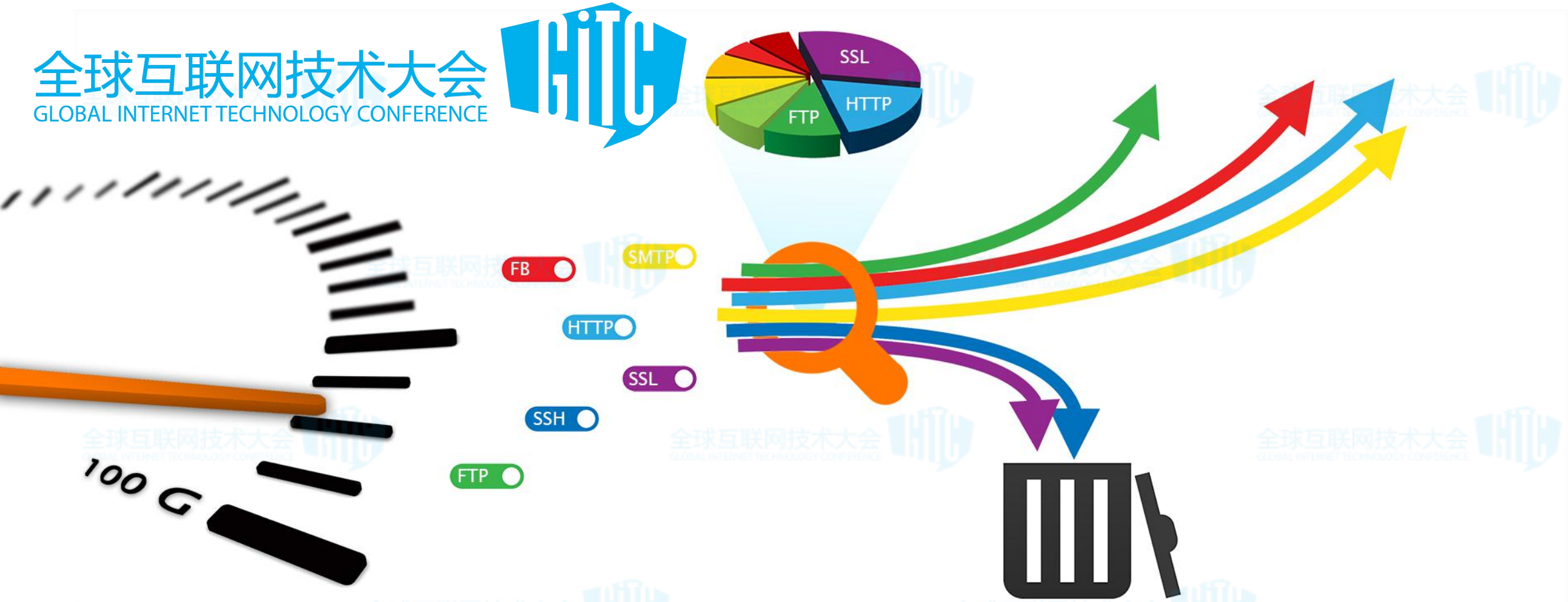
全球互联网技术大会
GLOBAL INTERNET TECHNOLOGY CONFERENCE



流量安全分析平台建设

何艺

About me

何艺

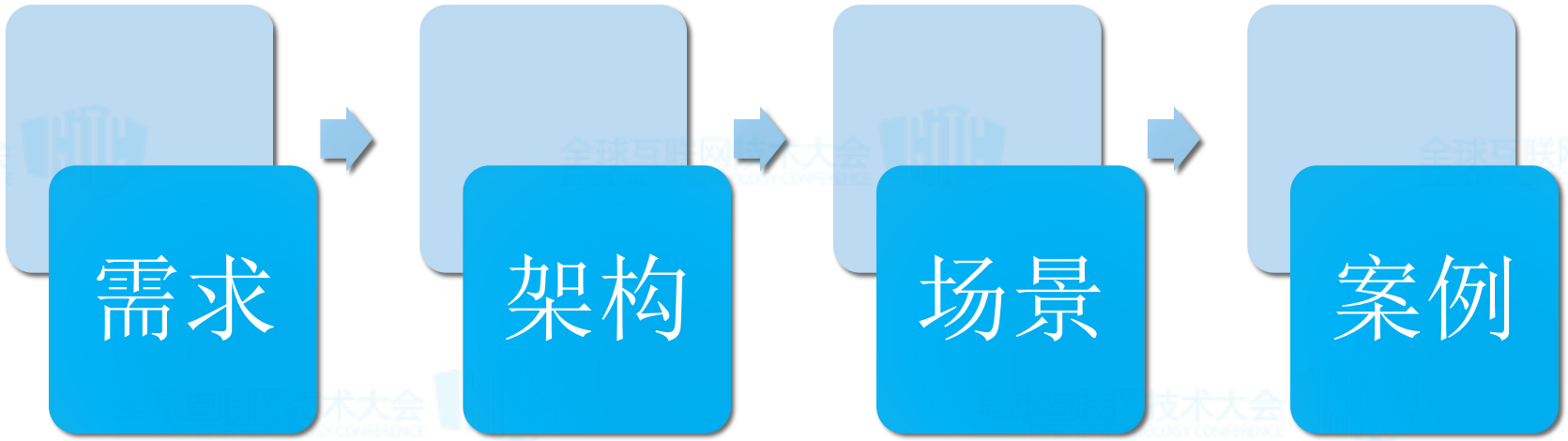
工作经历：

- 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

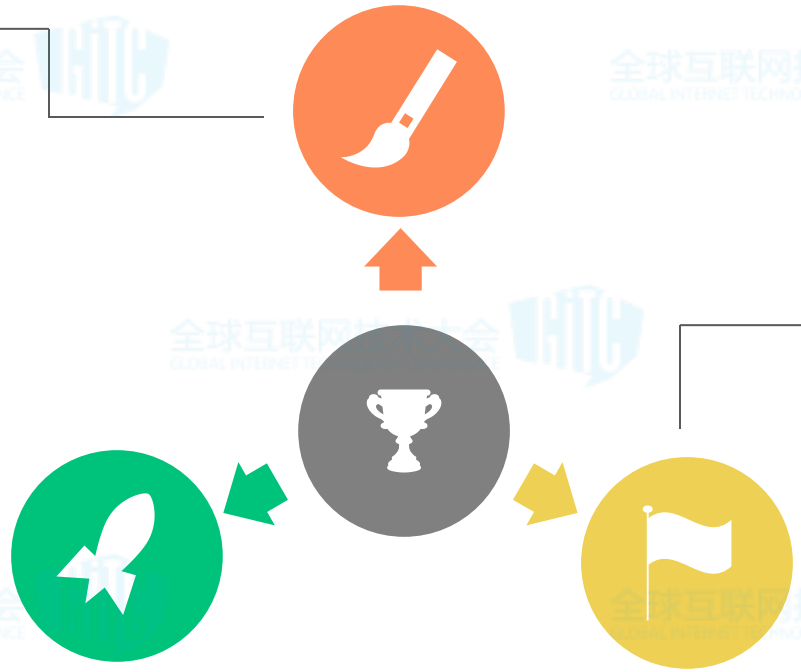
攻防如何博弈？

防护 检测

检测、感知的目的

有什么？

孤岛系统
违规系统
……



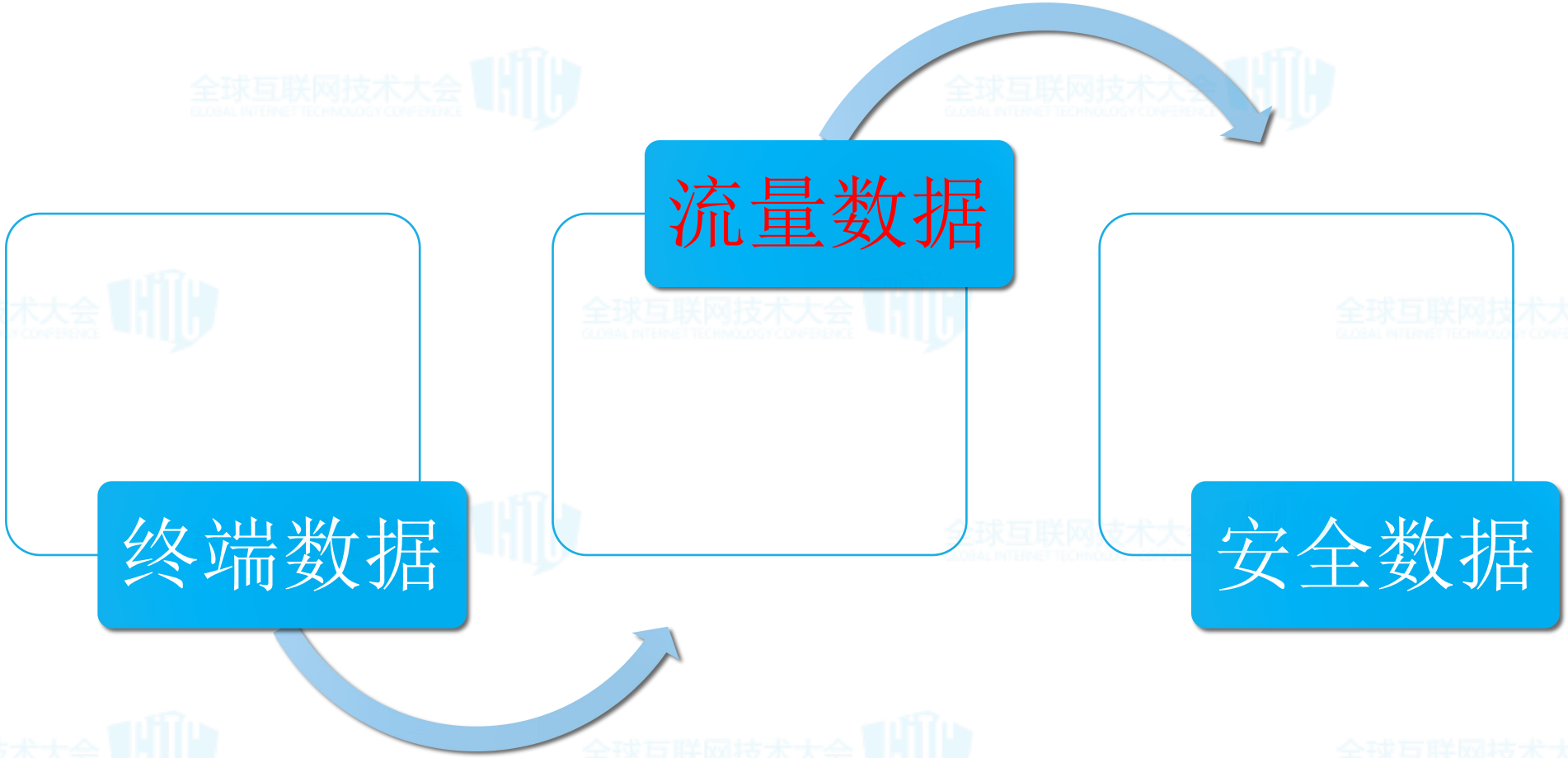
在干嘛？

连接对象
方式方法
通信内容
……

有什么问题？

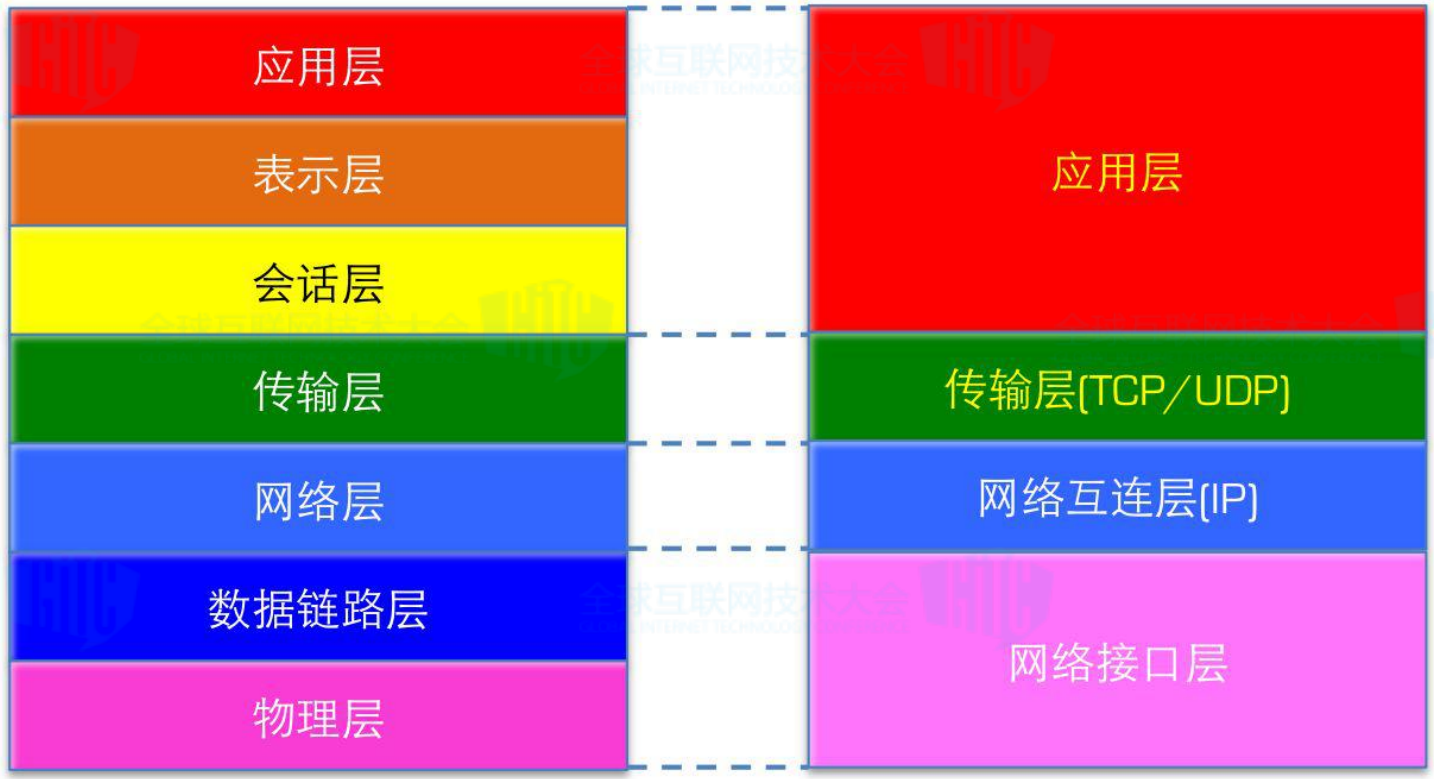
风险、漏洞
安全事件
异常访问
……

数据来源

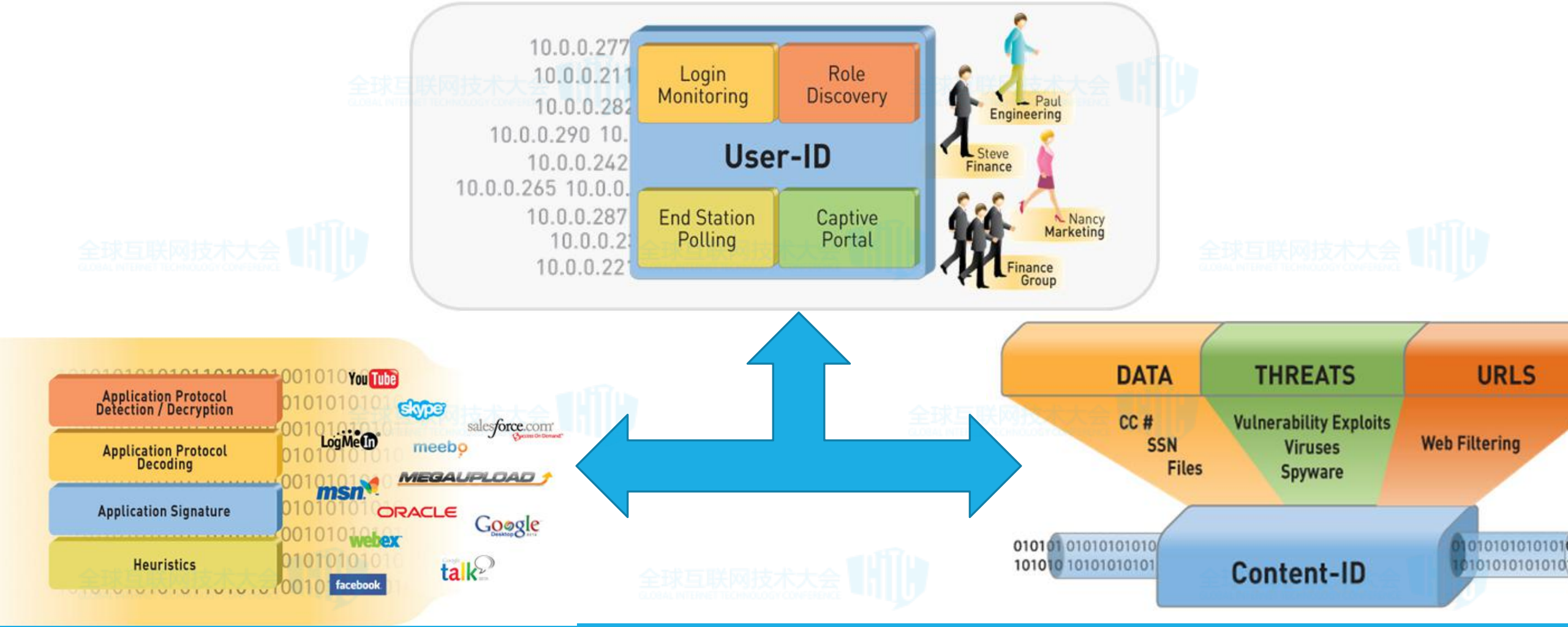


传统流量分析缺陷

- 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


10.0.0.277
10.0.0.211
10.0.0.282
10.0.0.290 10.
10.0.0.242
10.0.0.265 10.0.0.
10.0.0.287
10.0.0.2
10.0.0.22
Login Monitoring
Role Discovery
User-ID
End Station Polling
Captive Portal
Paul Engineering
Steve Finance
Nancy Marketing
Finance Group
Application Protocol Detection / Decryption
Application Protocol Decoding
Application Signature
Heuristics
YouTube
skype
salesforce.com
LogMeIn
meebo
MEGAUPLOAD
msn
ORACLE
Google
webex
facebook
talk
DATA
THREATS
URLS
CC #
SSN
Files
Vulnerability Exploits
Viruses
Spyware
Web Filtering
Content-ID

安全需求

威胁识别

漏洞利用、扫描、C&C、异常访问、威胁情报

资产发现

自动化资产发现、端口、版本、关系

内容解析

服务、应用、版本、通信内容解析

协议解析

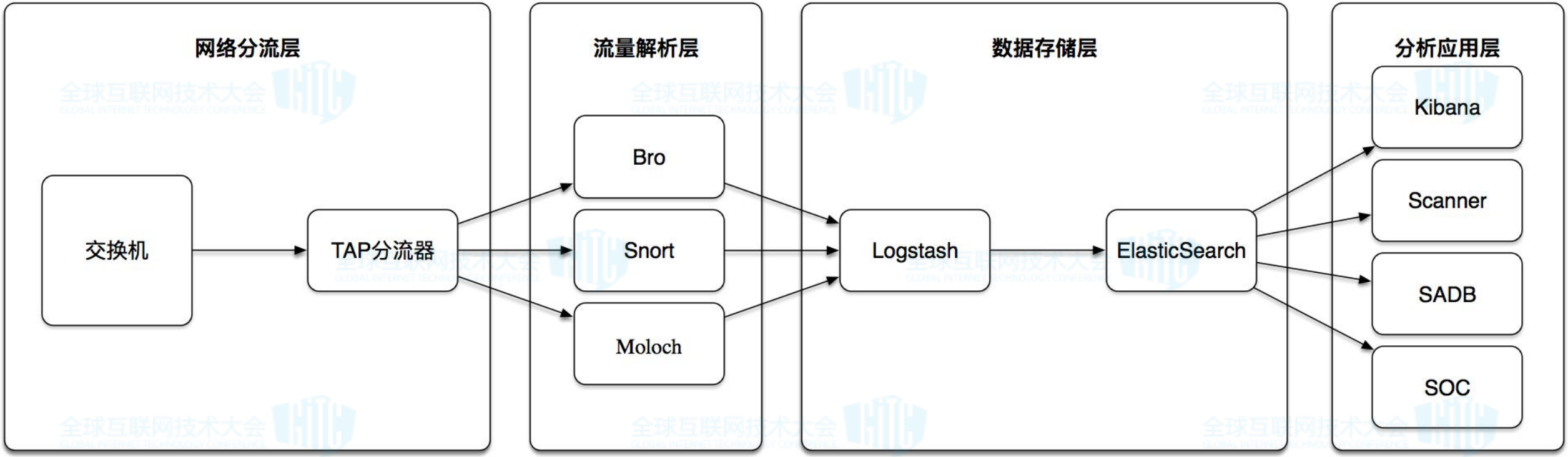
5元组信息、会话时长、包数量、大小等

全流量存储

原始流量保存，索引

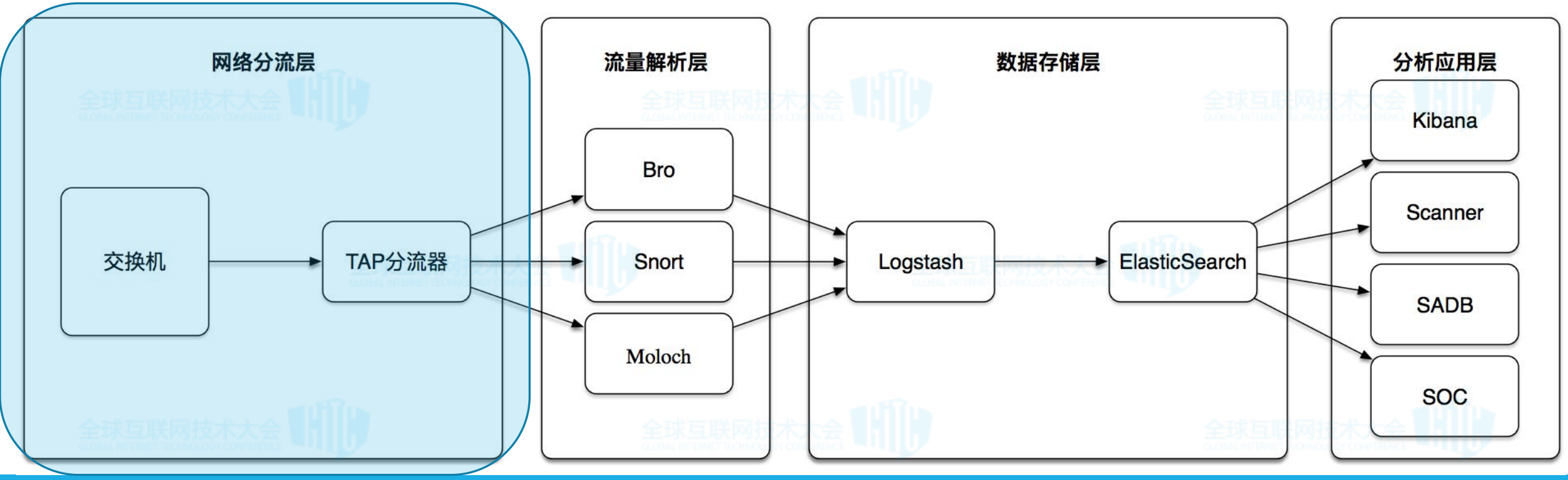
系统架构

1. 多场景适应
2. 易扩展



网络分流层

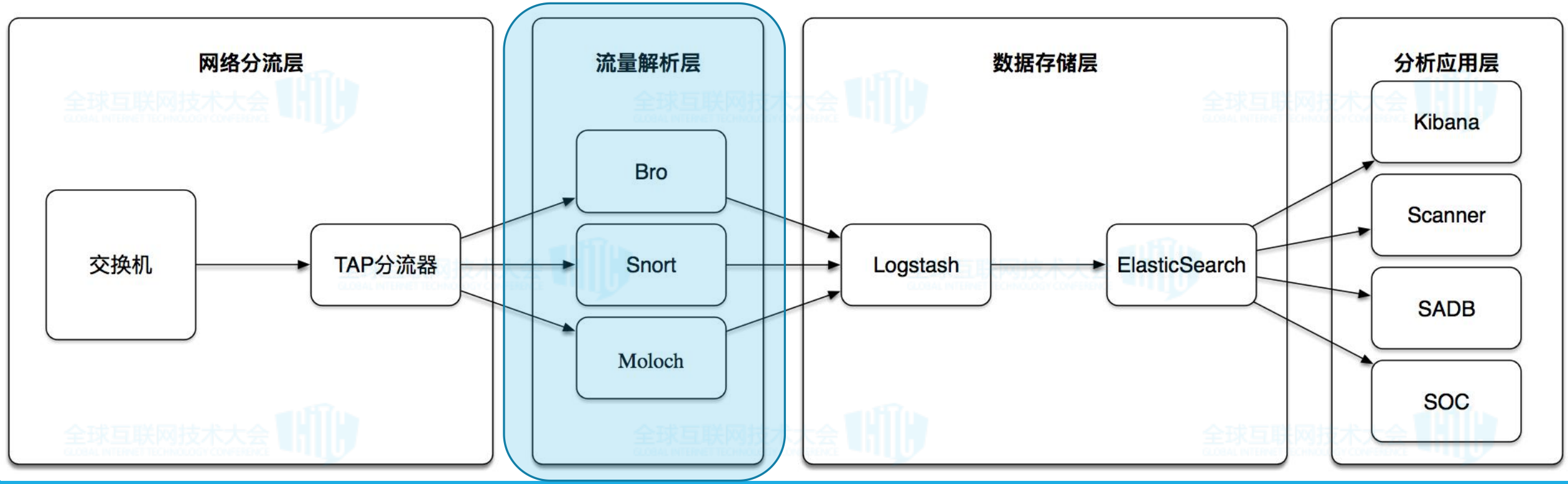
1. 数据一路多出
2. 数据一路多分



流量解析层

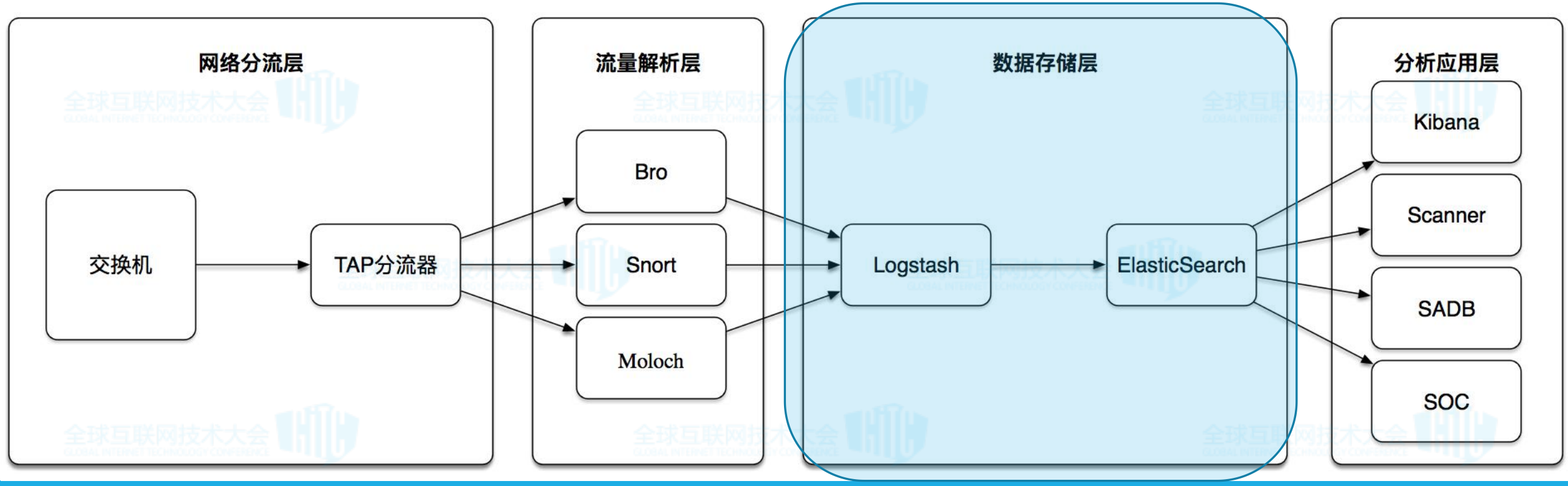
1. Bro：DPI内容识别
2. Snort：NIDS特征匹配告警
3. Moloch：全原始流量抓取，分析固证

about suricate



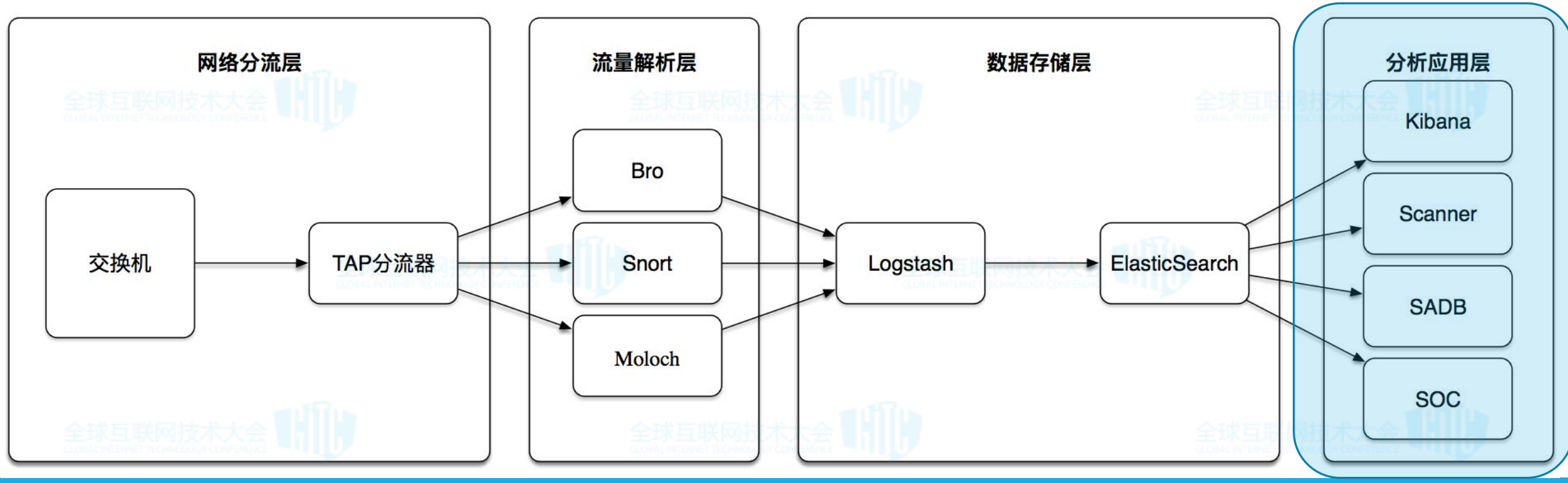
数据存储层

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



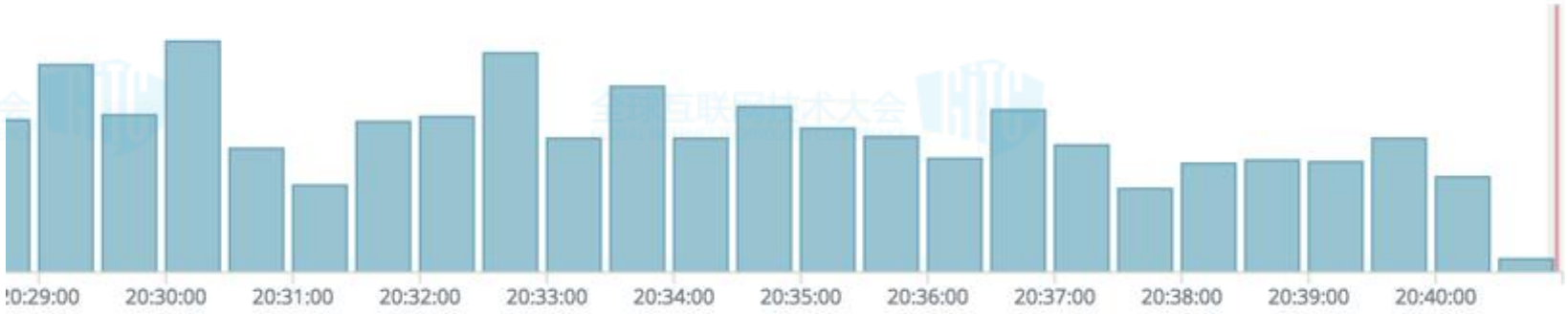
分析应用层

让数据产生价值的地方！



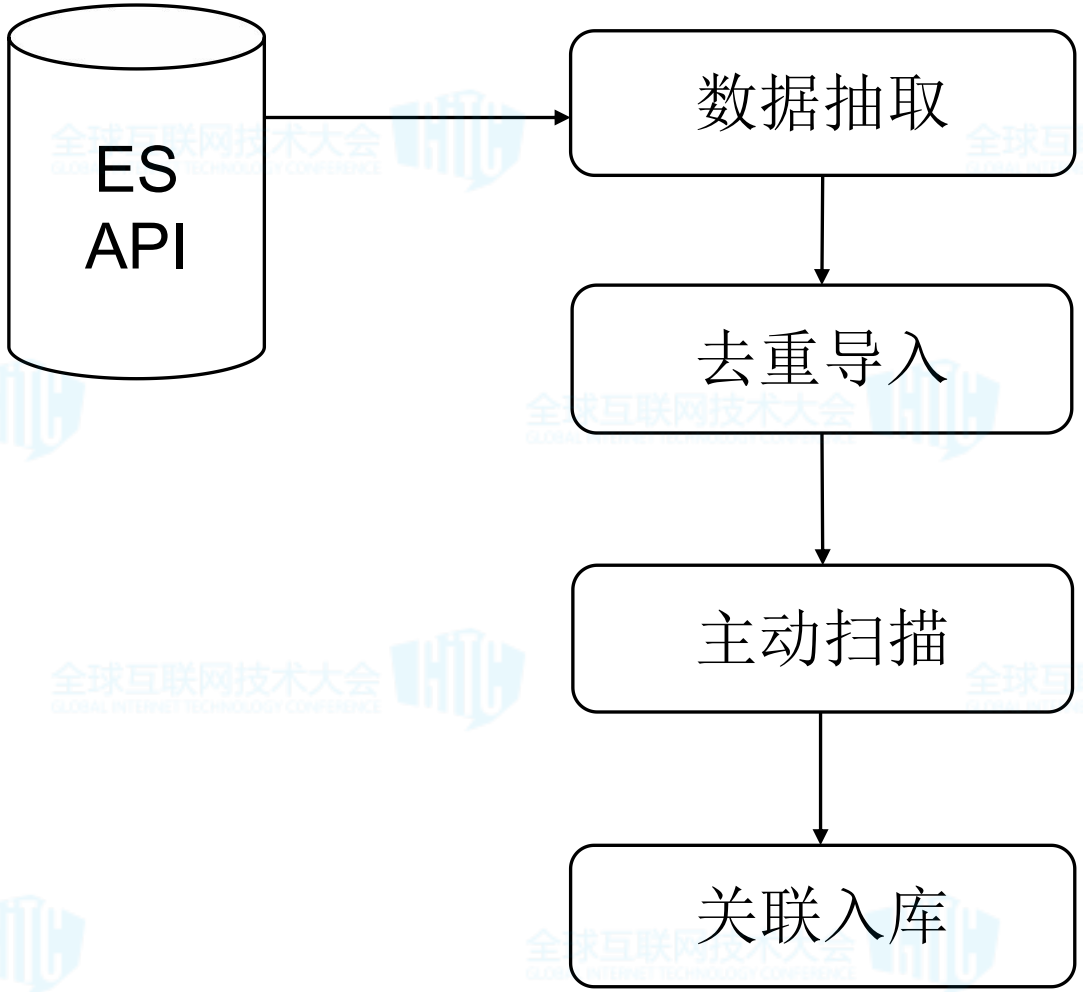
资产自动发现

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

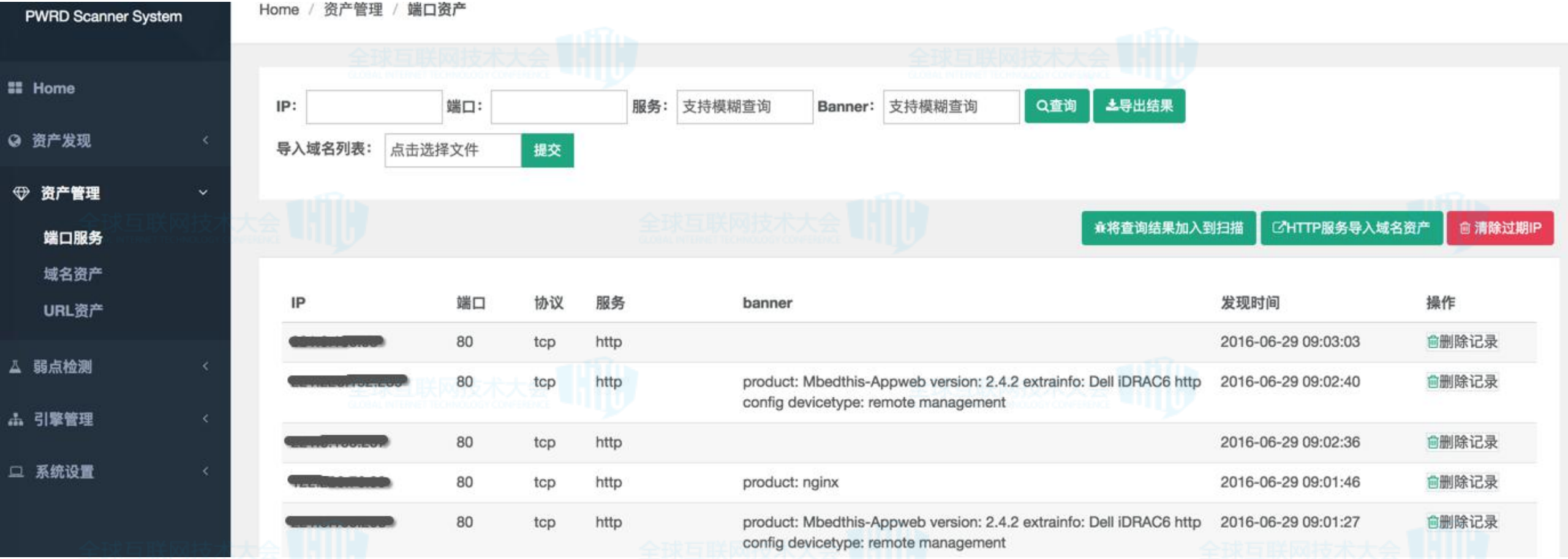


host	software_type	port	name	unparsed_version
[redacted] 8	HTTP::SERVER	80	Apache	Apache/2.4.10 (Debian)
[redacted]	HTTP::SERVER	80	QZHTTP	QZHTTP-2.38.20
[redacted]	HTTP::SERVER	80	QZHTTP	QZHTTP-2.38.20
[redacted] 6	HTTP::SERVER	80	Apache	Apache/2.4.10 (Debian)
[redacted]	HTTP::APPSERVER	80	Servlet	Servlet/2.4 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
查询
导出结果
导入域名列表:
点击选择文件
提交
将查询结果加入到扫描
HTTP服务导入域名资产
清除过期IP
IP
端口
协议
服务
banner
发现时间
操作
80 tcp http 2016-06-29 09:03:03 删除记录
80 tcp http product: Mbedthis-Appweb version: 2.4.2 extrainfo: Dell iDRAC6 http config devicetype: remote management 2016-06-29 09:02:40 删除记录
80 tcp http 2016-06-29 09:02:36 删除记录
80 tcp http product: nginx 2016-06-29 09:01:46 删除记录
80 tcp http product: Mbedthis-Appweb version: 2.4.2 extrainfo: Dell iDRAC6 http config devicetype: remote management 2016-06-29 09:01:27 删除记录

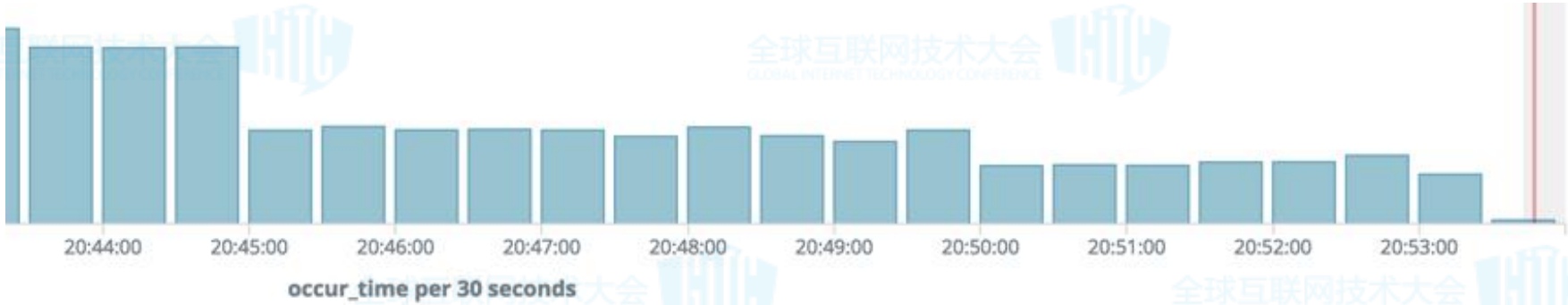
被动式web漏洞扫描

用途：

- 发现未知漏洞
- 发现未知攻击
- 免爬虫扫描

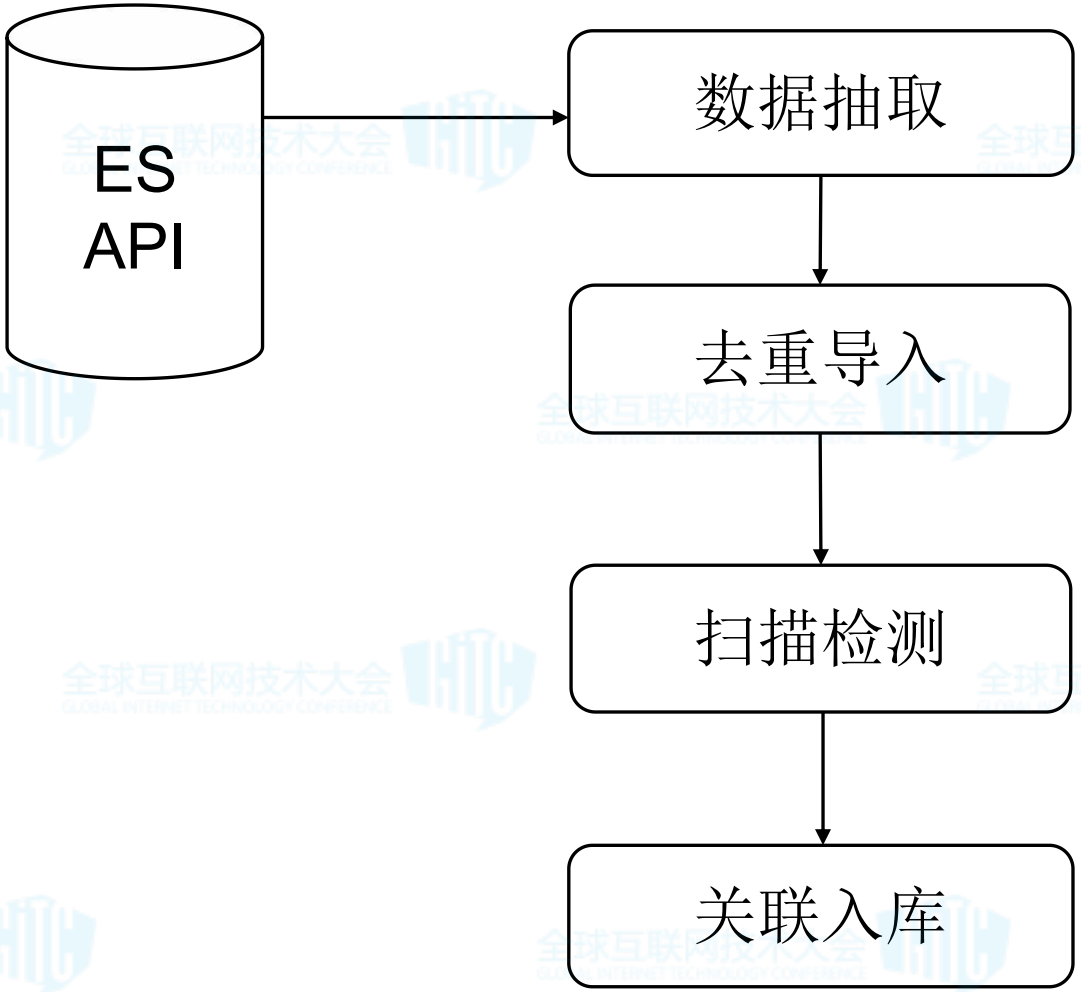
数据：

- bro-http



host	dst_port	uri	method	post_body	status_code	user_agent	cookie
[redacted]	80	[redacted]	GET	-	200	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0	[redacted]

被动式漏洞扫描



案例-被动式web漏洞扫描

威胁情报分析

1 域名检测

bro-dns
bro-http

2 URI检测

bro-http
bro-smtp

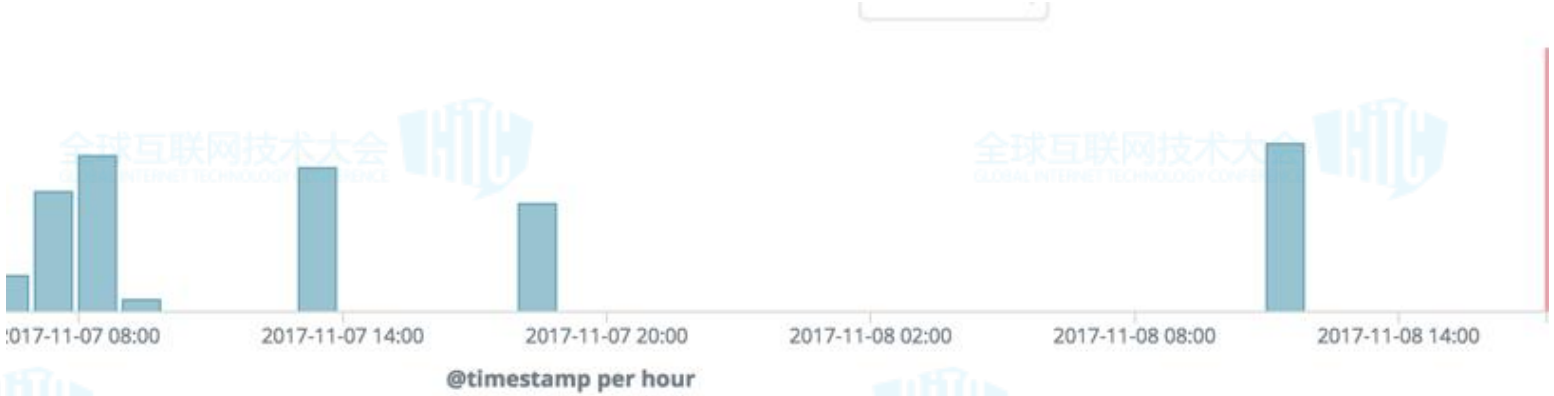
3 IP检测

bro-conn

4 HASH检测

bro-files

案例-威胁情报分析



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

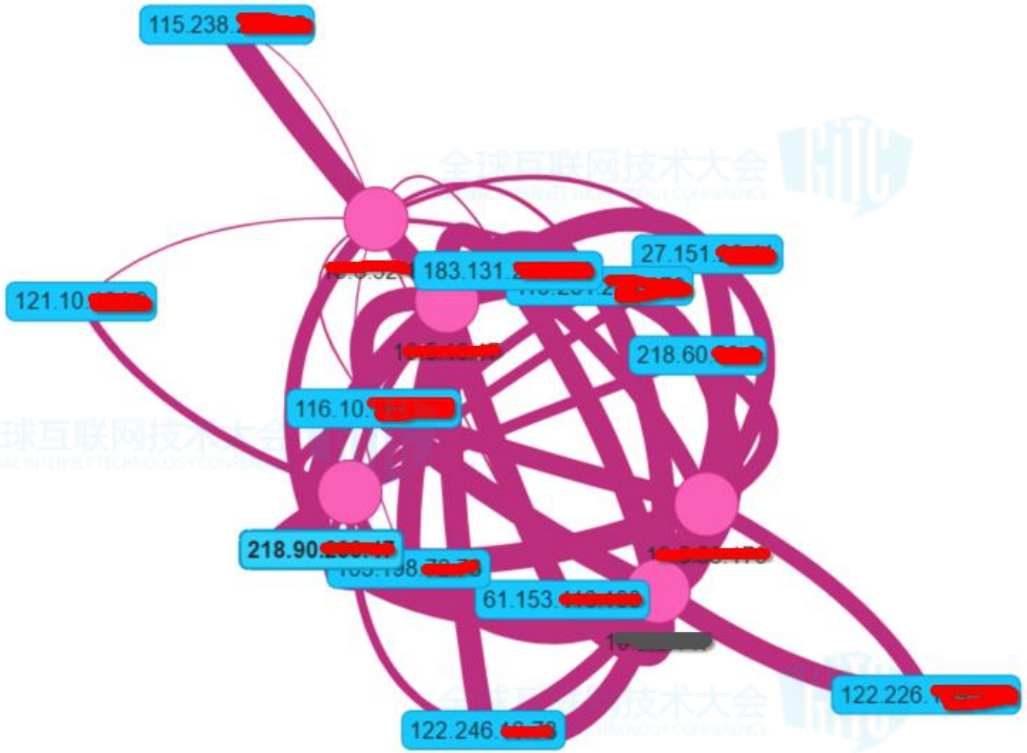
案例-复用http服务后门

1. 绕过防火墙ACL规则
2. 特定IP生效

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

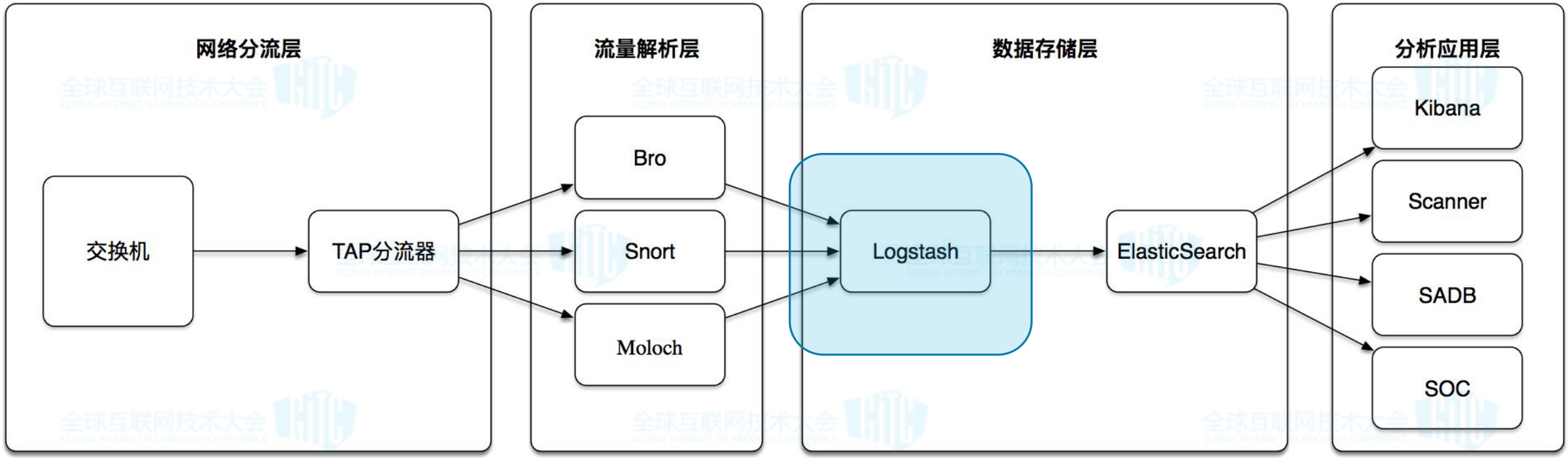


SOC\SIEM对接

1. 复杂事件处理
2. 关联规则
3. 自动化告警
4. 联动

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