IBM UK Newsroom

IBM Delivers Watson for Cyber Security to Power Cognitive Security Operations Centers

• Over 40 Companies Across a Dozen Industries Tap Watson Security Technology

• New Innovations Include Watson-Powered Chatbot & Voice-Powered Security Assistant Research Project

CAMBRIDGE, MA - 13 Feb 2017: IBM Security (NYSE: IBM) today announced the availability of Watson for Cyber Security, the industry's first augmented intelligence technology designed to power cognitive security operations centers (SOCs). Over the past year, Watson has been trained on the language of cybersecurity, ingesting over 1 million security documents. Watson can now help security analysts parse thousands of natural language research reports that have never before been accessible to modern security tools.

According to IBM research, security teams sift through more than 200,000 security events per day on average, leading to over 20,000 hours per year wasted chasing false positives.[1] The need to introduce cognitive technologies into security operations centers will be critical to keep up with the anticipated doubling of security incidents over the next five years and increased regulation globally.[2]

Watson for Cyber Security will be integrated into IBM's new Cognitive SOC platform, bringing together advanced cognitive technologies with security operations and providing the ability to respond to threats across endpoint, network, users and cloud. The centerpiece of this platform is IBM QRadar Advisor with Watson, a new app available in the IBM Security App Exchange, which is the first tool that taps into Watson's corpus of cybersecurity insights. This new app is already being used by Avnet, University of New Brunswick, Sogeti, Sopra Steria and 40 other customers globally to augment security analysts' investigations into security incidents.

With the dramatic growth in security events, IBM has also invested in research to bring cognitive tools into its global X-Force Command Center network, including a Watson-powered chatbot currently being used to interact with IBM Managed Security Services customers. IBM also revealed a new research project, code-named Havyn, pioneering a voice-powered security assistant that leverages Watson conversation technology to respond to verbal commands and natural language from security analysts.

"Today's sophisticated cybersecurity threats attack on multiple fronts to conceal their activities, and our security analysts face the difficult task of pinpointing these attacks amongst a massive sea of security-related data," said Sean Valcamp, Chief Information Security Officer at Avnet. "Watson makes concealment efforts more difficult by quickly analyzing multiple streams of data and comparing it with the latest security attack intelligence to provide a more complete picture of the threat. Watson also generates reports on these threats in a matter of minutes, which greatly speeds the time between detecting a potential event and my security

team's ability to respond accordingly."

The IBM Cognitive SOC

As security teams evolve their strategies and tactics to thwart cybercriminals, the introduction of cognitive technologies into today's security operations centers will be critical to keep pace. A recent IBM study found that only 7 percent of security professionals are using cognitive tools today, but that usage is expected to triple over the next 2-3 years.[3]

The IBM Cognitive SOC platform puts cognitive technologies into security analyst's hands, enhancing their ability to fill gaps in intelligence and act with speed and accuracy. The IBM QRadar Advisor with Watson app brings cognitive capabilities to aid security analysts in their investigations and remediation through IBM's QRadar security intelligence platform. The solution assists in the investigation of potential threats by correlating Watson's natural language processing capabilities across security blogs, websites, research papers along with other sources, with threat intel and security incident data from QRadar, which can shorten cyber security investigations from weeks and days, to minutes.

"The Cognitive SOC is now a reality for clients looking to find an advantage against the growing legions of cybercriminals and next generation threats," said Denis Kennelly, Vice President of Development and Technology, IBM Security. "Our investments in Watson for Cybersecurity have given birth to several innovations in just under a year. Combining the unique abilities of man and machine intelligence will be critical to the next stage in the fight against advanced cybercrime."

To extend the ability of the Cognitive SOC to endpoints, IBM Security also is announcing a new endpoint detection and response (EDR) solution called IBM BigFix Detect. The solution helps organizations gain full visibility into the constantly changing endpoint threat landscape while bridging the gap between malicious behavior detection and remediation. BigFix Detect is making EDR accessible and actionable, providing security analysts with the ability to see, understand and act on threats across their endpoints through a single platform, and delivers targeted remediation on impacted endpoints enterprise-wide in minutes.

When paired with the orchestration and automation capabilities of IBM Resilient's Incident Response Platform (IRP), clients can turn cognitive SOC insight into action across enrichment, remediation, and mitigation functions. The IBM Cognitive SOC also brings together other technologies from IBM Security including i2 for cyber threat hunting and IBM X-Force Exchange.

Cognitive Security Services and Innovations

IBM will also help clients design, build and manage cognitive security operations centers globally through IBM Managed Security Services. Over the past five years, IBM has built over 300 security operations centers for clients in dozens of industries, including consumer packaged goods, retail, banking and education. Clients can choose to have IBM build their Cognitive SOC on-premise or manage it virtually via the IBM Cloud as part of the IBM X-Force Command Center network.

IBM's global network of X-Force Command Centers are using IBM's cognitive capabilities like QRadar Advisor with Watson to enhance the investigation of security events. Another promising use case is a new research

project code-named Havyn, which brings a voice to the cognitive SOC. The goal of Havyn is to create a voice-powered security assistant that can interact with security analysts on topics such as real-time threat updates and information on an organization's security posture.

The Havyn project uses Watson APIs, BlueMix and IBM Cloud to provide real-time response to verbal requests and commands, accessing data from open source security intelligence, including IBM X-Force Exchange, as well as client-specific historic data and their security tools. For example, Havyn can provide security analysts with updates on new threats that have appeared and recommended remediation steps. Havyn is currently being tested by select researchers and analysts within IBM Managed Security Services.

Watson is also currently engaging with clients daily via a new chatbot tool deployed in IBM's X-Force Command Center network, which manages over 1 trillion security events per month. Clients can choose to ask Watson questions via instant messaging about their security posture or network configurations. For example, clients can ask Watson questions about a device or ticket status. The tool is also capable of executing commands from IBM MSS customers, such as reassigning a ticket to a new owner.

For more information on Watson for Cyber Security and the Cognitive SOC, visit: http://www-03.ibm.com/security/cognitive/.

Journalists and bloggers *can download b-roll and video about Watson for Security and the Cognitive SOC at http://ibm.newsmarket.com/Global/Latest-News/ibm-delivers-watson-for-cyber-security-to-power-cognitive-security-operations-centers/s/27b21670-d4c9-4177-ba8f-d64203678aea*

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] Infographic: Watson for Cyber Security: Shining a light on Unstructured Data

[2] IBM 2016 Cyber Security Intelligence Index analysis

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

Contact(s) information

John Galvez

UK External Relations 07734-104275john.galvez@uk.ibm.com
