The Cognitive Era of Security

OUT THINKING THREATS BY LEVERAGING AUTOMATION FOR BETTER HUMAN DECISION MAKING

Peter Allor
Senior Security Strategist, IBM Security

18 October 2016
IT transformation
Today’s security drivers

- Advanced Attacks
- Innovation
- Skills Gap
- Compliance
- Human Error
Traditional security practices are unsustainable

85 security tools from 45 vendors

1.5 MILLION unfilled security positions by 2020

68 PERCENT of CEOs are reluctant to share incident information externally
Hard to stay safe

<table>
<thead>
<tr>
<th>Year</th>
<th>Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td>800+ Million</td>
</tr>
<tr>
<td>2014</td>
<td>1+ Billion</td>
</tr>
<tr>
<td>2015</td>
<td>Unprecedented Impact</td>
</tr>
</tbody>
</table>

- Average time to identify data breach: 201 days
- Average cost of a U.S. data breach: $7M
The Changing Dynamics of Cyber Threats

Hackers no longer need to be experts at:

- Programming languages
- Coding skills
- IT literacy
- Network concepts
- Fraud knowledge
Increasing Variety of Threats

Individuals and Organizations have to contend with:

- Legacy
- Innovation
- Social Networks
- Business Imperatives
Sources of Economic Imbalance in Cyber Security

- Must defend against multiple threat actors
- Must constantly maintain and monitor defensive measures
- Greater demand for skilled resources increases costs
- Accuracy and responsiveness are essential

- Can target multiple vulnerable organizations
- Identify and exploit a single lapse in defensive measures
- Tools and services reduce the skills required to engage in malicious activities
- Option to employ multiple methods of attack over a period of time
Approaches to Shift the Economic Balance

Source: David Bianco

- Furious
- Frustrated
- Inconvenienced

- Hash Values: Trivial
- IP Addresses: Easy
- Domain Names: Simple
- Network/Host Artifacts: Annoying
- Tools: Challenging
- TTPs: Tough!
### Three gaps to address – in intelligence, speed and accuracy

<table>
<thead>
<tr>
<th>Intelligence gap</th>
<th>Speed gap</th>
<th>Accuracy gap</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>#1</strong> most challenging area due to insufficient resources is threat research (65% selecting)</td>
<td><strong>The top cybersecurity challenge today and tomorrow is reducing average incident response and resolution time</strong></td>
<td><strong>#2</strong> most challenging area today is optimizing accuracy alerts (too many false positives)</td>
</tr>
<tr>
<td><strong>#3</strong> highest cybersecurity challenge today is keeping current on new threats and vulnerabilities (40% selecting)</td>
<td>This is despite the fact that <strong>80%</strong> said their incident response speed is much faster than two years ago</td>
<td><strong>#3</strong> most challenging area due to insufficient resources is threat identification, monitoring and escalating potential incidents (61% selecting)</td>
</tr>
</tbody>
</table>

**Addressing gaps while managing cost and ROI pressures**
The next era of security

PERIMETER CONTROLS

INTELLIGENCE and INTEGRATION

COGNITIVE, CLOUD, and COLLABORATION
Unlock new possibilities.

The world’s first Cognitive analytics solution using core Watson technology to help analysts understand, reason, and learn about security topics and threats.
Application of Cognitive Computing to Cyber Security

- Understanding of natural language, images and other sensory information
- Complex reasoning and deep interaction with experts
- Hypothesis and question generation across arbitrary domains; meta-heuristic to automate algorithm choices
Watson on Jeopardy!
Watson
Cognitive systems scale knowledge

**Understand**
Adapt and make sense of all data; “read” text, “see” images and “hear” natural speech with context

**Reason**
Interpret information, organize it and offer explanations of what it means, with rationale for the conclusions

**Learn**
Accumulate data and derive insight at every interaction, perpetually
Most security knowledge is **untapped**…

**Traditional Security Data**
- Security events and alerts
- Logs and configuration data

**Human Generated Knowledge**
- User and network activity
- Threat and vulnerability feeds

**A universe of security knowledge dark to your defenses**
- Threat intelligence
- Research documents
- Industry publications
- Forensic information
- Conference presentations
- Analyst reports
- Blogs

- Webpages
- Wikis
- News sources
- Wikis
- Newsletters
- Tweets
Evolving to meet current and future security operations needs with cognitive enabled cyber security

Cognitive security solutions harness the power of **language comprehension** in performing threat research, apply **deductive reasoning** and **self-learning** capabilities to direct security practitioners to contextually relevant information and deliver advise on the course of action.
Manual Activities of a SOC Analyst

Review your security incidents in QRadar

Review the data (events / flows that made up that incident)

Expand your search to capture more data around that incident

Decide which incident to focus on next

Get the name of the Malware

Pivot the data multiple ways to find outliers (such as unusual domains, IPs, file access)

Start another investigation around each of these IPs.

Take these newly found IOCs from the internet and search from them back in QRadar.

Find other internal IPs are potentially infected with the same Malware.

Review the payload outlying events for anything interesting (domains, MD5s, etc)

Search X-Force Exchange + Google + Virus Total + your favourite tools for these outliers / indicators. Find new Malware is at play

Search more websites for information about IOC (indicators of compromise) for that Malware
Take these newly found IOCs from the internet
QRadar Advisor with Watson for Cyber Security unlocks a new partnership between security analysts and their technology.

Security Analytics:
- Data correlation
- Pattern identification
- Thresholds
- Policies
- Anomaly detection
- Prioritization

IBM Watson for Cyber Security

Corpus of Knowledge

Understand | Reason | Learn

Watson For Cyber Security

- Threat identification
- Additional indicators
- Relationships
- Evidence

- Alerts
- Security Events and anomalies
- User activity
- Vulnerabilities
- Configuration
- Other
Practical Application to Present Day Use Cases

Enrichment of the security incident with insights from Watson for Cyber Security followed by further refinement by QRadar Advisor is empowering our customers to better identify and understand sophisticated threats in their environment.

<table>
<thead>
<tr>
<th>Identify</th>
<th>Understand</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patient Zero</td>
<td>Name, Family, Sources, Delivery Method, Impact</td>
</tr>
<tr>
<td>Compromised Hosts</td>
<td>Target Vulnerabilities, Objective, Attack Sequence, Scope</td>
</tr>
<tr>
<td>Misused Privileged Identity</td>
<td>Target System, Motive, Objective, Duration</td>
</tr>
</tbody>
</table>
Revolutionizing how security analysts work

Gain powerful insights
- Tap into the vast array of data to uncover new patterns
- Get smarter over time and build instincts

Reduce the security skills gap
- Triage threats and make recommendations with confidence, at scale and speed

Save time and costs
- Handle mass minutiae, so you can work on offense not endless defense
Goal: Shorten the Effective Lifecycle of a Cyber Threat

Leverage Cognitive techniques that mimic human intuition around advanced threats
There are numerous potential use cases where we could envision cognitive security playing a key role.

- **Enhance your SOC analysts**
- **Speed response with external intelligence**
- **Identify threats with advanced analytics**
- **Strengthen application security**
- **Improve (Lower) enterprise risk**
# Evolving to Cognitive

Scale and magnify human cognition by leveraging automation

<table>
<thead>
<tr>
<th>Technique</th>
<th>Outcome</th>
</tr>
</thead>
</table>
| **Human-centric communications** | • Advanced visualizations  
• Interactive vulnerability analysis, risk assessment, remediation, possible attribution | • Ease the task of the security analyst |
| **Natural language sources and processing** | • Textual descriptions of past and current security breaches  
• Integrated vulnerability data per application and OS version | • Consolidate threat intelligence |
| **Continuous machine learning** | • Deep learning and ensemble weighting techniques  
• Continuous extraction of features and patterns | • Context in real time  
• Improve threat analyst decision-making |
| **Evidence-based reasoning** | • Provide evidence  
• Spot flawed logic | • Enable analysts to weigh possible alternative outcomes  
• Improve human reasoning |
# IBM Security Strategy

## LEAD in strategic domains

### Security Operations and Response
- Incident Response
- Security Intelligence and Analytics
- Vulnerability and Patch Management
- Endpoint and Network Protection
- User Behavior Analytics

### Information Risk and Protection
- Cloud Security
- Mobile Security
- Identity Governance and Access Management
- Data Protection
- Application Security
- Advanced Fraud Prevention

### Security Research and Threat Intelligence

---

## SUPPORT the CISO agenda
- Advanced Threats
- Cloud
- Mobile and Internet of Things
- Compliance Mandates
- Skills Shortage

## ACCELERATE with key innovation
- Cognitive
- Cloud
- Collaboration

---

*IBM Security Strategy*
A Global Leader in Enterprise Security

IBM Security

- #1 in enterprise security software and services*
- 7,500 people
- 12,000+ customers
- 133 countries
- 3,500+ security patents
- 15 acquisitions since 2005

*According to Technology Business Research, Inc. (TBR) 2016
To get a Copy of this presentation and More information

1. Fill out the Form
2. Get your gift
3. Visit IBM Lounge and Get Free LinkedIn Photo
Appendix and resources
IBM Security Solution offers

http://www.maas360.com/

IBM MaaS360 is first EMM to achieve FedRAMP
Learn More > Watch the Video >

Take the Free 30-Day Trial
Start Your Trial>

Latest in Secure Mobile Technology


IBM X-Force® Exchange is a cloud-based threat intelligence platform. It enables you to rapidly research the latest global security threats, aggregate actionable intelligence and collaborate with your peers. IBM X-Force Exchange is supported by one of the most recognized security research teams in the world—IBM X-Force.

First Year is FREE

IBM Security AppScan Standard resources

Software Trial: IBM Security AppScan Trial
Try a full-featured version of the software.
Try trial


30-Day Trial: IBM Security AppScan Mobile Analyzer
Try the software

IBM Security Solution offers

Welcome

This interactive model is based upon a Forrester Consulting study, The Total Economic Impact of IBM Security Guardium. Working with IBM customers, Forrester identified and quantified key benefits of investing in Guardium:

- Improved process efficiency in meeting security and compliance requirements.
- Reduced cost to recover from a breach.
- Reduced likelihood of regulatory fines.
- Avoided cost of labor to develop in-house monitoring and auditing capabilities.
- Avoided cost of labor for ongoing support of in-house monitoring and auditing capabilities.

---

IBM Security Guardium Vulnerability Assessment

Evaluation Edition

Get the download


---

IBM Security QRadar named a leader in Gartner's SIEM Magic Quadrant

Get the report


---
IBM Security Solution offers

Online Demo: IBM Cloud Security Enforcer
Respond rapidly to cloud-based threats

Solution Brief: Secure cloud application usage with IBM Cloud Security Enforcer
Safely connect users to cloud applications and help protect the business against cloud-based threats


http://www.ibm.com/common/ssi/cgi-bin/ssialias?subtype=SP&infotype=PM&htmlfid=WGS03064USEN&attachment=WGS03064USEN.PDF
A new way to think about security

IBM Security
Intelligence. Integration. Expertise.

**Intelligence** is the new defense
It helps prevent threats faster and make more informed decisions

**Integration** is the new foundation
It puts security in context and automates protection

**Expertise** is the new focus
It is essential to leverage global knowledge and experience to stay ahead
Learn more about IBM Security

IBM Security

Intelligence. Integration. Expertise.

No. 1 enterprise security vendor in total revenue

25 industry analyst reports rank IBM Security as a LEADER

130+ countries where IBM delivers managed security services

12K+ clients protected including...

90% of the Fortune 100 companies

Visit our website ibm.com/security

Watch our videos on YouTube IBM Security Channel

Read new blog posts SecurityIntelligence.com

Join IBM X-Force Exchange xforce.ibmcloud.com

Follow us on Twitter @ibmsecurity
THANK YOU
Background
Watson saves the security analyst valuable time

Watson continuously crawls the internet for all information related to security in blogs, reports, advisories, and vulnerability disclosures.
Watson helps uncover new previously unknown connections

Watson aggregates local analytics with its own insight and quickly determines two possible malware families and an exploit kit (Locky or Dridex)
Watson determines the specific campaign (Locky) and discovers more infected endpoints, sending results to incident response team.
Watson for cyber security will significantly reduce response time

Manual threat analysis

IBM Watson for cyber security assisted threat analysis

Quick and accurate analysis of security threats, saving precious time and resources
The Result: Watson for cyber security will enable breakthrough insights after analyzing unstructured articles and other corpus data in minutes.

I found three observables relationships that share indicators with the Locky campaign. Let me show you the relationships and the reasoning process.
With the help of Watson, Rafael can become more proactive

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

- Faster investigations
- Clear backlog easier
- Increased investigative skills
- Heavy lifting done beforehand

Rafael
Security Analyst

Less time on the mundane, more time being human!
IBM Watson for cyber security and IBM QRadar

IBM QRadar Security Intelligence Platform

QRadar sends Watson a pre-analyzed security incident

Watson for cyber security

Watson automatically provides response back to Security Analyst on probability of threat and best practices, resulting in substantial time savings

IBM QRadar Security Intelligence Platform

Internal Security Events and Incidents

External Security Knowledge
Watson enables greater insights by ingesting extensive data sources.

**INGEST**

- Threat databases
- Research reports
- Security textbooks
- Vulnerability disclosures
- Popular websites
- Blogs and social activity
- Other

**LEARN**

**TEST**

**EXPERIENCE**

IBM Watson for cyber security

Corpus of knowledge

- Security events
- User activity
- Configuration information
- Vulnerability results
- System and app logs
- Security policies
- Other

Enterprise Security Analytics

Correlated enterprise data

Human Generated Security Knowledge

Sourced by available IBM Security and IBM Research
Not just a search engine, we’re teaching Watson to understand and interpret the language of security

Rich dictionaries enable Watson to link all entity representations

<table>
<thead>
<tr>
<th>Threat Name</th>
<th>Zeus / zbot</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hash</td>
<td>6d2a1b03-b216-4cd8-9a9e-8827af6ebf93</td>
</tr>
<tr>
<td>Infection Methods</td>
<td>Spam messages, drive-by downloads, browser exploitation</td>
</tr>
<tr>
<td>IoC Artifact</td>
<td>Windows\system32\twext.exe</td>
</tr>
</tbody>
</table>
Machine learning enables Watson for cyber security to teach itself

**MALWARE**
*Entity*

**FUNCTIONALITY**
*Entity association cause*

**BEHAVIOR**
*Relating verb*

**RULE**
*One malware to many effects*

- **Locky** is ransomware distributed via malicious .doc files attached to spam email messages
- Known **functionality** includes encrypting files on a victim’s computer and requiring the victim to pay ransom to decrypt the files
- **Zeus (or zbot)** is a strain of malware that creates a botnet to collect massive amounts of stolen information and execute attacks
- Known **functionality** includes stealing bank credentials, and giving attackers access and control of your PC
Beyond mere algorithms, Watson evaluates supporting evidence

**Question**: What vulnerabilities are relevant to **CryptoLocker** infections?

- Research reports
- Security websites
- Publications
- Threat intelligence
- Internal scans
- Asset information

**Score and Weigh**:
- Quantity
- Proximity
- Relationship
- Domain truths / business rules
Imagine if you could…

**PROTECT** against tomorrow’s risks, today
How do I get started when all I see is chaos?

- Threat sharing
- IP reputation
- Incident and threat management
- Malware protection
- Workload protection
- Device management
- Sandboxing
- Network visibility
- Content security
- Log, flow, data analysis
- Fraud protection
- Identity management
- Virtual patching
- Data access control
- Access management
- Criminal detection
- Privileged identity management
- Vulnerability management
- Anomaly detection
- Incident response
- Data monitoring
- Application security management
- Antivirus
- Entitlements and roles
- Endpoint patching and management
- Transaction protection
- Application scanning
- Cloud access security broker
- Anomaly detection
- Incident response
- Indicators of compromise
- Application security management
- Antivirus
- Entitlements and roles
- Endpoint patching and management
- Transaction protection
- Application scanning
- Cloud access security broker
An integrated and intelligent security immune system

- **Security Ecosystem**
  - Endpoint patching and management
  - Antivirus
  - Malware protection

- **Threat Intelligence**
  - Incident and threat management
  - Firewalls
  - Sandboxing
  - Virtual patching
  - Network visibility

- **Network**
  - Incidents and threat management
  - Sandboxing
  - Virtual patching
  - Network visibility

- **Endpoint**
  - Log, flow, data analysis
  - Anomaly detection

- **Security Analytics**
  - Vulnerability management
  - Incident response

- **Mobile**
  - Transaction protection
  - Device Management
  - Content security

- **Data and Apps**
  - Data monitoring
  - Data access control
  - Application scanning
  - Application security management

- **Cloud**
  - Cloud access security broker
  - Workload protection

- **Identity and Access**
  - Privileged identity management
  - Entitlements and roles
  - Access management
  - Identity management

- **Advanced Fraud**
  - Fraud protection
  - Criminal detection