IBM Watson for Cyber Security rende cognitivi i Security Operations Center (SOC)

Oltre 40 aziende di oltre dieci settori d'industria si avvalgono della tecnologia di sicurezza di Watson. Tra le novità un chat bot alimentato da Watson e un progetto di ricerca per un assistente alla security a comando vocale

Cambridge - 13 feb 2017: IBM Security (NYSE: IBM) ha annunciato la disponibilità di Watson for Cyber Security, la prima tecnologia di intelligenza aumentata del settore, progettata per rendere cognitivi i Security Operations Center (SOC). Nel corso dell'ultimo anno, Watson è stato addestrato al linguaggio della cyber security, alimentato da oltre 1 milione di documenti in materia, ed è ora in grado di aiutare gli analisti a esaminare migliaia di rapporti di ricerca in linguaggio naturale, in precedenza inaccessibili anche ai più moderni strumenti per la sicurezza.

Secondo le ricerche di IBM, i team della sicurezza vagliano in media più di 200.000 eventi al giorno, il che si traduce in più di 20.000 ore l'anno consumate a inseguire falsi positivi.[1] La necessità di introdurre le tecnologie cognitive nei Security Operations Center sarà cruciale per tenere il passo con il raddoppiamento degli incidenti di sicurezza previsto nei prossimi 5 anni e con l'aumento della regolamentazione a livello mondiale.[2]

Watson for Cyber Security sarà integrato nella nuova piattaforma Cognitive SOC di IBM, che riunisce tecnologie cognitive e attività di sicurezza per rispondere alle minacce relative a endpoint, reti, utenti e cloud. L'elemento centrale di questa piattaforma è costituito da IBM QRadar Advisor with Watson, il primo strumento in grado di sfruttare il corpus di informazioni di cybersecurity di Watson. Questa nuova app è già utilizzata da Avnet, University of New Brunswick, Sopra Steria e altri 40 clienti a livello globale per potenziare le indagini degli analisti sugli incidenti di sicurezza.

IBM ha investito anche nella ricerca per mettere a disposizione gli strumenti cognitivi alla sua rete globale di X-Force Command Center, incluso un chat bot alimentato da Watson, al momento utilizzato per interagire con i clienti dei Managed Security Services IBM. È stato presentato inoltre un nuovo progetto di ricerca, dal nome in codice Havyn, primo esperimento di un assistente di sicurezza a comando vocale in grado di rispondere a comandi verbali e al linguaggio naturale degli analisti grazie alla tecnologia di conversazione di Watson.

"Oggi le minacce sempre più sofisticate alla sicurezza informatica colpiscono su vari fronti per nascondere le loro attività e gli analisti hanno l'arduo compito di individuare questi attacchi in un mare di dati correlati alla sicurezza", afferma Sean Valcamp, Chief Information Security Officer di Avnet. "Watson rende più difficile gli sforzi di occultamento, analizzando rapidamente diversi flussi di dati e confrontandoli con le informazioni sugli attacchi più recenti, per fornire un quadro più completo della minaccia. Inoltre, Watson genera report su tali minacce nel giro di minuti, riducendo enormemente il tempo tra il rilevamento di un potenziale evento e la possibilità per il team di sicurezza di rispondere di conseguenza".

IBM Cognitive SOC

Oltre all'evoluzione delle strategie e delle tattiche dei team di sicurezza per contrastare i criminali informatici, l'introduzione delle tecnologie cognitive negli attuali Security Operations Center sarà essenziale per tenere il passo. Un recente studio di IBM ha rilevato che solo il 7 percento dei professionisti della sicurezza utilizza attualmente strumenti cognitivi, ma tale impiego è destinato a triplicarsi nel corso dei prossimi 2-3 anni.[3]

La piattaforma IBM Cognitive SOC mette le tecnologie cognitive nelle mani degli analisti della sicurezza, migliorandone la

capacità di colmare le lacune nelle informazioni e di agire con velocità e precisione. L'app IBM QRadar Advisor with Watson fornisce funzionalità cognitive per aiutare nelle indagini e negli interventi correttivi tramite la piattaforma di security intelligence QRadar di IBM. La soluzione assiste nell'indagine delle potenziali minacce correlando le capacità di elaborazione del linguaggio naturale di Watson su blog, siti web, documenti di ricerca sulla sicurezza, unitamente ad altre fonti, con le informazioni sulle minacce e i dati degli incidenti di sicurezza provenienti da QRadar, riducendo i tempi di indagine da settimane e giorni a minuti.

"Cognitive SOC è ormai una realtà per i clienti che vogliono avere un vantaggio rispetto alle crescenti schiere di criminali informatici e alle minacce di prossima generazione", afferma Denis Kennelly, Vice President di Development and Technology, IBM Security. "I nostri investimenti in Watson for Cyber Security hanno generato importanti innovazioni in poco meno di un anno. La combinazione delle abilità esclusive dell'uomo e dell'intelligenza artificiale sarà cruciale per la prossima fase nella lotta contro il crimine informatico più evoluto".

Per estendere agli endpoint la capacità di Cognitive SOC, IBM Security annuncia inoltre una nuova soluzione EDR (Endpoint Detection and Response), chiamata IBM BigFix Detect. La soluzione aiuta le organizzazioni ad acquisire piena visibilità sullo scenario delle minacce agli endpoint in continua evoluzione, colmando inoltre il divario tra rilevazione dei comportamenti con finalità criminale e rimedi. BigFix Detect rende l'EDR accessibile e immediatamente utilizzabile, fornendo agli analisti della sicurezza la capacità di vedere, comprendere e intervenire sulle minacce in tutti i loro endpoint, attraverso un'unica piattaforma, e fornisce rimedi mirati sugli endpoint interessati, in tutta l'azienda, nel giro di minuti.

In abbinamento alle funzionalità di orchestrazione e automazione della Incident Response Platform (IRP) di IBM Resilient, i clienti possono trasformare le informazioni dei SOC cognitivi in azione, attraverso funzioni di potenziamento, correzione e mitigazione. IBM Cognitive SOC comprende inoltre altre tecnologie di IBM Security, tra cui i2 per la ricerca delle minacce informatiche e IBM X-Force Exchange.

Servizi di sicurezza cognitivi e innovazioni

IBM aiuterà inoltre le aziende a progettare, realizzare e gestire Security Operations Center cognitivi a livello globale attraverso IBM Managed Security Services. Negli ultimi 5 anni IBM ha creato oltre 300 Security Operations Center per i clienti in decine di settori, tra cui distribuzione di beni di largo consumo, vendite al dettaglio, banche e istruzione. I clienti possono scegliere di affidarsi a IBM per la creazione del proprio Cognitive SOC in locale, oppure di gestirlo virtualmente tramite IBM Cloud nell'ambito della rete di X-Force Command Center IBM.

La rete globale di X-Force Command Center sfrutta le funzionalità cognitive di IBM, come IBM QRadar Advisor with Watson, per migliorare l'indagine sugli eventi di sicurezza. Un'altra applicazione promettente è un nuovo progetto di ricerca, dal nome in codice Havyn, che dà voce al SOC cognitivo. L'obiettivo di Havyn è creare un assistente di sicurezza a comando vocale, in grado di interagire con gli analisti su argomenti quali aggiornamenti sulle minacce in tempo reale e informazioni sul livello di sicurezza di un'organizzazione.

Il progetto Havyn utilizza le API di Watson, BlueMix e IBM Cloud per fornire una risposta in tempo reale a richieste e comandi verbali, accedendo ai dati di security intelligence open source, tra cui IBM X-Force Exchange, e ai dati storici specifici e agli strumenti di sicurezza dei clienti. Ad esempio, Havyn può fornire agli analisti della sicurezza aggiornamenti sulle nuove minacce comparse e sui rimedi consigliati. Havyn è attualmente in fase di sperimentazione presso ricercatori e analisti selezionati nell'ambito di IBM Managed Security Services.

Watson interagisce inoltre giornalmente con i clienti tramite un nuovo strumento di chat bot implementato nella rete X-Force Command Center di IBM, che gestisce più di 1 trilione di eventi di sicurezza al mese. I clienti possono scegliere di utilizzare la messaggistica istantanea per porre a Watson domande in merito al loro livello di sicurezza o alle configurazioni di rete, oppure domande sullo stato di un dispositivo o di un ticket. Lo strumento è in grado inoltre di eseguire comandi impartiti dai clienti IBM MSS, come ad esempio la riassegnazione di un ticket a un nuovo titolare.

Per maggiori informazioni su Watson for Cyber Security e IBM Cognitive SOC, visitate:http://www-03.ibm.com/security/cognitive/

I giornalisti e i bloggerpossono scaricare il b-roll e il video su Watson for Security e IBM Cognitive SOC dal sito: 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?CP=1

IBM Security
IBM Security offre un portafoglio d'offerta tra i più avanzati e integrati di prodotti e servizi per la sicurezza aziendale. Il portafoglio, supportato dalla ricerca di IBM X-Force® nota in tutto il mondo, consente alle organizzazioni di gestire con efficacia il rischio e di difendersi dalle minacce emergenti. IBM gestisce una delle più vaste organizzazioni al mondo di ricerca, sviluppo ed erogazione di servizi in tema di sicurezza, monitora 35 miliardi di eventi di sicurezza al giorno, in più di 130 paesi, e detiene più di 3.000 brevetti in materia. Per ulteriori informazioni, visitate il sito www.ibm.com/security, seguite @IBMSecurity su Twitter, oppure visitate il blog di IBM Security Intelligence.

Testo obbligatorio di limitazione della responsabilità: *Le dichiarazioni di IBM riguardanti i programmi, le indicazioni e gli intenti futuri sono soggette a modifica o ritiro senza preavviso, ad esclusiva discrezione di IBM. Nelle decisioni di acquisto non si deve fare affidamento sulle informazioni riguardanti i potenziali prodotti futuri, che sono intese unicamente a delineare l'indirizzo generale dei nostri prodotti. Le informazioni citate riguardanti i potenziali prodotti futuri non costituiscono un impegno, una promessa o un obbligo giuridico a fornire materiali, codici o funzionalità. Le informazioni sui potenziali prodotti futuri non possono essere incorporate in alcun contratto. Lo sviluppo, il rilascio e la tempistica delle caratteristiche o funzionalità future descritte per i nostri prodotti restano a nostra esclusiva discrezione.*

---

[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

Contatti

Claudia Ruffini

IBM Media Relations +39 335 6325093cla@it.ibm.com

https://it.newsroom.ibm.com/2017-02-13-IBM-Watson-for-Cyber-Security-rende-cognitivi-i-Security-Operations-Center-SOC