

流量安全分析平台建设

何艺

About me

何艺

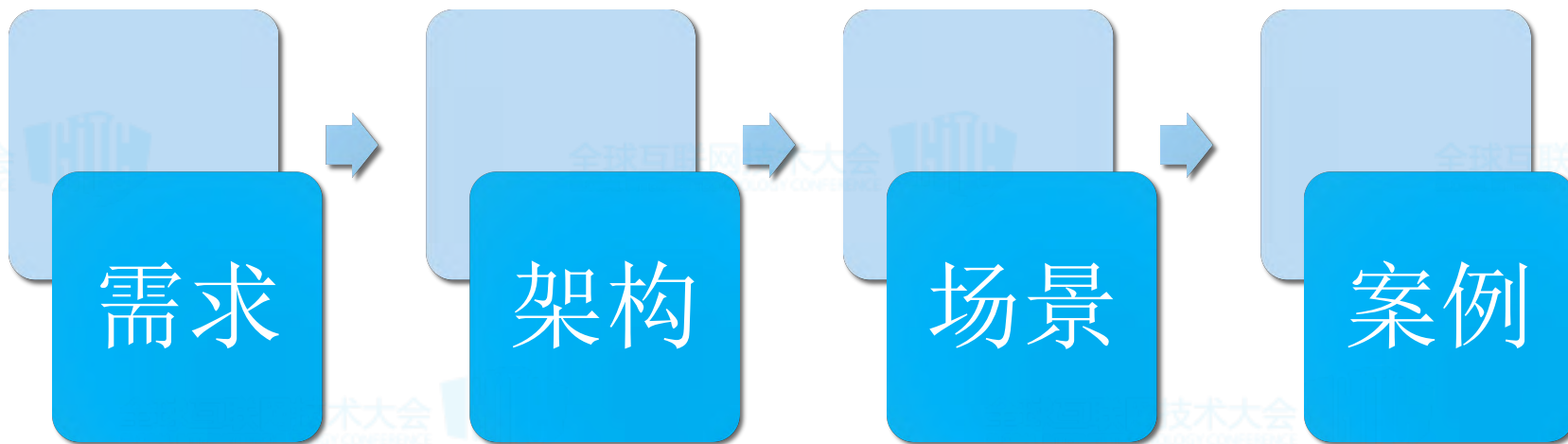
工作经历：

- 2004 – 2011 CNCERT网络安全组 组长
- 2011 – now 完美世界信息安全部 总监

关注领域：

企业安全治理、安全平台架构设计和实施、安全分析、追踪溯源

议题



你是哪一种？

世界上有三种人

被黑过

不知道被黑过

不承认被黑过

攻防如何博弈？

防护

检测



检测、感知的目的

有什么？

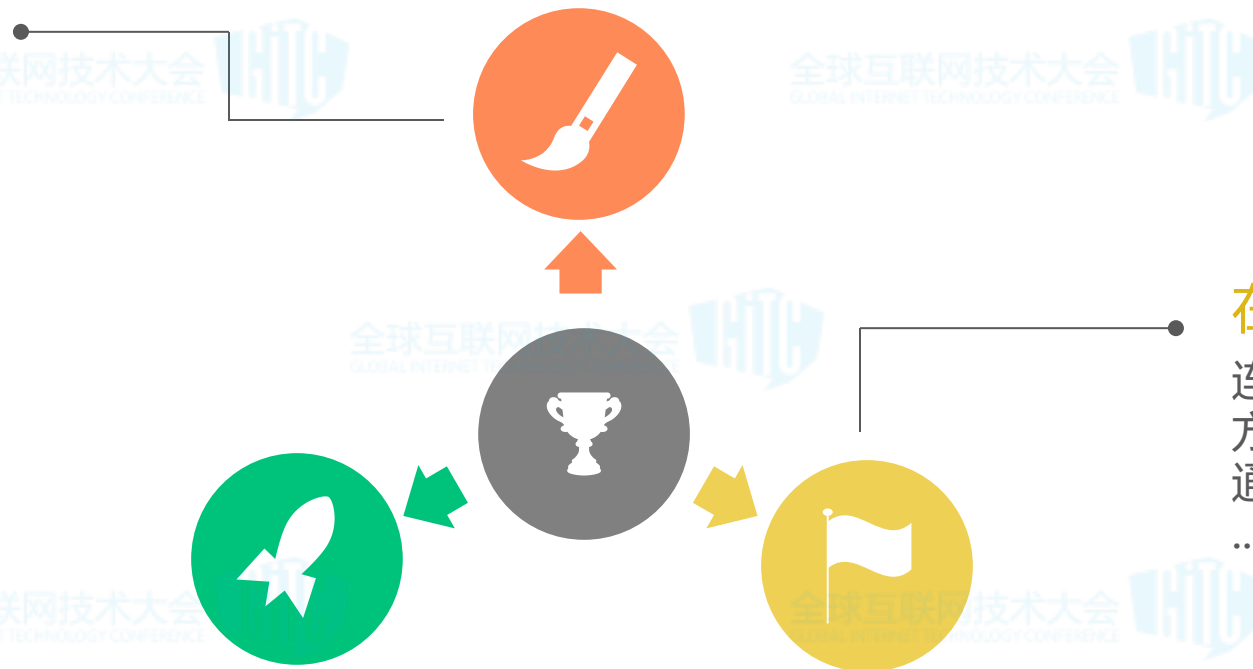
孤岛系统
违规系统
.....

有什么问题？

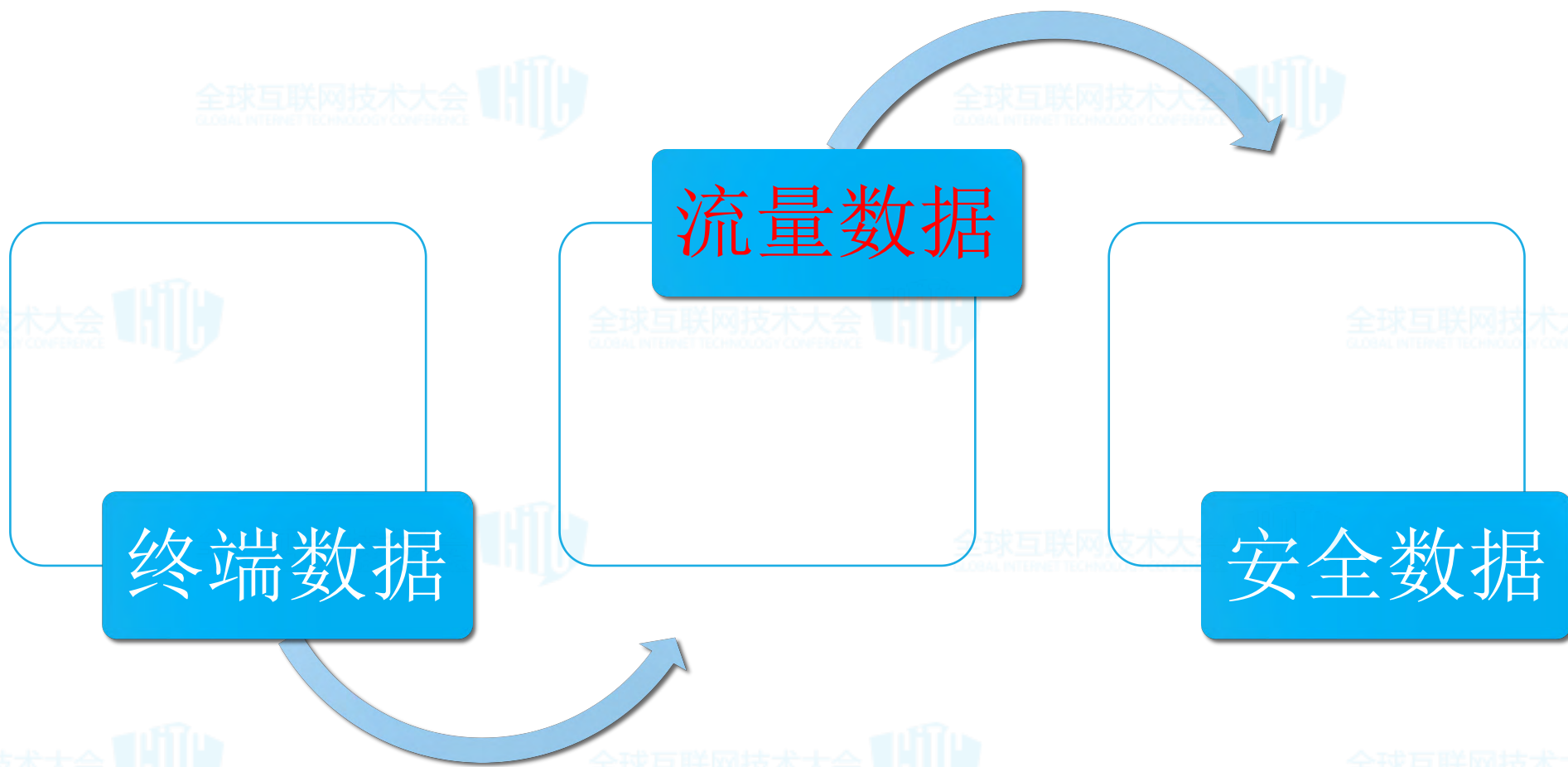
风险、漏洞
安全事件
异常访问
.....

在干嘛？

连接对象
方式方法
通信内容
.....

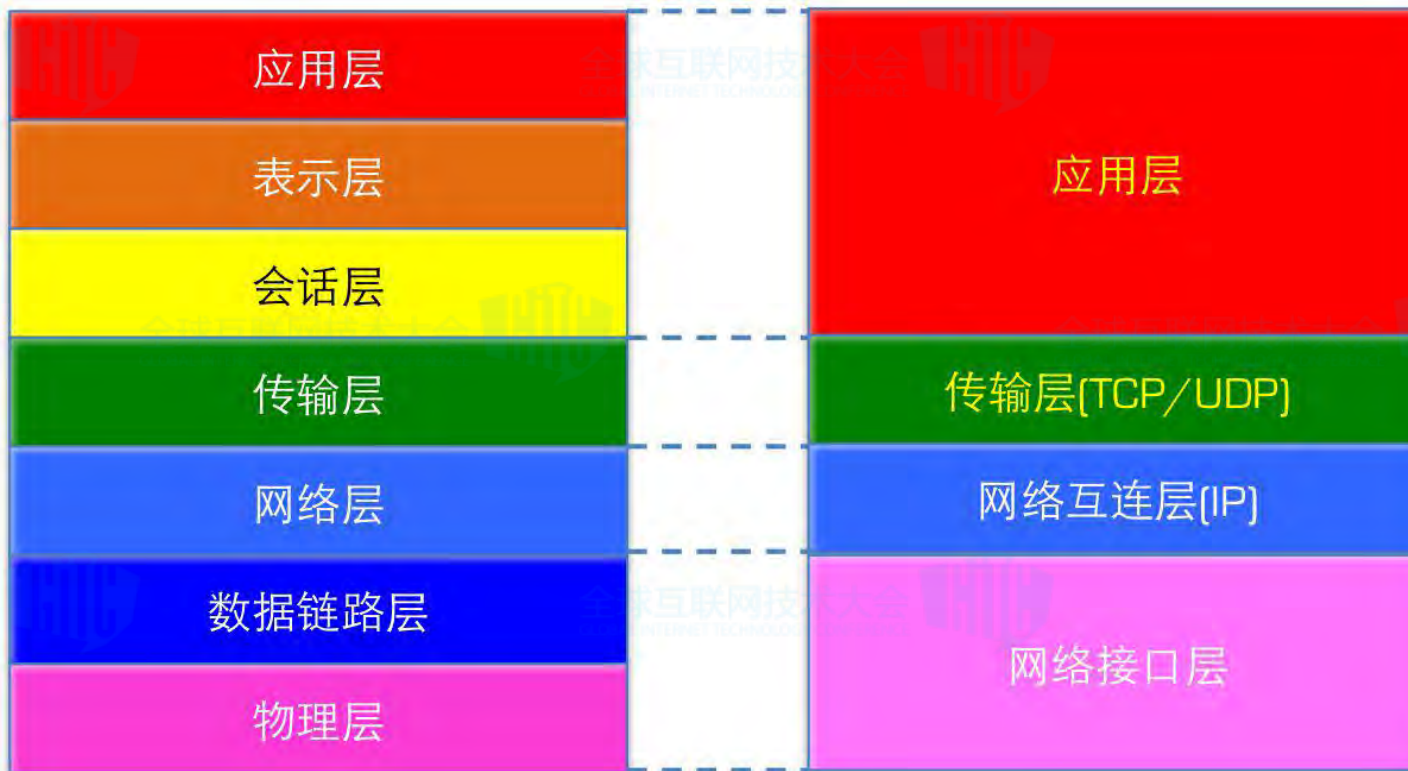


数据来源

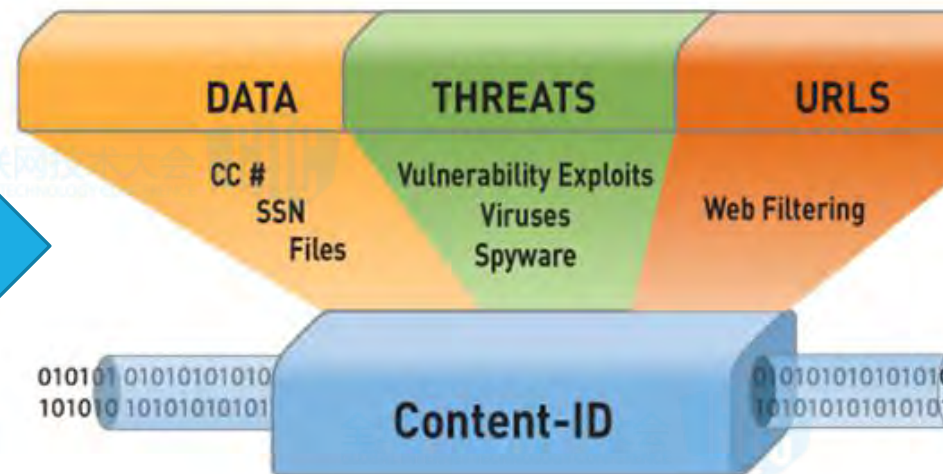
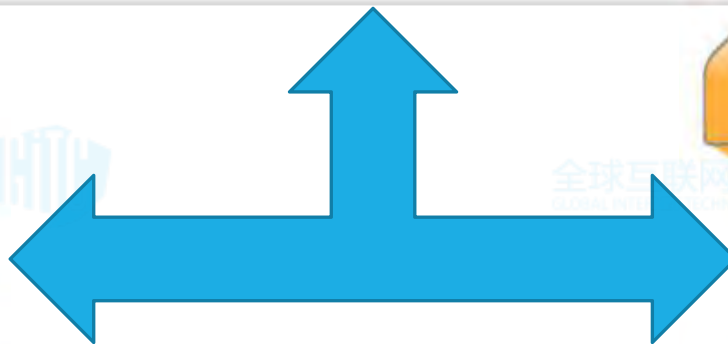
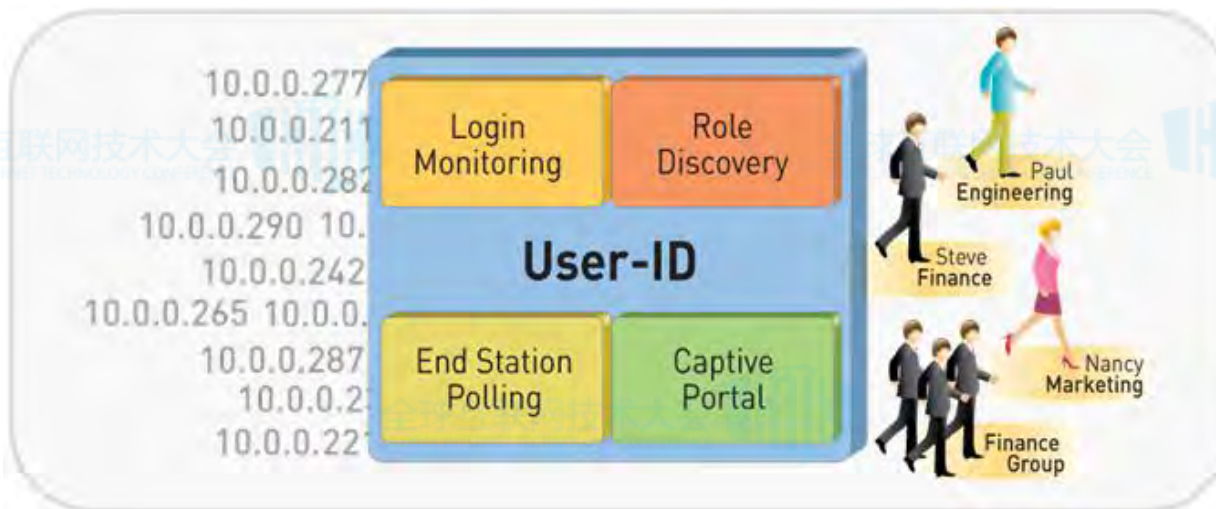


传统流量分析缺陷

- 基于传输层
- 知其然不知其所以然
- 适用于趋势分析



应用层检测的最佳实践



安全需求

全球互联网技术大会
GLOBAL INTERNET TECHNOLOGY CONFERENCE

全球互联网技术大会
GLOBAL INTERNET TECHNOLOGY CONFERENCE

全球互联网技术大会
GLOBAL INTERNET TECHNOLOGY CONFERENCE

资产发现

自动化资产发现、端口、版本、关系

协议解析

5元组信息、会话时长、包数量、大小等



威胁识别

漏洞利用、扫描、C&C、异常访问、威胁情报

内容解析

服务、应用、版本、通信内容解析

全流量存储

原始流量保存，索引

全球互联网技术大会
GLOBAL INTERNET TECHNOLOGY CONFERENCE

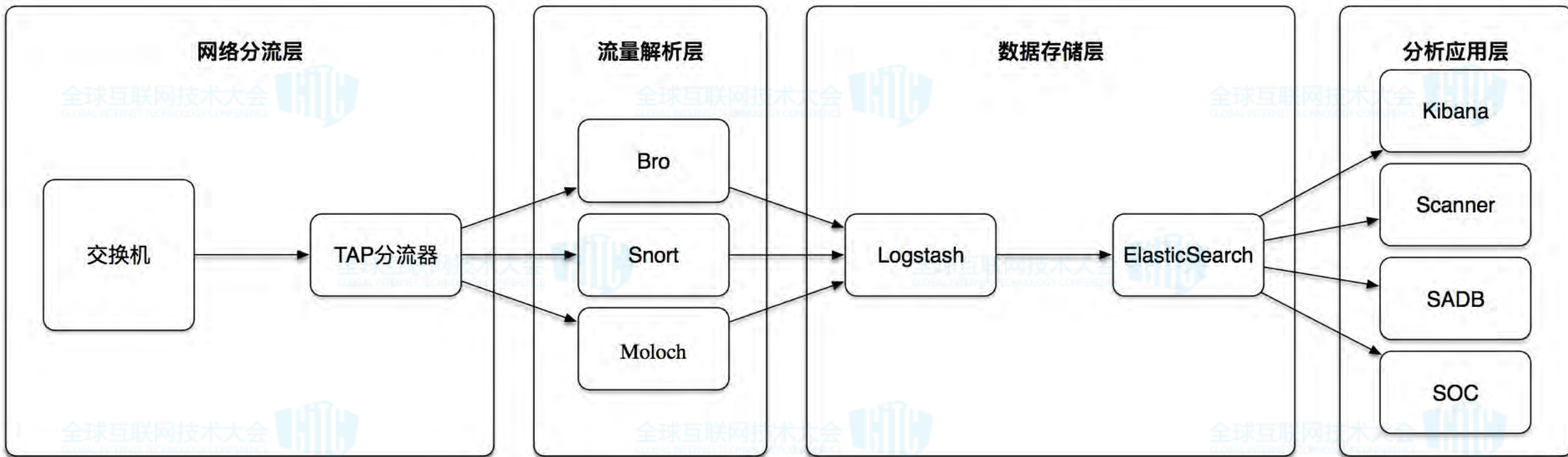
全球互联网技术大会
GLOBAL INTERNET TECHNOLOGY CONFERENCE

全球互联网技术大会
GLOBAL INTERNET TECHNOLOGY CONFERENCE

系统架构

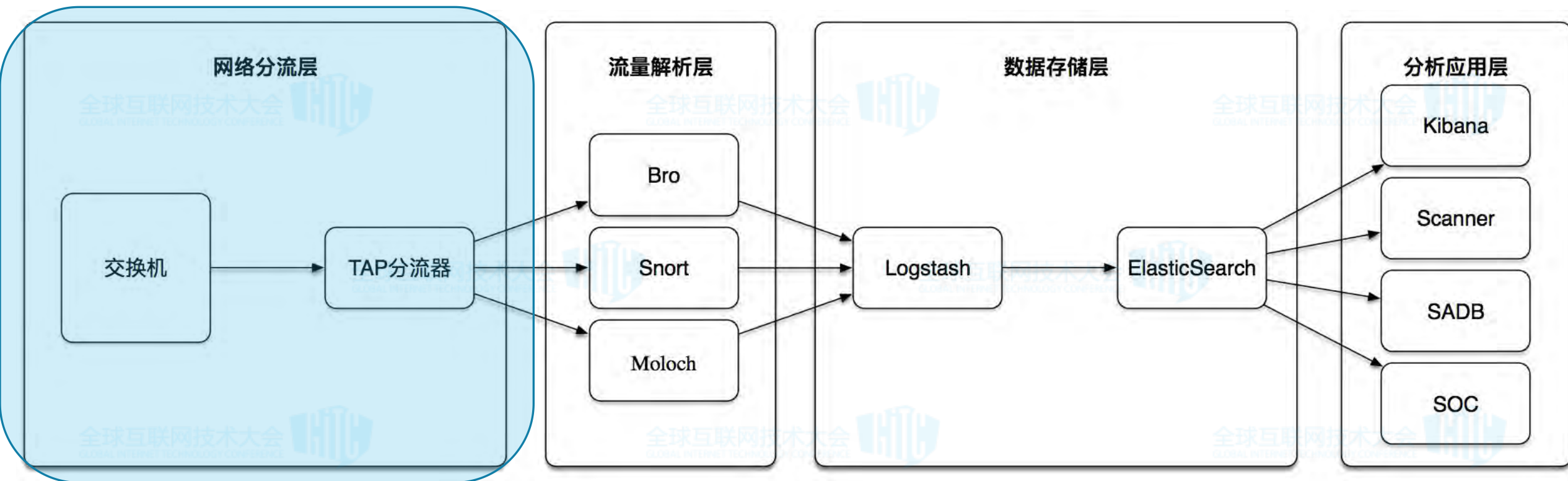
1. 多场景适应

2. 易扩展



网络分流层

1. 数据一路多出
2. 数据一路多分

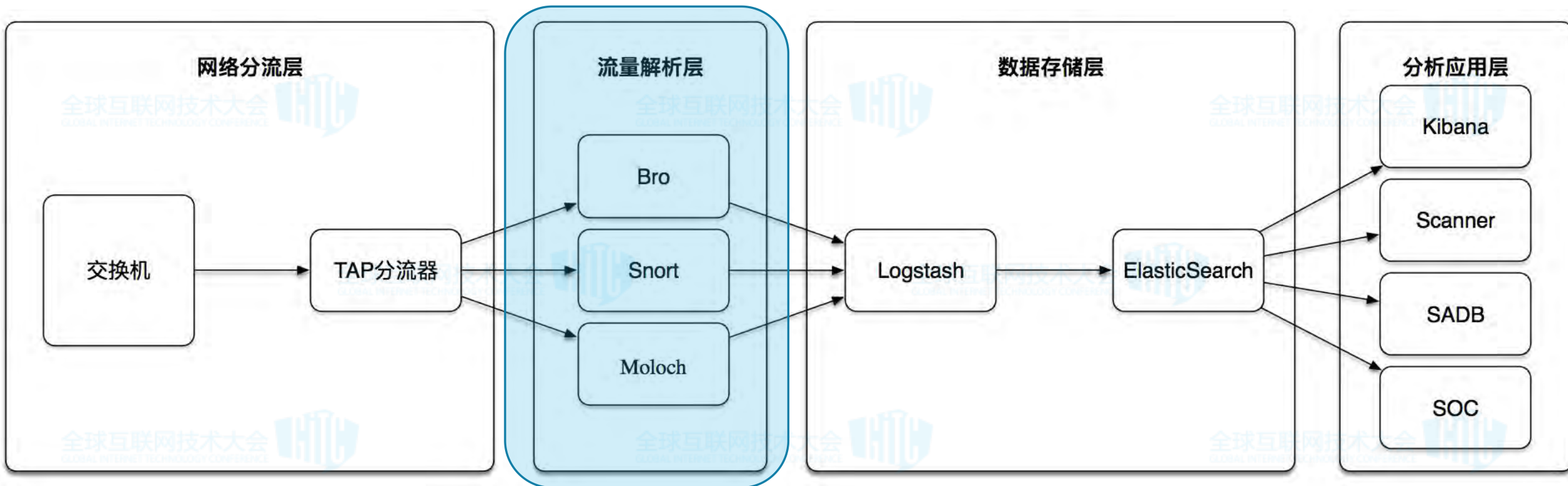


流量解析层

1. Bro : DPI内容识别

2. Snort : NIDS特征匹配告警

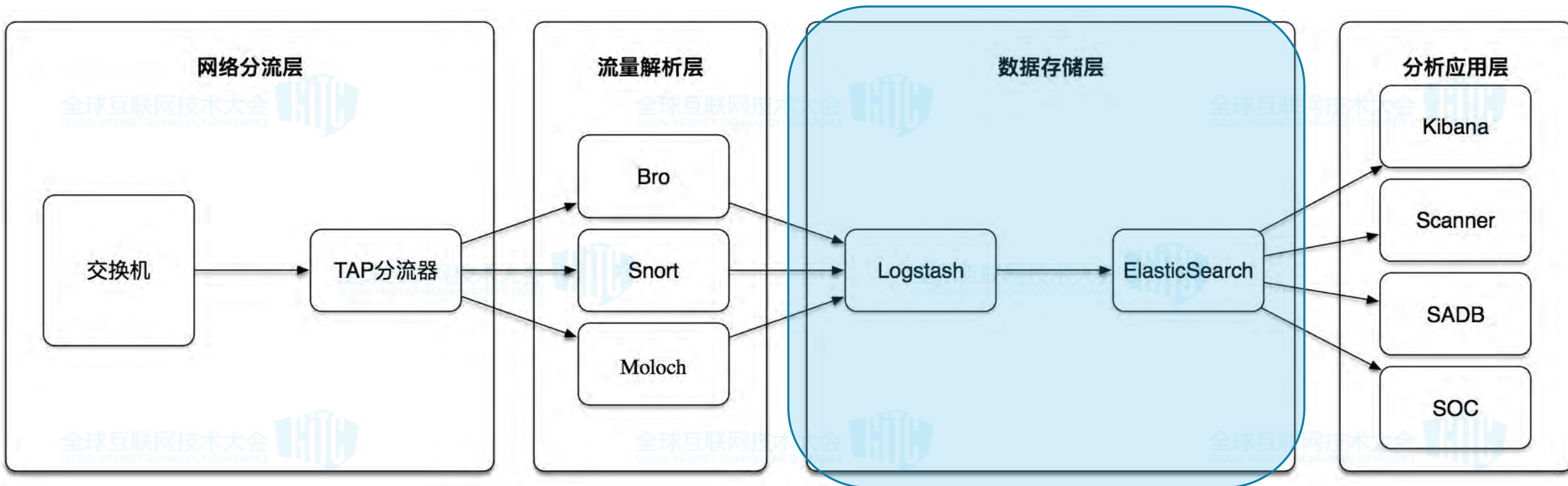
3. Moloch: 全原始流量抓取, 分析固证
about suricate



数据存储层

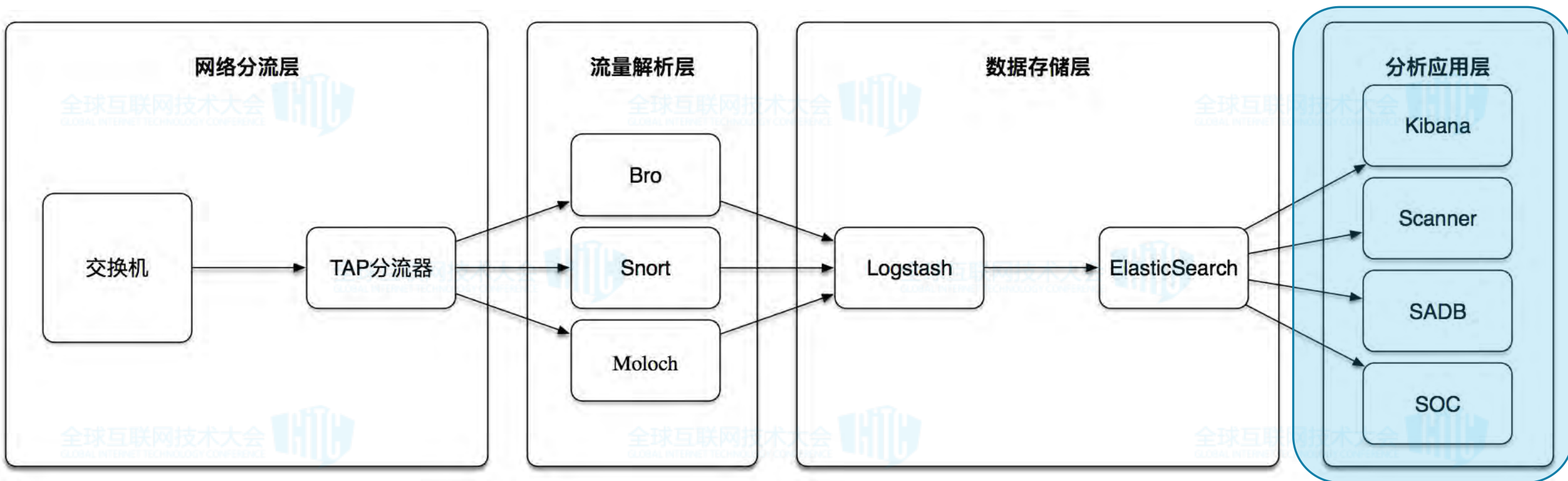
1. 数据统一格式化处理
2. 海量数据存储

3. 全文索引
4. 易于使用



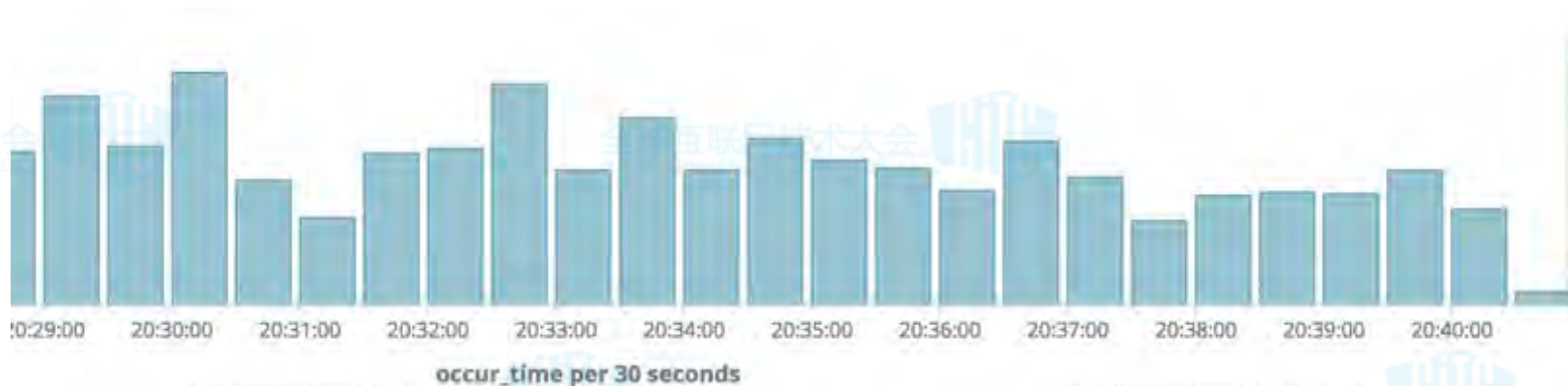
分析应用层

让数据产生价值的地方！



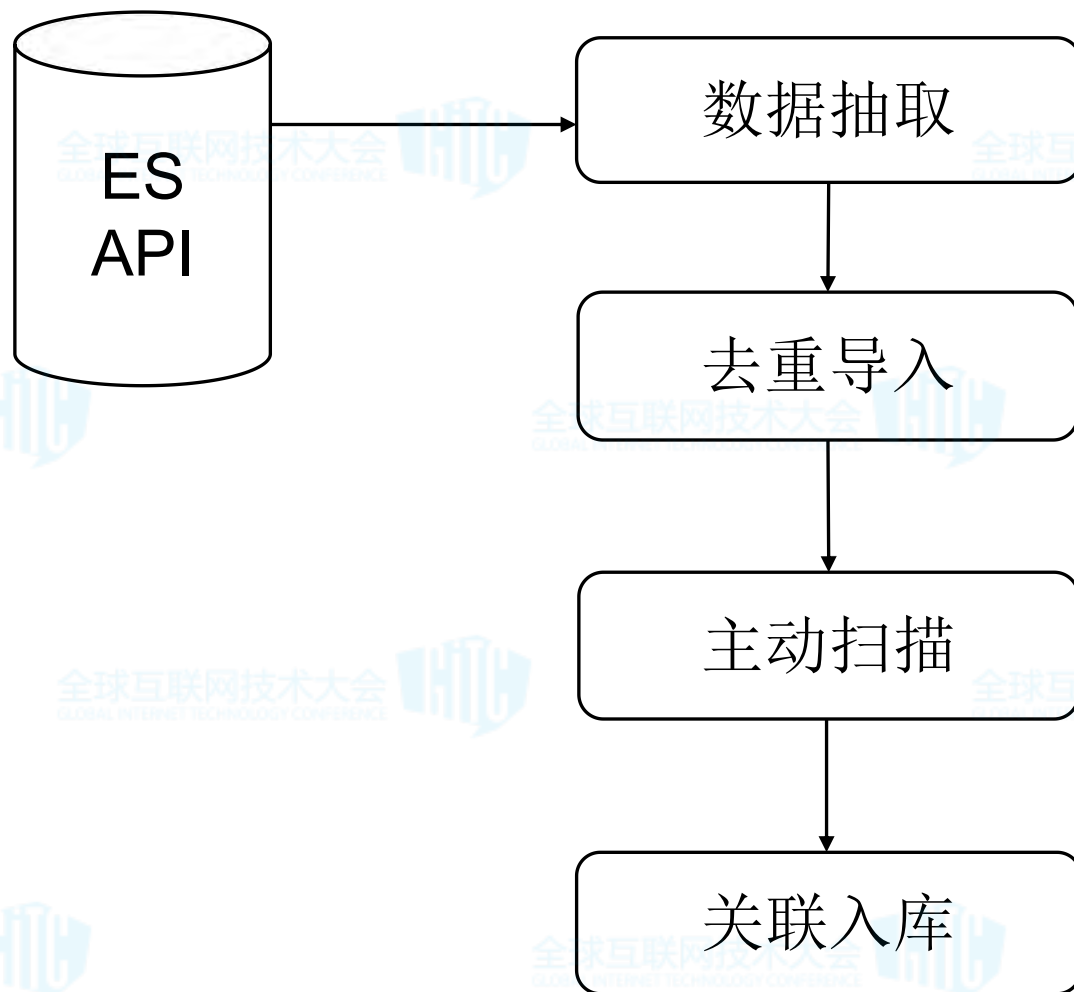
资产自动发现

- 主机识别：bro-knowhosts
- 服务识别：bro-conn、
- 应用识别：bro-software、snort-openid



| host | software_type | port | name | unparsed_version |
|-----------------|-----------------|------|---------|------------------------|
| [REDACTED] 8 | HTTP::SERVER | 80 | Apache | Apache/2.4.10 (Debian) |
| [REDACTED] | HTTP::SERVER | 80 | QZHTTP | QZHTTP-2.38.20 |
| [REDACTED] | HTTP::SERVER | 80 | QZHTTP | QZHTTP-2.38.20 |
| [REDACTED] 6 | HTTP::SERVER | 80 | Apache | Apache/2.4.10 (Debian) |
| [REDACTED] | HTTP::APPSERVER | 80 | Servlet | Servlet/2.4 JSP/2.0 |

资产自动发现



案例 - 资产自动扫描

PWRD Scanner System

- Home
- 资产发现
- 资产管理
- 端口服务
- 域名资产
- URL资产
- 弱点检测
- 引擎管理
- 系统设置

Home / 资产管理 / 端口资产

IP: 端口: 服务: 支持模糊查询 Banner: 支持模糊查询

导入域名列表:

| IP | 端口 | 协议 | 服务 | banner | 发现时间 | 操作 |
|------------|----|-----|------|--|---------------------|-------------------------------------|
| [REDACTED] | 80 | tcp | http | | 2016-06-29 09:03:03 | <input type="button" value="删除记录"/> |
| [REDACTED] | 80 | tcp | http | product: Mbedthis-Appweb version: 2.4.2 extrainfo: Dell iDRAC6 http config devicetype: remote management | 2016-06-29 09:02:40 | <input type="button" value="删除记录"/> |
| [REDACTED] | 80 | tcp | http | | 2016-06-29 09:02:36 | <input type="button" value="删除记录"/> |
| [REDACTED] | 80 | tcp | http | product: nginx | 2016-06-29 09:01:46 | <input type="button" value="删除记录"/> |
| [REDACTED] | 80 | tcp | http | product: Mbedthis-Appweb version: 2.4.2 extrainfo: Dell iDRAC6 http config devicetype: remote management | 2016-06-29 09:01:27 | <input type="button" value="删除记录"/> |

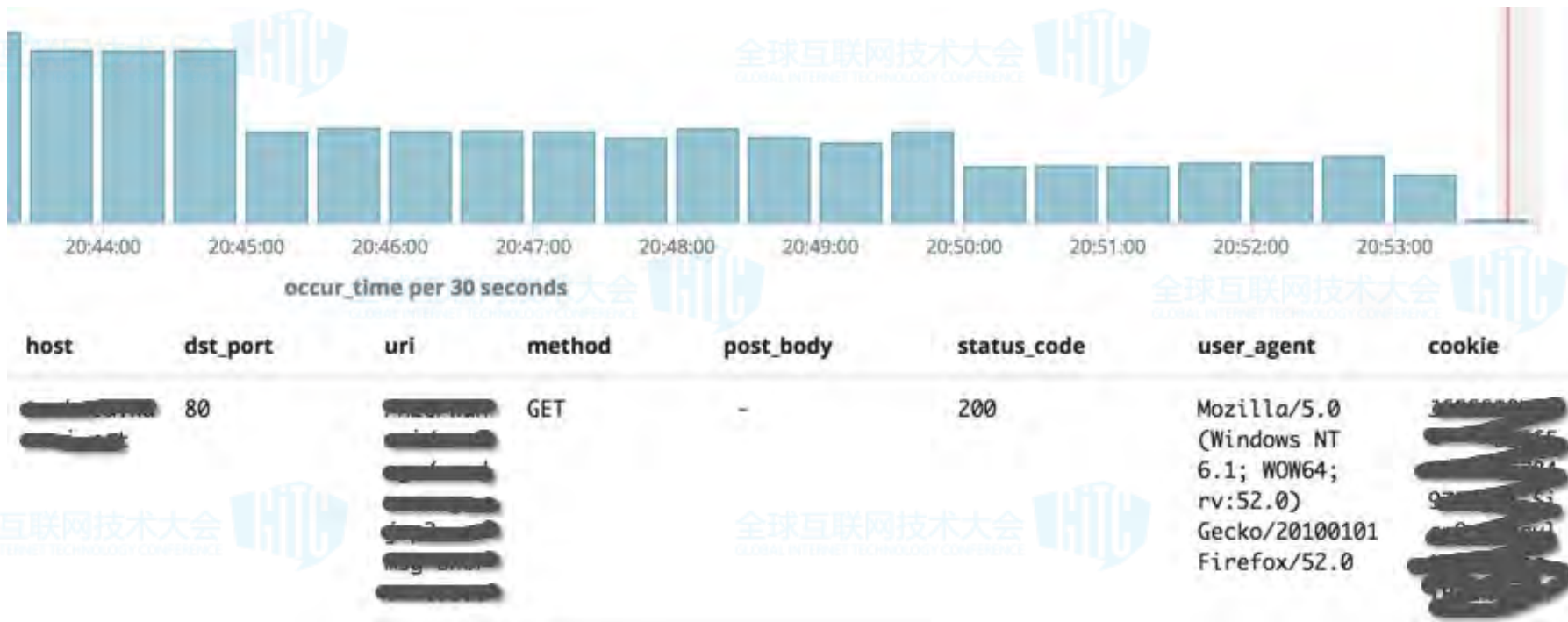
被动式web漏洞扫描

用途：

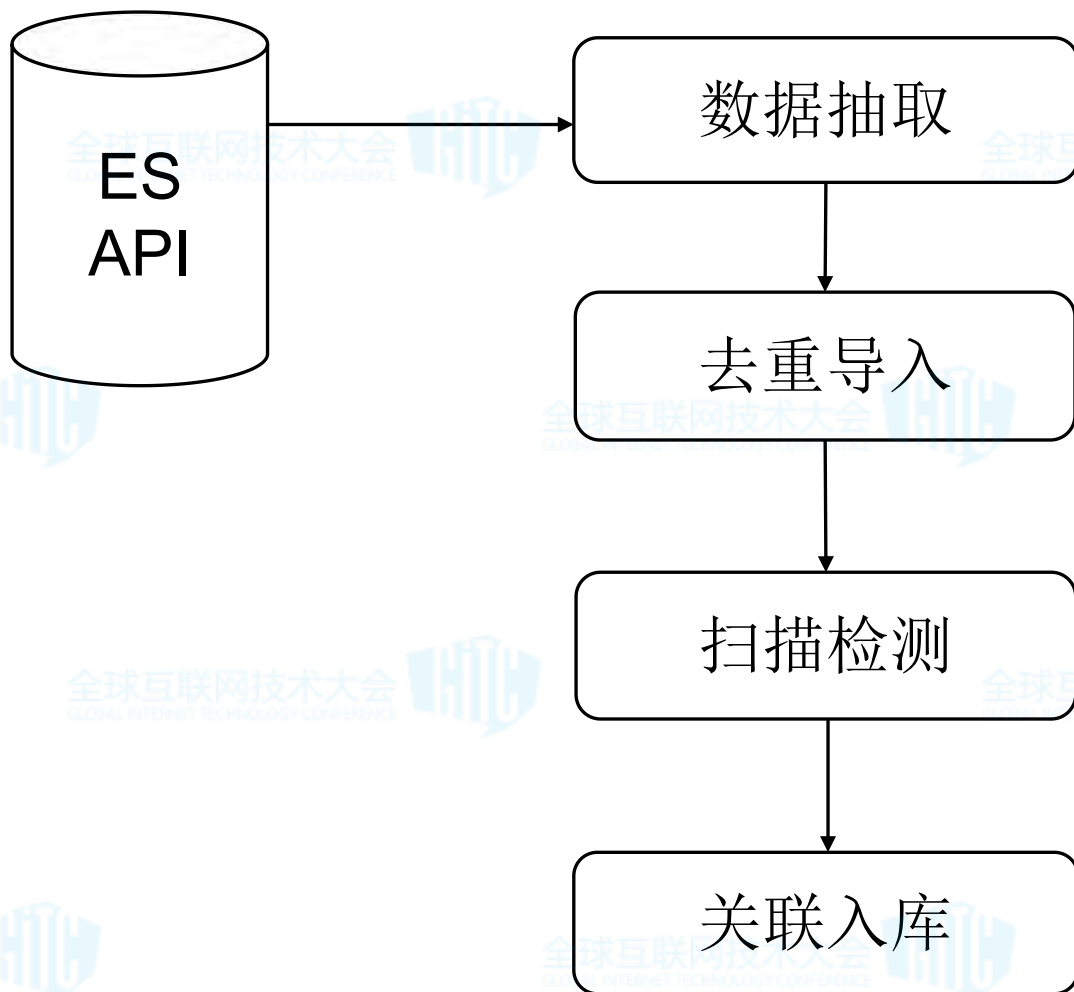
- 发现未知漏洞
- 发现未知攻击
- 免爬虫扫描

数据：

- bro-http



被动式漏洞扫描



案例-被动式web漏洞扫描



PWRD Scanner System

- Home
- 资产发现
- 资产管理
 - 端口服务
 - 域名资产
 - URL资产
- 弱点检测
- 引擎管理

Home / 资产管理 / URL资产

域名: 请求方法: URL关键字: POST_BODY关键字:

导入:

| 域名 | 请求URL | 请求方法 | 发现时间 | 操作 |
|------------|--|------|---------------------|----------------------|
| ██████████ | http://██████████?type=1&pageNum=1&pageSize=10 | POST | 2017-10-27 12:24:51 | 删除记录 |
| ██████████ | http://██████████/list.do?categoryId=1 | POST | 2017-10-27 12:24:51 | 删除记录 |
| ██████████ | http://██████████?type=1&pageNum=1&pageSize=10 | POST | 2017-10-27 12:24:51 | 删除记录 |



威胁情报分析

域名检测

1

bro-dns
bro-http

URI检测

2

bro-http
bro-smtp

IP检测

3

bro-conn

HASH检测

4

bro-files

案例-威胁情报分析



@timestamp per hour

| hit_api | type | trace_src_ip | detection | detail.intel_types | detail.families |
|------------------|----------------|--------------|------------|--------------------|-----------------|
| virusbook domain | threats_domain | [REDACTED] | [REDACTED] | C2 | |
| virusbook domain | threats_domain | [REDACTED] | [REDACTED] | Malware | |
| virusbook domain | threats_domain | [REDACTED] | [REDACTED] | Suspicious, C2 | Ramnit |
| virusbook domain | threats_domain | [REDACTED] | [REDACTED] | Suspicious, C2 | Ramnit |
| virusbook domain | threats_domain | [REDACTED] | [REDACTED] | Suspicious, C2 | Ramnit |

案例-复用http服务后门

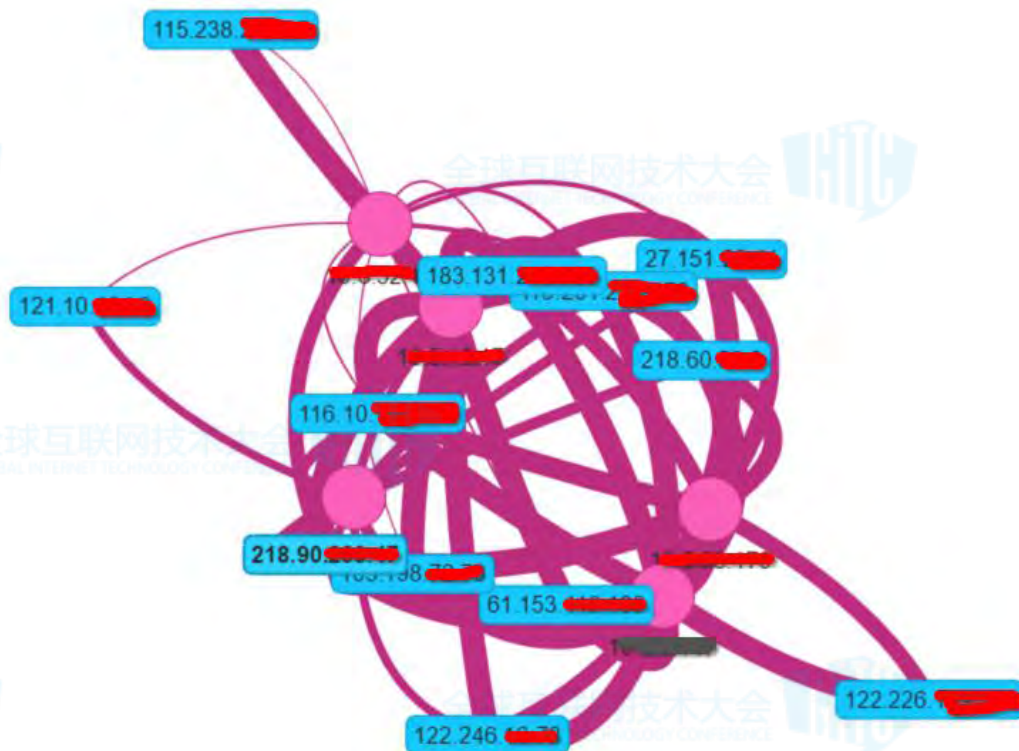
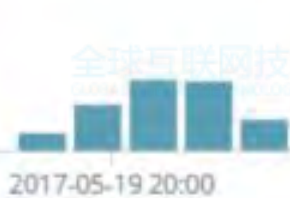
1. 绕过防火墙ACL规则

2. 特定IP生效

| | | | | | | | | |
|--------------------------------|------------|------------|------------|----|-----|-----|-----------|---------|
| ▶ July 24th 2017, 19:16:57.081 | [REDACTED] | [REDACTED] | [REDACTED] | 80 | ssh | tcp | 495,317 | 33,343 |
| ▶ July 24th 2017, 17:08:23.277 | [REDACTED] | [REDACTED] | [REDACTED] | 80 | ssh | tcp | 3,430,101 | 161,631 |
| ▶ July 24th 2017, 16:30:55.492 | [REDACTED] | [REDACTED] | [REDACTED] | 80 | ssh | tcp | 569,797 | 75,343 |
| ▶ July 24th 2017, 17:07:48.986 | [REDACTED] | [REDACTED] | [REDACTED] | 80 | ssh | tcp | 3,125 | 3,951 |
| ▶ July 24th 2017, 17:07:44.916 | [REDACTED] | [REDACTED] | [REDACTED] | 80 | ssh | tcp | 3,125 | 3,951 |
| ▶ July 24th 2017, 17:07:28.356 | [REDACTED] | [REDACTED] | [REDACTED] | 80 | ssh | tcp | 3,125 | 3,951 |
| ▶ July 24th 2017, 15:50:57.438 | [REDACTED] | [REDACTED] | [REDACTED] | 80 | ssh | tcp | 842,213 | 37,551 |
| ▶ July 24th 2017, 15:50:57.436 | [REDACTED] | [REDACTED] | [REDACTED] | 80 | ssh | tcp | 842,213 | 37,551 |

案例-后门访问

1. 特定时间访问
2. 固定访问频率
3. 特定C2地址



SOC\SIEM对接

1. 复杂事件处理
2. 关联规则
3. 自动化告警
4. 联动

查询条件

时间范围 2017-11-13 20:27:19 ~ 2017-11-13

关键字

Q Search

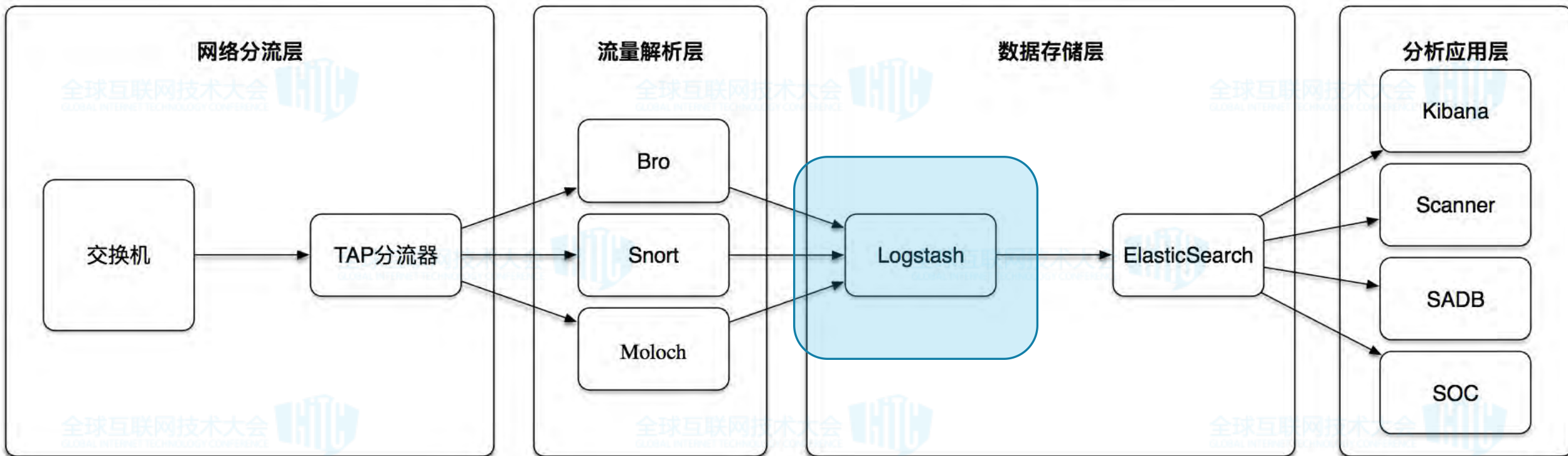
Show 100 entries

[批量误报](#) [批量忽略](#)

| <input type="checkbox"/> | 产生时刻 | 事件名称 | 源IP | 用户 | 目的IP | 目的端口 | 状态 | 报告人 | 工单key | 操作 |
|--------------------------|-----------------------|--------------------------------|------------|------------|------|------|-----|-----|-------|--|
| <input type="checkbox"/> | 2017-11-13 下午 9:26:24 | 暗云 / Pengex / 异鬼 / 魔融 - 肉鸡上线监控 | [REDACTED] | [REDACTED] | | | 未处理 | | | 提交工单 误报 忽略 追溯 |
| <input type="checkbox"/> | 2017-11-13 下午 9:26:24 | 暗云 / Pengex / 异鬼 / 魔融 - 肉鸡上线监控 | [REDACTED] | [REDACTED] | | | 未处理 | | | 提交工单 误报 忽略 追溯 |
| <input type="checkbox"/> | 2017-11-13 下午 9:26:24 | 暗云 / Pengex / 异鬼 / 魔融 - 肉鸡上线监控 | [REDACTED] | [REDACTED] | | | 未处理 | | | 提交工单 误报 忽略 追溯 |
| <input type="checkbox"/> | 2017-11-13 下午 9:26:24 | 暗云 / Pengex / 异鬼 / 魔融 - 肉鸡上线监控 | [REDACTED] | [REDACTED] | | | 未处理 | | | 提交工单 误报 忽略 追溯 |
| <input type="checkbox"/> | 2017-11-13 下午 | 暗云 / Pengex / 异鬼 / 魔融 - 肉鸡上线监控 | [REDACTED] | [REDACTED] | | | 未 | | | 提交工单 误报 |

机器学习

1. 监督学习的数据(特征、标签)
2. 无监督学习的聚类数据



案例-机器学习应用





完美世界安全应急响应中心
security.wanmei.com

Q A