Security at the Speed of A.I.

Chris Bontempo
Vice President, Marketing, Routes & Offerings
North America


IBM

Who is IBM Security?

- Largest enterprise cybersecurity provider
- Leader in 12 security market segments
- 8,000+ security employees
- 20+ security acquisitions
- 70B+ security events monitored per day

IBM Security can help transform your security program

Strategy and Risk

Advance Security Maturity
- Strategy and Planning
- Risk Assessments
- Advisory Services

Build Leadership and Culture
- X-Force Cyber Range
- X-Force Comes to You
- X-Force Cyber Tactical Operations Center

Threat Management

Detect and Stop Advanced Threats
- Security Operations Consulting
- X-Force Threat Mgmt. Services
- X-Force Red
- QRadar
- X-Force Detect

Orchestrate Incident Response
- Resilient
- X-Force IRIS

Master Threat Hunting
- i2 Intelligence Analysis
- QRadar Advisor with Watson

Digital Trust

Protect Critical Assets
- SDLC Consulting
- Data Protection Services
- Guardium
- Data Risk Manager
- Multi-cloud Encryption
- Key Lifecycle Manager

Govern Users and Identities
- Identity Mgmt. Services
- Identity Governance
- Cloud Identity
- Access Manager
- Secret Server

Deliver Digital Identity Trust
- Trusteer
- Cloud Identity

Secure Hybrid Cloud
- Infrastructure and Endpoint Services
- Hybrid Cloud Security Services
- QRadar Cloud Analytics
- Cloud Identity
- Guardium for Cloud

Unify Endpoint Management
- Endpoint Mgmt. Services
- MaaS360

Cybersecurity is a universal challenge

60%
growth in new vulnerabilities over last 2 years

11%
increase in cyber attacks in 2018

1.8 million
unfilled cybersecurity jobs by 2022

$6 trillion
lost to cyber crime over the next 2 years

With more cyber attacks targeting more vulnerabilities and not enough skilled cyber security specialists to fight back, where will we find solutions?

The cyber security industry will apply Artificial Intelligence to cyber security problems to address this challenge.

AI “Hype” and the need to establish trust

Nextgov

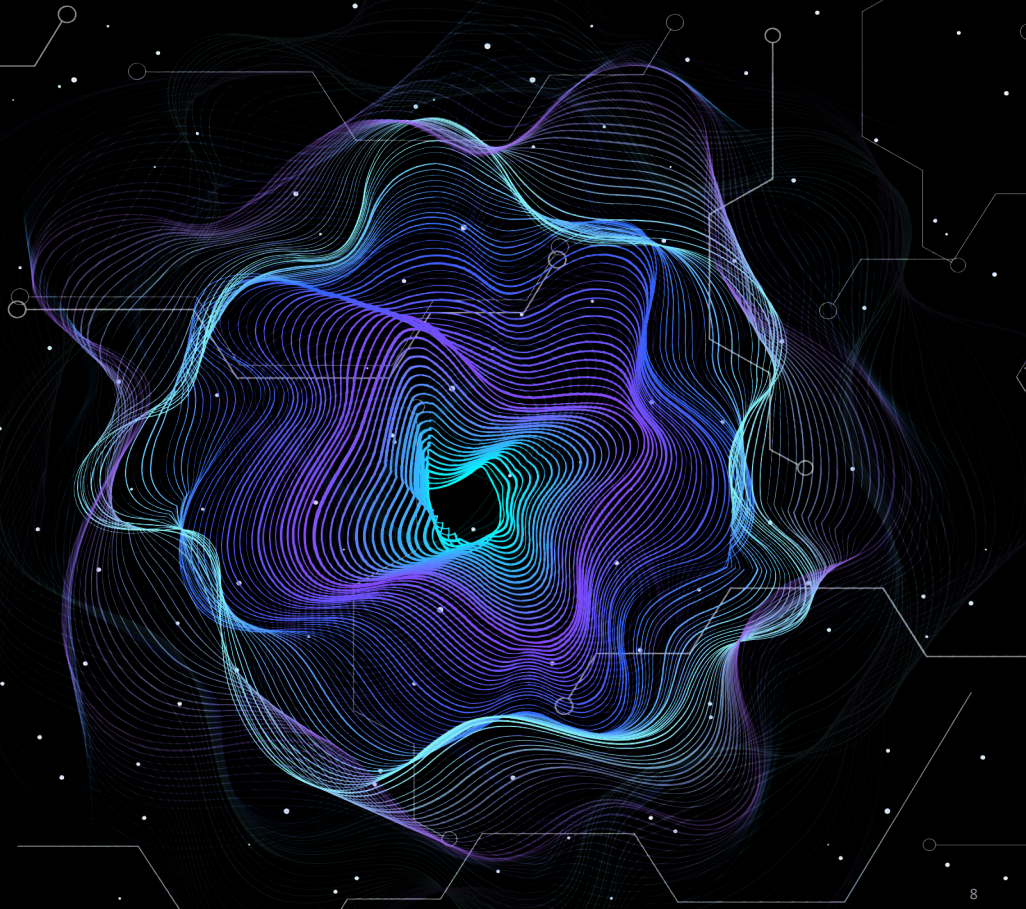
April 2019

The Promise
and Limitations
of AI in Cybersecurity

WIRED

April 2019

AI Can Help
Cybersecurity—
If It Can Fight
Through the Hype



AI misconceptions have resulted in low adoption rates

20%

of enterprises leverage AI

2019 Cyber Resilient Ponemon Report

35%....

AI hasn't had time to mature and my team isn't interested in being early adopters

27%....

Adopting AI is too complicated for my limited security team

Addressing AI bias for security

IBM helps
to eliminate AI bias
based on three key
factors

People

Making sure
we have the
necessary
skilled experts
to develop AI
in an unbiased manner

Algorithms

We have mature models and
utilize technology
like OpenScale that
help to monitor
and test algorithms
for bias

Data

We use large data sets
as part of the feedback loop
that help us not only tune
our AI but also check for bad
AI patterns on an
on-going basis

Threat actors use of AI

AI-powered attacks

Automate
Generate targeted phishing attacks on Twitter

Refine
Neural network powered password crackers

Evade
Generative adversarial networks learn novel steganographic channels

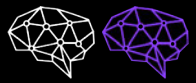
Attacking AI

Poison
Chatbot poisoning based on Twitter responses

Evade
Attacks on computer vision for facial recognition biometrics and autonomous vehicles

Harden
Genetic algorithms and reinforcement learning (OpenAI Gym) to evade malware detectors

Theft of AI

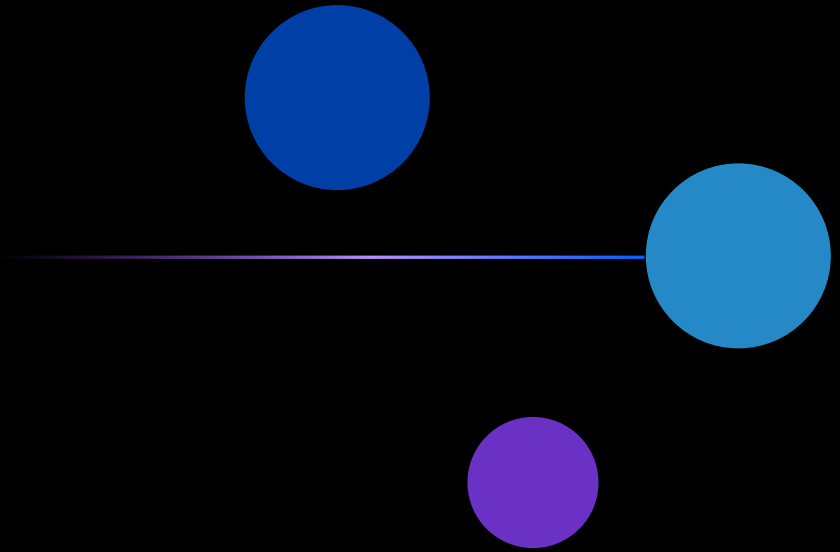


Theft
Stealing machine learning models via the public

Transferability
Practical black-box attacks learn surrogate models for transfer attacks

Privacy
Model inversion attacks steal training data

Security must innovate to keep pace with demand and surpass attack velocity



AI technologies can help you…

Learn

Scan and filter billions of structured and unstructured data sources to continually improve your threat and cyber risk knowledge.

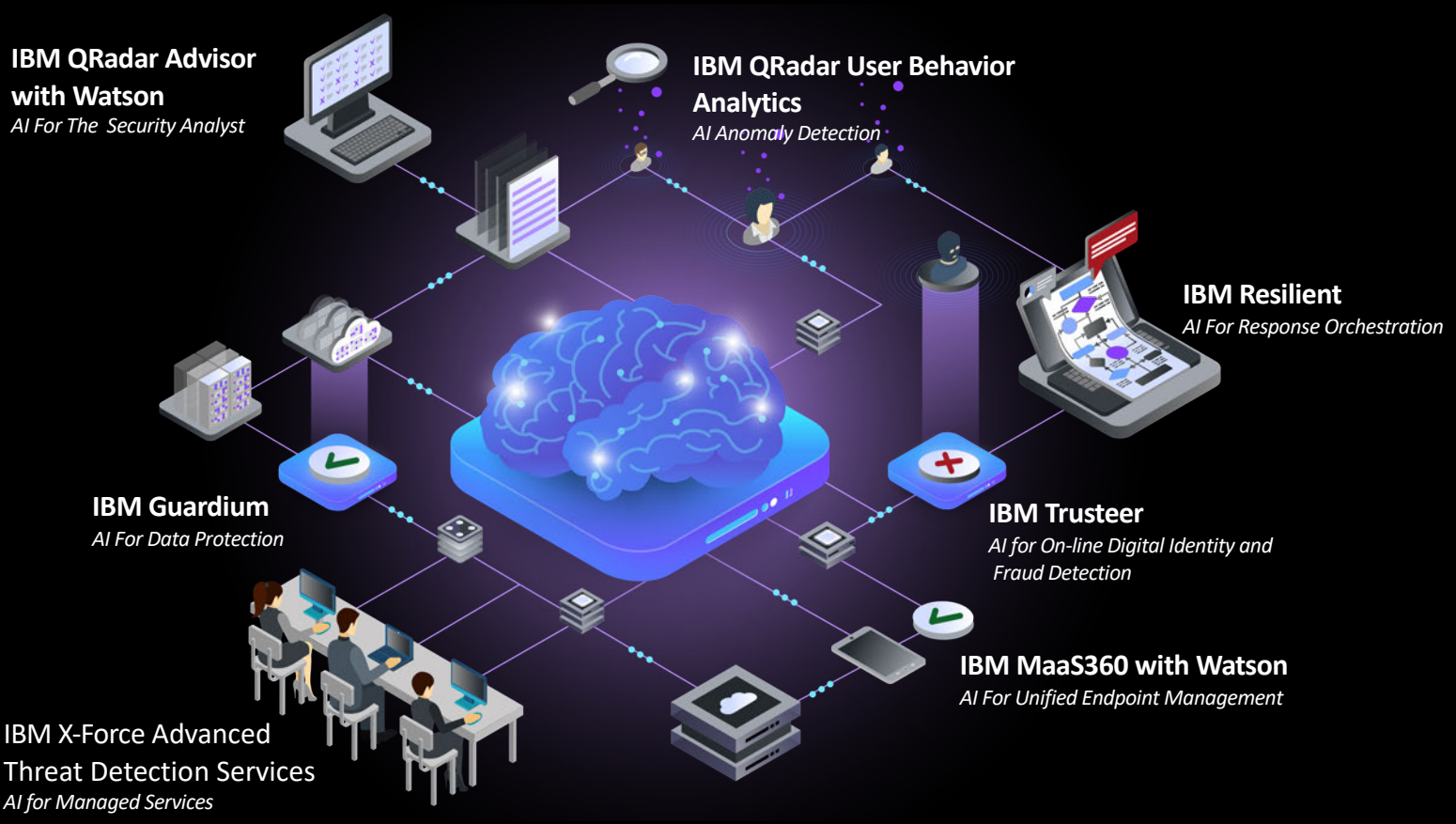
Reason

Gather insights and use reasoning at “machine” speed to correlate relationships between threats, allowing you to detect and respond to threats up to 60 times faster.

Augment

AI augments human intelligence, it doesn’t replace it. Eliminate time-consuming tasks and utilize curated risk analysis to reduce the amount of time it takes to make critical decisions and launch an orchestrated response.

IBM Security AI solutions since 2015



IBM Security at the speed of AI

Predictive analytics

Security and fraud teams can identify threats in real-time, mitigating risks and minimize customer impact as AI learns

Correlated threat intelligence

AI reasoning provides analysts with relevant information and threat data in seconds versus minutes

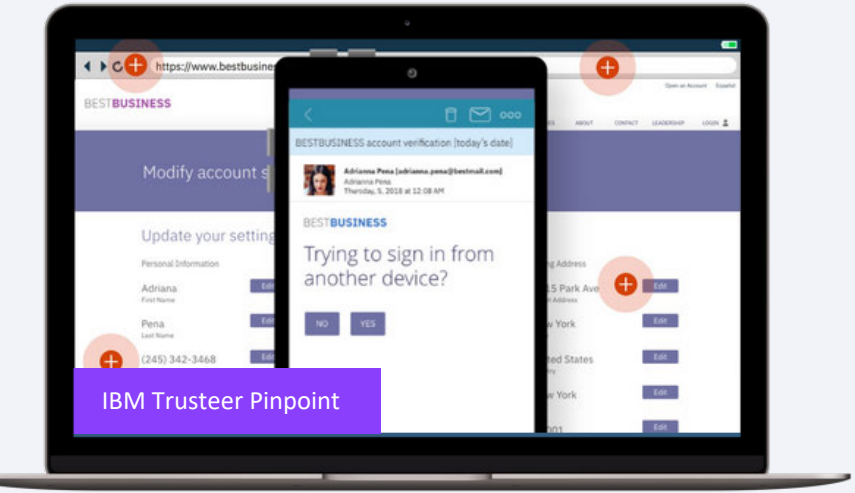
Trusted advisors and response

Augment your security teams so they can focus on critical items while automating response and notifications processes

Establish digital trust and prevent fraud

>85% detection of
account take over attempts
from IcedID malware redirect attacks

- Large US Bank



Predict

~50% **of institutions face losses every year from new and existing account fraud**

-

- AI can identify fraudulent and unauthorized access in real-time
  - Utilize embedded behavioral biometric analytics
- Manage digital identity and establish trust across the entire omnichannel customer lifecycle
- Create a frictionless user experience by applying AI to assess identity risk and authenticating as necessary

Automatically uncover the full scope of a security incident

"**Watson will come back within 3 to 4 minutes** with even some of the most complicated queries we run."

- Senior enterprise security analyst, technology solutions
  Forrester Total Economic Impact – June 2019

IBM QRadar Advisor with Watson

~50% of institutions face skills shortages leading to longer investigation and dwell times

-

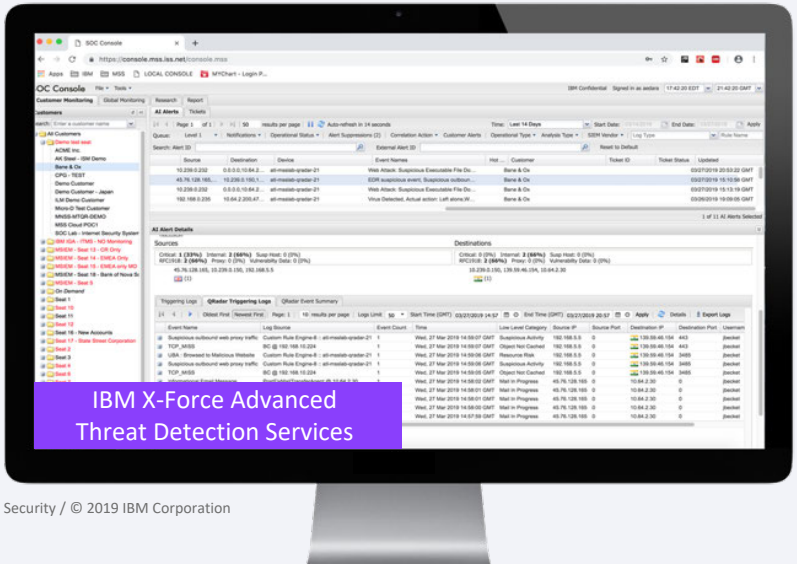
- Leverage AI to force multiply security team's investigation efforts
- Drive consistent and deeper investigations
  - Align incidents to MITRE ATT&CK
- AI allows for reduced dwell times
  – MTTD & MTTR
  - Act on contextualized Watson feedback using internal and external threat intelligence feeds

Focus on critical items while automating response and notifications

70-80%

automation of L1 monitoring cases

- IBM Managed Security Services, June 2019

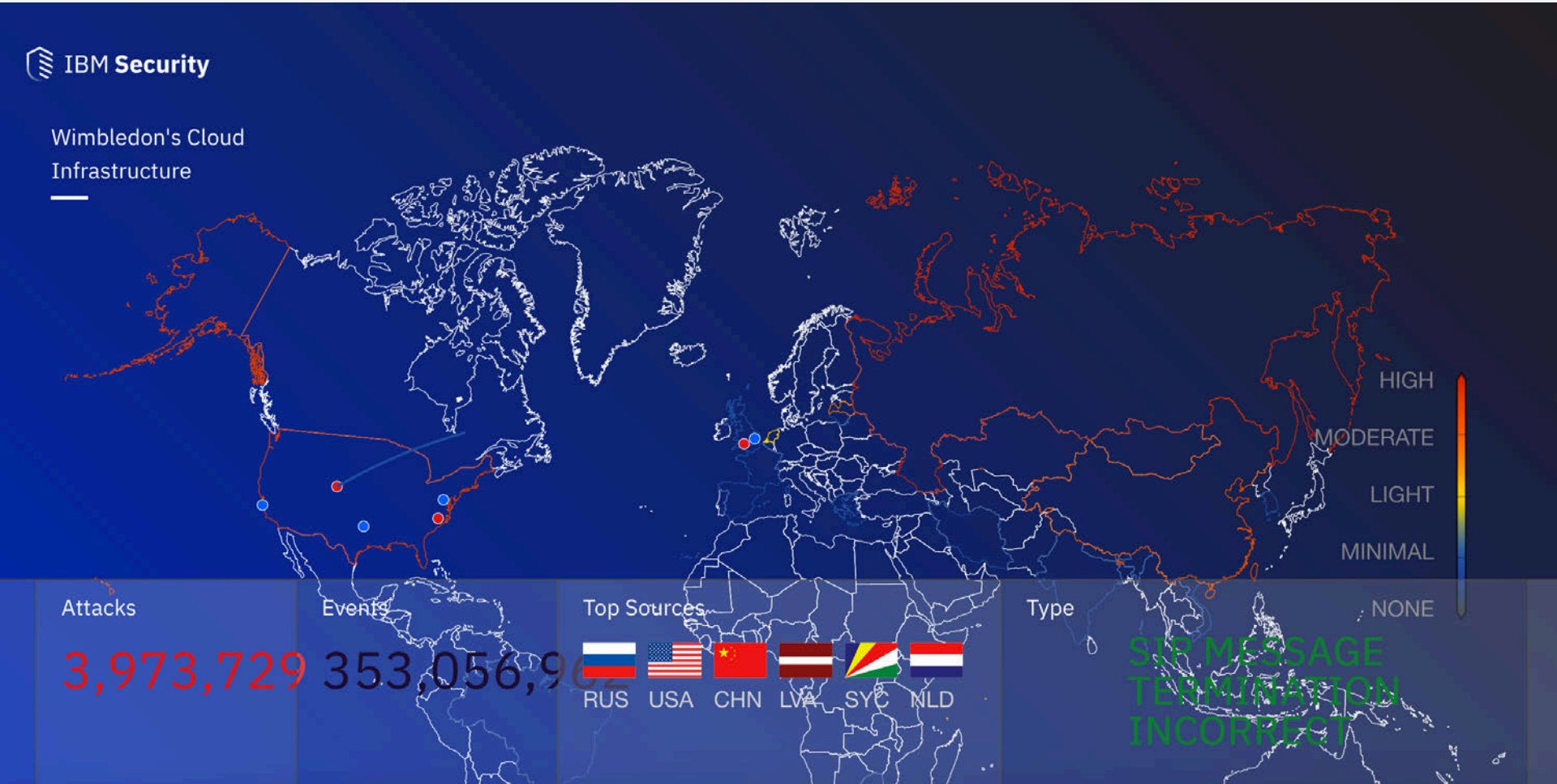


~70% of Tier 1 Cyber Analyst time spent chasing info & false positives; 45 minute wait time before triage process even starts

-

- AI is able to reduce analyst response time
  - Continually updated with analyst feedback
- Value added offense enrichment leading to reduced analyst handle time
  - AI uses 37 different predictors engineered from the offense data collected
- Higher accuracy and disposition consistency
  - Supervised machine learning classification algorithms predicting analyst response
- Reduced false positives and threat offense prioritization

A.I. in Action – protecting Wimbledon



IBM Security

Take your next steps with IBM Security

Download

the 2019 Ponemon Cyber Resilience Report

Save

X-Force IRIS's number 1-888-241-9812

Learn

How IBM Research is advancing AI www.research.ibm.com/artificial-intelligence/

Visit

the X-Force Cyber Range bit.ly/X-ForceCommand

Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube/user/ibmsecuritysolutions

IBM Security

IBM

Predictive Analytics Across Our Portfolio

What we predict…	Product	Models used	Inputs	Output
Insider Threats	QRadar UBA	Peer grouping, time-series, anomaly	Security logs and events	Risk score of users
Malicious Traffic	QRadar Network Insights	Random forest	Network data	Risk score of flows
Botnet Domains	X-Force DNS Analytics QRadar DNS Analytics	Multiple	DNS data, registrar info	Domain risk score and reputation
Vulnerable Code	AppScan Intelligent Code / Findings	Random forest, logistic regression	Scans from benchmark set of applications	New vulnerability rules, reduced false positives
Database Attacks	Guardium Outlier Detection	Anomaly, user and DB cluster	Sql queries, errors, file access activity	Abnormal activity, hourly risk score
Risky User Access	IAM Governance, Authentication	Outlier detection with peer group	IAM data, logs and UBA alerts	Risk score of users, apps
Fraudulent Users	Trusteer Behavioral Biometrics	Random forest	Keystrokes, app, mouse usage	Risk score of users
Phishing Websites	Trusteer Cognitive Phishing	Random forest	URLs and website content	Risk score of suspected sites

Intelligence Consolidation & Trusted Advisors

What we do…	Product	Models used	Inputs	Output
Security intelligence consolidation	Watson for Cybersecurity	Watson Natural Language Understanding	Unstructured content, web content	Cybersecurity contextual knowledge base
Automatic offense investigations	QRadar Advisor	Multiple	QRadar events	Root cause analysis, augmented context
Virtual Cybersecurity Analyst	IBM Havyn	Watson Speech	Voice, unstructured content, threat content	Contextual security information, spoken content
Mobile endpoint management advisor	MaaS360 Advisor	Watson	Unstructured content, threat alerts, etc.	Personalized mobile endpoint management recommendations
Mobile end-user self-service assistant	MaaS360 AI Assistant	Watson Speech	User commands, calendar and email contents, support knowledge base	Coordinates calendar and email activities; provides real-time end-user support
Advise threat disposition & automate action taken	X-Force Advanced Threat Detection Services	Gradient Bosting, Random Forest, Deep Learnng, Ensemble	SIEM alerts investigated & dispositioned by SOC analysts on rolling basis	Automatic threat disposition & escalation