IBM Security

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

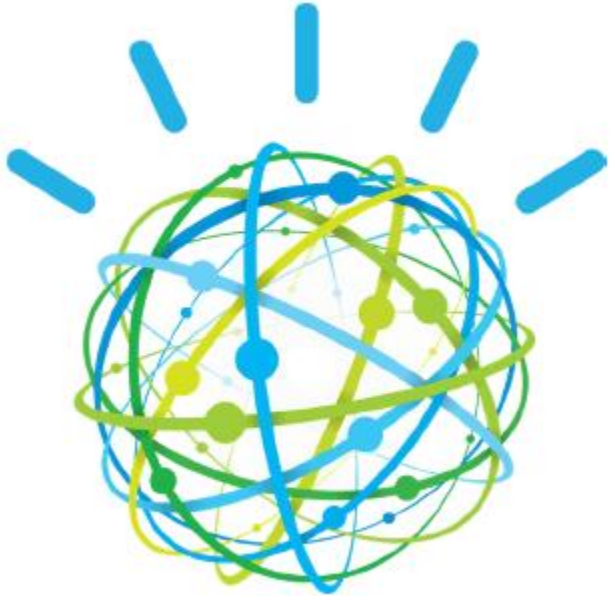
Banche e Sicurezza 2016 – Milan 26th-27th May

IBM

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

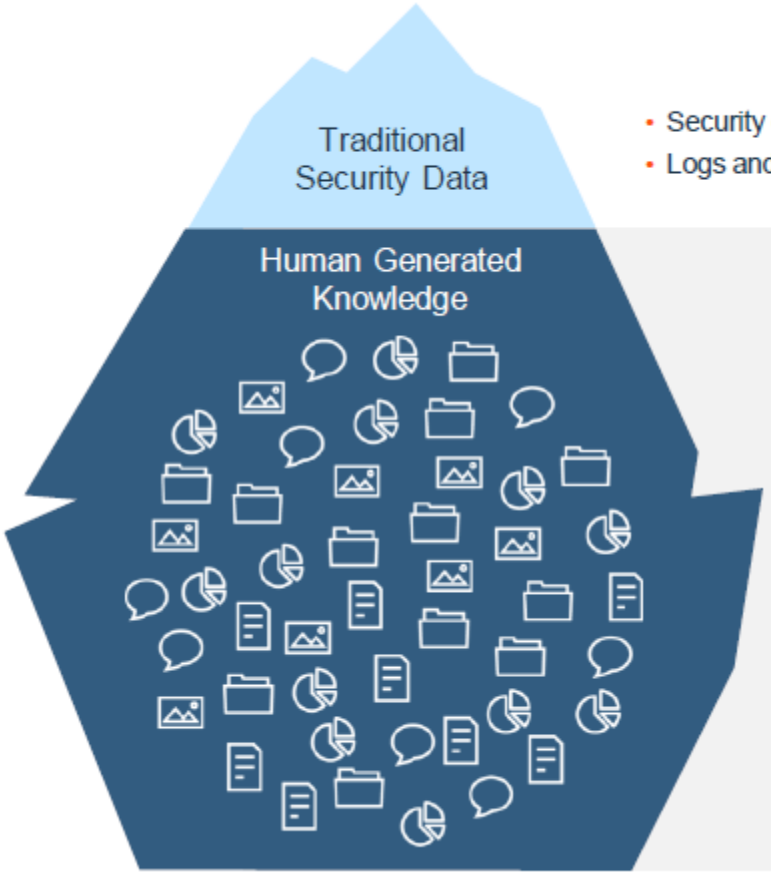
Cognitive is ushering in a new era of Security

- **Perimeter controls: security that confines.**
- **Security intelligence: security that helps you think.**
- **Cognitive Security: security that understands, reasons and learns.**

Pre- 2005 | **2005 +** | **2015 +**

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



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

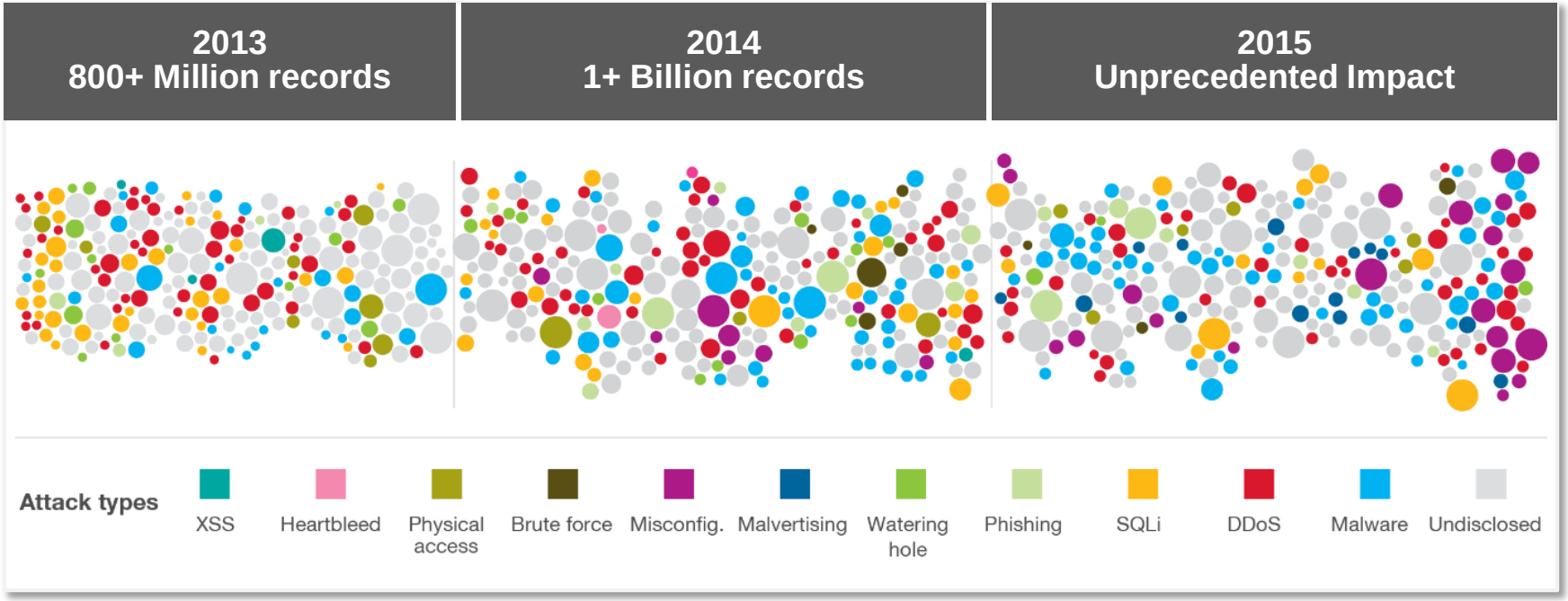
A universe of security knowledge Dark to your defenses

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

V2016-2-11

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

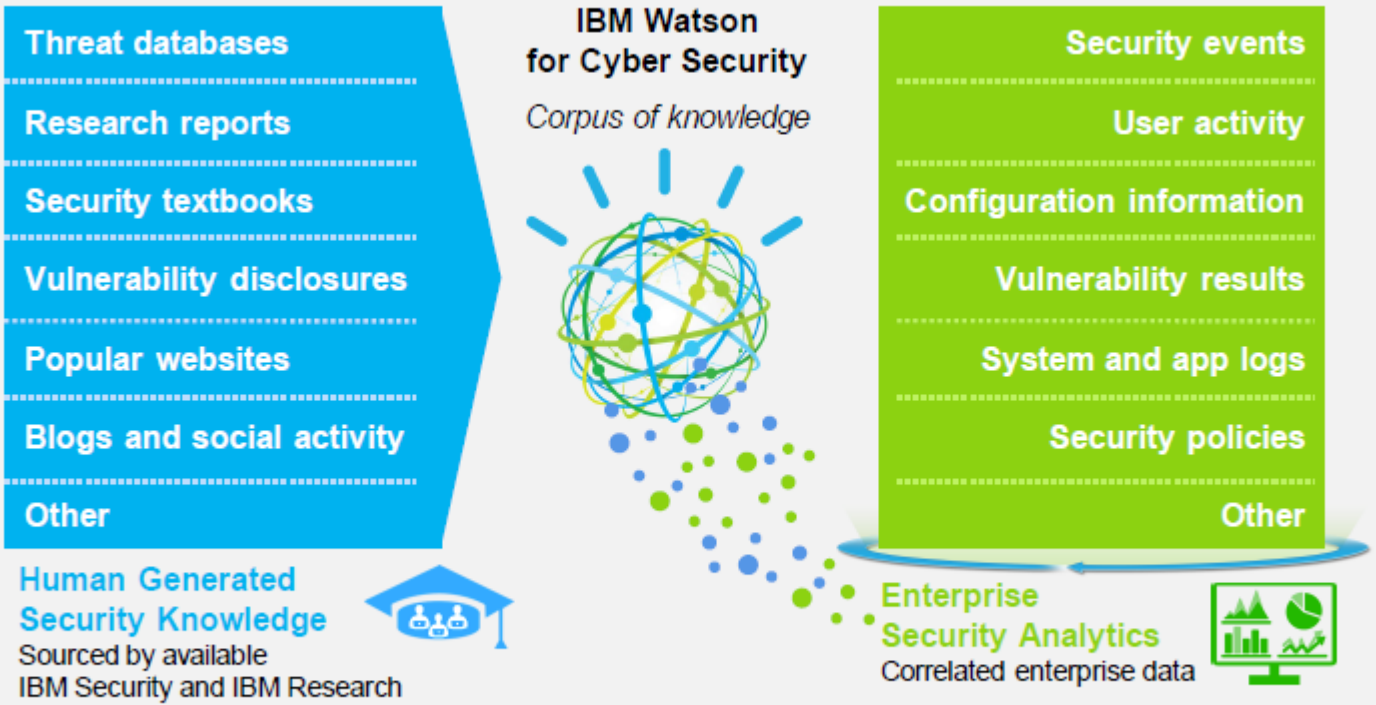
Security Analytics

- 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

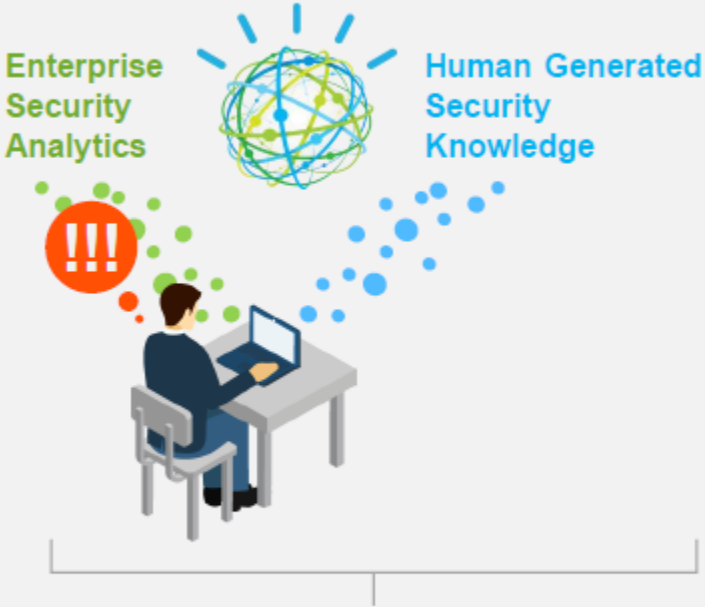
IBM Watson enables great insights by ingesting extensive data sources



Cognitive: revolutionizing how security analysts work

SECURITY ANALYST

SECURITY ANALYST and WATSON



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

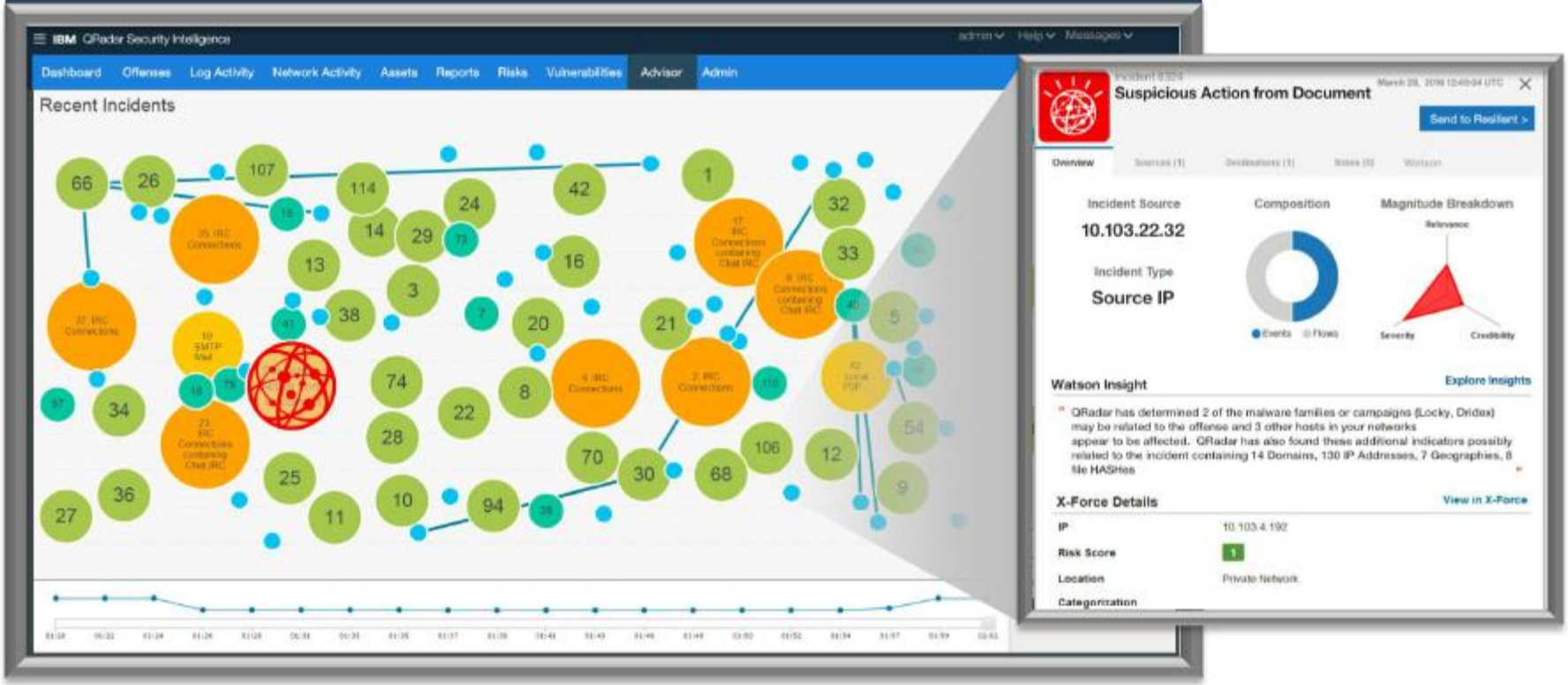
- Triage threats and make recommendations with confidence, at scale and speed

Save time and costs

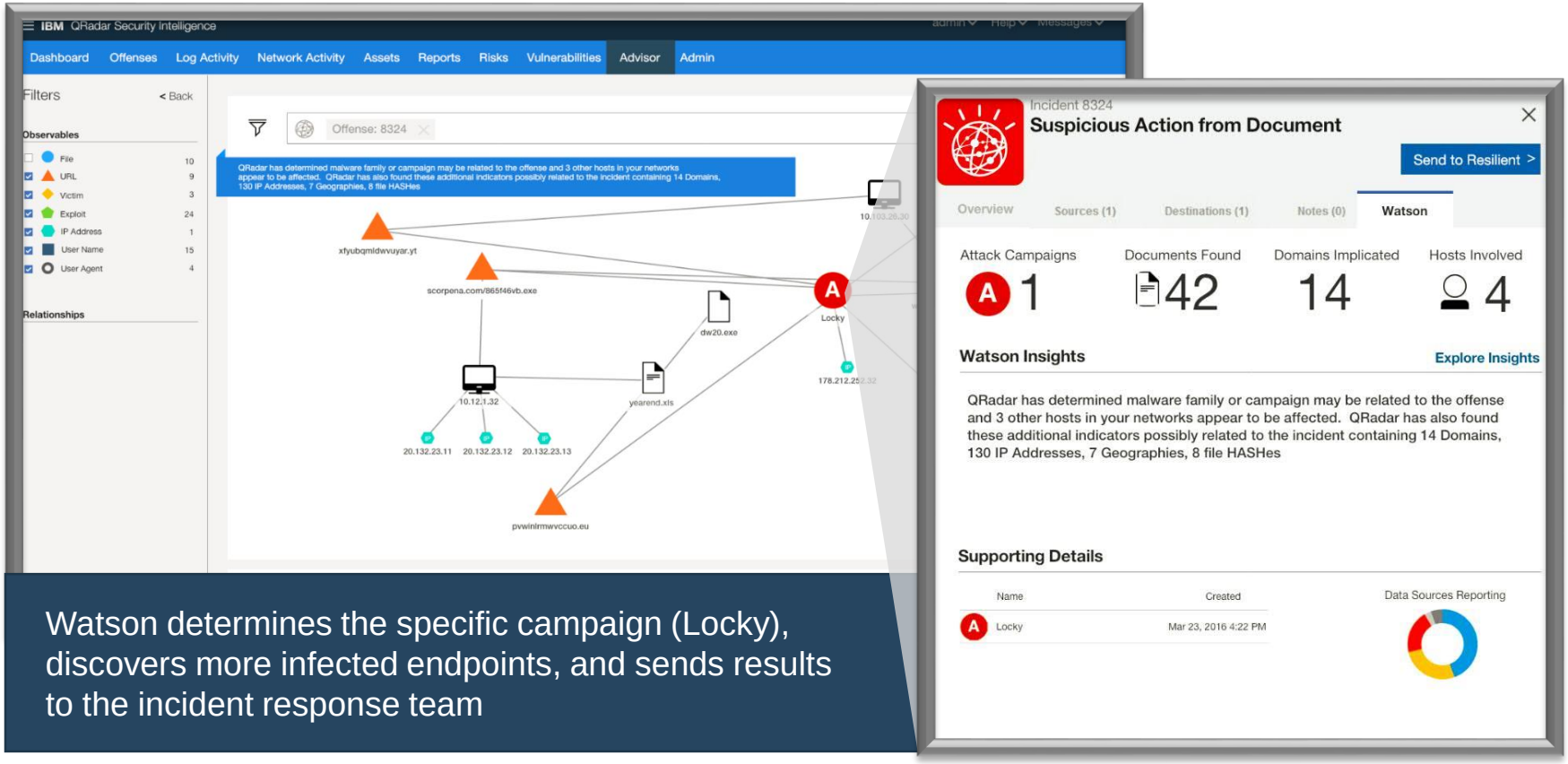
- Handle mass minutiae, so you can work on offense not endless defense

IBM Watson saves analysts valuable time spent trying to keep pace

Watson continuously crawls the internet for all information related to security in blogs, reports, advisories, and vulnerability disclosures



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



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 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/

IBM Security

THANK YOU

FOLLOW US ON:

ibm.com/security

ibm.com/security/cognitive/

@ibmsecurity

youtube/user/ibmsecuritysolutions

IBM