# 图说企业安全建设

## 看屌丝是怎样建设安全基础设施

--- 小米安全中心：康竟淞

新浪微博：@淡定淞淞

# 前言

- 权限管理
  - Godlike -- 认证，授权，审计（AAA）
  - Medusa -- 密码管理
- 入侵检测
  - NIDS -- Suricata+ELK
  - LIDS -- OSSEC
- Web安全
  - Webscan -- 扫描平台
- 安全防护
  - Shield -- 应用防火墙
- 数据分析
  - 安全日志分析
  - 流量分析

# Godlike

- 关键字：
  - Google authenticator
  - Cmdrecorde
  - Kerberos
  - Ldap

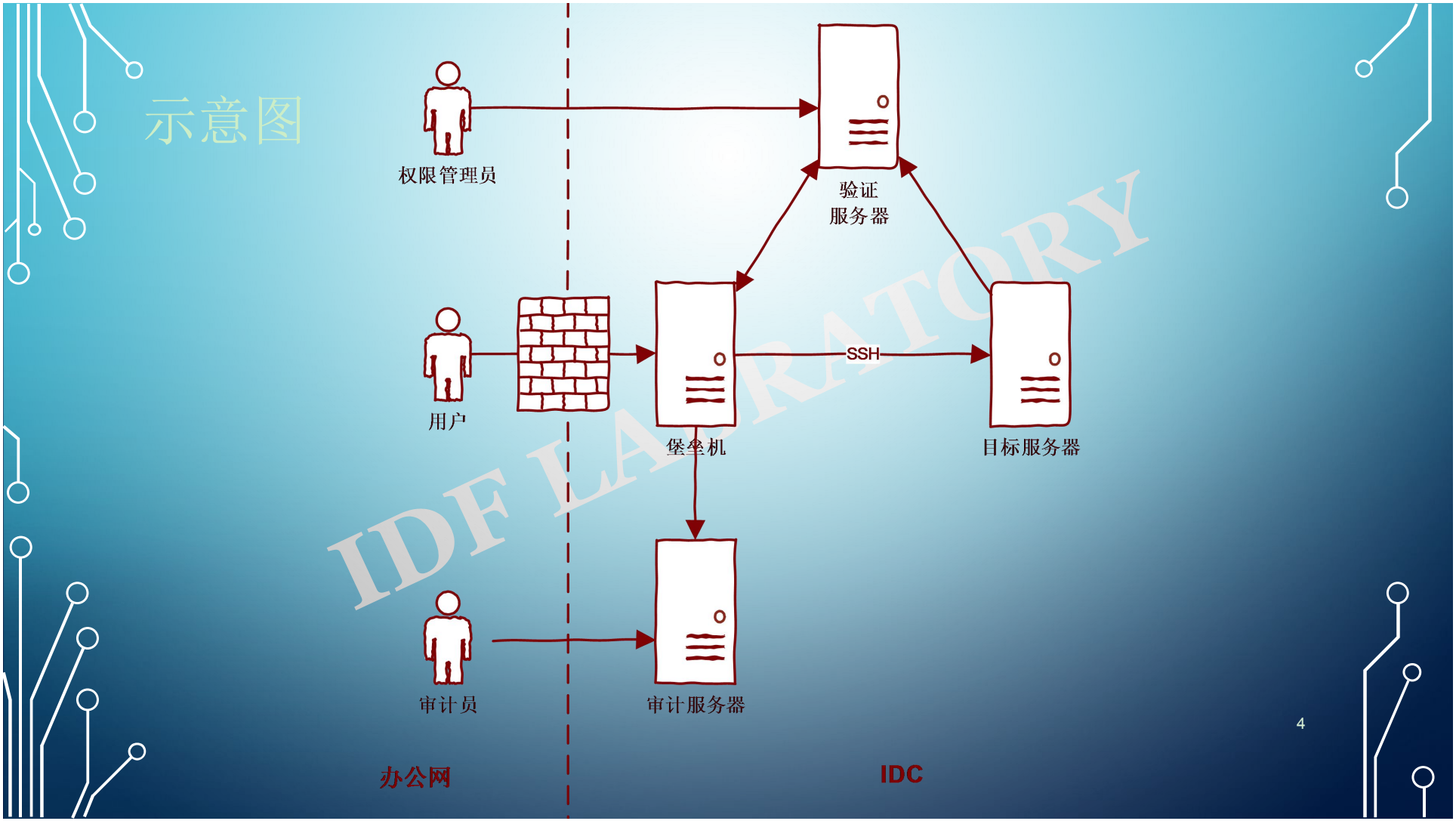
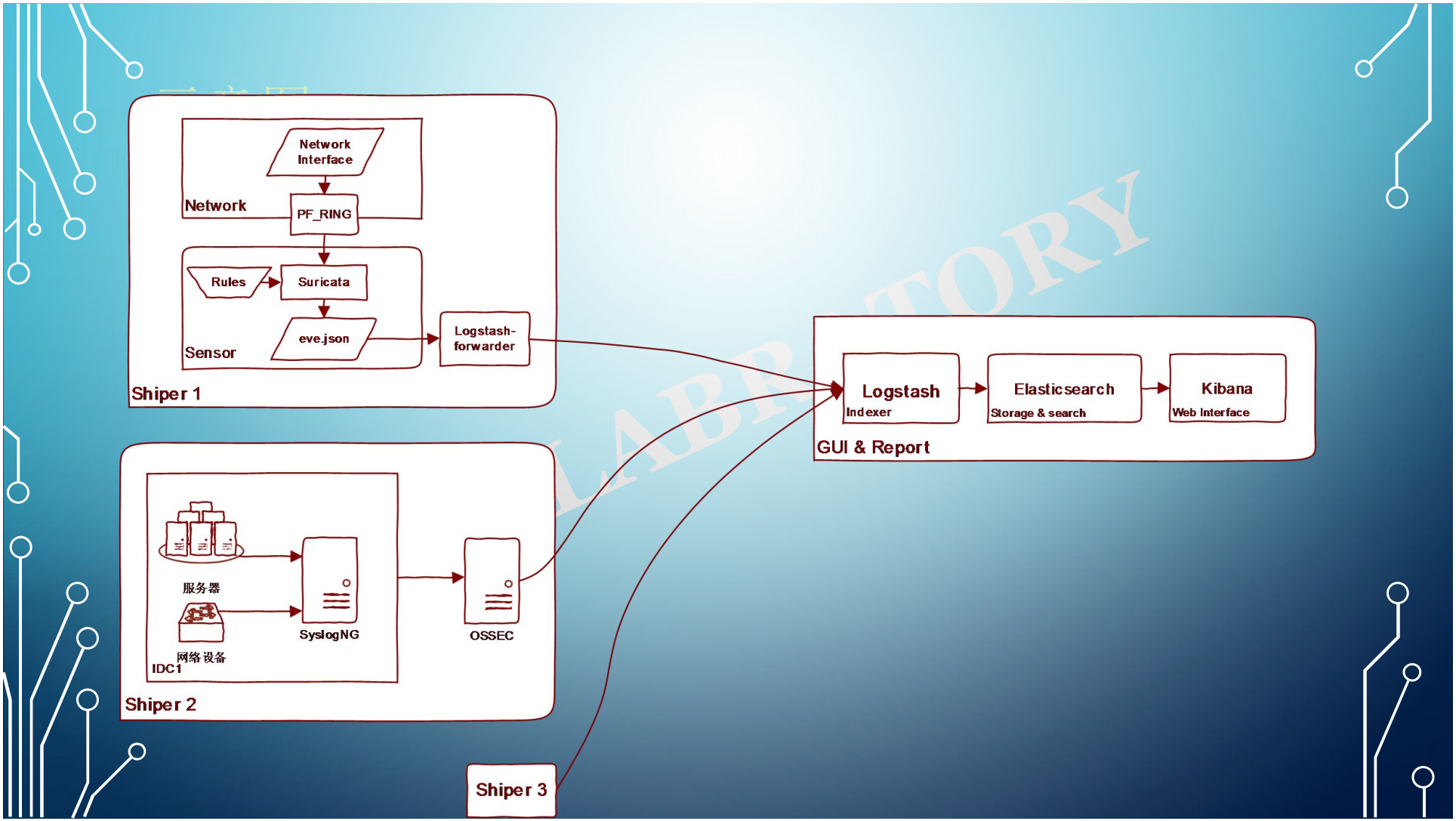


示意图
权限管理员
验证
服务器
用户
SSH
堡垒机
目标服务器
审计员
审计服务器
办公网
IDC
IDF LABORATORY

# 各角色界面

# ids

- 关键字：
  - Suricata
  - ELK（elasticsearch + Logstash + Kibana）
  - Ossec
  - SyslogNG

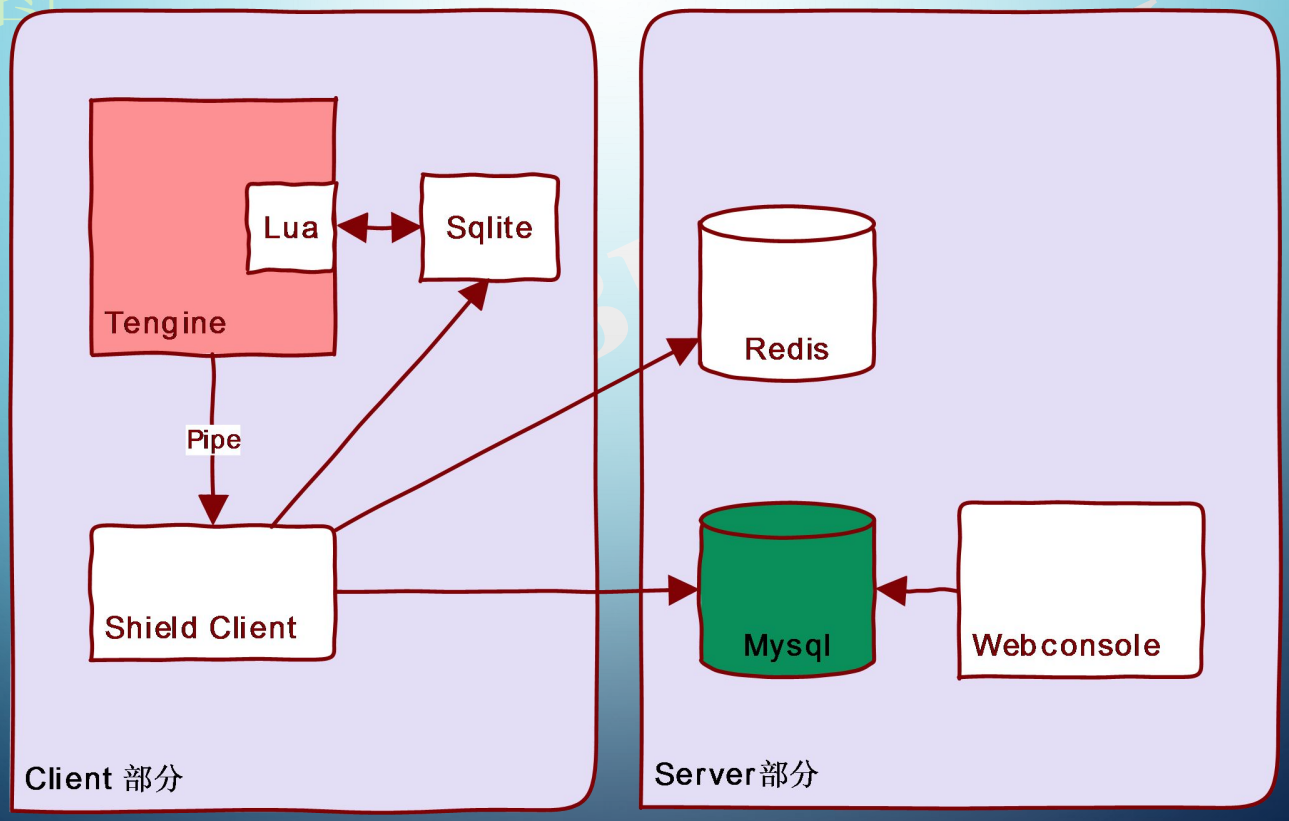

Network Interface
Network
PF_RING
Rules
Suricata
eve.json
Sensor
Logstash-forwarder
Shiper 1
服务器
网络设备
IDC1
SyslogNG
OSSEC
Shiper 2
Shiper 3
Logstash
Indexer
Elasticsearch
Storage & search
Kibana
Web Interface
GUI & Report


HIGH
View | Zoom Out | alert.severity:"1" (0) count per 30m | (0 hits)
1.00
0.75
0.50
0.25
0.00
16:00
07-25
MIDDLE
View | Zoom Out | alert.severity:"2" (1485) count per 1h | (1485 hits)
80
60
40
LOW
View | Zoom Out | alert.severity:"3" (1343) count per 1h | (1343 hits)
150
100
WORLD
Kazakhstan: 58
CHINA
SOURCE
100%
0
8
11

# Shield

- 关键字：
  - Nginx
  - Lua
  - Redis

示意图

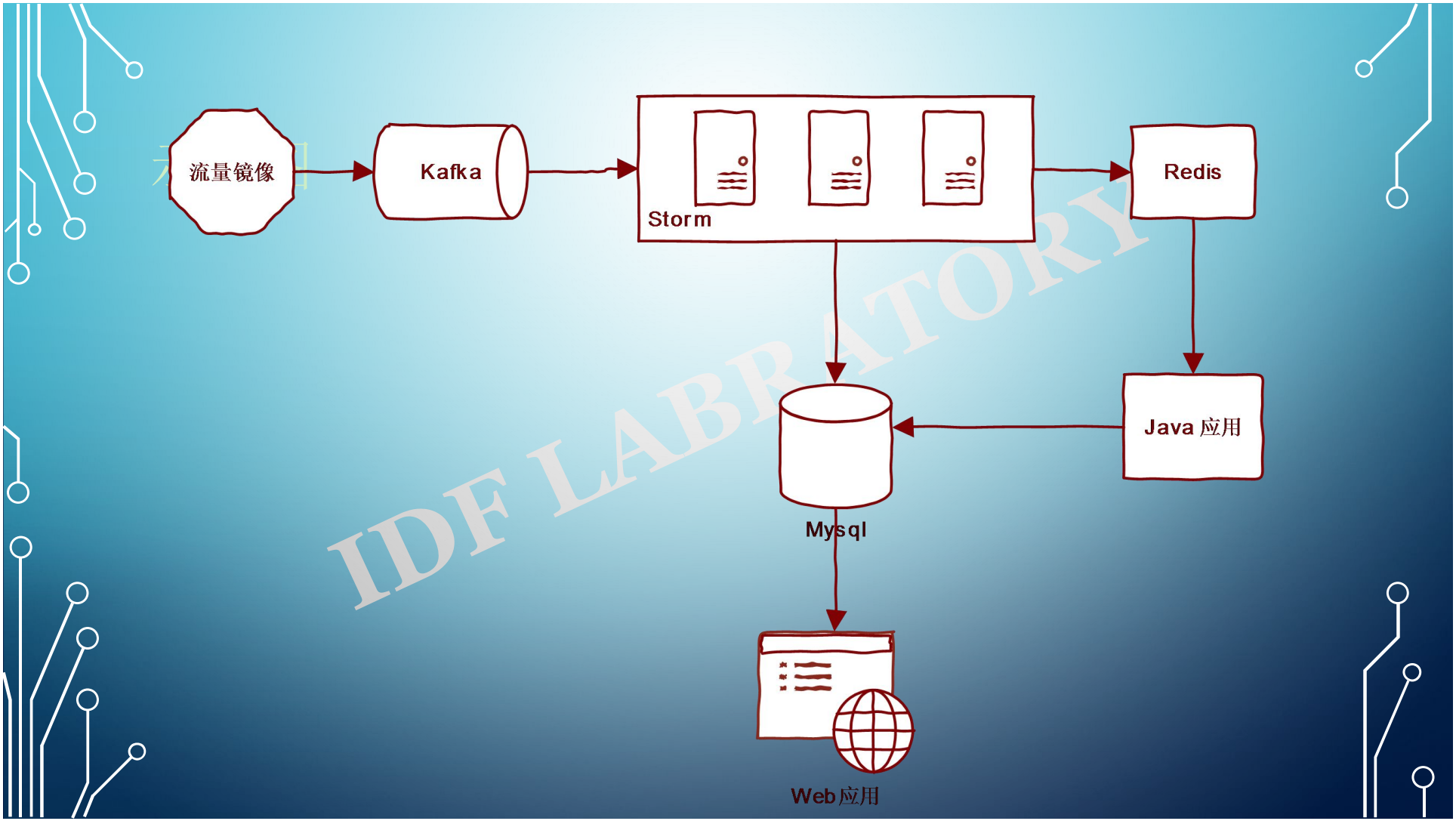

Lua
Sqlite
Tengine
Pipe
Shield Client
Redis
Mysql
Webconsole
Client 部分
Server部分

# 界面图

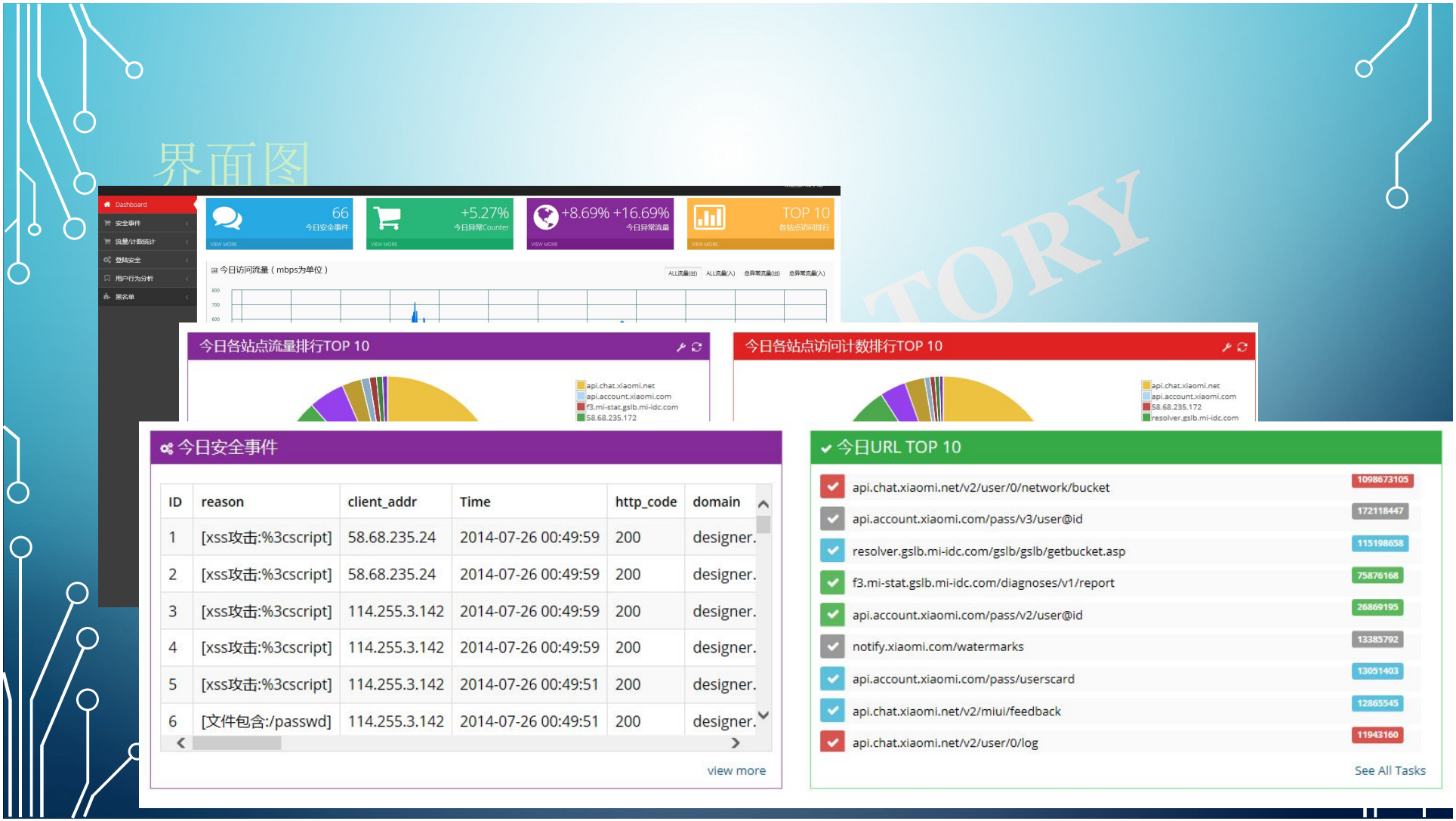

X-waf
规则配置
客户端信息
日志记录
用户管理
AREA
ADD
配置
规则
白名单
拦截模式开关
拦截模式
监控模式
全局开关
启用waf
关闭waf
是否立即更新
立即更新
只保存不更新
最后更新
提交

# 安全日志分析

- 关键字：
  - Kafka
  - Storm
  - Redis


流量镜像
Kafka
Storm
Redis
Java 应用
Mysql
Web 应用
IDF LABRATORY

# 界面图


Dashboard
安全事件
流量/计数统计
登陆安全
用户行为分析
黑名单
66
今日安全事件
+5.27%
今日异常Counter
+8.69% +16.69%
今日异常流量
TOP 10
今日访问流量（mbps为单位）
今日各站点流量排行TOP 10
api.chat.xiaomi.net
api.account.xiaomi.com
f3.mi-stat.gslb.mi-idc.com
58.68.235.172
今日各站点访问计数排行TOP 10
api.chat.xiaomi.net
api.account.xiaomi.com
58.68.235.172
resolver.gslb.mi-idc.com
今日安全事件
ID
reason
client_addr
Time
http_code
domain
1
[xss攻击:%3cscript]
58.68.235.24
2014-07-26 00:49:59
200
designer.
2
[xss攻击:%3cscript]
58.68.235.24
2014-07-26 00:49:59
200
designer.
3
[xss攻击:%3cscript]
114.255.3.142
2014-07-26 00:49:59
200
designer.
4
[xss攻击:%3cscript]
114.255.3.142
2014-07-26 00:49:59
200
designer.
5
[xss攻击:%3cscript]
114.255.3.142
2014-07-26 00:49:51
200
designer.
6
[文件包含:/passwd]
114.255.3.142
2014-07-26 00:49:51
200
designer.
view more
今日URL TOP 10
api.chat.xiaomi.net/v2/user/0/network/bucket
1098673105
api.account.xiaomi.com/pass/v3/user@id
172118447
resolver.gslb.mi-idc.com/gslb/gslb/getbucket.asp
115198658
f3.mi-stat.gslb.mi-idc.com/diagnoses/v1/report
75876168
api.account.xiaomi.com/pass/v2/user@id
26869195
notify.xiaomi.com/watermarks
13385792
api.account.xiaomi.com/pass/userscard
13051403
api.chat.xiaomi.net/v2/miui/feedback
12865545
api.chat.xiaomi.net/v2/user/0/log
11943160
See All Tasks


Q&A
IDF LABRATORY
THANKS!