法谈互联网安全建设

林鵬

2018.11

自我介绍



11

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

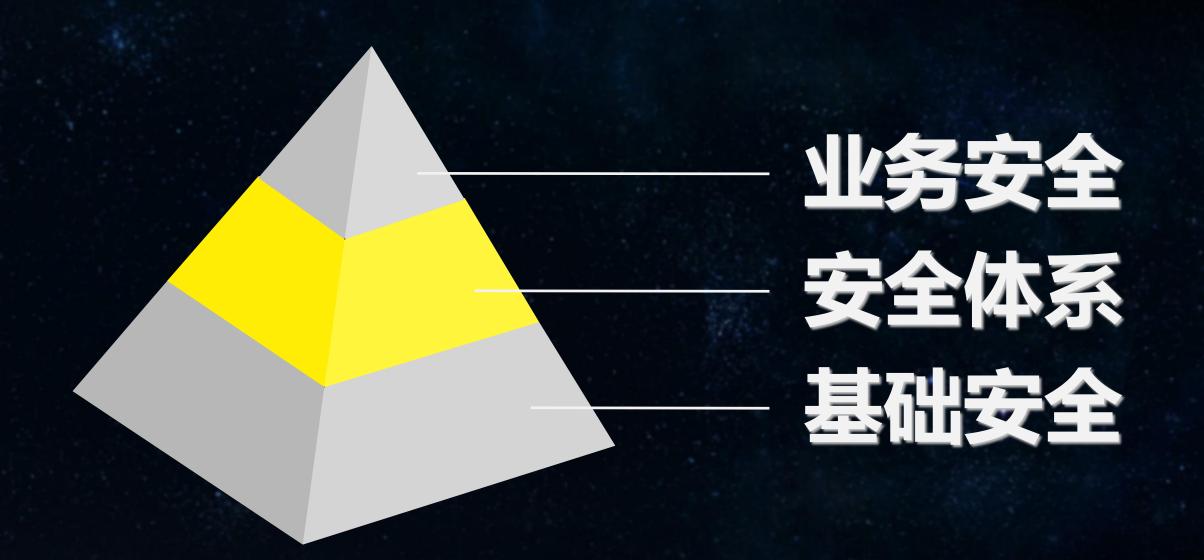
圆圈理论



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





基础安全

Username: admin

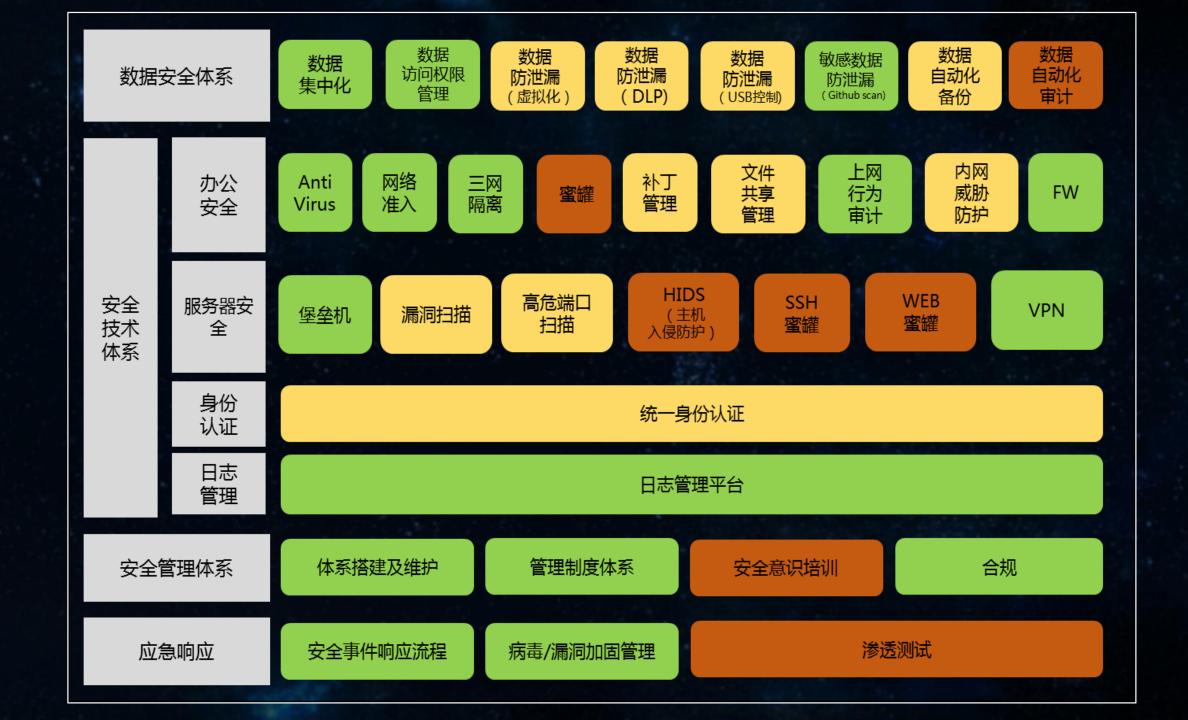
Password: admin

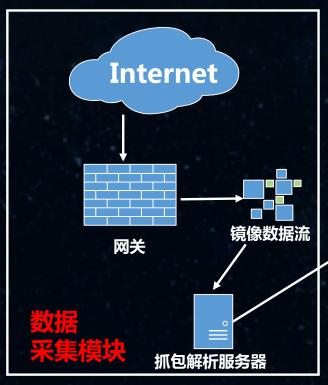
运维安全

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



人员安全





抓包 摆渡程序





基于攻击IP的统计	^ X
IP地址	次数统计
112.74.50.29	22389
121.40.99.171	10506
121.40.95.149	3529
114.55.105.16	3430
114.215.84.21	953
121.42.158.68	805
120.26.105.246	287
120.26.106.134	287
61.161.196.138	74
123.125.71.17	71

基于告警名称的统计	^ ×	
告警名称	次数统计	
JAVA未知爬虫	42475	
百度爬虫	4059	
Google爬虫	108	
PYTHON未知爬虫	31	
SQLMAP扫描工具测试	17	
PHPMYADMIN扫描探测	9	
PHP敏感信息泄露	5	
SQL POST UNION ATTACK !!!	3	
TOMCAT MANAGER扫描探测	3	
360补天扫描器敏感信息探测	2	
The second secon		

基于域名的统计	^ X
域名	次教统计
api.ffan.com	42409
wechat.ffan.com	1276
www.ffan.com	1080
portal.ffan.com	994
admin.ffan.com	282
film.ffan.com	188
m.ffan.com	137
ffce.ffan.com	79
jf.ffan.com	57
h5.ffan.com	36

URL地址 次數统 计 /cloudparking/v2/upload/realtimeSpaces 8690 /cloudparking/v2/upload/outParkingData 2457

攻击者IP对应的告警名称(uniq)数量

^ X

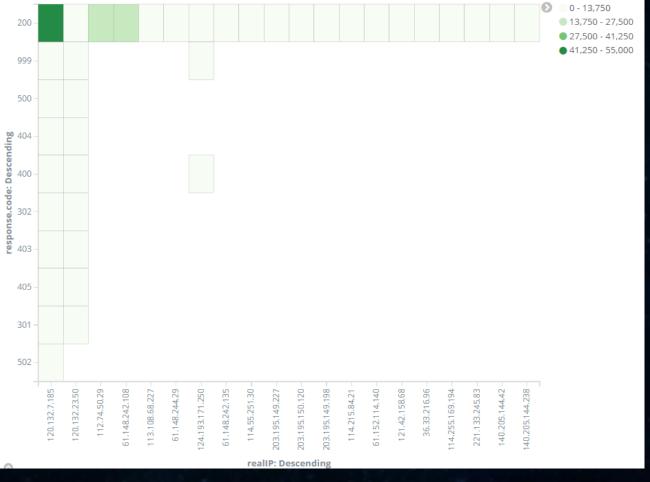
IP地址	次数统计
220.181.158.106	2
120.26.106.134	1
123.125.71.117	1

告警名称对应的reqlIP(uniq)数量

^ X

告警名称	次数统计
百度爬虫	211
JAVA未知爬虫	37
Google爬虫	13





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



安全体系



控制域	一級文件 (策略)▼	二级文件 (办法)▼	三级文件 (规范、手册、基线 ▼	四級文件 (表单、记录) ▼	文档名称
A.5信息安全策略	ISMS-A-01				网科集团信息安全管理策略
A 6/宣告之会织行		ISMS-B-01			网科集团信息安全组织管理办法
A.6信息安全组织				ISMS-B-01-01	信息安全管理组织成员名单
		ISMS-B-02			人力资源管理
A.7人力资源安全		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管理手册
		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
A.8资产管理			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		网科集团数据安全管理规范
				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			网络科技集团数据管理办法(草案)
A.9访问控制		ISMS-B-06			业务系统权限管理办法草窠(2017版)
A 10歲和兴		ISMS-B-07			网科集团密钥安全管理办法
A.10密码学				ISMS-B-07-01	密钥生命周期各阶段记录基本要素
A.11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









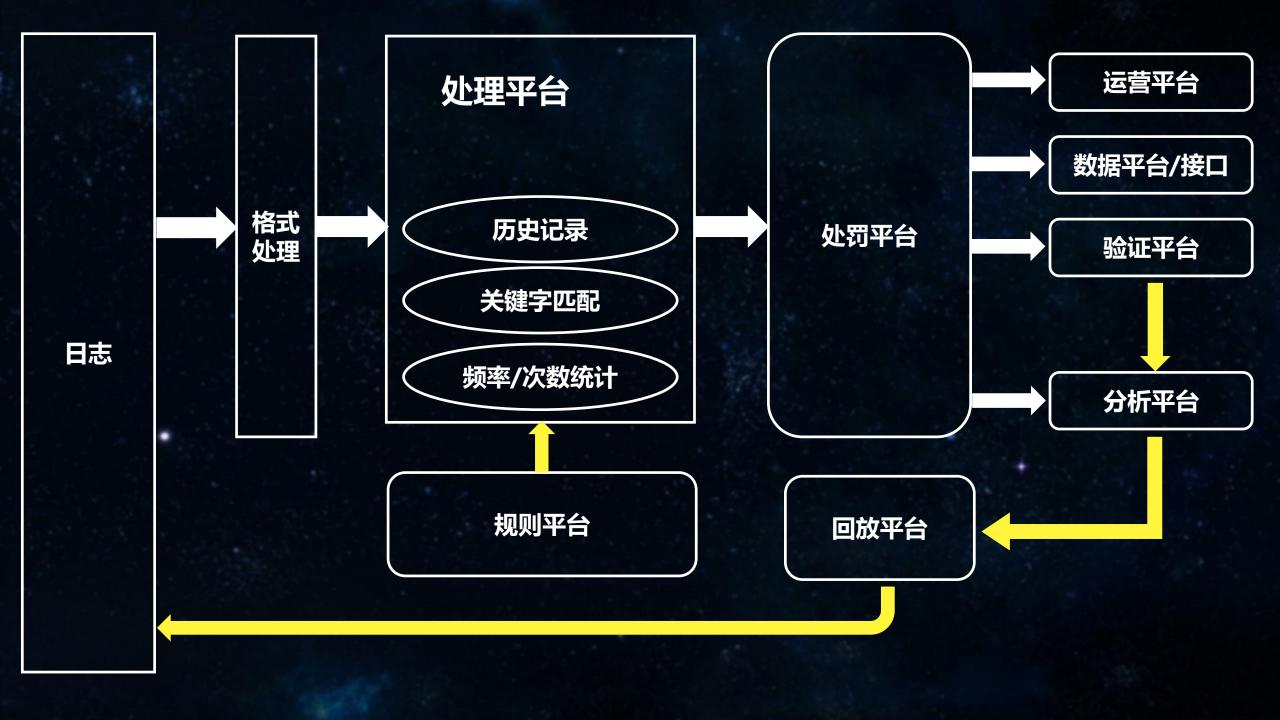
代办各银行储蓄卡一套齐全(身份证、银行卡、网银U盾、手机号码卡、开户资料单 *开户,无任何交易记录。方便客户洗黑,取现,各种用途。(陶宝交易,代收*)

*** 編行卡)QQ:509∞**













欢迎您. maxin33

业务规则管理

日志切分规则管理

日志规则监控



- 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



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





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

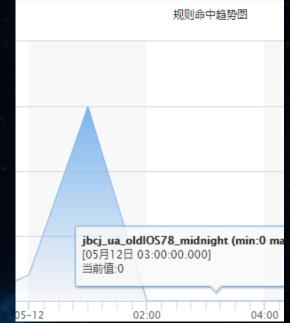
May 11th 2017, 15:40:24.193 - May 12th 2017, 15:40:2



- ・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



300 200 05:00 @timestamp per 30 minutes Time ruleLabel rulelevel May 12th 2017, 15:39:31.655 isSimulator_siedc 3.008 May 12th 2017, 15:39:11.716 isSimulator_siedc 3,008 May 12th 2017, 15:38:25.981 isSimulator_siedc

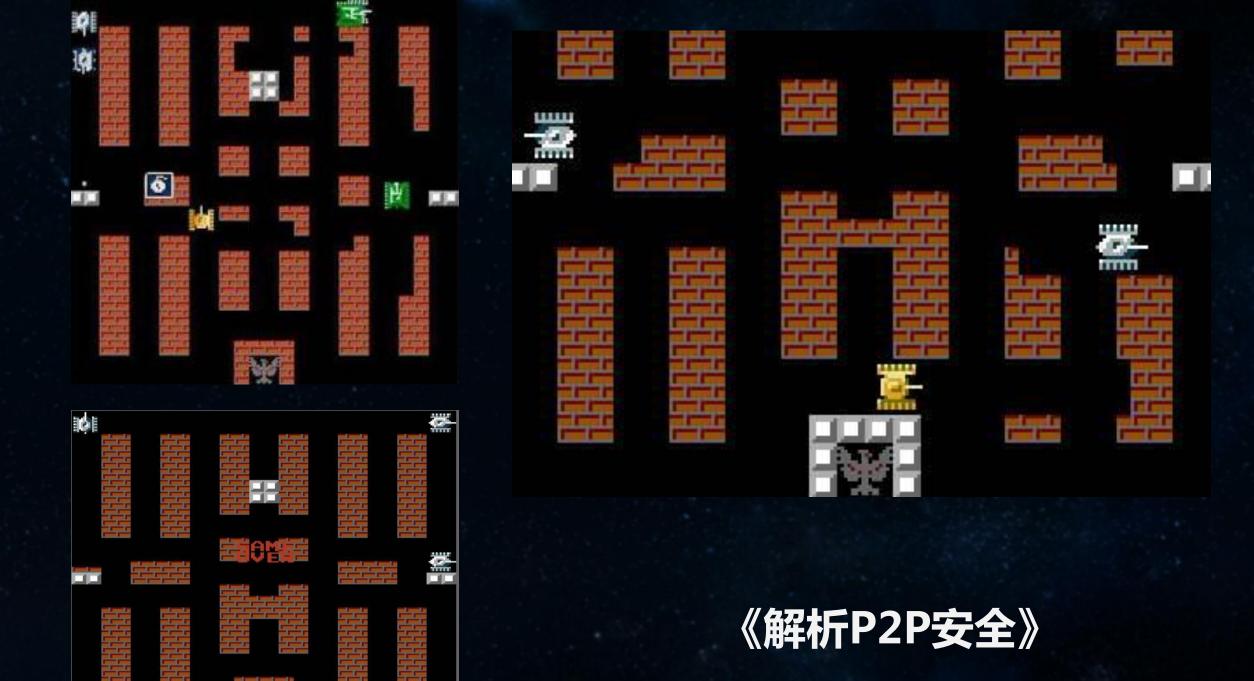


风控

- ✓ 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



关于机器学习的应用

先假设你有一只兔子。

算法入门



假设有人又给了你另一只兔子,



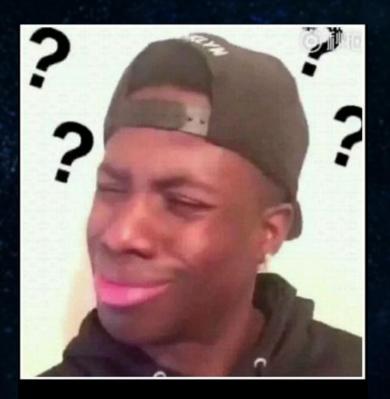
现在,数一下你所拥有的兔子数量,你会得到结果是两只。也就是说一只兔子加一只兔子等于两只兔子,也就是一加一等于二。

$$1 + 1 = 2$$

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

$$\begin{split} \log \Pi(N) &= \left(N + \frac{1}{2}\right) \log N - N + A - \int_{N}^{\infty} \frac{\overline{B}_{1}(x) \mathrm{d}x}{x}, \quad A = 1 + \int_{1}^{\infty} \frac{\overline{B}_{1}(x) \mathrm{d}x}{x} \\ &\log \Pi(s) = \left(s + \frac{1}{2}\right) \log s - s + A - \int_{0}^{\infty} \frac{\overline{B}_{1}(t) \mathrm{d}t}{t + s} \end{split}$$



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



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

