

# IBM Watson Cognitive Cyber Security

SECURITY FOR A NEW ERA OF COMPUTING

OUTTHINK THREATS WITH SECURITY THAT UNDERSTAND, REASONS AND LEARNS



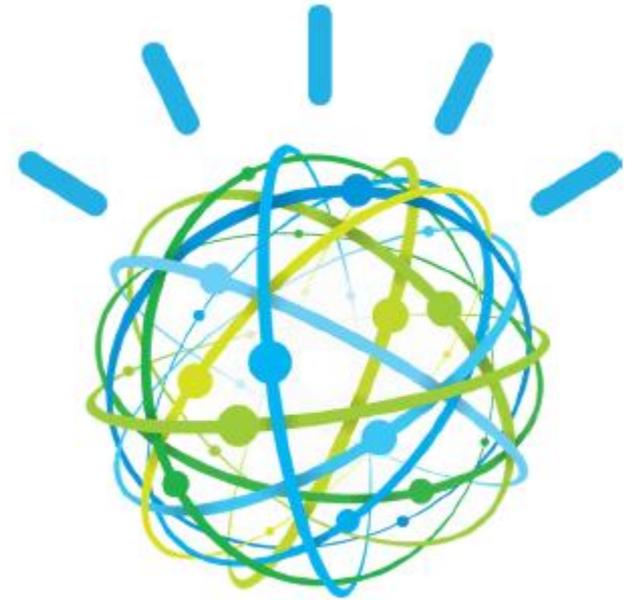
**Mauro Proserpio**

IBM Distinguished Engineer

# Introducing... IBM Watson *for Cyber Security*

## Unlock new possibilities.

The world's first Cognitive analytics solution using core Watson technology to help analysts understand, reason, and learn about security topics and threats.



**ARMONK, NY – May 10, 2016** – IBM Security today announced Watson for Cyber Security, a new cloud-based version of the company's cognitive technology trained on the language of security as part of a year-long research project.

# Today's security drivers



# Cognitive is ushering in a new era of Security

- **Perimeter controls:** security that confines.

Pre- 2005



- This kept data secure by restricting access, yet started to prove ineffective as hackers found workarounds.

- **Security intelligence:** security that helps you think.

2005 +



- This includes real time monitoring of how data is accessed – and by whom. Analytics are then used to detect deviations, helping security experts address the biggest issues first.

- **Cognitive Security:** security that understands, reasons and learns.

2015 +



- Security intelligence is no longer enough, as it can only identify and prioritize known threats, not emerging ones. Cognitive Security fills the gap by making sense of the 80% of data that's unstructured – available in thousands of research reports, conference materials, academic papers, news articles, blog posts, industry alerts and more.

# A tremendous amount of security knowledge is created for human consumption, but most of it is untapped

## Traditional Security Data

- Security events and alerts
- User and network activity
- Logs and configuration data
- Threat and vulnerability feeds

## Human Generated Knowledge



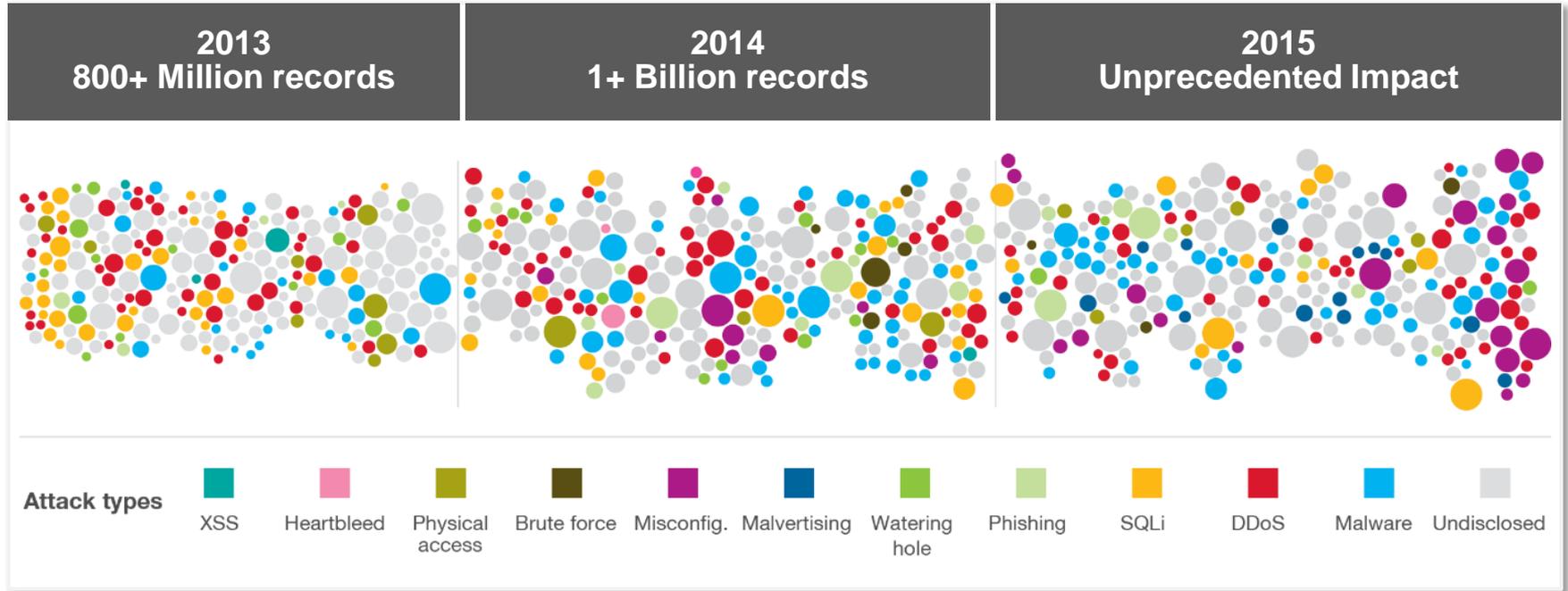
## A universe of security knowledge Dark to your defenses

Typical organizations leverage only 8% of this content\*

Examples include:

- Research documents
- Industry publications
- Forensic information
- Threat intelligence commentary
- Conference presentations
- Analyst reports
- Webpages
- Wikis
- Blogs
- News sources
- Newsletters
- Tweets

# Security: A Big Natural Language Data Problem



- Thousands of textual vulnerability descriptions
- Thousands of security bulletins and articles
- Hundreds of Security and Bad Actor forums, social media
- Rich language and technical jargon

**IBM Watson is an ideal solution set to augment Security Intelligence**

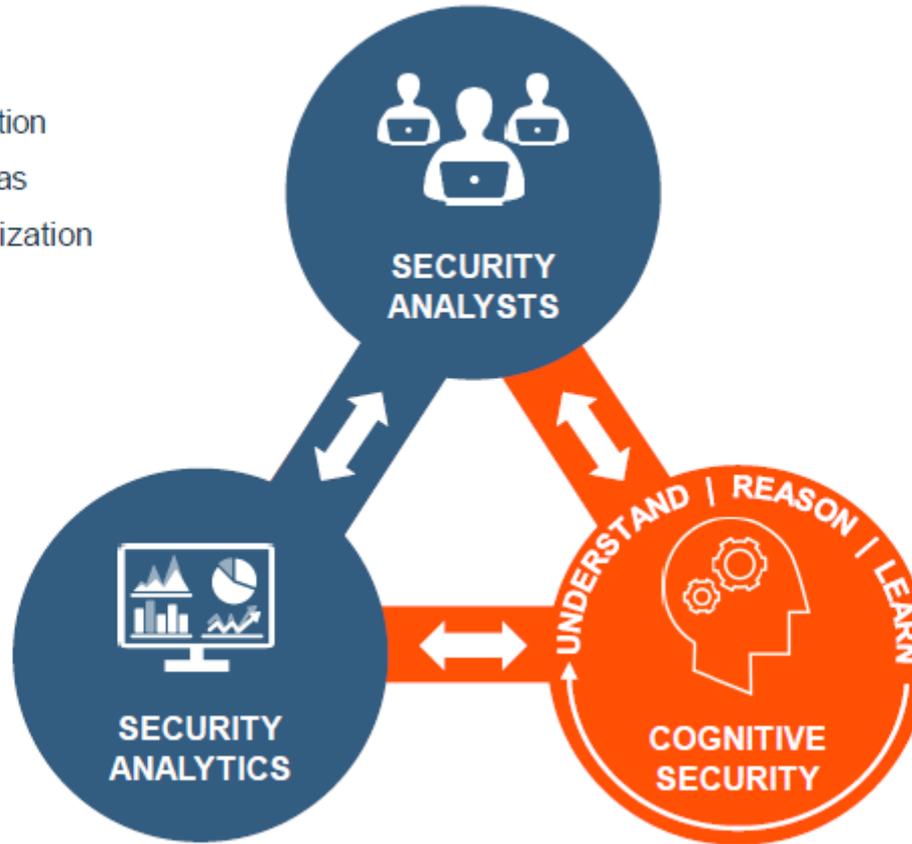
# Cognitive systems bridge this gap and unlock a new partnership between security analysts and their technology

## Human Expertise

- Common sense
- Abstraction
- Morals
- Dilemmas
- Compassion
- Generalization

## Security Analytics

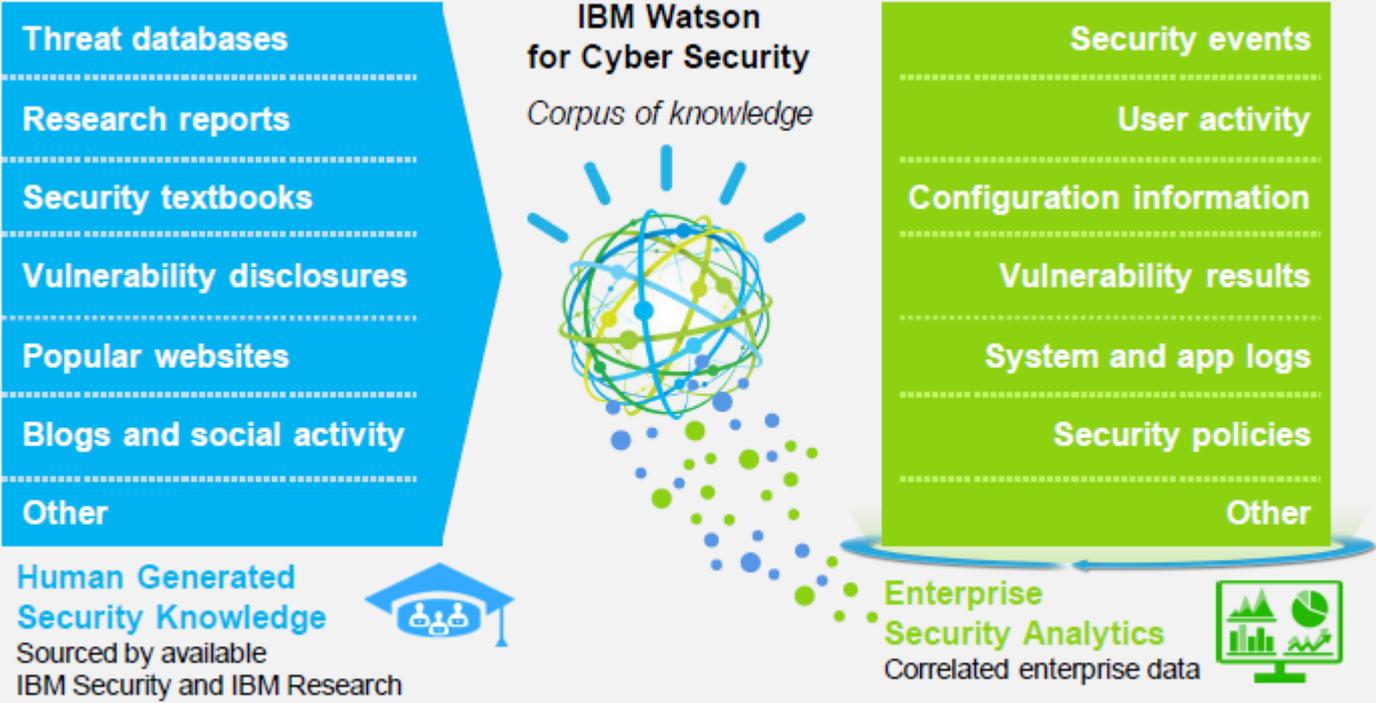
- Data correlation
- Pattern identification
- Anomaly detection
- Prioritization
- Data visualization
- Workflow



## Cognitive Security

- Unstructured analysis
- Natural language
- Question and answer
- Machine learning
- Bias elimination
- Tradeoff analytics

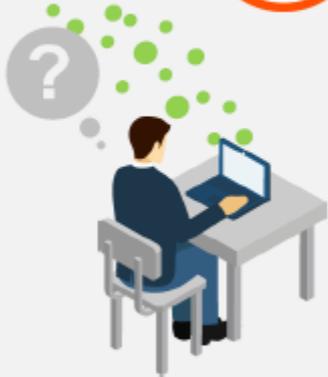
# IBM Watson enables great insights by ingesting extensive data sources



# Cognitive: revolutionizing how security analysts work

## SECURITY ANALYST

Enterprise  
Security  
Analytics



## SECURITY ANALYST and WATSON

Enterprise  
Security  
Analytics



Human Generated  
Security  
Knowledge



Cognitive Security

### Gain powerful insights

- Tap into the vast array of data to uncover new patterns
- Get smarter over time and build instincts

### Reduce the security skills gap

- Triage threats and make recommendations with confidence, at scale and speed

### Save time and costs

- Handle mass minutiae, so you can work on offense not endless defense



# IBM Watson provides evidence for effective analysis reducing the resolution time and resources

The screenshot displays the IBM QRadar Security Intelligence interface. The main view shows a network diagram for 'Offense: 8324'. A blue callout box states: 'QRadar has determined malware family or campaign may be related to the offense and 3 other hosts in your networks appear to be affected. QRadar has also found these additional indicators possibly related to the incident containing 14 Domains, 130 IP Addresses, 7 Geographies, 8 file HASHes'. The diagram includes nodes for 'xfyubqmidwvuyar.yt', 'scorpena.com/86546vb.exe', '10.103.25.30', '10.12.1.32', '20.132.23.11', '20.132.23.12', '20.132.23.13', 'yearend.xls', '178.212.251.32', and 'pwinlrmwccuo.eu'. A red circle with 'A' labeled 'Locky' is connected to several nodes.

Overlaid on the right is a detailed incident analysis panel for 'Incident 8324' titled 'Suspicious Action from Document'. It features a 'Send to Resilient' button and tabs for 'Overview', 'Sources (1)', 'Destinations (1)', 'Notes (0)', and 'Watson'. The 'Overview' tab shows:

- Attack Campaigns: 1 (Locky)
- Documents Found: 42
- Domains Implicated: 14
- Hosts Involved: 4

The 'Watson Insights' section contains the same callout text as the main interface. The 'Supporting Details' section includes a table:

Name	Created	Data Sources Reporting
Locky	Mar 23, 2016 4:22 PM	

Watson determines the specific campaign (Locky), discovers more infected endpoints, and sends results to the incident response team

# Cognitive Security Use Cases

## Enhance your SOC analysts

Cognitive systems can understand a vast sea of structured and unstructured data, to help quickly move the value of a junior analyst from a level 1 to a 2 or 3. Cognitive systems can automate ingesting information – such as research reports and best practices – to give real-time input. Previously, this knowledge and insight could only be obtained from years of experience.

## Speed response with external intelligence

When the next Heartbleed hits, people will blog about how to protect yourself from it. Even though a signature is not available yet, there is natural language online that can help you answer the question. Cognitive systems can crawl to quickly discover how to protect against the next zero-day exploit.

## Identify threats with advanced analytics

Cognitive systems may use analysis methods such as machine learning, clustering, graph mining and entity relationship modelling to identify potential threats. They can help speed detection of risky user behaviour, data exfiltration and malware detection before damage occurs.

## Strengthen application security

Cognitive systems can understand the semantic context of your analytics and data, while exploring code and code structures. They can take thousands of vulnerability findings and refine results to a small set of actionable items – and take you to locations in your code where you can fix them.

## Improve enterprise risk

In the future, cognitive systems could analyze corpuses of interactions, the nature of those interactions and their susceptibility to develop risk profiles for organizations, corporate actions, training and re-education. Cognitive systems could use natural language processing to find sensitive data in an organization and redact it.

## Conclusion... IBM Watson *for Cyber Security*

# Cognitive security

Evolve your defenses with security that understands, reasons and learns

Cognitive ultimately plays into a framework built on the basics of traditional security. Security intelligence is not going away; it's a key building block of cognitive security. What cognitive does is gives us a way to triage threat intelligence and detection, and provide actionable information, at a speed and scale like never before.

<http://www-03.ibm.com/security/cognitive/>

<http://www-03.ibm.com/security/>



# THANK YOU

## FOLLOW US ON:

 [ibm.com/security](https://ibm.com/security)

 [ibm.com/security/cognitive/](https://ibm.com/security/cognitive/)

 [@ibmsecurity](https://twitter.com/ibmsecurity)

 [youtube.com/user/ibmsecuritysolutions](https://youtube.com/user/ibmsecuritysolutions)

© Copyright IBM Corporation 2016. All rights reserved. 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 ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.