

构建规模化企业级风险感知体系

SPEAKER

张天琪



促进软件开发领域知识与创新的传播



关注InfoQ官方信息
及时获取QCon软件开发者
大会演讲视频信息



[北京站] 2016年12月2日-3日

咨询热线: 010-89880682



[北京站] 2017年4月16日-18日

咨询热线: 010-64738142

关于我

张天琪 | 上海斗象科技联合创始人兼CTO

曾就职于知道创宇、阿里巴巴
OWASP、ISC、GSMA等行业会议演讲者
多次获Google、微软、Twitter等知名厂商官方致谢
专注应用安全攻防，安全产品研究与研发。

关于我们



国内最大的互联网安全新媒体，同时也是爱好者们交流、分享技术的最佳平台



高效透明的企业级安全服务平台



下一代安全监控与风险分析管理平台

安全大事件

Uh oh, Yahoo! Data Breach May Have Hit Over 1 Billion Users

Friday, September 30, 2016 Swati Khandelwal

70 1.9K 516 300 40 887



The massive data breach that Yahoo! confirmed to the world last week is believed to have been carried out by a "state-sponsored actor" in 2014, which exposed the accounts of over 1 billion Yahoo users.

But, now it seems that Yahoo has downplayed a mega data breach and tried to play it off as a blunder.

Recently the information security firm InfoArmor that analyzed the data breach stating that the data breach was the work of seasoned cyber criminals who targeted Yahoo accounts to an Eastern European nation-state.

昨天晚上，据HackerNews网站一则新闻披露，土耳其国民信息数据库遭到泄露，涉及 49,611,709 位土耳其公民，泄露出的信息包括每个人的身份证ID、姓名、父母亲姓名、性别、出生日期、出生地、身份证注册地址、居住地详细地址（直到门牌号）。

当我们这个世界正在熟睡之际，地球的某一端又出事了，昨天晚上，土耳其全国国民底裤被扒了，惨不忍睹。4900万土耳其国民信息泄露，披露此信息的网站为http://185.100.87.XXX/，内容很简单，仅嘲笑了土耳其国民信息加密方法及保护措施的无能，随后即放出了数据库下载链接给全世界。。。

Turkish Citizenship Database











REEBUF 关注黑客与极客 首页 分类阅读 文库 小酒馆 公开课

快报！快报！NSA被黑，或有可能成为第二个TheHackingTeam事件！
Mickeyyyyyy 2016-08-16 +20 共302594人围观，发现 57 个不明物体 资讯

Name	Size
BANANAGLEE	6 items
BARGLEE	1 item
BLATSTING	7 items
BUZZDIRECTION	2 items
EXPLOITS	8 items
OPS	6 items
SCRIPTS	33 items
TOOLS	15 items
TURBO	2 items

NSA HACKED!
Private Hacking Tools & Exploits Leaked

Top 10 breaches

 myspace	359,420,698	MySpace accounts
 NETEASE www.163.com	234,842,089	NetEase accounts ?
 in	164,611,595	LinkedIn accounts
	152,445,165	Adobe accounts
 badoo	112,005,531	Badoo accounts 🔥 ?
	93,338,602	VK accounts
	68,648,009	Dropbox accounts
 tumblr.	65,469,298	tumblr accounts
 iMesh	49,467,477	iMesh accounts
 Fling.com	40,767,652	Fling accounts 🔥

FFIEC、FISMA、CyberScope Reporting Protocol、GLBA、HIPAA/HITECH、NERC、PCI、SCAP、SOX
CERT、CIS、COBIT/ITIL、DISA STIG、FDCC、IBM iSeries、ISO、NIST、NSA.....

做了这么多的合规、基线、补丁稽查，却仍然做不好安全？

投入成本低？

安全团队
消极怠工？

安全防护设备
功能不够？

攻防体系的不对称

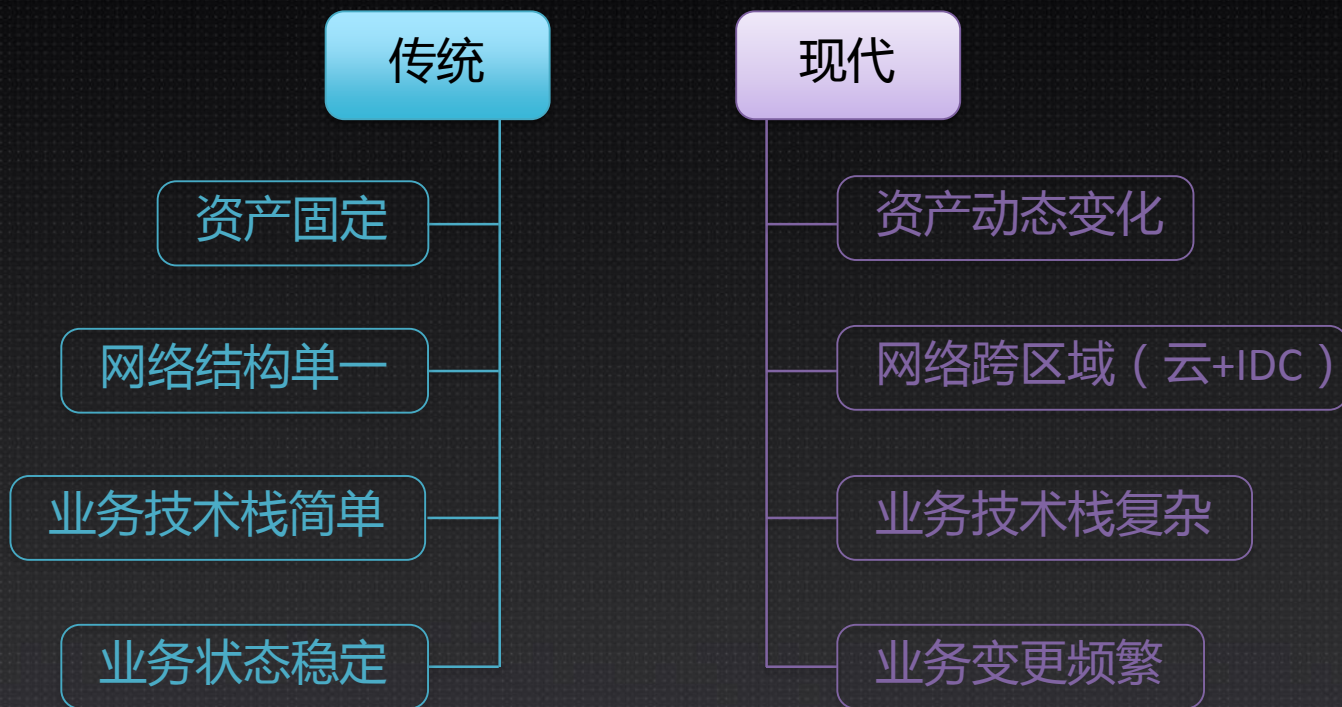
技术层面：防御通常具有滞后性

信息不对称：攻击者 > 安全人员
如：社工库、信息渠道获取&分享、社会工程学

攻击面：防护 — 需要考虑到方方面面
攻击 — 目标明确，有各种绕过防护的方法

经济角度：攻击 — 收益明确、主动性强
防御 — 工作被动、常抱有侥幸&懒惰心理

企业安全需求进化



企业安全体系进化

以漏洞为中心

聚焦于检测

主要针对普通攻击手法

高度依赖基于特征的检测

检测未知风险能力极小

线性流程

以风险为中心

聚焦于收集

分析不同工具、策略

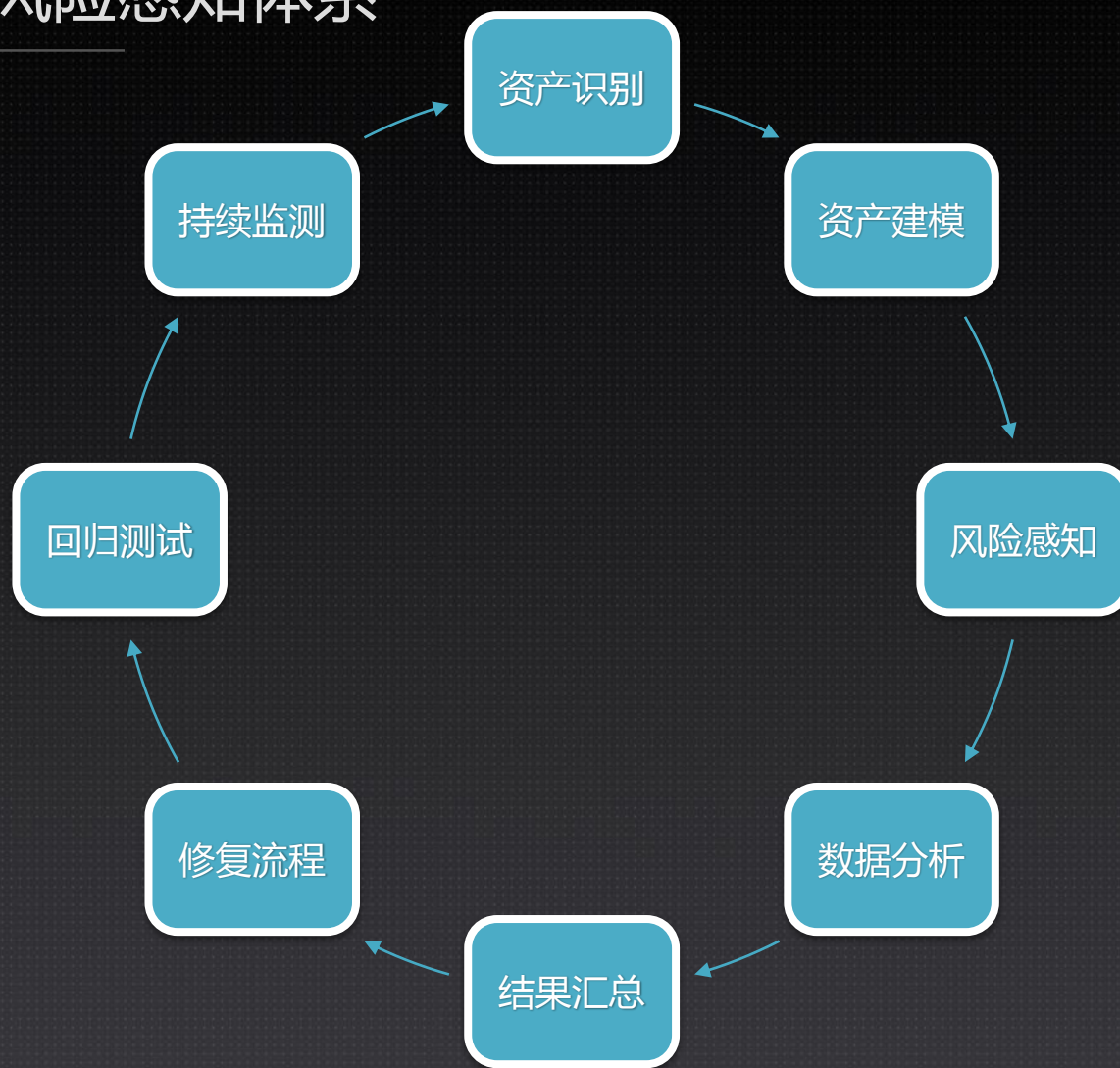
利用所有数据源

超出已知特征感知风险

循环流程

如何快速解决？

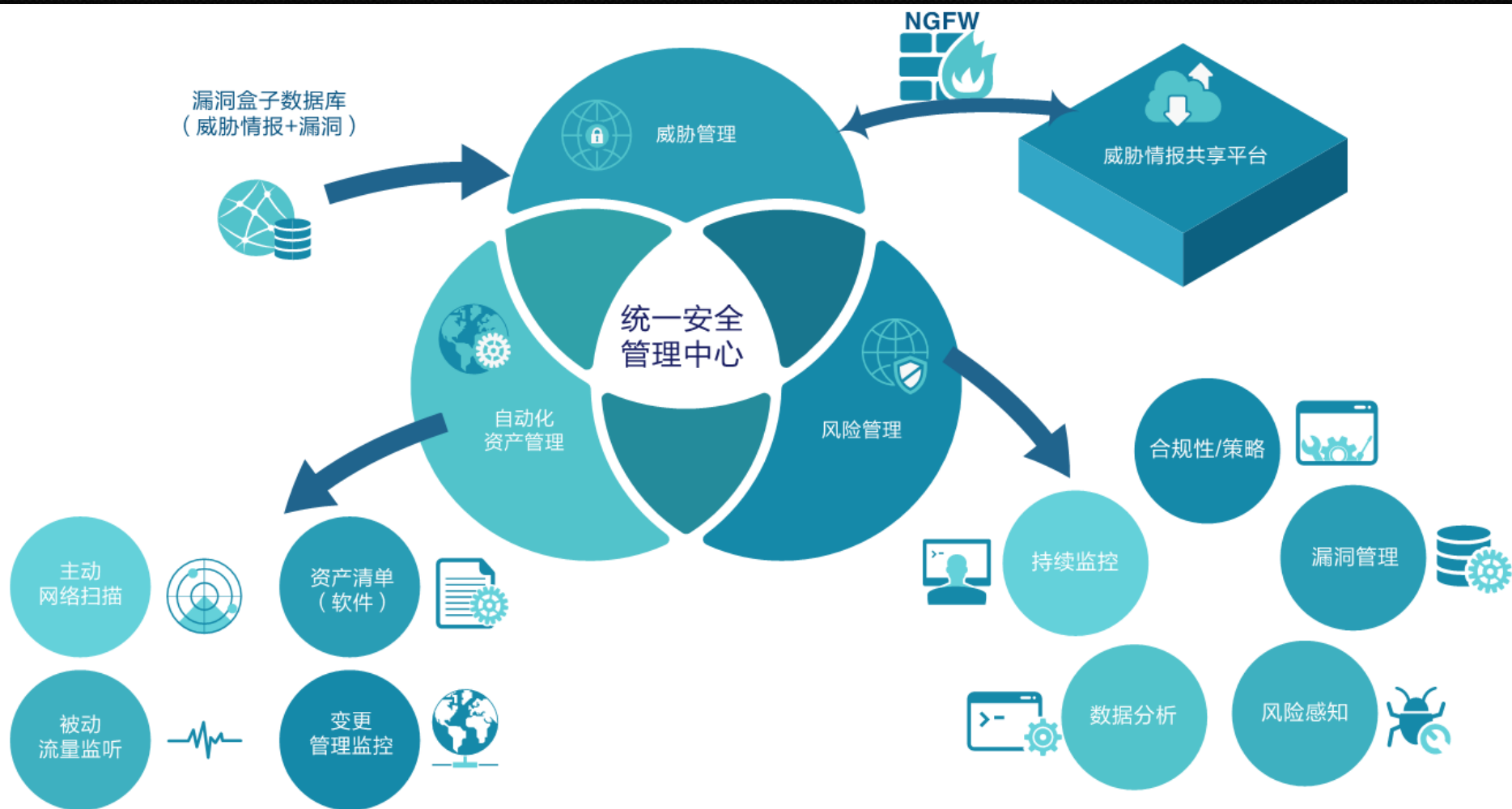
构建企业风险感知体系



安全管理产品的进化



下一代风险感知体系



解决哪些问题？

安全闭环

事后

- 纠正
- 恢复
- 溯源

事中

- 监测
- 阻止

事前

- 预防
- 预测

以资产为核心：确立基本面

资产发现



资产模型

- 自动化清点IT资产及遗忘资产
- 灵活修改资产模型
- 资产标签化、业务结构拓扑化
- 对发现每一资产建立基线模型

资产监测

- 对IT资产监测及变更管理
- 深入发现暴露在外面的设备、端口、应用程序，降低整体攻击面
- 及时发现资产变更带来的风险，如挂马、暗链
- 第一时间有针对性的发现安全风险，如0-Day漏洞

以资产为核心



人员资产

- 姓名
- 用户名
- 密码
- 邮箱
- 工号
- 身份证
- 外网资源 (github repo , 网盘 , blog , etc..)
-

资产发现姿势

Passive

基于流量

基于日志

Active

端口扫描/指纹识别

NMAP

ZMAP

MASSCAN

全网资产搜索引擎 (ZoomEye、SHODAN、Censys)

暴力破解

爬虫

区域传送

IP反查

ICP备案反查

注册人/注册邮箱反查

SSL证书使用者备用名称

Certificate Transparency

Google Hack

Github Hack

crossdomain.xml

Sitemap

robot.txt

PassiveDNS

运营商合作

开源情报 (Alienvault、IBM XForce、VirusTotal、Pingly)

子域C段扩展

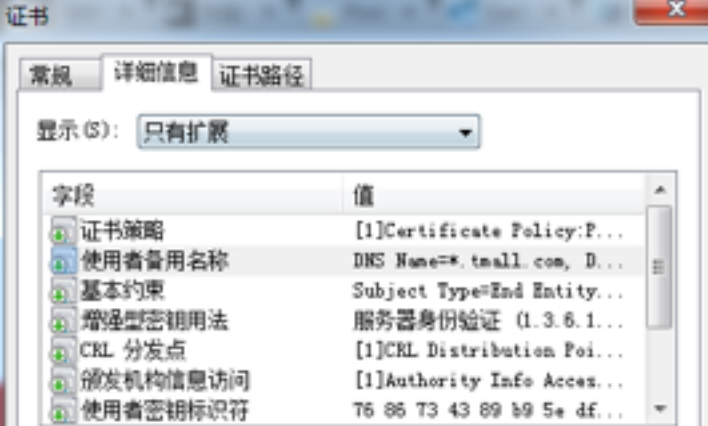
全网资产搜索引擎 (ZoomEye、SHODAN、Censys)

Google Hack

Github Hack

关联IP

子域发现



证书使用者备用名称

证书透明度



了解证书详细信息的更多信息

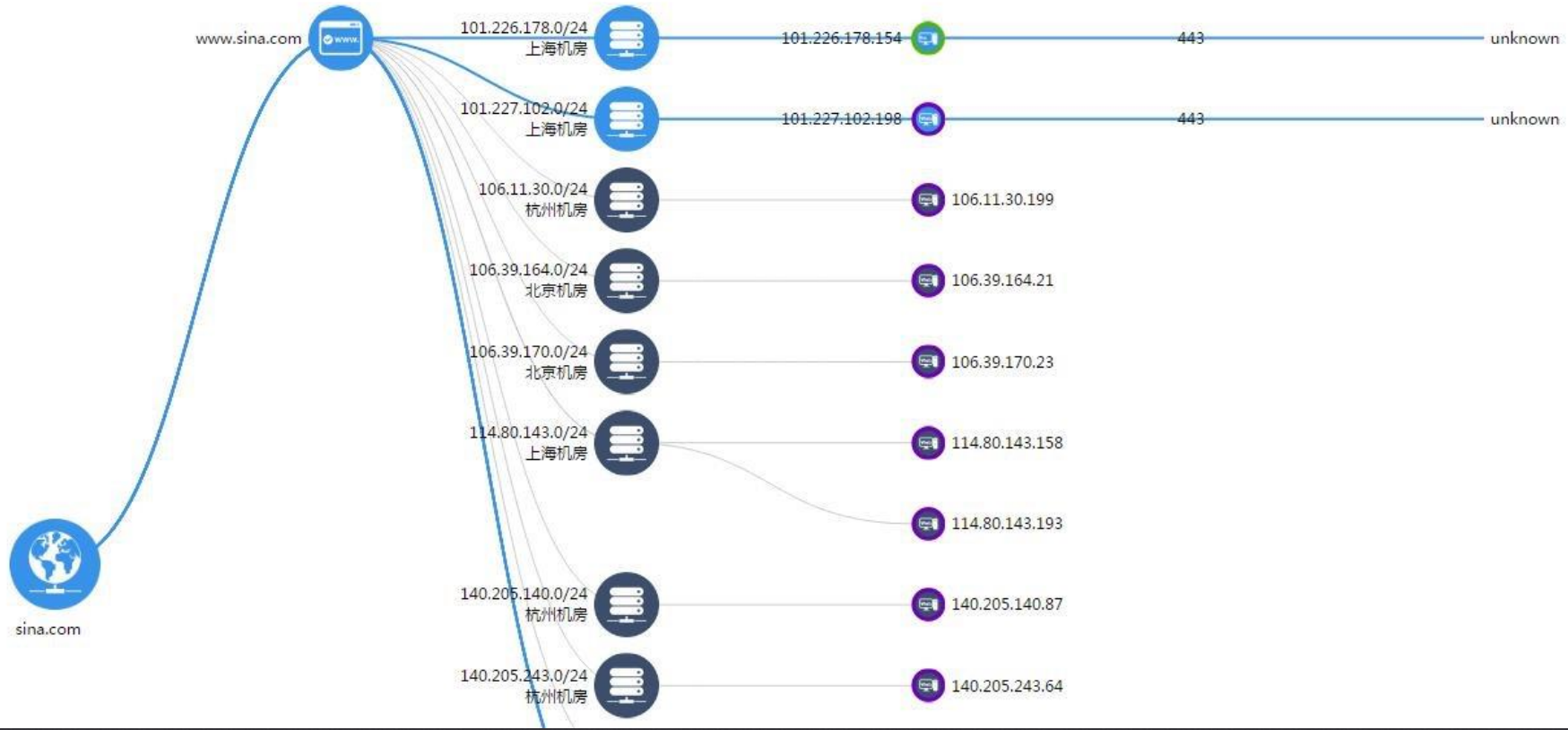
Logged At	Not Before	Identity	Issuer Name
2016-10-16	2016-09-27	prod2 uber.com	C=IL, O=StartCom Ltd., OU=StartCom Certification Authority, CN=StartCom Class 1 DV Server CA
2016-10-16	2016-09-27	szymon gruszecki has hacked prod2 uber.com	C=IL, O=StartCom Ltd., OU=StartCom Certification Authority, CN=StartCom Class 1 DV Server CA
2016-10-12	2015-12-23	*.cn.gcp.uber.com	C=US, O=DigiCert Inc., CN=DigiCert SHA2 Secure Server CA
2016-10-12	2015-12-23	cn.gcp.uber.com	C=US, O=DigiCert Inc., CN=DigiCert SHA2 Secure Server CA
2016-10-12	2016-08-12	*.cfe.uber.com	C=US, O=DigiCert Inc., CN=DigiCert SHA2 Secure Server CA
2016-10-12	2016-08-12	cfe.uber.com	C=US, O=DigiCert Inc., CN=DigiCert SHA2 Secure Server CA
2016-10-12	2016-07-23	team.uber.com	C=US, O=DigiCert Inc., CN=DigiCert SHA2 Secure Server CA
2016-10-11	2016-09-21	prod2 uber.com	C=IL, O=StartCom Ltd., OU=StartCom Certification Authority, CN=StartCom Class 1 DV Server CA
2016-10-10	2016-08-16	lent.uber.com	C=US, O=DigiCert Inc., CN=DigiCert SHA2 Secure Server CA
2016-09-27	2016-09-27	prod2 uber.com	C=IL, O=StartCom Ltd., OU=StartCom Certification Authority, CN=StartCom Class 1 DV Server CA
2016-09-27	2016-09-27	szymon gruszecki has hacked prod2 uber.com	C=IL, O=StartCom Ltd., OU=StartCom Certification Authority, CN=StartCom Class 1 DV Server CA
2016-09-21	2016-09-21	prod2 uber.com	C=IL, O=StartCom Ltd., OU=StartCom Certification Authority, CN=StartCom Class 1 DV Server CA
2016-09-16	2016-04-26	mobile-content.uber.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
2016-08-11	2016-04-29	accessibility.uber.com	C=US, O=DigiCert Inc., CN=DigiCert SHA2 Secure Server CA
2016-08-05	2016-02-03	cn-geo1.uber.com	C=US, O=DigiCert Inc., CN=DigiCert SHA2 Secure Server CA
2016-07-22	2016-07-22	signup.uber.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2016-04-28	2016-04-06	bizblog.uber.com	C=US, O=DigiCert Inc., CN=DigiCert SHA2 Secure Server CA
2016-04-27	2016-04-26	documents.uber.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
2016-04-27	2016-04-27	signup.uber.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2016-04-14	2016-03-11	transparencyreport.uber.com	C=US, O=DigiCert Inc., CN=DigiCert SHA2 Secure Server CA
2016-03-08	2016-02-29	safetyreport.uber.com	C=US, O=DigiCert Inc., CN=DigiCert SHA2 Secure Server CA
2016-03-07	2014-04-11	blog.uber.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign Domain Validation CA - SHA256 - G2
2016-02-29	2014-08-19	team.uber.com	C=US, O=DigiCert Inc., CN=DigiCert SHA2 Secure Server CA
2016-02-05	2015-08-26	experience.uber.com	C=US, O=DigiCert Inc., CN=DigiCert SHA2 Secure Server CA
2015-12-16	2015-12-14	join.uber.com	C=US, O=DigiCert Inc., CN=DigiCert SHA2 Secure Server CA
2015-09-11	2015-07-15	pages.et.uber.com	C=US, O=DigiCert Inc., CN=DigiCert SHA2 Secure Server CA
2015-07-30	2015-01-28	eng.uber.com	C=US, O=DigiCert Inc., CN=DigiCert SHA2 Secure Server CA
2015-07-25	2014-11-13	image.et.uber.com	C=US, O=DigiCert Inc., CN=DigiCert SHA2 Secure Server CA
2015-07-25	2015-07-15	view.et.uber.com	C=US, O=DigiCert Inc., CN=DigiCert SHA2 Secure Server CA
2015-07-25	2015-07-15	click.et.uber.com	C=US, O=DigiCert Inc., CN=DigiCert SHA2 Secure Server CA
2015-07-19	2014-11-13	image.et.uber.com	C=US, O=DigiCert Inc., CN=DigiCert SHA2 Secure Server CA
2015-07-12	2014-11-13	image.et.uber.com	C=US, O=DigiCert Inc., CN=DigiCert SHA2 Secure Server CA
2015-07-10	2015-01-28	people.uber.com	C=US, O=DigiCert Inc., CN=DigiCert SHA2 Secure Server CA
2015-07-08	2014-11-13	image.et.uber.com	C=US, O=DigiCert Inc., CN=DigiCert SHA2 Secure Server CA
2015-06-25	2014-11-13	image.et.uber.com	C=US, O=DigiCert Inc., CN=DigiCert SHA2 Secure Server CA
2015-06-10	2015-05-12	drive.uber.com	C=US, O=DigiCert Inc., CN=DigiCert SHA2 Secure Server CA
2015-06-08	2015-04-28	brand.uber.com	C=US, O=DigiCert Inc., CN=DigiCert SHA2 Secure Server CA
2015-06-02	2015-05-12	newsroom.uber.com	C=US, O=DigiCert Inc., CN=DigiCert SHA2 Secure Server CA

- 总览
- 资产构成
- 端口信息
- 资产识别

- 冷门资产 (最近一周内访问次数少于100次资产)
- 新增资产 (本次监测最新发现资产)
- 离线资产 (最近一次访问因某种原因不可达的资产)

域名: 1 IP: 14 端口/服务: 6

主域 sina.com



应用安全风险感知流程

企业资产



感知策略



风险扫描



安全风险感知报告



主动感知引擎，对企业关联资产进行安全风险感知



安全风险

安全漏洞

全面的漏洞规则库：OWASP-TOP10、CVE、CNVD

SQL注入、命令注入

跨站脚本攻击-XSS

失效的认证和会话管理

不安全的直接对象引用

跨站伪造请求-CSRF

安全配置错误

尚未验证的重定向和转发

运维风险

配置文件核查

权限过大

控制宽松

内部端口对外

弱口令

敏感数据外泄

开发后门

人为弱点

威胁情报

互联网漏洞平台

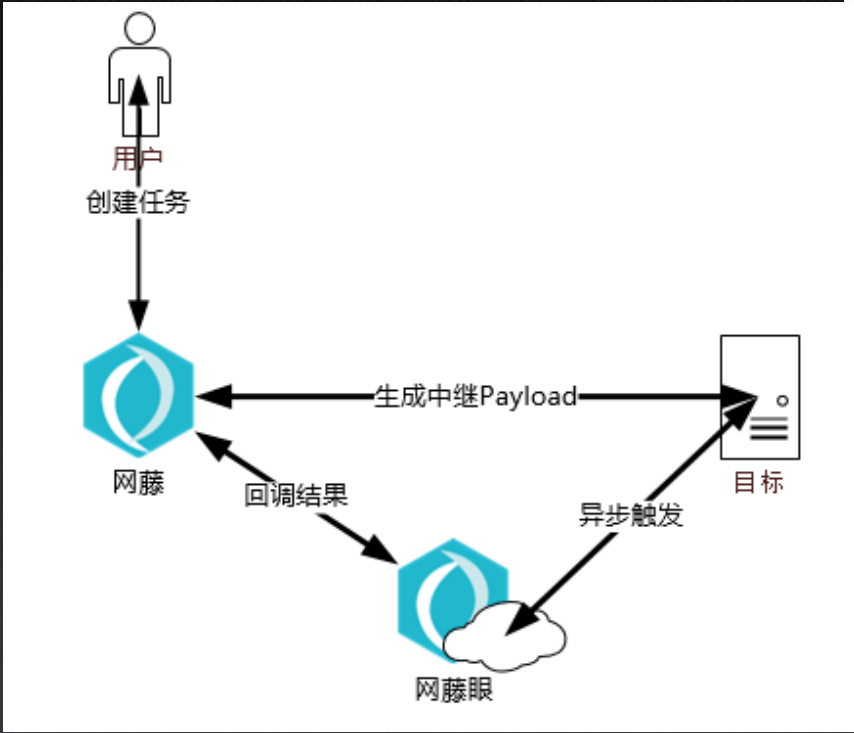
全网数据侦查

最新安全动态

数据联动分析

细节决定成败

- 智能分析登录表单=>扩展攻击面
- 异步漏洞检测机制=>适应现代复杂业务
- 资产增量监控=>细粒度监控基本面

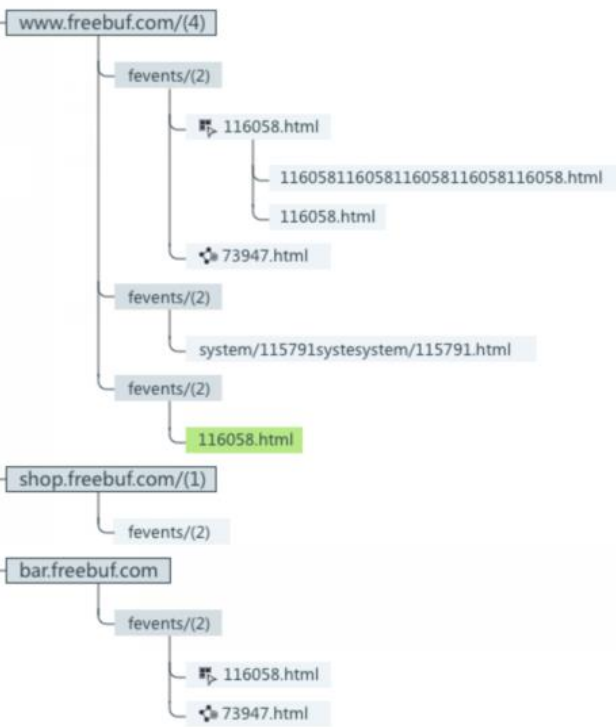


参数

参数	值
登陆URL	http://[REDACTED]:111/
登陆方式	form

用户名	密码
wangfa	最近一次检测时间：2016-08-09 18:13
lina	🔍 登录地址 🌐 测试地址 🟢 最近一次爬虫新增地址
zhangji	
lili	
liujing	

Freebuf.com



风险地址

http://oa.██████.com:7001

参数

用户名	密码	手机	邮箱
herong@██████.com	N/A	N/A	herong@██████.com
herong@██████.com	N/A	N/A	herong@██████.com
jqueen@██████.com	3.*****+13	N/A	N/A
N/A	8*****104432	N/A	gaoyandong@██████.com
N/A	2*****ff5038	N/A	ningzelin@██████.com

Ruby On Rails secret token configuration file

If the Rails secret token is known, it can allow for remote code execution (db.com/exploits/27527/)

```
# Be sure to restart your server when you modify this file.
```

```
# Your secret key for verifying the integrity of signed cookies.
```

```
# If you change this key, all old signed cookies will become invalid!
```

```
# Make sure the secret is at least 30 characters and all random,
```

```
# no regular words or you'll be exposed to dictionary attacks.
```

```
Reflector::Application.config.secret_token = '49bbe6e2074c588ed27e9c7fa1133069  
93fc343d8b5101cf9aae9f6b5d6e8e624395a94b34ef1300f70ae1541293'
```

互联网敏感数据收集

攻击路径预测

→ 漏洞矩阵

→ 可利用矩阵，评估攻击向量

→ 对外开放端口汇总

→ 资产互联关系

→ 应用服务



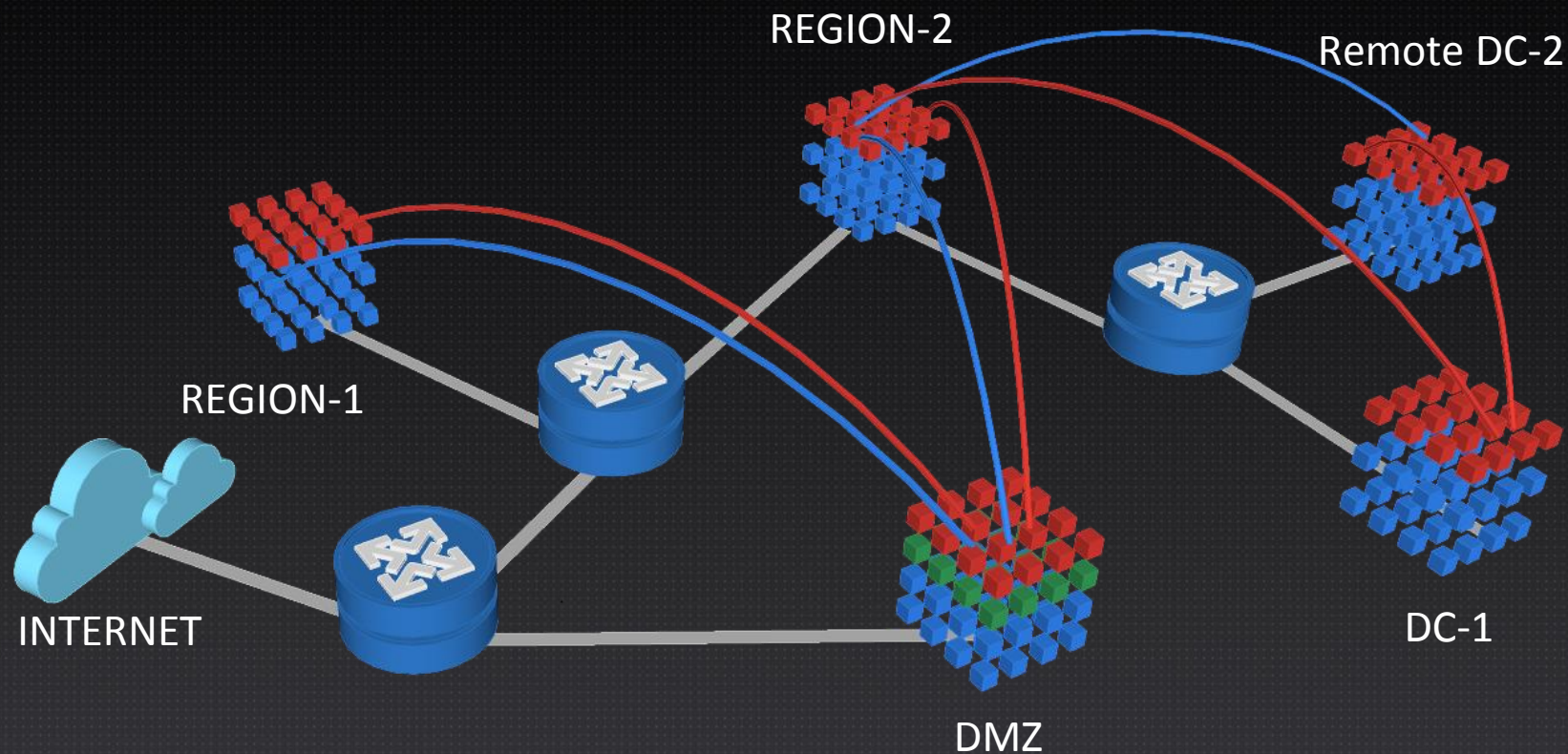
1、在公网当中存在可利用漏洞的资产

2、浏览互联网的客户端存在可利用的漏洞

3、系统信任的客户端存在可利用的漏洞

4、信任的第三方（外包、合作伙伴、供应商、服务提供者）

攻击路径预测 (Predicting Attack Paths)



日志导向



- 系统日志均分散存放在各系统设备上，缺少归档备份
- 日志分散存放在系统本地，技术上无法保证不被故意篡改和删除
- 系统及安全设备日志中的安全事件往往容易被忽视
- 日志记录格式不规范，未制定统一的日志记录规范，记录字段各异，存储形式多样化
- 缺少日志分析功能，缺少将各事件进行关联分析的基础

审计导向



- 内控要求
- 等级保护要求
- 人行要求 - 个人金融信息保护
- 银监会要求 - 信息科技风险管理指引
- 日志分析和审计的工作量十分巨大、复杂度越来越高
- 日志缺乏有效管理、事后审计无法及时发现风险、缺乏挖掘隐匿风险及违规现象的手段等问题，部分监管要求也未能落地

可视化导向



- 互联网出口网络流量缺少安全监控
- 防止高级持久性威胁
- 预防&监测敏感数据泄露
- 安全事件及时发现和响应，并进一步取证调查和分析
- 提供可视化资产管理、威胁管理、风险评估中安全事件的监控、分析、处置和漏洞管理的统一安全管理平台

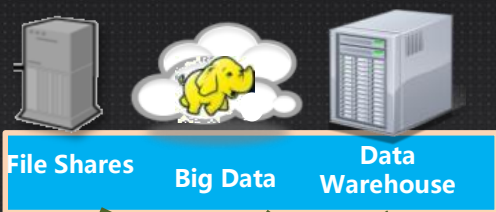
多维度数据智能分析

日志事件收集
数据上下文关联分析



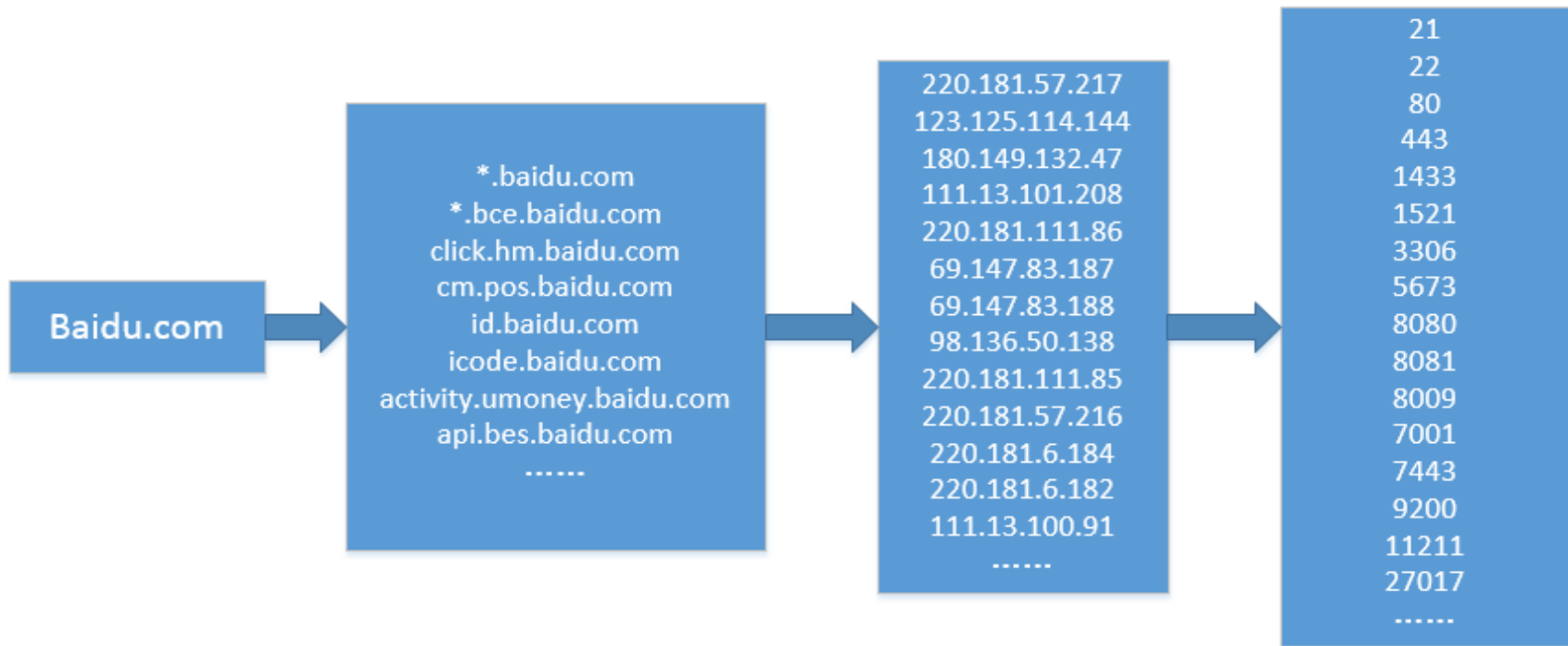
异构的日志事件收集

日志 & Layer 7 网络活动

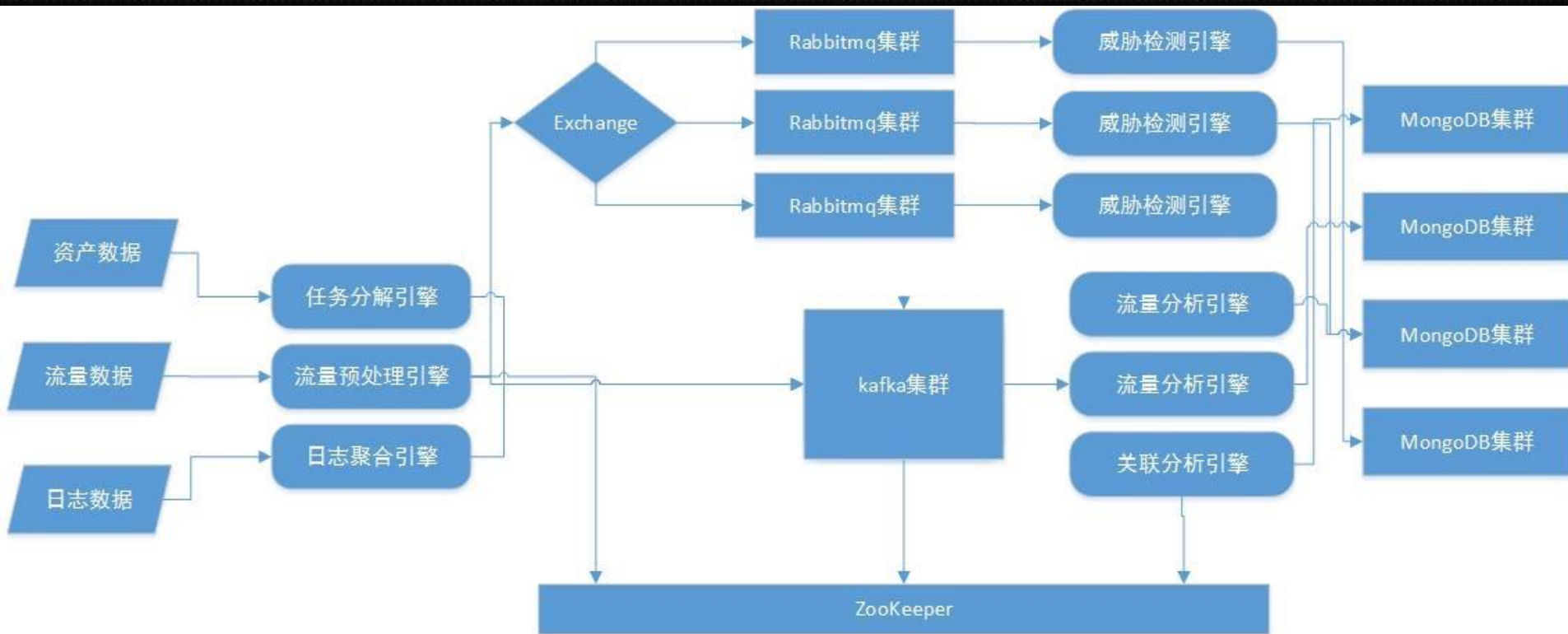


如何规模化？

1 task = 10000 Job
1000 task = ?? job



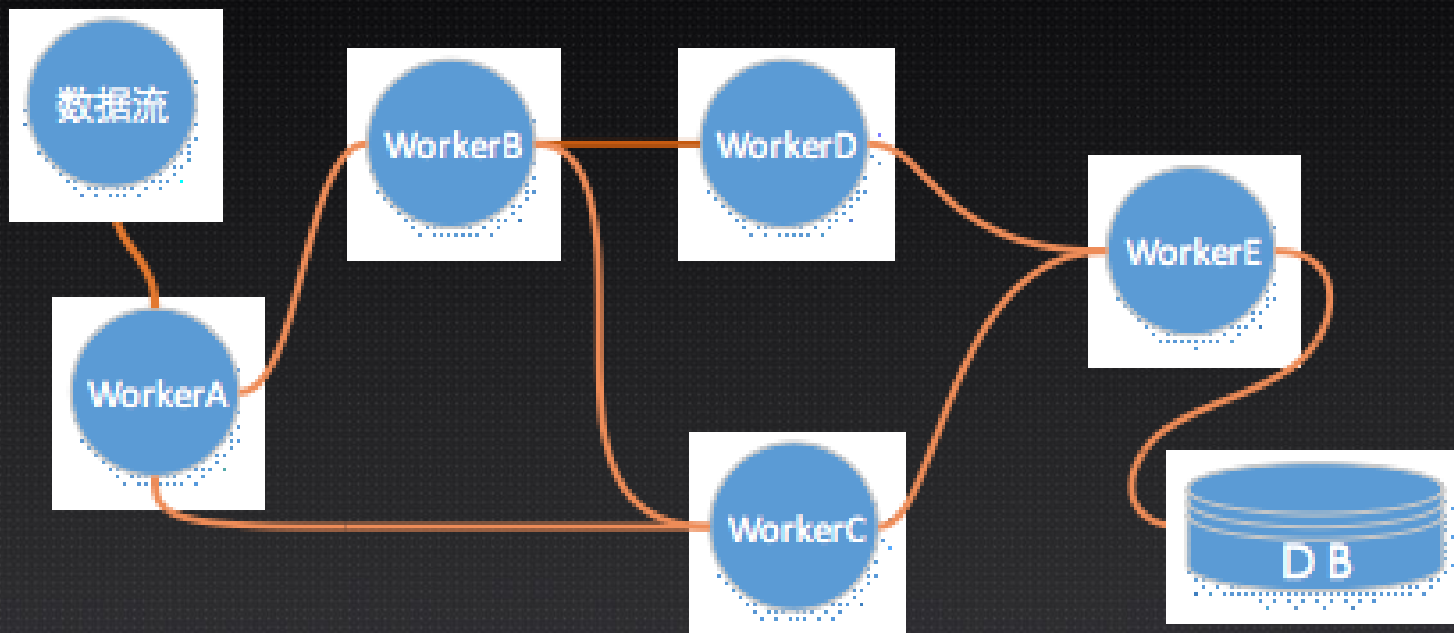
分布式基础架构



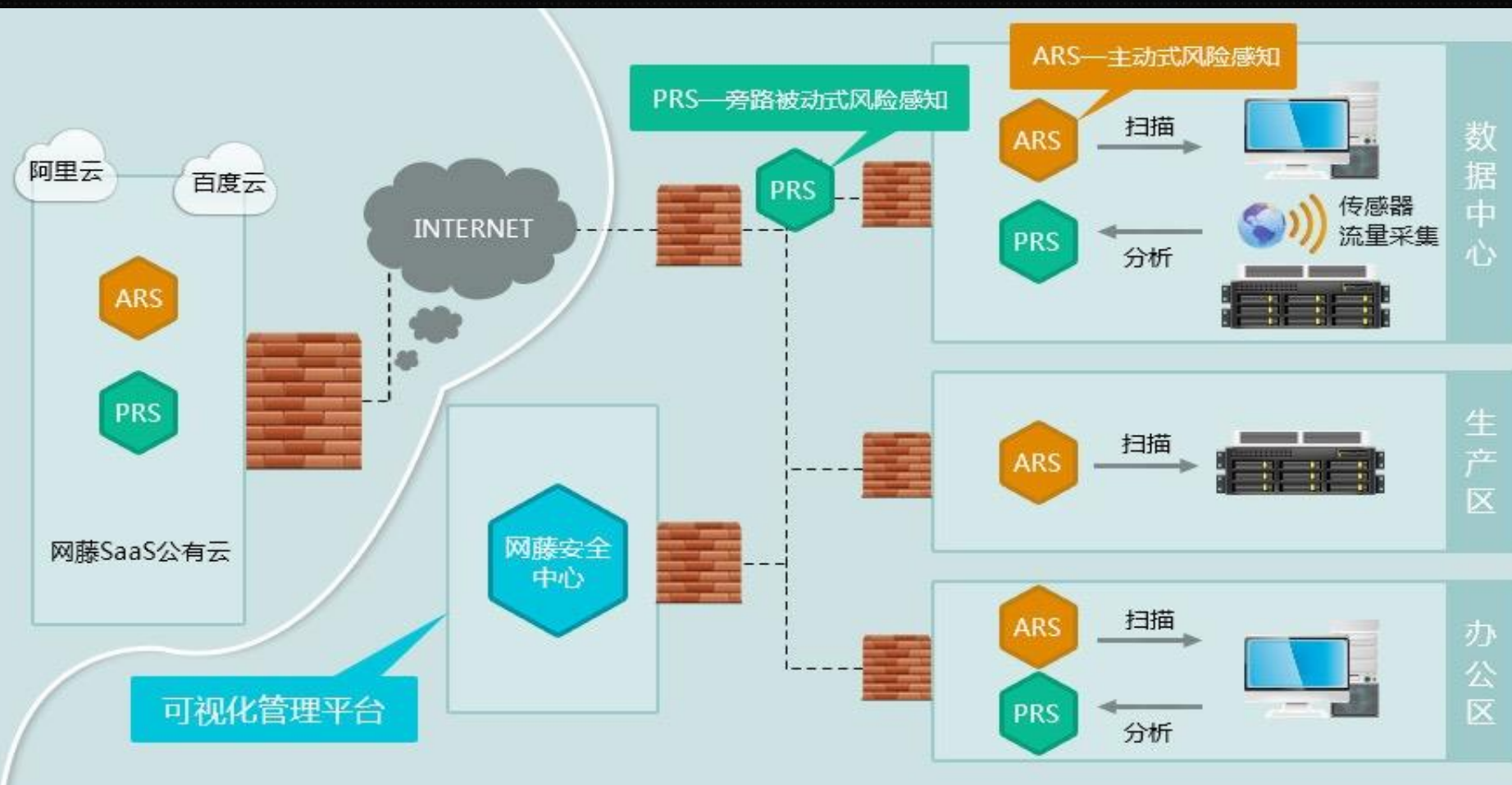
Docker集群化部署

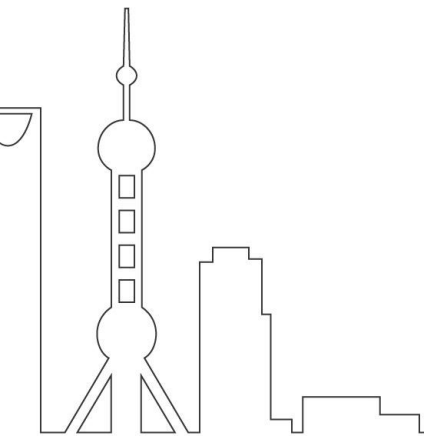
流式任务处理

协程+异步大并发 I/O



主动风险感知+被动风险感知+可视化安全中心=企业一体化风险感知体系





Thanks!

International Software Development Conference