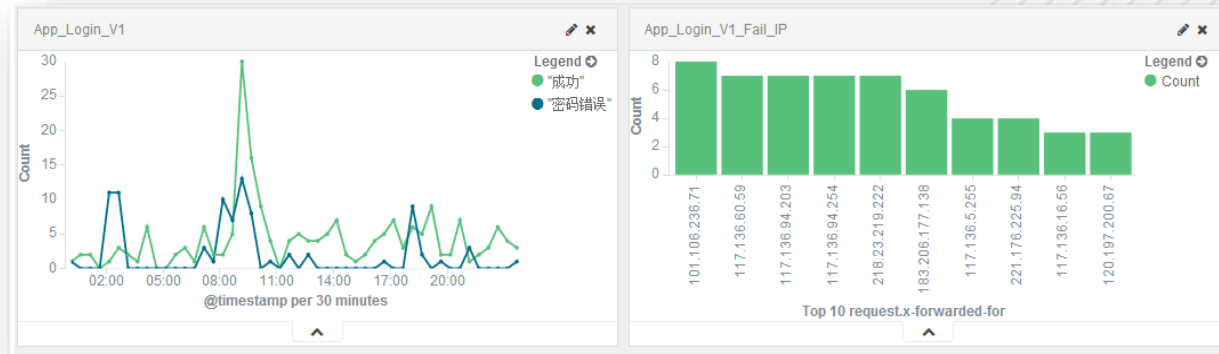
## “短信炸弹”行为监控

通过对线上所有短信验证接口进行实时监控



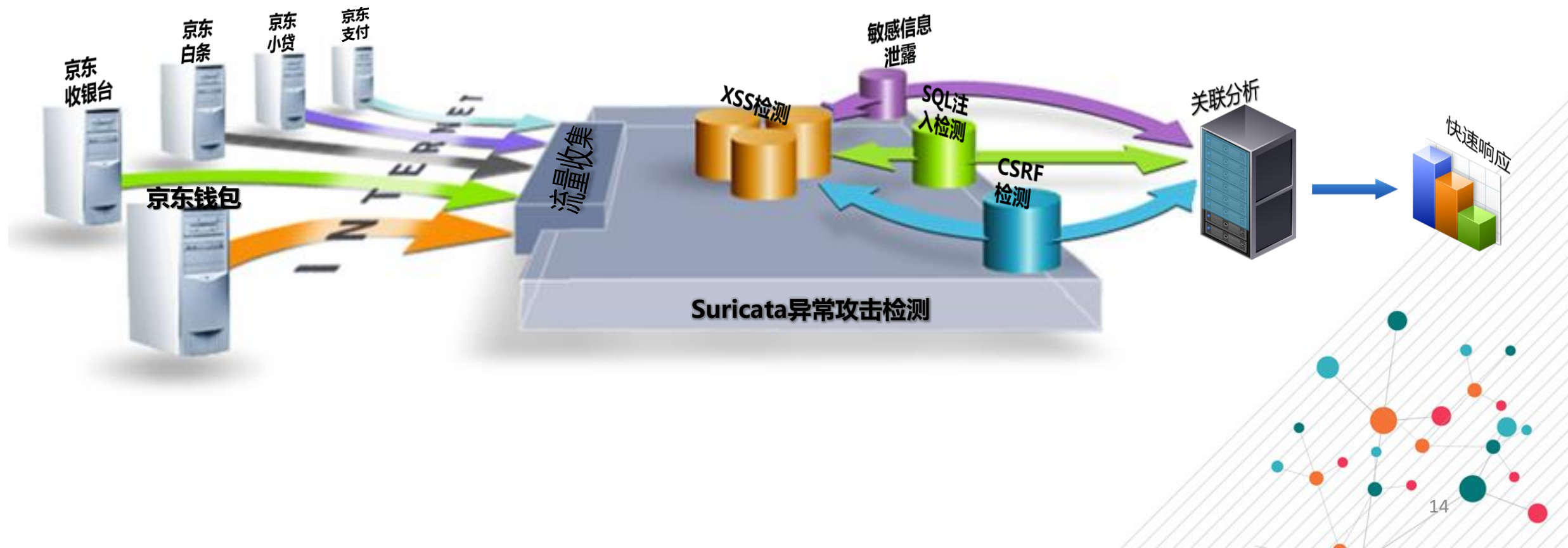
## “垃圾帐号注册”行为监控

通过对线上所有业务的注册行为(频繁注册)进行实时监控



# Web安全检测平台(波塞冬Poseidon)

Web安全检测平台：通过Suricata对全流量进行web应用安全检测，包括XSS跨站脚本攻击、SQL注入攻击、CSRF跨站请求伪造、目录遍历等安全威胁

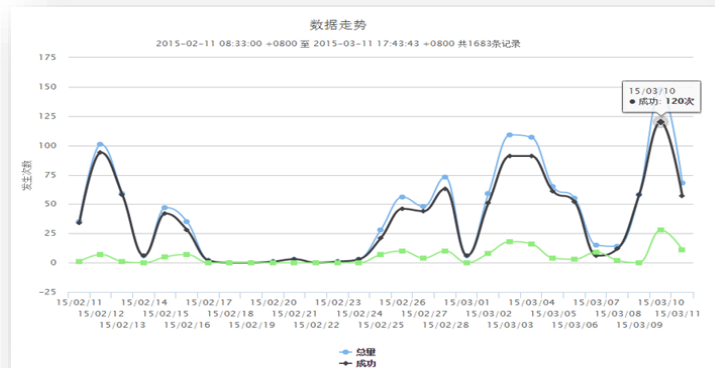


# Web安全检测平台(波塞冬Poseidon)

## 攻击类型

异常行为摘要	高级搜索	时间	种类	用户	执行结果	国家	城市	详细数据
详细列表		03/11 17:47:49	支付0		成功	CN	Chaoyang	[src_ip=>"60.247.77.253", code=>"200", method=>"POST", real_uri=>"cashier.jd.com/quick/asyncGetVerifyCode.action", "amount">"[REDACTED]"]
详细记录		03/11 17:47:49	支付0		成功	CN	Beijing	[src_ip=>"123.88.246.209", code=>"200", method=>"POST", real_uri=>"cashier.jd.com/quick/asyncGetVerifyCode.action", "amount">"[REDACTED]"]
实时报警		03/11 17:47:49	APP登录	13866444832	失败	CN	Hefei	[src_ip=>"36.63.16.22", code=>"200", method=>"POST", real_uri=>"m.wangyin.com/user/appLogin"]
分频分析		03/11 17:47:49	APP登录	16287354563	成功	CN		[src_ip=>"117.136.72.167", code=>"200", method=>"POST", real_uri=>"m.wangyin.com/user/appLogin"]
WEB登录		03/11 17:47:49	支付0		成功	CN	Hefei	[src_ip=>"120.210.161.94", code=>"200", method=>"POST", real_uri=>"cashier.jd.com/quick/asyncGetVerifyCode.action", "amount">"[REDACTED]"]
WEB注册		03/11 17:47:49	APP登录	15511297686	成功	CN	Hebei	[src_ip=>"111.225.100.236", code=>"200", method=>"POST",
APP登录								
APP注册								
JS联合登录								
验证码验证								

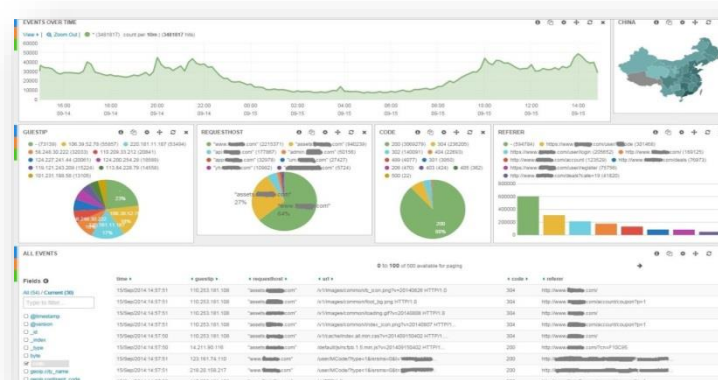
## 受攻击业务



## 攻击源IP

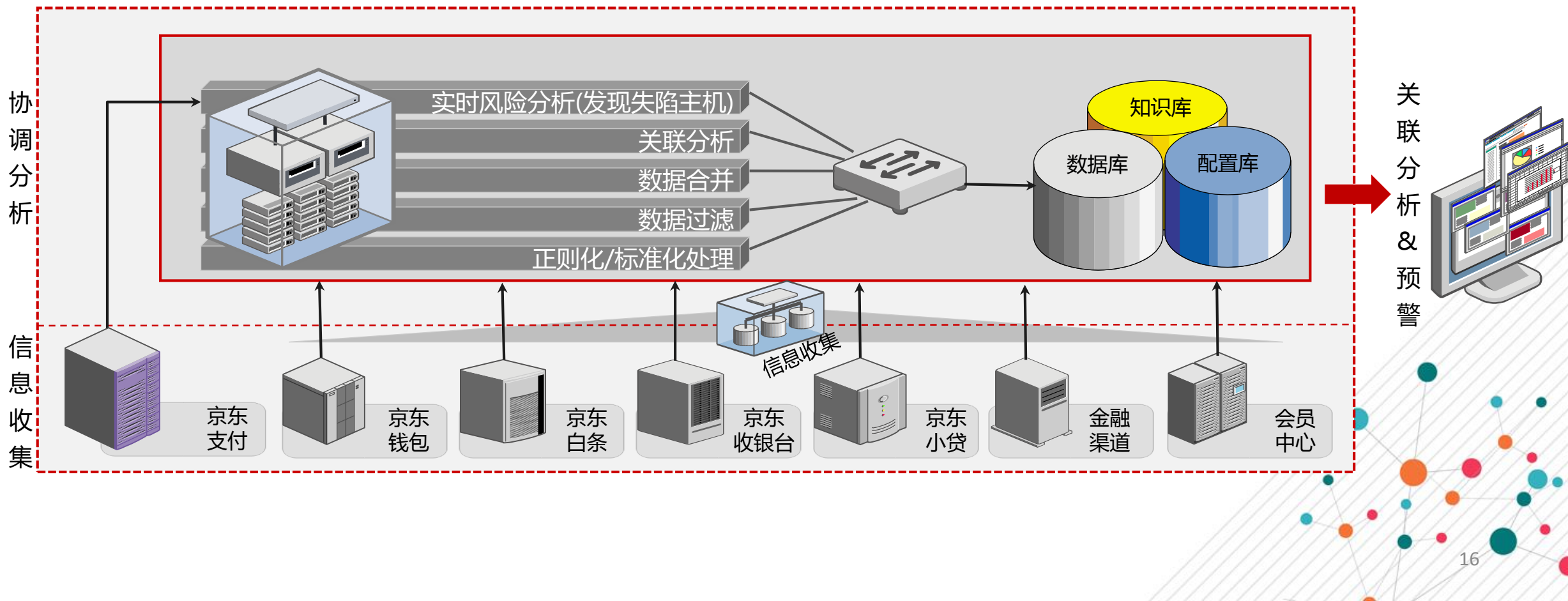
IP排名	源IP	国家	省市	总条数	失败量	成功率	操作
216.9	[REDACTED]	CN	Tianjin	123	115	6%	时间段内所执行行为: 异常行为
154.221	[REDACTED]	CN	Beijing	77	0	100%	时间段内所执行行为: 异常行为
172.16.172.130	[REDACTED]	CN	Chengdu	66	0	100%	时间段内所执行行为: 异常行为
155.106.15.76	[REDACTED]	CN	Beijing	67	6	91%	时间段内所执行行为: 异常行为
155.117	[REDACTED]	CN	Jiangxi	56	47	16%	时间段内所执行行为: 异常行为
194.221	[REDACTED]	CN	Hangzhou	46	0	100%	时间段内所执行行为: 异常行为
199.219	[REDACTED]	CN	Jinan	43	0	100%	时间段内所执行行为: 异常行为
154.226	[REDACTED]	CN	Chengdu	43	1	97%	时间段内所执行行为: 异常行为
155.13	[REDACTED]	CN	Nanjing	42	1	97%	时间段内所执行行为: 异常行为
	[REDACTED]	CN	Hakou	42	0	100%	时间段内所执行行为: 异常行为

## 攻击趋势统计



# 主机安全检测平台(雅典娜Athena)

主机安全检测平台：通过部署agent的方式到每台服务器上，实现对文件完整性监控、恶意代码扫描、登录行为监控、进程监控、主机流量监控等功能



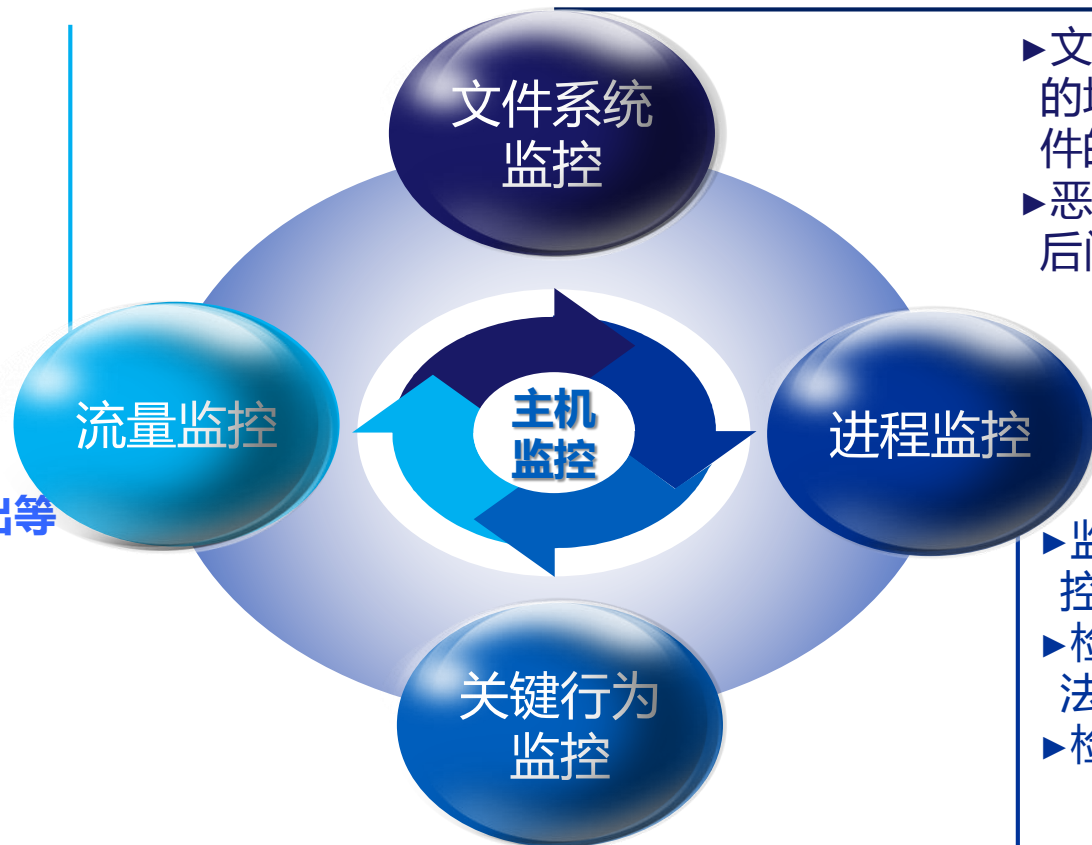


# 主机安全检测平台(雅典娜Athena)

主机安全检测平台主要包括：文件系统监控、进程监控、关键行为监控及性能监控四部分。

## ► 主机流量异常

► SSH及MySQL的登录、登出等进行行为监控

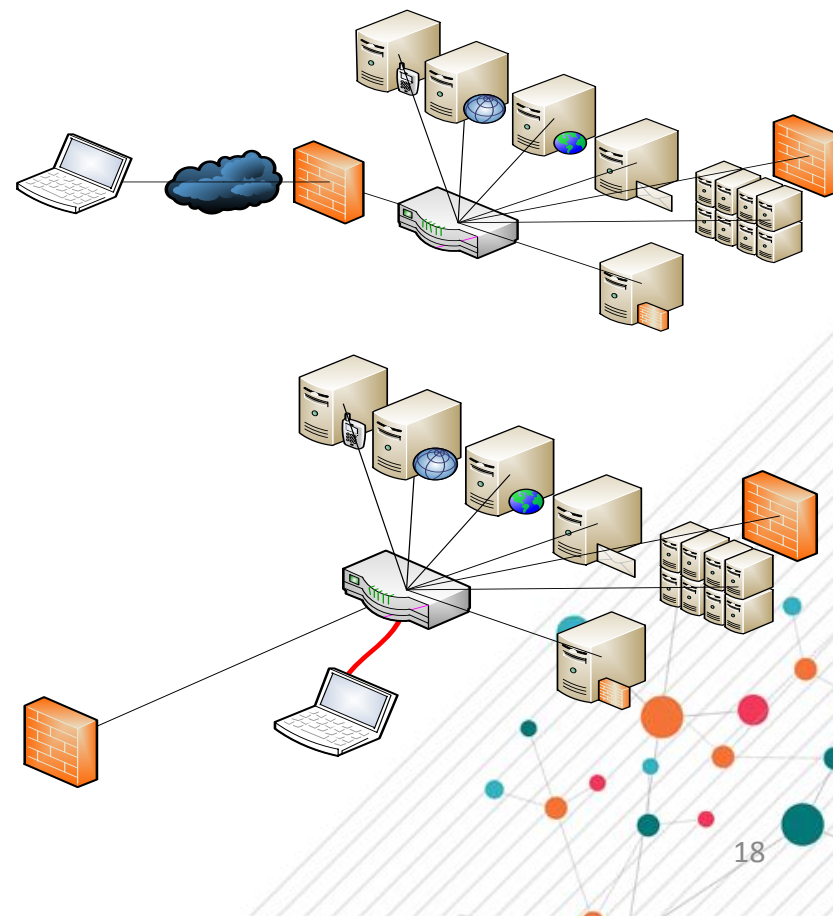
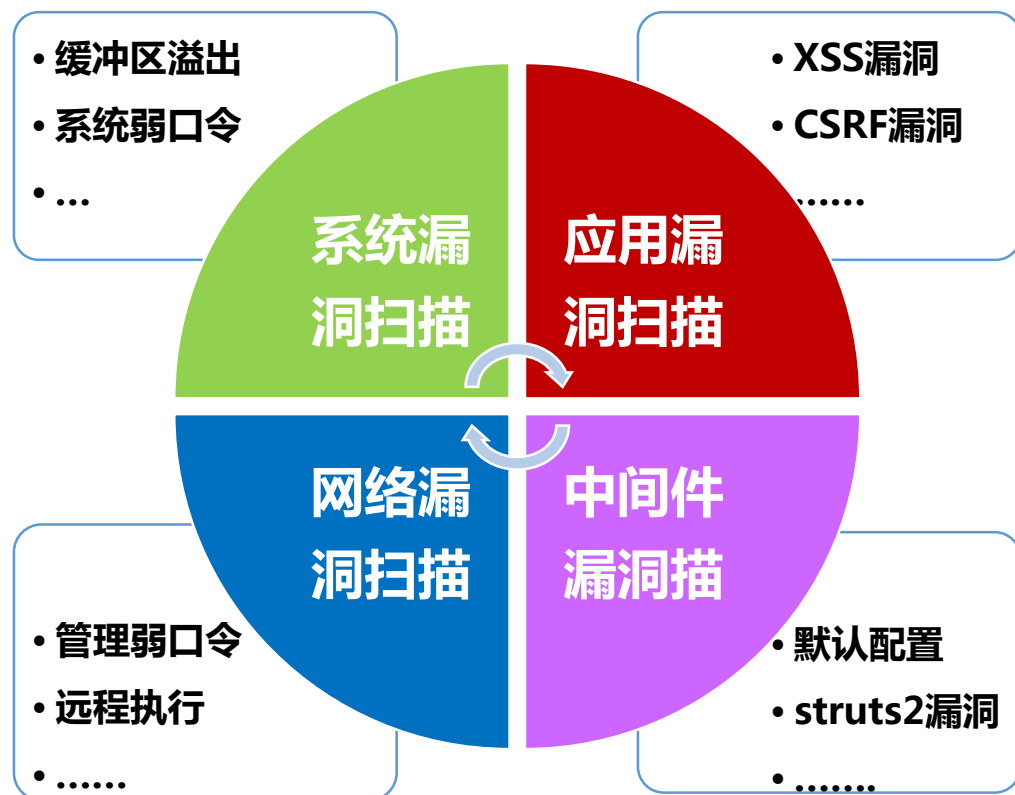


- 文件完整性监控：对文件系统的增删查进行监控，对重要文件的修改进行记录；
- 恶意文件检测，包括（木马、后门、病毒等）分析

- 监控进程创建、敏感进程监控
- 检测建立进程的用户是否合法
- 检测父进程是否合理

# 漏洞扫描平台(哈底斯Hades)

基于W3AF搭建的漏洞扫描平台是一个Web应用程序攻击检查框架，可以通过灵活的添加漏洞检测插件进行突发0day以及日常漏洞扫描



- 一、业务安全的现状与挑战
- 二、如何保证业务安全运营
- 三、安全平台应用案例介绍
- 四、安全平台后续规划

# 宙斯系统实际应用场景

使用宙斯平台进行安全事件分析与响应

事件分析&解决过程

## 事件解决

- 1、测试业务是否修复
- 2、管理后台上线

## 取证及处置跟踪

- 1、留存所有访问日志
- 2、通知研发第一时间修复漏洞

## 事件分析

- 1、根据分析确定攻击者利用垂直越权漏洞得到后台管理员权限

## 事件分析

- 1、找到重要IP整个操作痕迹
- 2、后来的某一个请求由一个普通用户修改成管理员

## 事件分析

- 1、访问后台的请求中筛选访问修改后台密码的请求
- 2、通过分析筛选得到几个重要源IP

## 事件响应及回溯

- 1、通过后台立即将密码改回防止业务风险
- 2、立即在ES全流量当中筛选访问后台的全部请求

## 事件发现及报告

- 1、发现某系统运营管理后台管理员密码被改
- 2、宙斯平台第一时间发出报警



- 一、业务安全的现状与挑战
- 二、如何保证业务安全运营
- 三、安全平台应用案例介绍
- 四、安全平台后续规划

隐私保护

用户画像

威胁情报

态势感知

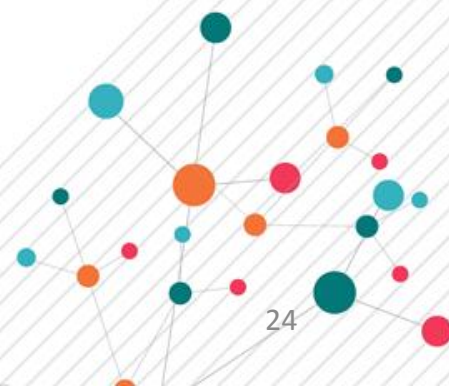


# 京东金融宙斯安全防御平台 - 规划

京东金融宙斯安全防御平台规划：从以**漏洞为中心**的防御思路，向以**威胁为中心**进行转化，最终实现**数据来驱动业务安全**。



谢谢！





Thank you