IBM UK Newsroom

IBM Watson for Cyber Security Beta Program Launches with 40 Clients Globally

Cognitive Systems Cited as New Priority by Nearly 60 Percent of Security Professionals

ARMONK, N.Y. - 06 Dec 2016: IBM Security (NYSE: IBM) today announced that global leaders in banking, healthcare, insurance, education and other key industries have joined the IBM Watson for Cyber Security beta program. Sun Life Financial, University of Rochester Medical Center, Avnet, SCANA Corporation, Sumitomo Mitsui Banking Corporation, California Polytechnic State University, University of New Brunswick and Smarttech will be amongst 40 organizations testing Watson's ability to assist in the battle against cybercrime.

Today's increasingly challenging security environment has created the need for more intelligence to identify and prioritize threats, which is in turn increasing the workload of security analysts with more alerts and anomalies to process than ever. Watson for Cyber Security uses intelligent technologies like machine learning and natural language processing, which can help security analysts make better, faster decisions from vast amounts of data.

A recent study from the IBM Institute for Business Value shows that nearly 60 percent of security professionals believe emerging cognitive technologies will be a critical part of changing the tides in the war on cybercrime.[1]

"Customers are in the early stages of implementing cognitive security technologies," said Sandy Bird, Chief Technology Officer, IBM Security. "Our research suggests this adoption will increase three fold over the next three years, as tools like Watson for Cyber Security mature and become pervasive in security operations centers. Currently, only seven percent of security professionals claim to be using cognitive solutions."

IBM Watson for Cyber Security Beta Program Underway

Watson for Cyber Security takes advantage of IBM's leading cognitive technology, which is being trained to understand the unique language of security. By applying intelligent technologies like machine learning and natural language processing, Watson can help security analysts make better decisions from structured data, as well as the massive amount of unstructured data that has been dark to an organization's defenses until now.

Fortune 500 companies and organizations spanning industries such as finance, travel, energy, automotive and education are currently working with Watson for Cyber Security, helping to refine Watson's cyber security capabilities and pilot real-world use cases. Avnet, California Polytechnic State University, SCANA Corporation, Smarttech, Sun Life Financial, Sumitomo Mitsui Banking Corporation, University of New Brunswick and University of Rochester Medical Center are amongst the first set of customers already working with Watson for Cyber Security as part of the initial beta program. The beta program will increase to 40 companies in coming

weeks.

These beta customers are leveraging Watson in their current security environments to bring additional context to their cyber security data, with new use cases such as:

- Determining whether or not a current security “offense” is associated with a known malware or cybercrime campaign; if so, Watson can provide background on the malware employed, vulnerabilities exploited and scope of the threat, among other insights.
- Better identifying suspicious behavior; Watson provides additional context to user activity outside of the primary suspicious behavior, which can provide better guidance to whether or not an activity is malicious.

Working with these beta customers, IBM is continuing to enhance Watson’s understanding of the cyber security data and refine how Watson can seamlessly integrate into day to day security operations.

Study Shows Cognitive Security on the Rise

The IBM Institute for Business Value recently surveyed over 700 security professionals to gauge perspectives on the challenges, benefits and opportunities for cognitive security technologies.

Nearly 60 percent of those surveyed believe that cognitive technologies will mature soon enough to significantly slow down cybercriminals in the near future. While only 7 percent said their organizations are currently in the process of implementing cognitive security solutions, 21 percent said they will implement these solutions over the next 2-3 years, representing a 3x increase in adoption.

Security professionals also said that the top benefit they expect to see from cognitive technologies is improved detection and incident response decision-making capabilities, which was indicated by 40 percent of respondents. Currently, the average data breach takes organizations an average of 201 days to identify and an average of 70 days to contain.[2] Security professionals expect cognitive to play a big part in reducing this time by providing them with better data to make fast decisions.

To download the full report, visit: ibm.biz/cyberimmunity

Expanding Cognitive and Intelligence across IBM Security Portfolio; Investing in World-class Skills

As development of Watson for Cyber Security continues, IBM continues to build more advanced analytics and cognitive capabilities into other areas of its security portfolio, as well as its deep bench of world-class security professionals, including the following:

- Applying behavioral analytics to better understand the usage patterns of insiders—employees, contractors and partners—and to determine if their credentials have been compromised, via IBM QRadar User Behavior Analytics.
- Using patented analytics, machine learning and behavioral biometrics capabilities to help prevent banking fraud with IBM Trusteer Pinpoint Detect, which analyzes how users interact with banking websites, creating gesture models that can become increasingly more accurate over time.

- Leveraging machine learning to help clients find potential vulnerabilities in their applications faster with IBM Application Security on Cloud.
- Visualizing data access in a single 3D view empowers security teams to detect and flag suspicious activities before they turn into a breach, using IBM Security Guardium
- Hiring nearly 2,000 experts into its Security business, including more than 600 in the US, in the past two years, including world-class developers, consultants, and research professionals.

About IBM Security
IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, enables organizations to effectively manage risk and defend against emerging threats. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 35 billion security events per day in more than 130 countries, and holds more than 3,000 security patents. For more information, please visit www.ibm.com/security, follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog.

Required Disclaimer Language: *IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion. Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision. The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract. The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.*

# # #

---

[1] IBM Institute of Business Value Study: Cybersecurity in the Cognitive Era

[2] IBM / Ponemon Cost of a Data Breach study, 2016
