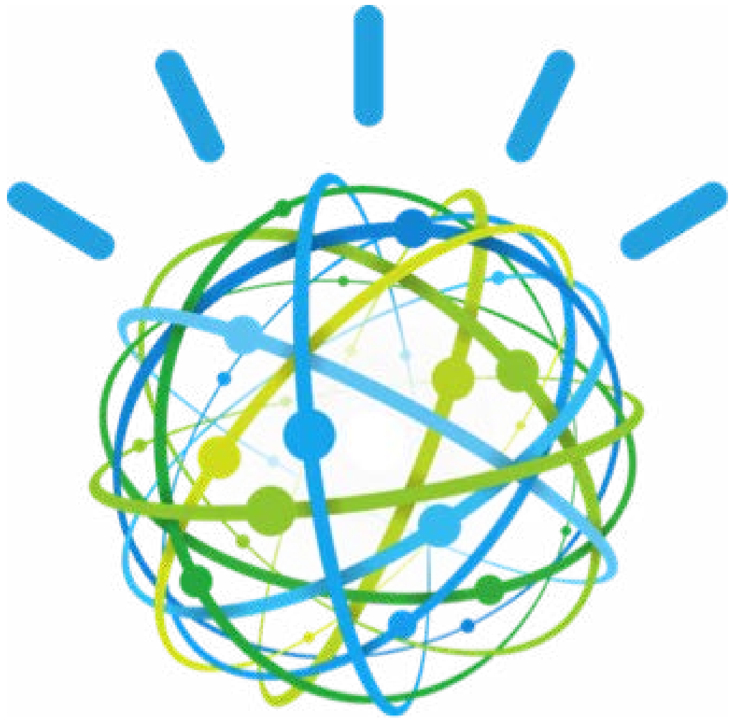
Highlights

- Extend your IBM® QRadar® deployment with the cognitive security capabilities of IBM QRadar Advisor with Watson®
- Unlock the power of cognitive security to uncover new insights and rapidly respond to threats
- Leverage the huge amount of security information that most organizations never use
- Take advantage of the speed IBM Watson brings to digesting and accessing security information
- Try it in your environment with a 30-day trial version of QRadar Advisor with Watson, available to current QRadar customers

Unlock the power of cognitive security with Watson

Connect obscure data points humans can't see on their own to uncover hidden threats

Chances are, your organization has a good grip on cybersecurity. You're collecting data on events and alerts, logs and configurations, and user and network activity. But is your good grip really just a good start? Think how much more you could do if your threat-fighting strategies could also draw on information that is largely untapped today, from academic research, industry publications, wikis, blogs and other sources. Think how much more effective your efforts could be if you could add information generated by *people* to information generated by *technology*.



Cognitive security delivers a new world of insight

QRadar Advisor with Watson extends your IBM QRadar Security Intelligence Platform deployment with cognitive security. Now you can go beyond gathering data from your own systems. You can supplement it with knowledge created worldwide—and with the ability of Watson to use that knowledge to understand, reason and learn about security topics and threats.

Two solutions together make one powerful tool

Know the scope of the challenge

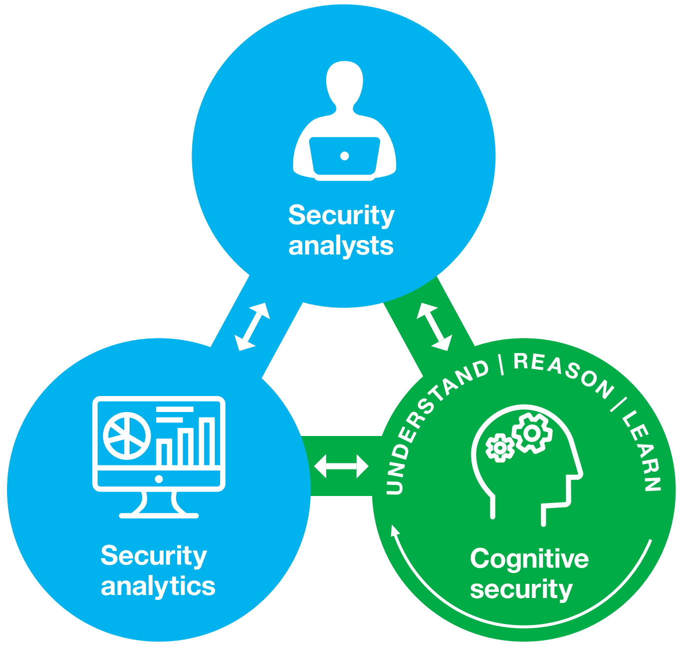
Today's threats are big. The IBM X-Force® database has documented 96,000 security vulnerabilities—including 8,956 from 2015 alone.[1] The average cost of an enterprise data breach has reached USD4 million.[2] And the likelihood that an organization will suffer multiple attacks in a given two-year period is as high as 29 percent.[2]

Build a powerful threat response

To protect your enterprise, you need help that's just as big. You need to unlock insight that can help you better prevent and remediate advanced threats. Begin with the common sense, insights and ability to generalize that comes from human expertise. Add the ability of security analytics to correlate data, identify behavioral patterns and anomalies, and prioritize and manage workflows. Now, with QRadar Advisor with Watson and IBM Watson for Cyber Security, you can extend those capabilities further with cognitive security's power to analyze unstructured as well as structured data, understand natural language, and respond. Now you can draw on the huge amount of security information most organizations never use, simply because they cannot tap the vast majority of security knowledge that is unstructured.

Understand how threats behave

QRadar detects threats. QRadar Advisor with Watson provides cognitive abilities that can help your team deal with them. Working together, these technologies can mimic human thought to understand advanced threats, triage threats and make recommendations about dealing with potential or actual attacks. For a malware-borne strike attempting to access and exfiltrate intellectual property, for example, QRadar Advisor with Watson makes it possible to analyze structured and unstructured information to identify the threat, understand how that threat behaves and what indicators occur in the typical attack chain, and analyze how the attack may have progressed.



▸ To learn more about QRadar, visit the web page and read the white paper.

[1] "IBM X-Force Threat Intelligence Report 2016," *IBM Corp.*, February 2016.

[2] "2016 cost of Data Breach Study: Impact of Business Continuity Management," *Ponemon Institute*, June 2016.

[3] Christie Schneider, "The biggest data challenges that you might not even know you have," *IBM Watson Blog*, May 2016.

Intelligence addresses core security issues

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. QRadar can detect unusual behavior; an analyst can decide whether it's dangerous. 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. What's more, the combination of QRadar Advisor with Watson provides a solution that not only ingests data, but also reasons and derives its own knowledge from it—discovering linkages that may otherwise go unnoticed and presenting information most relevant to the investigation.

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. You don't want to react to false positives without reflection. That would put too much of your network on unnecessary lockdown. But you can't let your data traffic go unexamined, either. A better approach is to equip your enterprise with QRadar Advisor with Watson. The IBM approach gives you the benefit of highly evolved detection and verification techniques. X-Force security researchers analyze hundreds of millions of data points to address both sides of the detection coin.

Speed: How fast is now?

Even the most accurate intelligence is worthless if it's delivered too late. Dedicated, always-on monitoring systems can alert security personnel in near real time. That could mean beating a spear phishing email to a recipient's inbox, or minimizing damage by isolating data-encrypting ransomware before it spreads to upstream data stores.

Forty-eight percent of breaches described in a 2016 IBM study were caused by malicious or criminal attacks. Average cost per compromised record?

USD170.[2]

- Learn more from the Ponemon Institute about the impact of cyber attacks globally and in individual countries.
- Get more insight into today's enterprise threats from IBM X-Force.

[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.

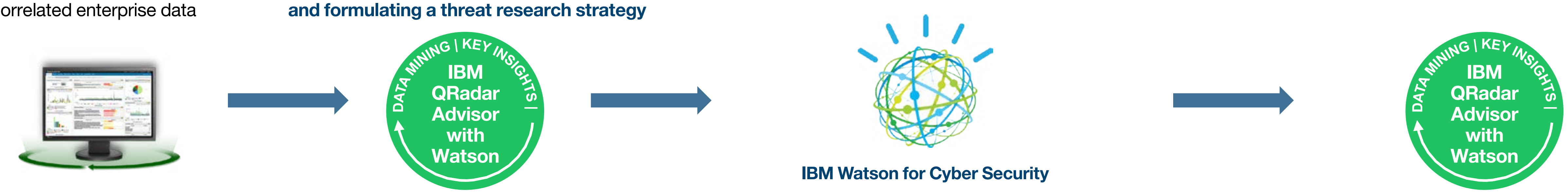
Scale cognitive tasks to augment human skills

Scale up with cognitive technology

Security analysts are called on to keep up with vast amounts of relevant security information from diverse sources ranging from vulnerability reports to conference proceedings—and then to apply the information. That can be especially hard for small organizations, but even large enterprise teams can be swamped by data overload.

QRadar Advisor with Watson can relieve some of the strain by helping security staff to analyze security incidents. That means security teams can spend more time planning to prevent security breaches, not just reacting to them.

SCALE AND OPTIMIZE THE COGNITIVE TASKS OF A SECURITY ANALYST


DATA MINING | KEY INSIGHTS |
IBM QRadar Advisor with Watson
DATA MINING | KEY INSIGHTS |
IBM QRadar Advisor with Watson

Enterprise security analytics
Correlated enterprise data

IBM QRadar Security Intelligence Platform

Gain local context leading to the incident and formulating a threat research strategy

- Review the incident data
- Review the outlying events for anything interesting (domains, MD5s, etc.)
- Pivot on the data to find outliers (such as unusual domains, IPs, file access)
- Expand your search to capture more data

Perform the threat research and develop expertise

IBM Watson for Cyber Security

- Search IBM X-Force Exchange + unstructured data (blogs, security websites, bulletins, etc.) + virus total + your favorite tools for these outliers / indicators → Find new malware that is at play
- Get the name of the malware
- Search more websites for information about indicators of compromise (IOCs) for that malware

Apply the intelligence gathered to investivate and qualify the incident

- Take these newly found IOCs from the internet and investigate them locally
- Qualify the incident based on insights gathered from threat research
- Find that other internal IPs are potentially infected with the same malware
- Start another investigation around each of these IPs

Learn more about Watson for Cyber Security.

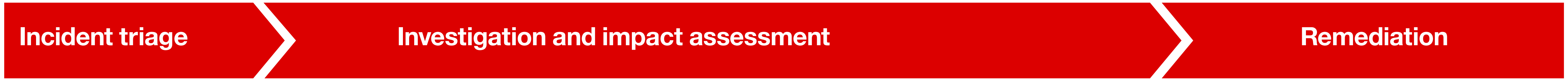
Gain the benefit of speed

Response that's faster than ever

As if drawing informed security conclusions from mountains of human-generated information weren't enough, there's still another factor that's critical to enterprise security: speed. 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 assists with threat analysis. It enables you to navigate the knowledge Watson has that pertains to a specific security incident, evaluate the evidence, and provide analysts with insights in minutes rather than the hours or days conventional approaches require.

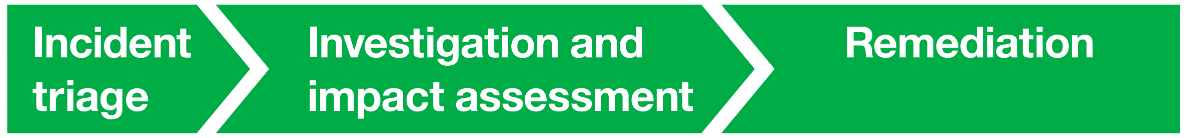
IBM WATSON FOR CYBER SECURITY REDUCES RESEARCH AND RESPONSE TIME

Threat analysis conducted manually



Time required:
Days to weeks

Threat analysis assisted by IBM Watson for Cyber Security



Time required:
Minutes to hours

Quick and accurate analysis of security threats, saving precious time and resources

- Read the cognitive security study.
- Watch QRadar Advisor with Watson in action.

Why choose IBM Security?

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 the 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.

Install the application in minutes

QRadar Advisor with Watson is available as a downloadable application—with a 30-day no-charge trial for existing QRadar customers—from IBM Security App Exchange, the dedicated site for application extensions and enhancements for IBM Security products. Installation takes only a few minutes, and, following the trial, it's easy to convert the trial into a service subscription using a simple license key.

Use QRadar Advisor with Watson with confidence

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 that leverages Watson for Cyber Security for reasoning and the larger context of cybersecurity issues. 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 anonymized identifiers of the kind that many companies are already using for scanning and other security functions.

For more information

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

Existing QRadar customers can download a

30-day trial

of QRadar Advisor with Watson.

- To learn more about IBM Security App Exchange visit the web page.

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 organizations 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 organizations 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 organizations, monitors 15 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit: **ibm.com**/financing

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
February 2017

IBM, the IBM logo, ibm.com, IBM Watson, QRadar, and X-Force are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.