Research Report

The New Era of Analytics/Cognitive-Driven Cybersecurity

Executive Summary

For several years we've been reporting on the trend of using analytics in systems management to isolate faults, simplify management, improve performance and gain new insights. Our argument has been that machines can perform certain analytics tasks more quickly and with greater accuracy than humans can. With machine analytics, systems administrators are able to do their jobs more efficiently. And, with analytics tools, enterprises are able to hire fewer, less skilled individuals to perform systems management tasks (addressing skills shortages while growing expertise using machine assistance).

> ***The same phenomenon, using analytics to streamline administrative activities, has now been applied to security software. With analytics extensions, traditional security software has become even more effective at identifying intrusions, finding vulnerabilities and detecting patterns. These analytics extensions help security administrators do their jobs more efficiently by analyzing vast amounts of data more quickly than humanly possible.***

Over the past year we've seen "cognitive computing" play an increasingly important role in security administration, and, when combined with machine analytics, we see a new era of cognitive security evolving. In this new cognitive security era, humans will have an *assistant* – "Watson for Cybersecurity". (Watson is IBM's moniker for its cognitive machine learning, reasoning, natural language processing environment that, when coupled with security analytics software, provides security administrators with the most potent set of tools on the planet for resisting incursion and protecting data).

The way that Watson for Cybersecurity works is that it taps into large corpuses of information (such as the 100,000 documented software vulnerabilities in the IBM X-Force Exchange database , as well as the 100,000 security research papers and 700,000 security blogs published each year) to derive new insights. Watson can understand, reason and learn about security terminology, topics, threats and more by analyzing structured and unstructured data (including data from security blogs, articles and reports). Watson formulated answers that can fill-in the gaps in the knowledge of even the best security administrators – thus assisting the administrator find the best solution. Obscure data points that might not be recognized by humans can be found and analyzed. The end result is that Watson's deep insights help security administrators determine the best course of action to remediate situations or reduce exposure.

> ***IBM has branded its security operations center/Watson for Cyber Security offering as the "Cognitive SOC". And it is within the Cognitive SOC that Clabby Analytics expects much of the groundbreaking security activity in the industry to take place over the next decade.***

As we look back at IBM's efforts in the security marketplace over the past few years, we find that the company has led industry efforts to collaboratively tackle cybersecurity problems. IBM has led the industry trend toward analytics-enabling security software. IBM has invested heavily in building a next-generation cognitive computing environment that can greatly assist security experts in the performance of their duties. Further, IBM has introduced several security Software-as-a-Service (SaaS) and managed service offerings that make it easier for enterprises of all sizes to more easily implement enterprise-class security. And IBM has worked inclusively with over four hundred 3rd party security vendors to help build a rich portfolio of security offerings.

In this *Research Report, Clabby Analytics* takes a closer look at IBM's security strategy, its analytics/cognitive product offerings, and its security services – and what we see is a company in the midst of cognitively-enabling its software portfolio to help make security administrators more efficient, while delivering more and more SaaS and managed service offerings via the IBM cloud. This portfolio can help enterprises of all sizes take advantage of enterprise-strength security services.

Background

Human cybersecurity experts can no longer keep up with the volume, variety and level of sophistication of cyberattacks – whether those attacks come from external or internal sources. The sheer number of attacks are just too many; and the methods, approaches, scams and viruses are just too varied and are becoming even more sophisticated. Adding to this, data is now moving through amorphous clouds; or being accessed by mobile devices – making it even more difficult to protect data at rest or on the fly. And new technologies such as the Internet-of-Things (IoT) introduce new access points and vulnerabilities that can potentially be exploited by cybercriminals.

Given this backdrop, how can enterprises better secure data? The traditional approach has been to implement an enterprise security strategy that puts in place policies and procedures that ensure that data is handled in a secure fashion – and that puts in place measures (such as firewalls and data encryption) that ensure the integrity of the systems, networks and data. By putting in place policies that limit human errors, that help overcome social engineering exposures and that discourage the misuse of technology, security experts can better focus on the task of looking for and/or protecting against internal and external breaches.

The problems with the traditional approach, however, are:

- To keep up with the volume of internal/external cyberattacks, an army of highly skilled security experts are required;
- It's hard to find the deeply skilled individuals needed to fight cybercrime;
- Deep skill sets can be very costly;
- Humans may not be able to respond as quickly to vulnerabilities as systems; and,
- Humans may not find all vulnerabilities.

To address these problems, business communities around the world are collaborating – sharing attack and vulnerability information in an effort to catalog vulnerabilities and threats in real time. Security software vendors are also "analytics-enabling" their applications, making it possible for systems to analyze vast amounts of monitored data, looking for anomalies that can then be addressed by human security experts. And some security software vendors are starting to exploit machine learning and cognitive computing technologies that can take advantage of large "corpuses" of data to identify new threats or find new patterns – and, in some cases, recommending corrective actions.

IBM's Security Strategy: The Collaborative, Cognitive and Cloud Foundations
IBM's security strategy is focused on:

1. Working *collaboratively* with industry partners and customers to tackle the cybersecurity problem;
2. Enriching its software portfolio with analytics capabilities – and greatly enhancing its offerings with "Watson" (the name of the company's cognitive computing environment) *cognitive computing* services; and,
3. Delivering its solutions in both traditional on-premises form as well as via the *cloud as SaaS and managed service* offerings.

The Collaborative Element
IBM's collaboration story starts with the company's X-Force threat intelligence research. IBM's X-Force research team maintains one of the largest and most authoritative vulnerability databases in the computing industry – a database that combines IBM threat research findings with other research sources including publicly disclosed data and commercial vulnerability data. The purpose of this X-Force database is to provide preemptive information to customers to help them stay ahead of vulnerability threats. X-Force updates are delivered through security content updates to customers who use the service. The X-Force Exchange platform serves as a means to engage clients and the general public by providing cloud access to threat intelligence, enabling users to share insights and collaborate with peers. The X-Force organization also shares its findings via IBM X-Force Threat Intelligence Reports, X-Force Research reports, and X-Force topical research papers.

> ***What is important here is that IBM has created an organization dedicated to identifying threats – and has opened its database to clients and the general public. Users of this database can access humongous IBM's X-Force database and share the latest intelligence with peers in order to preemptively deal with threats in real-time. Also important – the X-Force database is "global", comprised of feedback from all around the globe (some vendors also maintain threat databases – but those databases are sometimes regionalized and compartmentalized).***

Over the past several months IBM has introduced several new ways to collaborate, including:

- IBM's acquisition of *Resilient*, a collaboration platform where internal and external security executives join together using a playbook, offering users an approach to resolve vulnerability threats by collaborating with a security operations center (SOC);
- The *X-Force Command Cyber Range* – an environment that simulates cyberattacks, allowing customers to train on methods of identifying attacks and responding to them;
- An upgrade to IBM's SOC in Atlanta, a facility that handles over 35 billion security events per day – and the introduction of a new SOC in Cambridge, Massachusetts – both sites collaborate with IBM customers;
- The formation of the company's *X-Force IRIS team* (incident response and intelligence service) – with more than 100 cybersecurity consultants located around the world who can work with customers to identify the sources of cyberattacks, and help defend and remediate security issues; and,
- The *IBM App Exchange* – a site where third parties can work with IBM to enhance their software and deliver new security application solutions (current number of solutions is 88).

Cognitive

The two major benefits of cognitive security are that machines can find anomalies more quickly than humans – thus improving response-to-threat time; and, analytics/cognitively-driven machines are capable of identifying intrusion patterns that humans simply don't notice.

In days gone by, the battle of securing enterprise data was fought using firewalls; endpoint protection; anti-virus software; authentication and authorization techniques – and largely involved using humans to thwart external and internal network security breaches. In the future, security administrators will have a deep learning assistant – Watson – to help secure systems/network infrastructure, protect data and resist intruders.

IBM COGNITIVE SECURITY OPERATIONS CENTER WITH WATSON FOR CYBER SECURITY

Currently, as part of its "Cognitive SOC" (security operations center) offerings, IBM has cognitively-enabled its "QRadar Advisor" – now known as "QRadar Advisor with Watson"; its MaaS360 (Mobility-as-a-Service) management environment for smartphones, tablets, laptops, IoT devices and other endpoints; and its BigFix Detect endpoint detection and response environment. And it is reasonable to assume that IBM will also cognitively enable its recently acquired i2 visual investigation and analysis environment; its AppScan vulnerabilities analysis environment; its Resilient Systems operations and response platform; and its Trusteer phishing detection engine in short order. It is also reasonable to assume that numerous other security products in IBM's broad security portfolio will become "Watson-enabled" – as will the more than 400 security offerings coming from IBM partners over time.

What we are talking about here is a major shift in security management – a shift where a virtual assistant greatly augments the knowledge base of human administrators – making them far more efficient and effective at their jobs. Cognitive computing is on a path to become pervasive in the security community.

A closer look at the existing cognitively-enabled Cognitive SOC programs shows that QRadar Advisor with Watson shows IBM's QRadar formulating a "threat query" which it forwards to Watson for Cyber for additional analysis. Watson for Cyber Security searches its corpus of structured and unstructured data– and it searches for other threat entities that may be related to an incident. The information gleaned by Watson for Cyber Security is then refined by QRadar – using insights found by QRadar, by Watson for Cyber Security and by the security administrator to identify the cause of the incident. With all of this information, a security administrator can better rectify a given problem.

IBM's BigFix is an endpoint detection and response environment, designed to identify malicious behavior at the point where external threats begin – on the external facing network. When used with Watson for Cyber Security, the combo can deliver targeted remediation to endpoints that have been compromised quickly – within minutes – helping cut off cyberattacks.

IBM's MaaS360 Advisor with Watson works in conjunction with the Watson cognitive computing environment to identify potential policy and application security improvements; to proactively address vulnerabilities in real time – and it uses peer benchmarks to make tailored recommendations. This service can ask Watson to identify policies on mobile devices, take a baseline of policies, look for ongoing opportunities to protect users. Watson can also be used to critique a client's mobile security policies.

IBM's Trusteer phishing engine will work with Watson to assess Web pages and add suspects to a blacklist if suspicious URLs are deemed risky.

Cloud
In March, 2017, *Clabby Analytics* attended IBM's "Interconnect 2017" conference – the company's big cloud exposition. At this event, IBM showed an integrated, secure, cohesive Watson/analytics hybrid cloud environment on which a variety of IBM software solutions can run. The design of this environment is distinctly different from the design of competing clouds that lack similar deep cognitive and analytics elements.

On the demonstration floor of the conference, there were dozens of formerly on-premises software products from IBM's rich portfolio of home grown analytics, transaction processing and integrated software solutions that had been moved to the company's enterprise-strength hybrid cloud. It is clear that the company has an initiative underway to move as many applications as can be rationalized to the company's analytics/cognitive hybrid cloud environment. Further, we talked with IBM representatives who are specifically charged with aggressively recruiting 3rd party software suppliers to build their solutions as service deliveries on IBM hybrid clouds.

In days gone by, security was an "on premises" problem. Enterprises purchased software to secure firewalls, to authorize users, to authenticate users, to prevent virus intrusion, and so on. But with the volume, variety and level of sophistication of incursions or attempted incursions, securing the enterprise perimeter as well as protecting enterprise data from internal malfeasance has become far too difficult for some enterprises – especially small- and mid-sized businesses. Accordingly, IBM is now offering managed security services through its cloud. And the business community is responding affirmatively – IBM's security division posted 14% year-to-year growth in cloud deliver services last year.

What Security Services Does IBM Deliver?
IBM's security services fall into seven categories:

1. Data application security services;
2. Offensive security testing;
3. Incident response and intelligence services;
4. Identity and access management;
5. Infrastructure and endpoint security;
6. Security strategy, risk and compliance; and,
7. Security intelligence and optimization.

IBM's data and application security services help secure data and applications. The company's offerings are based on its Guardium offerings (see this *Clabby Analytics* report for further details on the Guardium line). The company also offers application security on cloud consulting services.

IBM's offensive security testing services include a programmatic approach to security testing of all types, including human, hardware, IoT, application and infrastructure. The IBM X-Force Red portal helps provide visibility into asset vulnerabilities and offensive security reporting facilities.

IBM X-Force incident response and intelligence services are backed by an organization that helps prepare clients to instantly respond to security incidents. The services offered include a proactive retainer program known as IBM X-Force IRIS Vision Retainer and cybersecurity consulting services to deal with active threats.

IBM's identity and access management services protect against breaches, and include identity and access strategy and assessment, cloud identity, and insider threat protection services.

IBM's infrastructure and endpoint security aim at transforming existing email, Web, network, server and endpoint environments into modern, well secured environments through managed security services, cloud security services, network protection services (such as a managed firewall service), and through managed detection and response services.

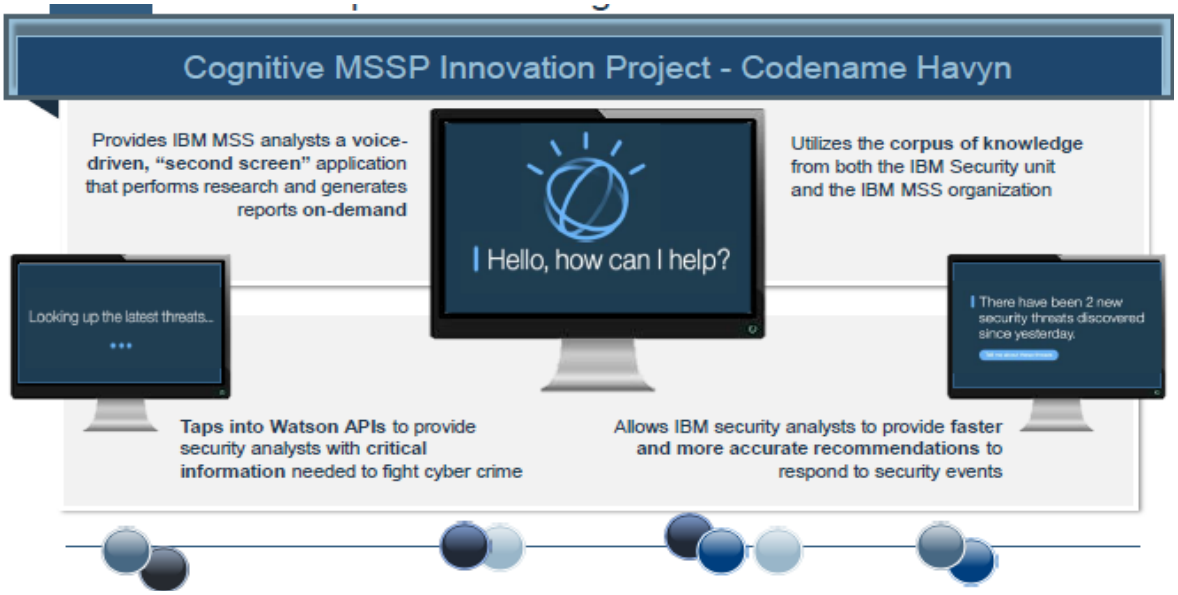
The company's security strategy, risk and compliance service aims at meeting regulatory requirements. This service makes recommendations for the better management of risks, compliance and governance – and includes IBM's GDPR privacy service.

IBM's security intelligence and optimization service aims at proactively detecting and prioritizing threats. This service is designed to assist clients throughout the Threat Management lifecycle, including strategic security operations center planning and deployment, 24x7 threat monitoring and analysis, rules and use case management, and closed-loop intelligence processing. This offering also includes services from the IBM X-Force Command Centers such as the IBM X-Force Hosted Threat Analysis Service. Managed SIEM and strategic SCO consulting are two important services in this area.

A Closer Look at the Watson Assistant: The Havyn Project

Think of security analysts managing their systems, network, application, database, endpoint, mobile and IoT environments using two screens. Their screen runs a variety of security and analytics software – while an adjoining screen, the Watson virtual assistant, combs through mountains of data (such as the IBM XForce Exchange vulnerabilities database), through reports, through blogs and other sources of structured and unstructured information looking for new insights into a given problem. The security analyst talks to the Watson assistant, no need to move to another keyboard to interact. Security programs on the security analyst's desk can also interact programmatically with the Watson assistant by tapping into Watson application program interfaces (APIs). Using this approach, security analysts are now better able to make more informed decisions; plus the Watson assistant may provide that analysts with new insights such as insights into a benign activity or pattern that may prove to be a real threat. These activities are illustrated in Figure 1 – and they represent the future of security administration in the cognitive security era.

Figure 1 – The Watson Security Assistant



Source: IBM Corporation – March, 2017

Summary Observations

The primary message in this report has been that analytics/cognitive-driven technologies are in the process of changing the IT security industry. Security software combined with analytics and cognitive computing is poised to aid security administrators attempting to deal with overwhelming volumes of security information, a wide variety of attack strategies and new sophisticated attack methods.

What we observed in this report is that a new era of analytics/cognitive security administration is underway. We described how a "*Watson assistant*" – "IBM's Watson for Cyber Security" – is now playing an increasingly important role in securely managing the IT environments of the future.

We believe that enterprises IT executives will benefit from the use of cognitive technologies in two ways:

1) They will be able to drive down human-related security costs by providing humans with analytics/cognitive tools that will make it possible to better manage cyber threats. Accordingly, fewer people will be needed to manage IT security; the problem of finding "deep skills" will be mitigated through machine skills augmentation; and lesser skilled/lesser cost individuals will be able to fill in the security employment gaps; and,
2) Human IT security managers will become more efficient. Security software combined with Watson for Cyber Security will help find the sources of problems more quickly, identify possible ways to remediate problems – and find problems that humans didn't even know existed.

We also noted that IBM's security strategy is based on three initiatives: 1) community collaboration; 2) cognitive computing; and, 3) cloud integration and service delivers. It should be known that this strategy appears to be working extremely well for IBM, as the company can now boast the #1 position in enterprise security software sales; security products and services have generated more than $2 billion for the company; and the company's security revenues are significantly outpacing competitors in year-to-year growth (especially with particularly strong SaaS performance).

The way we see it, the combination of IBM's security software portfolio, industry third party security solutions – and Watson analytics/cognitive computing facilities – will change the way that IT security is delivered and administered in the future. Enterprises looking to reduce security exposure and risk – and looking to reduce security skills shortages and costs – would be well served to start building their "Cognitive SOC" strategy based on IBM's cognitively-enabled portfolio today.

Clabby Analytics
http://www.clabbyanalytics.com
Telephone: 001 (207) 239-1211