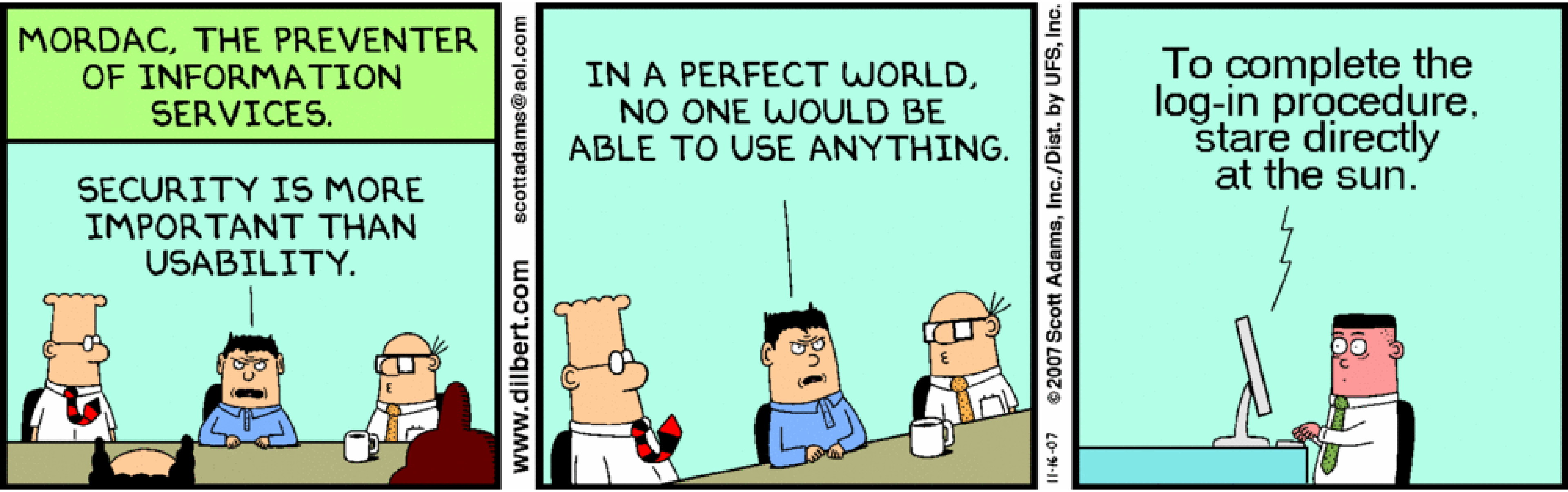
Cyber Threat Intelligence

Presentation by:

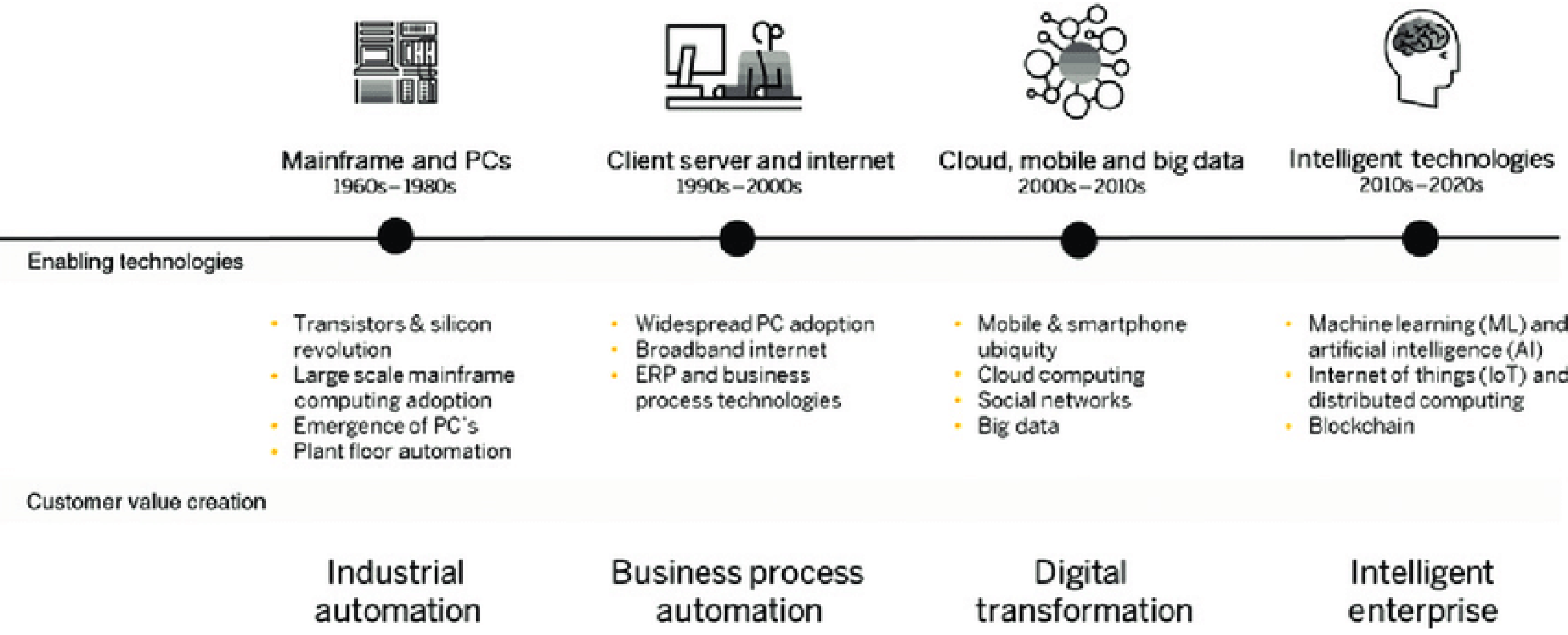
Musa Wesutsa
Managing Director, Sentinel Africa
CISSP, CISA, CDPO, CISO

December 2020

Competing Priorities


MORDAC, THE PREVENTER OF INFORMATION SERVICES.
SECURITY IS MORE IMPORTANT THAN USABILITY.
scottadams@aol.com
www.dilbert.com
IN A PERFECT WORLD, NO ONE WOULD BE ABLE TO USE ANYTHING.
11-16-07
© 2007 Scott Adams, Inc./Dist. by UFS, Inc.
To complete the log-in procedure, stare directly at the sun.

Evolution of IT



Mainframe and PCs
1960s–1980s

Client server and internet
1990s–2000s

Cloud, mobile and big data
2000s–2010s

Intelligent technologies
2010s–2020s

Enabling technologies

- Transistors & silicon revolution
- Large scale mainframe computing adoption
- Emergence of PC's
- Plant floor automation

- Widespread PC adoption
- Broadband internet
- ERP and business process technologies

- Mobile & smartphone ubiquity
- Cloud computing
- Social networks
- Big data

- Machine learning (ML) and artificial intelligence (AI)
- Internet of things (IoT) and distributed computing
- Blockchain

Customer value creation

Industrial automation

Business process automation

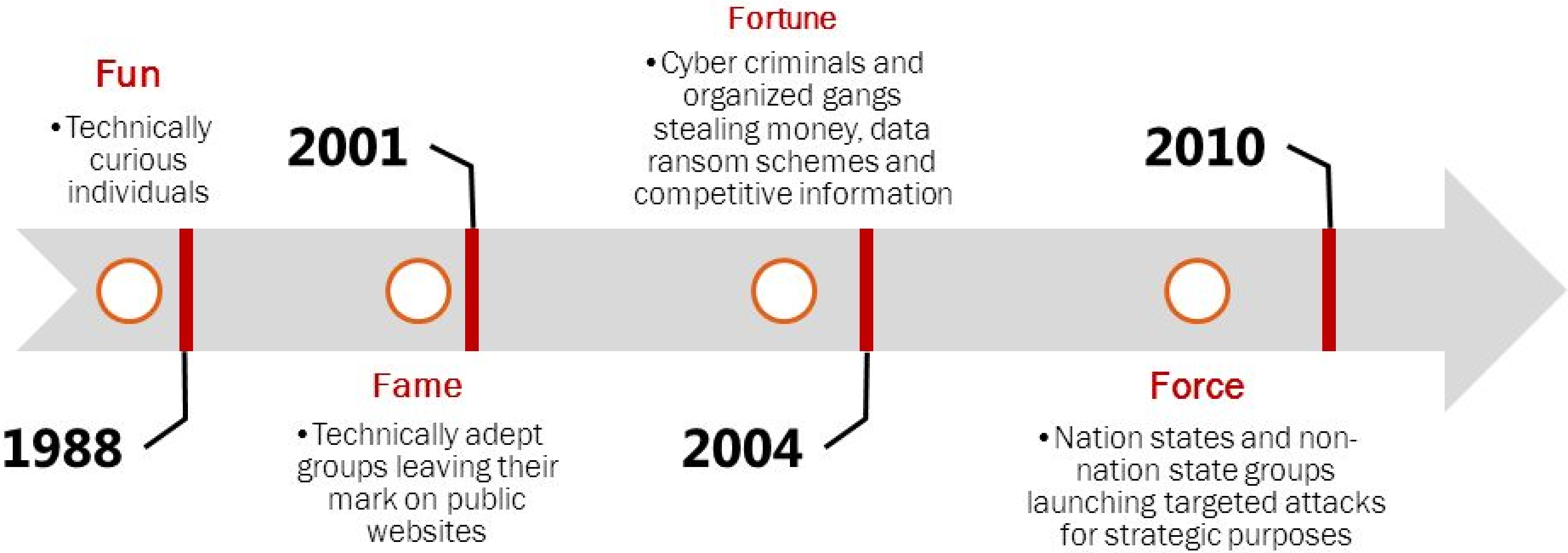
Digital transformation

Intelligent enterprise

CENTRALISED → DATA LOCATION → DECENTRALISED

Evolution of Cyber Attacks

Cyber Threats on the Private Sector



1988

Fun

- Technically curious individuals

2001

Fame

- Technically adept groups leaving their mark on public websites

2004

Fortune

- Cyber criminals and organized gangs stealing money, data ransom schemes and competitive information

2010

Force

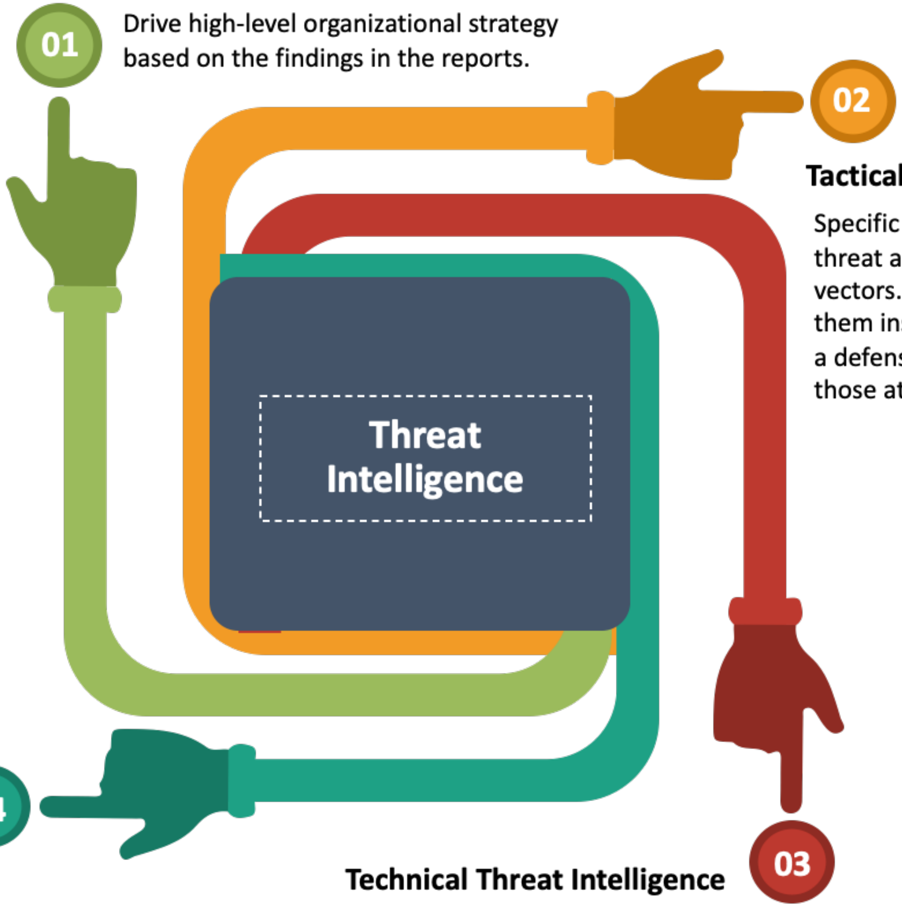
- Nation states and non-nation state groups launching targeted attacks for strategic purposes

Definition

"Cyber threat intelligence is information about threats an organization has or is exposed to, their modus operandi, motive, and the business impact in the event of such attack. This intelligence is used to identify, prepare, and protect the organization from cyber threats"

EC-COUNCIL

Threat Intelligence Levels



Strategic Threat Intelligence

Drive high-level organizational strategy based on the findings in the reports.

Tactical Threat Intelligence

Specific details to understand threat actors and the attack vectors. Intelligence gives them insights on how to build a defense strategy to mitigate those attacks.

Technical Threat Intelligence

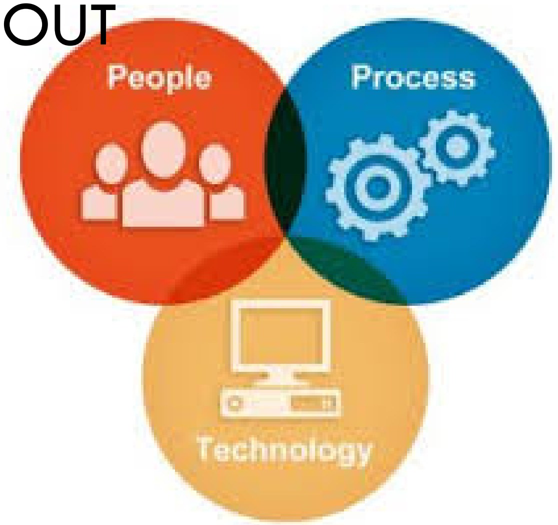
Focuses on Indicators of Compromise and creates a base to analyze such attacks.

Operational Threat Intelligence

Knowledge of the attack with insights on factors like nature, motive, timing, and how an attack is carried out..

Conditions Necessary for Fraud

- Malicious, culpable, compromised / motivated insider. 58% insider threat.
- A breakdown in a process or an existing process weakness e.g. no segregation of duties, lack of privilege access management, IT in ops
- Monitoring technology is not detective, is missing or we are monitoring the wrong thing. WHAT ABOUT LOGS?



Compromised Controls

- USB Ports access (Policy violation)
- Processes: life cycle of credit from application to approval and disbursement.
- Credit application without uploading scanned copies of the physical application forms
- User behavioural analysis: This is extended to customers as well (example: debit card withdrawal limits changed)

Threat Intelligence Life Cycle

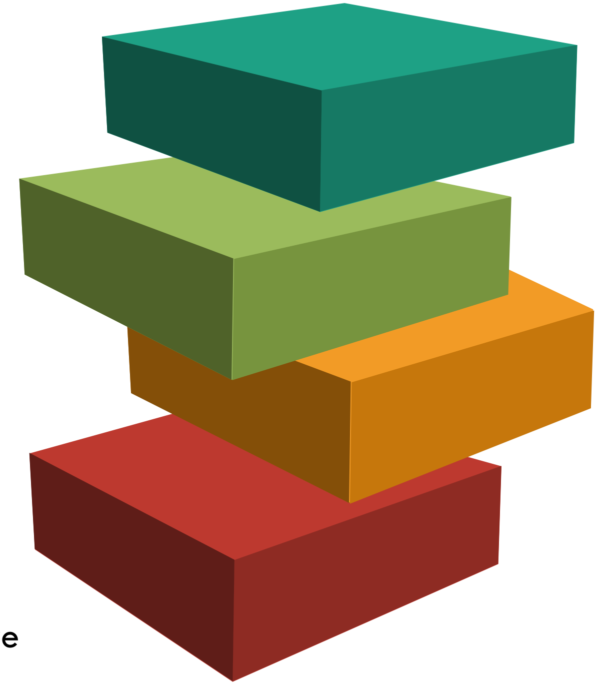
ICPAK
Uphold Public Interest

1. Collect

Collect historical and real time data (data warehouse, database, event logs etc.

2. Processing

Provide context to the data (from policies, processes, normal user behavior, transaction limits etc.



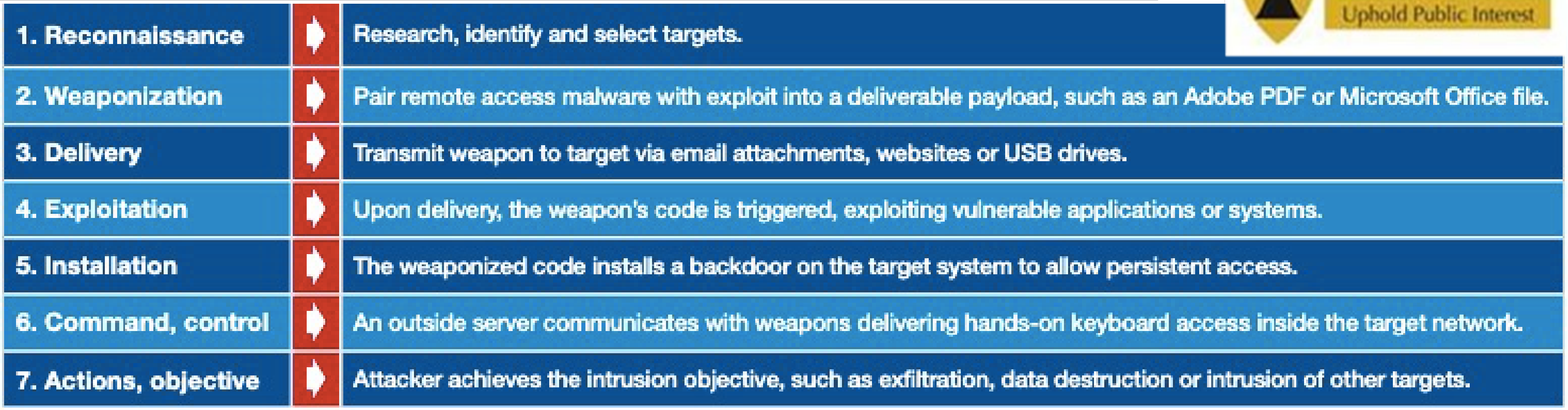
3. Analysis

Flag out abnormal user behaviour, transactions above limit, events outside the norm.

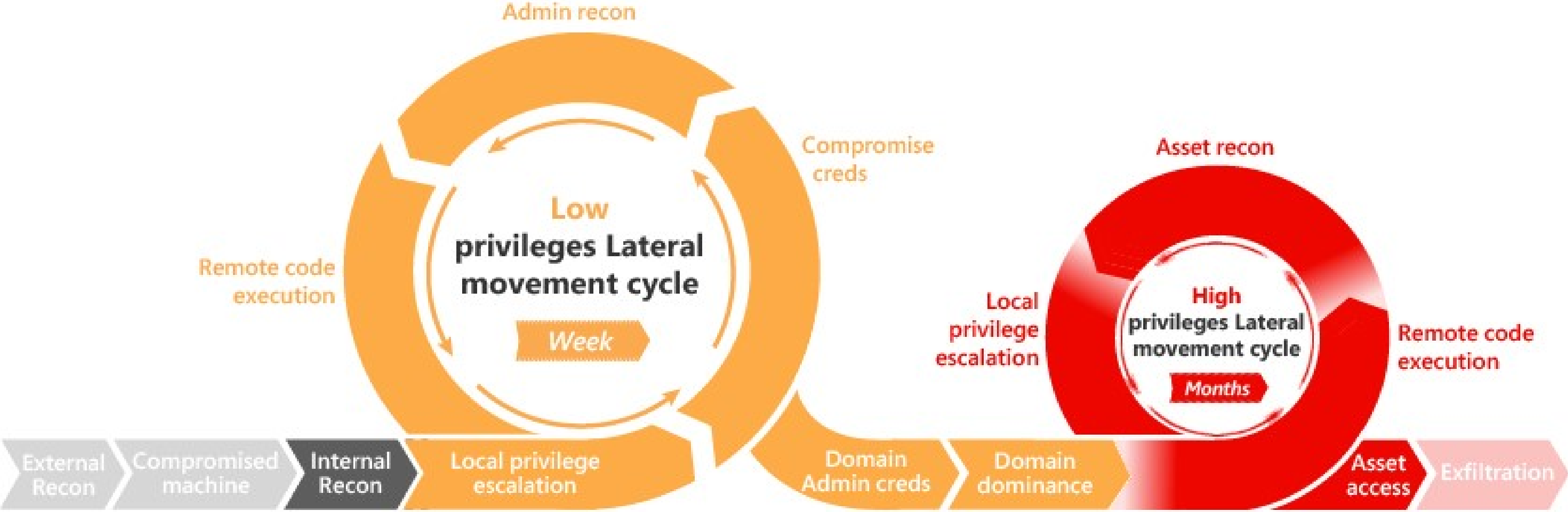
4. Dissemination

Share intelligence with relevant stakeholders and business/ process owners for decision-making, feedback.

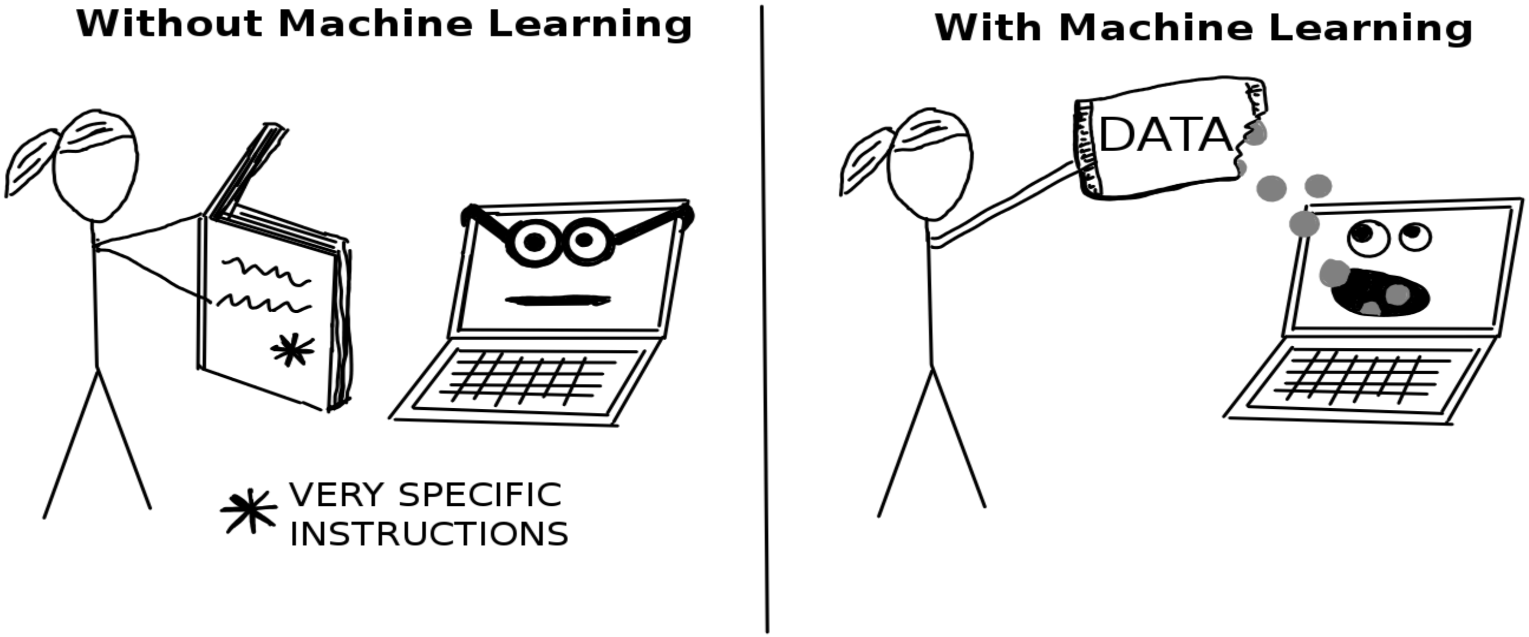
Cyber Kill Chain



1. Reconnaissance	Research, identify and select targets.
2. Weaponization	Pair remote access malware with exploit into a deliverable payload, such as an Adobe PDF or Microsoft Office file.
3. Delivery	Transmit weapon to target via email attachments, websites or USB drives.
4. Exploitation	Upon delivery, the weapon's code is triggered, exploiting vulnerable applications or systems.
5. Installation	The weaponized code installs a backdoor on the target system to allow persistent access.
6. Command, control	An outside server communicates with weapons delivering hands-on keyboard access inside the target network.
7. Actions, objective	Attacker achieves the intrusion objective, such as exfiltration, data destruction or intrusion of other targets.



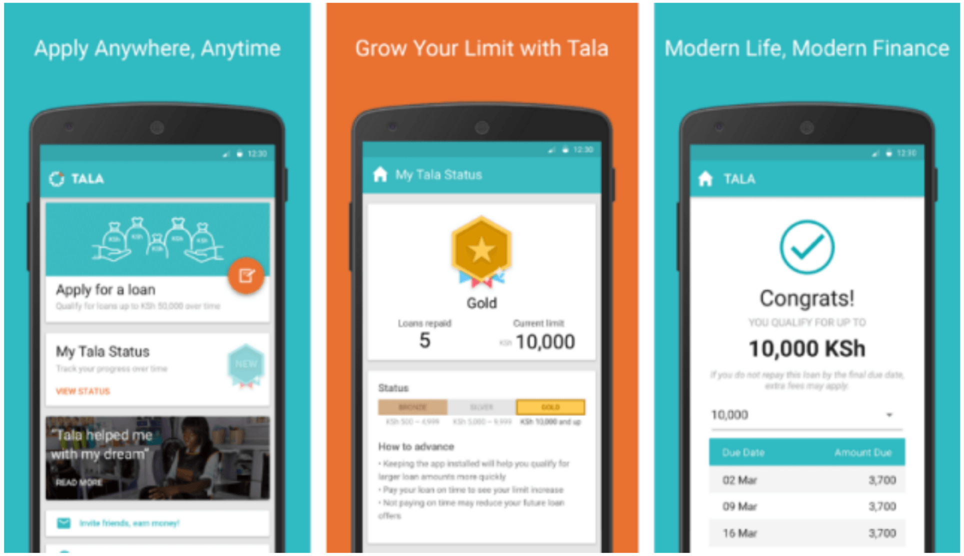
Approaches in Fraud Detection



- Humans learn from experience
- Machines follow instructions
- Making machines learn from ~~experience~~ data while autonomously learning from real-world interactions and datasets fed to them is what is referred to as machine learning

Business Application

ICPAK
Uphold Public Interest


Apply Anywhere, Anytime

TALA

Apply for a loan
Qualify for loans up to KSh 50,000 over time

My Tala Status
Track your progress over time
VIEW STATUS

"Tala helped me with my dream"
READ MORE

Invite friends, earn money!

Grow Your Limit with Tala

My Tala Status

Gold

Loans repaid	Current limit
5	KSh 10,000

Status

BRONZE	SILVER	GOLD
KSh 500 – 4,999	KSh 5,000 – 9,999	KSh 10,000 and up

How to advance
- Keeping the app installed will help you qualify for larger loan amounts more quickly
- Pay your loan on time to see your limit increase
- Not paying on time may reduce your future loan offers

Modern Life, Modern Finance

TALA

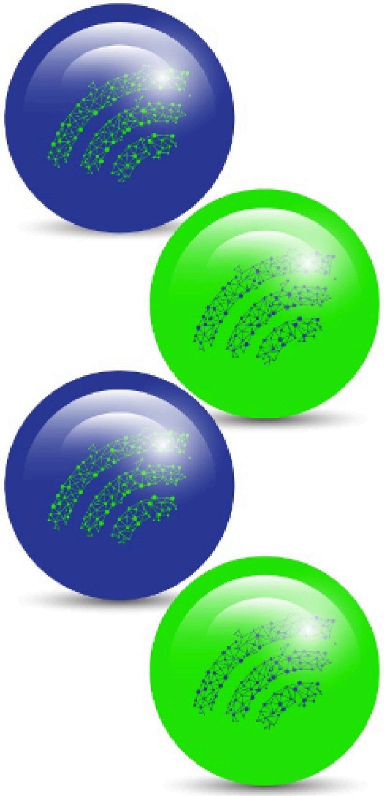
Congrats!
YOU QUALIFY FOR UP TO
10,000 KSh
If you do not repay this loan by the final due date, extra fees may apply.

10,000

Due Date	Amount Due
02 Mar	3,700
09 Mar	3,700
16 Mar	3,700

Approaches in Fraud Detection

ICPAK
Uphold Public Interest



Rule-based
Defining certain rules and label actions that do not match them as anomalous and potentially worth checking

Supervised Learning
Use historic data to detect anomalous and potentially fraudulent behavior

Unsupervised learning
Take advantage of recent advances in machine learning and leverage large amounts of data

Ensemble models
Combine different algorithms to achieve greater accuracy of anomaly/fraud detection

Machine Learning Approach

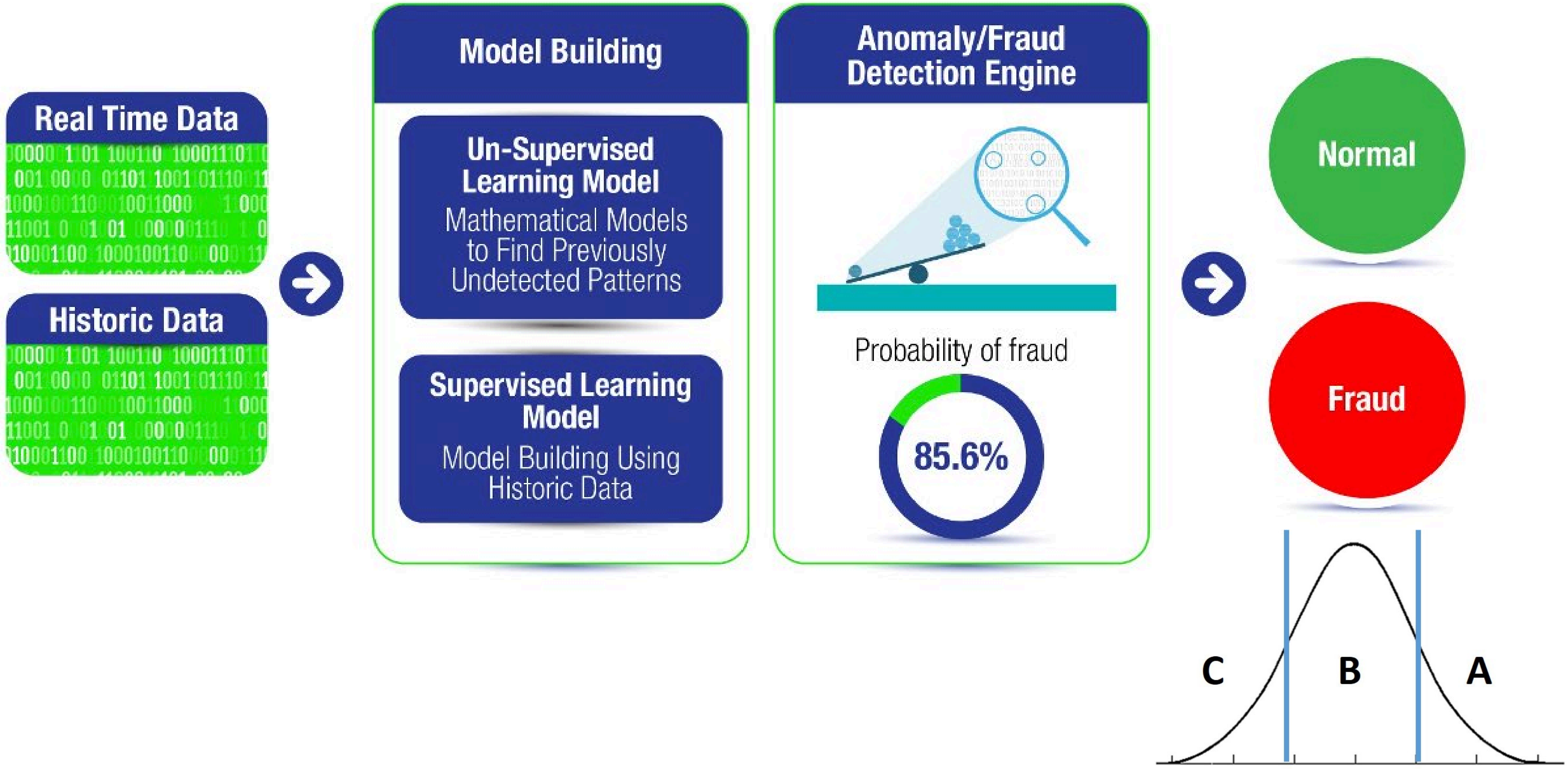
SUPERVISED LEARNING

- Based on labelled datasets
- Computer is given correct input and output pairs
- Labels are used to tell the model the expected output
- Algorithm accuracy is measured on how well it detects data with similar patterns from subsequent transactions.

UNSUPERVISED LEARNING

- Starts without labelled dataset
- Model groups data based on similar behaviour / patterns
- Outliers are flagged after grouping of the data.

Machine Learning Approach



Real Time Data

Historic Data

Model Building

Un-Supervised Learning Model
Mathematical Models to Find Previously Undetected Patterns

Supervised Learning Model
Model Building Using Historic Data

Anomaly/Fraud Detection Engine

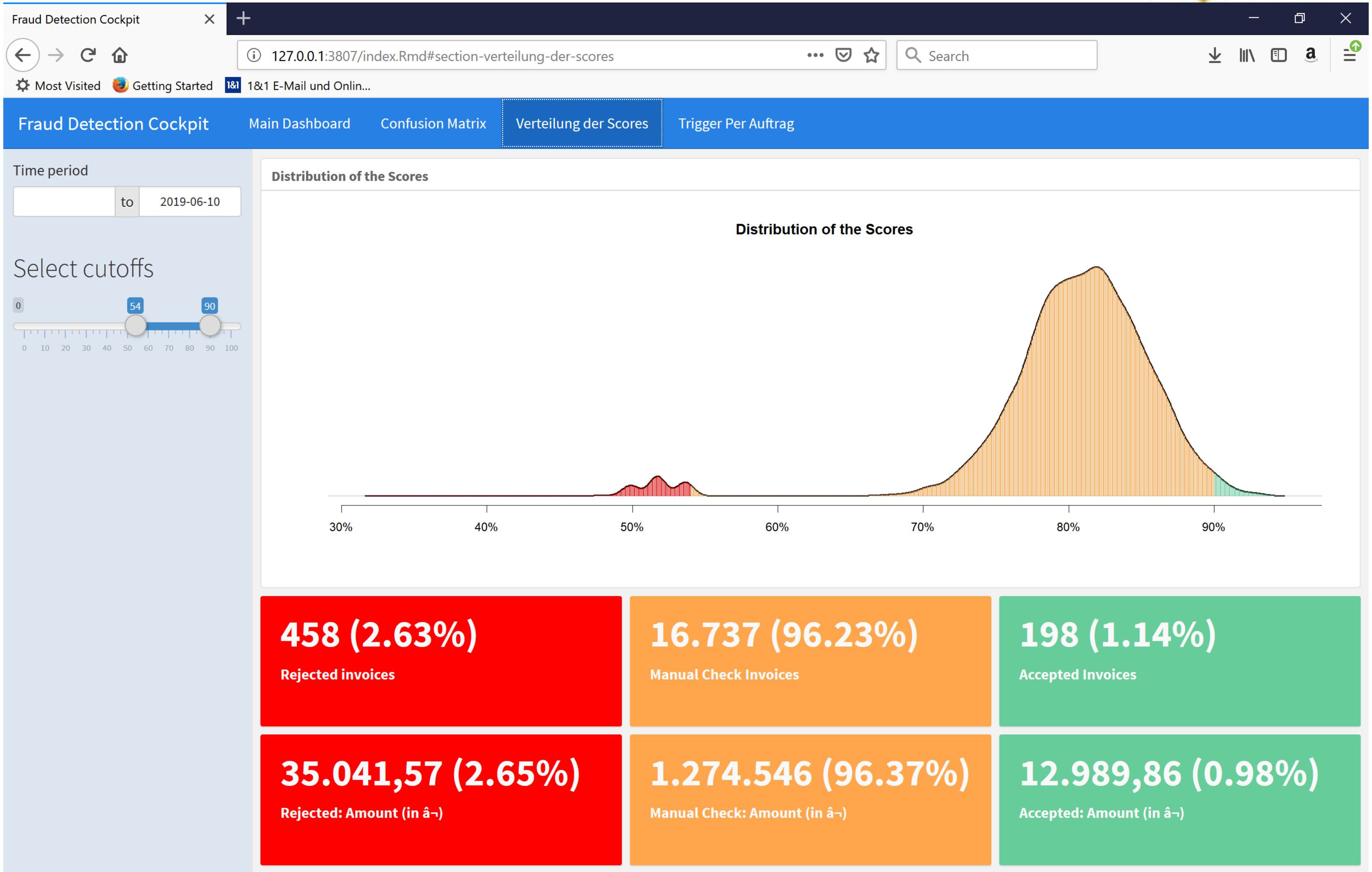
Probability of fraud

85.6%

Normal

Fraud

Machine Learning Approach



Time period

to 2019-06-10

Select cutoffs

Distribution of the Scores

Distribution of the Scores

458 (2.63%)
Rejected invoices

16.737 (96.23%)
Manual Check Invoices

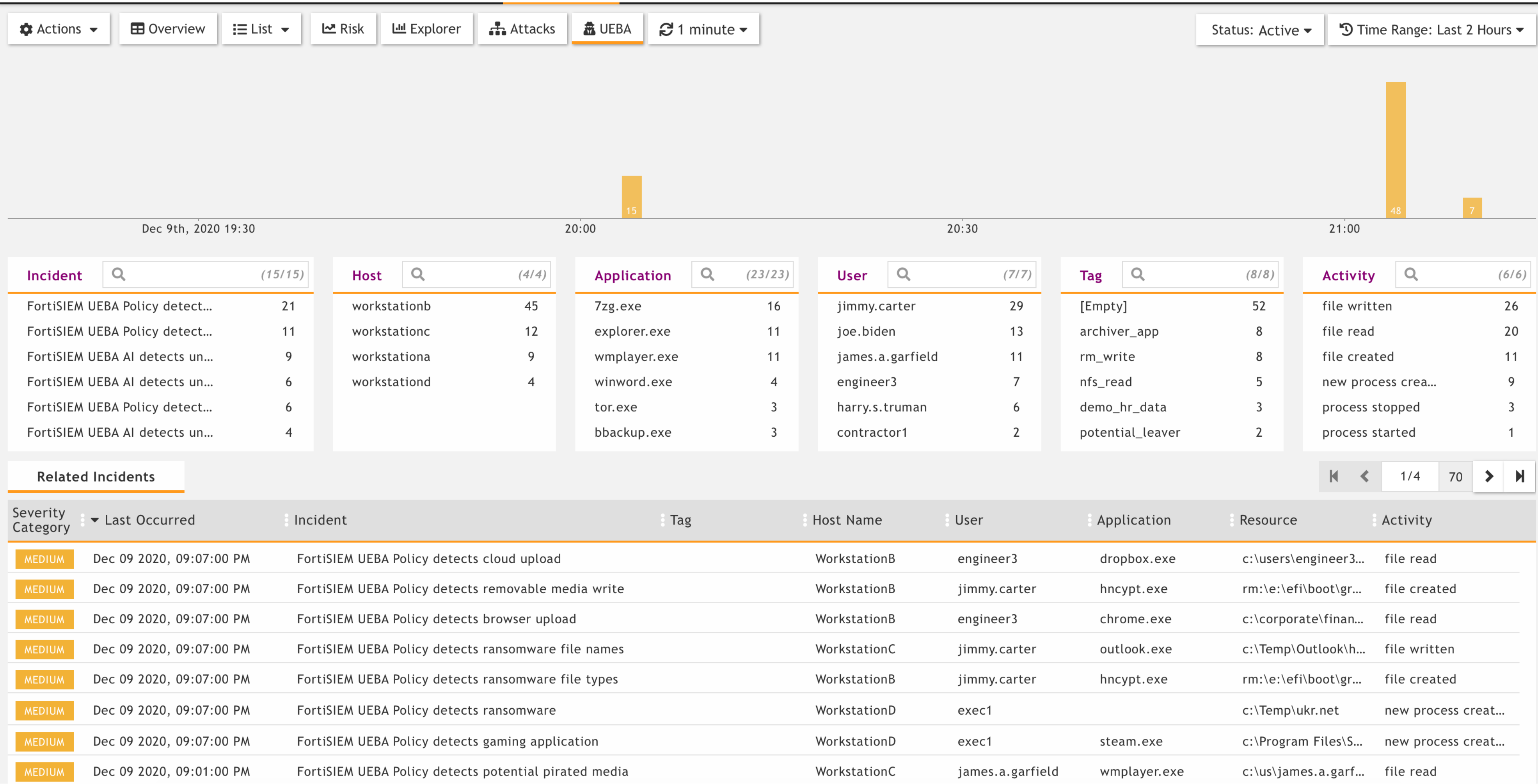
198 (1.14%)
Accepted Invoices

35.041,57 (2.65%)
Rejected: Amount (in â¬)

1.274.546 (96.37%)
Manual Check: Amount (in â¬)

12.989,86 (0.98%)
Accepted: Amount (in â¬)

Monitoring from a SOC



Incident (15/15)	
FortiSIEM UEBA Policy detect...	21
FortiSIEM UEBA Policy detect...	11
FortiSIEM UEBA AI detects un...	9
FortiSIEM UEBA AI detects un...	6
FortiSIEM UEBA Policy detect...	6
FortiSIEM UEBA AI detects un...	4

Host (4/4)	
workstationb	45
workstationc	12
workstationa	9
workstationd	4

Application (23/23)	
7zg.exe	16
explorer.exe	11
wmplayer.exe	11
winword.exe	4
tor.exe	3
bbackup.exe	3

User (7/7)	
jimmy.carter	29
joe.biden	13
james.a.garfield	11
engineer3	7
harry.s.truman	6
contractor1	2

Tag (8/8)	
[Empty]	52
archiver_app	8
rm_write	8
nfs_read	5
demo_hr_data	3
potential_leaver	2

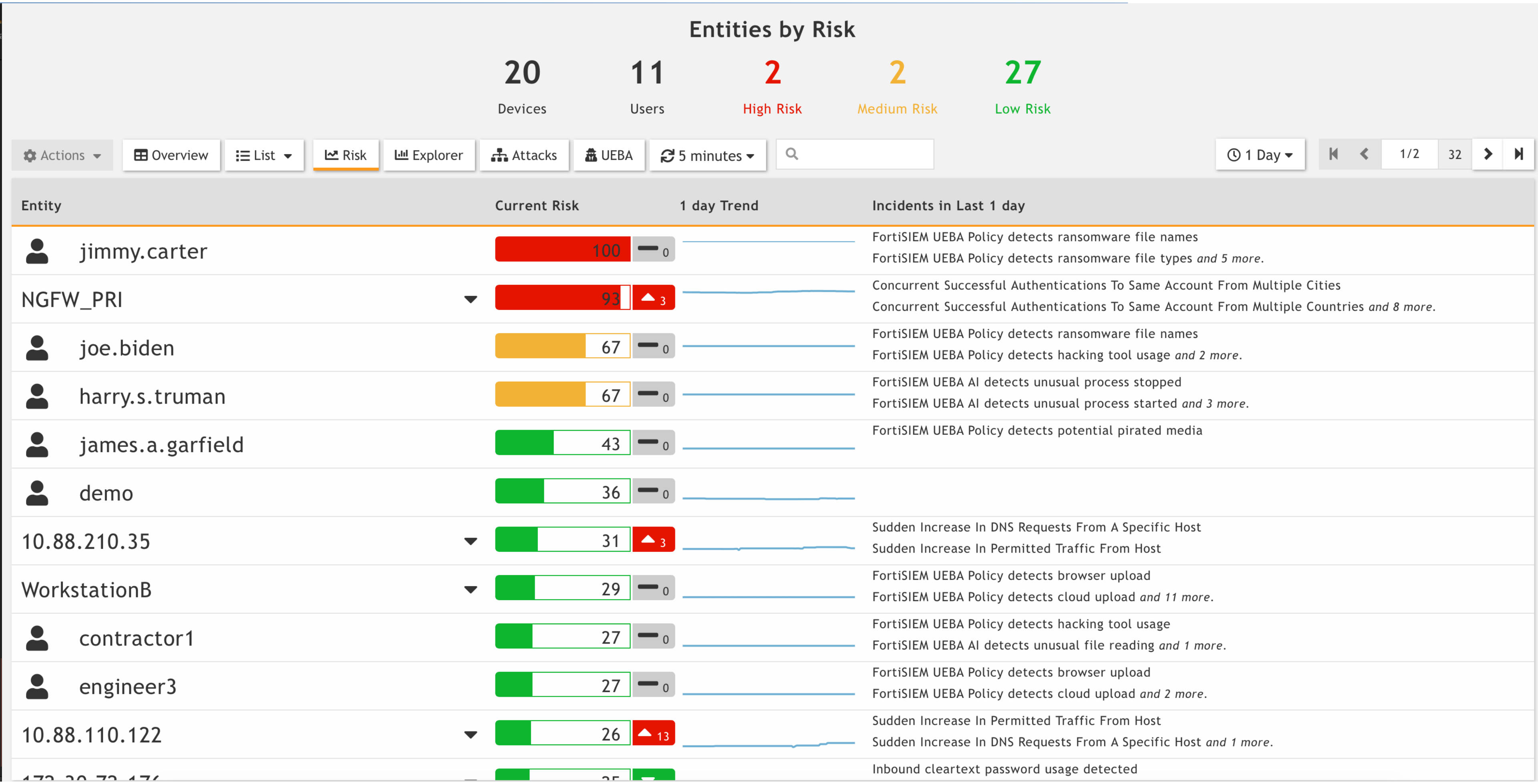
Activity (6/6)	
file written	26
file read	20
file created	11
new process crea...	9
process stopped	3
process started	1

Related Incidents

1/4 70

Severity Category	Last Occurred	Incident	Tag	Host Name	User	Application	Resource	Activity
MEDIUM	Dec 09 2020, 09:07:00 PM	FortiSIEM UEBA Policy detects cloud upload		WorkstationB	engineer3	dropbox.exe	c:\users\engineer3...	file read
MEDIUM	Dec 09 2020, 09:07:00 PM	FortiSIEM UEBA Policy detects removable media write		WorkstationB	jimmy.carter	hncypt.exe	rm:\e:\efi\boot\gr...	file created
MEDIUM	Dec 09 2020, 09:07:00 PM	FortiSIEM UEBA Policy detects browser upload		WorkstationB	engineer3	chrome.exe	c:\corporate\finan...	file read
MEDIUM	Dec 09 2020, 09:07:00 PM	FortiSIEM UEBA Policy detects ransomware file names		WorkstationC	jimmy.carter	outlook.exe	c:\Temp\Outlook\h...	file written
MEDIUM	Dec 09 2020, 09:07:00 PM	FortiSIEM UEBA Policy detects ransomware file types		WorkstationB	jimmy.carter	hncypt.exe	rm:\e:\efi\boot\gr...	file created
MEDIUM	Dec 09 2020, 09:07:00 PM	FortiSIEM UEBA Policy detects ransomware		WorkstationD	exec1		c:\Temp\ukr.net	new process creat...
MEDIUM	Dec 09 2020, 09:07:00 PM	FortiSIEM UEBA Policy detects gaming application		WorkstationD	exec1	steam.exe	c:\Program Files\S...	new process creat...
MEDIUM	Dec 09 2020, 09:01:00 PM	FortiSIEM UEBA Policy detects potential pirated media		WorkstationC	james.a.garfield	wmplayer.exe	c:\us\james.a.garf...	file read

Monitoring from a SOC



Entities by Risk

20	11	2	2	27
Devices	Users	High Risk	Medium Risk	Low Risk

Entity	Current Risk	1 day Trend	Incidents in Last 1 day
jimmy.carter	100 ▬ 0		FortiSIEM UEBA Policy detects ransomware file names FortiSIEM UEBA Policy detects ransomware file types *and 5 more.*
NGFW_PRI	93 ▲ 3		Concurrent Successful Authentications To Same Account From Multiple Cities Concurrent Successful Authentications To Same Account From Multiple Countries *and 8 more.*
joe.biden	67 ▬ 0		FortiSIEM UEBA Policy detects ransomware file names FortiSIEM UEBA Policy detects hacking tool usage *and 2 more.*
harry.s.truman	67 ▬ 0		FortiSIEM UEBA AI detects unusual process stopped FortiSIEM UEBA AI detects unusual process started *and 3 more.*
james.a.garfield	43 ▬ 0		FortiSIEM UEBA Policy detects potential pirated media
demo	36 ▬ 0		
10.88.210.35	31 ▲ 3		Sudden Increase In DNS Requests From A Specific Host Sudden Increase In Permitted Traffic From Host
WorkstationB	29 ▬ 0		FortiSIEM UEBA Policy detects browser upload FortiSIEM UEBA Policy detects cloud upload *and 11 more.*
contractor1	27 ▬ 0		FortiSIEM UEBA Policy detects hacking tool usage FortiSIEM UEBA AI detects unusual file reading *and 1 more.*
engineer3	27 ▬ 0		FortiSIEM UEBA Policy detects browser upload FortiSIEM UEBA Policy detects cloud upload *and 2 more.*
10.88.110.122	26 ▲ 13		Sudden Increase In Permitted Traffic From Host Sudden Increase In DNS Requests From A Specific Host *and 1 more.*
172.20.72.176	25		Inbound cleartext password usage detected

Conclusion

Threat intelligence is knowledge that allows you to prevent or mitigate against cyberattacks.

Rooted in data, threat intelligence provides context like

- who is attacking you
- what their motivation and capabilities are,
- and what indicators of compromise in your systems to look for

This helps you make informed decisions about your security.

ICPAK

Credibility. Professionalism. Accountability

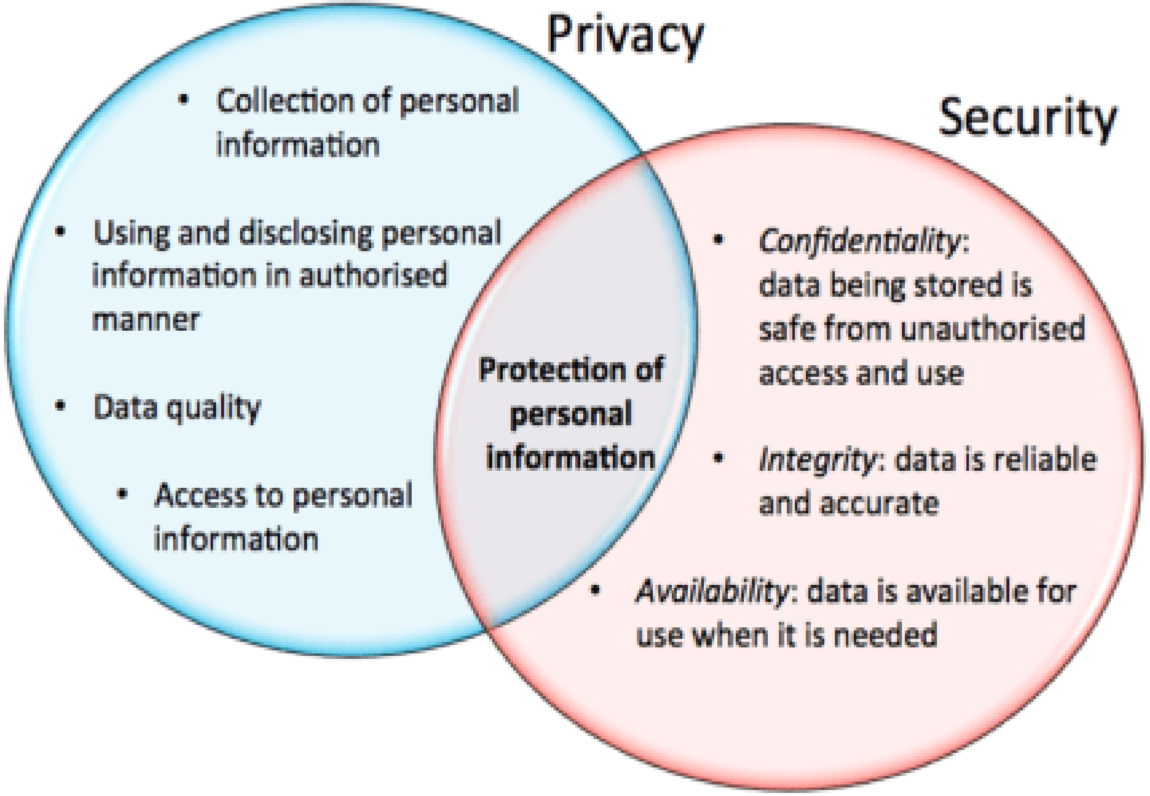
Data Privacy

Presentation by
MUSA WESUTSA
Managing Director, Sentinel Africa Consulting

Data Privacy

Data Privacy is NOT Data Security

Privacy concerns itself with Personally Identifiable Information i.e. with a natural person (Data Subject)



Privacy

- Collection of personal information
- Using and disclosing personal information in authorised manner
- Data quality
- Access to personal information

Protection of personal information

Security

- *Confidentiality*: data being stored is safe from unauthorised access and use
- *Integrity*: data is reliable and accurate
- *Availability*: data is available for use when it is needed

Security concerns itself with information (hard and softcopy / digital) that is of value to an organisation. (Information Asset)

Personally Identifiable Information

Personally Identifiable Information / Personal data

any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier

Special Categories of data

- Race
- Ethnic Origin
- Political opinions
- Religious or philosophical beliefs
- Trade Union Membership
- Genetic Data
- Biometric data
- Health data
- Sexual Orientation

Data on Biography

- Data on Birth
- Marital Status
- Social Security Number
- Criminal Records
- Email Address
- Phone Number
- Residence Address
- Bank Information

Data on Appearance

- Facial Recognition
- Eye Color
- Skin Color
- Hair Color
- Height
- Weight

Data on Education and Job

- Working Hours
- Salary
- Certificates
- Assessments
- Time Tracking
- Tax Information
- Student Number
- Grades

Data on Private Life

- Photos
- Videos
- Messages
- Phone Calls
- IP Addresses
- Browser/Cookies
- Geo-tracking data

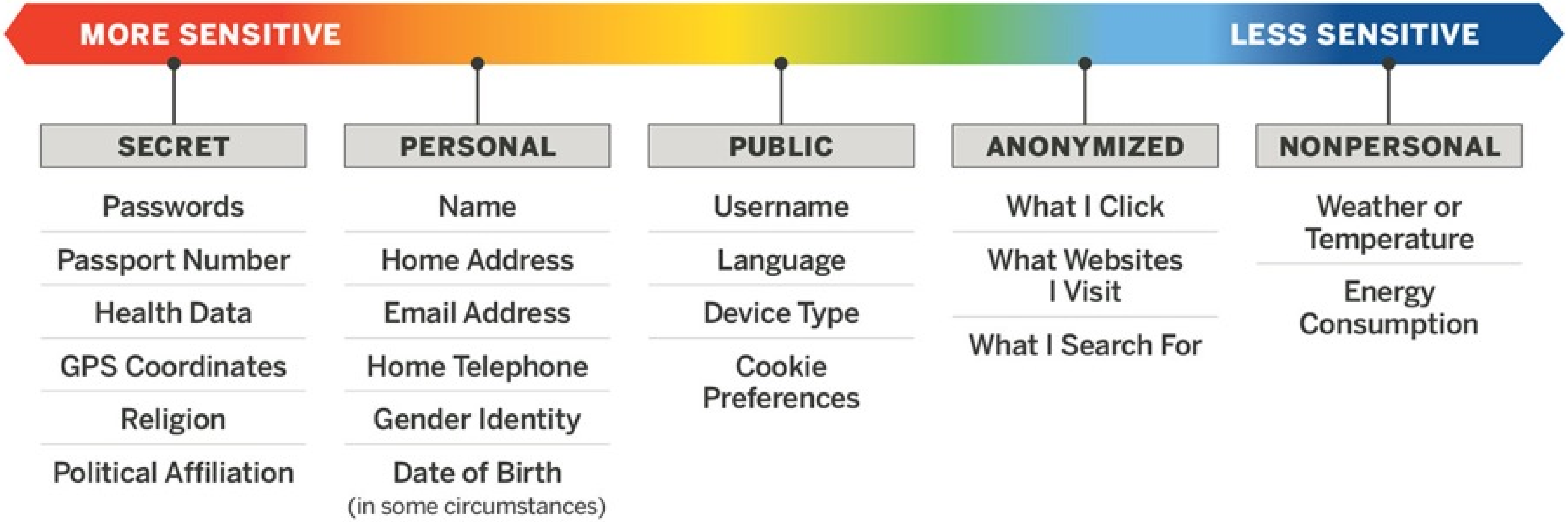
Data on Health

- Information about sick leaves
- Doctor visits
- Medical History
- Genetic Data
- Allergies
- Fitness Data

Personally Identifiable Information

ICPAK

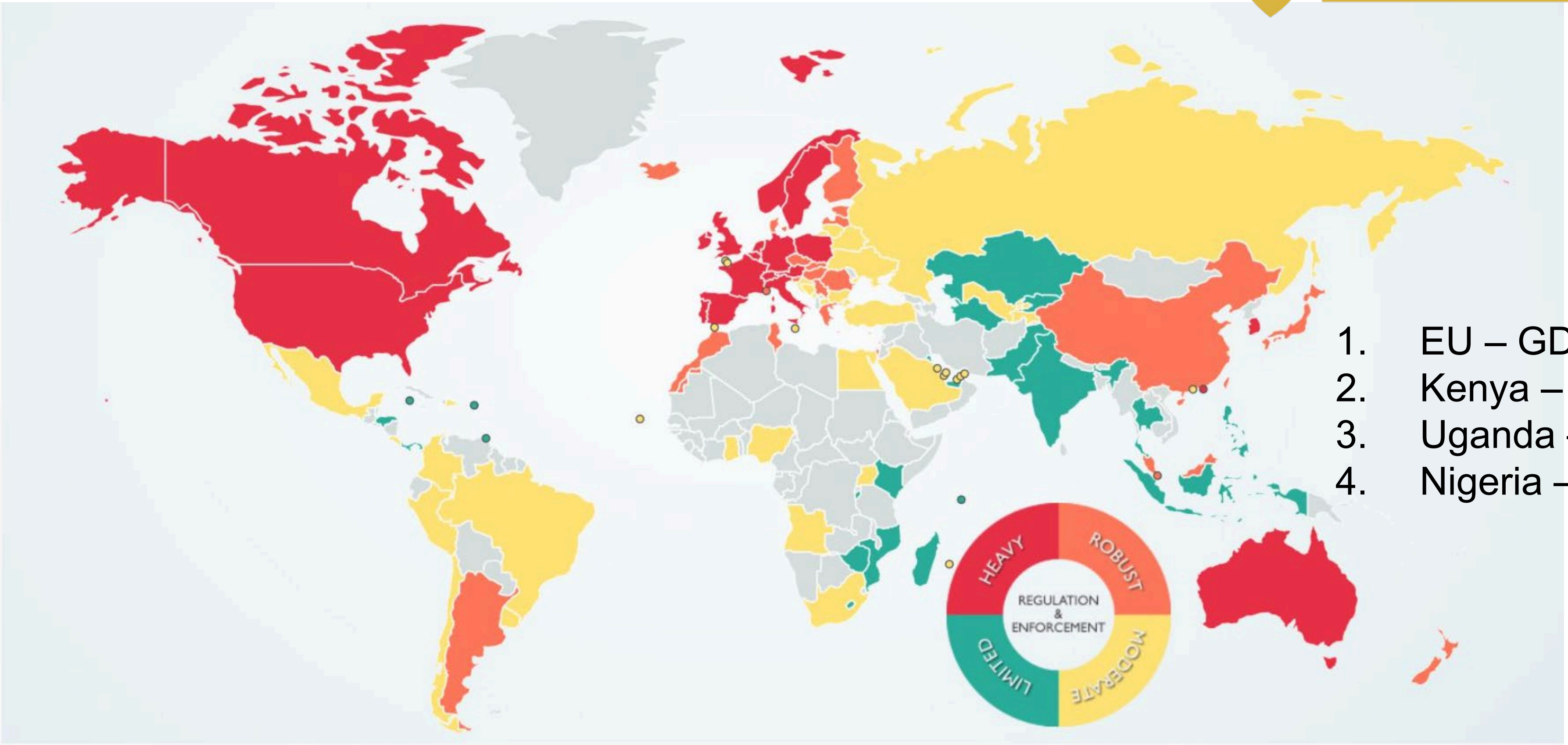
Credibility. Professionalism. Accountability



MORE SENSITIVE — LESS SENSITIVE

SECRET	PERSONAL	PUBLIC	ANONYMIZED	NONPERSONAL
Passwords	Name	Username	What I Click	Weather or Temperature
Passport Number	Home Address	Language	What Websites I Visit	Energy Consumption
Health Data	Email Address	Device Type	What I Search For	
GPS Coordinates	Home Telephone	Cookie Preferences		
Religion	Gender Identity			
Political Affiliation	Date of Birth (in some circumstances)			

Global Reach



1. EU – GDPR
2. Kenya – DPA
3. Uganda – DPA
4. Nigeria – DPR

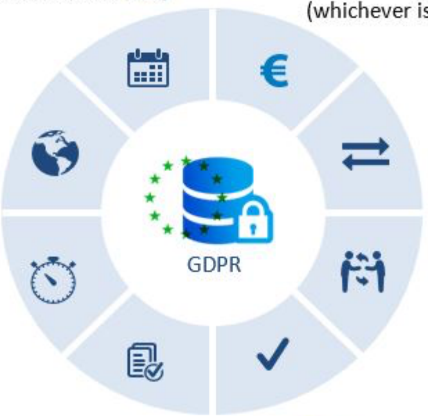
Source: https://www.dlapiperdataprotection.com/

Vision: A world class Professional Accountancy Institute.

GDPR-EU

GDPR IN A NUTSHELL

GDPR constitutes the protection of personal data of employees, customers and others and broadens the rights of individuals with respect to their Personal Data.



Goal: Effective date **May 2018**

Penalties of **up to 4%** of worldwide turnover or €20M (whichever is the highest)

Guarantees that physical persons can **access, modify, restore and erase** their data. **3 to 11 human rights laws** to be passed with a view to compliance.

Collect clear, **informed and provable consent** from individuals.

Secure data against risk of loss, theft or disclosure.

Document the **measures taken** and the protection procedures.

Inform the **National Commission for Information Technology and Civil Liberties within 72 hours** of a personal data breach.

Worldwide scope: all companies that collect, process and store personal data

KENYA - DPA

Kenya Data Protection Law

IN A NUTSHELL

The Kenya Data Protection Law came into force on 25th November 2019 with the aim of promoting innovation and protecting the data of individuals

01 | PART I - PRELIMINARY

Terms and Definitions, Object and Purpose – fails to recognize fairness and transparency, storage limitation, accountability

02 | PART II - ESTABLISH OFFICE OF DP COMMISSIONER

Office and appointment of the Data Commissioner

03 | PART III – REGISTRATION OF CONTROLLERS AND PROCESSORS

Roles of organization, requirements on types of personal data to be processed and purpose, office of the DPO

04 | PART IV – PRINCIPLES AND OBLIGATIONS OF PERSONAL DATA PROTECTION

Principles of data protection, rights of the data subject

05 | PART V – GROUNDS FOR PROCESSING OF SENSITIVE DATA

Grounds for processing sensitive personal data, categories of sensitive data

06 | PART VI – TRANSFER OF PERSONAL DATA OUTSIDE OF KENYA

Data localization, proper safeguards if outside of Kenya

07 | PART VII - EXEMPTIONS

Exemptions to regulations on processing of data e.g. national security, historical, scientific research and archival etc.

08 | PART VIII – ENFORCEMENT PROVISIONS

Administrative fines i.e.. 5 Millions

09 | PART IX – PROVISIONS ON DELEGATED POWERS

Powers delegated to the Cabinet Secretary

Vision: A world class Professional Accountancy Institute.

Data Privacy Concerns

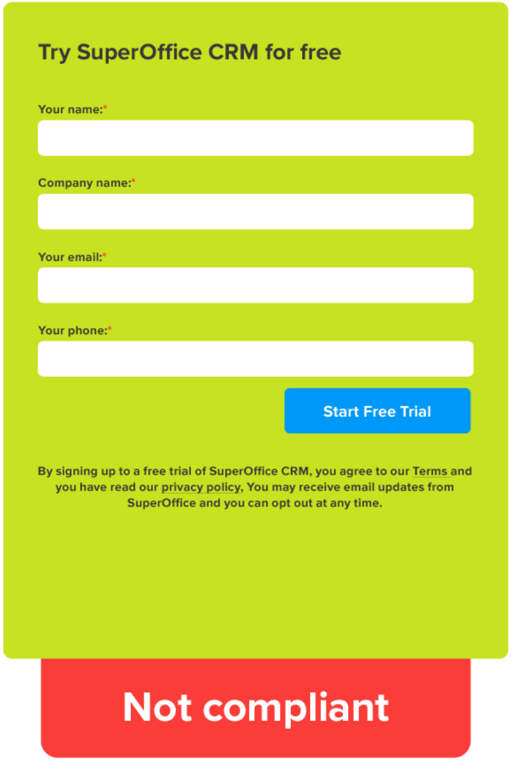
Legal Bases for Processing Personal Data

1. Consent – Consent must be freely given, clear, and easy to withdraw.
2. Performance of a Contract – The data processing activity is necessary to enter into or perform a contract with the data subject.
3. Legitimate Interest – This is a processing activity that a data subject would normally expect from an organization that it gives its personal data to do, like marketing activities and fraud prevention.
4. Vital Interest – This is a processing activity commonly seen in emergency medical care situations.
5. Legal Requirement – The processing activity is necessary for a legal obligation, such as an information security, employment or consumer transaction law.
6. Public Interest – A processing activity that would occur by a government entity or an organization acting on behalf of a government entity.

Data Privacy Concerns

Challenges with Legal Bases

1. There must be only one legal basis for processing at a time, and that legal basis must be established before the processing begins.
2. Whichever legal basis is chosen must be demonstrable at all times.



Try SuperOffice CRM for free

Your name:*

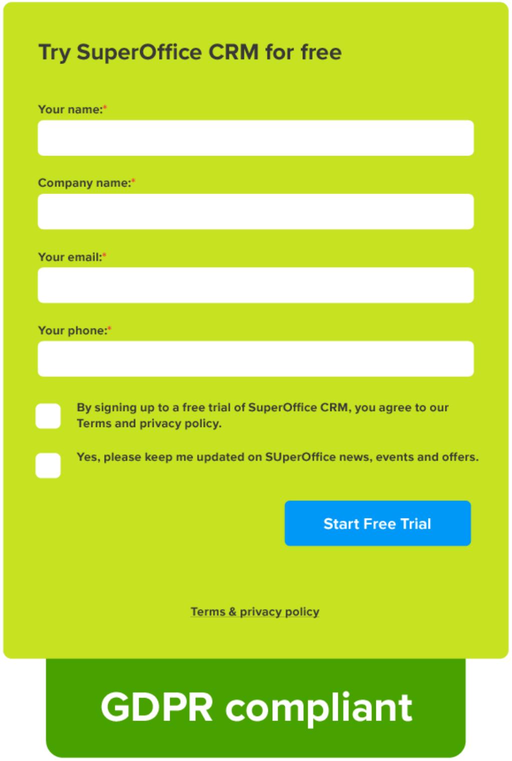
Company name:*

Your email:*

Your phone:*

By signing up to a free trial of SuperOffice CRM, you agree to our Terms and you have read our privacy policy, You may receive email updates from SuperOffice and you can opt out at any time.

Not compliant



Try SuperOffice CRM for free

Your name:*

Company name:*

Your email:*

Your phone:*

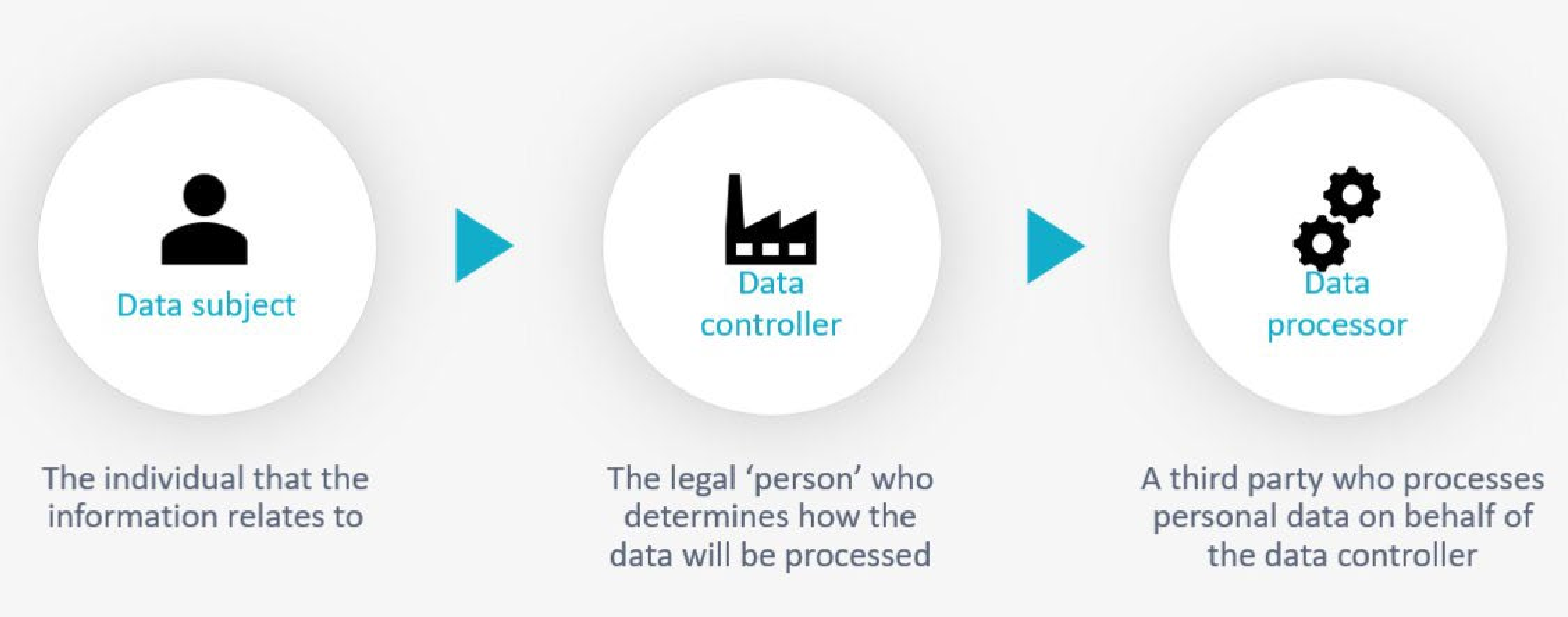
□ By signing up to a free trial of SuperOffice CRM, you agree to our Terms and privacy policy.

□ Yes, please keep me updated on SUperOffice news, events and offers.

Terms & privacy policy

GDPR compliant

Data Privacy Concerns



Data subject

The individual that the information relates to

Data controller

The legal 'person' who determines how the data will be processed

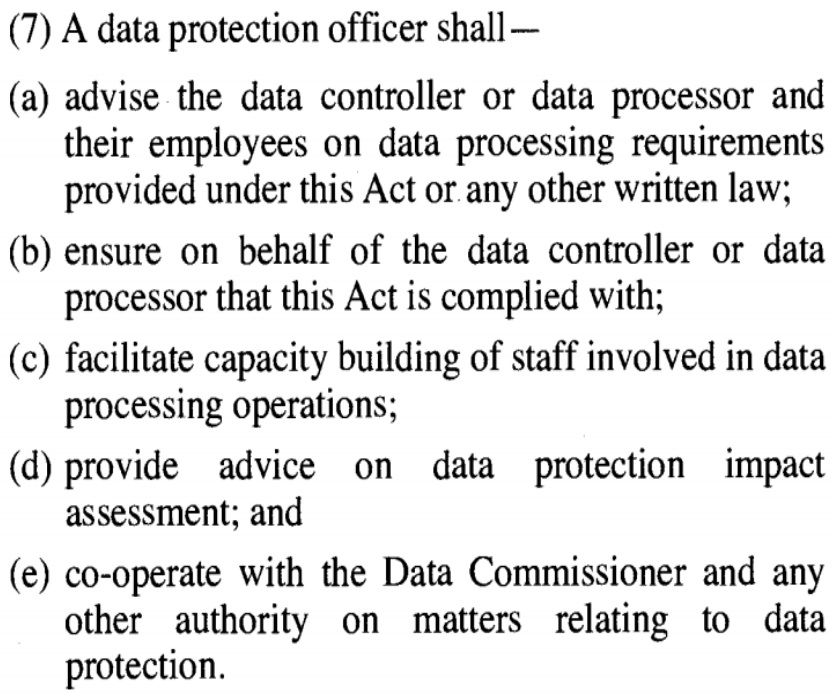
Data processor

A third party who processes personal data on behalf of the data controller

Data Protection Officer

DPO tasklist

- □ Inform and advise people whose work is affected by GDPR
- □ Monitor compliance with GDPR
- □ Oversee data protection impact assessment
- □ Cooperate with supervisory authority
- □ Act as contact point between company and supervisory authority



(7) A data protection officer shall—

(a) advise the data controller or data processor and their employees on data processing requirements provided under this Act or any other written law;

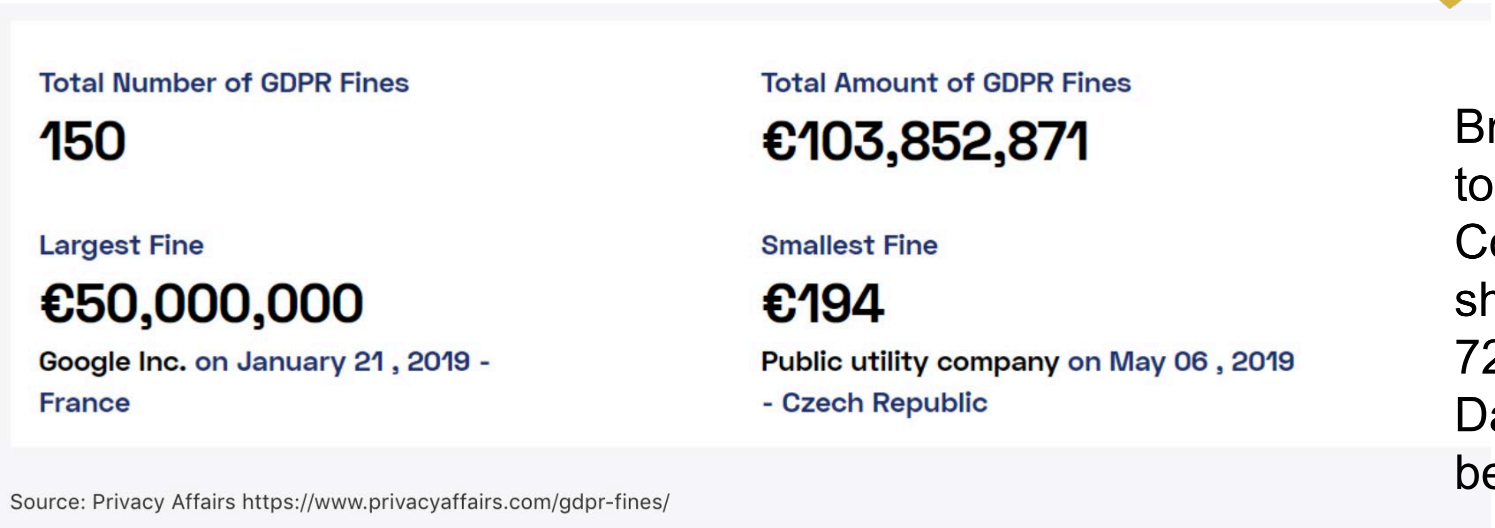
(b) ensure on behalf of the data controller or data processor that this Act is complied with;

(c) facilitate capacity building of staff involved in data processing operations;

(d) provide advice on data protection impact assessment; and

(e) co-operate with the Data Commissioner and any other authority on matters relating to data protection.

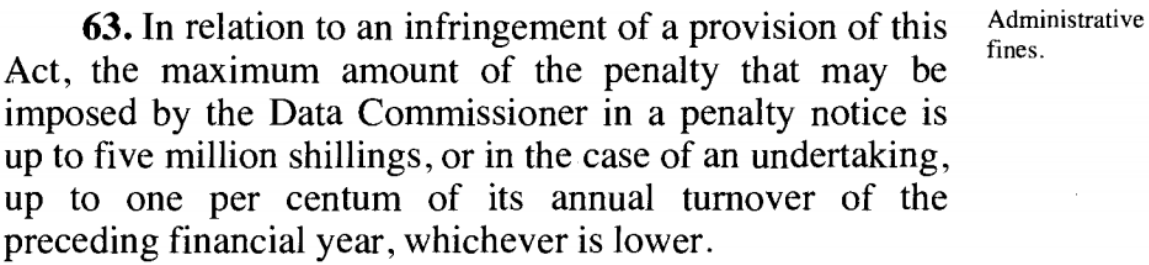
Data Protection Fines



Total Number of GDPR Fines	Total Amount of GDPR Fines
150	€103,852,871
Largest Fine	Smallest Fine
€50,000,000	€194
Google Inc. on January 21 , 2019 - France	Public utility company on May 06 , 2019 - Czech Republic

Source: Privacy Affairs https://www.privacyaffairs.com/gdpr-fines/

Breach notification to the Data Commissioner should be within 72 hours of the Data Controller being aware



Administrative fines.

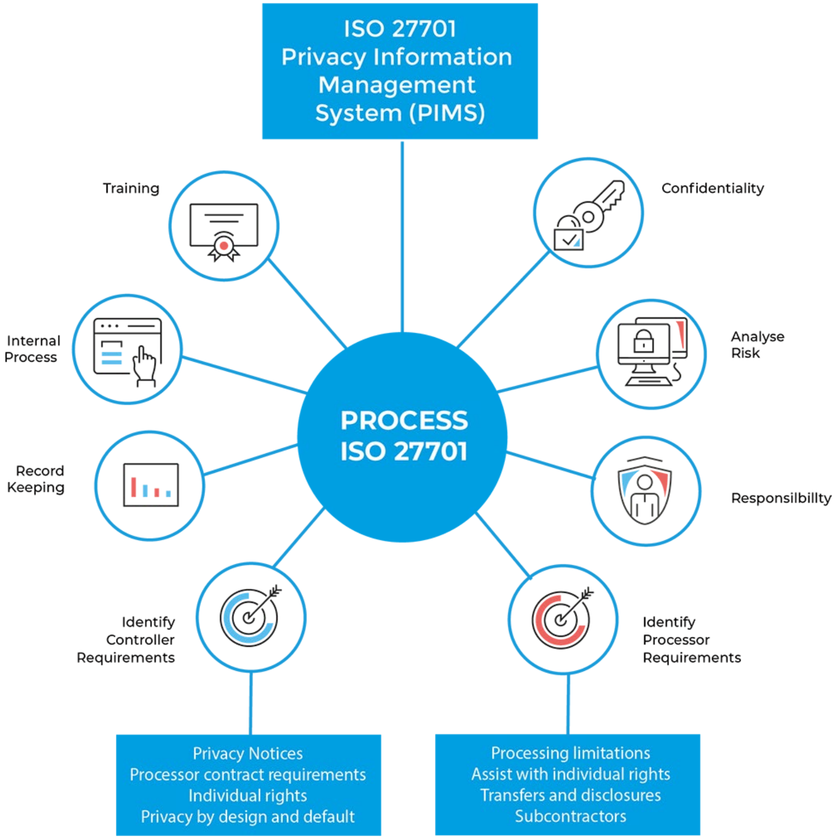
63. In relation to an infringement of a provision of this Act, the maximum amount of the penalty that may be imposed by the Data Commissioner in a penalty notice is up to five million shillings, or in the case of an undertaking, up to one per centum of its annual turnover of the preceding financial year, whichever is lower.

Under the DPA we also have to compensate the Data Subject upto and including for distress and other non-financial losses

Data Protection Compliance

1. Determine first whether you are a Data Controller or a Data Processor
2. Conduct a DPA Compliance Assessment
3. Conduct Awareness (Strategic, Tactical, Operations) and Training (CDPO)
4. Establish and Implement a Framework for Data Protection against a Standard e.g. ISO27701

https://www.dlapiperdataprotection.com/



Questions & Comments

ICPAK
Credibility. Professionalism. Accountability

Vision: A world class Professional Accountancy Institute.

My Contacts

MUSA WESUTSA O'WAKWABI
MANAGING DIRECTOR – SENTINEL AFRICA CONSULTING LTD
5th Flr. RAINBOW TOWER, MUTHITHI ROAD, WESTLANDS, NAIROBI
musa.wesutsa@sentinelafrica.co.ke
+254716572399

Sentinel Africa
Risk Management Consultants

Vision: A world class Professional Accountancy Institute.