日志与攻击行为分析

鹏元征信有限公司

PENGYUAN CREDIT SERVICE CO.,LTD.

熊海明　Xhm1n9@T00ls.net

鹏元征信有限公司安全专家，现负责安全测试与运营工作。擅长渗透测试、代码审计、入侵溯源、日志分析，对信息安全建设、安全运营有丰富经验。

日志分析目的

日志采集注意事项

安全检测场景

攻击行为分析

日志分析目的

通过对企业内部的各项数据进行汇总关联分析，感知可能正在发生的攻击，从而规避存在的安全风险。

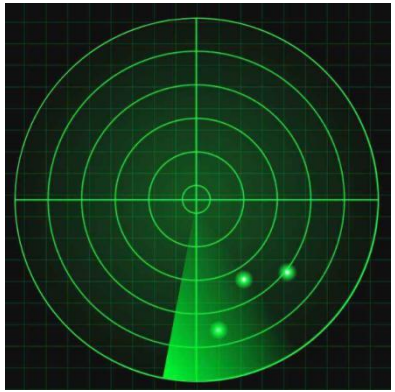
安全趋势

攻击检测

应急响应

入侵溯源

.....



安全可见能力

日志采集注意事项

前期数据的采集，要从分析的角度去思考，数据分析时需要哪些维度数据。引出下面5个问题。

1 采集哪些数据

- 设备日志
- 应用日志
- 系统认证日志
- 业务日志

.....

2 数据在哪

- /var/log/
- c:\windows\system32\winevt\logs\
- api接口
- 安全设备

.....

日志采集注意事项

3 如何收集

- rsyslog
- ftp/scp/rsync

.....

4 是否遗漏

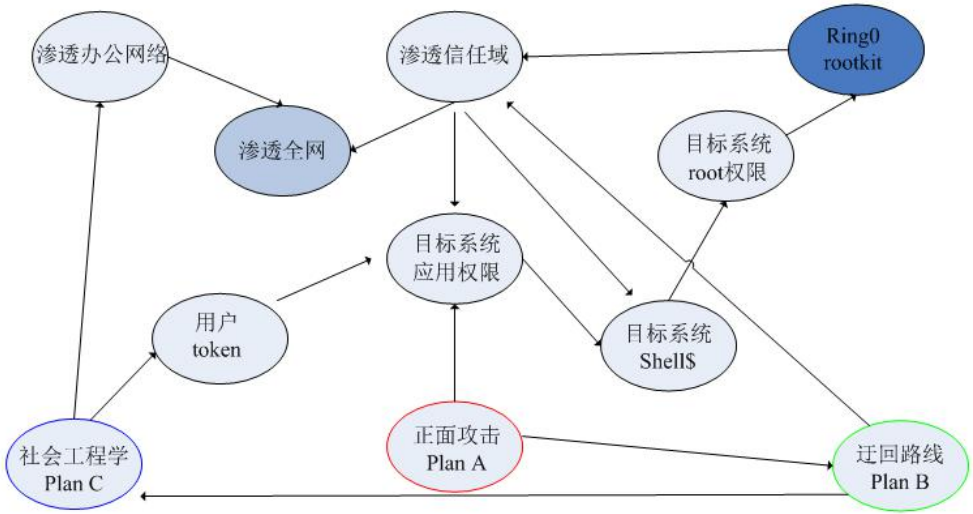
- 收集是否完整、重复

5 数据质量如何

- 确认内容是否符合需求

安全检测场景

黑客攻击路径



安全检测场景

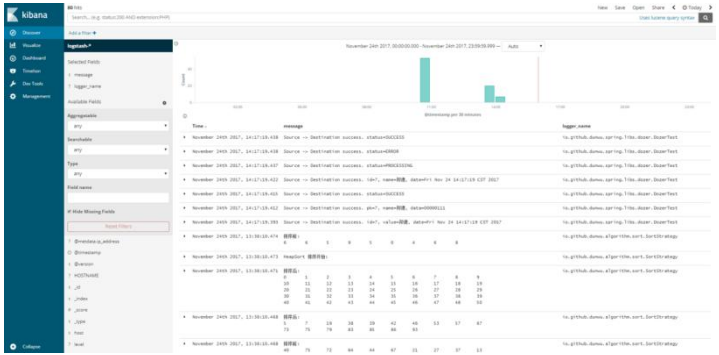
安全防守 、检测场景

场景分析时应充分考虑自身业务情况、攻防经验、防御体系方法论和反APT的杀伤链模型，借鉴里面的防御思路尽量覆盖到安全各个维度及场景。

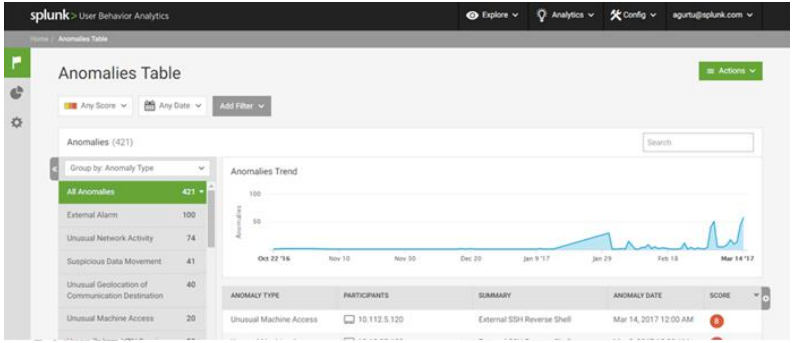
攻击行为分析

分析平台

ELK



Splunk



日志

一条合格的日志应该能够说明什么人、在什么时间、什么地方做了什么事及结果怎样。

攻击行为分析

一个正常的web请求是这样的

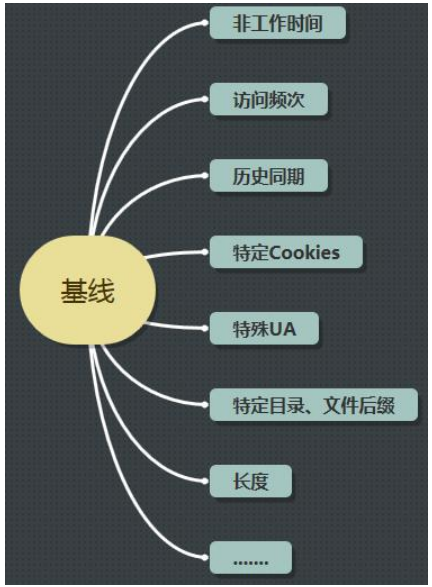
```
123.57.155.110 - - [02/Oct/2016:21:50:39 +0800] "POST /auth-login HTTP/1.0" 200
144 "/auth-login.html" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/49.0.2623.22 Safari/537.36 SE 2.X MetaSr 1.0" "-"
```

而异常的web请求

```
101.200.76.70 - - [02/Oct/2016:21:01:58 +0800] "GET /;print(md5(acunetix_wvs_secur
(Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0
101.200.76.70 - - [02/Oct/2016:21:02:08 +0800] "GET / HTTP/1.0" 200 4370 "-" "Mozi
like Gecko) Chrome/41.0.2228.0 Safari/537.21" ";print(md5(acunetix_wvs_security_te
101.200.76.70 - - [02/Oct/2016:21:02:08 +0800] "GET / HTTP/1.0" 200 4370 "-" "Mozi
like Gecko) Chrome/41.0.2228.0 Safari/537.21" "';print(md5(acunetix_wvs_security_t
101.200.76.70 - - [02/Oct/2016:21:02:20 +0800] "GET /css/ HTTP/1.0" 403 162 "-" "'
101.200.76.70 - - [02/Oct/2016:21:02:49 +0800] "GET /find.html HTTP/1.0" 200 3930
(Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0
101.200.76.70 - - [02/Oct/2016:21:02:49 +0800] "GET /find.html HTTP/1.0" 200 3930
"Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome
101.200.76.70 - - [02/Oct/2016:21:02:49 +0800] "GET /find.html HTTP/1.0" 200 3930
101.200.76.70 - - [02/Oct/2016:21:02:59 +0800] "GET /sys/ HTTP/1.0" 200 151 "-" "M
(KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21" "${@print(md5(acunetix_wvs_s
```

攻击行为分析

正常中发现异常!



策略:

应用层攻击检测
- 注入
- 跨站
- 代码执行
- .....

网络层攻击检测
- DDOS攻击
- 端口扫描
- 木马病毒
- .....

主机层攻击检测
- 暴力破解
- 提权
- .....

业务层攻击检测
- 刷号、撞库
- .....

安全域访问控制
- 非预期的跨域访问
- .....

攻击行为分析

在异常中确认攻击！

攻击行为分析——案例

ssh暴力破解攻击

来自192.168.2.121的IP正在尝试暴力破解本机adm账号

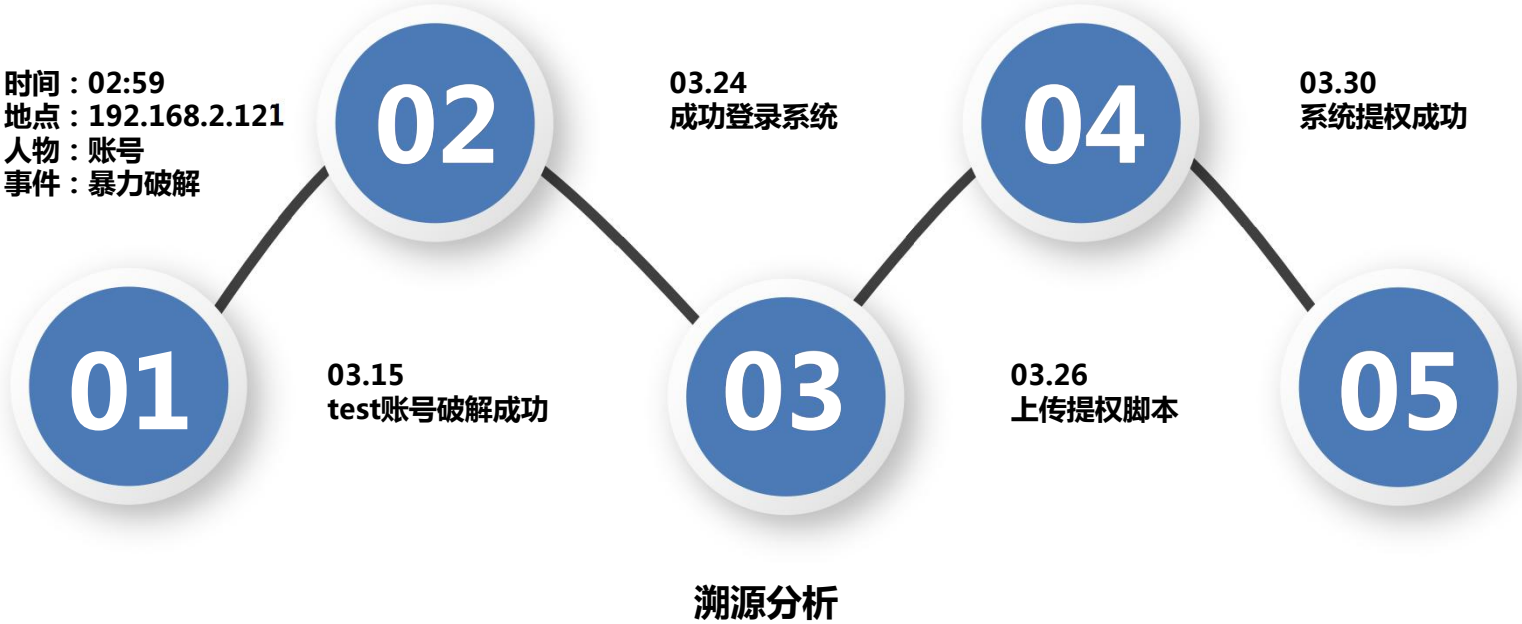
攻击行为分析——案例


```
Jun 28 03:15:16 webserver sshd[6195]: Accepted password for test from 192.168.2.121 port 3922 ssh2
Jun 28 03:15:32 webserver test_shell_cmd: [/home/test]    2  [2016-06-28 03:15:32] [192.168.2.121] cd /tmp
Jun 28 03:15:32 webserver test_shell_cmd: [/tmp]    3  [2016-06-28 03:15:32] [192.168.2.121] ls
Jun 28 03:24:27 webserver sshd[6271]: Accepted password for test from 192.168.2.121 port 4174 ssh2
Jun 28 03:24:27 webserver sshd[6275]: subsystem request for sftp        1、打开sftp准备上传
Jun 28 03:24:28 webserver sftp-server[6276]: session opened for local user test from [192.168.2.121]
Jun 28 03:24:28 webserver sftp-server[6276]: opendir "/home/test"
Jun 28 03:24:28 webserver sftp-server[6276]: closedir "/home/test"
Jun 28 03:25:33 webserver sftp-server[6276]: opendir "/tmp"
Jun 28 03:25:33 webserver sftp-server[6276]: closedir "/tmp"        2、选择要上传的目录
Jun 28 03:25:36 webserver sshd[6275]: subsystem request for sftp
Jun 28 03:25:36 webserver sftp-server[6299]: session opened for local user test from [192.168.2.121]
Jun 28 03:25:36 webserver sftp-server[6299]: open "/tmp/semtex.c" flags WRITE,CREATE,TRUNCATE mode 0666
Jun 28 03:25:36 webserver sftp-server[6299]: close "/tmp/semtex.c" bytes read 0 written 2437
Jun 28 03:25:36 webserver sftp-server[6276]: opendir "/tmp"
Jun 28 03:25:36 webserver sftp-server[6276]: closedir "/tmp"        3、上传文件到/tmp中
Jun 28 03:25:39 webserver sftp-server[6276]: session closed for local user test from [192.168.2.121]
Jun 28 03:25:39 webserver sftp-server[6299]: session closed for local user test from [192.168.2.121]
```

攻击行为分析——案例

提权成功

攻击行为分析——案例


时间：02:59
地点：192.168.2.121
人物：账号
事件：暴力破解
02
03.24
成功登录系统
04
03.30
系统提权成功
01
03.15
test账号破解成功
03
03.26
上传提权脚本
05
溯源分析

攻击行为分析——案例

Xshell后门检测

```
sa*******mkpmnmixivemirmwlvajdkctcjp*******aqplm.tfvduaplkil*******bv.nylalobghyhirgh.com
sajsajaj*******jjmjmmhjdkgmmwlvajdkjtcmiycxj*******fqgpcs.jsnwap.nylalobghyhirgh.com
sajajlyoogrmkpmnmi*******lvajdkctcjpymyjlfmoqjyaq*******uap.lkil*******grcpbv.nylalobghyhirgh.com
sajajlyoogr*******rmwlvajdkctcjpy********v.duaplkilcogrcpbv.nylalobghyhirgh.com
sajajlyoogrm*******fpjwmwlvaj*******ybloooljwaqpp.gsoskwdkl*******siqduix.nylalobghyhirgh.com
```

数据传输疑似通过DNS外带

业务能力输出

天下信用

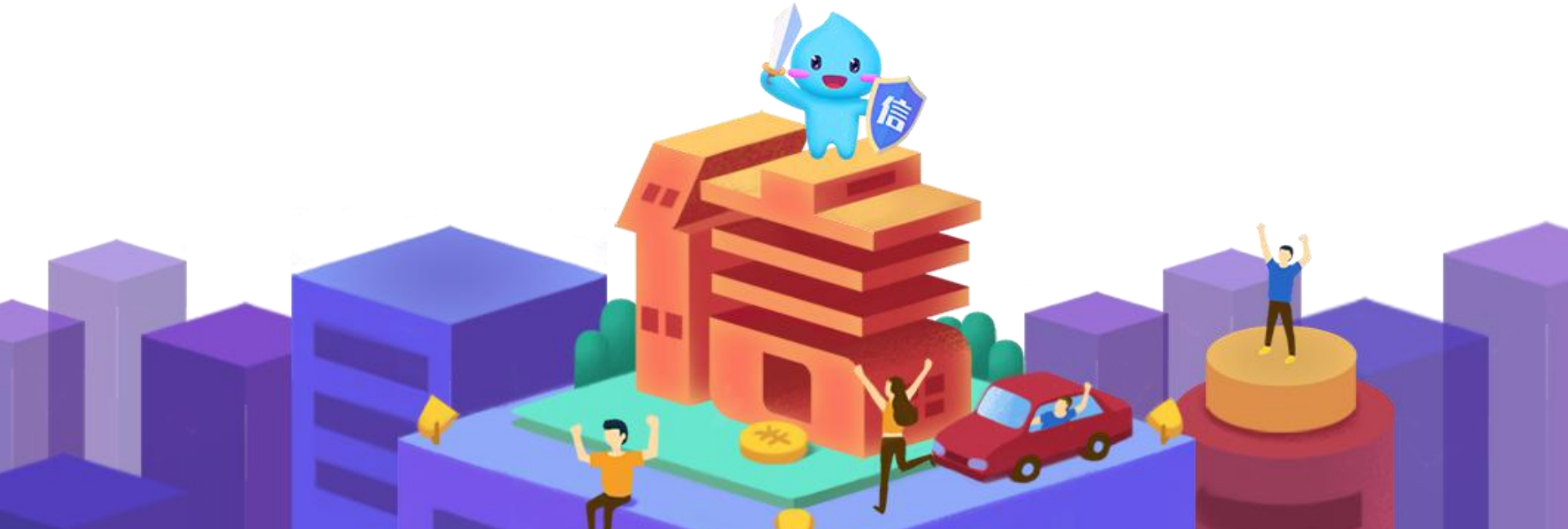
天下信用是权威的互联网信息查询服务平台。基于鹏元征信有限公司十余年来的大数据信息服务经验，专业提供个人报告查询、企业报告查询、诚信生态开放产品和服务。

4年	600万	3万笔/日

天下信用

2018年7月25日

天下信用失信惩戒联盟



天下信用失信惩戒联盟

问：什么是失信惩戒联盟？

失信惩戒联盟是由天下信用发起，旨在建立一个反欺诈联盟，为联盟成员提供失信回款渠道服务，促进联盟成员业务健康有序发展。

问：加入联盟有什么用？

- 联盟成员联合信用惩戒
- 追缴欠款，用户查询报告时风险警示，引导还款
- 依托鹏元生态体系，联合惩戒

天下信用失信惩戒联盟

联盟的特点

其他联盟情况

- 上传数据复杂
- 需定时更新
- 接口开发复杂
- 惩戒能力不强
- ……

天下信用失信惩戒联盟特点

- 上传数据方便
- 提交数据字段少
- 无需开发接口
- 还清后开具结清证明
- 全方位联合惩戒，效果明显
- ……

天下信用失信惩戒联盟

联盟服务流程图

天下信用失信惩戒联盟

失信惩戒联盟产品已于7月25日推出

现已有5家机构加入联盟，陆续接洽中

预计9月推出API产品

合作热线：400-612-1133

合作邮箱：BD@pycredit.cn

天下信用失信惩戒联盟

鹏元生态信用惩戒
B端数据查询

C端查询报告
信用教育

联盟成员上传数
据

谢谢

鹏元征信有限公司

PENGYUAN CREDIT SERVICE CO.,LTD.