REUTERS/Mark Blinch

Leveraging Artificial Intelligence and Advanced Data Analytics to Combat Data Breaches

July 11, 2017

The Good Ole Days

Today's Risk Picture

- No longer just about theft of information, but now includes:
  - Disruption & destruction
  - Weaponization of information

- New or improved tactics
  - Cloud-scale attack engines (botnets)
  - Sophisticated fake sites

- New regulations

What do you see as the Cyber Security Trends?

- Weak or stolen credentials continue to be the #1 tactic for attackers
- Evolution to hybrid on-premise & in-cloud world
- Top threats continue to be phishing, ransomware, unauthorized clouds, data loss through email, fraud targets, etc.
- It’s not enough to have incident response policy/plan, it needs to be exercised
- Outsource of security & compliance programs
- Technology is outpacing our ability to comprehend the risk (think: self-driving cars)

What is AI ?

Artificial Intelligence

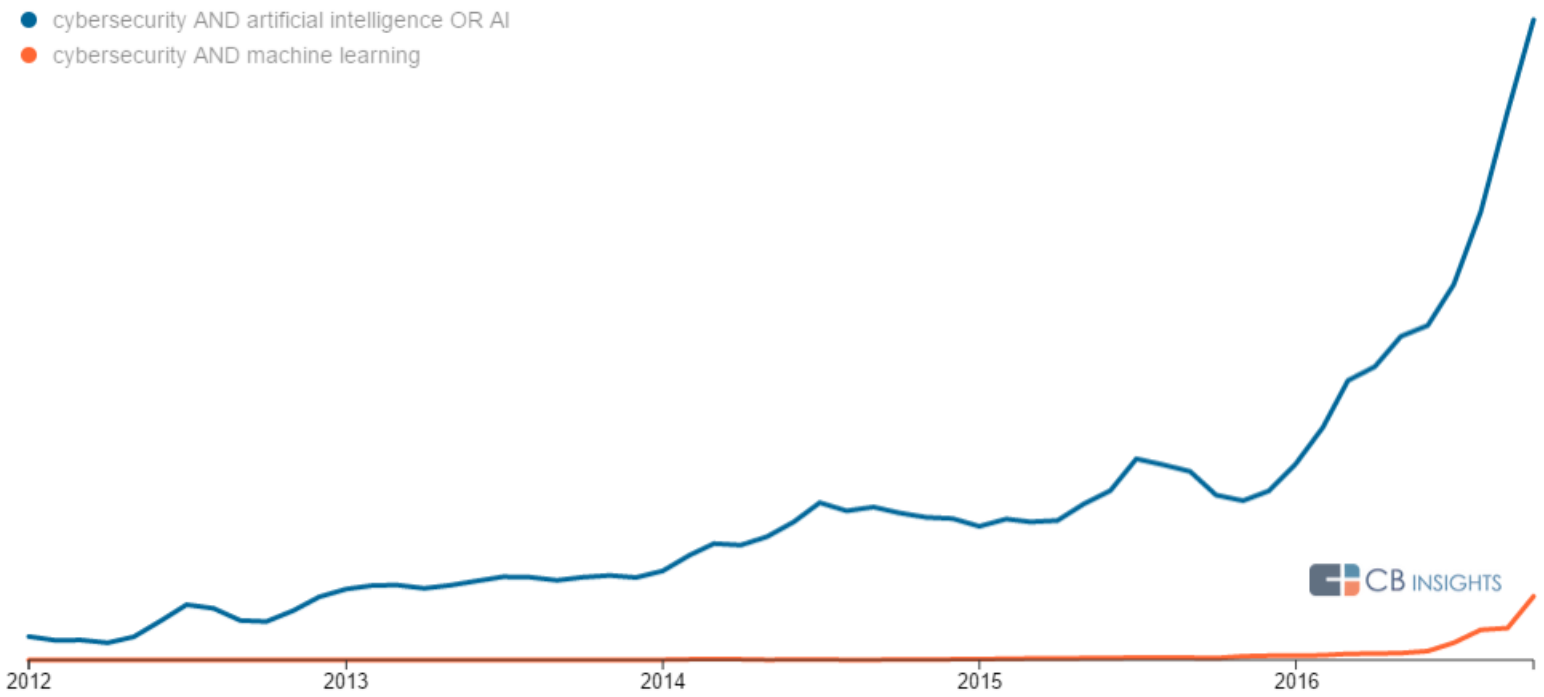
- The development of computer systems that are able to perform human like tasks
- Recognizing speech, reading text, translating languages, finding patterns

Machine Learning

- Subfield of Artificial Intelligence that involves methods to make machines learn using data without explicitly programming
- Think about how you would teach a machine or child to read the letter A

Cognitive Computing

- Simulation of human thought process with an ability to reason and contextualize
- How does a journalist decide which story is worth writing, an analyst making a recommending, a lawyer deciding which cases to cite.


cybersecurity AND artificial intelligence OR AI
cybersecurity AND machine learning
CB INSIGHTS
2012
2013
2014
2015
2016

AI toolkit

Finding Information

- Search
- Recommendation
- Question Answering
- Outlier detection

Analyzing

- Classifiers
- Clustering
- Statistical learning methods
- Entity Resolution

Decision Making

- Predictive Analytics

What can be done to reduce risk?

- Define an information security policy
- Classify your data
- Determine if there are regulatory requirements
- Define who needs what level of access
- Critically assess your on-prem security is compared to that of a cloud provider
- Security-first training & education programs

Applicability to Data Breaches

- 50% of data breaches remain undiscovered for months[4]
- Bad actors only need a few minutes to gain access to critical data.
- Historically crafting and subsequently detecting threat signatures was the most common approach
- However, they are useless with the rise of point and click exploit kits since attackers create unique (previously unseen) signatures for each attack

What do we need to be doing

- We need to utilize self-learning analytics and anomaly detection techniques to monitor activity across multiple network assets and real-time data streams in order to identify threats as they occur without having specific knowledge of the exact signature.
- These analytics immediately detect anomalies in network traffic and data flows, while also quickly recognizing new “normal” activity, thus minimizing false-positive alerts.
- Temporal Topic modeling example

Any Challenges with this approach

- Scale
- Sometimes minute changes
- Scattered data
- AI is not foolproof (adverse examples used to make an image recognition engine think that it's seeing an ostrich when it's actually seeing a building: http://karpathy.github.io/2015/03/30/breaking-convnets/)
- Random noise can be added to images to break image processing networks, even though the noise is barely visible to human eyes. https://arxiv.org/pdf/1607.02533v2.pdf

What problems could machine learning & AI solve for cybersecurity?

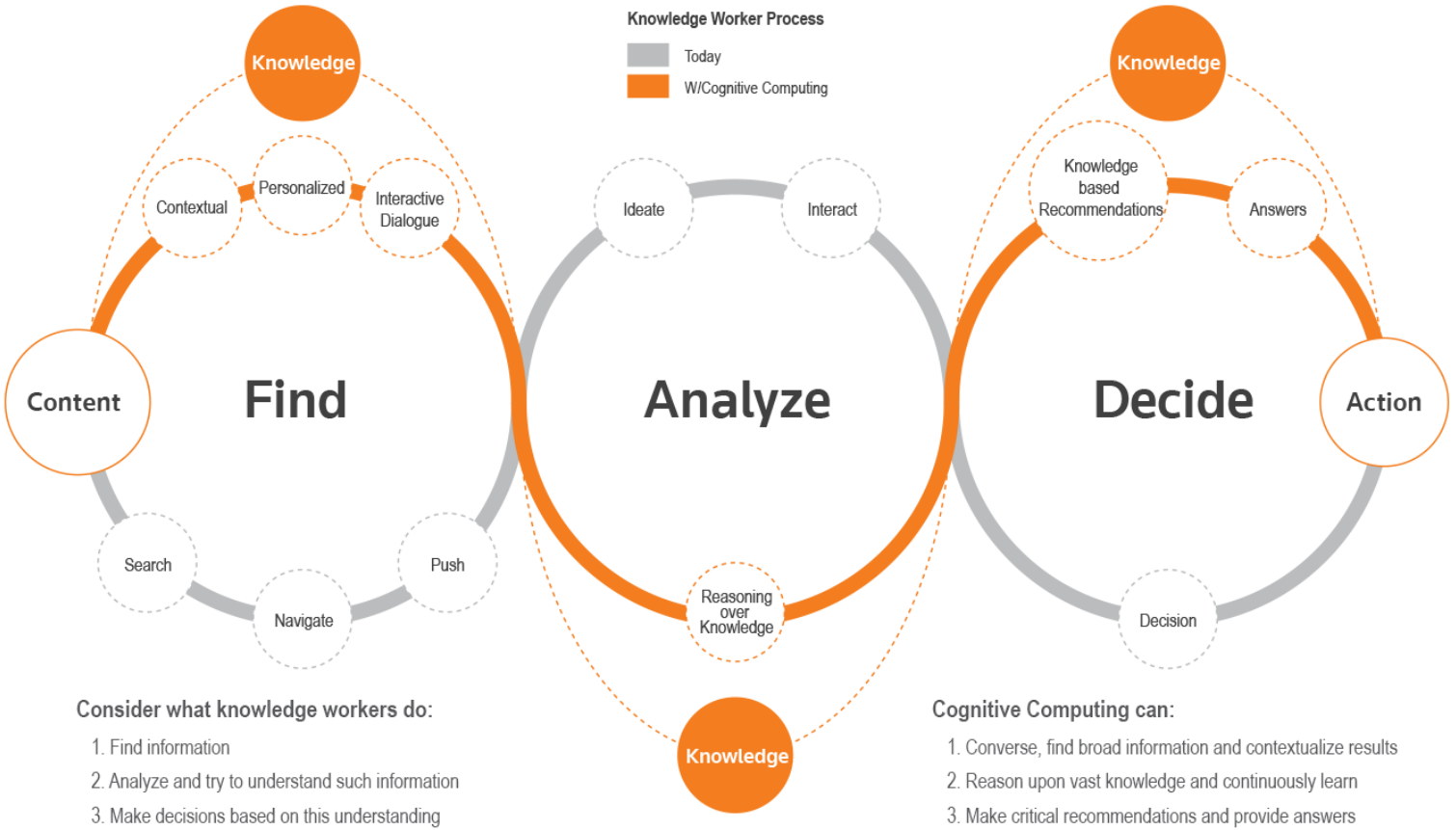
- Overcome the “big data problem”
- Assess data security regardless of location
- Oversee compliance with laws & regulations
- Supplement skills shortage
- Prepare to counter hacker use of AI

Who is building cybersecurity AI solutions?

What’s next …

Knowledge work

- Knowledge work can be differentiated from other forms of work by its emphasis on "non-routine" problem solving that requires a combination of convergent, divergent, and creative thinking. – Wikipedia

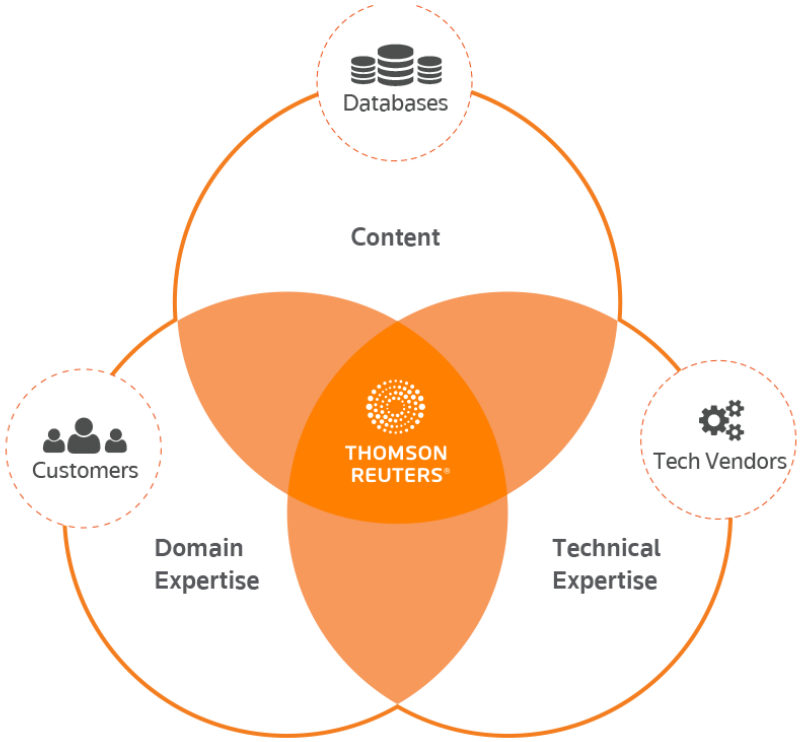


Consider what knowledge workers do:

1. Find information
2. Analyze and try to understand such information
3. Make decisions based on this understanding

Cognitive Computing can:

1. Converse, find broad information and contextualize results
2. Reason upon vast knowledge and continuously learn
3. Make critical recommendations and provide answers

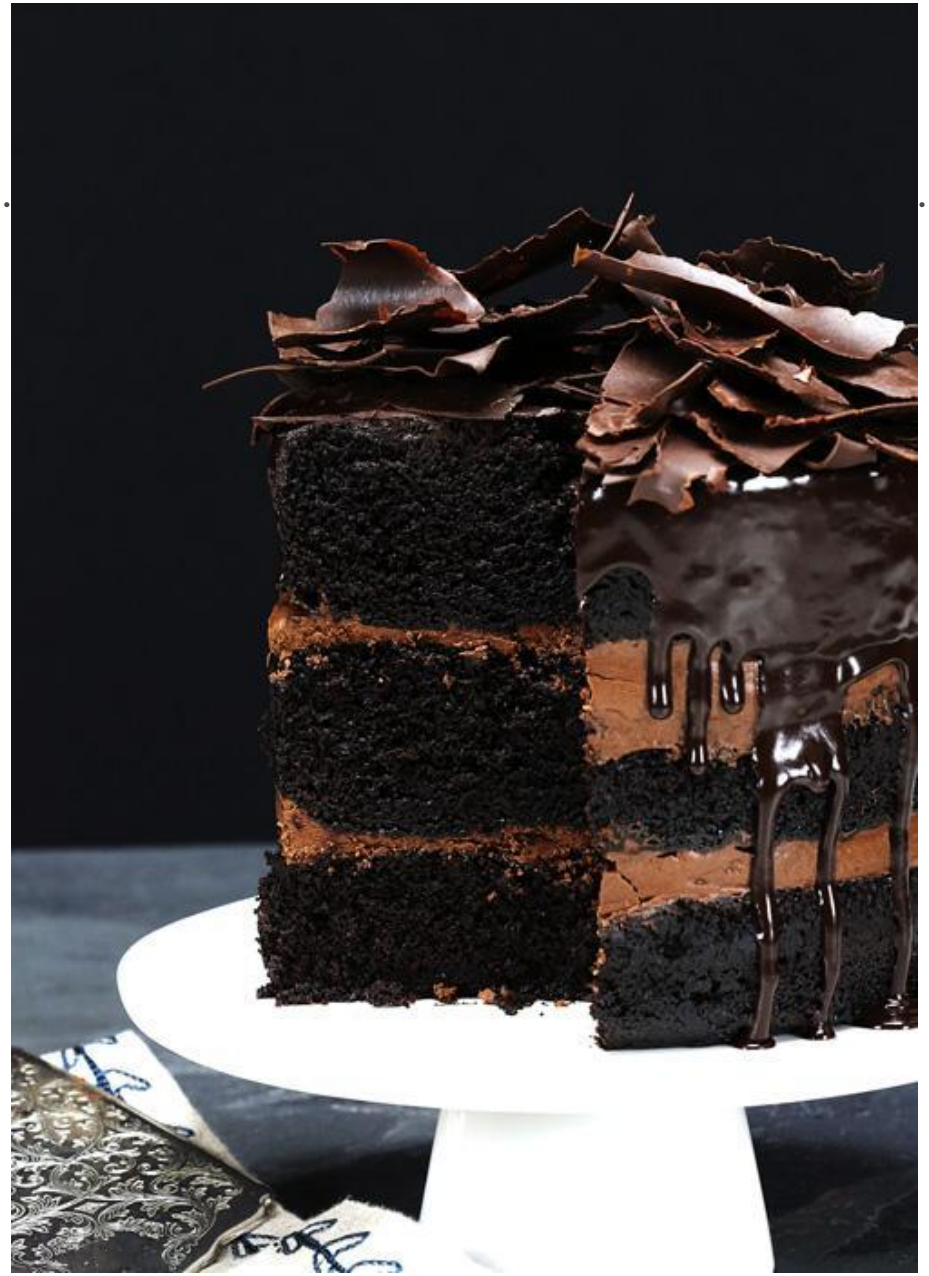

Databases
Content
Customers
THOMSON
REUTERS®
Tech Vendors
Domain
Expertise
Technical
Expertise

Resources:

1. "AI Is the Future of Cybersecurity, for Better and for Worse" – HBR, May 8, 2017
2. "Is Cybersecurity a Second Coming for AI?" – Forbes May 23, 2017
3. 100 Startups Transforming Industries with AI
4. Verizon report on Data Breaches

Thank you for attending !


granulated sugar
dutch-processed cocoa powder
DRY
INGREDIENTS
baking powder
salt
baking soda
all-purpose flour
WET
INGREDIENTS
canola oil
large eggs
buttermilk
brewed coffee
vanilla extract
semi-sweet chocolate



THOMSON REUTERS