AI and Analytics in Security Development

—

Mattias Johansson
Director of Development,
IBM Security

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

Global Security Centers

IBM X-Force Command Centers

Solution Development Centers | Security Research Centers

IBM Security Development Lab @Taipei

Established in 2010

- Network Security development center for IBM

The only Security CoE in China/HK/TW

- Developing products for IBM WW customers

A Lab of Innovations

- Accumulated 160+ patents in 9 years
- 7 IBM Master Inventors

Broad Coverage of IBM Security Portfolio

Threat Management

Detect and Stop Advanced Threats

- QRadar
- QRadar DNS Analytics
- QRadar App Assistant
- Mail Protector
- X-Force Exchange
- X-Force Red

Orchestrate Incident Response

- Resilient

Master Threat Hunting

- QRadar Advisor with Watson
- QRadar User Behavior Analytics

Digital Trust

Secure Hybrid Cloud

- Guardium for Cloud

What is AI?

Artificial Intelligence (AI) is the simulation of human intelligence using a combination of technologies

An AI system can:

1. Reason (make assumptions, test, predict)
2. Learn (feedback loop)
3. Convey information natural to humans

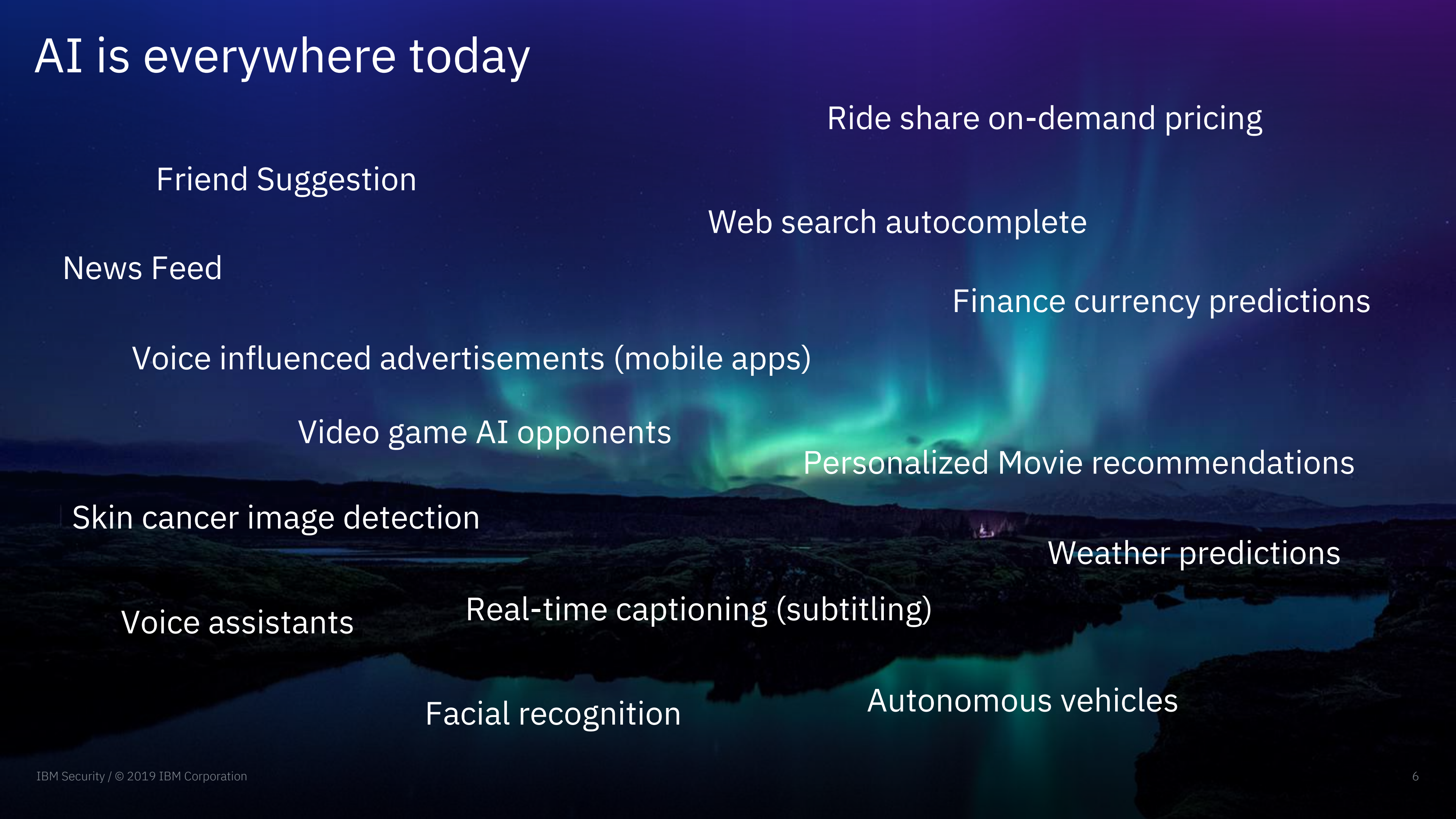
... and it does all of the above **autonomously**

SCHWARZENEGGER
In the Year of Darkness, 2029
the rulers of this planet
devised the ultimate plan.
They would reshape the
Future by changing the Past.
The plan required something
that felt no pity. No pain.
No fear.
Something unstoppable. They created
THE
TERMINATOR
Hemdale Presents a Pacific Western Production of a James Cameron Film
Arnold Schwarzenegger "The Terminator" Michael Biehn, Linda Hamilton and Paul Winfield
Make-Up Effects By Stan Winston · Executive Producers John Daly and Derek Gibson
Written by James Cameron with Gale Anne Hurd · Produced by Gale Anne Hurd
ORION Directed by James Cameron · Prints by DeLuxe®
R

How about Analytics?

Analytics help predict data based on live/historical data but it depends on **human interaction**

AI is everywhere today



Ride share on-demand pricing

Friend Suggestion

Web search autocomplete

News Feed

Finance currency predictions

Voice influenced advertisements (mobile apps)

Video game AI opponents

Personalized Movie recommendations

Skin cancer image detection

Weather predictions

Real-time captioning (subtitling)

Voice assistants

Autonomous vehicles

Facial recognition

Guess what. Bad actors are using AI to...

Dynamically probe your defenses

...to pivot attack vectors dynamically

Create new breeds of Malware

...a new specimen of Malware is created every 3-4 seconds

Automate highly personalized phishing attacks

...based on your social media posts and profile

...and much more

Where do we apply AI in Cybersecurity?

Threat Intelligence Data

Use AI to **collect** threat insights from massive amount of security data

Use AI to **generate** actionable threat intelligence from massive amount of security data

In-app services and SOC

Use AI to **convey** hidden relationships in complex security context

Use AI to **prioritize** events, offenses, and incidents

Automated orchestration and response

Inside Development

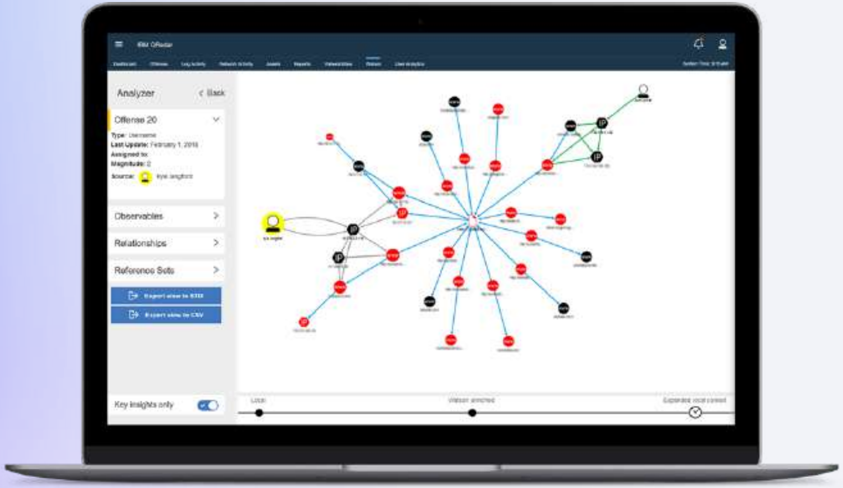
Protect service offerings

Brand Protection

AI Toolkit

Speed up your SOC with AI

IBM **QRadar Advisor with Watson**



Type: Username
Last Update: February 1, 2018
Assigned to:
Magnitude: 2
Source: kyle langford

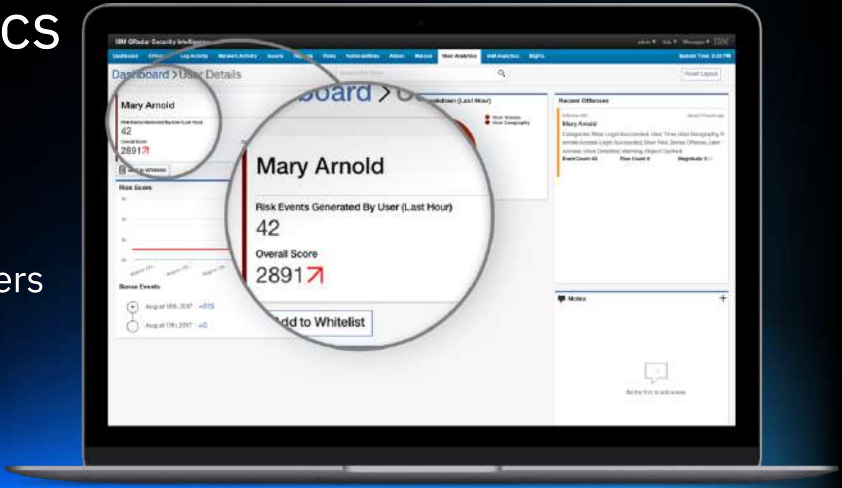
Force multiply your team’s effectiveness with AI

- Automatically connect the dots for more decisive threat escalation
- Speed response and visualize attack stages using MITRE ATT&CK
- Gain insights from Watson’s 10B+ security data points

IBM QRadar Advisor with Watson uses AI to:

- Collect Threat Intelligence from unstructured data
- Prioritize offenses
- Map MITRE ATT&CK tactics

IBM QRadar User Behavioral Analytics



Mary Arnold

Risk Events Generated By User (Last Hour)
42

Overall Score
2891

Detect insider threats with machine learning

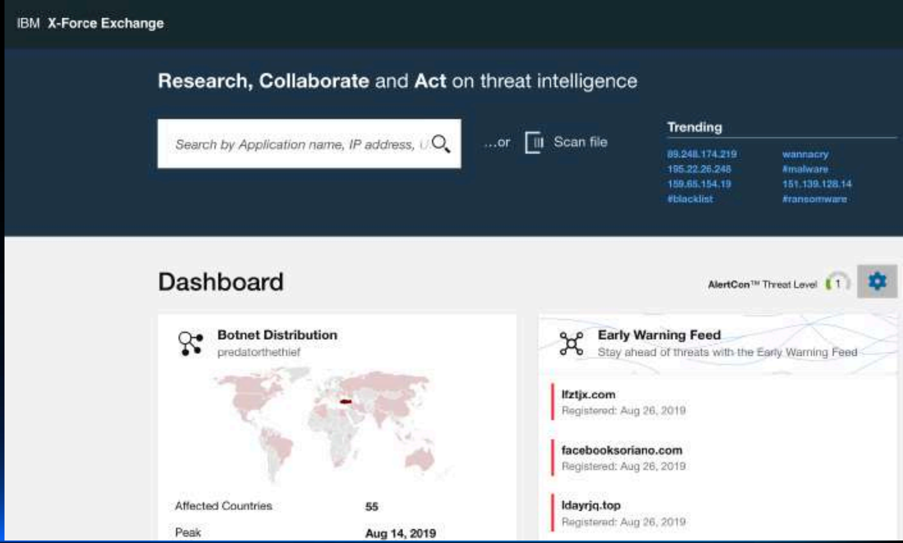
- Continuously learns behaviors to predict malicious users
- Generate detailed risk scores for individual users
- 16K+ free downloads from X-Force App Exchange

UBA uses Machine Learning for peer group analysis

- Data Uploaded to Remote Networks
- Outbound Transfer Attempts
- Access Activity
- Authentication Activity
- Suspicious Activity
- Data Downloaded
- and much more…

Includes ML toolkit for the end user to build new ML rules

IBM X-Force Exchange



Research, Collaborate and **Act** on threat intelligence

Trending

89.248.174.219
195.22.26.248
159.65.154.19
#blacklist
wannacry
#malware
151.139.128.14
#ransomware

Dashboard

Botnet Distribution
predatorthethief

Affected Countries	55
Peak	Aug 14, 2019

Early Warning Feed
Stay ahead of threats with the Early Warning Feed

lfztjx.com
Registered: Aug 26, 2019

facebooksoriano.com
Registered: Aug 26, 2019

ldayrjq.top
Registered: Aug 26, 2019

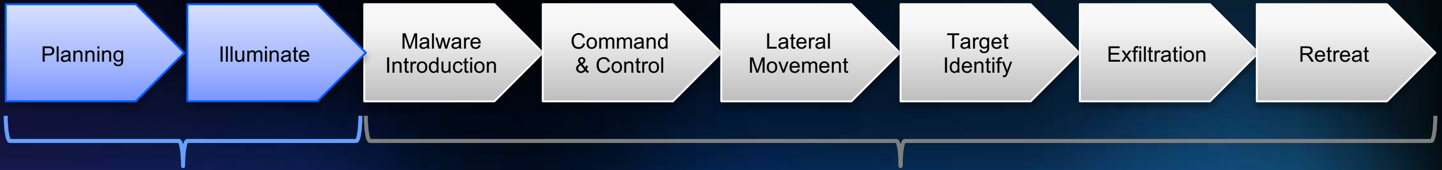
X-Force Use AI to collect and generate Threat Intelligence

- Botnet traps
- SPAM traps
- Whois Analytics – bad actor identification
- Image driven phishing / squatting analytics
- Use AI for web site categorization
- Use AI to prioritize Threat Intelligence
- Use AI to protect the service itself

DNS Analytics

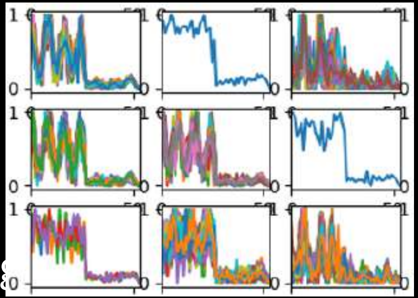
Quad9

Most solutions focus on detecting threats AFTER it has been introduced into a customers environment



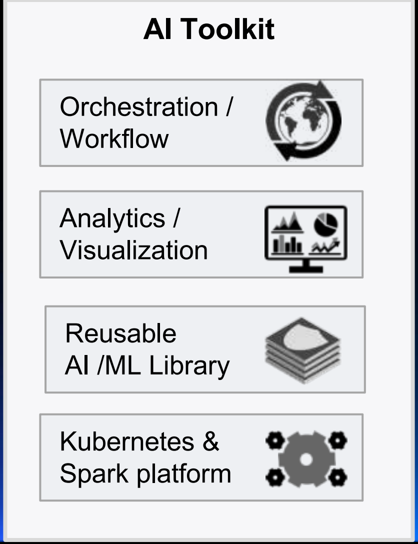
AI stops threats before the attack by detecting and blocking the C&C structure as soon as it is set up

Gartner Kill Chain



- Joint project with Quad9
- AI updates block lists in real time (near zero false positives)
- Analytics: DGA, Squatting, Tunneling, Amplification, Fast flux, etc.
- QRadar DNS Analytics app – detect malicious traffic and compare with

AI Toolkit



AI Toolkit

Orchestration / Workflow

Analytics / Visualization

Reusable AI /ML Library

Kubernetes & Spark platform

- Internal Development resource that allows Development teams to:
  - Stop re-inventing the wheel…
  - RE-use existing infrastructure (SaaS service, data stores, etc)
  - RE-use already developed analytics
  - RE-use already developed transforms
  - RE-use already developed workflows

IBM Research

- Deep Learning
- Blockchain based network for Threat Sharing

- Challenges
  - Bias
  - Explainability
  - Adversarial attacks

Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube/user/ibmsecuritysolutions

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.

IBM **Security**