
51CTO
WOT 2015
“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：

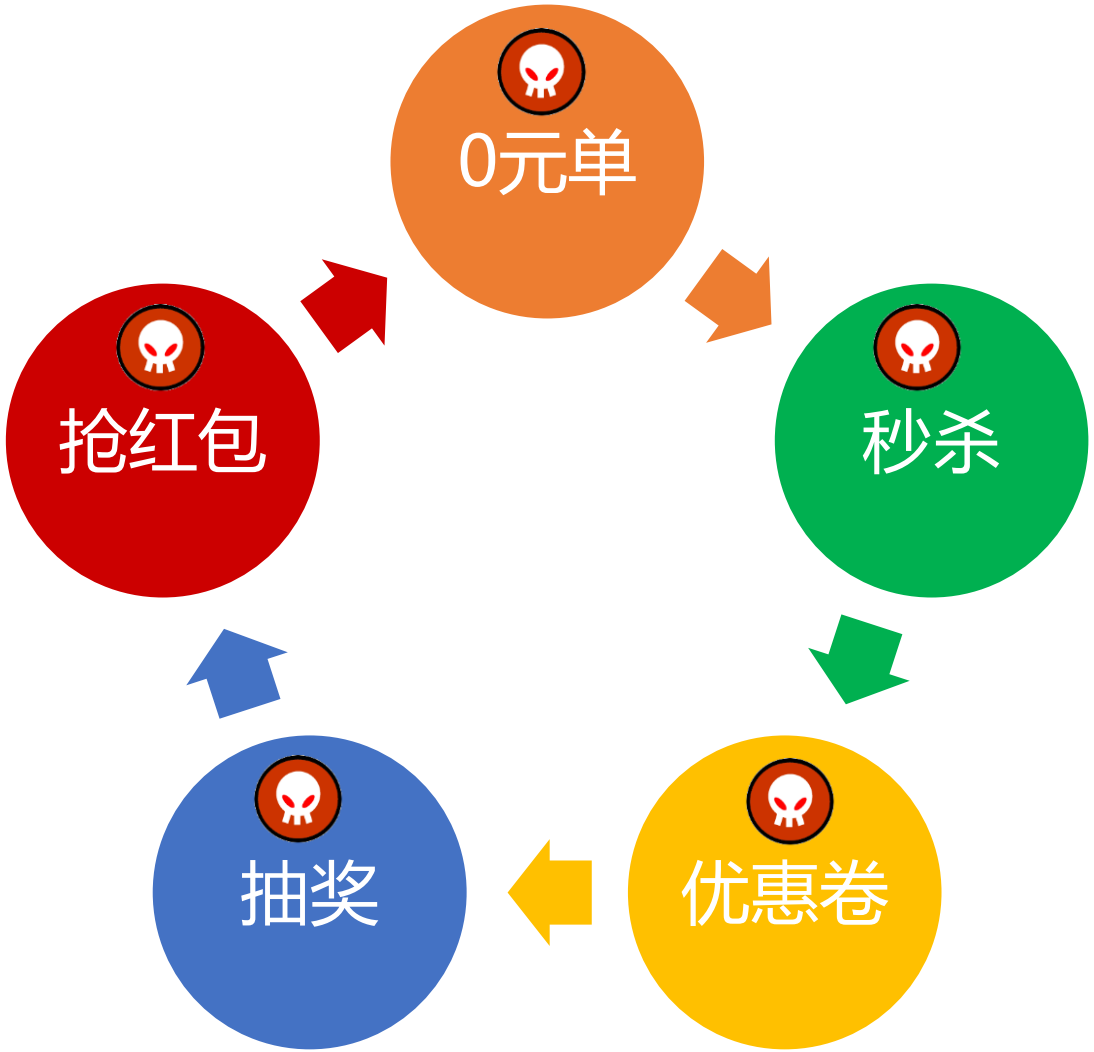
- 垃圾帐号注册
- 撞库扫号
- 平行权限
- 活动作弊
- 钓鱼欺诈

- 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：

**1. 整体安全威胁**

- 从整体层面考虑业务安全与技术安全风险

**5. 低耦合、扩展性强**

- 从业务数据流角度不嵌入业务核心逻辑，不降低系统效率，扩展性强适应业务的流量突增

**京东金融宙斯安全防御平台**

**2. 业务风险事件**

- 对撞库、扫号、刷单以及盗卡等异常业务行为进行检测和防御

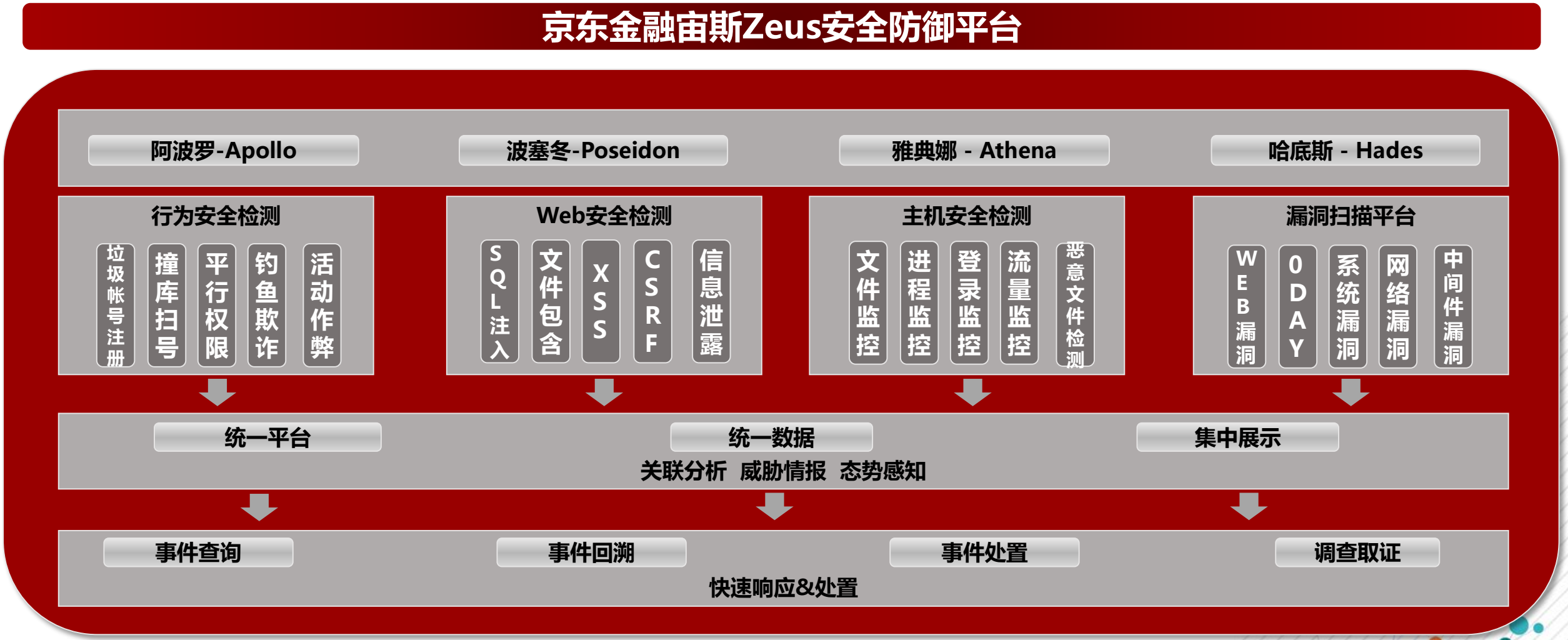
**4. 全业务流量日志存储与实时查询**

- 用户敏感操作、异常行为实时分析与存储

**3. Web安全攻击**

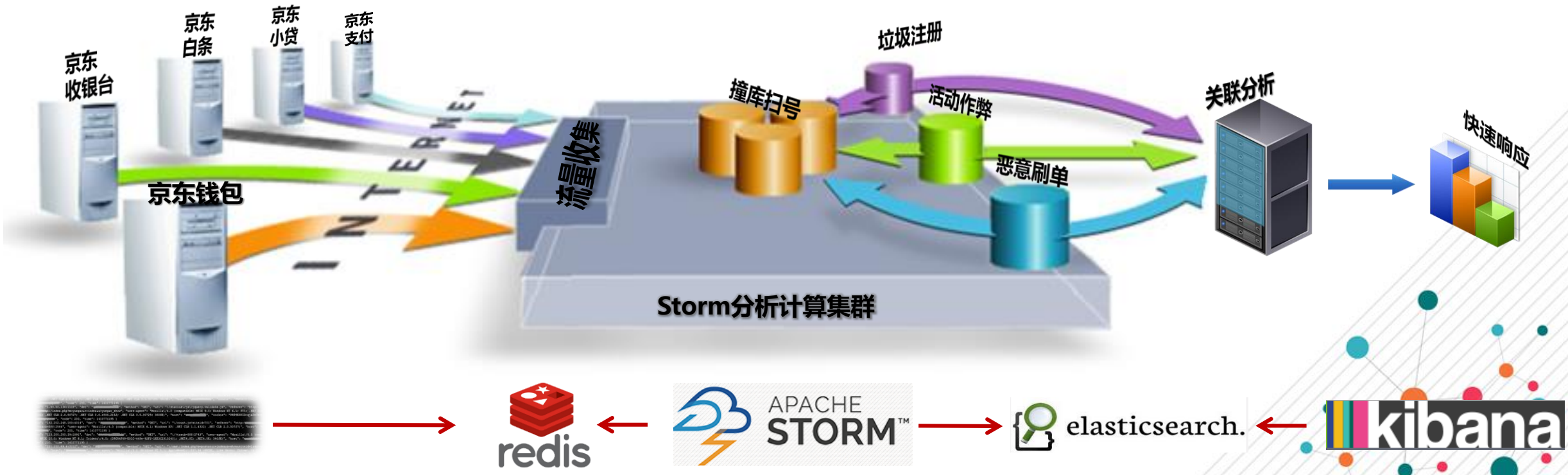
- 对主要的web攻击进行检测和防御包括：XSS跨站脚本攻击、CSRF跨站请求伪造、SQL注入、目录遍历等

# 京东金融宙斯安全防御平台



# 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。

流量收集

- 全流量镜像
- 流量解析
- 流量重组

流量分析

- 业务安全风控模型
- 动态规则匹配
- 事件识别

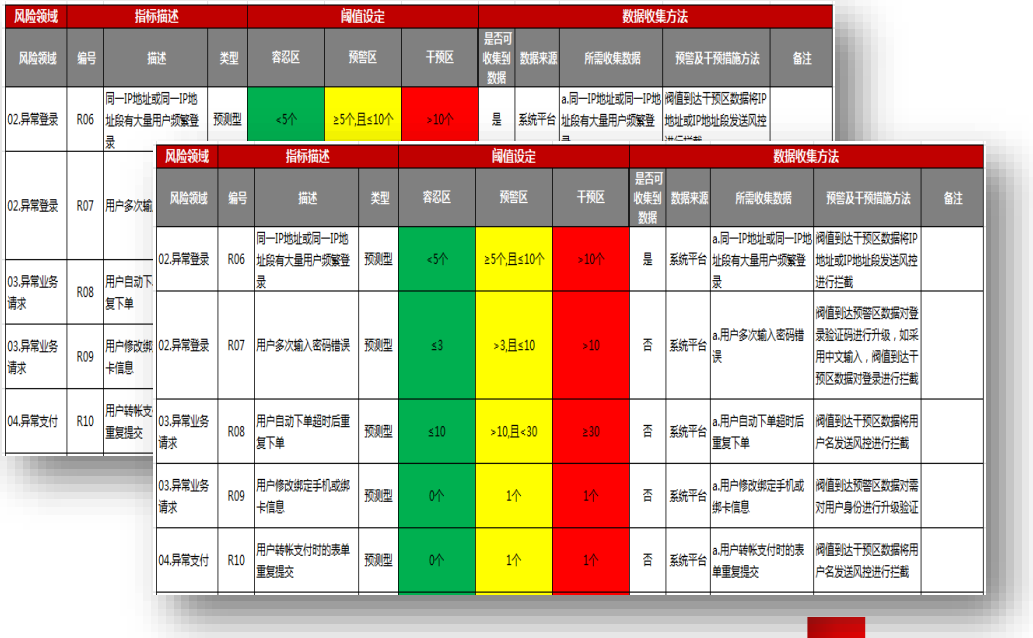
数据存储

- 数据存储
- 实时查询
- 威胁情报

快速响应

- 事件预警
- 系统接口
- 拦截阻断

# 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 | 阀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 | |
| 02.异常登录 | R07 | 用户多次输入密码错误 | 预测型 | ≤3 | >3,且≤10 | >10 | 否 | 系统平台 | a.用户多次输入密码错误 | 阀值到达预警区数据对登录验证码进行升级，如采用中文输入，阀值到达干预区数据对登录进行拦截 | |
| 03.异常业务请求 | R08 | 用户自动下单超时后重复下单 | 预测型 | ≤10 | >10,且<30 | ≥30 | 否 | 系统平台 | a.用户自动下单超时后重复下单 | 阀值到达干预区数据将用户名发送风控进行拦截 | |
| 03.异常业务请求 | R09 | 用户修改绑定手机或绑卡信息 | 预测型 | 0个 | 1个 | 1个 | 否 | 系统平台 | a.用户修改绑定手机或绑卡信息 | 阀值到达预警区数据对需对用户身份进行升级验证 | |
| 04.异常支付 | R10 | 用户转帐支付时的表单重复提交 | 预测型 | 0个 | 1个 | 1个 | 否 | 系统平台 | a.用户转帐支付时的表单重复提交 | 阀值到达干预区数据将用户名发送风控进行拦截 | |

## 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阀值
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

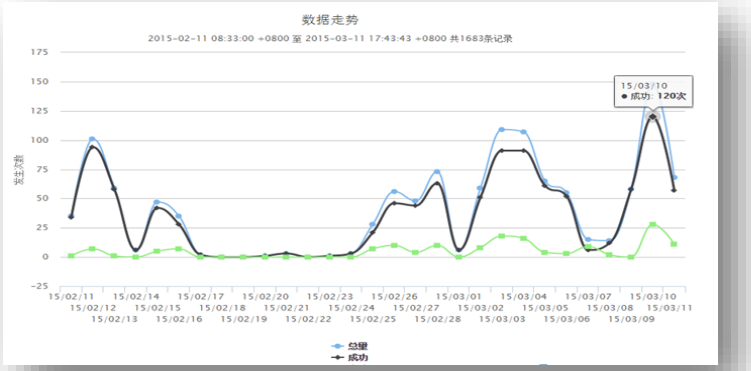
| 风险领域 | 指标描述 | | | 阈值设定 | | | 数据收集方法 | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 风险领域 | 编号 | 描述 | 类型 | 容忍区 | 预警区 | 干预区 | 是否可收集到数据 | 数据来源 | 所需收集数据 | 预警及干预措施方法 | 备注 |
| 02.异常登录 | R06 | 同一IP地址或同一IP地址段有大量用户频繁登录 | 预测型 | <5个 | ≥5个,且≤10个 | >10个 | 是 | 系统平台 | a.同一IP地址或同一IP地址段有大量用户频繁登录 | 阀值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

## 垃圾注册监控

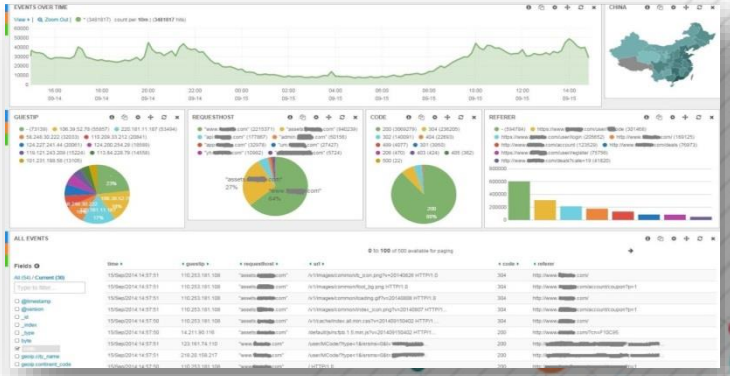



通过对线上流量的实时监控，实现对注册URL请求进行实时监控，包括垃圾注册、养号等行为可在第一时间产生报警及时作出响应。


## 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。

## 安全态势感知

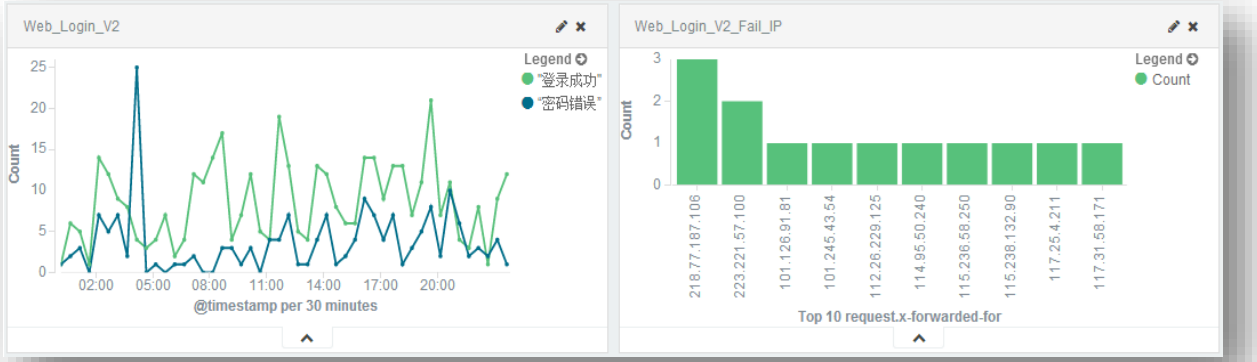


通过对业务安全事件的关联分析，导出威胁情报及业务安全态势感知。

# 行为安全检测平台(阿波罗Apollo)

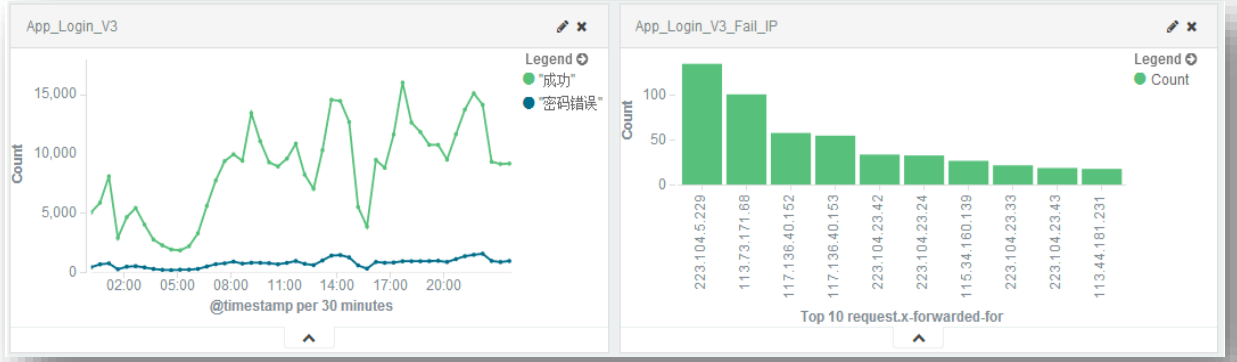
## “暴力破解”行为监控

通过对线上业务登录成功及失败行为的实时监控



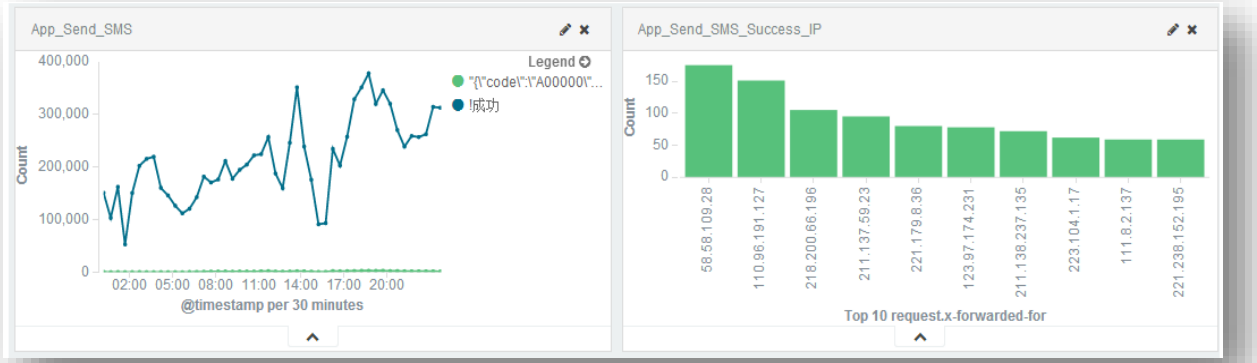

## “撞库扫号”行为监控

通过对线上业务登录成功及失败行为的实时监控



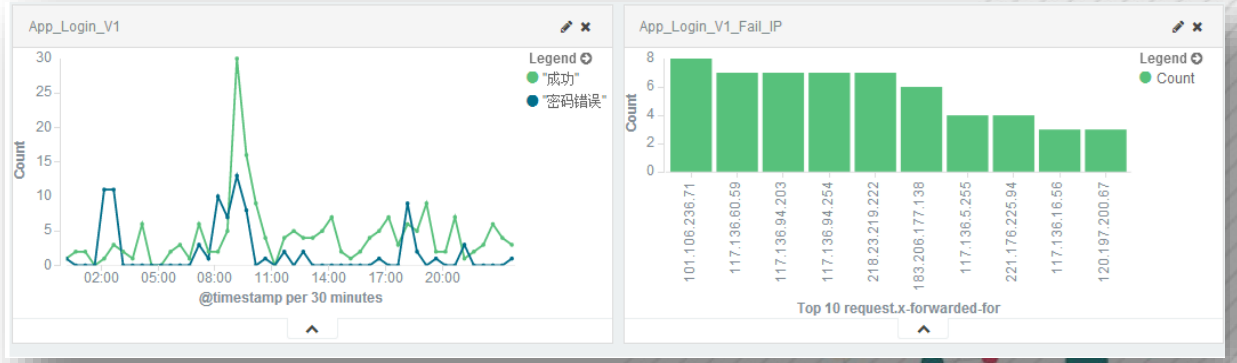

## “短信炸弹”行为监控

通过对线上所有短信验证接口进行实时监控



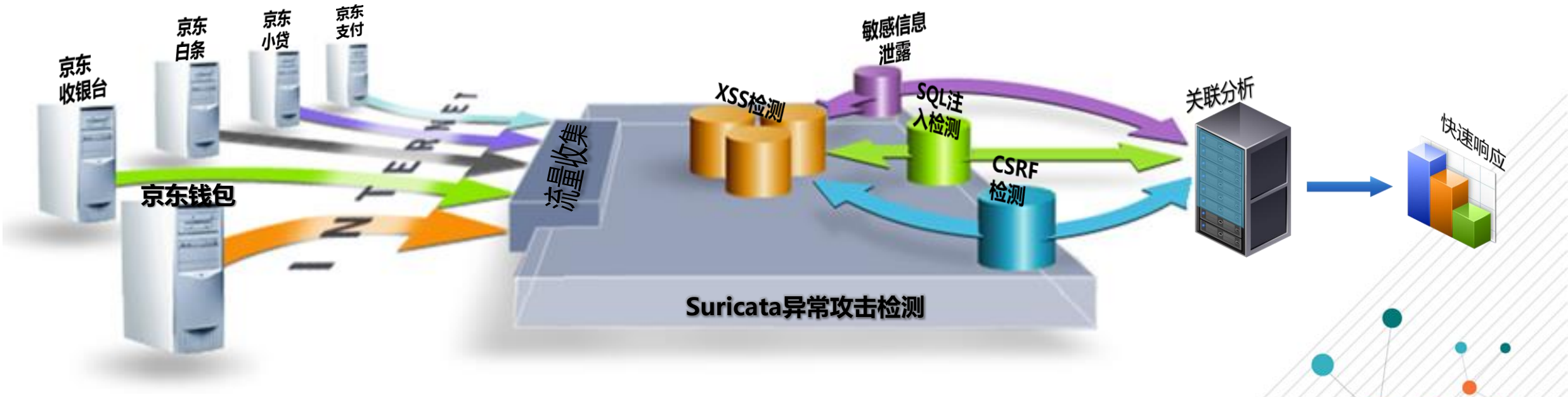

## “垃圾帐号注册”行为监控

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)

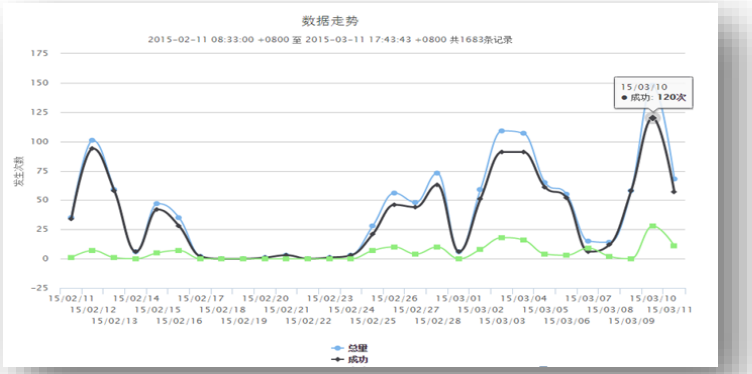
Web安全检测平台：通过Suricate对全流量进行web应用安全检测，包括XSS跨站脚本攻击、SQL注入攻击、CSRF跨站请求伪造、目录遍历等安全威胁



# Web安全检测平台(波塞冬Poseidon)

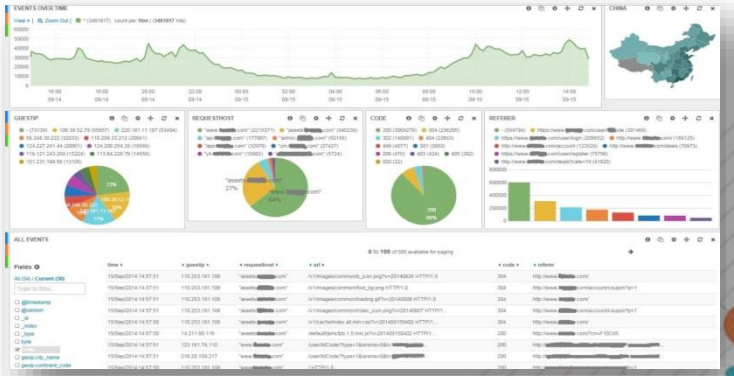
## 攻击类型


## 受攻击业务



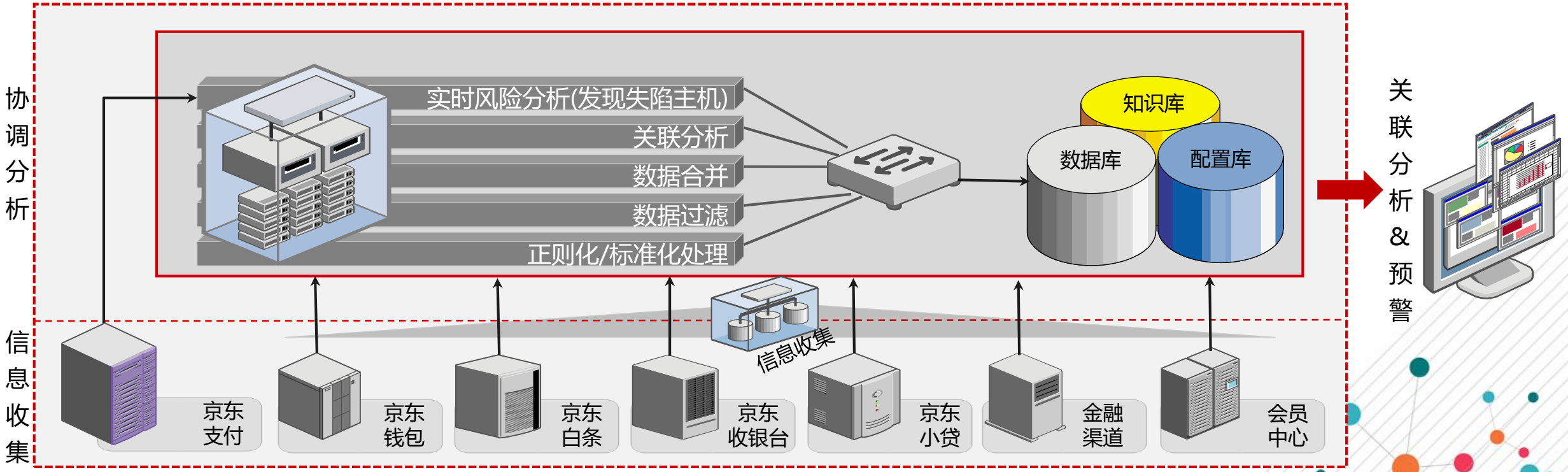

## 攻击源IP


## 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

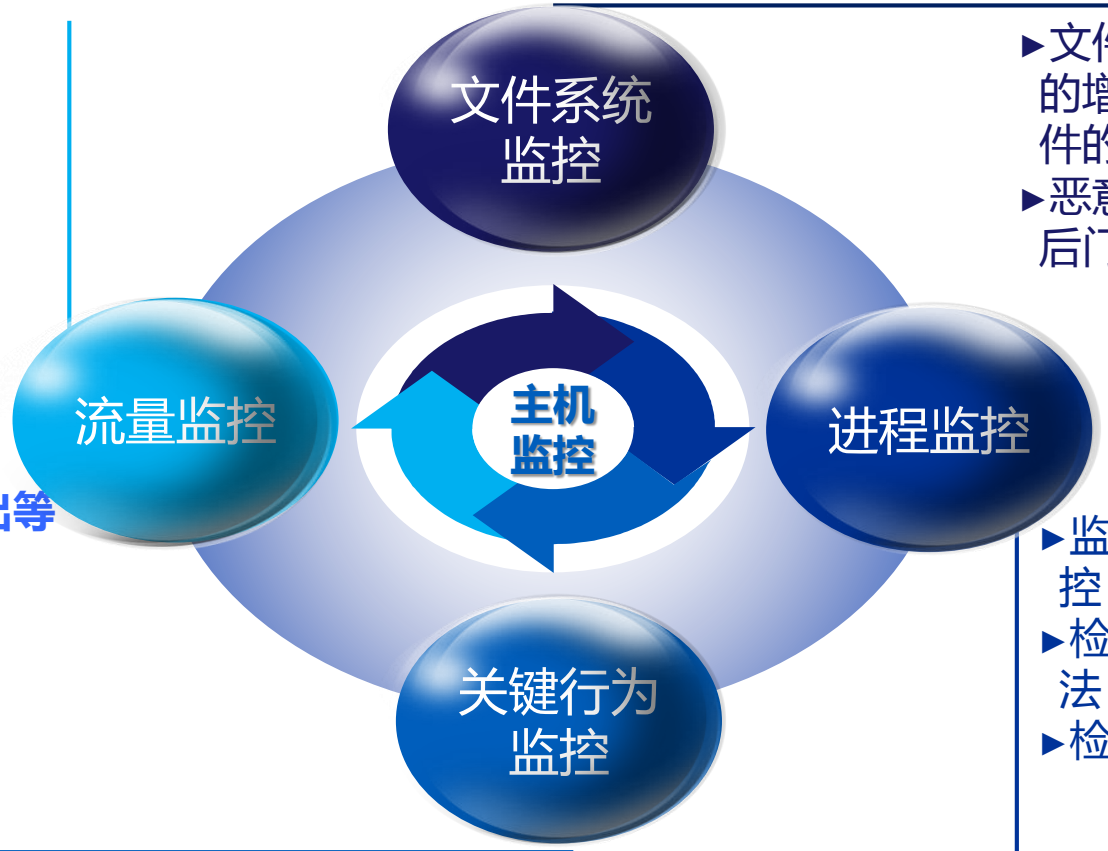


# 主机安全检测平台(雅典娜Athena)

**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**

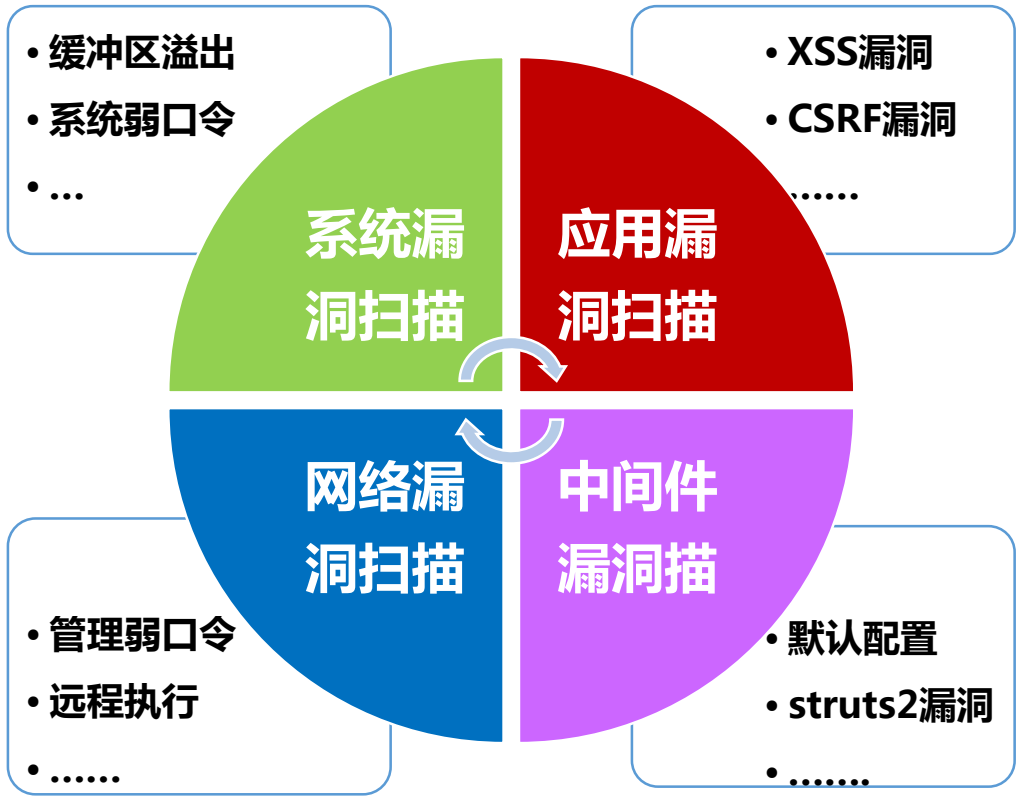


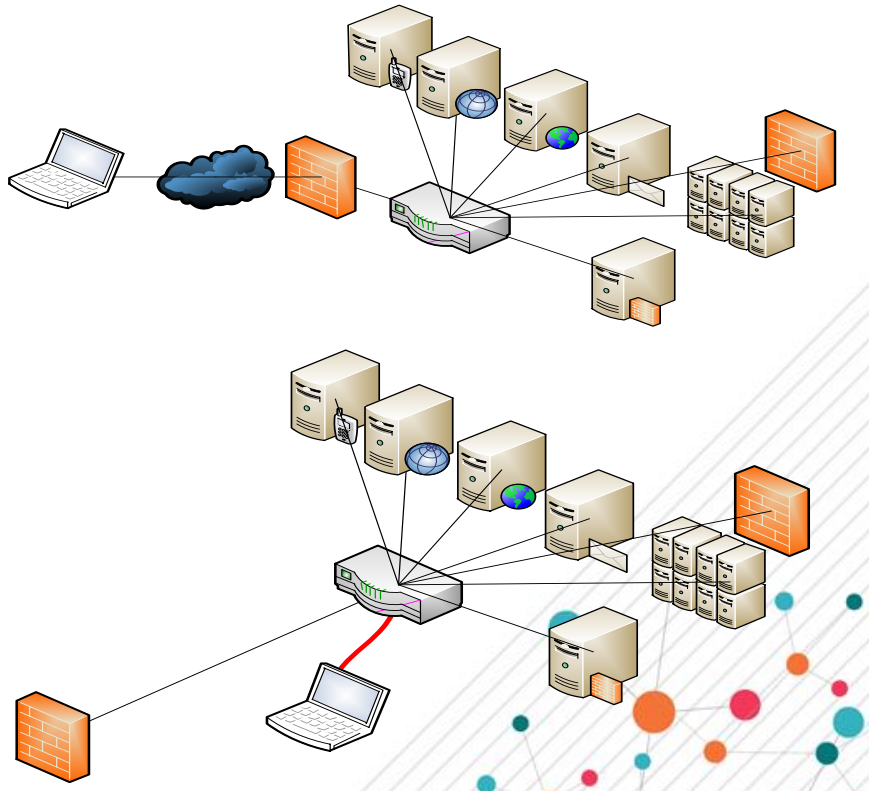

- 文件完整性监控：对文件系统的增删查进行监控，对重要文件的修改进行记录；
- 恶意文件检测，包括（木马、后门、病毒等）分析

- 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