

浅谈互联网安全建设

林 鹏

2018.11

自我介绍



猎豹移动

今 猎豹移动



林鹏



2012-2014 当当网

2015-2018 万达电商

“

不可胜者，守也；可胜者，攻也。守则不足，攻则有余。善守者，藏于九地之下，善攻者，动于九天之上，故能自保而全胜也。

”



孙子兵法.军形篇

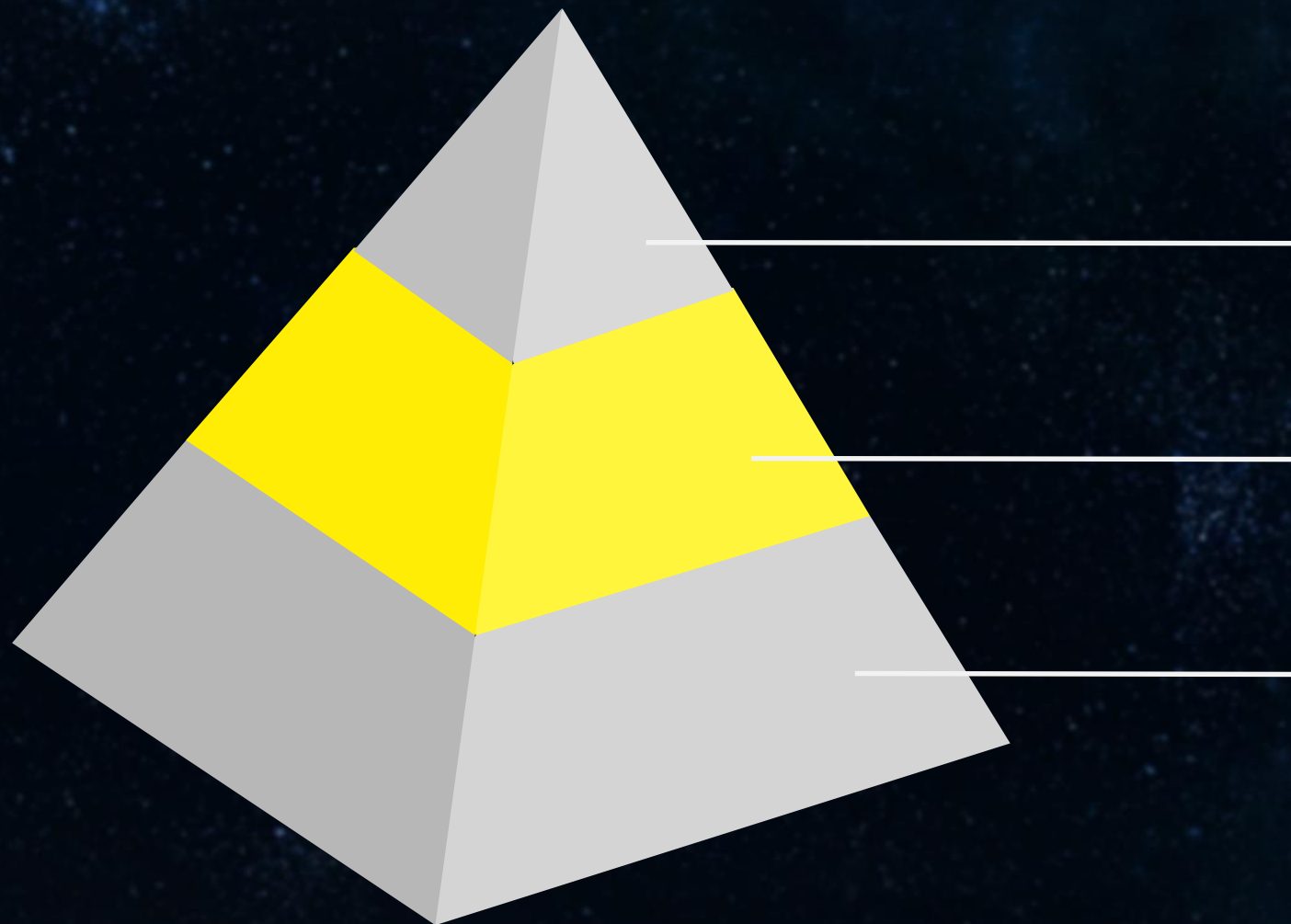
圆圈理论



伴随着企业规模的扩大，
防御的面也随之扩大，
即意味着受攻击的面增大

电商金融面临的主要风险类型





业务安全

安全体系

基础安全

基础安全



password : admin
password : admin

运维安全

- ✓ 流量镜像
- ✓ 端口扫描
- ✓ 日志分析
- ✓ 主机检测
- ✓ 配置规范
- ✓ 备份/升级
- ✓

开发安全

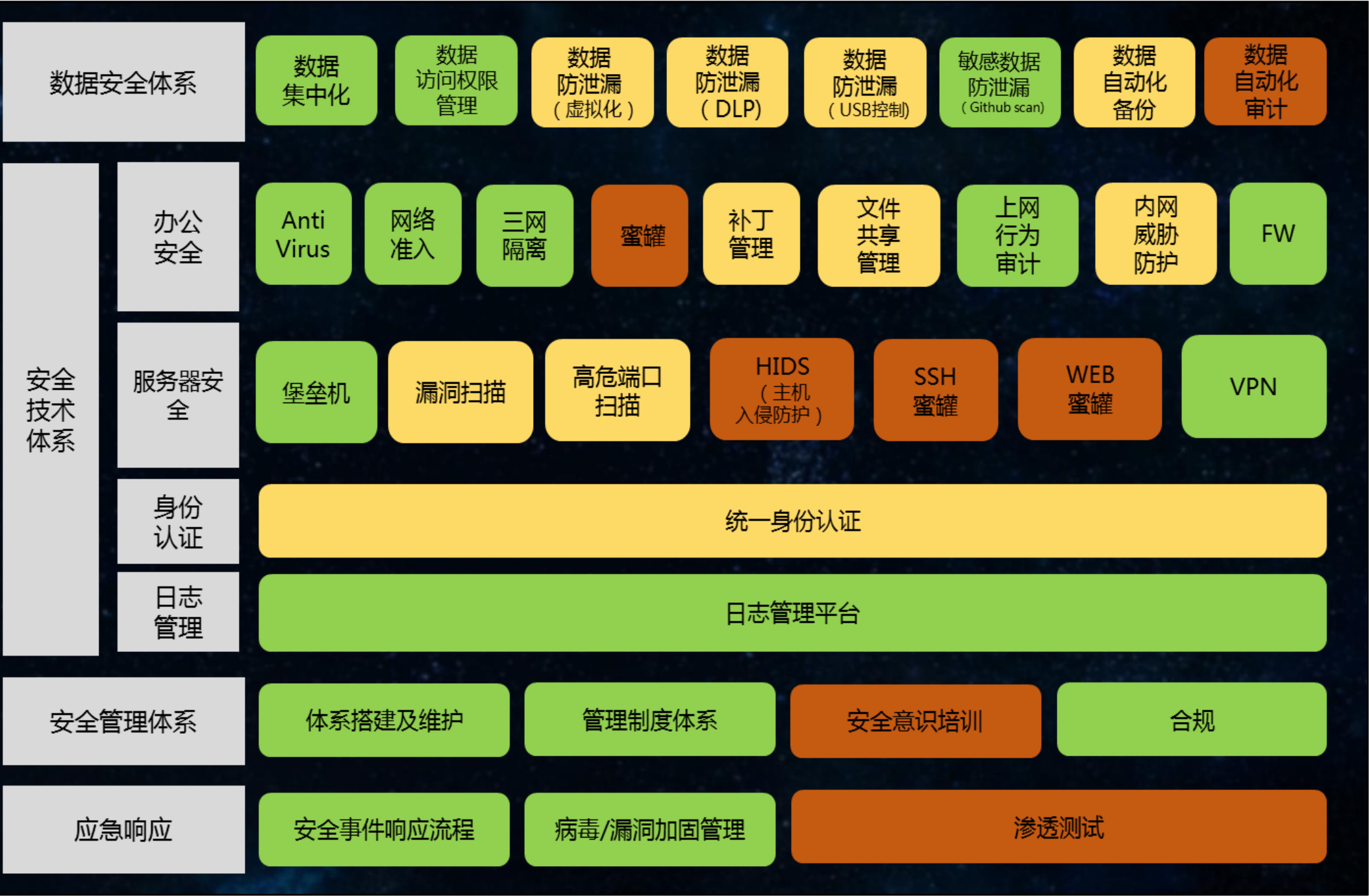
- ✓ 代码安全
- ✓ 后台安全
- ✓ 功能逻辑
- ✓ 权限管理

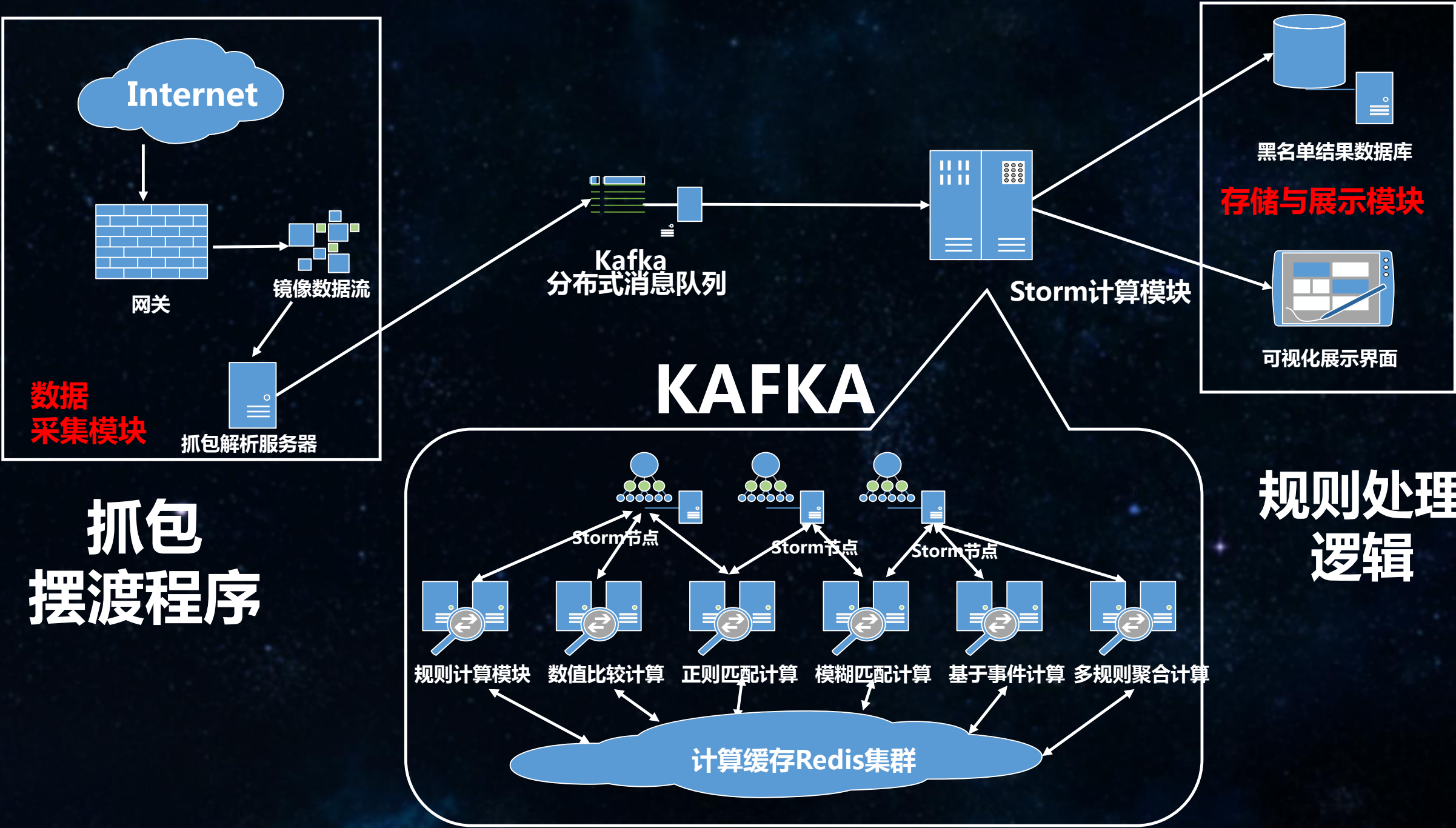
办公安全

环境安全

人员安全







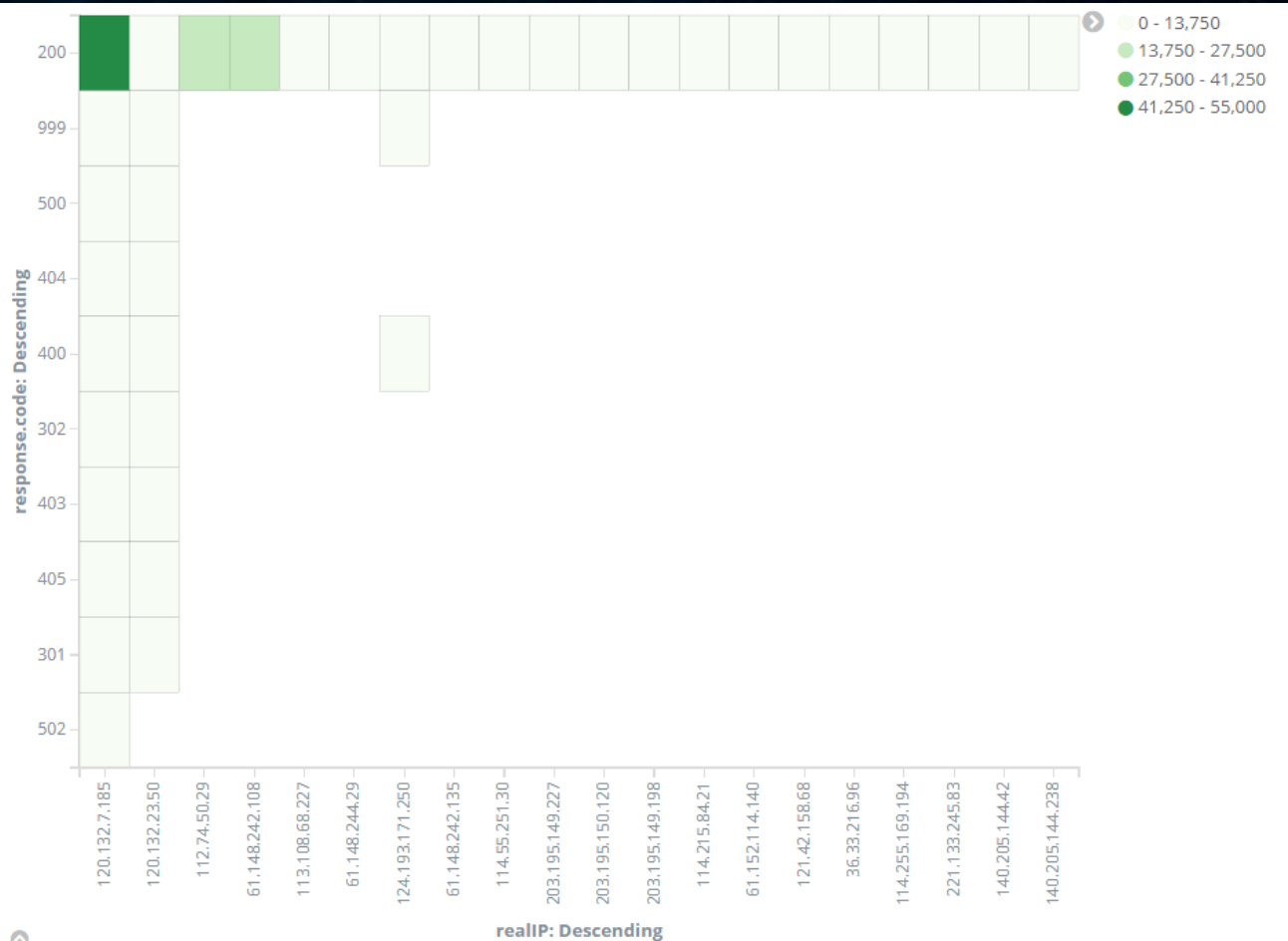
飞凡网络攻击地图

2016年12月15日星期四
17:32:15



目标IP	攻击次数
94:10982	64
1:10000	13
:10982	13
:80	12
10000	6
0	6
:10982	3
:80	2

spider 119
sql 0



关于设备告警/日志



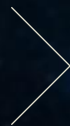
要有人去看告警



要优化告警内容



要用，要琢磨



更多《浅谈安全监控》

安全体系



控制域	一级文件 (策略)	二级文件 (办法)	三级文件 (规范、手册、基线)	四级文件 (表单、记录)	文档名称
A5信息安全策略	ISMS-A-01				网科集团信息安全管理策略
A6信息安全组织		ISMS-B-01			网科集团信息安全组织管理办法
				ISMS-B-01-01	信息安全管理组织成员名单
A7人力资源安全		ISMS-B-02			人力资源管理
		ISMS-B-03			网科集团人员安全管理办法
			ISMS-C-01		网科集团员工信息安全手册
A8资产管理		ISMS-B-04			网科集团信息资产安全管理办法
				ISMS-B-04-01	信息资产登记表
				ISMS-B-04-02	信息密级表
				ISMS-B-04-03	免密级标识清单
				ISMS-B-04-04	信息使用申请书
				ISMS-B-04-05	信息控制要求
			ISMS-C-02		网科集团ISMS文件与记录管理办法
				ISMS-C-02-01	现行有效文件清单表
				ISMS-C-02-02	信息安全记录借阅登记表
			ISMS-C-03		网科集团数据安全规范
				ISMS-C-03-01	系统数据使用申请单
				ISMS-C-03-02	数据安全基线
		ISMS-B-05			网科集团数据管理办法(草案)
A9访问控制		ISMS-B-06			业务系统权限管理办法草案(2017版)
A10密码学		ISMS-B-07			网科集团密码安全管理办法
				ISMS-B-07-01	密码生命周期各阶段记录基本要素
A11物理和环境安全		ISMS-B-08			
		ISMS-B-09			网科集团数据备份与恢复管理办法
				ISMS-B-09-01	备份数据恢复申请表
		ISMS-B-10			网科集团账号口令安全管理办法
				ISMS-B-10-01	特权账号登记表
				ISMS-B-10-02	超级管理员账号口令使用修改记录

业务安全

[#] 提供线报免费与发 [#]

注册个数: 线程数:

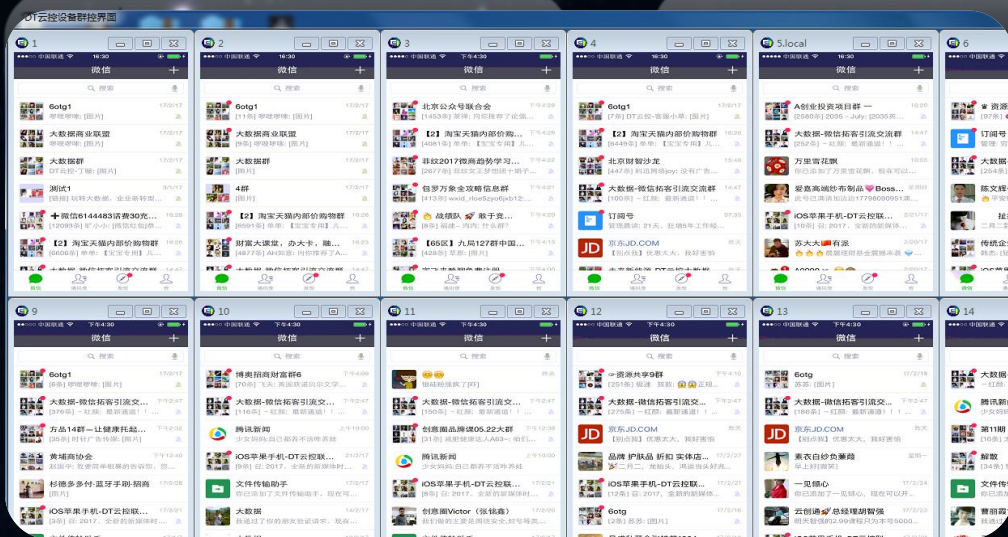
快码账号: 快码密码:

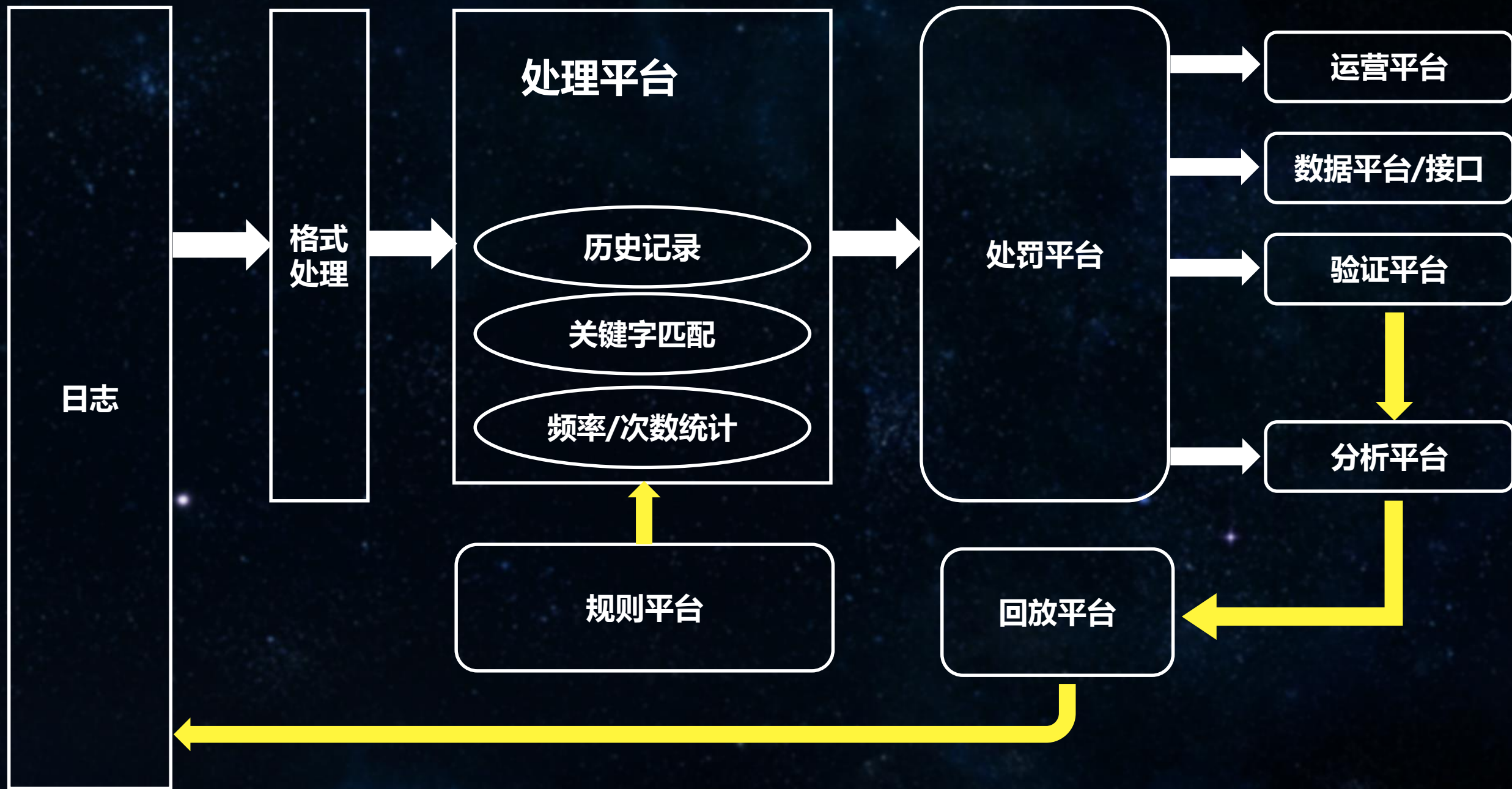
代理API地址:

adsl拨号换IP设置

连接名称: 账号: 密码:

注册几个换IP: [快码平台注册](#) [点我加群](#)







FFS系统规则编辑包括：

- 日志切分规则管理
- 风险规则管理
- 日志规则监控

规则集名字 target: target action:

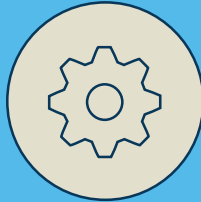
Name: 规则名称

source: login-all

varName: varName method:

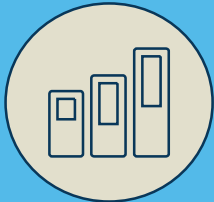
interval: 单位秒

起始时间: 开始时间 结束时间



风险规则编辑包括：

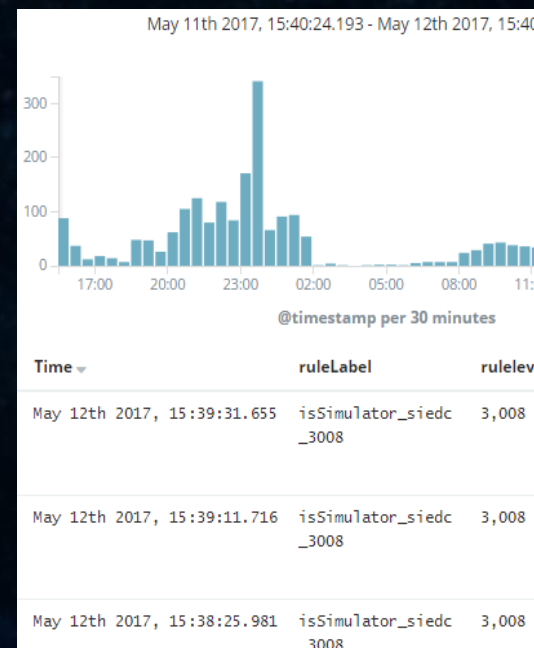
- 数据来源选择
- 规则维度的计算方式及阈值
- 风险输出的类型及分值



- 可以在日志规则监控页面
- 查看每条规则最近1小时、24小时以及总的命中数
- 并根据所选时间范围生成图表



- 我们在ES里面保存了一份命中记录的日志
- 也可以通过ES来全局查看规则的命中情况

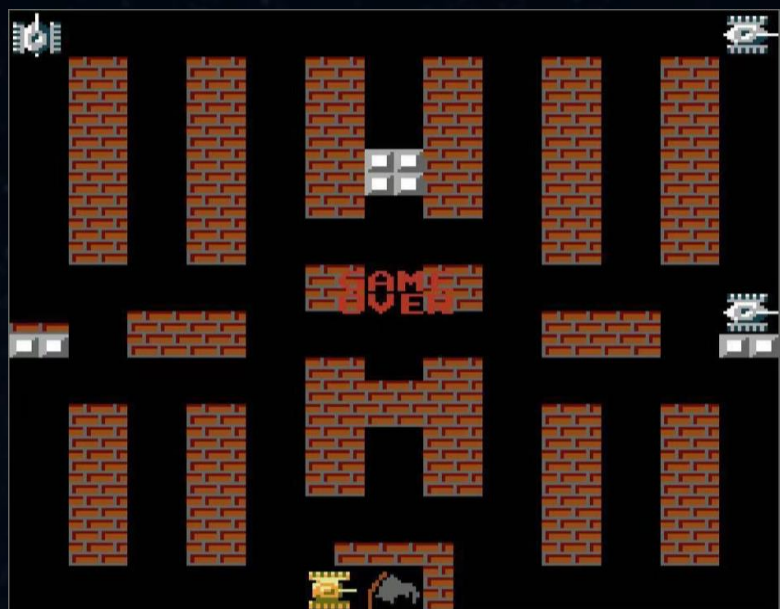


风控

- ✓ 风控的介入 / 接入点
- ✓ 有无新注册渠道
- ✓ 是否有冻结机制（零用钱 / 积分）
- ✓ 是否可以设置兑换流程
- ✓ 活动前的安全验证



- ✓ 前端验证
- ✓ url中的空格会变成 %20
- ✓ 活动后期的账号问题
- ✓ 设立门槛
- ✓ 黑名单
- ✓ 与客服有沟通机制



《解析P2P安全》

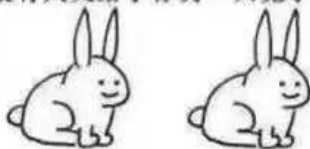
关于机器学习的应用

算法入门

先假设你有一只兔子。



假设有人又给了你另一只兔子。



现在，数一下你所拥有的兔子数量，你会得到结果是两只。也就是说一只兔子加一只兔子等于两只兔子，也就是一加一等于二。

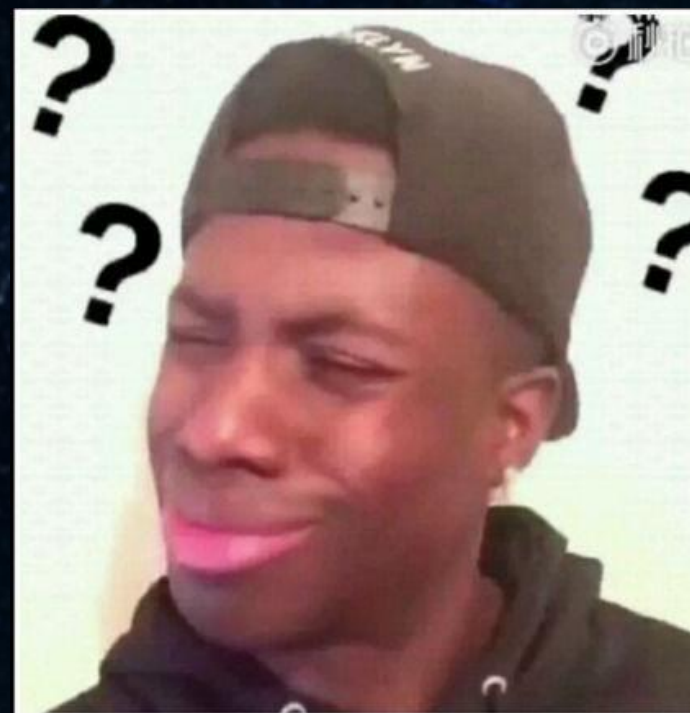
$$1 + 1 = 2$$

那么，现在你已经对算术的基本原理有了一定了解，就让我们来看一看下面这个简单的例子，来把我们刚刚学到的知识运用到实践中吧。

试试看！
例题 1.7

$$\log \Pi(N) = \left(N + \frac{1}{2}\right) \log N - N + A - \int_N^{\infty} \frac{\overline{B}_1(x) dx}{x}, \quad A = 1 + \int_1^{\infty} \frac{\overline{B}_1(x) dx}{x}$$

$$\log \Pi(s) = \left(s + \frac{1}{2}\right) \log s - s + A - \int_0^{\infty} \frac{\overline{B}_1(t) dt}{t + s}$$



WTF? !

DGA恶意域名判断

Alex排名

Bing收录

域名长度

页面内容

普通后缀

信息熵+TF-IDF

Cname

+

归一化

+

(SVM/CNN)

- 背锅侠
- 救火队
- 规则制定者



这锅谁他娘的来背一下

安全

运维

开发

产品

安全



运维



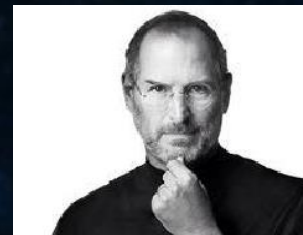
沟通：
安全工作的基础

开发



换位思考：
安全工作能否进展下去

产品



谢谢！

林鹏 | linpeng@cmcm.com | 微信：yagamipeng

