

FREETALK

2018 北京站

如何优雅的响应漏洞

REEBUF



漏洞响应的六思

FREETALK

2018 北京站

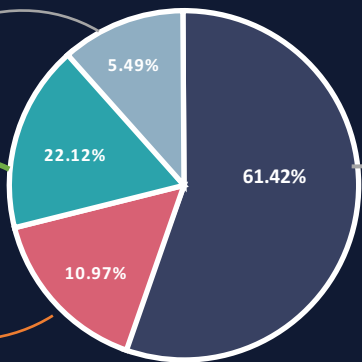


影响很小的低危漏洞

影响一般的中危漏洞

非高可利用的高危漏洞

高可利用性漏洞



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

如何在归档漏洞

如何在洞海茫茫中搜集漏洞

如何运营漏洞

如何在漏洞中识别水洞

如何跟踪漏洞

如何在漏洞响应阶段处理漏洞



标准化的重要性

FREETALK

2018 北京站



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
.....



Hacker's Blog



Vulnerabilities/Exploits



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

DEFCON
窝



Hacker Conference



洞



Security Teams



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微博
seebug's paper
HackerOne
.....

InfoSec News



Security Community



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,
TOOLS, BlackHat, 漏洞时代, SRC, 知识星球, ...

FreeBuf

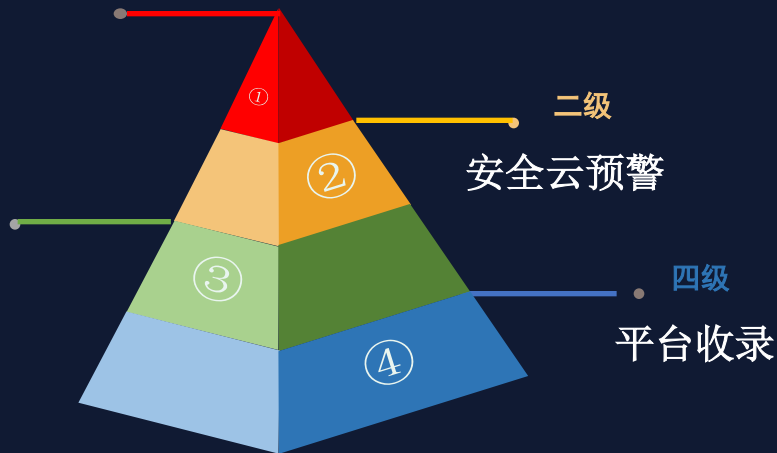


如何在漏洞中识别水洞



一级
公司预警

三级
千里目预警



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



如何跟踪漏洞

FREETALK

2018 北京站

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

FREETALK

2018 北京站

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

FREETALK
2018 北京站

漏洞归档文件

01

02

漏洞详细分析文档

漏洞环境操作文档

请输入任意关键词进行搜索

🔍清除搜索

点击过滤重点数据

➕添加

共有数据：9 条

<input type="checkbox"/>	序号	名称	重要...	爆发时间	CVE 编号	Bugtra...	分析人...	类型	链接	状态	备注	详情	操作
<input type="checkbox"/>	1	D-Link DIR-868L 1.12 Cross S...	否	2018-05-08			无...	network_d...	https://packetstormsecurity.com	未处理		👤🔍🗑️🔗	🗑️
<input type="checkbox"/>	2	Adobe Flash Player CVE-2018...	否	2018-05-08	CVE-2018-4944	104101	无...	video_a...	https://helpx.adobe.com/security	处理中		👤🔍🗑️🔗	🗑️
<input type="checkbox"/>	3	Adobe Connect CVE-2018-499...	否	2018-05-08	CVE-2018-4994	104102	无...	web_ex...	https://helpx.adobe.com/security	处理中		👤🔍🗑️🔗	🗑️
<input type="checkbox"/>	4	Adobe Creative Cloud APSB18...	否	2018-05-08	CVE-2018-499...	104103	无...	web_vex...	https://www.securityfocus.com/b	未处理		👤🔍🗑️🔗	🗑️
<input type="checkbox"/>	5	Microsoft Internet Explorer Uns...	否	2018-05-09		103998	无...	web_wse...	https://www.securityfocus.com/b	未处理		👤🔍🗑️🔗	🗑️
<input type="checkbox"/>	6	MySQL Multi-Master Manager ...	否	2018-05-08	CVE-2017-144...		无...			处理中		👤🔍🗑️🔗	🗑️
<input type="checkbox"/>	7	Palo Alto Networks readSessi...	否	2018-05-07	CVE-2017-15944	102079	无...	network_v...	https://packetstormsecurity.com	未处理		👤🔍🗑️🔗	🗑️
<input type="checkbox"/>	8	Weblogic反序列化	是	2018-04-18	CVE-2018-2628		无...	web...		未处理		👤🔍🗑️🔗	🗑️
<input type="checkbox"/>	9	Drupal远程代码执行漏洞	是	2018-04-13	CVE-2018-7600		无...			未处理		👤🔍🗑️🔗	🗑️

漏洞复盘

04

03

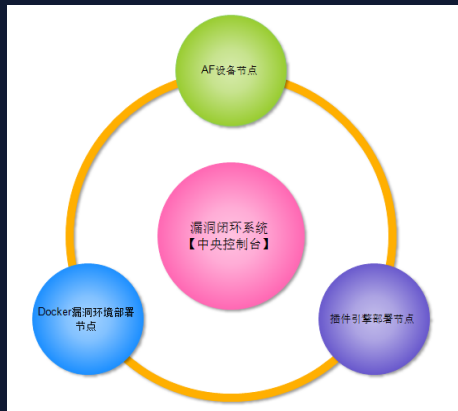
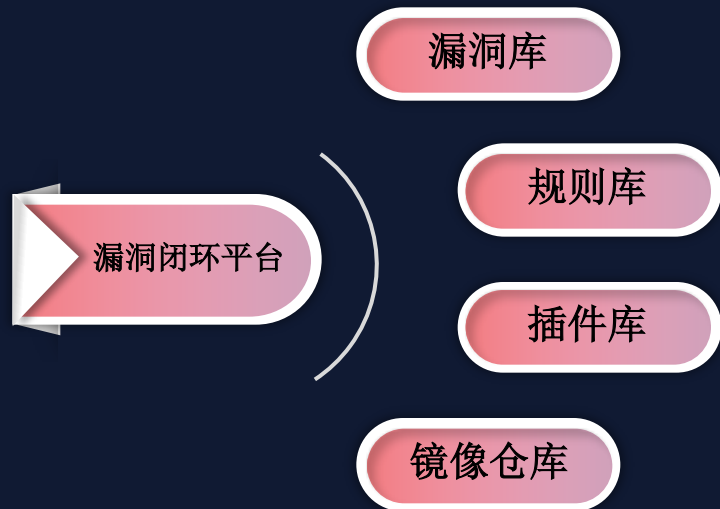
漏洞报告

预警 + 分析 + 数据 = 报告



基于漏洞闭环的跟踪平台

FREETALK
2018 北京站

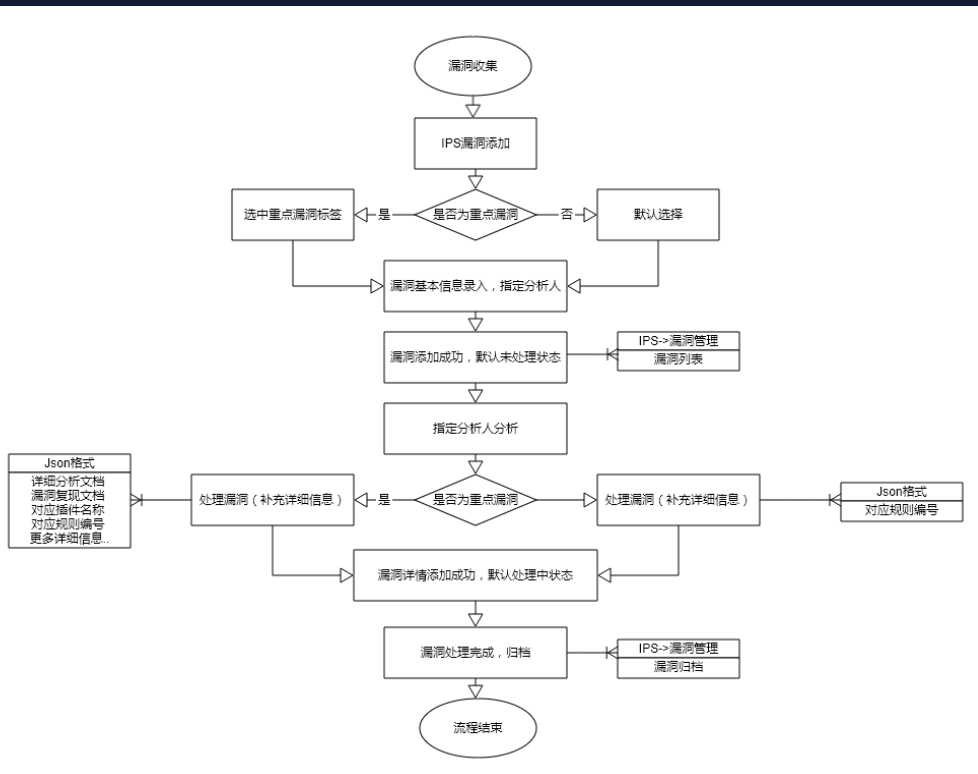
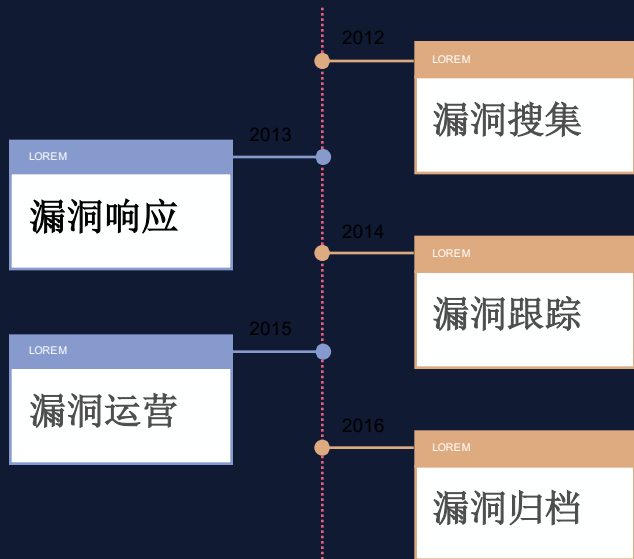


基于漏洞闭环的跟踪平台

FREETALK

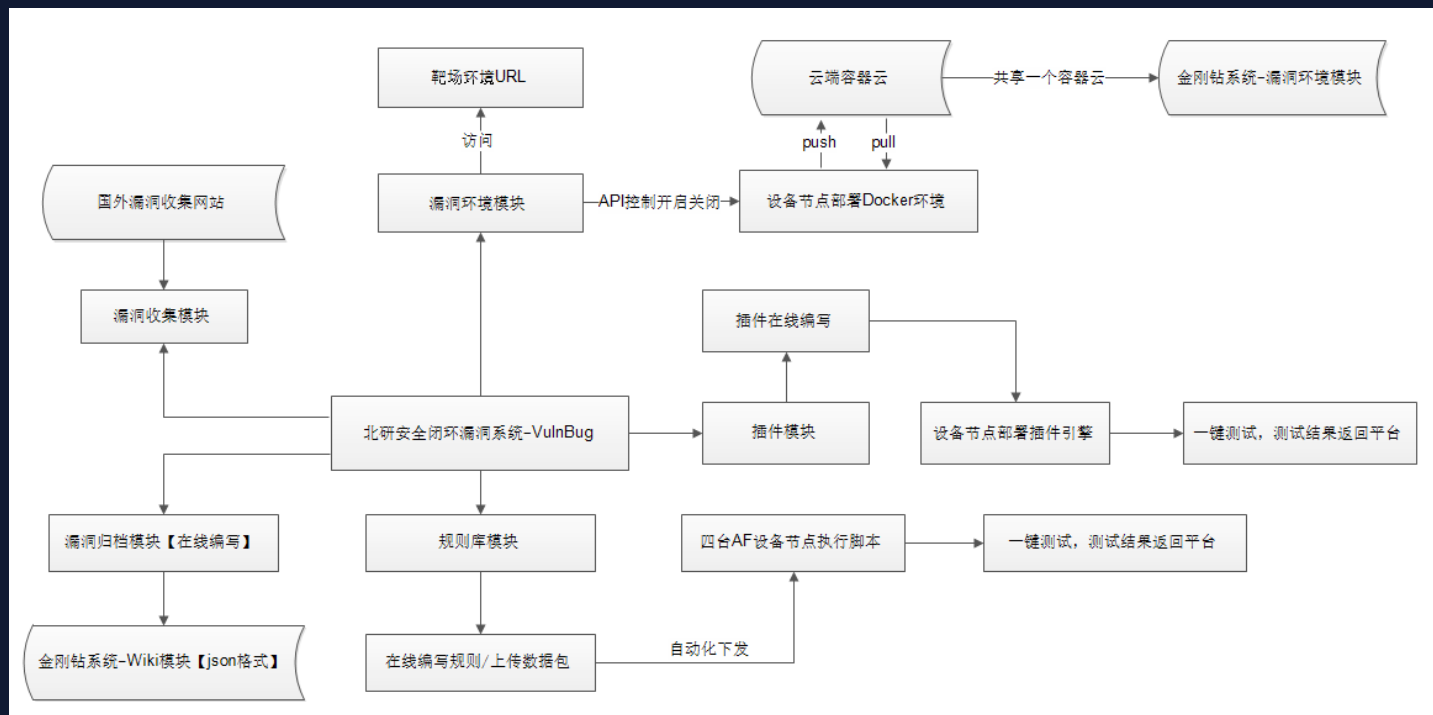
2018 北京站

流程图



基于漏洞闭环的跟踪平台基功能架构

FREETALK
2018 北京站



漏洞闭环的跟踪平台->漏洞库

FREETALK
2018 北京站



Q&A



FREETALK

2018 北京站



REEBUF

