IBM Watson™

IBM Security

IBM®

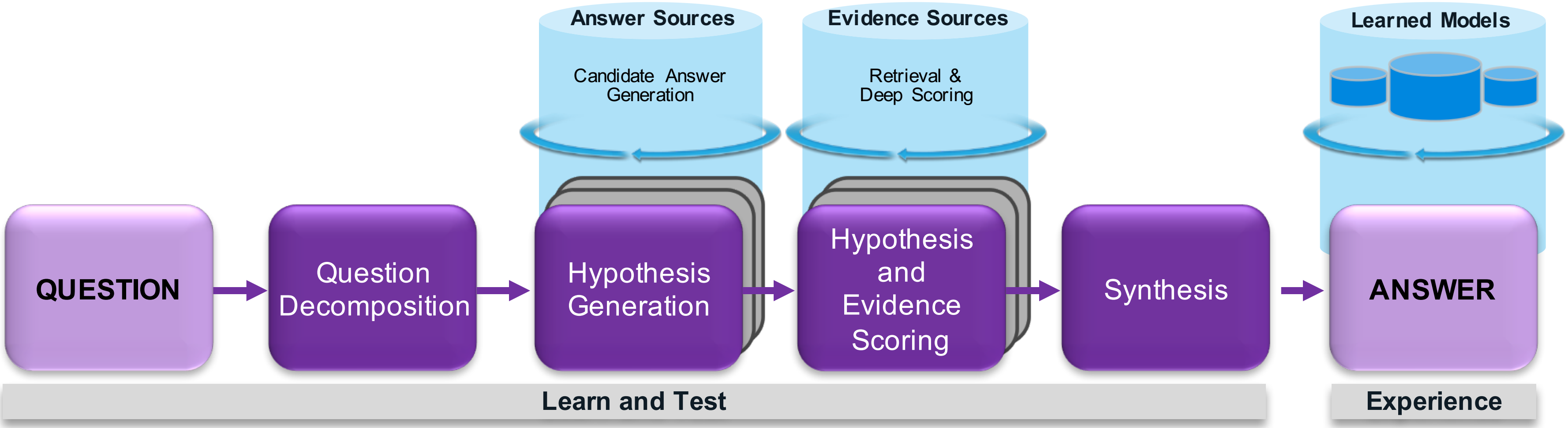
Security and Risk in the Cognitive Era

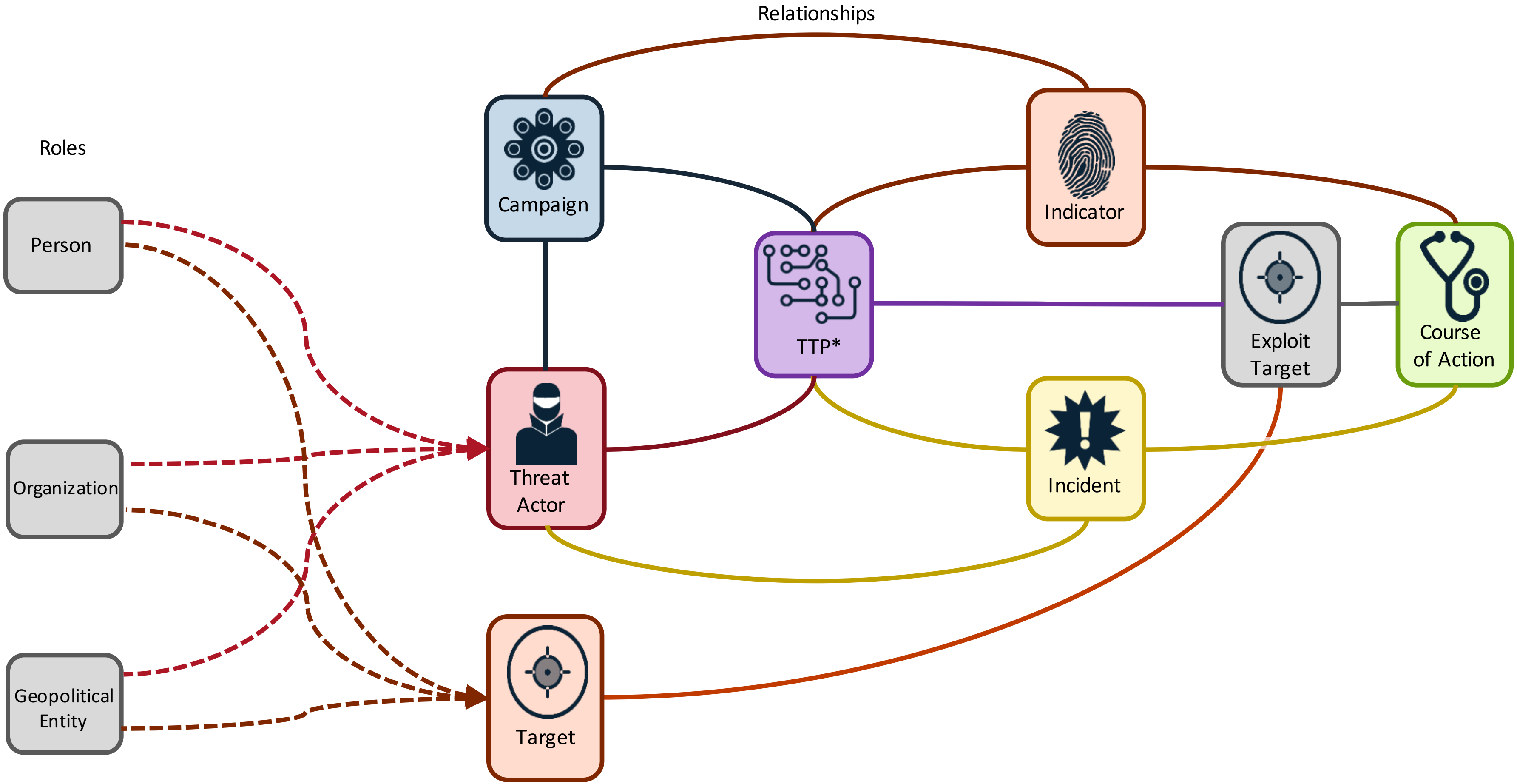
Jeb Linton
IBM Watson Chief Security Architect

Cognitive Security: Use of Cognitive Computing to augment existing Security technology with an *understanding of formerly opaque unstructured data*.

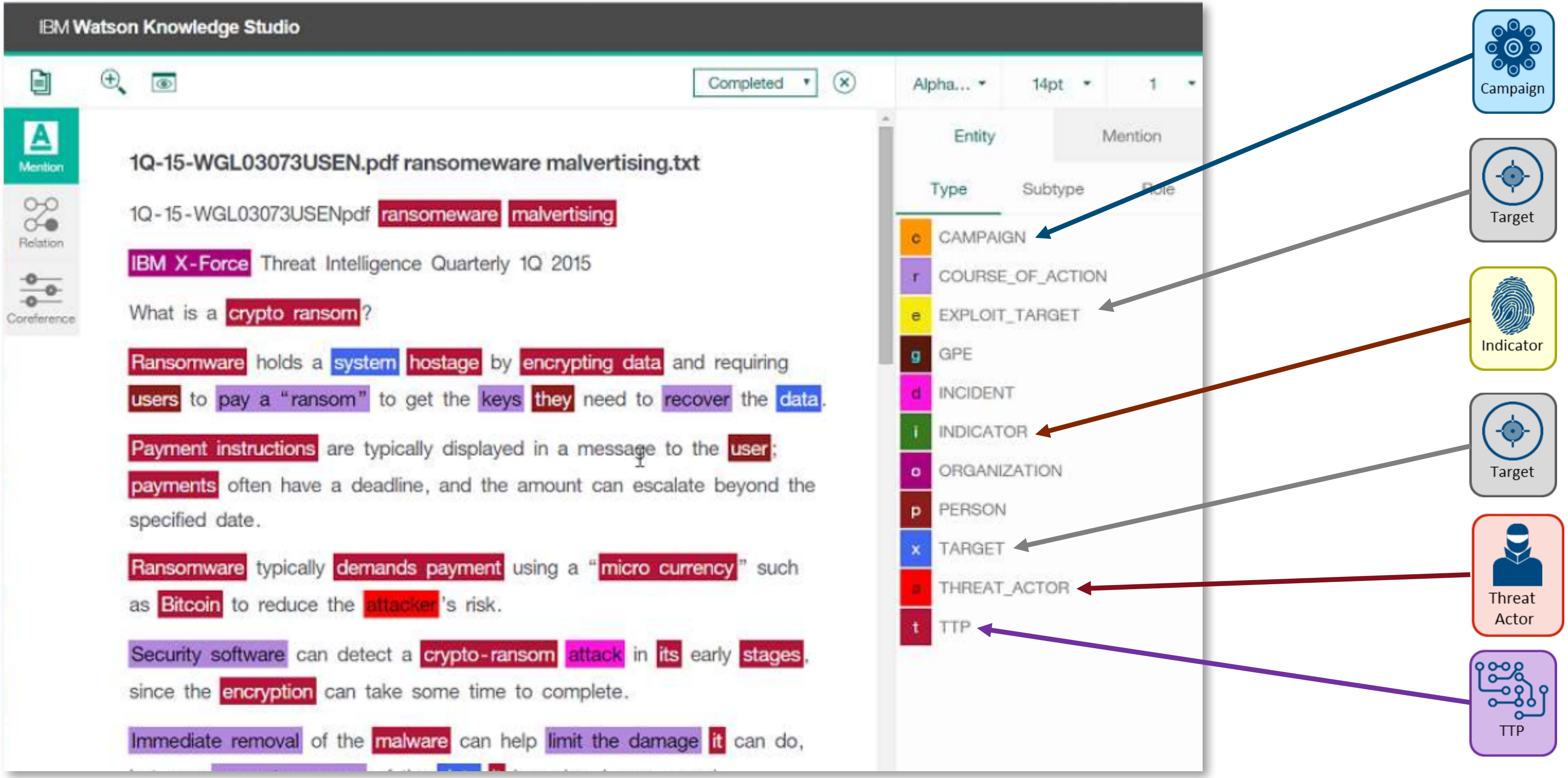
- **DMZ Firewall**: Multiple denies, same source
- **Proxy**: Invalid authentication attempt
- **RAS**: Multiple failed login attempts followed by success
- **AD**: User **[Researcher]** logged in
- **NetFlow**: Traffic detected from RAS to sensitive data stores
- **Database**: User **[Researcher]** accessed and exported data
- **Proxy**: High volume transfer to external destination

- **IBM MSS**: The password-stealing function of Dyre is the focus…
- **Blogspot**: We're seeing an unrecognized phishing attack using…
- **LinkedIn**: **[BadActor]** and **[Researcher]** are now connected
- Facebook: **[Researcher]** I think my accounts were hacked – be careful friends!
- **IRC**: Thanks for all the advice on social engineering!
- **Darkweb**: Who wants to buy these designs? Bidding starts now.


Answer Sources
Candidate Answer Generation
Evidence Sources
Retrieval & Deep Scoring
Learned Models
QUESTION
Question Decomposition
Hypothesis Generation
Hypothesis and Evidence Scoring
Synthesis
ANSWER
Learn and Test
Experience



*Tactics, Techniques, and Procedures



IBM Watson Knowledge Studio

Completed

Alpha... 14pt 1

Mention

Relation

Coreference

1Q-15-WGL03073USEN.pdf ransomeware malvertising.txt

1Q-15-WGL03073USENpdf ransomeware malvertising

IBM X-Force Threat Intelligence Quarterly 1Q 2015

What is a crypto ransom?

Ransomware holds a system hostage by encrypting data and requiring users to pay a "ransom" to get the keys they need to recover the data.

Payment instructions are typically displayed in a message to the user; payments often have a deadline, and the amount can escalate beyond the specified date.

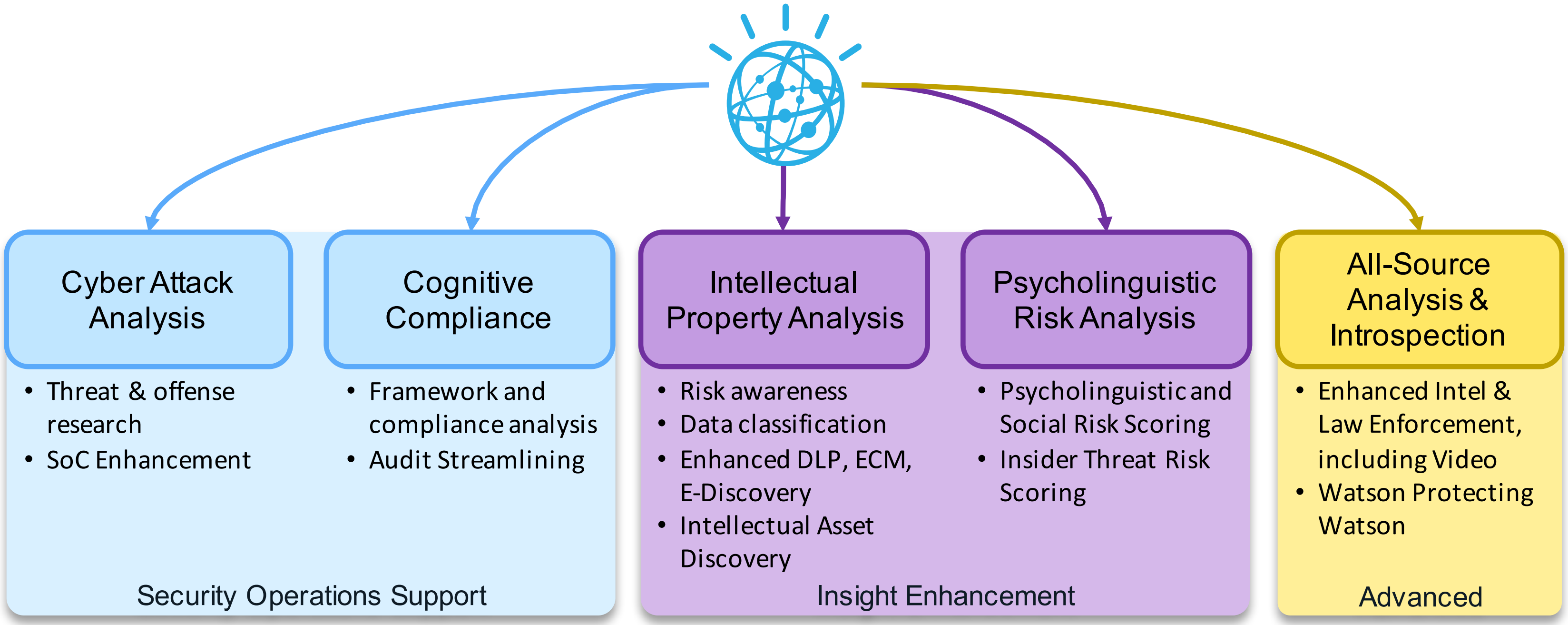
Ransomware typically demands payment using a "micro currency" such as Bitcoin to reduce the attacker's risk.

Security software can detect a crypto-ransom attack in its early stages, since the encryption can take some time to complete.

Immediate removal of the malware can help limit the damage it can do,

Entity	Mention

Type	Subtype	Role
c	CAMPAIGN	
r	COURSE_OF_ACTION	
e	EXPLOIT_TARGET	
g	GPE	
d	INCIDENT	
i	INDICATOR	
o	ORGANIZATION	
p	PERSON	
x	TARGET	
a	THREAT_ACTOR	
t	TTP	



Cyber Attack Analysis

- Threat & offense research
- SoC Enhancement

Cognitive Compliance

- Framework and compliance analysis
- Audit Streamlining

Security Operations Support

Intellectual Property Analysis

- Risk awareness
- Data classification
- Enhanced DLP, ECM, E-Discovery
- Intellectual Asset Discovery

Psycholinguistic Risk Analysis

- Psycholinguistic and Social Risk Scoring
- Insider Threat Risk Scoring

Insight Enhancement

All-Source Analysis & Introspection

- Enhanced Intel & Law Enforcement, including Video
- Watson Protecting Watson

Advanced

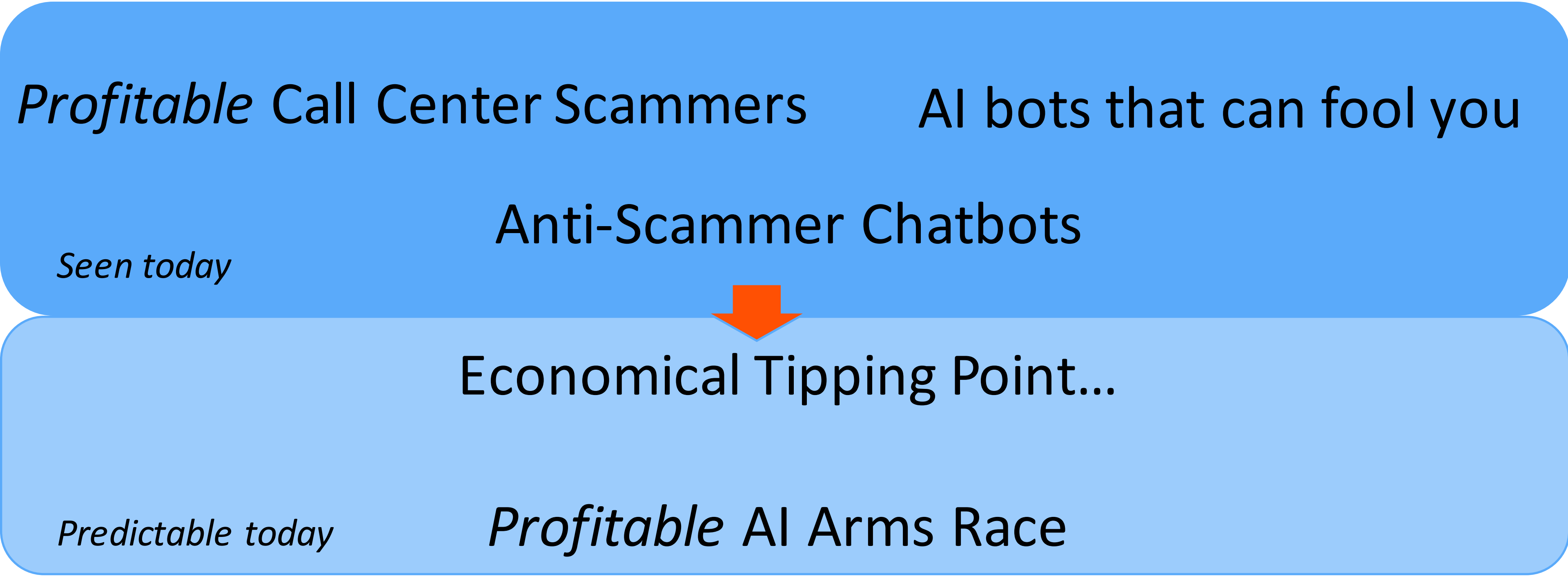
**Watson is capable of all functionality today via custom engagement - estimated timeline is for turnkey service availability

Profitable Call Center Scammers

AI bots that can fool you

Anti-Scammer Chatbots

Seen today



Profitable Call Center Scammers

AI bots that can fool you

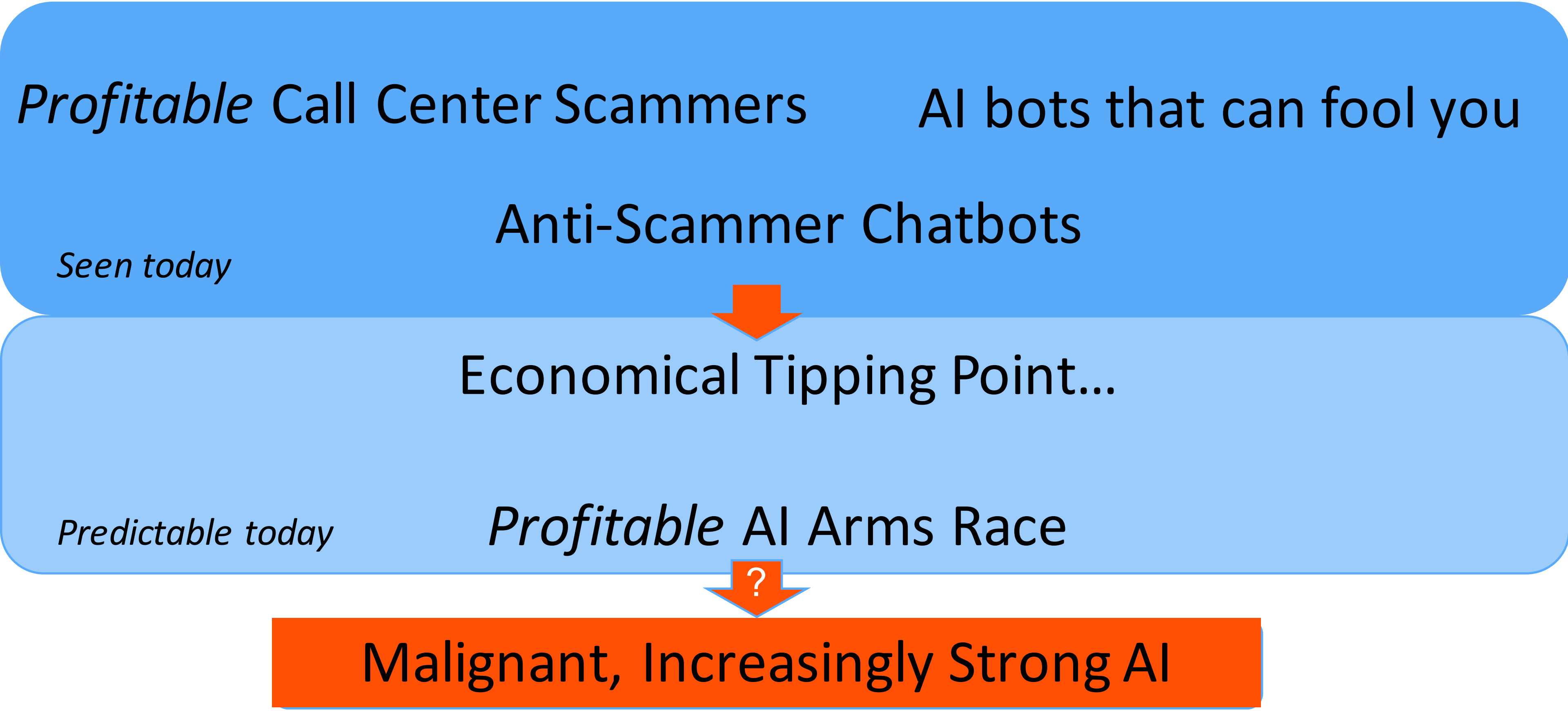
Anti-Scammer Chatbots

Seen today

Economical Tipping Point…

Predictable today

Profitable AI Arms Race



Profitable Call Center Scammers

AI bots that can fool you

Anti-Scammer Chatbots

Seen today

Economical Tipping Point…

Predictable today

Profitable AI Arms Race

?

Malignant, Increasingly Strong AI

IBM Watson™

IBM Security

IBM®

THANK YOU

www.ibm.com/security
www.ibm.com/watson

The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and / or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANYSYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.