IBM UK Newsroom

IBM Watson to Tackle Cybercrime

ARMONK, N.Y. - 10 May 2016: IBM Security (NYSE: IBM) 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. To further scale the system, IBM plans to collaborate with eight universities to greatly expand the collection of security data IBM has trained the cognitive system with.

Training Watson for Cyber Security is a critical step in the advancement of cognitive security. Watson is learning the nuances of security research findings and discovering patterns and evidence of hidden cyber attacks and threats that could otherwise be missed. Starting this fall, IBM will work with leading universities and their students to further train Watson on the language of cybersecurity, including: California State Polytechnic University, Pomona; Pennsylvania State University; Massachusetts Institute of Technology; New York University; the University of Maryland, Baltimore County (UMBC); the University of New Brunswick; the University of Ottawa and the University of Waterloo.

Today's news is part of a pioneering cognitive security project to address the looming cybersecurity skills gap. IBM efforts are designed to improve security analysts’ capabilities using cognitive systems that automate the connections between data, emerging threats and remediation strategies. IBM intends to begin beta production deployments that take advantage of IBM Watson for Cyber Security later this year.

IBM’s world-renowned X-Force research library will be a central part of the materials fed to Watson for Cyber Security. This body of knowledge includes 20 years of security research, details on 8 million spam and phishing attacks and over 100,000 documented vulnerabilities.

Watson to Address Looming Security Skills Gap

The volume of security data presented to analysts is staggering. The average organization sees over 200,000 pieces of security event data per day[1] with enterprises spending $1.3 million a year dealing with false positives alone, wasting nearly 21,000 hours[2]. Couple this with 75,000-plus known software vulnerabilities reported in the National Vulnerability Database[3], 10,000 security research papers published each year and over 60,000 security blogs published each month[4]– and security analysts are severely challenged to move with informed speed.

Designed on the IBM Cloud, Watson for Cyber Security will be the first technology to offer cognition of security data at scale using Watson's ability to reason and learn from "unstructured data" – 80 percent of all data on the internet that traditional security tools cannot process, including blogs, articles, videos, reports, alerts, and other information. In fact, IBM analysis found that the average organization leverages only 8 percent of this unstructured data. Watson for Cyber Security also uses natural language processing to understand the vague and imprecise nature of human language in unstructured data.

As a result, Watson for Cyber Security is designed to provide insights into emerging threats, as well as recommendations on how to stop them, increasing the speed and capabilities of security professionals. IBM will also incorporate other Watson capabilities including the system’s data mining techniques for outlier detection, graphical presentation tools and techniques for finding connections between related data points in different documents. For example, Watson can find data on an emerging form of malware in an online security bulletin and data from a security analyst's blog on an emerging remediation strategy.

“Even if the industry was able to fill the estimated 1.5 million open cyber security jobs by 2020, we’d still have a skills crisis in security,” said Marc van Zadelhoff, General Manager, IBM Security. “The volume and velocity of data in security is one of our greatest challenges in dealing with cybercrime. By leveraging Watson’s ability to bring context to staggering amounts of unstructured data, impossible for people alone to process, we will bring new insights, recommendations, and knowledge to security professionals, bringing greater speed and precision to the most advanced cybersecurity analysts, and providing novice analysts with on-the-job training."

Universities to Help Train IBM Watson for Cyber Security

IBM plans to collaborate with eight universities that have some of the world's best cybersecurity programs to further train Watson and introduce their students to cognitive computing. The universities include: California State Polytechnic University, Pomona; Pennsylvania State University; Massachusetts Institute of Technology; New York University; UMBC; the University of New Brunswick; the University of Ottawa and the University of Waterloo.

Students will help train Watson on the language of cybersecurity, initially working to help build Watson's corpus of knowledge by annotating and feeding the system security reports and data. As students work closely with IBM Security experts to learn the nuances of these security intelligence reports, they’ll also be amongst the first in the world to gain hands-on experience in this emerging field of cognitive security. This work will build on IBM's work in developing and training Watson for Cyber Security. IBM currently plans to process up to 15,000 security documents per month over the next phase of the training with the university partners, clients and IBM experts collaborating.

These documents will include threat intelligence reports, cybercrime strategies and threat databases. Training Watson will also help build the taxonomy for Watson in cybersecurity including the understanding of hashes, infection methods and indicators of compromise and help identify advanced persistent threats.

In another effort to further scientific advancements in cognitive security, UMBC today also announced a multi-year collaboration with IBM Research to create an Accelerated Cognitive Cybersecurity Laboratory (ACCL) in the College of Engineering and Information Technology. Faculty and students working in the ACCL will apply cognitive computing to complex cybersecurity challenges to build upon their own prior research. They will also collaborate with IBM scientists and leverage IBM's advanced computing systems to add speed and scale to new cybersecurity solutions.

"This collaboration will allow our students and faculty to work with IBM to advance the state-of-the-art in cognitive computing and cybersecurity," said Anupam Joshi, director of UMBC’s Center for Cybersecurity and chair of computer science and electrical engineering, at UMBC, who will lead the ACCL at UMBC.

For more information on today’s announcement and cognitive security visit: www.ibm.com/security/cognitive. Continue the conversation at @IBMSecurity #CognitiveSecurity.

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 20 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 2015 Cybersecurity Intelligence Index*

[2] *The Cost of Malware Containment, by Ponemon Institute, published January 2015*

[3] *The National Vulnerability Database*

[4] *IBM X-Force Analysis*

Related resources

Photo

Training IBM Watson for Cyber Security

The IBM Watson Knowledge Studio tool will be used by IBM and its eight university partners to help annotate documents used to train IBM Watson for Cyber Security. (Credit: IBM)

Students and IBM Train Watson for Security

IBM’s Chief Watson Security Architect Jeb Linton demonstrating to University of Maryland Baltimore County student Lisa Mathews how to teach IBM’s Watson the language of security, Tuesday, May 10, 2016, Baltimore, MD. IBM will work with 8 universities to train Watson for Cyber Security, so that the next generation of security professionals can leverage the power of “cognitive” technology to defend against cyberattacks. (Mitro Hood/Feature Photo Service for IBM)

---

https://uk.newsroom.ibm.com/2016-May-10-IBM-Watson-to-Tackle-Cybercrime