IBM Security
Artificial Intelligence and Machine Learning applied to Cyber Security

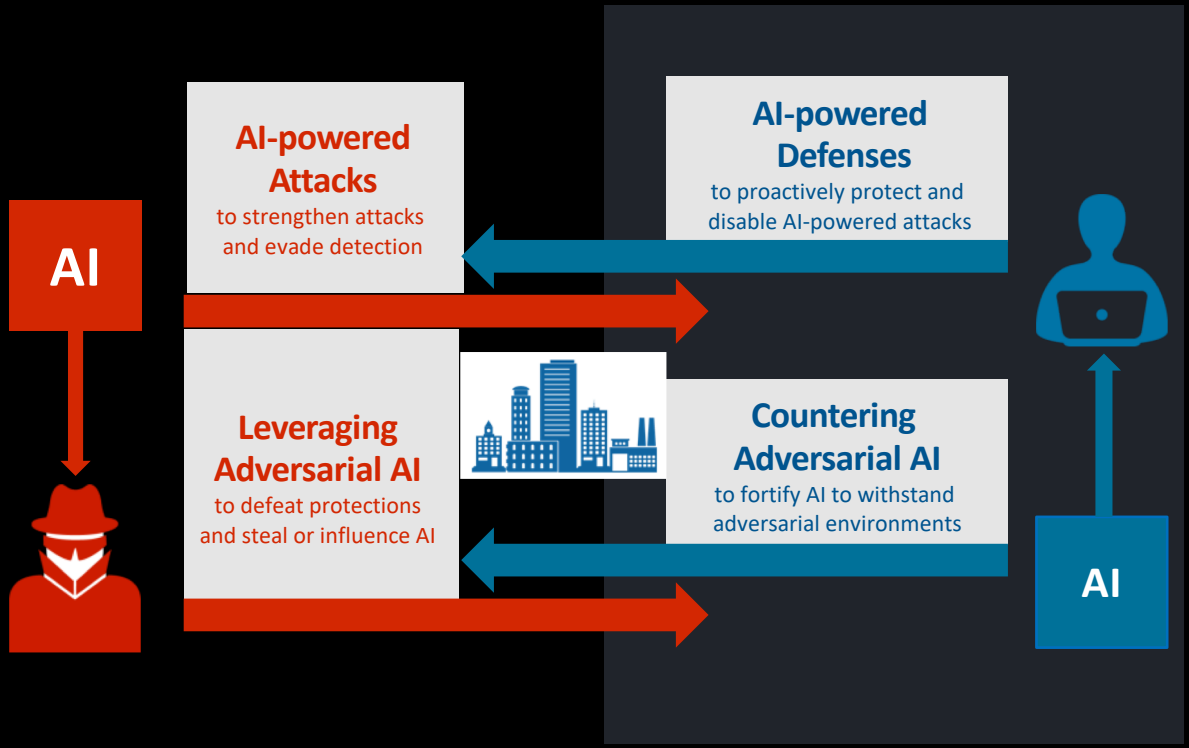
Vincenzo Conti
Security Services Delivery Manager, Italy

IBM Security

Two sides of Cyber Security & AI

Vincenzo Conti
Security Services Delivery Manager, Italy
IBM Security

AI vs AI - Two sides of Cyber Security & AI



Security solutions help …

Protect **Detect** **Respond**

But security professionals struggle with
too much data, too **few skills**, too **little time**

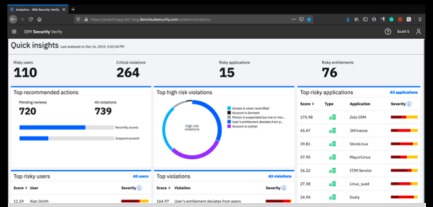
AI brings **speed** and **accuracy** so we can…

Proactively **Protect** More accurately **Detect** **Respond** faster

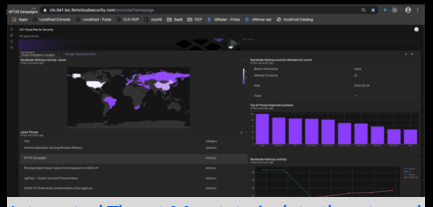
… and **lower costs** of security operations

Defender's Use of AI in Security

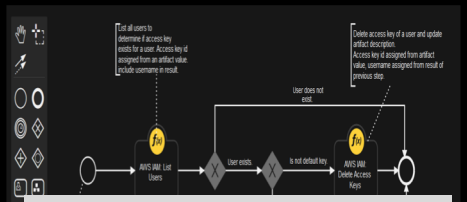
	Proactively Protect	More Accurately Detect	Accelerate Response
Key security challenges?	- **Track high-value assets** and information flow in the enterprise - **Continuously** evaluate **risk posture** to flag and remediate business impacts - **Enforce policy controls** to stop the intrusion, data loss, and business disruption	- **Anomalous activity** based on correlated telemetry from all systems & intelligence - **Smarter attacks that leverage AI to evade** the current generation of **security controls** - **Increased attack surface & alert volume** due to cloud and 5G	- **Prioritize incidents** and **automate forensic** activity with the context of business risk. - **Build best practices workflows & actions** based on decision-making ability - **Automated interactions** with the distributed environment **to mitigate incidents**
How AI/ML can address security challenges?	- Enhanced **data classification** based on NLP techniques & **deep learning** - **Multi-dimensional risk scoring** for **prioritization & continuous compliance** - **Automatic drift detection** & policy provisioning **with role mining techniques**	- **Continuous ML & anomaly detection** (Modeling Behavioral data, Cognitive Phishing Detection) - Corroboration of **threat kinetics** and **threat detection** (Correlation) - **Unsupervised ML, automa**ted rule analysis, **effective detection** & recommendations	- **Supervised ML based** analysis for threat disposition - **Graph-based analytics** to **investigate alert**s and **collaborative** threat **hunting** - **Decision support engine** to compose automation rules and protection policies
IBM Security offerings	- X-Force, Cloud Identity, Guardium, Trusteer	- QRadar UBA, Guardium, Trusteer, X-Force, CP4S (TII, DE)	- CP4S, MSS ATDS, QRadar Watson Advisor, MaaS 360, Resilient



Reduce IAM complexity with Analytics & Risk driven approach



Integrated Threat Mgmt. to isolate threats and reduce false positives



Respond 8x faster with out of the box playbooks; integration with Ansible

AI for managing Cybersecurity threats

Threat Detection

Model behaviors and identify emerging and past threats

Trusted Advisors

Reason about security events for triage and response

Active Defense

Shift risk to adversaries and manipulate decision making

AI for managing Cybersecurity threats

Threat Detection

Model behaviors and identify emerging and past threats

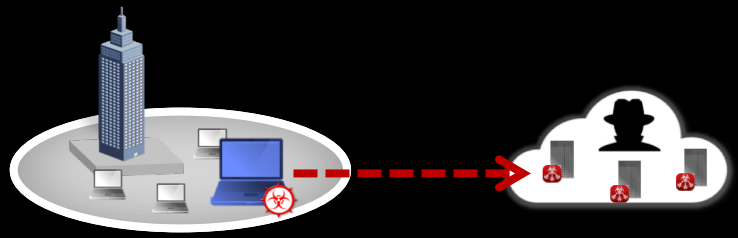
Trusted Advisors

Reason about security events for triage and response

Active Defense

Shift risk to adversaries and manipulate decision making

Stealthy beaconing behavior detection



Infected machine

Malicious operator

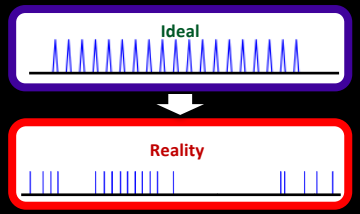
Big data problem

Millions distinct source/ destination ID pairs

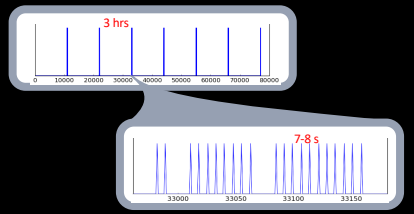
Terabytes of compressed data to process

Billions event records

Complicated behaviors



Periodicities at multiple time scales



AI for managing Cybersecurity threats

Threat Detection

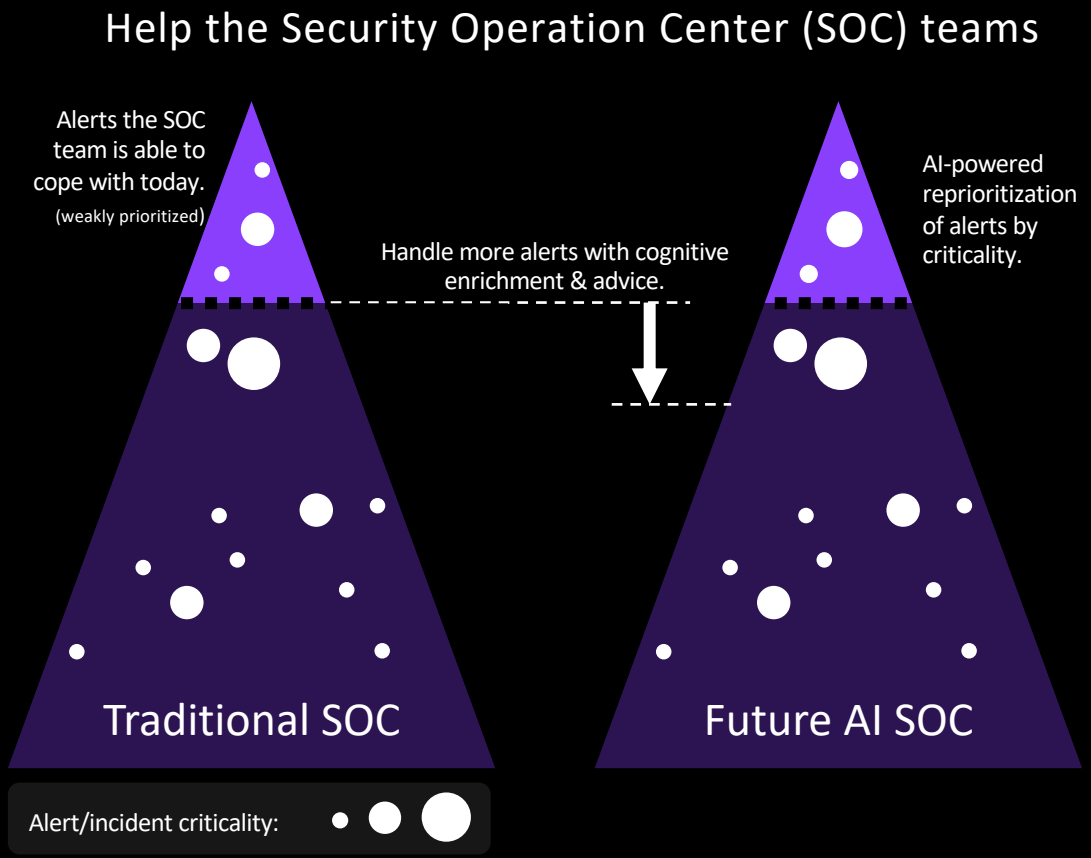
Model behaviors and identify emerging and past threats

Trusted Advisors

Reason about security events for triage and response

Active Defense

Shift risk to adversaries and manipulate decision making

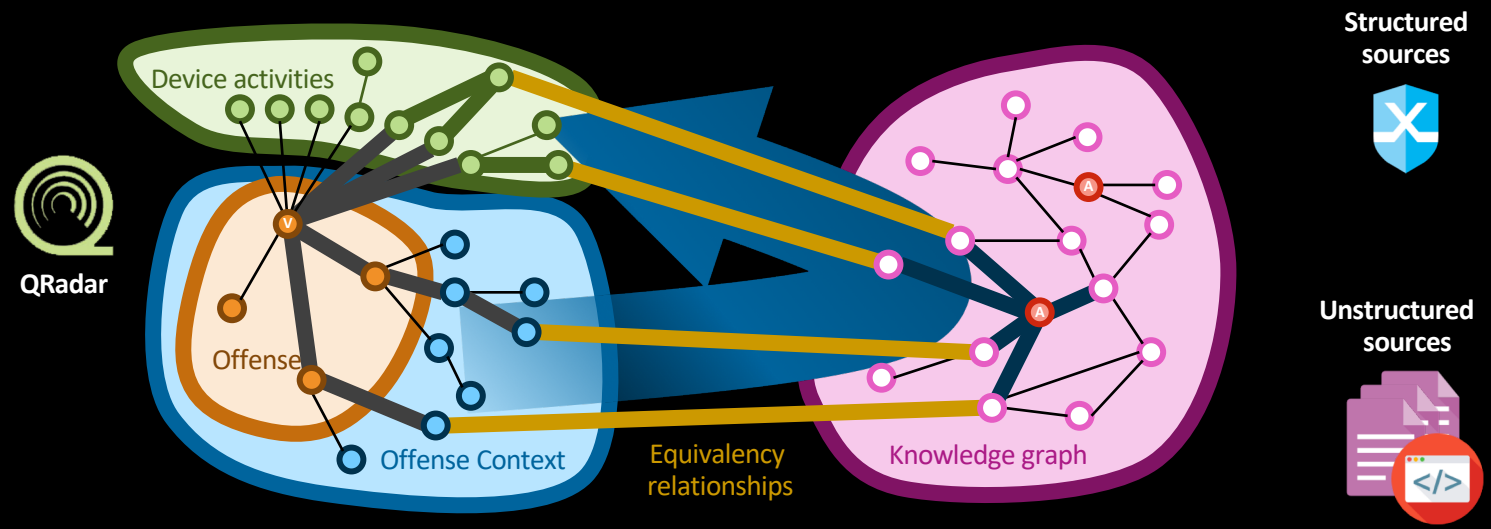


Example: Trusted Advisor for Cyber Offenses

Evidence-based Reasoning and Cognitive Exploration

Offense Context Graph
Local Kinetics and Event Data

Security Knowledge Graph
Security and Threat Information



AI for managing Cybersecurity threats

Threat Detection

Model behaviors and identify emerging and past threats

Trusted Advisors

Reason about security events for triage and response

Active Defense

Shift risk to adversaries and manipulate decision making

Cyber Deception Stack

non-intrusive, dynamic threat sensors for offensive deterrence
(traps, misdirection, disinformation, and uncertainty)

Applications
Honey-patching sensors
(patch and weaponize production services)

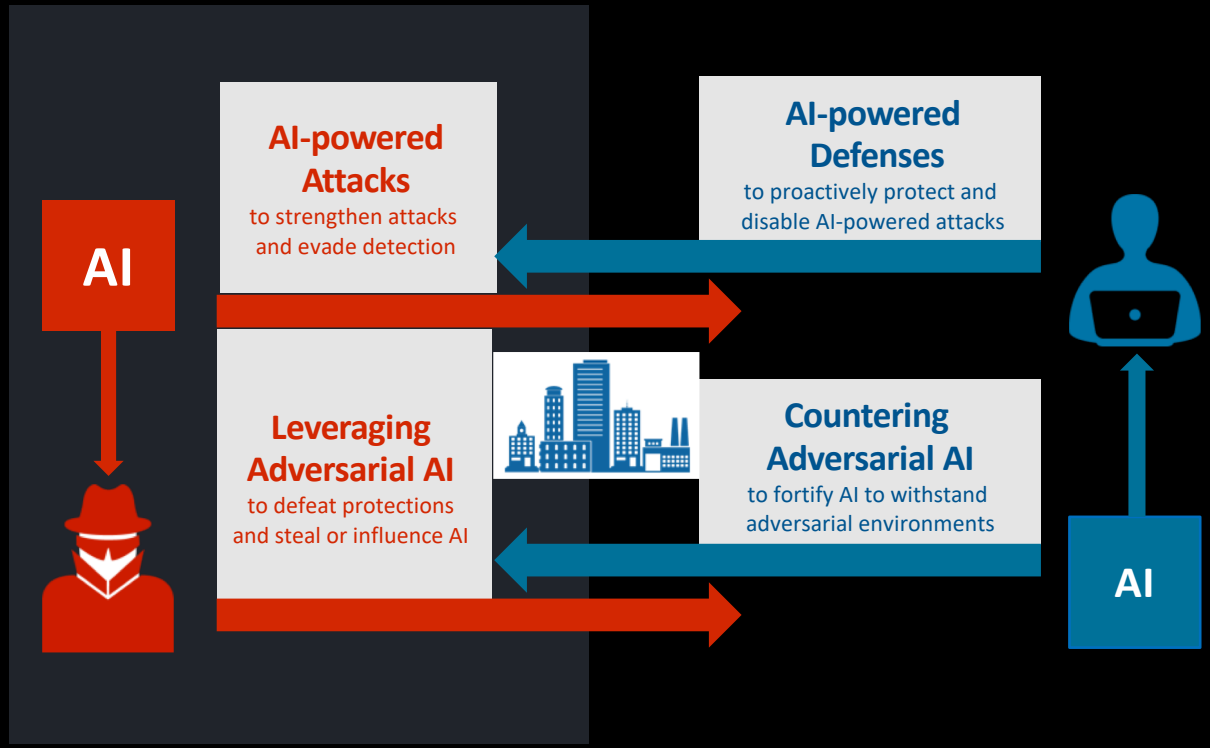
Operating System
Scarecrows
(make legitimate systems look fake)

Operating System
Decoy filesystem and **breadcrumbs**
(ransomware, rootkits, and data theft protection)

Endpoints
Service projection
(overlay honey services atop endpoints)

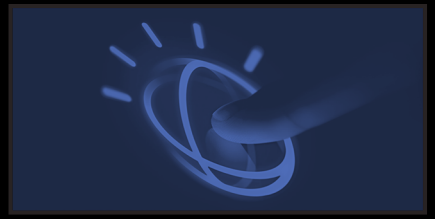
Network
Deception routing
(transparent injection of network decoys)

AI vs AI - Two sides of Cyber Security & AI



New attacks use disruptive technology with devastating results

Attackers are the first to exploit new technologies to launch sophisticated attacks at scale



ARTIFICIAL INTELLIGENCE

Attack tools get smarter

AI-powered malware
Deeplocker

Adversarial AI
Corrupting, stealing data and models from AI Services, e.g., Microsoft Tay chatbot

CLOUD

Attack surface gets bigger

Cloud on Cloud Attacks
Microsoft Azure Attacks, AWS S3 Bucket Misconfigurations

Micro-architectural flaws
Spectre, Meltdown and Foreshadow

IoT

Attack targets get physical

Insecure Internet-Connected Devices
Jeep on the Sprint Network

Consumer IoT Devices4
BlackEnergy malware attacked 3 Ukraine power plants leaving 230K people without power, baby monitors infected by Mirai botnet led to attacks on Dyn and Netflix

AUTOMATION

Attack campaigns get faster

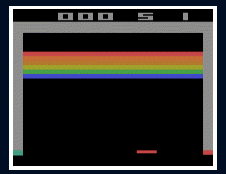
Devastating malware
Ransomware like Wannacry, NotPetya

Dangers of increased automation
Flash crash in high frequency trading based on automated Twitter ingestion of fake news

Attackers are using AI to defeat cybersecurity

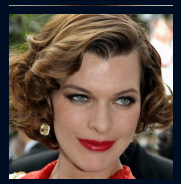
AI Powered Attacks

- **Generate:** DeepHack tool learned SQL injection
- **Automate:** Generate targeted phishing attacks on Twitter
- **Refine:** Neural network powered password crackers
- **Evade:** Generative adversarial networks learn novel steganographic channels



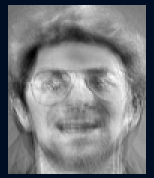
Attacking AI

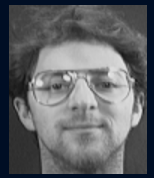
- **Poison:** Microsoft Tay chatbot poisoning via Twitter (and Watson Urban Dictionary “poisoning”)
- **Evade:** Real-world attacks on computer vision for facial recognition biometrics and autonomous vehicles
- **Harden:** Genetic algorithms and reinforcement learning (OpenAI Gym) to evade malware detectors



Theft of AI

- **Theft:** Stealing machine learning models via public APIs
- **Transferability:** Practical black-box attacks learn surrogate models for transfer attacks
- **Privacy:** Model inversion attacks steal training data

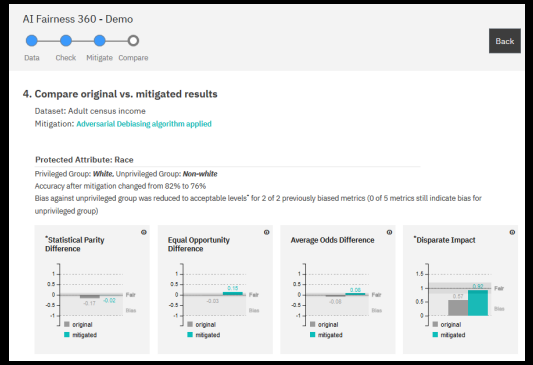




Trusted AI : Fairness, Explainability, Robustness

IBM AI Fairness 360

aif360.mybluemix.net

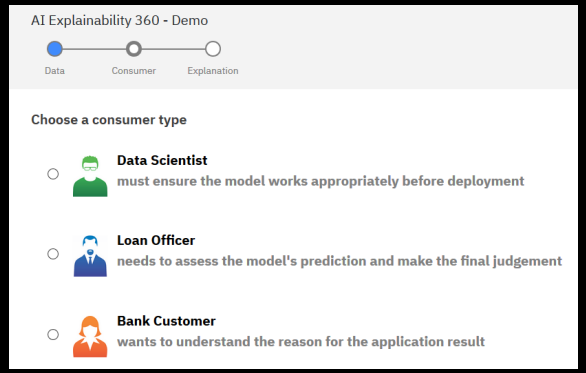


open source toolkit for detecting & mitigating bias in ML models:

- 70+ fairness metrics
- 10 bias mitigators
- Interactive demo illustrating 5 bias metrics and 4 bias mitigators
- extensive industry tutorials and notebooks

IBM AI Explainability 360

aix360.mybluemix.net

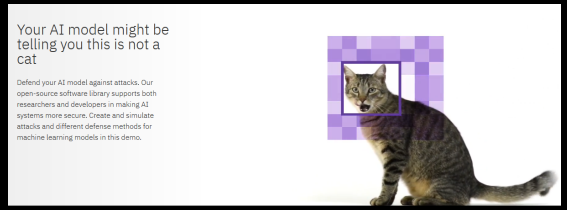


open source toolkit for explaining ML models & data

- 10 explainability algorithms
- Interactive demo showing 3 algorithms in credit scoring application
- 13 tutorial notebooks covering use cases in finance, healthcare, lifestyle, retention, etc.
- Extensive documentation and taxonomy of explainability algorithms

IBM Adversarial Robustness 360

art-demo.mybluemix.net



open source toolkit for defending AI from attacks

- Supports 10+ frameworks
- 19 composable and modular attacks (including adaptive white- and black-box)
- 10 defenses, including detection of adversarial samples and poisoning attacks
- Robustness metrics, certifications and verifications
- 30 notebooks covering attacks and defenses

Learn more on this topic

- **Artificial intelligence for a smarter kind of cybersecurity**
https://www.ibm.com/security/artificial-intelligence

- “**Artificial Intelligence and Cybersecurity For Dummies, IBM Limited Edition**”
https://www.ibm.com/account/reg/signup?formid=urx-31245

- Security and Artificial Intelligence FAQ
https://www.ibm.com/downloads/cas/ZQROXRBK

- Cost of a Data Breach Report: Impact of automation and AI
https://www.ibm.com/account/reg/signup?formid=urx-46355

Artificial Intelligence and Machine Learning applied to Cyber Security

AI to protect data

Vincenzo Conti
Security Services Delivery Manager, Italy
IBM Security

Data is sprawling everywhere, making it hard to protect and govern

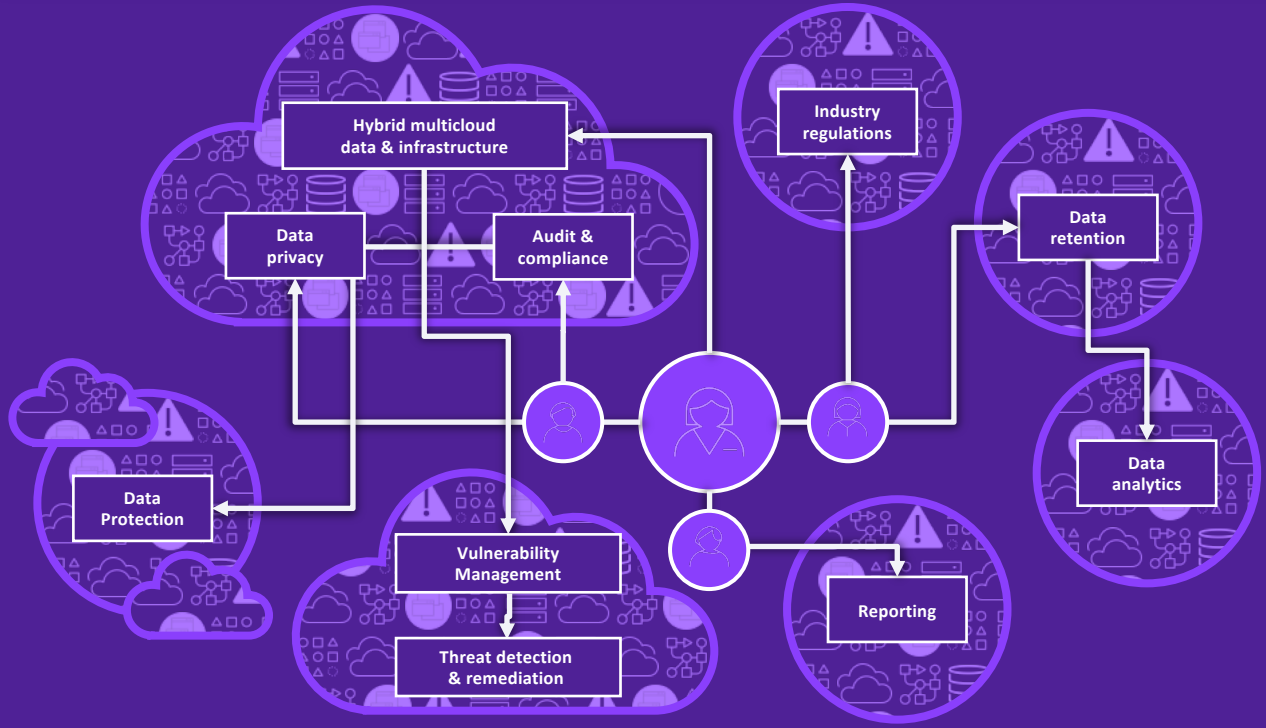
Expanding data footprint across hybrid multi-clouds increase attack surface, resulting in a host of new data security, privacy & compliance challenges

Issues are compounded by:

- Digital transformation
- Need to leverage data for new business value
- Ever growing data volumes
- Growing privacy and compliance mandates

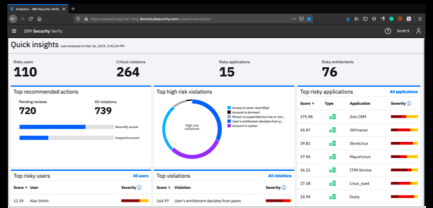
Structured & unstructured data across on-premises, public & private cloud environments

- Databases
- Open source DB
- Big data
- Files
- Containers
- Mainframe

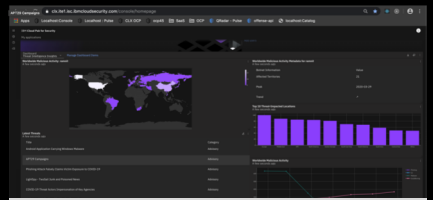


Defender's Use of AI in Security

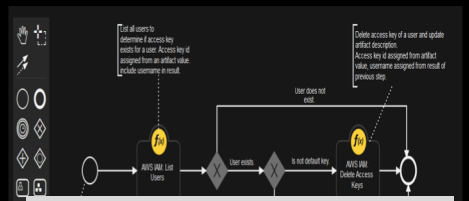
	Proactively Protect	More Accurately Detect	Accelerate Response
Key security challenges?	- **Track high-value assets** and information flow in the enterprise - **Continuously** evaluate **risk posture** to flag and remediate business impacts - **Enforce policy controls** to stop the intrusion, data loss, and business disruption	- **Anomalous activity** based on correlated telemetry from all systems & intelligence - **Smarter attacks that leverage AI to evade** the current generation of **security controls** - **Increased attack surface & alert volume** due to cloud and 5G	- **Prioritize incidents** and **automate forensic** activity with the context of business risk. - **Build best practices workflows & actions** based on decision-making ability - **Automated interactions** with the distributed environment **to mitigate incidents**
How AI/ML can address security challenges?	- Enhanced **data classification** based on NLP techniques & **deep learning** - **Multi-dimensional risk scoring** for **prioritization & continuous compliance** - **Automatic drift detection** & policy provisioning **with role mining techniques**	- **Continuous ML & anomaly detection** (Modeling Behavioral data, Cognitive Phishing Detection) - Corroboration of **threat kinetics** and **threat detection** (Correlation) - **Unsupervised ML, automa**ted rule analysis, **effective detection** & recommendations	- **Supervised ML based** analysis for threat disposition - **Graph-based analytics** to **investigate alert**s and **collaborative** threat **hunting** - **Decision support engine** to compose automation rules and protection policies
IBM Security offerings	- X-Force, Cloud Identity, Guardium, Trusteer	- QRadar UBA, Guardium, Trusteer, X-Force, CP4S (TII, DE)	- CP4S, MSS ATDS, QRadar Watson Advisor, MaaS 360, Resilient



Reduce IAM complexity with Analytics & Risk driven approach



Integrated Threat Mgmt. to isolate threats and reduce false positives

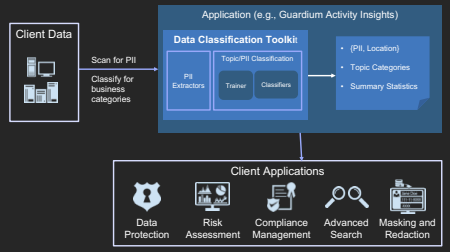


Respond 8x faster with out of the box playbooks; integration with Ansible

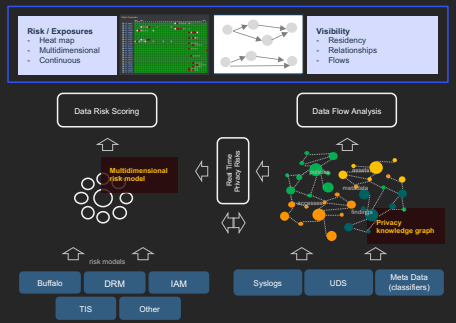
Examples of ML/AI to Protect digital assets (data)

Protect (Assess)

Data classification

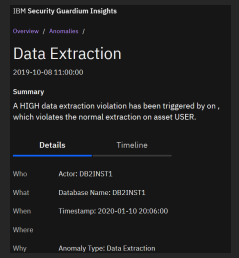


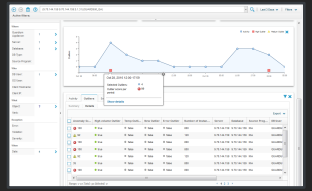
Data flow and risk analysis



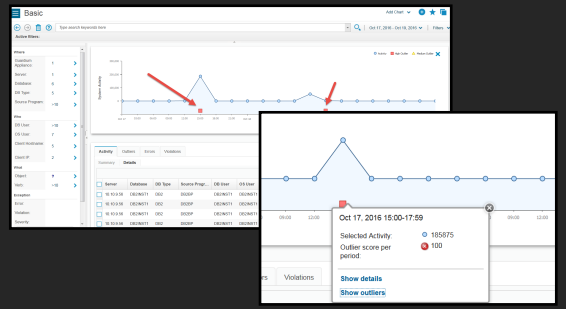
Detect (Understand)

Sequence-based Predictive Analytics



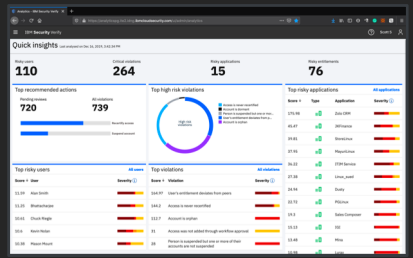


Outlier Detection

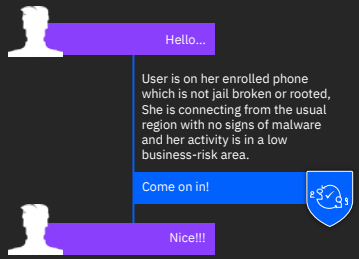


Respond (Act)

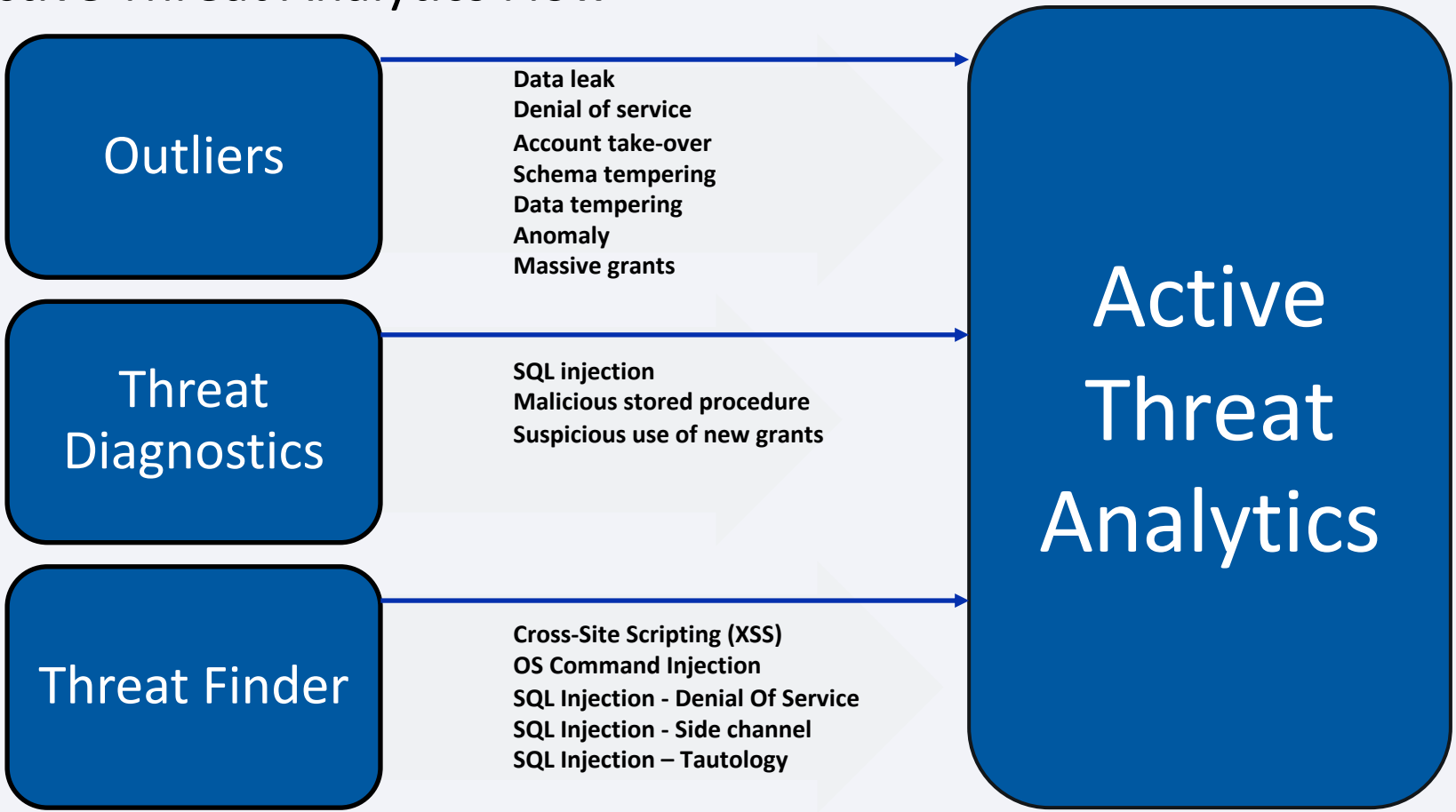
Risk based Certification



User / Data Access Enforcement



Active Threat Analytics Flow



Learn more on this topic

- **Artificial intelligence for a smarter kind of cybersecurity**
https://www.ibm.com/security/artificial-intelligence

- “**Artificial Intelligence and Cybersecurity For Dummies, IBM Limited Edition**”
https://www.ibm.com/account/reg/signup?formid=urx-31245

- Security and Artificial Intelligence FAQ
https://www.ibm.com/downloads/cas/ZQROXRBK

- Cost of a Data Breach Report: Impact of automation and AI
https://www.ibm.com/account/reg/signup?formid=urx-46355

Artificial Intelligence and Machine Learning applied to Cyber Security

AI to protect users

Digital identity is at the center of all of our lives

Vincenzo Conti
Security Services Delivery Manager, Italy
IBM Security

How do you know it’s really your customer or employee?

$6.5 billion to $7 billion in annual account takeover losses

How do you know your new customer is not a fraudster who stole someone’s identity?

More than $3 billion lost per year to new account fraud

How can you make authentication as painless as possible for your customers, while keeping bad actors out?

US businesses lose more than $62 billion annually due to poor customer experience.

How can you prevent fraudsters from gaining access and control of customer or employee credentials?

More than 15 billion stolen credentials posted on the dark web

Does identity risk detection apply to your users?

Employees on home PC/WIFI

Employees on Trusted VPN

Mobile employees on managed devices

Partially controlled devices (at best….)

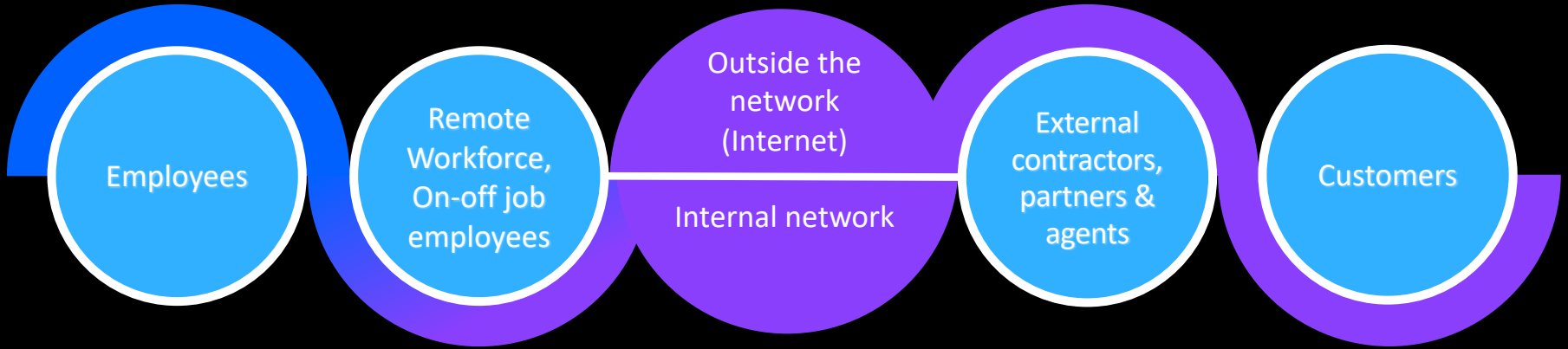
Partially controlled connections (WIFI, VPN)

Partially controlled behavior

Uncontrolled devices

Uncontrolled connections

Uncontrolled behavior



Employees on premise

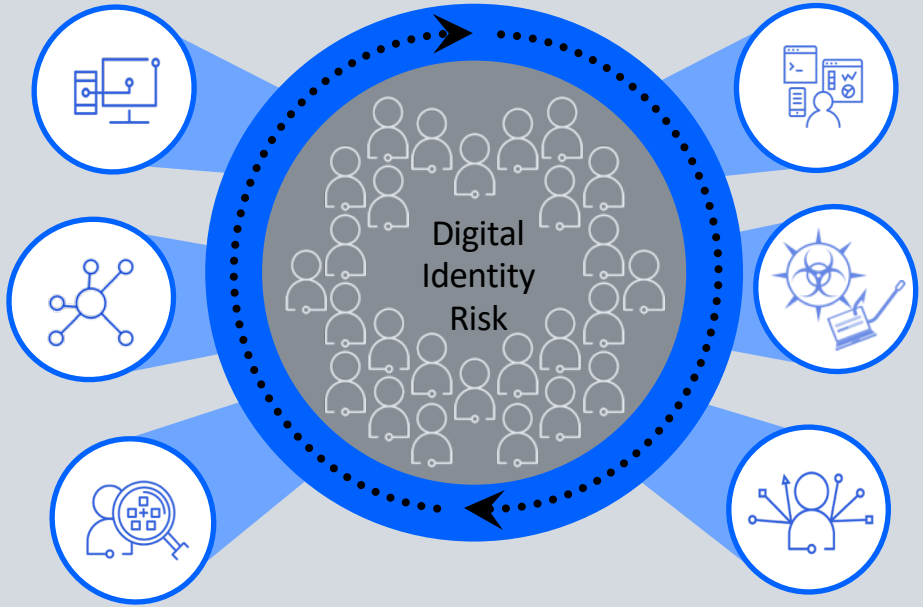
Inspecting a wide range of identity risks

What

Device
Device fingerprint and hygiene

Environment
Network Connection
Connection type/risk

Passive Behavior
User typing, mouse movement and journey analysis



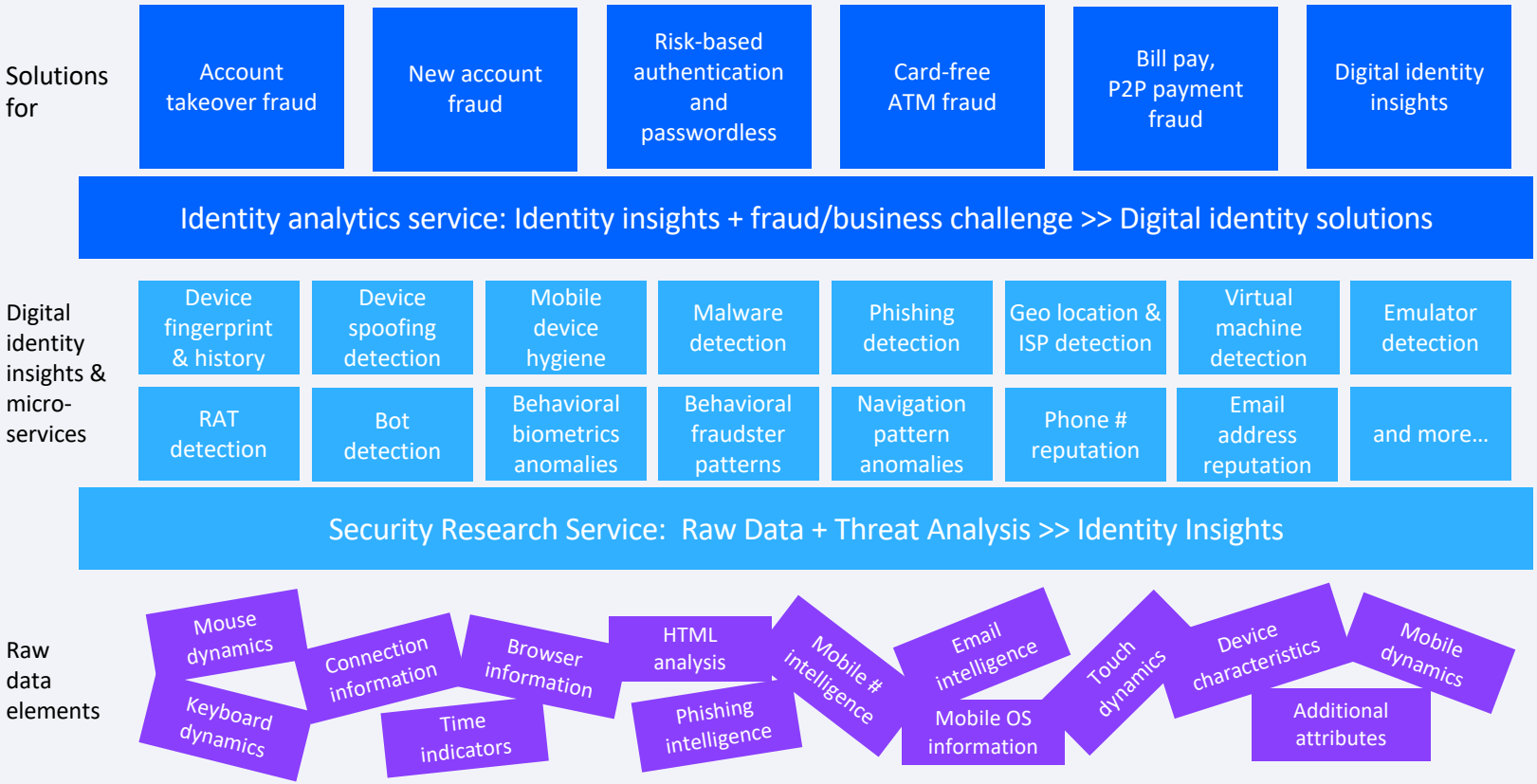
How

Anomaly Detection
User's current and historical activity

Fraud Patterns
Distinct fraud identifiers

Consortium Data
Tagged good/bad attributes

AI stack for Digital Identity risks detection



Learn more on this topic

- **Artificial intelligence for a smarter kind of cybersecurity**
https://www.ibm.com/security/artificial-intelligence

- “**Artificial Intelligence and Cybersecurity For Dummies, IBM Limited Edition**”
https://www.ibm.com/account/reg/signup?formid=urx-31245

- Security and Artificial Intelligence FAQ
https://www.ibm.com/downloads/cas/ZQROXRBK

- Cost of a Data Breach Report: Impact of automation and AI
https://www.ibm.com/account/reg/signup?formid=urx-46355

Thank you

Follow us on:

ibm.com/security

Ibm.com/security/artificial-intelligence

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube.com/ibmsecurity