千里之外，洞悉风险

APSARA EVOLUTION 10-

——网站安全即服务

2016 THE COMPUTING CONFERENCE

江慧敏
深信服科技 安全营销总监

主办单位：杭州
Alibaba Group 阿里巴巴集团
战略合作伙伴：intel

你的网站真的安全吗？

更高级的手段，更精准的攻击

传统的攻击（过去）：漏洞扫描 → DDoS攻击 → 口令破解 → 会话劫持 → 越权访问 → 身份伪造 → 逻辑漏洞

随着时代的变迁，黑客的攻击手段变的也越来越复杂，从开始传统的攻击向精准、定向转变。

精准、定向攻击（现在）：鱼叉 → 水坑 → APT攻击 → 僵尸网络 → 撞库攻击 → 钓鱼网站 → 社会工程学

黑客视角，利用精准、定向攻击，来模拟客户真实场景

扫码观看大会视频

被黑了还不知道

——漏洞被通报了才知道

漏洞概要

缺陷编号： WooYun-2016-209836

漏洞标题： 某市人民政府sql注入打包/多个数据库泄露

相关厂商： [redacted]人民政府

漏洞作者： by刺心

提交时间： 2016-05-18 16:20

公开时间： 2016-07-04 10:40

漏洞类型： SQL注射漏洞

危害等级： 高

自评Rank： 15

漏洞状态： 已交由第三方合作机构(cncert国家互联网应急中心)处理

各方面压力

被黑了还不知道

——数据库被泄露了才知道

[redacted]影业被黑，大量信息泄露

[redacted]12-06 22:11:11 来源: 福布斯中文网(上海)

黑客组织“和平卫士”（Guardians of Peace，简称GOP）泄露了[redacted]ony Pictures）的大量数据，我发现其中有为数不多但并非无关紧要的信用卡信息（大部分都可以在费用表或者承包商支付文件中找到），也有各种护照信息（在酒店发票和移民申请中找到）。软件安全公司Identity Finder进行的分析还在泄露的文件中发现了47,426个社保号码。

我还发现了很多薪资信息以及要求进行的医疗检查种类。不少员工的薪资都超过了100万美元，所以在这些信息被公之于众后，它们可能会成为很好的人才引进项目。

重大经济损失

扫码观看大会视频

被黑了还不知道

——网页被篡改了才知道

形象/公信力下降

扫码观看大会视频

部署了WAF和其他安全设备？
——攻击者总是能突破防御壁垒

网站已是众矢之的
- 攻击技术普及化
- 攻击收益明确化
- 攻击行为产业化

攻防技术不对等
- 防御技术总是落后于攻击技术发展
- 未知攻，焉知防

未知威胁层出不穷
- 0day漏洞公开叫卖
- 高级攻击逃逸技术防不胜防

通过人工服务进行周期性的检测和响应？

慢！

- 周期检测，问题发现不及时
- 人工响应，人员协调到位需要时间
- 依靠人员素质，标准化程度差

更好的办法

1

持续检测替代周期性检测

将周期性的检测做到持续的进行，及时发现风险

2

快速响应处置替代人工响应服务

将临时协调人员进行响应处置的方式做到快速的响应处置

如何实现？

——建立“云+端”服务体系

- ✓ 通过安全云服务平台的大数据关联、智能分析锁定风险链条，及时感知隐藏的入侵威胁
- ✓ 通过快速检测、主动响应、持续加固的“三位一体”快速迭代，结合“云+端”设备联动，防患于未然，避免威胁扩大

建立“云+端”服务体系

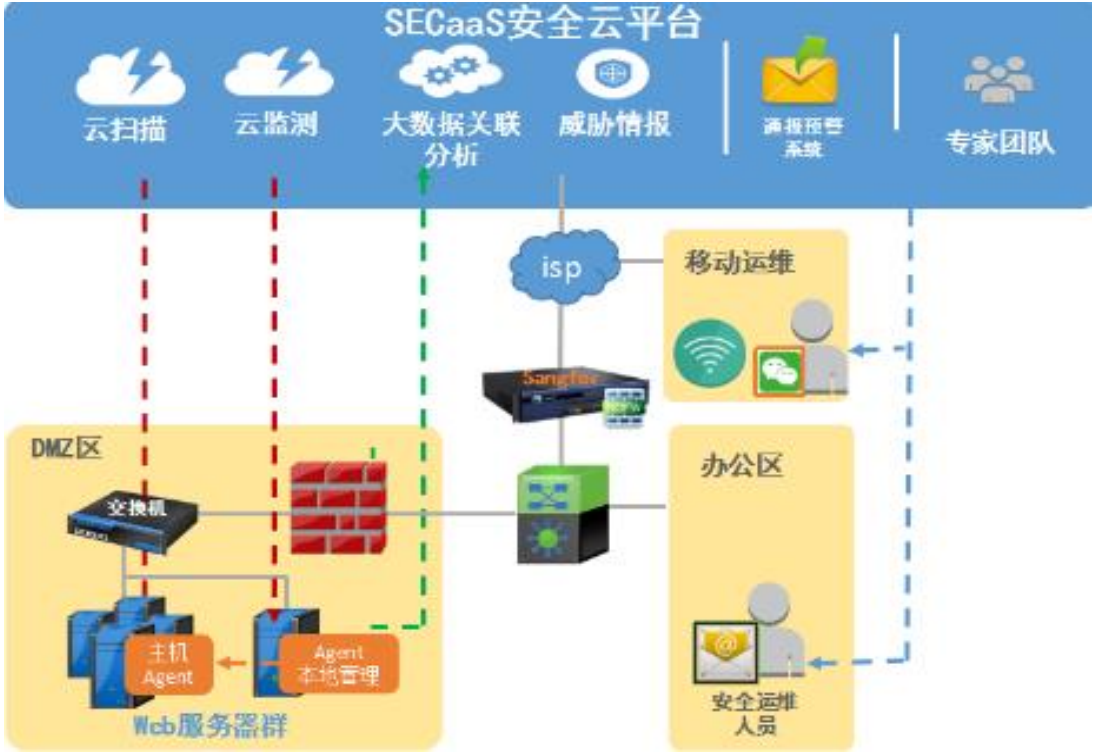
持续检测
让用户成为第一个也是最后一个知道自己安全问题的人

持续加固
通过不断优化安全策略以及及时给出加固建议，助力用户抵御新型威胁

快速响应
通过主动快速的事件响应能在威胁主动扩大前及时处置

我们的方案
——网站安全即服务

- 深信服安全服务云、端点安全插件以及下一代防火墙NGAF，形成“云+端”联动，全面的检测和防御能力
- 基于NGAF双向流量检测的未知威胁发现能力
- 专职应急专家云端快速响应，提供全生命周期问题处置服务



扫码观看大会视频

千里之外，洞悉风险

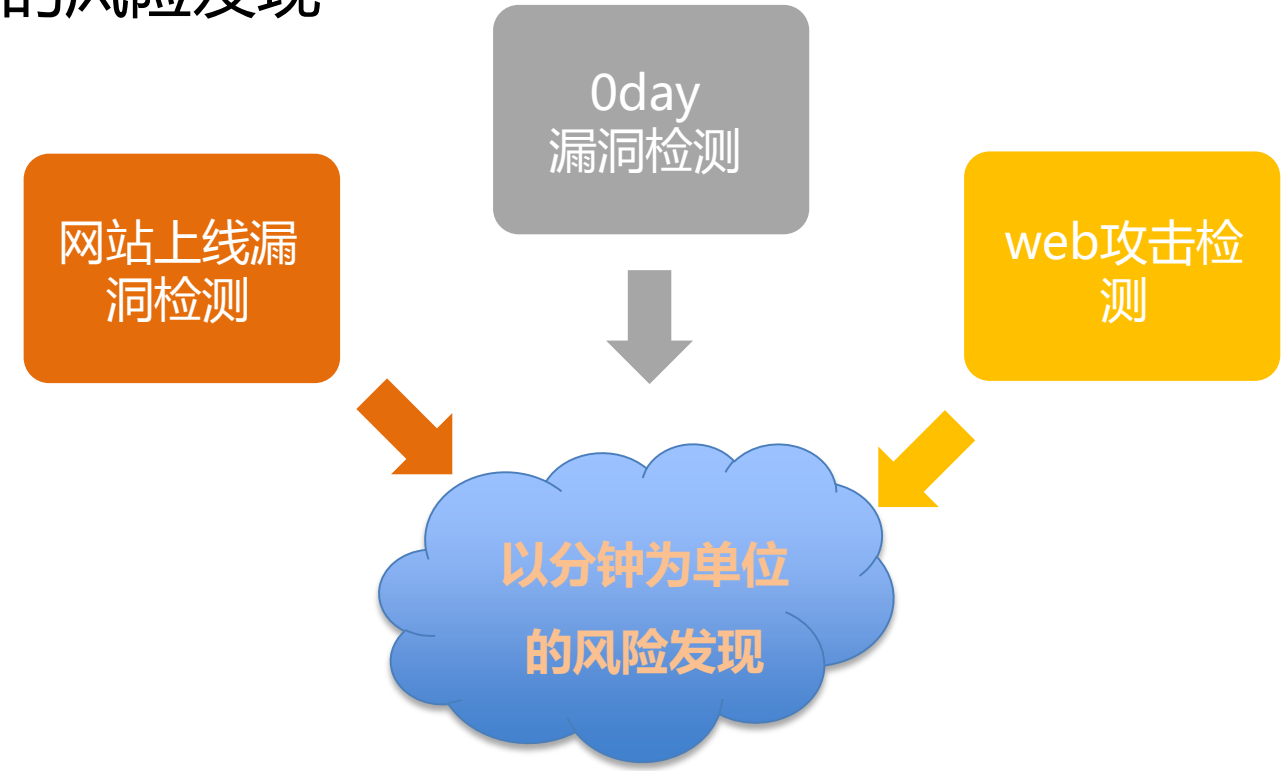
检测响应的要求

- 持续监测
- 快速响应
- 持续加固

深信服

- 实时检测
  - 7*24小时实时检测
  - 云端、边界、主机端全网视角检测
- 主动响应
  - 秒级高危事件告警
  - 分钟级主动联系响应处理
- 持续加固提升
  - 特征库持续升级防御新型高级威胁
  - 安全巡查防御加固策略调优

分钟级的风险发现



快速主动响应

微信推送告警

专家排查

智能辅助决策

扫码观看大会视频

持续加固提升

- 特征库持续升级 防御新型威胁
- 安全巡查
- 防御加固策略调优
- 主动推送安全报告

扫码观看大会视频

混合IT下网站安全即服务

2016 The Computing Conference

THANKS

SANGFOR
深信服科技