

RSA® Conference 2018

Singapore | 25–27 July | Marina Bay Sands

SESSION ID: SEM-W01E

BRINGING AI TO THE CYBERSECURITY BATTLE

Vikas Desai

Cybersecurity Advisor

IBM

@VBDSecurity

<https://vikasdesai.github.io>

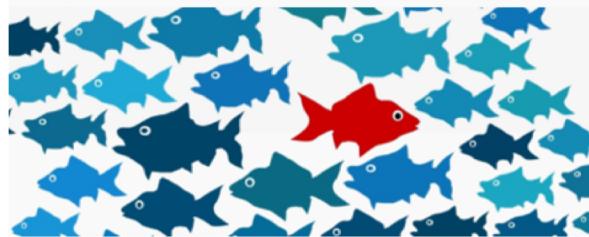


Uses of AI in Security



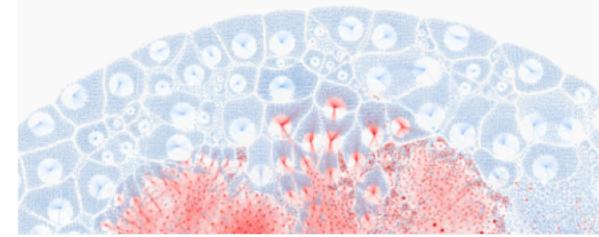
Predictive Analytics

- **Approach:** Model behaviors and identify emerging and past threats and risks
- **Applications:** Network, user, endpoint, app and data, cloud
- **Examples:** Beacons, DNS analytics, user behavior



Intelligence Consolidation

- **Approach:** Curation of intelligence and contextual reasoning
- **Applications:** Structured and unstructured (NLP) data sources
- **Examples:** Intelligence Feeds, Augmented Intelligence



Trusted Advisors & Response

- **Approach:** Reason about security events for triage and response
- **Applications:** Cognitive SOC analyst, orchestration, automation and digital guardian
- **Examples:** SoC Augmentation, SOAR applications



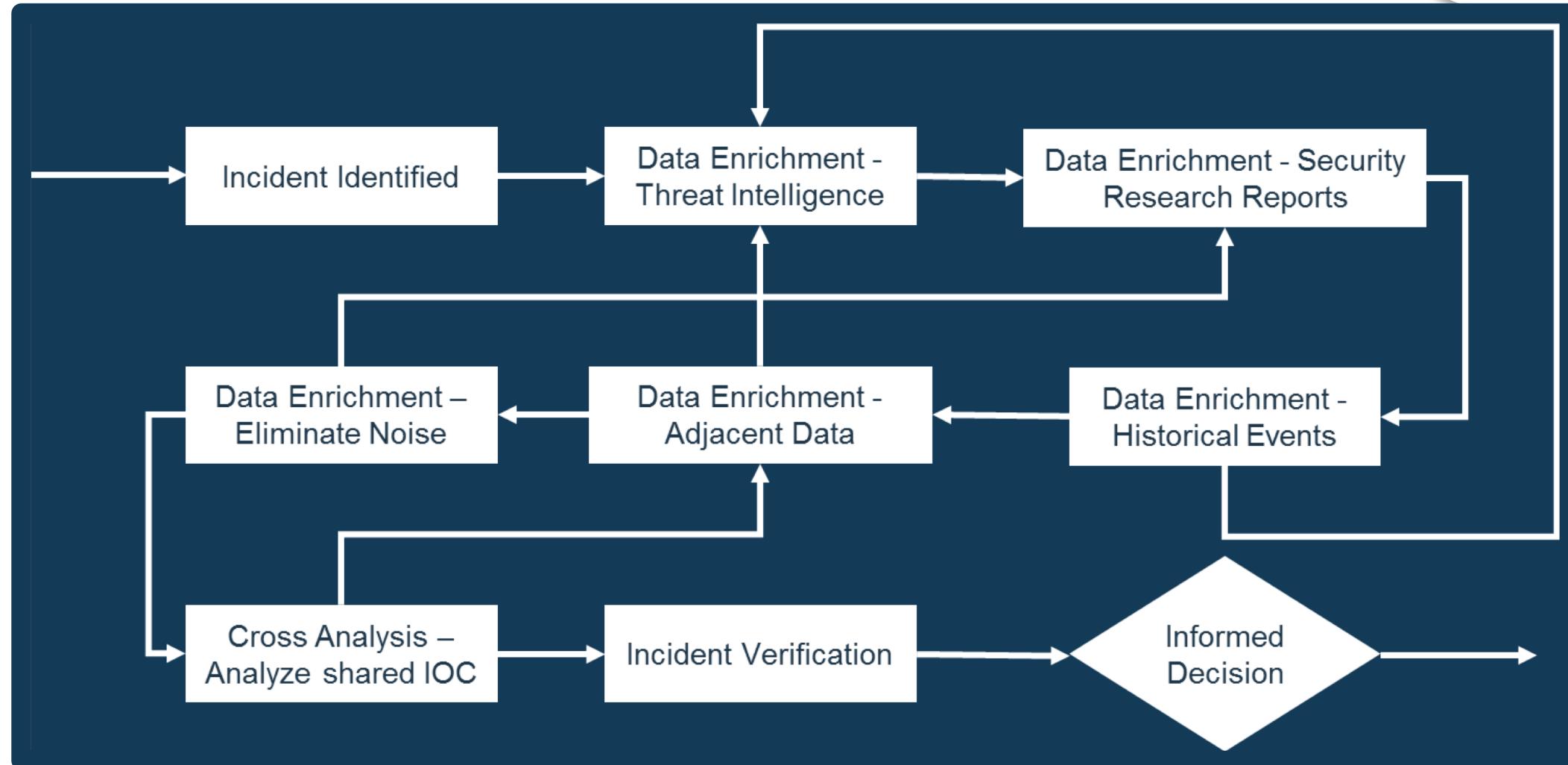
RSA® Conference 2018
Asia Pacific & Japan



AUGMENTED INTELLIGENCE

Trusted Advisors & Response

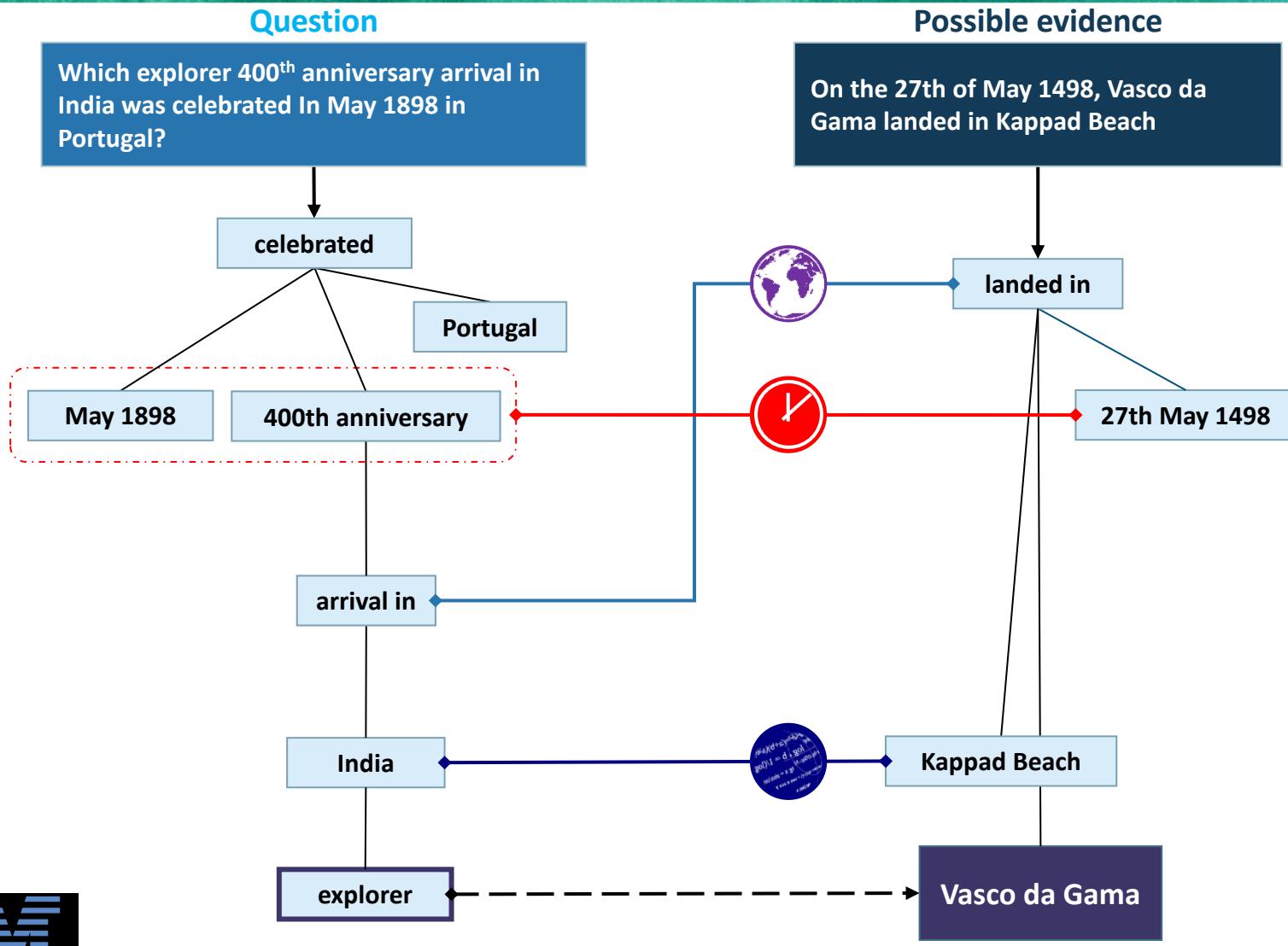
Incident Investigation Today



So What Do we Need?



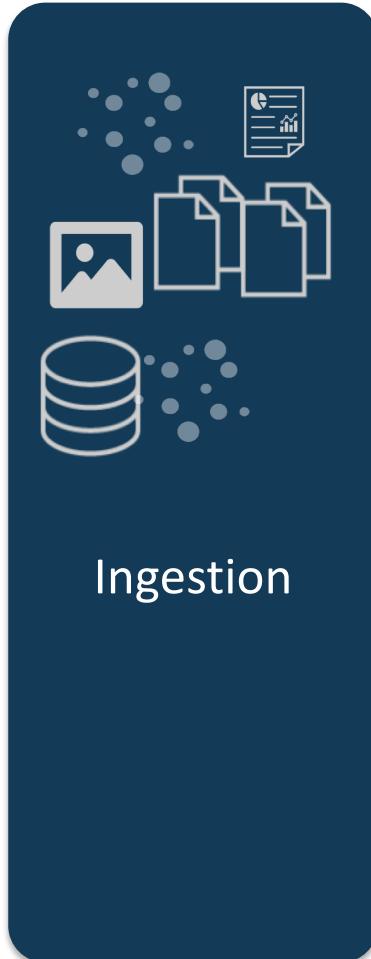
#RSAC



Legend

- Temporal Reasoning
 - GeoSpatial Reasoning
 - Statistical Paraphrasing
 - Reference Text
 - Answer

Watson for Cybersecurity



Ingestion



Classification
and
Normalization



Natural
Language
Processing



Training and
Learning

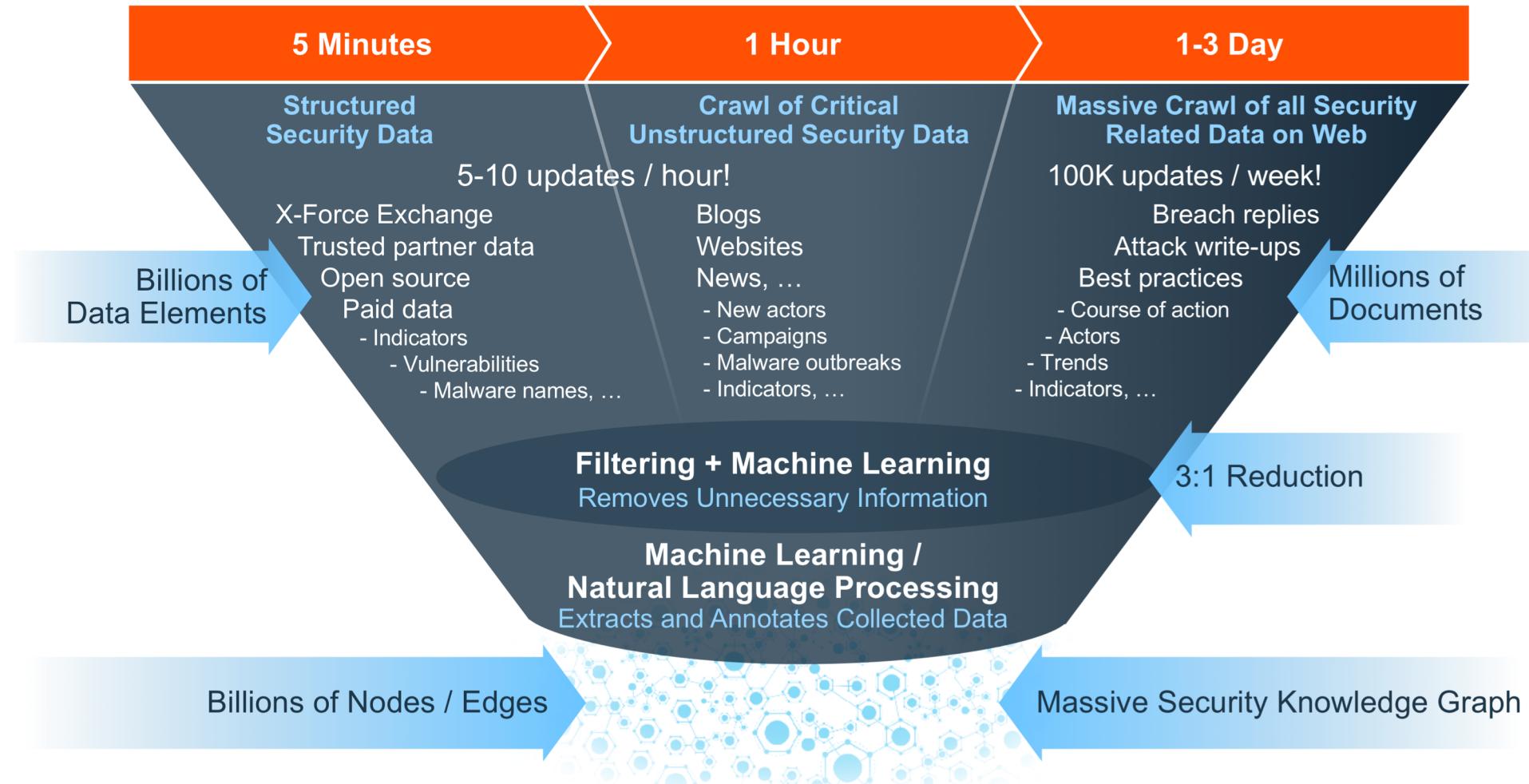


Knowledge
Graphs



RSA® Conference 2018
Asia Pacific & Japan

Ingestion – Building the knowledge



Natural Language Processing / Understanding



User Generated Content: "What's interesting about TSPY_BANKER.YYSI is that it uses the social media network Pinterest in its command and control (C&C) routines. The comments, which look something like "104A149B245C120D," are decoded (by replacing letters with a dot) and the result is an IP address for the server hosting the phishing page. This tactic allows cybercriminals to quickly change the location of their servers in order to avoid detection, Trend Micro said in a blog post...the attackers leveraged exploits for two patched Internet Explorer vulnerabilities, CVE-2013-2551 and CVW-2014-0322"

Watson understands: TSPY_BANKER.YYSI [MALWARE] it [MALWARE REFERENCE] its [MALWARE REFERENCE] command and control (C&C) routines. Instead of contacting a C & C server, the Trojan [MALWARE] accesses comments ...which look something like "104A149B245C120D" [INDICATOR].

Site : <https://www.securityweek.com/banking-trojan-abuses-pinterest-cc-routines>



RSA®Conference2018
Asia Pacific & Japan

Training and Learning



RSA® Conference 2018
Asia Pacific & Japan



DEMO

QRadar advisor with Watson

QRadar Advisor for Watson



Accelerated Analysis

- Uses AI to analyze real-time incidents for triage
 - Automatically investigates evidence for an alert or anomaly against Watson and applies 'reasoning' to identify the likely threat
- Gathers external and internal threat indicators from alert
- Performs external (threat intelligence research) and internal research on indicators and entities (hash, domain, IP, users, filename etc.)
- Highlights the existence and identity of threat or outliers
- Offers natural language search bar for security only information to speed up assessment

Intelligent Investigation

- Identifies if communication with threat has occurred or was blocked
- Highlights if malware has executed
- Identifies criticality of systems impacted in incident and shows high value assets
- Gives visibility to higher priority risks and threats from insiders
 - Integrated with User Behavior Analytics (UBA) app to show user's risk scores
 - Reveals previous behaviors and actions of users
- Connects other threat entities from original offense to show relationship
- Provides input for ad-hoc investigation against collections of users and entities

Faster Response

- Provides pertinent information to take action on escalation
- Performs automatic hunting for indicators
- Exports threat and indicators to IR process for remediation and/or blocking
- Automatically adds additional discovered threat indicators to watch lists to reduce risk of missing threats



Build a Cognitive SOC

50x

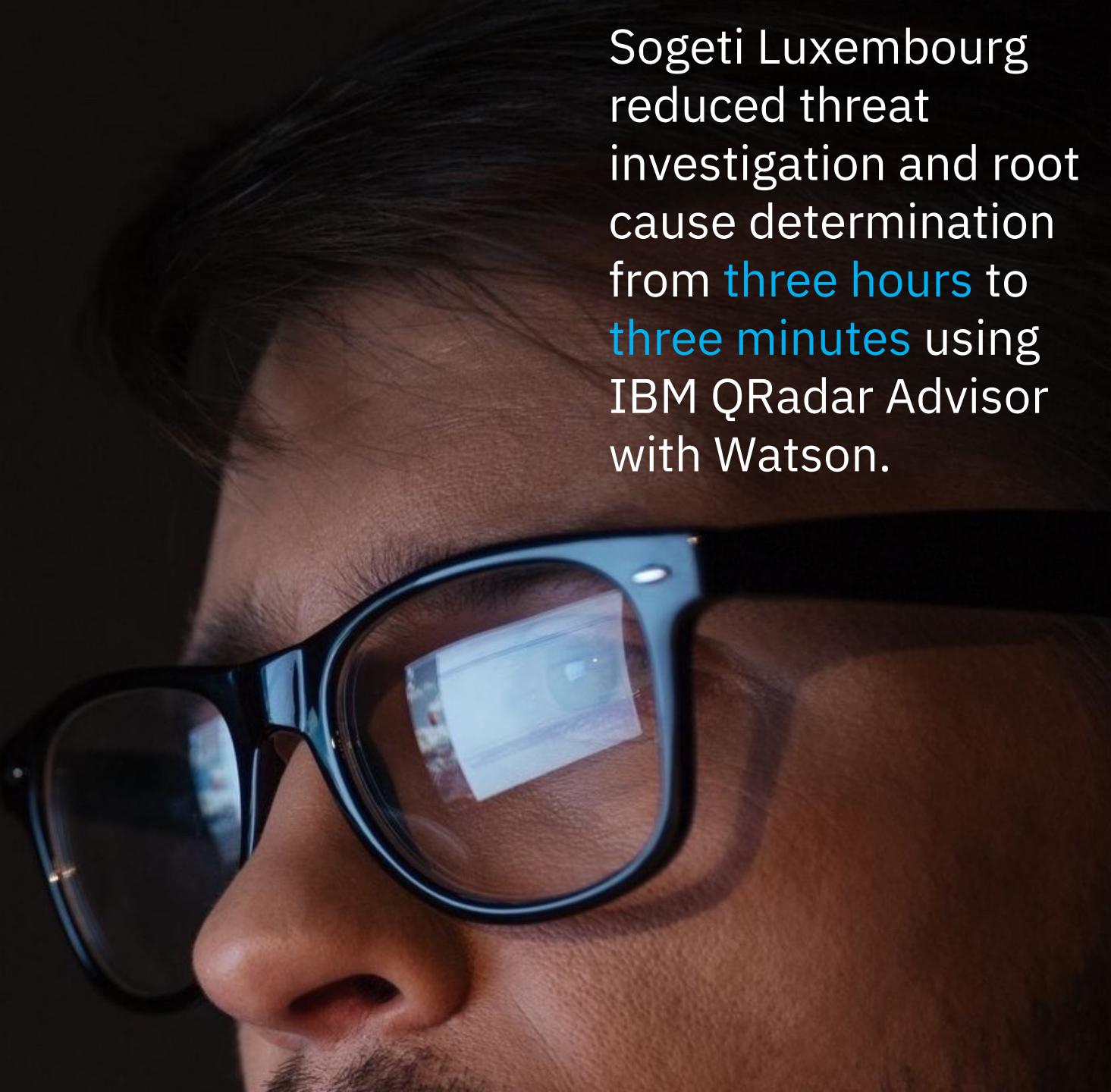
Faster threat investigation

10x

More actionable threat indicators

Outcomes

- *Applied business context to use cases*
- *Lowered risk of missing threats*
- *Reduced time to investigate*
- *Accelerated response efforts*



Sogeti Luxembourg reduced threat investigation and root cause determination from **three hours** to **three minutes** using IBM QRadar Advisor with Watson.

RSA® Conference 2018
Asia Pacific & Japan



USER BEHAVIOR

Predictive Analytics

The connected world has created new challenges



Customers want convenient mobile, online and cross-channel access

Threat mitigation can impact customer experience

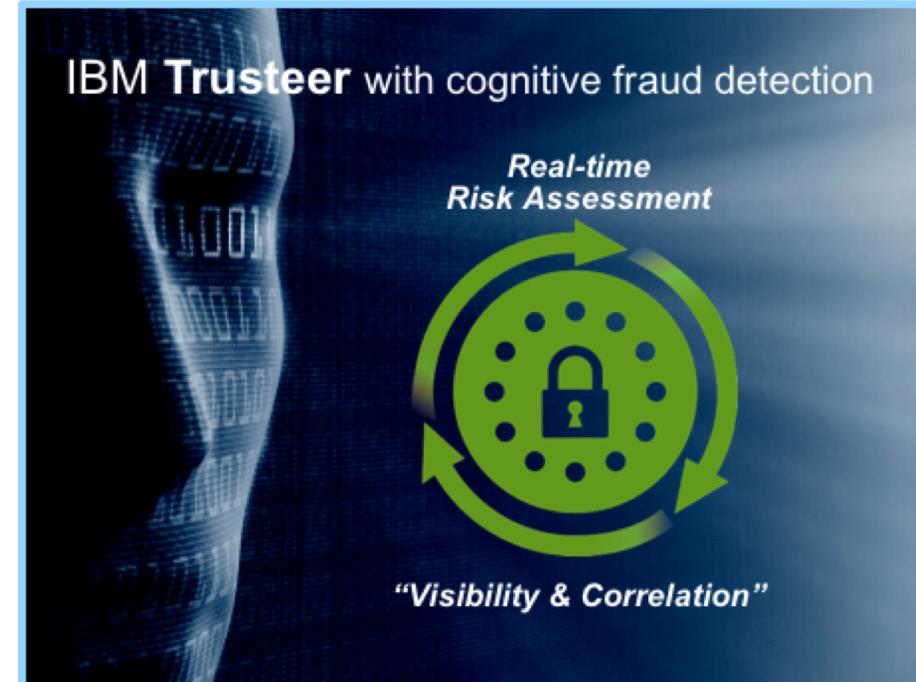


New, faster transactions can create new risks

Customers' Value Drivers – Predictive Analytics



- Improve Customer Experience
 - Reduce user friction
 - Proactive fraud prevention
 - Faster dispute resolutions
- Strengthen authentication
 - Detection of Account Take Over, Remote Access Tools...
 - Real-time fraud detection
 - Continuous and Invisible passive user authentication
- Cost Reduction
 - Improve true positive detection rates (less fraud)
 - Reduce false positive detection rates (less work)
 - Faster fraud dispute resolutions (less fraud and less work)



Let's look at Keystroke Dynamics



User Name

Password

Key Usage

Pattern Attributes Collection(JS Collectors)

- Capitalized letters(shift/caps lock)
- Changes(Delete/Backspace)
- Control Combinations(language)
- Traversing fields
- Pasting(Ctrl-V/right click)
- General Movements

Key Strokes

Pattern Attributes Collection(JS Collectors)

- Typing speed
- Dwell Time
- Flight Time
- Digraph patterns
- Trigraph Patterns
- Total Keystrokes



Let's look at Keystroke Dynamics



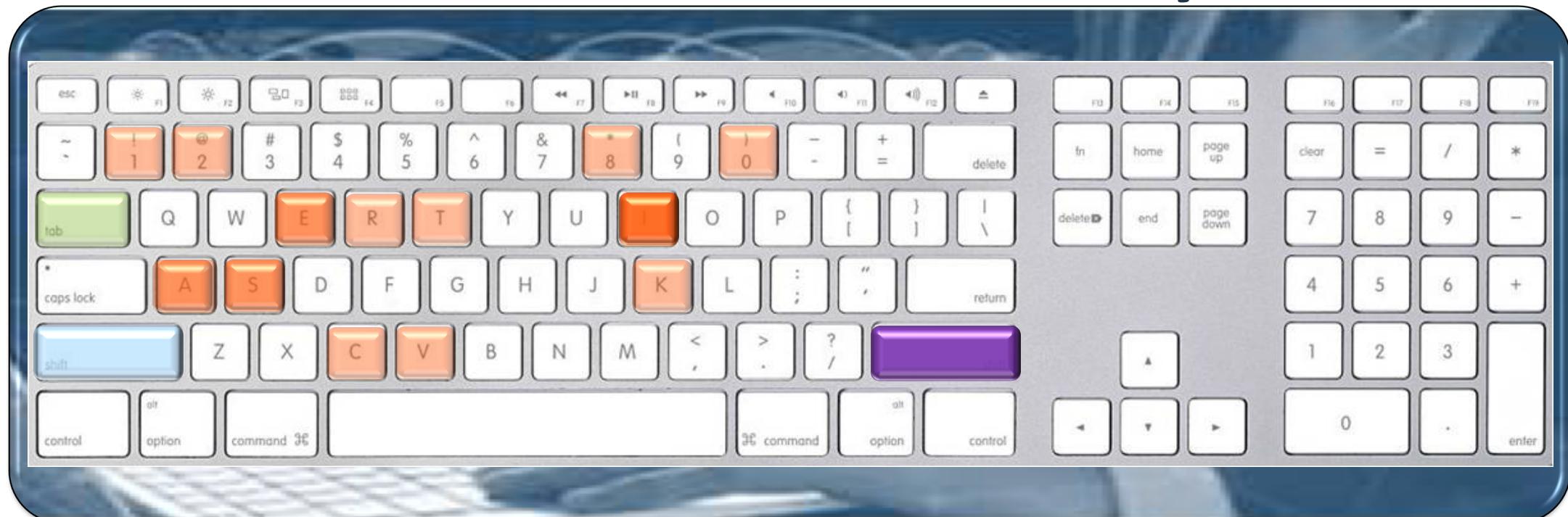
#RSAC

User Name

Password

VikasDesai

Security2018



RSA® Conference 2018 Asia Pacific & Japan

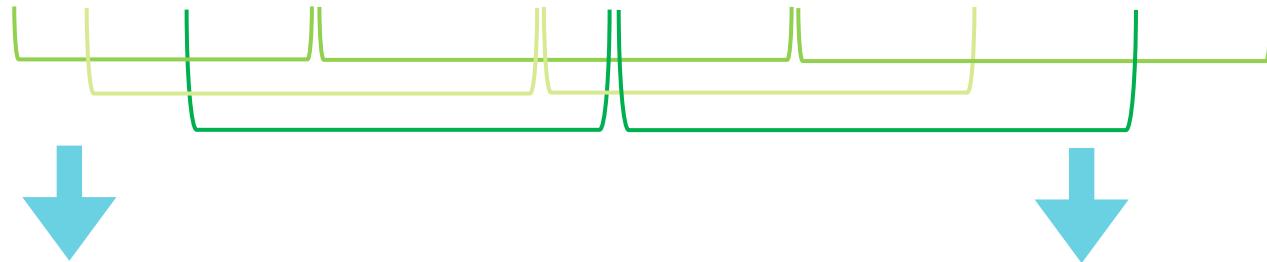
Let's look at Keystroke Dynamics



Di-Graph



Tri-Graph



Aggregated Comparison



Total time



Avg. D-U



Avg. U-D

Signal Comparison



Dwell Time Down-Up



Typing Speed Down-Down



Flight Time Up-Down

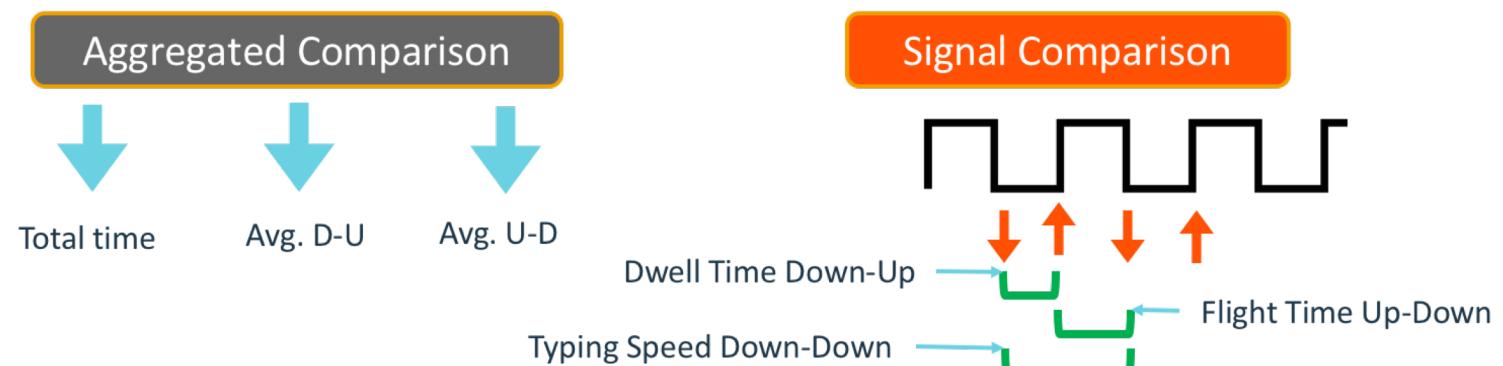
RSA Conference 2018
Asia Pacific & Japan



Feature Engineering



- Dwell Time – The amount of time a key stays pressed
 - Down-Up (DU)
- Flight Time – The amount of time needed to release the previous key and press the next key
 - Up-Down (UD)
- Typing Speed – The amount of time between 2 key presses
 - Down-Down (DD)
- Average Dwell time
- Average Flight Time
- Average Typing Speed



RSA® Conference 2018
Asia Pacific & Japan

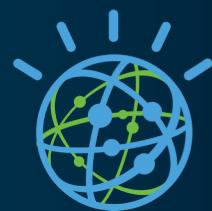
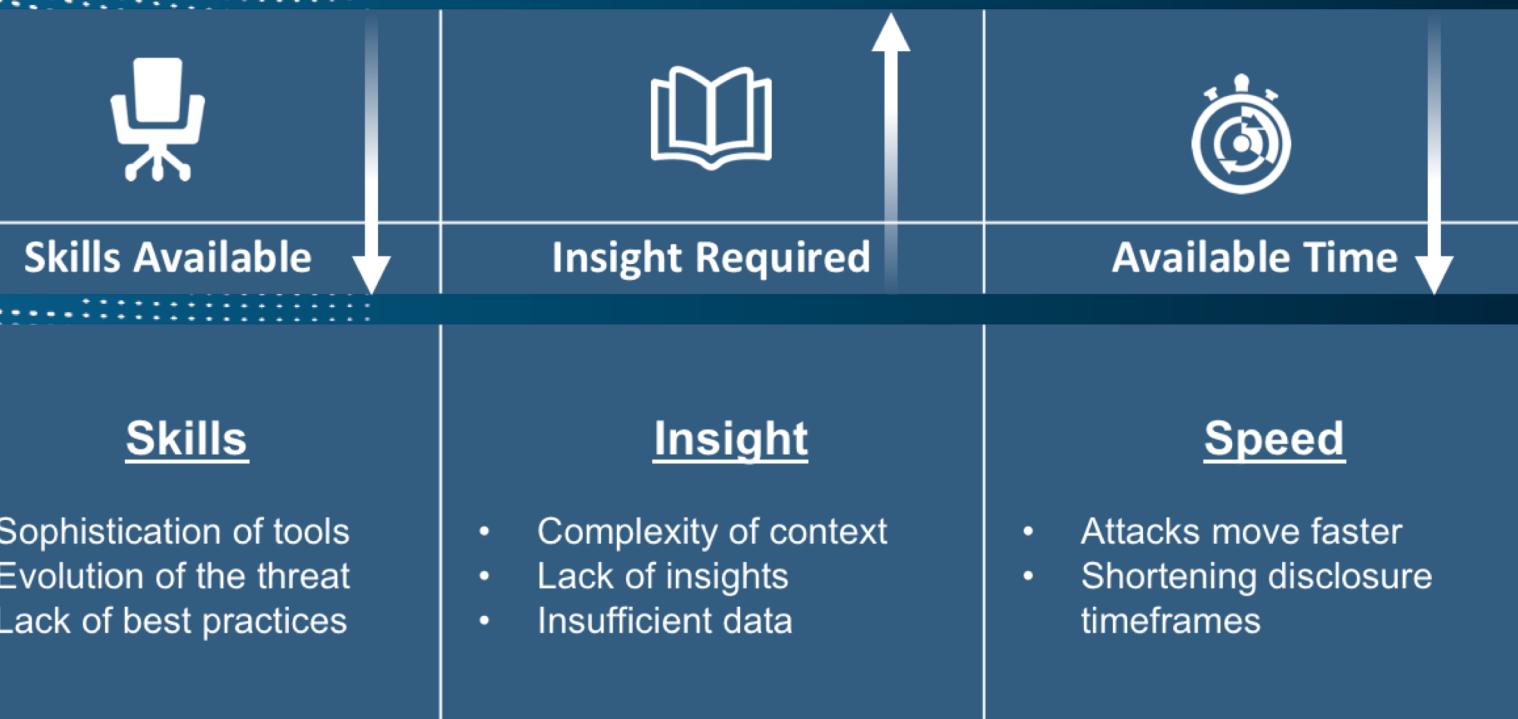
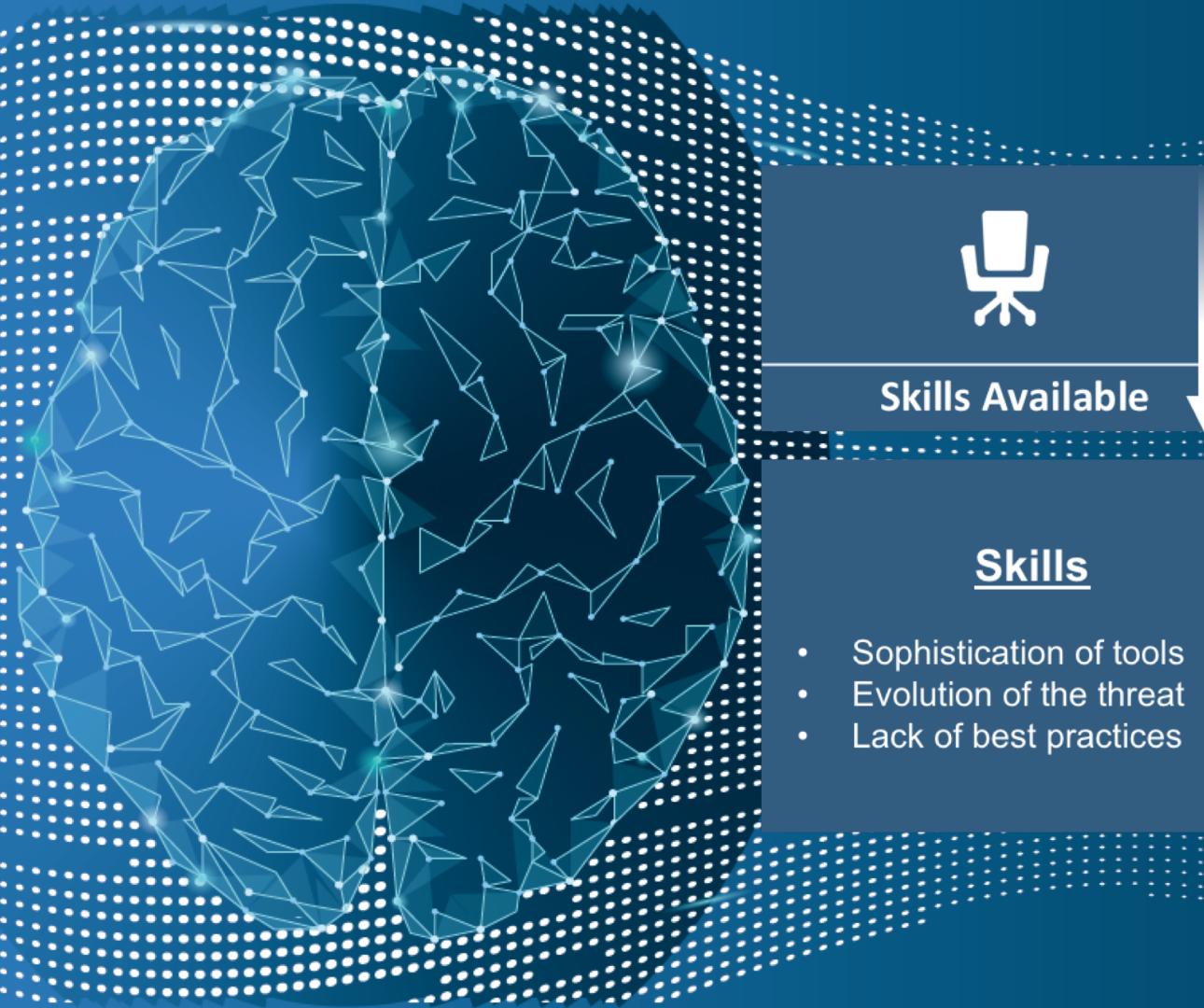


DEMO

Keystroke Dynamics

<https://vikasdesai.github.io/keystroke-dynamics/>

Why do we need AI?





Learn + Explore = Apply

Educate yourself

Stay informed

Leverage AI to secure
yourself

<https://vikasdesai.github.io>

<https://www.ibm.com/security/artificial-intelligence>



THANK YOU

FOLLOW US ON:

-  ibm.com/security
-  securityintelligence.com
-  xforce.ibmcloud.com
-  [@ibmsecurity](https://twitter.com/ibmsecurity)
-  youtube/user/ibmsecuritysolutions



© Copyright IBM Corporation 2017. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

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.