企业安全与威胁情报

汽车之家　纪舒瀚

我是谁

- 姓名：纪舒瀚
- id：H5
- 汽车之家安全负责人，自0到1
- 阿里巴巴，淘宝安全，双11、双12

大纲

- 企业安全的理解
- 威胁有什么
- 情报的价值
- 落地的方式

痛

- 脱裤
- 后门
- 内网漫游
- 薅羊毛

企业安全

前提：企业类型

- 基础安全
- 风控
- 内审

企业安全-基础设施

- 防火墙
- WAF
- IDS/IPS
- SOC
- …

企业安全-防线

- 边界
- 业务应用
- 主机
- 数据

企业安全-对抗

- 管理机制：人VS(人or机器)
- 标准化流程
- 技术-人的力量
- 安全与业务的对抗

最终交付的安全状态

威胁

- 内部：人、业务
- 外部：hacker、黑产

威胁-内部

- 人意识，密码
- 业务裸奔
- 外包
- 频繁变更

威胁-外部

- 黑产链
- 周期性的攻击
- 一些意外

情报

- SRC
- 众测
- 扫描器
- 监控

落地的方式

- 防御-监控-响应
- 花样式布点
- 响应机制

落地的方式


-80 中国电信
22:55
94%
全部消息
筛选
今天 14:33
消息通知
SOC 监测有压缩文件提醒
Count:1
IP:
Path:/ html/e /
PerUserData/arc/
su /_zhangxi
baoma-0520.zip
2016-06-21 14:33
今天 15:33
消息通知
SOC 异常文件提醒
Count:1
IP:
Path:/ web/deploy/
mallpe 0011/WEB-INF/lib/
el-1.0-SNAPSHOT.jar
ret:Avira:Java/Dldr.Kara.AZ;
2016-06-21 15:33

我们的交付

威胁的先扬后抑，寻找对抗的平衡点

谢谢