FREETALK

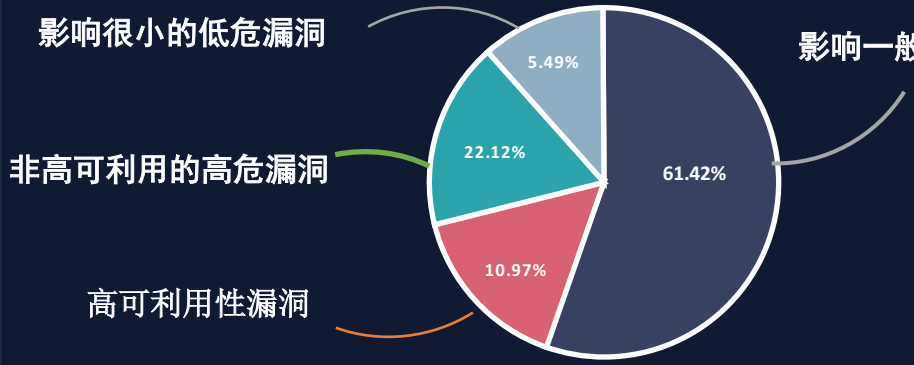
2018 北京站

如何优雅的响应漏洞

FREEBUF

漏洞响应的六思

FREETALK
2018 北京站



共收录1209个漏洞，其中：

高可利用性漏洞：238个
非高可利用的高危漏洞：267个
影响一般的中危漏洞：742个
影响很小的低危漏洞：66个

FREEBUF

标准化的重要性


漏洞搜集
自动化收集 + 人工筛选 = 录入平台
定级金字塔模型 + 漏洞专家培养方案
漏洞定级分发
漏洞响应
响应流程标准化
（漏洞预警+漏洞复现+漏洞检测+漏洞防御）
漏洞跟踪
跟踪流程标准化
（补丁+用户+变形+原理+影响）
漏洞运营
运营流程标准化
（效果 + 市场）
漏洞归档
归档流程标准化
（分析报告+标准化漏洞格式）

如何在洞海茫茫中搜集漏洞

FREETALK
2018 北京站

离别歌-phith0n
ADog's Blog
bsmali4的小窝
安全工搬砖笔记
独自等待-信息安全博客
sky's自留地
暗月|博客
0xCC
.....

Exploit-DB
PacketStorm-Exploits
SecurityFocus
Bugtraq
Full Disclosure
Seebug漏洞社区
SCAP中文社区
.....

DEFCON
窝

Google Security
小黑屋
Web Security Blog – Acunetix
安全弱点实验室
FireEye Threat Research Blog
勾陈安全实验室
腾讯科恩实验室官方博客
seebug's paper
HackerOne
.....

FreeBuf
RoarTalk
MottoIN

91Ri.org, SecWiki News,

安全脉搏, 安全盒子, ...

先知安全技术社区, 吾爱破解, i春秋社区, 看雪论坛,
T0OLS, BlackHat, 漏洞时代, SRC, 知识星球 , ...

FREEBUF

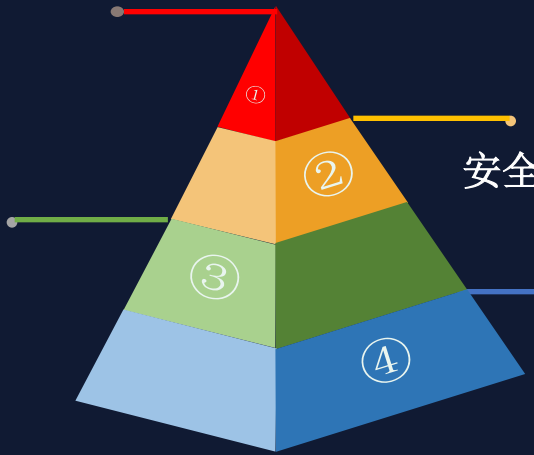
如何在漏洞中识别水洞

一级
公司预警

二级
安全云预警

三级
千里目预警

四级
平台收录



如何在漏洞响应阶段处理漏洞

FREETALK
2018 北京站

漏洞检测

云眼平台插件

云镜平台插件

插件标准化

插件在线编写 + 下发测试 + 部署上线

漏洞防御

IPS规则库

WAF规则库

规则库标准化

规则在线编写 + 下发测试 + 部署上线

漏洞预警

前言
千里百科
漏洞描述
漏洞复现
影响版本
修复建议
参考链接
深信服解决方案

预警标准化模板

根据级别推送到不同接口人

漏洞复现

超融合架构

云端镜像仓库

Docker模板

云+端的漏洞靶场部署

FREEBUF

如何跟踪漏洞

补丁跟踪

跟踪漏洞补丁

用户跟踪

受影响客户推送

变形跟踪

收集变形攻击脚本（其他检测方案），更新云眼平台插件。

收集变形绕过数据包，更新AF库

原理跟踪

漏洞原理分析文章

绕过补丁方案

影响跟踪

统计影响分布

如何运营漏洞

跟踪变形攻击 1

收集变形攻击脚本（其他检测方案）

分析漏洞原理找出绕过补丁方案

调整规则和插件的准确性 2

收集变形绕过数据包，更新AF库

更新云眼平台插件

深入影响跟踪 3

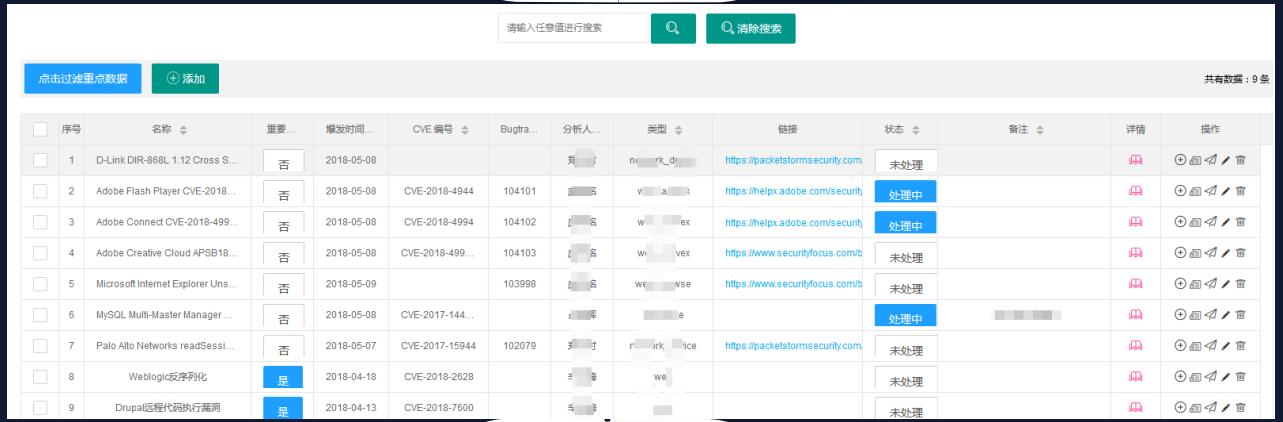
设备+云平台联动形成大数据平台，统计漏洞影响分布

如何归档漏洞

01 漏洞归档文件

02 漏洞详细分析文档

漏洞环境操作文档



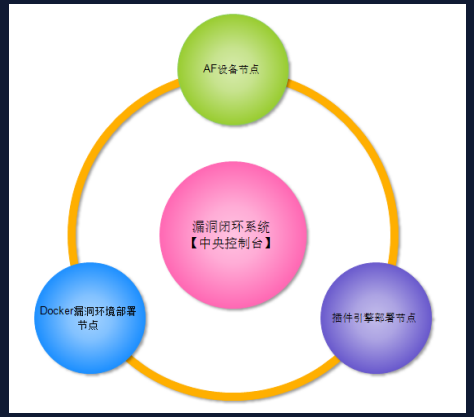
04 漏洞复盘

03 漏洞报告

预警 + 分析 + 数据 = 报告

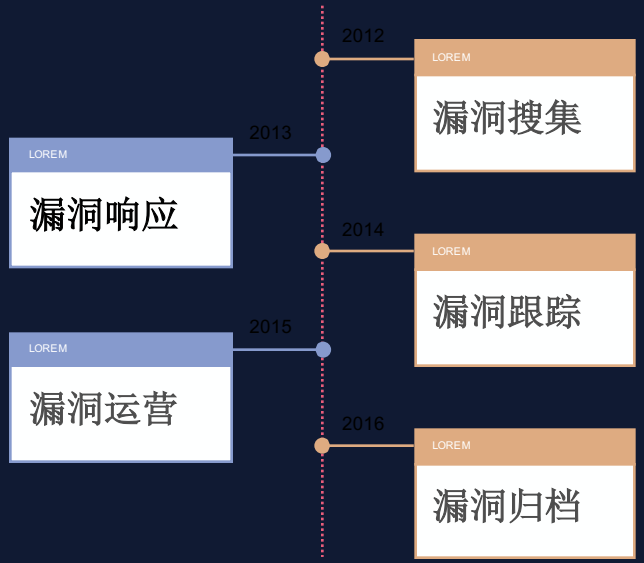
基于漏洞闭环的跟踪平台

- 漏洞闭环平台
  - 漏洞库
  - 规则库
  - 插件库
  - 镜像仓库

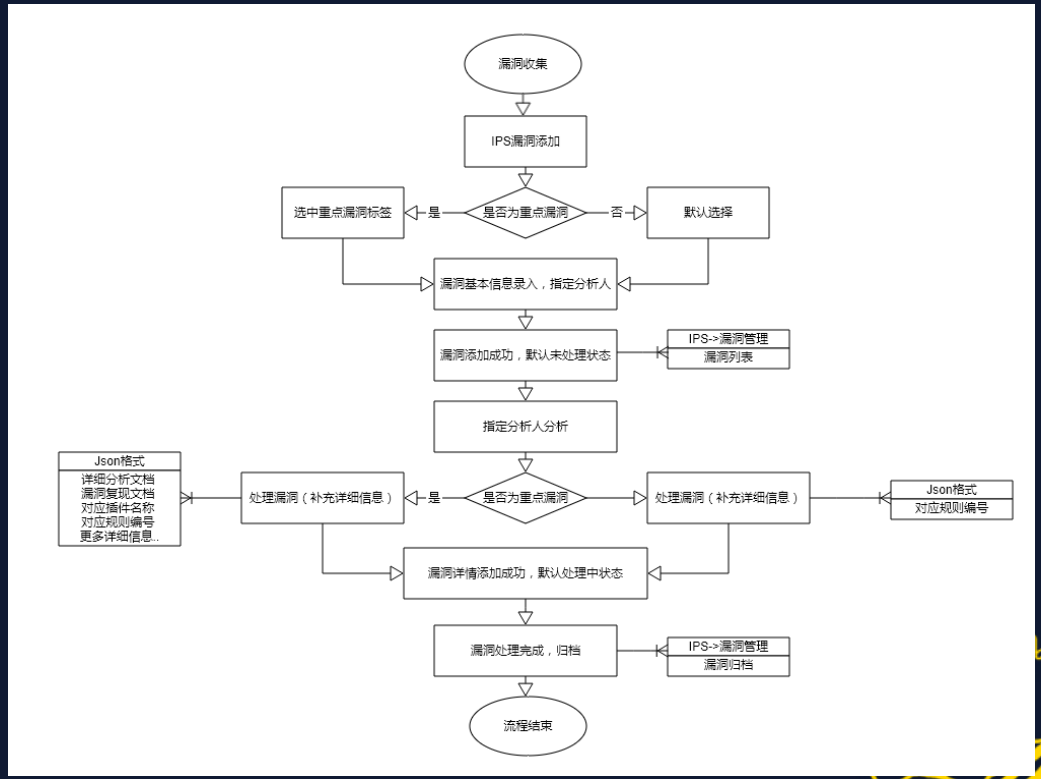


- 2012 后端：Flask
- 2013 前端：AngularJS+Bootstrap
- 2014 消息队列：RabbitMQ
- 2015 部署方式：wsgi+Supervisor+gunicorn+nginx

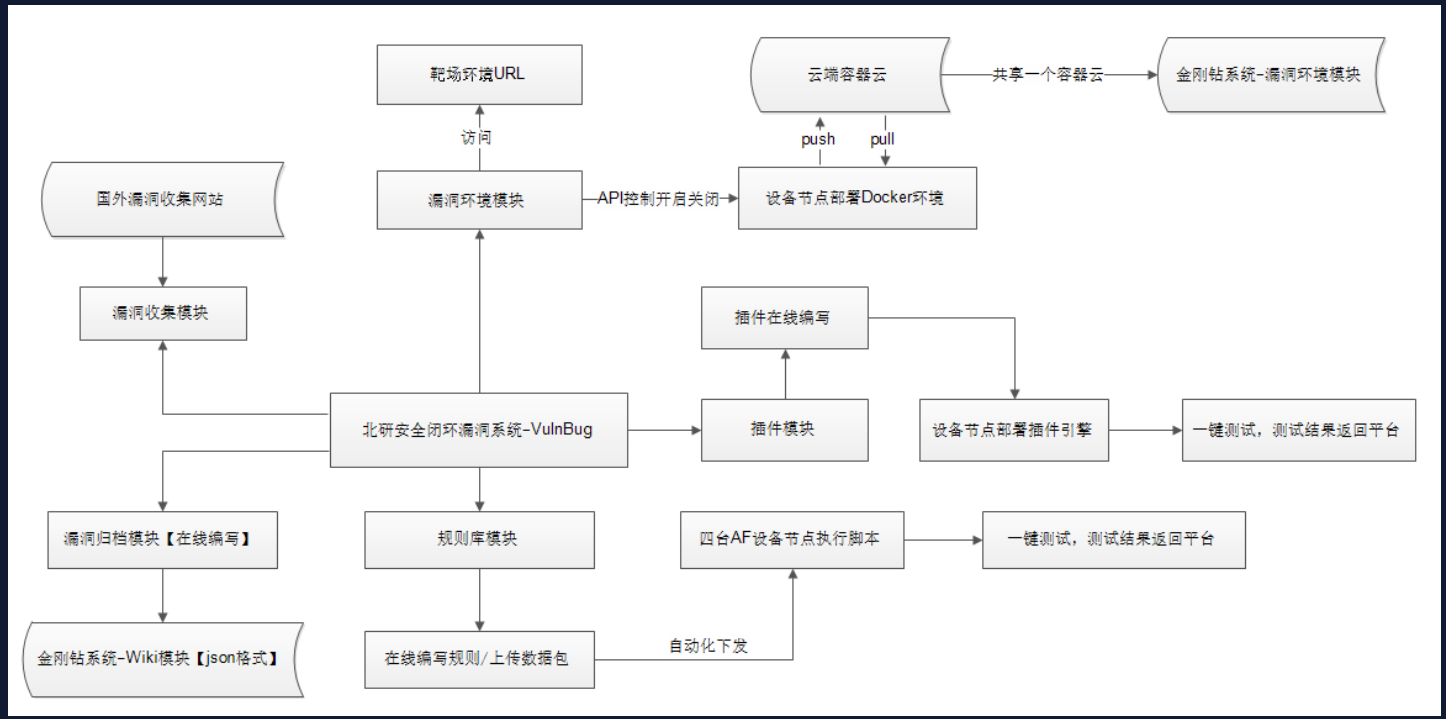
基于漏洞闭环的跟踪平台



流程图



基于漏洞闭环的跟踪平台基功能架构



漏洞闭环的跟踪平台->漏洞库

FREETALK
2018 北京站

漏洞名称
漏洞小类
备注
漏洞对象
漏洞大类
漏洞重要等级
爆发时间
微软漏洞编号
CNVD
规则编号
漏洞参考链接
CVE编号
分析人
漏洞影响版本
环境操作文档
状态
漏洞描述
链接
漏洞详细分析
插件编号
SF编号
Bugtraq编号
类型
漏洞解决方案

FREEBUF

Q&A

FREETALK
2018 北京站

FREEBUF