OpsWorld 运维世界大会·深圳站

跨平台的安全运维建设实践

青藤云安全：黄楼

运维世界 Ops World

01 资产梳理

02 命令审计

03 行为监控

04 响应机制

运维世界 Ops World

资产梳理

运维工作的第一件事

运维世界 Ops World

网络设备

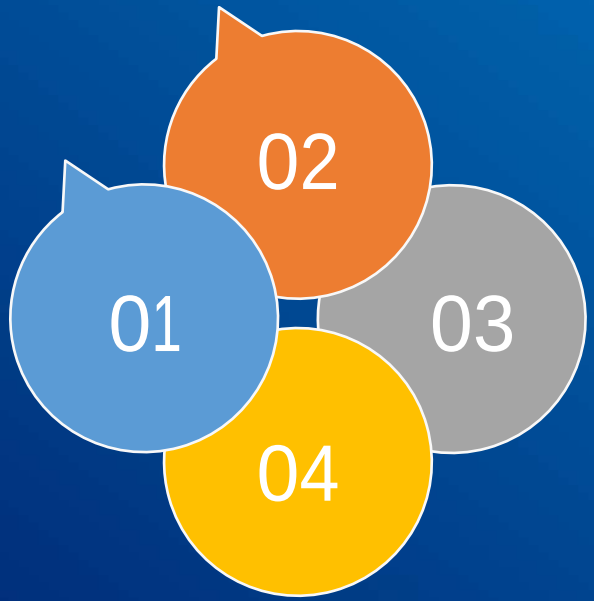
机柜、路由器、防火墙、交换机、存储

01

服务器资产

服务器型号、配置信息、所属机柜、机房、OS、内网IP

02



网络资产

公网IP列表、网段划分、路由映射关系、端口开放策略和网络拓扑

03

业务属性

业务分组、数据库、WEB、微服务、负责人、上下架、云/物理机

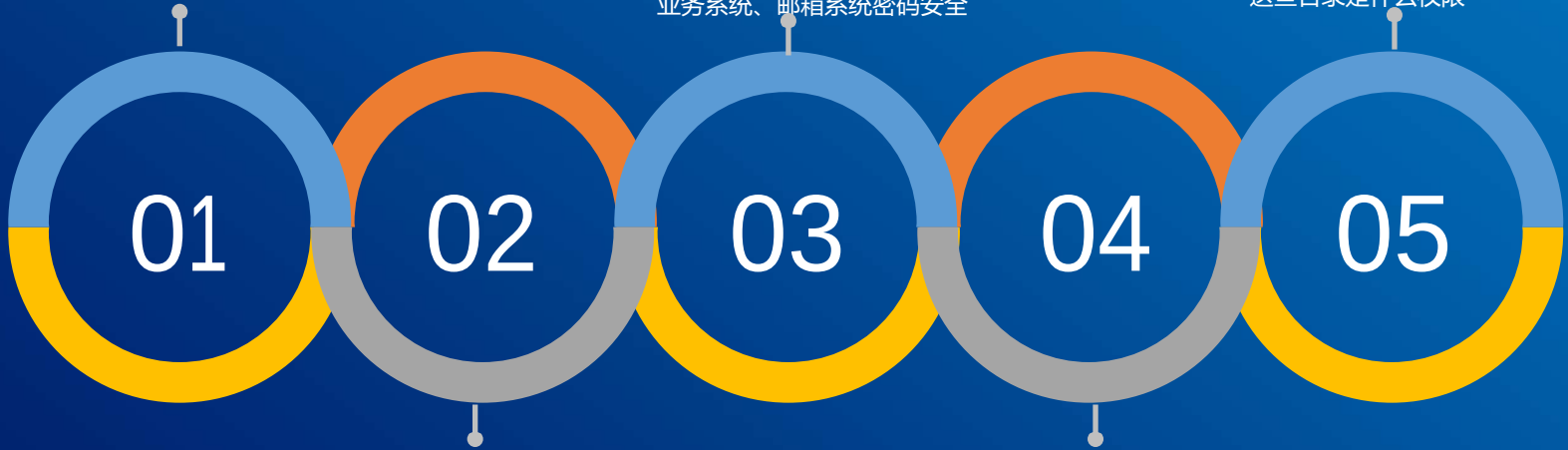
04

运维关心的资产

运维世界 Ops World

风险资产梳理

安全运维工作的第一件事



主机管理

主机数量、IP、计算机名
操作系统、业务分组

帐户安全

多少服务器上有多少帐户
有多少root权限帐户
有多少无密码sudo账户
验证密码或私钥Key的安全
业务系统、邮箱系统密码安全

网站信息

哪些网站部署在哪些业务组的
哪些服务器上
网站配置路径在哪个目录
这些目录是什么权限

进程服务

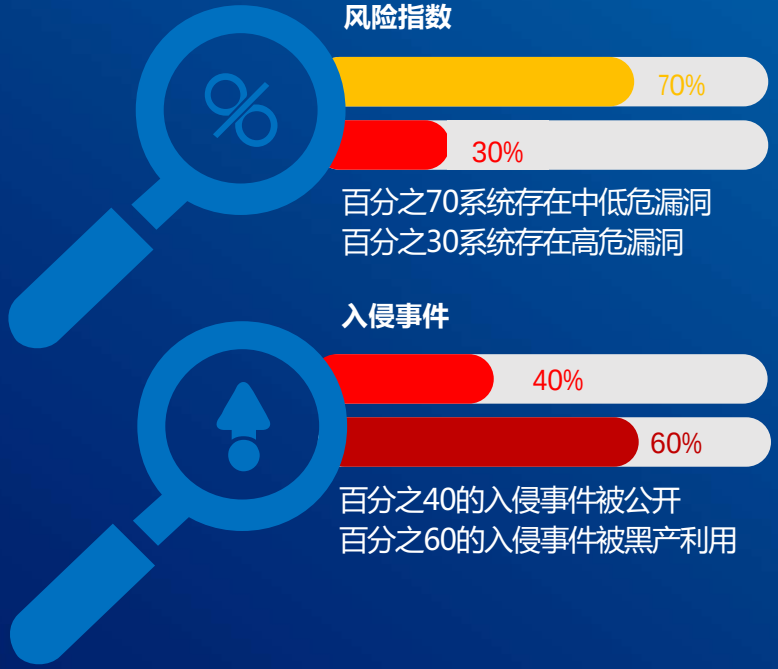
哪些机器运行了哪些进程服务
分布在哪个业务组
哪些是业务进程
哪些是系统进程
哪些框架？是否开源？

端口

哪些服务器监听哪些端口
哪些端口外部可以访问
哪些端口限制哪些IP访问


定制每个业务及操作系统的安全配置基线
安全基线
提升安全意识规范运维操作避免策略失效
安全验证
配置检查
对帐户密码的安全策略配置和系统服务的安全策略配置进行周期性的检查
登录安全
对所有登录系统的日志进行安全分析
IP白名单
设定公司IP白名单，防止异常登录
异常登录
分析不同地域IP和异常登录时间及时告警
及时发现系统漏洞和补丁定制解决方案
跟进漏洞
结合业务评估影响，提供修复方法推进
推进修复
软件漏洞
对系统软件包进行漏洞补丁的检查和修复
网站安全
对网站目录进行Webshell后门和风险文件检查
网站后门
通过内容关键词匹配和相似度匹配发现
风险文件
对源代码(svn,git)目录、数据库备份文件、压缩包进行检查

风险统计



风险指数

70%

30%

百分之70系统存在中低危漏洞
百分之30系统存在高危漏洞

入侵事件

40%

60%

百分之40的入侵事件被公开
百分之60的入侵事件被黑产利用

弱密码

例如操作系统弱密码、网站后台弱密码、OA系统弱密码、邮箱系统弱密码、AD域账户弱密码、其他办公业务系统弱密码

关键信息泄露

例如网站目录放压缩包、备份文件；github上放运维脚本，特别是包含公司初始密码的邮件报警脚本

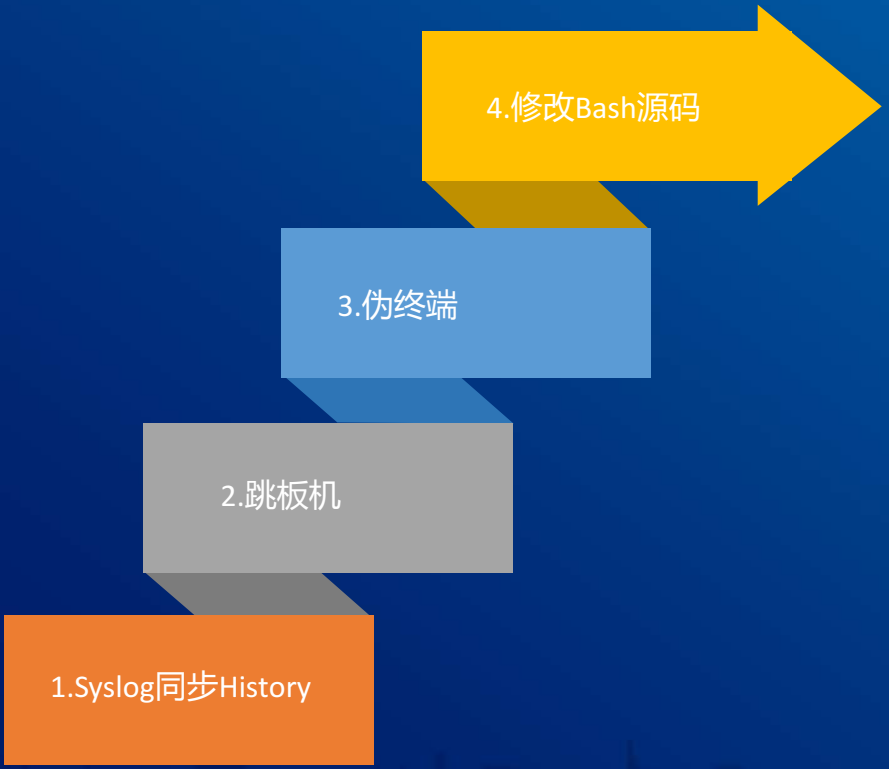
产品漏洞

例如OpenSSL心脏滴血、Bash破壳、glibc幽灵、ImageMagck、Redis写文件等等远程直接利用等高危漏洞

运维世界
Ops World

命令审计

运维规范的重要标准



黑客无法绕过但复杂度高

通过记录并且使用Agent收集日志实时上传，数据量小，而去黑客无法绕过

输入输出太大

伪终端可以记录所有屏幕的输入输出，但是日志超大，审计也非常不方便

多系统多终端

Bash、zsh、csh每一个都去研究源码，修改、编译、打包、安装

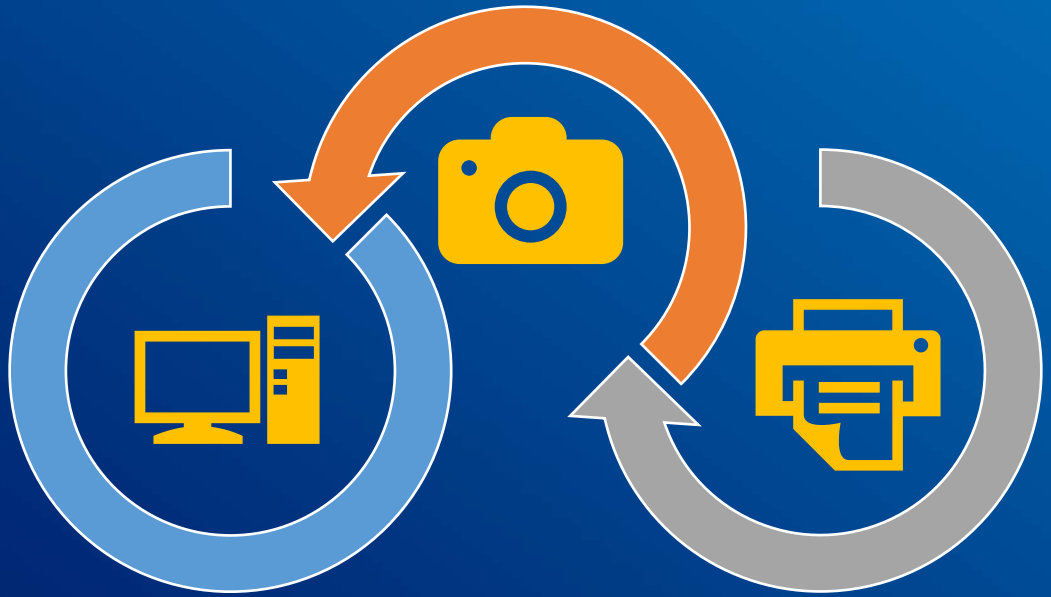
流量问题

所有人操作所有服务器都通过跳板机，随便传点文件，大家就卡不动了

绕过审计

```
export HISTFILE=/dev/null
export HISTSIZE=0
export HISTIGNORE=*
unset HISTFILE
```

实时记录上报



用户命令操作

分析审计告警

运维世界 Ops World

但是谁登录的系统？

OpenLDAP统一认证

审计哪些东西？

删除关键文件，命令行直接带密码，下载黑客工具。。。

运维世界 Ops World

行为监控

恶意行为实时发现

Redis写文件示例

```
127.0.0.1:6379> config set dir /home/wwwroot/default/
OK
127.0.0.1:6379> config set dbfilename redis.php
OK
127.0.0.1:6379> set webshell "<?php phpinfo(); ?>"
OK
127.0.0.1:6379> save
```

运维世界 Ops World

异常文件操作

redis进程写authorized_keys

passwd、shadow文件被读写

登录日志文件被清除

反弹会话

nc反弹会话

php、java等反弹bash会话

暴力破解

暴力尝试sshd登录

暴力尝试vsftp登录

提权行为

低权限进程fork出roo权限的子进程

通过Linux内核的事件通知机制，可以写程序获得事件的详细信息进行行为分析操作

运维世界 Ops World

响应机制

如何快速应急响应

分析漏洞提供修复方案

评估漏洞对业务的影响

定制修复计划和时间节点

统计受影响的服务器

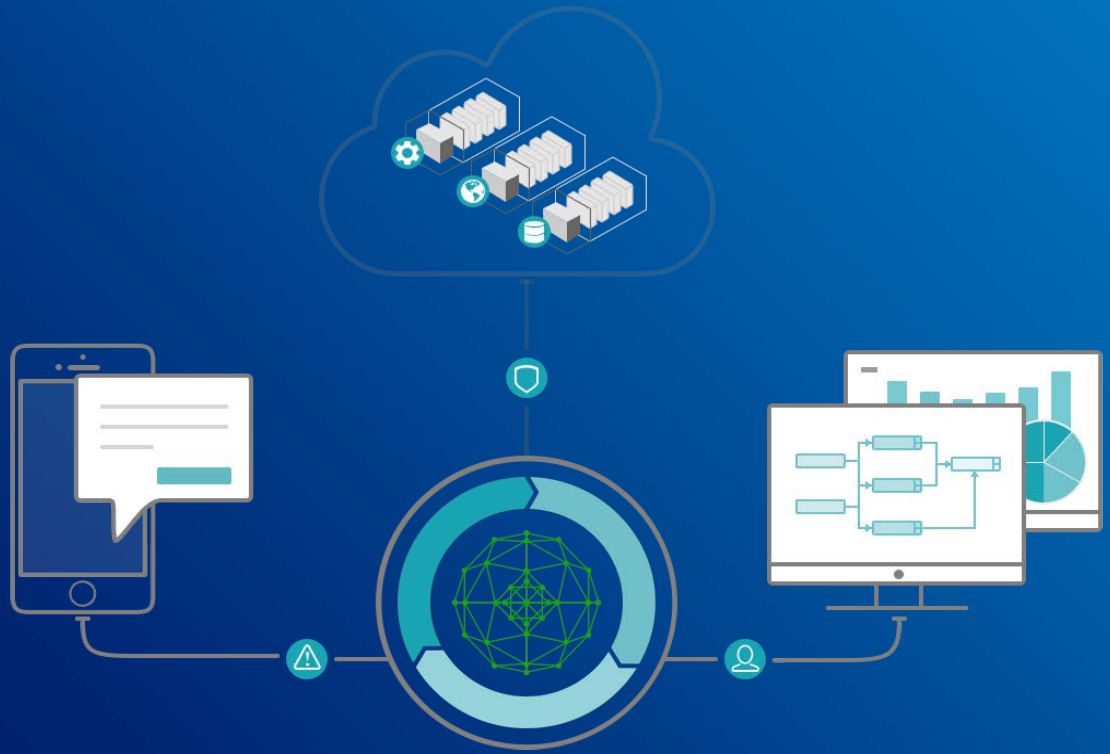
通过前面以及梳理出来的资产，可以快速定位某个发现漏洞的业务范围和具体的Ip地址列表

联动协调

联动协调各项目组、各部门涉及人。提供IP列表和漏洞分析报告以及修复方法

记录安全修复时间

通告漏洞影响范围内的所有人员，防止此类事件再次发生



如何跨平台

运维世界 Ops World

关于我们

青藤云安全是国内首家对标Gartner自适应安全体系的安全产品

公司于2014年8月在北京正式成立，天使投资650W，2015年8月份拿到A轮融资6000W。

自适应安全
国内首家对标Gartner产品

融资事件
2014.8 天使轮 650W
2015.8 A轮 6000W

标杆客户
人人行借贷宝
小米
平安科技

版本发布
2017 Q1 发布 v3.0

运维世界 Ops World

在对的时间和对的人做对的事

0X001

THANKS