Thursday, July 9, 2020 | 1:00 pm ET

BEFORE WE BEGIN

We will send you the recording

Submit your questions anytime. We'll do Q&A all throughout

Please complete our exit survey

THE Moderator

Mark Scarmozzino

Regional Manager, 4iQ

Mark Scarmozzino, CAMS is a Regional Director at 4iQ, and recently joined 4iQ with responsibility for business development and relationship management in the banking and financial services division. Mark is certified as an Anti-Money Laundering Specialist ("CAMS") by the Association of Certified Anti-Money Laundering Specialists ("ACAMS"). Prior to joining 4iQ, Mark was a Managing Director at ACA Telavance, and has over 30 years of global banking and financial services industry experience, including extensive expertise in Anti-Money Laundering, fraud, global economic sanctions, and regulatory compliance. Prior to ACA Telavance, Mark was a Senior Account Manager with Fiserv Risk & Compliance Solutions and a Vice President & Business Development Executive at Daylight Forensics & Advisory, a leading global regulatory consulting firm.

Speaker

Uday Gulvadi

Director, Stout

Uday Gulvadi is a Director in the Disputes, Compliance, & Investigations group at Stout and a financial crimes, internal audit, and risk advisory practice leader with over 20 years of experience. Uday has significant expertise advising boards, audit committees and senior management on their most challenging financial crimes compliance, governance and risk and compliance matters. Uday is an industry recognized thought leader and subject matter expert on enterprise risk management, AML and sanctions program governance, model validations, risk-based internal audits, information technology, and cybersecurity audit and controls.

Uday has extensive international business experience as a leader with national and regional advisory firms and has worked with clients and successfully completed engagements in the US, Europe and Asia.

Speaker

Fotis Konstantinidis

Managing Director, Stout

Fotis Konstantinidis is a Managing Director and leads the Artificial Intelligence and Digital Transformation practice at Stout. He has over 17 years of experience in data mining and advanced analytics, digital strategy, alignment of security with business strategy and integration of digital technologies in enterprises. His experience includes data transformation and business intelligence, use of machine learning to maximize real business value and AI-based cybersecurity capabilities across digital products. Fotis has also led large digital transformation and security and risk management programs in both private and public companies. He has completed cybersecurity assessments helping clients ensure compliance with cybersecurity laws and data privacy regulations, such as GDPR, CCPA, PCI and HIPAA.

Prior to joining Stout, Fotis held leadership positions leading AI-driven products and services at CO-OP Financial Services, McKinsey & Company, Visa and Accenture.

Speaker

Erin Brown

Intelligence Analyst and Cryptocurrency Specialist, 4iQ

Erin Brown has worked in the field of intelligence analysis for over 8 years, with 6 years served in the UK government. Responsible for conducting investigations on behalf of 4iQ and their customers, Erin is a superuser of 4iQ solutions. With several years of experience working on complex cyber and cryptocurrency investigations, Erin has extensive knowledge of current cyber trends and investigative techniques to uncover real identities of cybercriminals and attribute their activities. Erin previously worked for the UK government and held several roles, as a Financial investigator, Policy advisor and Cyber Intelligence Analyst working on investigations concerning cybercrime and nation-state actors. Following this Erin worked at Elliptic as a Cryptocurrency investigator and trainer, working with law enforcement and industry partners, advising them on how to investigate cryptocurrency frauds and other malicious activity. Erin holds a BA Hons in History from the University of Stirling, a MSc in Government, Policy, and Politics from Birkbeck and a GDL in Law from City University.

Cyber risk and Mitigation strategies

20Minute

STOUT

Cyber Risks

Assessment, Prevention & Detection Strategies

Cyber Risk – Time of increased vulnerability

Businesses in Survival Mode

- Decreased focus on Cyber Risks
- IT security teams stretched & reactive.
- Hastily configured tools
- Bandwidth & licensing constraints

Challenges of Remote Working

- Secure environment bypassed
- Home networks have lax security
- Shared workspace could risk violating privacy laws

Cyber Attack – Common Techniques

Phishing Schemes

- COVID-19 related lures
- URLs / downloads of purported safety information or infection maps
- Claims to have PPE masks / face shields
- Impersonate senior executives to request payment

Malware

- Users download software that steals, encrypts or hijacks computer functions.
- Cause - hacked websites, downloading infected files or opening emails from device that lacks anti-malware security.

Ransomware

- Attacker gains access to and locks down access to vital data.
- Ransom / Fee is demanded

Denial Of Service

- Attacker seeks to render computer system unavailable
- Accomplished by flooding targeted machine with superfluous requests to overload systems and prevent legitimate requests from being fulfilled

Cyber Risk Identification & Assessment

Enterprise value source

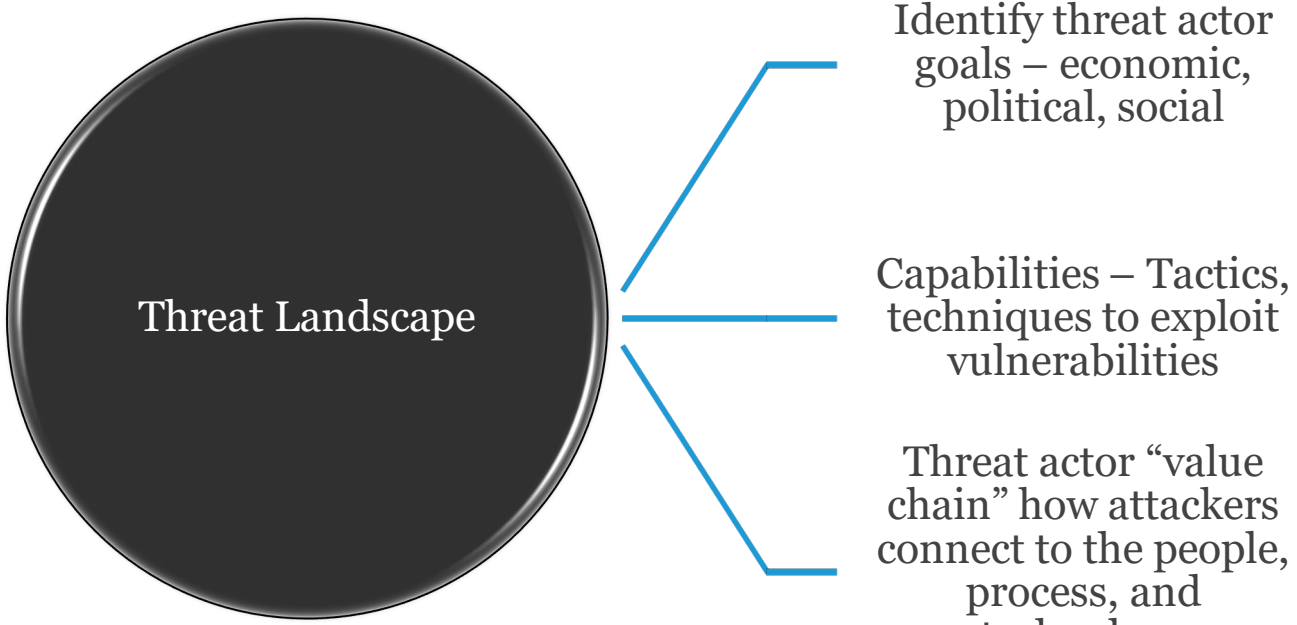
Business Process

Data/ Information assets

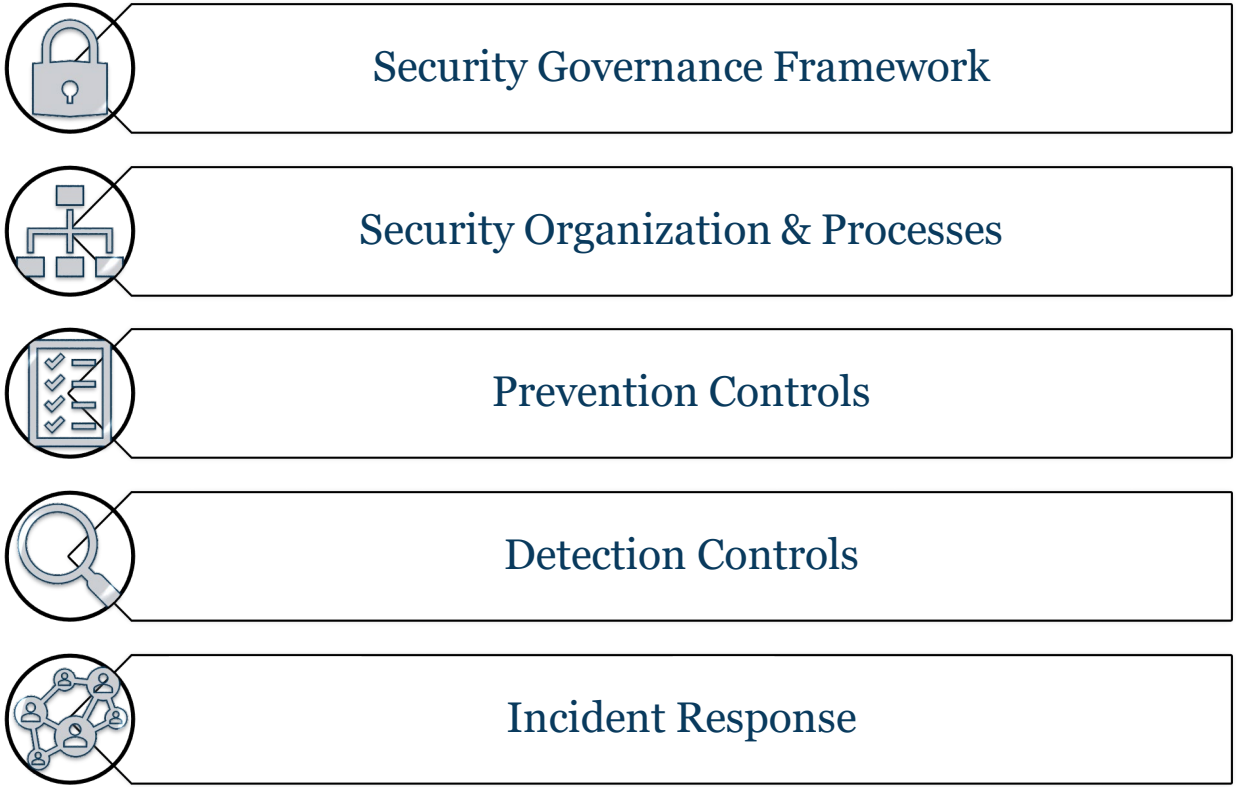
Vulnerabilities

Threat actors

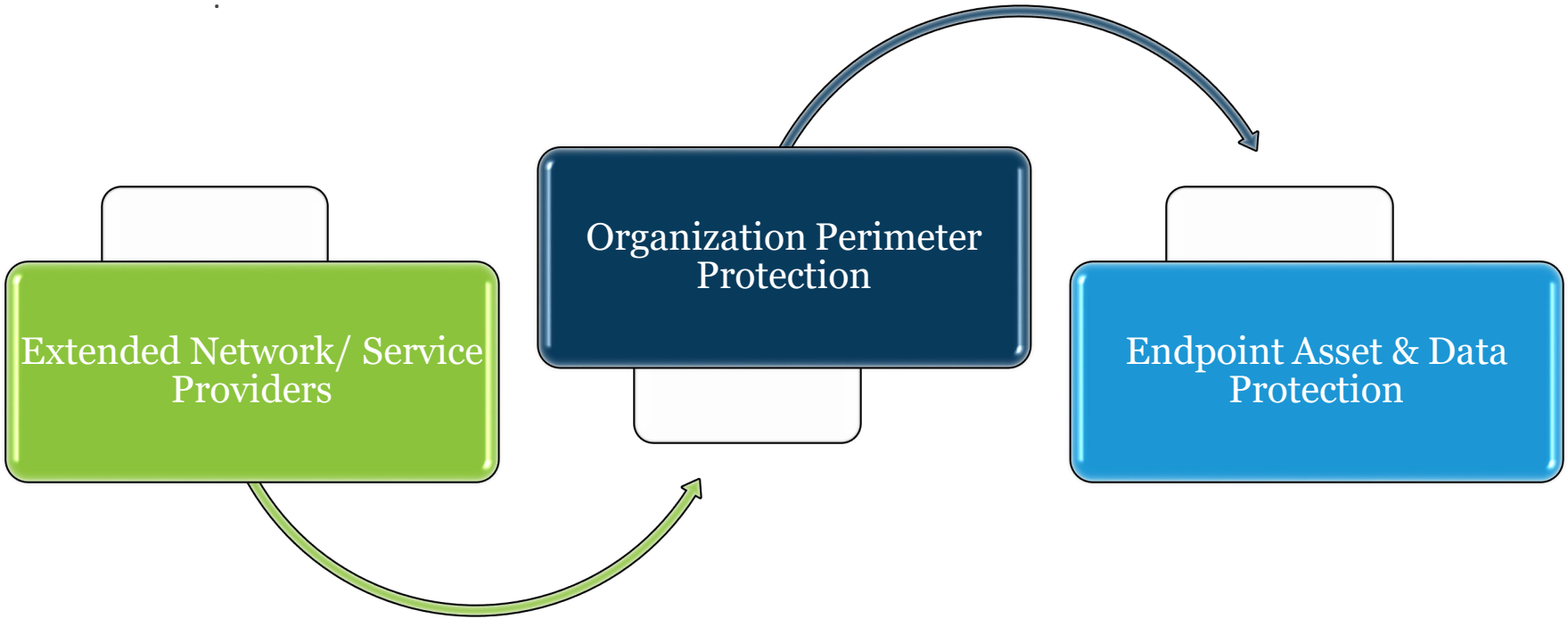
Cyber Threat Assessment



Cyber Risk Prevention & Detection Strategies



Cyber Risk Prevention & Detection Strategies



Polling Question 1

Machine Learning in Cyber Security

Machine learning (ML) approach to cyber threats

STOUT

THREATS[1]

- Information Gathering — Sniffing
- Intrusions — ATO
- Malware — Virus
- Intrusion Attempts — Login
- Fraud — Phishing
- Availability Attacks — DoS
- Abusive Content — Spam

COMPONENTS

- NETWORK
- ENDPOINT
- APPLICATION
- USER

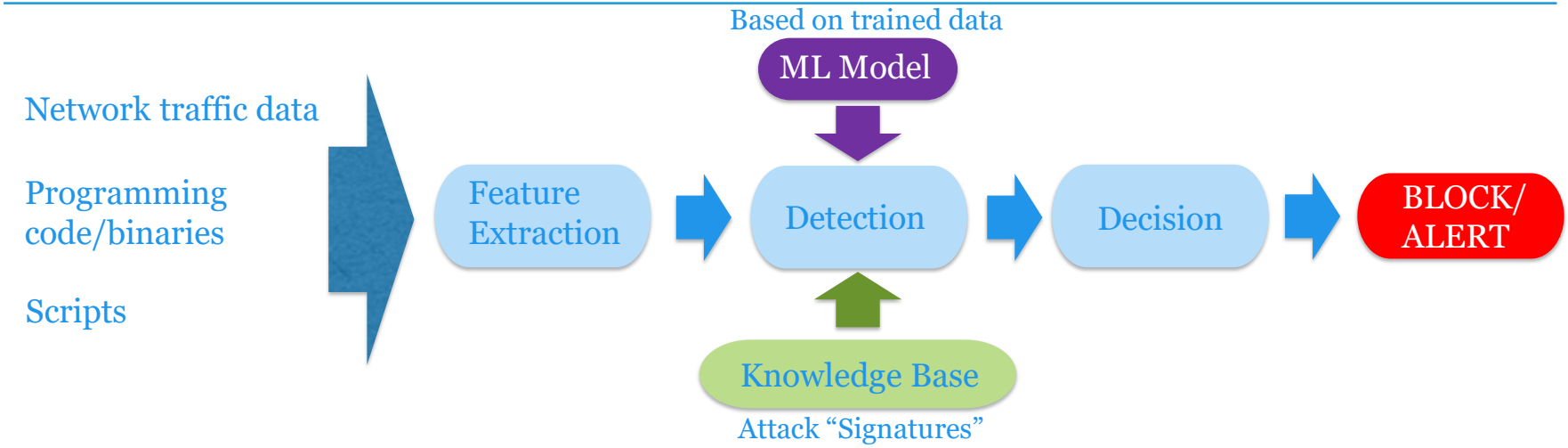
OBJECTIVES/ACTIONS[2]

ML METHODS

- ANOMALY DETECTION
- PATTERN RECOGNITION
- Classification — SUPERVISED LEARNING
- Clustering — UNSUPERVISED LEARNING

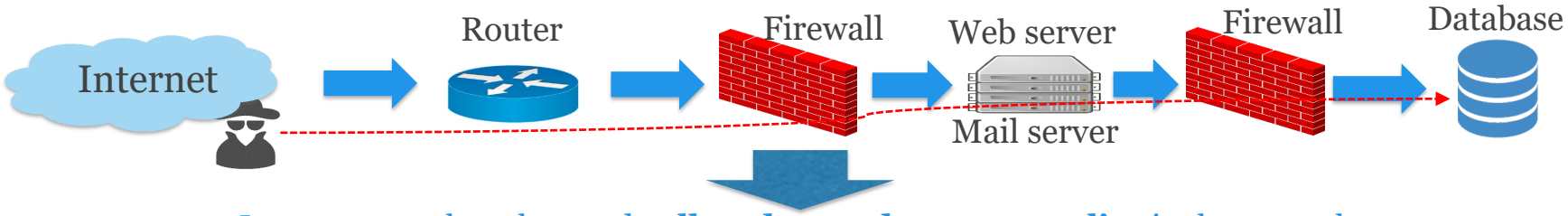
1 EU Agency (ENISA) taxonomy
2 Gartner PPDR model

ML/AI vs Traditional methods in cybersecurity



TRADITIONAL	MACHINE LEARNING
Targets known attacks	Recognizes new abnormal patterns
Static rules-based. Reactive	Dynamic. Keeps improving by learning
Prone to human error	Efficient and automated

Case study: How ML methods protect network breaches



Inspect network packets and **collect data to detect anomalies** in the network

CHALLENGES

1. **Not standardized anomaly detection techniques**, i.e., completely different for wired vs wireless networks
2. **Large amounts of data that contain noise** and make it difficult to detect anomalies
3. Data are not labeled, i.e., it is not known **which traffic patterns correspond to unusual behavior**
4. **Intruders are aware of traditional techniques**; need for more sophisticated methods

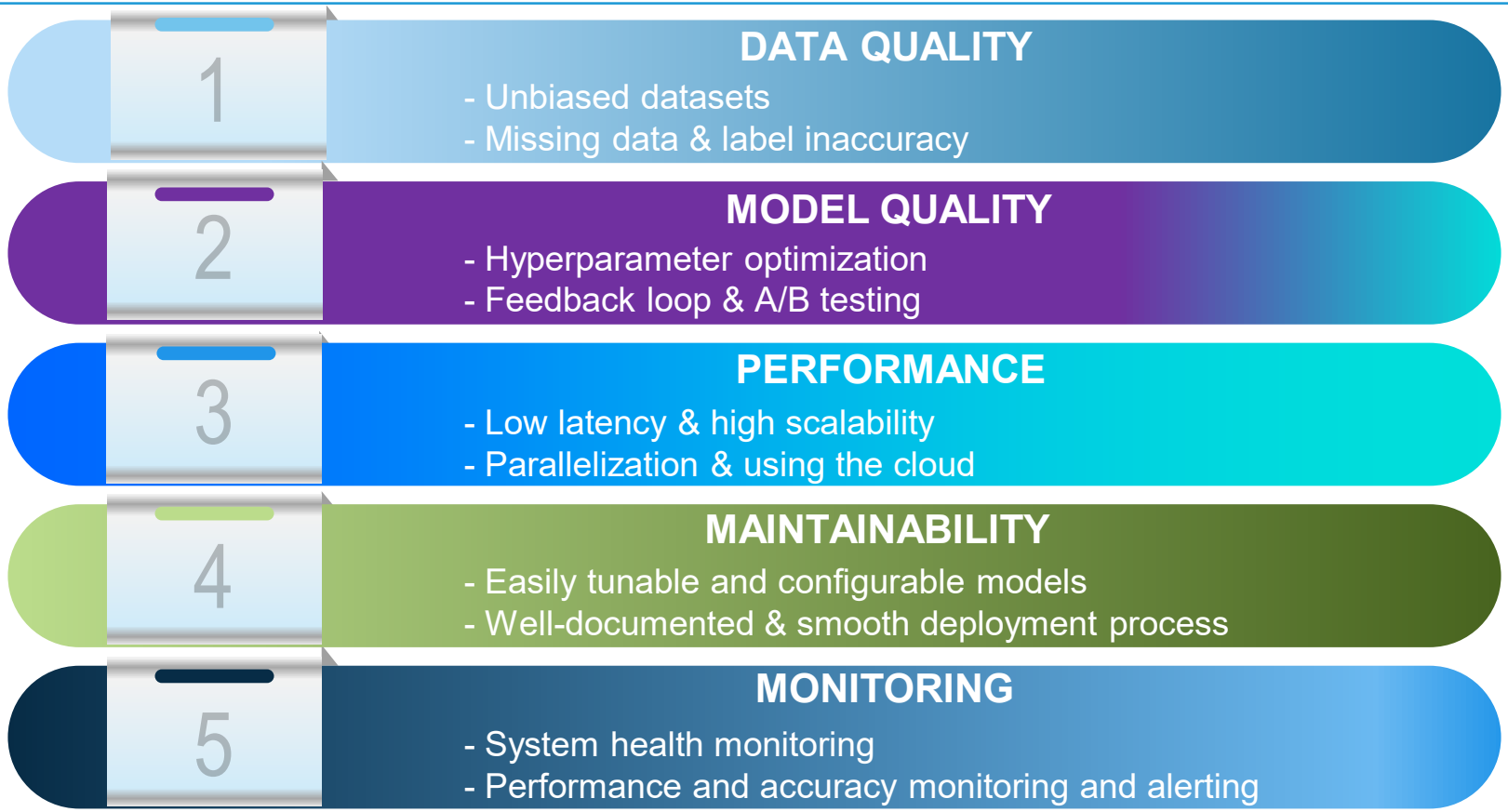
SOLUTIONS

SUPERVISED — CLASSIFIER → **Model learns from a comparable public dataset** and classifies new traffic data to categories such as DoS, privilege escalation attempts or unauthorized access

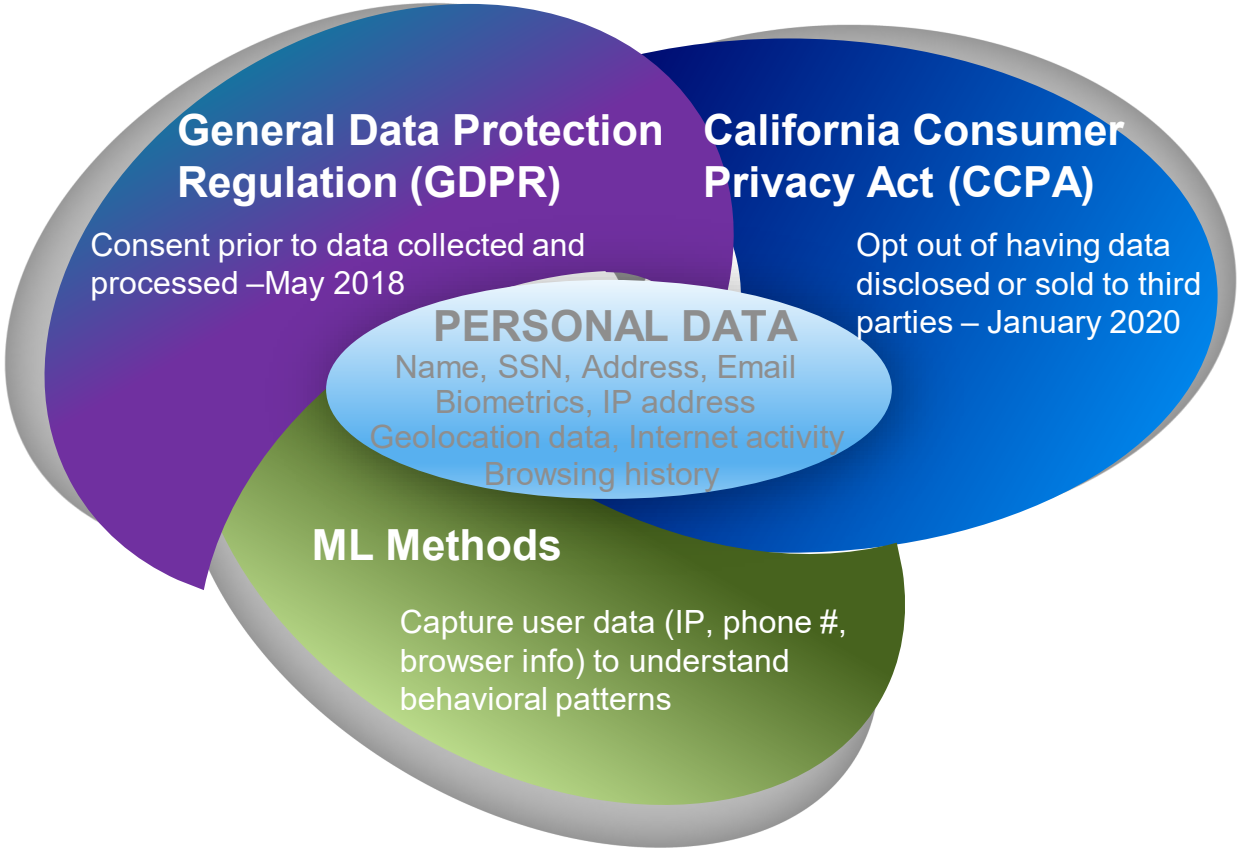
UNSUPERVISED — CLUSTERING → **Model figures out the categories/clusters** of data and it chooses the data category every new data point belongs based on similar data values

Deploying production-ready security ML systems

STOUT



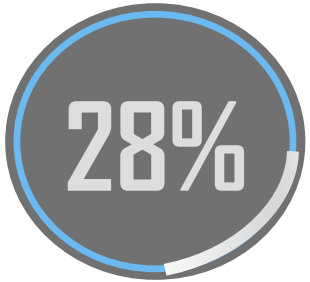
ML and data privacy regulations



- ANONYMIZATION
- MASKING
- ENCRYPTION
- EXPLAINABILITY

AI-assisted data breaches are a growing concern

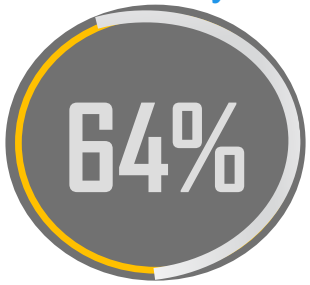
Likelihood to experience a data breach of at least 10K records[1]



Average cost of a data security breach in 2020[2]

Days needed to detect data breaches[3]

Percentage of executives that say AI lowers cost to detect threats by 12%[4]



AI/ML methods are the future in cybersecurity

1 Security Intelligence study, 2018 2 Juniper Research study 3 IBM Ponemon Institute 4 Centrify survey

Polling Question 2

Data breach life Cycle and Tools

20Minute

4iQ®

Life Cycle of a Breach.

Table of contents

What is a Breach?

What is a Data Breach?

4iQ defines a data breach as a confirmed incident where credentials, personal, medical, financial or other records with sensitive data have been accessed or disclosed due to being hacked or leaked, whether deliberately or by accident.

What is contained in a Data Breach?

Bank Information

INCOME TAX NUMBER

BANK/ CREDIT CARD NUMBER

IBAN

CRYPTO-CURRENCY

Identifiable Information

PASSPORT NUMBER

DRIVERS LICENSE

SOCIAL SECURITY NUMBER

NATIONAL ID NUMBER

Medical Information

MEDICAL INSURANCE PROVIDER

MEDICAL INSURANCE NUMBER

INSURANCE ACCOUNT NUMBER

INSURANCE PROVIDER

Personal Information

NAME

USERNAME

SURNAME

PASSWORD

PHONE NUMBER

EMAIL

DATE OF BIRTH

HOME ADDRESS

MOTHER'S MAIDEN NAME

Business Information

COMPANY

DOMAIN

EIN, DUNS, SAFE, SoS

Some examples...

tvman (97%) Seller Level 3 (2697) Trust Level 3
Verified Seller : / Trusted Seller :
Positive Feedback : (97%)
Member since : Sep 15, 2019
Last Login : Feb 07, 2020
Sales : 2697
Orders : 0

Sold : *0* Times
Origin Country : World Wide
Ship to : World Wide
Payment : Full Escrow
Product class : Physical Package
Quantity : Unlimited Available

Sale Price : 35.00 USD / 0.00358877 BTC
Sale Price : 35.00 USD / 0.43870644 XMR
Sale Price : 35.00 USD / 0.47827275 LTC
Sale Price : 35.00 USD / 0.08035448 BCH

Shipping Options :
Default - 1 Day - 0.00 USD / 0.00000000 BTC

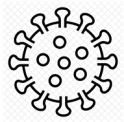
Pricing

Country	Price for Passport	Price for Passport + Driving license	Price for Passport + ID card	Price for Passport + Driving license + ID card
Australia	600 Euro	700 Euro	700 Euro	800 Euro
Belgium	500 Euro	600 Euro	600 Euro	700 Euro
Brazil	450 Euro	-	-	-
Canada	600 Euro	700 Euro	700 Euro	800 Euro
Ireland	500 Euro	600 Euro	600 Euro	700 Euro
Italia	550 Euro	650 Euro	650 Euro	750 Euro
Finland	500 Euro	600 Euro	600 Euro	700 Euro
France	600 Euro	700 Euro	700 Euro	800 Euro
Germany	600 Euro	700 Euro	700 Euro	800 Euro
Malaysia	450 Euro	-	550 Euro	-
Netherlands	600 Euro	700 Euro	700 Euro	800 Euro
Norway	650 Euro	750 Euro	750 Euro	850 Euro
Poland	500 Euro	600 Euro	600 Euro	700 Euro
Portugal	500 Euro	600 Euro	600 Euro	700 Euro
Spain	550 Euro	650 Euro	650 Euro	750 Euro
Switzerland	650 Euro	750 Euro	750 Euro	850 Euro
Sweden	550 Euro	650 Euro	650 Euro	750 Euro
United Kingdom	650 Euro	750 Euro	-	-
USA	700 Euro	800 Euro	800 Euro	900 Euro

Passports:

Current Data Breach Trends

Covid-19 & Cyber Crime



Covid-19 has had immediate impact on the security posture of organizations across the globe. But what are some long-term trends?

- Cyber-attacks up **37%** since COVID-19
- **22% Americans** say they've been targeted by **digital fraud** related to COVID-19.
  23% increase in global **eCommerce transactions**.
- 2020-2021: **More breaches expected** due to the downturn of cyber security investments.

Focus on Government

Government breaches across the globe are increasing every year, putting nations and citizens at risk. Data is leveraged for a myriad of attacks.

- **23.9% Increase** in Government Breaches from 2018-2019.
- **3,867** government breaches expose over **356 Million** identity records in 2019
- **Rising geopolitical tensions result in exposed data being weaponized by nation states and criminal groups.**

Focus on Financial Services

Industry breaches have increased and cryptocurrency adoption is spreading globally with new communities and services being built and breaches.

- **4.3% Increase** in Financial Services breaches from 2018-2019.
- **57%** report higher fraud losses with account creation and ATO
- $**16.9 Billion** in fraud losses in 2019
- **Shift to high-impact identity and savings account fraud**

Massive Data & Identity-based Attacks

There's been an increase in big data packages circulating in underground markets. Threat actors are collecting, curating and correlating PII to build identity profiles for future crimes.

- **25.5% increase in raw identity records** exposed in the Dark Web from 2018-2019
- **88% of consumers** say their perception of a business improves when a business **invests in security**.

Polling Question 3

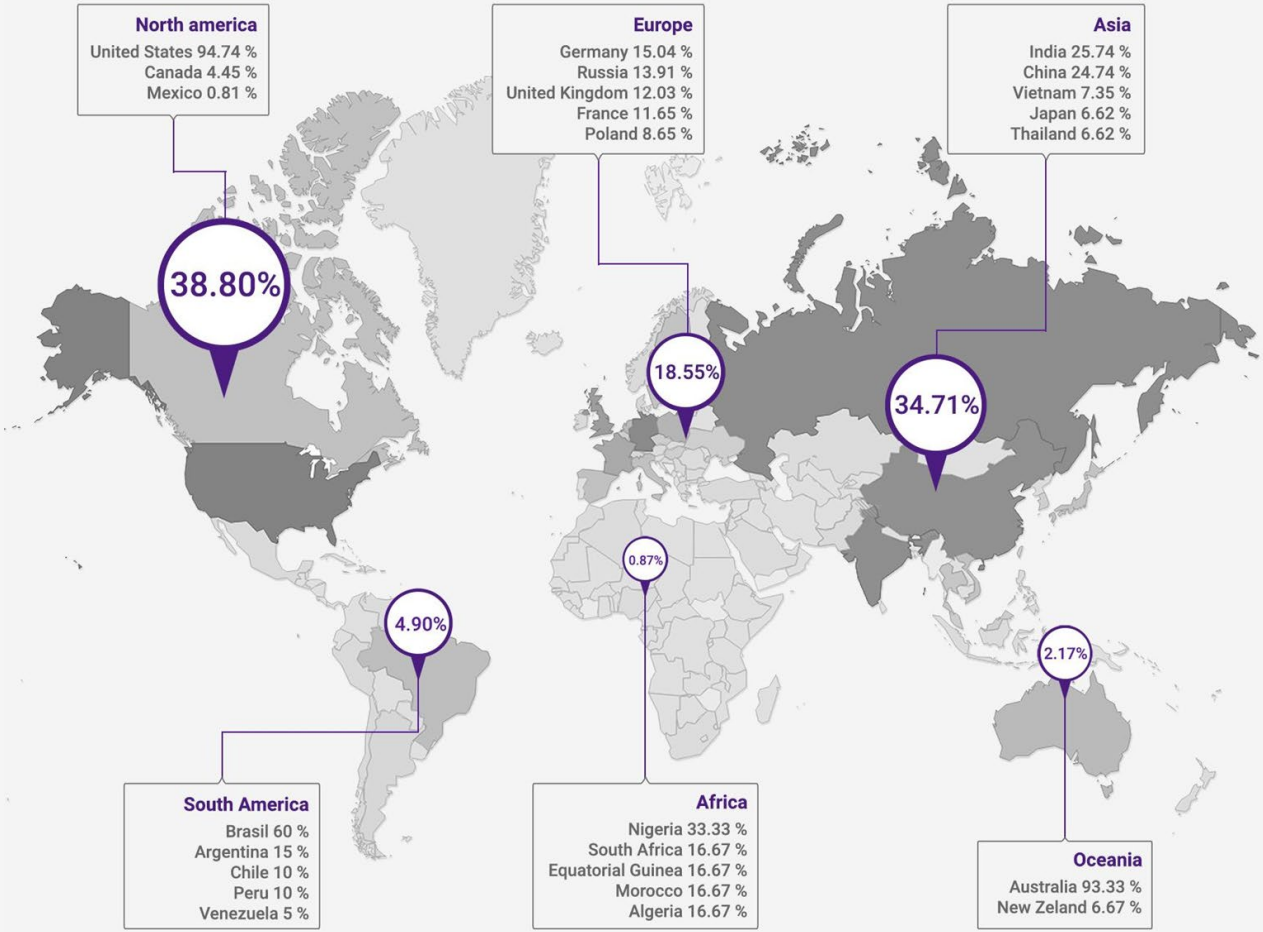
4iQ saw **18.7 Billion Raw Identity Records**

circulating, with **4.2 Billion New, Authentic Identity Records in 2019**

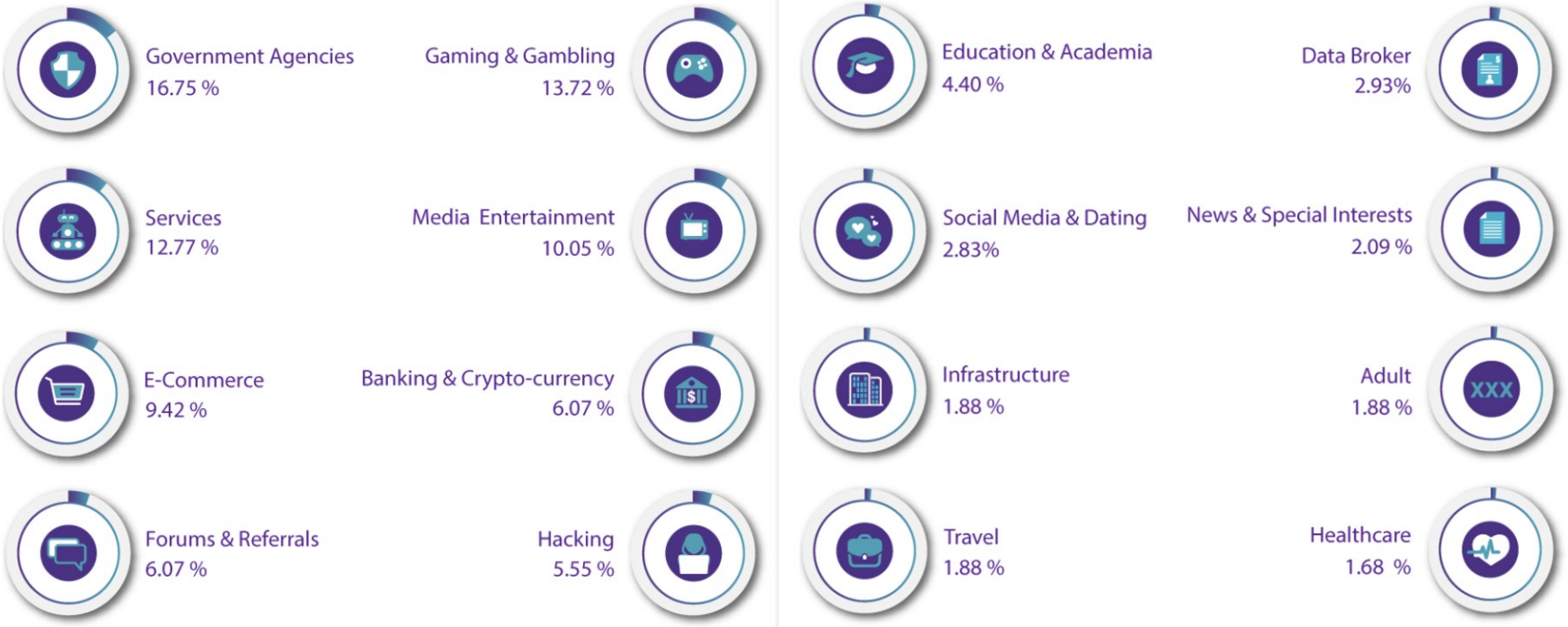
12,798 Real, New Identity Breaches

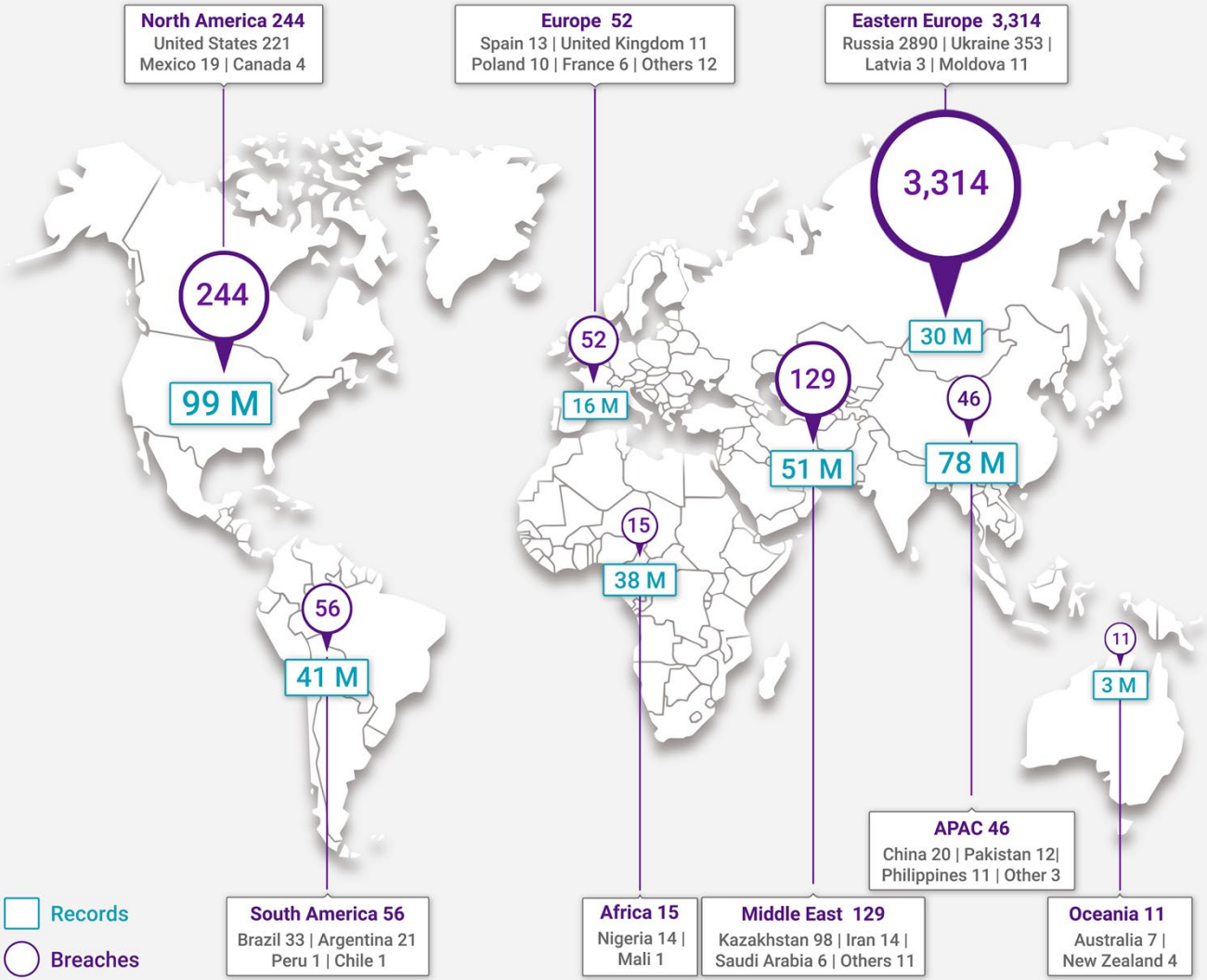
(16.5% higher than 2018)

Who Do Breaches Affect?



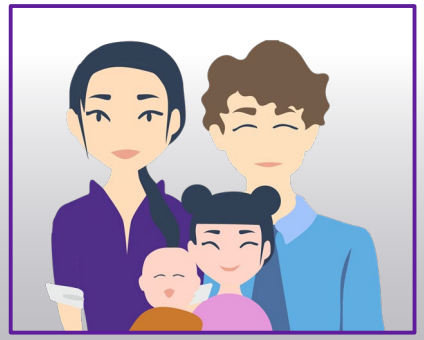
Breaches by Sector (2019)




North America 244
United States 221
Mexico 19 | Canada 4
Europe 52
Spain 13 | United Kingdom 11
Poland 10 | France 6 | Others 12
Eastern Europe 3,314
Russia 2890 | Ukraine 353 |
Latvia 3 | Moldova 11
244
99 M
52
16 M
3,314
30 M
129
51 M
46
78 M
56
41 M
15
38 M
11
3 M
APAC 46
China 20 | Pakistan 12|
Philippines 11 | Other 3
Records
Breaches
South America 56
Brazil 33 | Argentina 21
Peru 1 | Chile 1
Africa 15
Nigeria 14 |
Mali 1
Middle East 129
Kazakhstan 98 | Iran 14 |
Saudi Arabia 6 | Others 11
Oceania 11
Australia 7 |
New Zealand 4

What happens to Breach Data?

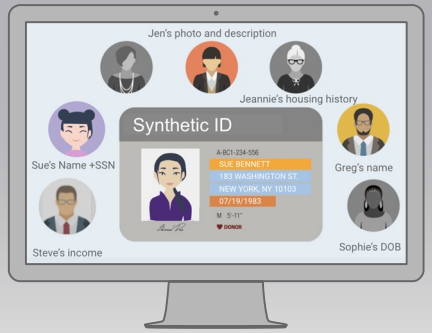
Hackers already have this data & are **using it to attack people**



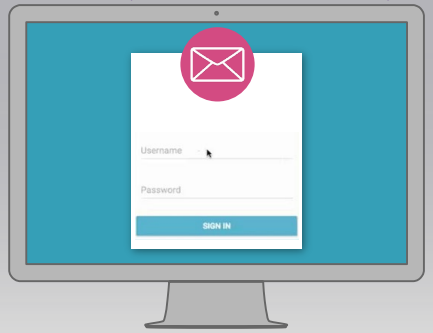
BLACK MARKETS

Where Everything Has a Price

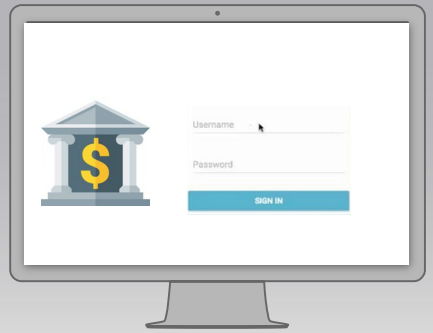
SYNTHETIC ID/IDTHEFT



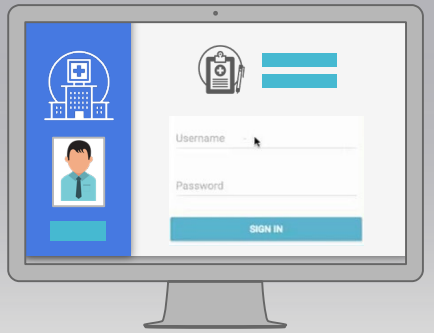
EMAIL (ACCT' TAKEOVER)



FINANCIAL FRAUD



COMPANY DATA



Unmask Adversaries

Executive Protection

Identity Protection

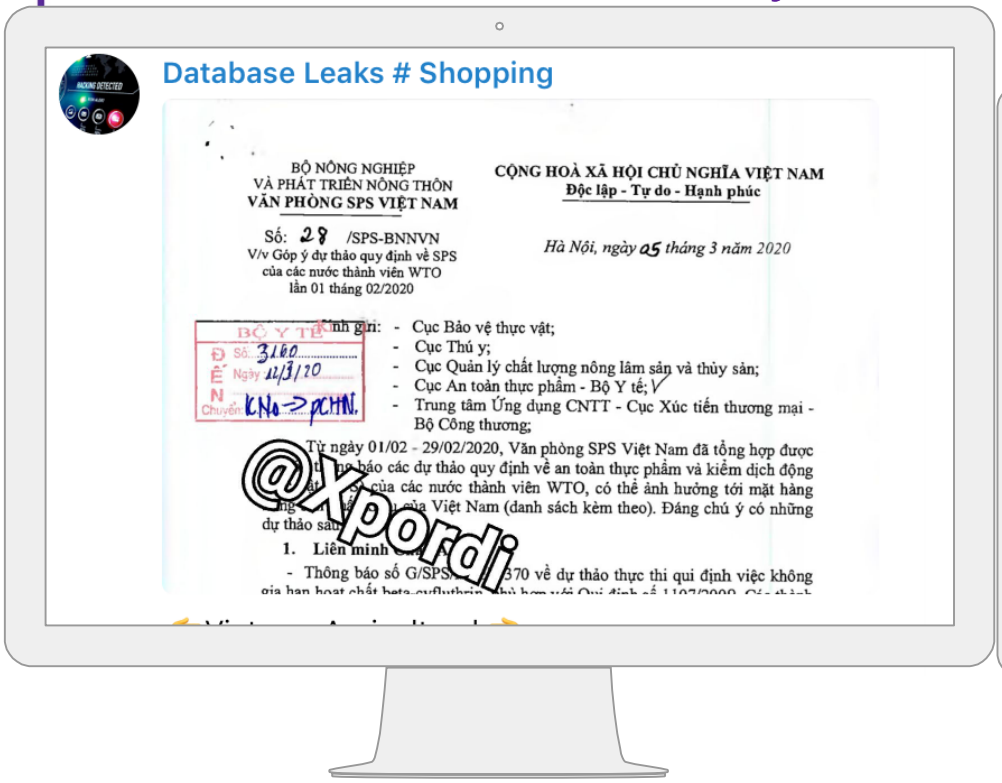
Domain Monitoring

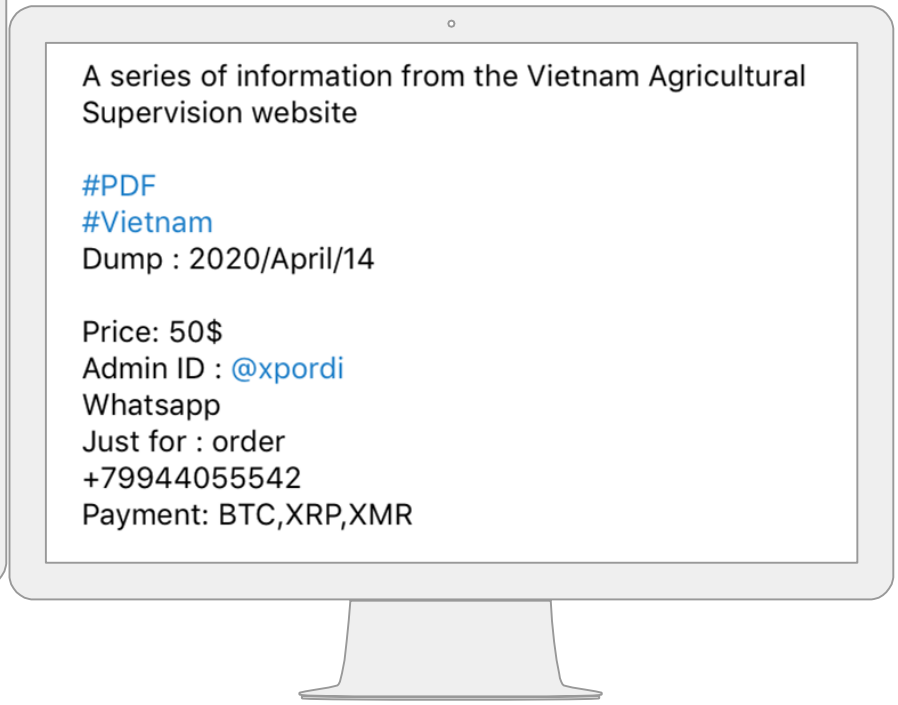
Password Validation

Polling Question 4

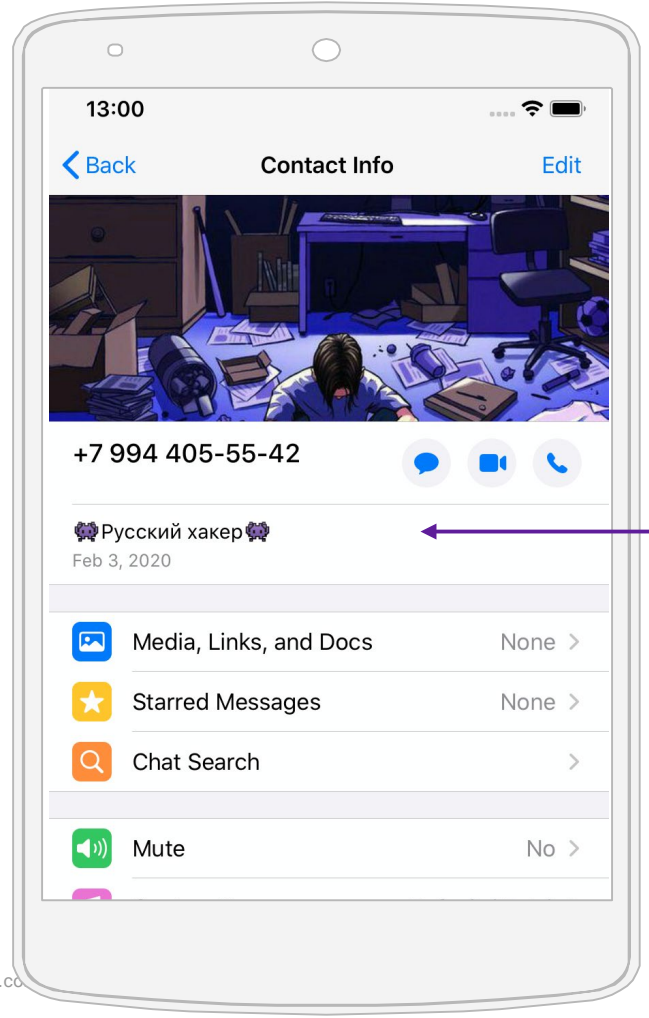
CASE STUDY

Seller with Social Security Numbers & other breached data



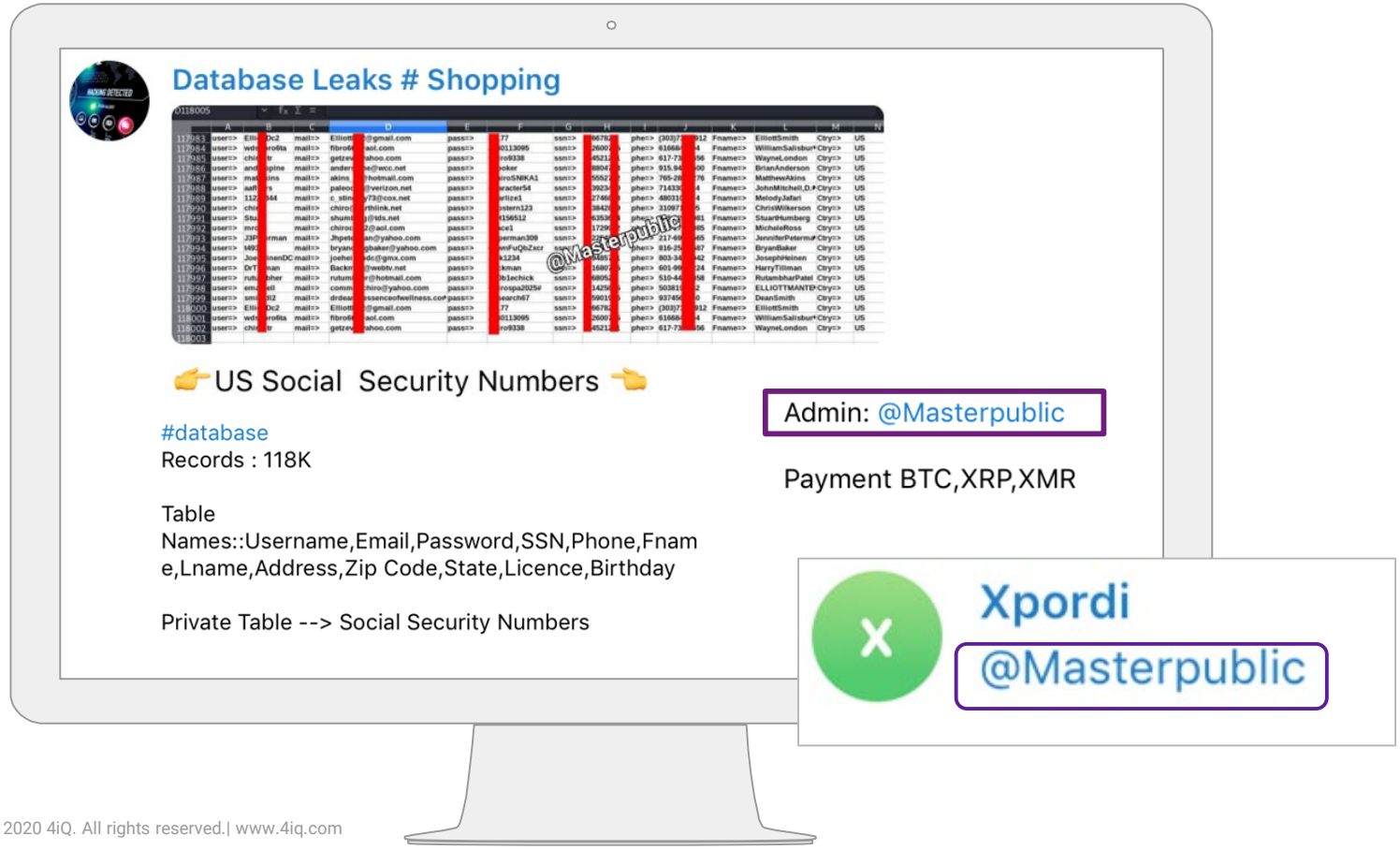


Whatsapp

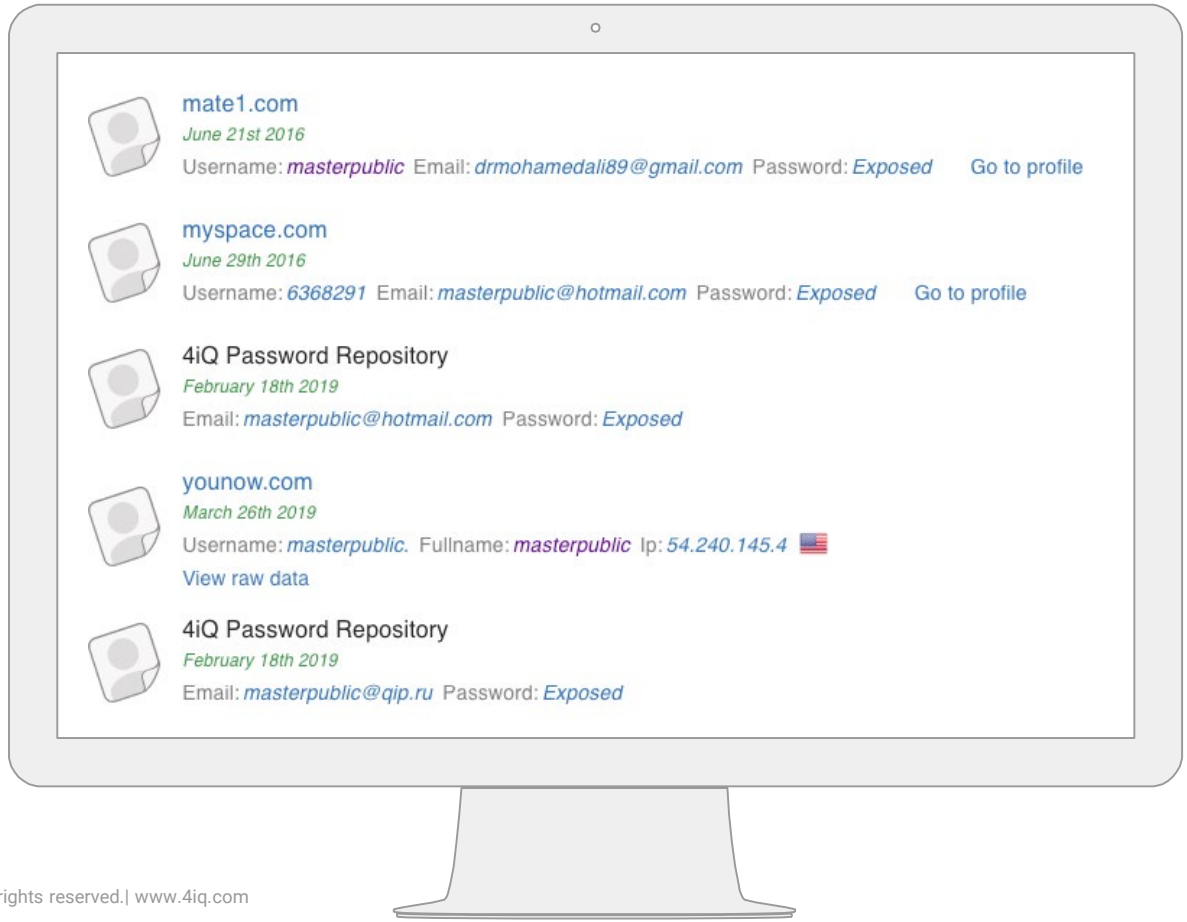


Translates to “Russian Hacker”

Changed name, now offering U.S. Social Security Numbers



Breach Results



Weaponized Data Breaches: Fueling Identity-based Attacks Across the Globe.

4iQ's latest report offers a unique perspective on how the underground Breach Economy reflects the severity of targeted public/private sector cyber intrusions and provides exclusive insight into what is reported (and not reported) in our news headlines today.

READ THE REPORT: https://4iq.com/2020-identity-breach-report/

Q & A

CONTACT US

Mark Scarmozzino
Los Altos, CA
mark.scamozzino@4iq.com
+1.917.691.7060

Erin Brown
Los Altos, CA
erin.brown@4iq.com

Uday Gulvadi
New York, NY
ugulvadi@stout.com
+1.646.810.4322

Fotis Konstantinidis
Los Angeles, CA
fkonstantinidis@stout.com
+1.310.601.2568

Thank you!