Highlights

- Use a trusted advisor for investigating and qualifying security incidents with a vast breadth of information
- Better understand and identify sophisticated security threats by tapping into unstructured data
- Analyse more security data more rapidly by leveraging the cognitive computing power of IBM Watson for Cyber Security
- Address challenges related to intelligence, speed and accuracy when investigating cyber threats.

Arm security analysts with the power of cognitive security

Detect and respond to threats at unprecedented speed and scale

Did you know that the average client monitored by IBM® Security experienced more than 54 million security events in 2016?[1] Enterprises spend USD1.3 million each year just dealing with false positives—amounting to 21,000 hours of investigation.[2] Among the data they must track, analysts are tasked with staying abreast of more than 75,000 known software vulnerabilities reported in the National Vulnerability Database[3] and more than 1 million security bulletins, threat reports and news articles published each year.[4] Sifting through existing data is another challenge. The average organisation leverages only eight percent of unstructured data such as blogs and videos.[5] Nevertheless, security teams are expected to move fast.

IBM QRadar Advisor with Watson provides security insights by drawing from a vast breadth of structured and unstructured data. The solution helps to transform security operations centre (SOC) capabilities by addressing challenges such as skills shortages, alert overloads, incident response delays, outdated security information and process risks—and can be downloaded in minutes from IBM Security App Exchange.

▸ Start a complimentary 30-day trial of QRadar Advisor with Watson.

"There is a massive amount of noise out there; the human brain can't process everything on a day-to-day basis. We need something to help, something like AI or cognitive technologies."

—Chad Holmes, Principal and Cyber-Strategy, Technology and Growth Leader (CTO) at Ernst & Young LLP

1 'IBM X-Force Threat Intelligence Index 2017,' *IBM X-Force,* March 2017.

2 'The cost of malware containment,' *Ponemon,* January 2015.

3 'National Vulnerability Database,' *Computer Security Resource Center,* National Institute of Standards and Technology, Accessed Mar 18, 2017.

4 'Cognitive security helps defend against cybercrime,' *SecurityIntelligence,* May 10, 2017.

5 'IBM Watson to tackle cybercrime,' *IBM Corp.,* May 10, 2016.

Tap into vast security knowledge

Built on the IBM Cloud, Watson for Cyber Security provides cognitive security at scale, using the ability to reason and learn from the unstructured data that comprises an estimated 80 percent of all data[1] which traditional security tools cannot process.

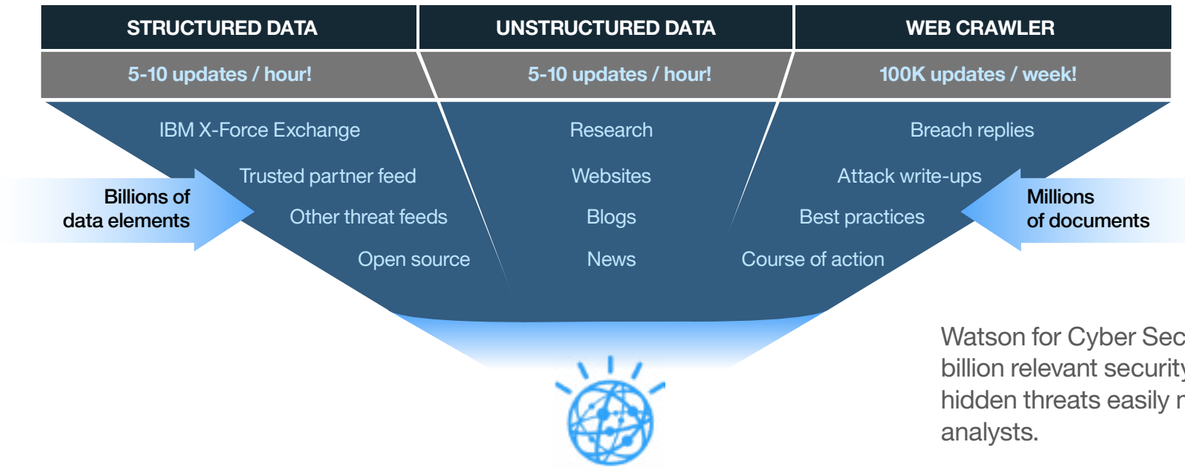
Watson for Cyber Security uses core Watson technology to ingest, reason and learn about security topics and threats, with a wide range of inputs, from blog posts and academic papers to security alerts from government agencies. Using natural language processing, Watson for Cyber Security helps to understand the human language in unstructured data that has previously been elusive to an organisation's security systems. It empowers analysts with insights relevant to specific security incidents to help identify and understand threats. By mining both structured and unstructured security data, Watson for Cyber Security augments the security analyst's ability to gain new insights and respond to threats rapidly and with greater confidence.

By using Watson for Cyber Security as a trusted advisor, security analysts can uncover insights into security incidents, while relying on a body of knowledge that continually grows and adapts, performs cognitive exploration of suspicious activities and behaviours and identifies both root causes and additional indicators of compromise (IOC) and related threat entities. This powerful solution learns, adapts and unlike humans, does not forget the data it gathers. The result is that it can give security teams 10 times as many actionable insights to uncover new threats as they had available before.[1] What's more, as an exclusively software-as-a-service (SaaS) offering, Watson for Cyber Security does not require additional hardware or deep on-premises analyst expertise.

<1 minute

Time Watson for Cyber Security requires to complete a complex analysis, which would take a human analyst more than one hour.[2]

Massive corpus of security knowledge



Watson for Cyber Security monitors 10+ billion relevant security nodes to reveal hidden threats easily missed by security analysts.

1 Christie Schneider, "The biggest data challenges that you might not even know you have," *IBM Watson Blogs,* May 25, 2016.

2 Results observed by clients who participated in the beta test program of QRadar Advisor with Watson.

Understand and identify sophisticated security threats

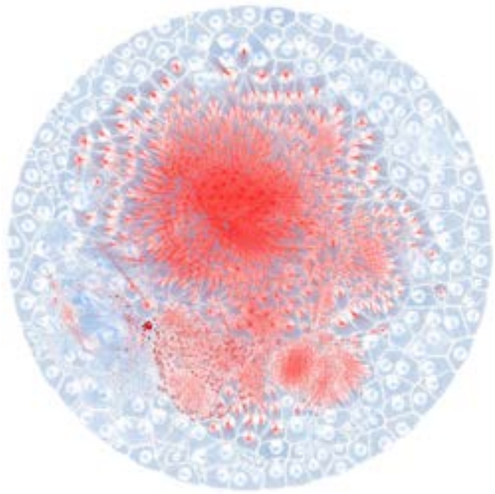
IBM QRadar Security Intelligence Platform analyses millions of events and network flows per minute to detect advanced threats across your enterprise. Watson for Cyber Security extends the capabilities of QRadar, leveraging the cognitive computing power of Watson to provide security analysts with a trusted advisor for investigating and qualifying security incidents and anomalies using vast amounts of structured and unstructured data.

How it works

When a QRadar offence or incident is delegated to QRadar Advisor with Watson, it first performs local data mining using observables in the offence to gather greater context around the incident, then devises a threat research query to perform knowledge and discovery on the offence by leveraging Watson for Cyber Security. Synthesizing local knowledge with external insights, QRadar Advisor with Watson makes threat investigation more effective and seamless.

Based on observables passed in the form of a threat research query from QRadar Advisor, Watson for Cyber Security taps into its vast knowledge base, gathered from millions of sources, including threat intelligence feeds, websites, forums and bulletins, to perform further analysis. Watson for Cyber Security derives insights, gathers IOCs and discovers other threat entities related to the original offence, such as malicious files, suspicious IP addresses or rogue entities and uses reasoning to identify the relationships between those entities. QRadar Advisor with Watson then prunes this information to focus on the key insights relevant to the current offence.

Analysts can then take further action based on the insights provided by QRadar Advisor with Watson by sending the offence information, along with supporting evidence and key insights returned by Watson, to the incident response team for remediation.



QRadar Advisor with Watson draws from more than 1 million security documents ingested by Watson to provide the full context and scope of an attack.

▸ Learn how IBM Watson technology helped alert a utility company that it was under attack.

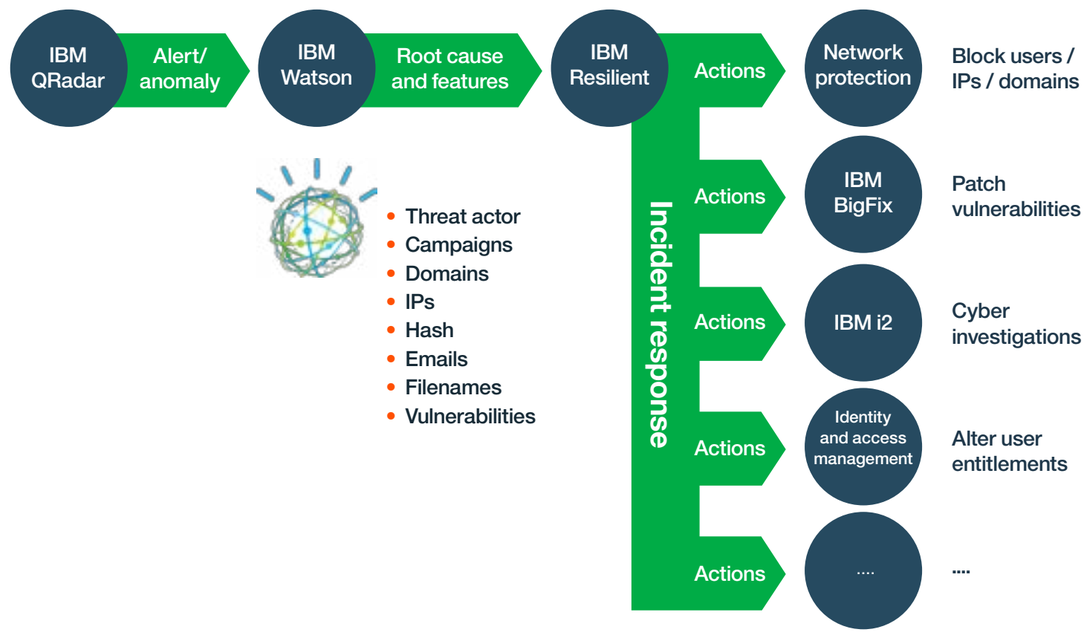
1 '[IBM X-Force Threat Intelligence Report 2016,](#)' *IBM Corp.*, February 2016.

2 '[IBM 2016 Cost of Data Breach Study: Global analysis,](#)' *IBM Corp.*, June 2016.

Rapidly navigate vast pools of knowledge to speed response times

As recent global cybersecurity attacks have demonstrated, cybercriminals strike quickly, often unexpectedly and speed is your greatest weapon to defeat them. So, whether it's doing the heavy lifting to help establish defenses against potential threats or responding with targeted precision to an attack that has already occurred, QRadar Advisor with Watson can help. It enables you to navigate the knowledge Watson has about a specific security incident, evaluate evidence and provide analysts with the necessary insights to take further action.

Accelerating the end-to-end response process



QRadar Advisor with Watson makes cognitive security immediately consumable and actionable.

"QRadar fired an offense on a user trying to connect to a botnet IP. The security analyst found five correlated indicators manually while Watson showed the extent of the threat with 50+ useful indicators."

—Large energy company.[1]

60x

The speed increase that QRadar Advisor with Watson provides over manual threat investigations.[1]

1 Results observed by clients who participated in the beta test program of QRadar Advisor with Watson.

Gain intelligence, speed and accuracy

Intelligence: A vital need

Some potential threats are easy to resolve. A weekend attempt to access the database may simply be an employee working from home. But for sophisticated attacks, the cognitive techniques of QRadar Advisor with Watson can help. It can ingest and correlate vast amounts of structured and unstructured security data available to uncover new threat patterns, triage threats and make recommendations with confidence. QRadar Advisor with Watson reasons and derives its insights from its vast knowledge base of security data to present the information most relevant to the investigation.

Speed: How fast is now?

Even the most accurate intelligence is worthless if it's delivered too late. Having the ability to identify and understand a threat within minutes is crucial to taking the right steps in preventing a large-scale attack.

Watson gives you the cognitive advantage to uncover hidden threats with automated insights, allowing analysts to tap into large amounts of real-time structured and unstructured data while investigating potential threats.

Accuracy: Discernment is key

A security system is only as trustworthy as it is accurate, both at consistently detecting actual threats and at rejecting false positives. This can be a tough balance. Cybercriminals rely on slipping through the same channels as legitimate users and applications, because they know you can't examine every packet in advance. QRadar Advisor with Watson gives you the benefit of highly evolved detection and identification techniques to accurately qualify incidents and stop threats.

"...L1 and L2 analysts arrived at the conclusion that it's not a security incident. The investigation with Watson was more instructive. It did the qualifying in minutes and determined that one of our client's hosts was compromised by a DDoS attack."

—QRadar Advisor with Watson client

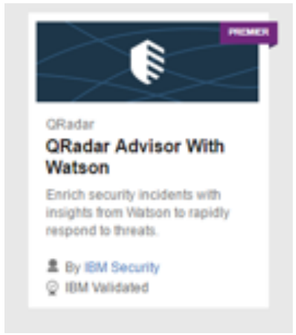
- Watch a video to see how QRadar Advisor with Watson identified the Poison Ivy malware.

Try QRadar Advisor with Watson for 30 days

Understanding how the power of cognitive can help your organisation is made simple with an easy-to-install application. QRadar Advisor with Watson is available to existing QRadar customers for a 30-day trial at no charge. It can be installed in minutes from IBM Security App Exchange, the dedicated site for application extensions and enhancements for IBM Security products. Following the trial, it's easy to convert the trial into a service subscription using a simple licence key.

Use QRadar Advisor with Watson with confidence

Cybercriminals operate by exploiting patterns of weakness and QRadar Advisor with Watson can help you identity and understand these threats. Once the client-side QRadar Advisor with Watson is installed with an on-premises or cloud-based instance of QRadar, the application communicates securely to its cloud-based counterpart, Watson for Cyber Security. Your network data remains fully protected QRadar Advisor with Watson does not send log files or sensitive enterprise information to the cloud. Instead, it retrieves knowledge from Watson using file names and anonymised identifiers of the kind that many organisations are already using for scanning and other security functions.



QRadar Advisor with Watson can be downloaded in minutes from the IBM Security App Exchange.

Existing customers can download a

complimentary 30-day trial

of QRadar Advisor with Watson.

Why IBM?

Using its industry-leading cognitive security capabilities, Watson can be your trusted advisor for making sense of a sea of structured and unstructured data. QRadar Advisor with Watson enables QRadar and Watson to work together to tap into a vast array of data to uncover new threat patterns, deliver faster, more accurate analysis of security threats and save precious time and resources in providing enterprise security. Whether meeting complex security needs with sophisticated analytics or supplementing the capabilities of a limited security team, QRadar Advisor with Watson delivers advanced IBM technology to help reduce enterprise security risk.

For more information

To learn more about QRadar Advisor with Watson, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/us-en/marketplace/cognitive-security-analytics

About IBM Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned X-Force research and development, provides security intelligence to help organisations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organisations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organisations, monitors 15 billion security events per day in more than 130 countries and holds more than 3,000 security patents.

IBM

IBM United Kingdom Limited
PO Box 41, North Harbour
Portsmouth, Hampshire PO6 3AU
United Kingdom

IBM Ireland Limited
Oldbrook House
24-32 Pembroke Road
Dublin 4

IBM Ireland registered in Ireland under company number 16226.

WGS03087-GBEN-01