Security and Risk in the Cognitive Era

Jeb Linton
IBM Watson Chief Security Architect
• **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.
Candidate Answer Generation

Retrieval & Deep Scoring

Hypothesis and Evidence Scoring

Synthesis

Learned Models

Learn and Test

Experience
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.
Insight Enhancement

Cyber Attack Analysis
- Threat & offense research
- SoC Enhancement

Cognitive Compliance
- Framework and compliance analysis
- Audit Streamlining

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

All-Source Analysis & Introspection
- Enhanced Intel & Law Enforcement, including Video
- Watson Protecting Watson

Security Operations Support

**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

Economical Tipping Point...

Profitable AI Arms Race
Profitable Call Center Scammers - AI bots that can fool you

Anti-Scammer Chatbots

Economical Tipping Point...

Profitable AI Arms Race

Malignant, Increasingly Strong AI