# Day168　应急响应-ELK日志分析系统&Yara规则&样本识别&特征提取&规则编写

# 蓝队应急-小迪安全

## 异常特征

- 主机安全
  - CPU满负载
  - 服务器莫名重启
  - 其它
- 网站安全
  - 被植入暗链
  - 出现Webshell
  - 网页文件被篡改
  - 其它
- 流量安全
  - 网络阻塞
  - 网络异常
  - 其它
- 数据安全
  - 泄露
  - 篡改
- 文件安全
  - 丢失
  - 异常
- 设备告警
  - 防火墙
  - 杀毒软件
  - 感知平台
  - 检测系统
  - 其它

## 处置流程

1. 准备阶段
   - 获取事件信息
   - 准备设备工具
2. 保护阶段
   - 断网
   - 备份
   - 数据恢复
   - 物理隔离
3. 检测阶段
   - 技术分析
4. 取证阶段
   - 确定攻击事件
   - 确定攻击时间
   - 确定攻击过程
   - 确定攻击对象
5. 处置阶段
   - 提出安全问题
   - 提出解决方案
   - 业务恢复
6. 总结阶段
   - 完整事件报告编写

## 问题排查

- 系统
  - Windows
    - 远控后门
      - 进程
      - 网络
    - 勒索病毒
      - 表现
    - 挖矿程序
      - 进程
      - 网络
    - 爆破攻击
      - 系统日志
    - DDOS攻击
      - 网络流量
      - CPU爆满
  - Linux
- Web
  - 源码
  - 数据库
  - 中间件
- 其他

## 工具平台


## 1.知识点

- 1、ELK日志系统使用
- 2、Yara规则检测使用

---

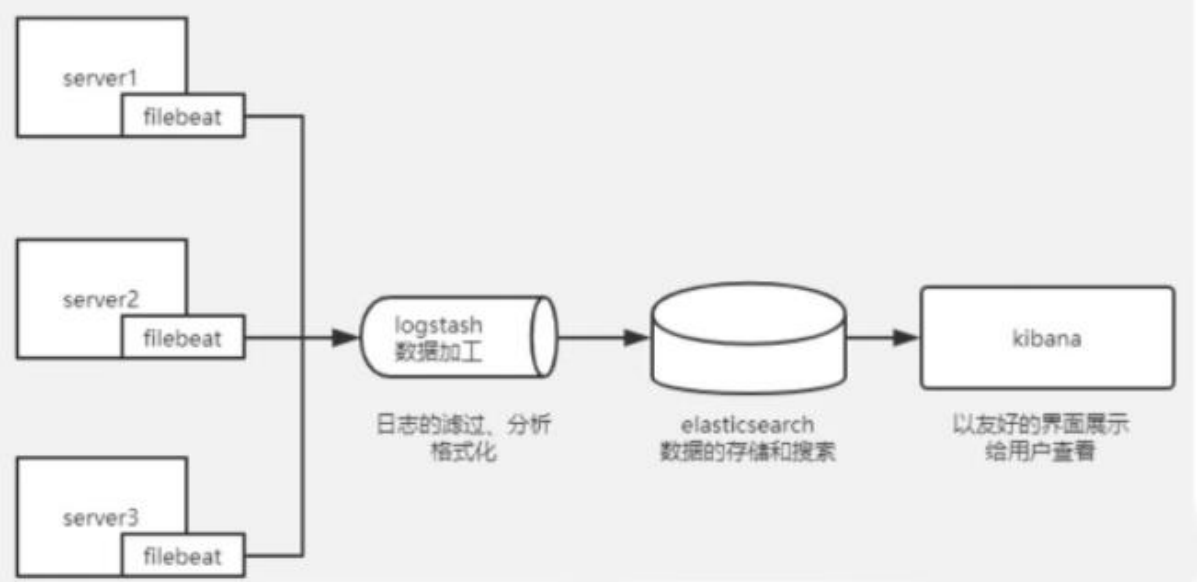
## 2.内容点

```
应急响应：
1、抗拒绝服务攻击防范应对指南
2、勒索软件防范应对指南
3、钓鱼邮件攻击防范应对指南
4、网页篡改与后门攻击防范应对指南
5、网络安全漏洞防范应对指南
6、大规模数据泄露防范应对指南
7、僵尸网络感染防范应对指南
8、APT攻击入侵防范应对指南
9、各种辅助类分析工具项目使用
```

```
朔源反制：
威胁情报，信息库追踪，设备反制，IDS&IPS等反制，工具漏洞反制，蜜罐钓鱼反制等
```

```
威胁情报相关平台：
Virustotal
深信服威胁情报中心
微步在线
venuseye
安恒威胁情报中心
360威胁情报中心
绿盟威胁情报中心
AlienVault
RedQueen安全智能服务平台
IBM X-Force Exchange
ThreatMiner
```

## 3.演示案例



## 3.1 ELK搭建使用-导入文件&监控日志&语法筛选

```
Elasticsearch:用于存储收集到的日志信息;
Logstash:用于收集日志转发给Elasticsearch;
Kibana:通过Web端的可视化界面来查看日志。
快速搭建:
https://mp.weixin.qq.com/s/rakuhGVSoUysso1VD5r0aA
三种模式:上传文件,特定分析,代理加入。
1、导入Web日志
2、导入系统日志
3、自动监控日志
```

## 3.2 Yara规则使用-规则检测&分析特征&自写规则

```
https://github.com/VirusTotal/yara
部分规则:https://github.com/Yara-Rules/rules
*应急工具包:https://www.cnsrc.org.cn/rules
yara 为yara使用程序
yarac 为编译yara规则工具

检测范围:
1、样本文件 2、内存数据 3、网络流量

特征提取:
1、多个样本同时对比筛选通用的数据
2、要根据样本的应用(分类,走的协议,文件头固定等)

1、利用已知规则库分析-挖矿样本&后门木马&勒索病毒
yara64.exe malware_index.yar -r
C:\Users\Administrator\Desktop\1

2、利用自写规则库分析-挖矿样本&Web内存马&工具指纹
```

```
-Yara规则内容支持字符串、正则表达式、十六进制进行匹配。
字符串：定义一个变量 $a = "字符串内容"
正则表达式：定义一个变量 $a = /正则表达式内容/
十六进制：定义一个变量 $a = {十六进制内容}
-Yara规则条件
and：与 or：或 not：非
all of them：所有条件匹配即告警
any of them：有一个条件匹配即告警
$a and $b and $c：abc同时匹配即告警
($a and $b) or $c：匹配a和b或c即告警
-Yara规则常用修饰符
nocase：不区分大小写
base64：base64字符串
xor：异或字符串
wide：宽字符

xmrig挖矿样本
提取：文件头，关键字，协议，域名等
rule xmrigdemo
{
    meta:
        tag="xmrigdemo"
        description = "test xmrigdemo"
        author="xiaodisec"

    strings:
        $hex = {4D 5A}
        $a = "stratum"
        $b = "xmrig"
        $c = "pool"

    condition:
```

```
        all of them
}

PHP内存马：
procdump.exe -accepteula -ma phpstudy_pro.exe php.dmp
yara64.exe demo1.yar PID
rule phpfindshell
{
    meta:
        tag="phpfindshell"
        description = "test phpfindshell"
        author="xiaodisec"

    strings:
        $a = "eval"
        $b = "exec"

    condition:
        all of them
}


Java内存马：
procdump.exe -accepteula -ma idea64.exe java.dmp
yara64.exe demo1.yar PID
rule jspfindshell
{
    meta:
        tag="jspfindshell"
        description = "test jspfindshell"
        author="xiaodisec"
```

```
81
82      strings:
83          $a = "org.apache.coyote"
84
85      condition:
86          all of them
87  }
```