

2017 Government
Analytics Forum
Transforming Government
in the Cognitive Era



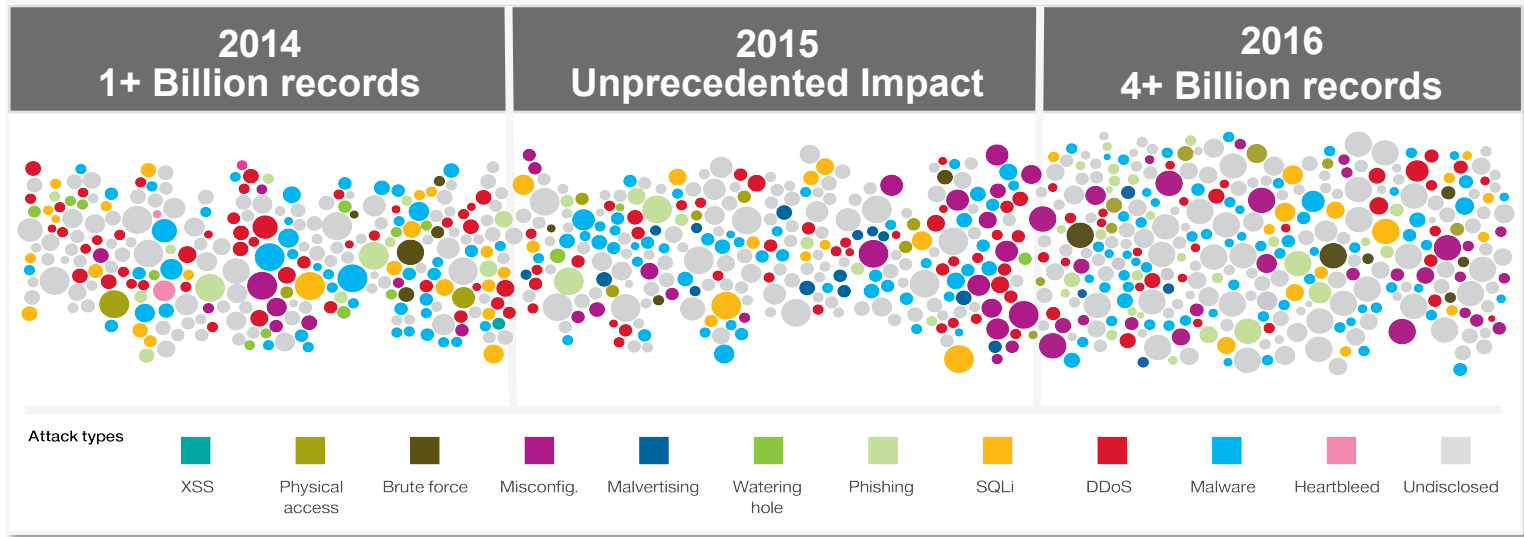
Cyber Threat Intelligence for Defense

Dr. Charles Li, CTO, GBS Cyber Security and
Biometrics, IBM

Bruce Cerretani, Federal Lead Solution Architect, IBM

#GOVANALYTICS2017

Cyber attackers break through conventional safeguards every day



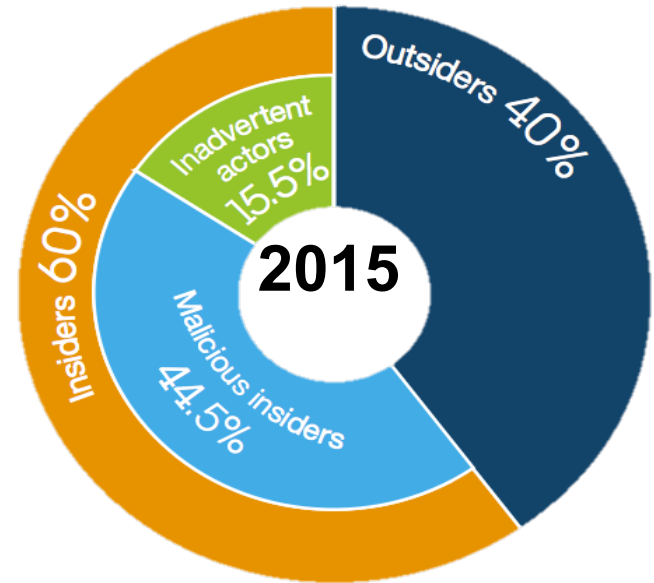
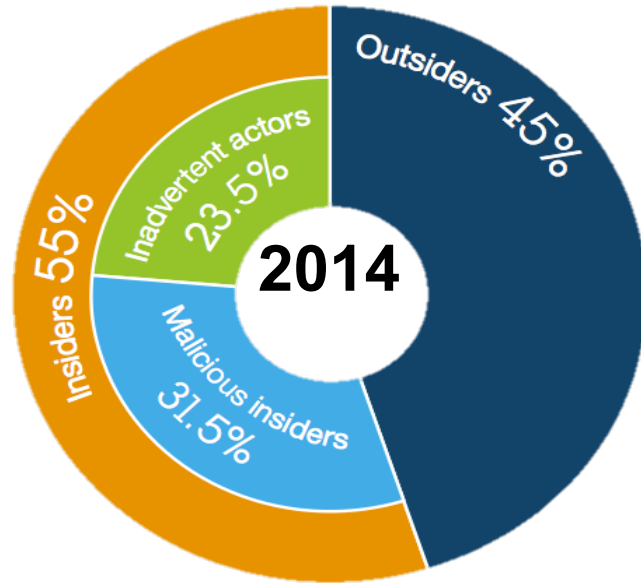
average time to identify data breach

201 days

average cost of a U.S. data breach

\$7 M

Who is attacking?



The majority of all attacks in 2014 and 2015 were carried out by **INSIDERS** ... in other words by **people you are likely to trust**.

Traditional security practices are unsustainable

85  security tools from

45  vendors

1.5 **MILLION** unfilled security positions by 2020

68 **PERCENT** of CEOs are reluctant to share incident information externally



Core concepts

#1 For Project Managers: Cybersecurity is about mission and cost effectiveness

Current State of Cybersecurity



CYBERSECURITY

We have limited resources and our end users don't fully appreciate the threats we face.

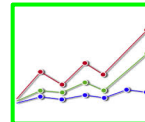
Desired State of Cybersecurity



Reducing Cost



Increasing Quality



Measurable Results

Improved Cyber Defense

Core concepts

#2 For Practitioners: One Pane of Glass providing actionable information

Current State of Cybersecurity



MONITOR FATIGUE

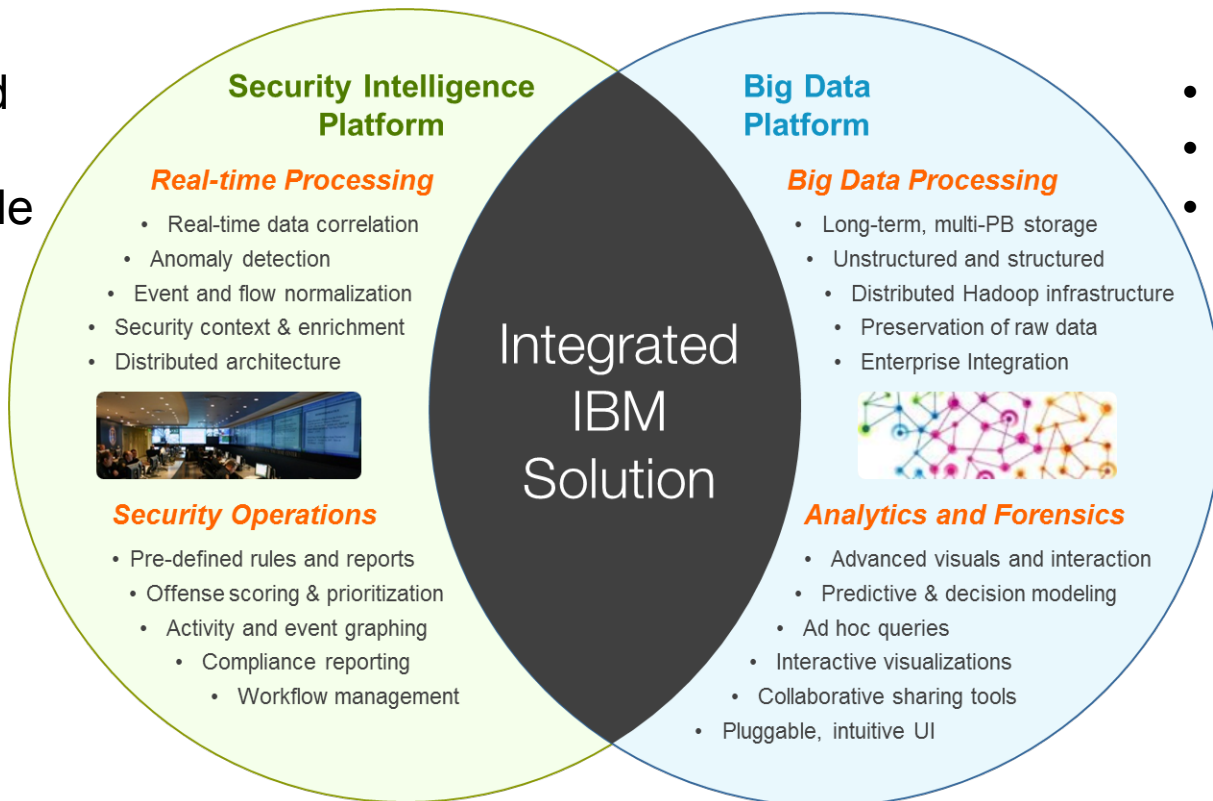
The last thing we need is yet another system to worry about.

Desired State of Cybersecurity



Integrated security, analytics and exploration

- Structured
- Analytical
- Repeatable



- Flexible
- Exploratory
- Ad-Hoc

Cognitive computing: A new capability for the new challenges

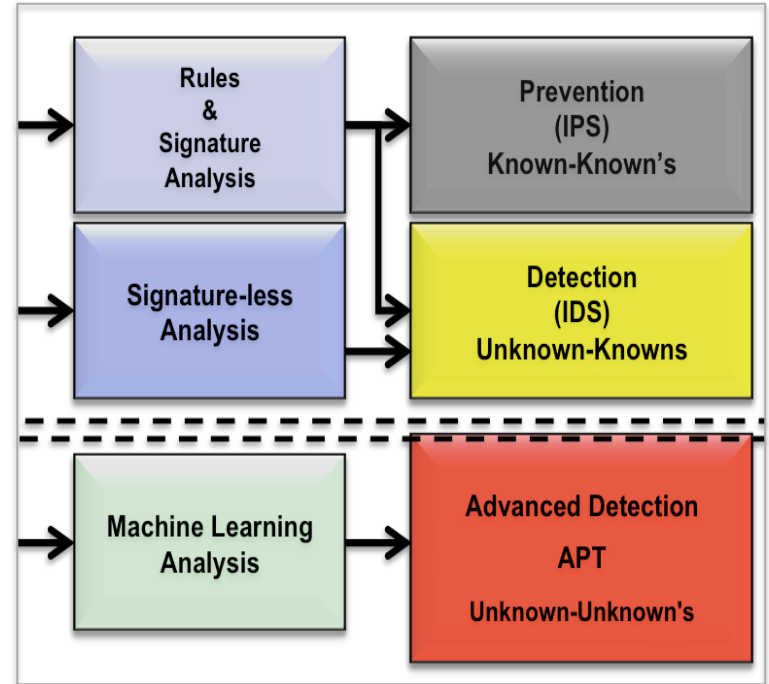


There are **known knowns**; there are things we know we know.

We also know there are **known unknowns**; that is to say we know there are some things we do not know.

But there are also **unknown unknowns**; there are things we do not know we don't know.

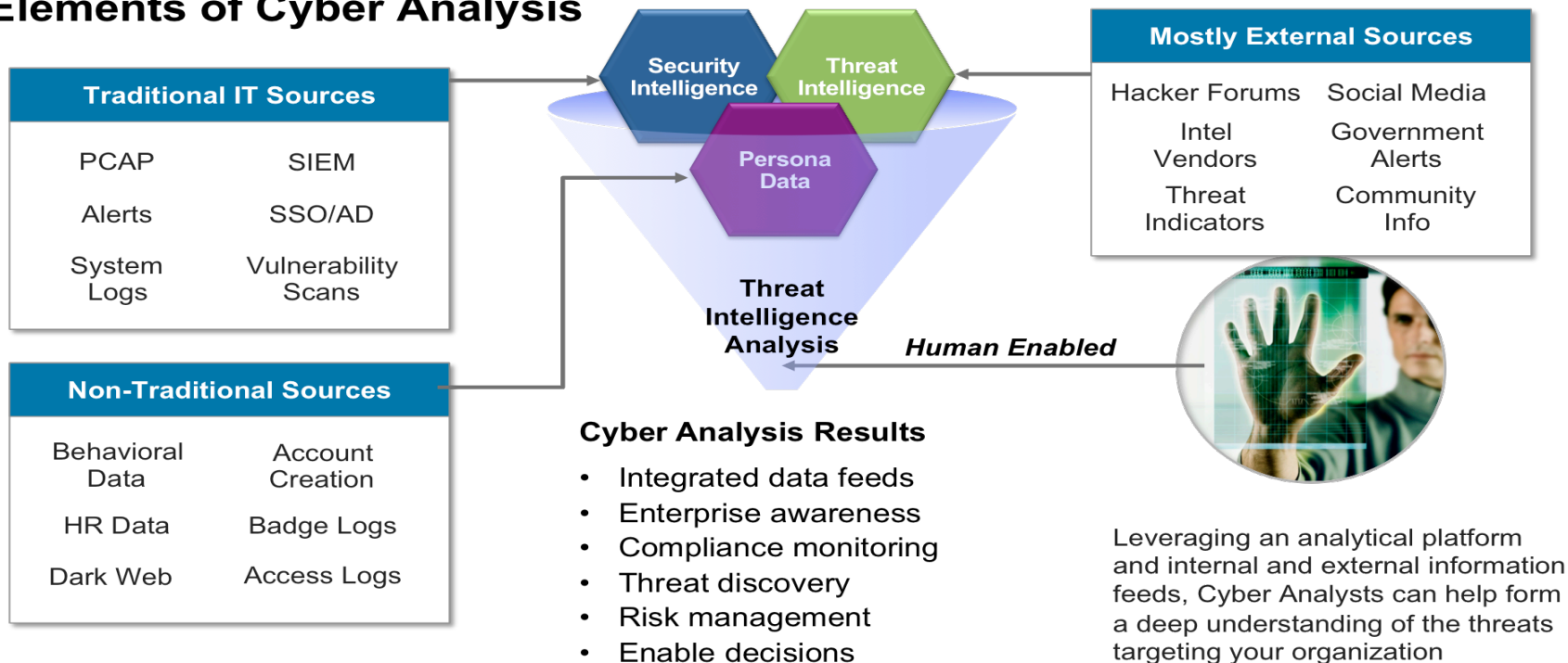
Donald Rumsfeld, US Secretary of Defense, Feb 2002



Today's Defense in Depth: Highly centric around Rules & Signatures based detection with non consistent use of advanced machine learning

Cognitive computing: A new capability for a holistic approach

Elements of Cyber Analysis



13

Most SIEM **INDICATORS** : do not consider non-traditional cyber sources to enrich their situational awareness and detection capabilities and provide little advise on how to deal with an attack

Cognitive computing models

The three fundamental models of Cognitive Computing...



MACHINES THAT LEARN OVER TIME

Extensive employment of agents that are based on Deep Learning methods and techniques trained to emulate the methods



MACHINES THAT INTERACT WITH HUMANS

Machines that can either respond to human stimulus or autonomously interaction with humans in a natural conversational manner that mimics human behavior and interaction



HUMAN COGNITIVE AUGMENTATION

Intelligence amplification (IA) (also referred to as cognitive augmentation and machine augmented intelligence) refers to the effective use of information technology in augmenting human intelligence

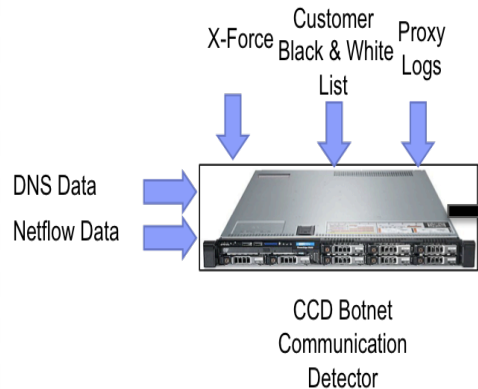
Cognitive computing changes the defense in depth landscape in a fundamental way

- Employment of advanced Machine Learning techniques that self learn to **adapting** threat attack vectors and tradecraft
- Utilizing and deriving insight from **non-traditional** cyber sources to **augment** classical Cyber detection and Intelligence analysis
- **Intuitive** and **human** like Natural Language interfaces that CISO's and SOC analyst can derive **Intelligence**
- Ability to ingest and analyze **massive** amounts of real-time and historical
- Providing real-time recommendation and courses of action to **remediate and minimize** cyber attacks



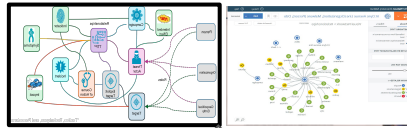
Addressing the cyber challenge with advanced machine learning, analytics and cognitive computing

Cognitive



Machine Learning
Advanced Low Observable
Detection Appliance

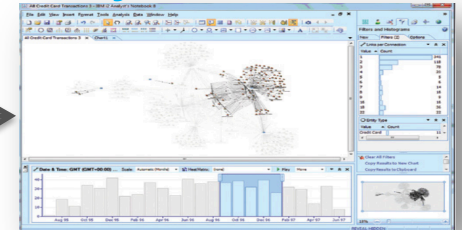
Knowledge Graphs



Security Intelligence Platform

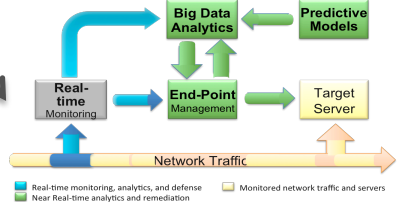
Watson for Cyber Security offers Deep Learning, Cognitive Cyber Intelligence

Analytics



Cyber Entity Resolution
Attacker Attribution-Correlation
Intelligence

Advanced Cyber Analytics (ACA)



Cyber Forensic Analysis and Remediation

As a result ...

Cyber analysts are overwhelmed with the amount of data – that's beyond human capabilities

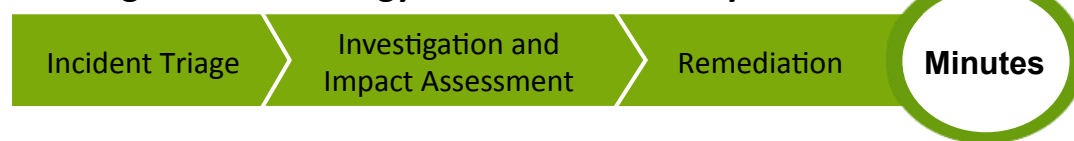
Cognitive Technology can now:

- Process this data and correlate cyber SIEM/Sensor data with cyber text
- Respond to threats with greater confidence at speed and scale
- And out think and outpace cyber threats

Manual threat analysis



IBM Cognitive Technology assisted threat analysis



2017 Government
Analytics Forum
Transforming Government
in the Cognitive Era



THANK YOU

QUESTIONS?

#GOVANALYTICS2017