

# 认知时代的安全体系

李承達(Chenta Lee)

IBM全球首席资讯安全架构师



# 为什么要谈认知安全?

- 我们在人工智能上有突破?
- 我们在量子运算上有突破?
- 认知安全其实是在对的地方,对的使用方法,去运用既有的人工智能技术

面对新型态的威胁,我们必须全方位了解非结构性的资料

80% of the world's data has been invisible.

Until now



## 世界上百分之八十的资料是没有结构性的

HEALTHCARE

99%

88%

growth by 2017

unstructured



**GOVERNMENT& EDUCATION** 

94%

84%

growth by 2017 unstructured

UTILITIES

93%

growth by 2017

84%

unstructured







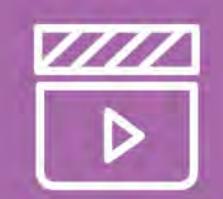
MEDIA

97%

82%

growth by 2017

unstructured









# 认知运算开创了资讯安全的新世代







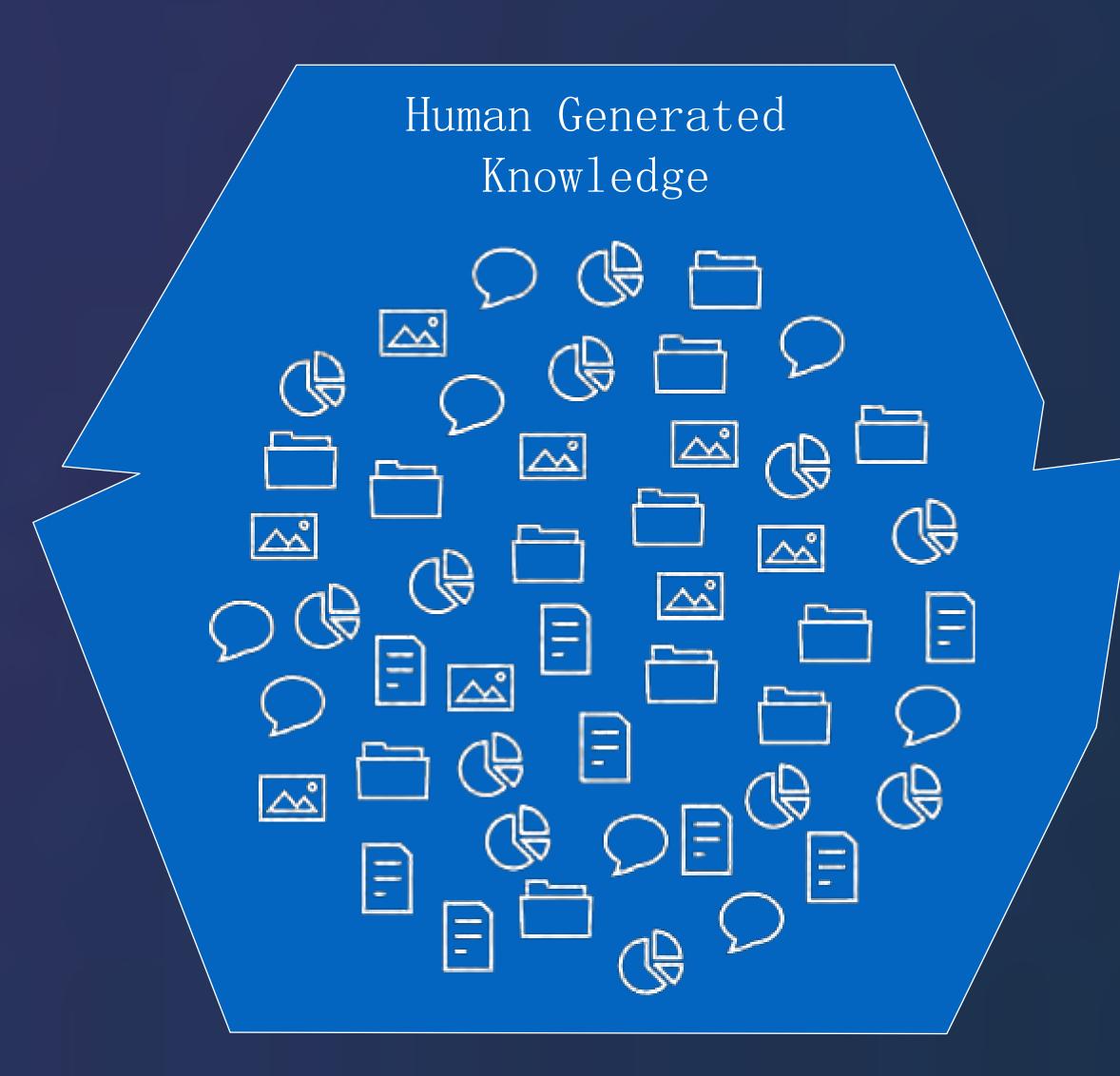
堡垒式防御

智能安全深度整合

认知运算 云计算 协同抵御



# 冰山下的那些事一大量的安全资讯



A universe of security knowledge Dark to your defenses 我们只利用了冰山下百分之八的资料

security blogs / year

news articles / year

security related

security research

papers / year

Industry publications

Forensic information

 Threat intelligence commentary

Analyst reports

Conference presentations

News sources

Newsletters

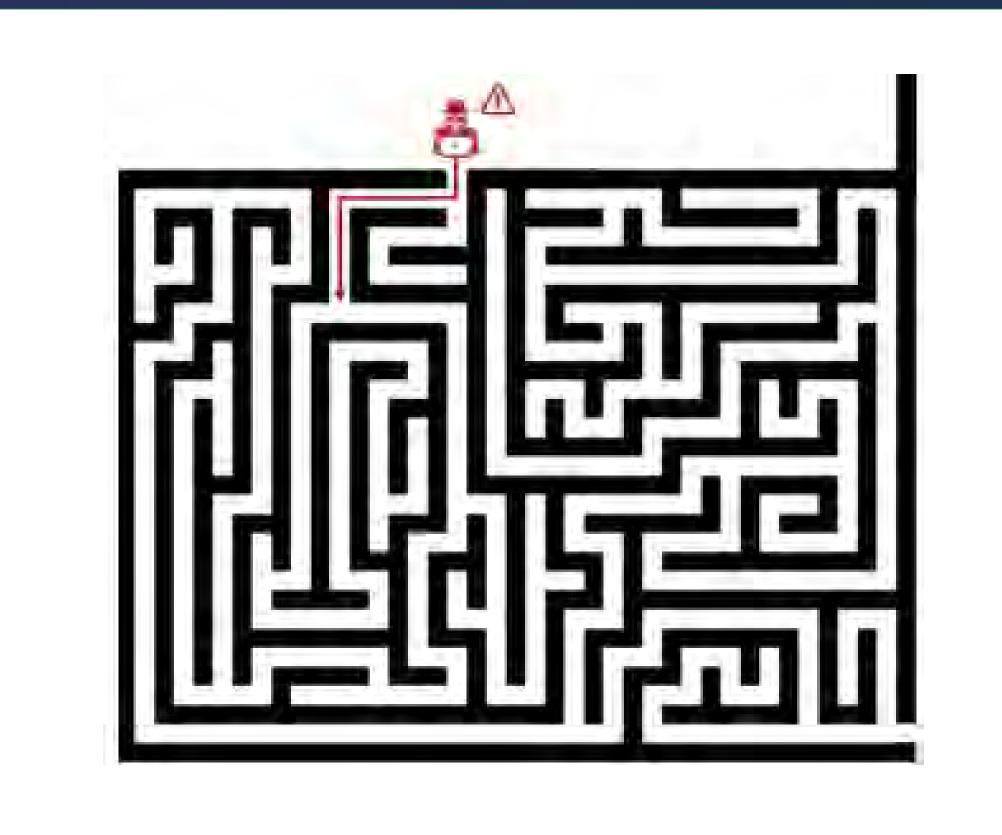
Tweets

Wikis

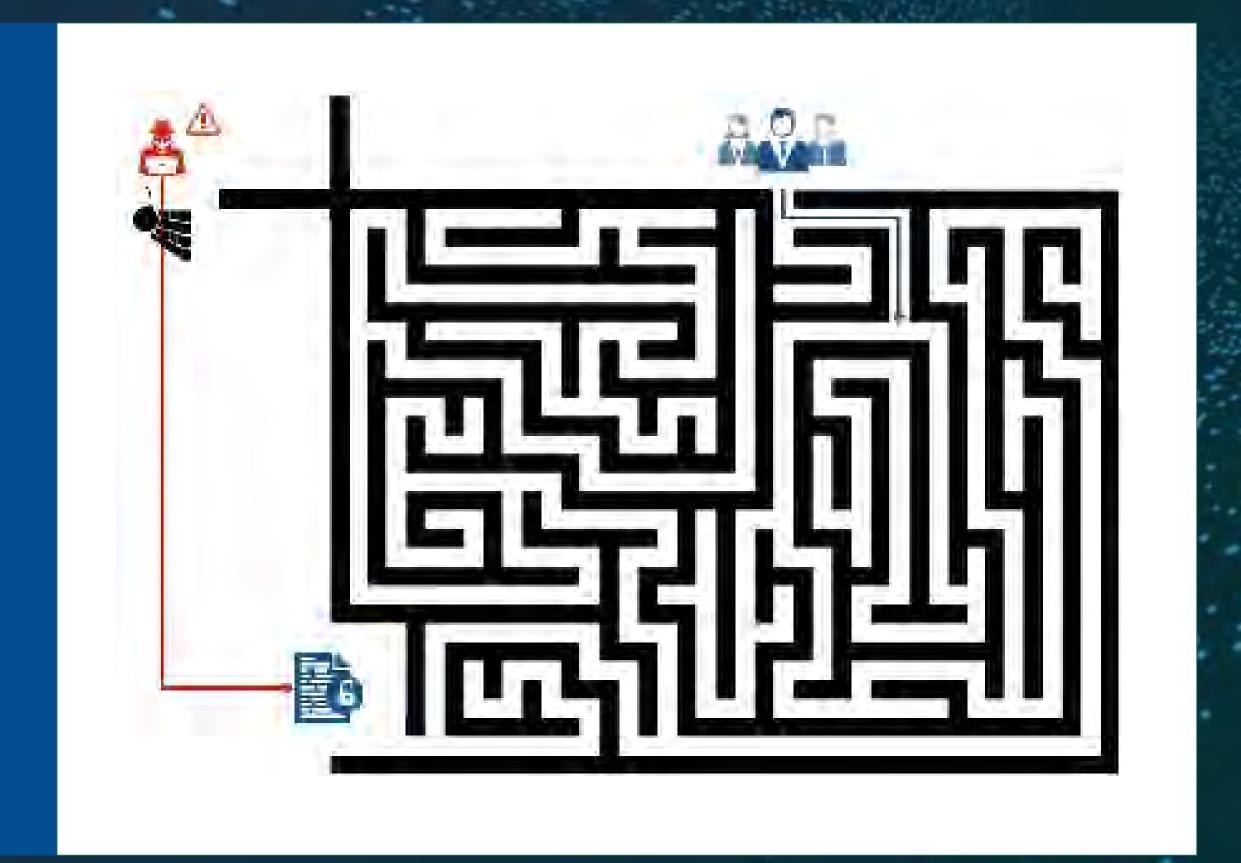


# 知己不知彼一道高一尺魔高一丈

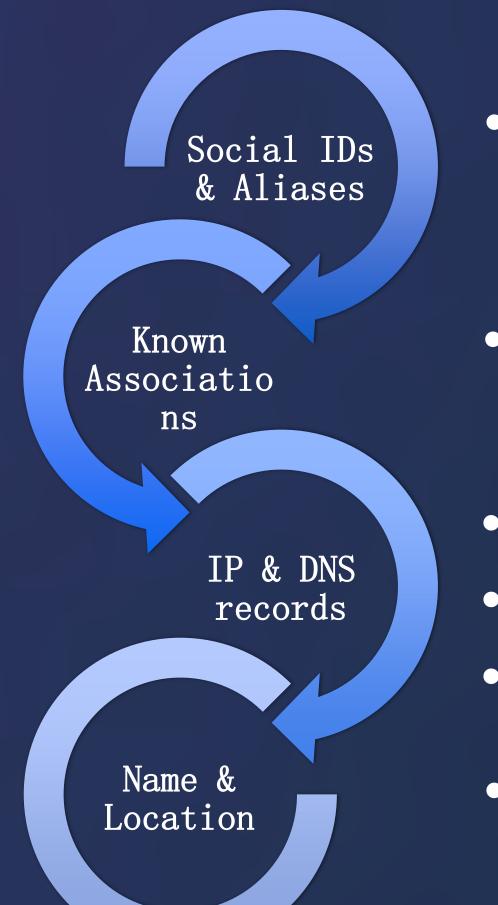
We think we blocked hackers



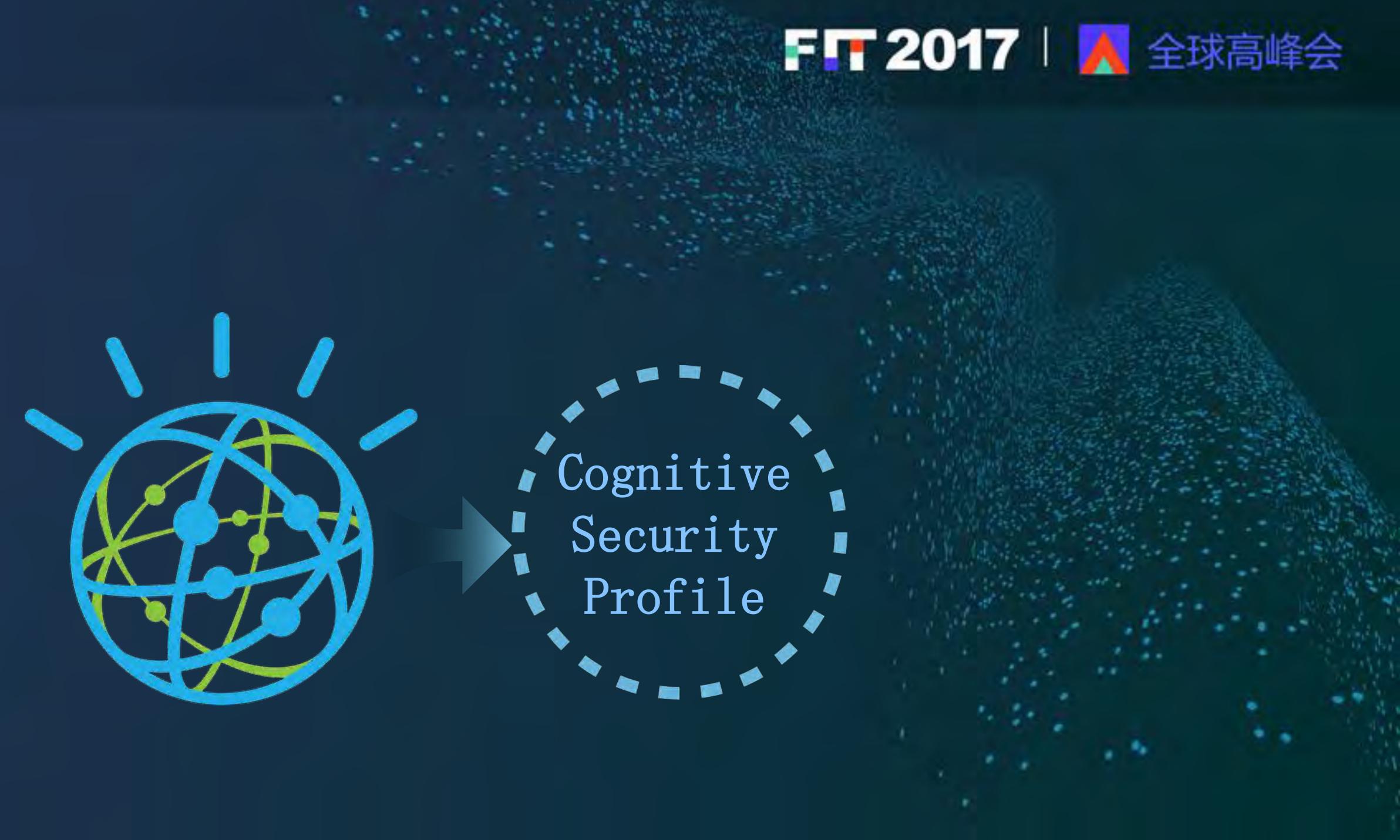
What actually happen is that we cannot trace hackers because we are in the maze







- john@company.com, Mr. Lee, DarkDragon
- •Tojava, JoTalbot
- •31. 170. 179. 179
- •ssndob.ru
- •spam@bad.com
- •Zack Lee, Russia





# 认知运算到底能做什么事情?

Facts (unstructured data)



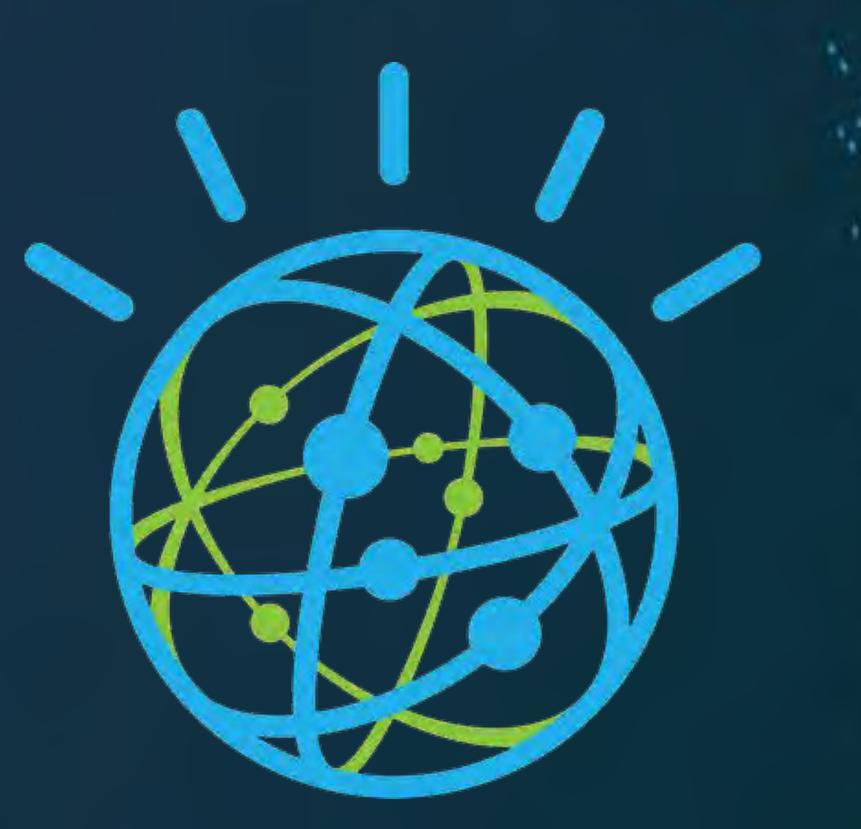
Questions

Answer

Hi Watson, I see 300 access from IP 5.6.7.8, should I be worry about it?

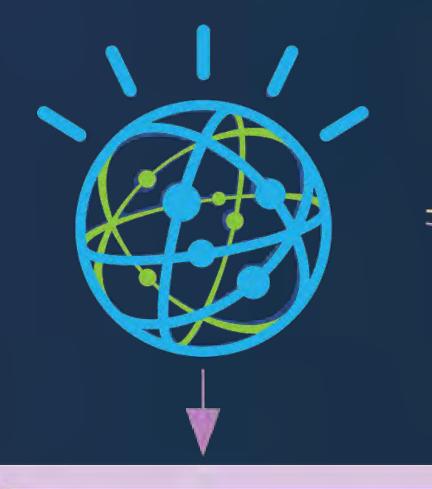
Hi Watson, how many user download file xyz will go to abc. com/test.php within 24 hours?

Hi Watson, how many attacks are related to 1.2.3.4 in health care industry in past 12 hours?





# 关键在于用对的方法使用认知运算



Security Augmentation Cognitive

Security Operations Support

Intellectual Property Analysis

Intention Monitoring

Insight Enhancement

Early Warning

Advanced



# 认知体系下的资讯安全架构

### 认知安全

大数据分析

深度的情资整合

专业资安团队的服务

行业的专精

传统资讯安全部署

- "真正的吸收了解所有的情资并加以运用"
- "找到所有有威胁的情报"
- "快速的识别真正的威胁"
- "我很忙,我只想知道真的有威胁的事件"
- "隔壁银行的资讯安全团队最近在忙啥?"
- "告诉我最即时的资安状态"



F-T 2017 / 全球高峰会

**Threat databases** 

Research reports

Security textbooks

**Vulnerability disclosures** 

Popular websites

Blogs and social activity

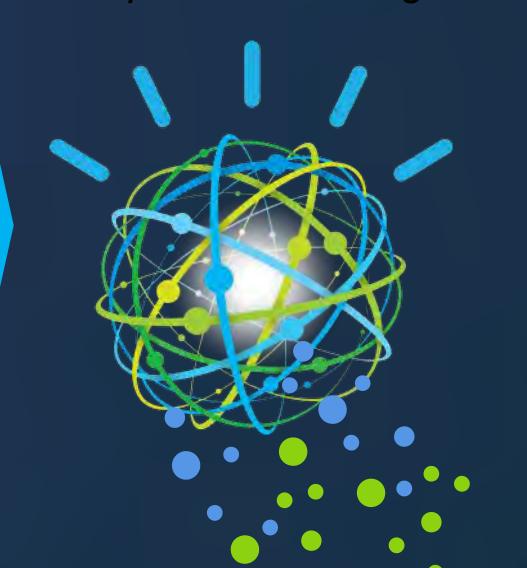
Other

Human Generated Security Knowledge

Sourced by available IBM Security and IBM Research

IBM Watson for cyber security

Corpus of knowledge



**Security events** 

**User activity** 

Configuration information

**Vulnerability results** 

System and app logs

Security policies

Other

Enterprise
Security Analytics
Correlated enterprise data





# 认知运算加强了感知能力

### 更深层的资安见解

Context and Intent

Relationships

Security Intelligence

Corporate Data

Public Data

Aliases

Associates

Threat Data (STIX/TAXII)

Data Feeds (syslog, LEEF, IPFIX, SNMP, APIs)

