



# 蜜罐的应用与识别技术

院长

Lenovo Security Analyst

LSRC ( <http://lsrc.Lenovo.com> )



# 概要

1

蜜罐介绍

2

部署蜜罐的关键技术

3

蜜罐的高级功能**&**案例

4

蜜罐安全





## 蜜罐是什么

蜜罐是存在漏洞的、暴露在互联网中的一个虚假的服务（器）  
其价值在于被扫描、攻击和攻陷

if 系统没有对外开放任何服务  
then 任何一个对它的连接尝试都是可疑的



# 蜜罐分类

## 按交互

### 高交互

1. 真实的系统&应用&漏洞
2. 数据捕获、分析、控制



### 低/中交互

1. 模拟的TCP/IP协议栈
2. 模拟的服务&漏洞



## 按类型

### 产品型

1. 容易部署
2. 实时报警



### 研究型

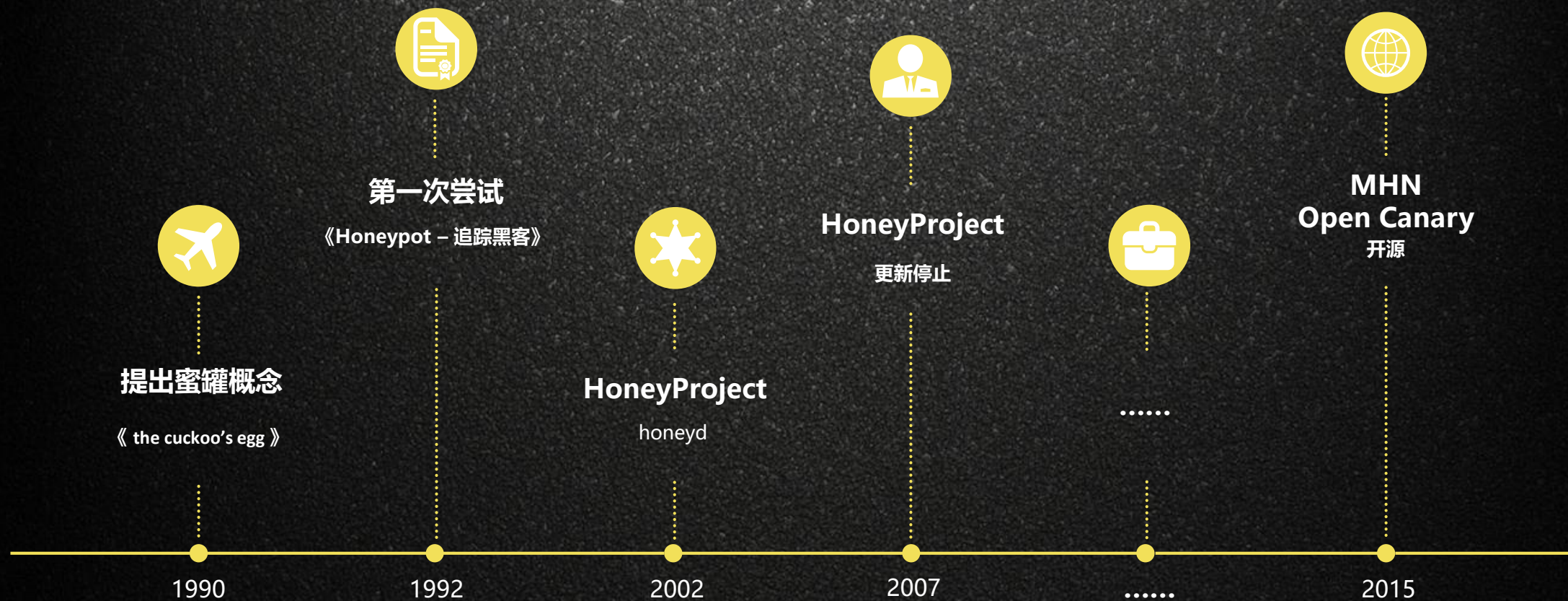
1. 高交互
2. 数据捕获



# 蜜罐分类

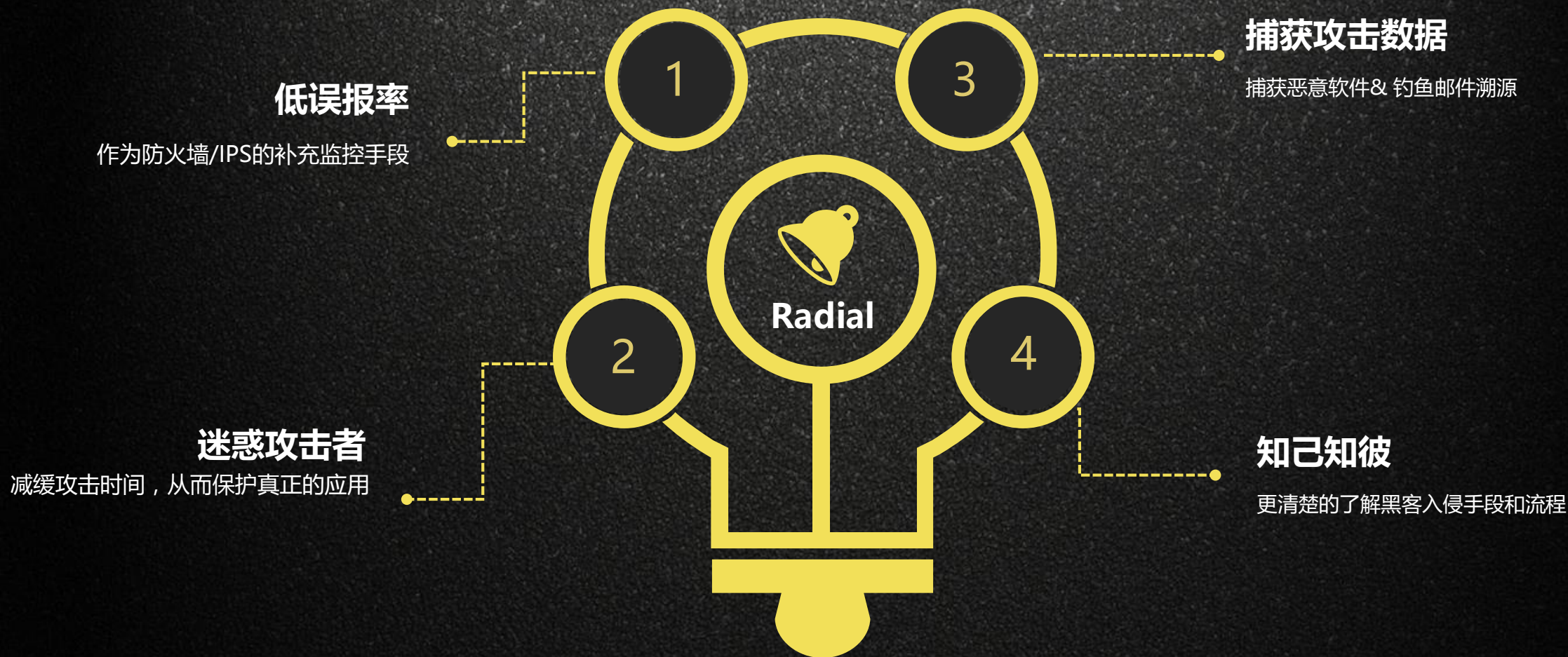


# 蜜罐发展史





# 蜜罐对企业安全的作用







## | OpenCanary

1. 开源
2. Python
3. 支持的功能
  - I. Windows
  - II. Linux
  - III. MySQL
  - IV. MsSQL
  - V. .....

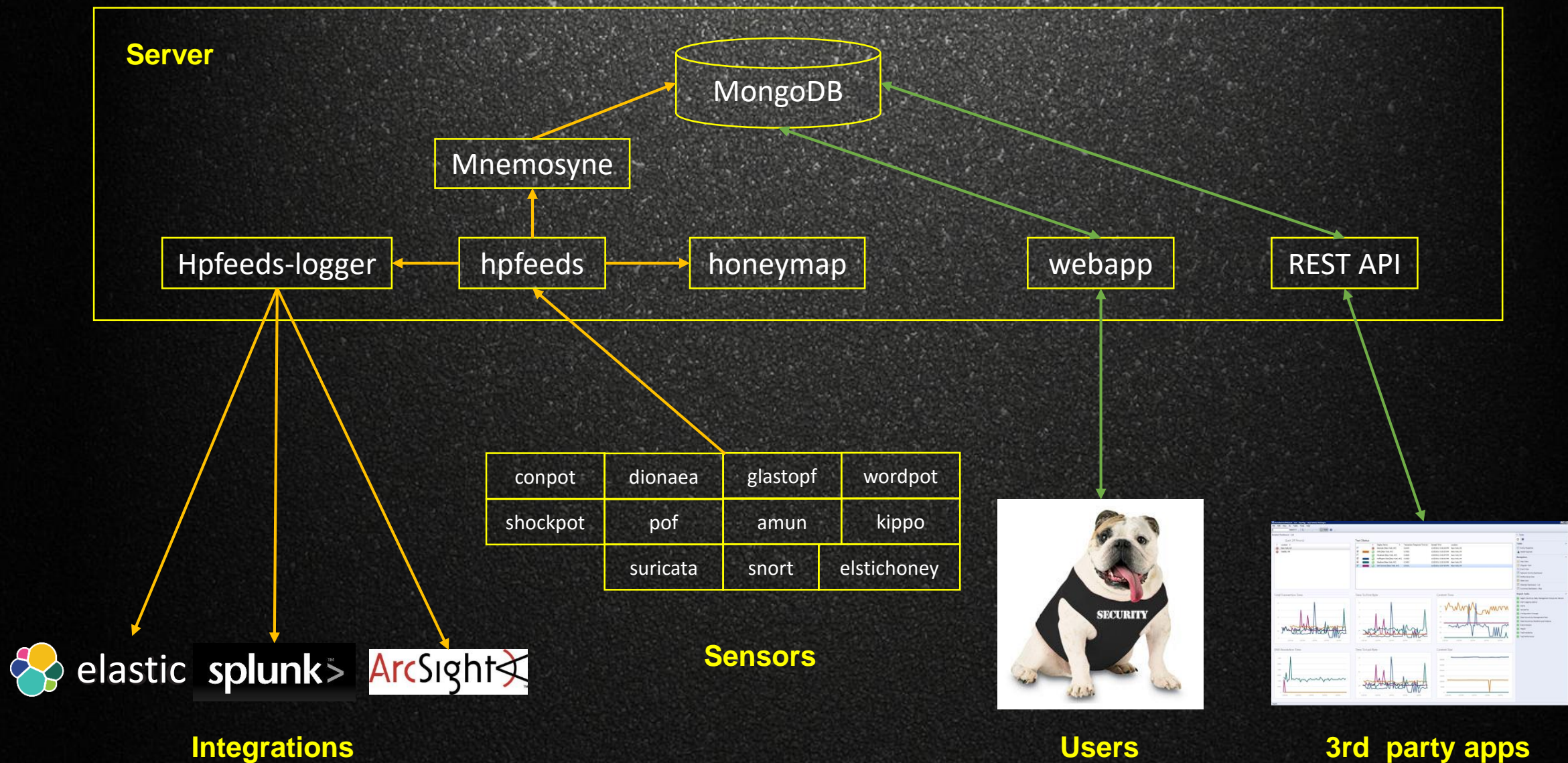


## MHN特点

1. 开源
2. Python
3. 框架
4. 支持的蜜罐
  - I. Kippo
  - II. Dionaea
  - III. Conpot
  - IV. Snort/Suricata
  - V. .....



# 蜜罐应用 - MHN架构





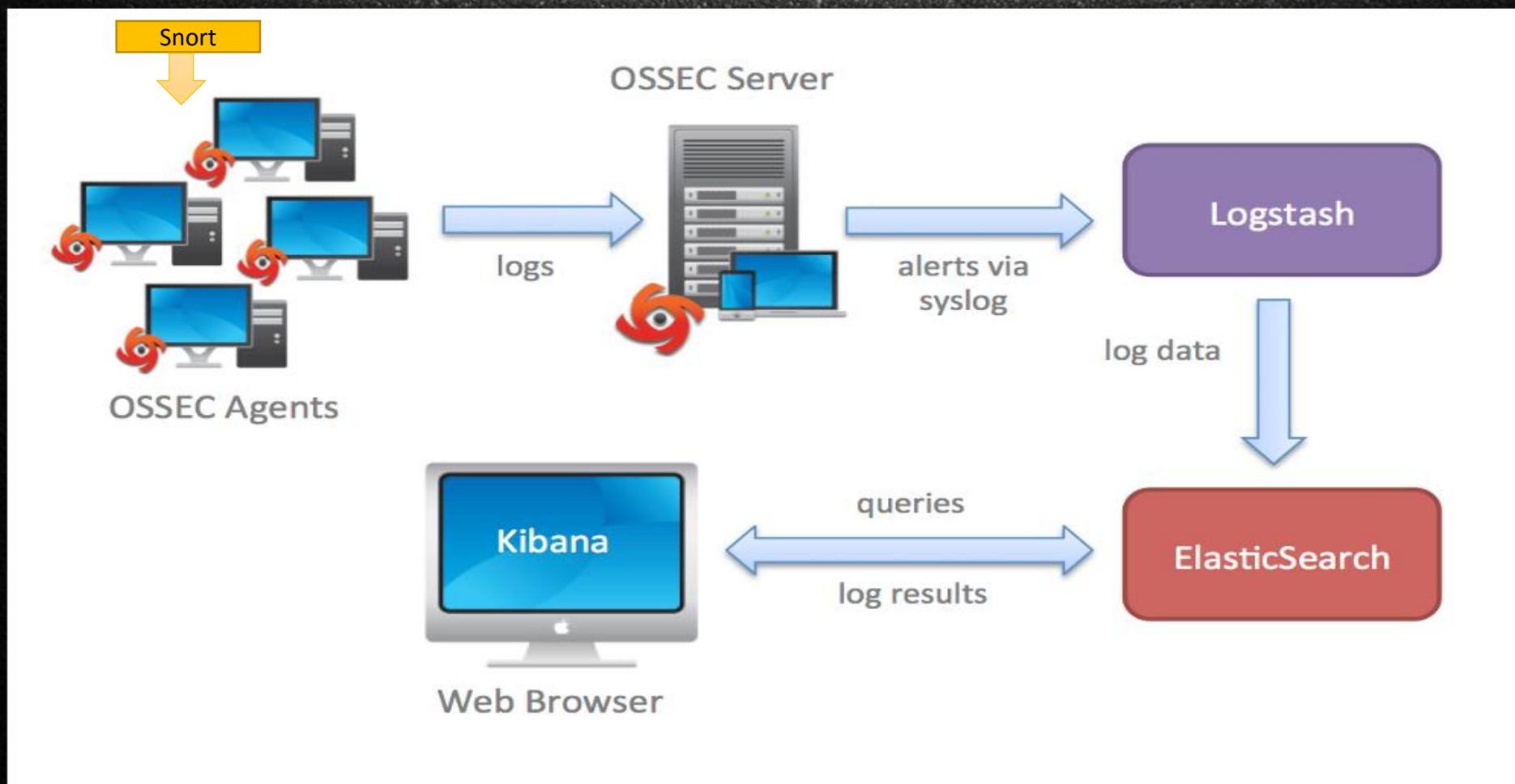


## 部署蜜罐的关键技术

1. 日志处理
2. 实时报警
3. 监控设备辅助



# 日志搜集





# 实时报警 - 地图





## 实时报警 - 微信

需要准备的东西：

注册微信企业号

添加部门成员

添加一个可以发送消息的应用

新建一个管理组，授权应用

需要从企业号提取的信息：

成员账号、组织部门ID

应用ID、CorpID、Secret

调用微信接口

access\_token:这是调用接口的凭证，通过CorpID和Secret获取

Shell脚本原理

curl -s -G #获取access\_token

curl --data url #传送凭证调用企业号接口

结合Splunk触发报警可以运行指定脚本的功能，将报警信息发送给指定管理员





## 安全监控设备的辅助与支持



日志收集



IPS



SIEM



管理员





## 蜜罐的高级功能&案例

1. 捕获恶意软件/发现蠕虫网络/钓鱼邮件溯源
2. 高级功能→模拟网络拓扑&欺骗扫描器
3. 捕获攻击者0day信息
4. 案例1：自制蜜罐自动报警（open canary）
5. 案例2：自制蜜罐捕获攻击者payload（\*\*\*cms）



## 分析攻击payload

1. 任意文件下载
2. SQL注入
3. Getshell
4. 绕过登录





## 蜜罐安全

1. 足够多的节点
2. 诱惑性的内容

1. 允许任何人进入，但是不允许任何人出去
2. 可以ping特定外网地址，允许访问其它蜜罐

1. 比对文件变化，发出报警
2. 根据警报时间筛选事件





## 蜜罐识别技术



### 检测低交互

低交互



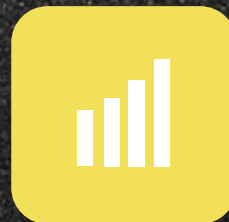
### 检测Rootkits

Rootkit



### 检测高交互

1. 检测和禁用sebek
2. 检测密墙
3. 逃避密网记录



### 检测高交互

1. VMware/QEMU
2. 用户模式Linux





## 附：常见蜜罐介绍



### \*\*\*高交互\*\*\*

#### 1. Mantrap

高交互（商用）

优点：提供了完整的操作系统，可以捕获到未知攻击

缺点：已停止更新

地址：<http://www.recourse.com>

#### 2. Argos

高交互（open source）

优点：QEMU动态污点分析技术

地址：<http://www.few.vu.nl/argos/>

#### 3. honeywall

高交互（open source）

数据捕获：iptables/snort/tcpdump/sebek

数据控制：iptables/snort\_inline

数据分析：hflowd/walleye

地址：<http://projects.honeynet.org/honeywall>

### \*\*\*Honeyd\*\*\*

中交互（open source）

优点：模拟任意网络拓扑

地址：<https://github.com/DataSoft/Honeyd>

### \*\*\*MHN\*\*\*

框架（opensource）

优点：可以继承多种蜜罐，日志功能强大

地址：<https://github.com/threatstream/mhn>

### \*\*\*OpenCanary\*\*\*

中交互（open source）

地址：<https://github.com/thinkst/opencanary>





THANK YOU