FORRESTER®

FOR SECURITY & RISK PROFESSIONALS

Quick Take: Your Next Security Analyst Could Be A Computer

IBM Announces Watson For Cyber Security

by Joseph Blankenship
with Michele Goetz, Stephanie Balaouras, Claire O'Malley, and Peggy Dostie

May 10, 2016

Why Read This Quick Take

IBM announced on May 10 that it is launching a project to use its cognitive computing technology, Watson, in cybersecurity. Working with eight universities, IBM intends to train Watson on the language of cybersecurity, giving security teams an intelligent resource to assist with investigations. This is a leap forward, both for cybersecurity and cognitive computing, as security teams will be able to employ Watson for practical applications in the security operations center.

Jeopardy Champion Watson Takes On Cybersecurity

Watson is best known in popular culture for soundly defeating Jeopardy champions Ken Jennings and Brad Rutter as well as featuring in catchy commercials with musician Bob Dylan, security expert Frank Abagnale, and others.[1] These entertaining displays of cognitive computing hint at Watson's capabilities but don't really show the practical application of the technology, which promises to assist with our most complex problems. Healthcare is an early use case for Watson as it analyzes patient medical records and presents treatment options to physicians.[2] Now, IBM will use Watson to address another complex problem: cybersecurity.

Security Teams Get Some Non-Trivial Help

On May 10, IBM Security announced a new initiative, Watson for Cyber Security.[3] As part of the initiative, IBM is working with eight universities to harness the power of cognitive computing for cyberdefense: California State Polytechnic University, Pomona; Pennsylvania State University; Massachusetts Institute of Technology; New York University; the University of Maryland, Baltimore County; the University of New Brunswick; the University of Ottawa; and the University of Waterloo. The collaboration will train Watson on the language of cybersecurity so that it can ingest and internalize

data from a multitude of sources, including security research, external blogs, social media sites, vulnerability disclosures, and threat databases. The goal is to turn Watson into a resource for security analysts to speed security processes and reduce false positives. Watson for Cyber Security will be delivered via a cloud-based version of the cognitive computing technology with beta production deployments starting later in 2016. With Watson for Cyber Security, IBM hopes to:

- **Alleviate the cybersecurity skills gap.** Hiring and retaining security practitioners, particularly analysts in the SOC, is difficult and expensive. According to our surveys, 58% of North American and European security decision-makers say hiring cybersecurity practitioners is a major challenge for them.[4] There will be an estimated 1 million cybersecurity job openings in 2016 with the number expected to increase to 1.5 million by 2019.[5] Having Watson as a resource for analysts will help fill gaps in security teams and make some processes more efficient. Security analysts will be able to leverage Watson for investigations, using Watson like an extra analyst that can answer questions and make recommendations.
- **Sift through massive volumes of data for insight.** Security analysts require systems to quickly analyze large volumes of data in order to detect and remediate threats before they hamper the business. Analysts must also determine which alerts are false positives. Cognitive computing technologies like Watson analyze unstructured data, finding patterns and making connections in it much faster than human analysts can, helping to find threats and identify false positives. Watson is unique in that it has natural language understanding that allows it to understand written text, and analysts can query it much as they would a human analyst.
- **Provide attack insights and recommendations.** IBM and its university partners are training Watson to recognize patterns in security data that signify threats, then make recommendations to human analysts for threat management. For example, if Watson detects a malware variant, it can query multiple sources for backup documentation and then make a recommendation to the human analyst about possible remediation steps.
- **Automate tedious manual processes.** Much of the work done by security analysts, such as correlating threat information, researching threats, and investigating alerts, is manual. Analysts rely on internal tools and external sources like blogs, threat databases, vulnerability disclosures, social media sites, and research reports for much of their investigative work. Using Watson, security analysts will be able to query multiple data sources simultaneously, accelerating the research and investigation process.

IBM Stands Alone In This Market

IBM is currently the only vendor with what it's calling a "cognitive security" solution, the combination of cognitive computing and cybersecurity. Other security vendors are using artificial intelligence techniques like machine learning for threat and anomaly detection, but none have the natural language processing capability of a technology like Watson.[6] While Watson for Cyber Security is an early

initiative, it positions IBM as a thought leader in cybersecurity and gives it a significant competitive advantage because there are not any security vendors today that can match the capabilities of Watson. In addition, Watson for Cyber Security is notable because it:

- **Combines well with other IBM security offerings.** Cognitive security fits in well with an IBM portfolio that includes security analytics, IPS, managed security services, and consulting. Watson for Cyber Security could be a potent add-on for IBM customers looking to bolster their security program. Clients using QRadar or IBM MSSP services in conjunction with Watson could receive automatically triaged alerts from the platform along with documented research and recommended actions. As the technology progresses in production environments, security teams could eventually trust it to take automatic remediation steps to stop malicious behavior.
- **Monetizes Watson in a strategic market.** Security, cloud, mobile, social, and Watson are all IBM strategic imperatives. According to our surveys, security represents about 21% of the IT budget across most industry sectors.[7] IBM is making a move to commercialize Watson in a market where security is a top board-level concern and firms are willing to spend even more to protect their customers' data and their own intellectual property.
- **Utilizes IBM threat research.** The X-Force research library is a key component of the training corpus the initiative partners are using to train Watson, providing terabytes of threat intelligence information for decision-making. X-Force is one of the older, more established research teams, with a database of discovered vulnerabilities going back to 1994, along with attack, security incident, malicious host, and IP reputation data.[8]

WHAT IT MEANS

Cognitive Computing Is A Game-Changing Technology For Security

The Watson for Cyber Security initiative is only a first step for utilizing cognitive computing in security, but it represents a huge advance in the tools available to security pros. If Watson for Cyber Security proves successful, firms will gain a major advantage on the attackers targeting them. Other security vendors will struggle to catch up, as IBM has a $1 billion investment in Watson and a broad security portfolio.[9] This will likely create a "haves and have nots" scenario where some large enterprise firms are able to use the technology before it becomes economical for smaller firms or competition enters the market. Security pros should watch the progress of the IBM initiative to gauge success and determine how and when they can utilize cognitive security.

Endnotes

[1] Source: Jo Best, "IBM Watson: The inside story of how the Jeopardy-winning supercomputer was born, and what it wants to do next," TechRepublic (http://www.techrepublic.com/article/ibm-watson-the-inside-story-of-how-the-jeopardy-winning-supercomputer-was-born-and-what-it-wants-to-do-next/).

Source: Jonathan Vanian, "Bob Dylan gets tangled up in Big Blue," Fortune, October 10, 2015 (http://fortune.com/2015/10/10/bob-dylan-watson-ibm/).

Source: "IBM Watson TV Spot, 'Frank Abagnale + IBM Watson on Security,'" iSpot.tv (https://www.ispot.tv/ad/AtFo/ibm-watson-frank-abagnale-ibm-watson-on-security).

[2] Cognitive computing is finding a foothold in the US healthcare industry, where scientists, doctors, payers, and patients are finding places to use this disruptive technology to optimize care, improve research discovery, and find waste and fraud. For example, tier one providers like Memorial Sloan Kettering and MD Anderson use IBM's Watson technology to give doctors better tools to establish oncology treatment paths. Forrester advises healthcare CIOs to step in now and understand these new scenarios of cognitive computing and the challenges facing this early market. The long-term impact of cognitive computing on healthcare will be massive. For more information, see the "Healthcare Meets Cognitive Computing" Forrester report.

[3] Source: "IBM Watson to Tackle Cybercrime," IBM press release, May 10, 2016 (http://www-03.ibm.com/press/us/en/pressrelease/49683.wss).

Source: "Cognitive security," IBM (http://www-03.ibm.com/security/cognitive/).

[4] New security objectives and approaches call for shifts in architecture and operations — but more importantly, for firms to renew their investments in their most valuable asset: employees. Over time, outdated skills, stagnated thinking, and complacency on the part of individuals and groups become a threat to the business. It's time for security and risk (S&R) leaders to invest not only in themselves and their staff, but all employees — because employees, not technologies, are responsible for designing and implementing the security strategy and driving behavioral change. For more information, see the "Maintain Your Security Edge" Forrester report.

[5] Source: Steve Morgan, "One Million Cybersecurity Job Openings In 2016," Forbes, January 2, 2016 (http://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/#364e4d257d27).

[6] Security analytics (SA) has garnered a lot of attention during the past few years. However, marketing hype and misunderstandings regarding SA have confused the market, making it difficult for security and risk (S&R) leaders to make informed decisions. For more information, see the "Counteract Cyberattacks With Security Analytics" Forrester report.

[7] Cybersecurity is now part of regular executive discussions and is being allocated budgets accordingly. Chief information security officers (CISOs) and their teams must exhibit business acumen in spending these budgets and demonstrate how they're reaching an appropriate state of cybersecurity readiness. For more information, see the "Cybersecurity Budgets Remain Strong, Skills Lag In 2016" Forrester report.

[8] Source: "IBM X-Force Research And Development is one of the most renowned commercial security research and development teams in the world." IBM (http://www-03.ibm.com/security/xforce/) and IBM X-Force (http://www.xforce.iss.net/%0D/index.html).

[9] Source: Tobias Schwarz, "IBM to invest $1 billion to create new business unit for Watson," Reuters, January 9, 2014 (http://www.reuters.com/article/us-ibm-watson-idUSBREA0808U20140109).

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

Engage With An Analyst

Gain greater confidence in your decisions by working with Forrester thought leaders to apply our research to your specific business and technology initiatives.

Analyst Inquiry

Ask a question related to our research; a Forrester analyst will help you put our research into practice and take the next step.

About analyst inquiry

Analyst Advisory

Put research into practice with in-depth analysis for your specific business and technology challenges.

About interactive advisory sessions

Client support

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

135061