

云中应急响应

沈勇

联席负责人, 上海分会, 云安全联盟CSA
Manager, Global Information Security, eBay

挑战*

机遇

挑战

- ▶ 防护/调查成本 >> 攻击成本
- ▶ 云将安全风险和安全资源的集约化
- ▶ 目前，云中安全资源不足
 - 重点关注应急响应 面临的挑战

云中应急响应面临的挑战

▶ 目的

- 控制损失
- 还原真相
 - 追究
 - 预防

▶ 应急响应包括

- 准备*
- 发现
- 初步响应
- 制定响应战术
- 复制(取证备份)
- 调查
- 实施安全措施
- 网络监听
- 恢复
- 报告
- 事后跟进

重点讨论 技术准备

节点准备1

▶ 身份管理

- AD/LDAP集成
- 禁止自动化脚本带明文口令
- 禁止本地Root账号远程登陆

▶ 主机加固

- Image安全管理：Image补丁自动化，发布自动化
- VM上线后安全配置和补丁自动化

节点准备2

- ▶ 下线主机， 镜像保存
 - 处理过敏感数据的保留时间更长
 - 符合取证要求
 - 自动化
- ▶ 取证镜像获取
 - 基于网络（取磁盘已不再现实）
 - 快速

节点准备3

- ▶ 关键文件 Hash值记录和更新（完整性管理）
 - 自动化
 - 远程存储
- ▶ 时间同步
- ▶ 安全备份
- ▶ 集中日志

网络准备

- ▶ 云网络防火墙/IDS
 - 部署点
 - 性能
 - 延时
- ▶ 当前局限于
 - 主机上 Firewall/IDS
 - 边界处 传统网络Firewall/IDS


挑战

机遇

应对 防护调查成本 >> 攻击成本

- ▶ 降低调查难度
 - 网络行为更多脚印，关键系统实名使用
- ▶ 增加攻击成本/后果
 - 随机抽样调查，重小罪罚
 - 联合同行一起建立黑名单
 - 联合个人信用记录

相关技术 云化

- ▶ 云中网络防火墙/IDS
 - ▶ 云计算身份管理
 - ▶ Image安全管理
 - ▶ 补丁管理
 - ▶ 文件完整性管理
 - ▶ 取证镜像工具
- 

收费模式适合云

- ▶ 安全硬件, 部署节点 → 公司, 站点, 年度
- ▶ 产品收费 → 服务收费 (按服务级别和客户规模)



沈勇

13817739002

york.shen@gmail.com

CSA 动态

CSA 新成果

▶ CSA斯诺登事件影响调查

调查全球客户，使用美国云服务商的意愿

66% 下降甚至取消有关项目

31% 无影响

3% 更喜欢

▶ SDP概念 – 软件定义边界

12月刚 发表