
ISC
2015
中国互联网安全大会
360互联网安全中心
ISC
2015
数据驱动安全
2015 中国互联网安全大会
China Internet Security Conference
罗晶
象云技术总监


ISC
2015
中国互联网安全大会
360互联网安全中心
ISC
2015
数据驱动安全
2015 中国互联网安全大会
China Internet Security Conference
云数据中心的安全运维
NETNIC
企商在线
象云
xiangcloud
可信云服务认证
TRUCS

内容摘要

一、敏感的安全话题

二、信息安全 VS 数据中心安全

三、数据中心的安全保障

四、云时代的安全挑战

一、敏感的安全话题

此章内容仅为新闻摘录，不代表我司对相关厂商的态度

2014新闻回顾：

- ✓ 支付宝找回密码功能存漏洞，用户欠款丢失
- ✓ 某网站安全支付不安全，大量信用卡信息泄露
- ✓ 微软停止XP支持
- ✓ OpenSSL心脏出血漏洞
- ✓ 某知名论坛800万用户信息泄露
- ✓ 苹果承认存在“安全漏洞”XcodeGhost 被黑客注入恶意代码
- ✓ 摩根大通银行数据泄露影响1/4美国人
- ✓ 智联招聘86万条简历数据泄露
- ✓ 遭黑客攻击 索尼影业信息泄露
- ✓ 12306再曝漏洞：用户密码身份证等敏感数据泄露

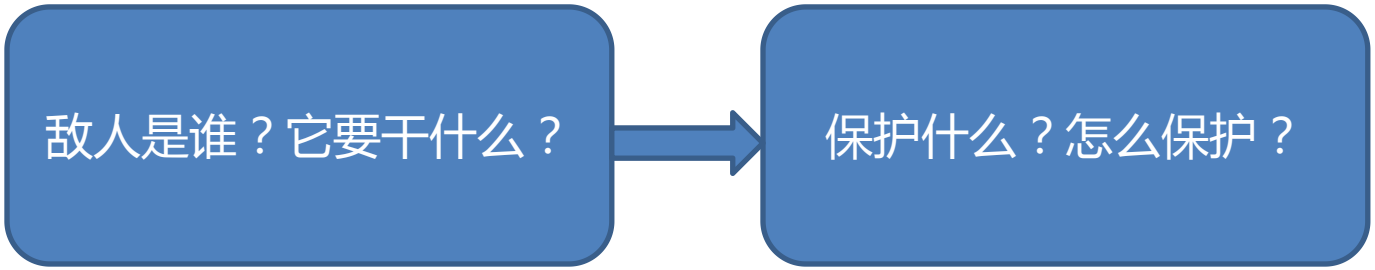
一、敏感的安全话题

数据中心常见的杀手：

- ✓ 2012年10月下旬，桑迪飓风一路席卷弗吉尼亚州、特拉华州、马里兰州和新泽西州时，曼哈顿与美国东沿岸大部分地区一样
- ✓ 2015.8.12, 天津港瑞海公司危险品仓库特别重大火灾爆炸事故，腾讯天津研发与数据存储中心、以及国家超级计算天津中心受到直接影响。
- ✓ 2015年5月27日,由于杭州市萧山区某地光纤被挖断,造成目前少部分用户无法使用支付宝
- ✓ 2013年7月22日，因光缆被市政道路施工挖断，微信发生连接故障，北京、上海、广东、浙江等地的部分微信用户无法正常使用
- ✓ 2015.8.22日，日本富士通集团在美国硅谷的数据中心最近遭遇停电，致使其一些云服务中断
- ✓ 2015.7.22日夜间,腾讯云遭遇史上最强DDoS攻击，大流量的DDoS恶意攻击，攻击峰值接近300G

安全问题无处不在， 如何应对？

IT安全在我们周围



信息安全战略

- 安全战略
- 安全架构与规划

- 传统安全问题：DDOS SSH 密码…
- 虚拟化，云计算问题：用户多元化需求…

信息安全管理

- 安全组织建立
- 安全流程合规

- 传统安全问题：上层过滤 防远程脚本 强密码…
- 云计算问题：运维自动化 备份 集群 …

内容摘要

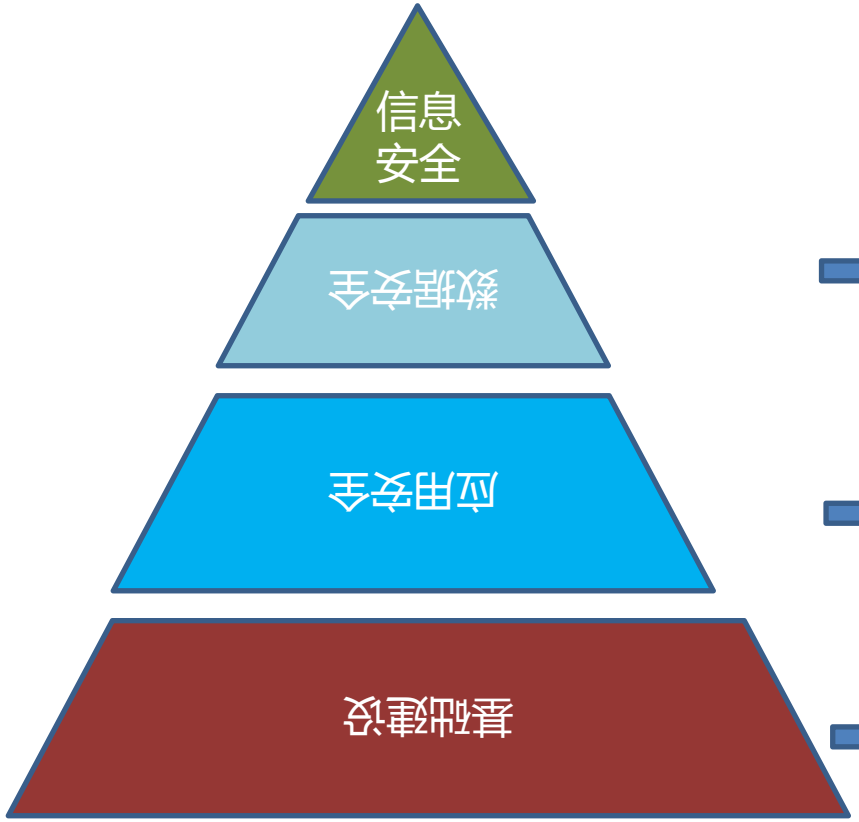
一、敏感的安全话题

二、信息安全 VS 数据中心安全

三、数据中心的安全保障

四、云时代的安全挑战

二、信息安全 VS 数据中心安全



分类分级 数据加密 数据传输

备份归档

权限安全 访问控制 日志审计

物理安全 网络安全 系统安全

云计算安全 虚拟化安全

安全运维

内容摘要

一、敏感的安全话题

二、信息安全 VS 数据中心安全

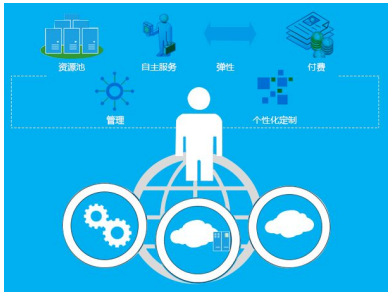
三、数据中心的安全保障

四、云时代的安全挑战

云时代IDC面临的挑战

企业级用户需求：

- 弹性扩展公有云
- 私有云管理服务器
- 混合云
- SDN CDN
- 专线、光纤
- 定制化数据中心
- 高标准自动运维



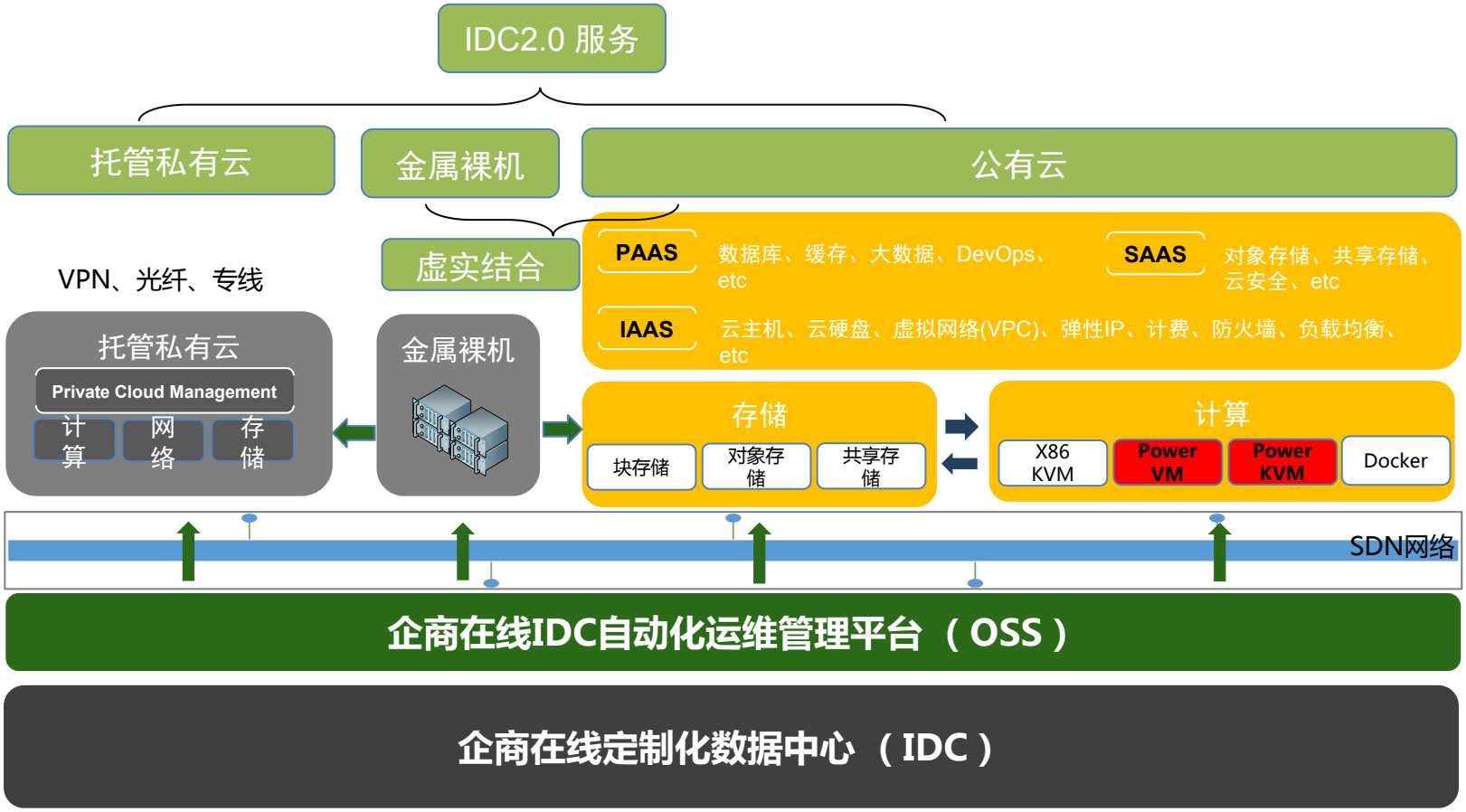
传统IDC

~~增值服务~~

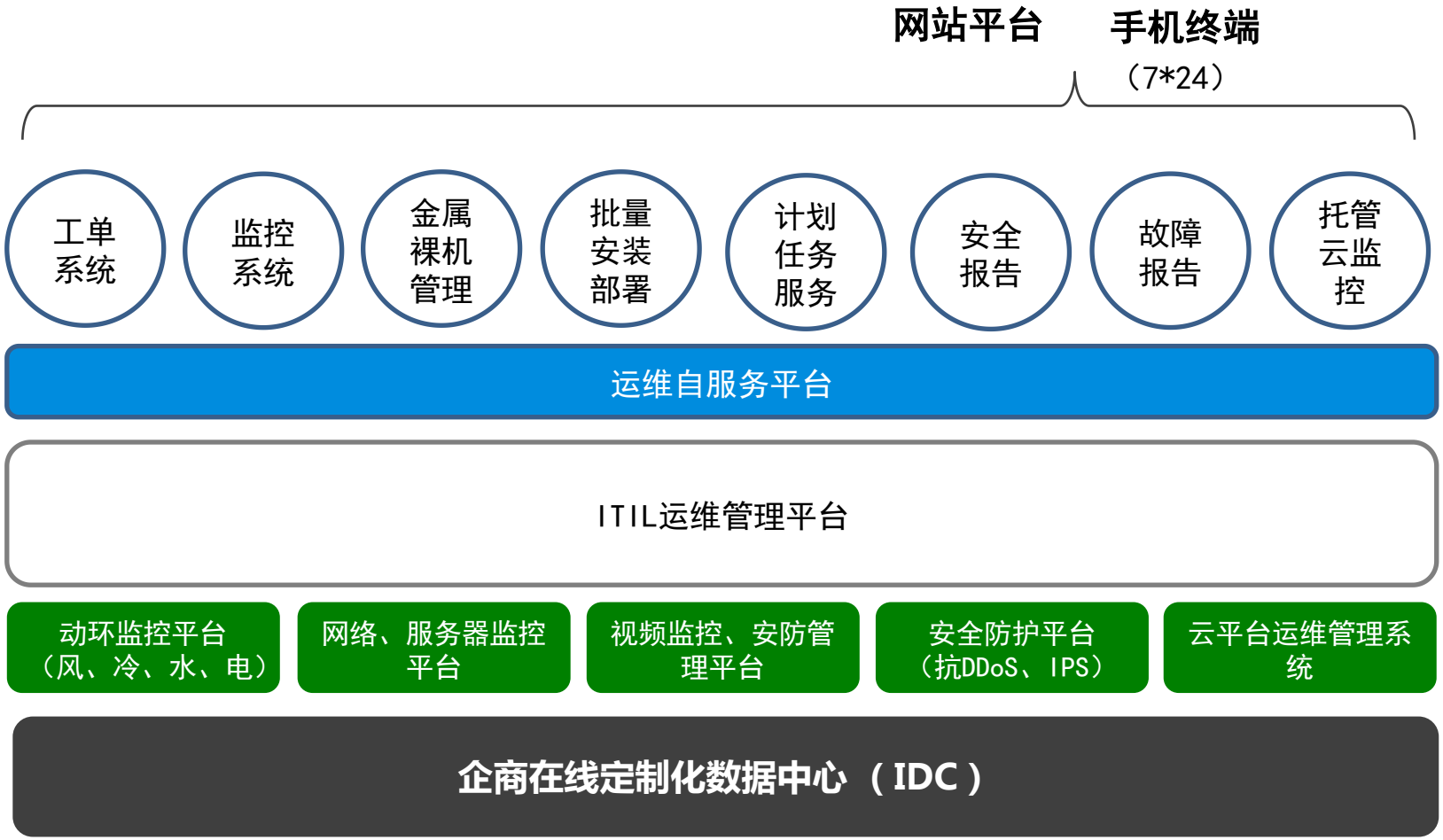
~~互联网带宽~~

~~风火水电~~

企商在线IDC 2.0（Portal）



企商在线 - IDC 2.0一体化运维



三、数据中心的安全保障

物理安全 风火水电

电力保障

多级电路保障机制 UPS电源 备用发电机 电力应用系统 发电机后备电源

物理管理

设备巡检机制 节假日，异常天气特巡 动环监控 标识管理

防火安全

环保，消防

安全防火线缆 气体灭火系统 细水雾系统 火灾报警系统（动环监控 ）

注：图片均来源企商在线机房实地拍摄

三、数据中心的安全保障

物理安全 访问控制

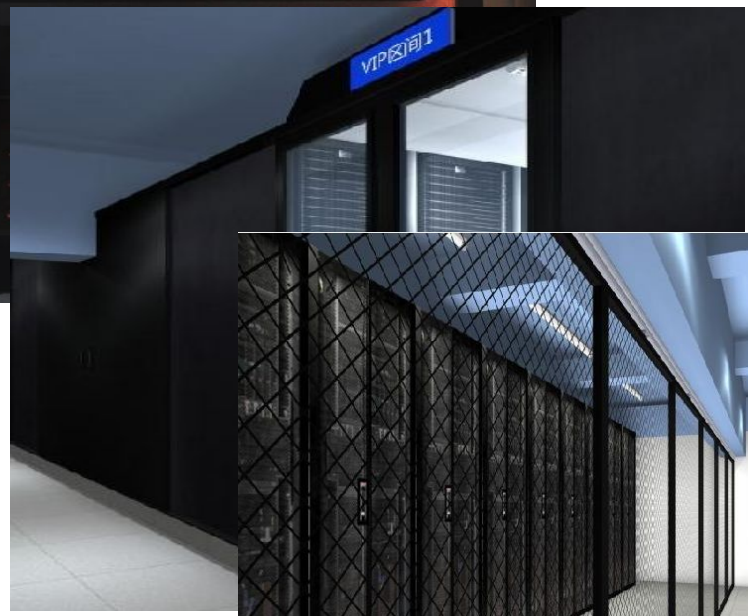
进出区域管理：门，门开关，身份识别，用户追踪

进出人员管理：用户授权，时间管理，门禁联动

报警和事件

安全等级 ：生物识别 卡（身份证） 密码

企商在线已经投入使用二代证认证系统及生物识别技术



三、数据中心的安全保障

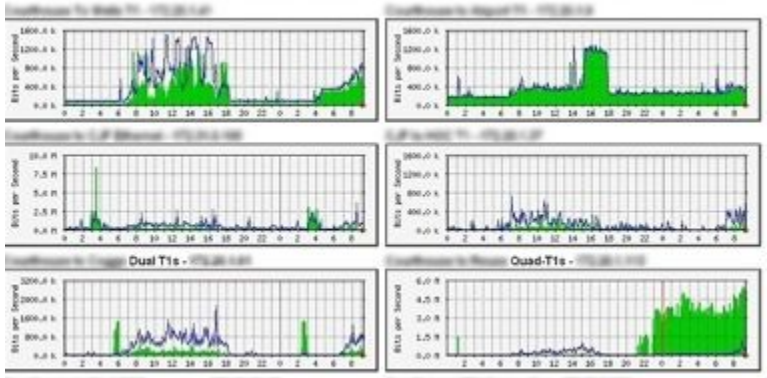
网络安全

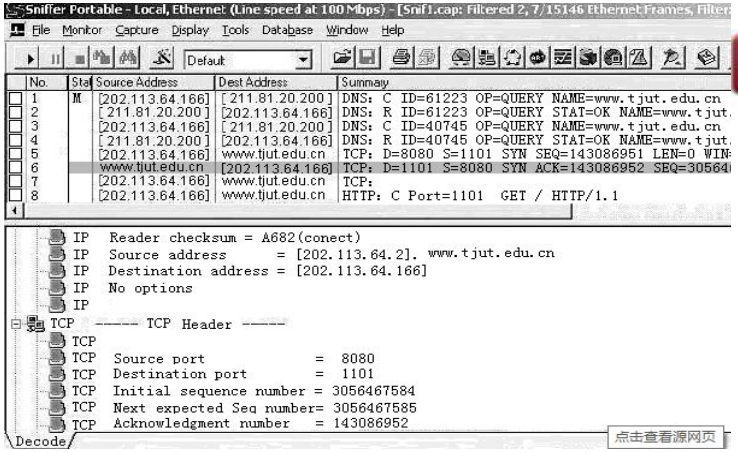
网络架构设计：互联网边界确认 双冗余确认 网络带宽确认

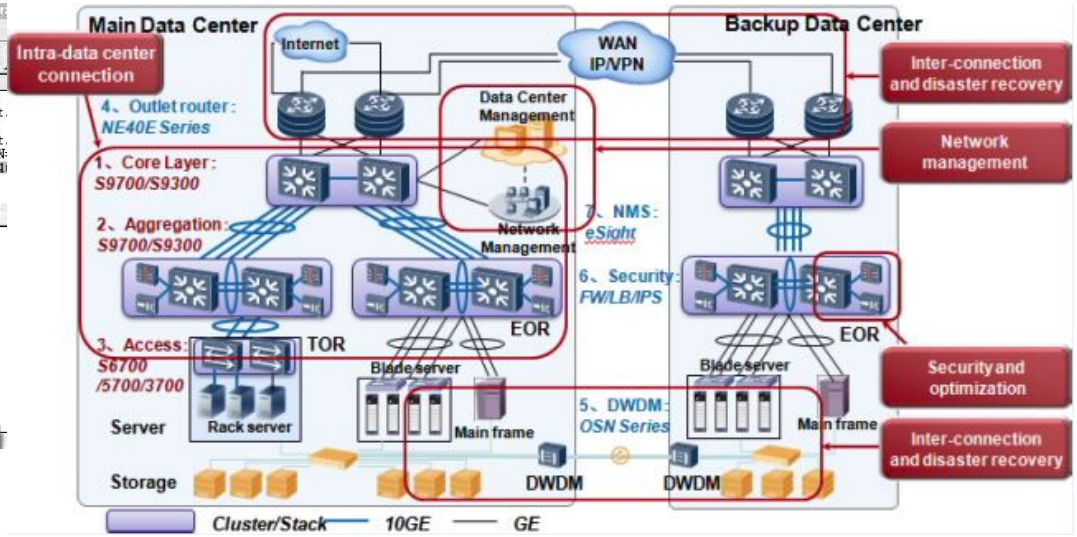
DDoS：增加资源 流量清洗 隐藏IP（分流）

网络流量监控：流量异常

内网探测 ARP SCAN SNIFFER ：核心端口监控







三、数据中心的安全保障

系统安全

弱口令：ssh telnet snmp mysql

DDoS: dns(反弹)放大攻击, ntp , scan

文件读取rsync nfs ： 用户权限管理

Database： InfluxDB mongodb (XSS) memcached (遍历敏感信息) redis (getshell)

信息泄露：Elasticsearch Hadoop

安全常见传统问题，在云时代下仍然存在。

三、数据中心的安全保障

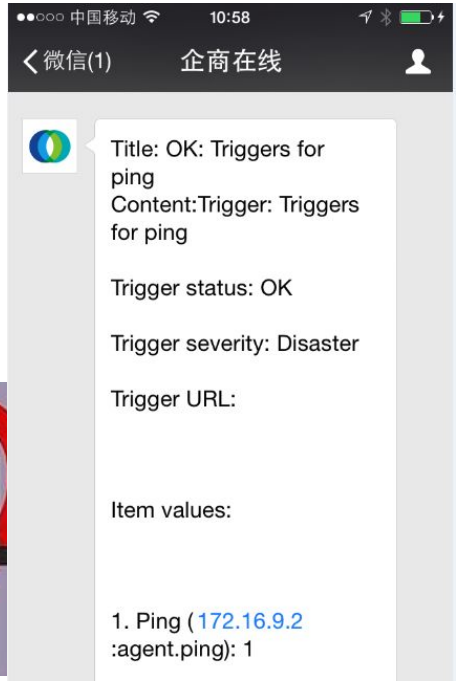
安全运维

BAT某分站修改了弱口令还更弱（可shell可内网） BAT内部员工接私活导致某qq.com域服务器shell进入内网 腾讯某系统配置不当导致Getshell

人员安全意识（**自己人害自己人**）：弱口令 备份

重大安全事件（**不可避免的天灾**）：心脏出血， struts2 漏洞，打补丁

自动化监控报警及修复（**尽量避免的人祸**）：减少误操作 快速定位 可追溯



内容摘要

一、敏感的安全话题

二、信息安全 VS 数据中心安全

三、数据中心的安全保障

四、云时代的安全挑战

四、云时代的安全挑战

✓ 传统信息安全技术不能满足云计算信息安全需求。

您的想法很多，我来帮助你完成。灵活的云时代，我必须有办法。

✓ 恶意软件、保密和访问认证等问题仍然存在云计算信息安全

专业的人，做专业的事情，我们和专业的人一起为解决您的问题

✓ 用户数据泄露或丢失使云计算信息安全面临的巨大的安全风险

分类，传统备份，云备份，分布备份，异地备份等多种选择，必有一款适合你

我们一起在努力，并已经解决部分问题。

M erci

O brigado

G racias

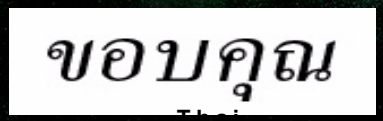
go raibh maith agat

Спасибо

G razie

T hank Y ou

ありがとうございました



D anke